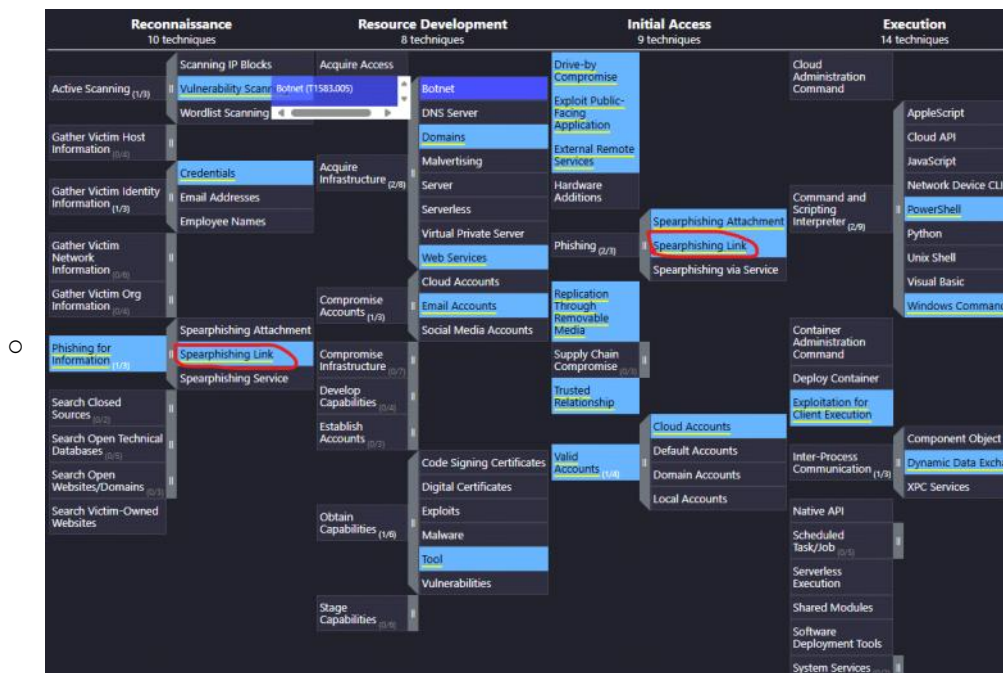


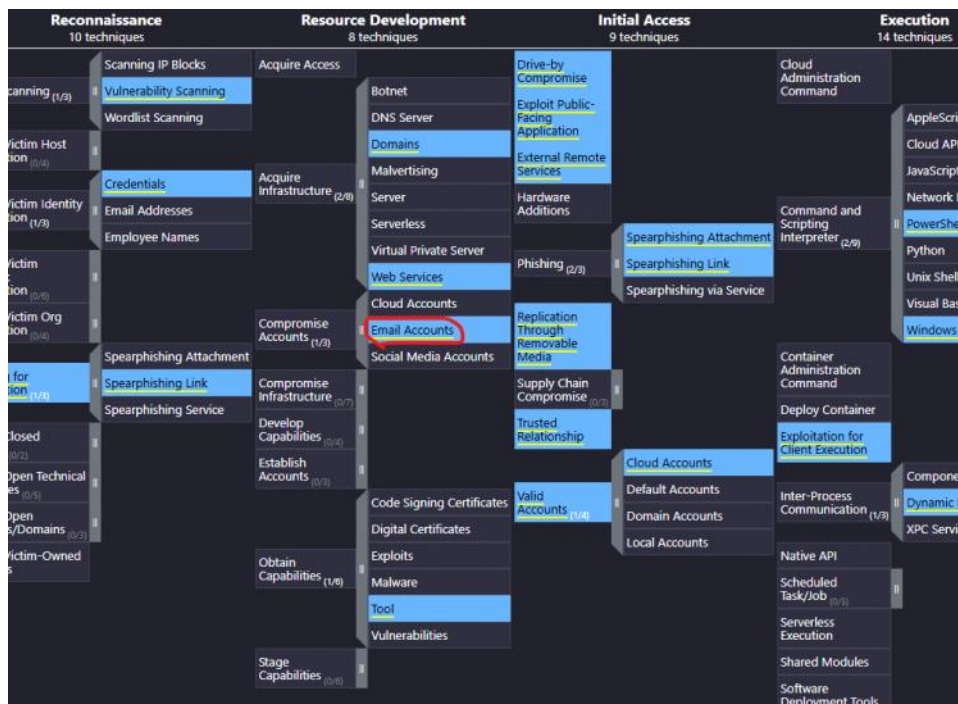
Eviction

quinta-feira, 23 de outubro de 2025 06:04

- Propósito do desafio:
 - O desafio trata-se basicamente de identificar, por meio de um ATT&CK Navigator modelado, táticas e técnicas do GRUPO APT 28.
- Task 1:
 - O enunciado queria saber qual subtécnica usada pelo grupo APT foi utilizada para fazer reconhecimento e acesso inicial



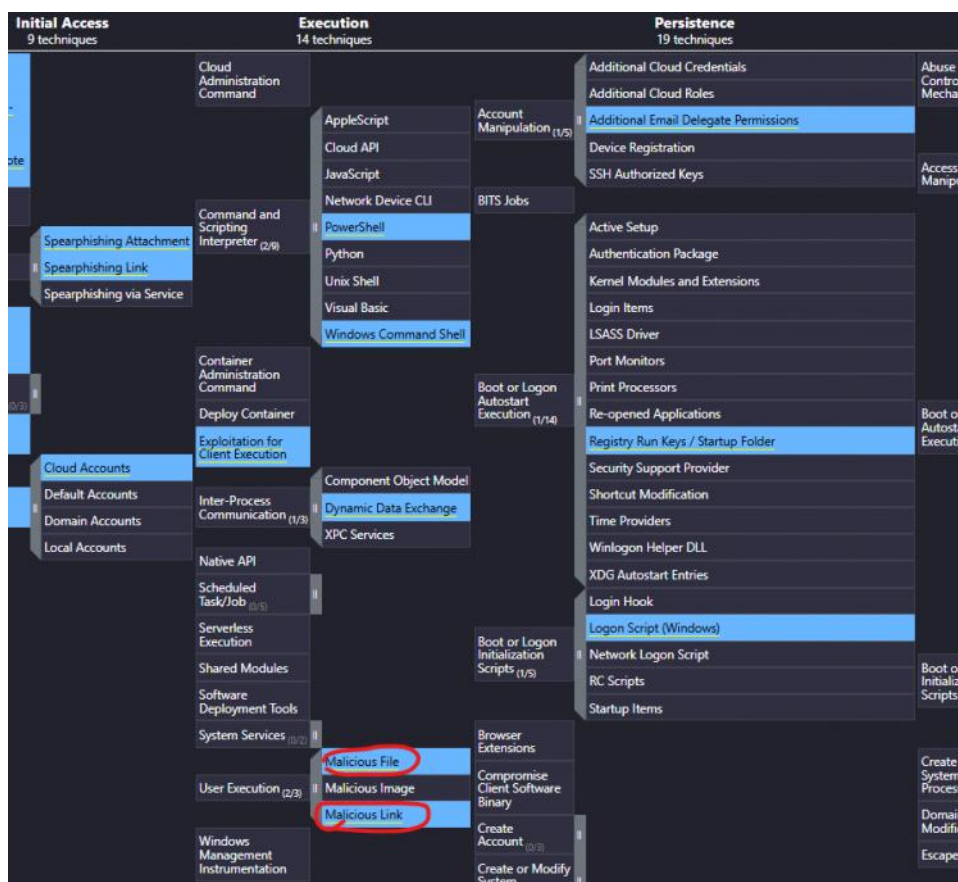
- Analisando, vemos que tanto na tática reconhecimento quanto acesso inicial, é a subtécnica Spearphishing Link - Ataque cibernético no qual o atacante finge ser uma entidade confiável para manipular.
- Task 2:
 - O enunciado relatou que o APT avançou da tática reconhecimento para desenvolvimento de recursos, gostaria de saber quais tipos de contas pode-se comprometer com esse desenvolvimento.



- Analisado os recursos desenvolvidos, nota-se que as contas de e-mails são as que podem comprometer.

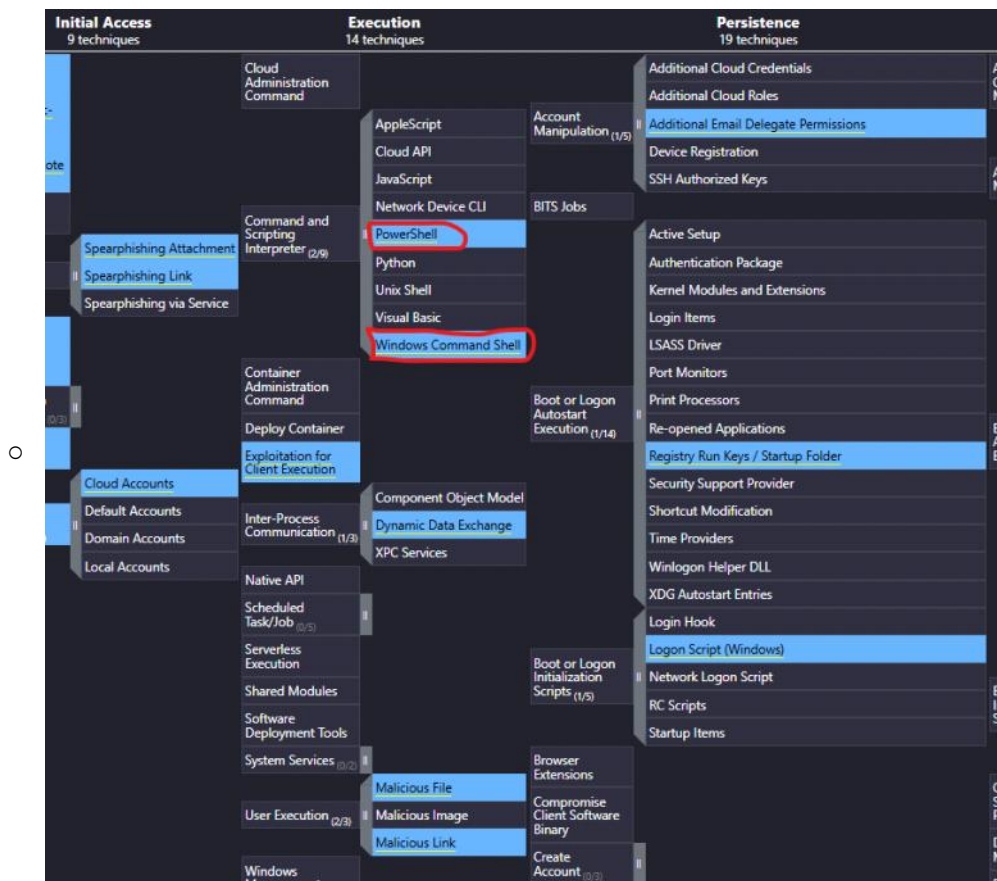
• Task 3:

- O enunciado relatou que o APT conseguiu acesso inicial por meio de engenharia social, gostaria de saber se teve sucesso na tática execução.



- Analisando a técnica de execução de usuários, vemos que por meio das subtécnicas arquivo malicioso e link malicioso, houve sucesso na execução por meio de engenharia social.

- Task 4:
 - O enunciado quer saber, quais foram os interpretadores de scripts que deram a execução bem sucedida das subtécnicas da questão anterior.



- Analisando a técnica de comando e interpretador de scripts, vimos que o Powershell e o Shell de comando windows(CMD) foram responsáveis para a execução dos arquivos da questão anterior.
- Task 5:
 - O enunciado quer saber, se em caso de alteração de registros com foco em persistência, quais chaves de registro deve-se observar.

| Execution 14 techniques | | Persistence 19 techniques | | Privilege Escalation 13 techniques | |
|---|--|--|--|--|---|
| AppleScript Cloud API JavaScript Network Device CLI PowerShell Python Unix Shell Visual Basic Windows Command Shell | Account Manipulation (1/5) | Additional Cloud Credentials Additional Cloud Roles Additional Email Delegate Permissions Device Registration SSH Authorized Keys | Abuse Elevation Control Mechanism (2/4) | Create Process with Token Manipulation (1/5) | Parent PID Spoofing SID-History Injection Token Impersonation/T... |
| | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |
| Component Object Model Dynamic Data Exchange XPC Services | BITS Jobs | Active Setup Authentication Package Kernel Modules and Extensions Login Items LSASS Driver Port Monitors Print Processors Re-opened Applications Registry Run Keys / Startup Folder Security Support Provider Shortcut Modification Time Providers Winlogon Helper DLL XDG Autostart Entries Login Hook Logon Script (Windows) Network Logon Script RC Scripts Startup Items | Access Token Manipulation (1/5) | Boot or Logon Autostart Execution (1/14) | Active Setup Authentication Package Kernel Modules and Extensions Login Items LSASS Driver Port Monitors Print Processors Re-opened Applications Registry Run Keys / Startup Items Security Support Provider Shortcut Modification Time Providers Winlogon Helper DLL XDG Autostart Entries Login Hook Logon Script (Windows) Network Logon Script RC Scripts Startup Items |
| | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |
| Malicious File Malicious Image Malicious Link | Boot or Logon Autostart Execution (1/14) | Boot or Logon Initialization Scripts (1/5) | Boot or Logon Initialization Scripts (1/5) | Create or Modify System Process (2/4) | Domain Policy Modification (2/2) |
| | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |

- O registro que lida com as chaves de inicialização do sistema, é o que deve ser observado em caso de alteração.

- Task 6:
 - O enunciado relatou que o APT executa binários para evadir defesas, quer saber qual é.

| | |
|--------------------------------------|--------------------|
| System Binary Proxy Execution (1/13) | CMSTP |
| | Compiled HTML File |
| | Control Panel |
| | InstallUtil |
| | Mavinject |
| | MMC |
| | Mshta |
| | Msixexec |
| | Odbcconf |
| | Regsvcs/Regasm |
| | Regsvr32 |
| | Rundll32 |
| | Verclsid |

- No navigator modelado, exige que é o Rundll32.

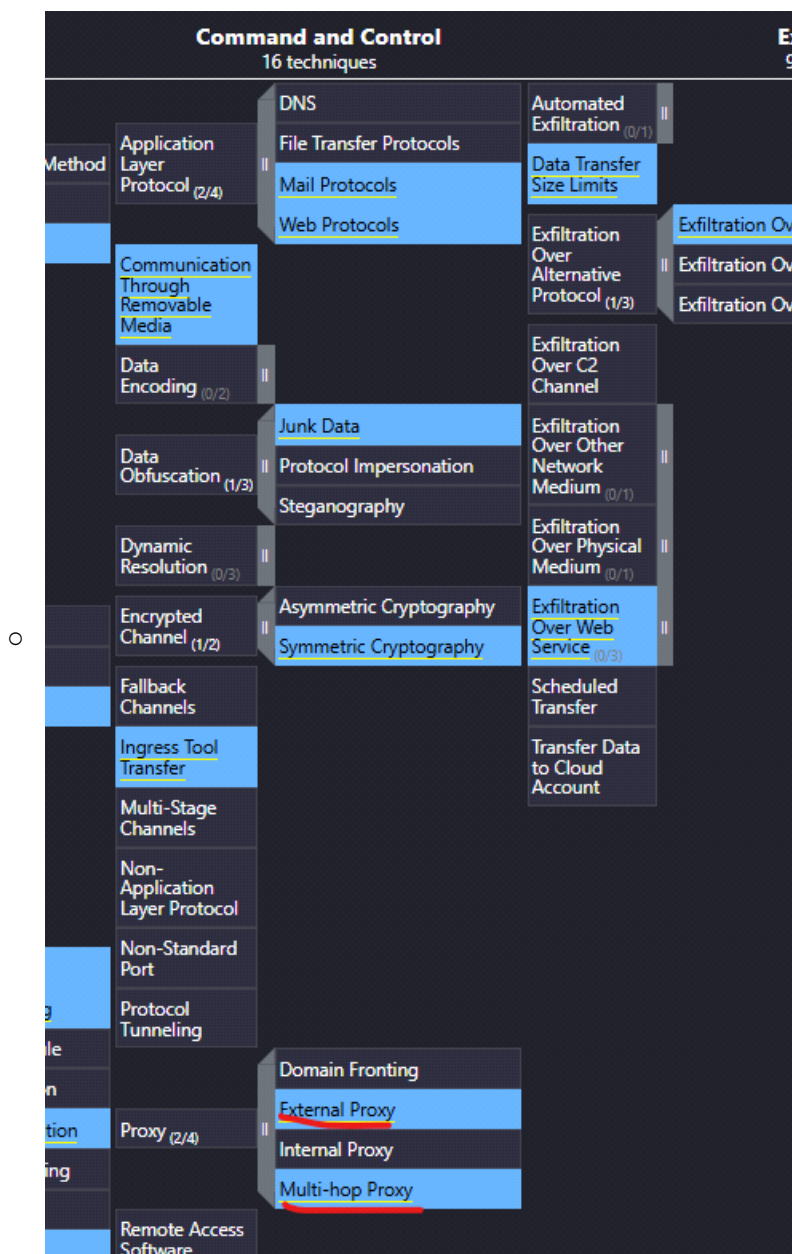
- Task 7:
 - O enunciado relatou que houve tcpdump - ferramenta de linha de comando para captura e análise de pacotes de rede e outras utilidades, em um dos hosts comprometidos, quer saber para o que foi utilizada essa ferramenta.

| Credential Access 17 techniques | | | Discovery 31 techniques | | |
|--|----|-----------------------------|----------------------------------|----|--|
| Adversary-in-the-Middle (0/3) | II | | Account Discovery (0/4) | II | |
| | | Credential Stuffing | Application Window Discovery | | |
| Brute Force (2/4) | II | Password Cracking | Browser Information Discovery | | |
| | | Password Guessing | Cloud Infrastructure Discovery | | |
| | | Password Spraying | Cloud Service Dashboard | | |
| Credentials from Password Stores (0/5) | II | | Cloud Service Discovery | | |
| Exploitation for Credential Access | | | Cloud Storage Object Discovery | | |
| Forced Authentication | | | Container and Resource Discovery | | |
| Forge Web Credentials (0/2) | II | | Debugger Evasion | | |
| | | Credential API Hooking | Device Driver Discovery | | |
| Input Capture (1/4) | II | GUI Input Capture | Domain Trust Discovery | | |
| | | Keylogging | File and Directory Discovery | | |
| | | Web Portal Capture | Group Policy Discovery | | |
| Modify Authentication Process (0/8) | II | | Network Service Discovery | | |
| Multi-Factor Authentication Interception | | | Network Share Discovery | | |
| Multi-Factor Authentication Request Generation | | | Network Sniffing | | |
| Network Sniffing | | | Password Policy Discovery | | |
| | | /etc/passwd and /etc/shadow | Peripheral Device Discovery | | |

- Foi identificado que a ferramenta tcpdump foi utilizada para fazer Network Sniffing, ou seja, capturar e analisar pacotes de rede.
- Task 8:
 - O enunciado relatou que o principal objetivo do APT era roubar propriedade intelectual dos repositórios de informação do alvo, quer saber qual repositório seria.

| Collection 17 techniques | | Comm |
|--|---------------------------|---------------------------------------|
| Adversary-in-the-Middle (0/3) | II | |
| Archive Collected Data (1/3) | II | Application Layer Protocol (2/4) |
| | Archive via Custom Method | |
| | Archive via Library | |
| | Archive via Utility | |
| Audio Capture | | Communication Through Removable Media |
| Automated Collection | | |
| Browser Session Hijacking | | Data Encoding (0/2) |
| Clipboard Data | | |
| Data from Cloud Storage | | Data Obfuscation (1/3) |
| Data from Configuration Repository (0/2) | II | Dynamic Resolution (0/3) |
| Data from Information Repositories (1/3) | II | Encrypted Channel (1/2) |
| | Code Repositories | |
| | Confluence | Fallback Channels |
| | Sharepoint | |
| Data from Local System | | Ingress Tool Transfer |
| Data from Network Shared Drive | | Multi-Stage Channels |
| Data from Removable Media | | Non-Application Layer Protocol |
| Data Staged (2/2) | II | Non-Standard Port |
| | Local Data Staging | |
| | Remote Data Staging | Protocol Tunneling |
| Email Collection (1/3) | II | |
| | Email Forwarding Rule | |
| | Local Email Collection | |
| | Remote Email Collection | Proxy (2/4) |
| | Credential API Hooking | |
| Input Capture (1/4) | II | Remote Access Software |
| | GUI Input Capture | |
| | Keylogging | |

- Na tática de coleção, vemos que para coletar dados de repositórios, foi utilizado o software Sharepoint.
- Task 9:
 - O enunciado relatou que embora o APT tivesse coletado os dados, ele não conseguiu se conectar ao C2 para exfiltrar dados, quer saber quais tipos de proxy o APT poderia usar para tal.



- Com esses dois tipos de proxy, o atacante poderia estabelecer comunicação com o servidor C2 e exfiltrar seus dados.