Lost in Translation: Threat Actors Use SEO Poisoning and Fake DeepL Sites to Distribute Gh0st RAT

By Defentive

Published: 2025-08-25 · Archived: 2026-04-05 17:54:57 UTC

Executive Summary

The Defensive Threat Research team has uncovered an ongoing malware campaign deploying Gh0st RAT through SEO poisoning and fake DeepL websites. This campaign primarily targets Chinese-speaking users, luring them into downloading malicious software disguised as the trusted DeepL translation tool. The downloaded payload is a remote access trojan known as Gh0st RAT — that enables attackers to surveil, control, and exfiltrate data from infected machines.

The campaign relies on manipulating search engine algorithms to push malicious domains to the top of search results. Once installed, Gh0st RAT establishes persistence and communicates with command-and-control (C2) servers, enabling long-term unauthorized access.

Press enter or click to view image in full size

Campaign Overview

Gh0st RAT is a longstanding and widely-used remote access trojan known for its stealth and control capabilities. Initially associated with espionage campaigns, it continues to be a preferred tool for threat actors targeting governments, businesses, and individuals.

This recent campaign showcases how SEO poisoning, a tactic where attackers manipulate search engine rankings, is being effectively used to deceive users seeking legitimate software. By creating convincing DeepL clones, attackers are able to trick users into infecting their own systems.

The campaign is currently active and primarily targets Chinese-speaking users. Threat actors are leveraging fake DeepL translation software websites as the lure, presenting them as legitimate download sources. These malicious sites are being promoted through SEO poisoning techniques, with a notable concentration of poisoned links appearing in Bing search results.

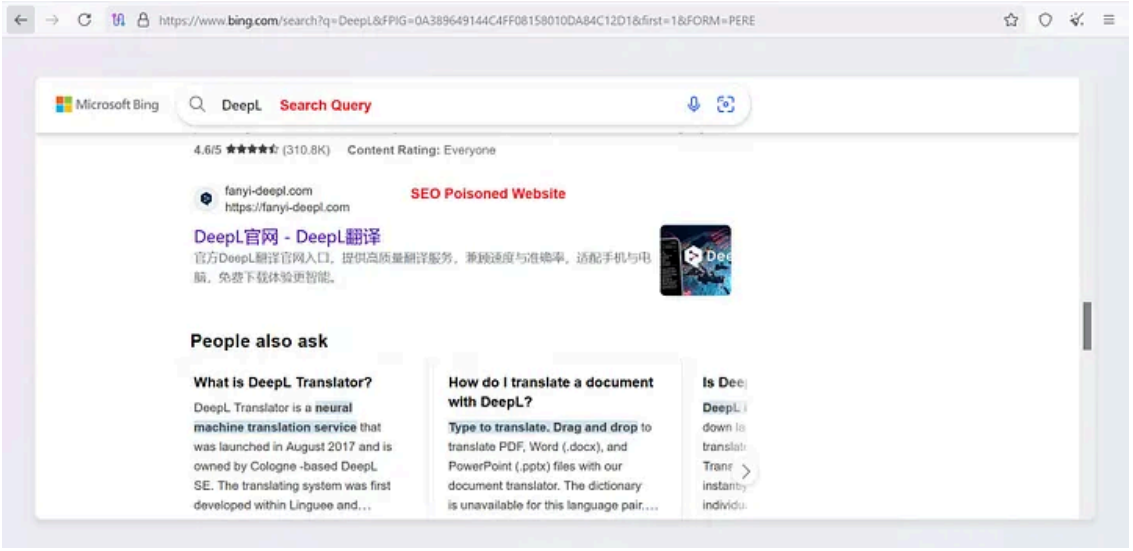
When users click on these links, they are led to archive files that conceal executable payloads. Once executed, these payloads install Gh0st RAT, enabling attackers to perform surveillance, steal sensitive data, and maintain

remote control over the victim's system.

Technical Analysis

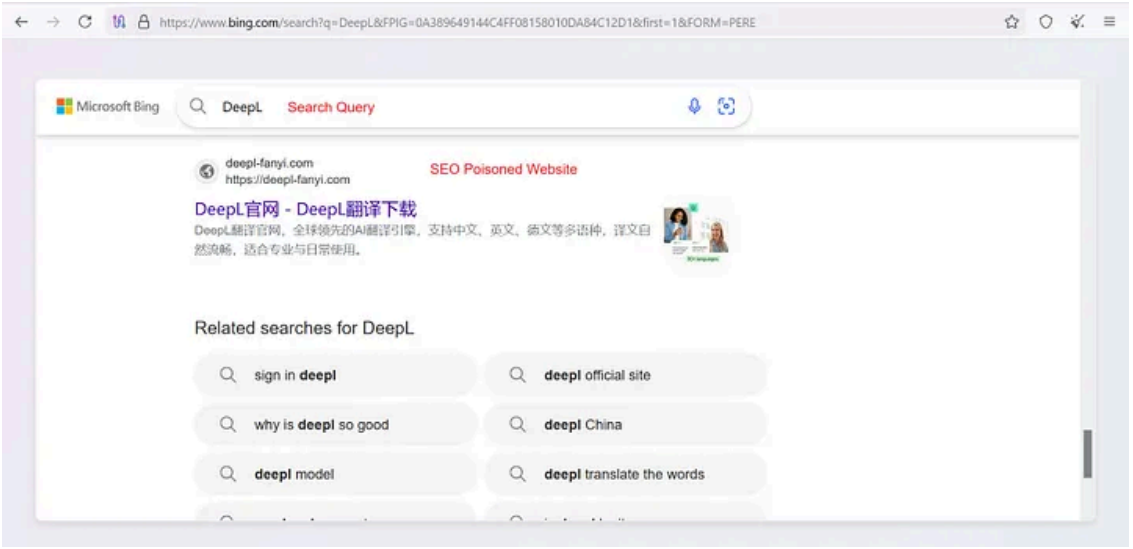
When a victim searches for keywords related to DeepL translation software in Chinese, they are often presented with poisoned search results prominently placed on page one of search engines — particularly Bing and Baidu, which are heavily used in the region. These top-ranked links lead unsuspecting users to fake DeepL download pages designed to impersonate the official DeepL Translator website (https://www.deepl.com/).

Press enter or click to view image in full size



Example 1 — SEO Poisoned Website

Press enter or click to view image in full size



Example 2 — SEO Poisoned Website

Our research team at Defentive successfully replicated this attack scenario, and the following section includes real-time screenshots and analysis of the malicious flow. The impersonated website closely mimics DeepL's branding and layout, featuring deceptive headers in Chinese such as: *"Experience DeepL Translator for Windows on the official DeepL website."*

Press enter or click to view image in full size

Website 1 — app-deepl[.]com

Press enter or click to view image in full size

Website 2 — deepl-fanyi[.]com

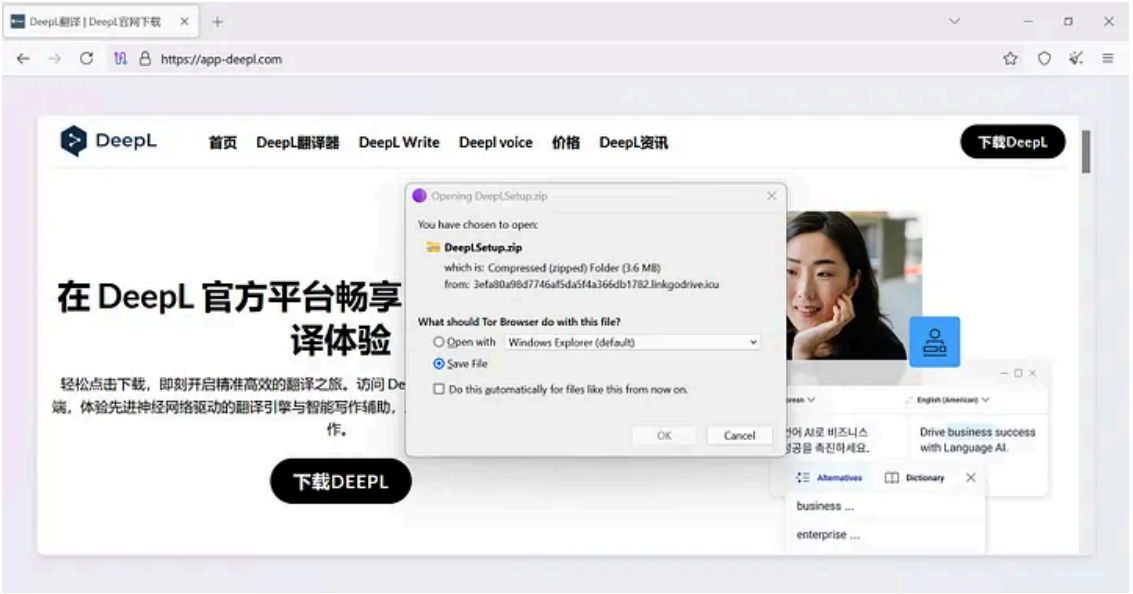
Press enter or click to view image in full size

Website 3 — fanyi-deepl[.]com

Once the victim clicks on the “Download DeepL” button, they are served a ZIP archive hosted on a suspicious domain controlled by the threat actor:

```
https[:]//3efa80a98d7746af5da5f4a366db1782[.]linkgodrive[.]icu/DeepLSetup[.]zip
```

Press enter or click to view image in full size



ZIP Download

The ZIP file — DeepLSetup.zip — contains a Microsoft Installer (MSI) file with the naming pattern:

```
DeepLSetup-{RandomDigits}.msi
```

Press enter or click to view image in full size

Fake DeepL Setup Installer (MSI)

Upon execution, the installer presents a legitimate-looking setup interface to create a false sense of authenticity, while silently deploying the Gh0st RAT malware in the background. This deceptive behavior enables the attacker to establish remote access to the victim's system without raising suspicion.

Get Defentive's stories in your inbox

Join Medium for free to get updates from this writer.

Remember me for faster sign in

During installation, the MSI drops a malicious executable — the actual Gh0st RAT payload — at the following location:

```
C:\\ProgramData\\S2ElrV\\mitey[.]exe
```

The Defentive research team confirmed this activity by capturing the following command-line execution, which initiates the malware under elevated privileges:

```
"C:\\WINDOWS\\Installer\\MSI3805[.]tmp" /EnforcedRunAsAdmin /DontWait "C:\\ProgramData\\S2ElrV\\mite
```

Persistence Mechanism

To maintain persistence on the compromised host, the malware modifies the Windows registry autorun key to execute the malicious binary at system startup:

- **Registry Key:** HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\Run

- **Name:** MyApplication
- **Value:** C:\ProgramData\S2ElrV\mitey[.]exe

Additionally, this variant drops a Windows Batch Script (bat) at the following path:

```
C:\\Users\\admin\\AppData\\Roaming\\5373631A[.]bat
```

The script continuously monitors the system for the presence of mitey[.]exe. If the process is not found, the script will re-launch it from its drop path, ensuring the RAT remains active even after termination attempts.

Command & Control (C2)

The Gh0st RAT malware communicates with its Command & Control (C2) server using the TCP protocol, which can often evade traditional security monitoring tools that rely on HTTP/HTTPS or DNS-based detections. This use of low-profile, custom TCP traffic introduces a significant blind spot, allowing threat actors to maintain covert access to compromised systems.

The Defentive Threat Research team successfully identified and intercepted the C2 infrastructure associated with this campaign. The active C2 endpoint was observed at:

```
154[.]23[.]221[.]136:1821
```

Further investigation revealed that this IP is hosted within the AS18186 (NEBULA-GLOBAL) autonomous system — an abused hosting provider based in Hong Kong, commonly leveraged in malware campaigns due to its lax abuse response and anonymity-friendly services.

Appendix

Indicators of Compromise

Domains

- deepl-fanyi[.]com
- fanyi-deepl[.]com
- app-deepl[.]com
- linkgodrive[.]icu

IP

- 154[.]23[.]221[.]136:1821

Hash

- e815f451f1f48085966b061cf8d6b0ebe88b77125ef23da4a00442f4705fb540

MITRE ATT&CK

Tactic Technique Technique ID Description / Relevance Reconnaissance Search Engine Discovery: Search Engines T1593.002 SEO poisoning used to manipulate search engine rankings for malicious sites. Initial Access Phishing: Spearphishing via Link T1566.002 Victims are lured via poisoned search results to click and download malware. Initial Access Drive-by Compromise T1189 Malicious websites serve malware without needing additional social engineering. Execution User Execution: Malicious File T1204.002 Users execute MSI or EXE files disguised as legitimate software. Execution Command and Scripting Interpreter: Windows Command Shell T1059.003 Batch files are used to monitor and reinitiate RAT processes. Persistence Registry Run Keys / Startup Folder T1547.001 Gh0st RAT adds a registry autorun entry to maintain persistence. Persistence Scheduled Task/Job: Scheduled Task T1053.005 Potential use for persistence (variant-dependent). Command and Control Non-Application Layer Protocol T1095 Gh0st RAT uses custom TCP communication for C2. Command and Control Application Layer Protocol: Web Protocols T1071.001 (optional) Some variants may use web-based protocols. Defense Evasion Obfuscated Files or Information T1027 Payloads may be packed or encrypted to evade detection. Defense Evasion Deobfuscate/Decode Files or Information T1140 Malware may decode itself during runtime. Exfiltration Exfiltration Over C2 Channel T1041 Data exfiltration uses the same C2 channel as command and control. Discovery System Information Discovery T1082 Malware gathers system data post-infection.

Conclusion

At Defentive, we don’t just react to cyber threats — we hunt them down before they reach your network. Our threat research team continuously monitors adversarial activity, tracks malware campaigns, and uncovers hidden infrastructure to deliver real-time, actionable intelligence. This Gh0st RAT campaign is just one example of how we proactively disrupt the attacker lifecycle and empower organizations with the insights they need to defend against even the most evasive threats. If you’re ready to elevate your threat detection and response capabilities, partner with Defentive — where cybersecurity meets precision.

https://www.defentive.com
