



Swinburne University of Technology Hawthorn Campus

Department of Computing Technologies

COS30015 IT Security

Assignment 2 - Semester 2, 2024

Part B Incident Situational Report

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

Having investigated all the artefacts provided by STARFLEET, they have requested a situation report update to understand the incident.

Compute the following template with your findings from your investigation.

STARFLEET SITREP		
Impacted STARFLEET Accounts	Student & Student ID	Minh Hoang Duong - 104487115
	Class	Fri, 2:30pm – 4:30pm
Chris Pike's credential. Admin (on the Domain Controller/DC\$).	Tutor	Yasas AkuruddaLiyanage Don
Incident Timeline	Impacted STARFLEET Hosts	
09 Sep 2024: 08:45:12: Chris Pike received the phishing email containing the "Lockheed_Martin_JobOpportunities.docx" malicious file 13:23:14: the malicious "Lockheed_Martin_JobOpportunities.docx" file was executed, possibly compromising Chris Pike's credentials.	UserLan-PC8 (UserLan-PC8\$) (Chris Pike's computer). <ul style="list-style-type: none">– Severity: High– Explain: As the device itself has been remotely accessed successfully, and encrypted all the files, the compromised severity is high.	

10 Sep 2024:

10:24:01: The threat actor gained initial access using Chris Pike's compromised account to Remote Access Machine (Remote\$) from a TOR exit node's IP address (171.25.193.25). (Remote Access Machine Sysmon log.)

11:21:00 – 11:25:50: The threat actor remotely brute-forces password to gain access to the Domain Controller machine (DC\$) from the Remote Access Machine (192.168.100.20). (DC.log.txt)

11:26:01: The brute-force attack succeeded, and the threat actor gained access to Domain Control machine (DC\$). (DC.log.txt)

12:01:00: The threat actor remotely connected to Chris Pike's computer from the Domain Controller machine (192.168.200.10), possibly moving agent.exe and RunMe.ps1.

14:35:33: The **agent.exe** file got executed on Chris Pike's computer.

(agent.exe-12345678.pf)

12 Sep 2024:

11:24:28: Samba_log recorded a malicious download attempt from external IP address 80.67.167.81 of the user Klong, downloading starfleet_secrets.txt (samba_log.csv)

Domain Controller (DC\$).

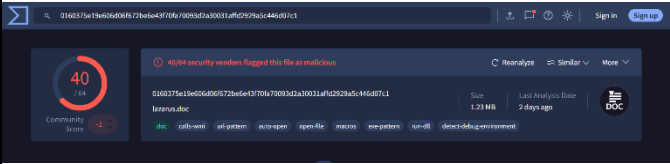
- **Severity:** High
- **Explain:** The device has been successfully remotely accessed with the privileged account of "admin", possibly the equivalent of a "root" account.

Remote Access Machine (Remote\$).

- **Severity:** Medium
- **Explain:** Even though the machine itself has been remotely accessed, there was no sign of any other destruction made by the adversaries. On the other hand, successfully malicious remote access is still considered a highly severe compromise.

All other devices in the domain that Mr Suru searched.

- **Severity:** Medium
- **Explain:** After Mr Suru's search across the domain for devices with RunMe.ps1 file on them, almost all the devices have been infected. Given that the RunMe.ps1 file contain the command to disable Window Defender real-time protect, there are no other sign of destruction being made.

IoCs Observed	TTPs Observed
<p>agent.exe:</p> <p>SHA256:</p> <pre>d806e3e0c84b0b7208fb4ba9df5cd7b8851abce5c0bbb3ee330560aaa139f243</pre> <p>Command:</p> <pre>powershell -EncodedCommand U2V0LUV4ZWV4ZWN1dGlvb1BvbG1jeSB1bnJlc3RyaWN0ZWQ=</pre> <p>RunMe.ps1</p> <p>Command:</p> <pre>U2V0LU1wUHJlZmV5ZW5jZSA0RGlzYWJsZVJlYWw0aW1lTW9uaXRvcmluZyAkdhJlZQ==</pre> <p>External IP address:</p> <p>171.25.193.25: accessing into RM machine (RM machine Sysmon log).</p> <p>80.67.167.81: indicating user Klinton downloading "starfleet_secrets.txt" (samba_log.csv).</p> <p>Spoofed email, suspicious email domain, spelling errors:</p> <p>Kaptian Kurk (captain.kirk) => spelling error</p> <p>captian[.]kirk@starfleet[.]com => spoofed email sender.</p> <p>mail[.]fakemail[.]com (183[.]81[.]169[.]238) => suspicious email domain.</p> <p>Lockheed_Martin_JobOpportunities.docx</p> <p>MD5/SHA256:</p> <pre>Hash: MD5= a27a9324d282d920e495832933d486ee, SHA256= 0160375e19e606d06f672be6e43f70fa70093d2a30031affd2929a5c446d07c1</pre> <p>Note: The hash was flagged as malicious</p>  <p>.locked file extension discovered on Chris Pike</p>	<p>Tactic: Reconnaissance (TA0043), Initial Access (TA0001), Privilege Escalation (TA0004), Defense Evasion (TA0005), Credential Access (TA0006), Lateral Movement (TA0008), Collection (TA0009), Exfiltration (TA0010), Impact (TA0010).</p> <p>Tactic, Technique:</p> <p>Reconnaissance (TA0043): Phishing(T1566) – Spearphishing Attachment(T1566.001)</p> <p>Initial Access (TA0001)/Privilege Escalation(TA0004): Valid Account (T1078) – Local Account (T1078.003)</p> <p>Defense Evasion (TA0005): Impact Defense(T1562) – Disable or Modify Tools (T1562.001).</p> <p>Credential Access (TA0006): Bruteforce (T1110).</p> <p>Lateral Movement (TA0008): Remote Service(T1021) - Remote Desktop Protocol (RDP) (T1021.001).</p> <p>Collection (TA0009): Data Staged(T1074) – Remote Data Staging (T1074.002)</p> <p>Exfiltration (TA0010): Exfiltration Over Alternative Protocol (T1048) - Exfiltration Over Unencrypted Non-C2 Protocol (T1048.003)</p> <p>Impact (TA0010): Data Encrypted for Impact (T1486)</p>

Remediation Advice**TTPs, Explanation & Remediation advice.**

Reconnaissance (TA0043): Phishing(T1566) – Spearphishing Attachment (T1566.001)

- **Explanation:** The adversary sent the phishing email containing a malicious .docx file to Mr Suru's email with a spoofed domain name and account.
- **Remediation advice:** STARFLEET could implement many email security technologies, filtering such as SPF (Sender Policy Framework) to help identify and authorize mail servers, domain names to be received, DKIM (DomainKeys Identified Mail) to prevent impersonating, and spoofing legitimate domains like the scenario above, DMARC (Domain-based Message Authentication Record), which is an email authentication method built on top of DKIM and SPF, to describe what to do with an email that fail SPF and DKIM. Other technologies included SEG (Secure email gateway), Content Disarm, and Reconstruction (CDR) to filter high-risk attachments like .exe, .docx, .ps1, .zip,... or potentially dangerous elements in those attachments like embedded script and macros.
- The corporation could also implement User training and awareness including, identifying phishing email like spoofed sender, suspicious contents and spelling errors, avoiding or sandboxing high-risk unexpected attachment, reporting to the IT (cybersecurity) department as human factors always play an important role in cyber security in general and in social engineering and phishing itself specifically.

Initial Access (TA0001)/Privilege Escalation(TA0004): Valid Account (T1078) – Local Account (T1078.003)

- **Explanation:** The adversary used Chris Pike's compromised local account collected from the above to gain initial access to Remote Access machine and using the same compromised account to escalated into UserLan-PC8 later on (Chris Pike's computer).
- **Remediation advice:** Given that the local account has been compromised, STARFLEET could implemented Multi-factor authentication (MFA) making it harder for the attacker to login and abuse compromised account even though that account has been compromised. The corporate could also implement Role-based Access control (RBAC) and enforcing least privilege principle to minimize destruction after the account being breached.

Defense Evasion (TA0005): Impact Defense(T1562) – Disable or Modify Tools (T1562.001).

- **Explanation:** The files RunMe.ps1 and partially agent.exe disable window defender realtime monitoring and loosen PowerShell execution policy in order for the malicious encryption process to be executed.
- **Remediation advice:** Given that the corporate only used window defender as the primary endpoint security for each machine, and could be disabled easily via

PowerShell command, STARFLEET could implement endpoint anti-virus such as MalwareByte, Kasperski total security or advanced Endpoint Detection and Response (EDR) like Crowdstrike Falcon for malicious process, software detection, and monitoring.

- Limiting script execution according to roles, disabling macros and unnecessary script by restricting tools like PowerShell, and CMD, and implementing Role-based Access control (RBAC) with least privilege principle enforcement could also help reduce the risk of malicious script execution given that Window Defender can only be disabled under administration privilege in window.

Credential Access (TA0006): Bruteforce (T1110).

- **Explanation:** The threat actor brute-forced the admin account into the Domain control machine from the Remote Access machine.
- **Remediation advice:** Implementing brute-force defense methods such as limiting login attempts, network traffic monitoring for repeated login attempts, and Multi-factor authentication. Strong password policies and password managers could also implemented to reduce the risk of successful brute-force attacks given that the attacker succeeded after only 15 attempts.

Lateral Movement (TA0008): Remote Service(T1021) - Remote Desktop Protocol (RDP) (T1021.001).

- **Explanation:** Throughout the attacking process, the threat actor utilized Remote Desktop Protocol (RDP, or port 3389) to move, and elevate between multiple machines from Remote Access, Domain Controller, and Chris Pike's computer.
- **Remediation advice:** high-risk communication protocols like 3389 (RDP), 22 (SSH), 23 (Telnet), 135 (RPC),... must be restricted by implementing firewalls, access control list to block unnecessary communication between machines (machine group), defining specific communication between each machine (groups) centralizing machine groups. Using Privileged Access Workstations (PAW), which means creating dedicated machines for administrators, and users with high privilege, would also reduce the risk of Lateral movement within the network.

Collection (TA0009): Data Staged(T1074) – Remote Data Staging (T1074.002)

Exfiltration (TA0010): Exfiltration Over Alternative Protocol (T1048) - Exfiltration Over Unencrypted Non-C2 Protocol (T1048.003)

- **Explanation:** The threat actor exfiltrated "starfleet_secrets.txt" by downloading directly via Samba.
- **Remediation advice:** Implementing Access control Lists (ACLs) and restricting permission based on roles and trusted IP address (private IP address) to limit access to Samba shares and disable Guess access given that the downloaded IP address is an outsider's public IP address. Setting up an alert for unusual file access and flagging important files for further alerting and notification. Hard drive, storage encryption like VeraCrypt, GnuPG, and BitLocker could also be implemented for further data security, reducing the risk of data breaches.

Impact (TA0010): Data Encrypted for Impact (T1486)

- **Explanation:** The threat actor encrypted mostly all of the files on Chris Pike's computer, and renamed mostly all of the files into ".locked" extension.
- **Remediation advice:** Regularly backup data and isolate backup storage to ensure redundancy, protecting them from ransomware attacks and data recovery as an incident response after important data is encrypted. Disabling Macros and scripting, deploying endpoint security like Kasperski Total Security, MalwareByte, or advanced endpoint detection and response (EDR) like CrowdStrike Falcon or SentinelOne to detect and respond to ransomware behavior, suspicious scripts, and commands.

In general, STARFLEET could also deploy multiple security measures facing the internet, including intrusion detection system (IDS), intrusion prevention system (IPS) for prevention against initial access via the internet, suspicious network traffic, and behavior detection. The corporation could also develop incident response plans, organize cyber security education, and practice to defend against cyber incidents.