

Watering Hole Attack Targets EmEditor Users with Information-Stealing Malware

 trendmicro.com/en_us/research/26/a/watering-hole-attack-targets-emeditor-users.html

January 22, 2026



Cyber Threats

TrendAI™ Research provides a technical analysis of a compromised EmEditor installer used to deliver multistage malware that performs a range of malicious actions.

By: Don Ovid Ladores, Yuya Sato, Yosuke Akiho Read time: 4 min (1191 words)

Key takeaways

- TrendAI™ Research provides an analysis of a software supply chain compromise involving EmEditor, a text editor widely used by developer communities globally. A compromised installer was used to deliver multistage malware that performs a range of malicious actions.
- The compromised version of the installer is capable of credential theft, data exfiltration, and follow-on intrusion through lateral movement. Because malicious behavior is deferred until after installation, it can bypass early detection and increase dwell time, raising the likelihood of operational disruption.
- Companies using Windows-based, third-party software distributed through public download channels are exposed to this risk. CISOs should check whether activities originating from trusted installers and developer tools are consistently monitored.

- TrendAI Vision One™ detects and blocks the IOCs discussed in this blog. TrendAI™ customers can also access tailored hunting queries, threat insights, and intelligence reports to better understand and proactively defend against this attack.

In late December 2025, EmEditor, a highly extensible and widely used text, code, and CSV editor developed by U.S.-based Emurasoft, published a [security advisory](#) warning users that its download page had been compromised. The attackers' objective was to distribute a compromised version of the program to unsuspecting users.

Figure 1. EmEditor posting an advisory regarding the compromise to their webpage [download](#)

EmEditor has longstanding recognition within Japanese developer communities as a recommended Windows-based editor. This suggests that the attackers are targeting this specific user base, or that they have a particular target among EmEditor users and used the compromised download page as delivery mechanism.

However, the threat actor responsible for this attack has yet to be identified. The timing also suggests that the attackers might have taken advantage of the year-end holiday period, when reduced staffing or more relaxed routines can increase the likelihood of security lapses.

Technical analysis of a compromised version of the installer

A compromised version of the installer is downloaded from the website of EmEditor. The package (an .MSI file) is modified such that once executed, it will spawn a PowerShell command to retrieve its first-stage code, which is located at a URL (EmEditorjp[.]com) crafted to make it look legitimate.

Figure 2. The compromised installer file has its CustomAction script modified to execute a malicious command. [download](#)

The first-stage payload then connects to two similar-looking URLs to retrieve two more scripts, which will be its main payload. The PowerShell script is obfuscated using a mix of string manipulation techniques (e.g., Insert, Remove, Replace, Substring, Trim). This is apparent throughout the script and is consistent with its successive payloads. After decryption, the URLs are executed through the Invoke-WebRequest (IWR) method:

- hxxps://EmEditorgb.com/run/mg8heP0r (Credential Theft, Disable ETW)
- hxxps://EmEditorde.com/gate/start/2daef8cd (Gather System-Info, Geofencing)

Figure 3. Deobfuscated code of the first stage

The second payload, after proper deobfuscation, is found as its main antisecurity mechanism. It also has other functions:

- Disable PowerShell Event Tracing for Windows (ETW)
- Credential theft
- Process detection (identify the security software installed in the system)
- Anti-virtualization
- Taking screenshots

[download](#)

Figure 4. The deobfuscated malware code showing how it accesses the ETW to disable it (top), and how deobfuscated and organized code on the malware showing how it accesses the Credential Manager (bottom)

[download](#)

The other payload is responsible for a different set of functions, mainly the following:

- System Fingerprinting
- Geofencing
- Command-and-control (C&C) reporting and data exfiltration
- Registry checking (for security applications)

[download](#)

Figure 5. The deobfuscated malware code showing how it accesses the Registry to gather and check for installed applications (top), and the deobfuscated and organized code showing how it collects specific system information (fingerprinting)

[download](#)

Based on its geofencing behavior, we assess that the threat actors are likely of Russian origin, or those from the Commonwealth of Independent States (CIS). This aligns with a common pattern observed among groups from this region, where “friendly” countries are excluded to reduce legal and operational risk. It excludes:

- Armenia
- Belarus
- Georgia
- Kazakhstan
- Kyrgyzstan

The malware sends all collected information to its C&C server at:

`hxxps://cachingdrive[.]com/gate/init/2daef8cd.`

Another notable detail we saw is the consistent presence of the unique string “**2daef8cd**” on its communication, suggesting that it may likely resemble some sort of Campaign ID.

As of now, there are already a few recorded instances of the URL being accessed by EmEditor users, suggesting that some have already been likely compromised prior to the company's announcement.

Security best practices against software supply chain attacks

This incident challenges longstanding assumptions that trusted software can be treated as lower priority during triage, and that installations — even from official vendors — is inherently less risky than exploit-driven intrusion. The following best practices can help organizations strengthen their ability to detect and contain this kind of threat:

- **Validate installer integrity.** Confirm digital signatures and perform file integrity checks before execution, even when installers are downloaded from official vendor sites. Where possible, compare against a trusted reference to detect tampering or unauthorized modification.
- **Govern usage of PowerShell.** Apply controls around PowerShell execution and enable robust logging. Monitor for obfuscated scripts and network-enabled commands, which are commonly abused for payload retrieval and staging.
- **Preserve endpoint telemetry and visibility.** Actively monitor for attempts to disable or interfere with logging mechanisms. Protecting telemetry helps maintain detection coverage when attackers attempt to operate with reduced visibility.
- **Enforce the principle of least privilege to credentials and networks.** Limit which processes and accounts can access credential storage and restrict where privileged credentials can be used. Monitor authentication activity for anomalies and attempted lateral movement.

For developers and software publishers, this kind of attack shows that protecting how software is built and delivered is just as important as securing the application itself:

- **Secure download and hosting infrastructure.** Apply strict access controls and monitoring to download servers and back-end storages. Monitor for unexpected file changes, redirects, or modifications that could indicate tampering with distributed installers.
- **Publish verifiable integrity information.** Provide file integrity information and make verification steps explicit so that users can confirm installer authenticity prior to execution.
- **Prepare an incident response plan.** Define procedures for responding to suspected supply chain compromise, including takedown of affected installers, certificate revocation, user notification, and coordination with security vendors.

Proactive security with TrendAI Vision One™

[TrendAI Vision One™one-platform](#) is the industry-leading AI cybersecurity platform that centralizes cyber risk exposure management, security operations, and robust layered protection.

TrendAI Vision One™ Threat Intelligence Hub

[TrendAI Vision One™ Threat Intelligence Hubproducts](#) provides the latest insights on emerging threats and threat actors, exclusive strategic reports from TrendAI™ Research, and TrendAI Vision One™ Threat Intelligence Feed in the TrendAI Vision One™ platform.

Emerging Threats:

[Watering Hole Attack Targets EmEditor Users With Information-Stealing Malware](#)

TrendAI Vision One™ Intelligence Reports (IOC Sweeping)

[Watering Hole Attack Targets EmEditor Users With Information-Stealing Malware](#)

Hunting Queries

TrendAI Vision One™ Search App

TrendAI Vision One™ customers can use the Search App to match or hunt the malicious indicators mentioned in this blog post with data in their environment.

EMEDITOR Command Lines:

| *processCmd:(powershell AND (emeditorjp.com OR emeditorgb.com/run/mg8heP0r OR emeditorde.com/gate/start/2daef8cd OR cachingdrive.com/gate/init/2daef8cd))*

More hunting queries are available for TrendAI Vision One™ with Threat Intelligence Hub entitlement enabled.

Indicators of Compromise (IOCs)

The indicators of compromise for this entry can be found .
Tags

[Research](#) | [Cyber Risk](#) | [Articles, News, Reports](#) | [Cyber Threats](#)

Copyright ©2026 Trend Micro Incorporated. All rights reserved.

This website uses cookies for website functionality, traffic analytics, personalization, social media functionality and advertising. Our Cookie Notice provides more information and explains how to amend your cookie settings. [Learn more](#)