Hive Pro

Threat Level

Amber

Hiveforce Labs

THREAT ADVISORY

ATTACK REPORT

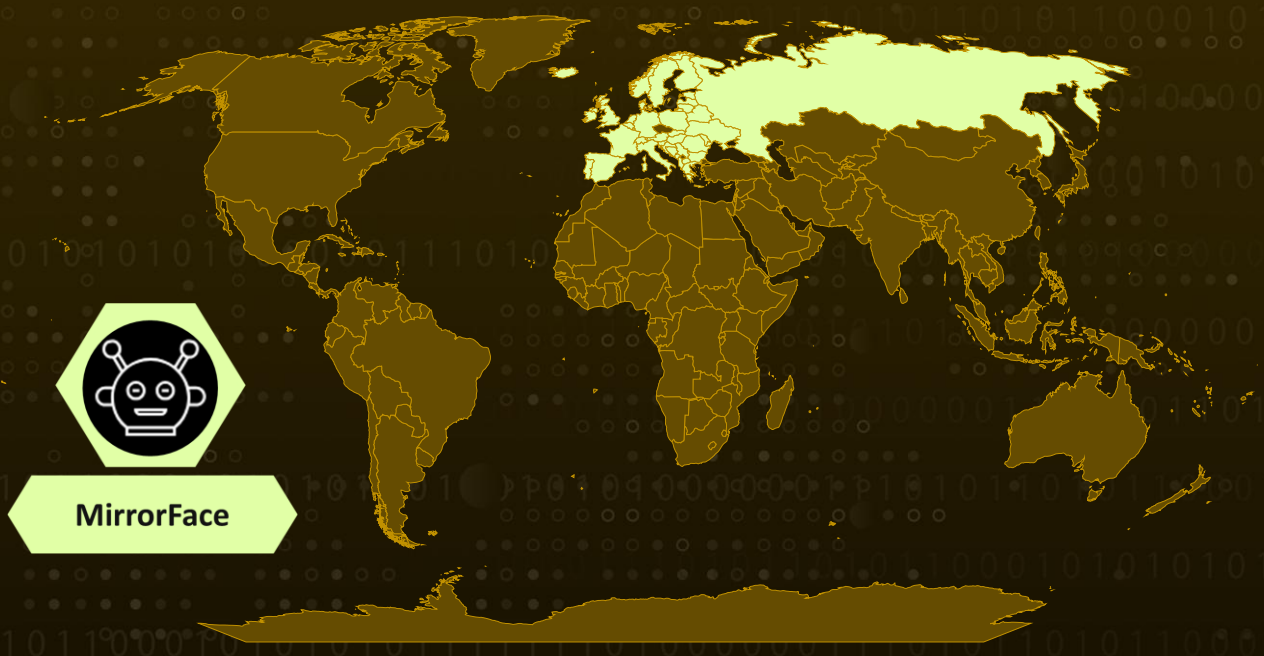
Operation AkaiRyū: MirrorFace Expands Cyberespionage to Europe with Revived Tools

Date of Publication	Admiralty Code	TA Number
March 19, 2025	A1	TA2025084

Summary

Attack Discovered: August 2024
Targeted Countries: Europe
Targeted Industry: Diplomatic Organization
Affected Platform: Windows
Actor: MirrorFace (aka Earth Kasha, Operation LiberalFace)
Malware: ANEL (aka UPPERCUT), AsyncRAT
Campaign: Operation AkaiRyū
Attack: In August 2024, a cyberespionage campaign by the China-aligned MirrorFace APT group was uncovered, marking its first known attempt to breach a European entity. Traditionally focused on Japan-linked targets, MirrorFace launched Operation AkaiRyū (Red Dragon in Japanese), unveiling a refreshed arsenal of tactics and tools. This campaign introduced a customized AsyncRAT, resurrected the ANEL backdoor, and leveraged a sophisticated execution chain to evade detection, deploying AsyncRAT inside Windows Sandbox for stealthy operations.

Attack Regions



Attack Details

#1 A cyberespionage campaign by the China-linked MirrorFace APT group is uncovered, targeting a Central European diplomatic institute in August 2024. Dubbed Operation AkaiRyū, this marks the first known instance of MirrorFace striking a European entity. The campaign introduced new tools and revived the ANEL backdoor. **MirrorFace** primarily focuses on espionage against organizations in Japan and entities tied to the country, including media, defense, financial institutions, think tanks, and academic sectors.

#2 In Operation AkaiRyū, MirrorFace launched spearphishing attacks to lure victims into opening malicious attachments. The group refined its tactics, now leveraging ANEL a tool long associated with APT10 but believed to have been abandoned in 2018. The discovery of a newer version (5.5.4) suggests that ANEL's development has resumed, supporting theories that MirrorFace may be a subgroup of APT10.

#3 Alongside ANEL, the group deployed AsyncRAT, embedding it into an execution chain within Windows Sandbox to evade detection. Additionally, they exploited Visual Studio Code remote tunnels a technique used to stealthily access compromised systems and execute arbitrary code. To maintain persistence, MirrorFace relied on its proprietary backdoor, HiddenFace, deploying it later in the attack chain. The group also used a signed McAfee executable to sideload ANEL, ensuring stealthy execution.

#4 The attack was highly deceptive. MirrorFace impersonated trusted organizations, referencing previous legitimate interactions to build credibility. Once the target engaged, the attackers sent a malicious OneDrive link containing a disguised LNK file. This file triggered a sophisticated execution chain, ultimately decrypting and deploying the ANEL backdoor. By leveraging signed applications from JustSystems Corporation, the group further masked its activities, making detection challenging.

#5 MirrorFace continues to evolve, integrating publicly available tools like AsyncRAT with custom enhancements, including sample tagging, Tor-based C&C communication, and a domain generation algorithm (DGA). These upgrades allow the group to tailor attacks to specific victims while evading detection. The resurgence of ANEL, combined with MirrorFace's innovative abuse of legitimate software, signals a growing threat landscape. Organizations must remain vigilant, strengthen their defenses against phishing attacks, and implement robust monitoring to detect anomalies before they escalate into full-scale breaches.

Recommendations

- **Enhance Email Security:** Implement robust email filtering to block phishing emails impersonating trusted entities. Use email authentication mechanisms like DMARC, SPF, and DKIM to prevent spoofed emails. Educate employees on identifying phishing attempts.
- **Enhance Endpoint Protection:** Deploy next-generation antivirus (NGAV) and endpoint detection & response (EDR) solutions to identify and block malware. Leverage behavioral analysis and machine learning-based detection to spot suspicious activity.
- **Restrict Execution of Macros and LNK Files:** Disable macros in Microsoft Office by default and block LNK files from untrusted sources to reduce the risk of malware infections. This prevents attackers from using malicious documents and shortcut files as entry points.
- **Monitor for Suspicious Activities:** Continuously monitor network activity for unusual remote access patterns, including potential abuse of Visual Studio Code remote tunnels. Implement application allowlisting to block unauthorized software execution, preventing attackers from exploiting legitimate applications like McAfee and JustSystems executables.

Potential MITRE ATT&CK TTPs

TA0042 Resource Development	TA0001 Initial Access	TA0002 Execution	TA0003 Persistence
TA0005 Defense Evasion	TA0007 Discovery	TA0009 Collection	TA0011 Command and Control
TA0010 Exfiltration	T1587 Develop Capabilities	T1587.001 Malware	T1585 Establish Accounts
T1585.002 Email Accounts	T1585.003 Cloud Accounts	T1588 Obtain Capabilities	T1588.001 Malware
T1588.002 Tool	T1566 Phishing	T1566.002 Spearphishing Link	T1053 Scheduled Task/Job

T1053.005 Scheduled Task	**T1059** Command and Scripting Interpreter	**T1059.001** PowerShell	**T1059.003** Windows Command Shell
T1204 User Execution	**T1204.001** Malicious Link	**T1204.002** Malicious File	**T1547** Boot or Logon Autostart Execution
T1547.001 Registry Run Keys / Startup Folder	**T1574** Hijack Execution Flow	**T1574.001** DLL Search Order Hijacking	**T1027** Obfuscated Files or Information
T1027.004 Compile After Delivery	**T1027.007** Dynamic API Resolution	**T1027.011** Fileless Storage	**T1055** Process Injection
T1070 Indicator Removal	**T1070.004** File Deletion	**T1070.006** Timestomp	**T1070.001** Clear Windows Event Logs
T1127 Trusted Developer Utilities Proxy Execution	**T1127.001** MSBuild	**T1140** Deobfuscate/Decode Files or Information	**T1622** Debugger Evasion
T1564 Hide Artifacts	**T1564.001** Hidden Files and Directories	**T1564.003** Hidden Window	**T1564.006** Run Virtual Instance
T1112 Modify Registry	**T1036** Masquerading	**T1036.007** Double File Extension	**T1218** System Binary Proxy Execution
T1221 Template Injection	**T1012** Query Registry	**T1033** System Owner/User Discovery	**T1057** Process Discovery
T1082 System Information Discovery	**T1124** System Time Discovery	**T1087** Account Discovery	**T1087.002** Domain Account
T1115 Clipboard Data	**T1113** Screen Capture	**T1001** Data Obfuscation	**T1001.001** Junk Data
T1568 Dynamic Resolution	**T1568.002** Domain Generation Algorithms	**T1573** Encrypted Channel	**T1071** Application Layer Protocol
T1071.001 Web Protocols	**T1132** Data Encoding	**T1132.001** Standard Encoding	**T1030** Data Transfer Size Limits

T1041 Exfiltration Over C2 Channel	**T1047** Windows Management Instrumentation	**T1560** Archive Collected Data	**T1090** Proxy
T1059.005 Visual Basic			

Indicators of Compromise (IOCs)

TYPE	VALUE
SHA1	018944FC47EE2329B23B74DA31B19E57373FF539, 68B72DA59467B1BB477D0C1C5107CEE8D9078E7E, 02D32978543B9DD1303E5B020F52D24D5EABA52E, 2FB3B8099499FEE03EA7064812645AC781AFD502, 9B2B9A49F52B37927E6A9F4D6DDB180BE8169C5F, AB65C08DA16A45565DBA930069B5FC5A56806A4C, 875DC27963F8679E7D8BF53A7E69966523BC36BC, 694B1DD3187E876C5743A0E0B83334DBD18AC9EB, F5BA545D4A16836756989A3AB32F3F6C5D5AD8FF, 233029813051D20B61D057EC4A56337E9BEC40D2, 8361F7DBF81093928DA54E3CBC11A0FCC2EEB55A, 1AFDCE38AF37B9452FB4AC35DE9FCECD5629B891, E3DA9467D0C89A9312EA199ECC83CDDF3607D8B1, D2C25AF9EE6E60A341B0C93DD97566FB532BFBE8
File Names	3b3cabc5, vsodscpl.dll, AtokLib.dll, CodeStartUser.bat, erBkVRZT.bat, useractivitybroker.xml, temp.log, tmp.docx, normal_.dotm, The EXPO Exhibition in Japan in 2025.docx.lnk, The EXPO Exhibition in Japan in 2025.zip, NK9C4PH_.zip, Tk4AJbXk.wsb
IPv4	45[.]32[.]116[.]146, 64[.]176[.]56[.]26, 104[.]233[.]167[.]135, 152[.]42[.]202[.]137, 208[.]85[.]18[.]4

TYPE	VALUE
TOR Address	vu4fleh3yd4ehpfpciinnwbnh4b77rdeypubhqr2dgfibjtvxpd xozid[.]onion, u4mrhg3y6jyfw2dmm2wnocz3g3etp2xc5thzx77uelk7mrk7qtj mc6qd[.]onion

References

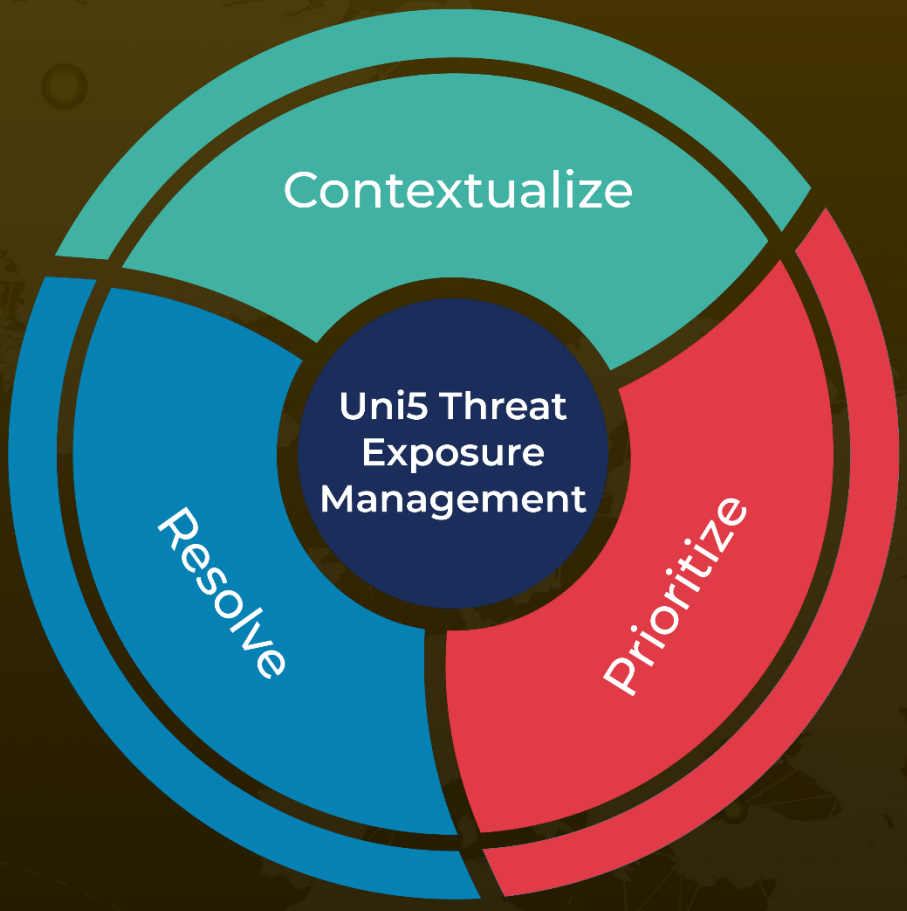
https://www.welivesecurity.com/en/eset-research/operation-akairyu-mirrorface-invites-europe-expo-2025-revives-anel-backdoor/

https://hivepro.com/threat-advisory/china-based-mirrorface-apt-group-targeting-japanese-political-entities/

What Next?

At **Hive Pro**, it is our mission to detect the most likely threats to your organization and to help you prevent them from happening.

Book a free demo with **HivePro Uni5**: Threat Exposure Management Platform.



REPORT GENERATED ON

March 19, 2025 • 6:50 AM

More at www.hivepro.com