Assignment 2 PART B

SITE REP for the STARFLEET incident as the Cyber Forensic Analysis

|  |  |  |
| --- | --- | --- |
| STARFLEET SITREP | | |
| Impacted STARFLEET Accounts | Student ID | Arun Ragavendhar Arunachalam Palaniyappan 104837257 |
| **Chris Pike** – His account credentials were stolen using a phishing email and were later used by the attacker to log in remotely.  **Admin** – The attacker brute-forced the Admin account from inside the network by password guessing and gained full control of the Domain Controller.  **Klingon** – This account was used to download a sensitive internal document. It was either fake, hijacked, or planted by the attacker. | Class | Friday – 06:30 PM to 08:30 PM |
| Tutor | Yasas Akkurudha Liyanage Don |
| Incident Timeline | Impacted STARFLEET Hosts | |
| **09 April 2025 – 06:45 PM (AEST)** – Chris Pike receives a phishing email pretending to be a job offer. It was sent from phish@fakeemail.com, masking as a STARFLEET contact. *(08:45 AM UTC)*  **09 April 2025 – 11:23 PM (AEST)** – Chris opens the attached document. A hidden script runs and steals his username and password. *(01:23 PM UTC)*  **10 April 2025 – 08:24 PM (AEST)** – Using the stolen credentials, the attacker logs into STARFLEET’s DMZ Remote Access system from an IP that belongs to the Tor network (171.25.193.25). *(10:24 AM UTC)*  **10 April 2025 – 09:26 PM (AEST)** – The attacker moves from the DMZ to the Domain Controller using brute-force to crack the Admin account password. *(11:26 AM UTC)*  **10 April 2025 – 10:01 PM (AEST)** – Another login happens from inside the network to Chris’s personal device (UserLan-PC8). *(12:01 PM UTC)*  **10 April 2025 – 10:15 PM (AEST)** – A PowerShell command is used to bypass script restrictions on Chris’s computer. *(12:15 PM UTC)*  **10 April 2025 – 10:18 PM (AEST)** – A script (RunMe.ps1) disables Windows Defender’s real-time protection. *(12:18 PM UTC)*  **11 April 2025 – 12:35 AM (AEST)** – The ransomware program (agent.exe) is run. It encrypts and locks out all the files. *(02:35 PM UTC)*  **25 April 2025 – 05:34 PM (AEST) / 07:34 AM (UTC)** The attacker opened the batch file AAAAAAAAAAAAAAAA.bat using Notepad (PID 6640), likely to check or make changes before running it. This shows they were interacting with the file manually.  **25 April 2025 – 05:50 PM (AEST) / 07:50 AM (UTC)** The attacker has SYSTEM Access. The batch file AAAAAAAAAAAAAAAA.bat is executed through cmd.exe (PID 8576) and it launched timeout.exe and conhost.exe at the same moment, On **MrSuru’s** system. The script ran in a loop and had persistence enabled.  **25 April 2025 – 05:52 PM (AEST) / 07:52 AM (UTC)** Shortly after, STARFLEET investigators captured memory using RamCapture64.exe (PID 416). This snapshot was taken while the batch script was still running. The file no longer exists on disk, proving it ran directly from memory and was never saved permanently. | **Impacted STARFLEET Hosts**  **Remote (DMZ Gateway)**  High impact  This was the attacker’s first entry point into the internal network using Remote Desktop Protocol.  **RM.20 (Server LAN)**  High impact  It was used to carry out the brute-force attack on the Admin account.  **Domain Controller (DC)**  Critical impact  SYSTEM access achieved. This gave the attacker full control over the STARFLEET network and allowed to push commands across all machines.  **UserLan-PC8 (Chris’s device)**  High impact  This is where the ransomware (agent.exe) was directly executed by direct login into the user account. All files were encrypted.  **DESKTOP-CRPG57R (MrSuru’s machine)**  High Impact  Direct brute force login by attacker failed, but SYSTEM scripts still ran here using domain-level push. The AAAAAAAAAAAAAAAA.bat Batch file ran in loop and was wiped after execution.  These hosts were not just targeted—they were each used as stepping stones to move forward in the attack. | |
|  |
|  |
|  |
|  |
|  |
|  |
|  |
|  |
|  |
|  |
|  |
|  |
|  |
|  |
|  |
|  |
|  |
|  |
|  |
|  |
|  |
|  |
|  |
|  |
|  |
|  |
|  |
|  |
|  |
|  |
|  |
|  |
|  |
|  |
|  |
|  |
| **Important Note:**  After the attacker cracked the Admin password (1q2w3e4r5t6y) on the Domain Controller, they gained SYSTEM-level access across the entire STARFLEET network. This gave them full control to run commands on any machine, even without logging into each one. For example, no one logged into MrSuru’s account, but malware and shutdown scripts still ran on his device because of this remote SYSTEM access. Only Chris Pike’s credentials were stolen — no other user accounts were cracked. All the damage came from having SYSTEM control over the network. | | |  |
| IOC’s Observed:   |  |  | | --- | --- | | **Type** | **Description** | | **File Names** | agent.exe — Malicious ransomware binary executed on Chris's machine (hash matched to known ransomware) | | RunMe.ps1 — PowerShell script to disable Windows Defender | | AAAAAAAAAAAAAAAA.bat — Batch script found in memory, not on disk; used to disable security features | | starfleet\_secrets.txt — Sensitive file exfiltrated from internal share | | **File Hashes** | 0160375e19e606d06f672be6e43f70fa70093d2a30031affd2929a5c446d07c1 — Phishing DOCX (VirusTotal confirmed) | | d806e3e0c84b0b7208fb4ba9df5cd7b8851abce5c0bbb3ee330560aaa139f243 — agent.exe (known ransomware sample) | | **PowerShell Commands** | Set-MpPreference -DisableRealtimeMonitoring $true – Defender turned off | | Set-ExecutionPolicy Unrestricted – allows execution of any script | | **Encoded Commands** | U2V0LU1wUHJlZmVyZW5jZSAtRGlzYWJsZVJlYWx0aW1lTW9uaXRvcmluZyAkdHJ1ZQ== and U2V0LUV4ZWN1dGlvblBvbGljeSB1bnJlc3RyaWN0ZWQ= (both decoded to security disabling commands) | | **External IPs** | 171.25.193.25 — Tor IP used to access DMZ via RDP (Event ID 4624) | | 80.67.167.81 — IP that downloaded starfleet\_secrets.txt (exfiltration) | | **Sender Email** | phish@fakeemail.com — Spoofed phishing sender | | **Sender IP** | 183.81.169.238 — Vietnam-based SMTP sender (from phishing email headers) | | **User Accounts** | Chris Pike — credentials phished and reused | | Admin — targeted and cracked through brute-force | | Klingon — used to download secrets.txt (likely created or hijacked) | | | |  |
| TTPs Observed:   |  |  |  |  | | --- | --- | --- | --- | | **#** | **MITRE ID** | **Name** | **Confirmed Evidence** | | 1 | **T1486** | Data Encrypted for Impact | agent.exe encrypted files (prefetch confirms execution) | | 2 | **T1059.001** | PowerShell | Set-MpPreference, Set-ExecutionPolicy – seen in memory & decoded | | 3 | **T1562.001** | Disable or Modify Tools | Defender was disabled via RunMe.ps1 | | 4 | **T1021.001** | Remote Services: RDP | RDP LogonType 10 used from DMZ and laterally inside | | 5 | **T1110** | Brute Force | Admin account cracked from RM.20 (Event ID 4625, then 4624) | | 6 | **T1133** | External Remote Services | Chris's account used via RDP from Tor IP (171.25.193.25) | | 7 | **T1078** | Valid Accounts | Chris Pike’s credentials reused | | 8 | **T1041** | Exfiltration Over C2 | starfleet\_secrets.txt downloaded by Klingon | | 9 | **T1071** | Application Layer Protocol | File transfer via network share/Samba logs | | 10 | **T1566** | Phishing | DOCX lure from phish@fakeemail.com, opened by Chris | | 11 | **T1556** | Modify Authentication Process | Admin login modified with brute-force success and SYSTEM access | | 12 | **T1053.005** | Scheduled Task or Job | Batch file (AAAAAAAAAAAAAAAA.bat) ran in loop 179+ times | | 13 | **T1070** | Indicator Removal | Event logs cleared, $MFT and $UsnJrnl missing, .Trash deletion | | 14 | **T1012** | Query Registry | Registry artefacts of PowerShell seen in memory strings (Set-MpPreference edits) | | | |  |
| Remediation Advice | | |  |
| 1. **Enable Multi-Factor Authentication (MFA) -** If Multi-Factor Authentication (MFA) had been enabled, this attack could have been stopped right at the beginning. Even though the attacker stole Chris Pike’s password, they would have needed a second step to log in. Chris would have seen a login request he didn’t make and could have reported it. That single alert could have blocked the attacker from ever getting into the STARFLEET network. 2. **Disconnect All Affected Devices Immediately** – This stops the attacker from making further lateral movements or continuing encryption. 3. **Reset All User and Admin Passwords** – Especially Chris Pike, Admin, and any suspicious accounts like Klingon. 4. **Scan for Malware and Scripts** – Search for and remove files like agent.exe and RunMe.ps1. 5. **Limit RDP Access** – Disable RDP if not needed. If required, use network rules to restrict access and monitor use. 6. **Segment the Network Properly** – The Domain Controller should never be accessible from user devices or servers like RM.20. 7. **Run Phishing Awareness Training** – Users should know how to spot fake emails and avoid risky clicks. 8. **Turn On Central Logging** – Use a SIEM system to gather and monitor logs across all devices. 9. **Block Known Bad IPs and Hashes** – Use threat intelligence to stop similar attacks before they start. 10. **Run a Full Forensic Investigation** – Check all impacted systems for hidden malware or other compromised accounts. | | |  |
|  |
|  |
|  |
|  |
|  |
|  |
|  |
|  |
|  |
|  |
|  |
|  |
|  |
|  |
|  |
|  |
|  |
|  |
|  |
|  |
|  |
|  |
|  |
|  |