Hive Pro

Threat Level

Red

HiveForce Labs

THREAT ADVISORY

ATTACK REPORT

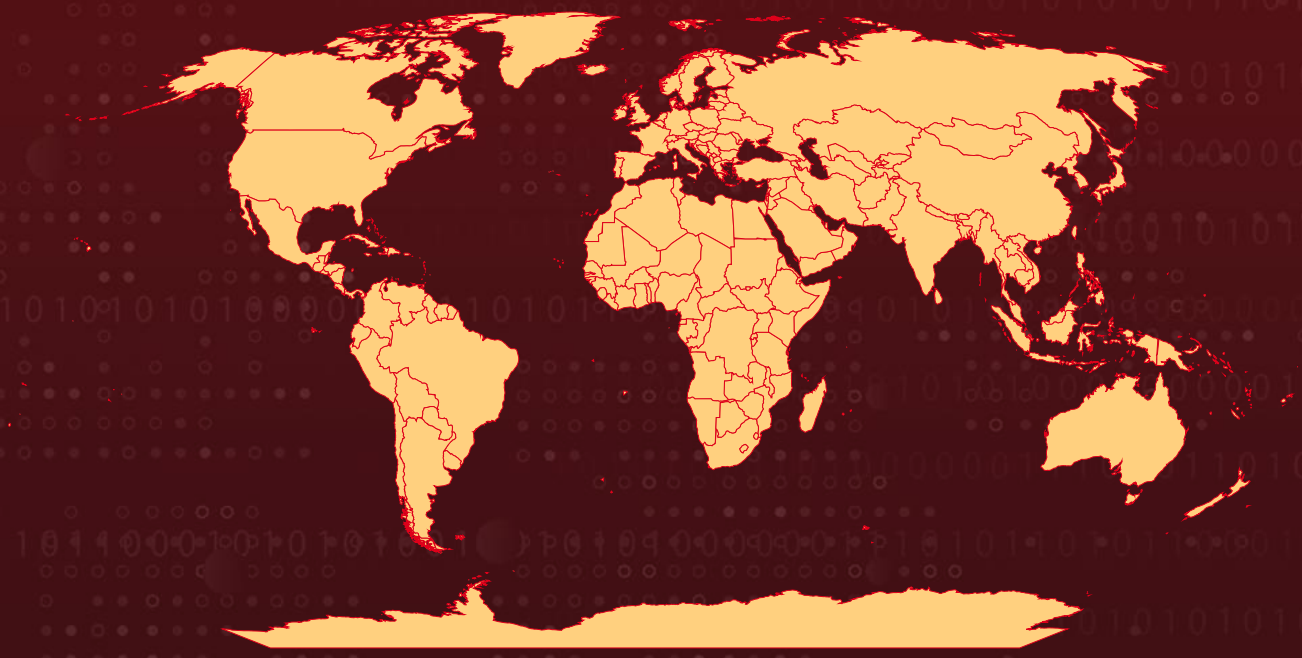
Stealit's New Trick: Packing Malware Inside Node.js Single Executables

Date of Publication	Admiralty Code	TA Number
October 13, 2025	A1	TA2025313

Summary

Attack Discovered: 2025
Targeted Countries: Worldwide
Affected Platform: Microsoft Windows
Malware: Stealit
Attack: The latest Stealit campaign marks a bold evolution in malware delivery, weaponizing Node.js's new Single Executable Application (SEA) feature to spread its payloads as standalone, disguised installers for games and VPNs. These self-contained executables don't need Node.js preinstalled, making them easier to deploy and harder to detect. The malware cleverly hides inside PyInstaller bundles and archives shared on sites like Discord and Mediafire, while its operator's market Stealit as a paid "data extraction" service complete with pricing plans, tutorials, and a Telegram channel. Stealit can steal browser data, crypto wallets, and system credentials. The campaign continues to evolve rapidly, showing how threat actors are adapting modern development tools like Node.js and Electron to power stealthier, more versatile attacks.

Attack Regions



Attack Details

#1 A recent Stealit malware campaign is using Node.js's experimental Single Executable Application (SEA) feature to deliver its malicious code as self-contained programs. It is noticed that the activity after many detections of a Visual Basic script that the malware uses to stay on infected systems. Instead of requiring a separate Node.js runtime, these SEA binaries run on their own and are disguised as installers for games or VPN tools. Attackers also hide samples inside PyInstaller bundles and compressed files uploaded to file-sharing sites and Discord to look like ordinary downloads.

#2 The group behind Stealit has refreshed its infrastructure and advertises the malware as a commercial service. Their control panel moved domains (previously stealituptaded[.]lol, now iloveanimals[.]shop) and markets the kit as a paid "data extraction" product with subscription plans, tutorial videos, and a Telegram channel. The offering includes Windows and Android packages and pricing that clearly indicate this is a for-sale RAT (remote access trojan) aimed at buyers seeking ready-made tools for stealing data or deploying ransomware.

#3 From a technical standpoint, the SEA installers include an embedded resource (NODE_SEA_BLOB) that contains the original script and file paths, which point to a shared Stealit codebase. The visible installer unpacks a large, obfuscated blob into memory and runs it with Node's module loader. Execution happens in stages: a small loader launches a second heavily obfuscated script, and that script triggers the routines that install and run the malware components.

#4 The malware actively tries to avoid analysis and detection. It checks system memory, CPU count, hostnames, and usernames against hardcoded lists, and searches for common analysis tools or suspicious files. If anything looks like a lab or sandbox, the program exits. If the environment looks normal, the malware writes a base64 authentication token to a temporary file, downloads additional components from attacker servers into randomized user folders, and uses PowerShell to add those folders to Windows Defender's exclusion list. Some components are packaged with Pkg, while newer samples are wrapped in Electron and encrypt their scripts with AES-256-GCM.

#5 The campaign uses multiple specialized binaries. One drops and runs a helper to extract browser data; another collects information from browsers, gaming platforms, and cryptocurrency wallets and kills interfering processes; and a main component connects to a command-and-control server to report victim details and receive commands. The goal stays the same across variants: establish persistence, harvest credentials and wallet data, and give attackers remote control, while continually changing delivery and obfuscation techniques to stay active and harder to detect.

Recommendations

Download Software Only from Trusted Sources: Avoid installing games, VPNs, or other software from file-sharing sites or links on Discord and social media. Always use official websites or verified app stores to minimize the risk of downloading trojanized installers.

Be Cautious with Suspicious Files and Archives: Do not open ZIP or RAR files received from unknown sources. If a file looks unexpected or includes executable (.exe) content, verify its legitimacy with your IT team before opening it.

Restrict Software Installation Privileges: Limit administrative rights for regular users. This helps prevent unauthorized installations and blocks malware from making system-wide changes or adding persistence mechanisms.

Detect and Remove Malicious Startup Entries: Inspect Windows Startup folders and scheduled tasks for unexpected Visual Basic or executable files (e.g., game_cache.exe, .vbs, or .lnk entries). Remove any files that are not part of legitimate programs.

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

TA0002 Execution	**TA0003** Persistence	**TA0005** Defense Evasion	**TA0006** Credential Access
TA0009 Collection	**TA0011** Command and Control	**T1059** Command and Scripting Interpreter	**T1059.007** JavaScript
T1027 Obfuscated Files or Information	**T1140** Deobfuscate/Decode Files or Information	**T1497** Virtualization/Sandbox Evasion	**T1059.005** Visual Basic

T1547 Boot or Logon Autostart Execution	**T1547.001** Registry Run Keys / Startup Folder	**T1555** Credentials from Password Stores	**T1555.003** Credentials from Web Browsers
T1083 File and Directory Discovery	**T1113** Screen Capture	**T1071** Application Layer Protocol	**T1204** User Execution
T1204.002 Malicious File	**T1132** Data Encoding	**T1027.002** Software Packing	**T1553** Subvert Trust Controls

Indicators of Compromise (IOCs)

TYPE	VALUE
SHA256	554b318790ad91e330dced927c92974d6c77364ceddfb8c2a2c830d8b58e203c, aa8f0988f1416f6e449b036d5bd1624b793b71d62889afdc4983ee21a1e7ca87, 5ea27a10c63d0bbd04dbea5ec08fe0524e794c74d89f92ac6694cfd8df786b1f, 083c4e0ffdc9edf0d93655ee4d665c838d2a5431b8064242d93a545bd9ad761b, 432b8414113a8c14c0305a562a93ed926e77de351bac235552a59cc02e1e5627, 8e1cf254d23e2b94c77294079336339ececf33a3e7ee1a3621ee4e0df0695ce5, 919a2107ac27e49cdaa60610706e05edfc99bd3f2e9ca75da4feb6a5f2517c27, e004f8e39e489dec74a13d99836ee5693bd509047ecf49f3fc14efc143a161b5, 818350a4fb4146072a25f0467c5c99571c854d58bec30330e7db343bceca008b, 8814db9e125d0c2b7489f8c7c3e95adf41f992d4397ed718bda8573cb8fb0e83, 24b3def3f374c5f17ec9f1a347c71d9c921155c878ab36e48dd096da418bf782, c38130d7cb43cf3da4858247a751d7b9a3804183db8c4c571b6eede0590474da

TYPE	VALUE
URLs	hxxps[:]//iloveanimals[.]shop/, hxxps[:]//iloveanimals[.]shop/user/login, hxxps[:]//root[.]iloveanimals[.]shop/download/save_data, hxxps[:]//root[.]iloveanimals[.]shop/download/stats_db, hxxps[:]//root[.]iloveanimals[.]shop/download/game_cache, hxxps[:]//root[.]iloveanimals[.]shop/panelping, hxxps[:]//root[.]stealituptaded[.]lol/download/save_data, hxxps[:]//root[.]stealituptaded[.]lol/download/stats_db, hxxps[:]//root[.]stealituptaded[.]lol/download/game_cache, hxxps[:]//cdn[.]discordapp[.]com/attachments/1395171942494896190/1413957011837816915/VrchatPlugin.rar?ex=68bdd195&is=68bc8015&hm=b9f359a7f75b84d1b860d2aa4dd92f8adad3a2feef5d82832f49d664a256ff7b&, hxxps[:]//www[.]mediafire[.]com/file/9ni7pgjxuw8pc6h/ShaderSetup.rar/file, hxxps[:]//download1529[.]mediafire[.]com/8006s55pduvgtQ0THBMZxcLtlrh20a5BnfF18n8YfGUB8P7M5U3mEQb-UYYDCrMHsSG0aWvnyy_LIMg2OnTc4kuNYmWzjWLQwOds-qSfhdO03NOQFAAaYCPiOvB8nU7mBEHe-3a5gDSufW6upPbFXyGlbzBTdtpcrVPXokNKOYZ9/c4zbp39q02jvrn8/Aykadia.rar,

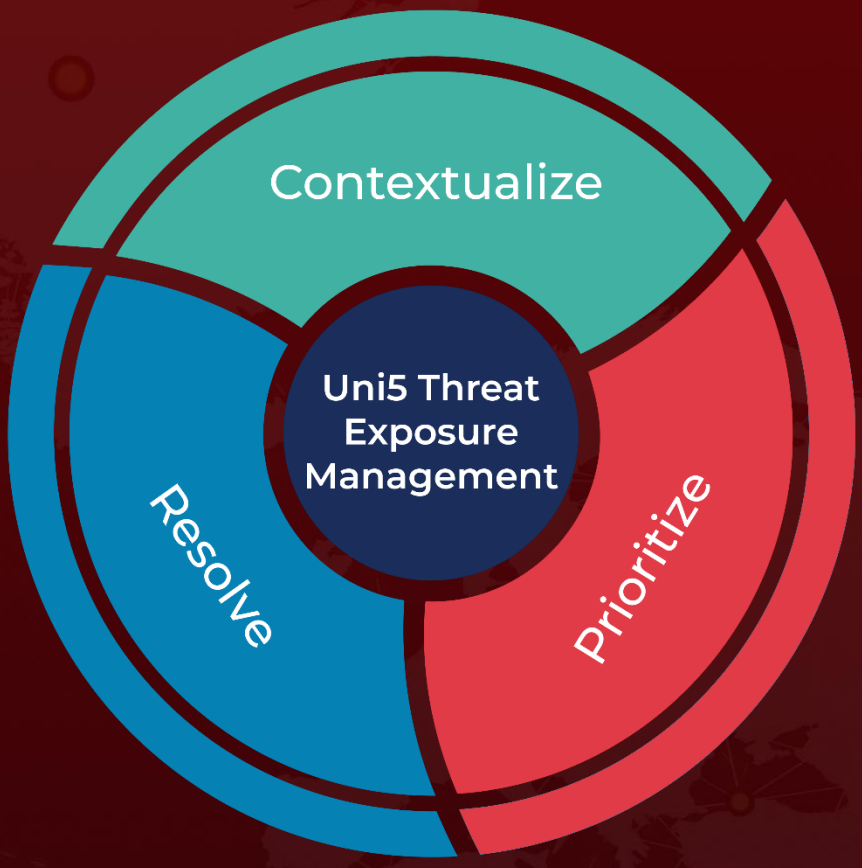
References

https://www.fortinet.com/blog/threat-research/stealit-campaign-abuses-nodejs-single-executable-application

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

October 13, 2025 • 8:30 AM

More at www.hivepro.com