ELCH Investigative Report

Incident Response Track

Mentor: Faiza Aziz

Team: IR FORCE

Team Members: Nour Mousa & Fatima Nezhadian

Jan 9, 2023

Executive summary

The office went under a ransomware attack which resulted in encryption of all files and file servers. The incident had initially started by a phishing attack. Lateral movement has been detected, and the IR team is suspicious of data exfiltration. The access to files were regained by restoring the most recent backups.
The impact of the attack has a decrease in employees' efficiency due to revoked access to the files. The estimated cost of a data breach per record as of 2022 according to IBM is $164 USD (app. $220 CAD).[i]

What is to be focused on after this attack:

- Keeps files in an encrypted format
- Activate MFA/2FA identification
- Improve the cyber security awareness trainings
- Consider investing on lateral movement prevention and data exfiltration prevention tools.

Actions (analytical findings):

1. Communication:

a. Due to the attack's disruption of day-to-day business processes and system failure that continues to spread laterally, this incident is classified as **high risk**. Which defines the communication plan to proceed for this attack.
b. Based on the communication plan, the initial communication was made with the IT help desk and the IT team manager on-site.
c. The IT manager has notified the head office about the incident to make key stakeholders aware via email, and held an immediate debrief virtual meeting with the CISO and CEO. The IT manager will provide updates every 4 hours to the IT helpdesk and direct them to act accordingly. Status reports will be sent to executive leadership every 12 hours via email. Once the incident has been closed the investigative report will be sent to the CISO and CEO and a meeting will be held to discuss recommendations and lessons learned.

2. Identification and incident verified:

a. The IT help desk and the IR team started to follow the incident response playbook, as the first step the IT help desk acted based on playbook instructions. The business manager was consulted for the business continuity plan.
b. The IR team investigated the attack more precisely and figured out the initial access was gained by using the active directory vulnerability such as CVE-2022-29623 that led to privilege escalation. The NIST Vulnerability Database was used to verify the type of vulnerability and its characteristics.
c. Preceding the initial access lateral movement is a possible incident since the attack is spreading over the company servers. To detect the lateral movement, the actions collected in the Table 1.

d. Survey studies of 2022 cyber attacks report that at least 60% of ransomware attacks include data exfiltration[ii]. The report from user credential logs, the network communication raise suspicion on data exfiltration. The IR team further investigated the network and user activity log to find any file related abnormal activity, and the investigation is continuing.

	Action	Result
1	Analyzed system log associated with windows task scheduler, remote desktop protocol (RDP), and PowerShell	Some abnormal activities were detected in task schedular.
2	Investigated the users' credential users and user activity log via Semperis Directory Service protector	Identified a new user with high privilege and downgrading of an administrator.
3	Investigated the network log	The log showed suspicious communication with an IP address belonging to Russia that was identified a C2 server.

Table 1. Lateral movement detection actions.

3. Containment measures:

a. The firewall rules were added to prevent connection to the Russian server.
b. YARA rules were added to IDS, and corresponding alert rules to the SIEM.
c. The vulnerabilities leading to the initial access and lateral movement were patched.

4. Recovery measures:

a. The most recent file backups were restored to regain access to the files.
b. Also, the workstations were restored from backup image.

Recommendations:

1. Provide training via awareness campaigns for employees on how to identify and report phishing attempts.
2. Activate MFA/2FA for all users, especially privileged accounts.
3. Regularly perform vulnerability scans and patch the system.
4. Store the data on file servers and systems in an encrypted format to prevent data exfiltration.
5. Invest in security data exfiltration prevention and lateral movement prevention tools such as Splunk, Titanium, Extrahop and many other tools.
6. Apply Zero-Trust security to the network to prevent lateral movement.

[i] https://www.ibm.com/reports/data-breach

[ii] https://titaniam.io/state-of-data-exfiltration-and-extortion-2022/