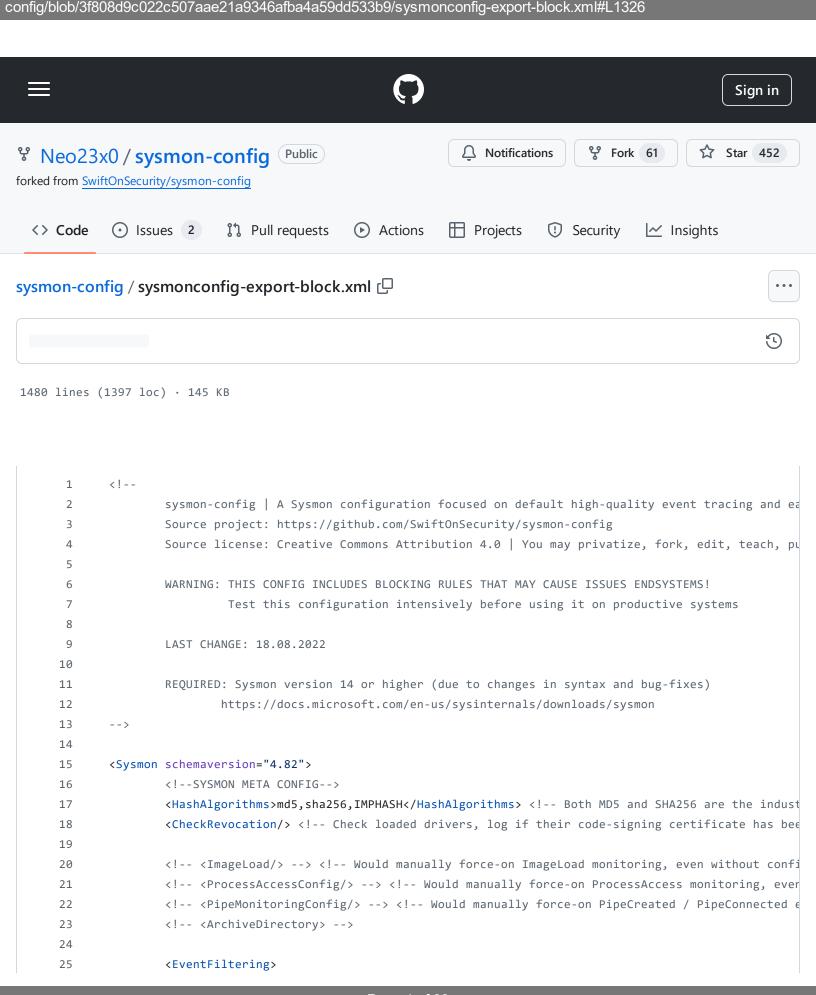
sysmon-config/sysmonconfig-export-block.xml at 3f808d9c022c507aae21a9346afba4a59dd533b9 · Neo23x0/sysmon-config · GitHub - 31/10/2024 16:28 https://github.com/Neo23x0/sysmon-



config/blob/3f808d9c022c507aae21a9346afba4a59dd533b9/sysmonconfig-export-block.xml#L1326

```
26
27
                        <!--SYSMON EVENT ID 1 : PROCESS CREATION [ProcessCreate]-->
28
                                     <!--COMMENT:
                                                               All processes launched will be logged, except for what matches a ru
                                                  to avoid user-mode executables imitating other process names to avoid loggi
29
30
                                                  Ultimately, you must weigh CPU time checking many detailed rules, against t
31
                                                   Beware of Masquerading, where attackers imitate the names and paths of legi
                                                   code signatures to validate, but Sysmon does not support that. Look into Ad
32
33
34
                                     <!--DATA: UtcTime, ProcessGuid, ProcessID, Image, FileVersion, Description, Product
                        <RuleGroup name="" groupRelation="or">
35
                                     <ProcessCreate onmatch="exclude">
36
37
                                                   <CommandLine condition="contains">\Machine\Scripts\Startup\ipamprovisioning
                                                   <!--SECTION: Microsoft Windows-->
38
                                                   <CommandLine condition="is">"C:\Windows\system32\cscript.exe" /nologo "Moni
39
                                                   <CommandLine condition="begin with"> "C:\Windows\system32\wermgr.exe" "-que
40
                                                   <CommandLine condition="begin with">C:\Windows\system32\wbem\wmiprvse.exe
41
                                                   <CommandLine condition="begin with">C:\Windows\system32\wbem\wmiprvse.exe
42
                                                   <CommandLine condition="is">C:\Windows\system32\wermgr.exe -upload</Command</pre>
43
                                                   <CommandLine condition="is">C:\Windows\system32\SearchIndexer.exe /Embeddir
44
                                                   <CommandLine condition="is">C:\windows\system32\wermgr.exe -queuereporting
45
                                                   <CommandLine condition="is">\??\C:\Windows\system32\autochk.exe *</CommandL</pre>
46
                                                   <CommandLine condition="is">\SystemRoot\System32\smss.exe</CommandLine> <!-</pre>
47
                                                   <CommandLine condition="is">C:\Windows\System32\RuntimeBroker.exe -Embeddir
48
                                                   <Image condition="is">C:\Program Files (x86)\Common Files\microsoft shared\
49
50
                                                   <Image condition="is">C:\Windows\System32\TokenBrokerCookies.exe</Image> <!</pre>
51
                                                   <Image condition="is">C:\Windows\System32\plasrv.exe</Image> <!--Windows: F</pre>
52
                                                   <Image condition="is">C:\Windows\System32\wifitask.exe</Image> <!--Windows:</pre>
53
                                                   <Image condition="is">C:\Windows\system32\PrintIsolationHost.exe</Image> <!</pre>
54
                                                   <Image condition="is">C:\Windows\system32\SppExtCom0bj.Exe</Image> <!--Windows\system32\SppExtCom0bj.Exe</Image> <!--Windows\system32\SppExtCom0bj.Exe</Ima
55
                                                   <Image condition="is">C:\Windows\system32\audiodg.exe</Image> <!--Windows:</pre>
56
57
                                                   <Image condition="is">C:\Windows\system32\conhost.exe</Image> <!--Windows:</pre>
                                                   <Image condition="is">C:\Windows\system32\mobsync.exe</Image> <!--Windows:</pre>
58
                                                   <Image condition="is">C:\Windows\system32\musNotification.exe</Image> <!--♭</pre>
59
                                                   <Image condition="is">C:\Windows\system32\musNotificationUx.exe</Image> <!-</pre>
60
                                                   <Image condition="is">C:\Windows\system32\powercfg.exe</Image> <!--Microsof</pre>
61
                                                   <Image condition="is">C:\Windows\system32\sndVol.exe</Image> <!--Windows: \</pre>
62
                                                   <Image condition="is">C:\Windows\system32\sppsvc.exe</Image> <!--Windows: $</pre>
63
                                                   <Image condition="is">C:\Windows\system32\wbem\WmiApSrv.exe</Image> <!--Wir</pre>
64
                                                   <IntegrityLevel condition="is">AppContainer</IntegrityLevel> <!--Windows: []</pre>
65
                                                   <ParentCommandLine condition="begin with">%%SystemRoot%%\system32\csrss.exe
66
                                                   <ParentCommandLine condition="is">C:\windows\system32\wermgr.exe -queuerepd
67
                                                   <CommandLine condition="is">C:\WINDOWS\system32\devicecensus.exe UserCxt/
68
69
                                                   <CommandLine condition="is">C:\Windows\System32\usocoreworker.exe -Embeddir
                                                   <ParentImage condition="is">C:\Windows\system32\SearchIndexer.exe</ParentIn</pre>
70
                                                   <!--SECTION: Windows:svchost-->
71
```

72	<commandline< td=""><td><pre>condition="is">C:\Windows\system32\svchost.exe -</pre></td><td>k appmodel -s</td></commandline<>	<pre>condition="is">C:\Windows\system32\svchost.exe -</pre>	k appmodel -s
73	<commandline< td=""><td><pre>condition="is">C:\Windows\system32\svchost.exe -</pre></td><td>k appmodel -p</td></commandline<>	<pre>condition="is">C:\Windows\system32\svchost.exe -</pre>	k appmodel -p
74	<commandline< td=""><td><pre>condition="is">C:\Windows\system32\svchost.exe -</pre></td><td>k appmodel<!--<code-->Cc</td></commandline<>	<pre>condition="is">C:\Windows\system32\svchost.exe -</pre>	k appmodel <code Cc
75	<commandline< td=""><td><pre>condition="is">C:\Windows\system32\svchost.exe -</pre></td><td>k appmodel -p</td></commandline<>	<pre>condition="is">C:\Windows\system32\svchost.exe -</pre>	k appmodel -p
76	<commandline< td=""><td><pre>condition="is">C:\Windows\system32\svchost.exe -</pre></td><td>k camera -s Fr</td></commandline<>	<pre>condition="is">C:\Windows\system32\svchost.exe -</pre>	k camera -s Fr
77	<commandline< td=""><td><pre>condition="is">C:\Windows\system32\svchost.exe -</pre></td><td>k dcomlaunch -</td></commandline<>	<pre>condition="is">C:\Windows\system32\svchost.exe -</pre>	k dcomlaunch -
78	<commandline< td=""><td><pre>condition="is">C:\Windows\system32\svchost.exe -</pre></td><td>k dcomlaunch -</td></commandline<>	<pre>condition="is">C:\Windows\system32\svchost.exe -</pre>	k dcomlaunch -
79	<commandline< td=""><td><pre>condition="is">C:\Windows\system32\svchost.exe -</pre></td><td>k defragsvc</td></commandline<>	<pre>condition="is">C:\Windows\system32\svchost.exe -</pre>	k defragsvc
80	<commandline< td=""><td><pre>condition="is">C:\Windows\system32\svchost.exe -</pre></td><td>k devicesflow</td></commandline<>	<pre>condition="is">C:\Windows\system32\svchost.exe -</pre>	k devicesflow
81	<commandline< td=""><td><pre>condition="is">C:\Windows\system32\svchost.exe -</pre></td><td>k imgsvc</td></commandline<>	<pre>condition="is">C:\Windows\system32\svchost.exe -</pre>	k imgsvc
82	<commandline< td=""><td><pre>condition="is">C:\Windows\system32\svchost.exe -</pre></td><td>k localService</td></commandline<>	<pre>condition="is">C:\Windows\system32\svchost.exe -</pre>	k localService
83	<commandline< td=""><td><pre>condition="is">C:\Windows\system32\svchost.exe -</pre></td><td>k localService</td></commandline<>	<pre>condition="is">C:\Windows\system32\svchost.exe -</pre>	k localService
84	<commandline< td=""><td><pre>condition="is">C:\Windows\system32\svchost.exe -</pre></td><td>k LocalService</td></commandline<>	<pre>condition="is">C:\Windows\system32\svchost.exe -</pre>	k LocalService
85	<commandline< td=""><td><pre>condition="is">C:\Windows\system32\svchost.exe -</pre></td><td>k localService</td></commandline<>	<pre>condition="is">C:\Windows\system32\svchost.exe -</pre>	k localService
86	<commandline< td=""><td><pre>condition="is">C:\Windows\system32\svchost.exe -</pre></td><td>k localService</td></commandline<>	<pre>condition="is">C:\Windows\system32\svchost.exe -</pre>	k localService
87	<commandline< td=""><td><pre>condition="is">C:\Windows\system32\svchost.exe -</pre></td><td>k localService</td></commandline<>	<pre>condition="is">C:\Windows\system32\svchost.exe -</pre>	k localService
88	<commandline< td=""><td><pre>condition="is">C:\Windows\system32\svchost.exe -</pre></td><td>k localService</td></commandline<>	<pre>condition="is">C:\Windows\system32\svchost.exe -</pre>	k localService
89	<commandline< td=""><td><pre>condition="is">C:\Windows\system32\svchost.exe -</pre></td><td>k localService</td></commandline<>	<pre>condition="is">C:\Windows\system32\svchost.exe -</pre>	k localService
90	<commandline< td=""><td><pre>condition="is">C:\Windows\system32\svchost.exe -</pre></td><td>k localService</td></commandline<>	<pre>condition="is">C:\Windows\system32\svchost.exe -</pre>	k localService
91	<commandline< td=""><td><pre>condition="is">C:\Windows\system32\svchost.exe -</pre></td><td>k localService</td></commandline<>	<pre>condition="is">C:\Windows\system32\svchost.exe -</pre>	k localService
92	<commandline< td=""><td><pre>condition="is">C:\Windows\system32\svchost.exe -</pre></td><td>k localService</td></commandline<>	<pre>condition="is">C:\Windows\system32\svchost.exe -</pre>	k localService
93	<commandline< td=""><td><pre>condition="is">C:\Windows\system32\svchost.exe -</pre></td><td>k LocalService</td></commandline<>	<pre>condition="is">C:\Windows\system32\svchost.exe -</pre>	k LocalService
94	<commandline< td=""><td><pre>condition="is">C:\Windows\System32\svchost.exe -</pre></td><td>k LocalSystemN</td></commandline<>	<pre>condition="is">C:\Windows\System32\svchost.exe -</pre>	k LocalSystemN
95		<pre>condition="is">C:\Windows\system32\svchost.exe -</pre>	-
96		<pre>condition="is">C:\Windows\system32\svchost.exe -</pre>	
97		<pre>condition="is">C:\Windows\system32\svchost.exe -</pre>	
98		<pre>condition="is">C:\Windows\system32\svchost.exe -</pre>	
99		<pre>condition="is">C:\Windows\system32\svchost.exe -</pre>	
100		<pre>condition="is">C:\Windows\system32\svchost.exe -</pre>	-
101		<pre>condition="is">C:\Windows\system32\svchost.exe -</pre>	-
102		<pre>condition="is">C:\Windows\system32\svchost.exe -</pre>	-
103		<pre>condition="is">C:\Windows\system32\svchost.exe -</pre>	-
104		<pre>condition="is">C:\Windows\system32\svchost.exe -</pre>	-
105		<pre>condition="is">C:\Windows\system32\svchost.exe -</pre>	-
106		condition="is">C:\Windows\system32\svchost.exe -	-
107		condition="is">C:\Windows\system32\svchost.exe -	_
108		condition="is">C:\Windows\system32\svchost.exe -	-
100		condition="is">C:\Windows\system32\svchost.exe -	
110		condition="is">C:\Windows\system32\svchost.exe -	
111		condition="is">C:\Windows\System32\svchost.exe -	
		-	
112		<pre>condition="is">C:\Windows\system32\sychost.exe - condition="is">C:\Windows\System32\sychost.exe -</pre>	-
113		<pre>condition="is">C:\Windows\System32\sychost.exe -</pre>	-
114		condition="is">C:\Windows\system32\sychost.exe -	-
115		condition="is">C:\Windows\system32\svchost.exe -	
116		<pre>condition="is">C:\Windows\system32\svchost.exe -</pre>	-
117	∠Commandlino	condition-"ic"\C:\Windows\cvctam2?\cvchoct ava -	v natevec _c F

sysmon-config/sysmonconfig-export-block.xml at 3f808d9c022c507aae21a9346afba4a59dd533b9 · Neo23x0/sysmonconfig · GitHub - 31/10/2024 16:28 https://github.com/Neo23x0/sysmon-config/blob/3f808d9c022c507aae21a9346afba4a59dd533b9/sysmonconfig-export-block.xml#L1326

11/	ACCUMUNATURE CONTRACTOR— 13 /C. (WITHOUWS \System32 \SYCHOSC, EAC -K HECSYCS -S	L

sysmon-config/sysmonconfig-export-block.xml at 3f808d9c022c507aae21a9346afba4a59dd533b9 config · GitHub - 31/10/2024 16:28 https://github.com/Neo23x0/sysmon-config/blob/3f808d9c022c507aae21a9346afba4a59dd533b9/sysmonconfig-export-block.xml#L1326	
comignates, or occupance race race realist race accessors year on the ring expert steek. At him 2 roze	

sysmon-config/sysmonconfig-export-block.xml at 3f808d9c022c507aae21a9346afba4a59dd533b9 · Neo23x0/sysmon-config/blob/3f808d9c022c507aae21a9346afba4a59dd533b9/sysmonconfig-export-block.xml#L1326	mon-
sormightions of the contract rate rate and according to the contract many that the contract	

sysmon-config/sysmonconfig-export-block.xml at 3f808d9c022c507aae21a9346afba4a59dd533b9 · Neo23x0/s config · GitHub - 31/10/2024 16:28 https://github.com/Neo23x0/sysmon- config/blob/3f808d9c022c507aae21a9346afba4a59dd533b9/sysmonconfig-export-block.xml#L1326	ysmon-
ooning/blob/610004000220007440214001641b4 140044000b6/6yonioniooning 6xport blook.ximi/21020	

sysmon-config/sysmonconfig-export-block.xml at 3f808d9c022c507aae21a9346afba4a59dd533b9 config · GitHub - 31/10/2024 16:28 https://github.com/Neo23x0/sysmon-config/blob/3f808d9c022c507aae21a9346afba4a59dd533b9/sysmonconfig-export-block.xml#L1326	
comignates, or occupance race race realist race accessors year on the ring expert steek. At him 2 roze	

sysmon-config/sysmonconfig-export-block.xml at 3f808d9c022c507aae21a9346afba4a59dd533b9 config · GitHub - 31/10/2024 16:28 https://github.com/Neo23x0/sysmon-config/blob/3f808d9c022c507aae21a9346afba4a59dd533b9/sysmonconfig-export-block.xml#L1326	
comignates, or occupance race race realist race accessors year on the ring expert steek. At him 2 roze	

sysmon-config/sysmonconfig-export-block.xml at 3f808d9c022c507aae21a9346afba4a59dd533b9 · Neo23x0/sysmon-config/blob/3f808d9c022c507aae21a9346afba4a59dd533b9/sysmonconfig-export-block.xml#L1326	mon-
sormightions of the contract rate rate and according to the contract many that the contract	

sysmon-config/sysmonconfig-export-block.xml at 3f808d9c022c507aae21a9346afba4a59dd533b9 config · GitHub - 31/10/2024 16:28 https://github.com/Neo23x0/sysmon-config/blob/3f808d9c022c507aae21a9346afba4a59dd533b9/sysmonconfig-export-block.xml#L1326	
comignates, or occupance race race realist race accessors year on the ring expert steek. At him 2 roze	

sysmon-config/sysmonconfig-export-block.xml at 3f808d9c022c507aae21a9346afba4a59dd533b9 config · GitHub - 31/10/2024 16:28 https://github.com/Neo23x0/sysmon-config/blob/3f808d9c022c507aae21a9346afba4a59dd533b9/sysmonconfig-export-block.xml#L1326	
comignates, or occupance race race realist race accessors year on the ring expert steek. At him 2 roze	

sysmon-config/sysmonconfig-export-block.xml at 3f808d9c022c507aae21a9346afba4a59dd533b9 · Neo23x0/sysmon-config/blob/3f808d9c022c507aae21a9346afba4a59dd533b9/sysmonconfig-export-block.xml#L1326	mon-
sormightions of the contract rate rate and according to the contract many that the contract	

sysmon-config/sysmonconfig-export-block.xml at 3f808d9c022c507aae21a9346afba4a59dd533b9 · Neo23x0/sysmon-config/blob/3f808d9c022c507aae21a9346afba4a59dd533b9/sysmonconfig-export-block.xml#L1326	mon-
sormightions of the contract rate rate and according to the contract many that the contract	

sysmon-config/sysmonconfig-export-block.xml at 3f808d9c022c507aae21a9346afba4a59dd533b9 · config · GitHub - 31/10/2024 16:28 https://github.com/Neo23x0/sysmon-config/blob/3f808d9c022c507aae21a9346afba4a59dd533b9/sysmonconfig-export-block.xml#L1326	Neo23x0/sysmon-
ourning/blob/blob/blob/blob/blob/blob/blob/blo	

CC	ysmon-config/sysmonconfig-export-block.xml at 3f808d9c022c507aae21a9346afba4a59dd533b9 onfig · GitHub - 31/10/2024 16:28 https://github.com/Neo23x0/sysmon-onfig/blob/3f808d9c022c507aae21a9346afba4a59dd533b9/sysmonconfig-export-block.xml#L1326	Neo23x0/sysmon-
	stilligi blobi oloooda oo 22200 i dada taada taada da oo ababa oo ayo iliga oxport blook.xiiiii 21020	

sysmon-config/sysmonconfig-export-block.xml at 3f808d9c022c507aae21a9346afba4a59dd533b9 · Neo23x0/syconfig · GitHub - 31/10/2024 16:28 https://github.com/Neo23x0/sysmon-config/blob/3f808d9c022c507aae21a9346afba4a59dd533b9/sysmonconfig-export-block.xml#L1326	/smon-

sysmon-config/sysmonconfig-export-block.xml at 3f808d9c022c507aae21a9346afba4a59dd533b9 · Neo23x0/sysmon-config/blob/3f808d9c022c507aae21a9346afba4a59dd533b9/sysmonconfig-export-block.xml#L1326	mon-
sormightions of the contract rate rate and according to the contract many that the contract	

CC	ysmon-config/sysmonconfig-export-block.xml at 3f808d9c022c507aae21a9346afba4a59dd533b9 onfig · GitHub - 31/10/2024 16:28 https://github.com/Neo23x0/sysmon-onfig/blob/3f808d9c022c507aae21a9346afba4a59dd533b9/sysmonconfig-export-block.xml#L1326	Neo23x0/sysmon-
	stilligi blobi oloooda oo 22200 i dada taada taada da oo ababa oo ayo iliga oxport blook.xiiiii 21020	

sysmon-config/sysmonconfig-export-block.xml at 3f808d9c022c507aae21a9346afba4a59dd533b9 · Neo23x0/sysmon-config/blob/3f808d9c022c507aae21a9346afba4a59dd533b9/sysmonconfig-export-block.xml#L1326	mon-
sormightions of the contract rate rate and according to the contract many that the contract	

sysmon-config/sysmonconfig-export-block.xml at 3f808d9c022c507aae21a9346afba4a59dd533b9 config · GitHub - 31/10/2024 16:28 https://github.com/Neo23x0/sysmon-config/blob/3f808d9c022c507aae21a9346afba4a59dd533b9/sysmonconfig-export-block.xml#L1326	
comignates, or occupance race race realist race accessors year on the ring expert steek. At him 2 roze	

sysmon-config/sysmonconfig-export-block.xml at 3f808d9c022c507aae21a9346afba4a59dd533b9 · Neo23x0/sysmon-config/blob/3f808d9c022c507aae21a9346afba4a59dd533b9/sysmonconfig-export-block.xml#L1326	mon-
sormightions of the contract rate rate and according to the contract many that the contract	

sysmon-config/sysmonconfig-export-block.xml at 3f808d9c022c507aae21a9346afba4a59dd533b9 · Neo23x0/sysmon-config/blob/3f808d9c022c507aae21a9346afba4a59dd533b9/sysmonconfig-export-block.xml#L1326	mon-
sormightions of the contract rate rate and according to the contract many that the contract	

sysmon-config/sysmonconfig-export-block.xml at 3f808d9c022c507aae21a9346afba4a59dd533b9 · Neo23x0/sysmon-config/blob/3f808d9c022c507aae21a9346afba4a59dd533b9/sysmonconfig-export-block.xml#L1326	mon-
sormightions of the contract rate rate and according to the contract many that the contract	

CC	ysmon-config/sysmonconfig-export-block.xml at 3f808d9c022c507aae21a9346afba4a59dd533b9 onfig · GitHub - 31/10/2024 16:28 https://github.com/Neo23x0/sysmon-onfig/blob/3f808d9c022c507aae21a9346afba4a59dd533b9/sysmonconfig-export-block.xml#L1326	Neo23x0/sysmon-
	stilligi blobi oloooda oo 22200 i dada taada taada da oo ababa oo ayo iliga oxport blook.xiiiii 21020	

sysmon-config/sysmonconfig-export-block.xml at 3f808d9c022c507aae21a9346afba4a59dd533b9 · Neo23x0/sysmor config · GitHub - 31/10/2024 16:28 https://github.com/Neo23x0/sysmon- config/blob/3f808d9c022c507aae21a9346afba4a59dd533b9/sysmonconfig-export-block.xml#L1326)-

sysmon-config/sysmonconfig-export-block.xml at 3f808d9c022c507aae21a9346afba4a59dd533b9 · Neo23x0/s config · GitHub - 31/10/2024 16:28 https://github.com/Neo23x0/sysmon- config/blob/3f808d9c022c507aae21a9346afba4a59dd533b9/sysmonconfig-export-block.xml#L1326	ysmon-
ooning/blob/clocodecodecodecordace race realiza racedacecobe/cyenneneering capeir block./kmi//21020	

ysmon-config/sysmonconfig-export-block.xml at 3f808d9c022c507aae21a9346afba4a59dd533b9 · Neo23x0/sysmononfig · GitHub - 31/10/2024 16:28 https://github.com/Neo23x0/sysmon-onfig/blob/3f808d9c022c507aae21a9346afba4a59dd533b9/sysmonconfig-export-block.xml#L1326	n-

sysmon-config/sysmonconfig-export-block.xml at 3f808d9c022c507aae21a9346afba4a59dd533b9 · Neo23x0/sysmon-config/blob/3f808d9c022c507aae21a9346afba4a59dd533b9/sysmonconfig-export-block.xml#L1326	mon-
sormightions of the contract rate rate and according to the contract many that the contract	

sysmon-config/sysmonconfig-export-block.xml at 3f808d9c022c507aae21a9346afba4a59dd533b9 · Neo23x0/sysmon-config · GitHub - 31/10/2024 16:28 https://github.com/Neo23x0/sysmon-config/blob/3f808d9c022c507aae21a9346afba4a59dd533b9/sysmonconfig-export-block.xml#L1326

1407 <hash< td=""><td>es condition="contains">IMPHASH=C547F2E66061A8DFFB6F5A3FF63C0A74</td></hash<>	es condition="contains">IMPHASH=C547F2E66061A8DFFB6F5A3FF63C0A74
1408 <hash< td=""><td>es condition="contains">IMPHASH=0588081AB0E63BA785938467E1B10CCA</td></hash<>	es condition="contains">IMPHASH=0588081AB0E63BA785938467E1B10CCA
1409 <hash< td=""><td>es condition="contains">IMPHASH=0D9EC08BAC6C07D9987DFD0F1506587C</td></hash<>	es condition="contains">IMPHASH=0D9EC08BAC6C07D9987DFD0F1506587C
1410 <hash< td=""><td>es condition="contains">IMPHASH=BC129092B71C89B4D4C8CDF8EA590B29</td></hash<>	es condition="contains">IMPHASH=BC129092B71C89B4D4C8CDF8EA590B29
1411 <hash< td=""><td>es condition="contains">IMPHASH=4DA924CF622D039D58BCE71CDF05D242</td></hash<>	es condition="contains">IMPHASH=4DA924CF622D039D58BCE71CDF05D242
1412 <hash< td=""><td>es condition="contains">IMPHASH=E7A3A5C377E2D29324093377D7DB1C66</td></hash<>	es condition="contains">IMPHASH=E7A3A5C377E2D29324093377D7DB1C66
1413 <hash< td=""><td>es condition="contains">IMPHASH=9A9DBEC5C62F0380B4FA5FD31DEFFEDF</td></hash<>	es condition="contains">IMPHASH=9A9DBEC5C62F0380B4FA5FD31DEFFEDF
1414 <hash< td=""><td>es condition="contains">IMPHASH=AF8A3976AD71E5D5FDFB67DDB8DADFCE</td></hash<>	es condition="contains">IMPHASH=AF8A3976AD71E5D5FDFB67DDB8DADFCE
1415 <hash< td=""><td>es condition="contains">IMPHASH=0C477898BBF137BBD6F2A54E3B805FF4</td></hash<>	es condition="contains">IMPHASH=0C477898BBF137BBD6F2A54E3B805FF4
1416 <hash< td=""><td>es condition="contains">IMPHASH=0CA9F02B537BCEA20D4EA5EB1A9FE338</td></hash<>	es condition="contains">IMPHASH=0CA9F02B537BCEA20D4EA5EB1A9FE338
1417 <hash< td=""><td>es condition="contains">IMPHASH=3AB3655E5A14D4EEFC547F4781BF7F9E</td></hash<>	es condition="contains">IMPHASH=3AB3655E5A14D4EEFC547F4781BF7F9E
1418 <hash< td=""><td>es condition="contains">IMPHASH=E6F9D5152DA699934B30DAAB206471F6</td></hash<>	es condition="contains">IMPHASH=E6F9D5152DA699934B30DAAB206471F6
1419 <hash< td=""><td>es condition="contains">IMPHASH=3AD59991CCF1D67339B319B15A41B35D</td></hash<>	es condition="contains">IMPHASH=3AD59991CCF1D67339B319B15A41B35D
1420 <hash< td=""><td>es condition="contains">IMPHASH=FFDD59E0318B85A3E480874D9796D872</td></hash<>	es condition="contains">IMPHASH=FFDD59E0318B85A3E480874D9796D872
1421 <hash< td=""><td>es condition="contains">IMPHASH=0CF479628D7CC1EA25EC7998A92F5051</td></hash<>	es condition="contains">IMPHASH=0CF479628D7CC1EA25EC7998A92F5051
1422 <hash< td=""><td>es condition="contains">IMPHASH=07A2D4DCBD6CB2C6A45E6B101F0B6D51</td></hash<>	es condition="contains">IMPHASH=07A2D4DCBD6CB2C6A45E6B101F0B6D51
1423 <hash< td=""><td>es condition="contains">IMPHASH=D6D0F80386E1380D05CB78E871BC72B1</td></hash<>	es condition="contains">IMPHASH=D6D0F80386E1380D05CB78E871BC72B1
1424 <hash< td=""><td>es condition="contains">IMPHASH=38D9E015591BBFD4929E0D0F47FA0055</td></hash<>	es condition="contains">IMPHASH=38D9E015591BBFD4929E0D0F47FA0055
1425 <hash< td=""><td>es condition="contains">IMPHASH=0E2216679CA6E1094D63322E3412D650</td></hash<>	es condition="contains">IMPHASH=0E2216679CA6E1094D63322E3412D650
1426 <hash< td=""><td>es condition="contains">IMPHASH=ADA161BF41B8E5E9132858CB54CAB5FB</td></hash<>	es condition="contains">IMPHASH=ADA161BF41B8E5E9132858CB54CAB5FB
1427 <hash< td=""><td>es condition="contains">IMPHASH=2A1BC4913CD5ECB0434DF07CB675B798</td></hash<>	es condition="contains">IMPHASH=2A1BC4913CD5ECB0434DF07CB675B798
1428 <hash< td=""><td>es condition="contains">IMPHASH=11083E75553BAAE21DC89CE8F9A195E4</td></hash<>	es condition="contains">IMPHASH=11083E75553BAAE21DC89CE8F9A195E4
1429 <hash< td=""><td>es condition="contains">IMPHASH=A23D29C9E566F2FA8FFBB79267F5DF80</td></hash<>	es condition="contains">IMPHASH=A23D29C9E566F2FA8FFBB79267F5DF80
1430 <hash< td=""><td>es condition="contains">IMPHASH=4A07F944A83E8A7C2525EFA35DD30E2F</td></hash<>	es condition="contains">IMPHASH=4A07F944A83E8A7C2525EFA35DD30E2F
1431 <hash< td=""><td>es condition="contains">IMPHASH=767637C23BB42CD5D7397CF58B0BE688</td></hash<>	es condition="contains">IMPHASH=767637C23BB42CD5D7397CF58B0BE688
1432 <hash< td=""><td>es condition="contains">IMPHASH=14C4E4C72BA075E9069EE67F39188AD8</td></hash<>	es condition="contains">IMPHASH=14C4E4C72BA075E9069EE67F39188AD8
1433 <hash< td=""><td>es condition="contains">IMPHASH=3C782813D4AFCE07BBFC5A9772ACDBDC</td></hash<>	es condition="contains">IMPHASH=3C782813D4AFCE07BBFC5A9772ACDBDC
1434 <hash< td=""><td>es condition="contains">IMPHASH=7D010C6BB6A3726F327F7E239166D127</td></hash<>	es condition="contains">IMPHASH=7D010C6BB6A3726F327F7E239166D127
1435 <hash< td=""><td>es condition="contains">IMPHASH=89159BA4DD04E4CE5559F132A9964EB3</td></hash<>	es condition="contains">IMPHASH=89159BA4DD04E4CE5559F132A9964EB3
1436 <hash< td=""><td>es condition="contains">IMPHASH=6F33F4A5FC42B8CEC7314947BD13F30F</td></hash<>	es condition="contains">IMPHASH=6F33F4A5FC42B8CEC7314947BD13F30F
1437 <hash< td=""><td>es condition="contains">IMPHASH=5834ED4291BDEB928270428EBBAF7604</td></hash<>	es condition="contains">IMPHASH=5834ED4291BDEB928270428EBBAF7604
1438 <hash< td=""><td>es condition="contains">IMPHASH=5A8A8A43F25485E7EE1B201EDCBC7A38</td></hash<>	es condition="contains">IMPHASH=5A8A8A43F25485E7EE1B201EDCBC7A38
1439 <hash< td=""><td>es condition="contains">IMPHASH=DC7D30B90B2D8ABF664FBED2B1B59894</td></hash<>	es condition="contains">IMPHASH=DC7D30B90B2D8ABF664FBED2B1B59894
1440 <hash< td=""><td>es condition="contains">IMPHASH=41923EA1F824FE63EA5BEB84DB7A3E74</td></hash<>	es condition="contains">IMPHASH=41923EA1F824FE63EA5BEB84DB7A3E74
1441 <hash< td=""><td>es condition="contains">IMPHASH=3DE09703C8E79ED2CA3F01074719906B</td></hash<>	es condition="contains">IMPHASH=3DE09703C8E79ED2CA3F01074719906B
1442 <hash< td=""><td>es condition="contains">IMPHASH=A53A02B997935FD8EEDCB5F7ABAB9B9F</td></hash<>	es condition="contains">IMPHASH=A53A02B997935FD8EEDCB5F7ABAB9B9F
1443 <hash< td=""><td>es condition="contains">IMPHASH=E96A73C7BF33A464C510EDE582318BF2</td></hash<>	es condition="contains">IMPHASH=E96A73C7BF33A464C510EDE582318BF2
1444 <hash< td=""><td>es condition="contains">IMPHASH=32089B8851BBF8BC2D014E9F37288C83</td></hash<>	es condition="contains">IMPHASH=32089B8851BBF8BC2D014E9F37288C83
1445 <hash< td=""><td>es condition="contains">IMPHASH=09D278F9DE118EF09163C6140255C690</td></hash<>	es condition="contains">IMPHASH=09D278F9DE118EF09163C6140255C690

```
config/blob/3f808d9c022c507aae21a9346afba4a59dd533b9/sysmonconfig-export-block.xml#L1326
```

```
<Hashes condition="contains">IMPHASH=03866661686829D806989E2FC5A72606</hash</pre>
1446
1447
                                  <Hashes condition="contains">IMPHASH=E57401FBDADCD4571FF385AB82BD5D6D/Hash
1448
1449
                                  <!-- Microsoft Office Programs Dropping Executables -->
1450
                                  <Image condition="image">winword.exe</Image>
1451
                                  <Image condition="image">excel.exe</Image>
                                  <Image condition="image">powerpnt.exe</Image>
1452
1453
                                  <Image condition="image">msaccess.exe</Image>
1454
                                  <Image condition="image">mspub.exe</Image>
                                  <Image condition="image">eqnedt32.exe</Image>
1455
1456
                                  <Image condition="image">visio.exe</Image>
                                  <Image condition="image">wordpad.exe</Image>
1457
                                  <Image condition="image">wordview.exe</Image>
1458
1459
1460
                                  <!-- LOLBINs that can be used to download executables -->
                                  <Image condition="image">certutil.exe</Image>
1461
                                  <Image condition="image">certoc.exe</Image>
1462
1463
                                  <Image condition="image">CertReq.exe</Image>
1464
                                  <!-- <Image condition="image">bitsadmin.exe</Image> (depends on the enviror
                                  <Image condition="image">Desktopimgdownldr.exe</Image>
1465
1466
                                  <Image condition="image">esentutl.exe</Image>
1467
                                  <Image condition="image">expand.exe</Image>
1468
                                  <Image condition="image">finger.exe</Image>
1469
1470
                                  <!-- Executables that should never drop an executable to disk (but may afte
1471
                                  <Image condition="image">notepad.exe</Image>
1472
                                  <Image condition="image">AcroRd32.exe</Image>
1473
                                  <Image condition="image">RdrCEF.exe</Image>
                                  <Image condition="image">mshta.exe</Image>
1474
1475
                                  <Image condition="image">hh.exe</Image>
                         </FileBlockExecutable>
1476
                 </RuleGroup>
1477
1478
1479
                 </EventFiltering>
1480
         </Sysmon>
```