Malicious activity

22546413_042414.html

MD5: A55E54C4D96F118ADA16274B593BB8EB

Start: 08.06.2022, 10:38 Total time: 289 s

Win7 32 bit Complete

cve-2022-30190 qbot

Indicators: Tracker: Qbot

Get sample | IOC | MalConf | Restart

Text report | Graph | ATT&CK | AI Summary (beta) | Export

CPU RAM

Processes Filter by PID or name Only important

912 SUS svchost.exe -k netsvcs
1k 515 176

528 SUS Explorer.EXE
15k 14k 438

2612 iexplore.exe "C:\Users\admin\AppData\Local\Temp\2254641...
3k 8k 156

2928 iexplore.exe SCODEF:2612 CREDAT:144385 /prefetch:2
880 3k 101

2204 iexplore.exe SCODEF:2612 CREDAT:333057 /prefetc...
350 299 75

3860 iexplore.exe SCODEF:2612 CREDAT:78857 /prefetch:2
1k 3k 109

2444 WinRAR.exe "C:\Users\admin\Downloads\22546413_042...
1k 984 93

1128 isoburn.exe "C:\Users\admin\AppData\Local\Temp\...
95 12 20

3576 iexplore.exe SCODEF:2612 CREDAT:726284 /prefetch:2
1k 777 101

2752 explorer.exe
201 60 40

1316 isoburn.exe "C:\Users\admin\Desktop\22546413_042414.img"
93 12 20

1380 rundll32.exe C:\Windows\system32\shell32.dll,OpenAs_RunD...
1k 761 151

2764 isoburn.exe "C:\Users\admin\Desktop\22546413_04241...
93 12 20

3008 isoburn.exe "C:\Users\admin\Desktop\22546413_042414.img"
93 12 20

3856 isoburn.exe "C:\Users\admin\Desktop\22546413_042414.img"
93 12 20

3480 chrome.exe
12k 1k 156

1128 chrome.exe --type=crashpad-handler "--user-data-dir=C:\...
99 9 22

2848 chrome.exe --type=gpu-process --field-trial-handle=1036,4...
481 23 77

2096 chrome.exe --type=utility --utility-sub-type=network.mojo...
5k 11k 73

derer --field-trial-handle=1036,4941...
344 17 48

derer --field-trial-handle=1036,4941...
342 17 48

derer --field-trial-handle=1036,4941...
305 17 48

u-process --field-trial-handle=1036,4...
405 22 76

HTTP Requests 27 | Connections 50 | DNS Requests 38 | Threats 0 | Filter by PID, name or url | PCAP

NETWORK | FILES | DEBUG

Timeshift	Headers	Rep	PID	Process name	CN	URL	Content
5931 ms	GET | 200: OK	?	2612	iexplore.exe		http://ctldl.windowsupdate.com/msdo...	
6899 ms	GET | 200: OK	?	2612	iexplore.exe		http://ocsp.digicert.com/MFEwTzBNM...	
31634 ms	GET | 200: OK	?	2612	iexplore.exe		http://ocsp.digicert.com/MFEwTzBNM...	4
80684 ms	GET | 200: OK	?	2612	iexplore.exe		http://ocsp.digicert.com/MFEwTzBNM...	4
175.87 s	GET | 200: OK	?	2096	chrome.exe		http://edgedl.me.gvt1.com/edgedl/chr...	24
186.99 s	GET | 200: OK	?	2096	chrome.exe	?	http://ctldl.windowsupdate.com/msdo...	6
229.87 s	OPTIONS 405: Method No...	?	1868	WINWORD.EXE	?	http://185.234.247.119/	1
229.88 s	HEAD | 200: OK	?	1868	WINWORD.EXE	?	http://185.234.247.119/123.RES	

Info [2276] chrome.exe Checks supported languages

Try community version for free! Register now