# Earth Kasha Updates TTPs in Latest Campaign Targeting Taiwan and Japan

By By: Hara Hiroaki Apr 30, 2025 Read time: 7 min (1919 words)

Published: 2025-04-30 · Archived: 2026-04-05 16:16:45 UTC

- APT group Earth Kasha continues its activity with a new campaign in March 2025 that uses spear-phishing to deliver a new version of the ANEL backdoor, possibly for espionage based on the campaign's victimology.
- In this campaign, the APT group believed to be a part of the larger APT10 group is targeting government agencies and public institutions in Taiwan and Japan. Potential impact could include information theft and sensitive data related to governance being compromised.
- The ANEL file from the 2025 campaign discussed in this blog implemented a new command to support an execution of BOF (Beacon Object File) in memory. This campaign also potentially leveraged SharpHide to launch the second stage backdoor NOOPDOOR.
- We provide recommendations for organizations to proactively secure their systems, including implementing a zero-trust approach to external and unrecognized One Drive links, and the continuous monitoring for any potential abuse of DNS over HTTPS.
- Trend Vision One™ detects and blocks the IOCs discussed in this blog. Trend Vision One customers can also access hunting queries, threat insights, and threat intelligence reports to gain rich context and the latest updates on Earth Kasha.

In our monitoring of advanced persistent threats, we observed a new campaign targeting Taiwan and Japan that can be attributed to Earth Kasha. We detected campaign activity in March 2025, and found that it uses spear-phishing to deliver a new version of the ANEL backdoor.

Earth Kasha, believed to be a part of the larger APT10 umbrella, has been conducting espionage campaigns since at least 2017 and are known to shift their techniques, tactics and toolsets frequently. Prior activity from the group was recorded in 2024, where they targeted individuals affiliated with political organizations, research institutions, thinktanks, and organizations related to international relations in Japan via spear-phishing. It appears that the group is expanding targets in their new spear-phishing campaign this year to include government agencies and public institutions in Taiwan and Japan.

We assume that the motivation behind this campaign is espionage and information theft based on the victimology and post-exploitation TTPs. Considering that Earth Kasha's origin is believed to be China, a potential espionage campaign targeting Taiwan and Japan has significant geopolitical implications.

In this blog, we will discuss the TTPs, and malware observed in Earth Kasha's latest campaign.

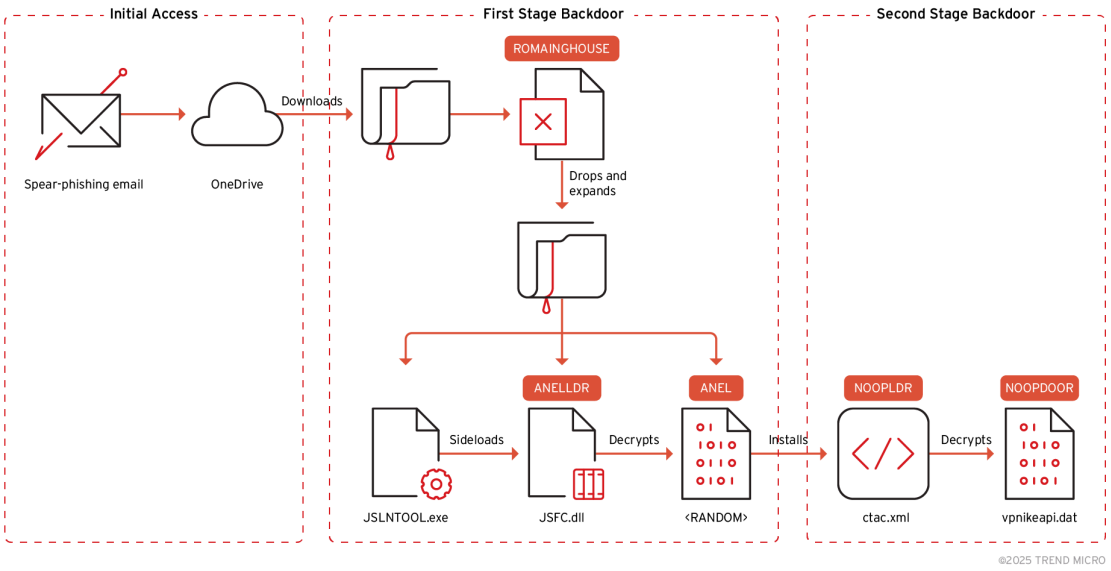


Figure 1. The observed infection chain of Earth Kasha's latest campaign in March 2025.

## Initial Access

The attack begins with a spear-phishing email: we have observed cases where the malicious emails were sent from a legitimate account, suggesting that compromised accounts could have been abused to deliver the malicious emails. The email embeds a OneDrive URL link that downloads a ZIP file which contains a malicious Excel file. The Excel filename and email subject are designed to capture the target's interest. Some of file names and email subjects used in this campaign are listed below:

- <REDACTED>_修正済み履歴書 (Japanese translated to English: <REDACTED>_Revised Resume)
- 臺日道路交通合作與調研相關公務出國報告 (Taiwanese translated to English: Report on Official Business Trips Abroad Related to Taiwan-Japan Road Transportation Cooperation and Research)
- 應徵研究助理-<REDACTED> (Taiwanese translated to English: Research Assistant Application-<REDACTED>)

## Dropper

The malicious Excel file is a macro-enabled dropper that we call ROAMINGMOUSE. Since the Earth Kasha's 2024 campaign, ROAMINGMOUSE has been used as an initial dropper to drop the ANEL components by implementing a simple sandbox evasion technique requiring user manipulation to trigger the malicious routine.

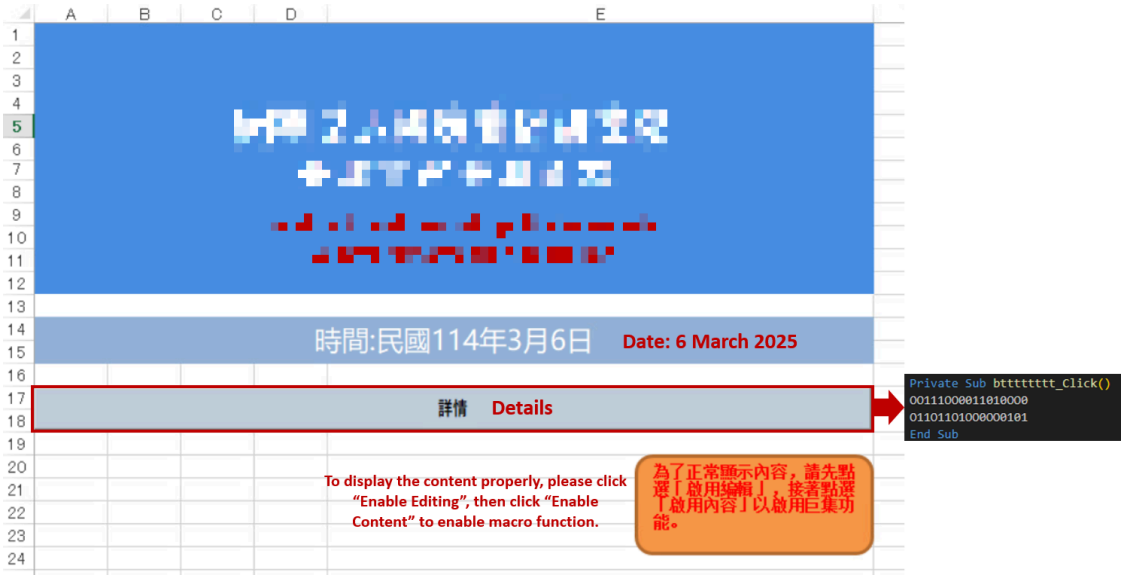


Figure 2. The malicious Excel file requires user manipulation to drop the ANEL components.

The use of a malicious Excel file is different from Earth Kasha's 2024 campaign where they used a malicious Word file. Apart from the change in file type, the malicious routine trigger was also switched from a mousemove event to the click event.

ROAMINGMOUSE then decodes the embedded ZIP file by using *Base64*, drops the ZIP on a disk, and expands its components. In this campaign, ROAMINGMOUSE dropped the following components:

- JSLNTOOL.exe, JSTIEE.exe, or JSVWMNG.exe: A legitimate application signed by 株式会社ジャストシステム (JustSystems Inc.)
- JSFC.dll: A malicious loader, dubbed ANELLDR
- <RANDOM>: An encrypted ANEL payload
- MSVCR100.dll: A legitimate DLL, dependency of EXE

The components were dropped onto following file paths:

- %LOCALAPPDATA%\Microsoft\Windows\<RANDOM>
- %LOCALAPPDATA%\Microsoft\Media Player\Transcoded Files Cache\<RANDOM>

After dropping the components, ROAMINGMOUSE launches the legitimate EXE as an argument of *explorer.exe* via WMI. The EXE then loads a malicious DLL, *JSFC.dll*, in the same directory via DLL sideloading.

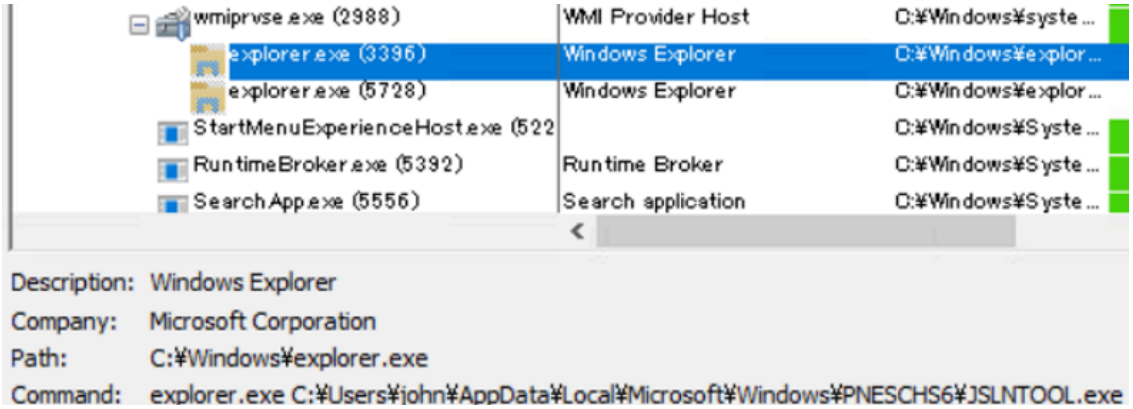


Figure 3. ROAMINGMOUSE launches the legitimate EXE as an argument of explorer.exe via WMI.

A notable observation from our investigation is that if ROAMINGMOUSE detects an installation of McAfee application, it changes its execution method to create a batch file in the startup folder that executes a legitimate EXE as an argument of *explorer.exe* without WMI.

## First stage backdoor: ANEL

*JSFC.dll*, a malicious loader dubbed ANELLDR, was observed in this campaign. It mostly has the same capabilities as the loader used in Earth Kasha's previous campaign. It decrypts an encrypted ANEL blob file in the same directory by using *AES-256-CBC* and LZO, and executes the ANEL in memory.

The ANEL file is known to embed its version number, which can help to understand how it evolves. However, since Earth Kasha's previous campaign in 2024, the ANEL file has been observed to have its version number encrypted. The ANEL file we observed in this new campaign also encrypted its version number.

```
sub_100068EE((void *)"&", 1u);
sub_1000C56C(&v44);
v69 = 42;
sub_1000176E("p6YlItx/H0BINIVSp0CSQfeaNC5z2q1yPoMSQ1iV+3w=");
v9 = v62;
v10 = (const CHAR *)sub_1000911C(v61);
v69 = 43;
sub_10001966((int)v41, v10, v9);
v69 = 11;
sub_10001AF4(1, 0);
nullsub_1(&v44);
v39 = 0;
CurrentProcess = GetCurrentProcess();
v12 = IsWow64Process(CurrentProcess, &v39);
if ( v12 == v39 && v12 )
{
  v69 = 44;
  sub_100068EE(" wow64", 6u);
}
```

Figure 4. The ANEL blob file now has its version number encrypted.

As for capabilities, it should be noted that there are no significant changes on command and control (C&C) communication protocols: this campaign continues to use a combination of custom ChaCha20, XOR, and LZO. However, we found that the ANEL file from the 2025 campaign implemented a new command to support the execution of a BOF (Beacon Object File) in memory. Table 1 summarizes the changes of supported commands on each ANEL file version.

| | 5.5.5 rev1 | 5.5.5 rev1 | 5.5.6 rev1 | 5.5.7 rev1 | unknown (2024-09) | unknown (2025-03) |
|---|---|---|---|---|---|---|
| 0x97A168D9697D40DD (download) | ✔ | ✔ | ✔ | ✔ | ✔ | ✔ |
| 0x7CF812296CCC68D5 (upload) | ✔ | ✔ | ✔ | ✔ | ✔ | ✔ |
| 0x652CB1CEFF1C0A00 (in-memory PE exec) | ✔ | ✔ | ✔ | ✔ | ✔ | ✔ |
| 0x27595F1F74B55278 (download and exec) | ✔ | ✔ | ✔ | ✔ | ✔ | ✔ |
| 0xD290626C85FB1CE3 (sleep) | ✔ | ✔ | ✔ | ✔ | ✔ | ✔ |
| 0x409C7A89CFF0A727 (get screenshot) | ✔ | ✔ | ✔ | ✔ | ✔ | ✔ |
| 0x596813980E83DAE6 (UAC bypass) | — | — | ✔ | ✔ | ✔ | — |
| 0x2BF5C7D6A162809 (BOF execution) | — | — | — | — | — | ✔ |
| Else (execute command) | ✔ | ✔ | ✔ | ✔ | ✔ | ✔ |



Table 1. A summary of the changes of supported commands on each ANEL file version

## ANEL backdoor post-exploitation

After installing the ANEL file, actors behind Earth Kasha obtained screenshots using a backdoor command and examined the victim's environment. To do this, we observed that the following commands were used:

- tasklist /v
- net localgroup administrators
- net user

The adversary appears to investigate the victim by looking through screenshots, running process lists, and domain information. We assume this is to find out whether they have infiltrated an intended target, as there are several cases where the threat actors did not proceed with the second stage backdoor. In the cases that they did proceed with the second stage backdoor, we observed that they downloaded NOOPDOOR components onto the *C:\ProgramData* folder using a backdoor command and executed it using following commands:

cmd /c C:\Windows\Microsoft.NET\Framework64\v4.0.30319\MSBuild.exe C:\ProgramData\ctac.xml

We also observed that Earth Kasha in this latest campaign potentially leveraged SharpHide for persistence: to launch NOOPDOOR through the Hidden Start (*hstart64.exe*), and to hide a UI of MSBuild on autorun. It possibly

injects SharpHide in the legitimate application process since the "*msiexec.exe*" was verified as legitimate, as can be observed in the following command:

C:\WINDOWS\system32\msiexec.exe action=create keyvalue="C:\ProgramData\hstart64.exe" arguments="/NOCONSOLE \"C:\Windows\Microsoft.NET\Framework64\v4.0.30319\MSBuild.exe C:\ProgramData\ctac.xml\""

Earth Kasha then removed the ANEL working directories by using following commands:

rd /s /q "C:\Users\<REDUCTED>\AppData\Local\Microsoft\Media Player\Transcoded Files Cache\<RANDOM>"

rd /s /q "C:\Users\<REDUCTED>\AppData\Local\Microsoft\Windows\<RANDOM>"

## Second stage backdoor: NOOPDOOR

We also observed that the adversary installed NOOPDOOR as its second-stage backdoor; NOOPDOOR is the sophisticated backdoor exclusively used by Earth Kasha since at least 2021. NOOPDOOR has been observed to continuously evolve by adding or removing minor features. An interesting update observed in NOOPDOOR during this campaign is that it supports to use DNS over HTTPS (DoH).

DoH is a relatively new technology to secure the user's privacy by resolving IP address over HTTPS, instead of DNS that doesn't support encryption. The new version of NOOPDOOR is designed to hide its IP lookup using the DoH protocol during C&C. NOOPDOOR embeds public DNS servers supporting DoH, such as Google and Cloudflare.

```
strcpy(
  v6,
  "https://dns.google/resolve?name= https://cloudflare-dns.com/dns-query?name= https://8.8.4.4/resolve?name= https://1."
  "1.1.1/dns-query?name=");
```

Figure 5. NOOPDOOR hides its IP lookup by using DNS over HTTPS (DoH).

NOOPDOOR generates a C&C domain through Domain Generation Algorithm (DGA) based on the current datetime as we have described in our previous blog, and then tries to resolve IP over DoH to hide suspicious domain name resolutions. Figure 6 illustrates how DoH works to get an IP. The result of DNS resolution will be returned in the HTTPS body.


Figure 6. NOOPDOOR tries to resolve IP over DoH to hide suspicious domain name resolutions.

## Conclusion and security recommendations

Earth Kasha continues to be an active advanced persistent threat and is now targeting government agencies and public institutions in Taiwan and Japan in its latest campaign which we detected in March 2025. Malicious actors behind the group continue to use spear-phishing to target their victims but employ slightly modified TTPs from their previous campaigns. A malicious Excel file now carries ROAMINGMOUSE, when before they used a Word file; additionally, the malicious routine trigger was also switched from a mousemove event to the click event.

The ANEL file we observed in this new campaign encrypts its version number like the ANEL file version from Earth Kasha's previous campaign in 2024, but we found that the ANEL file from the 2025 campaign implemented a new command to support an execution of BOF (Beacon Object File) in memory. This latest campaign also potentially leveraged SharpHide for persistence: to launch the second stage backdoor NOOPDOOR through the Hidden Start (hstart64.exe), and to hide a UI of MSBuild on autorun.

Enterprises and organizations, especially those with high-value assets like sensitive data relating to governance, as well as intellectual property, infrastructure data, and access credentials should continue to be vigilant and implement proactive security measures to prevent falling victim to cyberattacks. We recommend the following measures so enterprises can help secure against the TTPs discussed in this blog:

- Educate users on the risks of selecting and opening external or unrecognized OneDrive links and implement a zero-trust policy when interacting with such links and files on unrecognized emails.

- Monitor potential abuse of DNS over HTTPS.
- Disable macros downloaded from the internet.
- Maximize endpoint detection response tools to detect suspicious activity.

Proactive security with Trend Vision One™

Trend Vision Oneone-platform™ 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 Vision One customers can access a range of Intelligence Reports and Threat Insights. Threat Insights helps customers stay ahead of cyber threats before they happen and allows them to prepare for emerging threats by offering comprehensive information on threat actors, their malicious activities, and their techniques. By leveraging this intelligence, customers can take proactive steps to protect their environments, mitigate risks, and effectively respond to threats.

**Trend Vision One Intelligence Reports App [IOC Sweeping]**

Still in the Game: Earth Kasha's Continued Spear-Phishing Campaign targeting Taiwan and Japan

**Trend Vision One Threat Insights App**

Emerging Threats: Still in the Game: Earth Kasha's Continued Spear-Phishing Campaign targeting Taiwan and Japan

Threat Actor: Earth Kasha

**Hunting Query**

eventName:MALWARE_DETECTION AND (malName:*ROAMINGMOUSE*  OR malName:*ANEL* OR malName:*NOOPLDR* OR malName:*NOOPDOOR*)

eventSubId: 301 AND (hostName: *.srmbr.net OR hostName: *.kyolpon.com)

eventSubId: 204 AND (dst: 172.233.73.249 OR dst: 172.105.62.188 OR dst: 192.46.215.56 OR dst: 139.162.38.102)

## Indicators of Compromise (IoC)

Download the list of IoCs here.

Tags

---