Title: Compromised HostAnalysis

Group/Name: Aimé Fraser

Indicators and Technical Details

Datetime	Identifier (IP, Domain, URL, Hostname)	MITRE Technique ID	Analyst Comment
Saturday	NOC identifies a series of anomalous network events from a host within the GoodCorp network.		Security Analyst called in to assess the issue.
Saturday	RDPService is not Verified by Microsoft and is not located in c:\Windows\system32	T1574 Hijack Execution Flow	C:\Program Files (x86)\BdeUISrv.Exe See Figure 1.
Saturday	Scheduled Task set to repeat every minute indefinitely	T1053 Scheduled Task	The task began on 9/26/2020, likely when the compromised machine was first set up. The machine is dormant most of the time. It is activated only during CDCA weeks. No activity would be seen when the machine was not activated. See Figure 2.
Saturday	Process Explorer shows BdeUIsrv.exe opening and closing each minute.		See Figure 3.
Saturday	BdeUISrv.exe opens suspect DLLs.		Wtsapi32.dll is not verified by Microsoft and is not located in \System32. See Figure 4.
Saturday	BdeUiSrv.exe and wtsapi32.dll strings contain code.	T1219 Remote Access Software	Code enumerates antivirus and calls the website globaltechnegineers.org. See Figures 5, 6, and 7.
Saturday	The compromised machine beacons out but gets no response.	T1568 Dynamic Resolution	See Figures 8 and 9.
Saturday	The compromised machine sends out fake ARP requests	T1557.002 ARP Cache Poisoning	This would likely facilitate an attacker-in-the-middle scenario if the attacker site was operative. See Figure 10.
Saturday	Globaltechengineers.org is non-functional. (52.45.178.122		The Nation Cyber Security Centre (U.K) lists this site (with a different IP address. See Figure 11.

Executive Summary

On Saturday, the Network Operations Team identified a series of anomalous network events from a host within the GoodCorp network. The on-call security analyst came in to assess the network for potential compromise.

The network issues were caused by a host noisily trying to contact an apparently abandoned command-and-control server while also providing cover for a non-existent attacker-in-the-middle. Put another way, the machine was ready to be further compromised, but the attackers did not show up.

This event is relatively easy to shut down (see details at the end of this report), and there are no signs of additional compromise. However, it does GoodCorp the favor of revealing vulnerabilities that could draw the attention of state-sponsored Advanced Persistent Threats. These are formidable opponents and require a world-class defense. This event allows GoodCorp to prepare for something much worse.

Technical Summary

Wireshark analysis of the affected host revealed frequent ARP requests and responses between the host (10.20[.]44.4) and the router (10.20[.]44.1). During that time, the host also beaconed to 52.45[.]178.122 (globaltechengineers[.]org) 234 times. Figure 11 shows that zero bytes exited the network, as the site is not running.

This beaconing functionality resulted from a scheduled task of unknown origin. It executed the files C:\Program Files (x86)\BdeUISrv.exe and C:\Program Files (x86)\wtsapi.dll. These files were listed as being from Microsoft, but were not verified. They were also in a non-standard file location (See Figure 1). The scheduled task was set to run once a minute for an indefinite period (See Figure 2).

Analysis of the Event Logs shows that while RDP was running from startup, the only RDP connections to the host were from the SOC analyst workstation (10.20[.]44.8). This was double-checked against frequent random arp -a commands to look for additional connections. None were found (See Figures 9 and 12).

The UK's National Cyber Security Centre lists globaltechengineers[.]org as an indicator of compromise used by APT28, also known as Fancy Bear (See Figure 13). The report shows a different IP address. Similarly, the two files did not register as malicious by VirusTotal. These results are unsurprising, as Fancy Bear frequently changes IP addresses and updates their files.

Findings and Analysis

The unusual and noisy network traffic this exploit has caused is likely two prongs of the attack. The beaconing out was the host's attempts to contact the home server to get additional instructions to compromise the host and network. The website it calls is not operative, so it’s possible the exploit has been abandoned.

The frequent ARP requests are likely the set-up for an attacker-in-the-middle attack that did not happen. If an attacker had been lurking in the middle, those requests would have maintained the connection to keep up the game.

The attack's two processes need additional decrypting and analysis, but even a rough analysis shows signs of enumerating antivirus and other functions. These processes would have facilitated the installation of additional software. If the attacker were to pick up the connection, anything would be possible. They

could steal credentials for network access or banking, alter or delete files, exfiltrate files for espionage or extortion, or encrypt files for ransom.

It's concerning that the command-and-control website is a known indicator of compromise for Fancy Bear. This attacker could be Fancy Bear, one of its associate groups, or a copycat.

Fancy Bear is a well-known and sophisticated attacker. The US Dept of Justice has connected this group with the Russian government and indicted Russian intelligence officers for computer hacking, wire fraud, aggravated identity theft, and money laundering in connection with their attacks, such as the Ukraine energy grid, a French presidential election, the German Bundestag, and the opening ceremony of the 2018 Winter Olympics. The prosecutors said the suspects were from the same unit that targeted the Democratic National Committee in an attempt to influence the 2016 US presidential election.

Fancy Bear is an experienced and very sophisticated group that appears to have the full backing of the Russian government. Their campaigns align with Russian military and political goals and do not focus on financial gain.

Their tools, techniques, and practices evolve continually to find and exploit new avenues of compromise. They have been known to use phishing and spoofed websites with domain names that closely resemble legitimate sites the recipient will likely trust. Their carefully crafted phishing emails look the same as the company they are spoofing. The skill and dedication this group can bring to the table make them very effective.

Fancy Bear is known to keep a close eye on zero-day exploits and immediately use them before the target systems have been patched.

While this incident is minor, it suggests GoodCorp has vulnerabilities that APTs may want to exploit. A threat intelligence analysis of APT28 and its related groups would help GoodCorp's security and networking teams build a defense system to counter the threats posed by these groups.

In addition, the following mitigations can be put into place immediately.

Remediation and Recommendations

Remove the RDP scheduled task from the affected host.

Delete C:\Program Files (x86)\BdeUISrv.exe and C:\Program Files (x86)\wtsapi.dll

Create signatures and Yara rules using the two files and their strings of code.

M1051 Update Software
Update software regularly by employing patch management for externally exposed applications.

M1016 Vulnerability Scanning
Regularly scan externally facing systems for vulnerabilities and establish procedures to rapidly patch systems when critical vulnerabilities are discovered through scanning and through public disclosure

M1022 Restrict File and Directory Permissions
Set directory access controls to prevent file writes to the application search paths, both in the folders from which applications are run and the standard dylib folders.

DS0022 File Creation/Modification
Monitor for newly constructed dylibs. Monitor file systems for moving, renaming, replacing, or modifying dylibs. Changes in the set of dylibs that are loaded by a process (compared to past behavior) that do not correlate with known software, patches, etc., are suspicious. Check the system for multiple dylibs with the same name and monitor which versions have historically been loaded into a process.

M1018 User Account Management
Limit privileges of user accounts and remediate Privilege Escalation vectors so only authorized administrators can create scheduled tasks on remote systems.

DS0022 File ModificationMonitor Windows Task Scheduler stores in %systemroot%\System32\Tasks for change entries related to scheduled tasks that do not correlate with known software, patch cycles, etc.

DS0003 Scheduled Job Creation
Monitor for newly constructed scheduled jobs by enabling the "Microsoft-Windows-TaskScheduler/Operational" setting within the event logging service. Several events will then be logged on scheduled task activity, including Event ID 106 on Windows 7, Server 2008 R2 - Scheduled task registered; Event ID 4698 on Windows 10, Server 2016 - Scheduled task created;Event ID 4700 on Windows 10, Server 2016 - Scheduled task enabled;Event ID 4701 on Windows 10, Server 2016 - Scheduled task disabled.

DS0029 Network Traffic Content and Flow
Monitor network traffic for unusual ARP traffic, gratuitous ARP replies may be suspicious. Consider collecting changes to ARP caches across endpoints for signs of ARP poisoning. For example, if multiple IP addresses map to a single MAC address, this could be an indicator that the ARP cache has been poisoned. Monitor for network traffic originating from unknown/unexpected hardware devices. Local network traffic metadata (such as source MAC addressing) and usage of network management protocols such as DHCP may help identify hardware.

M1035 Limit Access to Resource Over Network
Create static ARP entries for networked devices. Implementing static ARP entries may be infeasible for large networks.

DS0029 Network Traffic
Monitor and analyze traffic patterns and packet inspection associated with protocol(s) that do not follow the expected protocol standards and traffic flows (e.g., extraneous packets that do not belong to established flows, gratuitous or anomalous traffic patterns, anomalous syntax, or structure). Consider correlation with process monitoring and command line to detect anomalous processes execution and command line arguments associated with traffic patterns (e.g., monitor anomalies in the use of files that do not normally initiate connections for respective protocol(s)). Monitor for newly constructed network connections sent or received by untrusted hosts. Monitor network data for uncommon data flows. Processes utilizing the network that do not normally have network communication or have never been seen before are suspicious.

M1038 Execution Prevention
Use application control to mitigate installation and use of unapproved software that can be used for remote access.

M1017 User Training
Users can be trained to identify social engineering techniques and phishing emails.

M1054 Software Configuration
Use anti-spoofing and email authentication mechanisms to filter messages based on validity checks of the sender domain (using SPF) and integrity of messages (using DKIM). Enabling these mechanisms within an organization (through policies such as DMARC) may enable recipients (intra-org and cross domain) to perform similar message filtering and validation.

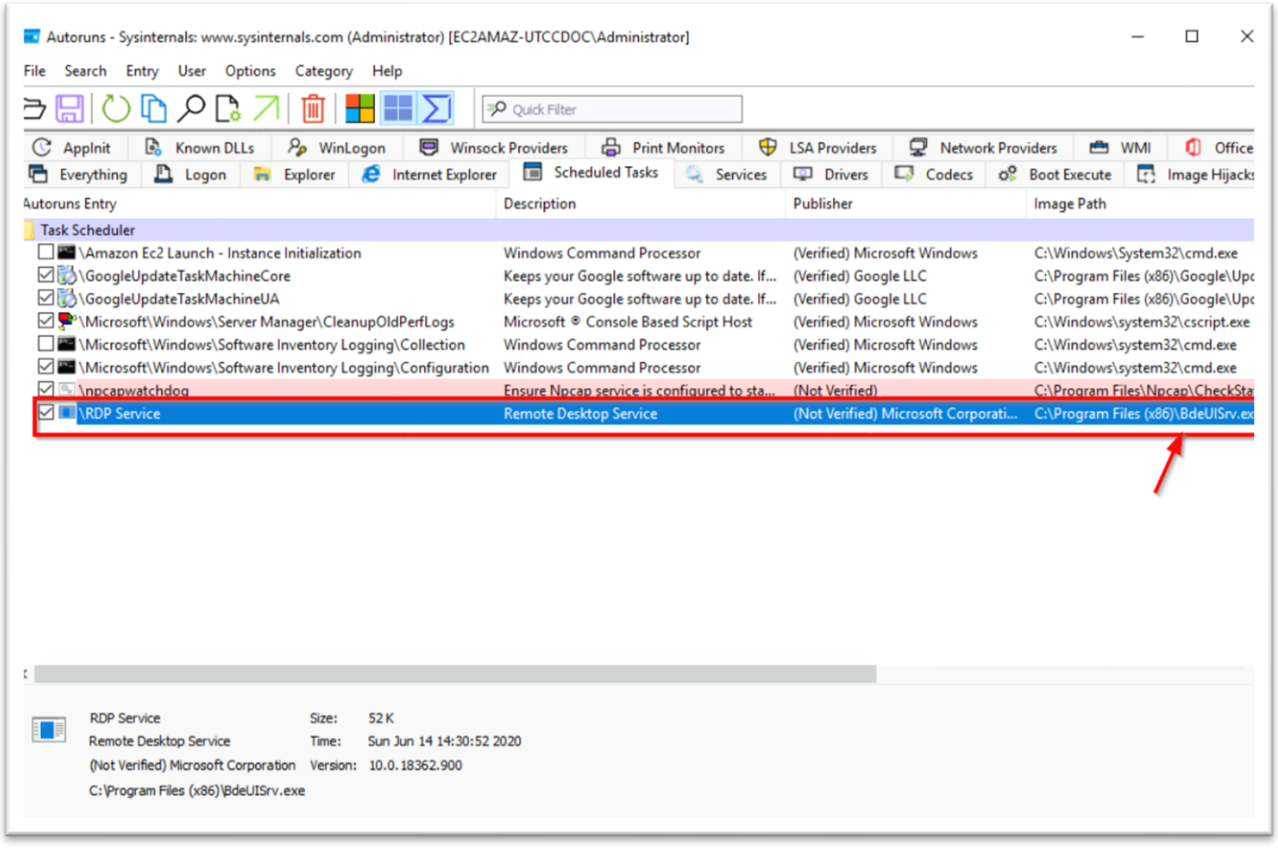


Figure 1RDP Service is a scheduled task. Its file is not verified by Microsoft and its path is not to \system32.

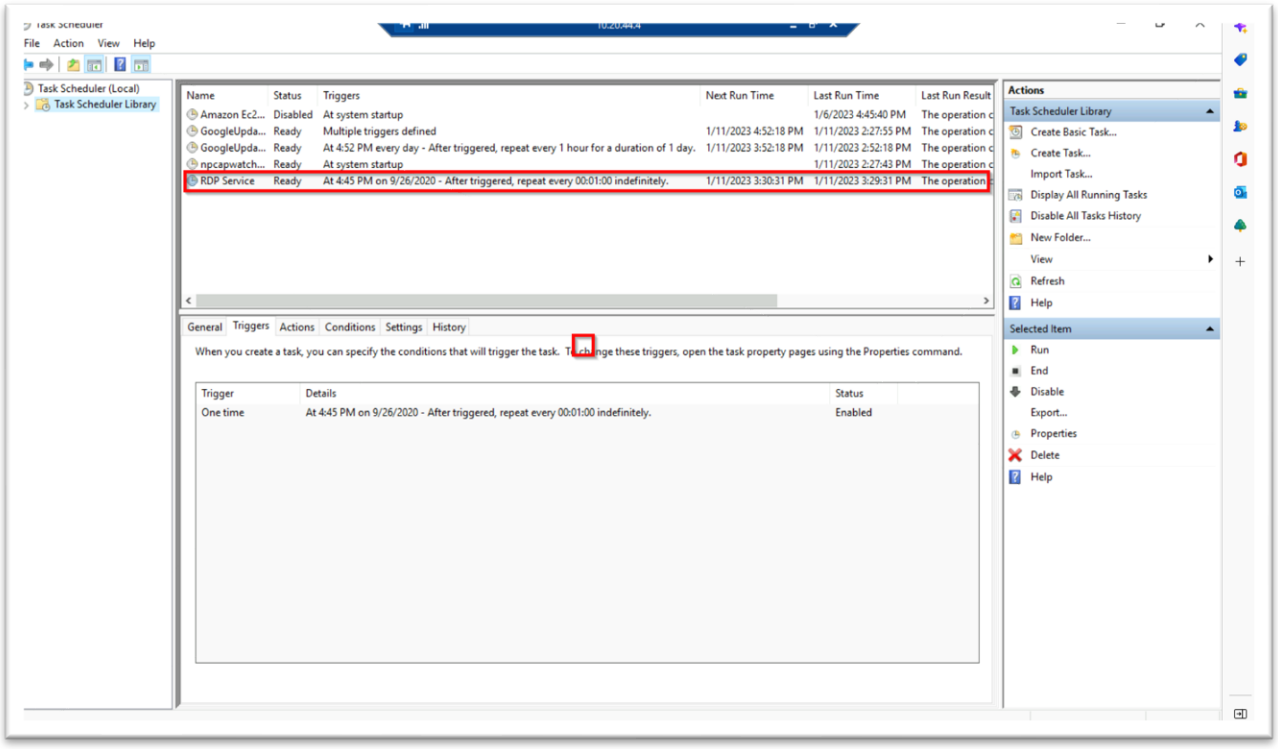


Figure 2. A Scheduled task is set to run every minute.

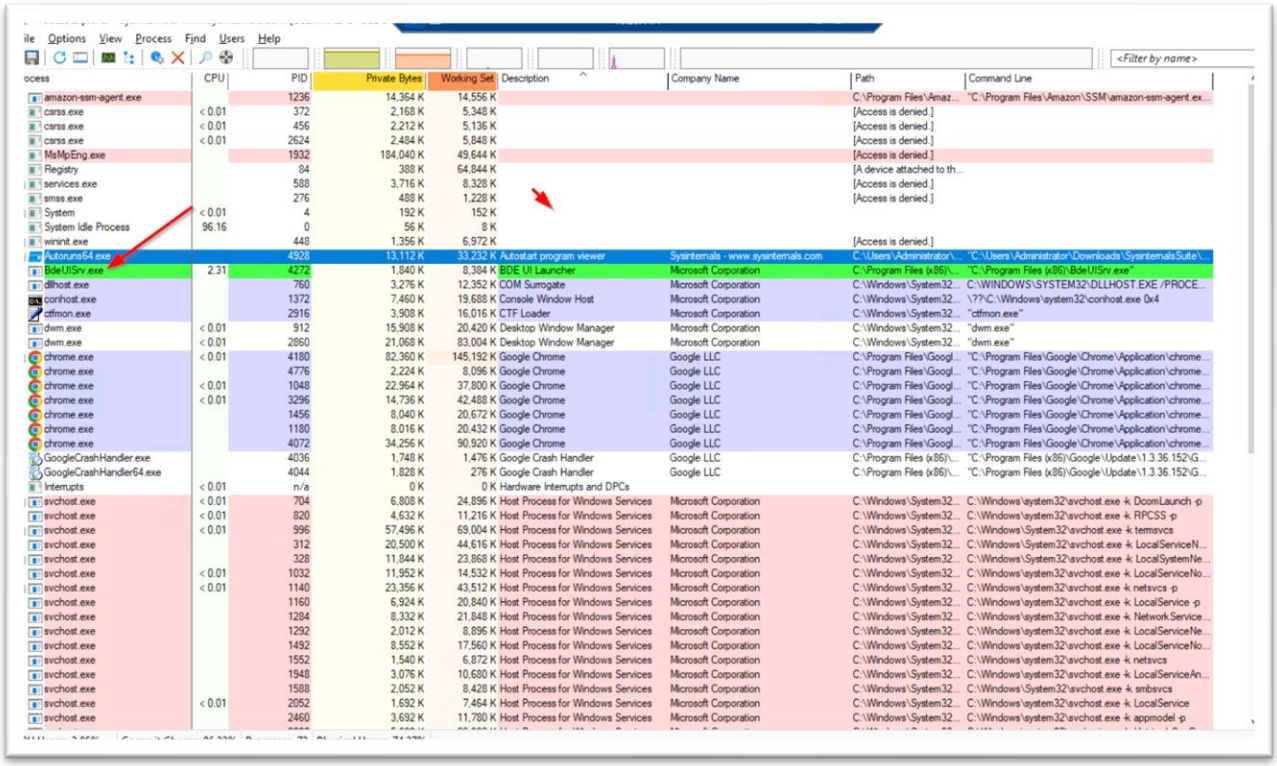


Figure 3. BdeUiSrv.exe runs once a minute as per the schedule.

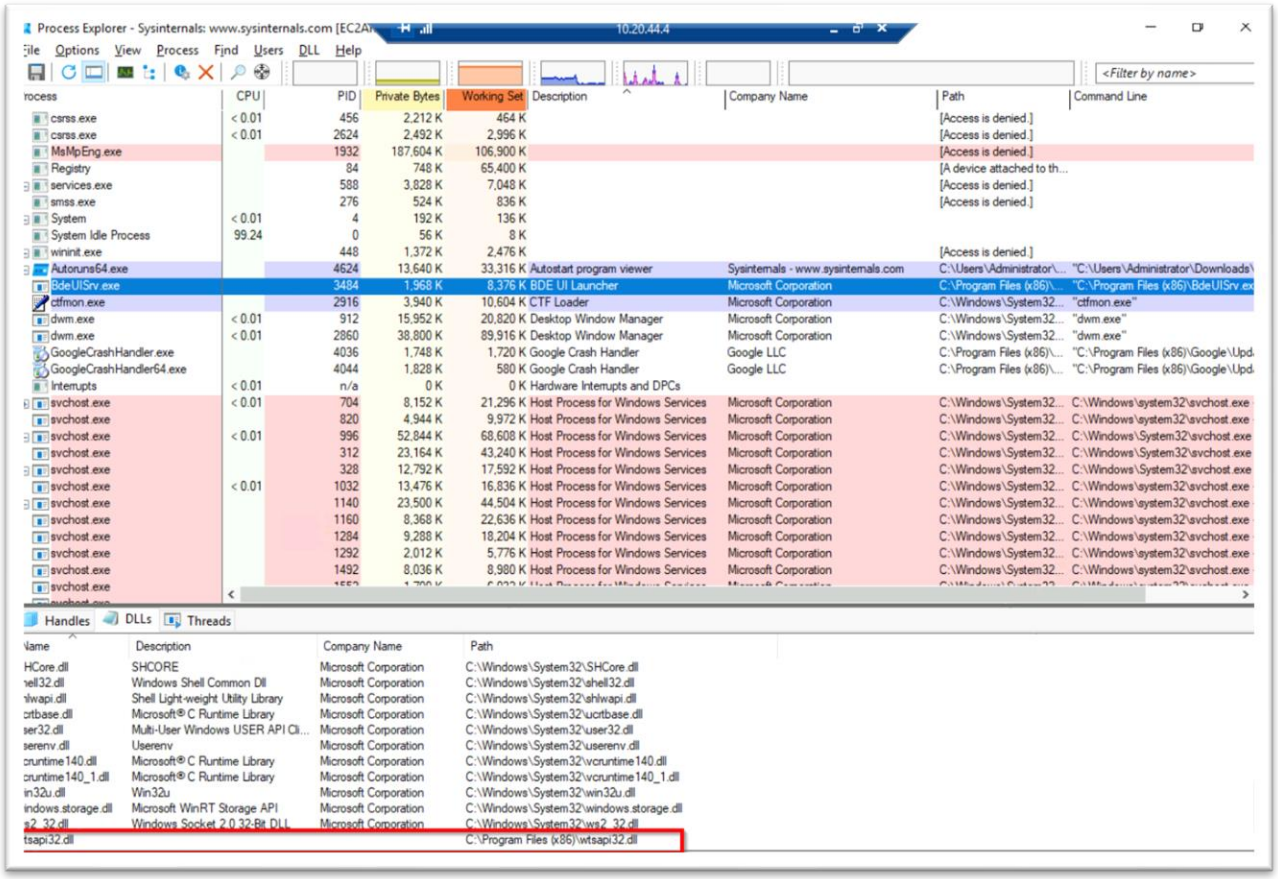


Figure 4. BdeUISrv.exe spawns wtsapi32.dll, unverified and not located in \System32

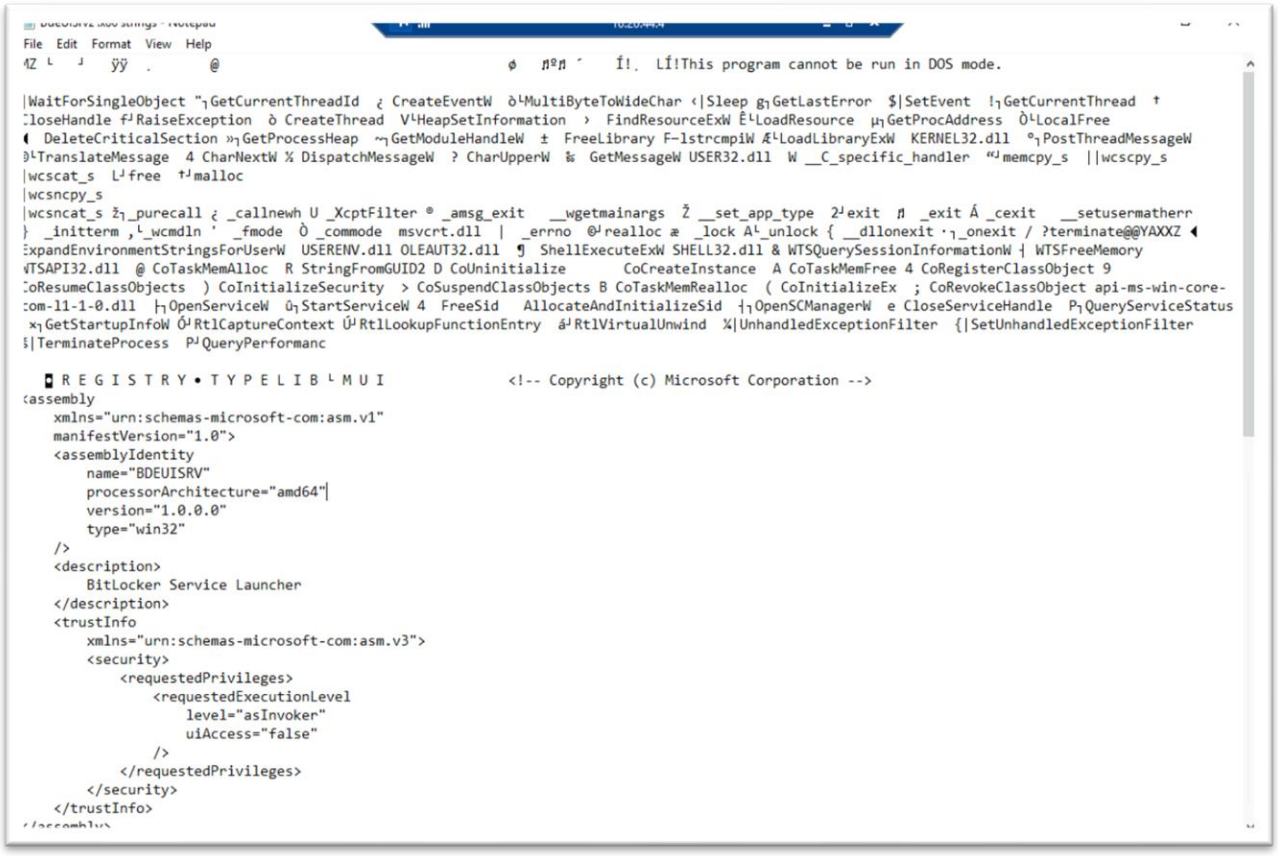


Figure 5. BdeUiSrv.exe contain code.

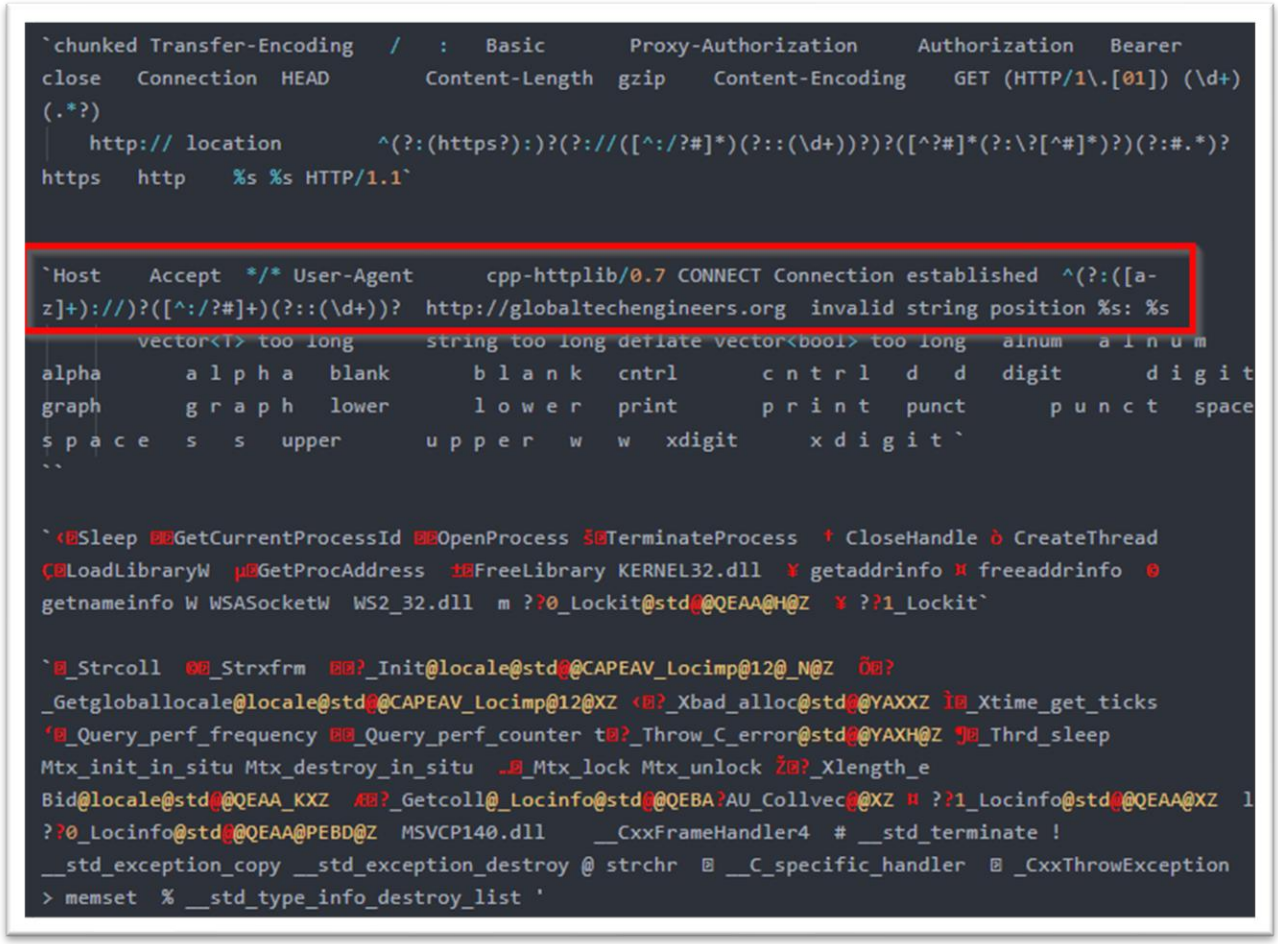


Figure 6. Directs to globaltechengineers.org. It also contains code to load additional DLLs and enumerate the machine.

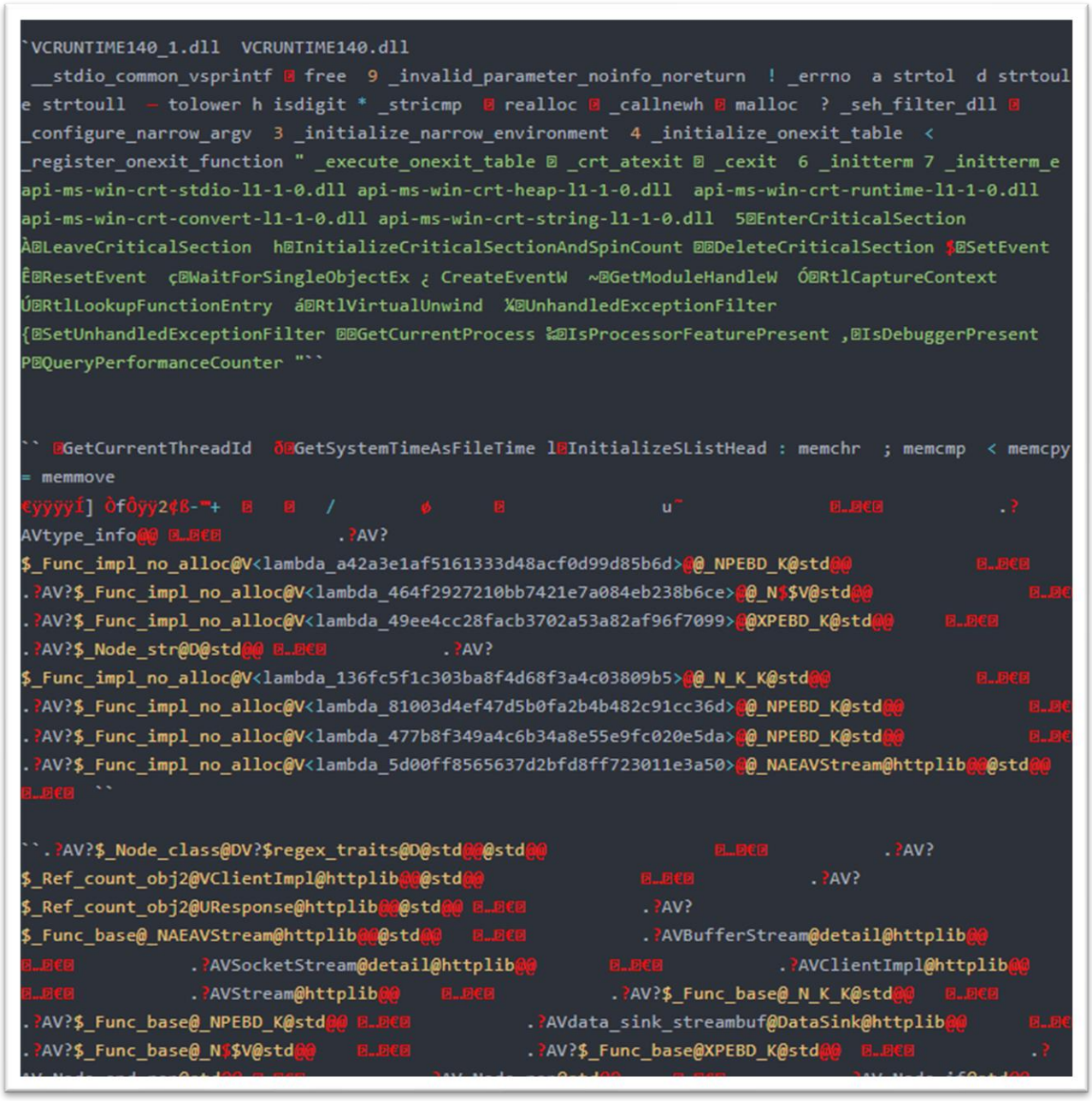
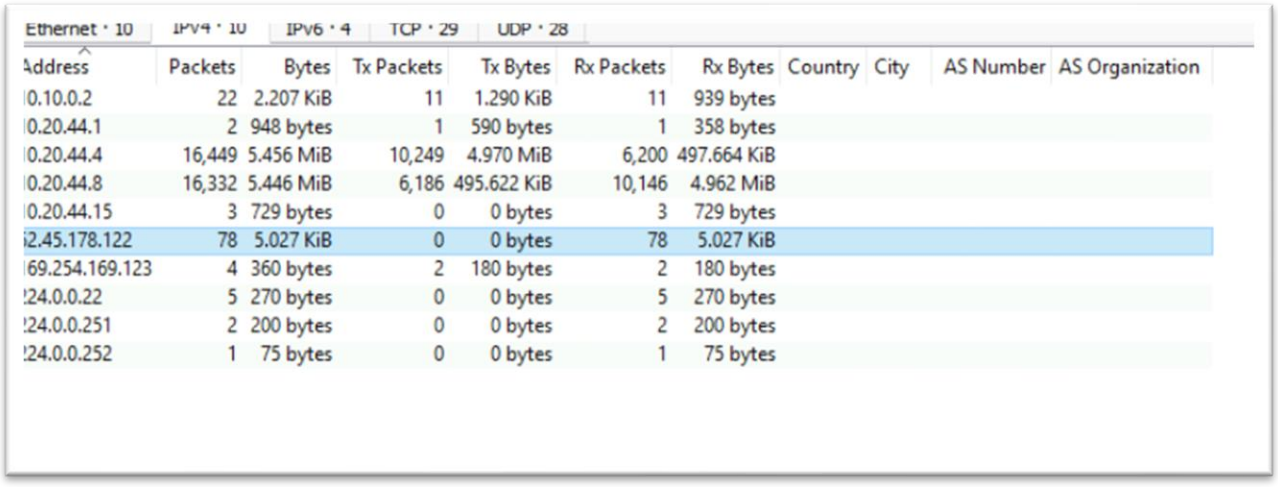
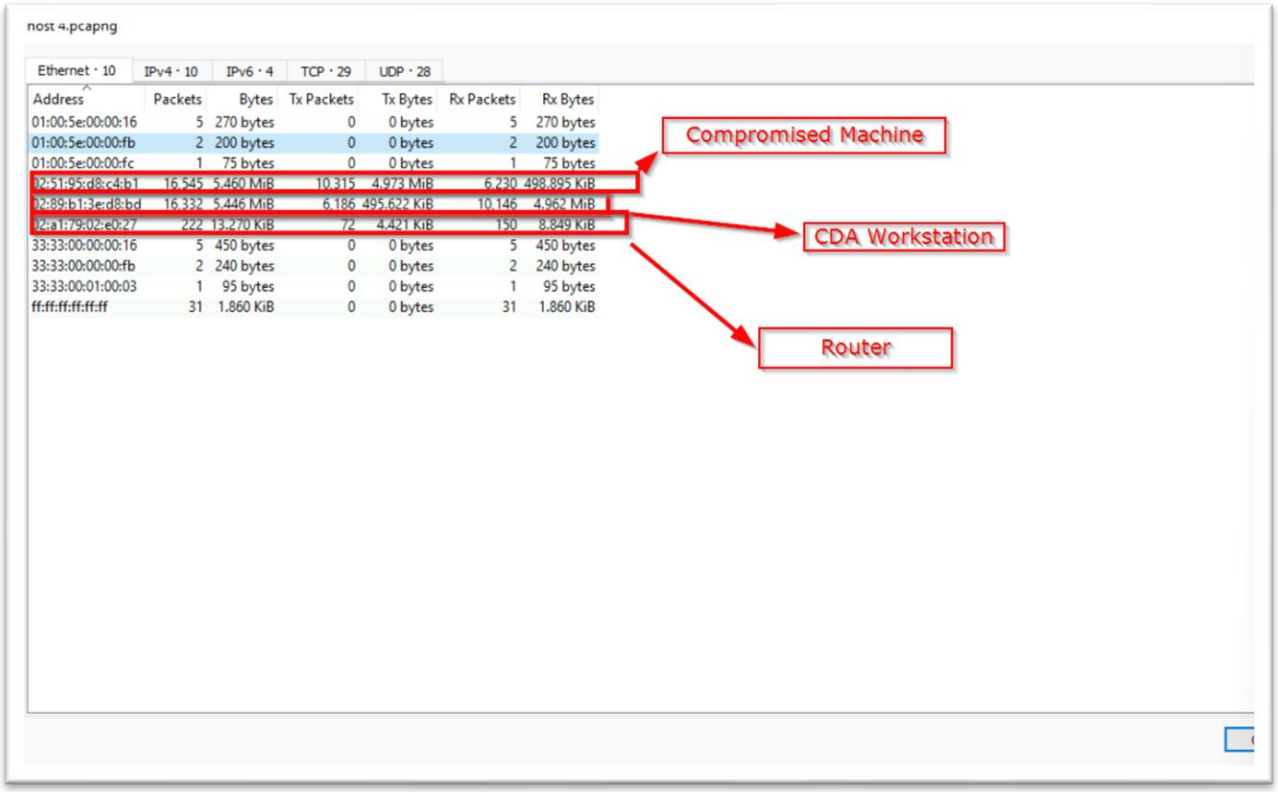


Figure 7. Additional code from wtsapi32.dll.



Address	Packets	Bytes	Tx Packets	Tx Bytes	Rx Packets	Rx Bytes	Country	City	AS Number	AS Organization
0.10.0.2	22	2.207 KiB	11	1.290 KiB	11	939 bytes				
0.20.44.1	2	948 bytes	1	590 bytes	1	358 bytes				
0.20.44.4	16,449	5.456 MiB	10,249	4.970 MiB	6,200	497.664 KiB				
0.20.44.8	16,332	5.446 MiB	6,186	495.622 KiB	10,146	4.962 MiB				
0.20.44.15	3	729 bytes	0	0 bytes	3	729 bytes				
2.45.178.122	78	5.027 KiB	0	0 bytes	78	5.027 KiB				
69.254.169.123	4	360 bytes	2	180 bytes	2	180 bytes				
24.0.0.22	5	270 bytes	0	0 bytes	5	270 bytes				
24.0.0.251	2	200 bytes	0	0 bytes	2	200 bytes				
24.0.0.252	1	75 bytes	0	0 bytes	1	75 bytes				

Figure 8. Highlighted endpoint is globaltechengineers.org See the following for explanation of the other endpoints.



Address	Packets	Bytes	Tx Packets	Tx Bytes	Rx Packets	Rx Bytes
01:00:5e:00:00:16	5	270 bytes	0	0 bytes	5	270 bytes
01:00:5e:00:00:fb	2	200 bytes	0	0 bytes	2	200 bytes
01:00:5e:00:00:fc	1	75 bytes	0	0 bytes	1	75 bytes
02:51:95:d8:c4:b1	16,545	5.460 MiB	10,315	4.973 MiB	6,230	498.895 KiB
02:89:b1:3e:d8:bd	16,332	5.446 MiB	6,186	495.622 KiB	10,146	4.962 MiB
02:a1:79:02:e0:27	222	13.270 KiB	72	4.421 KiB	150	8.849 KiB
33:33:00:00:00:16	5	450 bytes	0	0 bytes	5	450 bytes
33:33:00:00:00:fb	2	240 bytes	0	0 bytes	2	240 bytes
33:33:00:01:00:03	1	95 bytes	0	0 bytes	1	95 bytes
ff:ff:ff:ff:ff:ff	31	1.860 KiB	0	0 bytes	31	1.860 KiB

Figure 9. Only these points had meaningful traffic. The CDA Workstation remotely connected to the compromised machine. The other endpoints are part of GoodCorp network infrastructure.

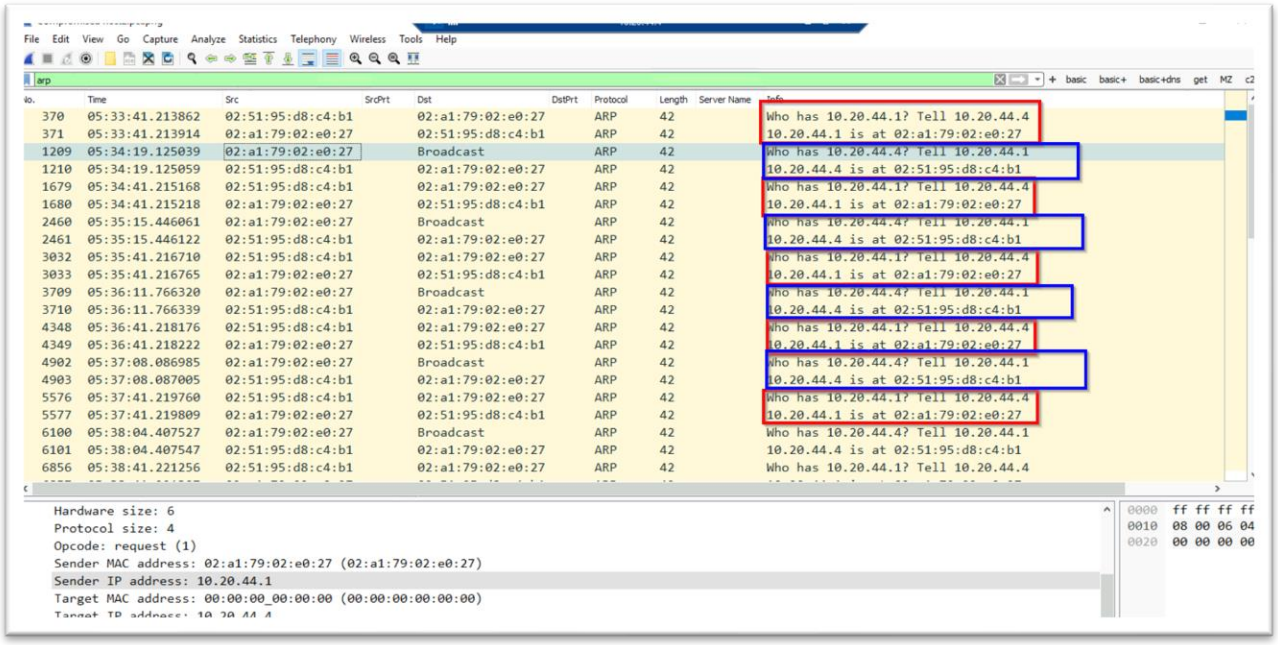


Figure 10. Rapid ARP requests between the compromised machine and GoodCorp router. If the connection to the attacker was complete, this would be used to "fool" the router into sending traffic through the attacker's machine.

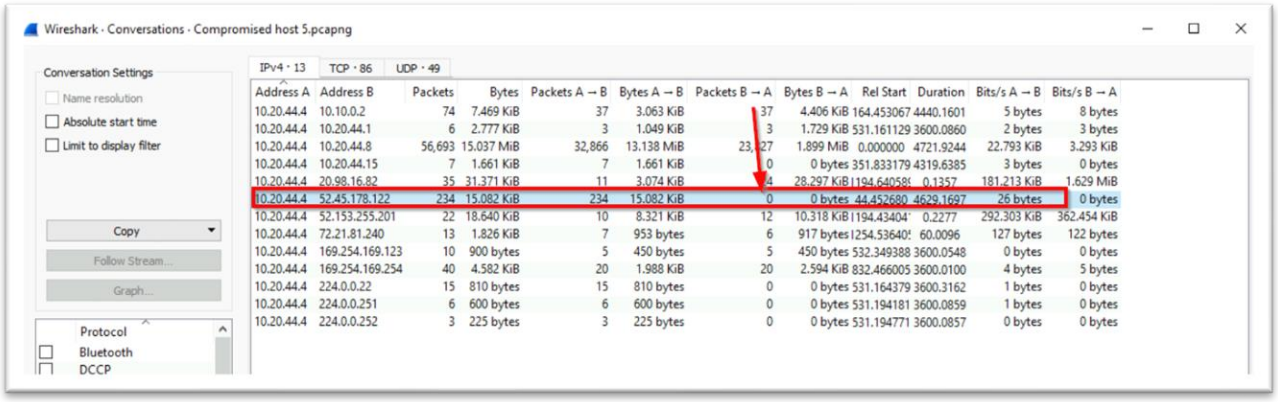


Figure 11. The host attempted to connect to globaltechengineers.org but it did not answer.

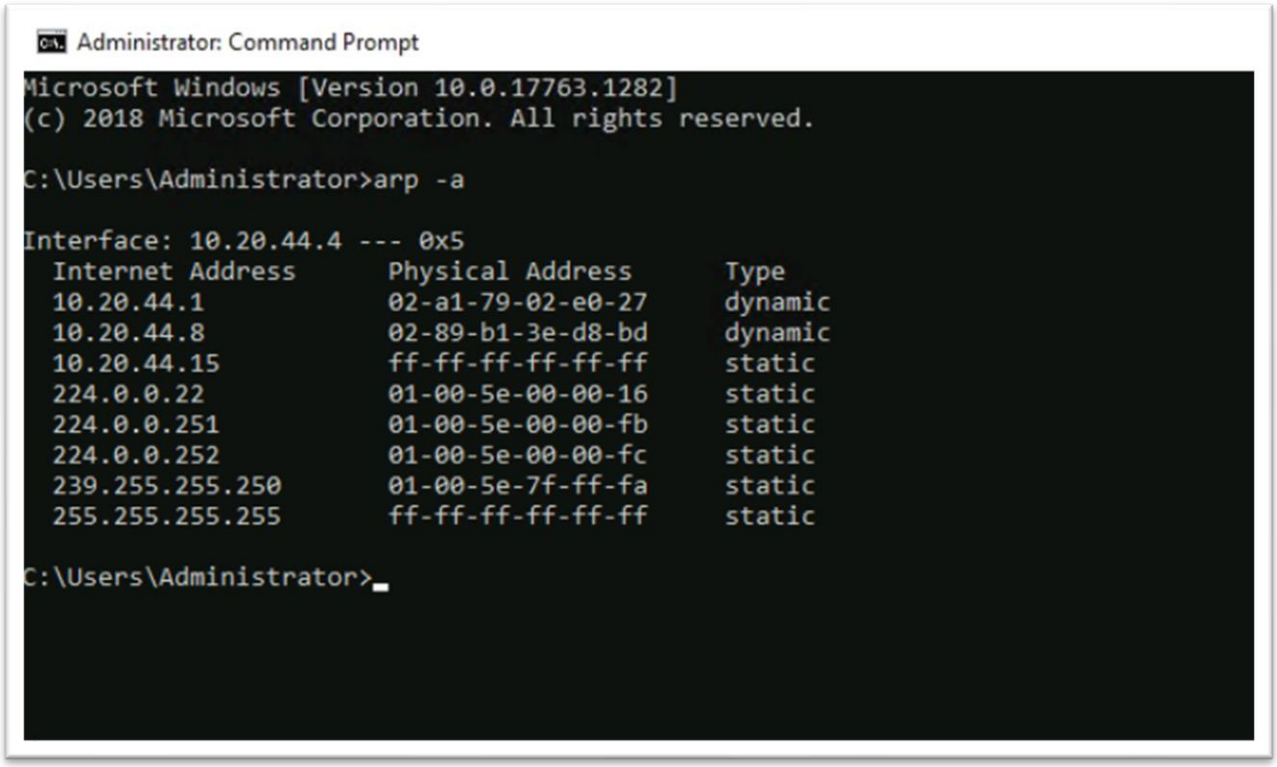
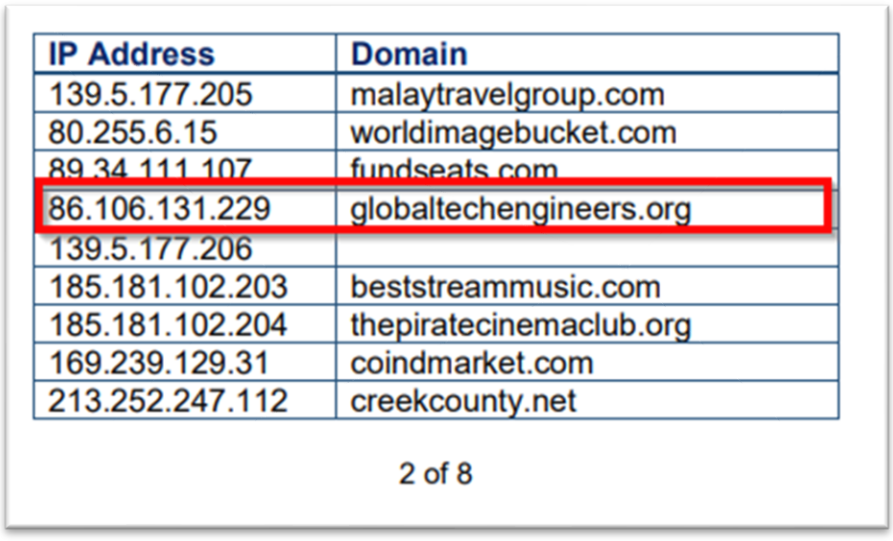


Figure 12. An arp -a command done at frequent intervals did not show any other connections to the host.



IP Address	Domain
139.5.177.205	malaytravelgroup.com
80.255.6.15	worldimagebucket.com
89.34.111.107	fundseats.com
86.106.131.229	globaltechengineers.org
139.5.177.206	
185.181.102.203	beststreammusic.com
185.181.102.204	thepiratecinemaclub.org
169.239.129.31	coindmarket.com
213.252.247.112	creekcounty.net

2 of 8

Figure 13. A portion of the UK National Cyber Security Centre listing sites known to be used by Fancy Bear.

--End--