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.

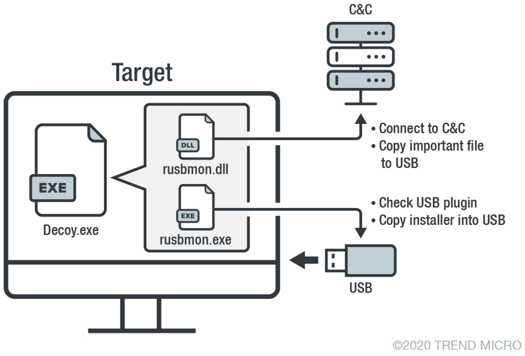


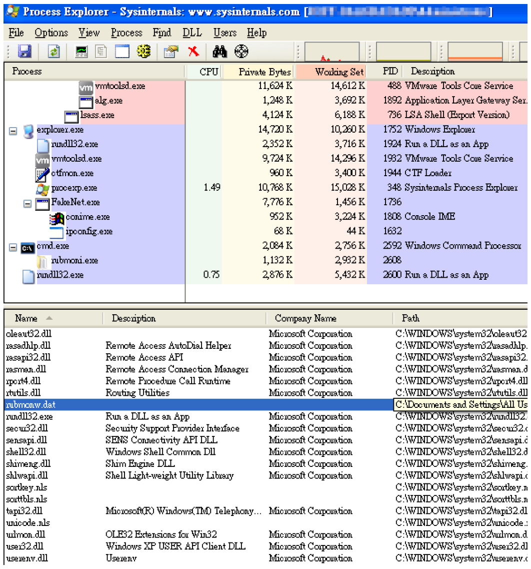
Figure 1: A sample scenario of the USBferry attack

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:

- The first version has a small component of TROJ_YAHOYAH. The malware tries to check if the target machine has a USB plug-in and copies the USBferry installer into the USB storage. The activities vary in target environments; some execute commands, source target files or folder lists, and copy files from physically isolated hosts to compromised hosts, among other things.
- The second version has the same capabilities as the first and combines components into one executable. This version also changes the malware location and its name to UF, an abbreviation for USBferry.
- The third version retains the previous versions' capabilities and improves its stealth in the target environment by residing in the *rundll32.exe* memory.


Process Explorer - Sysinternals: www.sysinternals.com [[redacted]]
File
Options
View
Process
Find
DLL
Users
Help

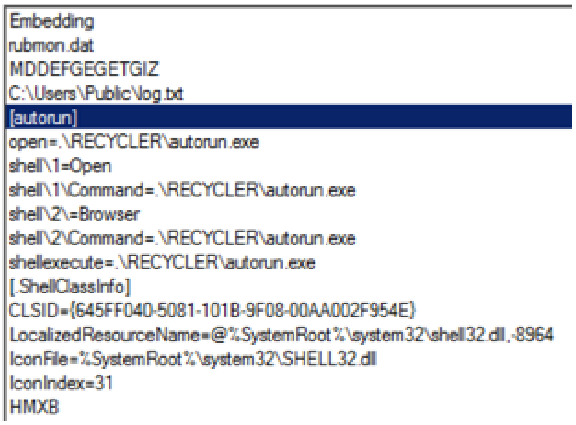
Process	CPU	Private Bytes	Working Set	PID	Description
vmtoolsd.exe		11,624 K	14,612 K	488	VMware Tools Core Service
alg.exe		1,248 K	3,692 K	1892	Application Layer Gateway Ser.
lsass.exe		4,124 K	6,188 K	736	LSA Shell (Export Version)
explorer.exe		14,720 K	10,260 K	1752	Windows Explorer
rundll32.exe		2,352 K	3,716 K	1924	Run a DLL as an App
vmtoolsd.exe		9,724 K	14,296 K	1932	VMware Tools Core Service
ctfmon.exe		960 K	3,400 K	1944	CTF Loader
procexp.exe	1.49	10,768 K	15,028 K	348	Sysinternals Process Explorer
FakeNet.exe		7,776 K	1,456 K	1736	
conime.exe		952 K	3,224 K	1808	Console IME
ipconfig.exe		68 K	44 K	1632	
cmd.exe		2,084 K	2,756 K	2592	Windows Command Processor
rubmoni.exe		1,132 K	2,932 K	2608	
rundll32.exe	0.75	2,876 K	5,432 K	2600	Run a DLL as an App

Name	Description	Company Name	Path
oleaut32.dll		Microsoft Corporation	C:\WINDOWS\system32\oleaut32.
rasadhlp.dll	Remote Access AutoDial Helper	Microsoft Corporation	C:\WINDOWS\system32\rasadhlp.
rasapi32.dll	Remote Access API	Microsoft Corporation	C:\WINDOWS\system32\rasapi32.
rasman.dll	Remote Access Connection Manager	Microsoft Corporation	C:\WINDOWS\system32\rasman.d
rpcrt4.dll	Remote Procedure Call Runtime	Microsoft Corporation	C:\WINDOWS\system32\rpcrt4.dll
rtutils.dll	Routing Utilities	Microsoft Corporation	C:\WINDOWS\system32\rtutils.dll
rubmonw.dat			C:\Documents and Settings\All Us
rundll32.exe	Run a DLL as an App	Microsoft Corporation	C:\WINDOWS\system32\rundll32.
secur32.dll	Security Support Provider Interface	Microsoft Corporation	C:\WINDOWS\system32\secur32.c
sensapi.dll	SENS Connectivity API DLL	Microsoft Corporation	C:\WINDOWS\system32\sensapi.c
shell32.dll	Windows Shell Common Dll	Microsoft Corporation	C:\WINDOWS\system32\shell32.d
shimeng.dll	Shim Engine DLL	Microsoft Corporation	C:\WINDOWS\system32\shimeng.
shlwapi.dll	Shell Light-weight Utility Library	Microsoft Corporation	C:\WINDOWS\system32\shlwapi.c
sortkey.nls			C:\WINDOWS\system32\sortkey.n
sorttbls.nls			C:\WINDOWS\system32\sorttbls.n
tapi32.dll	Microsoft(R) Windows(TM) Telephony...	Microsoft Corporation	C:\WINDOWS\system32\tapi32.dll
unicode.nls			C:\WINDOWS\system32\unicode.:
urlmon.dll	OLE32 Extensions for Win32	Microsoft Corporation	C:\WINDOWS\system32\urlmon.d
user32.dll	Windows XP USER API Client DLL	Microsoft Corporation	C:\WINDOWS\system32\user32.dl
userenv.dll	Userenv	Microsoft Corporation	C:\WINDOWS\system32\userenv.c

Figure 2: USBferry malware's first version, where the EXE file is the USBferry malware and the DLL file is trojan TROJ_YAHOYAH

How USBferry targets air-gapped systems

APT X has changed the way it uses the abovementioned USBferry versions in attacks. The group achieves infection by employing the USB worm infection strategy and ferrying a malware installer via USB into an air-gapped host machine.



```
Embedding
rubmon.dat
MDDEFGEGETGIZ
C:\Users\Public\log.txt
[autorun]
open=.\RECYCLER\autorun.exe
shell\1=Open
shell\1\Command=.\RECYCLER\autorun.exe
shell\2\=Browser
shell\2\Command=.\RECYCLER\autorun.exe
shellexecute=.\RECYCLER\autorun.exe
[.ShellClassInfo]
CLSID={645FF040-5081-101B-9F08-00AA002F954E}
LocalizedResourceName=@%SystemRoot%\system32\shell32.dll,-8964
IconFile=%SystemRoot%\system32\SHELL32.dll
IconIndex=31
HMXB
```

Figure 3. USBferry malware using USB worm infection strategy

The notable changes in the group's latest attack chain that uses version UF1.0 20160226 (detected by Trend Micro as TROJ_USBLODR.ZAHB-A) are as follows:

1. The decoy file first drops a *flash_en.inf* DLL file, which is a USBferry loader, and tries to load the encrypted USBferry malware.
2. The encrypted USBferry malware is embedded in the loader resource section, and the loader drops it into the *C:\Users\Public\Documents\Flash* folder and names it *flash.dat.*
3. After the encrypted payload is loaded, the loader injects a malicious DLL into *rundll32.exe*. The USBferry malware also loads a C&C configuration file and *flash_en.dat*, which is also located in the C:*\Users\Public\Documents\Flash.*
4. The USBferry malware then tries to connect to the download site and uses a Windows command to collect/copy target host data.