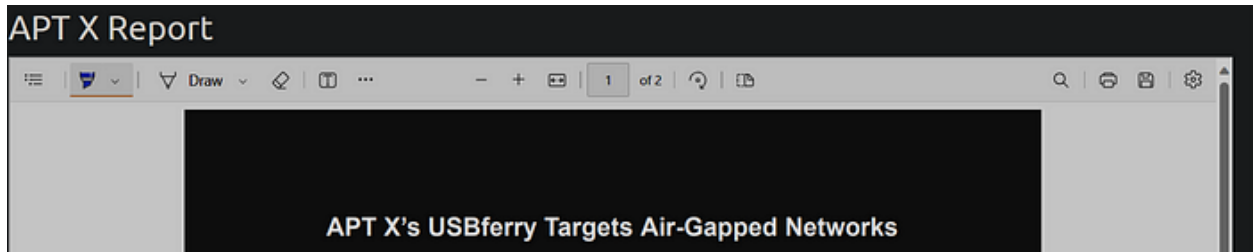
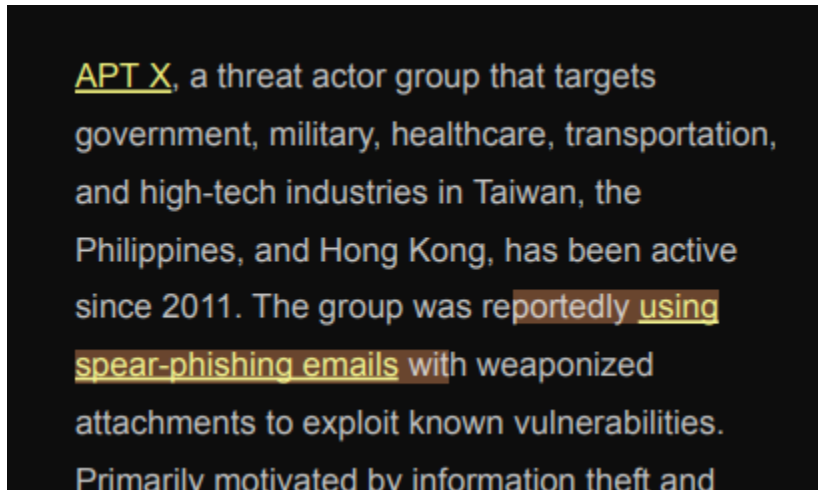


## TROOPER

**Q:** What kind of phishing campaign does APT X use as part of their TTPs?

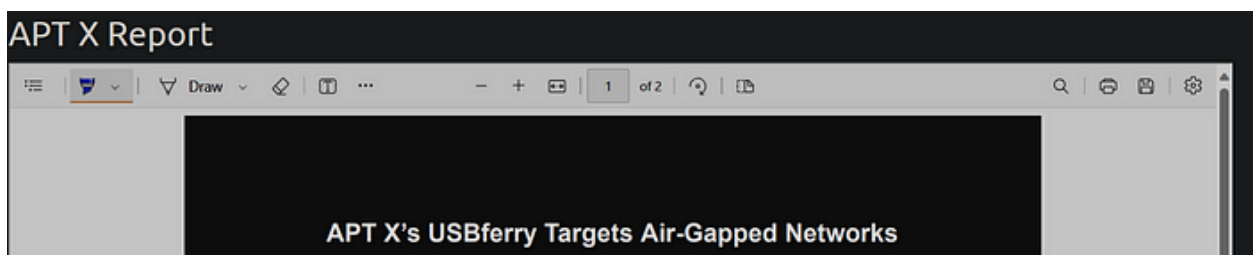


This answer is clearly mentioned in the report, so a quick review should give us what we need.



**A:** spear-phishing emails

**Q:** What is the name of the malware used by APT X?



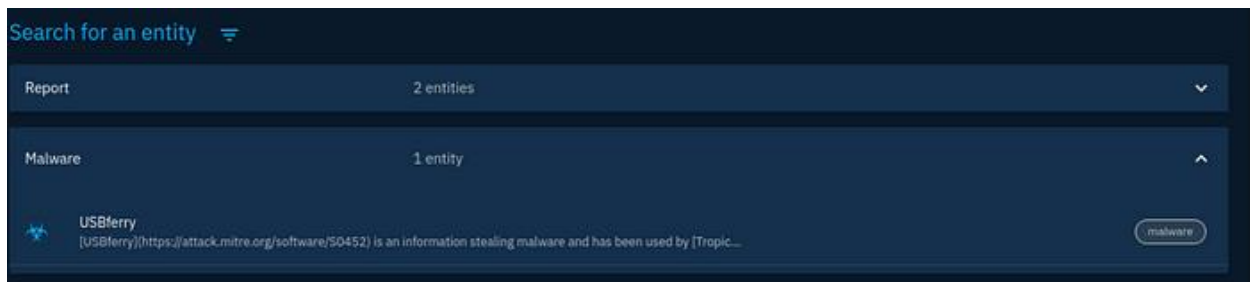
This is also straightforward and present within the report, just need to skim through it **carefully**.

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/agency/government

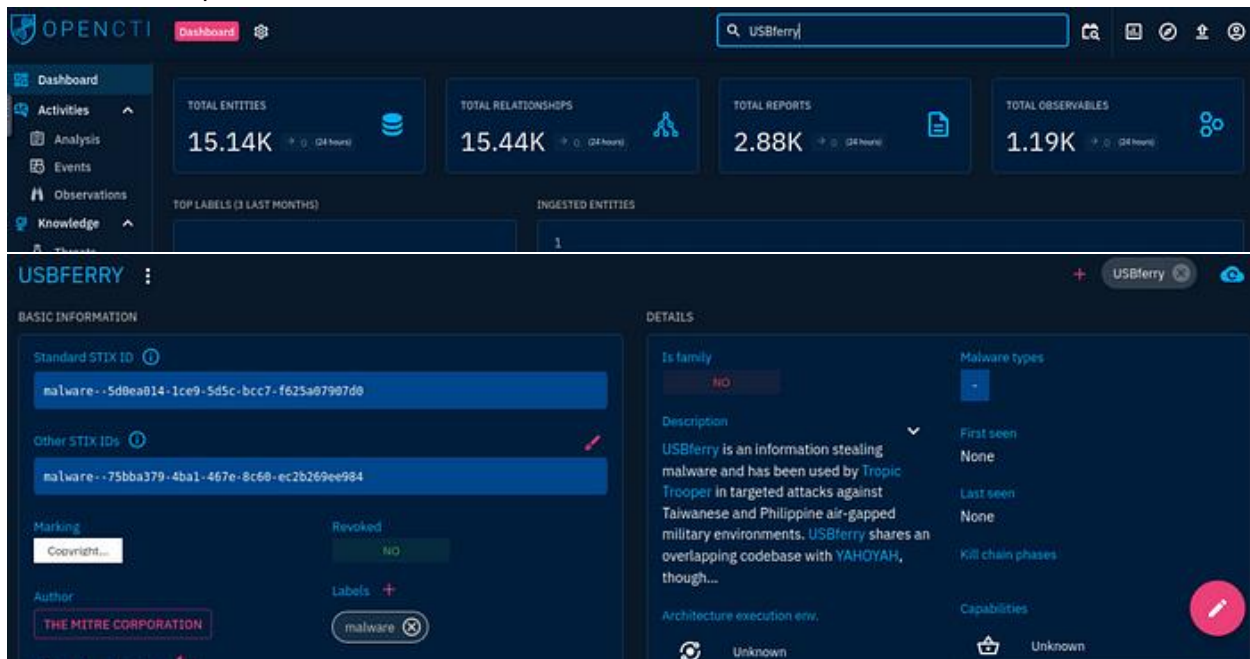
A: USBferry

Q: What is the malware's STIX ID?

For this, we'll need to use the provided Open CTI platform. Once logged in, use the search function to look for "USBferry."



You'll see two options, but select the one marked as "Malware."

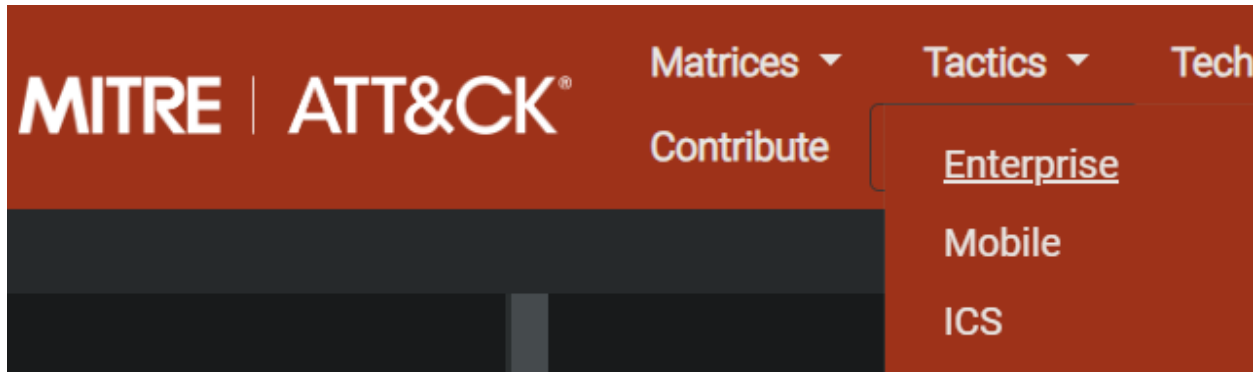


The STIX ID will be available there.

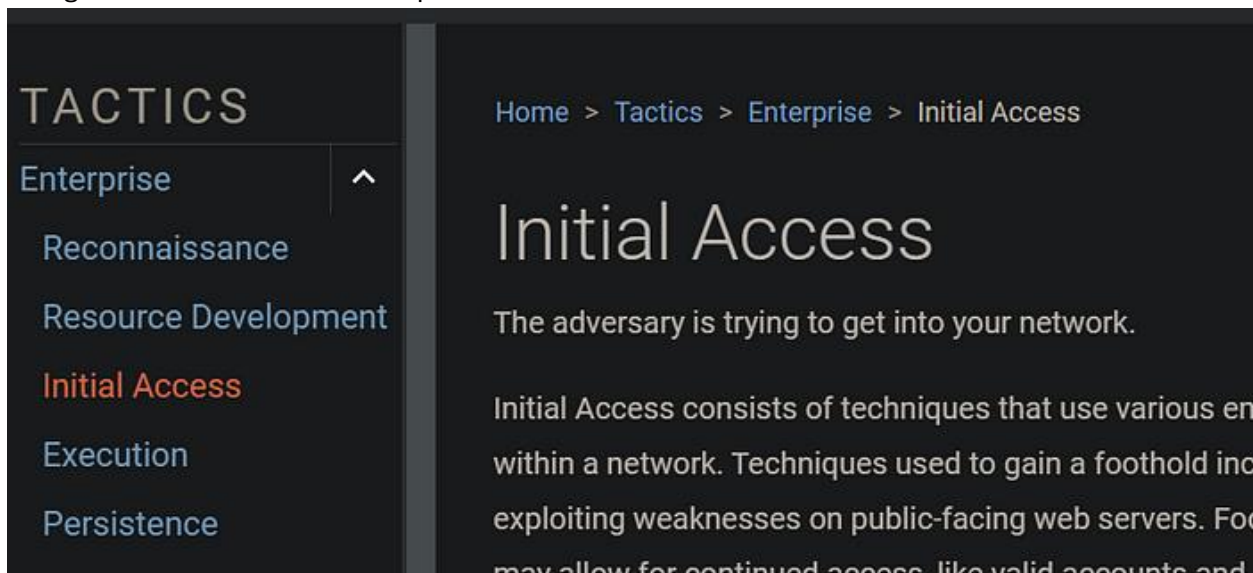
**A:** malware — 5d0ea014-1ce9-5d5c-bcc7-f625a07907d0

**Q:** With the use of a USB, what technique did APT X use for initial access?

This one involves visiting the MITRE ATT&CK website. Navigate to “Tactics” in the Enterprise section and look under “Initial Access.” The report mentions USB usage and air-gapped



Navigate to “Tactics” in the Enterprise section and look under “Initial Access.”



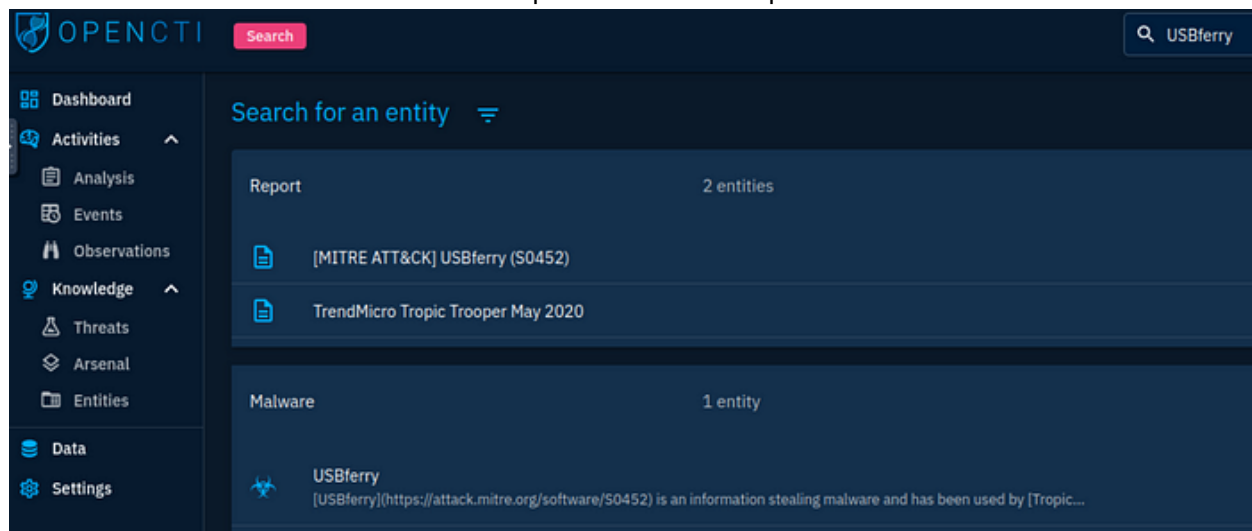
The report mentions USB usage and air-gapped

T1091	Replication Through Removable Media	Adversaries may move onto systems, possibly those on disconnected or air-gapped networks, by copying malware to removable media and taking advantage of Autorun features when the media is inserted into a system and executes. In the case of Lateral Movement, this may occur through modification of executable files stored on removable media or by copying malware and renaming it to look like a legitimate file to trick
-------	-------------------------------------	--

**A:** Replication Through Removable Media

**Q:** What is the identity of APT X?

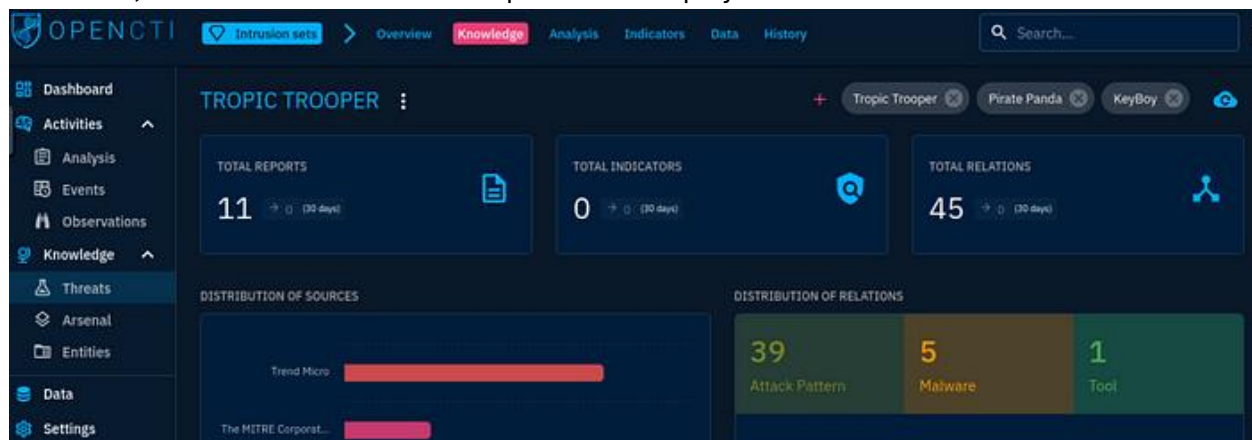
The answer for this is found in the same Open CTI search we performed earlier.



A: Tropic Trooper

Q: On OpenCTI, how many Attack Pattern techniques are associated with the APT?

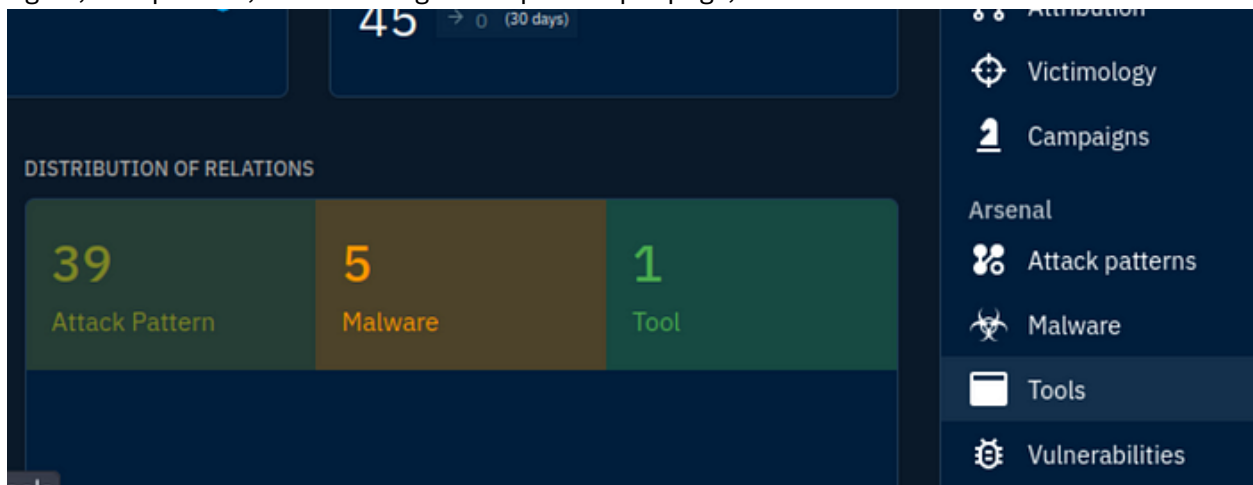
We can find this in Open CTI by searching for “Tropic Trooper,” then navigating to the “Knowledge” tab. There, the number of known attack patterns is displayed under the distribution section.



A: 39

Q: What is the name of the tool linked to the APT?

Again, on Open CTI, while viewing the Tropic Trooper page,



check the “Arsenal” section and select “Tools.”

RELATIONSHIP TYPE	NAME	ENTITY TYPE	START TIME	STOP TIME	CONFIDENCE
uses	BITSAdmin	Tool	Mar 14, 2018	Mar 14, 2018	LOW

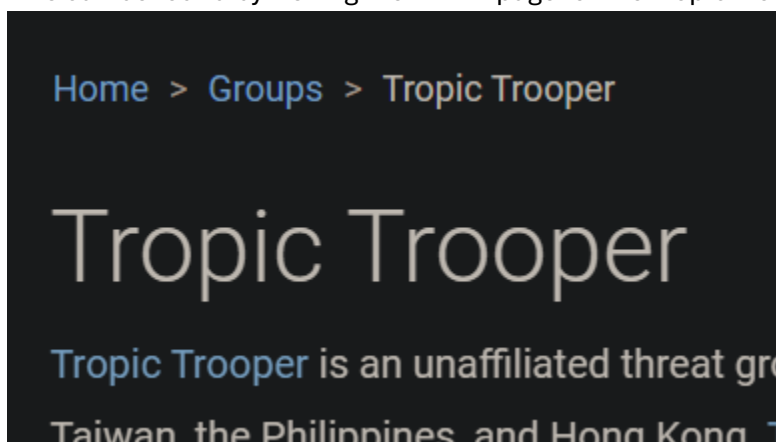
Attribution  
Victimology  
Campaigns  
Arsenal  
Attack patterns  
Malware  
Tools  
Vulnerabilities

The tool associated with the group will be listed there.

**A:** BITSAdmin

**Q:** Load up the Navigator. What is the sub-technique used by the APT under Valid Accounts?

This can be found by visiting the MITRE page for the Tropic Trooper group.



Once there, use the search function to locate "Valid Accounts." The specific sub-technique will be listed

Enterprise	T1078	.003	Valid Accounts: Local Accounts	Tropic Trooper has used known administrator account credentials to execute the backdoor directly. <sup>[3]</sup>
------------	-------	------	--------------------------------	--

A: Local Accounts

Q: Under what Tactics does the technique above fall?

Staying on the same MITRE page, The information is clearly shown on the right side of the page.

Enterprise	T1078	.003	Valid Accounts: Local Accounts	Tropic Trooper has used known administrator account credentials to execute the backdoor directly. <sup>[3]</sup>
------------	-------	------	--------------------------------	--

clicking on the T1078 technique will provide the related Tactics.

## Valid Accounts: Local Accounts

Other sub-techniques of Valid Accounts (4) ▾

Adversaries may obtain and abuse credentials of a local account as a means of gaining Initial Access, Persistence, Privilege Escalation, or Defense Evasion. Local accounts are those configured by an organization for use by users, remote support, services, or for administration on a single system or service.

Local Accounts may also be abused to elevate privileges and harvest credentials through OS Credential Dumping. Password reuse may allow the abuse of local accounts across a set of machines on a network for the purposes of Privilege Escalation and Lateral Movement.

ID: T1078.003

Sub-technique of: T1078

① Tactics: Defense Evasion, Persistence, Privilege Escalation, Initial Access

① Platforms: Containers, Linux, Windows, macOS

① Permissions Required: Administrator, User

The information is clearly shown on the right side of the page.

ID: T1078.003

Sub-technique of: T1078

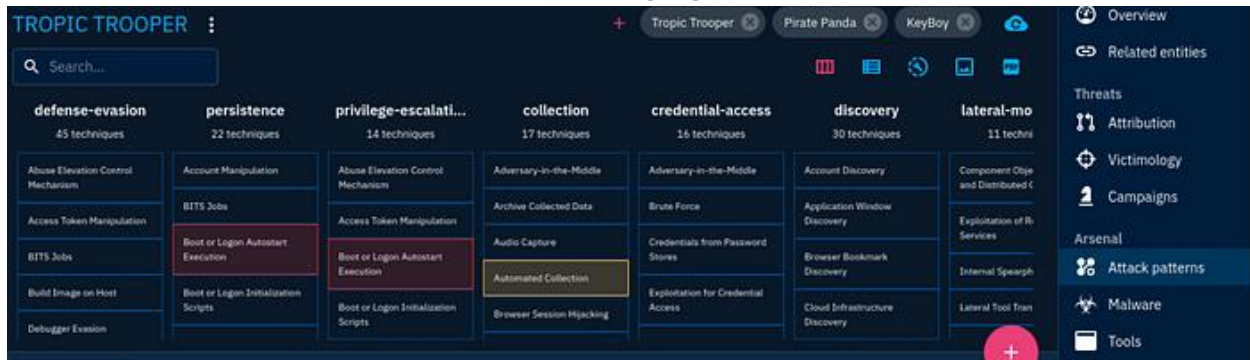
① Tactics: Defense Evasion, Persistence, Privilege Escalation, Initial Access

① Platforms: Containers, Linux,

A: Defense Evasion, Persistence, Privilege Escalation, Initial Access

Q: What technique is the group known for using under the tactic Collection?

For a change, let's return to Open CTI. In the "Arsenal" section, select "Attack Patterns" and look for the "Collection" tactic. The relevant technique is highlighted there.



**A:** Automated Collection