Pagina 8 - SonicWall NetExtender Trojan and ConnectWise Exploits Used in Remote Access Attacks

Classificações de Malware:

- cve (Exploit)
- trojan (Trojan)
- trojanized (Trojan)
- virus (Virus)
- infection (Virus)
- exploit (Exploit)
- backdoor (Backdoor)

Unknown threat actors have been distributing a trojanized version of SonicWall's SSL VPN NetExtender application to steal credentials from unsuspecting users who may have installed it."NetExtender enables remote users to securely connect and run applications on the company network," SonicWall researcher Sravan Ganacharisaid. "Users can upload and download files, access network drives, and use other resources as if they were on the local network."The malicious payload delivered via the rogue VPN software has been codenamedSilentRouteby Microsoft, which detected the campaign along with the network security company.SonicWall said the malware-laced NetExtender impersonates the latest version of the software (10.3.2.27) and has been found to be distributed via a fake website that has since been taken down. The installer is digitally signed by CITYLIGHT MEDIA PRIVATE LIMITED."This suggests that the campaign is targeting users searching for NetExtender on search engines like Google or Bing, and tricking them into installing it through spoofed sites propagated via known techniques like spear-phishing, search engine optimization (SEO) poisoning, malvertising, or social media posts.Two different components of the installer have been modified to facilitate the exfiltration of the configuration information to a remote server under the attacker's control.These include "NeService.exe" and "NetExtender.exe," which have be en altered to bypass the validation of digital certificates various NetExtender components and continue execution regardless of the validation results and exfiltrate the information to 132.196.198[.]163 over port 8080."The threat actor added code in the installed binaries of the fake NetExtender so that information related to VPN configuration is stolen and sent to a remote server," Ganachari said."Once the VPN configuration details are entered and the "Connect" button is clicked, the malicious code performs its own validation before sending the data to the remote server. Stolen configuration information includes the username, password, domain, and more."The development comes as G DATA detailed a threat activity cluster dubbed EvilConwi that involves bad actors abusing ConnectWise to embed malicious code using a technique calledauthenticodestuffing without invalidating the digital signature.The German cybersecurity companysaidit has observed a spike in attacks using this technique since March 2025. The infection chains primarily leverage phishing emails as an initial access vector or through bogus sites advertised as artificial intelligence (AI) tools on Facebook.These email messages contain a OneDrive link that redirects recipients to a Canva page with a "View PDF" button, which results in the surreptitious download and execution of a ConnectWise installer.The attacks work by implanting malicious configurations in unauthenticated attributes within the Authenticode signature to serve a fake Windows update screen and prevent users from shutting down their systems, as well as including information about the external URL to which the remote connection should be established for persistent access.What makes EvilConwi notable is that it offers malicious actors a cover for nefarious operations by conducting them using a trusted, legitimate, and maybe elevated system or software process, thereby allowing them to fly under the radar. ConnectWise has since revoked the certificate used to sign these binaries."By modifying these settings, threat actors create their own remote access malware that pretends to be a different software like an AI-to-image converter by Google Chrome," security researcher Karsten Hahn said. "They commonly add fake Windows update images and messages too, so that the user does not turn off the system while threat actors remotely connect to them."Discover real-time defense tactics to detect and block deepfakes, fake domains, and multi-channel scams before they cause damage.

We'll unpack how leading teams are using AI, privacy-first design, and seamless logins to earn user trust and stay ahead in 2025.Get the latest news, expert insights, exclusive resources, and strategies from industry leaders all for free.

Link: https://thehackernews.com/2025/02/finaldraft-malware-exploits-microsoft.html