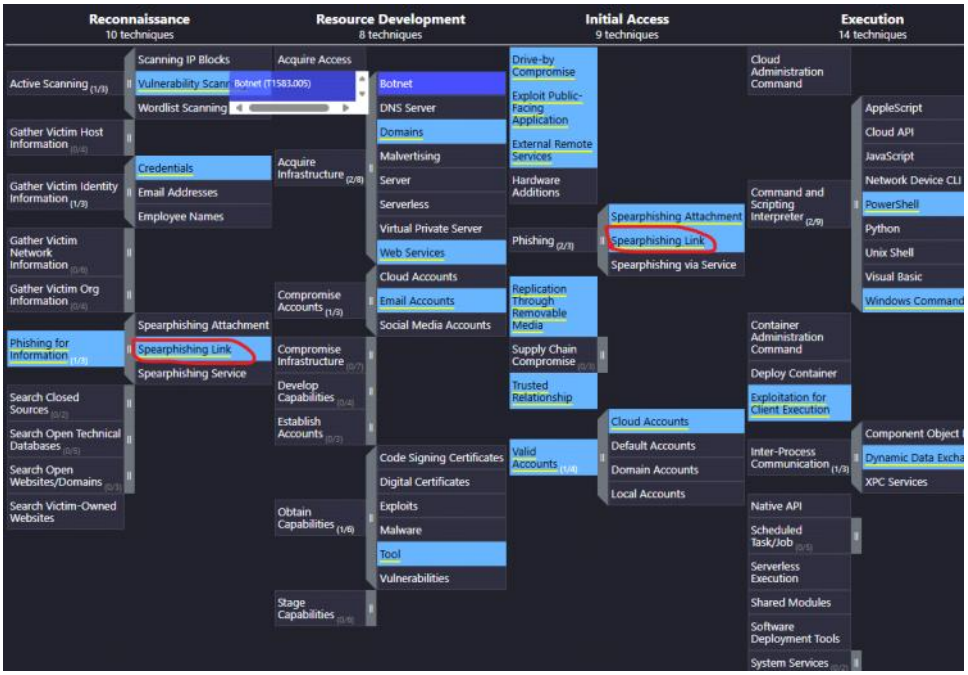
Eviction

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

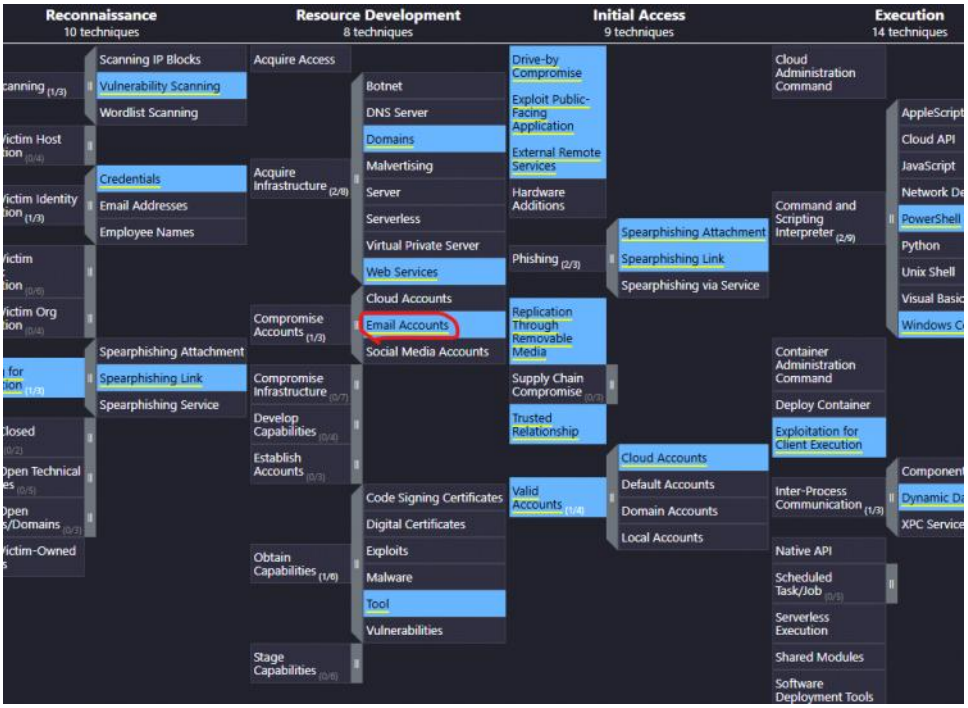
- Propósito do desafio:
  - O desafio trata-se basicamente de identificar, por meio de um ATT&CK Navigator modelado, táticas e técnicas do GRUPO APT 28.

- Task 1:
  - O enunciado queria saber qual subtécnica usada pelo grupo APT foi utilizada para fazer reconhecimento e acesso inicial



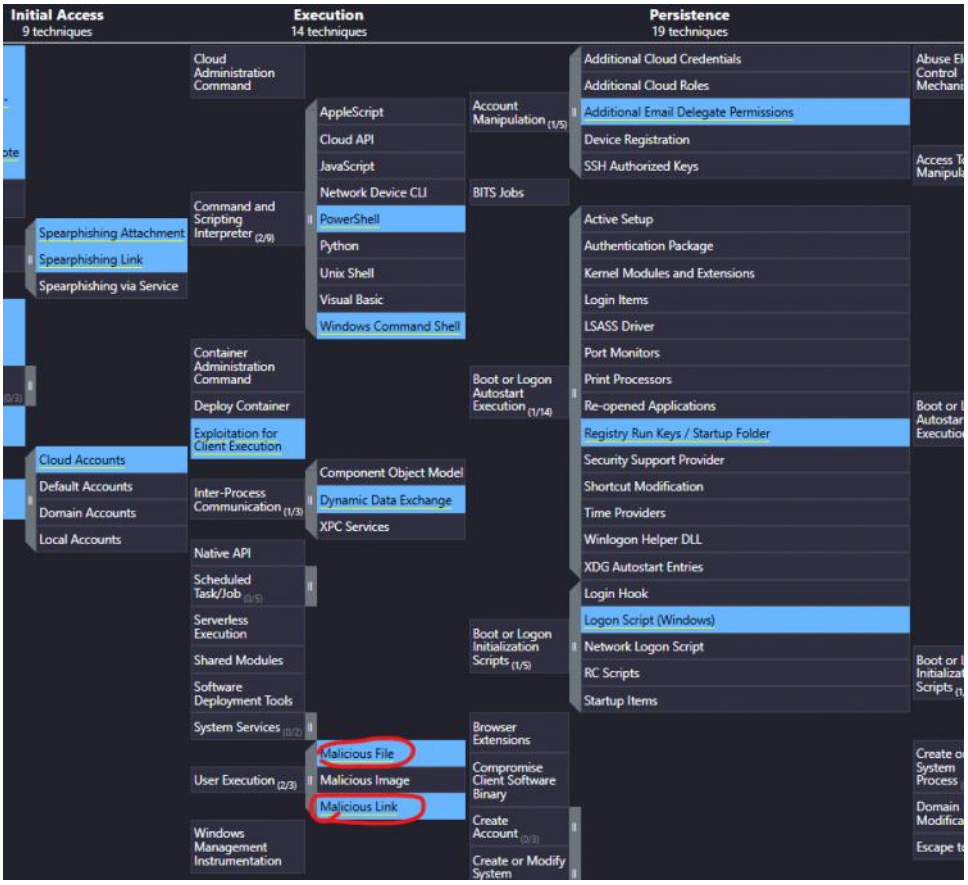
  - Analisando, vemos que tanto na tática reconhecimento quanto acesso inicial, é a subtécnica Spearphishing Link - Ataque cibernético no qual o atacante finge ser uma entidade confiável para manipular.

- 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.

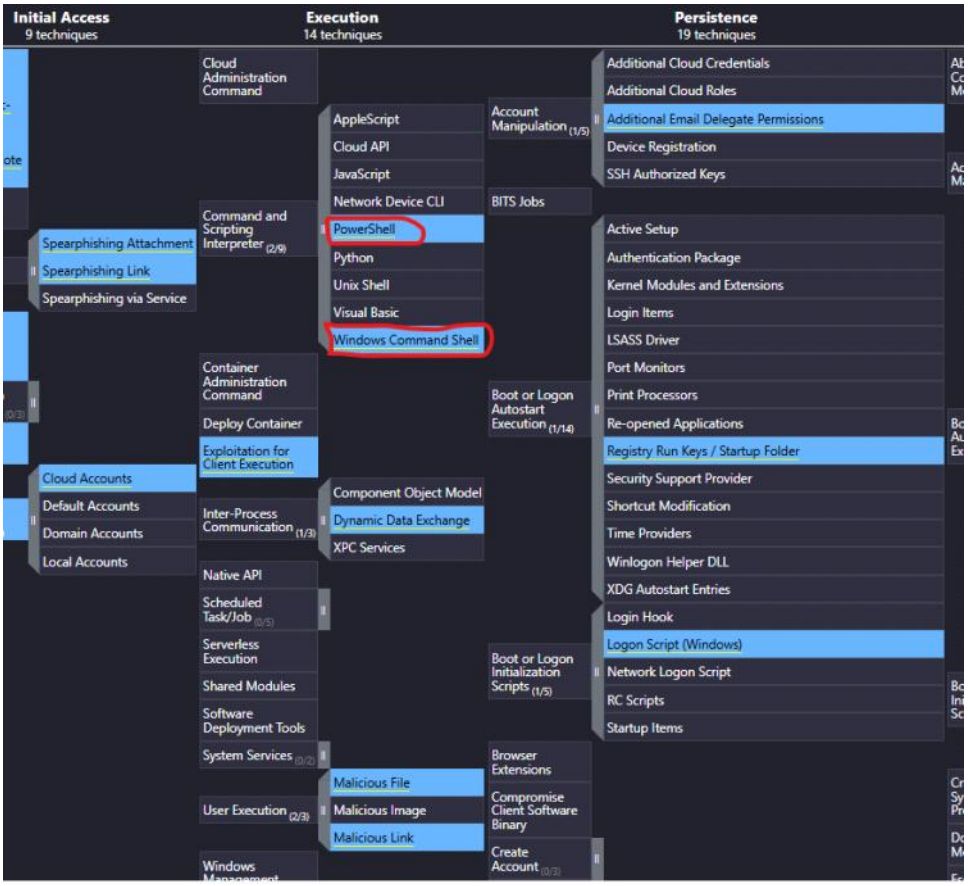


- Analisado os recursos desenvolvidos, nota-se que as contas de e-mails são as que podem comprometer.

- 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.

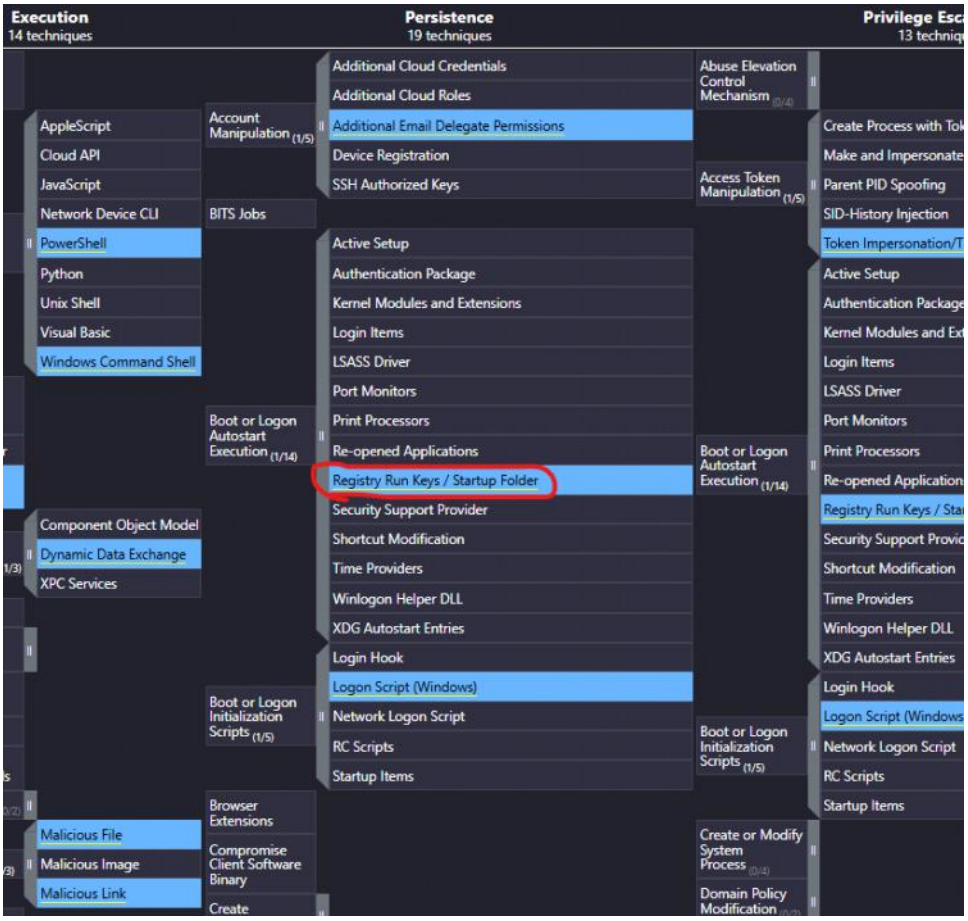


- Analisando a técnica de execução de usuários, vemos que por meio das subtécnicas arquivo malicioso e link malicioso, houve sucesso na execução por meio de engenharia social.

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

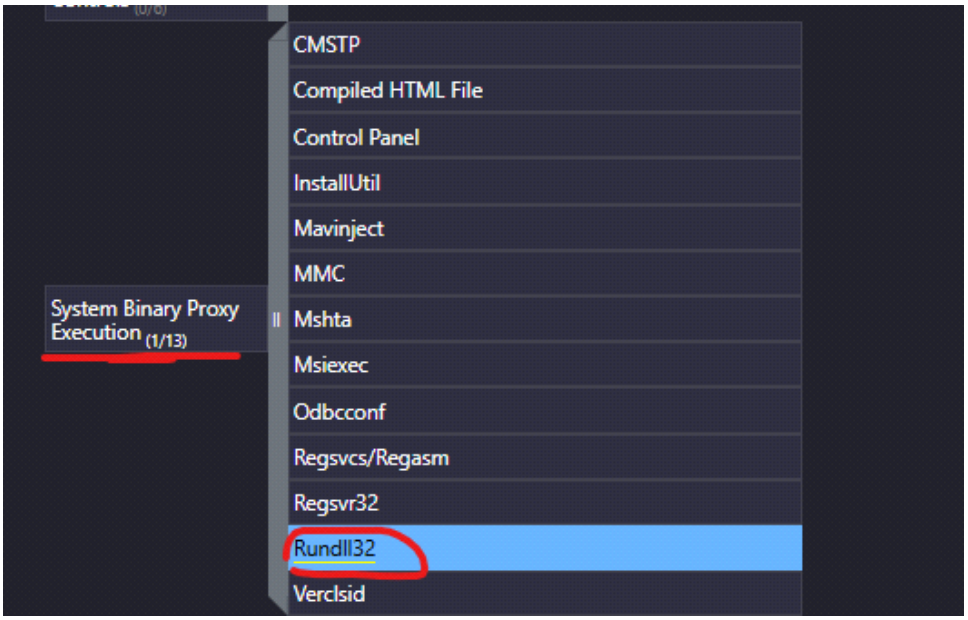
  - Analisando a técnica de comando e interpretador de scripts, vimos que o Powershell e o Shell de comando windows(CMD) foram responsáveis para a execução dos arquivos da questão anterior.

- Task 5:
  - O enunciado quer saber, se em caso de alteração de registros com foco em persistência, quais chaves de registro deve-se observar.



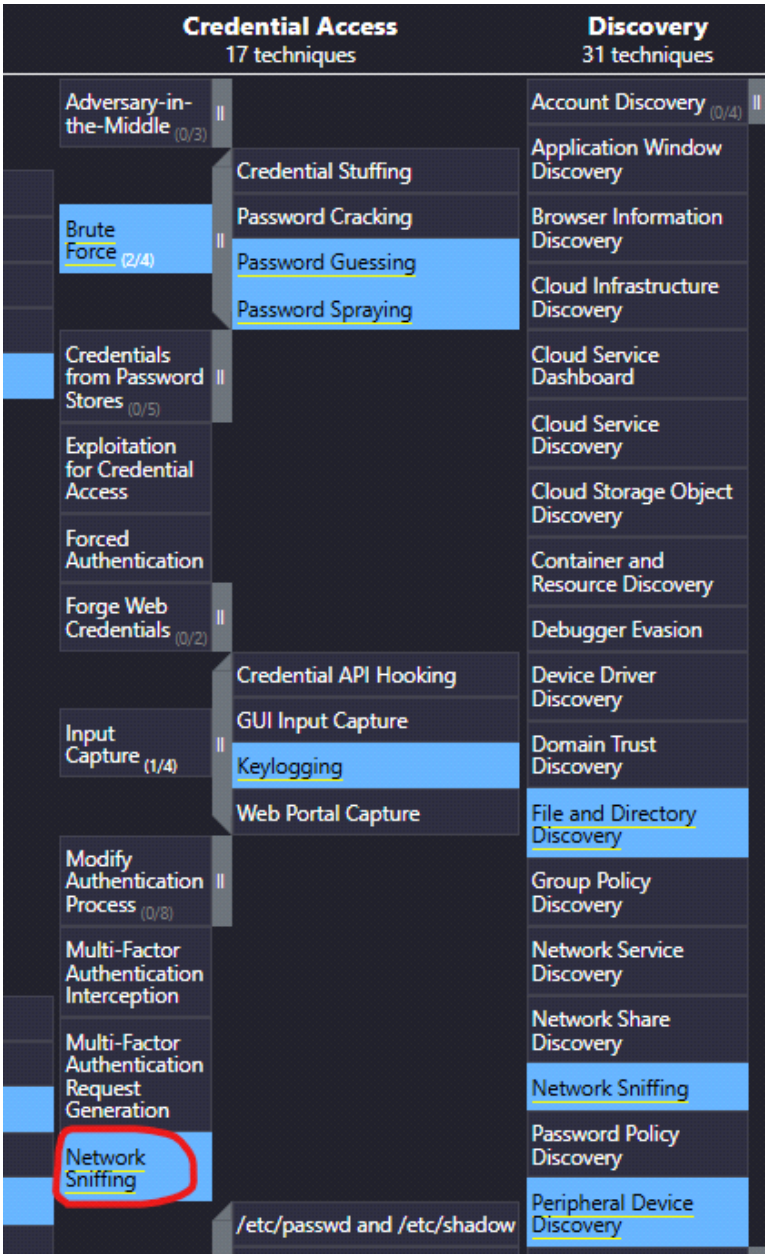
- O registro que lida com as chaves de inicialização do sistema, é o que deve ser observado em caso de alteração.

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



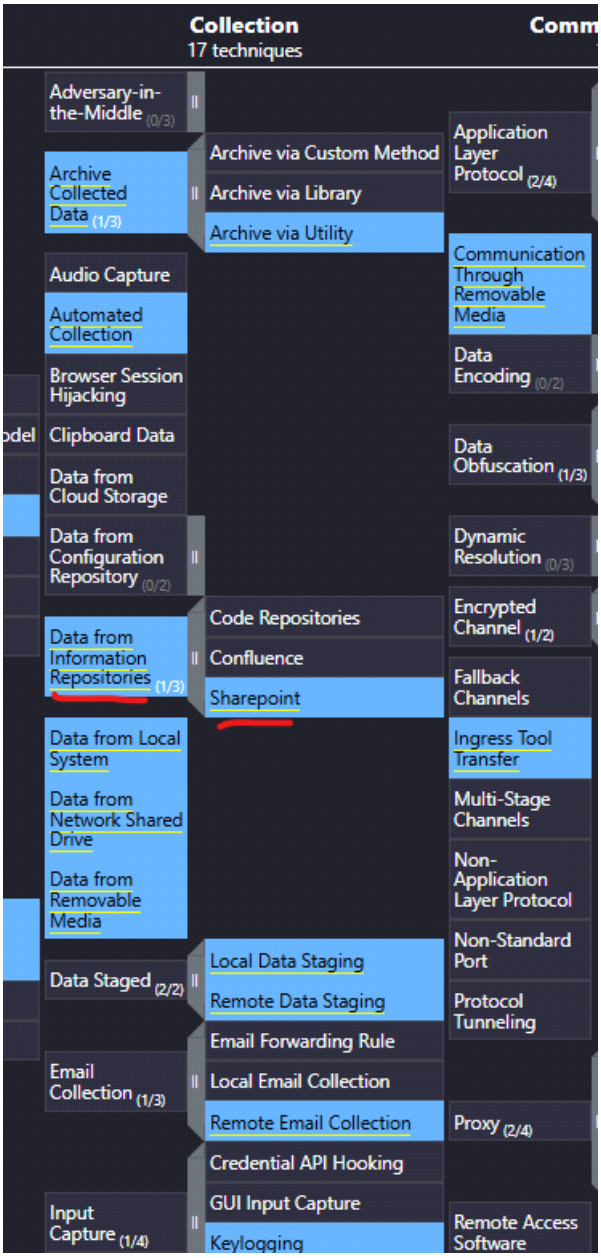
  - No navigator modelado, exibe que é o Rundll32.

- 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.



- 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.



- 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.

- Aprendizados desse desafio:
  - O mitre att&ck navigator consegue ser bem completo na questão de construir toda uma história relacionada a um evento cibernético, recomendável usar mais vezes para análise de casos.