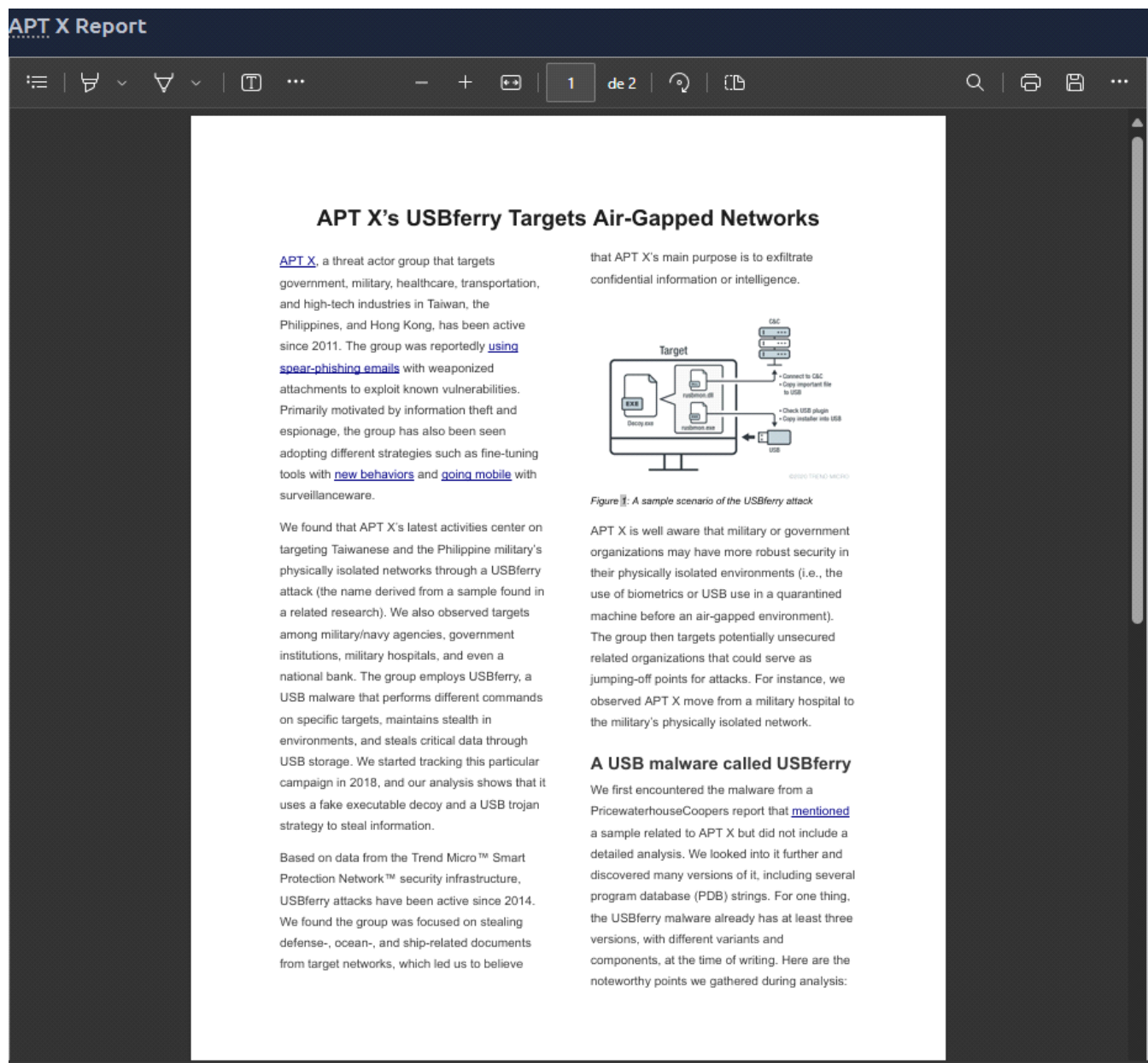


- Propósito do desafio:
 - O desafio consiste em responder um conjunto de perguntas referente ao APT e seu software malicioso analisado por meio das CTIs mitre att&ck - framework de técnicas e táticas de adversários e o openCTI - plataforma de código aberto utilizada para gerenciar CTI.
 - Além do uso dessas CTIs, o desafio disponibilizou um relatório em pdf sobre o APT e seu software malicioso.

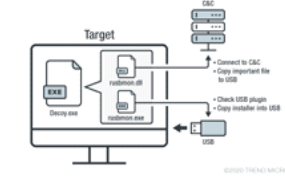


- Task 1:
 - A primeira questão estava querendo saber qual o tipo de campanha que fazia parte do TTP desse grupo.
 - Analisando o pdf fornecido, conseguimos a resposta que queremos.

APT X's USBferry Targets Air-Gapped Networks

APT X, a threat actor group that targets government, military, healthcare, transportation, and high-tech industries in Taiwan, the Philippines, and Hong Kong, has been active since 2011. The group was reportedly using spear-phishing emails with weaponized attachments to exploit known vulnerabilities. Primarily motivated by information theft and espionage, the group has also been seen adopting different strategies such as fine-tuning tools with new behaviors and going mobile with surveillanceware.

that APT X's main purpose is to exfiltrate confidential information or intelligence.



Task 2:

- A segunda questão queria saber o nome do malware usado por esse APT, facilmente conseguimos encontrar essa informação apenas olhando para o título do relatório disponibilizado.

APT X's USBferry Targets Air-Gapped Networks

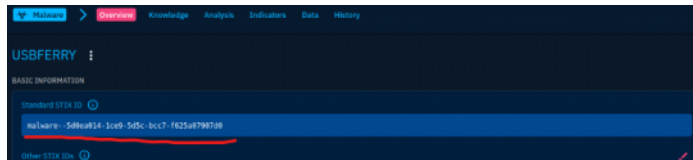
APT X, a threat actor group that targets government, military, healthcare, transportation, and high-tech industries in Taiwan, the Philippines, and Hong Kong, has been active since 2011. The group was reportedly using

that APT X's main purpose is to exfiltrate confidential information or intelligence.



Task 3:

- A terceira questão queria saber o ID STIX - linguagem padronizada para compartilhar informações de inteligência entre as organizações, do malware analisado, essa informação conseguimos extrair pesquisando sobre o malware no openCTI.



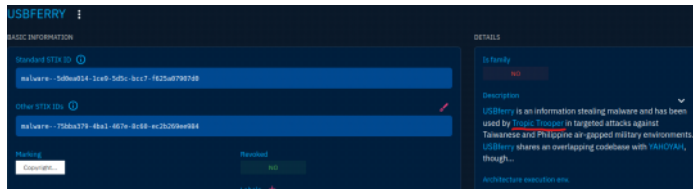
Task 4:

- A quarta questão queria saber a técnica utilizada pelo APT para acesso inicial, isso descobrimos analisando o navegador do mitre att&ck referente a esse grupo.



Task 5:

- A quinta questão queria saber o nome da organização por trás desse APT, essa informação conseguimos extrair nos detalhes do malware constados no openCTI.



Task 6:

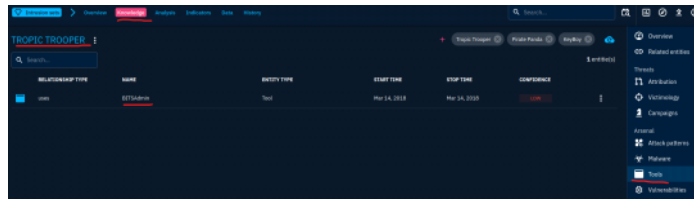
- A sexta questão queria saber quantos padrões de ataques estão relacionados ao grupo, para isso, basta pesquisarmos sobre o grupo no openCTI usando o nome que descobrimos na tarefa passada e ir até a aba de conhecimento de ameaças.



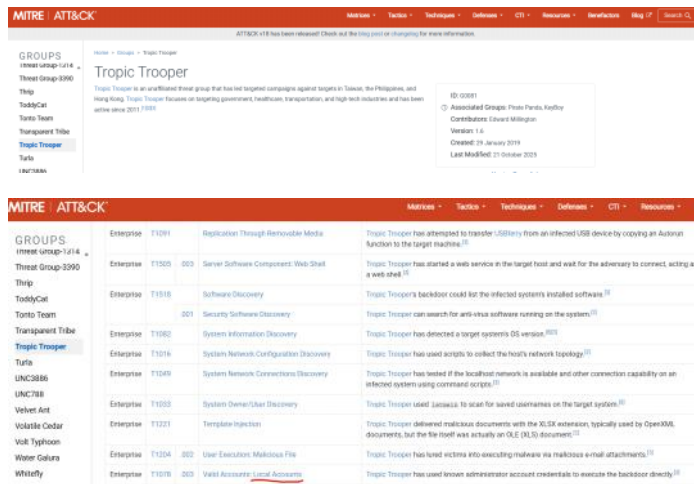
Task 7:

- A sétima questão queria saber o nome ferramenta que é comum esse grupo utilizar para

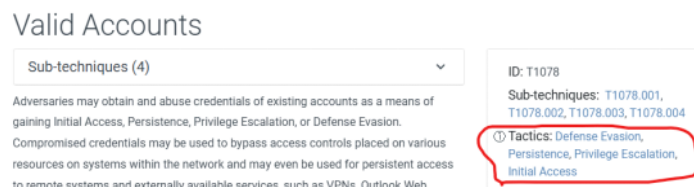
baixar, executar e persistir arquivos maliciosos de forma discreta, essa informação conseguimos adquirir indo até a seção de conhecimento de ameaça e depois na aba ferramentas.



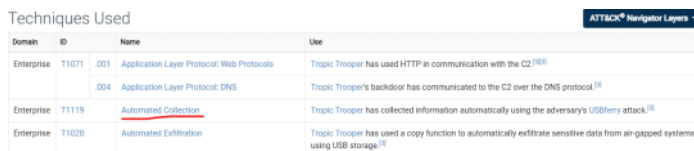
- Task 8:
 - A oitava questão queria saber a subtecnica da técnica Contas Validas utilizada pelo APT, essa informação conseguimos pesquisando sobre o APT no mitre att&ck, na categoria de técnicas utilizadas.



- Task 9:
 - A nona questão queria saber sob quais táticas estão relacionadas a técnica de Valid Accounts, isso descobrimos facilmente acessando a página da informação dessa técnica no mitre att&ck.



- Task 10:
 - A décima questão queria saber qual a tática que o grupo APT utiliza para fazer a etapa de Collection, isso conseguiremos descobrir voltando na página do nome do grupo APT no mitre att&ck e olhando a técnica relacionada a Collection.



- Aprendizados desse desafio:
 - Acabou sendo um desafio simples e acessível, serviu apenas para reforçar a importância de utilizar as CTIs para buscar inteligência sobre ameaças, quanto mais utilizar e mais refinado a maneira de usar, melhor e mais rápido conseguiremos os resultados desejados.