TIR-20260520 Everything You Need to Know About the EvilAI Malware Campaign

5/20/2026

Prepared for:

Aspire Technology Partners
25 James Way
Eatontown, NJ 07724

NOTICE:

This document is marked TLP: CLEAR, allowing recipients to share this information globally without any disclosure limitations.

This report is governed by the terms outlined in the Master Services Agreement (MSA) or any other master agreement between Aspire Technology Partners and the client receiving this report, along with the Statement of Work (SOW) or Order detailing the services that led to its creation.

Contributor(s)

Portia S. Cole
CTI Threat Researcher
Aspire Technology Partners
pcole@aspiretransforms.com

TABLE OF CONTENTS

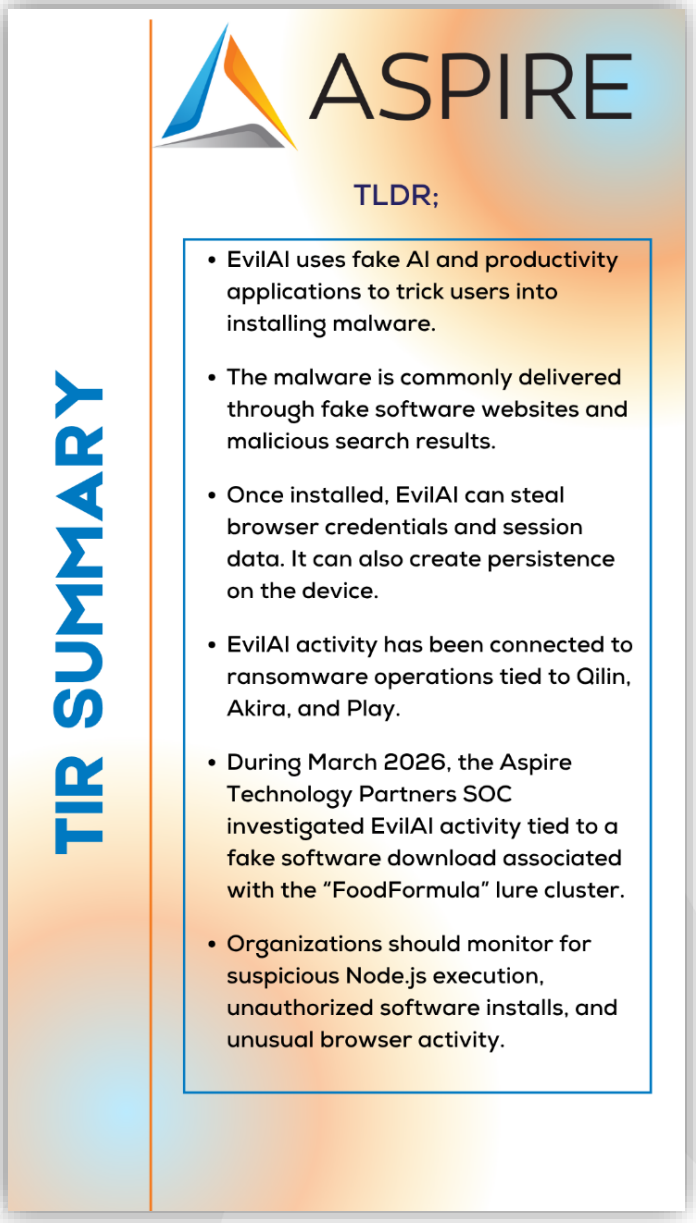
Executive Summary 3
EvilAI Malware 4
Threat Actors Who Use It 5
Aspire Case Study 7
Recent Attacks 8
Conclusion 9
Recommendations 9
MITRE MAP 11
Aspire Protects 11
Indicators of Compromise (IoCs) 12
Supporting Documentation 13
Appendix II: Disclaimer 14

Executive Summary

EvilAI is a malware campaign that hides inside fake productivity and AI-related applications. The user may think they are downloading a helpful tool, such as a PDF editor or AI utility. In reality, the malware runs in the background after the application is installed.

EvilAI has been linked to Initial Access Broker activity. Those brokers may use EvilAI to compromise environments and then sell that access to ransomware groups such as Qilin, Akira, and Play.

Aspire Technology Partners observed EvilAI activity during March 2026. The incident involved a malicious installer downloaded through Google Chrome from a fake domain. We will look at how EvilAI works, how ransomware groups are using it, and why organizations continue falling for these malicious applications.



EvilAI Malware

EvilAI is a malware campaign that was first publicly documented in 2025. The campaign uses fake applications that look like normal productivity software to hide malicious activity. Known lure applications include PDF editors, browser tools, recipe management software, manual finder utilities, and AI-themed applications. Many of the programs partially function as advertised, which lowers user suspicion and allows the malware to remain active longer before detection.

The malware is distributed through newly registered domains, malicious search advertisements, SEO manipulation, fake software portals, forums, and promoted social media links. Victims are typically convinced they are downloading free utilities or AI-enhanced software designed to improve productivity. Once executed, the applications launch hidden JavaScript payloads through `Node.js` while simultaneously presenting a legitimate-looking interface to the user. Researchers observed the malware using scheduled tasks, registry Run keys, and startup shortcuts to maintain persistence after reboot.

Browser Compromise

EvilAI targets Google Chrome and Microsoft Edge browsers. The malware steals browser session data, saved credentials, and authentication tokens. Many organizations use browsers to access Microsoft 365, VPN portals, cloud platforms, and internal systems. Researchers also observed the malware checking for installed security products before deploying additional payloads.

One of the more advanced aspects of EvilAI is its use of AI-generated obfuscation and anti-analysis logic. The malware has been observed using anti-analysis loops, Unicode homoglyph encoding, encrypted C2 traffic, and staged payload delivery. Some variants also used valid digital signatures obtained through fake shell companies created to acquire code-signing certificates. These tactics help the malware appear legitimate and avoid detection by traditional antivirus tools.

How Threat Actors Deliver EvilAI

- Malicious search advertisements
- SEO-poisoned search results
- Fake software download portals
- Social media promotion links
- Forum links advertising free utilities

- Trojanized AI and productivity applications
- Fake PDF editors and browser tools
- Downloads initiated through Google Chrome and Edge

Threat Actors Who Use It

EvilAI activity has been connected to ransomware groups including Qilin, Akira, and Play. In several cases, the malware was used to gain access to a system before additional malware or ransomware activity took place. It has also been observed stealing credentials and collecting information about the environment. In some cases, the malware maintained access for later use.

Qilin

Qilin is a ransomware operation believed to operate from Russian-speaking regions. The group became known for targeting healthcare, manufacturing, legal, and enterprise organizations through double-extortion attacks. Qilin operators typically steal sensitive data before encrypting systems, allowing them to pressure victims with both operational disruption and data leak threats.

EvilAI activity has also been observed in operations associated with Qilin. In several cases, the malware was used to gain access to a system before additional malware or ransomware activity took place. It has also been observed collecting credentials and creating persistence before the attackers moved further into the network.

Qilin TTPs

- Phishing and malicious software distribution
- Credential theft and browser session compromise
- Data exfiltration before encryption
- Use of legitimate remote administration tools
- Double-extortion tactics

Akira

Akira appeared in 2023 and quickly became one of the more active ransomware groups targeting organizations in North America and Europe. The group has targeted healthcare, education, retail, legal, and manufacturing organizations. Akira is known for using stolen credentials, VPN access, and remote access tools to move through a network after gaining entry.

EvilAI activity has also been linked to operations connected to Akira. In several cases, the malware was used to collect credentials, gather information about the environment, and maintain access before additional ransomware activity occurred. Some EvilAI variants were also observed checking for installed security software before attackers moved further into the network.

Akira TTPs

- Credential harvesting
- VPN and remote access abuse
- Browser session theft
- Lateral movement using legitimate tools
- Data theft before ransomware deployment

Play

Play is a ransomware group that has targeted government, retail, transportation, and technology organizations around the world. The group is known for moving quickly after gaining access to a network. Play operators often steal data and use compromised credentials or remote access tools to move through the environment.

EvilAI activity has also been connected to operations tied to Play. The malware has been observed creating persistence, communicating with external infrastructure, and collecting information about the environment before additional malware activity occurred. Some cases also linked the malware to staged payload delivery before ransomware deployment.

Play TTPs

- Initial access through compromised credentials
- Data theft and extortion

- Use of encrypted C2 channels
- Persistence through scheduled tasks and registry keys
- Reconnaissance of enterprise environments

Aspire Case Study

KitchenCanvas Installer Detected After Chrome Download

During March 2026, Aspire Technology Partners' SOC observed activity tied to the EvilAI malware campaign. The incident involved a suspicious installer named `KitchenCanvas_341652.exe` downloaded through Google Chrome from the domain foodformulasetup[.]com. Shortly after execution, Cisco Secure Endpoint generated an exploit prevention alert tied to the file. Analysts also observed suspicious DLL activity spawning from the executable after installation.

At the time of the incident, the file showed little or no malicious detections in public scanning tools. This matched other EvilAI cases where the fake applications initially appeared legitimate and avoided detection. Aspire's SOC reviewed activity on the device, checked the file's execution history, examined the Google Chrome download activity, and searched for related domain activity in Cisco Umbrella. Analysts confirmed the file had only executed on a single device during the investigation.

After the alerts were triggered, the endpoint was manually isolated from the network. SOC analysts started a full scan, blocked the domain through Cisco Umbrella, and reviewed the device for additional suspicious activity. The customer later chose to reimage the system as a precaution. No ransomware deployment or widespread compromise was identified during the investigation. However, the incident showed that these applications can still trigger suspicious activity while appearing normal to the user.

What Could Have Prevented the Incident

The incident started with a software download from a malicious website tied to the EvilAI campaign. Although the file initially appeared legitimate, a few steps may have reduced the risk of execution and compromise.

- Avoid downloading unknown software from search results or newly registered domains.

- Verify publishers and software reputation before executing downloaded applications.
    - Users should confirm the software publisher is legitimate and check the file reputation in tools like VirusTotal before opening downloaded files.

Recent Attacks

Qilin Attack on Asahi Group

In September 2025, Asahi Group Holdings reported a cyberattack that disrupted production at six beer plants in Japan. Days later, Qilin claimed responsibility for the attack and posted screenshots of alleged internal company documents online. The group also claimed to have stolen more than 9,300 files totaling roughly 27 GB of data. Beer production was temporarily disrupted before operations resumed on October 2, 2025. Security researchers later connected EvilAI activity and broader initial access operations to ransomware groups including Qilin.

Akira Attack Against Manufacturing Organizations

During 2025, Akira significantly increased attacks against manufacturing, healthcare, retail, and education organizations across North America and Europe. The group continued targeting organizations by using stolen credentials, VPN access, and remote access tools to move through compromised networks. Researchers also observed EvilAI-related activity overlapping with other ransomware operations tied to credential theft and staged malware delivery before encryption events occurred.

CONCLUSION

The EvilAI campaign relies heavily on user trust. The malicious applications used to deliver the malware often appear legitimate and may partially function after installation. In many cases, users do not realize anything suspicious has happened until security tools generate alerts or additional malware activity begins.

Applications associated with EvilAI are designed to look professional and blend in with normal user activity. Many organizations rely heavily on browsers and cloud platforms, which gives the malware opportunities to steal credentials and browser session data after execution. EvilAI is a reminder that some of the most convincing malware now looks like software people would normally trust and use every day.

Below is a recap of how the malware is delivered and what users and organizations should watch for:

What is the threat?

- Fake productivity and AI software hiding malware
- Browser credential and session theft
- Initial access operations tied to ransomware activity

What does the threat look like?

- Fake PDF editors, browser tools, and utility applications
- Downloads from malicious advertisements and fake software portals
- Node.js execution, scheduled tasks, and encrypted C2 traffic

RECOMMENDATIONS

Organizations should take malicious productivity software and AI-themed applications seriously, especially when employees download them from search results or third-party websites. Security teams should monitor for suspicious browser activity, unauthorized software installs, unusual Node.js execution, and other behavior that may indicate malware activity after installation.

Recommendations for Users

- Avoid downloading unknown utilities from search engines or social media advertisements.
- Download software only from trusted vendor websites instead of third-party download portals or promoted search results.
- Report suspicious browser behavior or unexpected application activity.
- Avoid storing unnecessary credentials in browsers.
- void running software that requests unexpected browser access or launches additional background processes after installation.

Recommendations for Organizations

- Monitor Node.js execution on enterprise endpoints.
- Restrict unauthorized software installations.
- Implement application allowlisting where possible.
- Monitor for scheduled task creation and new registry Run key activity tied to recently downloaded applications.
- Use DNS filtering to block malicious download domains.
- Monitor browsers for unusual credential access, session theft activity, or forced browser process termination.
- Review EDR telemetry for suspicious DLL spawning and JavaScript execution.
- Investigate newly observed software domains before allowing enterprise-wide access.

Note! *We value your feedback and want to make sure these reports are as helpful as possible. Take a minute to let us know what worked and what could be better by completing this form. Your input helps us improve what we deliver to your company.*

MITRE MAP

Initial Access	T1204 – User Execution
Execution	T1059.007 – Command and Scripting Interpreter: JavaScript
Persistence	T1053.005 – Scheduled Task/Job: Scheduled Task T1547.001 – Boot or Logon Autostart Execution: Registry Run Keys/Startup Folder
Credential Access	T1555 – Credentials from Password Stores
Defense Evasion	T1027 – Obfuscated Files or Information
Command and Control	T1071.001 – Application Layer Protocol: Web Protocols

ASPIRE PROTECTS

- **Aspire Managed XDR (MXDR)**
  - Aspire Managed XDR (MXDR) combines next-generation eXtended Detection and Response (XDR) technology, a 24x7 security operations center (SOC), and the expertise of a US-based team of security professionals to identify and respond to threats across a broader attack surface.

  - Building on the existing capabilities of Managed Detection and Response (MDR), Aspire Managed XDR integrates and correlates telemetry from endpoints, network, cloud, email, identity, and more. This advanced platform creates valuable context enabling end-to-end visibility across all threat vectors. Experienced security analysts and incident responders deliver 24x7 threat detection, analysis, and investigations – with both automated and human-led response actions to quickly mitigate cyberattacks.

- **Aspire Managed Detection and Response (MDR)**
  - Accelerate the maturity of your security operations and reduce risk with faster threat detection and response capabilities. Aspire MDR delivers

around-the-clock protection across cloud, network, and endpoints in one integrated solution.

- Our team of experts act as an extension of your IT operations to quickly identify and mitigate security threats before they impact your business.

- **Aspire Incident Response**
  - The ability to respond effectively to data breaches is critical to every organization. When attacks occur, IT leaders need a process that will ultimately maintain business continuity, protect the company reputation, and avoid fines, legal fees, and remediation costs.

  - Aspire offers incident response services to help you prepare for, manage, and recover from data breaches and network attacks. An experienced team uses industry-leading threat intelligence and the most current security technology to quickly respond to attacks, reduce damage, and minimize exposure.

INDICATORS OF COMPROMISE (IOCS)

Domains

- foodformulasetup[.]com
- 9mdp5f[.]com
- 5b7crp[.]com
- mka3e8[.]com
- y2iax5[.]com
- abf26u[.]com

File Names

- KitchenCanvas_341652.exe
- ManualFinderApp.exe
- PDF Editor.exe
- justaskjacky.exe
- manualshq.exe

SHA256 Hashes

- 3c1dbc3f56e91cc79f0014850e773a7f12bbfef06680f08f883b2bf12873eccc
- 8ecd3c8c126be7128bf654456d171284f03e4f212c27e1b33f875b8907a7bc65
- 49a4442e73521ecca8e56eb6dbc33f31eb7cfa5e62a499e552bcd29a29d79d8a
- b0c321d6e2fc5d4e819cb871319c70d253c3bf6f9a9966a5d0f95600a19c0983
- cb15e1ec1a472631c53378d54f2043ba57586e3a28329c9dbf40cb69d7c10d2c

SUPPORTING DOCUMENTATION

EvilAI Operators Use AI-Generated Code and Fake Apps for Far-Reaching Attacks | Trend Micro (US)

EvilAI

How EvilAI Tried to Speed Run a Triple Ransomware Attack

EvilAI Malware Mimics Legitimate Tools

EvilAI Operators Use AI-Generated Code and Fake Apps for Far-Reaching Attacks - Gurucul

EvilAI: From Fake App to Full C2

#StopRansomware: Play Ransomware — FBI

AI-Enhanced Malware Sports Super-Stealthy Tactics

Akira Ransomware: In-Depth Analysis, Detection, and Mitigation

EvilAI as AI-enhanced Tools to Exfiltrate Sensitive Browser Data and Evade Detections - Cyber Security News

RH-ISAC | EvilAI Malware Impersonating AI Tools to Target Manufacturing & Retail and Hospitality Organizations - RH-ISAC

Customer Service - TIR-20251112 Qilin Ransomware - Customer Support

Customer Service - TIR-20250128 Akira Ransomware - Customer Support

#StopRansomware: Play Ransomware | CISA

Akira Ransomware Threat Actor Profile - Tactics, Techniques, and Updates | Huntress

APPENDIX II: DISCLAIMER

This document and its contents are not intended to serve as legal advice and should not be used as a substitute for it. The results of a Security Risk Assessment are intended to guide the implementation of diligent measures to reduce the risk of potential vulnerabilities being exploited to compromise data.

While the Services and this report may offer information that the Client can use to support its compliance efforts, the responsibility for evaluating and fulfilling compliance obligations rests solely with the Client, not Aspire. This report does not guarantee or assure the Client's compliance with any law, regulation, or standard.