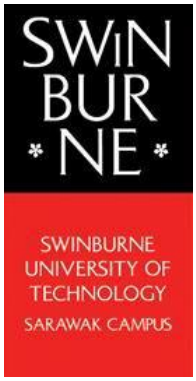

Swinburne University of Technology Hawthorn Campus
Department of Computing Technologies

COS30015 IT Security

Assignment 2 - *Semester 2, 2024*

Part A Incident Forensic Analysis

Student Name: Duong Minh Hoang

Student ID: 104487115

Due Date: AEST 23:59 on 31/10/2024.

Add your answers in the appropriate locations by replacing <answer> with your answer.

Impact at STARFLEET

1. What type of threat does this appear to be?

- This might be a ransomware attack as described in the scenario, all the files have been impacted, and are unable to open.

2. What is the indicator associated with this threat type?

- The indicator associated with this threat type is the **".locked" file extension.** In many ransomware attacks, files are often renamed to a new extension after being encrypted, rendering them inaccessible.

3. What main MITRE ATT&CK technique is associated with this incident type?

- The main MITRE ATT&CK technique associated with this incident is **T1486 – Data encrypted for impact.**

Unknow file identified

1. Is agent.exe a normal file?

- Agent.exe is not a normal file as Chris does not recall downloading it.

2. What type of file is agent.exe?

- Agent.exe is an EXECUTABLE file, a window-specific executable file format containing machine code to execute.

3. Analysing the agent.exe-12345678.pf file, has agent.exe been executed before?

- The agent.exe has been executed before according to the pf file on 10/09/2024, 14:35:33

4. How many times has the file been executed?

- The file has only been executed once.

5. What does this file allow an adversary to do?

- The file could allow an adversary to execute malicious code contained in the file itself, potentially giving them control or accessing the machine, tampering the CIA triad.

Signs of tampering

1. Can you make sense of this command? What is last part decoded?

- Yes, the powershell -EncodedCommand is used to run a command encoded in base64 format. So last part is decoded from base64 to “Set-ExecutionPolicy unrestricted”.

2. What does this command do?

- This command will set PowerShell execution policies to Unrestricted, allowing unsigned scripts to be run.

What was disabled

1. What does this script do?

- This script contains the provided encoded base64 string which could be translated into Set-MpPreference -DisableRealtimeMonitoring $true, which will **disable realtime monitoring of Window Defender scan and updates**.

2. Is the previous command and this script potentially related?

- The previous command and this script are potentially highly related as explained below.

3. Could it have allowed system changes which would allow agent.exe to be ran?

   The command disabled Window Denferder's real-time monitoring, opening the way for malicious files like agents.exe to be executed without being detected.

4. What device was this script copied from?

- This script was copied from a device within the internal of STARFLEET as explained below.

Signs of movement

1. What type of event is this?

- According to the Sysmon log entry provided, the provided EventID is 4624, indicating **an account was successfully logged on.**

2. Does this event confirm someone logged onto this device?

- This event does confirm someone logged onto the device.

3. Where did the connection occur from?

- According to Sysmon log entry, the connection seems to be occurred from **192.168.200.10**, which according to the STARFLEET topology, is **the Domain controller (DC)** machine, resided in the Server LAN.

4. What does the type/port indicate?

- The port indicated is **port 3389**, which is a assigned port for **Remote Desktop Protocol (RDP).**

5. What main MITRE ATT&CK tactic is represented here?

- The main MITRE ATT&CK tactic represented here is **Lateral Movement (TA0008)** (T1021.001 - Remote Services: Remote Desktop Protocol)**.**

Other indicators identified

1. What can be summarised from the events recorded in the log file?

- The events recorded in the Sysmon log file is a combination of failed log on attempt (EventID 4625), before a successful log on attempt (EventID 4624) at the end of the log file, indicating a password bruteforce attacks toward the Domain Controller (DC)

2. Was the attack successful?

- The attack was successful as indicated an successful log on attempt (EventID 4624) at the end of the log file explained above.

3. What account was targeted?

- The targeted account was the "Admin" account of Domain Controller as indicated in the log file.

4. Where did the connection originate from?

- The connection originate from **192.168.100.20,** in which according to the STARFLEET topology, is the **Remote access (RM)** machine resided in DMZ.

5. What does the type/port indicate?

- The port indicated is **port 3389**, which is a assigned port for **Remote Desktop Protocol (RDP).**

6. What main MITRE ATT&CK tactic is represented here?

- The main MITRE ATT&CK tactic represented here is **Lateral Movement (TA0008)** (T1021.001 - Remote Services: Remote Desktop Protocol) and **Privilege Escalation (TA0004)** (T1078 - Valid Accounts)**.**

7. Should a connection of this type be allowable between these two servers?

- Allowing RDP access from a less secure zone (DMZ) that is could be internet facing, despite residing behind a firewall, still presents a significant security risk. Therefore, connection like this type should not be allowable, must be heavily restricted and monitored.

Impacted Account

1. What is the original password used to access the DC?

   <answer>

2. What Cipher was used obtain the original password?

   <answer>

Initial Access

1. It appears the adversary logged into the Remote Access machine using a STARFLEET user account. What account was used?

- The adversary logged into the Remote access machine using the **Remote65** account, as indicated in the SubjectUserName.

2. What IP address was used to access the Remote Access machine (be careful to defang this IP address)

- The ip address used to access the Remote Access machine was 171[,]25[.]193[.]25 as indicated in the IpAddress field.

3. What is interesting about this IP address?

- This ip address is part of publicly available **Tor network**, more specifically **Tor exit node**, which is commonly used by attackers to anomynize connections.

4. What remote access method was used?

- The remote access method used was **RDP (Remote Desktop Protocol)** as indicated by port 3389.

Missing Data

1. What file was uniquely downloaded which could be a sensitive data leak?

- The unique downloaded file that could be a sensitive data leak is **"Starfleet_secrets.txt"**

2. What IP downloaded this file? (be careful to defang this IP address)

- The ip that downloaded this file is "80[.]67[.]167[.]81"

3. What is interesting about this IP address?

- The ip appears to be an external IP address, possibly outside of the internal STARFLEET network from many private 192.168.1.0/24 IP addresses

4. Who downloaded this file?

- According to the log, the file is downloaded by Klingon.

Incoming mail

1. Who is the proper sender of the email? (be careful to defang this domain)

- Even though the "from" field indicated that this email was sent from Kaptian Kirk or captain[.]kirk@starfleet[.]com, the email was sent from phish@fakeemail[.]com

2. What was IP address of this sender? (be careful to defang this IP address)

- The IP address of this sender is 183[.]81[.]169[.]238.

3. What is interesting about this IP?

- This ip address appears to be from an external source that is not associated with STARFLEET.

Patient zero

1. What is the name of the file?

- The name of the file is Lockheed_Martin_JobOpportunities.docx

2. What is the SHA256 hash of the file?

- The SHA256 hash of the file is 0160375e19e606d06f672be6e43f70fa70093d2a30031affd2929a5c44 6d07c1

3. Is the file safe?

- Even though the file looks like a harmless docx file, according to VirusTotal hash scanner, this file is a trojan known as **trojan.w97m/cobeacon**

4. How can you verify if the file is safe?

- In order to verify if the file is safe, we can utilize tool like VirusTotal, Hybrid Analysis, and anti virus like Malwarebytes and Kaspersky.

5. What threat group did this file come from?

- Since the file is using w97m, according to VirusTotal, this file might come from the cyber threat group known as Lazarus Group (G0032).

6. How might this file be analysed safely?

- This file can be analyzed by looking up the hash on the virus/thread database, checking for file metadata, script, macros, and signatures, or can be opened in a fully isolated environment like Sandbox Virtual Machine.

Easter Eggs (HD Only)

1. Easter Egg 1: <answer>

2. How did you find Easter Egg 1?

   <answer>

3. Easter Egg 2 (both name and content): <answer>

4. How did you find Egg 2?

   <answer>