Xây dựng kịch bản giả định trường hợp một máy nhân viên trong mạng doanh nghiệp bị nhiễm virus qua phishing mail, virus này đã lây lan qua máy chủ Domain Controller và có được danh sách user trong mạng. Mô tả các kỹ thuật tấn công theo MITRE ATT@CK.

\* THAM KHẢO:

vd: https://www.sygnia.co/blog/luna-moth-false-subscription-scams/

https://phishingquiz.withgoogle.com/

https://www.dfs.ny.gov/Twitter\_Report

https://www.phishing.org/

https://www.phishing.org/phishing-techniques

https://www.cyberproof.com/blog/double-bounced-attacks-with-email-spoofing-2022-trends

https://blog.knowbe4.com/report-phishing-remains-the-most-prevalent-cyber-threat

https://www.upwind.io/feed/how-adversaries-use-telegram-to-evade-detection

\* SƠ LƯỢC:

- Giải thích cơ bản:

+ Social engineering là một kỹ thuật thao túng nhằm khai thác rủi ro con người để lấy được thông tin có giá trị.

+ Phishing is the use of digital communications to trick people into revealing sensitive data or deploying malicious software. It is one of the most common forms of social engineering, typically performed via email.

+ Phishing mail: là emails chứa các tệp đính kèm hoặc link độc hại, được gửi qua các nền tảng xã hội. Là một dạng của kỹ thuật social engineering.

+ Spear phishing is a subset of email phishing in which specific people are purposefully targeted, such as the accountants of a small business.

+ Angler phishing is a technique where attackers impersonate customer service representatives on social media. This tactic evolved from people’s tendency to complain about businesses online.

+ Mục tiêu của Phishing mail: dựa trên các thông tin trong mail, làm victim tin tưởng mail an toàn vì có trusted sender, nội dung hợp lí, tên miền tin cậy. Sau đó victim sẽ tải hoặc truy cập link độc hại và tải về virus.

- Mô hình mạng:

+ 1 Máy kali: attacker

+ 1 Máy Windows server 2022: victim

+ 2 Máy client thuộc AD DC win 10: victim

- Kịch bản đề xuất:

+ Khiến victim bấm vào link

- Thực hiện:

+ Tạo web giả mạo gồm 2 stage: stage 1 tạo web uy tín khiến nạn nhân đăng nhập lấy thông tin/ stage 2 yêu cầu nạn nhân download phần mềm (tải tự động hoặc thủ công)

+ Tạo trojan, malware hoặc Link Manipulation để khai thác.

+ Tạo mail đến victim.

+ Victim bấm vào link.

+ Máy 1 bị nhiễm độc.

+ Sử dụng lateral movement đến Máy 2 và Domain Controller

+ Trích xuất thông tin từ Domain Controller.

+ Trả thông tin về máy attacker.

- MITRE ATTACK:

+ Reconnaissance: T1598.003 - Spearphishing Link

+ Initial Access: T1566.002 - Spearphishing Link

+ Execution: T1204.002 - Malicious File | T1059 - Command and Scripting Interpreter

+ Persistence: T1547 - Boot or Logon Autostart Execution

+ Credential Access: T1003 - OS Credential Dumping

+ Discovery: T1087.001/.002 - Account Discovery

+ Lateral Movement: T1021 - Remote Services

+ Collection:T1071.001 - Web Protocols

+ Command and Control: T1071.001 - Application Layer Protocol/Web protocols (bot telegram)

T1102.002 - Web Service/Bidirectional Communication