

Operation AkaiRyū: MirrorFace invites Europe to Expo 2025 and revives ANEL backdoor

 welivesecurity.com/en/eset-research/operation-akairyu-mirrorface-invites-europe-expo-2025-revives-anel-backdoor/

ESET Research

ESET researchers uncovered MirrorFace activity that expanded beyond its usual focus on Japan and targeted a Central European diplomatic institute with the ANEL backdoor



Dominik Breitenbacher

18 Mar 2025 , 21 min. read



In August 2024, ESET researchers detected cyberespionage activity carried out by the China-aligned MirrorFace advanced persistent threat (APT) group against a Central European diplomatic institute in relation to Expo 2025, which will be held in Osaka, Japan.

Known primarily for its cyberespionage activities against organizations in Japan, to the best of our knowledge, this is the first time MirrorFace intended to infiltrate a European entity. The campaign, which we uncovered in Q2 and Q3 of 2024 and named Operation AkaiRyū (Japanese

for RedDragon), showcases refreshed tactics, techniques, and procedures (TTPs) that we observed throughout 2024: the introduction of new tools (such as a customized AsyncRAT), the resurrection of ANEL, and a complex execution chain.

In this blogpost, we present details of the Operation AkaiRyū attacks and findings from our investigation of the diplomatic institute case, including data from our forensic analysis. ESET Research presented the results of this analysis at the [Joint Security Analyst Conference \(JSAC\)](#) in January 2025.

Key points of this blogpost:

- MirrorFace has refreshed its TTPs and tooling.
- MirrorFace has started using ANEL, a backdoor previously associated exclusively with APT10.
- MirrorFace has started deploying a heavily customized variant of AsyncRAT, using a complex execution chain to run it inside Windows Sandbox.
- To our knowledge, MirrorFace targeted a European entity for the first time.
- We collaborated with the affected Central European diplomatic institute and performed a forensic investigation.
- The findings obtained during that investigation have provided us with better insight into MirrorFace's post-compromise activities.

MirrorFace profile

MirrorFace, also known as Earth Kasha, is a China-aligned threat actor until now almost exclusively targeting companies and organizations in Japan but also some located elsewhere that have relationships with Japan. As explained in this blogpost, we now consider MirrorFace to be a subgroup under the APT10 umbrella. MirrorFace has been active since at least 2019 and has been reported to target media, defense-related companies, think tanks, diplomatic organizations, financial institutions, academic institutions, and manufacturers. In 2022, we [discovered](#) a MirrorFace spearphishing campaign targeting Japanese political entities.

MirrorFace focuses on espionage and exfiltration of files of interest; it is the only group known to use the LODEINFO and HiddenFace backdoors. In the 2024 activities analyzed in this blogpost, MirrorFace started using APT10's former signature backdoor, ANEL, in its operations as well.

Overview

Much like previous MirrorFace attacks, Operation AkaiRyū began with carefully crafted spearphishing emails designed to entice recipients to open malicious attachments. Our findings suggest that despite this group's foray beyond the borders of its usual hunting ground, the threat actor still maintains a strong focus on Japan and events tied to the country. However, this is not the first time MirrorFace has been reported to operate outside of Japan: [Trend Micro](#) and the [Vietnamese National Cyber Security Center](#) (document in Vietnamese) reported on such cases in Taiwan, India, and Vietnam.

ANEL's comeback

During our analysis of Operation AkaiRyū, we discovered that MirrorFace has significantly refreshed its TTPs and tooling. MirrorFace started using ANEL (also referred to as UPPERCUT) – a backdoor considered exclusive to APT10 – which is surprising, as it was believed that ANEL was abandoned around the end of 2018 or the start of 2019 and that LODEINFO succeeded it, appearing later in 2019. The small difference in version numbers between 2018 and 2024 ANELs, 5.5.0 and 5.5.4, and the fact that APT10 used to update ANEL every few months, strongly suggest that the development of ANEL has restarted.

The use of ANEL also provides further evidence in the ongoing debate about the potential connection between MirrorFace and APT10. The fact that MirrorFace has started using ANEL, and the other previously known information, such as similar targeting and malware code similarities, led us to make a change in our attribution: we now believe that MirrorFace is a subgroup under the APT10 umbrella. This attribution change aligns our thinking with other researchers who already consider MirrorFace to be a part of APT10, such as those at Macnica (report in Japanese), Kaspersky, ITOCHU Cyber & Intelligence Inc., and Cybereason. Others, as at Trend Micro, as of now still consider MirrorFace to be only potentially related to APT10.

First use of AsyncRAT and Visual Studio Code by MirrorFace

In 2024, MirrorFace also deployed a heavily customized variant of AsyncRAT, embedding this malware into a newly observed, intricate execution chain that runs the RAT inside Windows Sandbox. This method effectively obscures the malicious activities from security controls and hampers efforts to detect the compromise.

In parallel to the malware, MirrorFace also started deploying Visual Studio Code (VS Code) to abuse its remote tunnels feature. Remote tunnels enable MirrorFace to establish stealthy access to the compromised machine, execute arbitrary code, and deliver other tools. MirrorFace is not the only APT group abusing VS Code: Tropic Trooper and Mustang Panda have also been reported using it in their attacks.

Additionally, MirrorFace continued to employ its current flagship backdoor, HiddenFace, further bolstering persistence on compromised machines. While ANEL is used by MirrorFace as the first-line backdoor, right after the target has been compromised, HiddenFace is deployed in the later stages of the attack. It is also worth noting that in 2024 we didn't observe any use of LODEINFO, another backdoor used exclusively by MirrorFace.

Forensic analysis of the compromise

We contacted the affected institute to inform them about the attack and to clean up the compromise as soon as possible. The institute collaborated closely with us during and after the attack, and additionally provided us with the disk images from the compromised machines. This enabled us to perform forensic analyses on those images and uncover further MirrorFace activity.

ESET Research provided more technical details about ANEL's return to [ESET Threat Intelligence](#) customers on September 4th, 2024. Trend Micro [published](#) their findings on then-recent MirrorFace activities on October 21st, 2024 in Japanese and on November 26th, 2024 in English: these overlap with Operation AkaiRyū and also mention the return of the ANEL backdoor. Furthermore, in January 2025, the Japanese National Police Agency (NPA) published a [warning](#) about MirrorFace activities to organizations, businesses, and individuals in Japan. Operation AkaiRyū corresponds with Campaign C, as mentioned in the [Japanese version](#) of NPA's warning. However, NPA mentions the targeting of Japanese entities exclusively – individuals and organizations mainly related to academia, think tanks, politics, and the media.

In addition to Trend Micro's report and NPA's warning, we provide an exclusive analysis of MirrorFace post-compromise activities, which we were able to observe thanks to the close cooperation of the affected organization. This includes the deployment of a heavily customized AsyncRAT, abuse of VS Code remote tunnels, and details on the execution chain that runs malware inside Windows Sandbox to avoid detection and hide the performed actions.

In this blogpost, we cover two distinct cases: a Central European diplomatic institute and a Japanese research institute. Even though MirrorFace's overall approach is the same in both cases, there are notable differences in the initial access process; hence we describe them both.

Technical analysis

Between June and September 2024, we observed MirrorFace conducting multiple spearphishing campaigns. Based on our data, the attackers primarily gained initial access by tricking targets into opening malicious attachments or links, then they leveraged legitimate applications and tools to stealthily install their malware.

Initial access

We weren't able to determine the initial attack vector for all the cases observed in 2024. However, based on the data available to us, we assume that spearphishing was the only attack vector used by MirrorFace. The group impersonates trusted organizations or individuals to convince recipients to open documents or click links. The following findings on initial access align with those in the Trend Micro article, although they are not entirely the same.

Specifically, in Operation AkaiRyū, MirrorFace abused both McAfee-developed applications and also one developed by JustSystems to run ANEL. While Trend Micro reported Windows Management Instrumentation (WMI) and explorer.exe as the execution proxy pair for ANEL, we unearthed another pair: WMI and wlrmdr.exe (Windows logon reminder). We also provide an email conversation between a disguised MirrorFace operator and a target.

Case 1: Japanese research institute

On June 20th, 2024, MirrorFace targeted two employees of a Japanese research institute, using a malicious, password-protected Word document delivered in an unknown manner.

The documents triggered VBA code on a simple mouseover event – the malicious code was triggered by moving the mouse over text boxes placed in the document. It then abused a signed McAfee executable to load ANEL (version 5.5.4) into memory. The compromise chain is depicted in Figure 1.

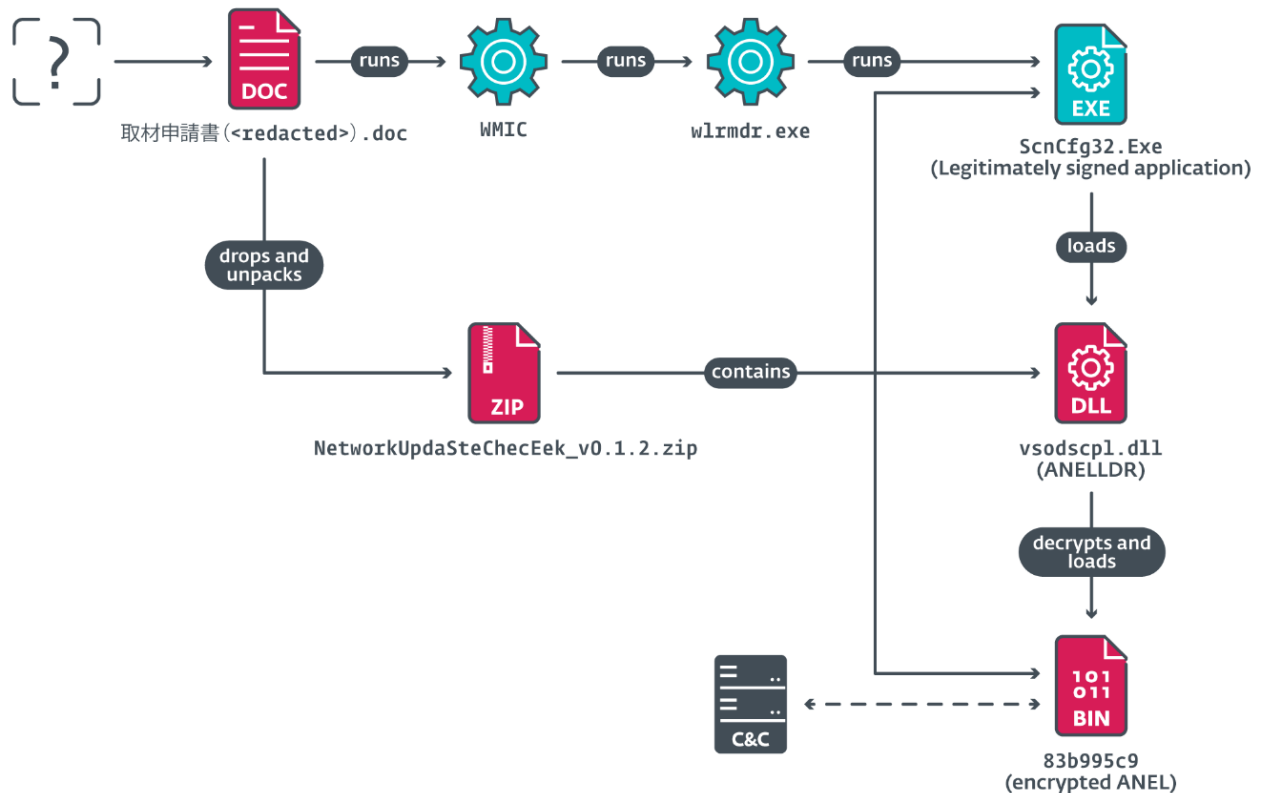


Figure 1. Compromise chain observed in June 2024

Case 2: Central European diplomatic institute

On August 26th, 2024, MirrorFace targeted a Central European diplomatic institute. To our knowledge, this is the first, and, to date, only time MirrorFace has targeted an entity in Europe.

MirrorFace operators set up their spearphishing attack by crafting an email message (shown in Figure 2) that references a previous, legitimate interaction between the institute and a Japanese NGO. The legitimate interaction was probably obtained from a previous campaign. As can be seen, this spearphishing set up message refers to the upcoming Expo 2025 exhibition, an event that will be held in Japan.



[Redacted] <andryfrewas@gmail.com> [Redacted]

Greeting from Tokyo

Dear [Redacted]-san,

I hope this email finds you well.

I have some references about the EXPO Exhibition in Japan in 2025, if you are interested please reply to this email and I will send it to you.

Best,
[Redacted]

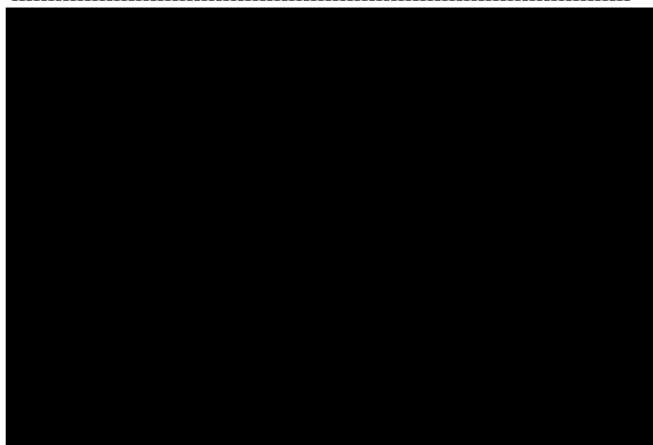



Figure 2. The first email sent to the target

This first email was harmless, but once the target responded, MirrorFace operators sent an email message with a malicious OneDrive link leading to a ZIP archive with a LNK file disguised as a Word document named The EXPO Exhibition in Japan in 2025.docx.lnk. This second message is shown in Figure 3. Using this approach, MirrorFace concealed the payload until the target was engaged in the spearphishing scheme.



[REDACTED] <andryfrewas@gmail.com> | [REDACTED]

Re: Greeting from Tokyo

 If there are problems with how this message is displayed, click here to view it in a web browser.
Click here to download pictures. To help protect your privacy, Outlook prevented automatic download of some pictures in this message.

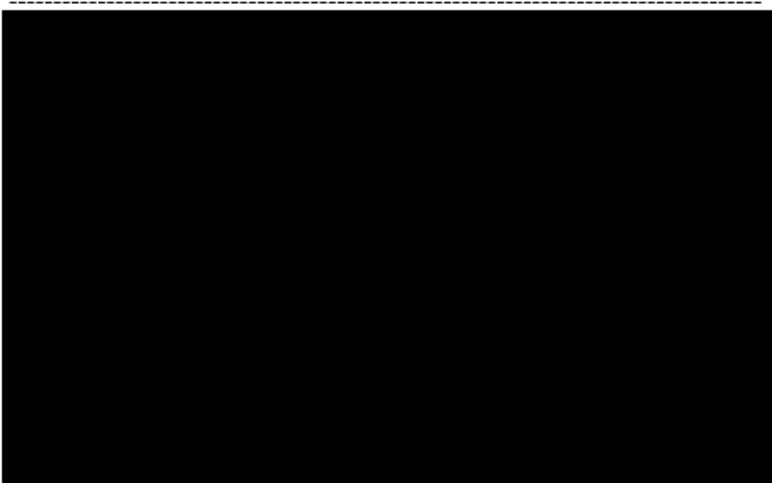


[The EXPO Exhibition in Japan in 2025](#)

Dear [REDACTED]-san,

I'm sending you the information about the EXPO Exhibition in Japan in 2025.
I wish you all the best.

[REDACTED]



2024年8月26日(月) 16:18 [REDACTED]:

Dear [REDACTED] - san,

Thank you very much for your email and looking forward to hearing new informations from you.

My best wishes to Tokyo,

[REDACTED]

[REDACTED]

CEO & Co-Founder

[REDACTED]

Figure 3. Second email sent by MirrorFace, containing a link to a malicious ZIP archive hosted on OneDrive

Once opened, the LNK file launches a complex compromise chain, depicted in Figure 4 and Figure 5.

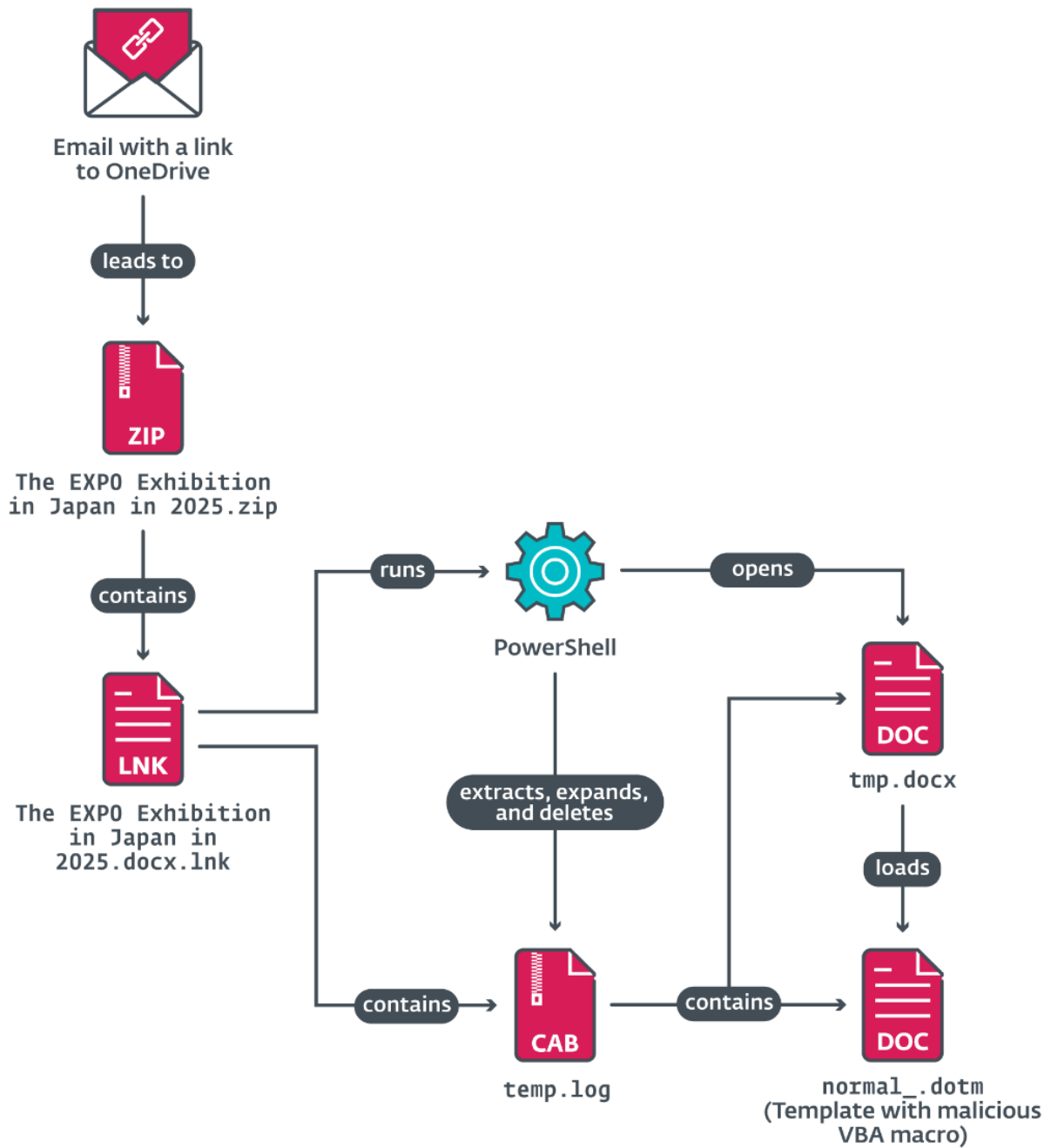


Figure 4 . First part of the compromise chain

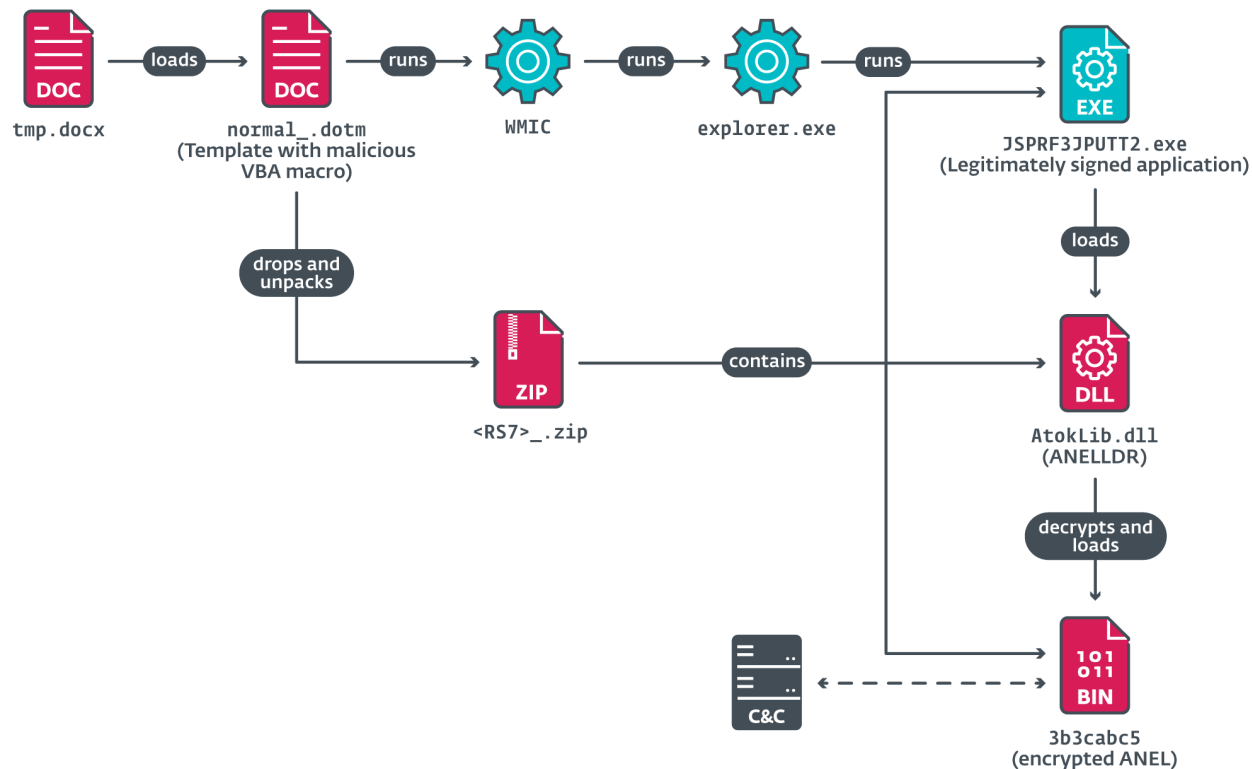


Figure 5. Second part of the compromise chain

The LNK file runs cmd.exe with a set of PowerShell commands to drop additional files, including a malicious Word file, tmp.docx, which loads a malicious Word template, normal_.dotm, containing VBA code. The contents of the Word document tmp.docx are depicted in Figure 6, and probably are intended to act as a decoy, while malicious actions are running in the background.

The EXPO Exhibition in Japan in 2025

Figure 6. Contents of the deceptive tmp.docx document shown to the target

The VBA code extracts a legitimately signed application from JustSystems Corporation to side-load and decrypt the ANEL backdoor (version 5.5.5). This gave MirrorFace a foothold to begin post-compromise operations.

Toolset

In Operation AkaiRyū, MirrorFace relied not only on its custom malware, but also on various tools and a customized variant of a publicly available remote access trojan (RAT).

ANEL

ANEL (also known as UPPERCUT) is a backdoor that was previously associated exclusively with APT10. In 2024, MirrorFace started using ANEL as its first-line backdoor. ANEL's development, until 2018, was described most recently in Secureworks' [JSAC 2019 presentation](#). The ANEL variants observed in 2024 were publicly described by [Trend Micro](#).

ANEL is a backdoor, only found on disk in an encrypted form, and whose decrypted DLL form is only ever found in memory once a loader has decrypted it in preparation for execution. ANEL communicates with its C&C server over HTTP, where the transmitted data is encrypted to protect it in case the communication is being captured. ANEL supports basic commands for file manipulation, payload execution, and taking a screenshot.

ANELLDR

ANELLDR is a loader exclusively used to decrypt the ANEL backdoor and run it in memory. Trend Micro described ANELLDR in their [article](#).

HiddenFace

HiddenFace is MirrorFace's current flagship backdoor, with a heavy focus on modularity; we described it in detail in this [JSAC 2024 presentation](#).

FaceXInjector

FaceXInjector is a C# injection tool stored in an XML file, compiled and executed by the Microsoft MSBuild utility, and used to exclusively execute HiddenFace. We described FaceXInjector in the same JSAC 2024 presentation dedicated to HiddenFace.

AsyncRAT

AsyncRAT is a RAT publicly available on [GitHub](#). In 2024, we detected that MirrorFace started using a heavily customized AsyncRAT in the later stages of its attacks. The group ensures AsyncRAT's persistence by registering a scheduled task that executes at machine startup; once triggered, a complex chain (depicted in Figure 7) launches AsyncRAT inside Windows Sandbox, which must be manually enabled and requires a reboot. We were unable to determine how MirrorFace enables this feature.

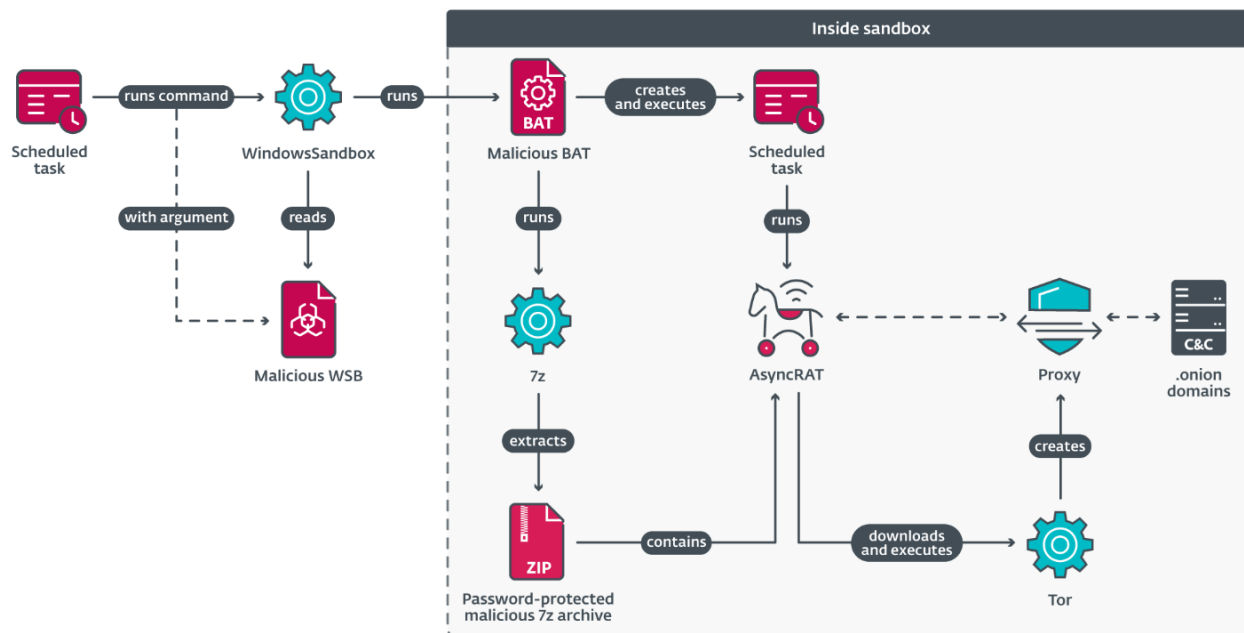


Figure 7. AsyncRAT execution chain

The following files are delivered to the compromised machine in order to successfully execute AsyncRAT:

- 7z.exe – legitimate 7-Zip executable.
- 7z.dll – legitimate 7-Zip library.
- <random>.7z – password-protected 7z archive containing AsyncRAT, named setup.exe.
- <random>.bat – batch script that unpacks AsyncRAT and runs it.
- <random>.wsb – Windows Sandbox configuration file to run <random>.bat.

The triggered scheduled task executes Windows Sandbox with <random>.wsb as a parameter. This file contains configuration data for the sandbox; see Figure 8.

```

1  <Configuration>
2    <Networking>Enable</Networking>
3    <MappedFolders>
4      <MappedFolder>
5        <HostFolder>C:\Users</HostFolder>
6        <SandboxFolder>C:\HostFiles</SandboxFolder>
7        <ReadOnly>>false</ReadOnly>
8      </MappedFolder>
9    </MappedFolders>
10   <LogonCommand>
11     <Command>C:\HostFiles\{49D82E3-CBB6-0486-6645-A4EFD285629}\erBkVRZT.bat</Command>
12   </LogonCommand>
13   <MemoryInMB>1024</MemoryInMB>
14 </Configuration>
15

```

Figure 8. Contents of a Windows Sandbox config file used by MirrorFace

In particular, the config file defines whether to enable networking and directory mapping, the dedicated memory size, and the command to execute on launch. In the file shown in Figure 8, a batch file located in the sandbox folder is executed. The batch file extracts AsyncRAT from the 7z

archive, then creates and launches a scheduled task that executes AsyncRAT every hour.

The AsyncRAT variant used by MirrorFace is heavily customized. The following are the main features and changes introduced by MirrorFace:

- **Sample tagging** – AsyncRAT can be compiled for a specific victim and MirrorFace can add a tag to the configuration to mark the sample. If the tag is not specified, the machine's NetBIOS name is used as the tag. This tag is further used in other introduced features as well.
- **Connection to a C&C server via Tor** – MirrorFace's AsyncRAT can download and start a Tor client, and proxy its communication with a C&C server through the client. AsyncRAT selects this option only if the hardcoded C&C domains end with .onion. This approach was selected in both samples we observed during the investigation of *Case 2: Central European diplomatic institute*.
- **Domain generation algorithm (DGA)** – An alternative to using Tor, this variant can use a DGA to generate a C&C domain. The DGA can also generate machine-specific domains using the aforementioned tag. Note that HiddenFace also uses a DGA with the possibility of generating machine-specific domains, although the DGA used in HiddenFace differs from the AsyncRAT one.
- **Working time** – Before connecting to a C&C server, AsyncRAT checks whether the current hour and day of the week are within operating hours and days defined in the configuration. Note that MirrorFace's AsyncRAT shares this feature with HiddenFace as well.

Visual Studio Code remote tunnels

Visual Studio Code is a free source-code editor developed by Microsoft. Visual Studio Code's remote development feature, *remote tunnels*, allows developers to run Visual Studio Code locally and connect to a development machine that hosts the source code and debugging environment. Threat actors can misuse this to gain remote access, execute code, and deliver tools to a compromised machine. MirrorFace has been doing so since 2024; however, it is not the only APT group that has used such remote tunnels: other China-aligned APT groups such as *Tropic Trooper* and *Mustang Panda* have also used them in their attacks.

Post-compromise activities

Our investigation into *Case 2: Central European diplomatic institute* uncovered some of MirrorFace's post-compromise activities. Through close collaboration with the institute, we gained better insight into the malware and tools deployed by MirrorFace, as seen in Table 1.

Note that the malware and tools are ordered in the table for easier comparison of what was deployed on each of the two identified compromised machines but doesn't reflect how they were deployed chronologically.

Table 1. Malware and tools deployed by MirrorFace throughout the attack

Tools	Notes	Machine A	Machine B
ANEL	APT10's backdoor that MirrorFace uses as a first-line backdoor.	•	•
PuTTY	An open-source terminal emulator, serial console, and network file transfer application.	•	•
VS Code	A code editor developed by Microsoft.	•	•
HiddenFace	MirrorFace's flagship backdoor.	•	•
Second HiddenFace variant	MirrorFace's flagship backdoor.	•	
AsyncRAT	RAT publicly available on GitHub .	•	•
Hidden Start	A tool that can be used to bypass UAC, hide Windows consoles, and run programs in the background.	•	
csvde	Legitimate Microsoft tool available on Windows servers that imports and exports data from Active Directory Domain Services (AD DS).		•
Rubeus	Toolset for Kerberos interaction and abuse, publicly available on GitHub .		•
frp	Fast reverse proxy publicly available on GitHub .		•
Unknown tool	Disguised under the name oneuu.exe. We were unable to recover the tool during our analysis.		•

The group selectively deployed post-compromise tools according to its objectives and the target's environment. Machine A belonged to a project coordinator and Machine B to an IT employee. The data available to us suggests that MirrorFace stole personal data from Machine A and sought deeper network access on Machine B, aligning the assumed objectives with the employees' roles.

Day 0 – August 27th, 2024

MirrorFace operators sent an email with a malicious link on August 26th, 2024 to the institute's CEO. However, since the CEO didn't have access to a machine running Windows, the CEO forwarded the email to two other employees. Both opened the harmful LNK file, The EXPO Exhibition in Japan in 2025.docx.lnk, the next day, compromising two institute machines and leading to the deployment of ANEL. Thus, we consider August 27th, 2024, as Day 0 of the compromise. No additional activity was observed beyond this foothold establishment.

Day 1 – August 28th, 2024

The next day, MirrorFace returned and continued with its activities. The group deployed several tools for access, control, and file delivery on both compromised machines. Among the tools deployed were PuTTY, VS Code, and HiddenFace – MirrorFace’s current flagship backdoor. On Machine A, MirrorFace also attempted to deploy the tool Hidden Start. On Machine B, the actor additionally deployed csvde and the customized variant of AsyncRAT.

Day 2 – August 29th, 2024

On Day 2, MirrorFace was active on both machines. This included deploying more tools. On Machine A, MirrorFace deployed a second instance of HiddenFace. On Machine B, VS Code’s remote tunnel, HiddenFace, and AsyncRAT were executed. Besides these, MirrorFace also deployed and executed frp and Rubeus via HiddenFace. This is the last day on which we observed any MirrorFace activity on Machine B.

Day 3 – August 30th, 2024

MirrorFace remained active only on Machine A. The institute, having started attack mitigation measures on August 29th, 2024, might have prevented further MirrorFace activity on Machine B. On Machine A, the group deployed AsyncRAT and tried to maintain persistence by registering a scheduled task.

Day 6 – September 2nd, 2024

Over the weekend, i.e., on August 31st and September 1st, 2024, Machine A was inactive. On Monday, September 2nd, 2024, Machine A was booted and with it MirrorFace’s activity resumed as well. The main event of Day 6 was that the group exported Google Chrome’s web data such as contact information, keywords, autofill data, and stored credit card information into a SQLite database file. We were unable to determine how MirrorFace exported the data, and whether or how the data was exfiltrated.

Conclusion

In 2024, MirrorFace refreshed its TTPs and tooling. It started using ANEL – believed to have been abandoned around 2018/2019 – as its first-line backdoor. Combined with other information, we conclude that MirrorFace is a subgroup under the APT10 umbrella. Besides ANEL, MirrorFace has also started using other tools such as a heavily customized AsyncRAT, Windows Sandbox, and VS Code remote tunnels.

As a part of Operation AkaiRyū, MirrorFace targeted a Central European diplomatic institute – to the best of our knowledge, this is the first time the group has attacked an entity in Europe – using the same refreshed TTPs seen across its 2024 campaigns. During this attack, the threat actor used the upcoming World Expo 2025 – to be held in Osaka, Japan – as a lure. This shows that even considering this new *broader* geographic targeting, MirrorFace remains focused on Japan and events related to it.

Our close collaboration with the affected organization provided a rare, in-depth view of post-compromise activities that would have otherwise gone unseen. However, there are still a lot of missing pieces of the puzzle to draw a complete picture of the activities. One of the reasons is MirrorFace's improved operational security, which has become more thorough and hinders incident investigations by deleting the delivered tools and files, clearing Windows event logs, and running malware in Windows Sandbox.

For any inquiries about our research published on WeLiveSecurity, please contact us at threatintel@eset.com.

ESET Research offers private APT intelligence reports and data feeds. For any inquiries about this service, visit the [ESET Threat Intelligence](#) page.

IoCs

A comprehensive list of indicators of compromise (IoCs) and samples can be found in [our GitHub repository](#).

Files

SHA-1	Filename	Detection	Description
018944FC47EE2329B23B74DA31B19E57373FF539	3b3cab5	Win32/MirrorFace.A	AES-encrypted ANEL.
68B72DA59467B1BB477D0C1C5107CEE8D9078E7E	vsodscpl.dll	Win32/MirrorFace.A	ANELLDR.
02D32978543B9DD1303E5B020F52D24D5EABA52E	AtokLib.dll	Win32/MirrorFace.A	ANELLDR.
2FB3B8099499FEE03EA7064812645AC781AFD502	CodeStartUser.bat	Win32/MirrorFace.A	Malicious batch file.
9B2B9A49F52B37927E6A9F4D6DDB180BE8169C5F	erBkVRZT.bat	Win32/MirrorFace.A	Malicious batch file.
AB65C08DA16A45565DBA930069B5FC5A56806A4C	useractivitybroker.xml	Win32/ FaceXInjector.A	FaceXInjector.
875DC27963F8679E7D8BF53A7E69966523BC36BC	temp.log	Win32/MirrorFace.A	Malicious CAB file.
694B1DD3187E876C5743A0E0B83334DBD18AC9EB	tmp.docx	Win32/MirrorFace.A	Decoy Word document loading malicious template normal_.dotm.

SHA-1	Filename	Detection	Description
F5BA545D4A1683675698 9A3AB32F3F6C5D5AD8FF	normal_.dotm	Win32/MirrorFace.A	Word template with malicious VBA code.
233029813051D20B61D0 57EC4A56337E9BEC40D2	The EXPO Exhibition in Japan in 2025.docx.lnk	Win32/MirrorFace.A	Malicious LNK file.
8361F7DBF81093928DA5 4E3CBC11A0FCC2EEB55A	The EXPO Exhibition in Japan in 2025.zip	Win32/MirrorFace.A	Malicious ZIP archive.
1AFDCE38AF37B9452FB4 AC35DE9FCECD5629B891	NK9C4PH_.zip	Win32/MirrorFace.A	Malicious ZIP archive.
E3DA9467D0C89A9312EA 199ECC83CDDF3607D8B1	N/A	MSIL/Riskware.Rubeus.A	Rubeus tool.
D2C25AF9EE6E60A341B0 C93DD97566FB532BFBE8	Tk4AJbXk.wsb	Win32/MirrorFace.A	Malicious Windows Sandbox configuration file.

Network

IP	Domain	Hosting provider	First seen	Details
N/A	vu4fleh3yd4ehpfpc iinnwbnh4b77rdeyp ubhqr2dgfibjtvxpd xozid[.]onion	N/A	2024-08-28	MirrorFace's AsyncRAT C&C server.
N/A	u4mrhg3y6jyfw2dmm 2wnocz3g3etp2xc5t hzx77uelk7mrk7qtj mc6qd[.]onion	N/A	2024-08-28	MirrorFace's AsyncRAT C&C server.
45.32.116[.]146	N/A	The Constant Company, LLC	2024-08-27	ANEL C&C server.
64.176.56[.]26	N/A	The Constant Company, LLC	N/A	Remote server for FRP client.
104.233.167[.]135	N/A	PEG-TKY1	2024-08-27	HiddenFace C&C server.

IP	Domain	Hosting provider	First seen	Details
152.42.202[.]137	N/A	DigitalOcean, LLC	2024-08-27	HiddenFace C&C server.
208.85.18[.]4	N/A	The Constant Company, LLC	2024-08-27	ANEL C&C server.

MITRE ATT&CK techniques

This table was built using version 16 of the MITRE ATT&CK framework.

Tactic	ID	Name	Description
Resource Development	<u>T1587.001</u>	Develop Capabilities: Malware	MirrorFace has developed custom tools such as HiddenFace.
	<u>T1585.002</u>	Establish Accounts: Email Accounts	MirrorFace created a Gmail account and used it to send a spearphishing email.
	<u>T1585.003</u>	Establish Accounts: Cloud Accounts	MirrorFace created a OneDrive account to host malicious files.
	<u>T1588.001</u>	Obtain Capabilities: Malware	MirrorFace utilized and customized a publicly available RAT, AsyncRAT, for its operations.
	<u>T1588.002</u>	Obtain Capabilities: Tool	MirrorFace utilized Hidden Start in its operations.
Initial Access	<u>T1566.002</u>	Phishing: Spearphishing Link	MirrorFace sent a spearphishing email with a malicious OneDrive link.
Execution	<u>T1053.005</u>	Scheduled Task/Job: Scheduled Task	MirrorFace used scheduled tasks to execute HiddenFace and AsyncRAT.
	<u>T1059.001</u>	Command-Line Interface: PowerShell	MirrorFace used PowerShell commands to run Visual Studio Code's remote tunnels.
	<u>T1059.003</u>	Command-Line Interface: Windows Command Shell	MirrorFace used the Windows command shell to ensure persistence for HiddenFace.
	<u>T1204.001</u>	User Execution: Malicious Link	MirrorFace relied on the target to download a malicious file from a shared OneDrive link.

Tactic	ID	Name	Description
	<u>T1204.002</u>	User Execution: Malicious File	MirrorFace relied on the target to run a malicious LNK file that deploys ANEL.
	<u>T1047</u>	Windows Management Instrumentation	MirrorFace used WMI as an execution proxy to run ANEL.
Persistence	<u>T1547.001</u>	Boot or Logon Autostart Execution: Registry Run Keys / Startup Folder	ANEL uses one of the startup directories for persistence.
	<u>T1574.001</u>	Hijack Execution Flow: DLL Search Order Hijacking	MirrorFace side-loads ANEL by dropping a malicious library and a legitimate executable (e.g., ScnCfg32.Exe)
Defense Evasion	<u>T1027.004</u>	Obfuscated Files or Information: Compile After Delivery	FaceXInjector is compiled on every scheduled task run.
	<u>T1027.007</u>	Obfuscated Files or Information: Dynamic API Resolution	HiddenFace dynamically resolves the necessary APIs upon its startup.
	<u>T1027.011</u>	Obfuscated Files or Information: Fileless Storage	HiddenFace is stored in a registry key on the compromised machine.
	<u>T1055</u>	Process Injection	FaceXInjector is used to inject HiddenFace into a legitimate Windows utility.
	<u>T1070.004</u>	Indicator Removal: File Deletion	Once HiddenFace is moved to the registry, the file in which it was delivered is deleted.
	<u>T1070.006</u>	Indicator Removal: Timestamp	HiddenFace can timestamp files in selected directories.
	<u>T1112</u>	Modify Registry	FaceXInjector creates a registry key into which it stores HiddenFace.
	<u>T1127.001</u>	Trusted Developer Utilities: MSBuild	MSBuild is abused to execute FaceXInjector.
	<u>T1140</u>	Deobfuscate/Decode Files or Information	HiddenFace reads external modules from an AES-encrypted file.
	<u>T1622</u>	Debugger Evasion	HiddenFace checks whether it is being debugged.

Tactic	ID	Name	Description
	<u>T1564.001</u>	Hide Artifacts: Hidden Files and Directories	MirrorFace hid directories with AsyncRAT.
	<u>T1564.003</u>	Hide Artifacts: Hidden Window	MirrorFace attempted to use the tool Hidden Start, which can hide windows.
	<u>T1564.006</u>	Hide Artifacts: Run Virtual Instance	MirrorFace used Windows Sandbox to run AsyncRAT.
	<u>T1070.001</u>	Indicator Removal: Clear Windows Event Logs	MirrorFace cleared Windows event logs to destroy evidence of its actions.
	<u>T1036.007</u>	Masquerading: Double File Extension	MirrorFace used a so-called double file extension, .docx.lnk, to deceive its target.
	<u>T1218</u>	Signed Binary Proxy Execution	MirrorFace used wlrmdr.exe as an execution proxy to run ANEL.
	<u>T1221</u>	Template Injection	MirrorFace used Word template injection to run malicious VBA code.
Discovery	<u>T1012</u>	Query Registry	HiddenFace queries the registry for machine-specific information such as the machine ID.
	<u>T1033</u>	System Owner/User Discovery	HiddenFace determines the currently logged in user's name and sends it to the C&C server.
	<u>T1057</u>	Process Discovery	HiddenFace checks currently running processes.
	<u>T1082</u>	System Information Discovery	HiddenFace gathers various system information and sends it to the C&C server.
	<u>T1124</u>	System Time Discovery	HiddenFace determines the system time and sends it to the C&C server.
	<u>T1087.002</u>	Account Discovery: Domain Account	MirrorFace used the tool csvde to export data from Active Directory Domain Services.
Collection	<u>T1115</u>	Clipboard Data	HiddenFace collects clipboard data and sends it to the C&C server.
	<u>T1113</u>	Screen Capture	ANEL can take a screenshot and send it to the C&C server.

Tactic	ID	Name	Description
Command and Control	<u>T1001.001</u>	Data Obfuscation: Junk Data	HiddenFace adds junk data to the messages sent to the C&C server.
	<u>T1568.002</u>	Dynamic Resolution: Domain Generation Algorithms	HiddenFace uses a DGA to generate C&C server domain names.
	<u>T1573</u>	Encrypted Channel	HiddenFace communicates with its C&C server over an encrypted channel.
	<u>T1071.001</u>	Standard Application Layer Protocol: Web Protocols	ANEL uses HTTP to communicate with its C&C server.
	<u>T1132.001</u>	Data Encoding: Standard Encoding	ANEL uses base64 to encode data sent to the C&C server.
Exfiltration	<u>T1030</u>	Data Transfer Size Limits	HiddenFace can, upon operator request, split data and send it in chunks to the C&C server.
	<u>T1041</u>	Exfiltration Over C2 Channel	HiddenFace exfiltrates requested data to the C&C server.



Copyright © ESET, All Rights Reserved