Sigma Rule List

Rule Title	Rule Author	Ruleset Name	ID	#Files	#Undetected Files
Autorun Keys Modification	Victor Sergeev, Daniil Yugoslavskiy, Gleb Sukhodolskiy, Timur Zinniatullin, oscd.community, Tim Shelton	Sigma Integrated Rule Set (GitHub)	c654002dc2859e8a2f74ec87ad6ff4deaaf0f42f99603aa964e30ed1b1f01cc1	21401557	53952
Suspicious Run Key from Download	Florian Roth	Sigma Integrated Rule Set (GitHub)	9bc88dec9bf37149ee55ca532e26602ba2ef11e86aa846ab6e0e461f12768b4c	8252741	5330
Stop Windows Service	Jakob Weinzettl, oscd.community	Sigma Integrated Rule Set (GitHub)	9afc79c8a56e6e5c4cbd55d203a7dce8efc4ed28aa315b736c842a88b1d3dd0e	6831397	38789
Net.exe Execution	Michael Haag, Mark Woan (improvements), James Pemberton / @4A616D6573 / oscd.community (improvements)	Sigma Integrated Rule Set (GitHub)	f1048c602439313e72f67c634350106ba7b709512529457a6f0a5eca6835bc89	6451515	35190
Milum malware detection (WildPressure APT)	Ariel Millahuel	SOC Prime Threat Detection Marketplace	30fcf3924a898a9d1747e89068ab2990c77ca3914a94aa78466d28a9d9da32bb	6291968	24
Non Interactive PowerShell	Roberto Rodriguez @Cyb3rWard0g (rule), oscd.community (improvements)	Sigma Integrated Rule Set (GitHub)	1c2e4db94ca79f939e94e29c04fb3b71467fc6f5b9c31db34fcce5a2fb3b856f	3991193	105250
Always Install Elevated Windows Installer	Teymur Kheirkhabarov (idea), Mangatas Tondang (rule), oscd.community	Sigma Integrated Rule Set (GitHub)	b7188ffaa64031d83c409b5110885c29570d52a6ba3bacaee0392371cf071016	3025326	55602
File Created with System Process Name	Sander Wiebing	Sigma Integrated Rule Set (GitHub)	e13498937de9343f50c1e8f315ce602aa238e37e21f3dbb15d3403c25afafe3e	2284944	13926
Windows Processes Suspicious Parent Directory	vburov	Sigma Integrated Rule Set (GitHub)	afd546ea5eff265c454f77f6e7641ade6e5a791d79de155fa27d377be1581535	1851752	92
Shade Ransomware (Sysmon detection)	Ariel Millahuel	SOC Prime Threat Detection Marketplace	d8f0141497fc47a78fbf41591174881fdf0e85f2937b08befec5c6273f8867d2	1673840	16
Suspicious desktop.ini Action	Maxime Thiebaut (@0xThiebaut)	Sigma Integrated Rule Set (GitHub)	cdd5a8ff564f3632d9613d1f4925baca8be40a01fe14c7ba3e30f51bf1ff3829	1397422	161
System File Execution Location Anomaly	Florian Roth, Patrick Bareiss, Anton Kutepov, oscd.community	Sigma Integrated Rule Set (GitHub)	25fc56c1bee673d7ff3edcf371e4d2a36c0af83222da348961b87735c8efa61f	1386967	622
Nibiru detection (Registry event and CommandLine parameters)	Ariel Millahuel	SOC Prime Threat Detection Marketplace	8bbea961d969188574b7fe958c971caadd38b955cc77f21093d7d5d266e4d697	1147667	54640
File deletion via CMD (via cmdline)	Ariel Millahuel	SOC Prime Threat Detection Marketplace	f9333cf120369debd56e4e238fffa10bdb2a1497c11e08a082befd02f9f3bdf2	923890	9083

Suspicious Svchost Process	Florian Roth	Sigma Integrated Rule Set (GitHub)	a0daa529834b3c5230b4524da005a6b6503e7cb061e298a8f74e0dc1fee0a008	845991	133
Windows PowerShell Web Request	James Pemberton / @4A616D6573	Sigma Integrated Rule Set (GitHub)	2637f98feb69311f94822998eb3c8b8d217e6c5767e071536ca54f9da830e236	805020	104
Execution from Suspicious Folder	Florian Roth	Sigma Integrated Rule Set (GitHub)	f8d48ec1128b00975e61e06393f6bb04a1d033a94c556d213b3bcb78a80589d8	643979	5419
Suspect Svchost Activity	David Burkett	Sigma Integrated Rule Set (GitHub)	dc04e64e69f5446c2a31920ee22415626307d5f3d0fb73ad81b9d3301a41000a	568031	87
Direct Autorun Keys Modification	Victor Sergeev, Daniil Yugoslavskiy, oscd.community	Sigma Integrated Rule Set (GitHub)	b5f76af9d8101930af8d4fee71f3a5395b47eff6bb88e581db02bf890242d79b	549037	130
CSRSS.exe spawned from unusual location (possible mimicking) (via cmdline)	SOC Prime Team	SOC Prime Threat Detection Marketplace	c3e407003db6c8b95e5a7dcbea08bddf8b53b265400c2feb32abfa523336257c	531710	11
Swisyn Trojan (Sysmon detection)	Ariel Millahuel	SOC Prime Threat Detection Marketplace	173f49a095aef2bc0480b5f8a8ae6c2d0e4125f9096d618a3865346b34d726fa	494316	108
Suspicious Program Location with Network Connections	Florian Roth	Sigma Integrated Rule Set (GitHub)	01b1cc2515aec2562e5e8cd3c88a60677a1acd2d680b289cf67fa493abe433d2	482076	5335
Scheduled Task Creation	Florian Roth	Sigma Integrated Rule Set (GitHub)	3bc9d14114a6b67367a24df21134d0564d6f08a0ad903d68f9b25e9d8b7f0790	431585	473
Startup Folder File Write	Roberto Rodriguez (Cyb3rWard0g), OTR (Open Threat Research)	Sigma Integrated Rule Set (GitHub)	56b8c79acb8e444c2b00be5c9d3cb8e33e863ccb3506d635f907a49cd053c84f	323029	118
Executables Started in Suspicious Folder	Florian Roth	Sigma Integrated Rule Set (GitHub)	934747e347848f3bf5d2222f0c29c4c6e42831b94a6e0ce77ff40017e5f11fd2	318156	2408
Suspicious Program Location Process Starts	Florian Roth	Sigma Integrated Rule Set (GitHub)	c593fd1eac248d2f05a155e6c8ef2682b9022a12bc03104ff8e9e7c40f585268	315071	2406
Execution File Type Other Than .exe	Max Altgelt	Sigma Integrated Rule Set (GitHub)	2104d1ee1ce64e7aa3dbd368652a54ce160e6a5751019af14601fc8fd1df8086	314199	3369
Possible Applocker Bypass	juju4	Sigma Integrated Rule Set (GitHub)	b9996fdb64c94bd97526744b8287a3b3b02ac4eceff0980c672209adae0be6e5	264915	225
Execution Of Not Existing File	Max Altgelt	Sigma Integrated Rule Set (GitHub)	d2b7b95657238f7c078b9a6a17689a6184c1cf349ffb183b174ad2bd84681b08	264483	3363

Nymaim Trojan (Sysmon detection)	Ariel Millahuel	SOC Prime Threat Detection Marketplace	a9d7fe3dd2aa50123d54b48a488447b37091616c00667ae7c459bf19dd1ad2e0	259838	1
Netsh Port or Application Allowed	Markus Neis, Sander Wiebing	Sigma Integrated Rule Set (GitHub)	7b1f3cd9ca9b55feb5fdd5c8e1821348f2d78745282b41055af44f88df612112	231089	34167
Reg Add RUN Key	Florian Roth	Sigma Integrated Rule Set (GitHub)	aa87efb252a9cf7bb1fb0114336bd08c338bc9046dd498d187c209cd94ddbc6a	212751	94
Suspicious Script Execution From Temp Folder	Florian Roth, Max Altgelt	Sigma Integrated Rule Set (GitHub)	96d2c399118cab5d249093badf4a85f0ef1889872b0191bdf131bcabc0994681	191135	351
Hiding Files with Attrib.exe	Sami Ruohonen	Sigma Integrated Rule Set (GitHub)	5c3ea6806114163b8cdf5735aeb07e702ab63e0e486f721df84cf675e2b0a04b	185112	3217
Suspicious Double Extension	Florian Roth (rule), @blu3_team (idea)	Sigma Integrated Rule Set (GitHub)	5ead81ee12f2097316af35270a1ac0f8623db054349c52ef366fc42a4b7d2de2	178102	89
WScript or CScript Dropper	Margaritis Dimitrios (idea), Florian Roth (rule), oscd.community	Sigma Integrated Rule Set (GitHub)	2020feadc9b3cf47558c219948361d9d3eb5347af91135f21bf711f6032bc817	164507	301
Service Execution	Timur Zinniatullin, Daniil Yugoslavskiy, oscd.community	Sigma Integrated Rule Set (GitHub)	3edfb66bbbe5056c7df0064ed6164a68632d8d476ab015091e0e33f5159d9052	162753	34088
Suspicious MsiExec Directory	Florian Roth	Sigma Integrated Rule Set (GitHub)	709fa572c6d4a06b81742c9cefd264b1debafc1f9b2aedc9798d5cb749d52458	152899	119421
Discovery of a System Time	E.M. Anhaus (originally from Atomic Blue Detections, Endgame), oscd.community	Sigma Integrated Rule Set (GitHub)	18ed38c04ceafb2aa0b9dcb106310ce76cb1473a4109b6a489663f5c250bd2a6	145178	33768
Suspicious ftp.exe	Victor Sergeev, oscd.community	Sigma Integrated Rule Set (GitHub)	89f260c1bb244a6c153a5d3a5951ec6f517e5e846823da8b22d1b5192f798e62	140392	5
HanaLoader (Sysmon detection)	Ariel Millahuel	SOC Prime Threat Detection Marketplace	38853c8efaf750ffd744961ebcbeb037146acaabb9ca85c445af59f87e98e44d	136734	2377
DropboxAES RAT (Sysmon detection)	Ariel Millahuel	SOC Prime Threat Detection Marketplace	8c558244a29064b6842314ce986116d2007b1087f6f8bb45ae883911d0155549	136723	2377
Suspicious Eventlog Clear or Configuration Using Wevtutil	Ecco, Daniil Yugoslavskiy, oscd.community	Sigma Integrated Rule Set (GitHub)	b8f19be4c7bf862dce0d4d1f7885f2207ddf93b3a33d8a6e16f3968c4fbb6491	134152	33764
Root Certificate Installed	oscd.community, @redcanary, Zach Stanford @svch0st	Sigma Integrated Rule Set (GitHub)	80e21a1883c10ba77d6f4a1b0b6903e9ba65d57e1874d2cd81b121f762481c64	133987	33777
Disable of ETW Trace	@neu5ron, Florian Roth, Jonhnathan Ribeiro, oscd.community	Sigma Integrated Rule Set (GitHub)	d85308a28516fa075ee74a4ffd11aea2be1f15add944422ade0969027648a3fa	133800	33759
Interactive AT Job	E.M. Anhaus (originally from Atomic Blue Detections, Endgame), oscd.community	Sigma Integrated Rule Set (GitHub)	c288d5891a082dd1f38d14b832960d7e1b88651dc301c6985be8e66b561bf95d	131707	4

Notepad Making Network Connection	EagleEye Team	Sigma Integrated Rule Set (GitHub)	eebf53f371a18d7f8d6992a935d2fbfe811f3d78552949a0597456693cffd553	131538	1303
Suspicious File Characteristics Due to Missing Fields	Markus Neis, Sander Wiebing	Sigma Integrated Rule Set (GitHub)	608e0e17d25bcba31de608552a073a6677d4f626ab55bce353a686eda3f60bcc	129037	4440
CurrentVersion NT Autorun Keys Modification	Victor Sergeev, Daniil Yugoslavskiy, Gleb Sukhodolskiy, Timur Zinniatullin, oscd.community, Tim Shelton, frack113 (split)	Sigma Integrated Rule Set (GitHub)	d706314122bff93e0dbdf079f1d1904d2f00407f34a893487d70105b1dc5b9ed	123393	3
Malicious payloads that are hidden in fake Windows error logs	Ariel Millahuel	SOC Prime Threat Detection Marketplace	e55945cd70c0ffa247fd76996326089548147e223588b2b6aeef053c1c0ce613	116466	180
New RUN Key Pointing to Suspicious Folder	Florian Roth, Markus Neis, Sander Wiebing	Sigma Integrated Rule Set (GitHub)	27b72c2678411f21ba21bd10b44b7e9c45594d5a5f61f14223b81a8906675039	112716	4928
Renamed Binary	Matthew Green - @mgreen27, Ecco, James Pemberton / @4A616D6573, oscd.community (improvements), Andreas Hunkeler (@Karneades)	Sigma Integrated Rule Set (GitHub)	686a5b6d5e098e507256a7207e9e4a237bb378c824f67f13ee0402525833b257	111591	758
Suspicious Process Start Locations	juju4, Jonhnathan Ribeiro, oscd.community	Sigma Integrated Rule Set (GitHub)	7776601555567f764fc3e22722bef1fdde521b5bdff9fff38f9031e9a3f7ce54	98830	5
File or Folder Permissions Modifications	Jakob Weinzettl, oscd.community	Sigma Integrated Rule Set (GitHub)	d1b3909fc498977f2008254e9e38903c16568e7a8aaaeb2eb0d1d4f155373408	93093	6027
Windows Network Enumeration	Endgame, JHasenbusch (ported for oscd.community)	Sigma Integrated Rule Set (GitHub)	7cb4a3985bd24a137550fa4c49b1da3fb949c3cf182a90950438e97aaad46378	88344	121
SideWinder Ransomware (Sysmon detection)	Ariel Millahuel	SOC Prime Threat Detection Marketplace	1f154d23ec03058edb48ed3380f862daca50719af728e0660a5dc14a5ab5b867	87686	6
FlowCloud RAT (TA410 Campaign)	Ariel Millahuel	SOC Prime Threat Detection Marketplace	159df9b8abe4902ba69f24455a788a64edcec473e20be350469118e1c586299d	87014	225
Suspicious DNS Query for IP Lookup Service APIs	Brandon George (blog post), Thomas Patzke (rule)	Sigma Integrated Rule Set (GitHub)	3a2766a08d32a855b604a786cddc0f76fee13e6ccd22e01d4878150f0ef1eebc	86020	19
Schedule system process	Joe Security	Joe Security Rule Set (GitHub)	02b55b29ddf740930b68c311ca7cd59354f8c35ceda86d09a3fb06f08b760857	85097	8
Suspicious Certutil Command	Florian Roth, juju4, keepwatch	Sigma Integrated Rule Set (GitHub)	f1e311405e4ccc1c99ed8213bdc24b813560700daa47ca78033edd0d8993ba04	80567	33

Regsvr32 Network Activity	Dmitriy Lifanov, oscd.community	Sigma Integrated Rule Set (GitHub)	a9fd3d8b393121d910bdb6416807881b8e231fde412098c46594fc45821d23ce	72807	11342
Regsvr32 Network Activity	Dmitriy Lifanov, oscd.community	Sigma Integrated Rule Set (GitHub)	e7df5abed193d7732536dcfeb0d58fbdfd844ab7c3ddd6186f9afa9ced7a6f61	72807	11342
Windows Credential Editor	Florian Roth	Sigma Integrated Rule Set (GitHub)	8c09b5d8aeac44d4ad6b76333ab77edf4453d9c7f7db00d879591acfc9f98479	72337	2
Maze Ransomware	Florian Roth	Sigma Integrated Rule Set (GitHub)	d807dbfa78ad565695bdfaa5793858aa25a153091a49b554975f48182344c78f	71958	0
CoViper Malware	Ariel Millahuel	SOC Prime Threat Detection Marketplace	17affcf8751489416a8bdd1c7819271220bd9bdd11f595b644b2966c3e3b1b80	70300	176
Compression Utility Passed Uncommon Directory (via cmdline)	SOC Prime Team	SOC Prime Threat Detection Marketplace	f4fe24c510771cfebac8ea12b6e86858e92ee0807f17f8dd0e23e2dc5e1b8049	69677	282
Floxif Trojan	Ariel Millahuel	SOC Prime Threat Detection Marketplace	98d1e74d54870538bf25e55522e0e31814ceaa32679120ff66addce78f4c461d	69390	174
TAIDOOR - Chinese RAT	Ariel Millahuel	SOC Prime Threat Detection Marketplace	e3cdbb4de2c006685f06e358196d7f41ab1098005328b93d9834acae72ddaef0	69031	1384
CLOP Ransomware detection (Sysmon)	Ariel Millahuel	SOC Prime Threat Detection Marketplace	94b16fc40ce61b0527bd124b84d6a631649e579c2c571a3dc68d4f0f9ee4aa76	64529	87
LOLBAS rundll32 without expected arguments (via cmdline)	SOC Prime Team	SOC Prime Threat Detection Marketplace	2fd6d2b16365ba7157eee4934b406ac7d530b4ec62cc1b45c69ee4f07989f139	63006	2241
K8h3d campaign (Sysmon detection)	Ariel Millahuel	SOC Prime Threat Detection Marketplace	2e5a93340aede0794b671d3b3d020fb719a3985e78a96970d36c5c326f2fef34	58981	448
New Service Creation	Timur Zinniatullin, Daniil Yugoslavskiy, oscd.community	Sigma Integrated Rule Set (GitHub)	0e01e0ac3c9d7b292996c00466851ff64ca8e3aabb384b096bddba88aa769464	56999	391
Frat Trojan (Loader detection)	Ariel Millahuel	SOC Prime Threat Detection Marketplace	e5340d719fcf66efd2a0ce9db73895f3154a53e10e72e001760230ca6aa22057	55186	0
LatentBot malware	Ariel Millahuel	SOC Prime Threat Detection Marketplace	f5653d51811614b162ab7311b24033c85bf166bbc322d83f4f72d0b9a366a01f	54554	7424

CARROTBAT Malware detection	Ariel Millahuel	SOC Prime Threat Detection Marketplace	e5937a80eca18cdaa94adaf02b89a4af91bb9605d3236af13685c8b481d9b1b1	53520	6
BackSwap Trojan detection	Ariel Millahuel	SOC Prime Threat Detection Marketplace	a5470af7af21c2bc99ebc438fe841b20ec62f530e6540dc01ce42deed3ffb1eb	53464	2
Suspicious Process Creation	Florian Roth	SOC Prime Threat Detection Marketplace	f09d5248ed8fc1a93251158bfda71f8144ccaf37fa922416ccd897498bff7c55	53350	138
Suspicious Screensaver Binary File Creation	frack113	Sigma Integrated Rule Set (GitHub)	ad081ff821748a3cd86b5954ef5c3d7d2a6602fe0b6e50ed47938b98bc184122	51963	2
Sakula RAT	Ariel Millahuel	SOC Prime Threat Detection Marketplace	1c2774ed7c4cad91219d007aa7101b09d19b442613cd2e3fc453726a7abd1b1a	50916	0
Regsvr32 Network Activity	Dmitriy Lifanov, oscd.community	Sigma Integrated Rule Set (GitHub)	dc313eb40a68f81f4e6cc8b4658215600b2bac992cb67ea873d40ba70e41b7b3	50411	233
CurrentControlSet Autorun Keys Modification	Victor Sergeev, Daniil Yugoslavskiy, Gleb Sukhodolskiy, Timur Zinniatullin, oscd.community, Tim Shelton, frack113 (split)	Sigma Integrated Rule Set (GitHub)	5bddd3dd0944d27f3ff8b03e8a8a01f5a9d14540ea1779da5683fe601557a364	45233	1
Microsoft Office Product Spawning Windows Shell	Michael Haag, Florian Roth, Markus Neis, Elastic, FPT.EagleEye Team	Sigma Integrated Rule Set (GitHub)	6a6edfdea6536f74ea66bf73682ed52f4b86435793ed76ff38e3ab0523f029f5	43326	11
vbc.exe execution.	Den iuzvyk	SOC Prime Threat Detection Marketplace	7f5e752d29abb27ef7222f5171fe6719092aa64cb1a11187e75e3efd277216b3	39753	1
Xmrig	Joe Security	Joe Security Rule Set (GitHub)	c9f2b527fcecda6141fde1caee187052676355bc055141a8caa6c22482fca3ad	38496	2
Suspicious MSHTA Process Patterns	Florian Roth	Sigma Integrated Rule Set (GitHub)	31e1f4457871d51593456a4331811513af82fe4e36d2b26a582dd6baa180a91d	35389	61
Drops script at startup location	Joe Security	Joe Security Rule Set (GitHub)	196a9c9222e3b003ccb0caadc29931d851129ba863f99545299786a032864d12	33944	32
Visual Basic Command Line Compiler Usage	Ensar Şamil, @sblmsrsn, @oscd_initiative	Sigma Integrated Rule Set (GitHub)	5cde8271bb36c24d7ac552a1d30127f3f00a08a681a90eff12e3eac68b72bf47	31223	1
Local Accounts Discovery	Timur Zinniatullin, Daniil Yugoslavskiy, oscd.community	Sigma Integrated Rule Set (GitHub)	ec63f6d5ea6cf1a23c7c491b28d6b350219d23a95ea95516ce0256730fb7912c	28130	367
Powershell Defender Exclusion	Florian Roth	Sigma Integrated Rule Set (GitHub)	7e416af5a1bb67fdbd2f30ae3f5da7f74583460b36546527c909c354fb5dcd00	24546	39

Suspicious Splwow64 Without Params	Florian Roth	Sigma Integrated Rule Set (GitHub)	c4e0758476210a09a3e470db05d2cbec0aebd511e48d351685c75970566f894f	23455	52
Oilrig	Ariel Millahuel	SOC Prime Threat Detection Marketplace	c01baa2540aeb8f23c067318100db0ab3618e37acf7e219372e750398969c606	22856	1687
ChChes Trojan (Sysmon detection)	Ariel Millahuel	SOC Prime Threat Detection Marketplace	a515be8db5d265bf43ba29f21c53f4e482fa0f7db4acc10054e85bc0c516a7ba	22196	1465
Failed Code Integrity Checks	Thomas Patzke	Sigma Integrated Rule Set (GitHub)	134564d292d785dff102940b8a1ee06dba2d462c5fb852124b3771a49d7885f1	20435	77
Suspicious Csc.exe Source File Folder	Florian Roth	Sigma Integrated Rule Set (GitHub)	b39586c79bf4d0d43c937efa6129ebb6f0b2cf03b7038a3a8234f84c147600f7	20269	413
Dot net compiler compiles file from suspicious location	Joe Security	Joe Security Rule Set (GitHub)	76e8bb8877ab40bd84b14fc93daffe9ff7ebe9440ce09916b5c63a302d62c918	19905	302
Pykspa Malware	Ariel Millahuel	SOC Prime Threat Detection Marketplace	daabc950b44baa5580ce5e56de6f2f363ce1854a5273ffd3ac321453e35a83b0	19171	4
PoetRAT detection	Ariel Millahuel	SOC Prime Threat Detection Marketplace	a9e98f5066d90fefc6c08a2a98baaaeecc9dcfccf65c96170128a898353b6d50	18654	1
Scheduled temp file as task from temp location	Joe Security	Joe Security Rule Set (GitHub)	90af0ea1f6d871f169dfb41b18545bf456f980c5d75f60f1293c34f071f6a31c	17165	37
Suspicious Compression Tool Parameters	Florian Roth, Samir Bousseaden	Sigma Integrated Rule Set (GitHub)	9ffd116f512698b4f9b310ee5526625ddf70dc16d7e3a87e744f709c8b537b2e	16633	48
Executable Used by PlugX in Uncommon Location	Florian Roth	Sigma Integrated Rule Set (GitHub)	660cdd939969505754f58fd81c22dc2f313f6b7a8fcfcc55f0a45d62d879734f	16402	17
Windows Suspicious Use Of Web Request in CommandLine	James Pemberton / @4A616D6573	Sigma Integrated Rule Set (GitHub)	f92451c8957e89bb4e61e68433faeb8d7c1461c3b90d06b3403c8f3d87c728b8	16231	53
Suspicious Del in CommandLine	frack113	Sigma Integrated Rule Set (GitHub)	c1c4c35f46055951f3124f8f5791b474f919c9dee2a42d1e737590c5eb7169a4	16109	2
Netsh Program Allowed with Suspcious Location	Sander Wiebing, Jonhnathan Ribeiro, Daniil Yugoslavskiy, oscd.community	Sigma Integrated Rule Set (GitHub)	adbbf1b1fe76c2a86e148fcc66a37c2f361f6d40ce55e510f70409c09d434ea2	16091	36

HVNC Attack (Sysmon detection)	Ariel Millahuel	SOC Prime Threat Detection Marketplace	0643197645f9051600e631515cbe8f526e02ae4556e6125c8f9bf640dcc17849	13490	4
Wmiprvse Spawning Process	Roberto Rodriguez @Cyb3rWard0g	Sigma Integrated Rule Set (GitHub)	1429a6819ff25aad68fb09601fb0b63c4be24919adfd25c4ad925ef8d47d8f22	12984	11
WSF/JSE/JS/VBA/VBE File Execution	Michael Haag	Sigma Integrated Rule Set (GitHub)	8b884f70bb47a8e06faf8f548fcfef77fe3802d22c310c4cdfa01f35cb030bac	12346	118
Dridex Process Pattern	Florian Roth, oscd.community	Sigma Integrated Rule Set (GitHub)	11ef2fbb89770dbec860f554810a4e34a33e1326589f9eaf562412ceba567f00	11688	100
Too Long PowerShell Commandlines	oscd.community, Natalia Shornikova	Sigma Integrated Rule Set (GitHub)	4b2c1a09ad8532fd7bf380feea00e848eb5daf3d246d1f4dac0ef853f29bc01c	10540	28
Suspicious Call by Ordinal	Florian Roth	Sigma Integrated Rule Set (GitHub)	b7eb83db20f6f8b5f580e107c2b6816110a31869a94de5e2797d917335d9fbc0	10444	3184
WannaCry Ransomware	Florian Roth (rule), Tom U. @c_APT_ure (collection), oscd.community, Jonhnathan Ribeiro	Sigma Integrated Rule Set (GitHub)	b8a9a3d755cac11238eb37aa06d272557143560758 72c2e2e140acfb3e8ab8b0	9898	19
XSL Script Processing	Timur Zinniatullin, oscd.community	Sigma Integrated Rule Set (GitHub)	e80db9df819552f83bb1bc542be2503390d7a47f3c26ea4db86797b530411d2c	9806	55
Change Default File Association	Timur Zinniatullin, oscd.community	Sigma Integrated Rule Set (GitHub)	6143134666e4626abac4d906c673c60d7fdb48a48b44f2817af790432cae836f	9599	10
Suspicious WMI Execution	Michael Haag, Florian Roth, juju4, oscd.community	Sigma Integrated Rule Set (GitHub)	29ea4c436137aafe4f4ab08ff716f2a03e416beb0802c5a009cfb266b5d948c6	9567	5
Suspicius Add Task From User AppData Temp	frack113	Sigma Integrated Rule Set (GitHub)	a219a0bf27f7f5f1acdc1fbdd83ff3d3f3711edd5b8111b967d8eb1575aa3b85	9262	14
PowerShell Script Run in AppData	Florian Roth, Jonhnathan Ribeiro, oscd.community	Sigma Integrated Rule Set (GitHub)	4975d97d556849fe2e336bf1c8a5012b84eefe1d4059c527aaa8ec3f903022b2	8899	30
MSHTA Spawning Windows Shell	Michael Haag	Sigma Integrated Rule Set (GitHub)	b9bc90b7745bcb3a2cf9de40d1d419d18ead6650040015c7f4755848e9bfdb05	8438	41
Suspicious Encoded PowerShell Command Line	Florian Roth, Markus Neis, Jonhnathan Ribeiro, Daniil Yugoslavskiy, Anton Kutepov, oscd.community	Sigma Integrated Rule Set (GitHub)	09a6527b05920e47aecbebf5df306d1c194b850076e73d74c3b9ead23b654425	8365	25
Suspicious Rundll32 Activity	juju4, Jonhnathan Ribeiro, oscd.community	Sigma Integrated Rule Set (GitHub)	0d7b38274ada42870a9b5fe59433cc701b21c18ef543b8c653d2e5dae0f93c0e	8215	329
Windows Shell Spawning Suspicious Program	Florian Roth	Sigma Integrated Rule Set (GitHub)	80bbf1ed6106205ab2926430c9634286f976b2fee4357dbacddec45b979a4422	7971	151
FromBase64String Command Line	Florian Roth	Sigma Integrated Rule Set (GitHub)	e75e9983c2277304aa1294c0b077a3139a8405cd1661ccf513a6c05a002acacf	7710	12

Pyvil RAT	Ariel Millahuel	SOC Prime Threat Detection Marketplace	1b78637b79c8dffe83e4631ca8812c2cab4799547d30fb65df21e42f1894053f	7701	136
Suspicious Service Binary Directory	Florian Roth	Sigma Integrated Rule Set (GitHub)	ecf07e5502e8c93b8a8359e6bde14af9098293d382223c0ecf59834a37cac953	7618	5
Mshta Spawning Windows Shell	Florian Roth	Sigma Integrated Rule Set (GitHub)	464455b93d1b76acf868754cca0e609af558267671ad641714ca27a923efb9ba	7370	50
Shadow Copies Deletion Using Operating Systems Utilities	Florian Roth, Michael Haag, Teymur Kheirkhabarov, Daniil Yugoslavskiy, oscd.community, Andreas Hunkeler (@Karneades)	Sigma Integrated Rule Set (GitHub)	ad5e4d4b939797a70a9aa742d979a4742c2cfedddd663fb1a43b2795c1e6054b	7221	4
Windows Defender Threat Detection Disabled	Ján Trenčanský, frack113, AlertIQ	Sigma Integrated Rule Set (GitHub)	baa17a6a8681c2a3d925f497f9c81458eab98535fd28d8909861aece2b9cb901	7020	5
Regsvr32 Command Line Without DLL	Florian Roth	Sigma Integrated Rule Set (GitHub)	c0cdd12b4805f2aebecbc0415332f2594acf1ae6d8d82da086eeac9a84bf0c37	6882	280
MSHTA Suspicious Execution 01	Diego Perez (@darkquassar), Markus Neis, Swisscom (Improve Rule)	Sigma Integrated Rule Set (GitHub)	7a63d1c1bf6ebb277b02d4893066d3732e3d7df562cfdbfee275bbc5c4de0951	6793	74
Highly Relevant Renamed Binary	Matthew Green - @mgreen27, Florian Roth	Sigma Integrated Rule Set (GitHub)	6a0e84509806d4477d42410fb267c817a01015e3dcc33e48330f8db0ba9709da	6695	136
Suspicious Driver Load from Temp	Florian Roth	Sigma Integrated Rule Set (GitHub)	539dcb36e9155d97ed39c68182bde1733b86e2785cbef70586ce6a771645c425	6625	2100
Conhost Parent Process Executions	omkar72	Sigma Integrated Rule Set (GitHub)	7b87fbdccf3c12011b709aab8b9bd4642bd61dc9880e0e1ce9ebb9901e2a3497	6397	102
Imports Registry Key From a File	Oddvar Moe, Sander Wiebing, oscd.community	Sigma Integrated Rule Set (GitHub)	d17374b215c7dec3cfb7a7588c3e1ba10e710be57c03928275fcfd3c65bd187b	6341	208
LOLBAS conhost.exe (via cmdline)	SOC Prime Team	SOC Prime Threat Detection Marketplace	b29d2dfc7edb1018f0384c6a0606a6f59a25bb2e9e1ff8a0fa4bad79d7d4121e	6226	47
Windows Defender Real-Time Protection Disabled	AlertIQ	Sigma Integrated Rule Set (GitHub)	19a5c3cad343931aed1e013cfe07ab95ba7b853ee5b40c6828fc766529e602bf	6140	1
Suspicious Copy From or To System32	Florian Roth, Markus Neis	Sigma Integrated Rule Set (GitHub)	de683a6054ff03b9c12e58c842648f759cfcf797f91dc01078d285e8f3f8e856	5853	49
Windows PowerShell Web Request	James Pemberton / @4A616D6573	Sigma Integrated Rule Set (GitHub)	226bf9a98dfb94416c0f984ecfd7e566a55fd0efe2af4257055b1f1be1501377	5780	65
Suspicious PowerShell Invocation Based on Parent Process	Florian Roth	Sigma Integrated Rule Set (GitHub)	c089503ba0204ebcc3605f01ef3ba76dfff60846f2bad81faf9eae455e81921b	5133	37

Created Files by Office Applications	Vadim Khrykov (ThreatIntel), Cyb3rEng (Rule)	Sigma Integrated Rule Set (GitHub)	5c100e376f43b26c0279b6ecab437d35499a64f73cd9c1b180f62e840eebd2a6	5103	3
MS Office Product Spawning Exe in User Dir	Jason Lynch	Sigma Integrated Rule Set (GitHub)	fb4acb832d8776634f7ad5e60b2ae16c329118186cc8dcf04d1ce959185c6264	5034	2
Windows Defender Threat Detection Disabled	Ján Trenčanský, frack113	Sigma Integrated Rule Set (GitHub)	fd0a272556e2d962e1ecfb8d8fa8ab6f1d728c870db382b0b56dc04e7bf20317	4975	4
Regsvr32 Anomaly	Florian Roth, oscd.community	Sigma Integrated Rule Set (GitHub)	455818bf9dc4423de74cdfa396a0735e0fd29acee7f47632575decb468b11cb5	4795	643
Suspicious PowerShell Parent Process	Teymur Kheirkhabarov, Harish Segar (rule)	Sigma Integrated Rule Set (GitHub)	a4d012f0f7c21ebed94f8e82f4910702fcbcd9d21bf70e4b1b039f48970d1bbc	4774	8
Add file from suspicious location to autostart registry	Joe Security	Joe Security Rule Set (GitHub)	ab2075510415e5fab5635dc30ecec20ea16d6bead9c4397297335c9520922561	4348	1
Windows PowerShell Web Request	James Pemberton / @4A616D6573	Sigma Integrated Rule Set (GitHub)	6291f85314c7d9966be831c56d3cdfb30f42c84f599273e73dac5c95e1122abf	4225	32
Copy itself to suspicious location via type command	Joe Security	Joe Security Rule Set (GitHub)	ca9a79f8e23430115778a41aa4671433713b393278e1a60331cbb991a0f30f82	4222	4
Possible Ransomware or Unauthorized MBR Modifications	@neu5ron	Sigma Integrated Rule Set (GitHub)	388ce51cb79d4deced7fce86e5dcf1e2eec1c04720fb2fc7e451d12abbd53416	4095	578
Shell Open Registry Keys Manipulation	Christian Burkard	Sigma Integrated Rule Set (GitHub)	cd6c2801be2f14154f9616435303948eacedd79025bd0646cb3c34bb536b7cab	4082	2
PowerShell Download from URL	Florian Roth, oscd.community, Jonhnathan Ribeiro	Sigma Integrated Rule Set (GitHub)	24c9049c81b149aa4537cce166e36f3697878dcdad3fab8b662889d154056d7c	4039	41
Suspicious command execution	Den Iuzvyk	SOC Prime Threat Detection Marketplace	2493810bc5072dfb469437cfe4848e404b84ec5690670b79ab60bdf138d06139	3813	0
Glupteba malware detection	Ariel Millahuel	SOC Prime Threat Detection Marketplace	f75c71f7be8a63670e0c606b582900d5a921916b46408da383beb0786cb5588f	3805	0
Bad Opsec Defaults Sacrificial Processes With Improper Arguments	Oleg Kolesnikov @securonix invrep_de, oscd.community, Florian Roth, Christian Burkard	Sigma Integrated Rule Set (GitHub)	53f67594c85a67cef198b525b556658fa4e46d1e49901472adbc8b7f0ba475a8	3627	0

Windows Registry Persistence COM Search Order Hijacking	Maxime Thiebaut (@0xThiebaut), oscd.community, Cédric Hien	Sigma Integrated Rule Set (GitHub)	7f5d257abc981b5eddb52d4a9a02fb66201226935cf3d39177c8a81c3a3e8dd4	3575	2435
Suspicious XOR Encoded PowerShell Command Line	Sami Ruohonen, Harish Segar (improvement)	Sigma Integrated Rule Set (GitHub)	312888984ff0222cd7bd45936afd14feea146948ac0e6941f3e0513e56d51e65	3438	58
Wuauclt Network Connection	Roberto Rodriguez (Cyb3rWard0g), OTR (Open Threat Research)	Sigma Integrated Rule Set (GitHub)	797b0bc9c2136612087c0b95b2f7917f60d1429162e72a7207861e247618dae3	3428	3
Bypass UAC via Fodhelper.exe	E.M. Anhaus (originally from Atomic Blue Detections, Tony Lambert), oscd.community	Sigma Integrated Rule Set (GitHub)	4793e3844bd4ee212795ee4a6bf167b869d51840732845bf0d2aa41f7481e6d7	3398	2
Group Modification Logging	Alexandr Yampolskyi, SOC Prime	Sigma Integrated Rule Set (GitHub)	48fbab3f0d31a3776ce8099e24b7c20af280fc9952c2d83fb8e54e4808a7d506	3379	10
Suspcious CLR Logs Creation	omkar72, oscd.community, Wojciech Lesicki	Sigma Integrated Rule Set (GitHub)	a0cf7d21374ebc3567492775f48033b67b0a81b95521f405e5be52f2950f9d18	3356	204
Xwizard DLL Sideloading	Christian Burkard	Sigma Integrated Rule Set (GitHub)	96b3df20cf0336e4751b0a85d9786ada6ce7185e05988a511f646967e712cc1d	3298	3
Suspicious Process Creation	Florian Roth, Daniil Yugoslavskiy, oscd.community (update)	Sigma Integrated Rule Set (GitHub)	b902e441638f8747df97dc2c59508d1d39ca9ab179b28132c51cee02b1d19152	3239	120
Windows Shell File Write to Suspicious Folder	Florian Roth	Sigma Integrated Rule Set (GitHub)	248820e948efae04f89b524348c8398f0b278befcaec4fafddf73e9c5dda0353	3084	31
Suspicious PowerShell Command Line	Teymur Kheirkhabarov (idea), Vasiliy Burov (rule), oscd.community	Sigma Integrated Rule Set (GitHub)	e6fdb32f143bba16a3ea06247ced55b7b90f8b5b5c6c26ddb95cdcf23908af8a	3002	15
Disable UAC Using Registry	frack113	Sigma Integrated Rule Set (GitHub)	80708cad12d59acde6c91bdfbb0ed867ffd0538e97f962f2ffd72040a66ecb6b	2917	0
Emotet RunDLL32 Process Creation	FPT.EagleEye	Sigma Integrated Rule Set (GitHub)	4e5ef297fadbdf1fbd3c57b71841275af9687495d2f45e59fcbabdba98315434	2792	0
Suspicious Execution of Taskkill	frack113	Sigma Integrated Rule Set (GitHub)	cd06da2f3978bdb24b3f3c8f83c7df917a910c6b29921d0e375e418f340d8f3d	2704	11
Powershell Used To Disable Windows Defender AV Security Monitoring	ok @securonix invrep-de, oscd.community, frack113	Sigma Integrated Rule Set (GitHub)	78a8ebe85ceee09aa63f018db033f8616308e95816c4f7429ba0bafe2d0995b9	2662	1
UNC2452 Process Creation Patterns	Florian Roth	Sigma Integrated Rule Set (GitHub)	f282a8660328d20195770b77f51561e6885408fc2136a6916d0380839cf39301	2610	0

Net.exe User Account Creation	Endgame, JHasenbusch (adapted to Sigma for oscd.community)	Sigma Integrated Rule Set (GitHub)	d83c79bbca4183561b4591dd3ce69faed2e6cfed3217f2658b85c237af7aceea	2600	15
Indirect Command Execution	E.M. Anhaus (originally from Atomic Blue Detections, Endgame), oscd.community	Sigma Integrated Rule Set (GitHub)	949493fff309832e61eefbc1517c38dc21116f3e97310be0dfd27ee7544382e1	2599	2
Suspicious Scheduled Task Creation Involving Temp Folder	Florian Roth	Sigma Integrated Rule Set (GitHub)	c81c0126a6006ad9dbec7215030642dac0a918f133b33aa4c077f9676d84cd58	2592	0
Suspicious Rundll32 Without Any CommandLine Params	Florian Roth	Sigma Integrated Rule Set (GitHub)	87574dead19ceb246e10ccb4cb4fd5009c71c46de0d77965d2170bfafc2c3b14	2575	0
Stealthy VSTO Persistence	Bhabesh Raj	Sigma Integrated Rule Set (GitHub)	c04f755b9283e9e31eead7707a061225ee4da75cf49c91823ff8aa1d7e026551	2535	535
HH.exe Execution	E.M. Anhaus (originally from Atomic Blue Detections, Dan Beavin), oscd.community	Sigma Integrated Rule Set (GitHub)	b0b20b09dd98169c1af4e8643b69d1bbe0cb12c553056b15d64e45d7726ff1b4	2342	514
PowerShell DownloadFile	Florian Roth	Sigma Integrated Rule Set (GitHub)	f0282b9dc90a1761ed8cfb90b52bc5f53c2c8ccbff1ca29790e8d17c7eae56dd	2240	10
Powershell Decrypt And Execute Base64 Data	Joe Security	Joe Security Rule Set (GitHub)	d77da6b7c1a6f6530b4eb82ca84407ff02947b235ab29c94eade944c4f51e499	2100	2
Delete shadow copy via WMIC	Joe Security	Joe Security Rule Set (GitHub)	be6d29855558a0e8c404486d8f1838ce35594866f126f9c1c62a9792e9c76be2	1961	0
Proxy Execution Via Explorer.exe	Furkan CALISKAN, @caliskanfurkan_, @oscd_initiative	Sigma Integrated Rule Set (GitHub)	b32b8c78e20435f731c3241fbfb6354a0b9f86ec81cc5ee202e0f0cf13bf110c	1955	3
Bitsadmin Download	Michael Haag, FPT.EagleEye	Sigma Integrated Rule Set (GitHub)	aca8c04f52d20c1f8ac7c5fda7686124759166ab9439145354e331faaf792bb9	1941	9
Tap Installer Execution	Daniil Yugoslavskiy, Ian Davis, oscd.community	Sigma Integrated Rule Set (GitHub)	47fed78a8bb63a7dee467bd25acd7bbfb704d602012f1a2228eb56c9f6760b7a	1830	161
Shell32 DLL Execution in Suspicious Directory	Christian Burkard	Sigma Integrated Rule Set (GitHub)	fbd6086058f7f1742827e4bf39c6a7b3d7cc32120c2f2cd39a924363da2fe8f6	1770	0
Valak Behavior (Sysmon and Cmdline)	Ariel Millahuel	SOC Prime Threat Detection Marketplace	95388dc52565d97f01bb478463530fac5eb3a7197bbf17fccbd415b4a10a7055	1726	38
Powershell download and execute file	Joe Security	Joe Security Rule Set (GitHub)	1fd2d09eff791a970cc2ad6da0820134ef9d52d4341ab32028edd04e8dd158bd	1722	0
Usage of Sysinternals Tools	Markus Neis	Sigma Integrated Rule Set (GitHub)	35df1aeee1f1078e25bb64a8af513db99a7df8736e4847041fddacedf6b747c9	1656	15

Suspicious Extexport Execution	frack113	Sigma Integrated Rule Set (GitHub)	942c07d4243aed525402c1e4e2f9880b477ba72abc7023c30c9c10737399e077	1644	0
rundll32 run dll from internet	Joe Security	Joe Security Rule Set (GitHub)	232de5bd44720ce2fb34b305f8385e685f63ee5e14d8845368072b2fa100a5f6	1612	245
Nocturnal Stealer	Ariel Millahuel	SOC Prime Threat Detection Marketplace	08655a77d7ea003dba35be4775284dd12a24f9469c9e93ad2d085afe3f4e91d8	1595	14
Suspicious PowerShell Parameter Substring	Florian Roth (rule), Daniel Bohannon (idea), Roberto Rodriguez (Fix)	Sigma Integrated Rule Set (GitHub)	1929e853315b3b5398e0837b2b8928a28ae8eec0611ebb41efc5e6b33e78cd6c	1538	6
Capture Wi-Fi password	Joe Security	Joe Security Rule Set (GitHub)	2e31c80fe0affb3753d7456883282043c5795a0abd5906589d7b67f0eb04076e	1506	5
CMSTP UAC Bypass via COM Object Access	Nik Seetharaman, Christian Burkard	Sigma Integrated Rule Set (GitHub)	a30845acd045e920f165087e59ac6d9461f6c4bfadfa52e4c518e3bcb9d8cb0c	1424	2
Modification of Boot Configuration	E.M. Anhaus (originally from Atomic Blue Detections, Endgame), oscd.community	Sigma Integrated Rule Set (GitHub)	2da0b3cba5dc2b56e1426049598590c54a224e6d15740b9b07c108e089c84520	1409	7
Whoami Execution	Florian Roth	Sigma Integrated Rule Set (GitHub)	4f50c176af3c65d3b67381b2eb36baf45f7c58aa2934ba1b9d94703fb60d977c	1395	102
Esentutl Volume Shadow Copy Service Keys	Roberto Rodriguez (Cyb3rWard0g), OTR (Open Threat Research)	Sigma Integrated Rule Set (GitHub)	e49ec9683ea49e495920eaed6f515ba9a16d6329c30e123a1b7fb158f03004fc	1236	16
Accessing WinAPI in PowerShell	Nikita Nazarov, oscd.community	Sigma Integrated Rule Set (GitHub)	6c44b18934e9ddd288d035d35a258c41fce2d5f5ebafc55ff866a95fb78db9c2	1234	31
Usage of Sysinternals Tools	Markus Neis	Sigma Integrated Rule Set (GitHub)	1e33259c56ec61269739a1b6f2e7e13760703a505f60b194702ff716a6fe0fbc	1225	110
Windows Crypto Mining Indicators	Florian Roth	Sigma Integrated Rule Set (GitHub)	6bbafdf03b2a79de4fa71f3fec777333b907de6172939c7a35b5bed23d4a4b82	1217	1
Rundll32 Without Parameters	Bartlomiej Czyz, Relativity	Sigma Integrated Rule Set (GitHub)	de72fd0fbb1418b8eddde8492f15f221fc84e0ca0d3ca576ccd0ff897fb98037	1202	0
Suspicious Calculator Usage	Florian Roth	Sigma Integrated Rule Set (GitHub)	379786e3d43f4df15525494f022a5e59f58acf961a0f2536f20ae374717a9fa0	1168	13
BlueMashroom DLL Load	Florian Roth	Sigma Integrated Rule Set (GitHub)	fa6fe737f5145762e909801e31b442ca6e73fb112f26179762cd60b5c64a4867	1163	285
Bladabindi backdoor	Ariel Millahuel	SOC Prime Threat Detection Marketplace	f47281ceea7e998eb629b82b6be68c1aaa23f6b18111420b7a52cd72b575f527	1153	0
Renamed jusched.exe	Markus Neis, Swisscom	Sigma Integrated Rule Set (GitHub)	395d81f2cea49ebe846ec75b230f6e7f8ff1541f56a65ee0ca6336a3730a5af3	1153	3

Mshta JavaScript Execution	E.M. Anhaus (originally from Atomic Blue Detections, Endgame), oscd.community	Sigma Integrated Rule Set (GitHub)	f6f3741fe7124168764638673 1e58cbb9eb5dd4b8db836bb 8840c3d02e5462b8	1137	5
LOLBAS rundll32 with unexpected forward slash paths (via cmdline)	SOC Prime Team, @SBousseaden	SOC Prime Threat Detection Marketplace	4df0b9d85eb21989ce009f13 4a8fae2edde67a305237b09a 9daae0c40abae0ac	1128	165
Brontok Trojan	Ariel Millahuel	SOC Prime Threat Detection Marketplace	cc37d2c965977a035bf3e0e5 adc5d1ad561e00eeecc80cde 19feb01566a5fa61	1127	1
Drops fake system file at system root drive	Joe Security	Joe Security Rule Set (GitHub)	4754f502f65f5684ed3a2e0c3 b8615d89d16535a2ad1fe25a c93f82423267ae1	1126	3
Exports Registry Key To a File	Oddvar Moe, Sander Wiebing, oscd.community	Sigma Integrated Rule Set (GitHub)	a5e61828c15a99ec1e32a76e 1f2d9bca2eba0d5d62d10197 c69a8988b85c445a	1093	6
Possible new Cobalt Strike dropper	Ariel Millahuel	SOC Prime Threat Detection Marketplace	3cb32dc8f1ba61964f235761e ac5b49d22264f521e003ce64 1a508eaff8d0eec	1017	48
Cabinet File Expansion	Bhabesh Raj	Sigma Integrated Rule Set (GitHub)	2c33916c73b8057eb865f965 b0e9e05fddeae85fa5405eee 775a7df4cd58173d	1012	18
Hurricane Panda Activity	Florian Roth	Sigma Integrated Rule Set (GitHub)	0595fd00a8b7a34a40b618e9 649d81ef7256ae0a3b3ceefe7 0821decfce1feb7	996	18
Squirrel Lolbin	Karneades / Markus Neis, Jonhnathan Ribeiro, oscd.community	Sigma Integrated Rule Set (GitHub)	556a1aa7c513ecf9a4f6edfb0 176deb074a2cf1447650e017 66fe9efee338c35	985	440
Mimikatz Command Line	Teymur Kheirkhabarov, oscd.community	Sigma Integrated Rule Set (GitHub)	338397ed109954fb8f766d68 49691b20570aadf79c77ac55 09047b25b9af2859	983	10
Schedule REGSVR windows binary	Joe Security	Joe Security Rule Set (GitHub)	c26e0207e75a84b37249afa1 4659448c57c0203d2220e804 9b52775ab00538dc	981	1
RDP Sensitive Settings Changed	Samir Bousseaden	Sigma Integrated Rule Set (GitHub)	c1a07dc6104bfa9dcd638f1c9 f04504dafbbb28fdf3a4f36dc 6af48802194787	959	17
Logon Scripts (UserInitMprLogonScript)	Tom Uelтschi (@c_APT_ure)	Sigma Integrated Rule Set (GitHub)	91fdd3ec700c41d38dcb9127 772f866ad831ade83c48c413 1aee4842d77be561	951	50
Suspicious Process Start Without DLL	Florian Roth	Sigma Integrated Rule Set (GitHub)	d473f1a87cdfa8e30ccefdd18 3b775109bfb012796c04ab06 be794c4b74ba1eb	950	0
Renamed ProcDump	Florian Roth	Sigma Integrated Rule Set (GitHub)	db74c62019a53e7519a73922 15062ee6be4525e5374b419 1fb8eeffc81cb981f	939	28
Tycoon Ransomware	Ariel Millahuel	SOC Prime Threat Detection Marketplace	c2a677a155b0fd75d813c22a 6dc0d1632310c42fafb3c2d5c b08090c75ce491e	933	55

Register Wscript In Run Key	Joe Security	Joe Security Rule Set (GitHub)	530f42d2839f1cd12564a3743f6b294d960920a76da960e2c17e5337c43df9c4	926	1
Suspicious Bitsadmin Job via PowerShell	Endgame, JHasenbusch (ported to sigma for oscd.community)	Sigma Integrated Rule Set (GitHub)	84a714b787a32a4edd32972c4a71a7d66d4a250549ad6c4b1a3faeb077c0bce6	920	10
Schedule CERTUTIL windows binary	Joe Security	Joe Security Rule Set (GitHub)	5afe0a8f1f7fbc102dbeb6382c6e3e9702f05c872dee6c8309d805831b7dbbe2	904	0
Winrar Execution in Non-Standard Folder	Florian Roth, Tigzy	Sigma Integrated Rule Set (GitHub)	99b7b3abf0ce8f702d10cc3f120ed16591df3c13fbda30b46e0623d93cdac439	899	2
Suspicious GUP Usage	Florian Roth	Sigma Integrated Rule Set (GitHub)	e52de558a2f45ea0c3633bf97f5181779246c0964d7003bd012f344221f012ba	860	0
Suspicious Remote Thread Created	Perez Diego (@darkquassar), oscd.community	Sigma Integrated Rule Set (GitHub)	5242ae9a7c0bb9967f443e598ba4d27edfa69ca76b6fbb7ad0d569f7e9067668	859	22
User Added to Local Administrators	Florian Roth	Sigma Integrated Rule Set (GitHub)	534ecedeba777d436d37888757fcae6c00842f791bdcb6c39d8c804ab3c6a535	849	3
Tap Driver Installation	Daniil Yugoslavskiy, Ian Davis, oscd.community	Sigma Integrated Rule Set (GitHub)	20135d843bc80e241d98b14cfdd38a8e122b0a032b2edd8e2dc631c53b5632ca	842	45
Copying Sensitive Files with Credential Data	Teymur Kheirkhabarov, Daniil Yugoslavskiy, oscd.community	Sigma Integrated Rule Set (GitHub)	8712e0baf2cbfba40ac1ad1854da93829b0f78d6eba117de03912aa985d46a79	826	2
WMI Event Subscription	Tom Ueltschi (@c_APT_ure)	Sigma Integrated Rule Set (GitHub)	07b95c7eb376ac65a345dc6a2c1cb03732e085818d93bd1ea2e7d3706619d78e	818	4
DUNIHI Malware	Ariel Millahuel	SOC Prime Threat Detection Marketplace	7c58e06f9c4bfbbca18106234f802a2f21fcd03ca11bcc0d10c040d1e451d4b1	793	0
ScreenConnect Remote Access	Florian Roth	Sigma Integrated Rule Set (GitHub)	29112c1d912aafdd95b322ff1127f1fde6560b1d2e3dc1484d11d9d222af7435	763	8
RDP Registry Modification	Roberto Rodriguez @Cyb3rWard0g	Sigma Integrated Rule Set (GitHub)	7aaf54115e7c0d8450b858520101c04264b58e033da253ad20a672a00b52b5ae	759	15
Local User Creation	Patrick Bareiss	Sigma Integrated Rule Set (GitHub)	8a5a3c45e4c0e75583d9be0aa76f935e9be8f878840cdddb49890be7a65180a6	753	10
DarkSide Ransomware Pattern	Florian Roth	Sigma Integrated Rule Set (GitHub)	5c4ba608ec7db931a6491db14857b098a88caf78b2c28087f16fa4aeeb05c8d0	733	0
Powershell adding suspicious path to exclusion list	Joe Security	Joe Security Rule Set (GitHub)	d933fed60e38128e7e3586361ae42b885a5285e04ab14da997282550a77a9059	732	2
Mimikatz Use	Florian Roth (rule), David ANDRE (additional keywords)	Sigma Integrated Rule Set (GitHub)	62e99f238afed27b43182594e90243db3ec17324c819a349f12ed55c015e5a71	724	0

Tasks Folder Evasion	Sreeman	Sigma Integrated Rule Set (GitHub)	ab8ea26663a3935bd7f1783455f465a74c106836d5a68c19a61dec68dd2596c0	689	0
Modifies the Registry From a File	Eli Salem, Sander Wiebing, oscd.community	Sigma Integrated Rule Set (GitHub)	876619ed554fa68bef3ccfc88d359efb8c1f05d0781e13279ff3c4ff29f4989d	686	13
Windows Credential Editor	Florian Roth	Sigma Integrated Rule Set (GitHub)	2120dcc15751868d99ce91b7721c2a27b2b8b8d542b4621a0ece4594a4cd73b2	671	0
Abused Debug Privilege by Arbitrary Parent Processes	Semanur Guneysu @semanurtg, oscd.community	Sigma Integrated Rule Set (GitHub)	9d455dd5e2e653e4afbec915a896019f9ca31a26fba6e2ba47b2a380780ed090	648	2
AdFind Usage Detection	Janantha Marasinghe (https://github.com/blueteam0ps)	Sigma Integrated Rule Set (GitHub)	1e88d14fe153e2c630eb9bdd7e321d7dc3d82670a31f1b36fc90cb6cbc362136	641	3
Suspicious Rundll32 Setupapi.dll Activity	Konstantin Grishchenko, oscd.community	Sigma Integrated Rule Set (GitHub)	f85bfb745e5bbdd54cf800d8d7e40f16b02685138c13830986a050536d69aa0d	641	159
Verclsid.exe Runs COM Object	Victor Sergeev, oscd.community	Sigma Integrated Rule Set (GitHub)	0cc6e99f887ebd84bef65b69e0c64f654364e79f53cf546f89d1507edd3bbb6b	641	3
CobaltStrike Load by Rundll32	Wojciech Lesicki	Sigma Integrated Rule Set (GitHub)	a92c2c006c3ed7f60668afcb77342db1049d166af7ab991eb0d6cd8c3e2b2a59	628	10
Execute DLL with spoofed extension	Joe Security	Joe Security Rule Set (GitHub)	90c63349e180656f865f6206a06dbee57bd3226b32eb61fba3e6c7c4452d4e1d	614	146
WMI Spawning Windows PowerShell	Markus Neis / @Karneades	Sigma Integrated Rule Set (GitHub)	1ca8739651295d88708cb5ddfb7a115ae0d202152a80ee4c7871e62f3509c938	596	0
NetWire	Joe Security	Joe Security Rule Set (GitHub)	f1f1e749b0e91b9e079a2fb92be3e128291eda84c02064028a1d037f450f864c	589	0
Droppers Exploiting CVE-2017-11882	Florian Roth	Sigma Integrated Rule Set (GitHub)	ea2bef709a3e478516f914938492950992d22f0077ede5a561e60f2c092f4dec	587	0
Powershell Download and Execute IEX	Joe Security	Joe Security Rule Set (GitHub)	317ff64a1d49452191210f7b55d7201e483352440ec851a9c716f6be7cfb7ec9	583	4
Suspicious Listing of Network Connections	frack113	Sigma Integrated Rule Set (GitHub)	90412c9cf799f0ce454d95cf6bdbef8b1264fbcde3cd6b065ae6aee265882a86	580	2
Suspicious PowerShell Keywords	Florian Roth, Perez Diego (@darkquassar)	Sigma Integrated Rule Set (GitHub)	a5f575ade1f2aaba452086d3418d8a893e94b28e30da42ad98b58df4a4fe9c2d	576	13
Tap Driver Installation	Daniil Yugoslavskiy, Ian Davis, oscd.community	Sigma Integrated Rule Set (GitHub)	7bd4ba31d00dc2c285a409cd7939611accc6c2934992f8e9cd0ce8c32ad0c40c	568	15
Logon Scripts (UserInitMprLogonScript) Registry	Tom Ueltschi (@c_APT_ure)	Sigma Integrated Rule Set (GitHub)	eb5ac2a9453d625eabdbb6cd9f3d499dc7ab375f902ebd8f915d5a3d033693ed	565	50

Suspicious PowerShell Download	Florian Roth	Sigma Integrated Rule Set (GitHub)	9e7977461c567e8bfbcdd316661d9ef710694b3de751c6ad76cf0dae3749c57b	559	13
Bypass UAC via CMSTP	E.M. Anhaus (originally from Atomic Blue Detections, Endgame), oscd.community	Sigma Integrated Rule Set (GitHub)	ae5debad574fb4590d5efc9d2e3614bb603a5670f3f9f926a42d2ecbf0de0291	554	3
North Korean RAT - BLINDINGCAN (Sysmon detection)	Ariel Millahuel	SOC Prime Threat Detection Marketplace	6bb61b38bbb774f185f535cafe7a2fc3b848377409dde9963a571d825562c79a	553	1
Register Jar In Run Key	Joe Security	Joe Security Rule Set (GitHub)	a251b526d9024ed7f489fe7b9c2182080e067f2d35068063c5fd326283d9b1ba	544	0
Pass the Hash Activity 2	Dave Kennedy, Jeff Warren (method) / David Vassallo (rule)	Sigma Integrated Rule Set (GitHub)	1e58f3b3a12845dad6be8befe76f8a0368d994ad5b069e672ac85d329bf336ed	523	0
Encoded PowerShell Command Line	Teymur Kheirkhabarov (idea), Vasiliy Burov (rule), oscd.community	Sigma Integrated Rule Set (GitHub)	157d3e7415430b97001871f8aecb592075581e05187450141e56c252318f2b26	522	5
Unauthorized System Time Modification	@neu5ron	Sigma Integrated Rule Set (GitHub)	fd18f89d9ade39f1b15ef9cc31ce8423991e3c873567ec9edc2cb1a45ac79f69	516	2
Suspicious PowerShell Invocations - Specific	Florian Roth (rule), Jonhnathan Ribeiro	Sigma Integrated Rule Set (GitHub)	5d6d29828f1f8db072b666bd85ae7074ac349c49205087a92da4084700e50657	515	12
Suspicious Service Installed	xknow (@xknow_infosec), xorxes (@xor_xes)	Sigma Integrated Rule Set (GitHub)	7cbbf00cea5dc446cd78a75bf887ac0cc4816a0c14fb2fc31cb6c2e5043641e3	513	0
Suspicious Userinit Child Process	Florian Roth (rule), Samir Bousseaden (idea)	Sigma Integrated Rule Set (GitHub)	1170a97b19098b92c7fea421765b81d0cea10e0140d9fed3c4d0769718c4b248	506	0
Application Whitelisting Bypass via DLL Loaded by odbcconf.exe	Kirill Kiryanov, Beyu Denis, Daniil Yugoslavskiy, oscd.community	Sigma Integrated Rule Set (GitHub)	e7b216cf44265cf356b012760fb4e0a6e04289ad81a1fe180bdb6b75c59729a0	487	0
Suspicious Curl Usage on Windows	Florian Roth	Sigma Integrated Rule Set (GitHub)	d86dfee683d0e96803dc8a153d15f7208afc774045e2d885ccaec10bdcef7831	474	27
CMSTP Execution Registry Event	Nik Seetharaman	Sigma Integrated Rule Set (GitHub)	ffeb4d256edb1234faf30da37a584025d92817eb5a21c5394c4c6d78e3922d95	468	5
CMSTP Execution	Nik Seetharaman	SOC Prime Threat Detection Marketplace	58d4fbfb0b53744348e77deba3d12df957601d7b27fda30abc676523e9634cda	460	3
Remote PowerShell Session Host Process (WinRM)	Roberto Rodriguez @Cyb3rWard0g	Sigma Integrated Rule Set (GitHub)	9c155c1f00478f6dbc65e449bb4e1ee8d14ca444d40cbb52bd6406320ff20282	456	0
Query Registry	Timur Zinniatullin, oscd.community	Sigma Integrated Rule Set (GitHub)	218d6661cbefbe4342fb5e6f0aa14df5602a3a39691bb19b246644804e6d341f	448	55

CVE-2021-1675 Print Spooler Exploitation Filename Pattern	Florian Roth	Sigma Integrated Rule Set (GitHub)	873bf5dd3d347e031a1a45c3c7da75768415ed8da25fe6136b24881f29b6ba3b	436	116
Quasar	Joe Security	Joe Security Rule Set (GitHub)	295f36b4fe50737f7d27a3862ea45297f78efdf77ab2decd501b4a852765ceaf	421	0
Suspicious RASdial Activity	juju4	Sigma Integrated Rule Set (GitHub)	c182c186baaff4acc155d390da0732179995f7767ef1710ca041111414a157f6	419	6
Malicious Base64 Encoded PowerShell Keywords in Command Lines	John Lambert (rule)	Sigma Integrated Rule Set (GitHub)	2741e38c5a55999659c8e2ffe6365a21db8ec070e03a5a2f78326209ada99b63	418	3
Suspicious Service DACL Modification	Jonhnathan Ribeiro, oscd.community	Sigma Integrated Rule Set (GitHub)	4e8b6e96f08290c2d17de56622ea6ab96e4e69ac05b74c3f70d52ed74f859533	416	0
Suspicious PROCEXP152.sys File Created In TMP	xknow (@xknow_infosec), xorxes (@xor_xes)	Sigma Integrated Rule Set (GitHub)	b33ac74e3c46a62df1698c5ebafdc2ab3f5907feff6e6ec1f73d273465b4aa5a	403	0
Sticky Key Like Backdoor Usage	Florian Roth, @twjackomo, Jonhnathan Ribeiro, oscd.community	Sigma Integrated Rule Set (GitHub)	bec9d927518cb9af8ee98a6cde08e6a1f05090534e3b3c24e8ced8ae93e15311	402	3
Microsoft Workflow Compiler	Nik Seetharaman, frack113	Sigma Integrated Rule Set (GitHub)	360867571c752aa9ec6da95a6c3db7a37dda60e6627df594f31f89692b8063d0	392	0
LimeRAT	Joe Security	Joe Security Rule Set (GitHub)	667c9dcf6079fd28997e3e2b10b629c8ddbbd7bdffee1889aef6476277791e13	381	0
Taskmgr as Parent	Florian Roth	Sigma Integrated Rule Set (GitHub)	bd4c20ecc3fa26779f917ddf7cd594af5a64805084e11c2a680ade82d77b01ed	370	1
Procdump Usage	Florian Roth	Sigma Integrated Rule Set (GitHub)	c3f48ada664e96b916cbb2ed88c7f622ced143f3f9e2c039bd4516f81e1c1e4a	365	1
Suspicious SYSTEM User Process Creation	Florian Roth (rule), David ANDRE (additional keywords)	Sigma Integrated Rule Set (GitHub)	d0b906c9286d892a8434845afa7551135e37841bdace5aa7fdf1c6bd9a823c73	361	14
Malicious behaviour on user login (Microsoft Windows - c0d0s0 group behavior)	Ariel Millahuel	SOC Prime Threat Detection Marketplace	bf0f7d2a84916abcc597e4a38a6231519b38af0223147ef15e28c7ab83f47c7d	355	6
Renamed PowerShell	Florian Roth, frack113	Sigma Integrated Rule Set (GitHub)	52606fbb97633e0a2c2581ff33bcb2bb212da3c00b02cbf971e5a0aa2f7b4cab	340	4
CMSTP Execution	Nik Seetharaman	SOC Prime Threat Detection Marketplace	7d8b8c88008f45dc07b07590cdf039437686d441d35e7204ba91a632ebc9439c	338	1

Sticky Key Like Backdoor Usage	Florian Roth, @twjackomo, Jonhnathan Ribeiro, oscd.community	Sigma Integrated Rule Set (GitHub)	dd211e6e9cebdae07f1d14d61650061c791829402d134a1a9e064ae72b6c4cd9	337	0
Ryuk Ransomware	Florian Roth	Sigma Integrated Rule Set (GitHub)	38e5073851afbf6c39ea309703c229e83988c6d3548896a389e9ef8795917947	329	0
File Dropped By EQNEDT32EXE	Joe Security	Joe Security Rule Set (GitHub)	4740c645e33c5fbe1595ad953f030f0aa29f78fcbd141282536d02587eb05d0f	327	0
Shadow Copies Creation Using Operating Systems Utilities	Teymur Kheirkhabarov, Daniil Yugoslavskiy, oscd.community	Sigma Integrated Rule Set (GitHub)	16e1527c32b0f67a6b8e3dfaa73ba62c13f73f46a6b0d5962dd823d9ecac933c	327	1
CMSTP Execution Process Creation	Nik Seetharaman	Sigma Integrated Rule Set (GitHub)	4ef4d3aed2ed44386659d6aefb7649de9568189358f367fb8708d1870d19fdc7	318	1
Command Line Execution with Suspicious URL and AppData Strings	Florian Roth, Jonhnathan Ribeiro, oscd.community	Sigma Integrated Rule Set (GitHub)	0585dd5b67e1bced48ad1dc8f9e0b66fd4e44c6e7c14dd5b385950c97e15b768	317	0
Qealler Detection Rule	Ariel Millahuel	SOC Prime Threat Detection Marketplace	2d552bed0d3218f870cdd17abb035a0f71ec2c158035fe612e2476aec61930f4	316	34
Steal Google chrome login data	Joe Security	Joe Security Rule Set (GitHub)	acba408186cae97e9de5ad46ba35ffdf61f94f181c5287bfd9e76aa1e5293b1b	315	0
SecurityXploded Tool	Florian Roth	Sigma Integrated Rule Set (GitHub)	b097e888f96f943b0d94d7835326dbbc76b3cf117fd9407832fbace74cb60f48	311	3
Suspicious aspnet_compiler.exe Execution	frack113	Sigma Integrated Rule Set (GitHub)	c72e2995683af253e803fa2fe4fb02eab21f864cf7e63657b4c1f5a21e5cd421	303	0
TA505 Dropper Load Pattern	Florian Roth	Sigma Integrated Rule Set (GitHub)	e6b2d2b9d4348a8c3ab985832a818688f8ed2f19e9f03c58867656810da91ae4	300	36
RDP Hijacking. RDP port changed.	Den Iuzvyk	SOC Prime Threat Detection Marketplace	a917e763c89ea31922fe3dede8cc03c807a8b52f1a6f9eb0152291fea14c9416	298	1
False Sysinternals Suite Tools	frack113	Sigma Integrated Rule Set (GitHub)	8652ffc2b3174864b7f93e2652bbeaa97cba1ce3a0949c10a85ea086c2478680	292	0
Suspicious Driver Install by pnputil.exe	Hai Vaknin @LuxNoBullshit, Avihay eldad @aloneliassaf, Austin Songer @austinsonger	Sigma Integrated Rule Set (GitHub)	8fd9d688a4929d85f6ba829ccf0fe235ff5f6bcc6ac25306e6425671b81eaa80	286	3
Successful Overpass the Hash Attempt	Roberto Rodriguez (source), Dominik Schaudel (rule)	Sigma Integrated Rule Set (GitHub)	e0a74a014c641b36f56f6bab87d33f003162f1e4a4e97882d055aa0c2fbc4064	285	0
Registry Persistence via Explorer Run Key	Florian Roth, oscd.community	Sigma Integrated Rule Set (GitHub)	1e3577ce99797b69eb40df7b9839ea82c3529cc36c44fdf5f4966c1966c44799	277	0

Suspicious PowerShell Cmdline	Teymur Kheirkhabarov (idea), Vasiliy Burov (rule), oscd.community	Sigma Integrated Rule Set (GitHub)	474582c275339926ac17574ab90c8246d89014d6b66a4312e8e3edb7277ffba0	271	4
Powerup Write Hijack DLL	Subhash Popuri (@pbssubhash)	Sigma Integrated Rule Set (GitHub)	c50b384b3d0f5d468c48abf6ac8fd6095727405ed00d170aeadf0fc1b4add34b	265	11
Spora Ransomware	Ariel Millahuel	SOC Prime Threat Detection Marketplace	4dce473be53cdc44d945acff82c6e5ef53b3304748f9aebc8d4f586230520785	265	45
Lazarus Activity	Bhabesh Raj	Sigma Integrated Rule Set (GitHub)	735c9c8d6f2afa0f395d670a4d21f211de96cbab610a1a63b20bcc981d975f0f	256	36
Emotet Process Creation	Florian Roth	Sigma Integrated Rule Set (GitHub)	ada08103432e4112d167b1d10f0fc02281936c8fcb181de17d5bca07755bac84	242	3
Register DLL with spoofed extension	Joe Security	Joe Security Rule Set (GitHub)	ff70195d476ffa7a3d8e0b1503ffeca1e8707431b00403dfa695732599b571f5	242	14
Suspicious PFX File Creation	Roberto Rodriguez (Cyb3rWard0g), OTR (Open Threat Research)	Sigma Integrated Rule Set (GitHub)	ec56e35983955cbc753846d06d67ba2cf88a10a498711ceb84afe1322ca958a1	238	13
Ryuk Ransomware	Vasiliy Burov	Sigma Integrated Rule Set (GitHub)	1a2c4b1ffc8f65b4edf9020cfc1b6203854d13592539752717c107cd6357489f	231	4
Koadic Execution	wagga, Jonhnathan Ribeiro, oscd.community	Sigma Integrated Rule Set (GitHub)	c5d484cc0502bed15307c6bcc483ba03518aaa99ca3cca09b01da3ea57317777	230	0
CreateRemoteThread API and LoadLibrary	Roberto Rodriguez @Cyb3rWard0g	Sigma Integrated Rule Set (GitHub)	7b3a31059be73d0a2a66f61915b2e5a4f5a37cea4d4de5e3cc8c24f5e2a310f1	228	4
Empire PowerShell Launch Parameters	Florian Roth	Sigma Integrated Rule Set (GitHub)	dae7277357ad237d5dfceb985bdbbaffa777a494f5cab14f067003795d395650	228	0
Office product drops script at suspicious location	Joe Security	Joe Security Rule Set (GitHub)	67124e7349285a993dc331738db576ef56c6cb9724bf1cea7695561498a0fb35	228	6
Mounted Windows Admin Shares with net.exe	oscd.community, Teymur Kheirkhabarov @HeirhabarovT, Zach Stanford @svch0st, wagga	Sigma Integrated Rule Set (GitHub)	816c82737c8262b4f167d02b04198105def46bd23ea282a655786d387e88118c	222	2
Whoami Execution Anomaly	Florian Roth	Sigma Integrated Rule Set (GitHub)	05b85f64fdf521b059aab9daf9d75829fa4a5febd27fe09ac0224e405b57a654	221	10
Suspicious PowerShell Download	Florian Roth	Sigma Integrated Rule Set (GitHub)	2db1db0eb3649cc130ae953a4803853a8ff8e44f3c4a06d42ed49eb3cabfb696	215	5
Operation Vicious Panda (COVID-19 Campaign)	Ariel Millahuel	SOC Prime Threat Detection Marketplace	cf68f11f087c4b3b504b67cb0a9e4a499e486a6de10aee0811ab515d3336d7f1	213	0
PowerShell Deleted Mounted Share	oscd.community, @redcanary, Zach Stanford @svch0st	Sigma Integrated Rule Set (GitHub)	7d4fc33c33fc31d17a2c9ee04cb6e1114c58cbeec3fa2b7cd4f5502b2d28d6ba	211	3

Usage of Sysinternals Tools	Markus Neis	Sigma Integrated Rule Set (GitHub)	c718a898b26d6c8f64602f1b33c49df17864599a9ba4a879a1ac22848dbda174	211	0
Password Filter DLL Modification (Sysmon Behavior)	Den Iuzvyk	SOC Prime Threat Detection Marketplace	cdcaebb2c5505eed7b1cf8cbaff3316fe62d1be1354a3d77d6e25bca67c753d6	210	5
Bad Opsec Powershell Code Artifacts	ok @securonix invrep_de, oscd.community	Sigma Integrated Rule Set (GitHub)	c5b3ab9b3a0221a66b1da487bf7bd851b4f9cf0a8e2b7b22e659e5fd42b40815	209	6
CrackMapExec PowerShell Obfuscation	Thomas Patzke	Sigma Integrated Rule Set (GitHub)	c5f36e07dfb01984d08d19db1fe7f194936f079b371ab900d58eff493b972744	205	1
ilasm.exe execution	Den iuzvyk	SOC Prime Threat Detection Marketplace	382ffab0f18db16a9fabc5be94893af76646b4a1c35d436ba2ae16961943008e	203	0
Windows Webshell Creation	Beyu Denis, oscd.community	Sigma Integrated Rule Set (GitHub)	a52a436bb2117d8c22878afc1facac963ffa5feca0046433c94396c44991c948	195	40
Always Install Elevated MSI Spawned Cmd And Powershell	Teymur Kheirkhabarov (idea), Mangatas Tondang (rule), oscd.community	Sigma Integrated Rule Set (GitHub)	742d7b1dbef016ab3810ec50354e231948fa035c8cacfec6b18f3a8fba03c2dc	191	15
UAC Bypass Tool UACMe	Christian Burkard	Sigma Integrated Rule Set (GitHub)	3c4f6f1af78c01c8d7d6fcdd27c3167044933fcdf73f667e973ce1068765ea16	191	0
Malicious PowerShell Commandlets	Sean Metcalf (source), Florian Roth (rule), Bartlomiej Czyz @bczyz1 (update), oscd.community (update)	Sigma Integrated Rule Set (GitHub)	bbb841b3f1cb3bdb122737ca0755cb93d982ecca4651de2822af469b59071f87	190	10
DUNIHI Malware	Ariel Millahuel	SOC Prime Threat Detection Marketplace	4e8573bf949d0f277bff56a18b256181b950262693a43cfad1d247e035aec8b5	178	0
Check external IP via Powershell	Joe Security	Joe Security Rule Set (GitHub)	4b3ac3a4fac3672c92791075c26f1e10555eb3385628b923bccd8cbbd5dc83a1	174	0
MSBuild connects to smtp port	Joe Security	Joe Security Rule Set (GitHub)	86905c36f5c4e855311f702723eec0c6a4dc9e9992fcec9b2ddcce685b7c2e09	169	0
Malicious PowerShell Keywords	Sean Metcalf (source), Florian Roth (rule)	Sigma Integrated Rule Set (GitHub)	5bd56545b7e384edee75e378b7ee025e05f6bcb012607cb6425ccedd54fdb070	159	9
Powershell Reverse Shell Connection	FPT.EagleEye, wagga	Sigma Integrated Rule Set (GitHub)	1b46ecd9aa9660208e7f7cbb3e4ad79d7fc469adb5c2c5dc81af712ebce9b80c	159	6
Covenant Launcher Indicators	Florian Roth, Jonhnathan Ribeiro, oscd.community	Sigma Integrated Rule Set (GitHub)	2957c0808592ab632134afd63650be8c47697a8350bb5cb19a8272b9da595777	156	0
NjRat Detection Rule	Ariel Millahuel	SOC Prime Threat Detection Marketplace	44649563045e4b39ea5ec24c20ca7aa44cde80384aa9b3de04a8bb30862d934e	156	0

Usage of Sysinternals Tools	Markus Neis	Sigma Integrated Rule Set (GitHub)	c2020adce966e19fbcd161d9dfee7f79c0db26018d089ec95e78e41a583fe0bd	154	10
Copy from Admin Share	Florian Roth, oscd.community, Teymur Kheirkhabarov @HeirhabarovT, Zach Stanford @svch0st	Sigma Integrated Rule Set (GitHub)	253df726683ee378cff180cb32526ec9f10b897edda084113b11cbeba118fbe3	152	0
Suspicious exeplorer.exe execution	Den Iuzvyk	SOC Prime Threat Detection Marketplace	2f0a10e6befc35eb8cf3d8af89b1db1a84a53b5aff114a90c2d1b0a3a697d1ac	152	4
Reg Disable Security Service	Florian Roth, John Lambert (idea)	Sigma Integrated Rule Set (GitHub)	0c3e5c376a4a569ab4a4f3217dd009bb34e695e5fa82da85111db47f2b801bc9	151	2
Office Applications Spawning Wmi Cli	Vadim Khrykov (ThreatIntel), Cyb3rEng (Rule)	Sigma Integrated Rule Set (GitHub)	58a51088691ea6b0bb320e61f961a96216f54913353095e97a5b5c6e94ce74fa	144	0
Use of CLIP	frack113	Sigma Integrated Rule Set (GitHub)	d1138c20627ece208ac948647342866415641b06510830449eb2bf7d2f32e4af	144	0
Detect Virtualbox Driver Installation OR Starting Of VMs	Janantha Marasinghe	Sigma Integrated Rule Set (GitHub)	3cbde0faee76f7509cfde702c1c324a83ac88cb58f0e0f74b2682a9b60369b1e	143	2
Regsvr32 Flags Anomaly	Florian Roth	Sigma Integrated Rule Set (GitHub)	0febc469c613c6ae3155a46fb291f1ebf74d38c09b1dbb5478c2f9f36af7b599	142	6
Trickbot Malware Activity	Florian Roth	Sigma Integrated Rule Set (GitHub)	1c7a83aaaaf300f7e44e597465797c7e812cc0c684756d1be37d0ac7acf0dc5c	141	0
Run temp file via regsvr32	Joe Security	Joe Security Rule Set (GitHub)	c70694dd88c0a5a32ad8a52ef4ad97a6525c281308ba84e791661580aab19264	140	17
MZRevenge Ransomware	Ariel Millahuel	SOC Prime Threat Detection Marketplace	aa09c929bbf92e934dc584324a80a81643f2c336dba38293142077f86bdde84b	139	25
Suspicious comandline paramethers(shellcode in the command line)	Den Iuzvyk	SOC Prime Threat Detection Marketplace	c6bf20aec5b9dd748265363c7d01846ca0a5fc666f1114770a8bb7f5e764e4e2	139	5
Possible Shim Database Persistence via sdbinst.exe	Markus Neis	Sigma Integrated Rule Set (GitHub)	f228d8546016f76e5942e38208fa8a55735339d54ec3f56e63b2b9133b037a7c	134	2
Delete Shadow Copy Via Powershell	Joe Security	Joe Security Rule Set (GitHub)	d91fb994dcf44dbdd52950e6db5cdf99eba912926494deb2f92f3f2dbf232740	131	0
Malicious PowerShell Commandlet Names	Markus Neis	Sigma Integrated Rule Set (GitHub)	a76fa0f689961152a23aa5f209a6af1314317a976fc0ce87fc515430cd043c5a	131	2

Exfiltration and Tunneling Tools Execution	Daniil Yugoslavskiy, oscd.community	Sigma Integrated Rule Set (GitHub)	6ba70df29bf2469a0e7931226da06a144c5e9044543a14e1fae2bcd6c17f9374	129	1
Finger.exe Suspicious Invocation	Florian Roth, omkar72, oscd.community	Sigma Integrated Rule Set (GitHub)	7014c2ce26877573641173ba99dcd8d8af4f637986c42be19651a8a37c5ead6f	129	0
UAC Bypass via Event Viewer	Florian Roth	Sigma Integrated Rule Set (GitHub)	1d6ad51b3643427cc3820debc181e8c8a71afff1bee8642632fd392fde905cf6	128	2
UAC Bypass via Event Viewer	Florian Roth	Sigma Integrated Rule Set (GitHub)	d37f057d76500ae8527178a9ea367395f2bde798f1cd048621be74f915b28aa7	128	0
Fsutil Suspicious Invocation	Ecco, E.M. Anhaus, oscd.community	Sigma Integrated Rule Set (GitHub)	4b8a086b898ff9eb51b0489b98e2619d0c9fe2cd94e29325ec8a4c2250220b8e	127	0
Lokibot Detection Rule	Ariel Millahuel	SOC Prime Threat Detection Marketplace	be942c1d0e5d410fdd49ca407572405db53d2cebec6927a56b86b1bf02d58983	126	0
Suspicious Curl File Upload	Florian Roth	Sigma Integrated Rule Set (GitHub)	63ca787b0e9b439877ff859851c650e60a39c37447b6c96420cafc38d94331db	123	7
Vulnerable Dell BIOS Update Driver Load	Florian Roth	Sigma Integrated Rule Set (GitHub)	10577bdb5cec4b94b7c1d5ddcb04041555da105e518503133907d995a05c68dee	123	18
Removal of Potential COM Hijacking Registry Keys	Roberto Rodriguez (Cyb3rWard0g), OTR (Open Threat Research)	Sigma Integrated Rule Set (GitHub)	85b8f7bd2db84db2632bf9e5b9b9402e829785f546868fe1a62c7a6002a6eb60	122	1
Raccine Uninstall	Florian Roth	Sigma Integrated Rule Set (GitHub)	ce4fb10349cd95756b2f98a27b259d71c99ec9e0323815f2e916737fcbd1d4ba	120	0
Remove Windows Defender Definition Files	frack113	Sigma Integrated Rule Set (GitHub)	bde07bc9414d410eaf67f99408a24b51b4b8d186451e641a9a90076cfac22613	120	0
Suspicious WMI Execution Using Rundll32	Florian Roth	Sigma Integrated Rule Set (GitHub)	97abad7c8edb5cdf286b45712f14b577d1653fa738d3d330a0473a1d48e5aac4	120	0
Netsh RDP Port Opening	Sander Wiebing	Sigma Integrated Rule Set (GitHub)	0edbdff715350e06427add8d168d0d14de79ec048ea17f4a243589e2ccdc63df	119	3
Renamed SysInternals Debug View	Florian Roth	Sigma Integrated Rule Set (GitHub)	1de55c288a6fd75ce590378bcc3b9bf02a66b8d45de5928d17d08339f5182586	119	2
Socelars Malware (Sysmon detection)	Ariel Millahuel	SOC Prime Threat Detection Marketplace	3b19facf348c1fe8db660733298928cb749e5dafe84ca3025f86b31129352e51	119	0
credwiz.exe DLL side loading	Den Iuzvyk	SOC Prime Threat Detection Marketplace	d83f2abd95409ecc8fb4d4930072a48b4a677def3d31b022a95e99d5873fc27a	117	1

Ramsay Malware Behavior	Ariel Millahuel	SOC Prime Threat Detection Marketplace	9a24e548df204cab86a6489b32a696d4f00e8933893536c518bc73e457c7f3a0	116	0
Suspicious Scripting in a WMI Consumer	Florian Roth, Jonhnathan Ribeiro	Sigma Integrated Rule Set (GitHub)	aa9824d65395eec625b665851ca4456503a8111e058eab9487c34500b30ee31f	115	0
Suspicious Use of Procdump	Florian Roth	Sigma Integrated Rule Set (GitHub)	bf45bfecf2446b7f2b7904bc35a7006ea9bfae3e8ba4d6ab35dfcb00095b0b9d	115	17
Lazarus Session Highjacker	Trent Liffick (@tliffick), Bartlomiej Czyz (@bczyz1)	Sigma Integrated Rule Set (GitHub)	d945c7338838af1692c329f71f0503023380291272 81ca66006ba926c9a9d854	114	0
Logon Scripts (UserInitMprLogonScript)	Tom Ueltschi (@c_APT_ure)	Sigma Integrated Rule Set (GitHub)	72753d1df5ca47138f6ac3de80cfbfccccb39052c6331addbb419e2b4a2f9752	113	0
Renamed PsExec	Florian Roth	Sigma Integrated Rule Set (GitHub)	d266707276cd7f46b3d33b3a78f17f69e9160d8f795bf07d8c7020b49aad1da3	113	4
Command Line Path Traversal Evasion	Christian Burkard	Sigma Integrated Rule Set (GitHub)	2a64ca949e5ce433b70a21b4be0e71e5ad0cd2465395fd093410ce2d33177cdc	112	0
North Korean RAT - BLINDINGCAN (Sysmon detection)	Ariel Millahuel	SOC Prime Threat Detection Marketplace	e8ccfecc9a57c342fda105daa1ce14b8913cb320d668dec39aa2e246fd6edbe7	111	0
Kill multiple process	Joe Security	Joe Security Rule Set (GitHub)	868e81758b31ab7d5c37adbd3798dbc1effacb9eeaad44e5f6c5f41c409fb786	109	0
Stop multiple services	Joe Security	Joe Security Rule Set (GitHub)	2319d1843957b572c6e41e1d83656e12eac1e5e75f59ac1ccc309c2b00e9ef86	106	0
Registry Persistence Mechanisms	Karneades, Jonhnathan Ribeiro	Sigma Integrated Rule Set (GitHub)	94ec0949b00016f88171e5d46125aad5bcbd3980d50085c2ae009dcd34e39190	105	11
Suspicious Shells Spawn by Java Utility Keytool	Andreas Hunkeler (@Karneades)	Sigma Integrated Rule Set (GitHub)	b7e93e0475f0c46a1c6bfd3f1f401e0a34bb9c8d73e2308101ed1368b5189de0	103	0
Writing Of Malicious Files To The Fonts Folder	Sreeman	Sigma Integrated Rule Set (GitHub)	50cc064f594178311fd316bf296afdcb85c962c45cbc15ab0984ca5de2940d67	101	0
Firewall Disabled via Netsh	Fatih Sirin	Sigma Integrated Rule Set (GitHub)	5a783ec4b26d8a6276f21c1226c5896266e2591f44f079ca9950892310b00429	99	2
VSSAudit Security Event Source Registration	Roberto Rodriguez @Cyb3rWard0g, Open Threat Research (OTR)	Sigma Integrated Rule Set (GitHub)	82ec398800a85ecb732c915486c59e1a4abe901700e658ccab6308f47245e33e	99	1
Curl Start Combination	Sreeman	Sigma Integrated Rule Set (GitHub)	78dc71a5599dc85b3d37a6ab0f014aa5110b2ce1b2346c8f2730e0c481977781	98	2
Advanced IP Scanner	@ROxPinTeddy, Nasreddine Bencherchali @nas_bench	Sigma Integrated Rule Set (GitHub)	eba28e9e2b6ff9e170e3534ea8b1e863757d5c976a9a84e4bbf5bd6ffeea5325	97	57

Shedule hidden powershell script	Joe Security	Joe Security Rule Set (GitHub)	9277300d8dfe7cfc29e41129553c4d7c59c4b709d4b1716c8fe9cc037c9bc29d	94	3
SoreFang Malware (Sysmon detection)	Ariel Millahuel	SOC Prime Threat Detection Marketplace	ef69867dec66e047e8894803bca76813e63b7a2f0d2bc6938e903f4accf5ae76	94	16
Bloodhound and Sharphound Hack Tool	Florian Roth	Sigma Integrated Rule Set (GitHub)	cfc47087b4c2d98cee5d80b1383b55212d8fe298ebc880e15c894f55123fa95a	93	0
Shells Spawn by Java	Andreas Hunkeler (@Karneades)	Sigma Integrated Rule Set (GitHub)	0eced37f0ea111b4f9b0de81cecda56610adc30fad4061274a488187f71b395d	93	2
Wake-On-Lan	Joe Security	Joe Security Rule Set (GitHub)	7695d2af7ecb7540baa69cd6442745f2c3bdd83d21c904b7a09b2d560c123439	93	0
Security Support Provider (SSP) Added to LSA Configuration	iwillkeepwatch	Sigma Integrated Rule Set (GitHub)	303ed88ac4fc55c5f589ac99388d35769e708b361f23a767523b143a6751efc0	92	1
Greenbug Campaign Indicators	Florian Roth	Sigma Integrated Rule Set (GitHub)	f29ccc5a8616c9c1119e794b857a0425268bf5ee86863b612092ec5e045863ed	90	1
Malicious Nishang PowerShell Commandlets	Alec Costello	Sigma Integrated Rule Set (GitHub)	b80c35f99523537c476487e505edb0c210eea308fa18707fdcd5aa54d136e3ce	90	1
Suspicious Code Page Switch	Florian Roth, Jonhnathan Ribeiro, oscd.community	Sigma Integrated Rule Set (GitHub)	843024550fd9239f814fd3dcd7f1f768fe7316501173bb485e673bdb9abf1d63	88	1
Powershell launch regsvr32	Joe Security	Joe Security Rule Set (GitHub)	59bdcb50161e15e215ceab8d779ba112cc633a8bde418fc87d450d05d5e78a78	86	2
Harvesting of Wifi Credentials Using netsh.exe	Andreas Hunkeler (@Karneades), oscd.community	Sigma Integrated Rule Set (GitHub)	9d07a4fa9892ca001b30724fd1594eff85b72585c8f1106889da7e97608509b4	83	0
Run Whoami as SYSTEM	Teymur Kheirkhabarov	Sigma Integrated Rule Set (GitHub)	6af189a96d12cb443ce812c507e6b5326d70cc43e4f8a8b179fd45d5acee44bd	82	4
Control Panel Items	Kyaw Min Thein, Furkan Caliskan (@caliskanfurkan_)	Sigma Integrated Rule Set (GitHub)	2f683c72a6ae438b4161918b9e82bb9c7e09f701f65f85be9231ced52084f219	80	4
MsiExec Web Install	Florian Roth	Sigma Integrated Rule Set (GitHub)	c56598b1a4dc67703e332a7df820b31b6690ea40d2352aead9f77f441f6f5b2d	80	0
Dynamic C Sharp Compile Artefact	frack113	Sigma Integrated Rule Set (GitHub)	764276dba9654bf07d000fa390ae98de360ac172927cf3ef64f2db6c5b9be3b2	79	0
Saefko RAT (Sysmon detection)	Ariel Millahuel	SOC Prime Threat Detection Marketplace	e036021928c6159521691ec6551a2b2c660a651ff2c69171bb3db4fc676b2e17	78	0
High Integrity Sdclt Process	Roberto Rodriguez (Cyb3rWard0g), OTR (Open Threat Research)	Sigma Integrated Rule Set (GitHub)	9076ea2849a39de53427fc7d336a9132ac1d6dea68e77efa6abafebd89ee90c9	77	0

UAC Bypass Using PkgMgr and DISM	Christian Burkard	Sigma Integrated Rule Set (GitHub)	5b0ad2dce2b0a9bde121d5016b3379c08f507ccce3f43e43a65fe518a16ba50c	76	1
Domain Trust Discovery	E.M. Anhaus (originally from Atomic Blue Detections, Tony Lambert), oscd.community, omkar72	Sigma Integrated Rule Set (GitHub)	e5bf067d8fc5f77622680e942156a44de63eda6026750ac80c29d0304dca435e	74	0
Modification Of Existing Services For Persistence	Sreeman	Sigma Integrated Rule Set (GitHub)	01b2124bf0e9019139ef617d15b67080610ffd3584d4fa0cf7c646bd3f11853b	73	0
Suspicious Execution of Systeminfo	frack113	Sigma Integrated Rule Set (GitHub)	f2a81aa24c1d19a09711179a71cd58fe057ab277cbef8632cc6a9281d5cf87dd	73	4
WinDivert Driver Load	Florian Roth	Sigma Integrated Rule Set (GitHub)	b7ad594d8528d4ee4c0201b1a0852d42e9fc45976e984ed534f502290031e73a	71	4
Office Autorun Keys Modification	Victor Sergeev, Daniil Yugoslavskiy, Gleb Sukhodolskiy, Timur Zinniatullin, oscd.community, Tim Shelton, frack113 (split)	Sigma Integrated Rule Set (GitHub)	0533bf39f662d089d6f317f51a9329a2865ffc0d84552c58c39a8d35672474a4	70	11
Abusing Findstr for Defense Evasion	Furkan CALISKAN, @caliskanfurkan_, @oscd_initiative	Sigma Integrated Rule Set (GitHub)	47d19568dce3538a5fd8f2ddbd8388f28dbd91d200dc9a91d8166cb957ace155	68	4
Sdclt Child Processes	Roberto Rodriguez (Cyb3rWard0g), OTR (Open Threat Research)	Sigma Integrated Rule Set (GitHub)	440b98d4bf30e3c39e7c17aa21aaa561647a4230e418cf901961b1604e27877c	68	0
Ngrok Usage	Florian Roth	Sigma Integrated Rule Set (GitHub)	c2e9abacba241e42d67c8d6ae1523533d3cb9769cf7315d401744e4266f91ffc	67	3
Recon Activity with NLTEST	Craig Young, oscd.community, Georg Lauenstein	Sigma Integrated Rule Set (GitHub)	1419b2c28c143f7062ef95f941065d5327c65890cab58ade41efd168132d8b3b	67	0
SMB Relay Attack Tools	Florian Roth	Sigma Integrated Rule Set (GitHub)	d702a3f44f93b4f3f9c5cd7b73d3901b2db7d1b3db3e051b5135849e3f812ecb	66	0
Application Whitelisting Bypass via Dnx.exe	Beyu Denis, oscd.community	Sigma Integrated Rule Set (GitHub)	da46c4a25c9b1a9291dd79b4539957b5ab71a6f2d75da9a90cfe48f74048a9a9	65	0
Data Compressed - rar.exe	Timur Zinniatullin, E.M. Anhaus, oscd.community	Sigma Integrated Rule Set (GitHub)	e5fedf5f2a45c0555943282d3dd05186495acc374df19f7735f92d6d648dd1bb	65	0
Malicious PowerView PowerShell Commandlets	Bhabesh Raj	Sigma Integrated Rule Set (GitHub)	c9a0fa3e3f43c8762528ddcca56a26673a3f37eb9077f2657884e8b847fb9ba8	63	10
Suspicious Reconnaissance Activity	Florian Roth, omkar72	Sigma Integrated Rule Set (GitHub)	6782835a8af9329207a47fe5076c3dff20a8803bafbda97ddc938ae379eaf8df	62	0
CMSTP Execution	Nik Seetharaman	Sigma Integrated Rule Set (GitHub)	ba18b1afcbf41aa13fd2cd7dc8e323b09854c6f046b4a98d07c2ea5d751d7584	61	0

Internet Explorer Autorun Keys Modification	Victor Sergeev, Daniil Yugoslavskiy, Gleb Sukhodolskiy, Timur Zinniatullin, oscd.community, Tim Shelton, frack113 (split)	Sigma Integrated Rule Set (GitHub)	11ecb99add36c59a082a478e7c117545e6404a0b28c77c007c135739df91a489	61	3
Malicious Windows Script Components File Execution by TAEF Detection	Agro (@agro_sev) oscd.community	Sigma Integrated Rule Set (GitHub)	1aed5dfd628d749d7b679eefe579532b3ff3ca46fecf65776910e7de7aaa6148	61	0
MSHTA Spwaned by SVCHOST	Markus Neis	Sigma Integrated Rule Set (GitHub)	c1db9b15fbf203a696f2047d6ce2c7c32283587487a72c4333b63b8005e6a37c	60	1
WMI Persistence - Script Event Consumer	Thomas Patzke	Sigma Integrated Rule Set (GitHub)	3b638ebc248d5ac99c1adb404e0b5f4adc3784b9af6f02b296381a950e9e8fdf	60	0
WMI Persistence - Script Event Consumer File Write	Thomas Patzke	Sigma Integrated Rule Set (GitHub)	f4ab9cd44db2481795fe0edd858471bda0d0b73d8e406124bf76a2a074ac5360	60	0
Powershell add exclusion path, extension and process	Joe Security	Joe Security Rule Set (GitHub)	177e7b167f988da0ec82090f6aaaa1ad7e74609b6832a0abb8759bc9e652fee2	59	0
Windows Credential Editor Registry	Florian Roth	Sigma Integrated Rule Set (GitHub)	6ebbbc78481d8b5c75483ddb2c7045a006678cbfbd915c2e6d0c0e5d2dfb736d	59	0
CoViper Malware	Ariel Millahuel	SOC Prime Threat Detection Marketplace	c388ee7bf8678acd149ab04cc3dc6f3d923b3c2a7684f42de0c984c16de1c023	58	0
Invoke-Obfuscation COMPRESS OBFUSCATION	Timur Zinniatullin, oscd.community	Sigma Integrated Rule Set (GitHub)	40db318f5624034dad47f954fe3a2bc47f2e09bc7d14e2311481d406665bde6a	58	0
Suspicious Debugger Registration Cmdline	Florian Roth, oscd.community, Jonhnathan Ribeiro	Sigma Integrated Rule Set (GitHub)	bf194ab090c7130529a9fd6a7f876d5fc008ceecf627db81eef41431ffaa3c53	57	1
Rar with Password or Compression Level	@ROxPinTeddy	Sigma Integrated Rule Set (GitHub)	02930d34935e0616b2711790272271498e2a5a03bcf66372f0985d2e89cee1af	55	7
Encoded FromBase64String	Florian Roth	Sigma Integrated Rule Set (GitHub)	b079b9bebaa7ac01f379d6d83aa123ec20bc9068b9a097e09aec5f87b42d91d1	54	2
Suspicious PowerShell Invocations - Generic	Florian Roth (rule)	Sigma Integrated Rule Set (GitHub)	20f6c9f89613e81c3c83ed81ee4dd3f5793d5910ebc8fbc5330174a7a74ecb54	54	0
MMC Spawning Windows Shell	Karneades, Swisscom CSIRT	Sigma Integrated Rule Set (GitHub)	db1e0cf723dcd4169ac8bc1fb3f0679715ccb323d3a3e42e23cc811efa0d9e98	53	0

PsExec Service Start	Florian Roth	Sigma Integrated Rule Set (GitHub)	7e4741cdaf6a396a8d975ad542687436b6beda2f0282db17805ebf9b52098289	53	0
CertReq.exe Lolbin	Den Iuzvyk	SOC Prime Threat Detection Marketplace	bc9b5e9188d37350da57ebc0b5b9ccc8a2ee828e827a15edb38904b64317a291	50	0
DNS Exfiltration and Tunneling Tools Execution	Daniil Yugoslavskiy, oscd.community	Sigma Integrated Rule Set (GitHub)	b5eeb195cf8da826ce09652556c789913808b5869a15ad6d6771d084721b65e0	50	0
WinSock2 Autorun Keys Modification	Victor Sergeev, Daniil Yugoslavskiy, Gleb Sukhodolskiy, Timur Zinniatullin, oscd.community, Tim Shelton, frack113 (split)	Sigma Integrated Rule Set (GitHub)	688632515df3a00cecdf2ee4e9316bea52edf73c9cb0889c10d336de857c293c	50	1
PipeMon malware detection (Winnti Group)	Ariel Millahuel	SOC Prime Threat Detection Marketplace	7f7471486789b0240cf2b95271088889269baee8e3fb42b0cdb6d71d7d37588d	49	17
Suspicious Netsh DLL Persistence	Victor Sergeev, oscd.community	Sigma Integrated Rule Set (GitHub)	cfb3049a2fd55cd1ff6721dc9b502008c4449922474c40b20b8f6fab4f51ce02	46	1
Suspicious WebDav Client Execution	Roberto Rodriguez (Cyb3rWard0g), OTR (Open Threat Research)	Sigma Integrated Rule Set (GitHub)	27f312fa081c26ea0c76a26a31e9c6fe7a974b36000c89db9e288fd1ca3a6e9e	46	1
Schedule script from internet via mshta	Joe Security	Joe Security Rule Set (GitHub)	a3c2a24a999f3a9870f6ace27e73e7bdf30d18dcf0bc4873bfe196f5bec81ad4	45	0
Automated Collection Command Prompt	frack113	Sigma Integrated Rule Set (GitHub)	511fcd38b1cd4057f3b3568707032548bac72899a4b3c932f3614c6d89d417bd	44	0
Explorer Root Flag Process Tree Break	Florian Roth	Sigma Integrated Rule Set (GitHub)	d44e9b6572a6737a34b18fd89f757237729293ed9959e5be7dd05d63e7f78622	44	4
Execute Scriptlet from internet Via Regsvr32	Joe Security	Joe Security Rule Set (GitHub)	1dfe86ef579952e7d83c7cab84e28986946f0660fc39224c8c471d29300a9885	43	0
Run Whoami Showing Privileges	Florian Roth	Sigma Integrated Rule Set (GitHub)	a9f6af870a74ed20bfbc784983dc7fa8aae28d336e2f79a8fa8b72c32d6a9fa0	43	1
Cmdkey Cached Credentials Recon	jmallette	Sigma Integrated Rule Set (GitHub)	396c0639fa0d38dbd62b1c1baa0fae0b008178fb81dfebaf1cc70a858c610190	42	3
MMC20 Lateral Movement	@2xxeformyshirt (Security Risk Advisors) - rule; Teymur Kheirkhabarov (idea)	Sigma Integrated Rule Set (GitHub)	047087ddae3ef4f27e871131c79addb166cb71593c4fb795a5d119d4d78cd0a7	42	2
Mounted Share Deleted	oscd.community, @redcanary, Zach Stanford @svch0st	Sigma Integrated Rule Set (GitHub)	407e4bde1473325159e680d149f0f254239a0a299c46a43635758710d7592f65	42	1
PsExec Tool Execution	Thomas Patzke	Sigma Integrated Rule Set (GitHub)	0846916c3d5af2a322cf42210119c1d28945f9733c842830a4caf16597462ac0	42	0

Monitoring For Persistence Via BITS	Sreeman	Sigma Integrated Rule Set (GitHub)	f9b2dcdba235a40678fcd4411540f98adc4caca054a247054eba6b040b37243e	41	0
UAC Bypass via Sdclt	Omer Yampel, Christian Burkard	Sigma Integrated Rule Set (GitHub)	9e30ed5d0167ae542ae090b30e0049496a63c5c9c63bb37e80d62532640cfc6b	41	0
Powershell downloading file from url shortener site	Joe Security	Joe Security Rule Set (GitHub)	f05d1fcd81ae053d34629eef4e2f082dd51622b2535713f47860649c3619d085	40	1
PsExec Tool Execution	Thomas Patzke	Sigma Integrated Rule Set (GitHub)	2638e4eb6733f565f75759fc7f3c7b2ce2d92f7a231f14859cad11aa82b929e9	39	0
Schedule VBS From Appdata	Joe Security	Joe Security Rule Set (GitHub)	b16d941c7cf2248881a4d3da266d63655713389cafe7f2606ceb2b73fbace067	39	0
Winlogon Helper DLL	Timur Zinniatullin, oscd.community	Sigma Integrated Rule Set (GitHub)	071f1cce27ada52da178afa07fd609ed14967f9058b386611411962f4c56b665	39	1
Automated Collection Command PowerShell	frack113	Sigma Integrated Rule Set (GitHub)	beee5a67cef9cbdfd4d0e1db0dc60dff160df233b0948d9988a2ca819a41727c	38	4
PowerShell Get Clipboard	Roberto Rodriguez (Cyb3rWard0g), OTR (Open Threat Research)	Sigma Integrated Rule Set (GitHub)	8a27ef77773c5b6e0ce2da04cdccf4f14f01015bd4dfadcb9f07ab0905d766a0	38	1
SquiblyTwo	Markus Neis / Florian Roth	Sigma Integrated Rule Set (GitHub)	293439c3a9a4af09073b054953f425c95028a6ac98eddc611a461090bd1f3373	38	0
Commun Autorun Keys Modification	Victor Sergeev, Daniil Yugoslavskiy, Gleb Sukhodolskiy, Timur Zinniatullin, oscd.community, Tim Shelton, frack113 (split)	Sigma Integrated Rule Set (GitHub)	aa1c4ee10caaa9d521b34246c51e0c22c8af0a4b7fdb1cdd9faf1182ef6dd14c	37	0
Suspicious DIR Execution	frack113	Sigma Integrated Rule Set (GitHub)	7752bbd4e940ef58081260cfa45b4ac6b149e2cecb836d79f5e61bfbdc237105	37	0
Suspicious Execution of Shutdown	frack113	Sigma Integrated Rule Set (GitHub)	157ee4e95270f64481c50464c0e4766830e1e2b38b214a98f9e3f977857c6c69	36	0
Sysprep on AppData Folder	Florian Roth	Sigma Integrated Rule Set (GitHub)	76d39c4238c645e864f006400ab59ebda393cfe12db20d6f7ec44eac3b27f6b3	36	0
PsExec Tool Execution	Thomas Patzke	Sigma Integrated Rule Set (GitHub)	91a0bf780670902c97c569d46226158bdd49738004799b58cd63cc4c9d63ea55	35	0
RDP Hijacking. Terminal Services Manipulation.	Den Iuzvyk	SOC Prime Threat Detection Marketplace	3d69986e07af4e5398ea63ef3256bdbbd6215aa1823e591de5088f16896f0c5d	35	0
MSBuild execute suspicous task	Joe Security	Joe Security Rule Set (GitHub)	850ce3b49e2fc441426c3b9ec59e195d417194b461fe480e76d2482bcd20112d	34	0

Psexec Accepteula Condition	omkar72 - https://www.fireeye.com/blog/threat-research/2020/10/kegtap-and-singlemalt-with-a-ransomware-chaser.html	Sigma Integrated Rule Set (GitHub)	38908b57fac2bfb8f5f8466c64aa654432aa3d6f14700b122a4c4afb85f51879	34	0
TAINTEDSCRIBE - North Korean Trojan (Hidden Cobra)	Ariel Millahuel	SOC Prime Threat Detection Marketplace	97f6a22231c4c8e243c104bf226d8fd3875f335f00fc724750e6b691770fbc5a	34	9
Suspicious Use of Procdump on LSASS	Florian Roth	Sigma Integrated Rule Set (GitHub)	a6a60c80601bd33b44e65b559f9e53c0b9237ab7f54ca97530065cd494662e3b	33	0
LSASS Memory Dump File Creation	Teymur Kheirkhabarov, oscd.community	Sigma Integrated Rule Set (GitHub)	b0e4aa7c882545a1b46a09c373f3abc99ee9ad92c5cb99e1b8764356501b3059	31	0
Meterpreter or Cobalt Strike Getsystem Service Start	Teymur Kheirkhabarov, Ecco, Florian Roth	Sigma Integrated Rule Set (GitHub)	22ddfce5e8a79e957f4dbdceb97e27d764b010d395a20fd45cf95a20d02b53e9	31	0
Netsh Port Forwarding	Florian Roth, omkar72, oscd.community	Sigma Integrated Rule Set (GitHub)	00fb9d21500af7c2b136a91e80c983e8f98843c063a63898c2775d7a5a91efa9	31	0
Powershell download and load assembly	Joe Security	Joe Security Rule Set (GitHub)	32fcfd50f2fcf0aa58bebfbfb09b7e32b7349a17a5c1aaea5b18783f458c4e9d	31	0
Suspicious Execution of Powershell with Base64	frack113	Sigma Integrated Rule Set (GitHub)	eb75f9de2201bfad4ef177dca85b0b8fa8e5a86ba2357af5301f72acbc5eb144	31	0
Suspicious Parent of Csc.exe	Florian Roth	Sigma Integrated Rule Set (GitHub)	b0e07fc365ce0d0690c84a20e3467a5be2301d1c4de1e87bcbb9cb9ea841222c	31	0
Possible Process Enumeration (Sysmon/Windows Logs).	Roman Ranskyi	SOC Prime Threat Detection Marketplace	1b3947466060dff55a89da9e24ec34cca8df9c4dbf704a3b3a9120eb3df96e3a	30	1
Turla Service Install	Florian Roth	Sigma Integrated Rule Set (GitHub)	8d5d550c1852a70e22df794241027e8fda50a74f9c87728f63752437404f20a8	30	0
Detected Windows Software Discovery	Nikita Nazarov, oscd.community	Sigma Integrated Rule Set (GitHub)	2f2546b453b2e10b60c4d6b1345bc05c2dc99e42daef2e236a11005d772937ad	29	2
Impacket Tool Execution	Florian Roth	Sigma Integrated Rule Set (GitHub)	bcdf3f22e3474c8f1ea65e450422f64bc2fb74de766f420de7cd57827679d7f7	29	0
Suspicious WMI Reconnaissance	frack113	Sigma Integrated Rule Set (GitHub)	c64577166c54aa12e6fafe9322a15fd35e2e359c52a4b545c470853d848557ec	29	3
TrustedPath UAC Bypass Pattern	Florian Roth	Sigma Integrated Rule Set (GitHub)	804e7993351b779b371021d0b762692107233efc595e1171e5f9ebc62b851247	29	0

Malicious behaviour on user login (Microsoft Windows - c0d0s0 group behavior)	Ariel Millahuel	SOC Prime Threat Detection Marketplace	27774785c899a25659566662ca41aadd02b66d6eb728811937ebaae069d82f5a	28	1
Suspicious Atbroker Execution	Mateusz Wydra, oscd.community	Sigma Integrated Rule Set (GitHub)	842f615741b9cfb621f4ae3f95d42e256251fe082e0f4c533c1633ffcc70adb8	28	0
QBot Process Creation	Florian Roth	Sigma Integrated Rule Set (GitHub)	0453733ce01d4d10623584c342bf2a905ff761f1fb7b0bfbadcb80e8d940c32b	27	0
Sysinternals SDelete Registry Keys	Roberto Rodriguez (Cyb3rWard0g), OTR (Open Threat Research)	Sigma Integrated Rule Set (GitHub)	d5a8c01fb27702ba8f9e0abb5ca03c7c11b6bbf635c3e08354c5106eb06c1c85	27	2
PowerShell Create Local User	@ROxPinTeddy	Sigma Integrated Rule Set (GitHub)	065b49beca5cc42953a5612a7a5342fd18266f128a46b1a788c3f358f775a191	26	1
Invoke-Obfuscation COMPRESS OBFUSCATION	Timur Zinniatullin, oscd.community	Sigma Integrated Rule Set (GitHub)	2cf6294605b971d082366887fa44157d3f99e7552181ee7314a2ba598a2e5d66	25	0
Operation Vicious Panda (COVID-19 Campaign)	Ariel Millahuel	SOC Prime Threat Detection Marketplace	ed562e5af5aba4e5887ef8b69c3f8410480a32e19b5c9e3f3fcd9bd0fd33a447	25	2
PowerShell Writing Startup Shortcuts	Christopher Peacock '@securepeacock', SCYTHE	Sigma Integrated Rule Set (GitHub)	537a092527e25f9e54a3ddb6667c0303fbda5891d2f933ec0fc62bd4a5572cb4	25	0
Remote PowerShell Session	Roberto Rodriguez @Cyb3rWard0g	Sigma Integrated Rule Set (GitHub)	acad8e3e215caeb927f20d9296b9e48f54d909e55d58cb5b27bb4d334ab477a6	25	2
Execute Scriptlet Via Regsvr32	Joe Security	Joe Security Rule Set (GitHub)	568224310775bb02fb9ae53d55d8f7c8bc1daf93e73db7670b15f8b6f421f00d	24	0
LOLBAS wsl.exe (via cmdline)	Den Iuzvyk	SOC Prime Threat Detection Marketplace	55bd30964b2c80cd229425cd10828e1b7c89462547581eb0c4a907c55c87f0a6	24	0
LSASS Memory Dumping	E.M. Anhaus (originally from Atomic Blue Detections, Tony Lambert), oscd.community	Sigma Integrated Rule Set (GitHub)	5e648013d43c5992b13c647c1b522a289f737e3c1ef665572f75f913fde57c5a	24	0
Powershell execute code from registry	Joe Security	Joe Security Rule Set (GitHub)	22f5c0268236153aea7f17b7fcb4e9a2ef903343534a9c2a98b5c1f8918bb9a5	24	0
Suspicious Service Path Modification	Victor Sergeev, oscd.community	Sigma Integrated Rule Set (GitHub)	8583e6aef0800332fe3fd71771daa3901bacd1a4e3b8ae12333da5f445913332	24	1
bitsadmin download and execute	Joe Security	Joe Security Rule Set (GitHub)	613bbc724cd17594b42667a8a5c4df0dff074adfb53a590f30f86743bc9b5b47	24	2
PowerShell as a Service in Registry	oscd.community, Natalia Shornikova	Sigma Integrated Rule Set (GitHub)	edeb7efda75eef0c30275df1148d63a2707963d2d9735d444a56536df2161a9e	23	0

Renamed Whoami Execution	Florian Roth	Sigma Integrated Rule Set (GitHub)	f22be736aa7b4ddd0d6ce96e785fbb7adbcb991517763b72a098333df9610f14	23	0
Shells Spawned by Web Servers	Thomas Patzke	Sigma Integrated Rule Set (GitHub)	ca0321ec695742141eb7a3fb00dfc04170d24e00d3f021803c488451d9c4648f	23	0
Discover Private Keys	frack113	Sigma Integrated Rule Set (GitHub)	2a86897d4c284135c8e21105377149da6e12d9f57525bfdccdfb55cf4b3425fc	22	0
Fireball Archer Install	Florian Roth	Sigma Integrated Rule Set (GitHub)	82119a59aede1b373e13f532ace644de8571caff9f04869378270de5b5881bc6	22	0
Relevant Anti-Virus Event	Florian Roth	Sigma Integrated Rule Set (GitHub)	39e7fb552f1143dc6ba79ca293aaea514c20448ec6241a53cf150f29298b942d	22	0
Winword Drops Script In Startup	Joe Security	Joe Security Rule Set (GitHub)	04a0af687c3b9094f9252dc38ead308fae7facf86cb7e4bf728075c9b17ed9dc	22	1
CreateMiniDump Hacktool	Florian Roth	Sigma Integrated Rule Set (GitHub)	b0407739067c1a391ad55a8b30a1c8109e9239a36d94cf389a4f842a53e36f73	21	0
Execute Script with spoofed extension	Joe Security	Joe Security Rule Set (GitHub)	206390e3b1deba575d9f4b3f8321fd015223f5177a8f486a56f6d74cd51afab4	21	0
Grabbing Sensitive Hives via Reg Utility	Teymur Kheirkhabarov, Endgame, JHasenbusch, Daniil Yugoslavskiy, oscd.community	Sigma Integrated Rule Set (GitHub)	4caa5ae7b301d0b7382caf525ab9dead072ea9efadc1f7cc59d8a59c20b0fe57	21	0
NetNTLM Downgrade Attack	Florian Roth, wagga	Sigma Integrated Rule Set (GitHub)	567e3d1c926bd9cf6698fc92a1b61254aa80f7d149c421f1d6acbf4fc8492e5f	21	2
System Scripts Autorun Keys Modification	Victor Sergeev, Daniil Yugoslavskiy, Gleb Sukhodolskiy, Timur Zinniatullin, oscd.community, Tim Shelton, frack113 (split)	Sigma Integrated Rule Set (GitHub)	e508e0cd0078f2c99fa9a87448bebda5652165ba069b1c9c4a89ecc4a2b385ca	21	0
Bazar Loader Detection (Sysmon detection)	Ariel Millahuel	SOC Prime Threat Detection Marketplace	6e25203533b4bcc3b9ce1805fbf4ec196d2fd6139dcf17880caf0e2952c3ebfe	20	0
Exchange Exploitation Activity	Florian Roth	Sigma Integrated Rule Set (GitHub)	a53120d1ec17fbf608c6da8cb88f544b76206e830dd4ec17155f718bf5851d0f	20	0
Execute dll with txt extension from temp location	Joe Security	Joe Security Rule Set (GitHub)	d8d01ff318fd81c3e8579c3f1dbc420f408beb4b67bc9be1a4bbdc759dce812a	20	0
Suspicious Sc Query	frack113	Sigma Integrated Rule Set (GitHub)	373890127a34a7d314b3d10d451aaacb806579ec3e9ed2515dbdd0a4d4bf7860	20	2
Wow6432Node CurrentVersion Autorun Keys Modification	Victor Sergeev, Daniil Yugoslavskiy, Gleb Sukhodolskiy, Timur Zinniatullin, oscd.community, Tim Shelton, frack113 (split)	Sigma Integrated Rule Set (GitHub)	3e5fe19fbbb767b861e93022c3f95d25e1618fc86be75b05326ee57b2f75633c	20	1

Cred Dump Tools Dropped Files	Teymur Kheirkhabarov, oscd.community	Sigma Integrated Rule Set (GitHub)	45248d2871f8e9f12191effed010f35a307cc4e1eb1350ad7dd486fc07bc0bdb	19	0
Defrag Deactivation	Florian Roth, Bartlomiej Czyz (@bczyz1)	Sigma Integrated Rule Set (GitHub)	f7c48f991deaa5a1f44d21dc156d1989c5c383f971da93ecc1eaf11928860293	19	0
NetNTLM Downgrade Attack	Florian Roth, wagga	Sigma Integrated Rule Set (GitHub)	5bced7470eb37ada15efd448b0a87615727c93557e648e225c3ee894c4b0ff08	19	0
CMSTP Execution	Nik Seetharaman	Sigma Integrated Rule Set (GitHub)	65ffc0ddb80d953bb500276c61b57ba48cb45df5128bb8264ab47e7f48b2c9ec	18	1
ExtExport.exe abuse	Den Iuzvyk	SOC Prime Threat Detection Marketplace	b74bcba954f168601bf9276abbb38f732599a67e11aa264ce29f8bc3f056aed3	18	0
NTFS Alternate Data Stream	Sami Ruohonen	Sigma Integrated Rule Set (GitHub)	535b54123e1e90e346eb48779d2bdc19508f9a3aef7f7cf48bddbbd43f953478	18	1
Root Certificate Installed	oscd.community, @redcanary, Zach Stanford @svch0st	Sigma Integrated Rule Set (GitHub)	fde7c67804bf2f25cc674d242987b96bb244126d9568bceb7c9a208193fe66a6	18	1
CVE-2021-26858 Exchange Exploitation	Bhabesh Raj	Sigma Integrated Rule Set (GitHub)	bea74b1863b1262ffbfa6ffd29da720d86bdcd7ad6ea4a27a2da1c563fcb5093	17	17
Defrag Deactivation	Florian Roth, Bartlomiej Czyz (@bczyz1)	Sigma Integrated Rule Set (GitHub)	8428866bf6cbf8ea04c18dc9a8ebd493a8a882a9b706b557f71d376cd69fda79	17	0
Possible Exchange CVE-2021-26858 (via file_event)	SOC Prime Team, Microsoft	SOC Prime Threat Detection Marketplace	0fe11fe110197a5d21d1f4c9b2fed3e8f8afe8066ffa9242e24a9a95abe2516a	17	17
Possible InstallerFileTake Over LPE CVE-2021-41379	Florian Roth	Sigma Integrated Rule Set (GitHub)	1649fcc98b56dc9cfc742a4a6df24ac3e91123ac466268300afc87e3f91191e2	17	0
Powershell Timestomp	frack113	Sigma Integrated Rule Set (GitHub)	5b5656801277c44d48ce3c9f4c8c393d55f8c0943d2c641d4968a012bd160f38	17	1
Sage Ransomware (Sysmon detection)	Ariel Millahuel	SOC Prime Threat Detection Marketplace	71d449cc65c29ab2e4fee214298f208b87225361a0f65f0f2e73bfd7875b1ef7	17	0
Suspicious Plink Remote Forwarding	Florian Roth	Sigma Integrated Rule Set (GitHub)	fd6a0f7521cf3dabf0d2ac45a1aed9f2e2029daa9d1fba9f71905bb34aa427ca	17	0
Taskmgr as LOCAL_SYSTEM	Florian Roth	Sigma Integrated Rule Set (GitHub)	1d1e002f037bffd9b91901474efbd1036622a788849898b81570d37d3ba34513	17	0
AnyDesk Silent Installation	Ján Trenčanský	Sigma Integrated Rule Set (GitHub)	8c68ebe0db23e4f70c3621d56e4ce298dcf255e61288342e6b4760dd0af96c85	16	0
Powershell create lnk in startup	Joe Security	Joe Security Rule Set (GitHub)	fd5c77e4a6ca9deb325d7525e8219d80cc70e6bbf765e2d75ab4f30f6be7cc9a	16	0

Suspicious Auditpol Usage	Janantha Marasinghe (https://github.com/blueteam0ps)	Sigma Integrated Rule Set (GitHub)	33a4a18ae1a3802586c239be79075294541594b5b603c230af39618577e03fae	16	0
Adwind RAT / JRAT	Florian Roth, Tom Uelтschi, Jonhnathan Ribeiro, oscd.community	Sigma Integrated Rule Set (GitHub)	e1d3ef681f53390850fb5bcd89f8d9388eebce85673fe6b8f766bd596275003d	15	0
CVE-2021-26857 Exchange Exploitation	Bhabesh Raj	Sigma Integrated Rule Set (GitHub)	6a562c9f35089d87a91ec35ae35044bfb9902969d69d04e8f50b1e9f2b14b4d0	15	15
Certutil Encode	Florian Roth, Jonhnathan Ribeiro, oscd.community	Sigma Integrated Rule Set (GitHub)	1b6510b58b9f16b947f9e665c0a3f3902f2d51f54d01596eb9545d8fd6631aa1	15	0
UMWorkerProcess Creating Unusual Child Process CVE-2021-26857 (via cmdline)	SOC Prime Team, Microsoft	SOC Prime Threat Detection Marketplace	777e78408dd5e81cb40b0dd4b18dc729cd882538beac8337067e6a2ceb940493	15	15
VBScript Payload Stored in Registry	Florian Roth	Sigma Integrated Rule Set (GitHub)	dc67cd797236fcf12f7a5e58c0d5fc50318e74f58c9d17e6bf7905e87c5a9c21	15	0
PowerShell Downgrade Attack	Harish Segar (rule)	Sigma Integrated Rule Set (GitHub)	c2de0fe89604a2026e004a0872e75e079b8632fcc9ef341e34017c52fbb2eba5	14	1
APT29	Florian Roth	Sigma Integrated Rule Set (GitHub)	976e44f1ea7fa22eaa455580b185aaa44b66676f51fe2219d84736dc8b997d3e	13	0
Clear PowerShell History	Ilyas Ochkov, Jonhnathan Ribeiro, Daniil Yugoslavskiy, oscd.community	Sigma Integrated Rule Set (GitHub)	860e5b755d1cea66957a1dad5567ffc45ea7e50f98c8c0958538a8507ec82f71	13	0
Credential Dumping Tools Service Execution	Florian Roth, Teymur Kheirkhabarov, Daniil Yugoslavskiy, oscd.community	Sigma Integrated Rule Set (GitHub)	be637f31d674fd7f3e36ce2982a40811732c7bbd70435fdb0378ab0bcbd73618	13	0
DNS Query for MEGA.io Upload Domain	Aaron Greetham (@beardofbinary) - NCC Group	Sigma Integrated Rule Set (GitHub)	8c60cfcbc7464b6af5d7b236a49a53fbfde22feb2036abbf947df7322a7343a0	13	4
Powershell Local Email Collection	frack113	Sigma Integrated Rule Set (GitHub)	7a8c60222c9d0320cd13f6c3e00c4279e2961daa1560bebf35dfe8f0de4387a4	13	0
Schedule binary from dotnet directory	Joe Security	Joe Security Rule Set (GitHub)	3c44dc412b67786cb131e2f723dbcfd035125eb3c04b66bc8baf4a7efe0ac581	13	0
Data Compressed - PowerShell	Timur Zinniatullin, oscd.community	Sigma Integrated Rule Set (GitHub)	1ea6262b9839c6f8aa32af503fb227a46a6f22b4778711e1a64f62b102e43a3e	12	0
Dumpert Process Dumper	Florian Roth	Sigma Integrated Rule Set (GitHub)	758c2b360e853174de27738caef97d466db11778427f5db30224884512b55494	12	0
InfDefaultInstall.exe .inf Execution	frack113	Sigma Integrated Rule Set (GitHub)	f6602c9cc48a37aa44fbfc4ffe4560e8f37e1934e365a235af4ae61c9571ded1	12	0
Mouse Lock Credential Gathering	Cian Heasley	Sigma Integrated Rule Set (GitHub)	3d2c6b32d1108da7c43b45888b3ec8440d9177641036131235b6409be1771ff7	12	0

NotPetya Ransomware Activity	Florian Roth, Tom Ueltschi	Sigma Integrated Rule Set (GitHub)	641862d7e2c86cdcc7b53162395c508471d30b1911e0be65fb335d6208a110b3	12	0
Powershell run code from registry	Joe Security	Joe Security Rule Set (GitHub)	09cf140e4816d8c5bcb37b98e996e455d8127cbccdf4287901654f824cf63f13	12	0
Root Certificate Installed	oscd.community, @redcanary, Zach Stanford @svch0st	Sigma Integrated Rule Set (GitHub)	0226d2c44e3b81cd4d31e7a8e55f6a3e3835b44939f721d5527b610071ebf40b	12	0
Session Manager Autorun Keys Modification	Victor Sergeev, Daniil Yugoslavskiy, Gleb Sukhodolskiy, Timur Zinniatullin, oscd.community, Tim Shelton, frack113 (split)	Sigma Integrated Rule Set (GitHub)	9acd91066b664aa3f4181a28555facbc432bae9a4c8502aa92ceae1de1f31753	12	0
Suspicious Regsvr32 Execution With Image Extension	frack113	Sigma Integrated Rule Set (GitHub)	f64c98dfb55189f8f65b8dc8c77a020a4c869933083e1b3ef087e4dba264e864	12	0
Sysmon Driver Unload	Kirill Kiryanov, oscd.community	Sigma Integrated Rule Set (GitHub)	7729210ddf59514a2d5ae300b6b3c3cd9b836719c40091d770a3b08bef6d735d	12	4
Advanced IP Scanner	@ROxPinTeddy	Sigma Integrated Rule Set (GitHub)	1e081f4ac10fa7ca5c1322255b4569d35b221c6b54e93ab5bd06bd891b690755	11	0
Compress Data and Lock With Password for Exfiltration With 7-ZIP	frack113	Sigma Integrated Rule Set (GitHub)	227d06b807fcca01531502ab9bf3471b44a2e7db88394d5d03f7e07a11adc2e3	11	4
Malicious behaviour on user login (Microsoft Windows - c0d0s0 group behavior)	Ariel Millahuel	SOC Prime Threat Detection Marketplace	a4380ca308017f92e049147ec46e562ab46b9642b1952944647bb9bf85e4c95d	11	0
Path To Screensaver Binary Modified	Bartlomiej Czyz @bczyz1, oscd.community	Sigma Integrated Rule Set (GitHub)	71c11c0cc84fa6ba12489ce6fb7a0c5729c809f47cf296aa025e7f514394f01b	11	0
PowerShell ShellCode	David Ledbetter (shellcode), Florian Roth (rule)	Sigma Integrated Rule Set (GitHub)	a8f93a6a21c54d549a6d042e48c067948add81f96231c70f83cdfa345b1f6cb3	11	0
Invoke-Obfuscation STDIN+ Launcher	Jonathan Cheong, oscd.community	Sigma Integrated Rule Set (GitHub)	fddefdc90062c691bc46bba8afb5fc6b455c1d7141337a963441437d5355a6c4	10	0
MZRevenge Ransomware	Ariel Millahuel	SOC Prime Threat Detection Marketplace	34b4fad92956929789617ef0c367187e5950267fc9fb902893bf5a6583ab5439	10	0
Password Dumper Remote Thread in LSASS	Thomas Patzke	Sigma Integrated Rule Set (GitHub)	68e65c1d21220f970cb6860795f7c6918fb617b028d783bcc58af027c5ee078c	10	0
RMSRemoteAdmin	Joe Security	Joe Security Rule Set (GitHub)	abb330cf6694939eee00022cc1eadd65b14603c20a76a3c590d95ef23c61b22e	10	0

Rclone Execution via Command Line or PowerShell	Bhabesh Raj, Sittikorn S, Aaron Greetham (@beardofbinary) - NCC Group	Sigma Integrated Rule Set (GitHub)	d682d09d3c15912248f0f367d755338bbf871b25380f62525ba288c8bf90689e	10	0
UAC Bypass Using ComputerDefaults	Christian Burkard	Sigma Integrated Rule Set (GitHub)	f0a2a0d6b300aa9b5100a3fcd8fda2e183d4c22f4c748ebf056b724965c77639	10	0
WMIC launch script from xsl file	Joe Security	Joe Security Rule Set (GitHub)	cc58aa96e11657d0df0ee460019755b19a5929a979fdadd56569d6b35c03fdba	10	0
Windows Crypto Mining Pool Connections	Florian Roth	Sigma Integrated Rule Set (GitHub)	5f96c8ad390b56fba16309ec092ccde0290c7896bd2bfd7c49b738c77dc36bde	10	0
Adwind RAT / JRAT	Florian Roth, Tom Ueltschi, Jonhnathan Ribeiro, oscd.community	Sigma Integrated Rule Set (GitHub)	9a837c56dc81ffe30b3cbb46efbb5eaef5933b049b212514e9bb4380f12623c0	9	0
Detected Windows Software Discovery	Nikita Nazarov, oscd.community	Sigma Integrated Rule Set (GitHub)	296c4235eb2d9969dd70271f37fd8708d44ea158f9a24508790c33c5b6003dae	9	1
PowerShell Credential Prompt	John Lambert (idea), Florian Roth (rule)	Sigma Integrated Rule Set (GitHub)	3673ff480d9b6da69d58b49cdbd4653446b39552e94717447405039cbb476c09	9	1
PowerShell ICMP Exfiltration	Bartlomiej Czyz @bczyz1, oscd.community	Sigma Integrated Rule Set (GitHub)	504cd1bcea14d3f138e4253108d6978349e99adf5984333e0d5d78865dd1a481	9	3
Powershell Exchange Snapin (via cmdline)	SOC Prime Team, Microsoft	SOC Prime Threat Detection Marketplace	1920836da8784b3f635f88d7c9216b6619a5f5613a5d53fefb342c817897a736	9	0
PsExec Tool Execution	Thomas Patzke	Sigma Integrated Rule Set (GitHub)	97af35b4172a9333d69b01cdb4d6c6f7b49b0f0d665b4bd4c66b4a3bb793547e	9	0
Trickbot Malware Recon Activity	David Burkett, Florian Roth	Sigma Integrated Rule Set (GitHub)	7cf68fc17a7548176432b7778814a6be12c78c6b34b7a55b4b5d457302f2c07a	9	0
Adwind RAT / JRAT	Florian Roth, Tom Ueltschi, Jonhnathan Ribeiro, oscd.community	Sigma Integrated Rule Set (GitHub)	a7648695383d3c54094a9a623178342f9965ac5977fdf3c70016e06b5d12fbdb	8	0
DarkRAT Botnet	Ariel Millahuel	SOC Prime Threat Detection Marketplace	5157203e484dbfa217f40f7089460a4c6713e54ef44ca66a31ec7d5c820f0d26	8	0
Disabling Windows Event Auditing	@neu5ron	Sigma Integrated Rule Set (GitHub)	d73609956e7379a0917a1fd771e4351b523579011a752df34e3ed749bf878180	8	0
Hidden Local User Creation	Christian Burkard	Sigma Integrated Rule Set (GitHub)	084f8f629ce19b2d68d7e27615e59a3ebea0e92f94d25fffcdf6981152cf5efe	8	0
Imports Registry Key From an ADS	Oddvar Moe, Sander Wiebing, oscd.community	Sigma Integrated Rule Set (GitHub)	004a32a3ac811e09e68ff3749364d27bd3064f5a8e6e2869b7b47cc6667b939e	8	0

Mustang Panda Dropper	Florian Roth, oscd.community	Sigma Integrated Rule Set (GitHub)	64ba6d12e9a7d24ab70539a41abdbb5f3b47f99268f5620467b24cd8118976be	8	0
New or Renamed User Account with '$' in Attribute 'SamAccountName'.	Ilyas Ochkov, oscd.community	Sigma Integrated Rule Set (GitHub)	6c5cfe607309f4bc96c1644752af6a875fd27ea6910ddff26e40a4ae64a26e05	8	0
Powershell launch wmic via class	Joe Security	Joe Security Rule Set (GitHub)	1f85dfeaa80a160e0d553a3ac8d1d5139a7622d4d146c43f52eedbe005757ba7	8	0
PsExec/PAExec Flags	Florian Roth	Sigma Integrated Rule Set (GitHub)	7e17cc0d521f2433baf3ca36bf22ec2946bb387a555fee75aff1c992849a2578	8	0
Suspicious SYSVOL Domain Group Policy Access	Markus Neis, Jonhnathan Ribeiro, oscd.community	Sigma Integrated Rule Set (GitHub)	ff263a69e24c4173f3baabd03b59d71e2dd4679b248e9bf0851bd9852043117c	8	3
Sysinternals SDelete Delete File	frack113	Sigma Integrated Rule Set (GitHub)	c79aec25ed8a3cf07f3a43954d8dda5823dc140075f59c4e0cae1e5a3aee8072	8	2
Blue Mockingbird	Trent Liffick (@tliffick)	Sigma Integrated Rule Set (GitHub)	047c4b3f6b03d9a7cd611e4baaeffab7d6854460859ecf302466ae225ddaf2c7	7	0
CreateMiniDump Hacktool	Florian Roth	Sigma Integrated Rule Set (GitHub)	b66ace0358aa3fe35f98b7d2f726aab76956778883e2fd65cbc867bae21e360a	7	0
Invoke-Obfuscation Obfuscated IEX Invocation	Daniel Bohannon (@Mandiant/@FireEye), oscd.community	Sigma Integrated Rule Set (GitHub)	30c408d940a17c92bda9a7a3661343cb4849cb5206311af462dfa18993f9f0c7	7	0
PowerShell Scripts Installed as Services	oscd.community, Natalia Shornikova	Sigma Integrated Rule Set (GitHub)	6f49f2ed2359b28b3bbcce4b12451150c3c512387446684ad0f02ffa5ca11b5b	7	0
Python Py2Exe Image Load	Patrick St. John, OTR (Open Threat Research)	Sigma Integrated Rule Set (GitHub)	433ecdf8469138ce151b9e283d8e892c2aaec8d0aa9a1f631efac7da11cb1ba8	7	0
Suspicious Cobalt Strike DNS Beaconing	Florian Roth	Sigma Integrated Rule Set (GitHub)	b55c667fef3a16ff308f801e44896c36f9754c98321c12bc516a13477130f4fd	7	0
Suspicious Export-PfxCertificate	Florian Roth	Sigma Integrated Rule Set (GitHub)	b1cd37588678d9d180fae5e3ac98088d0fb94bcf137b0f6b423ba503b9c48334	7	0
APT 37	Ariel Millahuel	SOC Prime Threat Detection Marketplace	c53c2f741a37b554e1a5a16737f3c6f27a5818e8474ade69f599e8d18b6df51a	6	0
Adwind RAT / JRAT	Florian Roth, Tom Ueltschi, Jonhnathan Ribeiro, oscd.community	Sigma Integrated Rule Set (GitHub)	211f7156257e48d853aa431ddfc3fc7b86ca8dabc95f61553575d821ab58fd76	6	0
CACTUSTORCH Remote Thread Creation	@SBousseaden (detection), Thomas Patzke (rule)	Sigma Integrated Rule Set (GitHub)	7b0f6b7c0939954a4e8dd01dcda83d20044a57808d265a6697c3580fde333062	6	0

DiskShadow and Vshadow launch detection	Eugene Nechiporenko, SOC Prime	SOC Prime Threat Detection Marketplace	85495f94a180f99ee2283759ac8a387cd3df5ff6802bcebcd6fd16bd75788af7	6	0
Dumpert Process Dumper	Florian Roth	Sigma Integrated Rule Set (GitHub)	f98998b2f0e9bb08954d741777bfdb257c7cb3dcce96f88af84ecf966e2e5695	6	0
Formbook Process Creation	Florian Roth, oscd.community, Jonhnathan Ribeiro	Sigma Integrated Rule Set (GitHub)	f260e0e6e3999276169e5a2b9378f676cfd85254be368003b2cd97e7d6b10e14	6	0
Office product drops executable at suspicious location	Joe Security	Joe Security Rule Set (GitHub)	e0e4a0d55b1462c34c5c59221f7b9ae4b1625aa019f157ee2d60b21d286df9b5	6	0
Rename system process and copy to suspicious location	Joe Security	Joe Security Rule Set (GitHub)	ae5e05ff7a2f5d6e654578b73a1ddc50baeec856b0ab003ad6852c80beb8b068	6	0
Renamed PAExec	Florian Roth	Sigma Integrated Rule Set (GitHub)	58a87adff5b80f1f00537e13c96a7a3ca3c24b661fb3d6f998ed9a120ad72ccf	6	0
Suspicious Commandline Escape	juju4	Sigma Integrated Rule Set (GitHub)	4ead40e4f0adc5e486cc7911fc0b0b94f05bfe0d27b5f0c2d24e0c803d089fc5	6	0
Suspicious Execution of Hostname	frack113	Sigma Integrated Rule Set (GitHub)	87d10b87f13ab6dd0ee17c311d476bcf6fce51f746e639542c1c6c08b6ae8071	6	0
Suspicious Extrac32 Execution	frack113	Sigma Integrated Rule Set (GitHub)	22466d36eb86be8a2f88344d2ad8707352f79b184489f7bc14547bcc6c82b9c1	6	0
Suspicious Query of MachineGUID	frack113	Sigma Integrated Rule Set (GitHub)	5b823c33b4d7a619c0190d52bf60fd92f6768d9bff34fb85446b00ca141f030a	6	1
Suspicious Reg Add Open Command	frack113	Sigma Integrated Rule Set (GitHub)	81f2a11aeadd681c5a2bbef5acdebbc356da424e56854a985e3c7eb0aded2fba	6	0
Suspicious ScreenSave Change by Reg.exe	frack113	Sigma Integrated Rule Set (GitHub)	a87fe4afa527fd01cbb17ee26918bbf87dacf9b429f97ede32b8831532ec4d59	6	0
TAIDOOR RAT DLL Load	Florian Roth	Sigma Integrated Rule Set (GitHub)	e8a94b22f6db7e94eaf7903de94492f4bdd5b91eaa24377a94e7e51bfdb8e562	6	0
Wmic Launch regsvr32	Joe Security	Joe Security Rule Set (GitHub)	4bd4adb7096f2875c9d4780cebd4f8cc5d8f98ae072aa38aea08cb38ea623042	6	0
Blue Mockingbird	Trent Liffick (@tliffick)	Sigma Integrated Rule Set (GitHub)	fb9f6bbd034578721056b64fb7a34b4e2726da17d1cbf5711dced3ab7cd005c7	5	1
Capture a Network Trace with netsh.exe	Kutepov Anton, oscd.community	Sigma Integrated Rule Set (GitHub)	ed43493e84bcb41bf4a6e8d03279fa79baffdfa16300655622641d8b9754d344	5	0

DInject PowerShell Cradle CommandLine Flags	Florian Roth	Sigma Integrated Rule Set (GitHub)	10bbdc113d1dc5813708dd95928a8d1a38b22ab4b85bc027daaf8ac7aae65c9b	5	0
Detected Windows Software Discovery	Nikita Nazarov, oscd.community	Sigma Integrated Rule Set (GitHub)	ddc07067e955f9f404023ebf4e274002f57acb50f1fe16fe88b6704df84b3864	5	0
HiveRAT detection	Ariel Millahuel	SOC Prime Threat Detection Marketplace	bfa9006c02a3c62043c1bd4c10f77dd29fc786bc22855e00928082034c4307cc	5	0
Lazarus Loaders	Florian Roth, wagga	Sigma Integrated Rule Set (GitHub)	c84a7ca7abbe3e5b0d2b85f57e26013cf82131739ccc06fb4271905d4a63f3ef	5	0
Malicious Service Installations	Florian Roth, Daniil Yugoslavskiy, oscd.community (update)	Sigma Integrated Rule Set (GitHub)	ed602524330bd363f87bc7980fbb46e0186704e38a27f85f7c6030f2ad6356b9	5	0
Netcat The Powershell Version	frack113	Sigma Integrated Rule Set (GitHub)	53b2cd18791dffbcc1b31b49b26f0068d68f366bccb84e299cb79ddcccaf04ee	5	0
Powershell AMSI Bypass via .NET Reflection	Markus Neis	Sigma Integrated Rule Set (GitHub)	4f48e177e42323bad59a64ab7de8ad6105458dbcdbb255b095f3c17aa618478f	5	0
Process Dump via Rundll32 and Comsvcs.dll	Florian Roth	Sigma Integrated Rule Set (GitHub)	31766028cc56afd6db535a222ec9ffa3a26c485dcd759324e890434acf17a601	5	1
RClone Execution	Bhabesh Raj, Sittikorn S	Sigma Integrated Rule Set (GitHub)	5c18d54d0d1977fcaa16d7b119948395edb249365b6c767ea18e95c6b44204a5	5	0
Shedule powershell with encoded command parameter	Joe Security	Joe Security Rule Set (GitHub)	915a39321a250831a95cbb6b6598214820d1be1095aee6555106a9ca7d02a36a	5	0
ShimCache Flush	Florian Roth	Sigma Integrated Rule Set (GitHub)	7755af8c0fe9118bb510e5bd0317a174fc59e613270dce762bbc67cac8f68d15	5	4
SyncAppvPublishingServer Execution to Bypass Powershell Restriction	Ensar Şamil, @sblmsrsn, OSCD Community	Sigma Integrated Rule Set (GitHub)	a8c3610f0218840679ca4d558856dbb0f5d711cabe7b939a9f283180553e2b77	5	0
wmic launch powershell and execute encrypted script	Joe Security	Joe Security Rule Set (GitHub)	016a456c70d6e45a65219e2ee0e3972cd7104bf98c318e2f088a07f71fde0d43	5	0
CobaltStrike Process Patterns	Florian Roth	Sigma Integrated Rule Set (GitHub)	f6b39e4a331f85ca7590bf725ff05b84567ac82eecf2ef761c60e4baed042482	4	0
Emissary Panda Malware SLLauncher	Florian Roth	Sigma Integrated Rule Set (GitHub)	49512d886fa3e8d9595464c693fad4fb93dcbdbc537cda049dacce772f11f38f	4	0

Findstr Launching .lnk File	Trent Liffick	Sigma Integrated Rule Set (GitHub)	2db81575319b095e5240489dc39a6070fb3e587fb35a6c988f38cbc71fede886	4	0
Logon Scripts (UserInitMprLogonScript)	Tom Ueltschi (@c_APT_ure)	Sigma Integrated Rule Set (GitHub)	c58463bc214d5126d24453ce3a2db9a54855641facf8d3dcf2e1a70b4cd47173	4	0
Ncat Execution	frack113	Sigma Integrated Rule Set (GitHub)	358a95254318aa55ff499eb64277dff47957ac37c6370873673433bd55e77cf8	4	0
New TaskCache Entry	Syed Hasan (@syedhasan009)	Sigma Integrated Rule Set (GitHub)	d62173552d7fce98c24a7040b784edf35cc6650d2e68ecf2d04f40c58d58cfda	4	0
Powershell download payload from hardcoded c2 list	Joe Security	Joe Security Rule Set (GitHub)	5c6454bb6fd16d176798dcb8685eabffc5295c27b7c2c471512f66343a885a24	4	0
RDP Hijacking. Last logged-on user changed.	Den Iuzvyk	SOC Prime Threat Detection Marketplace	13ed88b8063438c80d6eb6c7e9aeda38d201453d83fa949f65867ced46825db3	4	0
Removal Amsi Provider Reg Key	frack113	Sigma Integrated Rule Set (GitHub)	29e103486311c7c5f253e500ab6386c2aba984cb782efe903a88f082d3f70254	4	0
Spora Ransomware	Ariel Millahuel	SOC Prime Threat Detection Marketplace	a656aafe4c0cca78f1ad9cc5fe8f97b01ab237e247591a7100edef559c032f30	4	0
SyncAppvPublishingServer Execution to Bypass Powershell Restriction	Ensar Şamil, @sblmsrsn, OSCD Community	Sigma Integrated Rule Set (GitHub)	3bc75ee6104b1d450b245ac94167ae14c204c835e99ff14f840649b7ec5cb561	4	0
AnteFrigus Ransomware	Ariel Millahuel	SOC Prime Threat Detection Marketplace	8b18641dc7819baf3c131b24088048e3cf6ac0f5946f136a2c0b0b36a3754141	3	0
Credwiz util dropped by mshta for dll sideloading	Joe Security	Joe Security Rule Set (GitHub)	47b76425766ceb0d5f71f5b737ae4660dc4fcaa91295131395a542596953ef67	3	0
Equation Group DLL_U Load	Florian Roth	Sigma Integrated Rule Set (GitHub)	a6d1a36dcfe72a6d78f5dd3b78c79bc294296460a9b3adcd993bdd6409046c7f	3	0
Esentutl Gather Credentials	sam0x90	Sigma Integrated Rule Set (GitHub)	477a3302165776826dc440702e8eaed12303d2f1dc7a0fc02eb400d3f82f2e6b	3	0
Fodhelper UAC Bypass	Joe Security	Joe Security Rule Set (GitHub)	c5017f04443b7c88d4fe320734d24f38108f67663239bc00f5c164081e9b5e0a	3	0
GfxDownloadWrapper.exe Downloads File from Suspicious URL	Victor Sergeev, oscd.community	Sigma Integrated Rule Set (GitHub)	b72d2ff1b4c8867cd160c5e82653d122b03a4c6bca9ade97373922682058cce1	3	1

Java Running with Remote Debugging	Florian Roth	Sigma Integrated Rule Set (GitHub)	2e7d87bfbd32ac2342d15ebcc05f5ef626e85c6ff102705ba365a90790098278	3	0
Microsoft Office Add-In Loading	NVISO	Sigma Integrated Rule Set (GitHub)	87bbef1292c33b8d07238254d96faa4edbe7d7b241c05444918849684077237e	3	0
Modifies the Registry From a ADS	Eli Salem, Sander Wiebing, oscd.community	Sigma Integrated Rule Set (GitHub)	7d40150efe45672b8a7928c4d3ccb55e1238e89ead72dc4a08390a907fc57c17	3	0
Netcat The Powershell Version	frack113	Sigma Integrated Rule Set (GitHub)	16372019c3e1774b0a40174d12d8465e4bb4ecfac13a7148849c9b3d21282f37	3	0
Remote File Download using GfxDownloadWrapper.exe	Den Iuzvyk	SOC Prime Threat Detection Marketplace	16dd4d7c651cd862752fb483a4e7898c821603b1739b7aecb11298a6e931189e	3	1
Snatch Ransomware	Florian Roth	Sigma Integrated Rule Set (GitHub)	d48381be3227e49cd9d42fdf472184d9e4db1b4fbe72ee6048739f0af5913e9f	3	0
Suspicious Add User to Remote Desktop Users Group	Florian Roth	Sigma Integrated Rule Set (GitHub)	04ed3e23df49b07ebec11f2374d1ccce40bc71d867b1f8e29ea40b1b9e878ac3	3	0
Suspicious ConfigSecurityPolicy Execution	frack113	Sigma Integrated Rule Set (GitHub)	5b2e321b4ad7aa35a23d2181a655941dc96ea260435a6e1663158a7b2182a9fe	3	0
Suspicious Shells Spawn by Java	Andreas Hunkeler (@Karneades), Florian Roth	Sigma Integrated Rule Set (GitHub)	0119b24f133d3f3142f84b35c30b7b1c417c4418f4d18098200208947ac5d041	3	0
Suspicious Shells Spawn by WinRM	Andreas Hunkeler (@Karneades), Markus Neis	Sigma Integrated Rule Set (GitHub)	dff6f482b1c3296a1eba449d732fe05e7b9a61f56c3849298ee9d06cec81c941	3	0
TAIDOOR - Chinese RAT	Ariel Millahuel	SOC Prime Threat Detection Marketplace	fd151743b69be65652e958a898253090e87a94daf21f008ffacbfef9d8aebcbf	3	1
UAC Bypass Using IEInstal - File	Christian Burkard	Sigma Integrated Rule Set (GitHub)	00df1f50def5c07da9bb57ea8313bde4905aeeff9ebf1b2b923600351791bd23	3	0
UAC Bypass Using IEInstal - Process	Christian Burkard	Sigma Integrated Rule Set (GitHub)	36c54ff9b60bfb04067bb4fc3cb55f0efba4285c46c56123f298c17f0ff6aeb1	3	0
Windows 10 Scheduled Task SandboxEscaper 0-day	Olaf Hartong	Sigma Integrated Rule Set (GitHub)	edf3ca6a0c573fb6b3eae8a8a4a6dd129c1ddebc37dc457690fae45e9594a950	3	0
AWL Bypass with Winrm.vbs and Malicious WsmPty.xsl/WsmTxt.xsl	Julia Fomina, oscd.community	Sigma Integrated Rule Set (GitHub)	3ac562f761dce56ddce1ba6581aace41ae7b64cf2b9fd64295b4d9d43c26aa21	2	0
AWL Bypass with Winrm.vbs and Malicious WsmPty.xsl/WsmTxt.xsl	Julia Fomina, oscd.community	Sigma Integrated Rule Set (GitHub)	a84e26c881c97617cb1fd0ca767f6c6a6aef9dc2b22b7c5346b71449a2bb5bbc	2	1

Amadey Botnet detection (TA505)	Ariel Millahuel	SOC Prime Threat Detection Marketplace	472362d8dcad8c26a75836b16e7f1e1fa272f614affc2dd864632b8a3af7e12f	2	0
Bypass UAC via WSReset.exe	E.M. Anhaus (originally from Atomic Blue Detections, Tony Lambert), oscd.community	Sigma Integrated Rule Set (GitHub)	ced1e1a1282b5d51ede1ac7a7dcc08496c538aeeb8bc6ecc1f72af56cd773d04	2	0
Chafer Activity	Florian Roth, Markus Neis, Jonhnathan Ribeiro, Daniil Yugoslavskiy, oscd.community	Sigma Integrated Rule Set (GitHub)	01364fb1c5ccb780456530afa742fccc7c5de42d1cbac829fd6f4c435888f499	2	0
CrackMapExecWin	Markus Neis	Sigma Integrated Rule Set (GitHub)	4937cb1804ae450d1760b136159503b4a353a27a37e6b66253c12834ae1fa611	2	0
Credential Dumping Tools Service Execution	Florian Roth, Teymur Kheirkhabarov, Daniil Yugoslavskiy, oscd.community	Sigma Integrated Rule Set (GitHub)	61e2aaf48c321983d311349f6bced27944c28bcd53f96ee143d8a0a1c321a5f2	2	0
Decode DLL Via Certutil	Joe Security	Joe Security Rule Set (GitHub)	512a021b2a6002cdc06a23350dd7744a78311e5eacbe59b19864a594b50fc33e	2	0
Disable Microsoft Office Security Features	frack113	Sigma Integrated Rule Set (GitHub)	db422d3f89e405109467a926cbee52085ff1a33cf97bc054529a03a316dafa2e	2	0
Dnscat Execution	Daniil Yugoslavskiy, oscd.community	Sigma Integrated Rule Set (GitHub)	c625578e8b4d44c52ee346e1df82116ed7e4896e4caad93d0fdb7fba487dbfdf	2	0
Domain Trust Discovery	Jakob Weinzettl, oscd.community	Sigma Integrated Rule Set (GitHub)	50137e4985d62ff32fe9acc8ecd34bbc1e546bce28ae9d0c168c5bc0e62c2098	2	0
Encoded IEX	Florian Roth	Sigma Integrated Rule Set (GitHub)	6011c0e706a0ea8a69892186b9808f52466832e2c60ea353b876a15100a2c891	2	0
Evrial Stealer (Sysmon detection)	Ariel Millahuel	SOC Prime Threat Detection Marketplace	9d5974817e9c9eeb05c8b60f23de31930c84cb3eb8d247767b7fe7bdbec4ad23	2	0
Execution via WorkFolders.exe	Maxime Thiebaut (@0xThiebaut)	Sigma Integrated Rule Set (GitHub)	50d292f837567defe72f24a4b91ee437943cd8f35d5aedcf15979d3d253d38e9	2	2
HTML Help Shell Spawn	Maxim Pavlunin	Sigma Integrated Rule Set (GitHub)	03c63f09ca0da10cdd578a2b9318266b2f2ac550da5b256d00ce4c0cbbbedda0	2	0
Hijack Legit RDP Session to Move Laterally	Samir Bousseaden	Sigma Integrated Rule Set (GitHub)	69573f6b1ce64e7122c33aec2473e20ddf52e90291907115ac5515a58660b7dd	2	0
Invoke-Obfuscation Via Use Clip	Nikita Nazarov, oscd.community	Sigma Integrated Rule Set (GitHub)	1c3ea7c0333da16496964e50a5e57012a3b70695f952212351e08d08530da6d0	2	0
LSASS Process Memory Dump Files	Florian Roth	Sigma Integrated Rule Set (GitHub)	532253e22b4c2a6410e693838434b30d959a9ebc0c04a0c861eeb9d593879009	2	0
LockerGoga Ransomware	Vasiliy Burov, oscd.community	Sigma Integrated Rule Set (GitHub)	0c0ba5aebd0db3facb25385b2dbdc2b2a34be391da1993bc8a02c689608fba16	2	0

MSExchange Transport Agent Installation	Tobias Michalski	Sigma Integrated Rule Set (GitHub)	7e012de38821878c4217e8f825643266daebb69300fb51da895c540db3ca6916	2	2
Meterpreter or Cobalt Strike Getsystem Service Installation	Teymur Kheirkhabarov, Ecco, Florian Roth	Sigma Integrated Rule Set (GitHub)	9fd506c795090efa401ad8bb755474601cc0aaa7ebf5b75b096714bd0235016a	2	0
NTFS Vulnerability Exploitation	Florian Roth	Sigma Integrated Rule Set (GitHub)	411eb79dfeb1cc205d22228842bf9c45f6ea648d10de8bf3d08e9bdaa31e9d1f	2	0
New DLL Added to AppInit_DLLs Registry Key	Ilyas Ochkov, oscd.community, Tim Shelton	Sigma Integrated Rule Set (GitHub)	6f134f381913ef9221138f615280ca41e252e823168d7d580ab6e713e10beca2	2	0
New Hidden Tear ransomware variant	Ariel Millahuel	SOC Prime Threat Detection Marketplace	92dd4e3ca17ea4f0bdfb71304a8fcbbd234749a15c0c26579fac17253c4b2463	2	0
Office Security Settings Changed	Trent Liffick (@tliffick)	Sigma Integrated Rule Set (GitHub)	7210b6208abd6826bfdb8d8666ae792549157fe8070e355cad577fd8f9ef6499	2	0
PowerShell Get-Process LSASS in ScriptBlock	Florian Roth	Sigma Integrated Rule Set (GitHub)	cac21fdc92116671a9e24502beff8b3cc9b77c6d7a23b8f10aefa65821fd9014	2	0
Powershell Profile.ps1 Modification	HieuTT35	Sigma Integrated Rule Set (GitHub)	25ba0fd933ae7d522dfbe81f445736e4bb4015e2ab0ce76d436c139485e79e2e	2	0
Powershell Trigger Profiles by Add_Content	frack113	Sigma Integrated Rule Set (GitHub)	9ed950c94ef5dce1af4ac6ba1eb25704edd170e1a75506e3095eb362e63eab6b	2	0
PurpleSharp Indicator	Florian Roth	Sigma Integrated Rule Set (GitHub)	8cdb5f2da7eb9e3002ce4bbdd8a373b7dcd25103b4373f9b672e54f74c5316e0	2	0
Ranumbot Trojan (Sysmon detection)	Ariel Millahuel	SOC Prime Threat Detection Marketplace	9adcf2b748c0913ce46ec2734223045df982e2a86948b8740a48edd412720e70	2	0
Recon Information for Export with Command Prompt	frack113	Sigma Integrated Rule Set (GitHub)	e49a78894a2986a5fb30eb4ab25cd648d87db2a35906c29afc8fa6d7664f5e63	2	0
SamoRat Behavior (sysmon detection)	Ariel Millahuel	SOC Prime Threat Detection Marketplace	8a1644eccd8d683fe61a26387c655e1d85bff90b49640b5d8c65940e4e1973d0	2	0
Script Event Consumer Spawning Process	Sittikorn S	Sigma Integrated Rule Set (GitHub)	99d3f28b790cc9edbf77b5fddd446d2ec05f85ee550310a2a3863e3171a9bd54	2	0
Suspicious Dump64.exe Execution	Austin Songer @austinsonger, Florian Roth	Sigma Integrated Rule Set (GitHub)	5b1f1b40ef6ce717bbb2c8bc6cae3ad4d4530c3d907caaf29c131d784777fc01	2	0
Suspicious Esentutl Use	Florian Roth	Sigma Integrated Rule Set (GitHub)	6374ec2e5ca4f1bca3332d137882a6526e7230b5207c4de514d3b0a0a1e94fcb	2	0

Suspicious Get Local Groups Information with WMIC	frack113	Sigma Integrated Rule Set (GitHub)	386f2bc7492f0e981a3ff4d07a1e865250fb5f4de55f43a70e9ca3e91bd61e31	2	0
Suspicious Printer Driver Empty Manufacturer	Florian Roth	Sigma Integrated Rule Set (GitHub)	69f693a2bf7b4c283ad2afbd17043a7a25fd7596d7f26f5f77436d56ba9529e8	2	0
Suspicious Shells Spawn by SQL Server	FPT.EagleEye Team, wagga	Sigma Integrated Rule Set (GitHub)	084aa83f6231ad8f1641d3a19e8fd1cfef9a9cc7c1be4c416fdaf86ff56071fa	2	0
WMI Backdoor Exchange Transport Agent	Florian Roth	Sigma Integrated Rule Set (GitHub)	b02fbc5fd12d501dbd78749545483c506550bfb474efa9683e58ac4b2e4211b0	2	1
Wsreset UAC Bypass	Florian Roth	Sigma Integrated Rule Set (GitHub)	96334f64d755424fcec72b4881263e66f022d62103fd2ada696b2264912d1cf5	2	0
ZOHO Dctask64 Process Injection	Florian Roth	Sigma Integrated Rule Set (GitHub)	d0e9ddaa18a4b91ef3ab1e800b63bf10c6cc73617c12d346033dea7e84c6e584	2	2
ZxShell Malware	Florian Roth, oscd.community, Jonhnathan Ribeiro	Sigma Integrated Rule Set (GitHub)	9f3c5ba78b1be158567ab3b450ff989c464b256ea5a1f60dbf4fdf93d57d249d	2	0
Advanced IP Scanner	@ROxPinTeddy	Sigma Integrated Rule Set (GitHub)	654d8ac633b50e98138bcb448019dd2fcb8c0384ae47263728f8b4fd84b8ba98	1	0
Advanced IP Scanner	@ROxPinTeddy	Sigma Integrated Rule Set (GitHub)	946d2bbdd10c544f6435f9b58d066f0d418f7bf78478848e179abdd8b5ec19b8	1	0
Audio Capture via SoundRecorder	E.M. Anhaus (originally from Atomic Blue Detections, Endgame), oscd.community	Sigma Integrated Rule Set (GitHub)	9d251711b5a07fe8fb5fa341d8312ddbf0fd1b878b4a2d04e5feebb9885f1067	1	0
Cerber Ransomware	Ariel Millahuel	SOC Prime Threat Detection Marketplace	73c0a64c5562e339d22b6dd8487f58f08f817a078ee2d99fa508f2bcec9487d2	1	0
Changing RDP Port to Non Standard Number	frack113	Sigma Integrated Rule Set (GitHub)	dc0c536bf76ee17ec594024c9b331e97f259d945e0c52ca0f468b6d323906d8b	1	0
Cmd.exe CommandLine Path Traversal	xknow @xknow_infosec	Sigma Integrated Rule Set (GitHub)	66a17168752e700a1b57242bfc6b9a345959b5142a99316865e1d44df709c32f	1	0
CobaltStrike Service Installations	Florian Roth, Wojciech Lesicki	Sigma Integrated Rule Set (GitHub)	d47c2221db7aa13e5c3645ca6ec5b315a643a4b9f5a9e50af5bece9e79885196	1	0
CobaltStrike Service Installations in Registry	Wojciech Lesicki	Sigma Integrated Rule Set (GitHub)	eaeadfa6378455d35bc7d294a678cf68a5a8c6c2b5417d038a80d96bdf2e76de	1	0
Code Execution via Pcwutl.dll	Julia Fomina, oscd.community	Sigma Integrated Rule Set (GitHub)	d893a429c2ce543e3a265b3794e1845676e899c8dab1ac888aca5607d9821ae7	1	0
CreateMiniDump Hacktool	Florian Roth	Sigma Integrated Rule Set (GitHub)	8618cac2c2c1ec1d0e5b729eab2f28a1585a023728c5aaa9fa184b786b52a337	1	0

Custom Class Execution via Xwizard	Ensar Şamil, @sblmsrsn, @oscd_initiative	Sigma Integrated Rule Set (GitHub)	c0bd5b42809f6cdda07709c25bc0f42cbb0a674ce80ec8c63788ef1efd31cdc5	1	0
Detected Windows Software Discovery	Nikita Nazarov, oscd.community	Sigma Integrated Rule Set (GitHub)	01357d5e887b9f5de970cbdf4e5303b1faff6ff0de49e5ae4c516f933c8a951b	1	0
Domain Trust Discovery	Den Iuzvyk	SOC Prime Threat Detection Marketplace	4fba485fa9f02eb8d0e28a7b84276fb6a276943a2948a62fe3d614248af840fd	1	0
Dotnet.exe Exec Dll and Execute Unsigned Code LOLBIN	Beyu Denis, oscd.community	Sigma Integrated Rule Set (GitHub)	3fba0f206c1c867f04a34552b850e8eeb0b219621923d394bddad4789f293152	1	0
Drops a DLL with WLL extension to the startup	Joe Security	Joe Security Rule Set (GitHub)	0a0b097696bd0b36b7d1443e446cbff6c2146d7a93cacaf2838ed0fe366b61d9	1	0
Enable Restricted Admin Mode To Bypass MFA (via sysmon)	SOC Prime Team	SOC Prime Threat Detection Marketplace	7b0a12d70498be6b75106baeadc6572fa8f03b6e6ce96998c3c84f14e5dd19a6	1	0
Execution in Webserver Root Folder	Florian Roth	Sigma Integrated Rule Set (GitHub)	d11dfd4a7ffb536505adf98a4b97c1540b6e89a26661bf9f238b4a4d8f3133a9	1	0
Hide copy and delete itself	Joe Security	Joe Security Rule Set (GitHub)	e491fecd17c16aecfb3b5ac96288fcdcf7c8ec061a8b1649da4e907b511f1208	1	0
IIS Native-Code Module Command Line Installation	Florian Roth	Sigma Integrated Rule Set (GitHub)	cc3ea4eefe5144350cce95a37a83b5a54cb1c3588b6a08901eb81ce60a358d20	1	0
Indirect Command Execution By Program Compatibility Wizard	A. Sungurov , oscd.community	Sigma Integrated Rule Set (GitHub)	d4b25cba1a95e034ae6766147690611472b8ce274332b1aee27da6faa04335a0	1	0
Invoke-Obfuscation Via Stdin	Nikita Nazarov, oscd.community	Sigma Integrated Rule Set (GitHub)	92f548de44082f5573a9a1cde5e0716b71988288605c254b85f32d8f3405ef83	1	0
Invoke-Obfuscation Via Use Clip	Nikita Nazarov, oscd.community	Sigma Integrated Rule Set (GitHub)	cf3869e5aa623f0e8acc74d1afaf5036cb7bbbcb1418a1af1670aef332fd2115	1	0
Malicious PE Execution by Microsoft Visual Studio Debugger	Agro (@agro_sev), Ensar Şamil (@sblmsrsn), oscd.community	Sigma Integrated Rule Set (GitHub)	833d1e3036176fa960339790e9389d39187ba0c444aa4b1f1d3adc81c860b9fd	1	0
Malicious Payload Download via Office Binaries	Beyu Denis, oscd.community	Sigma Integrated Rule Set (GitHub)	f8ff90356c4ca9019d85273206850b0132e8b3209bcc1d4931bf59b71450a496	1	1

Malicious Service Installations	Florian Roth, Daniil Yugoslavskiy, oscd.community (update)	Sigma Integrated Rule Set (GitHub)	8054438d5b821755b2dbd5820a438b44688606dc8617bca3756bd60c75e15aee	1	0
Mavinject Inject DLL Into Running Process	frack113	Sigma Integrated Rule Set (GitHub)	22a0144a5fa16f342a409df0a0b3ea1292a72b8e43c7c844bf06d68f5330fbf4	1	0
Moriya Rootkit	Bhabesh Raj	Sigma Integrated Rule Set (GitHub)	14054e3c5398e3efeb36907b873cd44b2e3e1f45c872fd35fc93fe027f026822	1	0
Netsh Helper DLL	Den Iuzvyk	SOC Prime Threat Detection Marketplace	67f08eeb3f74c7dcf4b8985150f3df56b390aec0e1d3edb45a75c360f73c0134	1	1
New Shim Database Created in the Default Directory	frack113	Sigma Integrated Rule Set (GitHub)	c028d3fbfe3db756b5129f320616cde63b9929b02e91fb76c1b12fb726eafb71	1	0
Office starup folder persistance.	Den Iuzvyk	SOC Prime Threat Detection Marketplace	4f71ac3f10bbbdb0bda74ee81dba1206ffd26e184cc17f7391a0ca82ad838257	1	0
Password Provided In Command Line Of Net.exe	Tim Shelton (HAWK.IO)	Sigma Integrated Rule Set (GitHub)	356834a41f1b8ed94c954435f27d64f970ba67b17ac5474ddb8357cfbb8de8d8	1	0
Ping Hex IP	Florian Roth	Sigma Integrated Rule Set (GitHub)	a78012a975b5cccbdd9caf22ce8a5065aa442b2459190ab2a3a0b39e1eb66bee	1	0
Possible Privilege Escalation via Weak Service Permissions	Teymur Kheirkhabarov	Sigma Integrated Rule Set (GitHub)	6a8c7191c56707b059d6c77b850fd9a1f9bc6c202dd771d100565edecef8686b	1	0
Possible SPN Enumeration	Markus Neis, keepwatch	Sigma Integrated Rule Set (GitHub)	5185237d06d1d2c6fa9f5b9940219760620e7dd4f1db2fbff05f0b081ce4967e	1	0
PowerShell ADRecon Execution	Bhabesh Raj	Sigma Integrated Rule Set (GitHub)	8f33121f45ae912b9307a03c4dc5d5309016b47eb4b2d937c74e55cda019203e	1	1
Powershell delayed execution via ping command	Joe Security	Joe Security Rule Set (GitHub)	9a4875b9a93f7ed6dd4f6259f58f0ff372f1351c267c6d112364a3064aeae82f	1	0
Process Dump via Comsvcs DLL	Modexp (idea)	Sigma Integrated Rule Set (GitHub)	fc647ef855e070dd8c71ac9bee02eb59a9124eded234012d31fef82c72b8c1b0	1	0
PsExec/PAExec Escalation to LOCAL SYSTEM	Florian Roth	Sigma Integrated Rule Set (GitHub)	95ab10477326346ad231600df85597b403502c24947739b6a2b5bf75469a3024	1	0
Recon Information for Export with PowerShell	frack113	Sigma Integrated Rule Set (GitHub)	713f92f086b68096c3f56ca930b031275ba60fcd9b0986dca0e69d63a349fe11	1	0

Registry Key Creation or Modification for Shim DataBase	frack113	Sigma Integrated Rule Set (GitHub)	8c893b41c5a28ef36c6b16d709f057af26436898776837e685d30b93672c2de1	1	0
Renamed MegaSync	Sittikorn S	Sigma Integrated Rule Set (GitHub)	5ed404c9cabd248ba80d6d5852fc81ff9c668726a632eb06be9595bd5b80d869	1	0
Run Once Task Execution as Configured in Registry	Avneet Singh @v3t0_, oscd.community	Sigma Integrated Rule Set (GitHub)	a670267e081a215d8a32b1cf6cb799023ff0667dc9da2d474cf20a91e4f2a2cc	1	0
Scarab Ransomware	Ariel Millahuel	SOC Prime Threat Detection Marketplace	c3b33a6ba821d844c3bfc5a217489aca877dc9bc6c76c84e4d8cabd6a320bd7b	1	0
Shadow Copies Access via Symlink	Teymur Kheirkhabarov, oscd.community	Sigma Integrated Rule Set (GitHub)	3b5b0346a9d3b5b510bfd33a67662439c44419ada001c73160bdcc75d76b2d3b	1	0
Suspicious AdFind Execution	FPT.EagleEye Team, omkar72, oscd.community	Sigma Integrated Rule Set (GitHub)	cb903e3e20e158519f1431d1978e1d50abf68706bbedd496258a99a785f2ec00	1	0
Suspicious Certreq Command to Download	Christian Burkard	Sigma Integrated Rule Set (GitHub)	90480b0d96dd273a177b536ad0b17f114b0426bdb4c6e04d4692da954658bac1	1	0
Suspicious Desktopimgdownldr Command	Florian Roth	Sigma Integrated Rule Set (GitHub)	beb013be28477c7cc6a96b5e49885366af682311b00c0ad036f6df272f0d73bf	1	0
Suspicious PrinterPorts Creation (CVE-2020-1048)	EagleEye Team, Florian Roth	Sigma Integrated Rule Set (GitHub)	9f4d9015afcdadf3e8a90bd3b8b01cae40397eca61dc45580339296224e1b40f	1	0
SyncAppvPublishingServer VBS Execute Arbitrary PowerShell Code	frack113	Sigma Integrated Rule Set (GitHub)	37beaf97b85714dccecd452e684c29d067adea49095ddf3ec6631dc8acf14337	1	0
UAC Bypass Using ChangePK and SLUI	Christian Burkard	Sigma Integrated Rule Set (GitHub)	a334f66679d3e373f49f08113614e79457c624e8ef315085de12c285bc5d7d4e	1	0
UAC Bypass via Event Viewer	Florian Roth	Sigma Integrated Rule Set (GitHub)	c7f53a29488cdfc8b3ab7ecb4699f5c655615954b2d1ff9209e2dba026e30dbc	1	0
VMToolsd Suspicious Child Process	behops, Bhabesh Raj	Sigma Integrated Rule Set (GitHub)	bd7b9679a8b4de81c85050399fe9679a23a1ea3bb48ef31509d208152db750f4	1	0
WINEKEY Registry Modification	omkar72	Sigma Integrated Rule Set (GitHub)	585081efe7df5aaf634ee8b6187b3f8adb0c8156cbcc8f25867ffec4654fc697	1	0
Webshell Detection With Command Line Keywords	Florian Roth, Jonhnathan Ribeiro, Anton Kutepov, oscd.community	Sigma Integrated Rule Set (GitHub)	fadc206ec1e9e99804969634aed9b633228630e0a72122317cd3e674846a8c7c	1	0

Windows Credential Editor	Florian Roth	Sigma Integrated Rule Set (GitHub)	efb250f52392ac4446104881ff38dafa4934fa84d2f3357065c51b4873c737fc	1	0
Winnti Malware HK University Campaign	Florian Roth, Markus Neis	Sigma Integrated Rule Set (GitHub)	fa921a7a680703d8b1c263a0eba9bec48b3361492b6ea0424931dba980c317fd	1	0
msiexec download and execute	Joe Security	Joe Security Rule Set (GitHub)	80df93b91d026bd6faf3f28497aecc8b5a81a6553fe9336a204b11f4dcef8733	1	0
(SIGRED) CVE-2020-1350 DNS Remote Code Exploit [via HTTP/Proxy Logs]	SOC Prime Team	SOC Prime Threat Detection Marketplace	2c660e94b9dd36c78c57a2250c28533823a79106701103f8b2a662501cc2a379	0	0
(SIGRED) CVE-2020-1350 DNS Remote Code Exploit [via HTTP/Proxy Logs]	SOC Prime Team	SOC Prime Threat Detection Marketplace	f45ee46c268733c28e2e456cd180b06976bca8e8fc0819a141d83778e7e6908b	0	0
AD Object WriteDAC Access	Roberto Rodriguez @Cyb3rWard0g	Sigma Integrated Rule Set (GitHub)	58cec962c267e019fa838d36e02695d7254409214165d3ac1363b49e8711131a	0	0
AD Privileged Users or Groups Reconnaissance	Samir Bousseaden	Sigma Integrated Rule Set (GitHub)	14cbefe2ccc7618cf17e2c9b92743b97fbf394277a7c17c58ebb3d942aa0a0fd	0	0
AD User Enumeration	Maxime Thiebaut (@0xThiebaut)	Sigma Integrated Rule Set (GitHub)	1a4024d9c095d28a1da18eb257926feded8ec7d7ea03762f6eab63b22a41721e	0	0
ADCS Certificate Template Configuration Vulnerability	Orlinum , BlueDefenZer	Sigma Integrated Rule Set (GitHub)	6d83e2c5d3c8dd6baf3897d1fcfef08e8e7745f60a8712ff35acc679d26b2db6	0	0
ADCS Certificate Template Configuration Vulnerability with Risky EKU	Orlinum , BlueDefenZer	Sigma Integrated Rule Set (GitHub)	145c680f84c610717ce0f64126642e2075071657c6b04077e58c08042f45b3dd	0	0
ADCSPwn Hack Tool	Florian Roth	Sigma Integrated Rule Set (GitHub)	945059b9924f612aec04c225310cee7009f0951805322568a62ebbefb71e63b0	0	0
ADFS Adapter Process Spawns (via cmdline)	SOC Prime Team, Microsoft	SOC Prime Threat Detection Marketplace	5b090817d20c98f190eec819a6c655b46a96324e58e3195a7f9c5e076fae6acb	0	0
ADFS Database Named Pipe Connection	Roberto Rodriguez @Cyb3rWard0g	Sigma Integrated Rule Set (GitHub)	4066789e2f52a62b211079b31d3fecc622acde6f0aab1c5127584333f498102c	0	0
ADSelfService Exploitation	Tobias Michalski, Max Altgelt	Sigma Integrated Rule Set (GitHub)	adb52649fba655a7c618328f8a47138b0829cd7ee3ff23c599542d6103b29a92	0	0
AKO Ransomware	Ariel Millahuel	SOC Prime Threat Detection Marketplace	bb075da0c850b7587ce9434aef02a948171b3545ebd0914125d7f5fe4fa590dd	0	0

APT 37	Ariel Millahuel	SOC Prime Threat Detection Marketplace	2c9099b138fc55d5fdb1dce07ff366a656ee06b6ff8dd57d238ce00e61809e4e	0	0
APT PRIVATELOG Image Load Pattern	Florian Roth	Sigma Integrated Rule Set (GitHub)	396dd003148797c25c2cb63e8f2c6e0b3973ed37675f9c214f6a40a269c94131	0	0
APT User Agent	Florian Roth, Markus Neis	Sigma Integrated Rule Set (GitHub)	e2b73603c9441b256be9bab1ccd758407a6d6470859f0f6cb838ff2eadc08006	0	0
APT29 Google Update Service Install	Thomas Patzke	Sigma Integrated Rule Set (GitHub)	34f4cff056f24abe91bb29dc04a37ee746a4255101a21724b9ff28d79785247a	0	0
APT29 Google Update Service Install	Thomas Patzke	Sigma Integrated Rule Set (GitHub)	e6247b8fe178e47b7e98f318da90608dc7aaf94fa99fe8e933f0a05b6498bdb4	0	0
APT40 Dropbox Tool User Agent	Thomas Patzke	Sigma Integrated Rule Set (GitHub)	572ac9027db60bae5654b7a9bc5d58e315db0810b08d8142c6db54f5e9e7ed24	0	0
AWL Bypass with Winrm.vbs and Malicious WsmPty.xsl/WsmTxt.xsl	Julia Fomina, oscd.community	Sigma Integrated Rule Set (GitHub)	1d0bd876f993864d8a65e33ce45e152f3e49063e858a74169b77923d673483a8	0	0
AWL Bypass with Winrm.vbs and Malicious WsmPty.xsl/WsmTxt.xsl	Julia Fomina, oscd.community	Sigma Integrated Rule Set (GitHub)	3f84ecf411a71bd8d115a14303c8eac0baf1a7d57c27f81e99c78b2bff51f3c5	0	0
AWL Bypass with Winrm.vbs and Malicious WsmPty.xsl/WsmTxt.xsl	Julia Fomina, oscd.community	Sigma Integrated Rule Set (GitHub)	d51a28a580a981a8c30c17c8985ac1d2bb9187f6dd4a55cf24b6f0c4cfc4c1f4	0	0
AWS Attached Malicious Lambda Layer	Austin Songer	Sigma Integrated Rule Set (GitHub)	0650616005d1cf25b22be420f69ef9f6271137f0d29697a56f3346877ffd37f8	0	0
AWS CloudTrail Important Change	vitaliy0x1	Sigma Integrated Rule Set (GitHub)	4ef2dc5f6a20a823034706154832eb2b6caacbdd7526d5f72b41b87b661c18b9	0	0
AWS Config Disabling Channel/Recorder	vitaliy0x1	Sigma Integrated Rule Set (GitHub)	1ca012603accfb34b464b1a408012216374690743be9979de051b99b95859e64	0	0
AWS EC2 Disable EBS Encryption	Sittikorn S	Sigma Integrated Rule Set (GitHub)	7cc31b5a6e3bb9dfe917930e9cff98c24e1477f39b93c17de733f572469e6746	0	0
AWS EC2 Download Userdata	faloker	Sigma Integrated Rule Set (GitHub)	52870d4d2756b6f3dde8066072d0df3fffc2208a2f13a11ad8dda6663fc6c12d	0	0
AWS EC2 Startup Shell Script Change	faloker	Sigma Integrated Rule Set (GitHub)	839d04c92bee18b43af5b78244d9a121efb5f27e4eebc842ae6c62a6c9e4b4f3	0	0

AWS EC2 VM Export Failure	Diogo Braz	Sigma Integrated Rule Set (GitHub)	510922d4a963b58fd4765ade7ccec8ec0d323813387711be4acd2577afcd50d5	0	0
AWS EFS Fileshare Modified or Deleted	Austin Songer @austinsonger	Sigma Integrated Rule Set (GitHub)	320cb5ec91c7d2c86ae27ee1a995b6a6fad692c4dd4716db1bddc009cef68f24	0	0
AWS EFS Fileshare Mount Modified or Deleted	Austin Songer @austinsonger	Sigma Integrated Rule Set (GitHub)	557ffbb2dc96ead10718f0ce8e23abbd4520126cb5eb85b94b8f3d19e7ff6442	0	0
AWS EKS Cluster Created or Deleted	Austin Songer	Sigma Integrated Rule Set (GitHub)	633e9cc212d624837b46fa0381b5cb0f70e8a41bb219ae76550b862d16340cc1	0	0
AWS ElastiCache Security Group Created	Austin Songer @austinsonger	Sigma Integrated Rule Set (GitHub)	82c9482509e59596843bf9c369a8a818e8248c0b8cd43217762ccd4546d5471e	0	0
AWS ElastiCache Security Group Modified or Deleted	Austin Songer @austinsonger	Sigma Integrated Rule Set (GitHub)	886c07a825a6d3bd1d71d9238ecd1c47fe341acccd997dfca9df6d55d0ce1924	0	0
AWS Glue Development Endpoint Activity	Austin Songer @austinsonger	Sigma Integrated Rule Set (GitHub)	535cda9e5250683c27341783e572cb03b5946e3a3930ed6e7ec71fb51411adc6	0	0
AWS GuardDuty Important Change	faloker	Sigma Integrated Rule Set (GitHub)	315526975358ad2d0fa1b5c44442eda68a1a8a523b0c894de935ec21708b66ab	0	0
AWS IAM Backdoor Users Keys	faloker	Sigma Integrated Rule Set (GitHub)	8ccb5db92041ee60e6fab70bedfd8e59fb916edc1226612863ffd244a78e453d	0	0
AWS Lambda Function Created or Invoked	Austin Songer @austinsonger	Sigma Integrated Rule Set (GitHub)	3bf7f1b2fd7fe897356a4416891664478c352bcff4a562abbb4e29d59be58cad	0	0
AWS Macie Evasion	Sittikorn S	Sigma Integrated Rule Set (GitHub)	2caf12ef20a741df57dbd3af15b2018c587c7143520a8c077a4fb25e6dd8d75e	0	0
AWS RDS Master Password Change	faloker	Sigma Integrated Rule Set (GitHub)	5ce71a8dd2051186eb3bc827687f0161dcd856a3aa78737ffc610f6040d4166c	0	0
AWS Root Credentials	vitaliy0x1	Sigma Integrated Rule Set (GitHub)	9a3dad9567f385fd12f06417761f939eaf3bc223c50daac4c997e6f50f690b0c	0	0
AWS Route 53 Domain Transfer Lock Disabled	Elastic, Austin Songer @austinsonger	Sigma Integrated Rule Set (GitHub)	91af3f000e86d4d90b8e282d15d62993f5d5ca87f5375dee075988c20a572c22	0	0
AWS Route 53 Domain Transferred to Another Account	Elastic, Austin Songer @austinsonger	Sigma Integrated Rule Set (GitHub)	79dd906114c4b150b65cf759c1c0d1d83d74766afc2feb337b08ee12e340a013	0	0

AWS S3 Data Management Tampering	Austin Songer @austinsonger	Sigma Integrated Rule Set (GitHub)	14d9fe2befc885c1ed6ef46a55bc25f96407917c2385e324b8515b53a65d4b36	0	0
AWS STS AssumeRole Misuse	Austin Songer @austinsonger	Sigma Integrated Rule Set (GitHub)	ab071ff54304ef514871c1e84cc731ded005fa0ccda3b66616554a41d88efa5e	0	0
AWS STS GetSessionToken Misuse	Austin Songer @austinsonger	Sigma Integrated Rule Set (GitHub)	6994df5208389be2d74373903274ef547c51d5eed02015e25e143b1932795aef	0	0
AWS SecurityHub Findings Evasion	Sittikorn S	Sigma Integrated Rule Set (GitHub)	4e8ffcd6780ba56d1f2fa59f77317ebf859a2bf43c4be7719f81b9e03dd5c83d	0	0
AWS Suspicious SAML Activity	Austin Songer	Sigma Integrated Rule Set (GitHub)	173a650247a0aa08e4f7d1fbb1ab2154526c9f23e45d9bbfaab1313385bc23ac	0	0
AWS User Login Profile Was Modified	toffeebr33k	Sigma Integrated Rule Set (GitHub)	943930b25869dfad30c94e1eec864e899816b0d8b783767e1940cd6e0138d53c	0	0
Abusable Invoke-ATHRemoteFXvGPUDisablementCommand	frack113	Sigma Integrated Rule Set (GitHub)	1ed460e3d1d675508d6550ae97b5b02fb7d2a41633cf104dd13ec5e3898fb4d8	0	0
Abusable Invoke-ATHRemoteFXvGPUDisablementCommand	frack113	Sigma Integrated Rule Set (GitHub)	3f23a6c297c45d5a9d63d790d48c7f197bedbf2e2a62d28b67dec7a5a79e3196	0	0
Abusable Invoke-ATHRemoteFXvGPUDisablementCommand	frack113	Sigma Integrated Rule Set (GitHub)	aa47fee25ec87cbc15062b8d3f7e0acb8e38a64de307365aeec8cfbe02f12c8e	0	0
Abusable Invoke-ATHRemoteFXvGPUDisablementCommand	frack113	Sigma Integrated Rule Set (GitHub)	c16e468ec3aab5a450c958946bf9ad962dd0a0b337178f1bdc125ca014779760	0	0
Abusable Invoke-ATHRemoteFXvGPUDisablementCommand	frack113	Sigma Integrated Rule Set (GitHub)	cb8936fcf36d16982575da13504782d400992adaac08cd26ba7845c4a4279dee	0	0
Abusable Invoke-ATHRemoteFXvGPUDisablementCommand	frack113	Sigma Integrated Rule Set (GitHub)	e78750ceeb186d5ea5bbcfb7f9ba741b6d8d9978b25212d97a252621b5af87cf	0	0
Abuse of Service Permissions to Hide Services in Tools	Andreas Hunkeler (@Karneades)	Sigma Integrated Rule Set (GitHub)	31469fa3c8d37b7e80913d07ce5549c9371e193ac3f0d3211f519adbb2de950c	0	0
Abusing Azure Browser SSO	Den Iuzvyk	Sigma Integrated Rule Set (GitHub)	08cc3358fc66df84bafea574255088ebf9e6d0b56cc08317abc1bc31f94bab4b	0	0
Abusing Azure Browser SSO	Den Iuzvyk	SOC Prime Threat Detection Marketplace	3a3618c16315d61e28176798a3bb0420bd03a4732de42920b67e1c038effc0cc	0	0
Abusing Print Executable	Furkan CALISKAN, @caliskanfurkan_, @oscd_initiative	Sigma Integrated Rule Set (GitHub)	f96e4beae00ea6ddb52dd039e1527892e6c52cdc577988ec8e7730fd3b4cd9a7	0	0

Abusing Windows Telemetry For Persistence	Sreeman	Sigma Integrated Rule Set (GitHub)	215ab0e3f729db474131b73eb9950bd1decd0ab51c4d221a489c48004d3684e0	0	0
Abusing Windows Telemetry For Persistence	Sreeman	Sigma Integrated Rule Set (GitHub)	29f4b4ab96f93520895ca3d47ccf106f5a6fecadf74906d79a302829883cd114	0	0
Abusing Windows Telemetry For Persistence	Sreeman	Sigma Integrated Rule Set (GitHub)	37508447092b61198dba6c2077887c7bd32c0396716095cb8e25593a16b30929	0	0
Abusing Windows Telemetry For Persistence	Sreeman	Sigma Integrated Rule Set (GitHub)	9fc475ae448749ce7b6c7760c27eaa960cebb3e61dd32ccdd1ffa55dc831eff2	0	0
Abusing Windows telemetry CompatTelRunner.exe(Audit Rule)	Den Iuzvyk	SOC Prime Threat Detection Marketplace	879510fbd52dc559762564e9dcee6b800c7ebe8846c237911775cf3f6d8d3cd9	0	0
Abusing Windows telemetry CompatTelRunner.exe(Sysmon Behavior)	Den Iuzvyk	SOC Prime Threat Detection Marketplace	18fa931666e2ae680fb1e0dcec0ba06dadd31ca6b52d9c619bb42fca8b7d7048	0	0
Access to ADMIN$ Share	Florian Roth	Sigma Integrated Rule Set (GitHub)	9b8b6fde8104ca3626c27c746a6e6e07d3f8c89905e685f9a05cb5f6f4edc379	0	0
Accesschk Usage After Privilege Escalation	Teymur Kheirkhabarov (idea), Mangatas Tondang (rule), oscd.community	Sigma Integrated Rule Set (GitHub)	cd3d7a697c3c3677aa8da2c29a31ba2c427c6efdde2818deab23f432540c2193	0	0
Accessing Encrypted Credentials from Google Chrome Login Database	frack113	Sigma Integrated Rule Set (GitHub)	51e8e5e690970ad68d784525926120f9a5afde96ebd20253e92cea0d07d54399	0	0
Accessing WinAPI in PowerShell for Credentials Dumping	oscd.community, Natalia Shornikova	Sigma Integrated Rule Set (GitHub)	a683beca7674cad333d64a1ffe5ac971414b265f15a99e2f9d2c7ff967cc2fe2	0	0
Accessing WinAPI in PowerShell. Code Injection.	Nikita Nazarov, oscd.community	Sigma Integrated Rule Set (GitHub)	780e368b7c4c2665f3cbcc6184c03b9147726ab5239f4c01341cbc02775dafda	0	0
Account Enumeration on AWS	toffeebr33k	Sigma Integrated Rule Set (GitHub)	c2d1da71047d12f3e9e82a9b10ae31b7f37c8a89483a537c7049c6f83abd4cb0	0	0
Account Lockout	AlertIQ	Sigma Integrated Rule Set (GitHub)	1fe55c2a4747185813415dd5f4e3e497c4f1fc14e546ea9fe496f104438a0870	0	0

Account Tampering - Suspicious Failed Logon Reasons	Florian Roth	Sigma Integrated Rule Set (GitHub)	5589ef9f2fa4b4fc38d9e2634cb65b59cc829a86599e808fda10586d97094d5b	0	0
AcidBox Activity	Den Iuzvyk	SOC Prime Threat Detection Marketplace	7036d84b791069d70f9a381859bbfdaf7d37a698a47948b343a49a64ab652cce	0	0
Active Directory Kerberos DLL Loaded Via Office Applications	Antonlovesdnb	Sigma Integrated Rule Set (GitHub)	a2eee7390841d2713ce09ab45175d989688027fe2141938274b88a1dfe11b75c	0	0
Active Directory Parsing DLL Loaded Via Office Applications	Antonlovesdnb	Sigma Integrated Rule Set (GitHub)	6691a047173376a6c37e4a5a5a2ca36610041e928c2900eb7665491f798ff07e	0	0
Active Directory Replication from Non Machine Account	Roberto Rodriguez @Cyb3rWard0g	Sigma Integrated Rule Set (GitHub)	db12e3072dac7d4a4e8f67282fbba19b12ef761b40ea26359caeec8051cefcd2	0	0
Active Directory User Backdoors	@neu5ron	Sigma Integrated Rule Set (GitHub)	b0cd1653d4d8f0519ad99bcf040b2db9dd835f2df6daa9087c3e4e0a13beb319	0	0
Activity Performed by Terminated User	Austin Songer @austinsonger	Sigma Integrated Rule Set (GitHub)	02b84310ae0b2a94f86e5369d7ec39f1a701aed32bc6728b909b446f929745c1	0	0
Activity Related to NTDS.dit Domain Hash Retrieval	Florian Roth, Michael Haag	Sigma Integrated Rule Set (GitHub)	36868991a76ff137e30dea5f77cced4da2254db444c41aa5f83cc7ba6b8fed48	0	0
Activity from Anonymous IP Addresses	Austin Songer @austinsonger	Sigma Integrated Rule Set (GitHub)	efecf6d62b61312f886723f752a5c2ee5188a1bac0ee585294f03e08291d66b8	0	0
Activity from Infrequent Country	Austin Songer @austinsonger	Sigma Integrated Rule Set (GitHub)	b9be4401ecfc9259f3e9b16e77573b0abed2cf0df93e746abce40e64e7cea7d4	0	0
Activity from Suspicious IP Addresses	Austin Songer @austinsonger	Sigma Integrated Rule Set (GitHub)	c020af8eea2544a4fee04ed5143d696c1224c429b3a7871cc87b00b8d5c6cc8f	0	0
Add Port Monitor Persistence in Registry	frack113	Sigma Integrated Rule Set (GitHub)	8dbe594a0f4eb93aed5bfffd0545b03cb0d8c91d229a169700c0d5a7b140795b	0	0
Addition of Domain Trusts	Thomas Patzke	Sigma Integrated Rule Set (GitHub)	f354ac1a99792012ceaef04ee732d816f1a2d9dee2e30492295b794811ed0e46	0	0
Addition of SID History to Active Directory Object	Thomas Patzke, @atc_project (improvements)	Sigma Integrated Rule Set (GitHub)	d755877a01e9e73bfd7efde3363de1b7976022aad16110c5a4b2995a9f8604f2	0	0

Admin User Remote Logon	juju4	Sigma Integrated Rule Set (GitHub)	ba345e8f98204602e6652f9d41bec21ffed8e55fe558a98315201eec3993eefe	0	0
Advanced IP Scanner	@ROxPinTeddy	Sigma Integrated Rule Set (GitHub)	5fbf642a60f85b04f337ffeb9e377bf01fbe1ca8b9325ead915068bbec2ec06c	0	0
Advanced Port Scanner	Nasreddine Bencherchali @nas_bench	Sigma Integrated Rule Set (GitHub)	fb482f5fd709d1ae001f190ee187e694e6ae6473e73b36e57e49b6908a1544c3	0	0
Adwind RAT / JRAT	Florian Roth, Tom Uelтschi, Jonhnathan Ribeiro, oscd.community	Sigma Integrated Rule Set (GitHub)	2430fe9fd6e24946c8534bace62f59a139bd0871a15e594408a81134d905d1c3	0	0
Adwind RAT / JRAT	Florian Roth, Tom Uelтschi, Jonhnathan Ribeiro, oscd.community	Sigma Integrated Rule Set (GitHub)	29d8efa02d53ac611d0b491bedaddbcd34e06668c553dd702b761afceca6d91c	0	0
Adwind RAT / JRAT	Florian Roth, Tom Uelтschi, Jonhnathan Ribeiro, oscd.community	Sigma Integrated Rule Set (GitHub)	40b38a30ad910fcc157b48f5890f35898cc92ae17559bda1764e434dfc37c1d4	0	0
Adwind RAT / JRAT	Florian Roth, Tom Uelтschi, Jonhnathan Ribeiro, oscd.community	Sigma Integrated Rule Set (GitHub)	6b74b152297fb45850c046a229ca64920ee9d973e33fdb61c3954a849baa882e	0	0
AeDebugProtected Reg Key Persistance	Den Iuzvyk	SOC Prime Threat Detection Marketplace	a3febaea6fa1eefc8642f7d848d0b2d4f2b70c0359fa395d9e8ee921c218b36d	0	0
Alternate PowerShell Hosts	Roberto Rodriguez (Cyb3rWard0g), OTR (Open Threat Research)	Sigma Integrated Rule Set (GitHub)	1ff53e9fd6749954464f3ac22171fc115796cbc09d5ac9331d6db4cad674287e	0	0
Alternate PowerShell Hosts	Roberto Rodriguez @Cyb3rWard0g	Sigma Integrated Rule Set (GitHub)	5b34558f1c4d3065989635055533ba223585e99be44e2b0e319dfc6946c50ee2	0	0
Alternate PowerShell Hosts	Roberto Rodriguez @Cyb3rWard0g	Sigma Integrated Rule Set (GitHub)	66d3c05927db71e9d8760c5353ef8a161521b446c0b6cb8ea538a081d2d15e8f	0	0
Alternate PowerShell Hosts	Roberto Rodriguez @Cyb3rWard0g	Sigma Integrated Rule Set (GitHub)	b98a87132b8f25c1b28f308d62a1f37edb6a16c239e5d98a314a15853193b18c	0	0
Alternate PowerShell Hosts Module Load	Roberto Rodriguez @Cyb3rWard0g	Sigma Integrated Rule Set (GitHub)	0b70b2266832f57d7fcd62d232b3b469d8788c9a97ee87dfac1147dbd08533a2	0	0
Alternate PowerShell Hosts Pipe	Roberto Rodriguez @Cyb3rWard0g	Sigma Integrated Rule Set (GitHub)	ba100a757ed85b5b1b191f9aa12c8123ef59a9afd99c6cb8fdaeb4f7bd4e12fa	0	0
Amadey Botnet detection (TA505)	Ariel Millahuel	SOC Prime Threat Detection Marketplace	cec4465383805716c59e96f51fd252bb21a3cba08cb59dfe0e21d49eaaee228a	0	0
Anonymous User Changed Machine Password	SOC Prime Team	SOC Prime Threat Detection Marketplace	5262477d283c94c8a282e110700640abccc3d50d92a485af02adb2a0ed079358	0	0
AntiVM	Joe Security	Joe Security Rule Set (GitHub)	53c56007ae94680c26786bcd895d2087db975d72635c0646c8e0ee8b2ca6539b	0	0

Antivirus Exploitation Framework Detection	Florian Roth	Sigma Integrated Rule Set (GitHub)	b74dd119e6b8a4b8160d85ec696dd1b8f9d9990a6eebdc5abee1ce10d635d8fa	0	0
Antivirus Hacktool Detection	Florian Roth	Sigma Integrated Rule Set (GitHub)	c199a1ab724951efd7b45265fbdd55c15874411108f51d080ff79caf07509ed8	0	0
Antivirus Password Dumper Detection	Florian Roth	Sigma Integrated Rule Set (GitHub)	26728f84df236571280d6d8d3ec2ef0250723676cf344e0e4b29b397901037d5	0	0
Antivirus PrinterNightmare CVE-2021-34527 Exploit Detection	Sittikorn S, Nuttakorn T	Sigma Integrated Rule Set (GitHub)	22284a04af59d3dfb90caff89d34cb8f366f73553f1aa99101a46e88e4200b71	0	0
Antivirus Relevant File Paths Alerts	Florian Roth, Arnim Rupp	Sigma Integrated Rule Set (GitHub)	a3fdf9ece7053d2030dc642bd2eb70cd4c3a3e45f7939313db5d59ae6fec42db	0	0
Antivirus Web Shell Detection	Florian Roth, Arnim Rupp	Sigma Integrated Rule Set (GitHub)	0abd8831aa5efdcfa40c619dadeb24d85fa74d097fa44e68d639accddb2a7e70	0	0
Apache Segmentation Fault	Florian Roth	Sigma Integrated Rule Set (GitHub)	723a6621f9b140b510c7f46523b33c69c2beb3f9e824516e07e5bb83aa5b0d26	0	0
Apache Threading Error	Florian Roth	Sigma Integrated Rule Set (GitHub)	2210d9229d212ebd79a69712d72ae5590caccd7f8c47f91331c431e3394f87ce	0	0
AppInstaller Attempts From URL by DNS	frack113	Sigma Integrated Rule Set (GitHub)	8c20386ca2239562a26b808135071390e3abe7434cb251781a4656b1b4cf71e6	0	0
AppLocker Bypass via Regsvr32	Joe Security	Joe Security Rule Set (GitHub)	2331619a69009fbe3cead24a909b7e9d42ffb14b71caa6d83ee04fce114b10eb	0	0
Application Whitelisting Bypass via Bginfo	Beyu Denis, oscd.community	Sigma Integrated Rule Set (GitHub)	3a9675abeacca74d231073efcc4c362ddc755278240288e69cd34b2f2052cffc	0	0
Application Whitelisting Bypass via Dxcap.exe	Beyu Denis, oscd.community	Sigma Integrated Rule Set (GitHub)	208e2a3b52a6d211e7c5b85a6b02a3d7b276c3d13e266917a5e033a43cc39d85	0	0
Arbitrary Shell Command Execution Via Settingcontent-Ms	Sreeman	Sigma Integrated Rule Set (GitHub)	1eb1f4796a2c05305c0e6fb961bac3fd02861464a7d6bc3d1a35461737101c81	0	0
Arcadyan Router Exploitations	Bhabesh Raj	Sigma Integrated Rule Set (GitHub)	0274ce4cedfe4942275222ff262ad3bc4a6d9230e7d8aa753adaf19da3b08ebe	0	0
Artrta Trojan (Sysmon detection)	Ariel Millahuel	SOC Prime Threat Detection Marketplace	a460ea212cd93f867529a23e3064a9972f4e4b97bbba5f916b427016caaccd93	0	0

Atbroker Registry Change	Mateusz Wydra, oscd.community	Sigma Integrated Rule Set (GitHub)	15ae81a84c9a92e5ffb3bc1c4cecc28883ece49fc1ceef55d745ac094ece0622	0	0
Atera Agent Installation	Bhabesh Raj	Sigma Integrated Rule Set (GitHub)	25ae1d6038813be4c6c9dd482574522a1ec3ed0d01450b06b4673f94bef1aa71	0	0
Atlassian Confluence CVE-2021-26084	Bhabesh Raj	Sigma Integrated Rule Set (GitHub)	56b5ba6ff40bf2213da0f48c868136707e52c6ca8ac602bf6013d111e87ea977	0	0
Audio Capture	Pawel Mazur	Sigma Integrated Rule Set (GitHub)	a4baf3681957e567a0dcabca982a74d6ef27a7f4371c330e743abb82201ce772	0	0
Audio Capture via PowerShell	E.M. Anhaus (originally from Atomic Blue Detections, Endgame), oscd.community	Sigma Integrated Rule Set (GitHub)	db002a5ffd8be8305184d197dda045b272ab439c9fc205a6ce985e3eb911df70	0	0
Audit CVE Event	Florian Roth	Sigma Integrated Rule Set (GitHub)	0c184188e5202d857b8ad97911db2679f4da47c8ff9498e869e2794f4b017d77	0	0
Auditing Configuration Changes on Linux Host	Mikhail Larin, oscd.community	Sigma Integrated Rule Set (GitHub)	08bdc4ce556bc84980d5552bb3426a25d11cc00dfa1d2ca4e727b609ad595cb6	0	0
Automated Collection Bookmarks Using Get-ChildItem PowerShell	frack113	Sigma Integrated Rule Set (GitHub)	9fa49f4a1e9253459c99846a03ce69d8e029b42640efba5e158e2455b6c0f5fc	0	0
Azorult and XMRigCC behavior	Ariel Millahuel	SOC Prime Threat Detection Marketplace	312ca94426dbc718ff09f09e6a43b898190a0aaf80ccbf8bbc1faeab30a2381d	0	0
Azorult and XMRigCC behavior	Ariel Millahuel	SOC Prime Threat Detection Marketplace	eb88bdebe1990354c146b84c3335fe5d42136e63848540b27845073f1f61fd4d	0	0
Azure AD Health Monitoring Agent Registry Keys Access	Roberto Rodriguez (Cyb3rWard0g), OTR (Open Threat Research), MSTIC	Sigma Integrated Rule Set (GitHub)	3bfeb8cfe94b16cd5b7f3c96024b95509404dee7b48144b2af8aa5ce4779de13	0	0
Azure AD Health Service Agents Registry Keys Access	Roberto Rodriguez (Cyb3rWard0g), OTR (Open Threat Research), MSTIC	Sigma Integrated Rule Set (GitHub)	bbe20978cff2db9667ec877573b1107ee982ff6d743fa80d3cbf2b74771a384a	0	0
Azure Active Directory Hybrid Health AD FS New Server	Roberto Rodriguez (Cyb3rWard0g), OTR (Open Threat Research), MSTIC	Sigma Integrated Rule Set (GitHub)	74b3585358a705f41a3c47ca255f4fdf226f80d67efcd8180692d9830cb0cddc	0	0
Azure Active Directory Hybrid Health AD FS Service Delete	Roberto Rodriguez (Cyb3rWard0g), OTR (Open Threat Research), MSTIC	Sigma Integrated Rule Set (GitHub)	79b78dee5286fabf9074e377bf3ad75038d8b8d9a5087f439b47b5c962e9a221	0	0
Azure Application Credential Modified	Austin Songer @austinsonger	Sigma Integrated Rule Set (GitHub)	8249fead423c34843b4256f38229856595e4938b344740799a977671a8721be9	0	0

Azure Application Deleted	Austin Songer @austinsonger	Sigma Integrated Rule Set (GitHub)	2ca197a0660bd80fe905e4ca00acc28acc9704a89ac7f82e3b3f99f91c2277bc	0	0
Azure Application Gateway Modified or Deleted	Austin Songer	Sigma Integrated Rule Set (GitHub)	99cfccf0f7621c216ab9a6e574118c7d08bd147ed24fdfc923c1bef27869dd2e	0	0
Azure Application Security Group Modified or Deleted	Austin Songer	Sigma Integrated Rule Set (GitHub)	fee924d31493870a0e467e4c218281258f926382c4aed996e8c0ead7b0ffd1a1	0	0
Azure Container Registry Created or Deleted	Austin Songer @austinsonger	Sigma Integrated Rule Set (GitHub)	a50193cebf131589afa2e4c5caf4bd66397e7f3e21a007d2dceb8a4a87b50ef2	0	0
Azure DNS Zone Modified or Deleted	Austin Songer @austinsonger	Sigma Integrated Rule Set (GitHub)	43efaace741bf5e0b6dd18d8ac4cb9c2541ae1076b512e1bd743a3064a1e6bd6	0	0
Azure Device No Longer Managed or Compliant	Austin Songer @austinsonger	Sigma Integrated Rule Set (GitHub)	c81341f9f6cd4cd0b87566645bb2e5b8bcbf96eb3f70ff9b56ee3abf4854e84d	0	0
Azure Device or Configuration Modified or Deleted	Austin Songer @austinsonger	Sigma Integrated Rule Set (GitHub)	96deb162e4d7078c4d37c8e9299cd36a06bd4e7851a6667dbf6d26a2c982d28e	0	0
Azure Domain Federation Settings Modified	Austin Songer	Sigma Integrated Rule Set (GitHub)	cbd7365e52f94f02a513846714617391f68f6912003a2eb9a0bbacf128259b5b	0	0
Azure Firewall Modified or Deleted	Austin Songer @austinsonger	Sigma Integrated Rule Set (GitHub)	d45698a63ac241254c2e58e006dd45b43f164ffe1d0a192e9e4bfb69fd4d0a70	0	0
Azure Firewall Rule Collection Modified or Deleted	Austin Songer @austinsonger	Sigma Integrated Rule Set (GitHub)	4e5d8654f38840ce7dfb65eccbb26e41cf2087dc48fd3290abc364e99ff6c223	0	0
Azure Firewall Rule Configuration Modified or Deleted	Austin Songer @austinsonger	Sigma Integrated Rule Set (GitHub)	1966c63d48e697e85ff918b12a3933601905b8e608c26a39ba40d0802843a0a7	0	0
Azure Key Vault Modified or Deleted.	Austin Songer @austinsonger	Sigma Integrated Rule Set (GitHub)	8277b5e14bd624d703568cc728cc7573300e7157c6085a669f3c467b2b2dc91f	0	0
Azure Keyvault Key Modified or Deleted	Austin Songer @austinsonger	Sigma Integrated Rule Set (GitHub)	9cd4b711206e3c37197e34894fa230459f8f3973e55a8393632f7b4f394a0757	0	0
Azure Keyvault Secrets Modified or Deleted	Austin Songer @austinsonger	Sigma Integrated Rule Set (GitHub)	ca763651140713351 44bbd16aa1ff1702fba9628d9339290e6ad1ca4038485b0	0	0

Azure Kubernetes Admission Controller	Austin Songer @austinsonger	Sigma Integrated Rule Set (GitHub)	0f1f0dc48da97695cb6527b079cf0a309aa8c1f5330034f614fd18aa4a3a515d	0	0
Azure Kubernetes Cluster Created or Deleted	Austin Songer @austinsonger	Sigma Integrated Rule Set (GitHub)	ad11168ee302b9e417ef34de10e853a070a2255f619a0f2e5ce8093efa4125ec	0	0
Azure Kubernetes CronJob	Austin Songer @austinsonger	Sigma Integrated Rule Set (GitHub)	6f0756909a231b1de68feb41531a09f1b4aa980d4cb705216064bbf410c47f38	0	0
Azure Kubernetes Events Deleted	Austin Songer @austinsonger	Sigma Integrated Rule Set (GitHub)	8d931927daa9fe944bfee3fe82c6723e2f8c8daab9a97f657c6b92eec3f60413	0	0
Azure Kubernetes Network Policy Change	Austin Songer @austinsonger	Sigma Integrated Rule Set (GitHub)	fa73bc2ee70f7f45ebea4039e72ecbf9d55585af7633d7dc5ee78175f740c847	0	0
Azure Kubernetes Pods Deleted	Austin Songer @austinsonger	Sigma Integrated Rule Set (GitHub)	e96da18a9f7bce0ba8dbf0ea74585858e37bdf438c3a3acf0e69ad4f611d8e00	0	0
Azure Kubernetes RoleBinding/ClusterRoleBinding Modified and Deleted	Austin Songer @austinsonger	Sigma Integrated Rule Set (GitHub)	dcf545836738f2f84a8fe309688d2565d5db60f2003e89935f9c884ebde8b2f3	0	0
Azure Kubernetes Secret or Config Object Access	Austin Songer @austinsonger	Sigma Integrated Rule Set (GitHub)	dcea1ea1d9ac39af65a5f28568f16c91f9dc4c647daea19dce016dd2466bdbd8	0	0
Azure Kubernetes Sensitive Role Access	Austin Songer @austinsonger	Sigma Integrated Rule Set (GitHub)	23e30fa444fae1b172748e6a76e829b2b5bc2d747c0c6d679f757fbdb036198b	0	0
Azure Kubernetes Service Account Modified or Deleted	Austin Songer @austinsonger	Sigma Integrated Rule Set (GitHub)	8a73631fa6f0fa5dff761b9c6c0a3ccf6a66f656636666241850 3f105d17d8993	0	0
Azure Network Firewall Policy Modified or Deleted	Austin Songer @austinsonger	Sigma Integrated Rule Set (GitHub)	9899c52490520e420876ad5de364f9f956e993c38bb2bf6e26f7afad6560eee9	0	0
Azure Network Security Configuration Modified or Deleted	Austin Songer @austinsonger	Sigma Integrated Rule Set (GitHub)	d91818569830303d0793ec9cdf27d592e581e957caa02141080927e8d4debd7d	0	0
Azure New CloudShell Created	Austin Songer	Sigma Integrated Rule Set (GitHub)	168e1c35ae1332d1fde280357d55f94bc3fa72d5f623c5075dc9e95719b508e0	0	0
Azure Owner Removed From Application or Service Principal	Austin Songer @austinsonger	Sigma Integrated Rule Set (GitHub)	f497fa0952b0643d212e000f9beedfa0e38c340e126cc980759fd73aea3f074b	0	0

Azure Point-to-site VPN Modified or Deleted	Austin Songer @austinsonger	Sigma Integrated Rule Set (GitHub)	4fe122fb2f4694c438ef09c62c437757ffff5f2960a1d78aa757b6f0cdab3541	0	0
Azure Service Principal Created	Austin Songer @austinsonger	Sigma Integrated Rule Set (GitHub)	8e656dbfb37b60d6fef29014993072a6b8341f80dbd9d2ac0901fc71eb99b51f	0	0
Azure Service Principal Removed	Austin Songer @austinsonger	Sigma Integrated Rule Set (GitHub)	ce41462e381c9c869284161db12adbbf2078003b7ce16266c923d3dc021e19a0	0	0
Azure Subscription Permission Elevation Via ActivityLogs	Austin Songer @austinsonger	Sigma Integrated Rule Set (GitHub)	5fc1781e8afc3e000022771fd6678ed7bca2e931810fbe088916375a89ca353c	0	0
Azure Subscription Permission Elevation Via AuditLogs	Austin Songer @austinsonger	Sigma Integrated Rule Set (GitHub)	f1133baebe520b6bb3b6aa03c2a199e4297f5620463593d2698f7317285f40a5	0	0
Azure Suppression Rule Created	Austin Songer	Sigma Integrated Rule Set (GitHub)	c024312538da26140188fc0c40fb6fdffd2ba7813aeb307a59b8a7a73953de52	0	0
Azure Unusual Authentication Interruption	Austin Songer @austinsonger	Sigma Integrated Rule Set (GitHub)	a2fbabf1ea8e4593cac5c7ebaa8163ce713e0ccc9f65c8c76fd6ac40c53ccab9	0	0
Azure VPN Connection Modified or Deleted	Austin Songer @austinsonger	Sigma Integrated Rule Set (GitHub)	e0af5f08fe2a083cdd976c7c926cdeee6d6099cf28085ad65013d5a1c9041186	0	0
Azure Virtual Network Device Modified or Deleted	Austin Songer @austinsonger	Sigma Integrated Rule Set (GitHub)	caa2f19474e04314ce3f38bdc4f01d4f9704a841377ea129171fc6d2ec5f08e0	0	0
Azure Virtual Network Modified or Deleted	Austin Songer @austinsonger	Sigma Integrated Rule Set (GitHub)	daf496c3dedf483941f3040398af3b052a54fea0d8f410a2407b7284ae613dd4	0	0
AzureHound PowerShell Commands	Austin Songer (@austinsonger)	Sigma Integrated Rule Set (GitHub)	d745e174b185bed59eeb7c26c061f86404d4a74607b523973b17ee01d22e665f	0	0
Baby Shark Activity	Florian Roth	Sigma Integrated Rule Set (GitHub)	7e3c417e8dc74e72824b44e745f3abcd085e70e309ca15d279f127de94331f6e	0	0
BabyShark Agent Pattern	Florian Roth	Sigma Integrated Rule Set (GitHub)	65fc9733e96d5061d9c0158d5e935ee4fb89c6a3d5981ed3e2ee6eba8d7931bc	0	0
BackSwap Trojan detection	Ariel Millahuel	SOC Prime Threat Detection Marketplace	e578b7532f350b30e9614eb1a524f8d25975960eeaa667becc98ac9cd99c42ee	0	0
Backup Catalog Deleted	Florian Roth (rule), Tom U. @c_APT_ure (collection)	Sigma Integrated Rule Set (GitHub)	db25081a26915f454c9f9fc4dd73865d15100f764005bd361a8ec9eecee428d3	0	0

Bad Opsec Powershell Code Artifacts	ok @securonix invrep_de, oscd.community	Sigma Integrated Rule Set (GitHub)	c536e387a5fd3183e46be3c9a492ab73e5ade9b45179341ea25fcfe383cee92d	0	0
Banload Trojan Detection	Ariel Millahuel	SOC Prime Threat Detection Marketplace	cf78d5c37f3b09e94b3500edde1baaf99114e6503c98d1cedbf58f67f4e2b1de	0	0
Banload Trojan Detection	Ariel Millahuel	SOC Prime Threat Detection Marketplace	df75fb5e2add2e6674d7b5df931eb3ea32c98e61f6fcc4cb9e981b99fab72c52	0	0
Binary Padding	Igor Fits, Mikhail Larin, oscd.community	Sigma Integrated Rule Set (GitHub)	02cb79a02d071bcc40631d144c5a778d3326e0d2226089538e755f27dfac2048	0	0
Binary Padding	Igor Fits, oscd.community	Sigma Integrated Rule Set (GitHub)	3fbac61acf4870c524599db45e1b2dfc09b3058a0096d5fb5b9f1cbc7cde4fee	0	0
Bitsadmin to Uncommon TLD	Florian Roth	Sigma Integrated Rule Set (GitHub)	2e6f9336c9aa7e0fb900844db203acd64f2e49c46053557f76e819509277e0b2	0	0
Black Kingdom Ransomware	Ariel Millahuel	SOC Prime Threat Detection Marketplace	7b246ccd83dc04be953170d86f9c74b4e9d46071fbc612523b2b7b5564ea248e	0	0
BlackWater Malware (Sysmon detection)	Ariel Millahuel	SOC Prime Threat Detection Marketplace	39cd8a4762fefe23e71b4a9c925150241a4c887c22e6c33561f972f394454f55	0	0
Blackout Ransomware	Ariel Millahuel	SOC Prime Threat Detection Marketplace	85ed357648ddf115b4b4d1596a36cdf430f132c7262701da1960f5d9c685d48d	0	0
Blackout Ransomware	Ariel Millahuel	SOC Prime Threat Detection Marketplace	b5d26570d88e55e6f8513514b34cb8ae7122dfac66a407ee89e3136500fcec9b	0	0
Bladabindi backdoor	Ariel Millahuel	SOC Prime Threat Detection Marketplace	acbedd0b4dd2d93744542676c9afdfcf6f0f313229b26f137a2d979893bec5ff	0	0
Blue Mockingbird	Trent Liffick (@tliffick)	Sigma Integrated Rule Set (GitHub)	0cb9e146271e0c9ad794c98863e0e6d9c6ca19471bfea205eee4a276fecbd69d	0	0
Blue Mockingbird	Trent Liffick (@tliffick)	Sigma Integrated Rule Set (GitHub)	8f6a9e9bbcb601d1bc09093f383e8d8f1f7f09bf7d7e69843c14a7cd880ee0c1	0	0
Blue Mockingbird	Trent Liffick (@tliffick)	Sigma Integrated Rule Set (GitHub)	d0b6ca563c74d796de2ac3b8200508b7ea05a9ba9533d0d455ec1f717dd0b8d5	0	0
Blue Mockingbird	Trent Liffick (@tliffick)	Sigma Integrated Rule Set (GitHub)	f1ab359e7200763d0ebd605b4d6c074a821679006372360c1fef073501822e2b	0	0
Blue Mockingbird	Trent Liffick (@tliffick)	Sigma Integrated Rule Set (GitHub)	f723401b33927cfc6f265fefe66ce2982144e1ddeb991a3b47302b70b730b91a	0	0

Brute Force	Aleksandr Akhremchik, oscd.community	Sigma Integrated Rule Set (GitHub)	4307719a67c4c9c1343c12fa7fbdb91107ce614a895545a9b2de04426298134a	0	0
Buer Loader (Sysmon detection)	Ariel Millahuel	SOC Prime Threat Detection Marketplace	6327206ca6b0ae94eb02e02c0eda55e26020672bad83ed8831fcdc84f2c0f3ff	0	0
Buffer Overflow Attempts	Florian Roth	Sigma Integrated Rule Set (GitHub)	ad1714ed24aec2fa28551a247a666369e496ada2acb48b02b3b266083d75e6b1	0	0
Bunitu Trojan	Ariel Millahuel	SOC Prime Threat Detection Marketplace	3a8e7baeffec67b69220da8b8d25bcae45e047937d0f2f833052ef5ea532aa9a	0	0
Bypass UAC Using DelegateExecute	frack113	Sigma Integrated Rule Set (GitHub)	da3ec62084336efcb20f4f4e3a94268ca6c1665699d00b48e490be7fc41d2287	0	0
Bypass UAC Using Event Viewer	frack113	Sigma Integrated Rule Set (GitHub)	a0f94cedc18c397f576619978b15265938adc1cba9d431467d50db98d8a79972	0	0
Bypass UAC Using SilentCleanup Task	frack113	Sigma Integrated Rule Set (GitHub)	09bd87cd156913fd5b64ab548f700258c49833a235b205c8494f05634670d8d9	0	0
CARROTBAT Malware detection	Ariel Millahuel	SOC Prime Threat Detection Marketplace	793159445715fc7a8b862f94666ae175cf0a3f6ab66c76e3af31ac86638fa859	0	0
CLR DLL Loaded Via Office Applications	Antonlovesdnb	Sigma Integrated Rule Set (GitHub)	6362c65a14d81807ed78ab9e2fa99fbb546c067d39b3b63846c820e5c401e2e3	0	0
CLR DLL Loaded Via Scripting Applications	omkar72, oscd.community	Sigma Integrated Rule Set (GitHub)	5c2eb7356281203a2556ea40a71892ba7a369c46d5f2fc4574a427ac968c097c	0	0
CMSTP Execution	Nik Seetharaman	Sigma Integrated Rule Set (GitHub)	fcd2fd95fad355c5e2d783abef0cb21f5fcc96e6ed5e0637f465bb7e75cf9342	0	0
CMSTP Execution Process Access	Nik Seetharaman	Sigma Integrated Rule Set (GitHub)	87af8c0b574ec328882da2ed6ae28880f2577cf0bbe165ae6e19d50475c6d86a	0	0
COM DLL Loaded Via Microsoft Office Product (via sysmon)	SOC Prime Team	SOC Prime Threat Detection Marketplace	8f3c9743049559fb0309f2478f6d6c65e7de8ef0a27373e4c584779e3276979c	0	0
COM Hijack via Sdclt	Omkar Gudhate	Sigma Integrated Rule Set (GitHub)	ab8743ded66b586929aa13e45ceb037d6d8b0070893c7f23eb993baabe393a9d	0	0
COMPlus_ETWEnabled Command Line Arguments	Roberto Rodriguez (Cyb3rWard0g), OTR (Open Threat Research)	Sigma Integrated Rule Set (GitHub)	37c4f090dee0ead128c75a30b117563fd3376ddf2e4b622311b167c9a3b1ba18	0	0
COMPlus_ETWEnabled Registry Modification	Roberto Rodriguez (Cyb3rWard0g), OTR (Open Threat Research)	Sigma Integrated Rule Set (GitHub)	35fa58d3974ddf4be72ca9c5273ff5dfde7de065d8b27e4baef1189a9c10014d	0	0

COMPlus_ETWEnabled Registry Modification	Roberto Rodriguez (Cyb3rWard0g), OTR (Open Threat Research)	Sigma Integrated Rule Set (GitHub)	cc1b63adcbcba57ac6edb7913c2741cb0bee32fe4301f250ee4087ba643a654f	0	0
CVE-2010-5278 Exploitation Attempt	Subhash Popuri (@pbssubhash)	Sigma Integrated Rule Set (GitHub)	d934f98bfa1d3842f51f86448d12eaa5d7ae665d51986c839307e4494210607e	0	0
CVE-2020-0688 Exchange Exploitation via Web Log	Florian Roth	Sigma Integrated Rule Set (GitHub)	00d02232ebab9d4ccdb763022a32fda3d58da65c29159ed6992ba07072196b09	0	0
CVE-2020-0688 Exploitation Attempt	NVISO	Sigma Integrated Rule Set (GitHub)	5bbc9c67b6f5cb0d9b567b095ac079935288aace38c952feeefe24cca8db2fbf	0	0
CVE-2020-0688 Exploitation via Eventlog	Florian Roth, wagga	Sigma Integrated Rule Set (GitHub)	b8583b9acaa360ecfe76d00ff9d352cbdf6d3107d975a243b3ffb45ea03c67e9	0	0
CVE-2020-10148 SolarWinds Orion API Auth Bypass	Bhabesh Raj	Sigma Integrated Rule Set (GitHub)	b8a891b94f9eaba11d1c04c2500b004dcd5a7de6f8e0722ef3d08f910741c37e	0	0
CVE-2020-1350 DNS Remote Code Exploit [SIGRED] (via DNS)	SOC Prime Team	SOC Prime Threat Detection Marketplace	332d13dcb0a4e1a6c422484f6927e7408031f7270166ea37cf7f557c68ec5efa	0	0
CVE-2020-1350 DNS Remote Code Exploit [SIGRED] (via DNS)	SOC Prime Team	SOC Prime Threat Detection Marketplace	5cf068578d60f0e62a85062e3f528e2e675df78e1d1b2324b93218b97404a4bd	0	0
CVE-2020-1350 DNS Remote Code Exploit [SIGRED] (via cmdline)	SOC Prime Team	SOC Prime Threat Detection Marketplace	241626240096e85dd40e071e886b505b28444c8f3af6df03ef5c13b9d9776cda	0	0
CVE-2020-1350 DNS Remote Code Exploit [SIGRED] (via cmdline)	SOC Prime Team	SOC Prime Threat Detection Marketplace	bd554d600bee5054372f731217934ed318c54147855183a261c54405ef43c54a	0	0
CVE-2020-5902 F5 BIG-IP Exploitation Attempt	Florian Roth	Sigma Integrated Rule Set (GitHub)	28e45cf616425b3c243efdcab379f55c65b9c0717203ffc48f3c3f124c310ff5	0	0
CVE-2021-1675 Print Spooler Exploitation	Florian Roth	Sigma Integrated Rule Set (GitHub)	d7d444c9a70f46cddde00a1fd7df0120fbe71489ab597d307121ebaa8d8fabf6	0	0
CVE-2021-1675 Print Spooler Exploitation IPC Access	INIT_6	Sigma Integrated Rule Set (GitHub)	f011655155a4809262d5b5b289c20c070c7a7dec29d95846c91f3e39396d8bcc	0	0
CVE-2021-21972 VSphere Exploitation	Bhabesh Raj	Sigma Integrated Rule Set (GitHub)	2215493140650ea52f95acdf1c79355498c6a798bd8ab94a6943d450e765fd0c	0	0

CVE-2021-21978 Exploitation Attempt	Bhabesh Raj	Sigma Integrated Rule Set (GitHub)	82d6ddf5b00dd27b2c72d0ff170f126fdfad3155a287a936bd9d6075a8f8d944	0	0
CVE-2021-3156 Exploitation Attempt	Bhabesh Raj	Sigma Integrated Rule Set (GitHub)	236292ff7ca8a69ab14291cb8d62c04d3b02986279a40bf5a30c9345804f78bc	0	0
CVE-2021-3156 Exploitation Attempt	Bhabesh Raj	Sigma Integrated Rule Set (GitHub)	5d4f849169f7cbe8f891d2622b175e4a42e41f434ea0540e841504b3b7de6e41	0	0
CVE-2021-3156 Exploitation Attempt	Bhabesh Raj	Sigma Integrated Rule Set (GitHub)	908809e40074898d7b460586768c977b2a700582c38d0355eb3f7e823d8d2c59	0	0
CVE-2021-3156 Exploitation Attempt	Bhabesh Raj	Sigma Integrated Rule Set (GitHub)	ab3709539b01cbfabb623bf86f278fcfc6c5bb5e735e7b13392f184bd6bfbfc6	0	0
CVE-2021-3156 Exploitation Attempt	Bhabesh Raj	Sigma Integrated Rule Set (GitHub)	daa2b8c9a016f7a9553030afbe735cc198ea85e381594ee1f438d0c54496b152	0	0
CVE-2021-31979 CVE-2021-33771 Exploits by Sourgum	Sittikorn S	Sigma Integrated Rule Set (GitHub)	3fc8cf89558a3ec50308aea72b7745ae0f219f9882cda378f1cbf0487a7a3e32	0	0
CVE-2021-31979 CVE-2021-33771 Exploits by Sourgum	Sittikorn S	Sigma Integrated Rule Set (GitHub)	70390bef07d59937cec0216e008ce815799b4c22a5e260a684ed6bfac4fdcd1c	0	0
CVE-2021-31979 CVE-2021-33771 Exploits by Sourgum	Sittikorn S	Sigma Integrated Rule Set (GitHub)	9c20b726dcc3e2be564bb8c45c1c3372d7051d5cf3ff87aa65115c110cb62f4b	0	0
CVE-2021-31979 CVE-2021-33771 Exploits by Sourgum	Sittikorn S	Sigma Integrated Rule Set (GitHub)	a5aa00b412cd8e83e52f741ce80dafabe03f640d00ccf9f43a9c610344a8627c	0	0
CVE-2021-33766 Exchange ProxyToken Exploitation	Florian Roth, Max Altgelt, Christian Burkard	Sigma Integrated Rule Set (GitHub)	8f5525eb13728c689fc0e016fae75537d736213235bcab835284983e3ec2e37a	0	0
CVE-2021-40444 Process Pattern	@neonprimetime, Florian Roth	Sigma Integrated Rule Set (GitHub)	f438a85d4d0729d23171fa1823ccdb8541fc46f2e71ea2827ad42bc7f373a360	0	0
CVE-2021-40539 Zoho ManageEngine ADSelfService Plus Exploit	Sittikorn S, Nuttakorn Tungpoonsup	Sigma Integrated Rule Set (GitHub)	0c9b01c970160550c39d032237474fe010d45a8b283b53084a214bb65abf5fae	0	0
CVE-2021-41773 Exploitation Attempt	daffainfo, Florian Roth	Sigma Integrated Rule Set (GitHub)	785c77adf74a5ac52d0c7c196fb79ad631311bdc96913b8d2e2b6f6486c36578	0	0
Capture Credentials with Rpcping.exe	Julia Fomina, oscd.community	Sigma Integrated Rule Set (GitHub)	15be2ea21971f32bb037bc7f681259a4f9e1989cf78ab9a1dd5f8efe68cfcdbb	0	0

Cerber Ransomware	Ariel Millahuel	SOC Prime Threat Detection Marketplace	064b8f335c5dad53244cfd14a7c51a8fd536dc8c86741bd6699e06ffdc7563a1	0	0
Certificate Request Export to Exchange Webserver	Max Altgelt	Sigma Integrated Rule Set (GitHub)	9ec2157972ed064f3fd9dc25d8dd71195ab84c7747a3c17923cb09230442d76b	0	0
Chafer Activity	Florian Roth, Markus Neis, Jonhnathan Ribeiro, Daniil Yugoslavskiy, oscd.community	Sigma Integrated Rule Set (GitHub)	173b1203b0d58ac13e3b93542a1017cf3769eb4ba1be56bb4bc926e53578dc74	0	0
Chafer Activity	Florian Roth, Markus Neis, Jonhnathan Ribeiro, Daniil Yugoslavskiy, oscd.community	Sigma Integrated Rule Set (GitHub)	1d13c62f756a81c5138fc3c57236cc1ec96910a5b90687e628170734dae53640	0	0
Chafer Activity	Florian Roth, Markus Neis, Jonhnathan Ribeiro, Daniil Yugoslavskiy, oscd.community	Sigma Integrated Rule Set (GitHub)	1f40062e963356a7f04535a0f3fb4eec269440ca226f367f7b8bab940022cac4	0	0
Chafer Activity	Florian Roth, Markus Neis, Jonhnathan Ribeiro, Daniil Yugoslavskiy, oscd.community	Sigma Integrated Rule Set (GitHub)	353ed25aa9f2dfe8e0a56f2a3321d579ce4e7e8d20563769e0f02ff01ac06c3a	0	0
Chafer Activity	Florian Roth, Markus Neis, Jonhnathan Ribeiro, Daniil Yugoslavskiy, oscd.community	Sigma Integrated Rule Set (GitHub)	4207cea59e80ca7ec1b55f3bd2cfae0e47398daf8485c73feabf38a1484ac532	0	0
Chafer Activity	Florian Roth, Markus Neis, Jonhnathan Ribeiro, Daniil Yugoslavskiy, oscd.community	Sigma Integrated Rule Set (GitHub)	481b18e9f3ae67f2f52eafd5f02566e687c982a62597a8333ec6c4eb21f97fc8	0	0
Chafer Activity	Florian Roth, Markus Neis, Jonhnathan Ribeiro, Daniil Yugoslavskiy, oscd.community	Sigma Integrated Rule Set (GitHub)	5a93f630933a2040c4795df341b70fd08f3b7f1730c331cb6e025d13fe3d7d30	0	0
Chafer Activity	Florian Roth, Markus Neis, Jonhnathan Ribeiro, Daniil Yugoslavskiy, oscd.community	Sigma Integrated Rule Set (GitHub)	6d4dbcdef02bddd827d8a0739ad5f31dc3844674ae32cf4be9de19c3e4202940	0	0
Chafer Activity	Florian Roth, Markus Neis, Jonhnathan Ribeiro, Daniil Yugoslavskiy, oscd.community	Sigma Integrated Rule Set (GitHub)	b1eb7ac5e07136335fc21860603d89c40eb6488824477f00827b6749b15c1217	0	0
Chafer Activity	Florian Roth, Markus Neis, Jonhnathan Ribeiro, Daniil Yugoslavskiy, oscd.community	Sigma Integrated Rule Set (GitHub)	fed33455c8438e9a672de5f0fc2f48651ff0449b0427f5747e2b98db25e3088f	0	0
Chafer Malware URL Pattern	Florian Roth	Sigma Integrated Rule Set (GitHub)	cadeba64d91814a5bec0863ecd58722639024a5eb3b5f8e1059bf7ac84765c9f	0	0
Change Outlook Security Setting in Registry	frack113	Sigma Integrated Rule Set (GitHub)	ad1841979098a6b76c24ea780263b9da230373dc9a0d48d841538ec02cecb447	0	0
Change PowerShell Policies to a Unsecure Level	frack113	Sigma Integrated Rule Set (GitHub)	5572c8188426269a10ccb41fc8e9c8445391ac38a0917621b0a1ee05ec99aac9	0	0
Change to Authentication Method	AlertIQ	Sigma Integrated Rule Set (GitHub)	b48b8735d4b0c36f6b4415f9561a541fe792f70783e40570d3558a3bdb50c550	0	0
Check privilege of CMD via whoami	Joe Security	Joe Security Rule Set (GitHub)	07a05a43e0384cce9c41d6cb6ed256ebce6aea8c6455db044d755ece6063babe	0	0

Chthonic Banking Trojan	Ariel Millahuel	SOC Prime Threat Detection Marketplace	5915609df8f0f33be9c7c82797ba777d92dff34c96c4483d76ea06e3a514454e	0	0
Chthonic Banking Trojan	Ariel Millahuel	SOC Prime Threat Detection Marketplace	bb3d22a048ab0177787e51d23515065a6af77e3dad57b621b06f01af9fa36675	0	0
Cisco ASA FTD Exploit CVE-2020-3452	Florian Roth	Sigma Integrated Rule Set (GitHub)	58180314ba9a1b6fc6135d8a5452d7ec429cce39bb8a0ee05e19b8cf2240315e	0	0
Cisco Clear Logs	Austin Clark	Sigma Integrated Rule Set (GitHub)	f2d0601cc4bc2b37896ef81bb36379f95f6d6da0f54e5d298d76af6e9e34dfc6	0	0
Cisco Collect Data	Austin Clark	Sigma Integrated Rule Set (GitHub)	2c692110983c838f0baff38e18c9350ae3def6ff7afca5af55221519eed38387	0	0
Cisco Crypto Commands	Austin Clark	Sigma Integrated Rule Set (GitHub)	c3f4d338f538ec307b874891bf2dbd5f3ab916918bdca04a2ed53da9cb5ba3d5	0	0
Cisco Denial of Service	Austin Clark	Sigma Integrated Rule Set (GitHub)	c9b1080d16e9e0175fdcbb202f1842cefd864c57eaa6a64ff1c1b4d6a5e71ae4	0	0
Cisco Disabling Logging	Austin Clark	Sigma Integrated Rule Set (GitHub)	caab8d24d82768943d8a9bc5bc8ec1de7d099ef18de8846a7a84c7a0c123ae9e	0	0
Cisco Discovery	Austin Clark	Sigma Integrated Rule Set (GitHub)	922dd1761e6de8935b8deddf2c702455c9687e7ce9135ddc502be597a434ebf1	0	0
Cisco File Deletion	Austin Clark	Sigma Integrated Rule Set (GitHub)	a81d06d9e233156764ebf91e560a8a01fdf1b044beeaaa400b065b5be267cbb0	0	0
Cisco Local Accounts	Austin Clark	Sigma Integrated Rule Set (GitHub)	066ace76e41c5e84ccb56804255ccf2d9c27332fc287e77151b9a6bd70f1d723	0	0
Cisco Modify Configuration	Austin Clark	Sigma Integrated Rule Set (GitHub)	e1d658a7e96d34fae9c9489f15cc7e66d2d932e0902ae1d9b63e49f69008a557	0	0
Cisco Show Commands Input	Austin Clark	Sigma Integrated Rule Set (GitHub)	52e2f120bc6f6a2fdea0d88c7334e68be41c50e02ac50ad9447e3b97ccc8e8c8	0	0
Cisco Sniffing	Austin Clark	Sigma Integrated Rule Set (GitHub)	8acea30044d76f3304a28112da3f66be2f2b9d450a7cdd1784f9c45ad56191de	0	0
Cisco Stage Data	Austin Clark	Sigma Integrated Rule Set (GitHub)	3ba27fda76b2e27f70c6f07a668f4d28b5903a7813afffa184749aeb9b961725	0	0
Citrix ADS Exploitation CVE-2020-8193 CVE-2020-8195	Florian Roth	Sigma Integrated Rule Set (GitHub)	afd8157e130ac5b1e85a83666d958d63adfa7ab570ebfbdcabdc1b7034b9f9c1	0	0
Citrix Netscaler Attack CVE-2019-19781	Arnim Rupp, Florian Roth	Sigma Integrated Rule Set (GitHub)	98e0f69c0d080f1ab9346e1ebed9222049669b100a11bbaa8b110d9d96ad8828	0	0

Classes Autorun Keys Modification	Victor Sergeev, Daniil Yugoslavskiy, Gleb Sukhodolskiy, Timur Zinniatullin, oscd.community, Tim Shelton, frack113 (split)	Sigma Integrated Rule Set (GitHub)	acb1ec4240103205f334c8fe26431568a458950f7b86b59652440e1de4dc0449	0	0
CleanWipe Usage	Nasreddine Bencherchali @nas_bench	Sigma Integrated Rule Set (GitHub)	ede87d3abc8a99be3ca19ab4102e923f13e3f7b181cde6eddea9e6f1593b1e77	0	0
Clear Command History	Patrick Bareiss	Sigma Integrated Rule Set (GitHub)	c5903ffafd80f3200d3223dd44f4e4200331a8bfef040c23fc1812186018c6b9	0	0
Clear Linux Logs	Ömer Günal, oscd.community	Sigma Integrated Rule Set (GitHub)	4a4b8d80ea9937a6728e92b1079891255ed26e302f37e290db84bbaffc71c386	0	0
Clear PowerShell History	Ilyas Ochkov, Jonhnathan Ribeiro, Daniil Yugoslavskiy, oscd.community	Sigma Integrated Rule Set (GitHub)	2169a242b9139d712fde6f31781a606f5f50af9d5dd7474d415ae08a0cf96fb7	0	0
Clear PowerShell History	Ilyas Ochkov, oscd.community	Sigma Integrated Rule Set (GitHub)	Sigma Integrated Rule Set (GitHub)-dfba4ce1-e0ea-495f-986e-97140f31af2d	0	0
Clearing Windows Console History	Austin Songer @austinsonger	Sigma Integrated Rule Set (GitHub)	30041403950554ea68cae8436931add62874ca499364d423bd04a8ccb124d999	0	0
Cleartext Protocol Usage	Alexandr Yampolskyi, SOC Prime	Sigma Integrated Rule Set (GitHub)	1f1ab8a0a3fe05dc5f6db77a733d09949a236725db888a8fc8999542edaa9d84	0	0
Cleartext Protocol Usage	Alexandr Yampolskyi, SOC Prime	Sigma Integrated Rule Set (GitHub)	4ffd878e89c72b4ceec82aae1b81d7e86116017e259d0f026184c047ac87f080	0	0
Cleartext Protocol Usage	Alexandr Yampolskyi, SOC Prime	Sigma Integrated Rule Set (GitHub)	550069c609adf898c0cd2425bccf7458002df9eda036de658988e3fc1c99025d	0	0
Cleartext Protocol Usage	Alexandr Yampolskyi, SOC Prime	Sigma Integrated Rule Set (GitHub)	5a34aa084745df161fe9743db142a1c40cb5ee3886200a67d6ad228a51483a8a	0	0
Cleartext Protocol Usage	Alexandr Yampolskyi, SOC Prime	Sigma Integrated Rule Set (GitHub)	d2de6c91a552659c64031d52630045d58a65e9b7f816c23dffb75c531fe65479	0	0
Clipboard Collection of Image Data with Xclip Tool	Pawel Mazur	Sigma Integrated Rule Set (GitHub)	bba5d6f743a4d29df17318bea6702db4ec9ccad741bcfd230545482d2f75c48b	0	0
Clipboard Collection with Xclip Tool	Pawel Mazur, Roberto Rodriguez (Cyb3rWard0g), OTR (Open Threat Research), MSTIC	Sigma Integrated Rule Set (GitHub)	05e02a479959ef4e06411f4b132dbfbf2eff4ab9239d4732bc6b92c1762decc4	0	0
Clipboard Collection with Xclip Tool	Pawel Mazur	Sigma Integrated Rule Set (GitHub)	5750f0c9e7a5b3d955a1de73bac6ad176f1d221bbe3b3a3c29db1eba3f280619	0	0
Cobalt Strike DNS Beaconing	Florian Roth	Sigma Integrated Rule Set (GitHub)	ae9cf008e7075ab1e5658ff0f1449d564314bf06bb13fc381dda84df5e63e523	0	0
CobaltStrike BOF Injection Pattern	Christian Burkard	Sigma Integrated Rule Set (GitHub)	e1f2db3ffec989759e5467440cde906de0dd4aa563b137379e91daed32103267	0	0

CobaltStrike Malformed UAs in Malleable Profiles	Florian Roth	Sigma Integrated Rule Set (GitHub)	e4c423de550bfad9e2962081acef2175c6383ee5809f156dedc218690445bcc	0	0
CobaltStrike Malleable (OCSP) Profile	Markus Neis	Sigma Integrated Rule Set (GitHub)	acdef10f5ebf1c2a007b873f8340f11064f333ffafafbe6d5458758dfafd1a60	0	0
CobaltStrike Malleable Amazon Browsing Traffic Profile	Markus Neis	Sigma Integrated Rule Set (GitHub)	4c8dcd1969f5864da6d00d316324cc9c07906eb46dcd52cb5ef77dec09e5f886	0	0
CobaltStrike Malleable OneDrive Browsing Traffic Profile	Markus Neis	Sigma Integrated Rule Set (GitHub)	e3debddaebc6a6805b6ecd204901a61dc7771baba667b06ae7259af94cbd15da	0	0
CobaltStrike Named Pipe	Florian Roth, Wojciech Lesicki	Sigma Integrated Rule Set (GitHub)	acc7e9be68d0e1ad85dc9aafc935bc08834e6cc9a7cc48742991e53d197a46af	0	0
CobaltStrike Named Pipe Pattern Regex	Florian Roth	Sigma Integrated Rule Set (GitHub)	337224175c49faeb48d475b30549b027ea2f3c467baf9b22a069f35aebe5bd66	0	0
CobaltStrike Named Pipe Patterns	Florian Roth, Christian Burkard	Sigma Integrated Rule Set (GitHub)	905fc9490af8169f526089d670a3608b44417c93f5ab5a80be4f4e507ea02668	0	0
CobaltStrike Process Injection	Olaf Hartong, Florian Roth, Aleksey Potapov, oscd.community	Sigma Integrated Rule Set (GitHub)	a95251178853987552aca691c7ec1d2e31c91213e0e11f80fd3e7789a1234894	0	0
CobaltStrike Service Installations	Florian Roth, Wojciech Lesicki	Sigma Integrated Rule Set (GitHub)	07ed77ae45c45cd6dbde58702a9401f505bb4cd22daf19d09993a5c55b05ec21	0	0
CobaltStrike Service Installations	Florian Roth, Wojciech Lesicki	Sigma Integrated Rule Set (GitHub)	1528f16fe86df1015680377eab269f8383ca863cc09a040605bbd624ab36512e	0	0
CobaltStrike Service Installations	Florian Roth, Wojciech Lesicki	Sigma Integrated Rule Set (GitHub)	52fb124d4388460bedaa284c35492d9da80a1d697d6610dcdcfa5dc688ad118b	0	0
CobaltStrike Service Installations	Florian Roth, Wojciech Lesicki	Sigma Integrated Rule Set (GitHub)	bd6e98a1ffa061e8610929a967d533a5f85adf437c7f2694f4b79edcf04c254f	0	0
Code Executed Via Office Add-in XLL File	frack113	Sigma Integrated Rule Set (GitHub)	166571671ff0b50e7d6b641f7490790a2762897cb0cbbe9e2d489edb3d71010e	0	0
Code Injection by ld.so Preload	Christian Burkard	Sigma Integrated Rule Set (GitHub)	ef655b20c81f4dddb081e2c7fe6c60ee0ea86d7e37cdf55fe02cd0c8586de4d1	0	0
Commands to Clear or Remove the Syslog	Max Altgelt, Roberto Rodriguez (Cyb3rWard0g), OTR (Open Threat Research), MSTIC	Sigma Integrated Rule Set (GitHub)	82fe97976c538cbc804bd324c0c8e95c4df77ed62a637f5e1d33dd2d9c9b416d	0	0
Commands to Clear or Remove the Syslog	Max Altgelt	Sigma Integrated Rule Set (GitHub)	9a49b4476704bd301f2c0b13c87316f7e92aef899ef21b8e3f6db3c943390df6	0	0

Common Port with Unusual Service	SOC Prime Team	SOC Prime Threat Detection Marketplace	448567e1372cc2d57c61ba1258607614de4959656f08b0c769cc4a2d4b6adf6b	0	0
Communication To Mega.nz	Florian Roth	Sigma Integrated Rule Set (GitHub)	f13e798225ef1d32c44d8511ab7c95a58e93d46b8c833bfb47f55eb5d9bb69e2	0	0
Compress Data and Lock With Password for Exfiltration With WINZIP	frack113	Sigma Integrated Rule Set (GitHub)	b6ab11c7f95ec7eeb0c511d3c26533628fe403bbf4d5d8e13ba54958aa6899da	0	0
Confluence Exploitation CVE-2019-3398	Florian Roth	Sigma Integrated Rule Set (GitHub)	51b242528b12df33e19aef0d9c491da0899ee0c15706bd24fa1d8bbfdd0c0e20	0	0
Connection Proxy	Ömer Günal	Sigma Integrated Rule Set (GitHub)	70f387e708b9ab503041091a0b074a7d2aa84dea74f61b398fa6fc3f154dacaf	0	0
Container Image was Uploaded via Unusual Client.	Brandon Hart	SOC Prime Threat Detection Marketplace	0b491699d6ca77a7ec742e9676c80395862b7093ff6ffbfb2aa1d4d22e32f84e	0	0
Conti Backup Database	frack113	Sigma Integrated Rule Set (GitHub)	a8204898cf8fc5736e342a77657426a9af40b6b573152d2d6e852a3112dead6d	0	0
Conti Ransomware Execution	frack113	Sigma Integrated Rule Set (GitHub)	c41fdd8a72030a4b0b96e025a1f36e7970262ad1e17a4ad2a29f643cb2033927	0	0
Conti Volume Shadow Listing	Max Altgelt, Tobias Michalski	Sigma Integrated Rule Set (GitHub)	08ef6e8b498eef96cef9154fc59c951d935c3fc9b707146c4eca4567eaa5db9f	0	0
Conti Volume Shadow Listing	Max Altgelt, Tobias Michalski	Sigma Integrated Rule Set (GitHub)	0b3dd39a21682b0ad57453e8c2da509ea751696a9ed99cae7fb6658a7c77adde	0	0
Conti Volume Shadow Listing	Max Altgelt, Tobias Michalski	Sigma Integrated Rule Set (GitHub)	2904a54d46badb30ae1eda5e935bcbcc71f8a08303a31fb68bf9e1fb8f0f0858	0	0
Conti Volume Shadow Listing	Max Altgelt, Tobias Michalski	Sigma Integrated Rule Set (GitHub)	afa46c9c99b3c76a0450a8c7dface8fa7a53dda1c62644f81fd73ced0a0d096f	0	0
Copperhedge Malware (Hidden Cobra)	Ariel Millahuel	SOC Prime Threat Detection Marketplace	aa72a19331c2c067f40e6e48ff853baac0a3d4a25566bc66809995fc42cf7cd8	0	0
Correct Execution of Nltest.exe	Arun Chauhan	Sigma Integrated Rule Set (GitHub)	f2418d4c95e6ea8c75c68ad4358af3fc47e78b7630289f9d13fe04dc688a039b	0	0
CrackMapExec Command Execution	Thomas Patzke	Sigma Integrated Rule Set (GitHub)	4adf455dcb8e143b4df56b115b6a64714aa6d18f105e8e3d9859c02f686e393b	0	0
CreateDump Process Dump	Florian Roth	Sigma Integrated Rule Set (GitHub)	687da476fe7fa5f062fed8f4a4daf9774c0ac4734d817bf428d2c8de23a0b15f	0	0
CreateMiniDump Hacktool	Florian Roth	Sigma Integrated Rule Set (GitHub)	9ba3182e2ff92ecee64624cd2f1f24935f5ebeb42a5e6530cad6ea428e2941ea	0	0

CreateMiniDump Hacktool	Florian Roth	Sigma Integrated Rule Set (GitHub)	db9bea11b648e60a727a16af04702fe0746657460d47aa50814a4f7999f58cb6	0	0
Creation Exe for Service with Unquoted Path	frack113	Sigma Integrated Rule Set (GitHub)	3b925709ef1196fbdf20c495c5a7972944bd56a4ab342009ef41e3f3273c15af	0	0
Creation Of A Local User Account	Alejandro Ortuno, oscd.community	Sigma Integrated Rule Set (GitHub)	de6224d573389a0f865f0a33bd9bc3784cd12bf697150f8f8e0a9708a4e00199	0	0
Creation Of An User Account	Marie Euler	Sigma Integrated Rule Set (GitHub)	f796279cc60013c4736e3ef7e5a140375fba8a3d78694c9d524620326ae8efcf	0	0
Creation of a Local Hidden User Account by Registry	Christian Burkard	Sigma Integrated Rule Set (GitHub)	958ac16256f17b20c00b2a83f4bbad49236266d2b84e59eb2d3c29989efc96b0	0	0
Cred Dump-Tools Named Pipes	Teymur Kheirkhabarov, oscd.community	Sigma Integrated Rule Set (GitHub)	9eed77c2ef05fafded05e61ec71d8bdd695696543061ef8b84fca37d1606484e	0	0
Credential Dumping Tools Service Execution	Florian Roth, Teymur Kheirkhabarov, Daniil Yugoslavskiy, oscd.community	Sigma Integrated Rule Set (GitHub)	1243009f29fe311d9199398e8babee9294e8f9e57205fe6ebec6696ab0eec9e0	0	0
Credential Dumping Tools Service Execution	Florian Roth, Teymur Kheirkhabarov, Daniil Yugoslavskiy, oscd.community	Sigma Integrated Rule Set (GitHub)	25727cb75bc931bc91e433f5340be32ccedd13bf460a2fd8da5b1a8d8b4a369b	0	0
Credential Dumping Tools Service Execution	Florian Roth, Teymur Kheirkhabarov, Daniil Yugoslavskiy, oscd.community	Sigma Integrated Rule Set (GitHub)	433b594a58a12c33431c033f7e53c41d5f635df8cee206163112bfffde169958	0	0
Credential Dumping Tools Service Execution	Florian Roth, Teymur Kheirkhabarov, Daniil Yugoslavskiy, oscd.community	Sigma Integrated Rule Set (GitHub)	9a7af0218101ae1b67047098f1cf187e06c88982ba45ad3ef1c685c27788b02d	0	0
Credential Dumping Tools Service Execution	Florian Roth, Teymur Kheirkhabarov, Daniil Yugoslavskiy, oscd.community	Sigma Integrated Rule Set (GitHub)	ad25ab512a3789c7da7d55a7b60c4d528db1206a0a4d26f3f44d945cc456cc2d	0	0
Credential Dumping Tools Service Execution	Florian Roth, Teymur Kheirkhabarov, Daniil Yugoslavskiy, oscd.community	Sigma Integrated Rule Set (GitHub)	cda32da0a87ef0f9603fc5592471efd0b39082003d4bc39f06871a5dd4336130	0	0
Credential Dumping by LaZagne	Bhabesh Raj, Jonhnathan Ribeiro	Sigma Integrated Rule Set (GitHub)	8cca9e462f882fe58e9f320bb7380d7edbaaaab831521d9f739cca42cf64db37	0	0
Credential Dumping by Pypykatz	Bhabesh Raj	Sigma Integrated Rule Set (GitHub)	e7a973176dcaaa7050f1a216ca0d3075bfc12fecf2db13696af32148bd07d6bf	0	0
Credentials Dumping Tools Accessing LSASS Memory	Florian Roth, Roberto Rodriguez, Dimitrios Slamaris, Mark Russinovich, Thomas Patzke, Teymur Kheirkhabarov, Sherif Eldeeb, James Dickenson, Aleksey Potapov, oscd.community (update)	Sigma Integrated Rule Set (GitHub)	a293708df42b2beba9f1a26e123fed278dfc67f5946ce8c995b2800c58d69e2f	0	0

Credentials In Files	Igor Fits, oscd.community	Sigma Integrated Rule Set (GitHub)	26d8c61d691959676fb6d8b0217d408f4dde823800f79771a458011d3577ffbb	0	0
Credentials In Files	Igor Fits, Mikhail Larin, oscd.community	Sigma Integrated Rule Set (GitHub)	bb9fce766014ab2fb22106410384571f0217fa35e9914bdc3dd86452d8d4ed64	0	0
Credentials from Password Stores - Keychain	Tim Ismilyaev, oscd.community, Florian Roth	Sigma Integrated Rule Set (GitHub)	0a2ce7410c4271e6c41926b4fe0f5903a05d4a02cd8dcd4a273e86065b3f46b6	0	0
Cron Files	Roberto Rodriguez (Cyb3rWard0g), OTR (Open Threat Research), MSTIC	Sigma Integrated Rule Set (GitHub)	f74e8628441aa3b7bcbf82dd77cc025925e34078d02d169dd947db62675dbeaa	0	0
Cryptbot Stealer	Ariel Millahuel	SOC Prime Threat Detection Marketplace	06c9cbff1ed607186f04da92f2cf1648e2db7108306751e56b1e9f5123d11b60	0	0
Cryptbot Stealer	Ariel Millahuel	SOC Prime Threat Detection Marketplace	b2707a69365d76d4836147eeaf9407e838f5322fcbd5f89cf86c86f1ba4239d5	0	0
Crypto Miner User Agent	Florian Roth	Sigma Integrated Rule Set (GitHub)	ff0cfc194b0f8edd392e317c8a3d0e012351873096248a33ca36c2b71f5ab3a1	0	0
Cybergate RAT	Ariel Millahuel	SOC Prime Threat Detection Marketplace	e806ec700e831384b0d77c8508e1614d850eb5c7ccb89a9b745d0871c0136e5d	0	0
DCERPC SMB Spoolss Named Pipe	OTR (Open Threat Research)	Sigma Integrated Rule Set (GitHub)	9aca3bd938d644fb20cf3d83a10353ff1440153ab17579e69ed2ee17848c5d93	0	0
DCRat Malware	Ariel Millahuel	SOC Prime Threat Detection Marketplace	35dd39a15009dacc7bdd973a9fb1484b964accb38bbcb7a63bc0b1bf73131df0	0	0
DCRat Malware	Ariel Millahuel	SOC Prime Threat Detection Marketplace	d84b3a1cba66ed28c6c66d9a5dd807e984d42ba3b1e61ae45717b77695109095	0	0
DD File Overwrite	Roberto Rodriguez (Cyb3rWard0g), OTR (Open Threat Research), MSTIC	Sigma Integrated Rule Set (GitHub)	ae140eaae48e1659eb9013e9c7758cc3ebb59100fc5bce9ede4e8a0ca0fb76b7	0	0
DEWMODE Webshell Access	Florian Roth	Sigma Integrated Rule Set (GitHub)	9e465f124d03f3f4a5d575cc4d87bde86fda1fa3092da13a47c07f473c865bbc	0	0
DHCP Callout DLL Installation	Dimitrios Slamaris	Sigma Integrated Rule Set (GitHub)	08a22f080dbceb91fd6109159e695139744d9c12f6d94b12c35474b710aeb4ae	0	0
DHCP Server Error Failed Loading the CallOut DLL	Dimitrios Slamaris, @atc_project (fix)	Sigma Integrated Rule Set (GitHub)	11670a8f337ded0b6b72a5c41df4831c1b1da694f85e044e4afe1839d5dbc82d	0	0
DHCP Server Loaded the CallOut DLL	Dimitrios Slamaris	Sigma Integrated Rule Set (GitHub)	4928e3042535af018624a20ce17e807b66cf935200331da04e2db35a1b6cb695	0	0

DIT Snapshot Viewer Use	Furkan Caliskan (@caliskanfurkan_)	Sigma Integrated Rule Set (GitHub)	203a47b7ef9f6721efefc8005ca1492daf475a9b03afc70af3fde9780df06253	0	0
DLL Execution Via Register-cimprovider.exe	Ivan Dyachkov, Yulia Fomina, oscd.community	Sigma Integrated Rule Set (GitHub)	dd9b6910a5e264c2b56a7a735f0cfc2cab9c341775db4a260bbadf7815d05772	0	0
DLL Execution via Rasautou.exe	Julia Fomina, oscd.community	Sigma Integrated Rule Set (GitHub)	18ed0db67fcc790c2b7e9ff5c111ae3691af0b9f2d52618d41d7f956ce8aa598	0	0
DLL Injection with Tracker.exe	Avneet Singh @v3t0_, oscd.community	Sigma Integrated Rule Set (GitHub)	b829a2f1ed89d5380f218ac5f6e134b4301319062cf792789557f30f6f903d24	0	0
DLL Load via LSASS	Florian Roth	Sigma Integrated Rule Set (GitHub)	4dbf0d3da4d07dd172361786684269e5741eb3602ce1bf2c2c287041e8abe017	0	0
DNS Cache Enumeration(via CIM/WMI)	Den Iuzvyk	SOC Prime Threat Detection Marketplace	11f3c97d5bb96ad59c7eb445ca4feeab94c4ea4fbc54c6a6ff11061bab8a11b3	0	0
DNS Events Related To Mining Pools	Saw Winn Naung, Azure-Sentinel, @neu5ron	Sigma Integrated Rule Set (GitHub)	ed013f86bfbbcd25b8e462391d437165af76f6ca7e0b33cde4fceb2ee58d3e57	0	0
DNS HybridConnectionManager Service Bus	Roberto Rodriguez (Cyb3rWard0g), OTR (Open Threat Research)	Sigma Integrated Rule Set (GitHub)	3aadcde102c8a083c36e571f1926927d5bdeddec39fc0f3ca9c514988407c7fe	0	0
DNS RCE CVE-2020-1350	Florian Roth	Sigma Integrated Rule Set (GitHub)	c2b9377be93da37de7a04778f2a879e0e03b32b8aa2f1d0dd8b7c1ba72d7727b	0	0
DNS Server Error Failed Loading the ServerLevelPluginDLL	Florian Roth	Sigma Integrated Rule Set (GitHub)	a560dac7223fded812b9599d8c99d9973956309982969834 9739e8edeb365cc8	0	0
DNS ServerLevelPluginDll Install	Florian Roth	Sigma Integrated Rule Set (GitHub)	167ca4630ac31daedf547da8bb8695b2fbc83687b5dec494 38c407766e74c574	0	0
DNS ServerLevelPluginDll Install	Florian Roth	Sigma Integrated Rule Set (GitHub)	5935b25ff10421da2a478f9f484858a9599e6551a17272c7a4017c6e1a55df07	0	0
DNS ServerLevelPluginDll Install	Florian Roth	Sigma Integrated Rule Set (GitHub)	8435be4251ebdf2b4f18ae9d65faca381dc2fad4574c29cff3a962e5c9237487	0	0
DNS ServerLevelPluginDll Install	Florian Roth	Sigma Integrated Rule Set (GitHub)	8a0b41208edc45c1f006ab6da0f12b0b819a810a16ba4179e2ef632571eafa18	0	0
DNS ServerLevelPluginDll Install	Florian Roth	Sigma Integrated Rule Set (GitHub)	cfcbc45713ff3176a1284f986927a251f17c892931e878713 25476256b26bb0c	0	0
DNS TOR Proxies	Saw Winn Naung , Azure-Sentinel	Sigma Integrated Rule Set (GitHub)	1b16378c68113f05c5cf4b51586d582401449553cf4775243b8ce459ef59ef99	0	0
DNS TXT Answer with Possible Execution Strings	Markus Neis	Sigma Integrated Rule Set (GitHub)	8960985ab852fb33eb502577cd94683447f94e1a5299bfb607905f6a591cc78e	0	0

DNS Tunnel Technique from MuddyWater	@caliskanfurkan_	Sigma Integrated Rule Set (GitHub)	c2860e5a2a470c1dbb00003a43f3a9f04e5180cb5c7ec9e7a5bdcdfdd86a15a9	0	0
DNS-over-HTTPS Enabled by Registry	Austin Songer	Sigma Integrated Rule Set (GitHub)	0426d73fef7393ca82c3fbe1bedafc6d698e787d2cd679e17ae93a3b446a487f	0	0
DNSCat2 Powershell Implementation Detection Via Process Creation	Cian Heasley	Sigma Integrated Rule Set (GitHub)	b31e87788fbc1690d2371c0a80ebe27cf8c7a433c9a7f28b1a077ba534308772	0	0
DPAPI Domain Backup Key Extraction	Roberto Rodriguez @Cyb3rWard0g	Sigma Integrated Rule Set (GitHub)	d9a0bb3db2e444420bfe144e0ffc3f7e4dd9315a4792d088f6d79b706ac5fac0	0	0
DPAPI Domain Master Key Backup Attempt	Roberto Rodriguez @Cyb3rWard0g	Sigma Integrated Rule Set (GitHub)	084c47f6ea9d2126ec7b6b95e20cdf54557800f1b8394ae472f95b6162be6db1	0	0
DTRACK Process Creation	Florian Roth	Sigma Integrated Rule Set (GitHub)	fbcabbd5b0fb4855de3b0bcf6bd58239facf0733ad46f2269ef540d344acb5bb	0	0
Dacls RAT (Lazarus's Linux Malware)	Ariel Millahuel	SOC Prime Threat Detection Marketplace	79cabd2716a91ac3ac201a106a3c135e584d110d8527ac138457a5b89fb2b2a6	0	0
DarkRAT Botnet	Ariel Millahuel	SOC Prime Threat Detection Marketplace	097182ab9d206700057ec3ab10e6684d34c9b3ff109901a14fb1dbd8da889d95	0	0
Data Compressed	Timur Zinniatullin, oscd.community	Sigma Integrated Rule Set (GitHub)	fb2193574c75e35df0989335aac30e2e13f3b8163caf7eef46058ae407b19e98	0	0
Data Exfiltration to Unsanctioned Apps	Austin Songer @austinsonger	Sigma Integrated Rule Set (GitHub)	bae0cfa813856773ccb7c9ac2654b2f064928c841cb1442d6dda554b4e346c98	0	0
Data Exfiltration with Wget	Pawel Mazur	Sigma Integrated Rule Set (GitHub)	334aab46cbdf770ef0720448d240e1b67c2a759449b703fba9d425f1450d83f9	0	0
Decode Base64 Encoded Text	Daniil Yugoslavskiy, oscd.community	Sigma Integrated Rule Set (GitHub)	0f307ac40cafbbdb1e262b899732195a25952ad5bb013ca8e6d280eefd45a141	0	0
Decode Base64 Encoded Text	Daniil Yugoslavskiy, oscd.community	Sigma Integrated Rule Set (GitHub)	6101f5b902371808a5b407d66c189f259bec69ab6b4cf5b58a655af663843c71	0	0
Decode strings from lnk via findstr.exe	Joe Security	Joe Security Rule Set (GitHub)	9d57b9ed7a852960b15a4d2a7fb4faa9174893a98953c9f09989faab11ed110d	0	0
Default Cobalt Strike Certificate	Bhabesh Raj	Sigma Integrated Rule Set (GitHub)	19a7f2dd57b12f60486942900890081c7033fcf871e2c6ac4ddac91980374c15b	0	0
Default Credentials Usage	Alexandr Yampolskyi, SOC Prime	Sigma Integrated Rule Set (GitHub)	65501b5c31cfa5ab80e3a4512b833f9e4bb77ef303f17fc8839abf9c1b435969	0	0

Default Credentials Usage.	Alexandr Yampolskyi	SOC Prime Threat Detection Marketplace	3ed924bf0f9ebfc7642bd2eb1a2b925d801ff58fd267c5066fe579c55051e5cc	0	0
Default PowerSploit and Empire Schtasks Persistence	Markus Neis, @Karneades	Sigma Integrated Rule Set (GitHub)	40b130caca0f58482d7bae973cb51c3d6c7a02a91a7f448a1c19eb96333f5a10	0	0
Defrag Deactivation	Florian Roth, Bartlomiej Czyz (@bczyz1)	Sigma Integrated Rule Set (GitHub)	1ab376818e4cb7b7005cf46c5c118f9d09e2779f289cd7f37afc5fca8fc6e4f5	0	0
Defrag Deactivation	Florian Roth, Bartlomiej Czyz (@bczyz1)	Sigma Integrated Rule Set (GitHub)	462e0455aac7979a208190934de4564c8d6f5759fa73ea355f31b871967ed1eb	0	0
Defrag Deactivation	Florian Roth, Bartlomiej Czyz (@bczyz1)	Sigma Integrated Rule Set (GitHub)	4a305b6df01e5870b2018b579218b7e7b94bcc24e0959629d5cd3812d771d39b	0	0
Delete Volume Shadow Copies Via WMI With PowerShell	frack113	Sigma Integrated Rule Set (GitHub)	57a9202655d8133d3a5eb0a9d51c9f5dedb6b15cfc700005f6f0d686df4f2ba2	0	0
Delete Volume Shadow Copies via WMI with PowerShell	frack113	Sigma Integrated Rule Set (GitHub)	7435e1880cdd78f155ad539eaf8348f3ea0d6fa1183fac382443553cac2159be	0	0
Deletes Backup Files	frack113	Sigma Integrated Rule Set (GitHub)	f15234ba5cc4c709633e015e497cce2bab7cd6f91b488b8c04ecfd5651e68749	0	0
Denied Access To Remote Desktop	Pushkarev Dmitry	Sigma Integrated Rule Set (GitHub)	755295cd9d58dfbf7808166ecd446d284fa160fe7f2e2b5673aeef6cc5cb0a44	0	0
Detect Sql Injection By Keywords	Saw Win Naung	Sigma Integrated Rule Set (GitHub)	7940d1dd84f2a311d67ac511006deeead549c05a4cadaca9908e1071a153106c	0	0
Detect XSS Attempts By Keywords	Saw Win Naung	Sigma Integrated Rule Set (GitHub)	abfc554e6723d78308adb5dd0917e5604dac15611a98637633eae81fc3aff08f	0	0
Detected Windows Software Discovery	Nikita Nazarov, oscd.community	Sigma Integrated Rule Set (GitHub)	45e686dc153cf8d6e5cf577bc67b50dc6668c51412eddb7aede600f65fd5e9f0	0	0
Detecting Fake Instances Of Hxtsr.exe	Sreeman	Sigma Integrated Rule Set (GitHub)	8dd172636988b9cdc1bf44aaceb27f6009d97516c54decea0812022b61cd8d7a	0	0
Detecting Sysmon on a Victim Host (via powershell)	Ariel Millahuel	SOC Prime Threat Detection Marketplace	9d639e1b707b6f24ae8b637df63d5ac02aac0933b062d3477fa84d3194dc4e7b	0	0
Detection of Possible Rotten Potato	Teymur Kheirkhabarov	Sigma Integrated Rule Set (GitHub)	45c3c61e20707c18533d763c9e1c0a2f3abd229bd485f75c933da3e4ba156186	0	0
Detection of PowerShell Execution via DLL	Markus Neis	Sigma Integrated Rule Set (GitHub)	5980c0048e6d0468659094b73e0c348afcf2c52a7842e03089c1279a023c70c9	0	0

Detection of PowerShell Execution via Sqlps.exe	Agro (@agro_sev) oscd.community	Sigma Integrated Rule Set (GitHub)	541caef712c71465ca223d69670a2ef4826f41323f21f161bc699c23ba201602	0	0
Detection of SafetyKatz	Markus Neis	Sigma Integrated Rule Set (GitHub)	5b2f81ece2c70e3e5e4dd770e0b9c755c90c099bf527d2b257d43e1193585d13	0	0
Devtoolslauncher.exe Executes Specified Binary	Beyu Denis, oscd.community (rule), @_felamos (idea)	Sigma Integrated Rule Set (GitHub)	336df26c319863147659e184f6387914d5b34b55eeb4dabe819907f747016967	0	0
Direct Syscall of NtOpenProcess	Christian Burkard	Sigma Integrated Rule Set (GitHub)	e01fcd88ad6ac5ad9762f652a28d6c714dc5ccf89b89c118bdd3bb33e5cf8abd	0	0
Disable Exploit Guard Network Protection on Windows Defender	Austin Songer @austinsonger	Sigma Integrated Rule Set (GitHub)	8c426cb2a8a98a743f8e95cb5717e867cc5d4d22fcc97255e10fac2d59176fac	0	0
Disable Important Scheduled Task	frack113	Sigma Integrated Rule Set (GitHub)	09601976d693769f1fe442a0618410420380d7de7aeec4e52c0ebe6e3ebebe56	0	0
Disable PUA Protection on Windows Defender	Austin Songer @austinsonger	Sigma Integrated Rule Set (GitHub)	09a64c87ba1b11c75a19c495d100b0ef9fa95955560f0e1b4f9f2842159caaef	0	0
Disable Security Events Logging Adding Reg Key MiniNt	Ilyas Ochkov, oscd.community	Sigma Integrated Rule Set (GitHub)	6eaa9c84915e6b68d49ea0ea6b069124ad33f6d9666e8baf43270a57ee9e1b2a	0	0
Disable Security Tools	Daniil Yugoslavskiy, oscd.community	Sigma Integrated Rule Set (GitHub)	d934cd2adbdfb7c12ed5f937e36ed253d3f53495f0194507c0ea80b55f983957	0	0
Disable Tamper Protection on Windows Defender	Austin Songer @austinsonger	Sigma Integrated Rule Set (GitHub)	bf1de3b61466c6018ee71be3f901fb544ddb30709a256ce88ddc19444b5a1ea1	0	0
Disable Windows IIS HTTP Logging	frack113	Sigma Integrated Rule Set (GitHub)	8e9b40932ae787a51edc9fadbb2fd842437eea7b83804b0090d7f069e2d0a5f2	0	0
Disable or Delete Windows Eventlog	Florian Roth	Sigma Integrated Rule Set (GitHub)	780ed5be93f71a397b1b6c9d95912c0781c2ed9114eef8fc5aec854bf80b1f2c	0	0
Disabled IE Security Features	Florian Roth	Sigma Integrated Rule Set (GitHub)	dd832d1e805b850c68be7f120da6482e6126a8ee0860e3355d54604a2040eee7	0	0
Disabled Users Failing To Authenticate From Source Using Kerberos	Mauricio Velazco, frack113	Sigma Integrated Rule Set (GitHub)	a87dc529f00cccdafd3037358d753f5b37bdbc5d5860e077d8794985d3d93f5d	0	0
Disabled Volume Snapshots	Florian Roth	Sigma Integrated Rule Set (GitHub)	570e42eea810ffc81d8b3f1b5d284c891c1ca4a897bc6a8d5307ba5ac4feebbe	0	0
Disabling Security Tools	Ömer Günal, Alejandro Ortuno, oscd.community	Sigma Integrated Rule Set (GitHub)	17b8565aac7819789a47a069aa7bbdb1c69f755edcfcb766c10e1d973768a357	0	0

Disabling Security Tools	Ömer Günal, Alejandro Ortuno, oscd.community	Sigma Integrated Rule Set (GitHub)	495b384015032ab9c529e649f340c35394c72a7ace8daf0aecc9b3fe7bb5f54e	0	0
Disabling Security Tools	Ömer Günal, Alejandro Ortuno, oscd.community	Sigma Integrated Rule Set (GitHub)	7657d165811c7f6d4f9ff55e9ce81d8405e42f6157faed664f28bbc8fe97e560	0	0
Disabling Security Tools	Ömer Günal, Alejandro Ortuno, oscd.community	Sigma Integrated Rule Set (GitHub)	7c1caf17a217864cc13be5d7320e631c61b949686fc630c72b5d143d1b4cdbbb	0	0
Disabling Security Tools	Ömer Günal, Alejandro Ortuno, oscd.community	Sigma Integrated Rule Set (GitHub)	df800176ac79cd510a92bccecd1ec64124d8917bd009406abd5457f353896225	0	0
Discord client stealer (AnarchyGrabber)	Ariel Millahuel	SOC Prime Threat Detection Marketplace	d513011ab49524e73ae98c85b1f902158f55f0412551679d5acbb03eee68c4a3	0	0
Django Framework Exceptions	Thomas Patzke	Sigma Integrated Rule Set (GitHub)	fad46f86c5fe8acee91d73cf5901cf64df547e2777230845acfe89b79cbf172a	0	0
Dllhost Internet Connection	bartblaze	Sigma Integrated Rule Set (GitHub)	0469df5507574c65082f62410c1cc9e493ba1daeff82396b38a60516c6f4187c	0	0
Domain User Enumeration Network Recon 01	Nate Guagenti (@neu5ron), Open Threat Research (OTR)	Sigma Integrated Rule Set (GitHub)	11a4140a5787cdd2ea81d81e4e06755144d3c4abe02a886ec68eeb79c5273223	0	0
Domestic Kitten FurBall Malware Pattern	Florian Roth	Sigma Integrated Rule Set (GitHub)	d75f4b248c10259b1011107000396926b1a9e5cd4b0031500be48aee109855b5	0	0
Donotgroup APT	Ariel Millahuel	SOC Prime Threat Detection Marketplace	431dbf8b11cf45bebac6646a5fe3c450c306b29edaf25977675ee072495216f8	0	0
Donotgroup APT	Ariel Millahuel	SOC Prime Threat Detection Marketplace	b3a4cba903a56c4b1c614cbde0de39dbec54a5aa5c8c8990df7f654b4a4c05ab	0	0
Download EXE from Suspicious TLD	Florian Roth	Sigma Integrated Rule Set (GitHub)	0182cb90eb98bcbd6b9724bdf7aa6f62ee6e327b059e24257dfd8339db0d3579	0	0
Download from Suspicious Dyndns Hosts	Florian Roth	Sigma Integrated Rule Set (GitHub)	d24da8eb78bf79c4be60dc23a68bd4ced6da6a3ad0eca8e8c2f4f43d08527e24	0	0
Download from Suspicious TLD	Florian Roth	Sigma Integrated Rule Set (GitHub)	5ccaad9297f4a0eab603caddab274e285f600daadd324b7ff0b1664d5fa19675	0	0
DragonFly variant (Goodor)	Ariel Millahuel	SOC Prime Threat Detection Marketplace	76c36e8978ca88131a604877350f6d74659dd6354870487d271706837731f68c	0	0
DragonFly variant (Goodor)	Ariel Millahuel	SOC Prime Threat Detection Marketplace	f9376b94f03fe9d6f1fa80fe124bddee8d9d51ee56b3e761e3b550f5717ea1e8	0	0

Dropping Of Password Filter DLL	Sreeman	Sigma Integrated Rule Set (GitHub)	ee1da0ec4e59bf6a30e8d78efcf41afcbe4babcee998f991aa62701b5fdb80df	0	0
Drovorub Malware Detection	Ariel Millahuel	SOC Prime Threat Detection Marketplace	00861734ad4b4865c4fd337b091aace8388feda059f681fa1a0d0a6659b55d31	0	0
Dump Credentials from Windows Credential Manager With PowerShell	frack113	Sigma Integrated Rule Set (GitHub)	5058b79d96d2165425d539e148ae3fe578dfa62b75b71f82ca2bd6bc347be4d5	0	0
DumpStack.log Defender Evasion	Florian Roth	Sigma Integrated Rule Set (GitHub)	9aa94cce0b20ff88d8c54a77c049e7d80f00af8ed4def6aa7395dc01692b5394	0	0
Dumpert Process Dumper	Florian Roth	Sigma Integrated Rule Set (GitHub)	4182b10f293111ccccca770ada467f9a23c6679818008b7436e1842cac95a691	0	0
Dumpert Process Dumper	Florian Roth	Sigma Integrated Rule Set (GitHub)	4f4552b72d1fdf1daa9803088eabda70a1a8259d5eae424fcbf3b7edae985b63	0	0
Dumpert Process Dumper	Florian Roth	Sigma Integrated Rule Set (GitHub)	9f11ecfc5795bbd9676baf8be43d9bd9f6da30f13022e7d97b279730326db7ad	0	0
Dumping Lsass.exe Memory with MiniDumpWrite Dump API	Perez Diego (@darkquassar), oscd.community	Sigma Integrated Rule Set (GitHub)	c2b930e9318dce446b4b4ed018e6ade935182bf7ca1404ae47923673beafee95	0	0
Dumping Process via Sqldumper.exe	Kirill Kiryanov, oscd.community	Sigma Integrated Rule Set (GitHub)	b8953b2fd9eedf5150cb430ec88f3653045e82c553904a73f87423600b427bee	0	0
Dumps Process Using tttracer.exe	Den Iuzvyk	SOC Prime Threat Detection Marketplace	1b2196c83bd73a6164882d3b22f19d200742a1d5541207b0e4b8684476e12ce2	0	0
Dupzom Trojan	Ariel Millahuel	SOC Prime Threat Detection Marketplace	68250cc49ef2301bbd3bc5104579a2f065206211acccf6978a71097bddd98d6d	0	0
Dupzom Trojan	Ariel Millahuel	SOC Prime Threat Detection Marketplace	b68ad5ecfba8b9b44e110368c029c99324cfa21b478209746fa0fcc441e51659	0	0
EDR WMI Command Execution by Office Applications	Vadim Khrykov (ThreatIntel), Cyb3rEng (Rule)	Sigma Integrated Rule Set (GitHub)	283d42c1fadd5e7b1d94efc708531703992e171a52b45eefe6e2eba61827fcdc	0	0
EKANS/SNAKE Ransomware (Sysmon detection)	Ariel Millahuel	SOC Prime Threat Detection Marketplace	164ef4a9c3213fa19bce8c0def1c7e491e774e8b12b55aaf55c5cc2732b4386f	0	0

EQNEDT32.EXE connecting to internet	Joe Security	Joe Security Rule Set (GitHub)	3b421cd3a4401c0dfc3d2c5613d705669e2bdcf8d998c4e363d2e1e5cbd328d4	0	0
Edit of .bash_profile and .bashrc	Peter Matkovski	Sigma Integrated Rule Set (GitHub)	cebaa2668c1b09efe1fcc6d468abfb9aa15dbba4c6e04246ba9e9f0bf407dc65	0	0
EfsPotato Named Pipe	Florian Roth	Sigma Integrated Rule Set (GitHub)	33bbc287fcdff32099d907d122b96db06214e7ef12bdbe38cc574df4fbcd94ff	0	0
Elise Backdoor	Florian Roth	Sigma Integrated Rule Set (GitHub)	7f1a0bd0e13fc71835ebb28c9bcd3329c320fbb38c22a6521ad2ec7afec74c71	0	0
Empire Monkey	Markus Neis	Sigma Integrated Rule Set (GitHub)	23618eea142f67106fec1f2e49084b25abad9af9614fd101fae65a465fce36f6	0	0
Empire Monkey	Markus Neis	Sigma Integrated Rule Set (GitHub)	5e739870e4f0680d4f5cb3caa8012e5362e20450756aaed3d6d5c2156e412a1c	0	0
Empire PowerShell UAC Bypass	Ecco	Sigma Integrated Rule Set (GitHub)	82469a7e6790faf9f415ad43cdf63ae3c4665bc5c9336e489f310de170797ea9	0	0
Empire UserAgent URI Combo	Florian Roth	Sigma Integrated Rule Set (GitHub)	2f9a27d9a32a1db53d0ad914de9cc96ab6822811498c2464c72d7ac1ae5ea6c8	0	0
Empty User Agent	Florian Roth	Sigma Integrated Rule Set (GitHub)	db3df2f3bab9e0691c10d2f198c0eed1ea877206a8230962360652fa37013d1e	0	0
Enable Windows Remote Management	frack113	Sigma Integrated Rule Set (GitHub)	7f8fcfb39f92617ac21dbc51e4c66b0663520cef30300bc28dd89572f6574253	0	0
Enabled User Right in AD to Control User Objects	@neu5ron	Sigma Integrated Rule Set (GitHub)	5b7c1293fd9b0e601e332e3957086d1d0c6a06bfadd6c43e4270efb3277d3f29	0	0
Enabling COR Profiler Environment Variables	Jose Rodriguez (@Cyb3rPandaH), OTR (Open Threat Research)	Sigma Integrated Rule Set (GitHub)	54d006ecd6dae89f884b01b6fbaa0d8010a9ab60d59993aa4d10c45146c3b4ca	0	0
Enabling RDP remotely using PsExec	Ruslan Mikhalov, SOC Prime Team	SOC Prime Threat Detection Marketplace	a0da5ca640c0db1d98b306ba62d3da18bb15ee97be16ca41d672fe2e8ebec17c	0	0
Enumerate Credentials from Windows Credential Manager With PowerShell	frack113	Sigma Integrated Rule Set (GitHub)	0470d9b3a45f6fadd111284469ea5f0dc2a9e4cebf5973ac13ec483c7c1e072b	0	0
Enumeration for Credentials in Registry	frack113	Sigma Integrated Rule Set (GitHub)	cf1e24c4e4b805857977d873b41de8cf08d618fa56ffb27ece5e9b41e84807d6	0	0
Enumeration via the Global Catalog	Chakib Gzenayi (@Chak092), Hosni Mribah	Sigma Integrated Rule Set (GitHub)	1305672c2572166a4d69a39b49ae88090a50a828e90fe74ecbcb764defc3658e	0	0

Equation Group C2 Communication	Florian Roth	Sigma Integrated Rule Set (GitHub)	ec2be6d2ee05ce5b9bbe5fa0e0c88445206d45c31719b20f8b334b51509702ca	0	0
Equation Group Indicators	Florian Roth	Sigma Integrated Rule Set (GitHub)	214644f8f8defe22c479a808c315e0abeab487ba6453aea73b617671e82afc64	0	0
Evasion Base64 decode arguments in Powershell. (Possible APT29 activity)	Roman Ranskyi	SOC Prime Threat Detection Marketplace	66bf1484dc26be16a812d0aad2d4ac6fb6a930d54d654fefdb5395f2f5bdd569	0	0
Evasive Azorult detection	Ariel Millahuel	SOC Prime Threat Detection Marketplace	bc6f9cb8f39b70734c26b70f509cd672b3173413fef65146e95364ccd778a60e	0	0
Event Tracing(ETW) .NET Bypassing	Den Iuzvyk	SOC Prime Threat Detection Marketplace	6069c607c41cfbdf480184c91403313c4f458c82732ed81f1cff013d545756f6	0	0
Eventlog Cleared	Florian Roth	Sigma Integrated Rule Set (GitHub)	21811843bfb7d3bd52d24ba751e69b943436736e36c5b88a3f0f5d4f80c042fd	0	0
Eventlog Cleared	Florian Roth	Sigma Integrated Rule Set (GitHub)	7ab84c6091a1b4ceb1d00bb8f3be32dcd111618b7e0b705f7a14f2696bd4527c	0	0
Eventlog Cleared	Florian Roth	Sigma Integrated Rule Set (GitHub)	eef34d2dd2c9264ef00f80ce3cee8c0b7232729bfb39f5f5258afc0701b750ba	0	0
EvilNum Golden Chickens Deployment via OCX Files	Florian Roth	Sigma Integrated Rule Set (GitHub)	c07dab99223af1d0dcc74e5419200d751c154be9bf5fb4f8817b718b80074034	0	0
Excel Network Connections	Christopher Peacock '@securepeacock', SCYTHE '@scythe_io', Florian Roth '@Neo23x0"	Sigma Integrated Rule Set (GitHub)	cfd44c3835317e846b18021a9060f4b9b011294ec53eb3ac1fad568abeb37922	0	0
Excel Proxy Executing Regsvr32 With Payload	Vadim Khrykov (ThreatIntel), Cyb3rEng (Rule)	Sigma Integrated Rule Set (GitHub)	368433c7157e0778f035c6c8b5a6cd0f273d860606bfa36f632144c7050b4c7d	0	0
Excel Proxy Executing Regsvr32 With Payload	Vadim Khrykov (ThreatIntel), Cyb3rEng (Rule)	Sigma Integrated Rule Set (GitHub)	769fe648255c0a237ee125f74d2685b54cf7799f6b5cffeae1f2fee47164091c	0	0
Exchange Exploitation CVE-2021-28480	Florian Roth	Sigma Integrated Rule Set (GitHub)	8b0df83cd0067e8ec609c343855fdc202dc02e08333f53087a98ea20ae5a5b9a	0	0
Exchange Exploitation Used by HAFNIUM	Florian Roth	Sigma Integrated Rule Set (GitHub)	fa61fa3a9e1eb0bec15a00e9a84860be9b60903bc1901454841437fa15d2b33e	0	0

Exchange PowerShell Snap-Ins Used by HAFNIUM	FPT.EagleEye	Sigma Integrated Rule Set (GitHub)	d6b23e65044f31aa0e870c30cfcb96f03b4e07207a6ee29c0ed9707981459b23	0	0
Exchange ProxyShell Pattern	Florian Roth, Rich Warren	Sigma Integrated Rule Set (GitHub)	64bc18e376a29a7021c54cb9dd0360d271fdc492dfe549706a750fcce1c06b85	0	0
Exchange Set OabVirtualDirectory ExternalUrl Property	Jose Rodriguez @Cyb3rPandaH	Sigma Integrated Rule Set (GitHub)	76f94274bd2a1a2e6fff0a84131b19b7a88097a0ecdf13f713b85cbe87821798	0	0
Exe Launched By ReflectiveLoader Dll	Joe Security	Joe Security Rule Set (GitHub)	fb6e575b96ef105d7648f2fbb84e53c968901fc34652bf51317f8fa76685654f	0	0
Executable from Webdav	SOC Prime, Adam Swan	Sigma Integrated Rule Set (GitHub)	c5b9b720930832b94426c87d7d20296939a583d3a341561476b195402c712b66	0	0
Executable from Webdav - Zeek	SOC Prime Team	SOC Prime Threat Detection Marketplace	39c77a2689a21b694239fd44d2ca79bd9fbdd010599631d811030596b2bb794d	0	0
Executable in ADS	Florian Roth, @0xrawsec	Sigma Integrated Rule Set (GitHub)	5be9da0a90b142239a3ff2819edf2283938855da3b4c80d63d8e6db63c2c4fe7	0	0
Execute Code with Pester.bat	Julia Fomina, oscd.community	Sigma Integrated Rule Set (GitHub)	4c7cd76bbfcbeccd5a632e9635a2ba08c7f1b72ecfc3b734d01e3a46c75c1779	0	0
Execute Files with Msdeploy.exe	Beyu Denis, oscd.community	Sigma Integrated Rule Set (GitHub)	01d30cac08cb23905f4eacf48a745712b09efd4d13ece8136df401f4fa5a9969	0	0
Execute From Alternate Data Streams	frack113	Sigma Integrated Rule Set (GitHub)	050886ba2f2b1f82f8131a47ce6b22fb2663a44155ba973da3477fde647c06a5	0	0
Execute Invoke-command on Remote Host	frack113	Sigma Integrated Rule Set (GitHub)	61dae8b0a35fc9369e410406f226b559d6c9cb12837347724e7c4f9281869910	0	0
Execution DLL of Choice Using WAB.EXE	oscd.community, Natalia Shornikova	Sigma Integrated Rule Set (GitHub)	99b21cfd2dee5c20c4ee150c1f8ff725e843b680ad0362dc10682baf38dba493	0	0
Execution in Outlook Temp Folder	Florian Roth	Sigma Integrated Rule Set (GitHub)	e10440993b0b656a1a8c6d3b8e4bbc81af5b7f7cc7b8373de18dea6d80adae4e	0	0
Execution of Renamed PaExec	Jason Lynch	Sigma Integrated Rule Set (GitHub)	bc6e1fabac9a6bb91d67a4a5439f899182862c791a4d2bb72fbaf27b552554d6	0	0
Execution via CL_Invocation.ps1	oscd.community, Natalia Shornikova	Sigma Integrated Rule Set (GitHub)	076e35f57ad985cac0733c6afe62d6b1e84acd633b22254d9de99c537d5d5c6f	0	0
Execution via CL_Invocation.ps1	oscd.community, Natalia Shornikova	Sigma Integrated Rule Set (GitHub)	c162774264013dd3be5fe01db608c8cd43087fb90d8ec4a8371ec6c119f1fef0	0	0
Execution via CL_Invocation.ps1 (2 Lines)	oscd.community, Natalia Shornikova	Sigma Integrated Rule Set (GitHub)	ceefb57442e718017497079909d69108b161f2d2e4a973242e7e2386648bee9b9	0	0

Execution via CL_Mutexverifiers.ps1	oscd.community, Natalia Shornikova	Sigma Integrated Rule Set (GitHub)	1394e1d2c663042f47108fb190ff989e13550eff19ce6db03ef09a0c5a92aaec	0	0
Execution via CL_Mutexverifiers.ps1	oscd.community, Natalia Shornikova	Sigma Integrated Rule Set (GitHub)	e0857d3351e317e009063a5853ed0234b65be28d6b94c9727a4473d4bd135d9c	0	0
Execution via CL_Mutexverifiers.ps1 (2 Lines)	oscd.community, Natalia Shornikova	Sigma Integrated Rule Set (GitHub)	389839a4c3b9d52b701fe26dbe2f77f37e841fec35467860ced1accddf84b24d	0	0
Execution via Diskshadow.exe	Ivan Dyachkov, oscd.community	Sigma Integrated Rule Set (GitHub)	1fc7c2d6af25fd4fb6af44ba89bae55555dbcfdcc31e586fd94298ac39ea011d	0	0
Execution via stordiag.exe	Austin Songer (@austinsonger)	Sigma Integrated Rule Set (GitHub)	c012b058c607c697ab3013783a9a418dd2b233fa1f22ea4f8160238a19c65577	0	0
Exploit Framework User Agent	Florian Roth	Sigma Integrated Rule Set (GitHub)	5568bf39e0e0778586bb12b9eec75fa632d667e59d9a2593a81fc3c1f92482df	0	0
Exploit SamAccountName Spoofing with Kerberos	frack113	Sigma Integrated Rule Set (GitHub)	864e1d1683353be902b628fefefe866931925fd28550796b04dc914f4e7ff53ea	0	0
Exploit for CVE-2015-1641	Florian Roth	Sigma Integrated Rule Set (GitHub)	d3c02a535ea8c2ccc601d4d5317b74c2389350cbeffab45fe35634fb61351840	0	0
Exploit for CVE-2017-0261	Florian Roth	Sigma Integrated Rule Set (GitHub)	9931af355487f8ba552a4261f563cca37a36e808d77f2dbc3857687968010e3a	0	0
Exploit for CVE-2017-8759	Florian Roth	Sigma Integrated Rule Set (GitHub)	9697bdf7c6b76b101974ea8a0feee97c4b309c7c74d5ccbf4e0c2b3a5e03f167	0	0
Exploitation of CVE-2021-26814 in Wazuh	Florian Roth	Sigma Integrated Rule Set (GitHub)	e9dbd9775b62ea76e1f299caeec38e889d5ade4d1b9f15f0125be4c6c34f6ed8	0	0
Exploited CVE-2020-10189 Zoho ManageEngine	Florian Roth	Sigma Integrated Rule Set (GitHub)	f85ce5948989e315c57d34da1951a85d6b29e1dd91e294fed17c4c5d2a65ca26	0	0
Exploiting CVE-2019-1388	Florian Roth	Sigma Integrated Rule Set (GitHub)	ca8e07ebb4a9e88b2988f1c2c1da442f21dd9e29212734cad87963436e07697a	0	0
Exploiting SetupComplete.cmd CVE-2019-1378	Florian Roth, oscd.community, Jonhnathan Ribeiro	Sigma Integrated Rule Set (GitHub)	aaf4513bd87abe8d41992949584d6e69d734d9f68ef90eaa97be26b350d990c6	0	0
Exports Critical Registry Keys To a File	Oddvar Moe, Sander Wiebing, oscd.community	Sigma Integrated Rule Set (GitHub)	dbe237db785de8531f797d5f0689f67cf0389152523f491db2c761f5888de930	0	0
Exports Registry Key To an Alternate Data Stream	Oddvar Moe, Sander Wiebing, oscd.community	Sigma Integrated Rule Set (GitHub)	9695789356ce1e4c280773e1a4990ee193bc17704d78da2b4acb48eed6061293	0	0
External Disk Drive Or USB Storage Device	Keith Wright	Sigma Integrated Rule Set (GitHub)	69ec9de0dde4471e41ee7ac007a2e667bee45fc610f59477cfcd75bb72afdf6a	0	0

External Facing ICS DNP3	SOC Prime Team	SOC Prime Threat Detection Marketplace	f91099b17f9d1bca0d4db4e5b0ad22f95649383e9cf2240cc0abc68540881418	0	0
External Proxy Detected (Overview Query)	SOC Prime Team	SOC Prime Threat Detection Marketplace	8871bb484e485ff18029d70ed25036cf72ae96f363232176d3f639f5ffc8c719	0	0
Extracting Information with PowerShell	frack113	Sigma Integrated Rule Set (GitHub)	4e243e6a618f306cfd754df3b30132c4fa518c4ad26b6d755244064cd3110b0f	0	0
F-Secure C3 Load by Rundll32	Alfie Champion (ajpc500)	Sigma Integrated Rule Set (GitHub)	ca26332fee8f2e589029cf0e8f2b212bae02121915a9cc3a2cefe4c1a96419c1	0	0
FASTCash 2.0 - North Korea's BeagleBoyz Robbing Banks	Ariel Millahuel	SOC Prime Threat Detection Marketplace	328842f9bf7293774dba7e98cfbc8dc38cc5c3bfd0b550b66f9f388d2364db6b	0	0
FASTCash 2.0 - North Korea's BeagleBoyz Robbing Banks	Ariel Millahuel	SOC Prime Threat Detection Marketplace	4f4f4d2ef9741a90d68b3e1ca5439694604fc80bcb02c3cbde70096562cc6000	0	0
FIN7's Backdoor "GRIFFON"	Ariel Millahuel	SOC Prime Threat Detection Marketplace	94db0c3a112be50fd02c2ff8b6bdb0ac37e92b752979f8c6f2e5563abe56be96	0	0
FIN7's Backdoor "GRIFFON"	Ariel Millahuel	SOC Prime Threat Detection Marketplace	b76c81cee8f9040791d362bde9fa5c5ec808c3d2f0fce6f9f4a04448b9e10018	0	0
FORMBOOK Detection	Ariel Millahuel	SOC Prime Threat Detection Marketplace	4675166eaef352485a92c18a16d156904430c5c7735fd58dba24cf182c23d60e	0	0
FORMBOOK Detection	Ariel Millahuel	SOC Prime Threat Detection Marketplace	eeee8664c6a13d9135d1338a6561c8e98c8d43e7769fb1532912f88a85cfc98d	0	0
Failed Logins with Different Accounts from Single Source System	Florian Roth	Sigma Integrated Rule Set (GitHub)	39c6740d7e5a4065ad484a47fdf900dac6ebb236a092d3a62ae08b42f997aaf4	0	0
Failed Logins with Different Accounts from Single Source System	Florian Roth	Sigma Integrated Rule Set (GitHub)	96209abdf48c67f20055c6bff1def00f64467ff7b6241d0f81f46fb6dd9c45ce	0	0
Failed Logins with Different Accounts from Single Source System	Florian Roth	Sigma Integrated Rule Set (GitHub)	c205af7876e4586e4a5a6daf3886f1baa3df67852a520806aa99706ca5d30f1d	0	0

Failed Logins with Different Accounts from Single Source System	Florian Roth	Sigma Integrated Rule Set (GitHub)	ca722b22c08d09482ee7e905dc151bc4c635059ae6cca8d5e7319d79d75a939b	0	0
Failed Logins with Different Accounts from Single Source System	Florian Roth	Sigma Integrated Rule Set (GitHub)	da16f0c4a5327c930eada87193754d50bfcbe86ae02f2b346843be759f3bf068	0	0
Failed Logins with Different Accounts from Single Source System	Florian Roth	Sigma Integrated Rule Set (GitHub)	e0dab5d045b0693435584647bbbacf51af451c35bf9073723e14ce5e9faa977a	0	0
Failed Logon From Public IP	NVISO	Sigma Integrated Rule Set (GitHub)	747bd73d4c017e43abc40ee62507a5889d075d5fde6a504c4d858fa2bcf544cf	0	0
Failed MSExchange Transport Agent Installation	Tobias Michalski	Sigma Integrated Rule Set (GitHub)	4ffd23c451cedb770f7b27887ee3bedb3bd28836fcf3f1af17ddfcc02f42244f	0	0
Fax Service DLL Search Order Hijack	NVISO	Sigma Integrated Rule Set (GitHub)	4bd3cd7f770c6c3ec6329529702f55c609cbd0c8220a36c08756e56a5eb0e553	0	0
File Creation by Office Applications	Vadim Khrykov (ThreatIntel), Cyb3rEng (Rule)	Sigma Integrated Rule Set (GitHub)	4c867f43073512dc59c123d57114baa298a7f696a87ca8842fba36f25783ba49	0	0
File Deletion	Ömer Günal, oscd.community	Sigma Integrated Rule Set (GitHub)	ca09f90f6791c066d3cb4ab07b1fbc4ed8bc75831b99eae0123b994db452cc63	0	0
File Download with Headless Browser	Sreeman, Florian Roth	Sigma Integrated Rule Set (GitHub)	ab434fe480ee2a7a4567eef38af37753eb61b2fe82708db1056313a73ab0fac0	0	0
File Time Attribute Change	Igor Fits, oscd.community	Sigma Integrated Rule Set (GitHub)	98a04cf3e09ed0fd0d955b1233d5da45cab63a5a2370ab7dc16a507783467e67	0	0
File Time Attribute Change	Igor Fits, Mikhail Larin, oscd.community	Sigma Integrated Rule Set (GitHub)	cf228b836870037eda6ce9d429595c3a3c8bb83b64b142fc4dae821bc43b3fd8	0	0
File Was Not Allowed To Run	Pushkarev Dmitry	Sigma Integrated Rule Set (GitHub)	9a03b6952f3ce7ab37238d17b0e583d82c02641e1cd9add5995da0319dc8e27f	0	0
File and Directory Discovery	Daniil Yugoslavskiy, oscd.community	Sigma Integrated Rule Set (GitHub)	3d3b45d016905389c43a4a14252fb73bf6a6f29ca1d925f44b19ff52a9bc0571	0	0
File and Directory Discovery	Daniil Yugoslavskiy, oscd.community	Sigma Integrated Rule Set (GitHub)	de61a9a6e51619752c9f8bf87bb41536abc4f6983711039dcef99b9732a26713	0	0
File or Folder Permissions Change	Jakob Weinzettl, oscd.community	Sigma Integrated Rule Set (GitHub)	2aa85d50392d0c934bd643168b9d6106622e796b2f125ccbfdbc65beb9d9328d	0	0
Files Dropped to Program Files by Non-Priviledged Process	Teymur Kheirkhabarov (idea), Ryan Plas (rule), oscd.community	Sigma Integrated Rule Set (GitHub)	0dec80af16a1229c7c8b9478448b6a3fe7a1cd392768c3d11e0cc1d3f56ce89c	0	0

FindPOS Banking Trojan (Sysmon detection)	Ariel Millahuel	SOC Prime Threat Detection Marketplace	b4f6a2934ee226030f077e9c78924c5b5a78d41ee66a0529dd426becc7b33ddd	0	0
Findstr GPP Passwords	frack113	Sigma Integrated Rule Set (GitHub)	6403688c88307224c6c37547c26a3634868d77d08502d77529f03daacc410a51	0	0
First Time Seen Remote Named Pipe	Samir Bousseaden	Sigma Integrated Rule Set (GitHub)	8f55e684b93688b5ada963a92be16b72c1a0cfc3cb3de96dd117b81f4ca48353	0	0
First Time Seen Remote Named Pipe - Zeek	SOC Prime Team	SOC Prime Threat Detection Marketplace	480a8350961bc4753587db029d2b4b67af4927083b258b8ac071d0dea69e5107	0	0
First Time Seen Remote Named Pipe - Zeek	Samir Bousseaden, @neu5ron	Sigma Integrated Rule Set (GitHub)	6dfb9593c473f7b52b104c46e0f2ae974fd27365b3fef076729065c3ceb7336d	0	0
Flash Player Update from Suspicious Location	Florian Roth	Sigma Integrated Rule Set (GitHub)	f98973bb4e1b72aebf2e59eaeb00827a358135f7260cf198ac43e31c7422e15b	0	0
FlowCloud Malware	NVISO	Sigma Integrated Rule Set (GitHub)	ac4c45d3a4b76d63ba2158cb0a11df8d1e2733506cb845e78700108737b600ee	0	0
FoggyWeb Backdoor DLL Loading	Florian Roth	Sigma Integrated Rule Set (GitHub)	668c7b595f169cd509eb51c29bc594ff624919395214381e2eac4fa7ff9e94ac	0	0
Format.com FileSystem LOLBIN	Florian Roth	Sigma Integrated Rule Set (GitHub)	9e9f93dcbdb926c3870d61f8a14fc94391072517d56855658b4592a4e886289c	0	0
Fortinet CVE-2018-13379 Exploitation	Bhabesh Raj	Sigma Integrated Rule Set (GitHub)	48f4e640f9feb5bf31487a870784507ef5f7d38f22e9b62e9bbd954a197833ca	0	0
Fortinet CVE-2021-22123 Exploitation	Bhabesh Raj, Florian Roth	Sigma Integrated Rule Set (GitHub)	c1c52f5ba98a73c39c7b7d859118c45a22218d1c92dbd128e54bcb34942092c7	0	0
Frat Trojan (Loader detection)	Ariel Millahuel	SOC Prime Threat Detection Marketplace	ea1d6297c25d9b1788bf0e9bb1ef3fe785a4ced33855144d3102a01fd227049a	0	0
GAC DLL Loaded Via Office Applications	Antonlovesdnb	Sigma Integrated Rule Set (GitHub)	10c0778367f03c51cf9136815b90c0d7a820fa857a135c645c55014481fd1395	0	0
GALLIUM Artefacts	Tim Burrell	Sigma Integrated Rule Set (GitHub)	13e966f80ac9708db929626d50e35b4c614959c0d209d09425ff454546ad372a	0	0
GALLIUM Artefacts	Tim Burrell	Sigma Integrated Rule Set (GitHub)	4aa39f58ddd2f2f3bdd80a29f42c84ca2fe61a048fc8819faaff5df28a22b7db	0	0
GALLIUM Artefacts	Tim Burrell	Sigma Integrated Rule Set (GitHub)	54e36ba8fed69643d4a587cef4fddde07614258a1c1996ed0c958450ccadf258	0	0
GALLIUM Artefacts	Tim Burrell	Sigma Integrated Rule Set (GitHub)	a28fbac5cff189dab10e229b3a0ae2e24b372d2b111d7262fd83043e661ef513	0	0

GALLIUM Artefacts	Tim Burrell	Sigma Integrated Rule Set (GitHub)	a43dac5f26c85a94239a74415d13e774debdccd841db311740a5727d95a105bb	0	0
GALLIUM Artefacts	Tim Burrell	Sigma Integrated Rule Set (GitHub)	a850462e96a471d0210fd57a8d09b89aa9d484414bb317ed6f8dfba6bfee5d84	0	0
GALLIUM Artefacts	Tim Burrell	Sigma Integrated Rule Set (GitHub)	d1012f082becc4692509094f0b3f52f4bfff06a6a239d05da80ed461dad4a230	0	0
GALLIUM Artefacts	Tim Burrell	Sigma Integrated Rule Set (GitHub)	fc4bbb141d939f93ce4dba43aa3b43e635f4dda080c5e27ee58529a1563dab8e	0	0
GUI Input Capture - macOS	remotephone, oscd.community	Sigma Integrated Rule Set (GitHub)	e8a715c11ff2888a95d902af6f79e1e2aac74e027662e679bf2d24be5d33ec77	0	0
Gamaredon Group Behavior (Sysmon detection)	Ariel Millahuel	SOC Prime Threat Detection Marketplace	0f97ccec7b149884820f61a172664b0ab480111696291696cb4b3e7ae011c34f	0	0
Gatekeeper Bypass via Xattr	Daniil Yugoslavskiy, oscd.community	Sigma Integrated Rule Set (GitHub)	7f400a75c32e600540f4565bd2cb4099e67aab98f70299b5fe20136c9bc9f13b	0	0
GatherNetworkInfo.vbs Script Usage	blueteamer8699	Sigma Integrated Rule Set (GitHub)	93d3c8484d953299cdaafb696acdb7e33fd8a569cd8682a0d501a122f2b8290b	0	0
Generic Password Dumper Activity on LSASS	Roberto Rodriguez, Teymur Kheirkhabarov, Dimitrios Slamaris, Mark Russinovich, Aleksey Potapov, oscd.community (update)	Sigma Integrated Rule Set (GitHub)	021958a970490c9f053ccc5d257c9c5f17746ceb0270b213e185a4c9354e912c	0	0
Geofenced Ru	Joe Security	Joe Security Rule Set (GitHub)	562da91a76462659002a010f3f5e20f6ea8d3c7771e342dce7b3d0b5b2421eb8	0	0
Get antivirus details via WMIC query	Joe Security	Joe Security Rule Set (GitHub)	6e2720fef4d33bcf8ad643d1ff91ff392e3afc91ad4446024cf5a4dfa46685aa	0	0
Get2 Downloader	Joe Security	Joe Security Rule Set (GitHub)	959a4fa9a66799f33b7f7ea4c82ec1869a3031768b47d0a7be1221b66ee355bd	0	0
Glupteba malware detection	Ariel Millahuel	SOC Prime Threat Detection Marketplace	7d6a15e8de84af0efc173edd7fc1d08b2c8d250be90a41056ded2b99d918271c	0	0
GoldenHelper Behavior (Sysmon detection)	Ariel Millahuel	SOC Prime Threat Detection Marketplace	85d7d4821cc1ccf999a9455b3045c5778b716b7140209df1e1293db41bbc0bea	0	0
Google Cloud DNS Zone Modified or Deleted	Austin Songer @austinsonger	Sigma Integrated Rule Set (GitHub)	4e9fe08e5c9be680bfaf33cddcd1081cd3aba686ce5077b1cd0b5856663dbe0e	0	0
Google Cloud Firewall Modified or Deleted	Austin Songer @austinsonger	Sigma Integrated Rule Set (GitHub)	75e61beb3d99547100af121b2ea1688aa808d3688450d44d493780d2cc802900	0	0

Google Cloud Kubernetes Admission Controller	Austin Songer @austinsonger	Sigma Integrated Rule Set (GitHub)	5790f7e831d8a6bc3ca5c218539243db16d6289b537af31c00d082fe78ed2c01	0	0
Google Cloud Kubernetes CronJob	Austin Songer @austinsonger	Sigma Integrated Rule Set (GitHub)	06da8a78620eee29e603c816960eae96dcb6ef22786be2395c7c89a4483be9c6	0	0
Google Cloud Kubernetes RoleBinding	Austin Songer @austinsonger	Sigma Integrated Rule Set (GitHub)	555a6561c2563b49ce91769c6ac3f56617339b3b8813f72c9fa1bd32ec71f74e	0	0
Google Cloud Kubernetes Secrets Modified or Deleted	Austin Songer @austinsonger	Sigma Integrated Rule Set (GitHub)	6ee389129056d76efea184ded09eba9cf1c324f400b3d0d50b87786d565d0e03	0	0
Google Cloud Re-identifies Sensitive Information.	Austin Songer @austinsonger	Sigma Integrated Rule Set (GitHub)	ddff51832fbd0426593249f7816c2949713da15d8f5f43d7bf73dbe4402ba1c3	0	0
Google Cloud SQL Database Modified or Deleted	Austin Songer @austinsonger	Sigma Integrated Rule Set (GitHub)	a916fae3b74465ca20244fcbd2427d10e602ebd5bd23e20c830516535a652466	0	0
Google Cloud Service Account Disabled or Deleted	Austin Songer @austinsonger	Sigma Integrated Rule Set (GitHub)	5162849b0852d05e10e767dcf89c82633c89592c636df59cea0c8d66143fef63	0	0
Google Cloud Service Account Modified	Austin Songer @austinsonger	Sigma Integrated Rule Set (GitHub)	26b1499ccf7a72e494ae575cfa25674e193d0d80f0ee981977d65e518bf7575f	0	0
Google Cloud Storage Buckets Enumeration	Austin Songer @austinsonger	Sigma Integrated Rule Set (GitHub)	f5a9b68010504eff3ab69d1406d28ce83a81c9b2399b5424d60221ca6c707c08	0	0
Google Cloud Storage Buckets Modified or Deleted	Austin Songer @austinsonger	Sigma Integrated Rule Set (GitHub)	432ac1fb76a98caf7e4c2c36dc767867c71c8241b3abb88c238e09dd1dd6eb52	0	0
Google Cloud VPN Tunnel Modified or Deleted	Austin Songer @austinsonger	Sigma Integrated Rule Set (GitHub)	1ec92cc5b58c4d0aba97c210716e4f4a0e3bc4148bac041b47e830680b25de8d	0	0
Google Full Network Traffic Packet Capture	Austin Songer @austinsonger	Sigma Integrated Rule Set (GitHub)	11db866a2c986c2622afc6b4e18e39a469b925ba219af228e1b93928526e7317	0	0
Google Workspace Application Removed	Austin Songer	Sigma Integrated Rule Set (GitHub)	7aad3ceec393171e628be57ad1507a50aaa34f68bfa8af505481b9406de81834	0	0
Google Workspace Granted Domain API Access	Austin Songer	Sigma Integrated Rule Set (GitHub)	7447e9cdd0e5729172c1c9f7143faf9ada51a1e939eb6100d7066e46913117c5	0	0
Google Workspace MFA Disabled	Austin Songer	Sigma Integrated Rule Set (GitHub)	a6f7ea87e017ce01123928b2e8c2bee1808d90c322c0fe3f8660c929ed149b5d	0	0

Google Workspace Role Modified or Deleted	Austin Songer	Sigma Integrated Rule Set (GitHub)	a941017b4f691cb4487bac97de7b0d0a9649ffd6b3f402774dde963b3e3ecdaa	0	0
Google Workspace Role Privilege Deleted	Austin Songer	Sigma Integrated Rule Set (GitHub)	9eb6ba62c47e14ada70fa08f7edc5aeb9118c433612b3feba5a7ce44fc77a909	0	0
Google Workspace User Granted Admin Privileges	Austin Songer	Sigma Integrated Rule Set (GitHub)	107b17aa4a3574e6f295747881192bc95a741ad7258df4c3d1abeb9bcd9031d5	0	0
Grafana Path Traversal Exploitation CVE-2021-43798	Florian Roth	Sigma Integrated Rule Set (GitHub)	e5ef12864d0d0ecf036674826506d6184e1b067e991808aa0e1ff455c7ac0dcd	0	0
GrandSteal Malware	Ariel Millahuel	SOC Prime Threat Detection Marketplace	4f31c3fa158f312c5152f83df386b1fb92e53b215040fb3ae268cbb215e31429	0	0
Grandoreiro banking trojan	Den Iuzvyk	SOC Prime Threat Detection Marketplace	43c3cf1aec99bd2e109fd3867cd77e17e8a24f54da3251b30dd592cf83272b56	0	0
Granting Of Permissions To An Account	sawwinnnaung	Sigma Integrated Rule Set (GitHub)	2c4ab12457b78f88ac5191037416703011e6de4aa39693b09e20823de2f0f42f	0	0
Guacamole Two Users Sharing Session Anomaly	Florian Roth	Sigma Integrated Rule Set (GitHub)	17fc2e35d07c0b3986643b473df8b54cf3371854ed30f7d65fe415a944ba6961	0	0
Guildma detection (sysmon and cmdline)	Ariel Millahuel	SOC Prime Threat Detection Marketplace	1e6ac5cb97a765bdc2b15c1ca55ec978b04d9511ddba2126304966bde1b17fde	0	0
Guildma detection (sysmon and cmdline)	Ariel Millahuel	SOC Prime Threat Detection Marketplace	3394ac20f81b6dbd77a611e1dfd1c52794b199583960710ebc28c01bae3a27a4	0	0
HTTP POST or PUT URI Non ASCII Character	SOC Prime Team	SOC Prime Threat Detection Marketplace	c4ee6e518d8bece54b732fc5a27bd8515ed478d3f31681891fab56111b6ca18f	0	0
Hack Tool User Agent	Florian Roth	Sigma Integrated Rule Set (GitHub)	9645aaedf8ece3691433afeb39dfddf3048958fa600acc234a56f522b4f41b8e	0	0
Hacktool Ruler	Florian Roth	Sigma Integrated Rule Set (GitHub)	cd304d70f67c3d14033f831971d45bee3264cc411ea28209db2f6d148ea9f2f6	0	0
HawkEye malware - Coronavirus scam (Sysmon detection)	Ariel Millahuel	SOC Prime Threat Detection Marketplace	06789be682ab6cf58699c03653b66c7f9299038c2c44e967e3c68a2e40fdbbdc	0	0

HawkEye malware - Coronavirus scam (Sysmon detection)	Ariel Millahuel	SOC Prime Threat Detection Marketplace	b7f993191f989d1f86bba4825f6e96a7c27e80b1bcdbf6ed6478ae89239222eb	0	0
Hidden Files and Directoriese	Pawel Mazur	Sigma Integrated Rule Set (GitHub)	6c95803fd57ca93faa4a13a1be90825b893e3d84ac45ca8c70e80cf1574d4028	0	0
Hidden Tear Ransomware	Ariel Millahuel	SOC Prime Threat Detection Marketplace	6416d92c1d6493914510053de27fbb52201520df66cac075111034d37aac4194	0	0
Hidden Tear Ransomware	Ariel Millahuel	SOC Prime Threat Detection Marketplace	b11fac69696a228f0a15679f595df7b336dde8d11522e2dfdd9e1004aacf5721	0	0
Hidden User Creation	Daniil Yugoslavskiy, oscd.community	Sigma Integrated Rule Set (GitHub)	809fde43d8c51148345ce94401363b56daa369da6e6bdb766f26a3a3af847f65	0	0
High DNS Bytes Out	Daniil Yugoslavskiy, oscd.community	Sigma Integrated Rule Set (GitHub)	2bc3d95bf98633de61ea95a005c1b04db78ea390377ce363fc04a09d20374cde	0	0
High DNS Bytes Out	Daniil Yugoslavskiy, oscd.community	Sigma Integrated Rule Set (GitHub)	4e81552b913384840b8f3b631ab5be105841ff6a829f1a496fd1e3e13effafba	0	0
High DNS Bytes Out	Daniil Yugoslavskiy, oscd.community	Sigma Integrated Rule Set (GitHub)	5d26dba8fce23cc9f2e893e61faa96cbbae4bce1e530e4154294172451e4a1b1	0	0
High DNS Bytes Out	Daniil Yugoslavskiy, oscd.community	Sigma Integrated Rule Set (GitHub)	a958051334fc197d28be902cc93f3d866e1ca9a16f90a70f21bd60a2f47fbc29	0	0
High DNS Bytes Out	Daniil Yugoslavskiy, oscd.community	Sigma Integrated Rule Set (GitHub)	db7861630c3853feeea696d711f739104df19b415fd9ba6c1a8fec46002a8fbf	0	0
High DNS Requests Rate	Daniil Yugoslavskiy, oscd.community	Sigma Integrated Rule Set (GitHub)	16b85da18d9082b3b4511ae7d959fbf89409bb88f17d708af4f48b0a422adefb	0	0
High DNS Requests Rate	Daniil Yugoslavskiy, oscd.community	Sigma Integrated Rule Set (GitHub)	2082aad99bb35c4089a7d806951cf7090bca3bdeb0a052f761dc38d878e58c57	0	0
High DNS Requests Rate	Daniil Yugoslavskiy, oscd.community	Sigma Integrated Rule Set (GitHub)	4d753950eaec7ac9fc0b84352b52a7d1e44cd4806bded593087c93032ce8e29a	0	0
High DNS Requests Rate	Daniil Yugoslavskiy, oscd.community	Sigma Integrated Rule Set (GitHub)	888de5606c7898a641ac0f06071d731769cd6a0c2a8638b9bd65e4c7832b4a8c	0	0
High DNS Requests Rate	Daniil Yugoslavskiy, oscd.community	Sigma Integrated Rule Set (GitHub)	fb55eac70ca85e41bd6aedae03e77e21466cde4d3e05bdccc80080c9df288d8f	0	0
High NULL Records Requests Rate	Daniil Yugoslavskiy, oscd.community	Sigma Integrated Rule Set (GitHub)	85891d3694d60dcdc316d135514866fe396add3b76b77fb7cb7757ce6012957c	0	0
High TXT Records Requests Rate	Daniil Yugoslavskiy, oscd.community	Sigma Integrated Rule Set (GitHub)	27156cd3bf11019c9f610f2ca55106a23d64717f78b7db1730a6b20daae7fc23	0	0

Hiloti Trojan	Ariel Millahuel	SOC Prime Threat Detection Marketplace	6bb0fcaf34349cee860ba3a315fdc7aed5aa00d66dcf54cae167073a246cf851	0	0
Hiloti Trojan	Ariel Millahuel	SOC Prime Threat Detection Marketplace	f8a63428721bcc8ad6de541a48e0a1f21d8e73a4f114603bcb7e9066042c502c	0	0
HiveRAT detection	Ariel Millahuel	SOC Prime Threat Detection Marketplace	1542db80b3c0353f1a027f7ddd3b1a2980335d4ef03fae03a4f951743f67648e	0	0
Host Without Firewall	Alexandr Yampolskyi, SOC Prime	Sigma Integrated Rule Set (GitHub)	b27d91650a86f43d59ca651fec4af5b7b4a87e4b4d5b89b819a3aa69c312b60e	0	0
HybridConnectionManager Service Installation	Roberto Rodriguez (Cyb3rWard0g), OTR (Open Threat Research)	Sigma Integrated Rule Set (GitHub)	517263a8c15fed9ded106be882b2ec39dde9a02250421088d9b2a222e1516406	0	0
HybridConnectionManager Service Installation	Roberto Rodriguez (Cyb3rWard0g), OTR (Open Threat Research)	Sigma Integrated Rule Set (GitHub)	6ba69204045297b2467cffd2d3908dc1588e213dfeaf62bb11c1778c9d93dcf0	0	0
HybridConnectionManager Service Running	Roberto Rodriguez (Cyb3rWard0g), OTR (Open Threat Research)	Sigma Integrated Rule Set (GitHub)	711a6c8a033fd8cc45c82ea8fdd9a7b6f95b70c88e157d2d67579ce7dff11b76	0	0
ISO Image Mount	Syed Hasan (@syedhasan009)	Sigma Integrated Rule Set (GitHub)	e6b3709b80b265ad0fed3cb1ec046dc0b3dfa6eba361f593c53333b71c662136	0	0
IcedID Downloader	Joe Security	Joe Security Rule Set (GitHub)	967066367d1b4b6d60bdc3bb6c06da99df284842490e627971ffc36d72138e44	0	0
Image Load of VSS_PS.dll by Uncommon Executable	Markus Neis, @markus_neis	Sigma Integrated Rule Set (GitHub)	90a2634e64f0a02343bf17b797e3d249061fdee81d36e5dac2d8e3fe2a2df280	0	0
Impacket Lateralization Detection	Ecco, oscd.community, Jonhnathan Ribeiro	Sigma Integrated Rule Set (GitHub)	3d5ac2209c46a9cb869f82a51ef7ec32954bc3ca32fe710929ac41137e9f7957	0	0
Impacket PsExec Execution	Bhabesh Raj	Sigma Integrated Rule Set (GitHub)	3f02ed054f271ff6065ad30572fa0e95c2bd16820da55d1ad40d10e8fafd0eca	0	0
In-memory PowerShell	Tom Kern, oscd.community, Natalia Shornikova, Tim Shelton	Sigma Integrated Rule Set (GitHub)	309cda68f6a1f23a3de3d6604cd71d89098ca2472c6cfaae572a5d4375389247	0	0
Indicator Removal on Host - Clear Mac System Logs	remotephone, oscd.community	Sigma Integrated Rule Set (GitHub)	adfe5f99b6a812a149fe86b53528239d9e7938e56d2864d1403950040a11e57b	0	0
Install Root Certificate	Ömer Günal, oscd.community	Sigma Integrated Rule Set (GitHub)	ec31a3e8dcd4d55b032d9d6697f403b4260762840a75ef84a25fec68f4d78fd6	0	0

InstallerFileTake Over LPE CVE-2021-41379 File Create Event	Florian Roth	Sigma Integrated Rule Set (GitHub)	b0c213591ac3b9d67559c62e06f44e984fa9cccd8eadc7126488916b8f112271	0	0
Interactive Logon to Server Systems	Florian Roth	Sigma Integrated Rule Set (GitHub)	287dcb23b97461c15bc628626d410d7134857f2a8a73b5867709120813e47c17	0	0
Invalid Users Failing To Authenticate From Single Source Using NTLM	Mauricio Velazco	Sigma Integrated Rule Set (GitHub)	bd35715e77f17842c47f4bd45fb125c2aee1c533dadb3de025a01b53ccdc7464	0	0
Invalid Users Failing To Authenticate From Source Using Kerberos	Mauricio Velazco, frack113	Sigma Integrated Rule Set (GitHub)	24e430c06c4928d27c8c23097b69829139af8fce404dbe51f3b1a45cfe4c963d	0	0
Invocation of Active Directory Diagnostic Tool (ntdsutil.exe)	Thomas Patzke	Sigma Integrated Rule Set (GitHub)	84d018445ff2f74f3d42483a4605f7bf5d16da359866d95b1be54371131e5836	0	0
Invoke-Obfuscation CLIP+ Launcher	Jonathan Cheong, oscd.community	Sigma Integrated Rule Set (GitHub)	07b20a8191672f390880af0dfccb1dcb42df51d9b0e0e5b4f4a34ae2636c385a	0	0
Invoke-Obfuscation CLIP+ Launcher	Jonathan Cheong, oscd.community	Sigma Integrated Rule Set (GitHub)	55d070128f8d768c5650c81c573dcfbad37b719f2e5b4c2e508c2a7fde28c9ba	0	0
Invoke-Obfuscation CLIP+ Launcher	Jonathan Cheong, oscd.community	Sigma Integrated Rule Set (GitHub)	61b487de335dac84b1a9bbd3816d5111cabce315463c02cb2953344caca3cd95	0	0
Invoke-Obfuscation CLIP+ Launcher	Jonathan Cheong, oscd.community	Sigma Integrated Rule Set (GitHub)	66ae2d866adeac92a15a12e31d3a3be37036f330111ae0f3fe3b7c895374ede1	0	0
Invoke-Obfuscation CLIP+ Launcher	Jonathan Cheong, oscd.community	Sigma Integrated Rule Set (GitHub)	66f7192930e6691d3b4ee72b4a6351242a104911c34cc2e563539db593bf6bc5	0	0
Invoke-Obfuscation CLIP+ Launcher	Jonathan Cheong, oscd.community	Sigma Integrated Rule Set (GitHub)	96f143150cf12b082ad12ff80043a40ce507e50dbf6f4c6d68fb1f4f0cbe1771	0	0
Invoke-Obfuscation CLIP+ Launcher	Jonathan Cheong, oscd.community	Sigma Integrated Rule Set (GitHub)	a4095d2245c467d53d473d6f0b5664e6043544a19c73bd87d555a5316ada37e7	0	0
Invoke-Obfuscation CLIP+ Launcher	Jonathan Cheong, oscd.community	Sigma Integrated Rule Set (GitHub)	bc4b79447cdefa2382da736b3a63a3ce5a01a6400ed11820db5ee38b981e2e34	0	0
Invoke-Obfuscation CLIP+ Launcher	Jonathan Cheong, oscd.community	Sigma Integrated Rule Set (GitHub)	d9fcc5b01474c94f013105b532ce885ebb7d8cedac210ff18bb921bd350afa1f	0	0
Invoke-Obfuscation CLIP+ Launcher	Jonathan Cheong, oscd.community	Sigma Integrated Rule Set (GitHub)	dd967df044da70a0ce8e3d0766de79d0c1392ca968e6c1f2755dc95b76062a7d	0	0
Invoke-Obfuscation COMPRESS OBFUSCATION	Timur Zinniatullin, oscd.community	Sigma Integrated Rule Set (GitHub)	23d33c003cb0a2893d558ec9fc1f759265b5200122f0155a81fd6da5eda7cb4a	0	0

Invoke-Obfuscation COMPRESS OBFUSCATION	Timur Zinniatullin, oscd.community	Sigma Integrated Rule Set (GitHub)	2abb23702384c2980e4ffe0dd690fcd4ba17539c7c79c6718252778eab17fcc1	0	0
Invoke-Obfuscation COMPRESS OBFUSCATION	Timur Zinniatullin, oscd.community	Sigma Integrated Rule Set (GitHub)	30afe98d3f1fe8511eb6a67ad5f0d954762e3ae473d2c53b390482613c6afe8e	0	0
Invoke-Obfuscation COMPRESS OBFUSCATION	Timur Zinniatullin, oscd.community	Sigma Integrated Rule Set (GitHub)	b5835a1f1f607f7c9b2995761947f379ab9343ac06637ece5caf60435a682e6c	0	0
Invoke-Obfuscation COMPRESS OBFUSCATION	Timur Zinniatullin, oscd.community	Sigma Integrated Rule Set (GitHub)	bf865a7d8524d34ec2fcf366103b431319a364992070da49982bf7a6bf68fcd2	0	0
Invoke-Obfuscation COMPRESS OBFUSCATION	Timur Zinniatullin, oscd.community	Sigma Integrated Rule Set (GitHub)	dc78b6b33628aead1fdeb14c4a18756a01373ea62b8d5462c0c12f0dc5dc8be0	0	0
Invoke-Obfuscation COMPRESS OBFUSCATION	Timur Zinniatullin, oscd.community	Sigma Integrated Rule Set (GitHub)	eacdd56ee69da6ba92a6f01f7d2cb4022f9ffb08eebd0a09a1e17012fc9f3307	0	0
Invoke-Obfuscation COMPRESS OBFUSCATION	Timur Zinniatullin, oscd.community	Sigma Integrated Rule Set (GitHub)	f39f375a39ff602aaeb463af7e29f879cf1e2728e1bfd0ce46c68ce463d545c9	0	0
Invoke-Obfuscation Obfuscated IEX Invocation	Daniel Bohannon (@Mandiant/@FireEye), oscd.community	Sigma Integrated Rule Set (GitHub)	02563551ca2b811c4f5ebea13242cffde0a8e5d1dbe9578a4e836117c3344457	0	0
Invoke-Obfuscation Obfuscated IEX Invocation	Daniel Bohannon (@Mandiant/@FireEye), oscd.community	Sigma Integrated Rule Set (GitHub)	229bed31b945cf52d288e09e87afafe82ddc418cc89ac78e4aa57bb1505f4e17	0	0
Invoke-Obfuscation Obfuscated IEX Invocation	Daniel Bohannon (@Mandiant/@FireEye), oscd.community	Sigma Integrated Rule Set (GitHub)	532d5adca424a8a32820d44f658dea5035219510229a38ea885eea469ae8f8a7	0	0
Invoke-Obfuscation Obfuscated IEX Invocation	Daniel Bohannon (@Mandiant/@FireEye), oscd.community	Sigma Integrated Rule Set (GitHub)	6e2b0909c3266faf43a0917df01825825b4ad958d6cdaa0a45c9cfe53e15affa	0	0
Invoke-Obfuscation Obfuscated IEX Invocation	Daniel Bohannon (@Mandiant/@FireEye), oscd.community	Sigma Integrated Rule Set (GitHub)	6e503c48dbf119e0821aab4c7ebde353e0b781363fe0c88ac53e10fabedeeb33	0	0
Invoke-Obfuscation Obfuscated IEX Invocation	Daniel Bohannon (@Mandiant/@FireEye), oscd.community	Sigma Integrated Rule Set (GitHub)	778d34341a09f9942b6754b257881e32f43e5eb36c396c5a7bf385626994b6a3	0	0
Invoke-Obfuscation Obfuscated IEX Invocation	Daniel Bohannon (@Mandiant/@FireEye), oscd.community	Sigma Integrated Rule Set (GitHub)	7c97dec04489c3636dd72432f11eeb579854a1d03d55419bafb059e73e43dd4c	0	0

Invoke-Obfuscation Obfuscated IEX Invocation	Daniel Bohannon (@Mandiant/@FireEye), oscd.community	Sigma Integrated Rule Set (GitHub)	89b3cbec0ebda2750669f9b5831ae50fb9a2e58ba9d9ecb76d82c553dd9fbaed	0	0
Invoke-Obfuscation Obfuscated IEX Invocation	Daniel Bohannon (@Mandiant/@FireEye), oscd.community	Sigma Integrated Rule Set (GitHub)	978e8ef0c97aa415779127f1b750df3d71553c0ed2f593b7499f7213094b8a22	0	0
Invoke-Obfuscation RUNDLL LAUNCHER	Timur Zinniatullin, oscd.community	Sigma Integrated Rule Set (GitHub)	013f9f3361dd5e5e166cef93640767e854c135731f7b10a6e86a582e2a3da454	0	0
Invoke-Obfuscation RUNDLL LAUNCHER	Timur Zinniatullin, oscd.community	Sigma Integrated Rule Set (GitHub)	15e77f32f6ce577059ce2a023014f97f6166500fe342a790642abbb2d7524dd1	0	0
Invoke-Obfuscation RUNDLL LAUNCHER	Timur Zinniatullin, oscd.community	Sigma Integrated Rule Set (GitHub)	36d028c2bbec04da64cd22e6d7ade29f0485073c4f2a33748b660bc41add11c5	0	0
Invoke-Obfuscation RUNDLL LAUNCHER	Timur Zinniatullin, oscd.community	Sigma Integrated Rule Set (GitHub)	5092dd88f643768409b7b033996ae9886f7916c352f876f58742e741c818de58	0	0
Invoke-Obfuscation RUNDLL LAUNCHER	Timur Zinniatullin, oscd.community	Sigma Integrated Rule Set (GitHub)	513a8ffd6dffc7c0f80d19848150c2e0de524c7115a18106ba96a0d789b07e1e	0	0
Invoke-Obfuscation RUNDLL LAUNCHER	Timur Zinniatullin, oscd.community	Sigma Integrated Rule Set (GitHub)	669e0fa4f936ba08d94a0d94b4ff0a17a257f5b85f14a70e608f1804ef1226ef	0	0
Invoke-Obfuscation RUNDLL LAUNCHER	Timur Zinniatullin, oscd.community	Sigma Integrated Rule Set (GitHub)	7943e73e12090a40bcc5a95e498a4655704cd76a8f1cc15acfef595e7f85a442	0	0
Invoke-Obfuscation RUNDLL LAUNCHER	Timur Zinniatullin, oscd.community	Sigma Integrated Rule Set (GitHub)	b81cfe0479a3286d77237d8297165880ec1fbe3652ad795ceb1abaa1eccb8d0f	0	0
Invoke-Obfuscation RUNDLL LAUNCHER	Timur Zinniatullin, oscd.community	Sigma Integrated Rule Set (GitHub)	d304bf8af334b938ef27fc29de6beeba9510de9abd801458029e2aad0a96a430	0	0
Invoke-Obfuscation RUNDLL LAUNCHER	Timur Zinniatullin, oscd.community	Sigma Integrated Rule Set (GitHub)	f4b87782d8c00059afd020eed2b619da907273f77ea5c3ba678a81e4a369045e	0	0
Invoke-Obfuscation STDIN+ Launcher	Jonathan Cheong, oscd.community	Sigma Integrated Rule Set (GitHub)	21fb91a013d99fcb0a512f126e1db671d61521863baf20148369276f4ce90a79	0	0
Invoke-Obfuscation STDIN+ Launcher	Jonathan Cheong, oscd.community	Sigma Integrated Rule Set (GitHub)	33f26be0d86ded162f5f9983f8ccec7e33739e7d61ce1550a476f8d6d9fb1585	0	0

Invoke-Obfuscation STDIN+ Launcher	Jonathan Cheong, oscd.community	Sigma Integrated Rule Set (GitHub)	3c63fdf3c3489825803565ebef9d7aa5574b069b7df909431ca0cd9bbfff1014	0	0
Invoke-Obfuscation STDIN+ Launcher	Jonathan Cheong, oscd.community	Sigma Integrated Rule Set (GitHub)	5a405d8959e0dbe9e8c85da1ee53bb94a514c82a1c85543bcde6cdb5fa6c8d81	0	0
Invoke-Obfuscation STDIN+ Launcher	Jonathan Cheong, oscd.community	Sigma Integrated Rule Set (GitHub)	7c91efe9f8bcf7588b12461abfce94d9de990787f00ec01fdc0378b6d0ea5f7f	0	0
Invoke-Obfuscation STDIN+ Launcher	Jonathan Cheong, oscd.community	Sigma Integrated Rule Set (GitHub)	8bc4688c4e1827de8ac2769dd693f5ee1d6a3dd731e0fa459a1d47788bc3ab77	0	0
Invoke-Obfuscation STDIN+ Launcher	Jonathan Cheong, oscd.community	Sigma Integrated Rule Set (GitHub)	a48b077866cf1527dd61081ba5998bcaeba2f75f76f2b644f786592b048ccc42	0	0
Invoke-Obfuscation STDIN+ Launcher	Jonathan Cheong, oscd.community	Sigma Integrated Rule Set (GitHub)	e65f5089591863acc7d1b0724c258c83ed40c7f2ef5a4d11da364c316768c806	0	0
Invoke-Obfuscation STDIN+ Launcher	Jonathan Cheong, oscd.community	Sigma Integrated Rule Set (GitHub)	f46e368df2720b7c679c6d8a7af787029a555248b2a687d244934f424619531f	0	0
Invoke-Obfuscation VAR+ Launcher	Jonathan Cheong, oscd.community	Sigma Integrated Rule Set (GitHub)	37472617d726e65dc836731e68fa4b615e3453db5924b2ed694f6d42f3fa2e7c	0	0
Invoke-Obfuscation VAR+ Launcher	Jonathan Cheong, oscd.community	Sigma Integrated Rule Set (GitHub)	46f308942e8413fc74d14eb28362c26efc33f463b1d70394188e9cc50989434c	0	0
Invoke-Obfuscation VAR+ Launcher	Jonathan Cheong, oscd.community	Sigma Integrated Rule Set (GitHub)	785b999a59eeb49c52b8de6db77180b2f32a1c32f55c5a66124df629511ee71e	0	0
Invoke-Obfuscation VAR+ Launcher	Jonathan Cheong, oscd.community	Sigma Integrated Rule Set (GitHub)	85c1b5321d15597e6d632e33d628537f69719336ffcaf3486716d44dc6a94690	0	0
Invoke-Obfuscation VAR+ Launcher	Jonathan Cheong, oscd.community	Sigma Integrated Rule Set (GitHub)	9e447b626bcce83fc27a2087f918f28e255669c87d60b118fea3f35a6276ace9	0	0
Invoke-Obfuscation VAR+ Launcher	Jonathan Cheong, oscd.community	Sigma Integrated Rule Set (GitHub)	9fac765a1fc90df763e78970562f2ec88d72f5a1b755dc6922c9df6f6b3283a3	0	0
Invoke-Obfuscation VAR+ Launcher	Jonathan Cheong, oscd.community	Sigma Integrated Rule Set (GitHub)	cf80a5797b65d0aae908c9fb7bdd2ffdf5cdbace0b8e61a02320a61266fddbce	0	0
Invoke-Obfuscation VAR+ Launcher	Jonathan Cheong, oscd.community	Sigma Integrated Rule Set (GitHub)	d5a5398fc7d4724a6543cb1b92710954d8f52105738cb1bd31d2db507b433082	0	0
Invoke-Obfuscation VAR+ Launcher	Jonathan Cheong, oscd.community	Sigma Integrated Rule Set (GitHub)	dbba719e722ed35e6290aec93e2c9879ef0eb3966254ad9f15c73b24f11ccf9e	0	0

Invoke-Obfuscation VAR+ Launcher	Jonathan Cheong, oscd.community	Sigma Integrated Rule Set (GitHub)	f0ed779291914bc6744829d783902b1aa18afca33fcdce512a6e6dcec594b8fe	0	0
Invoke-Obfuscation VAR++ LAUNCHER OBFUSCATION	Timur Zinniatullin, oscd.community	Sigma Integrated Rule Set (GitHub)	23598265f485b73118223796eab6ef3d4710b6c7855ae76fe8ef5e3156537361	0	0
Invoke-Obfuscation VAR++ LAUNCHER OBFUSCATION	Timur Zinniatullin, oscd.community	Sigma Integrated Rule Set (GitHub)	3481fdd9c7d7aa343ba20022ceec206525f19fda50c317ba5e59f6996102f4ce	0	0
Invoke-Obfuscation VAR++ LAUNCHER OBFUSCATION	Timur Zinniatullin, oscd.community	Sigma Integrated Rule Set (GitHub)	43fda3b4b26f2d722e172affac6a534e640b6f690827cb80f27eae7bf1121924	0	0
Invoke-Obfuscation VAR++ LAUNCHER OBFUSCATION	Timur Zinniatullin, oscd.community	Sigma Integrated Rule Set (GitHub)	56d1f6c5dcbbe1fd4ecdb87028f432b123ac0cf5fe37a336f0ed6c34521f370a	0	0
Invoke-Obfuscation VAR++ LAUNCHER OBFUSCATION	Timur Zinniatullin, oscd.community	Sigma Integrated Rule Set (GitHub)	9b7f8d96a709f458ef164dd0c2b1c0bd21506b6a9292710e95e822b262716fc0	0	0
Invoke-Obfuscation VAR++ LAUNCHER OBFUSCATION	Timur Zinniatullin, oscd.community	Sigma Integrated Rule Set (GitHub)	ac263989614ade79cd7024eb73729ba0d899416a4618b2b37f9fe886b6ae1ea6	0	0
Invoke-Obfuscation VAR++ LAUNCHER OBFUSCATION	Timur Zinniatullin, oscd.community	Sigma Integrated Rule Set (GitHub)	b85a3806145ca2440f6e4328faea04b4694be6c4dfad9550ca882b91babed162	0	0
Invoke-Obfuscation VAR++ LAUNCHER OBFUSCATION	Timur Zinniatullin, oscd.community	Sigma Integrated Rule Set (GitHub)	b95438303858dee4a1b7686bca97ba3c32d14bde4bccb73cd0cce0decef9cb1c	0	0
Invoke-Obfuscation VAR++ LAUNCHER OBFUSCATION	Timur Zinniatullin, oscd.community	Sigma Integrated Rule Set (GitHub)	f80b47791783e7ca801863d05a76bb83fb2ae70b2dc9d18a13fd9db9172baf46	0	0
Invoke-Obfuscation VAR++ LAUNCHER OBFUSCATION	Timur Zinniatullin, oscd.community	Sigma Integrated Rule Set (GitHub)	ff49fb699dd54313f9d61a9bba7e0c0021f31cf6bbad67452754dffe5f1a87f2	0	0
Invoke-Obfuscation Via Stdin	Nikita Nazarov, oscd.community	Sigma Integrated Rule Set (GitHub)	171e9c19da7073d50de0611f10f7fe49f18e33f0eb2271f1451e3122dd70da39	0	0

Invoke-Obfuscation Via Stdin	Nikita Nazarov, oscd.community	Sigma Integrated Rule Set (GitHub)	4c4b43817f5f5dcaf3aadb0e508301e535f4809ca042fa2cec1ae56068e38683	0	0
Invoke-Obfuscation Via Stdin	Nikita Nazarov, oscd.community	Sigma Integrated Rule Set (GitHub)	5a9474f49eedd6f514e9f05bd95d3fde3747f03da5803a359962b76fe04d3dc0	0	0
Invoke-Obfuscation Via Stdin	Nikita Nazarov, oscd.community	Sigma Integrated Rule Set (GitHub)	b3a5bd1f34b26d6c54d45604acabcec5814c2c266d0ab0547c722d22583b78e8	0	0
Invoke-Obfuscation Via Stdin	Nikita Nazarov, oscd.community	Sigma Integrated Rule Set (GitHub)	bba8cd2d0e60c82277d0117e4841b13ee087cacccbf6b9bdd7d3c83f0375582a	0	0
Invoke-Obfuscation Via Stdin	Nikita Nazarov, oscd.community	Sigma Integrated Rule Set (GitHub)	ca82d3c569666b788bdb9b704468045f733d45dac72cb22f0dc35242d6dd30ce	0	0
Invoke-Obfuscation Via Stdin	Nikita Nazarov, oscd.community	Sigma Integrated Rule Set (GitHub)	d9663bea4419d4e77af5748add1d59d90a3c136f0100ad05f55199c8b38636f0	0	0
Invoke-Obfuscation Via Stdin	Nikita Nazarov, oscd.community	Sigma Integrated Rule Set (GitHub)	e6338468914bbd534177587d16fde9881596bc9d1ac95c3a142e76a6d587e32c	0	0
Invoke-Obfuscation Via Stdin	Nikita Nazarov, oscd.community	Sigma Integrated Rule Set (GitHub)	ea2300c5e8a8dfac7a21e289614c34963c361bffda74ba0ddba16af4c009a74c	0	0
Invoke-Obfuscation Via Use Clip	Nikita Nazarov, oscd.community	Sigma Integrated Rule Set (GitHub)	0d70c217e51ad45cc6411546634b710d8a2bd8d7fe04cea155aa5a5274d4b8c1	0	0
Invoke-Obfuscation Via Use Clip	Nikita Nazarov, oscd.community	Sigma Integrated Rule Set (GitHub)	52417f5a914da422b1f4a12eae2a1fd94408538cc4aa1373f9a527d748628701	0	0
Invoke-Obfuscation Via Use Clip	Nikita Nazarov, oscd.community	Sigma Integrated Rule Set (GitHub)	62ac6078947c91fe388df8ac3354f7d5cab59710aa0d057148b72b409203a565	0	0
Invoke-Obfuscation Via Use Clip	Nikita Nazarov, oscd.community	Sigma Integrated Rule Set (GitHub)	76af6c7b5bbcbcbccfb2ea260489d66ab26fb91c612afce2eea8b5538bb36c35	0	0
Invoke-Obfuscation Via Use Clip	Nikita Nazarov, oscd.community	Sigma Integrated Rule Set (GitHub)	ce17aada5a7768055bbf5a416696626ce2063fc2947da124934a97f0ff076ba6	0	0
Invoke-Obfuscation Via Use Clip	Nikita Nazarov, oscd.community	Sigma Integrated Rule Set (GitHub)	f7ed971f190a397799a0730d5ae3ae4a8795ea76e42554768900a03c1bbf7ad2	0	0
Invoke-Obfuscation Via Use Clip	Nikita Nazarov, oscd.community	Sigma Integrated Rule Set (GitHub)	f8caa5c28a6fabe724cbb68e6a4175a973edeb9f4a0caf001cd768f207c2da3c	0	0
Invoke-Obfuscation Via Use Clip	Nikita Nazarov, oscd.community	Sigma Integrated Rule Set (GitHub)	ff8bf7ea172d6967d31c7cd3833e156278c00c013da4bed9d4b45159acd507cb	0	0
Invoke-Obfuscation Via Use MSHTA	Nikita Nazarov, oscd.community	Sigma Integrated Rule Set (GitHub)	0930a93e61dc6ca5c708a09f8f1a8c0dc24b8d942a8e8900144c6dee8703e343	0	0
Invoke-Obfuscation Via Use MSHTA	Nikita Nazarov, oscd.community	Sigma Integrated Rule Set (GitHub)	0e5566fb9e5f855f277b707f52ff16085f2976cb6768b08e3151b738f7cc6992	0	0

Invoke-Obfuscation Via Use MSHTA	Nikita Nazarov, oscd.community	Sigma Integrated Rule Set (GitHub)	2f4d7a7bc3e29eaeac5423c4d276d9a90586e6c3d4277f4d264c9d8aa54f6ec3	0	0
Invoke-Obfuscation Via Use MSHTA	Nikita Nazarov, oscd.community	Sigma Integrated Rule Set (GitHub)	437698a3ddc141ac75cb061590808bbcb7de0b4fb7ebaf60345f0549f4cc9816	0	0
Invoke-Obfuscation Via Use MSHTA	Nikita Nazarov, oscd.community	Sigma Integrated Rule Set (GitHub)	43cbdd33506d9ffaa0d9a81b702937c5941031eccf02bfa20564b42417d9ff47	0	0
Invoke-Obfuscation Via Use MSHTA	Nikita Nazarov, oscd.community	Sigma Integrated Rule Set (GitHub)	9e9633eb15bfbbe3ed0b8c01989e6bb38f91bdcfe4de5867c801ab39f781cce6	0	0
Invoke-Obfuscation Via Use MSHTA	Nikita Nazarov, oscd.community	Sigma Integrated Rule Set (GitHub)	a5d8322f8fd4a171b92a497efdb17590b3b6b58818835a034997d21e4270b693	0	0
Invoke-Obfuscation Via Use MSHTA	Nikita Nazarov, oscd.community	Sigma Integrated Rule Set (GitHub)	aa4d39be626c3fd4a68412b1a7760b0957c0c5b86f79eb893d14f58e7fce6c6d	0	0
Invoke-Obfuscation Via Use MSHTA	Nikita Nazarov, oscd.community	Sigma Integrated Rule Set (GitHub)	d851e8933dce5155d4504668c3fad20bca16e503e478165aad802dc4e5634563	0	0
Invoke-Obfuscation Via Use MSHTA	Nikita Nazarov, oscd.community	Sigma Integrated Rule Set (GitHub)	fa1bd4dbff85b70daad8ab600a4cfee9488c2ff0188d3cea00e84d7b073405ea	0	0
Invoke-Obfuscation Via Use Rundll32	Nikita Nazarov, oscd.community	Sigma Integrated Rule Set (GitHub)	2f55b73ec314c7381dc97abaeb5ef1469713fc1c552265bc1225b96c6ad6cc83	0	0
Invoke-Obfuscation Via Use Rundll32	Nikita Nazarov, oscd.community	Sigma Integrated Rule Set (GitHub)	4131754f7c0e71d23eac2114f63c2445f3ea1e8f38df8a76563917e98baf7123	0	0
Invoke-Obfuscation Via Use Rundll32	Nikita Nazarov, oscd.community	Sigma Integrated Rule Set (GitHub)	7d11bdaa4f671e75a6cf0ddb788f3ea6ff550f3371c61cb0a29f802ef5ac61d0	0	0
Invoke-Obfuscation Via Use Rundll32	Nikita Nazarov, oscd.community	Sigma Integrated Rule Set (GitHub)	93a7143b3c3623e84f71a4ba7087c95eadd288a96cc5205d70645fb23d9fd956	0	0
Invoke-Obfuscation Via Use Rundll32	Nikita Nazarov, oscd.community	Sigma Integrated Rule Set (GitHub)	a7908e5cb15379fd8bcf3a9689d34ff1a5a72ab4c6ca6d6c65e24d53ffbb2c13	0	0
Invoke-Obfuscation Via Use Rundll32	Nikita Nazarov, oscd.community	Sigma Integrated Rule Set (GitHub)	c7fc78f9f9afd5b257d906bddd5224d85c22d33c73eb36c94c9ee19f427defb0	0	0
Invoke-Obfuscation Via Use Rundll32	Nikita Nazarov, oscd.community	Sigma Integrated Rule Set (GitHub)	dc490d5d39ceac22ac7a184263ef179d60d4acaa65976183ddf786bd75366d9f	0	0
Invoke-Obfuscation Via Use Rundll32	Nikita Nazarov, oscd.community	Sigma Integrated Rule Set (GitHub)	f78da06c94256bbc6f7356a3883982528e6282d615f1a6c25c43ddaad4687c18	0	0
Invoke-Obfuscation Via Use Rundll32	Nikita Nazarov, oscd.community	Sigma Integrated Rule Set (GitHub)	fc25895e0aab53d526b1f268874e1f81955fb22d2d310fc8a14e2f4cc28a52b4	0	0
Invoke-Obfuscation Via Use Rundll32	Nikita Nazarov, oscd.community	Sigma Integrated Rule Set (GitHub)	fe3560ed4bbd6192e8416571fbbe1e5fe61a8b92201d44f818823f75e7f8578e	0	0

JNDIExploit Pattern	Florian Roth	Sigma Integrated Rule Set (GitHub)	67e1bb7efdc9f72507d792fffd9669f000bac02c81b6c5880693f3e473360550	0	0
JSOutProx RAT (Sysmon detection)	Ariel Millahuel	SOC Prime Threat Detection Marketplace	02be37dad81df3baa83c02c795e51416bda450b6272fe9585a50171a69535256	0	0
Jacksbot (Registry event and CommandLine parameters)	Ariel Millahuel	SOC Prime Threat Detection Marketplace	de380d617af0b2dd78f410efa4fc36f895a556759177b34f04dad90698a9b833	0	0
Jacksbot (Registry event and CommandLine parameters)	Ariel Millahuel	SOC Prime Threat Detection Marketplace	eed56e9a26e865b9accdc5a4ef7e681ca4b83deb2c6f21a65d28cac9e28547f1	0	0
Java Class Proxy Download	Andreas Hunkeler (@Karneades)	Sigma Integrated Rule Set (GitHub)	b86f637637bb79d44a1590bf2bb4feadebbd6c2757ea9c0016f1a9595504b17d	0	0
JexBoss Command Sequence	Florian Roth	Sigma Integrated Rule Set (GitHub)	a3bdc4cfa6129ab202d0c31fd0a1b62c238614b1ef2d063913d6414edf0845b7	0	0
Judgement Panda Credential Access Activity	Florian Roth	Sigma Integrated Rule Set (GitHub)	d891d43fe1fffa5c84fc567a5eaff4bcf0c35cfcfdaeda3284ed6d5becfcfe90	0	0
Judgement Panda Exfil Activity	Florian Roth	Sigma Integrated Rule Set (GitHub)	79e0e41a4f427cdb7337c02f6d2bf2f18272a145bf619561b749dc623133dc88	0	0
KONNI Malware behavior (APT37)	Ariel Millahuel	SOC Prime Threat Detection Marketplace	7f8871e9eb7dd4fee1e3a813c111693a960996e217fa6df263e3f2c45aa76a90	0	0
KONNI Malware behavior (APT37)	Ariel Millahuel	SOC Prime Threat Detection Marketplace	dac73d2c69f90d09101600bec5114075b4bfc85ce4fd276570acd4b4b4002ac3	0	0
Ke3chang Registry Key Modifications	Markus Neis, Swisscom	Sigma Integrated Rule Set (GitHub)	189d7c7c265aa63d59bd8d89a83cf406231c66f42999d77ba7e92640c28bc2e1	0	0
Kerberos Manipulation	Florian Roth	Sigma Integrated Rule Set (GitHub)	231c4645e3a84818601e73156d0ec49d61870632b546fe129f75f9795fa95b1a	0	0
Kerberos Network Traffic RC4 Ticket Encryption	sigma	Sigma Integrated Rule Set (GitHub)	78b71e2b045b325f1db537748abc852151228024bbcd946684eb402afddd7b1a	0	0
Koadic post exploitation rootkit	Joe Security	Joe Security Rule Set (GitHub)	6cfb40f83f69b8f6221133239461ee688e15ec2c65581eb5b5674a17e24831a1	0	0
Kwapirs Trojan Detection	Ariel Millahuel	SOC Prime Threat Detection Marketplace	5c5eb2e19924ab6d6c54d36e0730e90e8dfea2ee983a708a1ecf6a596cd7bd9c	0	0

Kwapirs Trojan Detection	Ariel Millahuel	SOC Prime Threat Detection Marketplace	96ca7fcb576c97b0d5789bb1536ba5039c9decf46b748ed501cc0945e90fb25e	0	0
LDAP Reconnaissance / Active Directory Enumeration	Adeem Mawani	Sigma Integrated Rule Set (GitHub)	afe088ee5f69ba6fb59e2c89d995b9a77ed2636f341d9222a077422e7ccb35d8	0	0
LNK File Download or Usage over HTTP	SOC Prime Team	SOC Prime Threat Detection Marketplace	ffd8e0662e18d53ff9cd24c140aa76098f09521d84cc29f2f00a17fa50a43e37	0	0
LNK File Download or Usage over SMB (Overview Query)	SOC Prime Team	SOC Prime Threat Detection Marketplace	a4d2269d88c903801fac5733945f9e7aa870b2b167f014df865f794d517e8907	0	0
LOLBAS Data Exfiltration by DataSvcUtil.exe	Ialle Teixeira @teixeira0xfffff, Austin Songer @austinsonger	Sigma Integrated Rule Set (GitHub)	4ca63f832211aa3558085e05e1123658cee6f4d5daa8c91fc9deeb13b8ab7b5a	0	0
LPE InstallerFileTake Over PoC CVE-2021-41379	Florian Roth	Sigma Integrated Rule Set (GitHub)	5aac8fe297cc2a7fde7dd8b7e3bc82990cbcba14f3acb11dfcd8306587c8b02d	0	0
LSASS Access Detected via Attack Surface Reduction	Markus Neis	Sigma Integrated Rule Set (GitHub)	563af56cc44b5473ca2297f9917233ed8264136d5730aed0bf08f98e4294e060	0	0
LSASS Access from Non System Account	Roberto Rodriguez @Cyb3rWard0g	Sigma Integrated Rule Set (GitHub)	c6493cb4442f7c6d607b594653ad5f32371b52193211d685ce4fa631017ee7cf	0	0
LSASS Access from Program in Suspicious Folder	Florian Roth	Sigma Integrated Rule Set (GitHub)	df0d05c25b308b1067253d6665734b787aee2e0d8b177c08f0fad5c83a9b598c	0	0
LSASS Memory Dump	Samir Bousseaden	Sigma Integrated Rule Set (GitHub)	63d1c446465d6c6205e2452b5fca8715042ebcc9bfa04624288ce34d07cfa028	0	0
Lateral Movement Indicator ConDrv	Janantha Marasinghe	Sigma Integrated Rule Set (GitHub)	c978aa658df36ee024186bee37eb8f5b1974ccfe8ded97a973bfe4dc6e197008	0	0
Lazarus Activity	Florian Roth	Sigma Integrated Rule Set (GitHub)	5239809b3d434a5fd867601486ba71288898a2f7c5d6c4370e4afdf12c7283c	0	0
Leviathan Registry Key Activity	Aidan Bracher	Sigma Integrated Rule Set (GitHub)	8d554899340394 27d1fae624f0b85085985ab01440f56559b26c68f7a6a1deb4	0	0
Linux Capabilities Discovery	Pawel Mazur	Sigma Integrated Rule Set (GitHub)	15f5291aefe8242b4be1908368af4c1c020bff933d962fa5c3d2690592a1d9db	0	0
Linux Crypto Mining Indicators	Florian Roth	Sigma Integrated Rule Set (GitHub)	a54f90d76f6357c3494a27966d9ddc15850d9dd07fd3848ac2a031ac149bec1a	0	0

Linux Crypto Mining Pool Connections	Florian Roth	Sigma Integrated Rule Set (GitHub)	94ce005adcd09f3ebc9f1adf5dfb87bc39cf45a1c8e1176675682711a53d88f5	0	0
Linux Network Service Scanning	Alejandro Ortuno, oscd.community	Sigma Integrated Rule Set (GitHub)	577e8f6fda6da02c80afa50ddf199a9e2817ae570e37dff3c743910d6e4dd273	0	0
Linux Network Service Scanning	Alejandro Ortuno, oscd.community	Sigma Integrated Rule Set (GitHub)	676feba35f86e9e41213bf2cd1daab4e4ad9143714e10f335981beeb7ba5d4a5	0	0
Linux Network Service Scanning	Alejandro Ortuno, oscd.community	Sigma Integrated Rule Set (GitHub)	7f6a694ee18581a5a2bb34e78f7cb079d0e12a465aa6639e291e138f6f308d27	0	0
Linux Network Service Scanning	Alejandro Ortuno, oscd.community	Sigma Integrated Rule Set (GitHub)	96c79bd2f46a79e85a3f40f6206e96a7cc2f097ac4d2dd574d735dccec840832	0	0
Linux Network Service Scanning	Alejandro Ortuno, oscd.community	Sigma Integrated Rule Set (GitHub)	e34284bbb0ad4c302ba9dd1fde4f2de41f24db62c0b7bbd57804d77d81b02119	0	0
Linux Remote System Discovery	Alejandro Ortuno, oscd.community	Sigma Integrated Rule Set (GitHub)	b76b38e7cf87e1b2f37b568047e66cfd972f62fbfdebc15ecff4adb21293b524	0	0
Linux Reverse Shell Indicator	Florian Roth	Sigma Integrated Rule Set (GitHub)	9627ed9b9dde6f0e9ce83624eb258b8c304ba56da7d651985c1e06a0ed0b4975	0	0
Linux Webshell Indicators	Florian Roth	Sigma Integrated Rule Set (GitHub)	f1ddd314aee4681dd4bc1821da4b796ecf94c8b1576209bb191b5a8dbdcdb26a	0	0
Liphyra Botnet	Ariel Millahuel	SOC Prime Threat Detection Marketplace	4596c900255dd64bed15c00f02fd2c020992da25e6600d3536b6b12b8992d409	0	0
Liphyra Botnet	Ariel Millahuel	SOC Prime Threat Detection Marketplace	98cabebe7a41e8259d15db20be2beb491b39babbd9a772c20ccf447f7a5c5490	0	0
LittleCorporal Generated Maldoc Injection	Christian Burkard	Sigma Integrated Rule Set (GitHub)	f10b695dfd304615f49826a39fd11fb539271f8272a9a80be8f070a758f8f025	0	0
Live Memory Dump Using Powershell	Max Altgelt	Sigma Integrated Rule Set (GitHub)	843f3a30bd6700683442b21bbfb20c59afbc32cc978b84e9b713a85d39d8cc90	0	0
Load Undocumented Autoelevated COM Interface	oscd.community, Dmitry Uchakin	Sigma Integrated Rule Set (GitHub)	87990351a4e0cbfe8406a67a021f9d9da456c915388fde098e654a87ba123617	0	0
Load of dbghelp/dbgcore DLL from Suspicious Process	Perez Diego (@darkquassar), oscd.community, Ecco	Sigma Integrated Rule Set (GitHub)	31e54e59e39fda87af874302c79fe8910fcd407edfed11f536cb042394e49c09	0	0
Loading of Kernel Module via Insmod	Pawel Mazur	Sigma Integrated Rule Set (GitHub)	e690fd8425bfb6339396e2e0b658a06d8dad95357a25603d9ed007d8acae6e6b	0	0

Local Groups Discovery	Ömer Günal, Alejandro Ortuno, oscd.community	Sigma Integrated Rule Set (GitHub)	0b93262008400f8b22d04eac398727ff17377f8b7f399741a879ed674b5940f3	0	0
Local Groups Discovery	Ömer Günal, Alejandro Ortuno, oscd.community	Sigma Integrated Rule Set (GitHub)	96830978814aeec9f41351cd26d413ad426a28c3bf7d6f3630ee7e9a578659b9	0	0
Local System Accounts Discovery	Alejandro Ortuno, oscd.community	Sigma Integrated Rule Set (GitHub)	db147f594af74bbd5641cf034cfa4ce699110ac6712abb1062141aefe2d13704	0	0
Local System Accounts Discovery	Alejandro Ortuno, oscd.community	Sigma Integrated Rule Set (GitHub)	e73eb94c02ee03d3d629b3d54b02d2cf6c9b1dab8a7831ba27d8da0c88755c94	0	0
Locked Workstation	Alexandr Yampolskyi, SOC Prime	Sigma Integrated Rule Set (GitHub)	b1f5ca9566ca9b549b32bfe57eee2e7ec1ae42a47aeba5cdf24c69c64e35dd5f	0	0
Loda RAT detection	Ariel Millahuel	SOC Prime Threat Detection Marketplace	53e145805bb5e6301f081883d8d97fc2ebfa40287aec49d411fbba030d1fa39c	0	0
Log4j RCE CVE-2021-44228 Generic	Florian Roth	Sigma Integrated Rule Set (GitHub)	8c495666d5450c3e2e0bb34d2cf7eef172c34ec61b80fb24f7ee56955d98c3cd	0	0
Log4j RCE CVE-2021-44228 in Fields	Florian Roth	Sigma Integrated Rule Set (GitHub)	a089911dd0c5c3ead7a5b984c73e7ff29d2a74b294849fe17ffc932bf33784e9	0	0
Logging Configuration Changes on Linux Host	Mikhail Larin, oscd.community	Sigma Integrated Rule Set (GitHub)	445f9624d922b1b8b49be62aa6ab367c68746e2b43bdbb4e2e6c630e88e18678	0	0
Login to Disabled Account	AlertIQ	Sigma Integrated Rule Set (GitHub)	1514d5d526c9b5a1a6c5e315c592705ba8e80d9698d2928aed28182666d2a2e3	0	0
Login with WMI	Thomas Patzke	Sigma Integrated Rule Set (GitHub)	19ef4372b7c2775276ff1cd9b0da8737a7f6e8739d252d7f90e3f3ba296d1c78	0	0
Logon Scripts (UserInitMprLogonScript)	Tom Ueltschi (@c_APT_ure)	Sigma Integrated Rule Set (GitHub)	4e10510e7f7c48be7d293bdd42d3c63dbb1c4ef878bb17ff20069102a6a1a6b1	0	0
Logon from a Risky IP Address	Austin Songer @austinsonger	Sigma Integrated Rule Set (GitHub)	96e45b283c76172a1e89d9798c6e7952bf70ba4017864f8b0941dbffd56f7055	0	0
LokiBot Trojan behavior (Sysmon).	Alexandr Yampolskyi, SOC Prime	SOC Prime Threat Detection Marketplace	25b0a9aa21e02bf2b942c3a842e1cee818237b7da5e121b08157b081a775e7dd	0	0
Lolbins Process Creation with WmiPrvse	Vadim Khrykov (ThreatIntel), Cyb3rEng (Rule)	Sigma Integrated Rule Set (GitHub)	eb1dbd652c505f66652af5683ecfecaacb1483523b07254e9d1eaee151af6ec9	0	0
Lsass Memory Dump via Comsvcs DLL	Roberto Rodriguez (Cyb3rWard0g), OTR (Open Threat Research)	Sigma Integrated Rule Set (GitHub)	3c0e931ed838b9556e57c7385ca8aa0e20d9e4a2256e761c1f13540f3df2f513	0	0
Lucifer Botnet Detection (Mimikatz Abuse)	Ariel Millahuel	SOC Prime Threat Detection Marketplace	b78dfe3c36a3641e35470c0d66caaab300392d55f5c4664b7541ee0d13af1e9f	0	0

MITRE BZAR Indicators for Execution	@neu5ron, SOC Prime	Sigma Integrated Rule Set (GitHub)	92c43f07a2d15dc0d84c316204afa24eb03535cb3460b7183fae873f9f93601e	0	0
MITRE BZAR Indicators for Persistence	@neu5ron, SOC Prime	Sigma Integrated Rule Set (GitHub)	41587ecc9bb28242c77b042aa99238dbce0be3451506ce1deaa512acac0d4481	0	0
MSBuild Launched By Scr	Joe Security	Joe Security Rule Set (GitHub)	8ad7367c9de9a165016d9a8b662d34004cffb1cf0000aa760ebe1742b6a83175	0	0
MSExchange Transport Agent Installation	Tobias Michalski	Sigma Integrated Rule Set (GitHub)	711b03ff1593b84b2c430081585f67ac7553da05293568f43b5d49201ac3715f	0	0
MSExchange Transport Agent Installation	Tobias Michalski	Sigma Integrated Rule Set (GitHub)	7c1f925effd9c12efb8a40826e8b85d7d92e1819d550b48add5d3bd5ee8421e2	0	0
MSExchange Transport Agent Installation	Tobias Michalski	Sigma Integrated Rule Set (GitHub)	9aa90df87bd198fdfd7ce530f731f1242cebb92ae8329996250469bfd299dfd7	0	0
MSExchange Transport Agent Installation	Tobias Michalski	Sigma Integrated Rule Set (GitHub)	e771c0dcabbf8a0f6d4bb616409030d867092a5b633c5f87b668c761e0a73c23	0	0
MSI Spawned Cmd and Powershell Spawned Processes	Teymur Kheirkhabarov (idea), Mangatas Tondang (rule), oscd.community	Sigma Integrated Rule Set (GitHub)	c7a8b63e31de07a842a530c5020291d2370e859b36aea25420f0d9744a271f6f	0	0
MSTSC Shadowing	Florian Roth	Sigma Integrated Rule Set (GitHub)	545e2b755dc7bda66c90dfd73d0da8d2692a4c7181d99d429ad2c0253be12ef7	0	0
MacOS Emond Launch Daemon	Alejandro Ortuno, oscd.community	Sigma Integrated Rule Set (GitHub)	839422d12551f797abb514fc052bfc852f3811d1b983090ecd6b6cf2f22d8ed9	0	0
MacOS Network Service Scanning	Alejandro Ortuno, oscd.community	Sigma Integrated Rule Set (GitHub)	4fff924a8370247252e1b93169b91f3d7ed7d41b98603cfd2b8ce78153c97dd3	0	0
MacOS Scripting Interpreter AppleScript	Alejandro Ortuno, oscd.community	Sigma Integrated Rule Set (GitHub)	6ecd0ccd55a70b96ebb8ad35b9fc18b56f99fdae0b1c2d235ba3300b9457b516	0	0
Macos Remote System Discovery	Alejandro Ortuno, oscd.community	Sigma Integrated Rule Set (GitHub)	f3cd8ef31c8b21a65b954ec79c8cab26887cd18d064a995d666dee41e8acec49	0	0
Mailbox Export to Exchange Webserver	Florian Roth, Rich Warren, Christian Burkard	Sigma Integrated Rule Set (GitHub)	993b4f45701b3ec9d79ce389b7e4b9ba421865eff166ec27145d75741b2609eb	0	0
Malicious Named Pipe	Florian Roth, blueteam0ps, elhoim	Sigma Integrated Rule Set (GitHub)	18beefa1a0a5830d767ea9fe1831ce5fc0abbffeccd3c5932ea06333ab16d451	0	0
Malicious Service Installations	Florian Roth, Daniil Yugoslavskiy, oscd.community (update)	Sigma Integrated Rule Set (GitHub)	6476024015d6f67313581ba841b49d2aa8a5bd55b43397bb49521162a7688649	0	0
Malicious Service Installations	Florian Roth, Daniil Yugoslavskiy, oscd.community (update)	Sigma Integrated Rule Set (GitHub)	9f944a38f9e33b70e2b645ce13a2ea1152481f589928dd164e9a2ca5ca452880	0	0
Malicious Service Installations	Florian Roth, Daniil Yugoslavskiy, oscd.community (update)	Sigma Integrated Rule Set (GitHub)	ed399c29991d5d0998f08a5930c2fb1aadbd51855a51b2b30d76a6bf630eabd9	0	0

Malicious ShellIntel PowerShell Commandlets	Max Altgelt, Tobias Michalski	Sigma Integrated Rule Set (GitHub)	fd4e3cdd5f9ec511509a9b456f37f38c1e40597b044a8b780d338b09445fcf05	0	0
Malicious behaviour on user login (Microsoft Windows - c0d0s0 group behavior)	Ariel Millahuel	SOC Prime Threat Detection Marketplace	fa6ee0e8f8cead534cdfd17b666caa7f1d01a684b482e45fc1dcc98c3a17c190	0	0
Malicious payloads that are hidden in fake Windows error logs	Ariel Millahuel	SOC Prime Threat Detection Marketplace	ca17d229059d9b7592cdb79afc25ca5111f033e6033346e481fcc97443e1cca9	0	0
Malicious utilization of mofcomp.exe via CMD	Ariel Millahuel	SOC Prime Threat Detection Marketplace	8b1787853632b3c011481b5856d0f67e76dcd5ca18b18c17758687641e424c52	0	0
Malware Shellcode in Verclsid Target Process	John Lambert (tech), Florian Roth (rule)	Sigma Integrated Rule Set (GitHub)	ffb6e23f9b9b02d3336ba381f296b796adbc31e0297afd8257cec5c40e66bd8b	0	0
Malware User Agent	Florian Roth	Sigma Integrated Rule Set (GitHub)	a352975e140ee0d8fd67c6be0d75ce52c7e74a2fc79700790bdaa343d062c5c4	0	0
Manipulation of User Computer or Group Security Principals Across AD	frack113	Sigma Integrated Rule Set (GitHub)	080f39fb13644d7055303fabf2a4ace323c7ca1c92ffe33c37a94ed397cecedd	0	0
Masquerading as Linux Crond Process	Timur Zinniatullin, oscd.community	Sigma Integrated Rule Set (GitHub)	9a46c620e21e78da1889a3e8f6dbe4070319becd3a7ef3bdc1d9b11595613ef8	0	0
MavInject Process Injection	Florian Roth	Sigma Integrated Rule Set (GitHub)	f7232cef6ad5bca28b27340de367589ba9ef580c1abb6dd69d8f2005a6473a4d	0	0
Metamorfo malware	Ariel Millahuel	SOC Prime Threat Detection Marketplace	d73a269ba693e8e5fa275faa3169b39f3228c9708fae0c818a2e076be89ebac8	0	0
Metasploit Or Impacket Service Installation Via SMB PsExec	Bartlomiej Czyz, Relativity	Sigma Integrated Rule Set (GitHub)	5a244f13e4984c1b2b7a499cb46ddf8b68c1ba5230d646cec6c578e0fc490e30	0	0
Metasploit Or Impacket Service Installation Via SMB PsExec	Bartlomiej Czyz, Relativity	Sigma Integrated Rule Set (GitHub)	ae51d2d67f9cc0555bac0f8f07cd0f21e85bf7996326a2ea736bf9240afc5c73	0	0

Metasploit Or Impacket Service Installation Via SMB PsExec	Bartlomiej Czyz, Relativity	Sigma Integrated Rule Set (GitHub)	c27cff6b98bff3ffc6f117f1ee7a6d6969aafd5a49ec2acfc599aeac2d16d3aa	0	0
Metasploit Or Impacket Service Installation Via SMB PsExec	Bartlomiej Czyz, Relativity	Sigma Integrated Rule Set (GitHub)	fb37de09ff35e1a563c8446c188e8763186905bd6f1231f36c4344b06b1c1e49	0	0
Metasploit SMB Authentication	Chakib Gzenayi (@Chak092), Hosni Mribah	Sigma Integrated Rule Set (GitHub)	22b00ff2151af3d4d5470dded7d187d4f3021d163003a5608c0f6ce4c476db3f	0	0
Meterpreter or Cobalt Strike Getsystem Service Installation	Teymur Kheirkhabarov, Ecco, Florian Roth	Sigma Integrated Rule Set (GitHub)	192e53b4eb1008e71a9b6e69068e10ea48a5dcaf61b1fc5d176c068bac8e1c8e	0	0
Meterpreter or Cobalt Strike Getsystem Service Installation	Teymur Kheirkhabarov, Ecco, Florian Roth	Sigma Integrated Rule Set (GitHub)	40660e5f6c68cd541236f69c088146a482a8ebd809f57b774378aa0152dca75f	0	0
Meterpreter or Cobalt Strike Getsystem Service Installation	Teymur Kheirkhabarov, Ecco, Florian Roth	Sigma Integrated Rule Set (GitHub)	40956f4e065cdfa5d7b282c6490d46c2ec2965fea47b1d597b61302386d09236	0	0
Meterpreter or Cobalt Strike Getsystem Service Installation	Teymur Kheirkhabarov, Ecco, Florian Roth	Sigma Integrated Rule Set (GitHub)	817e49977822d01e34c3e5dd05aba6ee11f45ab3c722bc7b2a2bb085226e41cc	0	0
Meterpreter or Cobalt Strike Getsystem Service Installation	Teymur Kheirkhabarov, Ecco, Florian Roth	Sigma Integrated Rule Set (GitHub)	9b174921e3b6661c344cd2c30a575a282bf403e050644ebc88bac4c93c5f47bd	0	0
Meterpreter or Cobalt Strike Getsystem Service Installation	Teymur Kheirkhabarov, Ecco, Florian Roth	Sigma Integrated Rule Set (GitHub)	bc197a778a20b521388a98e562298e644a301273af9279e8993a0b44cc59c8c8	0	0
Meterpreter or Cobalt Strike Getsystem Service Installation	Teymur Kheirkhabarov, Ecco, Florian Roth	Sigma Integrated Rule Set (GitHub)	ec12972980ba51f81e74946a518425d59ff6b1a2e43fa17be336b5e67b155fa7	0	0
Microsoft 365 - Impossible Travel Activity	Austin Songer @austinsonger	Sigma Integrated Rule Set (GitHub)	d3a30f1e296d56fea04ef46810f3df154d12cf590c5dc97084de9af8009056ab	0	0
Microsoft 365 - Potential Ransomware Activity	austinsonger	Sigma Integrated Rule Set (GitHub)	02ad8f012c03cc13afc7b6cd67d789e91979b43473e7203b074dd4d9f0b7a889	0	0

Microsoft 365 - Unusual Volume of File Deletion	austinsonger	Sigma Integrated Rule Set (GitHub)	be9779fe3da9967876ef067833b541b5c0d33a033ab69daea3ab20181ea1e000	0	0
Microsoft 365 - User Restricted from Sending Email	austinsonger	Sigma Integrated Rule Set (GitHub)	37b5a17283cb3c4128108fd34d6a17996547cba22f82cb66467c0ef87a0455a7	0	0
Microsoft Binary Github Communication	Michael Haag (idea), Florian Roth (rule)	Sigma Integrated Rule Set (GitHub)	dd661868928412c287335c1703782413d4880320931356edf3f1e713563d99e2	0	0
Microsoft Binary Suspicious Communication Endpoint	Florian Roth	Sigma Integrated Rule Set (GitHub)	d01338d0a87197c0e5132ec7b920332c01f5c9e8218c727591d81888d10a9754	0	0
Microsoft Defender Tamper Protection Trigger	Bhabesh Raj	Sigma Integrated Rule Set (GitHub)	1870d785edc3b42af09c0eb73a2aa3683103c07aea155f77f90275e694cb6a79	0	0
Microsoft Malware Protection Engine Crash	Florian Roth	Sigma Integrated Rule Set (GitHub)	d9bfe783bdd11d38a6493085cbd1c673a360226722228507fb920ef71b62895d	0	0
Microsoft Teams update.exe suspicious command argumets	Den Iuzvyk	SOC Prime Threat Detection Marketplace	1b4855885781ab5b82eba4b8b314d00176f5ac0f29ba84391f11660a70ecd421	0	0
Mimikatz DC Sync	Benjamin Delpy, Florian Roth, Scott Dermott	Sigma Integrated Rule Set (GitHub)	ec2307a906e3ea53e96b7874574d7a2e89921b6e7f541a663a6626661dcdc850	0	0
Mimikatz Detection LSASS Access	Sherif Eldeeb	Sigma Integrated Rule Set (GitHub)	ff1315c395da2bdbd410add740bc4f48077e8e1d846f3e2531758ed506a43645	0	0
Mimikatz In-Memory	sigma	Sigma Integrated Rule Set (GitHub)	dadac8ee034d1cee2ef5b7d9a388d1421c731a53717834507c67ffe1b14b5104	0	0
Mimikatz MemSSP Default Log File Creation	David ANDRE	Sigma Integrated Rule Set (GitHub)	1bf84826e67862a2c36769a8990e8a19bc79218d45bd297eac23f736bebb40c4	0	0
Mimikatz through Windows Remote Management	Patryk Prauze - ING Tech	Sigma Integrated Rule Set (GitHub)	847efb8ac13cfab516079fc4fc864f42a81274705a40c71c2e343e3ff59586c4	0	0
Modification of ld.so.preload	E.M. Anhaus (originally from Atomic Blue Detections, Tony Lambert), oscd.community	Sigma Integrated Rule Set (GitHub)	35fdcd5de6749c0a3648859877873d553a64b9d469a1b72223f3430a15ab10e7	0	0
Modirat Trojan	Ariel Millahuel	SOC Prime Threat Detection Marketplace	83d78690b6193fe5c1396f8bc78fdedf8ba876a1e3b33e73fbd88be9ad9ac43b	0	0

Modirat Trojan	Ariel Millahuel	SOC Prime Threat Detection Marketplace	8db76b3af1f01ca259e1dfb9ffced0b62d57908e3afda6d7190050a3651d0f35	0	0
Monero Crypto Coin Mining Pool Lookup	Florian Roth	Sigma Integrated Rule Set (GitHub)	0752dd4f3de82ada650a6c6ed1887cc940d8f55e130fec468ce0df9b2ec4ef25	0	0
Monitoring Winget For LOLbin Execution	Sreeman	Sigma Integrated Rule Set (GitHub)	12f03e6b0e193a0311b8fdfe379fc617a6b5ec4b6afd3fa4e2f8b3f1eb8774e8	0	0
Monitoring Wuauclt.exe For Lolbas Execution Of DLL	Sreeman	Sigma Integrated Rule Set (GitHub)	b7e3452e4a99ca10a2296ac99559c3c5ad282843dc9d00e99e744ca6725da3ae	0	0
Moriya Rootkit	Bhabesh Raj	Sigma Integrated Rule Set (GitHub)	4a9ddb920ad6eab5d240fd46b4a22a2839ea161414fab29fdcd567a468de9295	0	0
Moriya Rootkit	Bhabesh Raj	Sigma Integrated Rule Set (GitHub)	9dd3e22b848384bcb3c88ebef774e34383b1ce9ed5a38ae9e19b8002aa5e1197	0	0
Moriya Rootkit	Bhabesh Raj	Sigma Integrated Rule Set (GitHub)	e890924140d1c95de2b7a7fb0972af50a2c5721ef496761669c3aba2244f16e8	0	0
Moriya Rootkit	Bhabesh Raj	Sigma Integrated Rule Set (GitHub)	fd2423cd1fb181effe2fb4c56218d09921ebaa407b79513920ea5b24c9a3f645	0	0
Mshta Download Pastebin	Joe Security	Joe Security Rule Set (GitHub)	022d94a14c023de93a446a40880959661603927ebe5efff6b062cf01f85d2627	0	0
Multifactor Authentication Interupted	AlertIQ	Sigma Integrated Rule Set (GitHub)	486699d92cc29a0049da80bf790ffe339597bd00fe884682f96c34da8e130514	0	0
Multiple Abnormal non conforming HTTP Requests	SOC Prime Team	SOC Prime Threat Detection Marketplace	b6ffd0976104f055b1bd3ba49b801ac35b6e79610413ba345169d98aeae6b573	0	0
Multiple Clients to HTTP Using Unicode Host via HTTP - Possible Multiple Phishing Attempts	SOC Prime Team	SOC Prime Threat Detection Marketplace	511963c1db190bc62faca5bc4ca06521da4635570743caf2d3f9cd4d56ca50a5	0	0
Multiple Clients to HTTP Using Unicode Host via HTTP - Possible Multiple Phishing Attempts	SOC Prime Team	SOC Prime Threat Detection Marketplace	988a0ffb0a0f47129dd9b934dcb130f00534a2413639d8a3c688061cd4a9765e	0	0

Multiple Compressed Files Transferred Outbound	SOC Prime Team	SOC Prime Threat Detection Marketplace	b8fd2aa035454d18d6233196fd8163e8a2353d52c1aac77573478869e2f4e068	0	0
Multiple Compressed Files Transferred over HTTP	SOC Prime Team	SOC Prime Threat Detection Marketplace	7bad960058d62e8ad7b373e0f3e304754a2b6902377eb2e11113e17b75ccc3c7	0	0
Multiple Modsecurity Blocks	Florian Roth	Sigma Integrated Rule Set (GitHub)	3262aea4a6fe473c1bbccdfd23a7fdf4ca12d85cd72e7f33b38038ec0744e1c2	0	0
Multiple Remote SMB Connections from single client	SOC Prime Team	SOC Prime Threat Detection Marketplace	c8e5e581e3b175b3982cdbb599ff7f79477c6d33f45c778d0e404d3b39611c79	0	0
Multiple SSH Brute Inferences from Single IP	SOC Prime Team	SOC Prime Threat Detection Marketplace	169719cbc9d66e576e8fed121636ea4267a6c02afe08533153871190bf0ee2ae	0	0
Multiple Suspicious Resp Codes Caused by Single Client	Thomas Patzke	Sigma Integrated Rule Set (GitHub)	36b7f0b4e7ca31a80f5929c779c0b90ea599d134f5e18ed404448e5c7e4664d5	0	0
Multiple Users Attempting To Authenticate Using Explicit Credentials	Mauricio Velazco	Sigma Integrated Rule Set (GitHub)	c9d7284a26107f63bbe7266930bba513eee485e862028ef3d01f460fdfd13353	0	0
Multiple Users Failing to Authenticate from Single Process	Mauricio Velazco	Sigma Integrated Rule Set (GitHub)	b83947b9ca0aad485d29caf723d94bab0c256d4731fd51b5dd69d8ee931646f2	0	0
Multiple Users Remotely Failing To Authenticate From Single Source	Mauricio Velazco	Sigma Integrated Rule Set (GitHub)	4107edd5afd06ad49d102029bda7ae9f9b114dc56eb3f36ad01188bfdcdbf804	0	0
Multiple Windows Admin Share Connections	SOC Prime Team	SOC Prime Threat Detection Marketplace	9480e7a6092cdaee91f66357eb157816e36db05dcc021646b7b6bd3b1f0deba2	0	0
Multiple Windows Remote Registry Service Connections	SOC Prime Team	SOC Prime Threat Detection Marketplace	555ec13fb5fd2bac1c4c3d56534a101fe85e324759a14d2efbcff17a8ce0d68e	0	0
MustangPanda COVID-19 campaing	Ariel Millahuel	SOC Prime Threat Detection Marketplace	50f367f6a2c0c7a6e7071294d21ea586cf7ba6280290d19c28143cb5ba740344	0	0

MustangPanda COVID-19 campaing	Ariel Millahuel	SOC Prime Threat Detection Marketplace	6fa28d8cc3b3f717443e0a42b68552d7a87153b44f262b79824fdceb66d49c55	0	0
NPPSpy Hacktool Usage	Florian Roth	Sigma Integrated Rule Set (GitHub)	fe93afc27b2b53b9e4deb1b29d0172ddf97ab492beba618fda8529d8eb602bed	0	0
NTLM Logon	Florian Roth	Sigma Integrated Rule Set (GitHub)	7c3dc15fbc51dea715925bf595cd0f9e0a02de70e6c439f34e6f1f0e05748574	0	0
NanoCore	Joe Security	Joe Security Rule Set (GitHub)	270a1fb968dc6493ee107a0a5e9afce805af2cd2d8675f58a02c418e36821076	0	0
Nansh0u Campaign (Sysmon detection)	Ariel Millahuel	SOC Prime Threat Detection Marketplace	904193bc621aaa8bd679e31840889e7e0ebdd3012ad80cd285a787efa9a21a1e	0	0
Narrator's Feedback-Hub Persistence	Dmitriy Lifanov, oscd.community	Sigma Integrated Rule Set (GitHub)	4064f97b1b93e3d50e6d45f091287083f57a4143e79079ddd4afcae5bd61545f	0	0
Nemty Ransomware (LOLBins abuse)	Ariel Millahuel	SOC Prime Threat Detection Marketplace	b6e935f32e1e64aba00eeea36dedcf16c051a067fc0bd9e45ea29c807851976e	0	0
NetNTLM Downgrade Attack	Florian Roth, wagga	Sigma Integrated Rule Set (GitHub)	628b3cedd2ee451a4c293777e6a6b1405d7ff8640e456f6c947256490c60b5d7	0	0
NetNTLM Downgrade Attack	Florian Roth, wagga	Sigma Integrated Rule Set (GitHub)	bec1f52073fc2866f36490eba29525c7075bac3d5209203cfda883af578ca4f8	0	0
NetNTLM Downgrade Attack	Florian Roth, wagga	Sigma Integrated Rule Set (GitHub)	cf37bb8e1c6eb04a715e1acac3004996b87765e5a9a1641cd5f9ba489b398a21	0	0
NetWire RAT Registry Key	Christopher Peacock	Sigma Integrated Rule Set (GitHub)	ce5ddd582faff7ef5d678ca346465de3df879ce2fce177a243fb03283ce96f91	0	0
Netcat The Powershell Version	frack113	Sigma Integrated Rule Set (GitHub)	0fd4e2409b6a9d2d52410acd12bed00a2c98b5907728ae24ee86bc36d470b52d	0	0
Netcat The Powershell Version	frack113	Sigma Integrated Rule Set (GitHub)	afccc7dbdf0a361ce026bc9a376283952eb427865b9051cc07fd5ff5ed819482	0	0
Netsh Allow Group Policy on Microsoft Defender Firewall	frack113	Sigma Integrated Rule Set (GitHub)	631a83ba9daa9bb7ff02be55784068db1eeaa6935ea10809a1b8a8cf4ce2abd3	0	0
Netsh RDP Port Forwarding	Florian Roth, oscd.community	Sigma Integrated Rule Set (GitHub)	70c15fe82eef73d893f59ec3589b484917b941f103c9c29048472576af7e8cc8	0	0
Network Scans	Thomas Patzke	Sigma Integrated Rule Set (GitHub)	45df53aa30dc2cfa8b51eefcfc5610c077a28dd2cc8dc1e231a33ea4a8787dd7	0	0
Network Scans	Thomas Patzke	Sigma Integrated Rule Set (GitHub)	bb657f87ac9c438630487838d7c6786269418efb6f627897a245514632b7b71c	0	0

Network Scans	Thomas Patzke	Sigma Integrated Rule Set (GitHub)	bf8c0428428fa1278ad2e0afa0221c340e18931c689a1a74660e2b25a2a1860a	0	0
Network Scans Count By Destination IP	Thomas Patzke	Sigma Integrated Rule Set (GitHub)	0513b00d4770e8ba4e68a1bf68cab686e859e14797388dbcf6f51ea10f3042cc	0	0
Network Scans Count By Destination Port	Thomas Patzke	Sigma Integrated Rule Set (GitHub)	d59f72c28978b1e054ff60f91c7cbf0354f8d455e90795685535c1697fd3c945	0	0
Network Service Scanning Multiple IPs	SOC Prime Team	SOC Prime Threat Detection Marketplace	d2d4bc90121c2e5cb6f3b7884fe1e4c06a3a4c61c381e33eaf549354d0929db8	0	0
Network Service Scanning Multiple IPs for Open Port	SOC Prime Team	SOC Prime Threat Detection Marketplace	e06753fd5e71bee4c1603fb8e04f441b1a19e365ff520231341b58b5c9676d87	0	0
Network Share Discovery	SOC Prime Team	SOC Prime Threat Detection Marketplace	7cda33e78a2e154cdc2a2bbeb41857926b105d3f9e7750e0d39c1a6db9bf9563	0	0
Network Sniffing	Alejandro Ortuno, oscd.community	Sigma Integrated Rule Set (GitHub)	34a3b83c8ed31a73806fd506d538c5611d10141f5683c39ccd3e822a4e68da7b	0	0
Network Sniffing	Timur Zinniatullin, oscd.community	Sigma Integrated Rule Set (GitHub)	cec88cf573d8c7f5ff9c871e5caf9caf91adc563916947a89aad1491da2346ac	0	0
Network Sniffing	Timur Zinniatullin, oscd.community	Sigma Integrated Rule Set (GitHub)	e0fec53c12094131d1b4e307c8e9dcea040e6d3cbb6b5eff0144c5a71473253d	0	0
Neutrino Backdoor	Ariel Millahuel	SOC Prime Threat Detection Marketplace	c36594c085c33464fc5cde06dc8ae917de450f86a16aff6f5e7e0f6e3be73f2b	0	0
Neutrino Backdoor	Ariel Millahuel	SOC Prime Threat Detection Marketplace	d3b050f13506d1bf0507f478002af7a34e949fa40a2ef119fbc657f3a35de60a	0	0
New Application in AppCompat	Roberto Rodriguez (Cyb3rWard0g), OTR (Open Threat Research)	Sigma Integrated Rule Set (GitHub)	63f0997b285249bf20906023fb00f8eb00815314c790f67a70befd01625e8aeb	0	0
New DLL Added to AppCertDlls Registry Key	Ilyas Ochkov, oscd.community	Sigma Integrated Rule Set (GitHub)	4bdead82e3a6a57ba296d62ccea3f3cd1086e50cb50a9b58540d3e065c5c756b	0	0
New File Association Using Exefile	Andreas Hunkeler (@Karneades)	Sigma Integrated Rule Set (GitHub)	3616394136d97f22be2d8a0718627a44f64289b519a8ab455bef574a2a43961a	0	0
New Lolbin Process by Office Applications	Vadim Khrykov (ThreatIntel), Cyb3rEng (Rule)	Sigma Integrated Rule Set (GitHub)	8a45e61fc1757825afcd5eca531a7940c6b8fd8ed95faee7b3ea517339e0ee17	0	0
Nginx Core Dump	Florian Roth	Sigma Integrated Rule Set (GitHub)	7a4cd40845c7f590d81d5519efe14cb755da4ad7e8382cf1b793884653b688b5	0	0

Nibiru detection (Registry event and CommandLine parameters)	Ariel Millahuel	SOC Prime Threat Detection Marketplace	3debb91f02ff96ef7063287de5f4ac2a5b63133f3d2217b252f7ff735f72fe86	0	0
Non-privileged Usage of Reg or Powershell	Teymur Kheirkhabarov (idea), Ryan Plas (rule), oscd.community	Sigma Integrated Rule Set (GitHub)	27c02a5e277091bc1c5b7d2a04365e89a8787ee68e58616afd80ef5c26aa04de	0	0
Novter Botnet detection	Ariel Millahuel	SOC Prime Threat Detection Marketplace	f699b7b7fd20025dcb81e2586b58b97d0ba868dae7904c07e08849456012355d	0	0
Number Of Resource Creation Or Deployment Activities	sawwinnnaung	Sigma Integrated Rule Set (GitHub)	72c0e900a73e61f8d65b8fc1bc7424e17ed6404f198817556ef1b8bf780307f9	0	0
OMIGOD HTTP No Authentication RCE	Nate Guagenti (neu5ron)	Sigma Integrated Rule Set (GitHub)	37c2af49383c30c36d87b7215b22296e477d1b387c3b0c34cf3a3050d62099f1	0	0
OMIGOD SCX RunAsProvider ExecuteScript	Roberto Rodriguez (Cyb3rWard0g), OTR (Open Threat Research)	Sigma Integrated Rule Set (GitHub)	1aa03e3c54881b2badbac443dfd964bb5e89d65f3a4230ddb1349cd55dd16701	0	0
OMIGOD SCX RunAsProvider ExecuteScript	Roberto Rodriguez (Cyb3rWard0g), OTR (Open Threat Research), MSTIC	Sigma Integrated Rule Set (GitHub)	d532e92700eb248ec7d25152f456ce46ecee476d6fd76a7b3e07659c54d26855	0	0
OMIGOD SCX RunAsProvider ExecuteShellCommand	Roberto Rodriguez (Cyb3rWard0g), OTR (Open Threat Research)	Sigma Integrated Rule Set (GitHub)	57337e7a54cc7d5663f144c2d4051297cb796d11797ae6e1ca29ba67c27edb19	0	0
OMIGOD SCX RunAsProvider ExecuteShellCommand	Roberto Rodriguez (Cyb3rWard0g), OTR (Open Threat Research), MSTIC	Sigma Integrated Rule Set (GitHub)	5d1fd434b1c927d94f9fe4453395535db904af037d3b9d3ff45b6ef71c0f8e43	0	0
OceanLotus Registry Activity	megan201296, Jonhnathan Ribeiro	Sigma Integrated Rule Set (GitHub)	5a41f82caece4fe65bbe71be9148baa62a842cabce69fc96f25fcdbf97f8008d	0	0
Octopus Scanner Malware	NVISO	Sigma Integrated Rule Set (GitHub)	ad8390b7e69e5ce853f3c92ad2199323cf05de73cc23538d5f0c64b8f2ee6bfe	0	0
Offensive tool MaliciousDLLGenerator. DLL side loading(Sysmon)	Den Iuzvyk	SOC Prime Threat Detection Marketplace	83567691787215050fc2832d1859c46eef4d6ec184c2e86675a1cda9293f9656	0	0
Office Application Startup - Office Test	omkar72	Sigma Integrated Rule Set (GitHub)	d30a6ec556476631a5a9c60d8741c765b1c2e39b6c80bda1ad8bff961bbdae9a	0	0
Office Applications Spawning Wmi Cli	Vadim Khrykov (ThreatIntel), Cyb3rEng (Rule)	Sigma Integrated Rule Set (GitHub)	4e7dcf0bdb7133795dc5f59a3dce3f19d7a78ad417e3b41e7dea915b76bdfd5d	0	0

Office macro parent spofing injection	Den Iuzvyk	SOC Prime Threat Detection Marketplace	6633d004f33515072ffdd8f03f41910d3d9da5e01701655ea5e05259c72e6d05	0	0
Oilirg's "RDAT "Backdoor (Sysmon detection)	Ariel Millahuel	SOC Prime Threat Detection Marketplace	75f9172f5d8240599ba3e90228c244a661f19b8fecdf018defea7ea69584949	0	0
Oilrig	Ariel Millahuel	SOC Prime Threat Detection Marketplace	ea4cbf16bdb71984f5023f3f7cb99896b2f2fbbc624e3fed169da1b645de6150	0	0
Okta API Token Created	Austin Songer @austinsonger	Sigma Integrated Rule Set (GitHub)	37c62bd2bbcddc4acc9d1a5790917fced5f8bffd7529d17806bae479015d0438	0	0
Okta API Token Revoked	Austin Songer @austinsonger	Sigma Integrated Rule Set (GitHub)	0f26d84e2eba3bdbd5a67b63c111a77e2d63546e74143de49507314c059c0fd2	0	0
Okta Admin Role Assigned to an User or Group	Austin Songer @austinsonger	Sigma Integrated Rule Set (GitHub)	76ee74749375861af873800c29031bf76c1d499b124d9ea839ba8c40dee90c8e	0	0
Okta Application Modified or Deleted	Austin Songer @austinsonger	Sigma Integrated Rule Set (GitHub)	5146d9202bfee99aebeefa43c786b2e3719434b3ce05ab72c3c3b42d285cebe5	0	0
Okta Application Sign-On Policy Modified or Deleted	Austin Songer @austinsonger	Sigma Integrated Rule Set (GitHub)	2ef17e10bfa93f6d655fd5a9f9191f5ac2f485b9a0dd458d450ad6d3337261e9	0	0
Okta MFA Reset or Deactivated	Austin Songer @austinsonger	Sigma Integrated Rule Set (GitHub)	ec810333c5b5e59400842656cc184df2783f47b5b55d0030bfa5a4f21568df9c	0	0
Okta Network Zone Deactivated or Deleted	Austin Songer @austinsonger	Sigma Integrated Rule Set (GitHub)	fe00ea6d901a92c5ecc5302f0e36994a890f1b517bb02510b6a368f421ec89c9	0	0
Okta Policy Modified or Deleted	Austin Songer @austinsonger	Sigma Integrated Rule Set (GitHub)	1c210d6fdbd5b2ba495cbd1a803fad26f2c34786e6b979f4ce8e88872a25db23	0	0
Okta Policy Rule Modified or Deleted	Austin Songer @austinsonger	Sigma Integrated Rule Set (GitHub)	ae0100a24042add9897a943949ccd1e1e3f8c310cd5979cf48accbce725cd423	0	0
Okta Security Threat Detected	Austin Songer @austinsonger	Sigma Integrated Rule Set (GitHub)	82f25417bf76cf8b64d66b26bf54c4850a4187772d8094d02f3f8eb64bc20bf4	0	0
Okta Unauthorized Access to App	Austin Songer @austinsonger	Sigma Integrated Rule Set (GitHub)	4ac129ccafdbbfad46a3392c4e73182ba5823ac3df49ac7d3e35e10cbf159b2a	0	0
Okta User Account Locked Out	Austin Songer @austinsonger	Sigma Integrated Rule Set (GitHub)	713536374c2a86507e8c3738a171b0b1ab7398e3b84b9a491e14890485ff6bb7	0	0
OneLogin User Account Locked	Austin Songer @austinsonger	Sigma Integrated Rule Set (GitHub)	989ec67196bdfe4759541550bbddc7a6be65ecf2debfc15598f3768a4000df04	0	0

OneLogin User Assumed Another User	Austin Songer @austinsonger	Sigma Integrated Rule Set (GitHub)	f0eee7a94251a99b6a747dc186b09c26d9850f1e61d9cbcb7a5939e633565f04	0	0
OpenWith.exe Executes Specified Binary	Beyu Denis, oscd.community (rule), @harr0ey (idea)	Sigma Integrated Rule Set (GitHub)	ea5ec4a6c95de7e028405041a4052a38c12bd6345847e628f0b4ed6648db62d1	0	0
Operation Wocao Activity	Florian Roth, frack113	Sigma Integrated Rule Set (GitHub)	0981b6a6bd3a352e954d4f808351eef72bde12f597fac067385a86f67f28169f	0	0
Operation Wocao Activity	Florian Roth, frack113	Sigma Integrated Rule Set (GitHub)	2e30c366dcaa537ae7d98a978f19c3a6bbf9b459e177978af689a71981ca468f	0	0
Operation Wocao Activity	Florian Roth, frack113	Sigma Integrated Rule Set (GitHub)	41500c83cd93f90f6d367be3449920cac482603fa9b7f4137f2576feb2ba50a8	0	0
Operation Wocao Activity	Florian Roth, frack113	Sigma Integrated Rule Set (GitHub)	a0774a9062d671fa2115dde2a5620ddb95c39200fc4fbcd5a7504ced2408c516	0	0
Operation Wocao Activity	Florian Roth, frack113	Sigma Integrated Rule Set (GitHub)	d4c0402f67c8a3748cf75523ef859b1c3b31b2503661858ec74bc3b5c7cad0af	0	0
Oracle WebLogic Exploit	Florian Roth	Sigma Integrated Rule Set (GitHub)	9bfd34293b2b68ab59c38057b018b43e4604ddd974aedeb628eb74f48467b2af	0	0
Oracle WebLogic Exploit CVE-2020-14882	Florian Roth	Sigma Integrated Rule Set (GitHub)	82dda926865821ca5e8c3ddb93fc4f69772bb79643d23c061dc2f359fcb25cee	0	0
Oracle WebLogic Exploit CVE-2021-2109	Bhabesh Raj	Sigma Integrated Rule Set (GitHub)	58f3096519d091461dc02d540c9ad2e2714378fc856af5b52dcd246cf062437e	0	0
Orcus RAT detection	Ariel Millahuel	SOC Prime Threat Detection Marketplace	870bd93000dae7789508610f80cf9f2862f3b3e9fefec9b3cba32617a75799cd	0	0
Orcus RAT detection	Ariel Millahuel	SOC Prime Threat Detection Marketplace	c71576208518c999b7feba529c697771d91ca38beb7d087c1d8ae78eba2c5bb0	0	0
Outlook C2 Macro Creation	@ScoubiMtl	Sigma Integrated Rule Set (GitHub)	6521fe44f6063c0c2459334902169e29975140f570d57f3ec5fb33d79f3b074b	0	0
Outlook C2 Registry Key	@ScoubiMtl	Sigma Integrated Rule Set (GitHub)	2f07ac019282aa31e768110336780c9cb961d1b01262e2beeea4f9f7c17a906eb	0	0
Outlook Form Installation	Tobias Michalski	Sigma Integrated Rule Set (GitHub)	b8ad31e84529c4f0ecaff3ccdb07e6876487faa4fe4e57f07afb4d3a104ed7c4	0	0
Overwrite Deleted Data with Cipher	frack113	Sigma Integrated Rule Set (GitHub)	d3e54936275abafa46d4b77891ec8f7fe6dd55d420fec613476144dd5d26f1a7	0	0
Overwriting the File with Dev Zero or Null	Jakob Weinzettl, oscd.community	Sigma Integrated Rule Set (GitHub)	fb9c58953377bc9ef08cbec4e7921e8bfd0bcea1b91c79a56cd7f21e179f5514	0	0

Oxypumper and Qwertminer detection	Ariel Millahuel	SOC Prime Threat Detection Marketplace	2e9004538d0ac25abf5f74d2ab10e6804e8c5a6d78ded8ec678d1d57791fdd4d	0	0
PCRE.NET Package Image Load	Roberto Rodriguez (Cyb3rWard0g), OTR (Open Threat Research)	Sigma Integrated Rule Set (GitHub)	314e0194b44c70b9c92c8fcd5ab2295e9f0c5d034db71b856dc14098ba319f82	0	0
PCRE.NET Package Temp Files	Roberto Rodriguez (Cyb3rWard0g), OTR (Open Threat Research)	Sigma Integrated Rule Set (GitHub)	298754861fb9b51e8da2c4490353502093fe96a301b2c943df1e6d6ccc641ea8	0	0
PSExec and WMI Process Creations Block	Bhabesh Raj	Sigma Integrated Rule Set (GitHub)	d5f9283f29961f497c15a772fe3eaf3852c91aaeca1034ffa8fbac0ad1e65b32	0	0
Pandemic Registry Key	Florian Roth	Sigma Integrated Rule Set (GitHub)	1280d1699ff038c66a632a34d113a985abe94aba7a198de85b3dec7e8c56e432	0	0
Pandemic Registry Key	Florian Roth	Sigma Integrated Rule Set (GitHub)	83870fe1bc3919a21d0e4bfe80e46298d498a92fede413336e99c62c736fde77	0	0
Pandemic Registry Key	Florian Roth	Sigma Integrated Rule Set (GitHub)	94c2e0c66ba5ec7b925ceb0b07bd496ceb43525c621caa6b3a18048c1c9ffd88	0	0
Pandemic Registry Key	Florian Roth	Sigma Integrated Rule Set (GitHub)	a1ba081fa2fecc17406857322da10c42bfd5d39b025a35029fa0fe1b55760821	0	0
Pandemic Registry Key	Florian Roth	Sigma Integrated Rule Set (GitHub)	f3d343e52cbeb2af747dd246bd8ea56b0de2c474c81d88ef7e6cd844d31fe85a	0	0
Pass the Hash Activity	Ilias el Matani (rule), The Information Assurance Directorate at the NSA (method)	Sigma Integrated Rule Set (GitHub)	28b05b77c561c979f988b8e68e0fd7bee5c3d69bebf583aefab5e6c03dbd30d4	0	0
Password Change on Directory Service Restore Mode (DSRM) Account	Thomas Patzke	Sigma Integrated Rule Set (GitHub)	d5526765d05068ba3b4fc756226bbb23764077a29b90a8d1b182c52b27247a96	0	0
Password Cracking with Hashcat	frack113	Sigma Integrated Rule Set (GitHub)	9621c87be63b1ea5e038a8d2759bc0bbe6a5ee4f322b9763fdc06f159d781698	0	0
Password Dumper Activity on LSASS	sigma	Sigma Integrated Rule Set (GitHub)	25dff248d062d94230b27dc2516c0e2a98f6760f4b5d93f07871a0f48b12c990	0	0
Password Policy Discovery	Ömer Günal, oscd.community, Pawel Mazur	Sigma Integrated Rule Set (GitHub)	70af2a777246077f95f00d88094a0d2d36234fe41d5cb79303b751759b327351	0	0
Path Traversal Exploitation Attempts	Subhash Popuri (@pbssubhash), Florian Roth (generalisation)	Sigma Integrated Rule Set (GitHub)	773cff12ec7cbfc99bc118e98518f2e0050d70dca13977467d5ec706e1253a9d	0	0
Persistence and Execution at Scale via GPO Scheduled Task	Samir Bousseaden	Sigma Integrated Rule Set (GitHub)	261e256e88ce2c0fee286d620d8ff6e77e8cd38f8b7edfda21eb83ac8d48a9b5	0	0
Persistent Outlook Landing Pages	Tobias Michalski	Sigma Integrated Rule Set (GitHub)	6ae750585488b213e225f24f0cd7693782801986e4406629424e8bba973f8645	0	0

Persistent Outlook Landing Pages	Tobias Michalski	Sigma Integrated Rule Set (GitHub)	7b23c3334a69965bcad3cbae78bfb96013d973e4eafe5031ea53c5b35acadb90	0	0
PetitPotam Suspicious Kerberos TGT Request	Mauricio Velazco, Michael Haag	Sigma Integrated Rule Set (GitHub)	ea26c5b32a6c3921fdfe6b9e3d229e17679f51ee8479750522d3af1a3e499d7e	0	0
Phorpiex Trojan	Ariel Millahuel	SOC Prime Threat Detection Marketplace	49cbcdd3c2bd2982afc88c5858d00892e8d508453878c1a3cd42562042976e54	0	0
Pingback Backdoor	Bhabesh Raj	Sigma Integrated Rule Set (GitHub)	12147457a137c617a8c55dbaedd9bc3c0cec1a58f0abd3a364a57af2b9dc7967	0	0
Pingback Backdoor	Bhabesh Raj	Sigma Integrated Rule Set (GitHub)	25fa9043dc7fef1e4d5f8f2c702b53d1134ca5d490bae826fd7ecf2551f3e2ce	0	0
Pingback Backdoor	Bhabesh Raj	Sigma Integrated Rule Set (GitHub)	5c3e50d74286082eb71b88893a78ffa754ccb9d60b9acce0bb0b8cb91d5ba31d	0	0
Pingback Backdoor	Bhabesh Raj	Sigma Integrated Rule Set (GitHub)	6445b62d62c302592ad18186139719c0e819f43d9a6beed3bf0ab7f2d451d194	0	0
Pingback Backdoor	Bhabesh Raj	Sigma Integrated Rule Set (GitHub)	ea92810a14a762b008597bcf3399fe14869e0f793089b7e162701a7be5def9bd	0	0
Pingback Backdoor	Bhabesh Raj	Sigma Integrated Rule Set (GitHub)	f384452415580cfacef78ec66267f7d0bfb736fee4faca1b9d7d41f0a7975af2	0	0
PoetRAT detection	Ariel Millahuel	SOC Prime Threat Detection Marketplace	9d199db1a634577d3f5cc20a856125c4d011cf3785ae959ddad5ca77431d81a2	0	0
Ponmocup Malware Behavior	Ariel Millahuel	SOC Prime Threat Detection Marketplace	552054511e656c379a350ba0be389fc00411a46c49cefaa5969933937782bd7f	0	0
PortProxy Registry Key	Andreas Hunkeler (@Karneades)	Sigma Integrated Rule Set (GitHub)	e95b67f51925e56d5e1ce56881ff5e65536dbd80108577670b3adf94d708f2e7	0	0
Possible App Whitelisting Bypass via WinDbg/CDB as a Shellcode Runner	Beyu Denis, oscd.community	Sigma Integrated Rule Set (GitHub)	93807d89530fb696ca050ed3db0953ce414b88509cf142223144b53058957b9a	0	0
Possible CVE-2020-1472 (zerologon)	SOC Prime Team	SOC Prime Threat Detection Marketplace	004fb7066c5a25b3f6a6420c6a8725fbc30258b16fb591b4c9b86b9da893d74d	0	0
Possible CVE-2020-1472 (zerologon)	SOC Prime Team	SOC Prime Threat Detection Marketplace	b2199e218352cf6a91e1a9ea26af1aa07e66c291293a802c8fdf82966b40dbe4	0	0

Possible CVE-2021-1675 Print Spooler Exploitation	Florian Roth, KevTheHermit, fuzzyf10w	Sigma Integrated Rule Set (GitHub)	bead488a4543b9f760689bdc7093fc4540098b5bcf3c09c678976c6ed6354eb2	0	0
Possible CobaltStrike PsExec filenames (via audit)	SOC Prime Team	SOC Prime Threat Detection Marketplace	a2858e2b79b3da9a5b4d1304cbcd84acf91d6a6062ca5f095b0d774272030879	0	0
Possible CobaltStrike PsExec filenames (via audit)	SOC Prime Team	SOC Prime Threat Detection Marketplace	a321323d7d6157b4259e681855280c87bb847b7bc7874bc3fabdbdf23ec563c7	0	0
Possible Coin Miner CPU Priority Param	Florian Roth	Sigma Integrated Rule Set (GitHub)	066bf65181967c1e98ac2f9df11a8fd671e19d04a92efcac223bb0d380b06fdf	0	0
Possible DC Shadow	Ilyas Ochkov, oscd.community, Chakib Gzenayi (@Chak092), Hosni Mribah	Sigma Integrated Rule Set (GitHub)	b2fec2248b287bf7e5d5226c97e0e035d64995c904571c48230b8adac0240d6b	0	0
Possible DNS Rebinding	Ilyas Ochkov, oscd.community	Sigma Integrated Rule Set (GitHub)	7a69b135d65a01f7902597771e9c5634482fc44f6a01ddde76c647a9b293f852	0	0
Possible DNS Tunneling	Patrick Bareiss	Sigma Integrated Rule Set (GitHub)	e5974527 86d564a9ef7996902a2c2c93c77f558932cbf4f4bdf5a3bc3bd8414f	0	0
Possible Data Collection Over SMB	SOC Prime Team	SOC Prime Threat Detection Marketplace	ac79c3ded0f25a49a60eeb6806049f4e21c47eff774ed79ceb760b8377ace4c6	0	0
Possible Data Collection related to Office Docs and Email Archives and PDFs	SOC Prime Team	SOC Prime Threat Detection Marketplace	d6ed6d774c0f9d1aa8f9e7c8d6e850cccf5682e206f4cf08de83bda6b90994fb	0	0
Possible DePriMon activity (via registry_event)	Ariel Millahuel	SOC Prime Threat Detection Marketplace	05a6eb84ba469846def921f914e3d8b9fbdd2692488b9f37c291938d73de1a2c	0	0
Possible Directory Traversal Web Server Attack	SOC Prime Team	SOC Prime Threat Detection Marketplace	c49479c5356b52e94528e552ed642e4987c6a5c700ed76ebe1536af2231219d0	0	0
Possible Exchange CVE-2021-26858 (via audit)	SOC Prime Team, Microsoft	SOC Prime Threat Detection Marketplace	e69ddf941adc94abece38df217d775b76868df2e2ea22a1ec52a70e9f236fe22	0	0
Possible Exchange CVE-2021-26858 (via audit)	SOC Prime Team, Microsoft	SOC Prime Threat Detection Marketplace	ff377bfd583855c832c7dd822b71dcb07ea79b550063b031c7e96add1d6524e5	0	0
Possible Exchange CVE-2021-26858 (via file_event)	SOC Prime Team, Microsoft	SOC Prime Threat Detection Marketplace	99b35216607149affdfa929b0e387d69d2806cbefee2308c2735848d194d344d	0	0

Possible Exploitation of Exchange RCE CVE-2021-42321	Florian Roth, @testanull	Sigma Integrated Rule Set (GitHub)	5a40221e67f7aba15ef82f3d0d7b2b844f8ae17825570bff630c88811cc4ad61	0	0
Possible F5 BIG-IP TMUI Attack CVE-2020-5902	Roman Ranskyi	SOC Prime Threat Detection Marketplace	218640966c9d97eb1eff96fd1e484617b91f4df0ea75bcf0e4e5cb6fdf8d99b6	0	0
Possible F5 BIG-IP TMUI Attack CVE-2020-5902	Roman Ranskyi	SOC Prime Threat Detection Marketplace	6479d3a228183d5f5cbc12cf06692c41fdde83f2aeac8f71a156a2a48b648a32	0	0
Possible F5 BIG-IP TMUI Attack CVE-2020-5902	Roman Ranskyi	SOC Prime Threat Detection Marketplace	88b5d334ee9ea111b57d657cd139707d075dd8ed6627da16a793126604d859dd	0	0
Possible F5 BIG-IP TMUI Attack CVE-2020-5902	Roman Ranskyi	SOC Prime Threat Detection Marketplace	c1f2f68a9cff2de7103eeb1fd31cdbaf1b6fa00837c80f48223a78b3610f8eee	0	0
Possible Flash 0day execute embedded in Word document. (Sysmon)	Roman Ranskyi	SOC Prime Threat Detection Marketplace	b817381a55e4395f3432afdeaba45bc656fe1d69add003ca93890ee9dbb88dc8	0	0
Possible HAFNIUM Webshell March 2021 (via web)	SOC Prime Team, Micrsoft	SOC Prime Threat Detection Marketplace	3f570551a3f5298bb8ffcdbfa6a8a34da33b20e2466ac118693efa67b24e4b43	0	0
Possible Impacket SecretDump Remote Activity	Samir Bousseaden, wagga	Sigma Integrated Rule Set (GitHub)	d662c9e44d08cdfba8767e63ec2258087b3839be1275833c535955e8dfdc962a	0	0
Possible Impacket SecretDump Remote Activity - Zeek	SOC Prime Team	SOC Prime Threat Detection Marketplace	0f0d88d275fc1726d496bdd1f93e157e9474e735b61dce0f2a1a7e62b73aa4d0	0	0
Possible Impacket SecretDump Remote Activity - Zeek	Samir Bousseaden, @neu5ron	Sigma Integrated Rule Set (GitHub)	9817f9971438f3d35c3ff932f369427b842af1830ee9d876b82315c2af4ec94b	0	0
Possible MS RDP Worm activity aka "BlueKeep" (CVE-2019-0708).	Roman Ranskyi	SOC Prime Threat Detection Marketplace	4f9d5b07a08c2a6f429d46dd58004d7b7cd97555012e4b197608622358100e0c	0	0
Possible Malicious Docker Image was Uploaded.	Brandon Hart	SOC Prime Threat Detection Marketplace	8883f6245da8667a77cc2858555fe077b1437141d61a2ce027184b194828a850	0	0

Possible PetitPotam Coerce Authentication Attempt	Mauricio Velazco, Michael Haag	Sigma Integrated Rule Set (GitHub)	8b1c0d38f0e9f17fd31e1b3ae1092dd248b2ae07a01e4a431516fa46995b8d0f	0	0
Possible PrintNightmare Print Driver Install	@neu5ron (Nate Guagenti)	Sigma Integrated Rule Set (GitHub)	ad5c13aa09c3e5f96d8d44e50e12cbf519a648471259976a40654ceb7215e58a	0	0
Possible Privilege Escalation via Service Permissions Weakness	Teymur Kheirkhabarov	Sigma Integrated Rule Set (GitHub)	eb45f6868e84101d08fc7e8ad4de6ebe7a9bdf7ab558ec191c3afe9857058360	0	0
Possible Process Hollowing Image Loading	Markus Neis	Sigma Integrated Rule Set (GitHub)	fcf7620e2328b946e9b3d0f404695a61a8943ec4865dcb48e4be1d1094ac3196	0	0
Possible Remote Password Change Through SAMR	Dimitrios Slamaris	Sigma Integrated Rule Set (GitHub)	b1713847a4daf31e020cbf71527ef33d0662b5c19661263ab551e6ad9fd67ab6	0	0
Possible Ruby on Rails CVE-2019-5418 PoC	Roman Ranskyi	SOC Prime Threat Detection Marketplace	6fba8939e048342afcf17dfc048d360bac3d5b6624cf12a22d156736dd818870	0	0
Possible Ruby on Rails CVE-2019-5418 PoC	Roman Ranskyi	SOC Prime Threat Detection Marketplace	75865efeda875bb8b0aac82fb3b5a47ff0e7f843016157ee8942621977061407	0	0
Possible Unknown Exchange 0 day March 2021 (via web)	SOC Prime Team, volexity	SOC Prime Threat Detection Marketplace	b9468847ca9a6e3d39ea2b21395d1127e2ffa91f808f3fc8942ef0d65b7f12f7	0	0
Possible VMWare vCenter Exploit CVE-2021-21972	SOC Prime Team	SOC Prime Threat Detection Marketplace	42df827de0dcea1b983942ba353a02fb956b2fde9a0ad6588f317f9ffd56110b	0	0
Possible VMWare vCenter Exploit CVE-2021-21972	SOC Prime Team	SOC Prime Threat Detection Marketplace	b9b880760f2efb391cc1fc7cb12a935b3838db71ee45575fc112bbe9b4a306a1	0	0
Possible Webshell - Rare PUT or POST by IP	SOC Prime Team	SOC Prime Threat Detection Marketplace	12b4ca0d87e88664b966d19bd99b3ccc51ff3c7ee9c0a5458b0f0675a0cd65cc	0	0
Possible Webshell - Rare PUT or POST by IP	SOC Prime Team	SOC Prime Threat Detection Marketplace	7a8435fc28a2572f17ab389949908468b06e249365c83e2203a00baa233b8eb2	0	0

Possible Windows Executable Download Without Matching Mime Type	SOC Prime Team	SOC Prime Threat Detection Marketplace	815d6d2c68a3ef44716300a07a6814032d253de34cd2f2be2648db1efc8c3b61	0	0
Possible Zerologon (CVE-2020-1472) Exploitation	Aleksandr Akhremchik, @aleqs4ndr, ocsd.community	Sigma Integrated Rule Set (GitHub)	e4567b8b5187e55fdafa46896fe44aa16e80e8299fdf616562294969ae32c7a6	0	0
Possible emails/attachments extraction by Emotet	Den Iuzvyk	SOC Prime Threat Detection Marketplace	413ee025b8a23df869f7342778fc274599e24cfb881e26cde55b06feddae06bd	0	0
Post CVE-2017-5638 exploitation	Ariel Millahuel	SOC Prime Threat Detection Marketplace	ac7133ba82228763e38c9dece3427e679698ee3bedde0c21e00adf3e4dfa06ac	0	0
Post CVE-2017-5638 exploitation	Ariel Millahuel	SOC Prime Threat Detection Marketplace	f0750e1ec35c54a3e4b96c31c30c90992261adc3f0dbfc07f1c841b4cd0b5be0	0	0
Potential Exfiltration of Compressed Files	Greg Howell, OTR (Open Threat Research)	Sigma Integrated Rule Set (GitHub)	1211ca2125800a5536381bbbaa31e5785a63d393b5361c9c79a2fdc9327a21df	0	0
Potential Forced External Outbound DCE_RPC	SOC Prime Team	SOC Prime Threat Detection Marketplace	2b3b8e854d19405e5e6c9c31054a6c326d1039ac85adacc9d7aa4959aa5f1fc0	0	0
Potential Forced External Outbound GSSAPI	SOC Prime Team	SOC Prime Threat Detection Marketplace	19c3e23b94517f688049e3988bf887fd740097d02ec462d5b0eb20e52f2b568f	0	0
Potential Forced External Outbound NTLM	SOC Prime Team	SOC Prime Threat Detection Marketplace	aad30630b73b0f4a4236cce2c8d814e292ee13ba01bebf01326ebda63aeacc7a	0	0
Potential Forced External Outbound SMB	SOC Prime Team	SOC Prime Threat Detection Marketplace	b7eb3b4728494a3c2f99e1d09ccee9a7405011f233c531096f5ae77b9367a6c9	0	0
Potential Forced LLMNR Lookup	SOC Prime Team	SOC Prime Threat Detection Marketplace	263ef200cd98649e7eb618ce3d0700e62dfddb6368b1167c164c8437f249eaaa	0	0
Potential PetitPotam Attack Via EFS RPC Calls	@neu5ron, @Antonlovesdnb, Mike Remen	Sigma Integrated Rule Set (GitHub)	21730cbb0a1909a9d76a80acd4bde103b4ccadc42883b227a3f9568259cfbfcf	0	0
Potential RDP Exploit CVE-2019-0708	Lionel PRAT, Christophe BROCAS, @atc_project (improvements)	Sigma Integrated Rule Set (GitHub)	8b02859a07f68105c212ab8620bad0936e88ff1273a8ea016f9c1c6c6789a39e	0	0

Potential Remote Desktop Connection to Non-Domain Host	James Pemberton	Sigma Integrated Rule Set (GitHub)	4c5c4668e312589fc1aa4db734482c2b724cda2ae380d3de9dfdac43ccd99fc4	0	0
Potentially Harmful Attachment	SOC Prime Team	SOC Prime Threat Detection Marketplace	5f9b3f2dc239f570301cb831ea6671acf4414fbb82a5dc4df877925dbc1176c8	0	0
PowerShell Base64 Encoded Shellcode	Florian Roth	Sigma Integrated Rule Set (GitHub)	dbe1887e879ebc1177cca950ec8a82a43b96e7015767750a0118dc61344ccdad	0	0
PowerShell Called from an Executable Version Mismatch	Sean Metcalf (source), Florian Roth (rule)	Sigma Integrated Rule Set (GitHub)	ed7108b00b6a517dcbcd529d98b8c8e1ed551160e89bbf03699b6fe2e3b49fc2	0	0
PowerShell Decompress Commands	Roberto Rodriguez (Cyb3rWard0g), OTR (Open Threat Research)	Sigma Integrated Rule Set (GitHub)	40fcac117060a3b800bb902b404dce3cc30abc9822159a68c7414603e70e131c	0	0
PowerShell Decompress Commands	Roberto Rodriguez (Cyb3rWard0g), OTR (Open Threat Research)	Sigma Integrated Rule Set (GitHub)	46f9d269c8a2f1c1c268482b8f189bfcb71e5f354e01cbc485f42aaa02be9a64	0	0
PowerShell Downgrade Attack	Florian Roth (rule), Lee Holmes (idea), Harish Segar (improvements)	Sigma Integrated Rule Set (GitHub)	68dfd4dca345ef6d2fe87835db75f6e538426102929780a6f37dddb7730cb7e8	0	0
PowerShell Encoded Character Syntax	Florian Roth	Sigma Integrated Rule Set (GitHub)	f25494bc9c5e8430fee8451d8958642f0d15778570833a0af3f2c0cc1592a4ca	0	0
PowerShell Execution	Roberto Rodriguez @Cyb3rWard0g	Sigma Integrated Rule Set (GitHub)	77eafc1cb5e5d7dea37874133cea2270c0c4189a07aa4cf039207c99c17281fb	0	0
PowerShell Execution (Potential event manifest tampering)	SecurityJosh, Roman Ranskyi	SOC Prime Threat Detection Marketplace	f2ffe839a68caf5469d7f0c6bba1649431891460f9c08271507f594cb5080470	0	0
PowerShell Get Clipboard	Roberto Rodriguez (Cyb3rWard0g), OTR (Open Threat Research)	Sigma Integrated Rule Set (GitHub)	524490479b353ff8d877b617014d2cbb9a65d782e87caae21e923760fd2ed255	0	0
PowerShell Get-Process LSASS	Florian Roth	Sigma Integrated Rule Set (GitHub)	8fecdfab629105e4822e49c9dae2daf531f93b9b9f4a90cb0ba780ea4a09adac	0	0
PowerShell Network Connections	Florian Roth	Sigma Integrated Rule Set (GitHub)	b5e9f310ab6a8611ea1b7b788e712f0f6bf452c3092675694cf6256931874071	0	0
PowerShell Obfuscation using SecureString	Den Iuzvyk	SOC Prime Threat Detection Marketplace	a885d4a4024ecfaa6ba2d4e707d9c8f3f22ff62b6990332557b511f2f8dd3198	0	0
PowerShell PSAttack	Sean Metcalf (source), Florian Roth (rule)	Sigma Integrated Rule Set (GitHub)	229ea6fc4268ad28126e92f6f1ebd4679c50f3be77030a58b60af12fa0ef8eb3	0	0

PowerShell Remote Session Creation	frack113	Sigma Integrated Rule Set (GitHub)	2edbd80b280a70f7636ca307800e2c61b25d829eca7c992125bf15782e91f688	0	0
PowerShell Rundll32 Remote Thread Creation	Florian Roth	Sigma Integrated Rule Set (GitHub)	b6b512a36600d72d464945b37dc5edcb606a3e429979c7f50e117d9a428ebaeb	0	0
PowerShell SAM Copy	Florian Roth	Sigma Integrated Rule Set (GitHub)	f82541606097e898ede6da39077c7fe527c1fcd403d041ebe375f28d5f4339fc	0	0
PowerShell Scripts Installed as Services	oscd.community, Natalia Shornikova	Sigma Integrated Rule Set (GitHub)	1364ad75b0dc2267d0c0662c954f3be5c9215494cf31c1e20fe403ea6c3e83c3	0	0
PowerShell Scripts Installed as Services	oscd.community, Natalia Shornikova	Sigma Integrated Rule Set (GitHub)	2cc62e06802026a69ee67d8dbae18471e27c0c724a1733602613735fb6fd72e5	0	0
PowerShell Scripts Installed as Services	oscd.community, Natalia Shornikova	Sigma Integrated Rule Set (GitHub)	445aaa2d9f84a2f2f097156daf5b3f2cf8034d25addcd37e1889105ca6dad11b	0	0
PowerShell Scripts Installed as Services	oscd.community, Natalia Shornikova	Sigma Integrated Rule Set (GitHub)	467dfca5cc97071e4d713c6a6403209934b96ad6317643eef8e56b83b8134f8e	0	0
PowerShell Scripts Installed as Services	oscd.community, Natalia Shornikova	Sigma Integrated Rule Set (GitHub)	8ccccb7310714bae7f496aec46cc573dd0bc8f2794b820a3070864fbdb99fdbb	0	0
PowerShell Scripts Installed as Services	oscd.community, Natalia Shornikova	Sigma Integrated Rule Set (GitHub)	f1c32a70362f7ed2aa5c0293edb9c51408a0bdb4a1d93b8f101b2d7c38590993	0	0
PowerShell Scripts Run by a Services	oscd.community, Natalia Shornikova	Sigma Integrated Rule Set (GitHub)	014598477a00db3dbeee84e541504e310712bfb7380fe0f6c18921580f829d4e	0	0
Powershell Create Scheduled Task	frack113	Sigma Integrated Rule Set (GitHub)	60d527fe5a592cbe8e98428d1412743b909d5625ec8bc91d20e8b6ee8b36db20	0	0
Powershell DNSExfiltration	frack113	Sigma Integrated Rule Set (GitHub)	a40151c9a2ec5e5671945aceabe6ad097c67f4d30456644230d8f9a37511a161	0	0
Powershell Detect Virtualization Environment	frack113	Sigma Integrated Rule Set (GitHub)	6e1823de286f8bef414c648f5738bec3bd40700cba3765da26e6500bc2d8e387	0	0
Powershell Execute Batch Script	frack113	Sigma Integrated Rule Set (GitHub)	ece68c3b6fda1fe5c7d8707c5dd9099cf564ed0e7e7b480e97278c475f10e5a7	0	0
Powershell Exfiltration Over SMTP	frack113	Sigma Integrated Rule Set (GitHub)	b09b9f74febb3e25b3de69614b6193a2740c00fe9e7ccf5e62f503de56c5c1bf	0	0
Powershell File and Directory Discovery	frack113	Sigma Integrated Rule Set (GitHub)	febfc891e8c04ffe16ce1a9eaf5731b0a321cf42be5c06aed06252ec31cdbb79	0	0
Powershell IEX Download In Base64	Joe Security	Joe Security Rule Set (GitHub)	47700446a254048704b602b4820482299b526c610cd8cfa3a164f19784195ba9	0	0
Powershell Install a DLL in System32	frack113	Sigma Integrated Rule Set (GitHub)	51fc69e23d6cd3acb20d821dbe95596fb6d8cc314866c51a6a23033b83818ee8	0	0

Powershell Keylogging	frack113	Sigma Integrated Rule Set (GitHub)	ed239970ee8d5e197f594aacc2fd6f6f6d3dae189b2b2aaea8c2f5d100939e42	0	0
Powershell Launched By Winword	Joe Security	Joe Security Rule Set (GitHub)	ed5457ba384a36ef60723b4fa6a186fb0048d8947aa3ad64ee30284ed1b8b658	0	0
Powershell LocalAccount Manipulation	frack113	Sigma Integrated Rule Set (GitHub)	b3caa02d87fceb141c3eb2e3715d1290976d6fdb56070c03362cd1fb6808f95d	0	0
Powershell Store File In Alternate Data Stream	frack113	Sigma Integrated Rule Set (GitHub)	dabcdcdecebe87ed3085b193d3ed09029f3556672622b42d5759dc816f0b6173	0	0
Powershell Suspicious Win32_PnPEntity	frack113	Sigma Integrated Rule Set (GitHub)	7cf1e08df2c1e71b9ecbab0ba652d8d7adc890f53db8c630b859d32064f3eb3a	0	0
Powershell WMI Persistence	frack113	Sigma Integrated Rule Set (GitHub)	d31a6afb995dab0473ccaefae327155cd4ba87afbabf6a872553475c50bb7182	0	0
Powershell download file and shellexecute	Joe Security	Joe Security Rule Set (GitHub)	f5d1804b36d00e52057d36ac92f04d0f6434083c9a000d916380a1c01f1c01c2	0	0
Powershell download file from base64 url	Joe Security	Joe Security Rule Set (GitHub)	1972682562285c42b2e838f027388654e2a212ce987a525c6d95784c7abb2d786	0	0
Powershell launch wscript	Joe Security	Joe Security Rule Set (GitHub)	2daf820a836b6725473b0e6ef3075aff5f25c39f1613ea91e098fa179d7a30a6	0	0
Powershell load assembly from internet	Joe Security	Joe Security Rule Set (GitHub)	e4b3ed1b620f60e713a7faf984b8fa2b870914dfe494ac56f99bffbb5133e11f	0	0
Powershell load assembly from registry	Joe Security	Joe Security Rule Set (GitHub)	5388b2590b9ed2f4d530c9eac824a7ddde5512e4224c1a64b5a6da98fee0fbeb	0	0
Powershell sleep and launch executable	Joe Security	Joe Security Rule Set (GitHub)	1f9a2d4cfcbbab989273e05d81a5ab3ca1e580cddc3b839707dc19d6731f93a9	0	0
Powerview Add-DomainObjectAcl DCSync AD Extend Right	Samir Bousseaden; Roberto Rodriguez @Cyb3rWard0g; oscd.community	Sigma Integrated Rule Set (GitHub)	d52fe14049b24733e329f274322c156982d55e21e66e25758d8e7bc91aa8c4fe	0	0
Predator The Thief (command-line detection)	Ariel Millahuel	SOC Prime Threat Detection Marketplace	1f8699a3474b828805b77c6ed86f5b86087391365eed233992d6ac3d289bc822	0	0
Predator The Thief (command-line detection)	Ariel Millahuel	SOC Prime Threat Detection Marketplace	5422d5ef2c42f4981afdae1e5ad6c5159df8099190c17da497f76919f0cfbcfc	0	0
Prefetch File Deletion	Cedric MAURUGEON	Sigma Integrated Rule Set (GitHub)	c865945cbecb1d16e71f70bbaf2926d63799a2a7a109ded595203301bc777f0d	0	0

PrintNightmare Powershell Exploitation	Max Altgelt, Tobias Michalski	Sigma Integrated Rule Set (GitHub)	9994b75f6dfdb006404fdee33726452e641b8b07bbd4b6c79f61249f3ef3c1d3	0	0
Printer Service Modification	Den Iuzvyk	SOC Prime Threat Detection Marketplace	16ca1eb37f09dfe266d2553018aa5c7f236b3fe27572ab1215a0f4fa1302f765	0	0
PrinterNightmare Mimimkatz Driver Name	Markus Neis, @markus_neis, Florian Roth	Sigma Integrated Rule Set (GitHub)	093a9d8f83c2689c873979bf87e2d4d8082037d9d782bf32ca870205e3992ffc	0	0
Privilege Escalation Preparation	Patrick Bareiss	Sigma Integrated Rule Set (GitHub)	9a8a7c1b00c147f05b82612499df919b5a2fd429c3bb0c64866b947ab39671e8	0	0
ProLock Ransomware Behavior	Ariel Millahuel	SOC Prime Threat Detection Marketplace	6f434a5ccf3c234c99a17756d76f7690d09d6c565f238cb77186e687baae2278	0	0
ProLock Ransomware Behavior	Ariel Millahuel	SOC Prime Threat Detection Marketplace	7a7f19c4b3dd631c48ffccc302c2a36f81088073798fbc563b9c645f20f5fb19	0	0
Process Discovery	Ömer Günal, oscd.community	Sigma Integrated Rule Set (GitHub)	0085bf33f8f7fe01581d6bf7c6463a6396d9843436e5c10f0da6186171d0b9c8	0	0
Process Dump via RdrLeakDiag.exe	Cedric MAURUGEON	Sigma Integrated Rule Set (GitHub)	5cdfd68738b7b527a6fe7958d3484f9854aad921a6148f39e7a6851417647792	0	0
ProcessHacker Privilege Elevation	Florian Roth	Sigma Integrated Rule Set (GitHub)	2149649a6e304c127fc371a6342964619569b0ba1bcd812d2381173324736db4	0	0
Processes Accessing the Microphone and Webcam	Roberto Rodriguez (Cyb3rWard0g), OTR (Open Threat Research)	Sigma Integrated Rule Set (GitHub)	b956cdd9fcde5ccf08a7776e2989b0bfad944b79dd75e20c11d38bb24dbfbfc6	0	0
Processes accessing the camera and microphone from suspicious folder	Den Iuzvyk	SOC Prime Threat Detection Marketplace	7b3cfa10cc9723d7c4fa50a1b3b77c1b9689fe594822023e09771ed6cbdce53f	0	0
Program Executions in Suspicious Folders	Florian Roth	Sigma Integrated Rule Set (GitHub)	22c7d8bc06e4a35a3045524848896a9e21533b194fcdbca7ed641a2a8fa7a4de	0	0
Protected Storage Service Access	Roberto Rodriguez @Cyb3rWard0g	Sigma Integrated Rule Set (GitHub)	67aa4f89c2b8f751b7be7a7123233e4baca5464a20c273bfce1d81fcd1589781	0	0
ProtocolHandler.exe Downloaded Suspicious File	frack113	Sigma Integrated Rule Set (GitHub)	b886d124810a581d5017eaa5d5eb0d9d6835919fc18f7f9b4c5939e0fba81825	0	0
Proxy Execution via Wuauclt	Roberto Rodriguez (Cyb3rWard0g), OTR (Open Threat Research), Florian Roth	Sigma Integrated Rule Set (GitHub)	d8bd87c5bebb059ab6031d2484dd86fc3c0f14c4dcadd27895205b1267ab7658	0	0

ProxyLogon MSExchange OabVirtualDirectory	Florian Roth	Sigma Integrated Rule Set (GitHub)	0c6a87dbb998eae574f7a8317bcb860cd4acabdaef209f25c80bc5fb2e54d5af	0	0
ProxyLogon Reset Virtual Directories Based On IIS Log	frack113	Sigma Integrated Rule Set (GitHub)	bd2871cff93ff62a864fd7b4e13617d202605e22089c562c84540f8a8d25392b	0	0
Ps.exe Renamed SysInternals Tool	Florian Roth	Sigma Integrated Rule Set (GitHub)	508460a99a052814512ff212e0f6f3bb5e1d3de21c79ff3e24f6d05463448b1d	0	0
PsExec Pipes Artifacts	Nikita Nazarov, oscd.community	Sigma Integrated Rule Set (GitHub)	d5a93fd832fa665cec13e7681c2db65b6feb3c719a2ea43cf408a884503fa0b3	0	0
PsExec Tool Execution	Thomas Patzke	Sigma Integrated Rule Set (GitHub)	1518bae3460d45d1166480cfdbf8f19603549ebe5930c037d7001c15d30c322b	0	0
PsExec Tool Execution	Thomas Patzke	Sigma Integrated Rule Set (GitHub)	4b9b15bf02c7c8b9fd6f4a020a6318957101b14776b4e6ab6375abc57ce2d101	0	0
PsExec Tool Execution	Thomas Patzke	Sigma Integrated Rule Set (GitHub)	7f0d5bf894afae6dab8a011197896b06675a9c3089b1b1ffffc6efca6e2eae29	0	0
PsExec Tool Execution	Thomas Patzke	Sigma Integrated Rule Set (GitHub)	8cab50a6d456060d4de01cc18fbe85b349cefb689386336cc8fe05f8854c9f31	0	0
PsExec Tool Execution	Thomas Patzke	Sigma Integrated Rule Set (GitHub)	a140e6a4ca5fb32569012656b50cf8d077ed195688bccda1b6cd6a7bcc32aea0	0	0
PsExec Tool Execution	Thomas Patzke	Sigma Integrated Rule Set (GitHub)	b677aa8615b26b7047d758b5e937e92d67219dafb0f4168698b819a2fd7dd925	0	0
PsExec Tool Execution	Thomas Patzke	Sigma Integrated Rule Set (GitHub)	cbdad3dc58dae0d5b7ccf82a897b981e992a31f8f2a45d86fb8554c1c5bafdb4	0	0
PsiXBot Malware behavior	Ariel Millahuel	SOC Prime Threat Detection Marketplace	63753d667c596fd59cca6de277c7a4f8062dd47fb2ae19a1efdda0cbb8d7692b	0	0
Psr.exe Capture Screenshots	Beyu Denis, oscd.community	Sigma Integrated Rule Set (GitHub)	959d7cd5c3bea11a5cd183693349bf492efb4f2d787903a7c74a5c24cbc60b34	0	0
Publicly Accessible RDP Service	Josh Brower @DefensiveDepth	Sigma Integrated Rule Set (GitHub)	84b66d47b8f699ef0111cfc0d68cdc2be9451bc55091156ee5cbb23cce133b76	0	0
Pulse Connect Secure RCE Attack CVE-2021-22893	Sittikorn S	Sigma Integrated Rule Set (GitHub)	ab8e48d7ca9cf33f92ac8c77e2ba4f029ae209d2bc21b576b7d3870ff51a9215	0	0
Pulse Secure Attack CVE-2019-11510	Florian Roth	Sigma Integrated Rule Set (GitHub)	a4eac94c575b5162661af9888cf6bf6e1c6b2765b9129be15a313f4f596de87b	0	0
PwnDrp Access	Florian Roth	Sigma Integrated Rule Set (GitHub)	3c12c79f550c4f0f3128094db8b532ddb7997afc5d22889d546ed3c68317e67c	0	0

Python Initiated Connection	frack113	Sigma Integrated Rule Set (GitHub)	e4d5f1be0673fa786cc8379c15338af08cdd11eed433bead9e801d6204d42a2d	0	0
Python SQL Exceptions	Thomas Patzke	Sigma Integrated Rule Set (GitHub)	c355e46fd180c68033fae6aa264ce176fc46107a47b4ad0a22812ae40f1fd65b	0	0
Pyvil RAT	Ariel Millahuel	SOC Prime Threat Detection Marketplace	1946000b4b23e17072b4e16f69f6d214b8cd744492cfc3d809c91c0250a9329a	0	0
Qealler Detection Rule	Ariel Millahuel	SOC Prime Threat Detection Marketplace	c272bf0614a45f345c008e393b47040de6ef75f4a3e3494853f36aa9768f0736	0	0
QuarksPwDump Clearing Access History	Florian Roth	Sigma Integrated Rule Set (GitHub)	d5fafba749f09175307d78b0d786f5482b76b825bb977157b90e432409119ff4	0	0
QuarksPwDump Dump File	Florian Roth	Sigma Integrated Rule Set (GitHub)	4517db7f1f005bd0a18fc8081dbef15a21dede187d618c62699e3b1d8668580b	0	0
Quick Execution of a Series of Suspicious Commands	juju4	Sigma Integrated Rule Set (GitHub)	ed973bd3154186b4b9179b400d5cad9f28291698fa066588f22e9cc1fb5f8ed9	0	0
Qulab Trojan (Covid-19 abuse)	Ariel Millahuel	SOC Prime Threat Detection Marketplace	15e1323de6b754fd8ed09a65a9756cee2a8cab604d50013ef15dfb651b0154ef	0	0
Qulab Trojan (Covid-19 abuse)	Ariel Millahuel	SOC Prime Threat Detection Marketplace	36a825331394fd916bee36fdbd94d6fc383f14774529b3c9facc40eb7f1ad066	0	0
Qulab Trojan (Covid-19 abuse)	Ariel Millahuel	SOC Prime Threat Detection Marketplace	82a3dfab9619a2d77e3d28664ef300769a61d65c3e3b1739dda336dc4af6cee0	0	0
Qulab Trojan (Covid-19 abuse)	Ariel Millahuel	SOC Prime Threat Detection Marketplace	d2fd35d9e091008717a1ddb2ba521ecdd25ba3b5491c719179b54b0b099349cb	0	0
RATicate Group behavior	Ariel Millahuel	SOC Prime Threat Detection Marketplace	d107f1b47b43fc725572a5dc8b69c66ee12cc6062ee0a67c4a35ac7cb778d95b	0	0
RDP Dashboard (Overview Query)	SOC Prime Team	SOC Prime Threat Detection Marketplace	71a226733f7f12aa303328c542409ef9b1016c750c4a8f78c86a615e3da3cf6a	0	0
RDP Hijacking. Last logged-on user changed.	Den Iuzvyk	SOC Prime Threat Detection Marketplace	5af33fb9edf5af983870138dd17270a22ec3c4046fa58eb0a27c209c5951b03c	0	0
RDP Login from Localhost	Thomas Patzke	Sigma Integrated Rule Set (GitHub)	3895d9722610797e2eb09dca91e1a804bb4eec6cc1ca5b81a937f13e4adc81f6	0	0

RDP Over Reverse SSH Tunnel	Samir Bousseaden	Sigma Integrated Rule Set (GitHub)	0fc2c398ce1141e654d51055a3df9803bd5e0031fec24100cf28a042b9b9df0a	0	0
RDP Possible Non User Login, Abnormal Screen Resolution	SOC Prime Team	SOC Prime Threat Detection Marketplace	ff0ab5b6cd3ebd7aeade8aa8b55790d7096ac7ba96d54a8ed6587d0c5f25da39	0	0
RDP over Reverse SSH Tunnel WFP	Samir Bousseaden	Sigma Integrated Rule Set (GitHub)	9ac83d94dd47e5c8ac03b8678d0569ce163716d072aa690ee44b67d5ae12510a	0	0
REvil Kaseya Incident Malware Patterns	Florian Roth	Sigma Integrated Rule Set (GitHub)	fc2108a980d79a05e920b28c15d995fa0652a1dda317ce1fa22da44d694541d3	0	0
Racoon malware detection	Ariel Millahuel	SOC Prime Threat Detection Marketplace	c5bc56057878575689e1e8062054f20ea3f118c0e52f17403445a2bb339ea3f9	0	0
Racoon malware detection	Ariel Millahuel	SOC Prime Threat Detection Marketplace	ef297eac8d295b521dbb1e207df57db1a1e62453c926eed3fd6bfc9460b6f6ed	0	0
Ransom X Behavior	Ariel Millahuel	SOC Prime Threat Detection Marketplace	016eb94fa1071faeb02a09e52d8d7e64b3702d3e8cdbb12683eb99da9b3b4889	0	0
Rare Scheduled Task Creations	Florian Roth	Sigma Integrated Rule Set (GitHub)	95b4be8473d9667e7c486d85a5a38d5d2a0fe7d4716c86448e7f15cbbd167c80	0	0
Rare Schtasks Creations	Florian Roth	Sigma Integrated Rule Set (GitHub)	52bcf8d53a2e9861ebf212d6fb5c8c8000ff4ad6aef25806a201b8115c7c5852	0	0
Rare Service Installs	Florian Roth	Sigma Integrated Rule Set (GitHub)	b4520bca6240f5cea8758ebfe31a5de0d007fb4ee971d1504eb4afaf9aaaf107	0	0
Rare Subscription-level Operations In Azure	sawwinnnaung	Sigma Integrated Rule Set (GitHub)	73526ac545356edf8d7771865258ba2671d34ed6c9c1e4e89dda4f64833fc5ca	0	0
Rasautou.exe execution.	Den iuzvyk	SOC Prime Threat Detection Marketplace	a34ca7a1c15bec9b90de6c46395088c6d253b54b770a60de680af7cd9943c085	0	0
Raw Disk Access Using Illegitimate Tools	Teymur Kheirkhabarov, oscd.community	Sigma Integrated Rule Set (GitHub)	a89a26f2bdfeb3c1f3e5ad8acf0a4a51ef45bb9859403cee7f91739b74d79dec	0	0
Raw Paste Service Access	Florian Roth	Sigma Integrated Rule Set (GitHub)	df29e480a1da07c9864f41b5f7bf34765c1d2ea9af15046dd3aec14367536f8f	0	0
Rclone Config File Creation	Aaron Greetham (@beardofbinary) - NCC Group	Sigma Integrated Rule Set (GitHub)	76a893bef53690d6ce9764427bd65300fe3d50440086afa77a1b15d3f777d9c1	0	0

Rclone Execution via Command Line or PowerShell	Aaron Greetham (@beardofbinary) - NCC Group	Sigma Integrated Rule Set (GitHub)	1f67c2169d6cb6e70c9bac22b944ff64fa959097dba5e8b963852d6c58fc8e1a	0	0
RdrLeakDiag Process Dump	Florian Roth	Sigma Integrated Rule Set (GitHub)	2d7bbe44a845a98779776b889cc1c74c4e424725151f7aae9eb73be3b70f4dac	0	0
Reconnaissance Activity	Florian Roth (rule), Jack Croock (method), Jonhnathan Ribeiro (improvements), oscd.community	Sigma Integrated Rule Set (GitHub)	e4f2c05322c3be28c50da39003b02312523eac5e2b83bf820349a063d6e18167	0	0
Reconnaissance Activity with Net Command	Florian Roth, Markus Neis	Sigma Integrated Rule Set (GitHub)	a6adbabf733244eb498c551ed9ba1387ba2997a06332e517c89b955160edea9a	0	0
RedLine Stealer (COVID-19 Campaign)	Ariel Millahuel	SOC Prime Threat Detection Marketplace	1d84ec4dfb91d5af2a7692cc37b5fe558279fe33b3b6ae373987f71ba7df5e8b	0	0
RedLine Stealer (COVID-19 Campaign)	Ariel Millahuel	SOC Prime Threat Detection Marketplace	4f3bb7ac672f51adf9d944139cabbb66f52ef10a9abcfea24b65ba3c1cfc1252	0	0
RedMimicry Winnti Playbook Dropped File	Alexander Rausch	Sigma Integrated Rule Set (GitHub)	d6c33aea206d318b0bebc06af8753c1497ad0abc154f4b62be36cc3893897876	0	0
RedMimicry Winnti Playbook Execute	Alexander Rausch	Sigma Integrated Rule Set (GitHub)	2c7173d7fd6c440ff57e03f67e736353c0d299567579d74292ce79ddb87df5b7	0	0
RedMimicry Winnti Playbook Inject	Alexander Rausch	Sigma Integrated Rule Set (GitHub)	13e4345b125509a08fb73bfaf0cf1f2320148020c7e45ab1cf8b47ef011db176	0	0
RedMimicry Winnti Playbook Registry Manipulation	Alexander Rausch	Sigma Integrated Rule Set (GitHub)	86b53f7f939e5987f63a77e6b31ad7f58f28592bead63b31894216d116ecd120	0	0
Redaman RAT	Ariel Millahuel	SOC Prime Threat Detection Marketplace	1544d96bd9a34be41d2e2c976346e9c6ced04c82b6490ad0606f48640531400a	0	0
Redaman RAT	Ariel Millahuel	SOC Prime Threat Detection Marketplace	ef28bd95f54d82f5f8245ca837359781d3cfb48f7f3e7401ef6bbebff3dbea8e	0	0
ReflectiveLoader	Joe Security	Joe Security Rule Set (GitHub)	f972e2d6ad7812da19ebfc6d0e73c5dba52f470a48646159facd3ffa24e4d8df	0	0
RegAsm connects to smtp port	Joe Security	Joe Security Rule Set (GitHub)	4ff400ac692a7dca2bab429bae7ab6cb7f2bae4525b1ba9420ef0b5137ebf1d2	0	0
Regedit as Trusted Installer	Florian Roth	Sigma Integrated Rule Set (GitHub)	40b85d8543b5dc00f22211f0dd2f05012b435d38fd8e170370986c189a9b39f2	0	0
Register dll at autostart location via regsvr32	Joe Security	Joe Security Rule Set (GitHub)	6e3d105ee67957d16975a4ff8dcbbb38b9c8dd21ccd2dc07e9c194a6c153ba98	0	0

Register new Logon Process by Rubeus	Roberto Rodriguez (source), Ilyas Ochkov (rule), oscd.community	Sigma Integrated Rule Set (GitHub)	f7cacbd7c0676adf78318bb6d9de688bc97c4aa69d5afa2f1d55866ce06b3867	0	0
Registry Dump of SAM Creds and Secrets	frack113	Sigma Integrated Rule Set (GitHub)	3e6aec9c264981c1c738cf2bb29a907f7fc01867b91cf31a6d4ba46d35129230	0	0
Registry Entries For Azorult Malware	Trent Liffick	Sigma Integrated Rule Set (GitHub)	4ad66d0e46670f58101e391ac2d114fc7e3b06243c7b81888faf05840934d168	0	0
Registry Parse with Pypykatz	frack113	Sigma Integrated Rule Set (GitHub)	e9fa03c18cdfe5568dbbe75862d4ab693fba40025a197a2021d576f54e3eaf76	0	0
Registry Persistence Mechanism via Windows Telemetry	Lednyov Alexey, oscd.community	Sigma Integrated Rule Set (GitHub)	ca3672e906735c6f2aa0f7aa73bd9796d29cd4f03ef8541b6bb17a0518502b51	0	0
Registry Persistence Mechanisms in Recycle Bin	frack113	Sigma Integrated Rule Set (GitHub)	661375a6a064f858d66665c13895d00ce56bb356ccda48cbc40727b9b6f4e220	0	0
Registry-Free Process Scope COR_PROFILER	frack113	Sigma Integrated Rule Set (GitHub)	f566e9fbc25004f90a7c502406100ff744d00b85ad929d568a47872238e1af75	0	0
Regsvr32 Network Activity	Dmitriy Lifanov, oscd.community	Sigma Integrated Rule Set (GitHub)	bcbb15efbb568b9a302a100e8cea3e019b9b8d04fbcd5d17a4439b424fe30e59	0	0
Relevant ClamAV Message	Florian Roth	Sigma Integrated Rule Set (GitHub)	5105b3bed3732f01c5689b867054b8ff7c5645b8ef18842d89506409437037e9	0	0
Remcos	Joe Security	Joe Security Rule Set (GitHub)	b50b6d86173debc4d608b981e7d6b5136092c515286d20c0eafcce3b7c411dde	0	0
Remote Code Execute via Winrm.vbs	Julia Fomina, oscd.community	Sigma Integrated Rule Set (GitHub)	38b612a88929aab8a1ee49b6e7616c06ee06da5daeb4e09a215f9c865d870910	0	0
Remote Desktop From Internet (via audit)	SOC Prime Team	SOC Prime Threat Detection Marketplace	96a069aeb5c6003d5e4ffe4aaf6d30be7b05d356c661367a348514a7c2c5beac	0	0
Remote Desktop Protocol Use Mstsc	frack113	Sigma Integrated Rule Set (GitHub)	257b13d5b7127756fd3872ae69c87afe430e3a8d7933cef87a19e05fc1658d70	0	0
Remote File Copy	Ömer Günal	Sigma Integrated Rule Set (GitHub)	1cde4fe7d0cd62ea67b1474e3fd6fe9a6931bd8af934f3a5e9b8c134d90bd7b5	0	0
Remote PowerShell Session	Roberto Rodriguez @Cyb3rWard0g	Sigma Integrated Rule Set (GitHub)	1cef3fd3818cc81e0b14412af94c6998bf6abb8a8d1f5ea344f2457a1f880d4c	0	0
Remote PowerShell Session	Roberto Rodriguez @Cyb3rWard0g	Sigma Integrated Rule Set (GitHub)	48a36a2180adc9f076d8a15c870bb4583783f4984a012d21d17fe64439511244	0	0
Remote PowerShell Session	Roberto Rodriguez @Cyb3rWard0g	Sigma Integrated Rule Set (GitHub)	d2a86c0c533d4197640ec3742c4054be9017d215efd16a8d462456a23db8a109	0	0

Remote PowerShell Sessions Network Connections (WinRM)	Roberto Rodriguez @Cyb3rWard0g	Sigma Integrated Rule Set (GitHub)	6590a6d9a0f48ca7180efed5cdf2aadb0d828795034779b5860a47b16c811835	0	0
Remote Registry Management Using Reg Utility	Teymur Kheirkhabarov, oscd.community	Sigma Integrated Rule Set (GitHub)	89100186dc0ee80d9ed100f7046a9a131a40270385fdcd8994b102aa36f06ae5	0	0
Remote Service Activity via SVCCTL Named Pipe	Samir Bousseaden	Sigma Integrated Rule Set (GitHub)	046ceb0cf9b6078b4d6bd583847ee8a30ecc082fb018cd5de8af33d9203a2519	0	0
Remote Task Creation via ATSVC Named Pipe	Samir Bousseaden	Sigma Integrated Rule Set (GitHub)	fde467e8c3cd6651030d60821479ab66e029e1c6541daa5a16b3611959c7b529	0	0
Remote Task Creation via ATSVC Named Pipe - Zeek	Samir Bousseaden, @neu5rn	Sigma Integrated Rule Set (GitHub)	236138dfbc31327293697d57944480418437a91071cb427e4f48f5755f2319df	0	0
Remote Task Creation via ATSVC Named Pipe - Zeek	SOC Prime Team	SOC Prime Threat Detection Marketplace	92258356e34556c631e9519ae4be82df3ecb4ccaf390d03c459a5df6a3705804	0	0
Remote WMI ActiveScriptEventConsumers	Roberto Rodriguez (Cyb3rWard0g), OTR (Open Threat Research)	Sigma Integrated Rule Set (GitHub)	820499826df98e19e14c24dac63db285b19863b3c8af168e63e83a6df9d864d8	0	0
Remote execution via sql extended stored procedure xp_cmdshell	Den Iuzvyk	SOC Prime Threat Detection Marketplace	375cb93c2bb69dad51d360b1936e69ba1b68424e34970ff0b9b9c6b9c98f989f	0	0
Remove Account From Domain Admin Group	frack113	Sigma Integrated Rule Set (GitHub)	2b323eb1de293c4dbf91041f23c3507c4aaf71c4bc36b04ccb8fc5731995a398	0	0
Remove Exported Mailbox from Exchange Webserver	Christian Burkard	Sigma Integrated Rule Set (GitHub)	bdfd4f3c151a5adc98ef77f6ac75cdfd440bb51043d01c27b94e2a5a63f4f4de	0	0
Remove Immutable File Attribute	Jakob Weinzettl, oscd.community	Sigma Integrated Rule Set (GitHub)	e28706c6a53a1d6ff572114998015648c27e89167c10379905d0cbc361712d41	0	0
Renamed MSHTA launching html	Joe Security	Joe Security Rule Set (GitHub)	eef2c27cd98b92f6ac98d5b6fa781fc1ef9fcb1fc12f0e72db41aa0308a33ad7	0	0
Renamed Powershell	Harish Segar, frack113	Sigma Integrated Rule Set (GitHub)	a470fbf97e0f7a4d42fd59ad6332c7521f57d919e725bc61c84ea7ee2e451426	0	0
Renamed ZOHO Dctask64	Florian Roth	Sigma Integrated Rule Set (GitHub)	0d4118d9a3bcc02c529a5322214c7e45fc4ad36aec272ddc3772230315188701	0	0

Replace Desktop Wallpaper by Powershell	frack113	Sigma Integrated Rule Set (GitHub)	0f1aa746beaad206dc77bb8542a498967f1fb26e0677a3fdf90cfd5cf5c22a75	0	0
Request A Single Ticket via PowerShell	frack113	Sigma Integrated Rule Set (GitHub)	7b7092f37f648c00a538947e2cb178b5c50e31e552b8bff8251ffaf4d4e49a68	0	0
Restore Public AWS RDS Instance	faloker	Sigma Integrated Rule Set (GitHub)	1a859b52b21821dc4f0a817ce7326759948e5b2065d00479202bffad5175fc08	0	0
RottenPotato Like Attack Pattern	@SBousseaden, Florian Roth	Sigma Integrated Rule Set (GitHub)	5389e8a683229a6fb7e29cc17dff4e0811d8239798f60128c6f63871d4bececd	0	0
Rubeus Hack Tool	Florian Roth	Sigma Integrated Rule Set (GitHub)	74f9a93f96bad4ba440f105a789ab5905ef284191baa105737e7ac861d13bd44	0	0
Ruby on Rails Framework Exceptions	Thomas Patzke	Sigma Integrated Rule Set (GitHub)	b3e15ce29c0578285d8af1d8092873431b79ef0d74202d48d1b55dccaaa861de	0	0
Run CertUtil from suspicious location	Joe Security	Joe Security Rule Set (GitHub)	d10fe75d3edfe38a67c070614eaf661fe0d608b0d0b81ed88ad9673766b25eba	0	0
Run Once Task Configuration in Registry	Avneet Singh @v3t0_, oscd.community	Sigma Integrated Rule Set (GitHub)	0e31671617efd7f7d79bdc60259af085a8ceadd59619e28e3f3d57d90ed1501d	0	0
Run PowerShell Script from ADS	Sergey Soldatov, Kaspersky Lab, oscd.community	Sigma Integrated Rule Set (GitHub)	b0a64287d64cf778925e076c13aae743cdb5da1000efa636d98364e0e42edf83	0	0
Run PowerShell Script from Redirected Input Stream	Moriarty Meng (idea), Anton Kutepov (rule), oscd.community	Sigma Integrated Rule Set (GitHub)	64fc279e6738ccc6db9319777992497 29de73acffc5034f83e3094bc34ab2011	0	0
Rundll32 Internet Connection	Florian Roth	Sigma Integrated Rule Set (GitHub)	4725cdcf2dfdd90c3aa0d331fae77d6ac8021c254701744a01444af04e9a0e69	0	0
Running Chrome VPN Extensions via the Registry 2 VPN Extension	frack113	Sigma Integrated Rule Set (GitHub)	09e6a0408f2c734eee75232ab5bc1dd09b1be6e414b3e10b4d2f9efdd69c2311	0	0
SAM Dump to AppData	Florian Roth	Sigma Integrated Rule Set (GitHub)	cdbc62d2dc895924c046364f27452f287723a2b72efb654ba041280d91f69acd	0	0
SAM Registry Hive Handle Request	Roberto Rodriguez @Cyb3rWard0g	Sigma Integrated Rule Set (GitHub)	d98473553a7ba81cf9e2ce17e305853d35be853a95ef549fc405dfa67f646391	0	0
SCM Database Handle Failure	Roberto Rodriguez @Cyb3rWard0g	Sigma Integrated Rule Set (GitHub)	4b5721fb3c1349a8cd1a6f9e87bed2fef39d379476067fe7fe05c685e4a9a382	0	0
SCM Database Privileged Operation	Roberto Rodriguez @Cyb3rWard0g	Sigma Integrated Rule Set (GitHub)	30a1135097fc1ebdc8fe0b030918fe2ad05ad4512d17062d8d1920bdd5cfbdbb	0	0
SILENTTRINITY Stager Execution	Aleksey Potapov, oscd.community	Sigma Integrated Rule Set (GitHub)	0f63070b903766c40f1681e44325de9e396c2b6dd03613b2686896de828564fd	0	0

SILENTTRINITY Stager Execution	Aleksey Potapov, oscd.community	Sigma Integrated Rule Set (GitHub)	8275c8ed59f78788721cb0f9d2fe01fae3fbfd381cd3c846fe2715c4a5f8adfc	0	0
SILENTTRINITY Stager Execution	Aleksey Potapov, oscd.community	Sigma Integrated Rule Set (GitHub)	982e0890a48832865614790 7a9d7da438f6a9b5f133b904 17b42dd585d158a15	0	0
SILENTTRINITY Stager Execution	Aleksey Potapov, oscd.community	Sigma Integrated Rule Set (GitHub)	d6d031ceeda5d6a3d7194bd6ec4d67e5ffb9cc743448939fdf278463bdd3e686	0	0
SILENTTRINITY Stager Execution	Aleksey Potapov, oscd.community	Sigma Integrated Rule Set (GitHub)	e20a4ca9a2ec3dbe28c1851ecdb7656f0b386147843cdb3a7f3d749bfb40defd	0	0
SMB Create Remote File Admin Share	Jose Rodriguez (@Cyb3rPandaH), OTR (Open Threat Research)	Sigma Integrated Rule Set (GitHub)	8ca9660ea1755b4e1702a1cae3092454355f15fc519799fdb87d3e6839afa23c	0	0
SMB Spoolss Name Piped Usage	OTR (Open Threat Research), @neu5ron	Sigma Integrated Rule Set (GitHub)	01306ab05e6ee3fec1a74538de482f1e109754346730be0a73742b46a7c7eaeb	0	0
SMB single file created then deleted successively	SOC Prime Team	SOC Prime Threat Detection Marketplace	7ffa016b10d3241bd89a2006ec066c969c740b97ae3cf7ec5cc91eabf2c6335d	0	0
SMBv3 Compression Enabled	Den Iuzvyk	SOC Prime Threat Detection Marketplace	5f65bceb308a9da7f66986e86311c701f4f34184d1833cfc7e465767fb18a102	0	0
SMInit exploit chain	Den Iuzvyk	SOC Prime Threat Detection Marketplace	e0fca2cc0e2ed43fc1a0c7b399ded68159180c4f82074a3f3124e26c3139fc6e	0	0
SMTP Email containing NON Ascii Characters within the Subject	SOC Prime Team	SOC Prime Threat Detection Marketplace	5b50e56fccf5b9b41516c2fc14cbfb85fad941e5eacb051891a2493db49fac93	0	0
SOURGUM Actor Behaviours	MSTIC, FPT.EagleEye	Sigma Integrated Rule Set (GitHub)	225f115c0a824b3ec735568b05a49394fa6da38bcdc9e2f71661b34a9bde1c53	0	0
SQL Client Tools PowerShell Session Detection	Agro (@agro_sev) oscd.communitly	Sigma Integrated Rule Set (GitHub)	8e776e236be945ae976b2513cef49318e8986b57ab334e2a8f2a9968f4a3081d	0	0
SSH Inference Abnormal Client Activity	SOC Prime Team	SOC Prime Threat Detection Marketplace	213b04a00fc3394df6cb347b642ceb29f5e7294a1d6d7203e21998962369643a	0	0
SSHD Error Message CVE-2018-15473	Florian Roth	Sigma Integrated Rule Set (GitHub)	5ac7c90edd2ba8133a86c284d95dae84b58026895599a4943646e0e39367e995	0	0
STOP Ransomware and Vidar Ransomware detection	Ariel Millahuel	SOC Prime Threat Detection Marketplace	4ae55153d32cc3b88c7e99d12dbcc4db828e7f96ec3ccbe3b8f662ef4d09e2ef	0	0

STRRAT Behavior (Sysmon Detection)	Ariel Millahuel	SOC Prime Threat Detection Marketplace	37be2d5ff063bab1272d9db26a35c83920a7ad21e155ae6c12c1730446b5194d	0	0
SVCHOST Credential Dump	Florent Labouyrie	Sigma Integrated Rule Set (GitHub)	bfad2de2a3ff697a6170b489903df374d7555714e903a5cd764894bec8d7b4df	0	0
Sakula RAT	Ariel Millahuel	SOC Prime Threat Detection Marketplace	dacddd5435eda2fc54dcf6d585d0e82a0379e27c838a82bebc8ec9f0c0ac9921	0	0
SamoRat Behavior (sysmon detection)	Ariel Millahuel	SOC Prime Threat Detection Marketplace	2fbdd381a1c20671e2c9bd733e716a02c99a470023981c60de3e3402ff08313f	0	0
Sapphire Ransomware (Sysmon detection)	Ariel Millahuel	SOC Prime Threat Detection Marketplace	af5ee1ff302412603f190ad74d459219970f99e1b5a92d952a2e953f522b38c3	0	0
Scanner PoC for CVE-2019-0708 RDP RCE Vuln	Florian Roth (rule), Adam Bradbury (idea)	Sigma Integrated Rule Set (GitHub)	6b75b0b00b5529a6a6d3fcf1ff03341ca43c3fa7fdfcc055f26dd0ba221f2213	0	0
Scarab Ransomware	Ariel Millahuel	SOC Prime Threat Detection Marketplace	e1354c1cc16fda38432e3dd01a191f253341fe937e23156238d85e90d8191395	0	0
Schedule Task Access or Manipulation over SMB	SOC Prime Team	SOC Prime Threat Detection Marketplace	c155230c5fcc90d90646898aa82112b6f73ac2e0dc430ad9dce7826e28297cdf	0	0
Schedule script as task	Joe Security	Joe Security Rule Set (GitHub)	80a5b002421fe7261fe436fe34fde2f1e2a0b5b1d5fb7fee3b2afe02f76952ba	0	0
Scheduled Cron Task/Job	Alejandro Ortuno, oscd.community	Sigma Integrated Rule Set (GitHub)	17e54e203e8a8aa2c9b914202cbafe7a371b6019f97729b83dc10a8f643dc884	0	0
Scheduled Cron Task/Job	Alejandro Ortuno, oscd.community	Sigma Integrated Rule Set (GitHub)	572b438b19c769d86cabf9aef66e7f6d1cadfa28c31734af9cc9577e10af72b7	0	0
Scheduled Task Deletion	David Strassegger	Sigma Integrated Rule Set (GitHub)	53299fc80451ec1c374dc7dcad4c9aee3f98bd1defb1b23e02900f2cf17d8c14	0	0
Scheduled Task/Job At	Ömer Günal, oscd.community	Sigma Integrated Rule Set (GitHub)	4b0543e80b3bd16b1e6ea919e7bc4a108b206468266597c7a5147cd615f35fe3	0	0
Screen Capture - macOS	remotephone, oscd.community	Sigma Integrated Rule Set (GitHub)	f4a2d13a06a29fbf2313f88753ab9955589a7aef45cfb0faea108c5bfac59ab3	0	0
Screen Capture with Import Tool	Pawel Mazur	Sigma Integrated Rule Set (GitHub)	ea2f87ff45a684c78cb46d65af3705037b7721905ce237e6daaa335a3fd7b5769	0	0
Screen Capture with Xwd	Pawel Mazur	Sigma Integrated Rule Set (GitHub)	c3c6c21ad23cac48bdee8d46a0a64de20e48510c5ed1617d23cb328129b7f580	0	0

Script Host Engine Modification	Den Iuzvyk	SOC Prime Threat Detection Marketplace	fcd207e8b19603f1d4e5450c04a2007f88780ea51861992a3e346474d646cbbd	0	0
SectorB06 Behavior (Sysmon detection)	Ariel Millahuel	SOC Prime Threat Detection Marketplace	6ffdda4e9d83f1b99a99568822f16d5a5a458ffccdb25fad469aaf2dbb8f0dd9	0	0
Secure Deletion with SDelete	Thomas Patzke	Sigma Integrated Rule Set (GitHub)	183ca715ffa97f30b076bb2c8793c0cb64221f3ad05c65fb425e3a38faac3645	0	0
Security Event Log Cleared	Saw Winn Naung	Sigma Integrated Rule Set (GitHub)	f32dc431e5951341656e9d55c58e0047b56f1beee18a05bd2b1e816ddbd10a17	0	0
Security Eventlog Cleared	Florian Roth	Sigma Integrated Rule Set (GitHub)	152b1150f7da94998822f9e55f3591b37d319fd7ce375004d24703a99aa957a5	0	0
Security Eventlog Cleared	Florian Roth	Sigma Integrated Rule Set (GitHub)	e20a3a5b38df7ceb5e94712485f6285fdd2ca0b40cf0a5eed31a42bbc779e4ff	0	0
Security Software Discovery	Daniil Yugoslavskiy, oscd.community	Sigma Integrated Rule Set (GitHub)	62a85e4a565b5b8609540a8aab58fbf730dd8330b219cb92da87bb5be582ebeb	0	0
Security Software Discovery	Daniil Yugoslavskiy, oscd.community	Sigma Integrated Rule Set (GitHub)	96f1ded9c8d78d6aecb533a9fdde682e09aa97bc94f4d21bd39577705c1d7547	0	0
Security Software Discovery by Powershell	frack113	Sigma Integrated Rule Set (GitHub)	f02d9a0f1e4d862f9d1b1d10a2f43de36d855212d5a70b671a8493d53a1b1722	0	0
Serv-U Exploitation CVE-2021-35211 by DEV-0322	Florian Roth	Sigma Integrated Rule Set (GitHub)	624b1600e93d3b9c6146b0136e00c73c8c809fe24a3f5299cbd4de5d727d1833	0	0
Service Control Manager Communication(RPC/TCP) Modification	Den Iuzvyk	SOC Prime Threat Detection Marketplace	b7809c2203acd7e06846efb5d0cddd1ab656f1e9f41b1f1bbff1bf84603a0a48	0	0
Service ImagePath Change with Reg.exe	frack113	Sigma Integrated Rule Set (GitHub)	3a4567bd735e7ae20a9b3bf3921ad6e9acdec3b957cdbdb4eebfd6feed5670d3	0	0
Service Registry Permissions Weakness Check	frack113	Sigma Integrated Rule Set (GitHub)	12c54ba61c9b654789342d689a197406cec675bbda5716b7749539b147856e21	0	0
Setuid and Setgid	Ömer Günal	Sigma Integrated Rule Set (GitHub)	8c6d633ce7d27d281b8cc113ebb409901529acad5564c5a8758ac987fc31b2b7	0	0
Shared Webroot	SOC Prime Team	SOC Prime Threat Detection Marketplace	3dbc7016da1cb9e2f97a1a07a36ceac8fa6a6df1669425785241bc69b0d6d966	0	0

SharpRDP execution	Den Iuzvyk	SOC Prime Threat Detection Marketplace	31cfc7594bce0379cd087a7f0fc2e2da4a491ff6b2df31db447eac7eec8b2d22	0	0
Shellshock Expression	Florian Roth	Sigma Integrated Rule Set (GitHub)	c6e62a3980f00e65b47fe7e5da5be2a0c6a37bd3ba4b893ee3c533fea9a42f74	0	0
Silence.Downloader V3	Alina Stepchenkova, Roman Rezvukhin, Group-IB, oscd.community	Sigma Integrated Rule Set (GitHub)	357adfc0bd514a2087509d1a67412a62f8823fd9caa3b6bcb80328828f9ed240	0	0
Silence.EDA Detection	Alina Stepchenkova, Group-IB, oscd.community	Sigma Integrated Rule Set (GitHub)	48a4a06b77cb84b45614503f3dd1035f0a83b236c4f840f9feab9be366a47d1d	0	0
SilentProcessExit Monitor Registrytion	Florian Roth	Sigma Integrated Rule Set (GitHub)	11ecefcf79daf3998440bd34d870da91d9c7644eb708e0f933349a5ec077fc87	0	0
SilentProcessExit Monitor Registrytion for LSASS	Florian Roth	Sigma Integrated Rule Set (GitHub)	04ff5b08364c475a034622812a1a7c93e181b8b348d6dc3b1fe28b11828e7d23	0	0
Silenttrinity Stager Msbuild Activity	Kiran kumar s, oscd.community	Sigma Integrated Rule Set (GitHub)	6a6afb8a168ede702164bc1169f8f046647310ca518ed5dd776966148a0e9532	0	0
Sitecore Pre-Auth RCE CVE-2021-42237	Florian Roth	Sigma Integrated Rule Set (GitHub)	ad5d590f46596f06240eee4586f7acc7d925fcf0ea9f364266b902bedd614224	0	0
Smoke Loader Behavior	Ariel Millahuel	SOC Prime Threat Detection Marketplace	0f0b6b52e3342eb0329e8ff51f0683aa5892c55d6d44aa49fcdbdf0f25761103	0	0
Smoke Loader Behavior	Ariel Millahuel	SOC Prime Threat Detection Marketplace	8d6d3b800ba936bb6910fd8bbf9551207e2288db95a5dafa6474e8a1d2f2d5fc	0	0
Sofacy Trojan Loader Activity	Florian Roth, Jonhnathan Ribeiro, oscd.community	Sigma Integrated Rule Set (GitHub)	c070e2f2f992c0ce37ed49db72f4c8ea1c3a9cc853e61535bd2625b5ae688b78	0	0
Solarwinds Launching Powershell With Base64 Encoding (via cmdline)	SOC Prime Team, Microsoft	SOC Prime Threat Detection Marketplace	30b4784c9d03d78a809bed19df233f6f95fc2c8325b32af97e0b1b8d24c6676e	0	0
Solarwinds SUPERNOVA Webshell Access	Florian Roth	Sigma Integrated Rule Set (GitHub)	81250a3a43500530ef04ff62b918cc5690b18cc4d09b4f77315012231acaa8bd	0	0
Solarwinds launching cmd.exe with echo (via cmdline)	SOC Prime Team, Microsoft	SOC Prime Threat Detection Marketplace	0174ab54fed285f5c38eceee197f8a60debfec2c3aa590604079831c288a9fb6	0	0
SonicWall SSL/VPN Jarrewrite Exploit	Florian Roth	Sigma Integrated Rule Set (GitHub)	e272203177abd4fd109dd93ae0e9913836f80a81b43eec0c819720c72843582c	0	0

Sophos Firewall Zero-Day explotation (Asnarök attack)	Ariel Millahuel	SOC Prime Threat Detection Marketplace	abea43cce1ab59b98d083a4bc5077c3e4acd49c745ee202f392405853fd46664	0	0
Source Code Enumeration Detection by Keyword	James Ahearn	Sigma Integrated Rule Set (GitHub)	91e80be4f3cb482bed8e242eb9e418e4fee5b1aaf32e61f4ae6d7def7d537d66	0	0
Space After Filename	Ömer Günal	Sigma Integrated Rule Set (GitHub)	96dade50824ff0a3a7ba5d5a9abc82419f0df174afff971fe0d7d87e74061785	0	0
Space After Filename - macOS	remotephone	Sigma Integrated Rule Set (GitHub)	2b3ab43da00d1cb60c0d3f837ce61f81355c37b68a1c3e826e66d68962c57752	0	0
Split A File Into Pieces	Igor Fits, oscd.community	Sigma Integrated Rule Set (GitHub)	3adbeb64ee2cc89f2825fbd133547fe3d84aac1ee5d48faaf2375b7c8364f74b	0	0
Split A File Into Pieces	Igor Fits, Mikhail Larin, oscd.community	Sigma Integrated Rule Set (GitHub)	712e9f7f7214c248ff6777f914a1cf282ba49bc580bbbe4bb40a38cfacec7927	0	0
Spring Framework Exceptions	Thomas Patzke	Sigma Integrated Rule Set (GitHub)	b9855abb1feaca99e5181199bf4d256c29f0150d137ed61e9cef83ce27764295	0	0
Startup Items	Alejandro Ortuno, oscd.community	Sigma Integrated Rule Set (GitHub)	80c9078b4f0a21412506961251c7253e037afc83c8a88cd362377082d1efaa30	0	0
Steganography Extract Files with Steghide	Pawel Mazur	Sigma Integrated Rule Set (GitHub)	9e28a144fe3121ecd3d91e846d0e1d5fb7be043db90ebdcda4ce1ddc629e0b78	0	0
Steganography Hide Files with Steghide	Pawel Mazur	Sigma Integrated Rule Set (GitHub)	2bc5697bb7a12c272490c67a3d83002e19dfb4722525786e91a4fba4c8b9ee97	0	0
Steganography Hide Zip Information in Picture File	Pawel Mazur	Sigma Integrated Rule Set (GitHub)	bb93f264dbaa005c9bc379b7db5eaa5cd680009288c824a9916340aef05188bc	0	0
Steganography Unzip Hidden Information From Picture File	Pawel Mazur	Sigma Integrated Rule Set (GitHub)	100e9962a68f74be52b70ad11285a16a1d1aa29e419831b60158672ee356b344	0	0
Sticky Key Like Backdoor Usage	Florian Roth, @twjackomo, Jonhnathan Ribeiro, oscd.community	Sigma Integrated Rule Set (GitHub)	210403ed0765f9206944ba0e7ae9a7fed3b74606aa7d5defd92b45c7565c50b4	0	0
Sticky Key Like Backdoor Usage	Florian Roth, @twjackomo, Jonhnathan Ribeiro, oscd.community	Sigma Integrated Rule Set (GitHub)	846842612cb81a07c0a4439f34127f7229a040a0618300a962ad5a95316f5417	0	0
Sticky Key Like Backdoor Usage	Florian Roth, @twjackomo, Jonhnathan Ribeiro, oscd.community	Sigma Integrated Rule Set (GitHub)	baf8cb1a268fb3d9173b5474a184cb8fd04489192832ac12dcd4d826248523b2	0	0
StoneDrill Service Install	Florian Roth	Sigma Integrated Rule Set (GitHub)	09c420a38066758c0236577ccb5fd401e138351217d25dbeae1220521c446472	0	0
Stop Or Remove Antivirus Service	frack113	Sigma Integrated Rule Set (GitHub)	7c4cece5b540c72f100dd8b8b7fc1c10727460ec0f36c75249e28ed51d6348ef	0	0

Successful Exchange ProxyShell Attack	Florian Roth, Rich Warren	Sigma Integrated Rule Set (GitHub)	e33130e6f328543f0b8bb35ef1bb2f92e015fe84965c32bf1d82d85dd00e1c1c	0	0
Successful IIS Shortname Fuzzing Scan	frack113	Sigma Integrated Rule Set (GitHub)	a46c1f051bcaa146c4a9adddc286b70714cb1365fe10a19aa2dcc7fd1aaaaf0f	0	0
Sudo Privilege Escalation CVE-2019-14287	Florian Roth	Sigma Integrated Rule Set (GitHub)	01dc28806687bbabc12e4c23cb8e022a4a81f459e26a267f34656b9e1aedf31e	0	0
Sudo Privilege Escalation CVE-2019-14287	Florian Roth	Sigma Integrated Rule Set (GitHub)	1ddcb9d1b179a17e011ac90c0294b7768bd99cc9d2a79c0df5506d870771953c	0	0
Sudo Privilege Escalation CVE-2019-14287	Florian Roth	Sigma Integrated Rule Set (GitHub)	284295b46bb8dd089813e305d695c5a0d85a5bde29f85e014d643b3cf63bbeb7	0	0
Sudo Privilege Escalation CVE-2019-14287	Florian Roth	Sigma Integrated Rule Set (GitHub)	37747140310b15c961b277ca418c6bcac1cfbd1a54e54df2a20cf743aa17f317	0	0
Sudo Privilege Escalation CVE-2019-14287	Florian Roth	Sigma Integrated Rule Set (GitHub)	75e40e43cc29db5d459f59bcc8d869264e37cb55976f57b0d731c18039306935	0	0
Suspect Svchost Memory Asccess	Tim Burrell	Sigma Integrated Rule Set (GitHub)	9fc70bf733b29bcd18e12529f975e24abdf01e3660221d791f76d57e02e2d527	0	0
Suspicious ADSI-Cache Usage By Unknown Tool	xknow @xknow_infosec	Sigma Integrated Rule Set (GitHub)	39b6e2d47cbb2139a0b088fb0f338071749fe923d01346e457f7ba2b0371e1b5	0	0
Suspicious Access to Sensitive File Extensions	Samir Bousseaden	Sigma Integrated Rule Set (GitHub)	c31fff6fad64dfd4138d6e166a46e20bf4a25db7117bc20b82965e7ed11982d3	0	0
Suspicious Access to Sensitive File Extensions - Zeek	Samir Bousseaden, @neu5ron	Sigma Integrated Rule Set (GitHub)	375d7fe36535214203bd98ae8bf81aecffb58ea5ae11de354f0140e7390327e2	0	0
Suspicious Access to Sensitive File Extensions - Zeek	SOC Prime Team	SOC Prime Threat Detection Marketplace	50e6edda507653e781908aed57ac737c10463c8aa7a2b28ec7724a716c0c9073	0	0
Suspicious Activity in Shell Commands	Florian Roth	Sigma Integrated Rule Set (GitHub)	9f38dd0d0f681b4185f6a6008d3904a10d8e2fe4e9dcf5aaba007262f1230dcb	0	0
Suspicious AdFind Enumerate	frack113	Sigma Integrated Rule Set (GitHub)	2abd81b6396ea687490b2d703ce07c1abd135ba398d89ab839c66e6a43f713f0	0	0
Suspicious Bitstransfer via PowerShell	Austin Songer @austinsonger	Sigma Integrated Rule Set (GitHub)	b19ad60b757e0d750b6426b1bf5fc68b705f7acf21dabd6e2a59f369493ff2e8	0	0
Suspicious C2 Activities	Marie Euler	Sigma Integrated Rule Set (GitHub)	7f495f7056b28211483e60f8f0510254ee64903ec5d127b9b822b085833218e9	0	0

Suspicious Camera and Microphone Access	Den Iuzvyk	Sigma Integrated Rule Set (GitHub)	f73e458cd36aac62c3443939924222027b1344d84127a52bf5623bcc692c86fc	0	0
Suspicious Child Process Created as System	Teymur Kheirkhabarov, Roberto Rodriguez (@Cyb3rWard0g), Open Threat Research (OTR)	Sigma Integrated Rule Set (GitHub)	84856c029af862b4a726da5944e6a57aaed5fda15c317414f9afeb3941c0010d	0	0
Suspicious Cmdl32 Execution	frack113	Sigma Integrated Rule Set (GitHub)	cf2baf60d63943d7200da28391b4e63298b2d186faf45b499b001ca84dc882ea	0	0
Suspicious Command Line Contains Azure TokenCache.dat as Argument (via cmdline)	SOC Prime Team	SOC Prime Threat Detection Marketplace	348e3e3f1264df658d94d7b48e449838ca835512c35891520db55b7b1f16160b	0	0
Suspicious Commands Linux	Florian Roth	Sigma Integrated Rule Set (GitHub)	3458d203410df750034bc6a6cf707cf905639d4ded28fbafac96941e0a0ec53a	0	0
Suspicious Computer Account Name Change CVE-2021-42287	Florian Roth	Sigma Integrated Rule Set (GitHub)	367ee44bfca23688ae0b0af0a5b6d5e824e751b28ac7849d1648bafb35b0448f	0	0
Suspicious Connection to Remote Account	frack113	Sigma Integrated Rule Set (GitHub)	71f9611fe50b2788a25e6b1c3fb3d035c5e04dfe73447ed185bfde157084fc72	0	0
Suspicious Control Panel DLL Load	Florian Roth	Sigma Integrated Rule Set (GitHub)	0791036b2af8420cef203df27c7840172deaafc554441f24ba507cd69d0d79e3	0	0
Suspicious Creation TXT File in User Desktop	frack113	Sigma Integrated Rule Set (GitHub)	965125e7c09a79de6429b9218659a7c8785c989273642091a7ebae3bfbe920c1	0	0
Suspicious Csi.exe Usage	Konstantin Grishchenko, oscd.community	Sigma Integrated Rule Set (GitHub)	d478344c6645595e8636745bd5f3fcc68955c4777726aba466ad93f133453add	0	0
Suspicious DNS Query with B64 Encoded String	Florian Roth	Sigma Integrated Rule Set (GitHub)	7c4c3ea7b520b1ed475e29a999863beeb5301ce2a0cee83a0b246f19f1e0601c	0	0
Suspicious DNS Z Flag Bit Set	@neu5ron, SOC Prime Team, Corelight	Sigma Integrated Rule Set (GitHub)	9520587a618269e5bf36ca31426edd352f0894b0dd96480e2a48554e5794148a	0	0
Suspicious Desktopimgdownldr Target File	Florian Roth	Sigma Integrated Rule Set (GitHub)	b01cb061a8ed4c005cf232ea599f09e2e3fdcc4033c23e74729723958607fce3	0	0
Suspicious Diantz Alternate Data Stream Execution	frack113	Sigma Integrated Rule Set (GitHub)	5888f710b830080c3505ccf3c3631d57eb9bd8be6b13d067fe7926dae9e72dc4	0	0
Suspicious Diantz Download and Compress Into a CAB File	frack113	Sigma Integrated Rule Set (GitHub)	b05a48e704cc2fbb722e3b3533e7b741751d8699bff15f6f28571133fe7611da	0	0

Suspicious Download from Office Domain	Florian Roth	Sigma Integrated Rule Set (GitHub)	a93dc62f3906167da8a6825eb9c1d7bd2ce6bfbb4ab3182329221f812e8374ee	0	0
Suspicious Driver Loaded By User	xknow (@xknow_infosec), xorxes (@xor_xes)	Sigma Integrated Rule Set (GitHub)	bb97779ed58fef8b7d6843a16b444d10cebd87234c0aab09d85ee1151b982c8d	0	0
Suspicious Encoded Scripts in a WMI Consumer	Florian Roth	Sigma Integrated Rule Set (GitHub)	06b69d9fb47d54903b8bff29c64d3bc3ad88eab8d9196cef1ed669080b206973	0	0
Suspicious Execution from Outlook	Markus Neis	Sigma Integrated Rule Set (GitHub)	f9e5ca1d53357c6179a23ffe1ed388ebe305e69c24b43fd23804a567a490780a	0	0
Suspicious Execution of Adidnsdump	frack113	Sigma Integrated Rule Set (GitHub)	5fcc3dcdd38e008741a75f024bab3a696ef8d9b4feba961448f2bbe027db5cf8	0	0
Suspicious Execution of SharpView Aka PowerView	frack113	Sigma Integrated Rule Set (GitHub)	fcd75941371f1c365f40d29f8498522d49065fb5ad8dc28a97b979603a6333ba	0	0
Suspicious Extrac32 Alternate Data Stream Execution	frack113	Sigma Integrated Rule Set (GitHub)	908072bc38c223e94e034ac7acafdfda27359b429525af331f388a7ef0e2b66c	0	0
Suspicious Findstr 385201 Execution	frack113	Sigma Integrated Rule Set (GitHub)	d58a7bc786bd9e9a6ecc6de92ba386f2e8ff1b3b96a65d1cdaa66db5cd0b94d1	0	0
Suspicious Get Information for AD Groups or DoesNotRequire PreAuth User	frack113	Sigma Integrated Rule Set (GitHub)	1bccdc208f191ae10d0fa42675f08a37e14e4f39ff07da3fc0c15510993f6e9c	0	0
Suspicious Get Information for AD Groups or DoesNotRequire PreAuth User	frack113	Sigma Integrated Rule Set (GitHub)	a205be34057679bd055b1f3cb3fd18d4d31f2b0bd776288ccba6be10b5a818e0	0	0
Suspicious Get Information for SMB Share	frack113	Sigma Integrated Rule Set (GitHub)	78af9841681cc3ae06f2b428827aa5b5f54e7e1cd67967a87cc99a5e7d4cfe18d	0	0
Suspicious Get Information for SMB Share	frack113	Sigma Integrated Rule Set (GitHub)	8f4c645fe661dc0ebdeff288f1761a20acf930f02e4c51bc48e6bafc245c1006	0	0
Suspicious Get Local Groups Information	frack113	Sigma Integrated Rule Set (GitHub)	098feee88c8a66070a3ec1f3c56be0ede46676cee2b799ba6d309360ce563ba7	0	0
Suspicious Get Local Groups Information	frack113	Sigma Integrated Rule Set (GitHub)	5ef6bc365a01e6ef90c1fc4f49006e9a8fe08e82c0a9ce80c10153915771547b	0	0
Suspicious GrantedAccess Flags on LSASS Access	Florian Roth	Sigma Integrated Rule Set (GitHub)	ed9636ccdbf53d675f6ffecccee23b849237a42f01ec09ad9ebf4ac4ed4a3afb	0	0

Suspicious HWP Sub Processes	Florian Roth	Sigma Integrated Rule Set (GitHub)	609a26363ca1233fc9637c9ef8d9c18feb2dc0dcf6b98ccb949a1913e739c3dc	0	0
Suspicious History File Operations	Mikhail Larin, oscd.community	Sigma Integrated Rule Set (GitHub)	946d8ac00870587827118a553b9209dbf76acb7e909425d91f177bde98fc1401	0	0
Suspicious History File Operations	Mikhail Larin, oscd.community	Sigma Integrated Rule Set (GitHub)	a9072027463739165675 8b0a5ab9ec371918d4a1e9d3ac56fd4d0f8719a7da72	0	0
Suspicious IO.FileStream	frack113	Sigma Integrated Rule Set (GitHub)	08e71eab529494c6cef4d7f699f5d95c87b1d954ee61b6f061d7005246b726af	0	0
Suspicious In-Memory Module Execution	Perez Diego (@darkquassar), oscd.community, Jonhnathan Ribeiro	Sigma Integrated Rule Set (GitHub)	4e3a7d5df089d2d7c80cf84bbba4e8a4363101ac03f6a9c758101f0c1bb010a4	0	0
Suspicious Inbox Forwarding	Austin Songer @austinsonger	Sigma Integrated Rule Set (GitHub)	487fc5687e250bef85f8102efa69086f801e489db41cb0f01c4bf4b1ed4827f3	0	0
Suspicious Interactive PowerShell as SYSTEM	Florian Roth	Sigma Integrated Rule Set (GitHub)	f8335c66f6b8aed850de5246bacec6f1eee18e5549c581e9892827d840e5720a	0	0
Suspicious Kerberos RC4 Ticket Encryption	Florian Roth	Sigma Integrated Rule Set (GitHub)	7f2bb7e386b3f3d057b64c70d36264a2c7163a1215e88b8731f9b87d919ca77d	0	0
Suspicious Kernel Dump Using Dtrace	Florian Roth	Sigma Integrated Rule Set (GitHub)	f1a72edd07dd4c90ef3c56a4aaab9034ebe25d9a2b5d3e9de4deb8877f60ea24	0	0
Suspicious Keyboard Layout Load	Florian Roth	Sigma Integrated Rule Set (GitHub)	1e8253d40fd15968a25971ec64e35f84f90536676b445d16184bde41a5fc6ba0	0	0
Suspicious LDAP-Attributes Used	xknow @xknow_infosec	Sigma Integrated Rule Set (GitHub)	0730743577ad7cca001768987a40afda61d7838e179b9c8f1053e72a1459048a	0	0
Suspicious LOLBIN AccCheckConsole	Florian Roth	Sigma Integrated Rule Set (GitHub)	bdd4b3cf901dc4fd7c4ee12323f20fd996bc0170c122f0566f5dbfbede875c23	0	0
Suspicious LSASS Process Clone	Florian Roth, Samir Bousseaden	Sigma Integrated Rule Set (GitHub)	489015366445b29d739d0c35ebba4e9278457dd045568abcf2266370379e7944	0	0
Suspicious Load DLL via CertOC.exe	Austin Songer @austinsonger	Sigma Integrated Rule Set (GitHub)	42f3abed5774e74cc80412cad617ceb1f8881fc484a38c351eed5b589c80dee3	0	0
Suspicious Log Entries	Florian Roth	Sigma Integrated Rule Set (GitHub)	3b172a1d01b7c198d455c2a17e8ae127ce5f5dba1c75a0a99cc77599f4ca78f7	0	0
Suspicious MacOS Firmware Activity	Austin Songer @austinsonger	Sigma Integrated Rule Set (GitHub)	71c75c172863712967d00b928953180528e3cb3b663a1722518a9271c3538625	0	0

Suspicious Multiple File Rename Or Delete Occurred	Vasiliy Burov, oscd.community	Sigma Integrated Rule Set (GitHub)	5cbe938f157b387106147682e156a8efa2d8aeb5efce0266d3c0081b69e12678	0	0
Suspicious NT Resource Kit Auditpol Usage	Nasreddine Bencherchali @nas_bench	Sigma Integrated Rule Set (GitHub)	a5d0ee315323a7612e8c53b5bbcba868cb9cf4a4b8ca2b5850b97eaf2c03f1e6	0	0
Suspicious Named Error	Florian Roth	Sigma Integrated Rule Set (GitHub)	b8b5a8000383b99cb6f14f2e8f17d927da0e92e965c625faa3cabe1e72b84323	0	0
Suspicious Netsh Discovery Command	frack113	Sigma Integrated Rule Set (GitHub)	25c7926ea5dfde7ab41cd4aeebfb89e01d4dcb8b7243522af4f643f690d857c7	0	0
Suspicious New Printer Ports in Registry (CVE-2020-1048)	EagleEye Team, Florian Roth, NVISO	Sigma Integrated Rule Set (GitHub)	2855d4d044bf08f00f380efb88fbd76fba4f8199fdab66a8c7aaad6d63bbe63e	0	0
Suspicious New-PSDrive to Admin Share	frack113	Sigma Integrated Rule Set (GitHub)	9b5bc7e38efe4f1b17f2a923ca4fbbd1303baf2899f224b7e40278aea60cfc64	0	0
Suspicious Nmap Execution	frack113	Sigma Integrated Rule Set (GitHub)	4225d7662d0eec6d20893e2e9f75328a37cc7a24ba7f1932e3c993cf482e46d5	0	0
Suspicious Non PowerShell WSMAN COM Provider	Roberto Rodriguez (Cyb3rWard0g), OTR (Open Threat Research)	Sigma Integrated Rule Set (GitHub)	b42a14d4eb96ec45f6bc9ca190be91d043f6ead5ff998b704aabb76605041d4b	0	0
Suspicious OAuth App File Download Activities	Austin Songer @austinsonger	Sigma Integrated Rule Set (GitHub)	fa3f7119a0c19e9ddb6bf3defe5e0797888e23ec789c8f3357af53a5f70c3c94	0	0
Suspicious OpenSSH Daemon Error	Florian Roth	Sigma Integrated Rule Set (GitHub)	e0a89459a9f05d408d482b9640980fec9bab82d2dd11083d04356a4055021f78	0	0
Suspicious Outbound Kerberos Connection	Ilyas Ochkov, oscd.community	Sigma Integrated Rule Set (GitHub)	55516cecb3b5273d1166f185e3e1bcd239eaaa5df10cea2fb888c3f4d4e4dbdf	0	0
Suspicious Outbound Kerberos Connection	Ilyas Ochkov, oscd.community	Sigma Integrated Rule Set (GitHub)	9c660d5fee16f15f8c327be10917fac3b7275a58ecb9ed73d49e0ac6c35a7df0	0	0
Suspicious Outbound RDP Connections	Markus Neis - Swisscom	Sigma Integrated Rule Set (GitHub)	dbfca88ab9ee6831be6d244ddd8d59d64840215c6266895aed60b0192f60f226	0	0
Suspicious Outbound SMTP Connections	frack113	Sigma Integrated Rule Set (GitHub)	3659f9925f327ac0ba2be9b3c8c7240f432c4b62f162b846c10410fff320b6f7	0	0
Suspicious PowerShell Download	Florian Roth	Sigma Integrated Rule Set (GitHub)	0c6e3c35fbd166dc96fbf3faf4f052230a9cc9db642ee3bee40f5c94d5938d03	0	0
Suspicious PowerShell Download	Florian Roth	Sigma Integrated Rule Set (GitHub)	124bf07ac70743e91b5698e3731aae0330fc182aa58036390f2a0457a90b5341	0	0

Suspicious PowerShell Download	Florian Roth	Sigma Integrated Rule Set (GitHub)	69130b2eb287f08303a7092222cc3a0be896a066b64f8b32f96d08ff4708e37f	0	0
Suspicious PowerShell Download	Florian Roth	Sigma Integrated Rule Set (GitHub)	9d6bbc732c370aae45fda2c0c962d9136afa87ecd165064208cb40aa877e4e5b	0	0
Suspicious PowerShell Download	Florian Roth	Sigma Integrated Rule Set (GitHub)	ddc4948cb3433762084af70db4c7d85a2cd1e48ee6ae8dc152412a50dfbb42db	0	0
Suspicious PowerShell Invocations - Generic	Florian Roth (rule)	Sigma Integrated Rule Set (GitHub)	3f1f1d4b840f1276832b328fab68511c28f6b7918e887279b03e6ea4735bef7d	0	0
Suspicious PowerShell Invocations - Generic	Florian Roth (rule)	Sigma Integrated Rule Set (GitHub)	d0b30db49f680fc7c412d09dc2099e655eb262fd5ef5b03fb5304663ab79137a	0	0
Suspicious PowerShell Invocations - Specific	Florian Roth (rule), Jonhnathan Ribeiro	Sigma Integrated Rule Set (GitHub)	355b439d3a90c89090f6f266afd2306ad6a03e5ca79228ad1be6e9cb6940491b	0	0
Suspicious PowerShell Invocations - Specific	Florian Roth (rule), Jonhnathan Ribeiro	Sigma Integrated Rule Set (GitHub)	7d262d8417cb03b2a9d2b935ae55980f22abc3aa7cffc36e57eda761068226dc	0	0
Suspicious PowerShell Mailbox Export to Share	Florian Roth	Sigma Integrated Rule Set (GitHub)	bdf323dec5fa58a6655db6a0ae8ed9322f1fae8288502705c60e0b1f38761a06	0	0
Suspicious PowerShell WindowStyle Option	frack113	Sigma Integrated Rule Set (GitHub)	5e2ea8c055dd73ea66238735323d0318c2a6c114047137146357b85f764b1101	0	0
Suspicious PsExec Execution	Samir Bousseaden	Sigma Integrated Rule Set (GitHub)	f04c595ca66281cfe11a9157fbeef36ddbee45cc4a5391471d010a08e4c14863	0	0
Suspicious PsExec Execution - Zeek	SOC Prime Team	SOC Prime Threat Detection Marketplace	5c9d17e0b9843d06a6bdc67aa64f2d0c4823a01681a54c83d94c7e3c0bbe2c66	0	0
Suspicious PsExec Execution - Zeek	Samir Bousseaden, @neu5ron	Sigma Integrated Rule Set (GitHub)	eee9047f1507bcd02b641cb229c21f615af4fb70ba87dbff05842699503530b4	0	0
Suspicious RDP Redirect Using TSCON	Florian Roth	Sigma Integrated Rule Set (GitHub)	2d1baec06e45f7d7bbd540486a817a6738253b8960068c5aee89c3123cfa1ac0	0	0
Suspicious RazerInstaller Explorer Subprocess	Florian Roth, Maxime Thiebaut	Sigma Integrated Rule Set (GitHub)	b656a8d4ce3cfd0545afa9a8754e22d2d051bd71f469b2d3d844ecf580dd0532	0	0
Suspicious Reg Add BitLocker	frack113	Sigma Integrated Rule Set (GitHub)	1e5c4651907cea569ba4493fc4d9c634d654da730dcdfa36412180bfb694dba9	0	0
Suspicious Registration via cscript.exe	Austin Songer @austinsonger	Sigma Integrated Rule Set (GitHub)	cff1e1978dab401a82f456bac2436b263ce457f5ad9e3283c8d77f7ab885b87a	0	0

Suspicious Rejected SMB Guest Logon From IP	Florian Roth, KevTheHermit, fuzzyf10w	Sigma Integrated Rule Set (GitHub)	f1f470f63c4d9b600bbc209212d3f1806b7b41154d14a15f0666241f96f786b1	0	0
Suspicious Remote Logon with Explicit Credentials	oscd.community, Teymur Kheirkhabarov @HeirhabarovT, Zach Stanford @svch0st	Sigma Integrated Rule Set (GitHub)	3f8d6ccb4e7555cba08aa888810b970a1a0a1f79d2a65b51f323b466542ae099	0	0
Suspicious Reverse Shell Command Line	Florian Roth	Sigma Integrated Rule Set (GitHub)	8e3a8f0b4e0bf72703dfa7509e194c8bd77b591184bf65292cf9c554fe5d7149	0	0
Suspicious Rundll32 Activity Invoking Sys File	Florian Roth	Sigma Integrated Rule Set (GitHub)	f4b9a5aba26ac1d465f55970b8defeab4a4704def7889e6c296b0f33cd1fad27	0	0
Suspicious Rundll32 Invoking Inline VBScript	Florian Roth	Sigma Integrated Rule Set (GitHub)	40e3e97976c84f512b11ec485b8dc54ce731851327fe05beff6b567fdfe2b91b	0	0
Suspicious Rundll32 Script in CommandLine	frack113	Sigma Integrated Rule Set (GitHub)	ee7fc4aa3dcf06ddc37a9dc24c2fe5a2d394cc53d560d2214a8f5455eedb6291	0	0
Suspicious Runscripthelper.exe	Victor Sergeev, oscd.community	Sigma Integrated Rule Set (GitHub)	11391eae2fbdc6dde630d27416798a88f2a185e1dc68c55e40fe03a2a85412de	0	0
Suspicious SQL Error Messages	Bjoern Kimminich	Sigma Integrated Rule Set (GitHub)	25642d4ac27c9f3036a7124392a66d0dad8e15e7f323995c82b1b9460ae3ffb5	0	0
Suspicious Scheduled Task Writ to System32 Tasks	Florian Roth	Sigma Integrated Rule Set (GitHub)	3da113395881b8606ab35684394038c9c59eb8dae1b899ed92a2c40df104f5aa	0	0
Suspicious Serv-U Process Pattern	Florian Roth	Sigma Integrated Rule Set (GitHub)	7456e5b742cfbd4f35bce2536feed29bf8c22343e4f695fdd04fbf7070d41396	0	0
Suspicious Spool Service Child Process	Justin C. (@endisphotic), @dreadphones (detection), Thomas Patzke (Sigma rule)	Sigma Integrated Rule Set (GitHub)	2445eef8bbfc5d52245783f3d3a39b67d2a9e863e057b9710358f473c4a0d9ed	0	0
Suspicious Subsystem for Linux Bash Execution	frack113	Sigma Integrated Rule Set (GitHub)	dfbb51364e0deb6fd01f82a709f96be117d3f57ab06c8ac5718d944050856808	0	0
Suspicious System.Drawing Load	Roberto Rodriguez (Cyb3rWard0g), OTR (Open Threat Research)	Sigma Integrated Rule Set (GitHub)	0e577377d486c7998da21b8bf8adfad459d2ee2c932fddd9aa595b43b009916c	0	0
Suspicious TSCON Start as SYSTEM	Florian Roth	Sigma Integrated Rule Set (GitHub)	ef15288703ebef641a550ecf3efe69b3c2eae2d9d03b9828ebc27e4474bd138a	0	0
Suspicious Typical Malware Back Connect Ports	Florian Roth	Sigma Integrated Rule Set (GitHub)	c819b1c2210c6c76f29e7d15825b104bbd98de4d9561a6c86a8b158afd0d2be9	0	0
Suspicious Unattend.xml File Access	frack113	Sigma Integrated Rule Set (GitHub)	ab4f3a9eb0931d1b25be0e6ec70048514d987acda1b98b078b334de53d084360	0	0

Suspicious Usage of the Manage-bde.wsf Script	oscd.community, Natalia Shornikova	Sigma Integrated Rule Set (GitHub)	ed5e62dadca0230ffc2a8a11cf9e699200080030ffff4d0d2fd4df79510c64c3	0	0
Suspicious Use of /dev/tcp	frack113	Sigma Integrated Rule Set (GitHub)	acaf2d56329609a17ef157534fe784b3570d4c344a3eff25b493f541a2526056	0	0
Suspicious Use of CSharp Interactive Console	Michael R. (@nahamike01)	Sigma Integrated Rule Set (GitHub)	a4fc89bb3700fe0a55cf04c68919916827d349edffbb82042fcceed68a55944d	0	0
Suspicious Use of PsLogList	Nasreddine Bencherchali @nas_bench	Sigma Integrated Rule Set (GitHub)	2a651ab66176323248a00a1c8f2e0c1d6e82ebbcb2c316bd3a1bce5391cc6b28	0	0
Suspicious User Agent	Florian Roth	Sigma Integrated Rule Set (GitHub)	d91df9da12337a7f5ee75bb073c3410a058eb5ed6b7c86b148e725f9059f75a0	0	0
Suspicious VBScript UN2452 Pattern	Florian Roth	Sigma Integrated Rule Set (GitHub)	7fb1daa4a8edb7a5b90b062c058870ef63fc97c3ef0e3208a4ebe707c2f77f8f	0	0
Suspicious VBoxDrvInst.exe Parameters	Konstantin Grishchenko, oscd.community	Sigma Integrated Rule Set (GitHub)	7f57d3ad9551dc7e9826a09268d6311674527871cd948f123fe51b8ad1b701aa	0	0
Suspicious VSFTPD Error Messages	Florian Roth	Sigma Integrated Rule Set (GitHub)	bbc1da4633ad6413fded73095affb9717c6e165f62cd9aad1ecfef998aa8db78	0	0
Suspicious WMIC ActiveScriptEventConsumer Creation	Florian Roth	Sigma Integrated Rule Set (GitHub)	c96db484de175e1b250b8157c4e848f441ffb92c370fec9a85857f015c6b8db8	0	0
Suspicious WSMAN Provider Image Loads	Roberto Rodriguez (Cyb3rWard0g), OTR (Open Threat Research)	Sigma Integrated Rule Set (GitHub)	33e7351552f382831af6bf73d86054bced055e64df091f572c94e9fc9e9a2a97	0	0
Suspicious Werfault.exe Network Connection Outbound	Sreeman	Sigma Integrated Rule Set (GitHub)	16c36a9e42bc4413ac1329f5dd42431a817722b75cea05ac07ebb3f65876cb0f	0	0
Suspicious Where Execution	frack113	Sigma Integrated Rule Set (GitHub)	46ae66dd22967fe384fb2758be37ee4bc4eb6756891eb9d7ebb29342e2dd03d1	0	0
Suspicious Windows ANONYMOUS LOGON Local Account Created	James Pemberton / @4A616D6573	Sigma Integrated Rule Set (GitHub)	95f1c4af26ab73ade968853c4fcf97de23d5c6004b49db4a07a2616054591b05	0	0
Suspicious Word Cab File Write CVE-2021-40444	Florian Roth, Sittikorn S	Sigma Integrated Rule Set (GitHub)	81b716bb22121eaedb941850fff6c213e7492ff4ee7564ae54606bc9dbb4fa57	0	0

Suspicious XOR Encoded PowerShell Command Line	Teymur Kheirkhabarov, Harish Segar (rule)	Sigma Integrated Rule Set (GitHub)	3df27b5ffb8110f82c5da9120fd9c1c88c792ef65770b7f2706fc60a04b9cc9c	0	0
Suspicious ZipExec Execution	frack113	Sigma Integrated Rule Set (GitHub)	4299b17cc3fb6f5ed2bc90d612e461452723118f5b71a85231879dcf7c197ead	0	0
Svchost DLL Search Order Hijack	SBousseaden	Sigma Integrated Rule Set (GitHub)	db5441b38e2fcbf39fea3bb39c740232381bd1357c8ff96f6df1ce0020169259	0	0
Symlink Etc Passwd	Florian Roth	Sigma Integrated Rule Set (GitHub)	e6c712d0b47b9ca26b1493414298a9db2aa7d1a7a22ae1dd2bbe3d98be6ebccd	0	0
SyncAppvPublishingServer Execute Arbitrary PowerShell Code	frack113	Sigma Integrated Rule Set (GitHub)	bd38197f39431ccbcd7225eae0595eed4788e30dee52b6db845bb259cc8a5490	0	0
SyncAppvPublishingServer Execution to Bypass Powershell Restriction	Ensar Şamil, @sblmsrsn, OSCD Community	Sigma Integrated Rule Set (GitHub)	15b8bc2b4085ebae022c2b20c71b4ff925bb2def0f422752e477ef64090acbb5	0	0
SyncAppvPublishingServer Execution to Bypass Powershell Restriction	Ensar Şamil, @sblmsrsn, OSCD Community	Sigma Integrated Rule Set (GitHub)	2f6c3876a6bf6c6982f41c7a31019b9025028a80428d75d0fbfadc485780f478	0	0
SyncAppvPublishingServer Execution to Bypass Powershell Restriction	Ensar Şamil, @sblmsrsn, OSCD Community	Sigma Integrated Rule Set (GitHub)	72c39d73d55d9033eaf48b2345a2731c21be042d5b6a492dd732ad728d06da24	0	0
SyncAppvPublishingServer Execution to Bypass Powershell Restriction	Ensar Şamil, @sblmsrsn, OSCD Community	Sigma Integrated Rule Set (GitHub)	8326a878ec5c1017e74941a7f45b60cfacf514ecaf4c2f5a787bfbecdc6bdf84	0	0
SyncAppvPublishingServer Execution to Bypass Powershell Restriction	Ensar Şamil, @sblmsrsn, OSCD Community	Sigma Integrated Rule Set (GitHub)	da7ba86aeba5af6786083f79201143e96dfb9aaa6f81136cb9deeffbda13a236	0	0
SysKey Registry Keys Access	Roberto Rodriguez @Cyb3rWard0g	Sigma Integrated Rule Set (GitHub)	00368348746af494ae4871162a2c3187af955e35e20fc2de34bda349b1883860	0	0
Sysinternals SDelete File Deletion	Roberto Rodriguez (Cyb3rWard0g), OTR (Open Threat Research)	Sigma Integrated Rule Set (GitHub)	13320004e8b7f532ff0dcbcc7a564fd60fa782490cdaf6e553e89088ded28e41	0	0

Sysmon Channel Reference Deletion	Roberto Rodriguez (Cyb3rWard0g), OTR (Open Threat Research)	Sigma Integrated Rule Set (GitHub)	f9f553ae3b418546ce1d60bc5be320fb809f42d2184eea0be3ebe38529115176	0	0
Sysmon Configuration Error	frack113	Sigma Integrated Rule Set (GitHub)	1cd7d30672aa97bf7ad987f1430427c4badcaf9359b200f28071d8b243834f07	0	0
Sysmon Configuration Modification	frack113	Sigma Integrated Rule Set (GitHub)	3bb0c88834d7140b8c654b55212f61356f2c8817acf24f1a8691d358280b0541	0	0
Sysmon Configuration Modification	frack113	Sigma Integrated Rule Set (GitHub)	abdfcf563f91cb4c9b132baa9fd47b92a1e20294c09c02d7571f6fe5505f21d7	0	0
Sysmon Configuration Modification	frack113	Sigma Integrated Rule Set (GitHub)	d46e95fee1af14f21e84edea54e4ff0adc9b091c82e403fd89cc53d93506d609	0	0
System Eventlog Cleared	Florian Roth	Sigma Integrated Rule Set (GitHub)	897e81991ba93eae2ef049bec91493dcbc61908766ac3d56284ce87250a69aed	0	0
System Information Discovery	Ömer Günal, oscd.community	Sigma Integrated Rule Set (GitHub)	0e346973181b79cd813d4507ff8c38d8a584a417939557faa5fa7158cf2ba7d0	0	0
System Information Discovery	Ömer Günal, oscd.community	Sigma Integrated Rule Set (GitHub)	3745b67648a34091bd1ecf4cfeeaba7bc12bfe1ffc83c8aea519f5888c1714ef	0	0
System Information Discovery	Ömer Günal, oscd.community	Sigma Integrated Rule Set (GitHub)	9920fd14e241024bdb1ef7da4f1d69e5ac14e3d81aa324f2395de1464b61d679	0	0
System Information Discovery	Ömer Günal, oscd.community	Sigma Integrated Rule Set (GitHub)	de46e7313e69231a749082946337322d32ab9e628663e5d92b61586d9c24d47f	0	0
System Information Discovery	Ömer Günal, oscd.community	Sigma Integrated Rule Set (GitHub)	fa3e44c9641ee88a3df1944a742869e28a10d6f37c0aab69e06413014fd5c890	0	0
System Information Discovery	Pawel Mazur	Sigma Integrated Rule Set (GitHub)	fb1fcb86cdb589a2d0fc7810aa7796360737fe3205f5d847d75ecf94876c080f	0	0
System Network Connections Discovery	Daniil Yugoslavskiy, oscd.community	Sigma Integrated Rule Set (GitHub)	036282b9889ec8d8a1cdaf902e26133c4af06ef02c074d48c4e063674b97b784	0	0
System Network Connections Discovery	Daniil Yugoslavskiy, oscd.community	Sigma Integrated Rule Set (GitHub)	bcce343b1b60fe2c9b0a19e6c49cd613e3cd470f7a5a4dc85811f8188fbdc872	0	0
System Network Discovery - Linux	Ömer Günal and remotephone, oscd.community	Sigma Integrated Rule Set (GitHub)	780133161bc77c6fd8e998a40218c5d992ba90b4ee08ea1e489f112b4f5739e6	0	0
System Network Discovery - macOS	remotephone, oscd.community	Sigma Integrated Rule Set (GitHub)	90acea841b97b3b53a1119f22723d62839805d36487dbabf612a9b724c86798b	0	0
System Owner or User Discovery	Timur Zinniatullin, oscd.community	Sigma Integrated Rule Set (GitHub)	db8f6a3c12b8841963a472baa0be9f352507e250365446a6638700e5e7035e32	0	0
System Shutdown/Reboot	Igor Fits, Mikhail Larin, oscd.community	Sigma Integrated Rule Set (GitHub)	96710ba7369fb8bd38beca2361ac7b7447c02e93a21426970ee43af5e1e039dc	0	0

System Shutdown/Reboot	Igor Fits, oscd.community	Sigma Integrated Rule Set (GitHub)	a915654969a7479839f83e157606f0d49d87567ec32f31c4b16352afecd90f27	0	0
SystemNightmare Exploitation Script Execution	Florian Roth	Sigma Integrated Rule Set (GitHub)	c8b63d7e7a86cd816ca0855c66d0465f223a68621bc59cdb85639e382e022118	0	0
Systemd Service Reload or Start	Jakob Weinzettl, oscd.community	Sigma Integrated Rule Set (GitHub)	2b9f58e2da3f441d888d64d4aca75b8c4f27198a10b76961e1a593881f018af3	0	0
T1021 DCOM InternetExplorer.Application Iertutil DLL Hijack	Roberto Rodriguez @Cyb3rWard0g, Open Threat Research (OTR)	Sigma Integrated Rule Set (GitHub)	325801736478f2eeb21dc4d27671455172bd5ba8978fd1c153bbf1bb560f4617	0	0
T1021 DCOM InternetExplorer.Application Iertutil DLL Hijack	Roberto Rodriguez @Cyb3rWard0g, Open Threat Research (OTR), wagga	Sigma Integrated Rule Set (GitHub)	9140e60563fcdfeb01d8d885f102c4b30ed9435ca18d2a4d8df9db6020ba2d0a	0	0
T1047 Wmiprvse Wbemcomn DLL Hijack	Roberto Rodriguez @Cyb3rWard0g, Open Threat Research (OTR)	Sigma Integrated Rule Set (GitHub)	1ed7550018ff4afc8c6f1d36eb7b0bbb2f831f5ac43cb0a16bbb96205616d858	0	0
T1086 PowerShell Execution	Roberto Rodriguez (Cyb3rWard0g), OTR (Open Threat Research)	Sigma Integrated Rule Set (GitHub)	83cb47f5a4ddfd9c34da01fa9f873a03f0cc58cc2778580cc726de414c3c0baf	0	0
TA410 LookBack and FlowCloud malware campaigns (Sysmon Behavior)	Den Iuzvyk	SOC Prime Threat Detection Marketplace	2d3ca95295f2fe12c6cbd5a13bb6f9b54f0f22d3a81dbc5b82c9bfbdae44f83b	0	0
TAIDOOR - Chinese RAT	Ariel Millahuel	SOC Prime Threat Detection Marketplace	680dcdde1b8bfe90bf9acba2d0f5e4c1c8b437fe2e5aa5068855ccda40180966	0	0
TAIDOOR - Chinese RAT	Ariel Millahuel	SOC Prime Threat Detection Marketplace	68bb411fd4bf6a1ffe552b343dac5d14f00ce686424e3b32e68ee2176ab8bce3	0	0
TAIDOOR - Chinese RAT	Ariel Millahuel	SOC Prime Threat Detection Marketplace	97b2c02dfa95bb4aaaff73fc548ad854d0cdd79e40c67de409e716ba04f8b372	0	0
TAINTEDSCRIBE - North Korean Trojan (Hidden Cobra)	Ariel Millahuel	SOC Prime Threat Detection Marketplace	fefa666b9dddab06dca15eb5c3a044757bbf7420794f459140fae014af5988af	0	0
Tamper Windows Defender	frack113	Sigma Integrated Rule Set (GitHub)	207c25c9408a94a6ab4fd79571c6f71741248f188bf163b2ca9ea8531bdf439e	0	0
Tap Driver Installation	Daniil Yugoslavskiy, Ian Davis, oscd.community	Sigma Integrated Rule Set (GitHub)	358d68998add69c3d9057a82193ae58f278aa61103f23b98603b6f2d7e59cb22	0	0

Tap Driver Installation	Daniil Yugoslavskiy, Ian Davis, oscd.community	Sigma Integrated Rule Set (GitHub)	a23d7badd6ad7bc64986003d146002a8cd02c1adab85136c45c522d5ab23e706	0	0
Tap Driver Installation	Daniil Yugoslavskiy, Ian Davis, oscd.community	Sigma Integrated Rule Set (GitHub)	c1693fcd30d2082a9f64e5a158f8acfbdb23a2e5ef0cb5c125a34a46c29a60d1	0	0
Tap Driver Installation	Daniil Yugoslavskiy, Ian Davis, oscd.community	Sigma Integrated Rule Set (GitHub)	e60d92b6ad7c18d80d842937fb0a3b1e49a9339611f31cf7f9fa688f0d1fc1fa	0	0
Tap Driver Installation	Daniil Yugoslavskiy, Ian Davis, oscd.community	Sigma Integrated Rule Set (GitHub)	f64fba8ff6db3ee854baecf3e208e1be45b8dd29c23b509f62062e55ebe28bb9	0	0
Telegram API Access	Florian Roth	Sigma Integrated Rule Set (GitHub)	8a8587aaa3d307de3f020fd9ddb543581dd561447576a463e570558a6e78a023	0	0
Telegram Bot API Request	Florian Roth	Sigma Integrated Rule Set (GitHub)	8119b0f5e55bcc32efeebba677769c41f458947ed836a43326d94ce77e2a6a0a	0	0
Terdot Trojan	Ariel Millahuel	SOC Prime Threat Detection Marketplace	758c4cbf66a128098c5bfb6abc15633535d24cb73c1c583c8b2e6453a93c6f80	0	0
Terdot Trojan	Ariel Millahuel	SOC Prime Threat Detection Marketplace	a05609887fbb50f52f95231dae41088de78c48b2f3559cbe4761af7069777c41	0	0
Terminal Server Client Connection History Cleared	Christian Burkard	Sigma Integrated Rule Set (GitHub)	f864355e26341358045facaf6f66106b0bf475ff0cd2a56ea6c2157735727c35	0	0
Terminal Service Process Spawn	Florian Roth	Sigma Integrated Rule Set (GitHub)	0232a28f98329276f53deac4ffd7ee149f868c8def851948c4af8e750be1b910	0	0
TerraMaster TOS CVE-2020-28188	Bhabesh Raj	Sigma Integrated Rule Set (GitHub)	69295716b447993c5584f18e294250daf69aa8bc979708f88313e47ca01e6793	0	0
Time Travel Debugging Utility Usage	Ensar Şamil, @sblmsrsn, @oscd_initiative	Sigma Integrated Rule Set (GitHub)	41bae2ae89409b6a1ff355df6e25112c56884876b18f7a5ca827d634fc1847f4	0	0
Time Travel Debugging Utility Usage	Ensar Şamil, @sblmsrsn, @oscd_initiative	Sigma Integrated Rule Set (GitHub)	ac619a6a73b5c0668aeb218c1580100bf9e6f7791822b92360cb51fb09394ccd	0	0
Time Travel Debugging Utility Usage	Ensar Şamil, @sblmsrsn, @oscd_initiative	Sigma Integrated Rule Set (GitHub)	afad13c67de2842888c6d4678ab0ab46d7369e91b6c7fb525482e91294e4ccad	0	0
Time Travel Debugging Utility Usage	Ensar Şamil, @sblmsrsn, @oscd_initiative	Sigma Integrated Rule Set (GitHub)	c5cd42b219e3389810b80d30f0df29501f964191e806ce3ad063b9cf5c621fb4	0	0
Time Travel Debugging Utility Usage	Ensar Şamil, @sblmsrsn, @oscd_initiative	Sigma Integrated Rule Set (GitHub)	f2baa9e77eedc1ad2bcabc55acff8e7d6273352d961c3bf3b07d58b3b7fd8bb7	0	0
Tinba Banking Trojan	Ariel Millahuel	SOC Prime Threat Detection Marketplace	af02ff0def6aec347fa7d49ff18febb8c477a257f2e7dc8ca67d0cdbe9dddb0a	0	0

Tirbot Trojan (Sysmon detection)	Ariel Millahuel	SOC Prime Threat Detection Marketplace	985b4d1a9a38675b5a512221d45a61dfdf349da41c92df19ae3776b712fe20e0	0	0
Transferring Files with Credential Data via Network Shares	Teymur Kheirkhabarov, oscd.community	Sigma Integrated Rule Set (GitHub)	b901cdb66cb3627f3cf9d508421eb3e34409337ecfea0476c0896c63c71dbd74	0	0
Transferring Files with Credential Data via Network Shares - Zeek	@neu5ron, Teymur Kheirkhabarov, oscd.community	Sigma Integrated Rule Set (GitHub)	c32a3e7518848a21d37b9b5d6a00e756e5ce36f0ba6f2b79a1304a7fa9f1369d	0	0
TropicTrooper Campaign November 2018	@41thexplorer, Microsoft Defender ATP	Sigma Integrated Rule Set (GitHub)	2490e3004ac94fbdd6f3d694aa2c24ec00b0193bcac04aad389d62a43350ce61	0	0
Turla ComRAT	Florian Roth	Sigma Integrated Rule Set (GitHub)	f8b1e8439f6b16f86828128a05821dfc35b5cedac0b0ef9588c00d9a12d0ef31	0	0
Turla Group Commands May 2020	Florian Roth	Sigma Integrated Rule Set (GitHub)	13b646717610af0f26e60da5f245b187d697983865f41f8426677226a1dd67e9	0	0
Turla Group Lateral Movement	Markus Neis	Sigma Integrated Rule Set (GitHub)	4ac69336261d41d0d7c5dabb3bbf3be9deae948f76c2139e4061f519c6fb043f	0	0
Turla Group Lateral Movement	Markus Neis	Sigma Integrated Rule Set (GitHub)	4ad16e7f0f86e364c4e7a74f240c76737de2845d3ff13e38a2c4437cfea2af8b	0	0
Turla Group Lateral Movement	Markus Neis	Sigma Integrated Rule Set (GitHub)	a84f3c195555e22fcc4045469fd306dbb60cf28e91ae7b9325eb49aeda608af7	0	0
Turla Group Lateral Movement	Markus Neis	Sigma Integrated Rule Set (GitHub)	baa2e26b5f61d81ea9128226f369bdc536ba0a183e703eaafc23228dffbd64bc	0	0
Turla Group Lateral Movement	Markus Neis	Sigma Integrated Rule Set (GitHub)	dca19d018ba977a72de3571dc1f68228d2444d8b447b50e25b07422b5b014d9c	0	0
Turla Group Named Pipes	Markus Neis	Sigma Integrated Rule Set (GitHub)	5c1a908c4195fe1b85776a2a1c86cef843d6c40a00070ca9c5ab3043dc19a164	0	0
Turla PNG Dropper Service	Florian Roth	Sigma Integrated Rule Set (GitHub)	2181500508cba32078d248a61c926bf73a4bb6ebc4bececfd9d4ac607b57151d	0	0
Tycoon Ransomware	Ariel Millahuel	SOC Prime Threat Detection Marketplace	a1c44f103e75c8295cdbb587af4bac07f2b77445d54c17a424e7dce924a981ce	0	0
Typical HiveNightmare SAM File Export	Florian Roth	Sigma Integrated Rule Set (GitHub)	f89983755305fab46f3677edade72743effd233979db77ffa6c51a9d1fb4a18c	0	0
UAC Bypass Abusing Winsat Path Parsing - File	Christian Burkard	Sigma Integrated Rule Set (GitHub)	bb336c05f65b92ba4f8c077675fd297597dc9e6a58d623eb2a05ba80991cf674	0	0

UAC Bypass Abusing Winsat Path Parsing - Process	Christian Burkard	Sigma Integrated Rule Set (GitHub)	3336002627a5fff9960ca0a12f53f9173bf13d359096c010f818ad83f0bd3d60	0	0
UAC Bypass Abusing Winsat Path Parsing - Registry	Christian Burkard	Sigma Integrated Rule Set (GitHub)	27a9b69a6e2addb8fe0735e96f0d27ace4b79d17eefd764ce3f0288f74cb21c1	0	0
UAC Bypass Using .NET Code Profiler on MMC	Christian Burkard	Sigma Integrated Rule Set (GitHub)	e72fb1b5f98a1609a868416ee85fb716eb8e4705f84b33fd471cf747357dea7c	0	0
UAC Bypass Using Consent and Comctl32 - File	Christian Burkard	Sigma Integrated Rule Set (GitHub)	0bc48db9b102772d4daac62f85032a7501fed1102a95f95e8414a0dd3e51732c	0	0
UAC Bypass Using Consent and Comctl32 - Process	Christian Burkard	Sigma Integrated Rule Set (GitHub)	45716a61474d8af25ba7318e0bcc946490ebaf1a0ea6c9a73d6fa3d572e58ae6	0	0
UAC Bypass Using Disk Cleanup	Christian Burkard	Sigma Integrated Rule Set (GitHub)	639d8d816b374bf0b59c239c80f872bc5c00756e4888cc7934f8a33386306d57	0	0
UAC Bypass Using DismHost	Christian Burkard	Sigma Integrated Rule Set (GitHub)	84ae6514a422f3ac64733fe09e8c77e483ddc11d6eec7b8b1f5bf41dade82970	0	0
UAC Bypass Using MSConfig Token Modification - File	Christian Burkard	Sigma Integrated Rule Set (GitHub)	1d94cdf7ebb62637f664d4e56943049dfd2e84e3a534202d08775a957375ee59	0	0
UAC Bypass Using MSConfig Token Modification - Process	Christian Burkard	Sigma Integrated Rule Set (GitHub)	fed3f4e9a7b7505b5d9cf3fa38366c77ae1afaf2a73f5ec6e4e82353cb87e312	0	0
UAC Bypass Using NTFS Reparse Point - File	Christian Burkard	Sigma Integrated Rule Set (GitHub)	b61e713566d145c79ce59678aadb8a675e19a1177e0477c9916dae6960d75e1e	0	0
UAC Bypass Using NTFS Reparse Point - Process	Christian Burkard	Sigma Integrated Rule Set (GitHub)	b04ae33635c5e4e7fe2dc9592b339835bcf2233b6e640991cf271389ea49fb2d	0	0
UAC Bypass Using WOW64 Logger DLL Hijack	Christian Burkard	Sigma Integrated Rule Set (GitHub)	136d5312f0c32e4f8a7ed5923499a1fb0d03c457a9b9ff2e66d2d833900dd856	0	0
UAC Bypass Using Windows Media Player - File	Christian Burkard	Sigma Integrated Rule Set (GitHub)	dea23a2bff0dfc0ed3530c94cc3fa73835c8ee53d7dc7b6426775799cb4c719e	0	0
UAC Bypass Using Windows Media Player - Process	Christian Burkard	Sigma Integrated Rule Set (GitHub)	ddadf6d9fd6af912e7f512980649fd8c1628beae5483c5f009920946687a91c0	0	0

UAC Bypass Using Windows Media Player - Registry	Christian Burkard	Sigma Integrated Rule Set (GitHub)	06a48f1443d5688a49e7b4d5436e507df7fcfeb8780da328f16235c4c06d927f	0	0
UAC Bypass Via Wsreset	oscd.community, Dmitry Uchakin	Sigma Integrated Rule Set (GitHub)	46af1a978d9d6da64e0730a4b0d6dfeb8cab34fe21a2fdc0d3b8e0a428e12c21	0	0
UAC Bypass WSReset	Christian Burkard	Sigma Integrated Rule Set (GitHub)	03fc63d53dd6f6eeb7fef5848db2e4cd11fc7177c187c398320bb3934b751d87	0	0
UAC Bypass With Fake DLL	oscd.community, Dmitry Uchakin	Sigma Integrated Rule Set (GitHub)	f7b3aa6e9bcd6bb0bf047e633bb513434546a05f9322c433f8df8c2355115339	0	0
UAC Bypass via Event Viewer	Florian Roth	Sigma Integrated Rule Set (GitHub)	3a5e9509b313781bf9324f49cac4a71e1e5e822abacd7f2707c6d32f8920aea1	0	0
UAC Bypass via Event Viewer	Florian Roth	Sigma Integrated Rule Set (GitHub)	4134cd9d74207db899c24fb73563c311684932a317e61fe905fdc29a75f69109	0	0
UIPromptForCredentials DLLs	Roberto Rodriguez (Cyb3rWard0g), OTR (Open Threat Research)	Sigma Integrated Rule Set (GitHub)	d95ca36c302040f620589faab34078391fb9db19ee77118e3ad298784775d65b	0	0
UMWorkerProcess Creating Unusual Child Process CVE-2021-26857 (via cmdline)	SOC Prime Team, Microsoft	SOC Prime Threat Detection Marketplace	282370a5b2c99cb2055e32a9c50853be0a162c16914c919ee60730f93e7a1902	0	0
UNC2452 PowerShell Pattern	Florian Roth	Sigma Integrated Rule Set (GitHub)	f91a07dae0817dd517cae4782092e392760c32e680fb4b40f69789c8ea2642c7	0	0
USB Device Plugged	Florian Roth	Sigma Integrated Rule Set (GitHub)	f231038326d2da7583778551de319d33b9b9529e55671b62cbdd58a4a4697507	0	0
UnReCom RAT (Possible New Adwind variant)	Ariel Millahuel	SOC Prime Threat Detection Marketplace	4d7d569ef6ec13af576994a62b027bbec44b85374393abedc5f477ee650e0455	0	0
UnReCom RAT (Possible New Adwind variant)	Ariel Millahuel	SOC Prime Threat Detection Marketplace	5dee39e59001813316f98d63213edd7684633d33a54507273b7feb22753fb9a32	0	0
Unauthenticated file read in Cisco ASA & Cisco Firepower CVE-2020-3452 (via web)	Roman Ranskyi	SOC Prime Threat Detection Marketplace	0cfd9195be7ced6620371c11ca6323fee3c0b5d0b9ea805f017a841110683b91	0	0
Unauthenticated file read in Cisco ASA & Cisco Firepower CVE-2020-3452 (via web)	Roman Ranskyi	SOC Prime Threat Detection Marketplace	789fc5bb01e3f3b18df9537ead68abfcaacecbf0a526ab8207c7e6f198d8a5e3	0	0

Uncommon External Facing Application Service	SOC Prime Team	SOC Prime Threat Detection Marketplace	1c5a833abe2b826a6d444da72f62ea23742c5770ece407730a66ef8300dbdcfd	0	0
Unidentified Attacker November 2018	@41thexplorer, Microsoft Defender ATP	Sigma Integrated Rule Set (GitHub)	120841a228484caff2f660319625b672d8b268d649f0522d99d2a59c6c60f3b3	0	0
Unidentified Attacker November 2018	@41thexplorer, Microsoft Defender ATP	Sigma Integrated Rule Set (GitHub)	8f2c777b3dc85aa4c4663fc4de3a1d8bd273ea3506fd8481a76de1a0ffb2c6b4	0	0
Unidentified Attacker November 2018	@41thexplorer, Microsoft Defender ATP	Sigma Integrated Rule Set (GitHub)	b08d52ecad9f030d424d9663403423559c1951018ae4cafc8f10b0ef2ad0f77f	0	0
Unidentified Attacker November 2018	@41thexplorer, Microsoft Defender ATP	Sigma Integrated Rule Set (GitHub)	b5002bc251d42658f759ab88719976f8698c099d4450bc798cdbf9e219cfab1e	0	0
Unidentified Attacker November 2018	@41thexplorer, Microsoft Defender ATP	Sigma Integrated Rule Set (GitHub)	c02ac5aedb6c89eac4725d7a30df43b4631994b8ad7cee3473099d0926df9a80	0	0
Uninstall Crowdstrike Falcon	frack113	Sigma Integrated Rule Set (GitHub)	7319e259606b1d76ca31570f4a8256ad40f0297486f907c00ae96d5721d87794	0	0
Unknown Exchange 0day Relevant Crash Event (via application)	SOC Prime Team, Microsoft	SOC Prime Threat Detection Marketplace	df18dcdc7e0de08d0a24ac99b5e39af9106c4594de1e213961a00f36bb1fb7cf	0	0
Unsigned Image Loaded Into LSASS Process	Teymur Kheirkhabarov, oscd.community	Sigma Integrated Rule Set (GitHub)	41a3e620fba7b86366fe885ba1b20dbaae2be7596e2e9b194ab65dae5e4a7b53	0	0
Ursa Trojan	Ariel Millahuel	SOC Prime Threat Detection Marketplace	8aa514ad684698cba9daddea167e737b38eac3917d5a8c44b11684e4fe0819f3	0	0
Ursa Trojan	Ariel Millahuel	SOC Prime Threat Detection Marketplace	d16ef015b59d30d0df3ba7fbe07aa8edeac37ec141c0ee5852c1a88ce602094a	0	0
Ursnif	megan201296	Sigma Integrated Rule Set (GitHub)	4e3571c62f910de9f4ea1bd62ee26b408ad26db209250c61eb74239ce71fc827	0	0
Ursnif Malware C2 URL Pattern	Thomas Patzke	Sigma Integrated Rule Set (GitHub)	d983b04ec090162c842c62845c96abbce6bba8d1a7611826053d7ba25fd8918c	0	0
Ursnif Malware Download URL Pattern	Thomas Patzke	Sigma Integrated Rule Set (GitHub)	f320e891edef939c4d89f2e964476f57bf9d8a92415164cce650183f1820be10	0	0
Usage of Sysinternals Tools	Markus Neis	Sigma Integrated Rule Set (GitHub)	6caf06038ef037f3ac3da62377560d3544dd6d6b89ac3959ecb666489940b9aa	0	0
Usage of renamed binaries(wmic, regsvr32)	Den Iuzvyk	SOC Prime Threat Detection Marketplace	c21c41fa3a1749d217cfe78b997b24c415176f9c5f587ddb417fb4893325d908	0	0

Use Get-NetTCPConnection	frack113	Sigma Integrated Rule Set (GitHub)	84f3662b966321c45129926b0bf88e5845313e0cd9f0b7ec89f79f37c2fbeaef	0	0
Use Get-NetTCPConnection	frack113	Sigma Integrated Rule Set (GitHub)	e69f9e383811e595a9561c923eddfc5df48f9e54f4df8fa281fcef6b501048ac	0	0
User Access Blocked by Azure Conditional Access	AlertIQ	Sigma Integrated Rule Set (GitHub)	c40f9bf14b74802e89f6f64d76fd9c7700fe103474cfc637cd33d1fef4c7f287	0	0
User Added to an Administrator's Azure AD Role	Raphaël CALVET, @MetallicHack	Sigma Integrated Rule Set (GitHub)	339c344d69b808b4c773cb492f914a59b8d3d67cc415f392ef0202cbe4837d7c	0	0
User Couldn't Call a Privileged Service 'LsaRegisterLogonProcess'	Roberto Rodriguez (source), Ilyas Ochkov (rule), oscd.community	Sigma Integrated Rule Set (GitHub)	11a18935f3a8e1e4c4cc09e59d69155a1777e2762605adcc495c58cc96abce1d	0	0
Using AppVLP To Circumvent ASR File Path Rule	Sreeman	Sigma Integrated Rule Set (GitHub)	e95a64931dc936ea0b79a4d48a5cf5f247dc55a78f0cb754480de9f58dcd9ce2	0	0
Using SettingSyncHost.exe as LOLBin	Anton Kutepov, oscd.community	Sigma Integrated Rule Set (GitHub)	90604343649b0a434f2aaf1ac225f1535b3d2b0766ba92bc80cfaed426f07695	0	0
Using Sticky-keys To Obtain Unauthenticated, Privileged Console Access	Sreeman	Sigma Integrated Rule Set (GitHub)	62e0a8cc199a4d0a9766d75ef3213180a3865b74ce2be5948d1bc1fc5aa68e49	0	0
Utilization of "expand.exe" to deploy files from "Temp" folders	Ariel Millahuel	SOC Prime Threat Detection Marketplace	ade628a427870c8c3442dd7aac9c2d401c3e96ef82d4b92d8128cdeeff3062e9	0	0
VBA DLL Loaded Via Microsoft Word	Antonlovesdnb	Sigma Integrated Rule Set (GitHub)	1c4b9974eadae6764e88b6287305d477f5d777a06dd5a75e4773cea197fb1b0a	0	0
VMware vCenter Server File Upload CVE-2021-22005	Sittikorn S	Sigma Integrated Rule Set (GitHub)	307fdbfc019c602d9b897165bdfdff09e71bae733f6e0a8b5305ca81f5f7cc6d	0	0
Valak Behavior (Sysmon and Cmdline)	Ariel Millahuel	SOC Prime Threat Detection Marketplace	bd88e7274c701ecb8921074eb102f73f8f0d4a5ac0708ddae5a1e369ef71569b	0	0
Valid Users Failing to Authenticate From Single Source Using Kerberos	Mauricio Velazco, frack113	Sigma Integrated Rule Set (GitHub)	a3ae92169de3a473b385950d6a3e85b2a991c8be31e68ccb84577f16515c3407	0	0

Valid Users Failing to Authenticate from Single Source Using NTLM	Mauricio Velazco	Sigma Integrated Rule Set (GitHub)	05e5abf2c5d151e82602b134f795f3449e651ab33f591a2f4a98aab8d54031f9	0	0
VeeamBackup Database Credentials Dump	frack113	Sigma Integrated Rule Set (GitHub)	912e511ef1e7ba499a5cf1552134869bb633ba21adbdddb20785e6c3ab04e761	0	0
Vjworm Trojan	Ariel Millahuel	SOC Prime Threat Detection Marketplace	a274e14c306334155818a08604184fc950850cf7facfe0df879c1608fda2cc4e	0	0
Volume Shadow Copy Mount	Roberto Rodriguez @Cyb3rWard0g, Open Threat Research (OTR)	Sigma Integrated Rule Set (GitHub)	632fbc79a450be1208f0c3c1246793ff703d551fb7163488db4d1de2b2483d5a	0	0
Vulnerable Netlogon Secure Channel Connection Allowed	NVISO	Sigma Integrated Rule Set (GitHub)	3f84718f22c39831d8b99ef0dc98874d6e50b02602ada051c9eafb98360fc647	0	0
WCE wceaux.dll Access	Thomas Patzke	Sigma Integrated Rule Set (GitHub)	183cf5523bdd58d20e93e3b2bb367c38caec4fe344a0aea45722954e9fe9ed9f	0	0
WMI Event Consumer Created Named Pipe	Florian Roth	Sigma Integrated Rule Set (GitHub)	01446bc086a25ac157aacfacf8ca447f2f195cd8dd67c3a8cb6a881dc5ac53be	0	0
WMI Modules Loaded	Roberto Rodriguez @Cyb3rWard0g	Sigma Integrated Rule Set (GitHub)	fb092b3aee3feb316c048a1249e1ac9639a63cac318318afd45bf38887b31b0c	0	0
WMI Persistence	Florian Roth, Gleb Sukhodolskiy, Timur Zinniatullin oscd.community	Sigma Integrated Rule Set (GitHub)	58154fd247cd9b589c6903a15ffa196e0e50cca640eeadc0ca86c289dbeae3bf	0	0
WMI Persistence	Florian Roth, Gleb Sukhodolskiy, Timur Zinniatullin oscd.community	Sigma Integrated Rule Set (GitHub)	85bc7739560701dd55a0c7eab1ee7b00c0ddea32b913c6e0b6798b889419591b	0	0
WMI Persistence	Florian Roth, Gleb Sukhodolskiy, Timur Zinniatullin oscd.community	Sigma Integrated Rule Set (GitHub)	a9246010da9b679de378be05b2d90c9171220c5fd5b0545883bdad8a49e9811c	0	0
WMI Persistence	Florian Roth, Gleb Sukhodolskiy, Timur Zinniatullin oscd.community	Sigma Integrated Rule Set (GitHub)	aa847a1640b2ae82a6149c6f0b44f8ec7170516b4502113a92de7898285ff89b	0	0
WMI Persistence	Florian Roth, Gleb Sukhodolskiy, Timur Zinniatullin oscd.community	Sigma Integrated Rule Set (GitHub)	f674f8881516524de991b8439ddd2248fd25bacea659a067680337c89b7a6c5b	0	0
WMI Persistence - Command Line Event Consumer	Thomas Patzke	Sigma Integrated Rule Set (GitHub)	2d6a5c8b5ff6663f305abc5b7d611b99089e2cf4ad71b0b3f9a89d8d05d71a89	0	0
WMI Reconnaissance List Remote Services	frack113	Sigma Integrated Rule Set (GitHub)	122d74917c1ba5d7e854a6a25e2ce8bd997bfe1398c7b5ddaaecb88edf02edd8	0	0

WMI Script Host Process Image Loaded	Roberto Rodriguez (Cyb3rWard0g), OTR (Open Threat Research)	Sigma Integrated Rule Set (GitHub)	81314be6adb2ae8f1bd104c4f35d68c8ff62ddfea655e64c5b1c92082b72d5ae	0	0
WMIC Loading Scripting Libraries	Roberto Rodriguez (Cyb3rWard0g), OTR (Open Threat Research)	Sigma Integrated Rule Set (GitHub)	022ee32433f415a35cf214d689b7c20ea4d29ed50a5be04595877663d8128997	0	0
WMIExec VBS Script	Florian Roth	Sigma Integrated Rule Set (GitHub)	860cd791b52ed03d76e2842429f67b1ac870f8f77a5a09b472fbbf3c964ee708	0	0
WMImplant Hack Tool	NVISO	Sigma Integrated Rule Set (GitHub)	6b93b7bce89874009dd0ecb10a52f610736bcb6d33fe425d9295732660f6b7ab	0	0
WSH RAT behavior	Ariel Millahuel	SOC Prime Threat Detection Marketplace	0d8ca71c713cdf5f939ca8eea9288f6c9c665f224016b4672972ff569c13bb16	0	0
WSH RAT behavior	Ariel Millahuel	SOC Prime Threat Detection Marketplace	c542efb138f0e8fde0df28089aa73fd35cd12a439000e607e4e10b10ecb3f743	0	0
WSL Execution	oscd.community, Zach Stanford @svch0st	Sigma Integrated Rule Set (GitHub)	4deaea65e083744047018aa4fd0ccf242ffa901cc82a5f427d710fbb717c213e	0	0
WScript Launched By Powershell	Joe Security	Joe Security Rule Set (GitHub)	dd10c5eb1b4cfd51330d892c57a9cfe7ce41ac02ee121c141435ea97a71bb073	0	0
Wannacry Killswitch Domain	Mike Wade	Sigma Integrated Rule Set (GitHub)	1835f85f70bcf5e9613228e05d8ab33dae73c11d41a4e5876ceb6f2002b31167	0	0
Wbadmin Delete Systemstateback up	frack113	Sigma Integrated Rule Set (GitHub)	9aae4742b47a403c0d2871d344a6076cd6b797a267bbe2d0b85e607927ef3dc9	0	0
Wdigest CredGuard Registry Modification	Roberto Rodriguez (Cyb3rWard0g), OTR (Open Threat Research)	Sigma Integrated Rule Set (GitHub)	6b2853b0e68d3b3c786df7c3960aa8764840caaee74ca35f04ee828c6df43a68	0	0
Wdigest Enable UseLogonCredential	Roberto Rodriguez (Cyb3rWard0g), OTR (Open Threat Research)	Sigma Integrated Rule Set (GitHub)	549fd181a20cb87efd19fddc858140d8495cd434cc6a9b662dcc7d8bb35804ae	0	0
Weak Encryption Enabled and Kerberoast	@neu5ron	Sigma Integrated Rule Set (GitHub)	2be706f3f2686605d5ee19c899ca7bdb688e826ad3b82c1c873627c8aad568bf	0	0
WebDav Put Request	Roberto Rodriguez (Cyb3rWard0g), OTR (Open Threat Research)	Sigma Integrated Rule Set (GitHub)	52301a573727517b97c3069178ccee0ad367c8581abc440bbad2eec03af8c709	0	0
Webshell Detection by Keyword	Florian Roth	Sigma Integrated Rule Set (GitHub)	82f06847ea3a21b3565bc4d6d23aa0872cca19e1c69046bfffc795ba9dc7f76e	0	0
Webshell ReGeorg Detection Via Web Logs	Cian Heasley	Sigma Integrated Rule Set (GitHub)	3b59889f7c01566d9506c1b2b7b8b37af0e7f21424d03390fc64c4f32e4328f6	0	0

Webshell Recon Detection Via CommandLine & Processes	Cian Heasley	Sigma Integrated Rule Set (GitHub)	d9519d30d9c273a67a5b26f64e780cfeec59454accd4f3237419da2afbb82c8d	0	0
Webshell Remote Command Execution	Ilyas Ochkov, Beyu Denis, oscd.community	Sigma Integrated Rule Set (GitHub)	6f8b96808977daa36d34a09923e361bdd17a9353c89c25c73253f29bb35b833d	0	0
WhoAmI as Parameter	Florian Roth	Sigma Integrated Rule Set (GitHub)	31e555cd1c55ce445dfd8bd7c10843187298b45b39b33ddf41b5bce83e212c86	0	0
WinRM Access with Evil-WinRM	frack113	Sigma Integrated Rule Set (GitHub)	5ad71f4134dddf8bef6aed44120ca9d774108b3c4e8b7e322ca38e989a8cf176	0	0
Windows Defender AMSI Trigger Detected	Bhabesh Raj	Sigma Integrated Rule Set (GitHub)	9944cda138f9f219e918f109ce968902b602a32f60c6ed006bb112b15ba2dede	0	0
Windows Defender Download Activity	Matthew Matchen	Sigma Integrated Rule Set (GitHub)	0de6e296fdb440317bd15b3aa29b6d99b17b08dea792264888e93fa3c62f9514	0	0
Windows Defender Exclusion Set	@BarryShooshooga	Sigma Integrated Rule Set (GitHub)	29051fc71a16779223e0e3bf42ba8b7a5e0b066a0b0cf3a34684da1337ca0f4b	0	0
Windows Defender Exclusions Added	Christian Burkard	Sigma Integrated Rule Set (GitHub)	20ee93291281ad45d4704a39eb182e955d4353c917a1872e15423a2ebfef6378	0	0
Windows Defender Exclusions Added	Christian Burkard	Sigma Integrated Rule Set (GitHub)	2231f93169c7efed228559b8ba20664ec6cf05f5a2df8494b89151752237fb8c	0	0
Windows Defender Exclusions Added	Christian Burkard	Sigma Integrated Rule Set (GitHub)	52d226d49903df8a4f8ad9d9c7932a887e76679a19f5dc4a55db4471cb55b454	0	0
Windows Defender Exclusions Added	Christian Burkard	Sigma Integrated Rule Set (GitHub)	aa5b43fba93f194b9cb53e9215833465cb9fbfb8f9787ee9ac6ec99db12d40b7	0	0
Windows Defender Malware Detection History Deletion	Cian Heasley	Sigma Integrated Rule Set (GitHub)	a69f67541c11d90298cb228bee82651387015e4cd30917b3511fde5c028f1eb0	0	0
Windows Defender Threat Detected	Ján Trenčanský	Sigma Integrated Rule Set (GitHub)	cf90b923dcb2c8192e6651425886607684aac6680bf25b20c39ae3f8743aebf1	0	0
Windows Defender Threat Detection Disabled	Ján Trenčanský, frack113	Sigma Integrated Rule Set (GitHub)	41872a2c86ff9bf310cf8a81b0235040c25793f1fe6255fdc5bf771cd716ddfc	0	0

Windows Defender Threat Detection Disabled	Ján Trenčanský, frack113	Sigma Integrated Rule Set (GitHub)	7998082d3f734247061e2d59f83e2a3a523414bed9e74c2adb7bcb0404abce97	0	0
Windows Defender Threat Detection Disabled	Ján Trenčanský, frack113	Sigma Integrated Rule Set (GitHub)	a6317aefcc7e070bf2d65b66a15af84858276fd8c4350ccb4cc0bc93261757ea	0	0
Windows Defender Threat Detection Disabled	Ján Trenčanský, frack113	Sigma Integrated Rule Set (GitHub)	ed87c230c6d4207b37197d5b9085406475eec57fdb0315aa3f474a07c39806f6	0	0
Windows Defender Threat Detection Disabled	Ján Trenčanský, frack113	Sigma Integrated Rule Set (GitHub)	f2d1be0ba54a53b3a9599c9697ecd28df209373ff460d809e0da374627734853	0	0
Windows Defender Threat Detection Disabled	Ján Trenčanský, frack113	Sigma Integrated Rule Set (GitHub)	f41376cbd0bf111c80a06c14f23ee727ec0a64de4ab379cc3853b54b5d945035	0	0
Windows Firewall Profile Disabled	Austin Songer @austinsonger	Sigma Integrated Rule Set (GitHub)	489692e72dc0017d68cdd2188f43e162f46de9955dce51c32323345919b76b0e	0	0
Windows Kernel and 3rd-Party Drivers Exploits Token Stealing	Teymur Kheirkhabarov (source), Daniil Yugoslavskiy (rule)	Sigma Integrated Rule Set (GitHub)	25ad3dcfbd1578bd1784acb166bf4273467664ef291ec4722fa1e4361346b135	0	0
Windows Management Instrumentation DLL Loaded Via Microsoft Word	Michael R. (@nahamike01)	Sigma Integrated Rule Set (GitHub)	3e47f5ae1f3a80668c79b22bb11fbfefb4a1a9c5078948a80bb884fa77e652e4	0	0
Windows Pcap Drivers	Cian Heasley	Sigma Integrated Rule Set (GitHub)	c93c0cd47a9a01f1270c2cc43da3d19744639e155de50e64311df30ce6763d16	0	0
Windows PowerShell Upload Web Request	frack113	Sigma Integrated Rule Set (GitHub)	80e1441e8251586c742da610b4bceb4d94fbe79f4e8b64b9745b6a11da90d7c1	0	0
Windows PowerShell User Agent	Florian Roth	Sigma Integrated Rule Set (GitHub)	107a4de06e843fc296a19ef4626692a39338e909a237bf8636b24aef02e6dbba	0	0
Windows PowerShell Web Request	James Pemberton / @4A616D6573	Sigma Integrated Rule Set (GitHub)	8f476a2016a135fab13276812845b457aa420dac974d15d909682f6d25fefbec	0	0
Windows Registry Persistence COM Key Linking	Kutepov Anton, oscd.community	Sigma Integrated Rule Set (GitHub)	3a5176242220f6a6e49fd00b2b47af50918dae9ca9edecfcfa843475d2e01df0	0	0
Windows Registry Trust Record Modification	Antonlovesdnb	Sigma Integrated Rule Set (GitHub)	9292d14bdf79582c701fad33de8f018f0151bb6acfc181fba0dd5d223cee498c	0	0

Windows Screen Capture with CopyFromScreen	frack113	Sigma Integrated Rule Set (GitHub)	f8a626af728b3adf32c5a523da76b149e1f41d45e55c4f3b2cb7895c3920b449	0	0
Windows Spooler Service Suspicious Binary Load	FPT.EagleEye, Thomas Patzke (improvements)	Sigma Integrated Rule Set (GitHub)	36004bbb9055623fa5dd3851566dfcd02d35df3bb87caf7ba2e7e876268fb66d	0	0
Windows Spooler Service Suspicious File Deletion	Bhabesh Raj	Sigma Integrated Rule Set (GitHub)	2905d462b4ac73a3e5bd0955b9303d3a939f9fd1715035a35ceccc567892e882	0	0
Windows Sysvol File Modification	SOC Prime Team	SOC Prime Threat Detection Marketplace	3d8c9cb6ebe5a3e7f4ebd1898e2d1b488d7b3118afdd8cf4e5a3e5bfd012a7ba	0	0
Windows Update Client LOLBIN	FPT.EagleEye Team	Sigma Integrated Rule Set (GitHub)	dab442a95ac4a7904c20db69e9f390b99d4b5268e3afd391c43a1c522ad4b3f7	0	0
Windows Update Error	frack113	Sigma Integrated Rule Set (GitHub)	879bef301d05e0c53bf1deb87f0ccdd7cba387cea145b72e6110cabcc2a30343	0	0
Windows WebDAV User Agent	Florian Roth	Sigma Integrated Rule Set (GitHub)	917187eb4a5bcdd061118cd2392a86d4b4a05e138f59f268c5906f5df879ff88	0	0
Winlogon Notify Key Logon Persistence	frack113	Sigma Integrated Rule Set (GitHub)	4edd1b8a91c2781bd88eb5be92c3ab1e0f5498018cb1efb7d6fe4df7f2be05c3	0	0
Winnti Pipemon Characteristics	Florian Roth, oscd.community	Sigma Integrated Rule Set (GitHub)	c1e10ac2693c07c301e475b876c1c19fee91b87063b8908441ea3c5279ae0f65	0	0
Winrar Compressing Dump Files	Florian Roth	Sigma Integrated Rule Set (GitHub)	751aa9f10bb034af3fd96ddfd10baf6ff799f92e0d2802249e1d957644c16591	0	0
Winword.exe Loads Suspicious DLL	Victor Sergeev, oscd.community	Sigma Integrated Rule Set (GitHub)	1441bc53b94995e7a28e23c96d5c3742700e48b1cb9d1954b559f58eba877e94	0	0
Wmic Launch Msiexec	Joe Security	Joe Security Rule Set (GitHub)	db017371e0e4d727e167ff37855a4a5e1c6a2341edbbe11beb3b97caecdcca09	0	0
Wmic Uninstall Security Product	Florian Roth	Sigma Integrated Rule Set (GitHub)	deb3cdf84cc34aa311e6bb923cb0b259584940b4e6d724a32706971b5147607f	0	0
Wmic download via msiexec	Joe Security	Joe Security Rule Set (GitHub)	0104f72cd9f54a0c07ad11f45d22d923453e62473b89d3af0a474a3bc1dceae7	0	0
Wmiprvse Wbemcomn DLL Hijack	Roberto Rodriguez (Cyb3rWard0g), OTR (Open Threat Research)	Sigma Integrated Rule Set (GitHub)	15aaaaea2f031734f9cdf2b6b2daccee96287228d9b63de3ef8ae60bb64c31d5	0	0
Wmiprvse Wbemcomn DLL Hijack	Roberto Rodriguez (Cyb3rWard0g), OTR (Open Threat Research)	Sigma Integrated Rule Set (GitHub)	62987a80e784c70fc4631c63515a0e98b3c705e1d044ad445298bdbe93ef6002	0	0
Wmiprvse Wbemcomn DLL Hijack	Roberto Rodriguez (Cyb3rWard0g), OTR (Open Threat Research)	Sigma Integrated Rule Set (GitHub)	b20f50174b7445b6c6fde810dcacb4c33c3a76f0102c37667f15cf44550c8ea8	0	0

Wmiprvse Wbemcomn DLL Hijack	Roberto Rodriguez (Cyb3rWard0g), OTR (Open Threat Research)	Sigma Integrated Rule Set (GitHub)	b2fa9548d438421a3ea1321b77228fbd3bd81a77dc8dc2f6b7c5ca51b335f139	0	0
Wow6432Node Classes Autorun Keys Modification	Victor Sergeev, Daniil Yugoslavskiy, Gleb Sukhodolskiy, Timur Zinniatullin, oscd.community, Tim Shelton, frack113 (split)	Sigma Integrated Rule Set (GitHub)	b8e0eed90b7762f65047e747e751f1b66397e091c997b89270e3f30cef044193	0	0
Write Protect For Storage Disabled	Sreeman	Sigma Integrated Rule Set (GitHub)	909789172b6e132b51b9baf5ca447732e8d01ea892f0b2af3d78463800617785	0	0
Writing Local Admin Share	frack113	Sigma Integrated Rule Set (GitHub)	e62e7dc0b12394b319cbb70f3b434d86a1a4e97c05c4cf3939efba22e4c603c7	0	0
Wscript download file into temp location from wordpress site	Joe Security	Joe Security Rule Set (GitHub)	e4fa44290012b08a6024fd7259647320ed7bcccd8f789391420ae07ec797c56c	0	0
Zeppelin Ransomware detection	Ariel Millahuel	SOC Prime Threat Detection Marketplace	1dd1813f8e36c59d89368c568c00d0b7df113cf1294162c9aa9daa50f72759d0	0	0
Zerologon Exploitation Using Well-known Tools	Demyan Sokolin @_drd0c, Teymur Kheirkhabarov @HeirhabarovT, oscd.community	Sigma Integrated Rule Set (GitHub)	b78e7cfa9a545243900dd20e214093ca8ccdfb84c4e2701d711df94c2325ad45	0	0
Zeropadypt Ransomware	Ariel Millahuel	SOC Prime Threat Detection Marketplace	2903b1fee135b2ab2e99ea7d454b87f0387bb5adbf0a87b8a952cdf559cc0fc0	0	0
Zip A Folder With PowerShell For Staging In Temp	frack113	Sigma Integrated Rule Set (GitHub)	14067c72922c986650e783f9228ddb9fe698c382df3698e163c4f670cf050465	0	0
Zip A Folder With PowerShell For Staging In Temp	frack113	Sigma Integrated Rule Set (GitHub)	4d383989e445c74fd8a77bd2cf57f7a1ffccaa221d9d197cc2167b4023e34425	0	0
Zip A Folder With PowerShell For Staging In Temp	frack113	Sigma Integrated Rule Set (GitHub)	4f19758bce122aae71a356110cf88e95df101e099a2b95e2472e44201244475d	0	0
Zip A Folder With PowerShell For Staging In Temp	frack113	Sigma Integrated Rule Set (GitHub)	70e3421aca89a28b1d599aafae9fdd903822e32a691eb39731812bc02f3b9dcb	0	0
Zip A Folder With PowerShell For Staging In Temp	frack113	Sigma Integrated Rule Set (GitHub)	c85d82a8951189fc9e17094e9738f8f03ee60e483cb4725d6062de14e1663ff1	0	0
Zip A Folder With PowerShell For Staging In Temp	frack113	Sigma Integrated Rule Set (GitHub)	deeb1a213004e4f328c59f035fe5bdbfe766ac3d8a0ea7f9a916c12bc145491f	0	0

Zip A Folder With PowerShell For Staging In Temp	frack113	Sigma Integrated Rule Set (GitHub)	f9da722f2b9be68744c84591d71fc78f53410669a0b7da802cb3abdb56d3fd72	0	0
dotNET DLL Loaded Via Office Applications	Antonlovesdnb	Sigma Integrated Rule Set (GitHub)	df9179ffc950a7d9549e0d76b5a95a94d3b366fcfde63b70a6b7a7215d0d97b5	0	0
iOS Implant URL Pattern	Florian Roth	Sigma Integrated Rule Set (GitHub)	c902b9b5f87c7faea1b8d842747d3620db497a294d8484a4d4f30d8efb95f770	0	0
ixware Stealer	Ariel Millahuel	SOC Prime Threat Detection Marketplace	8b103e0e94ed879b2e6703457646fa5fdedf95419931f137df2e5938b4c484be	0	0
ixware Stealer	Ariel Millahuel	SOC Prime Threat Detection Marketplace	c1badf4bce1bace265e5cf652abbe2eb12efdb34e62690f367fcb35a7dfa2c64	0	0
njRat payload	Den Iuzvyk	SOC Prime Threat Detection Marketplace	3199f91af1499ae38d1caaccdebf0b49c00acab265a73ae5522d9c9bb2d4178b	0	0
notepad++.exe DLL search order hijacking(Sysmon)	Den Iuzvyk	SOC Prime Threat Detection Marketplace	088db9822e808265d50798b894fa0f13dc765ec299836dddc752dfe4b8829071	0	0
powershell registry execution via wmic	Joe Security	Joe Security Rule Set (GitHub)	f33d9692bdb337bf2369df43be996b214f4819827e400c798075464804b0c4e2	0	0
rundll32 launch mshta and run script from internet	Joe Security	Joe Security Rule Set (GitHub)	529f06043b5ec852cb07ebe7880eaedad5dfcb5b041100dd85458b5ae5d43c1c	0	0
smbexec.py Service Installation	Omer Faruk Celik	Sigma Integrated Rule Set (GitHub)	5a4bf43081cef897622ab39eb1011671616e9b2dd0dbea9e10669d85790dcd9c	0	0
tencentsoso.exe DLL search order hijacking(Sysmon)	Den Iuzvyk	SOC Prime Threat Detection Marketplace	e11fbf7c8ec3e7d6d9b7b81e6199ac7b3c7ff5da85494aa9578263862a0bc54a	0	0