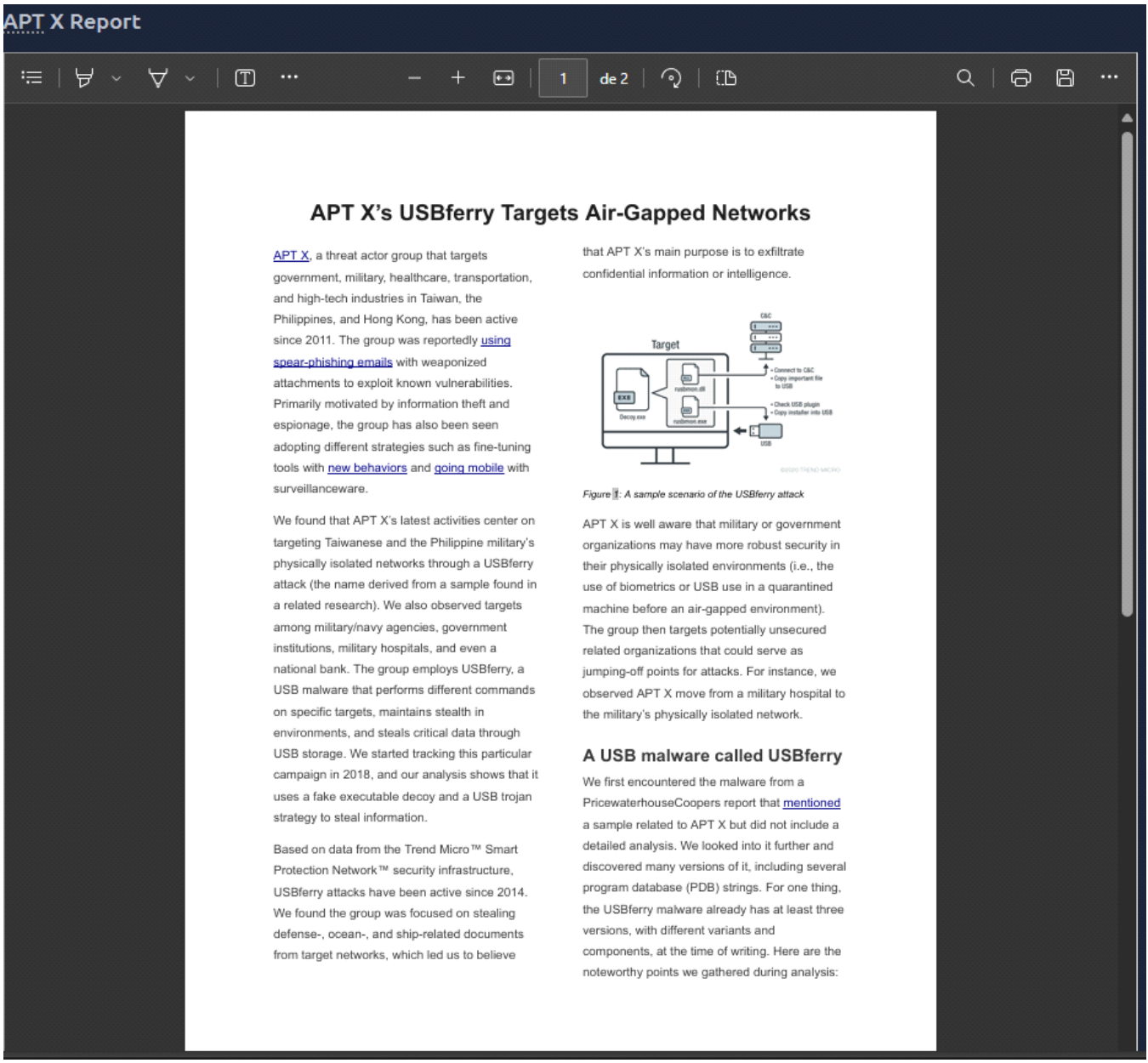
Trooper

sexta-feira, 31 de outubro de 2025 05:30

- 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.

  - 

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.

We found that APT X's latest activities center on targeting Taiwanese and the Philippine military's physically isolated networks through a USBferry attack (the name derived from a sample found in a related research). We also observed targets among military/navy agencies, government institutions, military hospitals, and even a national bank. The group employs USBferry, a USB malware that performs different commands on specific targets, maintains stealth in environments, and steals critical data through USB storage. We started tracking this particular campaign in 2018, and our analysis shows that it uses a fake executable decoy and a USB trojan strategy to steal information.

Based on data from the Trend Micro™ Smart Protection Network™ security infrastructure, USBferry attacks have been active since 2014. We found the group was focused on stealing defense-, ocean-, and ship-related documents from target networks, which led us to believe that APT X's main purpose is to exfiltrate confidential information or intelligence.

Figure 1. A sample scenario of the USBferry attack

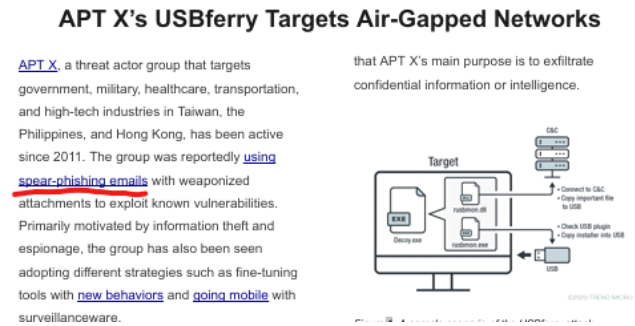
APT X is well aware that military or government organizations may have more robust security in their physically isolated environments (i.e., the use of biometrics or USB use in a quarantined machine before an air-gapped environment). The group then targets potentially unsecured related organizations that could serve as jumping-off points for attacks. For instance, we observed APT X move from a military hospital to the military's physically isolated network.

A USB malware called USBferry

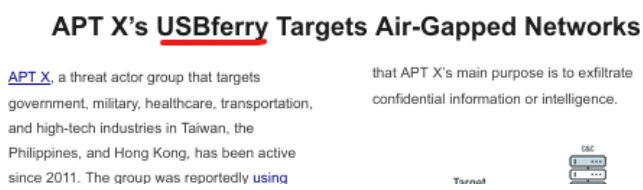
We first encountered the malware from a PricewaterhouseCoopers report that mentioned a sample related to APT X but did not include a detailed analysis. We looked into it further and discovered many versions of it, including several program database (PDB) strings. For one thing, the USBferry malware already has at least three versions, with different variants and components, at the time of writing. Here are the noteworthy points we gathered during analysis:

- Task 1:
  - A primeira questão estava querendo saber qual o tipo de campanha que fazia parte do TTP desse grupo.

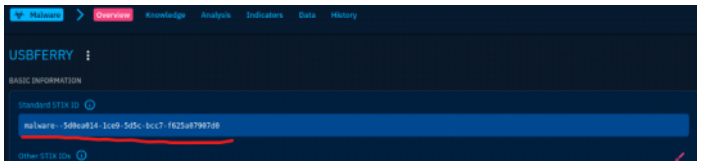
  - Analisando o pdf fornecido, conseguimos a resposta que queremos.



- 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.

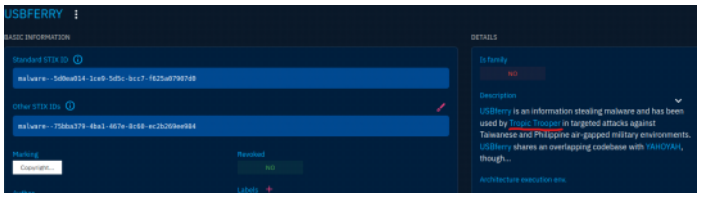


- Task 3:
  - A terceira questão queria saber o ID STIX - linguagem padronizada para compartilhar informações de inteligência entre as organizações, do malware analisado, essa informação conseguimos extrair pesquisando sobre o malware no openCTI.

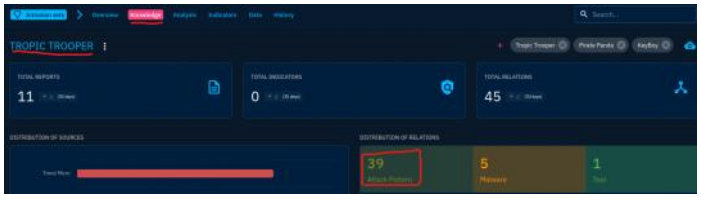


- Task 4:
  - A quarta questão queria saber a técnica utilizada pelo APT para acesso inicial, isso descobrimos analisando o navigator do mitre att&ck referente a esse grupo.

- 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.

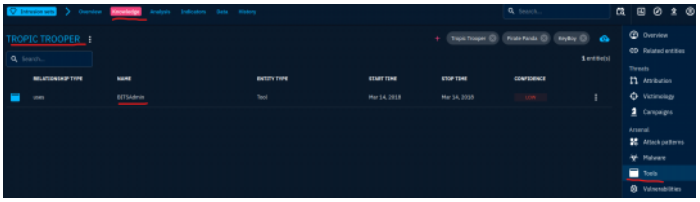


- Task 6:
  - A sexta questão queria saber quantos padrões de ataques estão relacionados ao grupo, para isso, basta pesquisarmos sobre o grupo no openCTI usando o nome que descobrimos na tarefa passada e ir até a aba de conhecimento de ameaças.



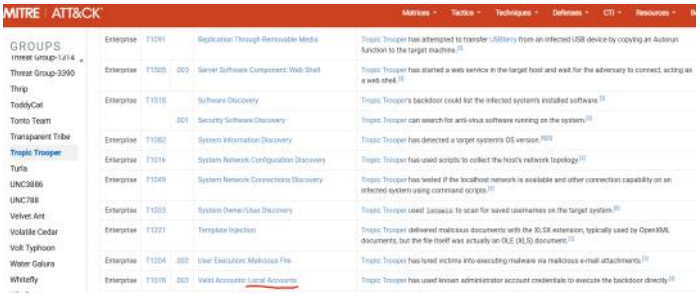
- Task 7:
  - A sétima questão queria saber o nome ferramenta que é comum esse grupo utilizar para

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.

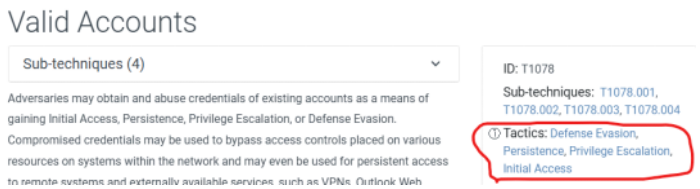
- 

- 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.

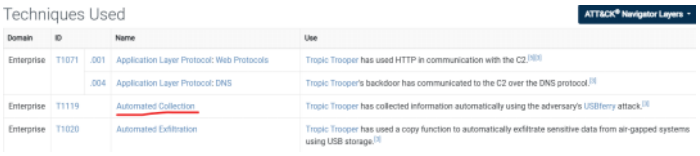
- 

- 

- 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.