EvilAI Malware Campaign Using Fake Productivity and AI Applications to Steal Credentials and Stage Further Malware

TL;DR

Organizations are seeing an increase in detections tied to the EvilAI malware campaign, which disguises malware as legitimate AI tools, PDF editors, browser utilities, and productivity software. The malware is commonly delivered through fake websites, sponsored search results, malvertising, and forum links.

Once installed, EvilAI can interact with Google Chrome and Microsoft Edge to steal stored browser credentials and session data, establish persistence, communicate with command-and-control (C2) infrastructure, and stage additional malware.

Researchers have linked the activity to Initial Access Broker operations that may later sell access to ransomware groups such as Qilin, Akira, and Play.

Overview

Aspire has observed customer detections related to the EvilAI malware campaign. Threat actors are distributing the malware through fake software installers posing as AI tools, PDF applications, browser utilities, and other free programs. Reported lure applications include:

- AppSuite
- Epi Browser
- JustAskJacky
- Manual Finder
- OneStart
- PDF Editor
- Recipe Lister
- Tampered Chef

The campaign relies on social engineering rather than exploiting a specific CVE. Threat actors use malicious advertisements, SEO-poisoned search results, social media links, and fake download pages to convince users to install the software themselves.

Once executed, EvilAI can interact with Google Chrome and Microsoft Edge to collect stored credentials, browser session data, and cookies. The malware also establishes persistence through scheduled tasks and registry Run keys before communicating with command-and-control (C2) infrastructure over HTTPS. Researchers observed scheduled tasks using the naming pattern `sys_component_health_{UID}`.

Organizations may continue seeing repeated detections because employees encounter these fake applications across multiple websites, ads, and search results. Many of the programs appear legitimate and function as they should, making them harder for users to recognize as malicious.

Researchers also identified EvilAI as a possible staging mechanism for additional malware. Reporting links the activity to Initial Access Brokers that may sell compromised access to ransomware groups including Qilin, Akira, and Play. Secondary payloads associated with the campaign include `ManualFinderApp.exe`, which has been tied to backdoor and credential theft activity.

Aspire Protects

- Block known malicious domains associated with EvilAI activity.
- Restrict unauthorized software installations where possible.
- Advise employees **not to download AI tools or free software from advertisements or unknown websites.**
- Monitor for suspicious scheduled tasks such as `sys_component_health_{UID}.`
- Investigate browser credential theft activity involving Google Chrome or Microsoft Edge.
- Reset credentials and revoke active sessions if compromise is suspected.
- Monitor for secondary payload delivery or ransomware-related activity after initial detection.

TTPs to Watch

Initial Access

- Drive-by Compromise [T1189] – The threat actor may use malicious websites, sponsored advertisements, and SEO-poisoned search results to distribute fake software installers.

Execution

- User Execution: Malicious File [T1204.002] – The threat actor may rely on users to manually download and execute fake AI tools and productivity software.

Persistence

- Scheduled Task/Job: Scheduled Task [T1053.005] – The threat actor may create scheduled tasks such as `sys_component_health_{UID}` to maintain persistence after reboot.

Credential Access

- Credentials from Password Stores [T1555] – The threat actor may attempt to collect stored browser credentials from Google Chrome and Microsoft Edge.
- Steal Web Session Cookie [T1539] – The threat actor may collect browser session cookies to hijack authenticated sessions.

Command and Control

- Application Layer Protocol: Web Protocols [T1071.001] – The threat actor may communicate with external infrastructure over encrypted HTTPS traffic.

IoCs

Domains

- usermanualvault[.]com
- chataigpt[.]pro

File Names

- ManualFinderApp.exe
- out.exe
- ManualFinder.msi

Scheduled Task Artifacts

- sys_component_health_{UID}

Runtime / Process Indicators

- AppData\Local\Programs\node\node.exe

Targeted Industries

Organizations that rely heavily on browsers, downloadable utilities, and AI-related productivity tools may encounter this activity.

- Education
- Energy
- Finance
- Healthcare
- Legal
- Manufacturing
- Public Sector
- Retail

Aspire Service Offerings

- **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 cyber attacks.
- **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.

Supporting Documentation

EvilAI
EvilAI Malware Masquerades as AI Tools to Infiltrate Global Organizations
TamperedChef serves bad ads, with infostealers as the main course | SOPHOS
Infostealers Strike Again: Malicious Installers Pass Through EDRs Undetected – CyberProof
EvilAI Operators Use AI-Generated Code and Fake Apps for Far-Reaching Attacks | Trend Micro (US)
EvilAI: From Fake App to Full C2
How EvilAI Tried to Speed Run a Triple Ransomware Attack