Hive Pro

Threat Level

Red

HiveForce Labs

THREAT ADVISORY

ATTACK REPORT

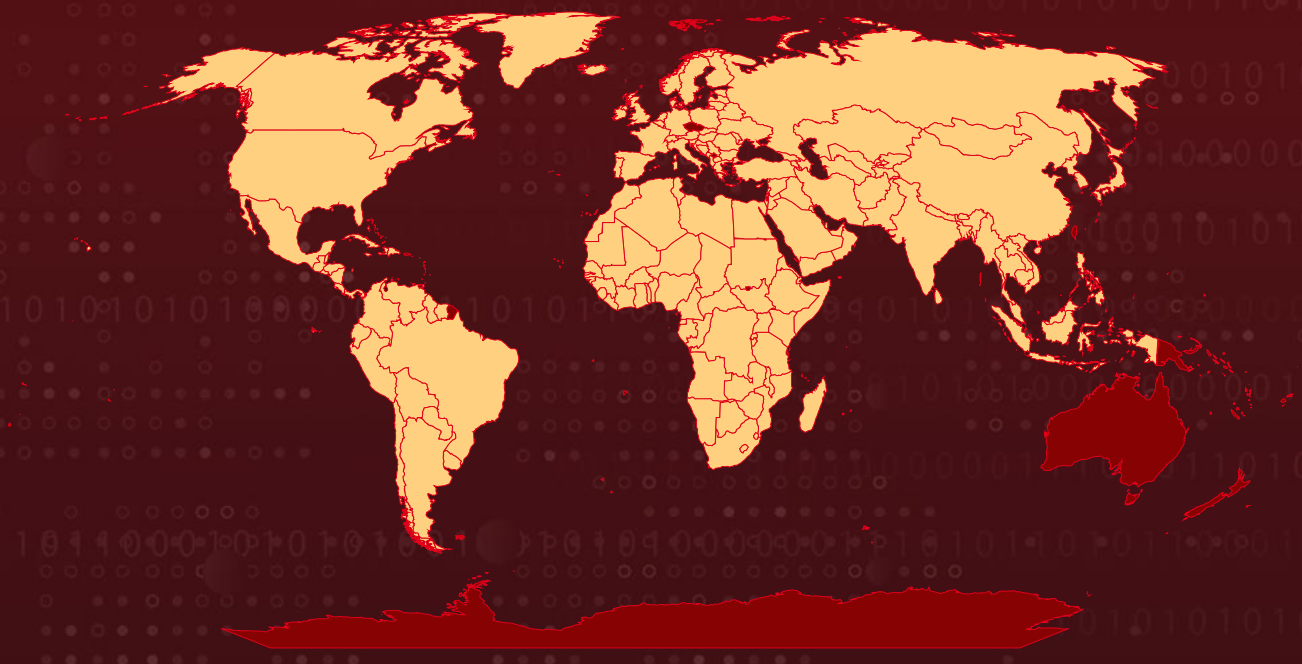
EvilAI Malware Exploits the Trust in Artificial Intelligence

Date of Publication	Admiralty Code	TA Number
September 15, 2025	A1	TA2025281

Summary

Attack Discovered: August 2025
Targeted Regions: Europe, Americas, AMEA
Targeted Industries: Manufacturing, Government, Healthcare, Technology, Retail, Education, Financial Services, Construction, Non-profit, Utilities
Affected Platform: Windows
Malware: EvilAI
Attack: EvilAI is a new malware that hides behind the mask of legitimate AI tools, luring users with polished interfaces, real functionality, and even stolen code-signing certificates to appear trustworthy. Once installed, it blends into systems by mimicking normal processes, creating disguised scheduled tasks, and using advanced obfuscation to stay hidden. Beyond the surface, it quietly communicates with command-and-control servers over encrypted channels, steals browser data, and prepares systems for further payloads. With infections spreading quickly across Europe, the Americas, and AMEA, and targeting various industries, EvilAI highlights how attackers are now weaponizing AI itself to outsmart defenses, making vigilance and adaptive security more critical than ever.

Attack Regions



Attack Details

#1 A new strain of malware is exploiting the popularity of artificial intelligence by masquerading as legitimate AI-powered tools. Disguised behind convincing interfaces and realistic functionality, these trojans slip into both personal and enterprise systems before raising any alarms. This malware family is dubbed EvilAI. The campaign highlights the growing difficulty of distinguishing authentic applications from malicious ones in today's AI-driven digital ecosystem.

#2 EvilAI has already achieved a striking global footprint, with Europe reporting the largest cluster of infections. The malware has not limited itself to one industry but has spread across manufacturing, government, public services, and healthcare sectors. By using clever social engineering and camouflaged code, the attackers have been able to infiltrate critical networks and establish persistent footholds.

#3 What makes EvilAI especially deceptive is its attention to detail. Malicious installers are distributed via newly registered websites, manipulated search results, online forums, and even paid advertisements. Once downloaded, the applications often function as advertised, be it productivity tools, document handlers, or AI enhancers, convincing users that they've installed legitimate software. The illusion is strengthened further by the misuse of digital signatures and trusted certificates, sometimes even obtained directly by attackers, to make the malware appear "verified" and safe to install.

#4 The technical underpinnings of EvilAI reveal a layered and resilient design. Its operators employ multiple obfuscation techniques, such as Unicode-encoded strings, hash-based control flow, and evasive process manipulation. Upon execution, the malware establishes encrypted communication channels with its command-and-control servers, enabling attackers to issue instructions, download additional payloads, modify registries, and execute stealthy background processes. By encoding traffic with AES-256-CBC and disguising scheduled tasks as legitimate Windows processes.

#5 EvilAI is currently being used as a staging platform for secondary payloads, potentially including information stealers, though its full capabilities are still under investigation. This uncertainty adds to the risk, as organizations may remain unaware of the depth of compromise. The rise of AI-generated malware like EvilAI underscores a pivotal shift in the threat landscape: attackers are now using the very tools meant to enhance productivity and innovation to outpace defenders.

Recommendations

- **Be cautious with downloads:** Only download software and AI tools from trusted, official sources. Avoid clicking on links from ads, forums, or social media posts, no matter how convincing they look.
- **Check before you trust:** Don't rely on looks alone. Even if an app has a polished interface or a "verified" certificate, it doesn't guarantee safety. Double-check the publisher's legitimacy and reviews before installing.
- **Strengthen defenses:** Use a reliable security solution that can detect suspicious behavior, not just known malware signatures. AI-powered malware needs modern, adaptive defenses.
- **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

TA0042 Resource Development	TA0001 Initial Access	TA0002 Execution	TA0003 Persistence
TA0005 Defense Evasion	TA0006 Credential Access	TA0007 Discovery	TA0010 Exfiltration
TA0011 Command and Control	TA0040 Impact	T1588 Obtain Capabilities	T1588.007 Artificial Intelligence
T1059 Command and Scripting Interpreter	T1059.007 JavaScript	T1053 Scheduled Task/Job	T1547 Boot or Logon Autostart Execution
T1547.009 Shortcut Modification	T1547.001 Registry Run Keys / Startup Folder	T1057 Process Discovery	T1518 Software Discovery

T1518.001 Security Software Discovery	**T1489** Service Stop	**T1555** Credentials from Password Stores	**T1036** Masquerading
T1189 Drive-by Compromise	**T1588.003** Code Signing Certificates	**T1047** Windows Management Instrumentation	**T1059.001** PowerShell
T1027 Obfuscated Files or Information	**T1070** Indicator Removal	**T1071** Application Layer Protocol	**T1071.001** Web Protocols
T1041 Exfiltration Over C2 Channel	**T1112** Modify Registry		

Indicators of Compromise (IOCs)

TYPE	VALUE
Filenames	justaskjacky.exe, manualshq.exe, PDF Editor.exe, index.js, {GUID}or.js, main.js
SHA256	8ecd3c8c126be7128bf654456d171284f03e4f212c27e1b33f875b8907a7bc65, 49a4442e73521ecca8e56eb6dbc33f31eb7cfa5e62a499e552bcd29a29d79d8a, b0c321d6e2fc5d4e819cb871319c70d253c3bf6f9a9966a5d0f95600a19c0983, cb15e1ec1a472631c53378d54f2043ba57586e3a28329c9dbf40cb69d7c10d2c, ad0655b17bbdbd8a7430485a10681452be94f5e6c9c26b8f92e4fcba291c225a, 95001359fb671d0e6d97f37bd92642cc993e517d2307f373bfa9893639f1a2bc, 9f369e63b773c06588331846dd247e48c4030183df191bc53d341fcc3be68851, cf45ab681822d0a4f3916da00abd63774da58eb7e7be756fb6ec99c2c8cca815, ce834dca38aeac100f853d79e77e3f61c12b9d4da48bb0a949d0a961bf9c0a27

TYPE	VALUE
URLs	hxxps[:]//9mdp5f[.]com, hxxps[:]//5b7crp[.]com, hxxps[:]//mka3e8[.]com, hxxps[:]//y2iax5[.]com, hxxps[:]//abf26u[.]com

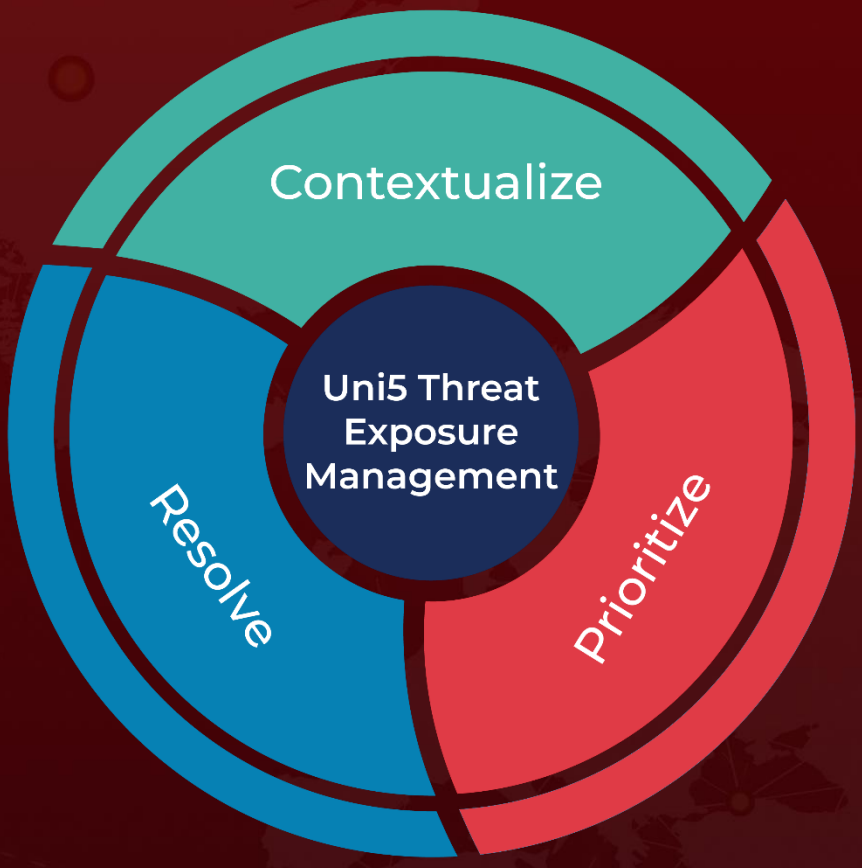
References

https://www.trendmicro.com/en_in/research/25/i/evilai.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

September 15, 2025 • 6:00 AM

More at www.hivepro.com