Hive Pro

Threat Level

Amber

Hiveforce Labs

THREAT ADVISORY

ATTACK REPORT

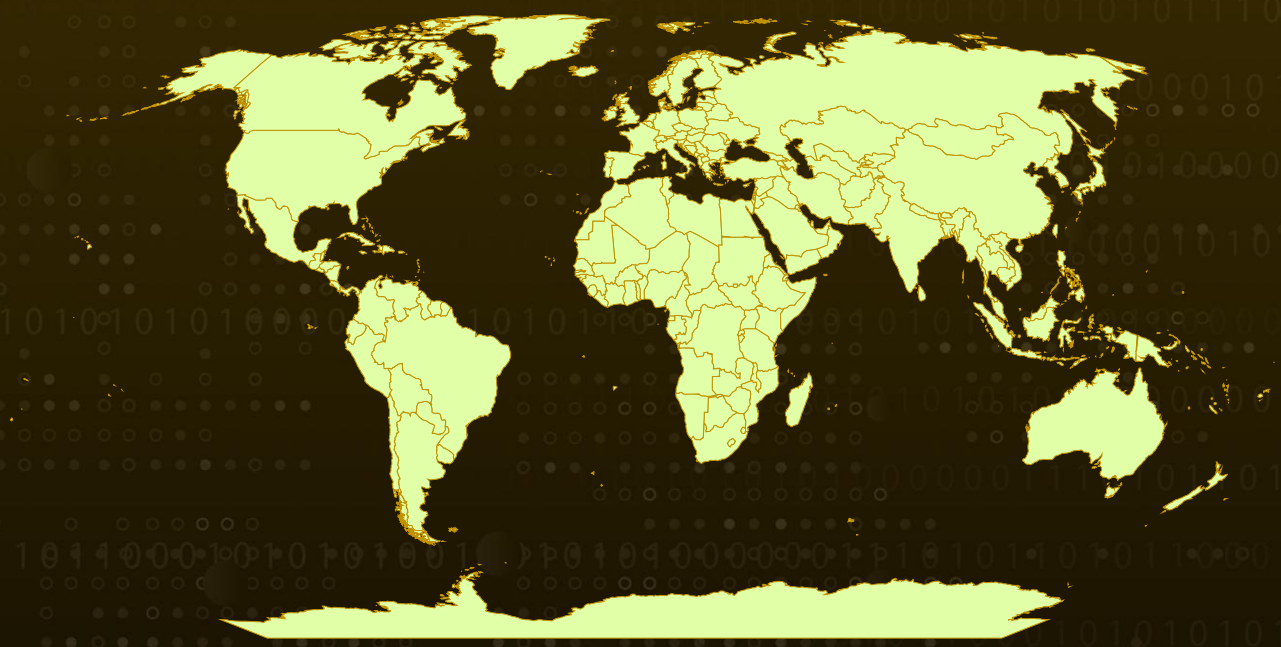
QuirkyLoader: A Silent Enabler of Modern Malware Families

Date of Publication	Admiralty Code	TA Number
August 22, 2025	A1	TA2025258

Summary

Attack Discovered: November 2024
Targeted Countries: Worldwide
Malware: QuirkyLoader
Attack: QuirkyLoader is a stealthy malware loader that spreads through phishing emails carrying malicious archive files. Once opened, it uses DLL side-loading and process hollowing to quietly inject encrypted payloads into trusted Windows processes, allowing it to deliver infostealers and RATs like Snake Keylogger, Remcos, and AsyncRAT. Recent campaigns in Taiwan and Mexico highlight how attackers are using this loader for both targeted and widespread infections, making it a growing enabler in the modern cybercrime landscape.

Attack Regions



Attack Details

#1 QuirkyLoader has surfaced as a highly adaptable malware loader, increasingly favored by cybercriminals to deliver a wide array of threats such as Agent Tesla, AsyncRAT, FormBook, MassLogger, Remcos, Rashadamanthys, and Snake Keylogger. Its main role is to act as a delivery system, giving attackers the ability to plant additional payloads and expand the scope of their operations. The infection chain typically begins with a phishing email, often sent through legitimate service providers or attacker-controlled servers. Inside these emails, victims find a malicious archive containing what looks like a harmless executable, an encrypted payload, and a hidden DLL that powers the loader's activity.

#2 Once the victim interacts with the archive, the infection sequence begins in earnest. The bundled executable activates the malicious DLL, which then injects its payload into trusted Windows processes using process hollowing. By hijacking legitimate processes like AddInProcess32.exe, InstallUtil.exe, and aspnet_wp.exe, QuirkyLoader masks its behavior within normal system operations.

#3 One of QuirkyLoader's more notable traits lies in how its DLL module is engineered. Built in C#.NET, it uses Ahead-of-Time (AOT) compilation, which transforms C# code into Microsoft Intermediate Language (MSIL) and then compiles it into native machine code. This approach makes the malware appear more like a traditional C or C++ program, bypassing the usual fingerprints of .NET binaries. For handling payloads, QuirkyLoader makes use of Win32 APIs to load encrypted data, which it then decrypts with a block cipher before execution.

#4 Some variants have taken this further by incorporating the Speck-128 cipher in CTR mode, which generates keystreams XORed against data in 16-byte segments. To stay under the radar, the malware also dynamically resolves Win32 APIs used in its injection routine. It carefully creates a suspended process, removes its original memory, writes its malicious payload into place, and then resumes execution.

#5 QuirkyLoader's presence has already been observed in real-world campaigns. In July 2025, two separate operations highlighted its use: in Taiwan, where employees of Nusoft Taiwan were targeted with Snake Keylogger, and in Mexico, where attackers indiscriminately deployed Remcos RAT and AsyncRAT. Infrastructure linked to these campaigns led back to the domain which hosted a Zimbra web client and presented an SSL certificate tied to it. These findings suggest attackers are leveraging both phishing and controlled infrastructure to support their operations. Taken together, QuirkyLoader represents a growing example of how loaders have evolved into sophisticated, multipurpose enablers of modern malware campaigns.

Recommendations

- **Be cautious with email attachments:** Most QuirkyLoader infections start with a phishing email carrying a malicious archive. Avoid opening unexpected attachments, especially ZIP or RAR files, even if they appear to come from known contacts or legitimate companies. When in doubt, verify with the sender through a separate channel before opening.
- **Restrict the use of scripting and admin tools:** QuirkyLoader abuses legitimate Windows processes like InstallUtil.exe to hide its activity. Limit the use of such tools where possible and monitor their activity to detect unusual behavior.
- **Monitor for suspicious domains and SSL certificates:** Attackers often use domains with legitimate-looking SSL certificates to distribute malware. Keep an eye on traffic to unusual domains and block access when needed.
- **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	**TA0005** Defense Evasion	**TA0011** Command and Control
T1566 Phishing	**T1566.001** Spearphishing Attachment	**T1204** User Execution	**T1574** Hijack Execution Flow
T1574.001 DLL	**T1027** Obfuscated Files or Information	**T1055** Process Injection	**T1055.012** Process Hollowing
T1140 Deobfuscate/Decode Files or Information	**T1218** System Binary Proxy Execution	**T1218.004** InstallUtil	**T1071** Application Layer Protocol
T1071.001 Web Protocols			

Indicators of Compromise (IOCs)

TYPE	VALUE
SHA256	011257eb766f2539828bdd45f8aa4ce3c4048ac2699d988329783290a7b4a0d3, 0ea3a55141405ee0e2dfbf333de01fe93c12cf34555550e4f7bb3fdec2a7673b, a64a99b8451038f2bbcd322fd729edf5e6ae0eb70a244e342b2f8eff12219d03, 9726e5c7f9800b36b671b064e89784fb10465210198fbbb75816224e85bd1306, a1994ba84e255eb02a6140cab9fc4dd9a6371a84b1dd631bd649525ac247c111, d954b235bde6ad02451cab6ee1138790eea569cf8fd0b95de9dc505957c533cd, 5d5b3e3b78aa25664fb2bfdbf061fc1190310f5046d969adab3e7565978b96ff, 6f53c1780b92f3d5affcf095ae0ad803974de6687a4938a2e1c9133bf1081eb6, ea65cf2d5634a81f37d3241a77f9cd319e45c1b13ffbaf5f8a637b34141292eb, 1b8c6d3268a5706fb41ddfff99c8579ef029333057b911bb4905e24aacc05460, d0a3a1ee914bcbfcf709d367417f8c85bd0a22d8ede0829a66e5be34e5e53bb9, b22d878395ac2f2d927b78b16c9f5e9b98e006d6357c98dbe04b3fd78633ddde, a83aa955608e9463f272adca205c9e1a7cbe9d1ced1e10c9d517b4d1177366f6, 3391b0f865f4c13dcd9f08c6d3e3be844e89fa3afbcd95b5d1a1c5abcacf41f4, b2fdf10bd28c781ca354475be6db40b8834f33d395f7b5850be43ccace722c13, bf3093f7453e4d0290511ea6a036cd3a66f456cd4a85b7ec8fbfea6b9c548504, 97aee6ca1bc79064d21e1eb7b86e497adb7ece6376f355e47b2ac60f366e843d, b42bc8b2aeec39f25babdcbbdaab806c339e4397debfde2ff1b69dca5081eb44, 5aaf02e4348dc6e962ec54d5d31095f055bd7fb1e58317682003552fd6fe25dc, 8e0770383c03ce69210798799d543b10de088bac147dce4703f13f79620b68b1,

TYPE	VALUE
SHA256	049ef50ec0fac1b99857a6d2beb8134be67ae67ae134f9a3c53699cdaa7c89ac, cba8bb455d577314959602eb15edcaa34d0b164e2ef9d89b08733ed64381c6e0
Domains	catherinereynolds[.]info, mail[.]catherinereynolds[.]info
IPv4	157[.]66[.]22[.]11, 103[.]75[.]77[.]90, 161[.]248[.]178[.]212

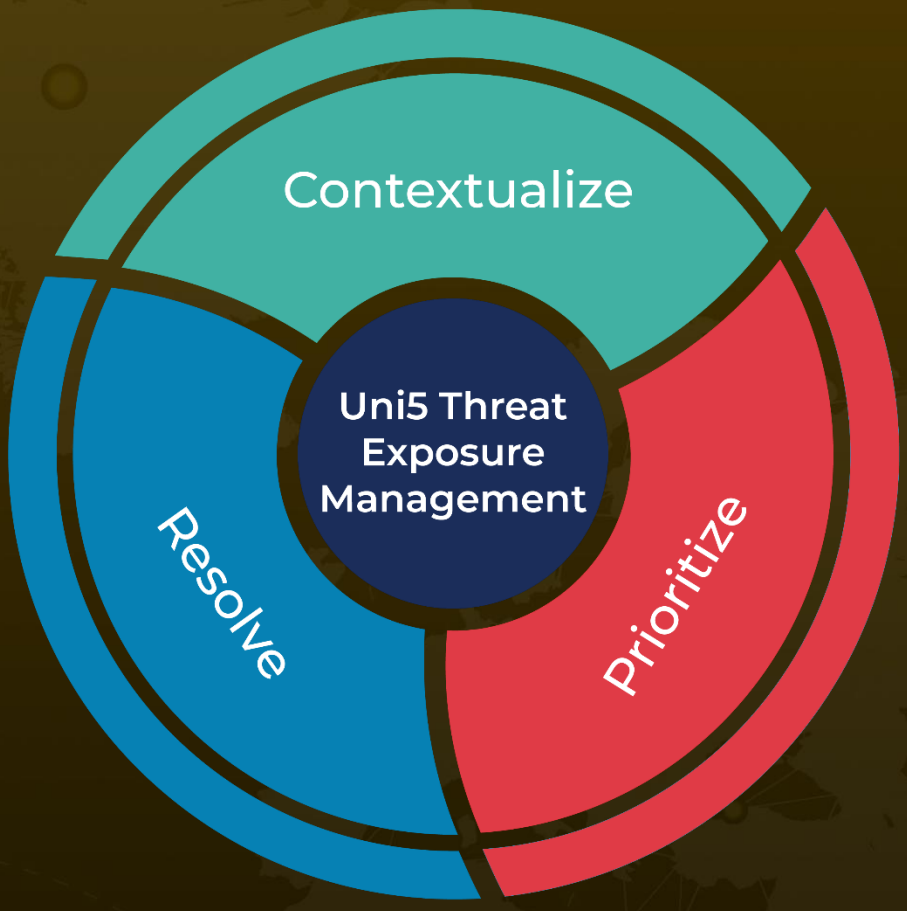
References

https://www.ibm.com/think/x-force/ibm-x-force-threat-analysis-quirkyloader

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

August 22, 2025 • 6:00 AM

More at www.hivepro.com