Google Cloud  Blog

Contact sales

Get started for free

Threat Intelligence

# The Spies Who Loved You: Infected USB Drives to Steal Secrets

July 11, 2023

**Mandiant**

Written by: Rommel Joven, Ng Choon Kiat

In the first half of 2023, Mandiant [Managed Defense](#) has observed a threefold increase in the number of attacks using infected USB drives to steal secrets. Mandiant tracked all of the cases and found that the majority of the incidents could be attributed to several active USB-based operation campaigns affecting both the public and private sectors globally.

Previously, we covered one of the campaigns that [leverages USB flash drives as an initial infection vector](#) and concentrates on the Philippines. In this blog post, we are covering two additional USB-based cyber espionage

Google Cloud    Blog

Contact sales    Get started for free

- **SOGU Malware Infection via USB Flash Drives Across Industries and Geographies**

  This is the most prevalent USB-based cyber espionage attack using USB flash drives and one of the most aggressive cyber espionage campaigns targeting both public and private sector organizations globally across industry verticals. It uses USB flash drives to load the SOGU malware to steal sensitive information from a host.

  Mandiant attributes this campaign to TEMP.Hex, a China-linked cyber espionage actor. TEMP.Hex likely conducted these attacks to collect information in support of Chinese national security and economic interests. These operations pose a risk to a variety of industries, including construction and engineering, business services, government, health, transportation, and retail in Europe, Asia, and the United States.

- **SNOWYDRIVE Malware Infection via USB Flash Drives, Targets Oil and Gas Organizations in Asia**

  This campaign uses USB flash drives to deliver the SNOWYDRIVE malware. Once SNOWYDRIVE is loaded, it creates a backdoor on the host system, giving attackers the ability to remotely issue system commands. It also spreads to other USB flash drives

Contact sales

Get started for free

Mandiant attributes this campaign to UNC4698, a
threat actor that has targeted oil and gas
organizations in Asia. Once the actor has gained
access to the system, they execute arbitrary payloads
using the Windows Command Prompt, use removable
media devices, create local staging directories, and
modify the Windows registry.

# SOGU Malware Infection via USB Flash Drives Across Industries and Geographies

Managed Defense first observed this campaign while
hunting for suspicious file write events in common
directories that threat actors use for their malware, tools,
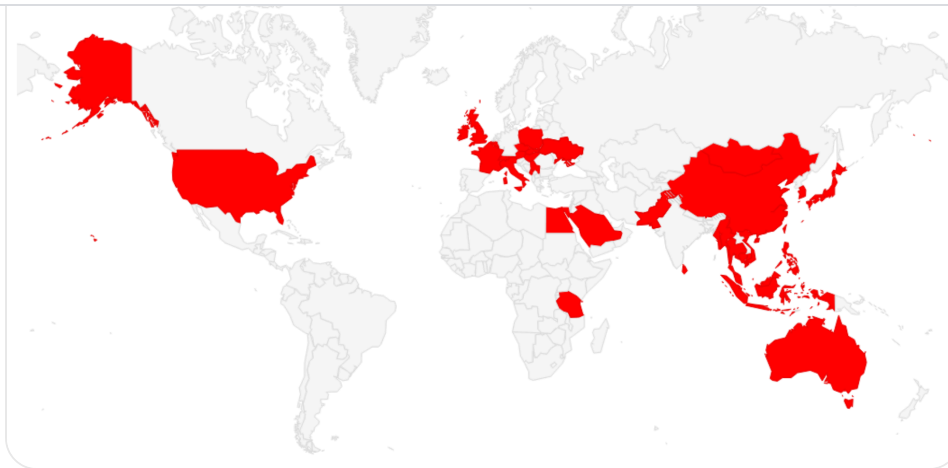or utilities.

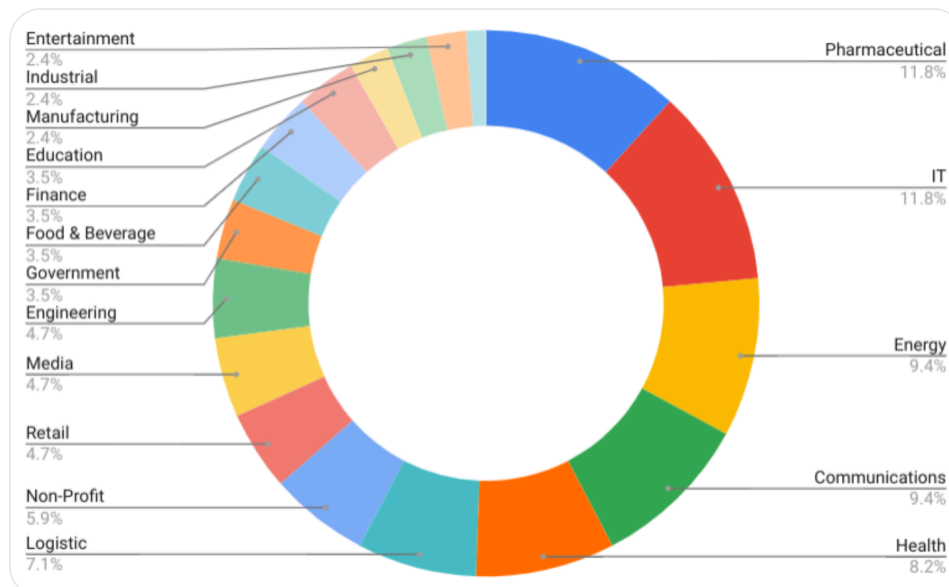*Figure 1: Geographic distribution of TEMP.HEX victims*



*Figure 2: Managed Defense investigation breakdown by industry*

# The Initial Infection

An infected USB flash drive is the initial infection vector. The flash drive contains multiple malicious software that
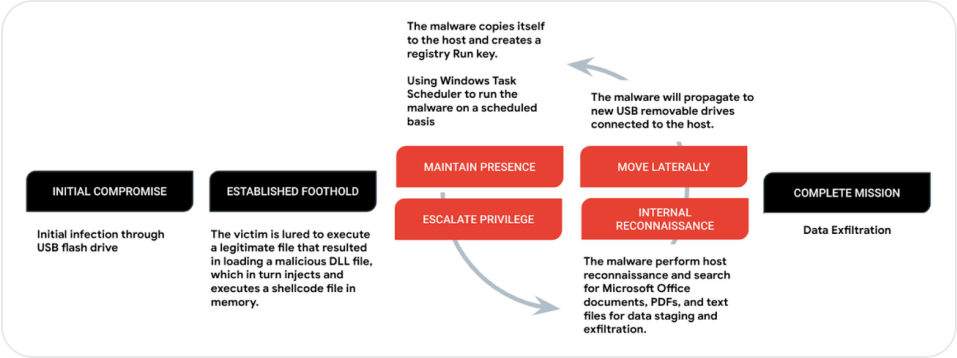
Google Cloud    Blog

Contact sales

Get started for free



*Figure 3: Attacker lifecycle*

# Established Foothold

The entire infection chain usually consists of three files: a legitimate executable, a malicious DLL loader, and an encrypted payload. Table 1 shows the commonly observed malware file paths and file names observed throughout the campaign.

| File Path | Benign Executable | Malicious DLL Loader |
|---|---|---|
| :\RECYCLER.BIN\1\ | CEFHelper.exe | wsc.dll |
| :\RECYCLERS.BIN\ | Smadav.exe | smadhook3 |
| :\RECYCLERS.BIN\ | AdobeUpdate.exe | hex.dll |

Google Cloud     Blog

Contact sales

Get started for free

*RECYCELRS.BIN*

When the legitimate executable is run, it will side-load a malicious DLL file, which we tracked as **KORPLUG**. The **KORPLUG** malware will then load a decrypted shellcode, commonly observed in the form of a .dat file, and execute it in memory. The shellcode is commonly observed as a backdoor that Mandiant tracked as **SOGU**, a backdoor written in C.

## Reconnaissance and Data Staging

The infection continues by dropping a batch file onto the RECYCLE.BIN file path. The batch file runs host reconnaissance commands and outputs the results to a file named **c3lzLmluZm8**. When decoded from Base64, the file name **c3lzLmluZm8** is "sys.info". The following commands to gather specific system metadata are executed:

- tasklist /v
- arp -a
- netstat -ano
- ipconfig /all
- systeminfo

**.xls**, **.xlsx**, and **.pdf**. It encrypts a copy of each file, encodes the original filenames using Base64, and drops the encrypted files in the following directories:

- C:\Users\<user>\AppData\Roaming\Intel\<SOGU CLSID>\<filename in Base64>
- <drive>:\RECYCLER.BIN\<SOGU CLSID>\<filename in Base64>

## Maintain Presence

To maintain its persistence on the system, the malware creates a directory that masquerades as a legitimate program and sets the directory's attribute to hidden. It then copies its main components to this directory, with the following commonly used file paths:

- C:\ProgramData\AvastSvcpCP
- C:\ProgramData\AAM UpdatesHtA
- C:\ProgramData\AcroRd32cWP
- C:\ProgramData\Smadav\SmadavNSK

Then, it creates a Run registry key with the same name as the directory created earlier. The Run registry keys are used to run programs automatically when a user logs on. The following are the commonly observed Run registry key entries.

- Value: AvastSvcpCP

- Text: C:\ProgramData\AAM UpdatesHtA\AAM Updates.exe

- Value: AcroRd32cWP

- Text: C:\ProgramData\AcroRd32cWP\AcroRd32.exe

- Value: SmadavNSK

- Text: C:\ProgramData\Smadav\SmadavNSK\Smadav.exe

In some SOGU variants, an additional scheduled task may be created to run the malware every 10 minutes to maintain persistence.

- SCHTASKS.exe /create /sc minute /mo 10 /tn "Autodesk plugin" /tr """"C:\ProgramData\Smadav\SmadavNSK\Smadav.exe"""" 644" /f

## Complete Mission

At the last stage of the attack lifecycle, the malware will exfiltrate any data that has been staged. The malware may include HTTP, HTTPS, a custom binary protocol over TCP or UDP, and ICMP to communicate with its command and control server. The malware was also found to support a wide range of commands, including file transfer, file execution, remote desktop, screenshot capture, reverse shell, and keylogging.

Google Cloud     Blog

Contact sales     Get started for free

payloads to spread to other systems and potentially collect data from air-gapped systems.

Mandiant tracks this event as Campaign 22-054.

# SNOWYDRIVE Malware Infection via USB Flash Drives, Targets Oil and Gas Organizations in Asia

Managed Defense first observed this campaign while hunting Windows Explorer process execution with a suspicious folder path (e.g., "F:\") specified on the command line. This behavior is commonly observed when a user is tricked into executing malware on USB drives. While this type of threat is not uncommon, Mandiant's relentless research and pursuit of every attack led to the discovery of yet another espionage campaign that uses USB drives to spread malware.

## The Initial Infection

An infected USB flash drive is the initial infection vector. The victim is lured to click on a malicious file that is masquerading as a legitimate executable. Upon executing

throughout the attacker's lifecycle.

---

*Figure 4: [Attacker lifecycle](#)*

# Established Foothold

The infection chain typically starts with an executable that serves as a dropper. The dropper is responsible for writing malicious files to disk and launching them. In one instance, a dropper named **USB Drive.exe** wrote the following encrypted files to **C:\Users\Public\SymantecsThorvices\Data**:

- aweu23jj46jm7dc
- bjca3a0e2sfbs
- asdigasur3ase
- sf33kasliaeae
- sf24acvywsake

The encrypted files contain executables and DLLs that are extracted and written in the directory C:\Users\Public\SymantecsThorvices\Bin.

These files can be broken down into four components, each consisting of a legitimate executable and a malicious DLL that is loaded via DLL search order

*Figure 5: Components and the execution chain of this campaign*

| Filename | Purpose |
|---|---|
| GUP.exe | Legitimate WinGup for Notepad++ |
| Silverlight.Configuration.exe | Legitimate Microsoft Silv |
| spoololk.exe | Legitimate VentaFax Sof |
| CUZ.exe | Legitimate CAM UnZip Software |
| VNTFXF32.dll | A malicious DLL loaded **spoololk.exe** to create persistence. |
| coreclr.dll | A malicious DLL loaded **Silverlight.Configurati** This malware will<br><br>• Drop and execute a shellcode-based |

Google Cloud    Blog    Contact sales    Get started for free

| | |
|---|---|
| | malicious utility that configures the host to evade detection.<br><br>• Infect other attached flash drives. |
| libcurl.dll | A malicious DLL loaded **GUP.exe**. It is an evasio that sets registry values show hidden files, hide extensions, and hide file are marked "system" an "hidden". |
| ZIPDLL.dll | **ZIPDLL.dll** is a memory dropper that injects a shellcode-based backd named **SNOWYDRIVE** i **CUZ.exe**. |

*Table 2: Malware components*

# Command and Control

The shellcode-based backdoor named SNOWYDRIVE generates a unique identifier based on the system name, username, and volume serial number. This identifier serves as a unique ID when communicating to its

Google Cloud    Blog

Contact sales

Get started for free

*Figure 6: Hard-coded domain observed in a SNOWYDRIVE variant*

The backdoor supports the following commands:

| Command ID | Description |
|---|---|
| 0x2 | Sleep |
| 0x3, 0x4 | Terminate reverse shell, exit |
| 0x5 | Create file |
| 0x6 | Write file or delete file |
| 0x7 | Initiate file upload |
| 0x8 | Continue file upload |
| 0x9 | Create cmd.exe reverse shell |
| 0xA | Execute reverse shell command |

Google Cloud    Blog                    Contact sales        Get started for free

| 0xC | List logical drives |
|-----|---------------------|
| 0xD | Start file/directory search |
| 0xE | Continue file/directory search |

*Table 3: SNOWYDRIVE supported commands*

## Maintain Presence

The registry value
HKCU\SOFTWARE\Microsoft\Windows\CurrentVersion\Run\
ushsguaei1hgba is used for persistence. It stores the path
of Silverlight.Configuration.exe.

## Lateral Movement

The malware copies itself to removable drives that are
plugged into an infected system. It creates the folder
"<drive_root>\Kaspersky\Usb Drive\3.0" on the removable
drive and copies the encrypted files that contain the
malicious components. An executable is extracted from
the file "aweu23jj46jm7dc" and written to <drive_root>\
<volume_name> .exe, which is responsible for extracting
and executing the content of  the encrypted files.

Mandiant's investigation and research identified local print shops and hotels as potential hotspots for infection. While some threat actors targeted specific industries or regions, Campaign 22-054 appears to be more opportunistic in nature. This campaign may be part of a long-term collection objective or a later-stage follow-up for subjects of interest to state-sponsored threat actors.

Organizations should prioritize implementing restrictions on access to external devices such as USB drives. If this is not possible, they should at least scan these devices for malicious files or code before connecting them to their internal networks.

# YARA Rules

## SOGU

SOGU is a backdoor written in C. The network protocol varies between samples and may include HTTP, HTTPS, a custom binary protocol over TCP or UDP, and ICMP. Supported commands include file transfer, file execution, remote desktop, screenshot capture, reverse shell, and keylogging.

```
rule M_Code_SOGU
{
```

Google Cloud     Blog     Contact sales     Get started for free

```
        description = "Hunting rule for SOGU
        sha256 = "8088b1b1fabd07798934ed3349edc

    strings:
        $sb1 = { 8B [2] C7 ?? 01 03 19 20 8B [2
        $sb2 = { 8B ?? 0C C7 ?? 01 03 19 20 8B

    condition:
        (uint16(0) == 0x5A4D) and (uint32(uint3
}
```

# FROZENHILL

FROZENHILL is a launcher written in C++ that is
configured to utilize existing files for execution and also
infects newly attached storage volumes with additional
malware.

```
rule M_Code_FROZENHILL
{
    meta:
        author = "Mandiant"
        description = "Hunting rule for FROZENH
        sha256 = "89558b4190abcdc1a2353eda59190

    strings:
```

```
    $str3 =  name_svchost  ascii
    $str4 = "run_cmd" ascii
    $str5 = "usb_dll_name" ascii
    $str6 = "name_mutex" ascii
    $str7 = "cmd /c \"%s\" %d" wide
    $str8 = { 8B 85 [4] 83 ?? 01 89 85 [4]

    condition:
        uint16(0) == 0x5A4D and uint32(uint32(0
}
```

## ZIPZAG

ZIPZAG is an in-memory dropper written in C++ that is
configured to overwrite portions of the loading process
with shellcode and transfer execution back to the process
for execution.

```
rule M_Code_ZIPZAG
{
    meta:
        author = "Mandiant"
        description = "Hunting rule for ZIPZAG"
        sha256 = "8a968a91c78916a0bb32955cbedc7
    strings:
        $str1 = { C6 45 ?? 55 C6 45 ?? 8B C6 45
```

Google Cloud    Blog

Contact sales

Get started for free

```
condition:
        uint16(0) == 0x5A4D and uint32(uint32(0
}
```

# SNOWYDRIVE

SNOWYDRIVE is a shellcode-based backdoor that communicates via a custom binary protocol over TCP. Supported commands include reverse shell creation, file transfer, file deletion, and disk enumeration.

```
rule M_Code_SNOWYDRIVE
{
    meta:
        author = "Mandiant"
        description = "Hunting rule for SNOWYDR
        sha256 = "964c380bc6ffe313e548336c9dfaa

    strings:
        $str1 = { C6 45 ?? 6B C6 45 ?? 65 C6 45
        $str2 = { C6 45 ?? 47 C6 45 ?? 65 C6 45
        $str3 = { C6 85 ?? FD FF FF 4C C6 85 ??
        $str4 = { C6 85 ?? FC FF FF 57 C6 85 ??

    condition:
```

Google Cloud　　Blog

Contact sales

Get started for free

# YARA-L Hunting Rules

The YARA-L syntax is derived from the YARA language developed by VirusTotal. The language works in conjunction with the Chronicle Detection Engine and enables you to hunt for threats and other events across large volumes of data.

Find out more about Google Chronicles.

```
rule hunting_T1091_User Execution: Malicious Fi
{
  meta:

    rule_name = "Replication Through Removable
    description = "This rule detects a file wri
author = "Mandiant Managed Defense"
    mitre_technique_name = "User Execution: Mal
    mitre_technique = "T1204"
    mitre_tactic_name = "Execution"
    platform = "Windows"


  events:
      $e.target.process.path = ":\RECYCLER.BIN
      $e.target.process.path = ":\RECYCLERS.BI
    }
```

Google Cloud        Blog

Contact sales        Get started for free

```
}

rule hunting_T1091_Replication_Through_Removabl
{
  meta:
    rule_name = "Replication Through Removable
    description = "This rule detects windows ex
author = "Mandiant Managed Defense"
    mitre_technique_name = "Replication Through
    mitre_technique = "T1091"
    mitre_tactic_name = "Lateral Movement,Initi
    platform = "Windows"

  events:
    $e.target.process = "explorer.exe" and
    {
      re.regex($e.principal.process.command_lin
      re.regex($e.principal.process.full_path,
    }

    condition:
        $e
}
```

# Indicators of Compromise

Google Cloud    Blog

Contact sales    Get started for free

| | | |
|---|---|---|
| SOGU | AvastAuth.dat | ebb7749069a9b5 |
| SOGU | hex.dll | b061d981d22445 |
| SOGU | adobeupdate.dat | 38baabddffb1d7 |
| SOGU | SmadHook32c.dll | fc55344597d540 |
| SOGU | smadavupdate.dat | 028201d92b2b4 |
| SOGU | wsc.dll | 722b15bbc15845 |
| SOGU | SmadavMain.exe | ab5d85079e299 |
| FROZENHILL | coreclr.dll | 848feec343111b |
| ZIPZAG | ZIPDLL.dll | e1cea747a64c0d |

| Malware Family | Network IOCs |
|---|---|
| SNOWYDRIVE | www.beautyporntube[.]com |
| SOGU | 45.142.166[.]112 |

Google Cloud   Blog

Contact sales

Get started for free

| SOGU | 45.251.240[.]55 |
|------|-----------------|
| SOGU | 43.254.217[.]165 |

## About Managed Defense Hunting

Cyber security hunting missions are a way to look for security breaches that bypass an organization's security controls. Managed Defense hunting missions based on Mandiant's real-time intelligence mapped to the MITRE ATT&CK framework.

Find out more about Managed Defense.

## About Threat Campaigns

Greater visibility into attacker operations: Threat Campaigns provides you with detailed information about active campaigns, including the tactics, techniques, and infrastructure used by attackers. This information can help you identify new threats and vulnerabilities, and prioritize your defensive actions.

Find out more about Threat Campaigns.

Google Cloud    Blog

Contact sales

Get started for free

## Validation Actions

Mandiant Advantage Security Validation can automate the following process to give you real data on how your security controls are performing against these threats.

The following table is a subset of MSV actions for one of the malware variants. Find out more about Mandiant Security Validation.

| VID | Name |
|---|---|
| A106-036 | Protected Theater - TEMP.Hex, SOGU, Execution, Variant #1 |
| A106-037 | Protected Theater - TEMP.Hex, SOGU, Execution via Malicious LNK, Variant #1 |
| A106-046 | Command and Control - TEMP.Hex, SOGU, Beacon, Variant #1 |
| A106-045 | Protected Theater - TEMP.Hex, SOGU, Create Install Directory, Variant #1 |
| A106-049 | Host CLI - TEMP.Hex, SOGU, Establish Persistence via Registry Run Key, Variant #1 |

| | |
|---|---|
| A106-051 | ... Variant #1 |
| A106-052 | Protected Theater - TEMP.Hex, SOGU, Network Registry Key Change, Variant #1 |
| A106-060 | Host CLI - TEMP.Hex, SOGU, Enumeration, Variant #1 |
| S100-257 | Malicious Activity Scenario - TEMP.Hex Campaign Spreading SOGU via Infected USB Drives, Variant #1 |

# Acknowledgements

This blog post is dedicated to the analysts in the Managed Defense team for their tireless work to develop new ways in defending our clients around the clock.

Special thanks to Matt Williams for his assistance in analyzing the malware samples and Matthew Hoerger and Lexie Aytes for creating the Mandiant Security Validation (MSV) actions. Martin Co for his inputs and review of this blog post.

Posted in [Threat Intelligence]

Google Cloud **Blog**

Contact sales

Get started for free

Threat Intelligence

Threat Intelligence

### Hybrid Russian Espionage and Influence Campaign Aims to Compromise Ukrainian Military Recruits and Deliver Anti-Mobilization Narratives

By Google Threat Intelligence Group • 10-minute read

### Investigating FortiManager Zero-Day Exploitation (CVE-2024-47575)

By Mandiant • 19-minute read

Threat Intelligence

Threat Intelligence

### How Low Can You Go? An Analysis of 2023 Time-to-Exploit Trends

By Mandiant • 10-minute read

### capa Explorer Web: A Web-Based Tool for Program Capability Analysis

By Mandiant • 6-minute read

Google Cloud

Blog

Contact sales

Get started for free

Google Cloud    Google Cloud Products    Privacy    Terms

Help    English