

- [Trend Micro](#)
- [About TrendLabs Security Intelligence Blog](#)



Search:

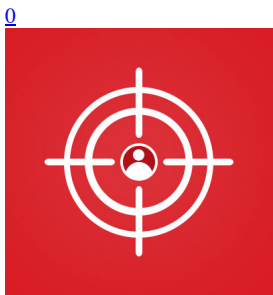
Go to...

- [Home](#)
- [Categories](#)

[Home](#) » [Malware](#) » Tropic Trooper's Back: USBferry Attack Targets Air-gapped Environments

Tropic Trooper's Back: USBferry Attack Targets Air-gapped Environments

- Posted on: [May 12, 2020](#) at 5:18 am
- Posted in: [Malware](#), [Targeted Attacks](#)
- Author: [Trend Micro](#)

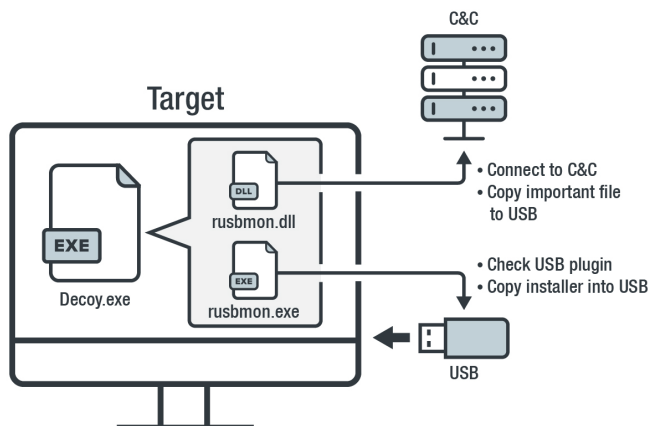


By **Joey Chen (Threats Analyst)**

[Tropic Trooper](#), 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 Tropic Trooper'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 Tropic Trooper's main purpose is to exfiltrate confidential information or intelligence.



©2020 TREND MICRO

Figure 1. A sample scenario of the USBferry attack

Tropic Trooper 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 Tropic Trooper move from a military hospital to the military's physically isolated network.

This blog post provides an overview of the USB malware called USBferry and its capabilities, as well as the other tools used to infiltrate physically isolated environments. Further details, including indicators of compromise (IoCs), can be read in the [technical brief](#).

A USB malware called USBferry

We first encountered the malware from a PricewaterhouseCoopers report that [mentioned](#) a sample related to Tropic Trooper 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.

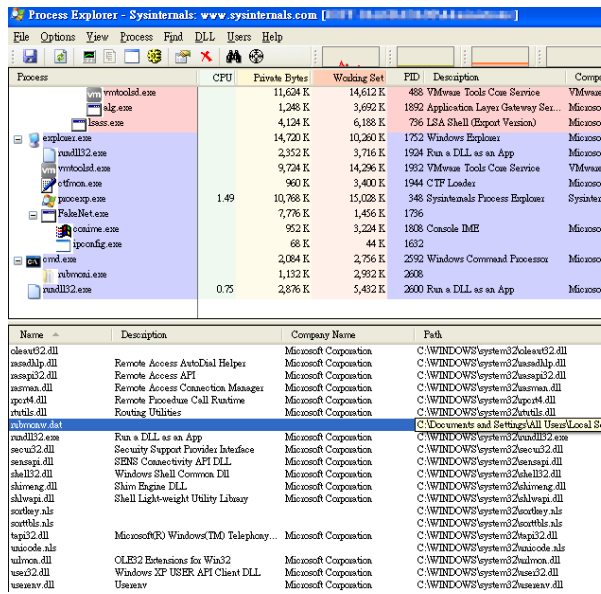


Figure 2. USBferry malware's first version, where the EXE file is the USBferry malware and the DLL file is trojan TROJ_YAHOYAH

- 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.

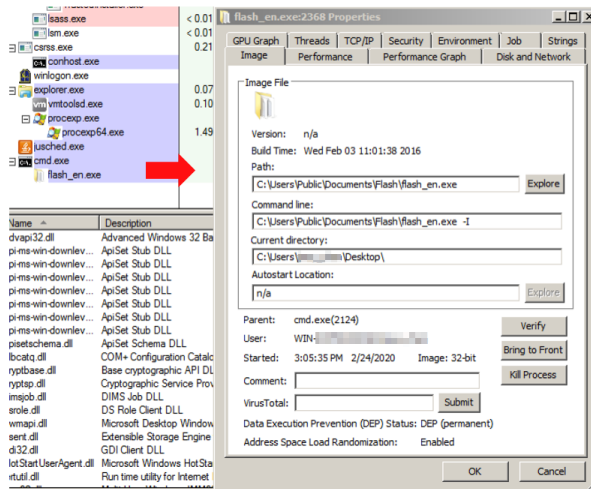


Figure 3. USBferry malware's second version combined into one file

- The third version retains the previous versions' capabilities and improves its stealth in the target environment by residing in the *rundll32.exe* memory.

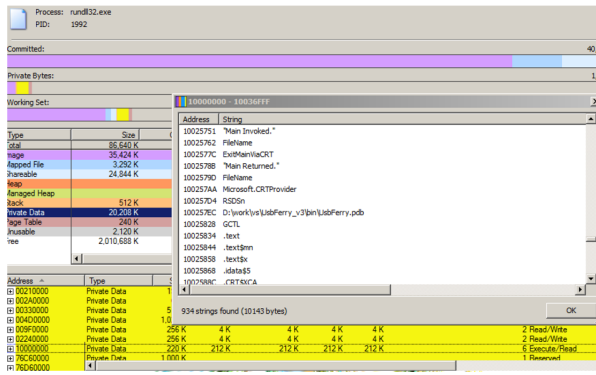


Figure 4. USBferry malware's third version becomes resident in memory

How USBferry targets air-gapped systems

In our [technical brief](#), we broke down how Tropic Trooper 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
MDDDFEGGETGIZ
C:\Users\Public\log.txt
[autorun]
open=-\RECYCLER\autorun.exe
shell\1=Open
shell\1\1=Command=-\RECYCLER\autorun.exe
shell\2=Browser
shell\2\1=Command=-\RECYCLER\autorun.exe
shell\execute=-\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 5. USBferry malware using USB worm infection strategy

Here we will discuss the notable changes in the group's latest attack chain that uses version UF1.0 20160226 (detected by Trend Micro as TROJ_USBL0DR.ZAHB-A):

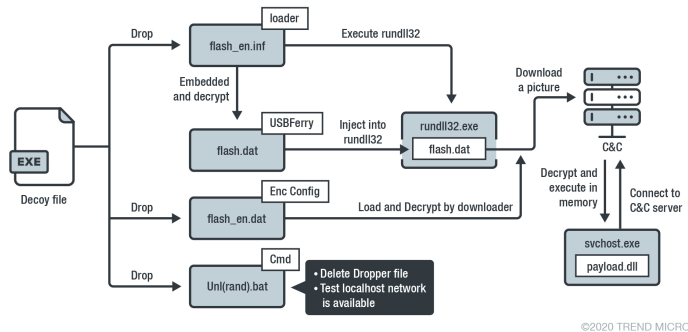


Figure 6. USBferry attack scenario, version UF1.0 20160226

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

This version checks for network connectivity; if it finds that the network is unavailable, it tries to collect information from the target machine and copy the collected data into USB storage. This way, the USB exfiltrates the information and sends it back to the C&C server.

Backdoors and other tools used by Tropic Trooper

Some backdoors used by Tropic Trooper use injection to execute its routines, while others execute directly and run itself consistently. The group also uses steganography to mask their backdoor routines and evade anti-malware and network perimeter detection. To find the full list of the backdoors we analyzed, check out our [technical brief](#).

Here we will tackle some of the noteworthy backdoors Tropic Trooper used.

- **WelCome To Svchost 3.2 20110818's backdoor** (detected as BKDR_SVCSHELL.ZAHC-A) – This backdoor bears similarities with a payload we [discussed](#) in our previous research. Based on the malware version number, this backdoor's first version was developed in or before 2011. This means that Tropic Trooper's activities have been ongoing for at least ten years now.

data:1002...	00000034	C	WELCOME To Svchost 3.2 20110818VwVw
data:1002...	00000009	C	twsmoqtl
data:1002...	00000005	C	INCS
data:1002...	00000023	C	IPSEC Network Connections Services
data:1002...	0000003B	C	Provide Services and Manager for IPSEC Network Connections
data:1002...	0000000A	C	mfo41.dll
data:1002...	0000000A	C	mfo61.dll
data:1002...	0000000C	C	rpert32.dll
data:1002...	0000000C	C	rpert16.dll
data:1002...	00000006	C	usb30
data:1002...	0000000A	C	usb30.sys
data:1002...	0000000A	C	mfo41.ini
data:1002...	0000000A	C	mfo41.dat
data:1002...	0000000E	C	MDDFEGEGHTGIZ

Figure 7. The backdoor version name, registered service name, and malware components' filenames

- **Welcome To IDShell 1.0 20150310's backdoor** (detected as BKDR_IDSHELL.ZTFC-A) – The purpose of this backdoor, which has two types, including a steganography jpg evasive, is to recon the target machine. Like other versions, it uses the DNS protocol to communicate with the backdoor controller. The traffic is encrypted to evade detection.

No.	Time	Source	Destination	Protocol	Length	Info
753	2461.682959			DNS	121	Standard query 0x3333 A 58000 TXT
754	2461.683892			DNS	135	Standard query response 0x3333 A 223.27.35.244 A 8
765	2483.681637			DNS	1066	Standard query 0x3333 A 58000 TXT
766	2483.682255			DNS	140	Standard query response 0x3333 A 223.27.35.244 A 8
770	2515.682562			DNS	1066	Standard query 0x3333 A 58000 TXT
771	2515.683166			DNS	140	Standard query response 0x3333 A 223.27.35.244 A 8
775	2547.683406			DNS	1066	Standard query 0x3333 A 58000 TXT
776	2547.683997			DNS	140	Standard query response 0x3333 A 223.27.35.244 A 8
778	2579.691320			DNS	1066	Standard query 0x3333 A 58000 TXT
779	2579.692063			DNS	140	Standard query response 0x3333 A 223.27.35.244 A 8
783	2611.692101			DNS	1066	Standard query 0x3333 A 58000 TXT
784	2611.693256			DNS	140	Standard query response 0x3333 A 223.27.35.244 A 8
786	2643.693051			DNS	1066	Standard query 0x3333 A 58000 TXT
787	2643.693765			DNS	140	Standard query response 0x3333 A 223.27.35.244 A 8
790	2654.771270			DNS	138	Standard query response 0x3333 A 223.27.35.244 A 8
791	2654.771524			DNS	90	Standard query 0x3333 A 58000 TXT
792	2654.772125			DNS	109	Standard query 0x3333 A 58000 TXT
793	2661.555033			DNS	134	Standard query response 0x3333 A 223.27.35.244 A 8
794	2661.555266			DNS	336	Standard query 0x3333 A 58000 TXT
795	2661.555472			DNS	336	Standard query 0x3333 A 58000 TXT
796	2661.555676			DNS	336	Standard query 0x3333 A 58000 TXT
797	2661.555818			DNS	336	Standard query 0x3333 A 58000 TXT

Figure 8. The backdoor's communication traffic

- **Hey! Welcome Server 2.0's backdoor** (detected as BKDR_TEBSHELL.ZTGK) – This is the latest version of the backdoor, available in 32-bit and 64-bit versions, which uses an invisible web shell for remote control and network security evasion. It runs the process as a service, hides backdoor communication in normal traffic, and uses customized TCP protocol. It also improves the way it handles wrong input commands and unauthorized access.

```

1 sc create gupdate binPath= "%C:\Program Files (x86)\Google\Update\GoogleUpdate.exe"
  /svc type= share type= interact start= auto DisplayName= "Google更新 服務 (gupdate)"
2 sc description gupdate "這會持續更新您的 Google。如果停用或中止這項服務程序，Google
  軟體將無法維持最新狀態，因而無法修正日後出現的安全性漏洞，甚至無法執行相關功能。如果沒有 Google
  軟體執行這項服務程序，它會自行解除安裝。"
3 sc config gupdate start= delayed-auto
4 reg add hklm\system\currentcontrolset\services\gupdate /v ErrorControl /t REG_DWORD /d 0 /f
5 net start gupdate

```

Figure 9. The executable version will install and name it as a Windows service, change registry to disable error display, and launch the service

Tropic Trooper also used other tools in their attacks, such as:

- Command-line remote control listener/port relay tool, which has different versions that can communicate with the backdoor.
- Backdoor payload/steganography payload execution loaders, which have two versions that can be used to successfully load the encrypted payload and subsequently delete itself and the payload.
- Port scanning tools, which are available on the internet.

The overview provided above highlights how putting critical information in physically isolated networks is not a bulletproof solution for defending against cyberespionage. Steganography isn't just used to deliver encrypted payloads; it can also be used to transfer information to a C&C server. Multiple hacking tools and components can also help facilitate successful attacks on different networks and environments. Threat actors like Tropic Trooper can also use an invisible web shell to hide its C&C server location and make incident response tricky.

MITRE ATT&CK Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion
Replication Through Removable Media	Rundll32	Hidden Files and Directories	Process Injection	Deobfuscate Files, Decode File Information
Trusted Relationship	Scripting	Registry Run Keys / Startup Folder	Web Shell	File Deletion
Valid Accounts	User Execution	Web Shell	Valid Accounts	Hidden Files and Directories
				Process Hijacking
				Scripting
				Valid Accounts

Best practices and Trend Micro solutions

The latest developments with Tropic Trooper indicate that they are well-prepared to target government institutions and military agencies for stolen intelligence. The group also takes a long time to perform reconnaissance and consequently infiltrate physically isolated networks. This research also underscores how threat actors could see potentially vulnerable targets as launch points for extending their attack attempts to other, more critical targets.

Understanding attack tactics and techniques can provide the needed context for assessing potential impact and adopting defensive strategies. Here are some measures that organizations can practice to thwart advanced persistent threats with security that employs actionable threat intelligence, network-wide visibility, and timely threat protection:

- **Enforce the principle of least privilege.** Employ [network segmentation](#) and data categorization to deter lateral movement and mitigate exposure.
- **Keep the system and its applications up-to-date.** Weaknesses in the network can serve as entry points for attacks. Enforce a strong [patch management](#) policy and consider [virtual patching](#) for legacy systems.
- **Regularly monitor your perimeter.** Adopt [cross-layer detection and response](#) across gateways, endpoints, networks, and servers to protect against a wide range of cybersecurity threats. [Firewalls](#) and [intrusion detection and prevention systems](#) can help defend against network-based attacks.

Organizations can take advantage of the [Trend Micro Apex One™](#) solution, which provides actionable insights, expanded investigative capabilities, and centralized visibility across the network through a variety of threat detection capabilities such as behavioral analysis that protects against malicious scripts, injection, ransomware, memory, and browser attacks.

A multilayered security solution such as [Trend Micro™ Deep Discovery™](#) can also be considered; it provides in-depth analysis and proactive response to attacks using exploits and other similar threats through specialized engines, custom sandboxing, and seamless correlation across the entire attack lifecycle, allowing it to detect these attacks even without any engine or pattern updates.

Read our [technical brief](#), which discusses in full our analyses of Tropic Trooper's recent activities, the USBferry malware, and IoCs.

Related Posts:

- [Operation ENDTRADE: Finding Multi-Stage Backdoors that TICK](#)
- [MuddyWater Resurfaces, Uses Multi-Stage Backdoor POWERSTATS V3 and New Post-Exploitation Tools](#)
- [Shifting Tactics: Breaking Down TA505 Group's Use of HTML, RATs and Other Techniques in Latest Campaigns](#)
- [Gamaredon APT Group Use Covid-19 Lure in Campaigns](#)

Say NO to ransomware.
Trend Micro has blocked over 100 million threats and counting

Learn how to protect Enterprises, Small Businesses, and Home Users from ransomware:

[ENTERPRISE >>](#)

[SMALL BUSINESS >>](#)

[HOME >>](#)

Tags: [cyberespionage](#)[KeyBoymilitary](#)[USB](#)[USBferry](#)

0 Comments TrendLabs Privacy Policy Login ▾

Recommend Tweet Share Sort by Best ▾

Start the discussion...

LOG IN WITH

OR SIGN UP WITH DISQUS

Name

Be the first to comment.

Subscribe Add Disqus to your siteAdd DisqusAdd

Security Predictions for 2020

- Cybersecurity in 2020 will be viewed through many lenses — from differing attacker motivations and cybercriminal arsenal to technological developments and global threat intelligence — only so defenders can keep up with the broad range of threats. [Read our security predictions for 2020.](#)

Business Process Compromise

- Attackers are starting to invest in long-term operations that target specific processes enterprises rely on. They scout for vulnerable practices, susceptible systems and operational loopholes that they can leverage or abuse. To learn more, [read our Security 101: Business Process Compromise.](#)

Recent Posts

- [May Patch Tuesday: More Fixes for SharePoint, TLS, Runtime, and Graphic Components Released](#)
- [Tropic Trooper's Back: USBferry Attack Targets Air-gapped Environments](#)
- [New MacOS Dacls RAT Backdoor Show Lazarus' Multi-Platform Attack Capability.](#)
- [Targeted Ransomware Attack Hits Taiwanese Organizations](#)
- [WebMonitor RAT Bundled with Zoom Installer](#)

Popular Posts

[Exposed Redis Instances Abused for Remote Code Execution, Cryptocurrency Mining](#)

[WebMonitor RAT Bundled with Zoom Installer](#)

[Exposing Modular Adware: How DealPly, IsErlk, and ManageX Persist in Systems](#)

[Coronavirus Update App Leads to Project Spy Android and iOS Spyware](#)

[New MacOS Dacls RAT Backdoor Show Lazarus' Multi-Platform Attack Capability](#)

Stay Updated

Email Subscription

- [Home and Home Office](#)
- |
- [For Business](#)
- |
- [Security Intelligence](#)
- |
- [About Trend Micro](#)

- Asia Pacific Region (APAC): [Australia](#) / [New Zealand](#), [中国](#), [日本](#), [대한민국](#), [台灣](#)
- Latin America Region (LAR): [Brasil](#), [México](#)
- North America Region (NABU): [United States](#), [Canada](#)
- Europe, Middle East, & Africa Region (EMEA): [France](#), [Deutschland / Österreich / Schweiz](#), [Italia](#), [Россия](#), [España](#), [United Kingdom / Ireland](#)

- [Privacy Statement](#)
- [Legal Policies](#)

- Copyright © 2020 Trend Micro Incorporated. All rights reserved.