Hive Pro

Threat Level

Amber

Hiveforce Labs

THREAT ADVISORY

ATTACK REPORT

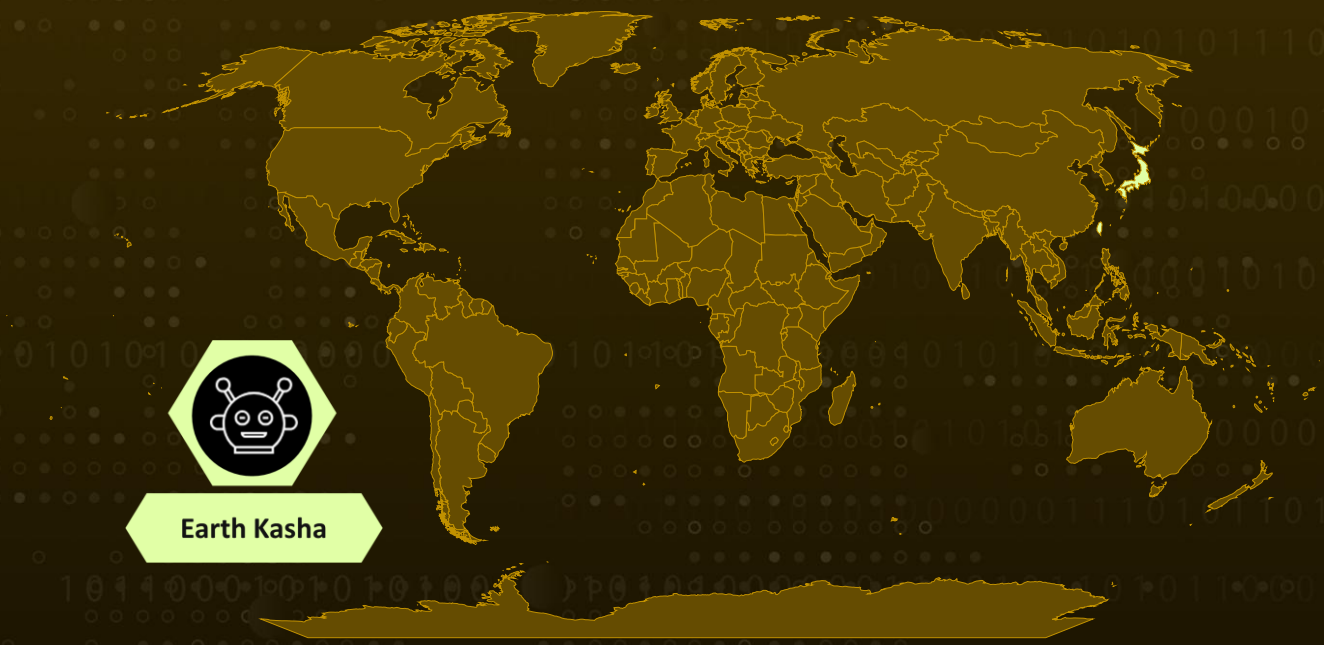
Earth Kasha Returns with New Tools in Its Cyber Espionage Campaign

Date of Publication	Admiralty Code	TA Number
May 9, 2025	A1	TA2025142

Summary

Attack Discovered: March 2025
Actor: Earth Kasha (aka MirrorFace, Operation LiberalFace)
Malware: NOOPDOOR, ANEL, ROAMINGMOUSE
Affected Industries: Government and Public Sector organizations
Targeted Countries: Taiwan and Japan
Attack: A new espionage campaign by Earth Kasha, part of China's APT10, is targeting government and public institutions in Taiwan and Japan. The attackers use spear-phishing emails with malicious Excel files to deploy ROAMINGMOUSE, which drops and runs malware through DLL sideloading. This leads to the in-memory execution of ANEL and, later, the stealthy NOOPDOOR backdoor, which supports encrypted DNS communications and evasion techniques, demonstrating Earth Kasha's continued evolution in cyber-espionage.

Attack Regions



Attack Details

#1 In March 2025, a new cyber-espionage campaign emerged, targeting government and public sector organizations in Taiwan and Japan. This operation is attributed to Earth Kasha, a part of the well-known APT10 threat actor umbrella. Earth Kasha has a long history of espionage activities dating back to 2017, consistently adapting its techniques and expanding its target scope.

#2 The attack begins with a spear-phishing email, carefully crafted and sent from a legitimate email account to build trust. The email includes a OneDrive link that downloads a ZIP file containing a malicious macro-enabled Excel document, designed to catch the recipient's attention through relevant filenames and subject lines. This Excel file acts as a dropper known as ROAMINGMOUSE, previously seen in Earth Kasha's operations.

#3 Once opened, ROAMINGMOUSE decodes an embedded ZIP archive using Base64, drops it to disk, and extracts its contents. The dropped components are placed in system-related directories. It then launches a legitimate executable as a parameter of explorer.exe using WMI, which loads a malicious DLL named JSFC.dll via DLL sideloading. If the target machine runs McAfee software, the malware adapts by using a batch file in the startup folder to execute the payload without relying on WMI.

#4 The dropped DLL, JSFC.dll, acts as a loader called ANELDR, which decrypts and runs an encrypted ANEL payload directly in memory. The decryption process combines AES-256-CBC, LZO compression, and custom encryption layers such as ChaCha20 and XOR. A key enhancement in this campaign is the added support for executing BOFs in memory, expanding ANEL's capabilities.

#5 Once installed, ANEL enables Earth Kasha to gather screenshots, inspect running processes, and review domain details to determine if the compromised machine belongs to a high-value target. If the system is deemed relevant, the attackers move to a second stage by deploying NOOPDOOR, a long-running backdoor exclusively used by Earth Kasha.

#6 To maintain persistence, the group may use SharpHide, launching NOOPDOOR via Hidden Start while suppressing any visible UI using MSBuild in autorun. NOOPDOOR itself has received updates in this campaign, including support for DoH a privacy-preserving method of resolving domain names. It uses public DNS services, with the malware generating C2 domains using a DGA tied to the current date and time. The resulting IP addresses are returned in the HTTPS response body, making detection more difficult. Earth Kasha previously conducted a campaign dubbed **Operation AkaiRyū**, during which they deployed a customized AsyncRAT and resurrected the ANEL backdoor.

Recommendations

Strengthen Email Security: Set up smart email filters to catch tricky phishing emails before they reach inboxes, especially ones with dangerous links or attachments. Also, teach your team how to spot suspicious emails like those with odd OneDrive links or ZIP files so they don't accidentally open something harmful.

Turn Off Macros When Possible: Stop Office apps (like Excel and Word) from running macros unless they're really needed. Set up rules to prevent files from running macros unless they're from a trusted source.

Watch for Hidden Program Launches: Monitor your systems for trusted programs (like explorer.exe) running unknown files or being used to sneak in malware. Pay special attention to anything using WMI (a Windows tool) to run programs in the background.

Block Suspicious Internet Connections: Use DNS filtering tools to block access to risky websites or unknown servers. Look out for unusual DNS traffic or patterns that might signal malware calling home using encrypted channels (like DoH).

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.

Potential MITRE ATT&CK TTPs

TA0001 Initial Access	**TA0002** Execution	**TA0003** Persistence	**TA0005** Defense Evasion
TA0007 Discovery	**TA0009** Collection	**TA0010** Exfiltration	**TA0011** Command and Control
T1566 Phishing	**T1566.002** Spearphishing Link	**T1047** Windows Management Instrumentation	**T1071** Application Layer Protocol

T1071.004 DNS	**T1547** Boot or Logon Autostart Execution	**T1036** Masquerading	**T1204** User Execution
T1573 Encrypted Channel	**T1573.002** Asymmetric Cryptography	**T1574** Hijack Execution Flow	**T1574.001** DLL
T1497 Virtualization/Sandbox Evasion	**T1027** Obfuscated Files or Information	**T1140** Deobfuscate/Decode Files or Information	**T1059** Command and Scripting Interpreter
T1113 Screen Capture	**T1057** Process Discovery	**T1572** Protocol Tunneling	**T1637** Dynamic Resolution
T1637.001 Domain Generation Algorithms			

Indicators of Compromise (IOCs)

TYPE	VALUE
Domains	srmbr[.]net, kyolpon[.]com
IPv4	172[.]233[.]73[.]249, 172[.]105[.]62[.]188, 192[.]46[.]215[.]56, 139[.]162[.]38[.]102, 139[.]84[.]131[.]62, 139[.]84[.]136[.]105, 45[.]32[.]116[.]146, 45[.]77[.]252[.]85, 208[.]85[.]18[.]4
SHA256	1e0a7737a484699d035c0568771c4834c0ff3fb9ba87aded3c86705e10e9bb0e, 2110b9a4c74d1c8be1aed6ebcff2351cad3d16574026fe4697a9c70810fb1d9e, 488201c08219f5cbd79d16702fb909d4e8ad8fa76819a21e0f262e2935e58dd2, 517ef26be8b9fb1af0e9780b244827af4937ad2fa4778a0bd2d9c65502ce54e1,

TYPE	VALUE
SHA256	63e813b5bf94bdec9ce35c9d7311f76c3a35728d158ade0a6487fc99c73dcf31, 69e2a259e0136b61a3acad3f8fad2c012c75c9d8e26e66a3f0af1e7c23506b5c, 6edf72495e03ca757fa55beb2ea02492f2e7a4b85ca287a9d08bbe60e390c618, 705e5f1245e59566895b1d456aee32d4bff672a6a00f2cd390d7d50c12316dee, 712b81f1a82b9ea9a304220ed87c47c329392c2ce040ed3bff936fe33456acff, 72ece359a3c6f286d174b9cccc7c963577749e38e28f5ecf00dd4c267478a693, 75d6f82962f380f772614249006887924 0c3c507427f477cf25268b524c30339, 7b61ed1049ba5f5b8d9725f32cff1ef1e72ef46e2a1dd87bd2b33e73e7333f44, 8cdcd674a0269945dd4c526b5868efb6df8854a127fd5449e57e89905511391d, 9569c4044f8cf32bc9a0513ed7c4497bb6ab71b701c53e58719ef259b3716751, 9c24b60574f39b0565442a79a629a2944672f56acca555e81275e5079382d98b, 9e4c155f4d096d9a0529e83fd21197f3dba20cc4eef48045fd018334384dd513, a12a34d329ccc305dca2306e2d698945f1413c013fe99d4bb069db2127f47806, a14c9ae22ca8bdb4971a03f61b2bcc5f140abb51c6922ab7c92ea09ee14dd3bd, a347e1efbfca3722c9e8cc86eba3b288f7e4fae9d386f2a8969faffb125a74c5, ac8c36075ac0085c7d1e96b3fc08c15a151373186e564486dd91d2e49b2dd287, ad050545b65ecbb2178f678c654d84d14986a77051897927e56b5c2893c33608, b56aa48721cd1119a9e06ed9c2f923a1dda5f9aa079dc0e4fd66ab37e33649e8, cb0848d79d2eef76e1d4ff602e0844d03b614d4c25a1b5e3f0ae5c33ea5500b9, cf6ed83d7dcc13f500486044d1af606ceb12c387568ccbb498e01cc7d8005dbd, e123fa2abf1a2f12af9f1828b317d486d1df63aff801d591c5e939eb06eb4cfc, e5b99572581df7a5116511be3f03b9f1a90611235b8288d9f59141876adb1ef1, eeec3a94500ecd025ecdd559e15e4679e26c1347e534944721abe416b49f3871,

TYPE	VALUE
SHA256	f502102c5c598d5b9e24f689a3b09b1d2f6702226049a573c421b765867391b3, fc8c574088af4f74cf84c5c04d522bb1665f548cb17c6192552eb9b783401009, 362b0959b639ab720b007110a1032320970dd252aa07fc8825bb48e8fdd14332, 78f7b98b1e6f089f5789019dab23ac38f77c662fd651ee212d8451ee61b2fc0c, 7fb4c9f041d4411311437e12427aaf09d369bc384faa2de4b5bc8ae36a42190e, 4f3ec89d5ea0a513afa3f49434f67b7e1540a4a8a93d078def950bd94d444723

References

https://www.trendmicro.com/en_us/research/25/d/earth-kasha-updates-ttps.html

https://hivepro.com/threat-advisory/operation-akairyu-mirrorface-expands-cyberespionage-to-europe-with-revived-tools/

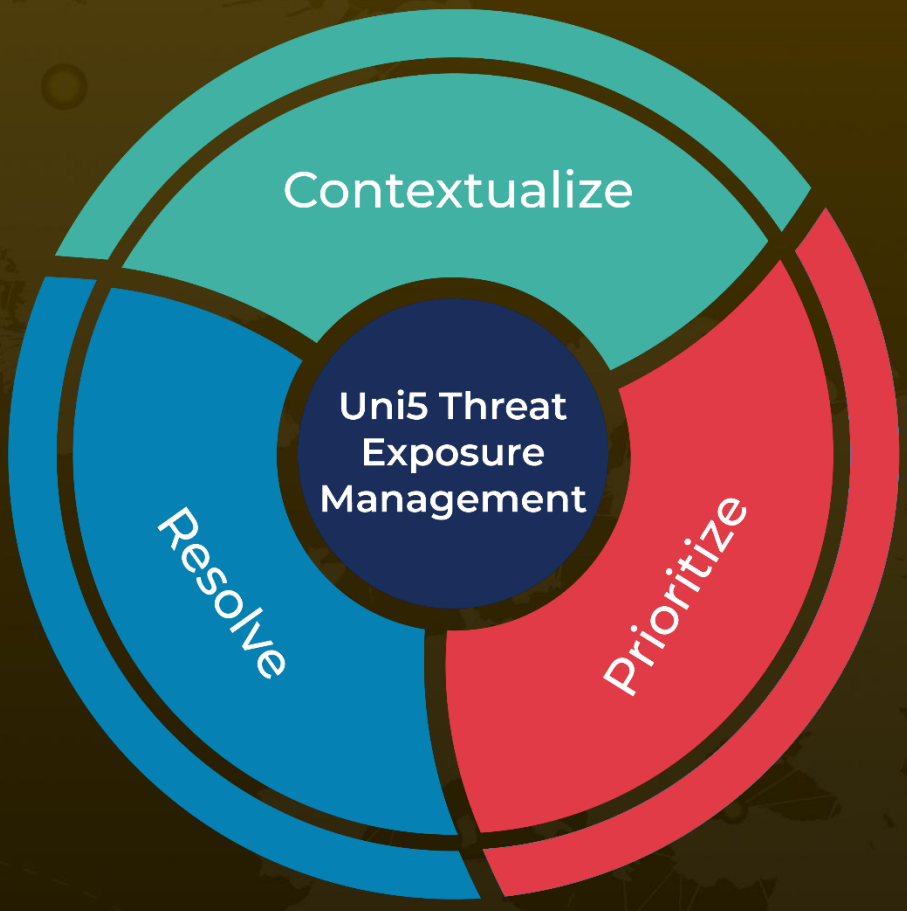
https://www.trendmicro.com/en_us/research/24/k/return-of-anel-in-the-recent-earth-kasha-spearphishing-campaign.html

https://www.trendmicro.com/en_us/research/24/k/lodeinfo-campaign-of-earth-kasha.html

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

May 9, 2025 • 5:30 AM

More at www.hivepro.com