Akira Ransomware: New Campaign Targets SonicWall Firewalls

Data: 2025-09-28 13:49:38

Autor: Inteligência Against Invaders

Redazione RHC:**28 September 2025 15:03**

Since late July 2025, a new wave of cyber attacks has been recorded targeting organizations equipped with SonicWall firewalls, with the active spread of the **Akira** ransomware.

According to researchers at Arctic Wolf Labs , malicious activity has significantly increased and continues to persist. Attackers gain initial access through **compromised SSL VPN connections** , successfully **bypassing multi-factor authentication (MFA)** . Once inside the network, they quickly move on to the encryption phase—in some cases, the dwell time before the ransomware was released was as short as **55 minutes** .

The exploited vulnerability and the role of stolen credentials

The hacks have been linked to CVE-2024-40766 , an access control vulnerability disclosed in 2024. The leading hypothesis is that *criminals previously harvested credentials from exposed and vulnerable devices, which they now exploited against already patched devices.* This explains why fully patched systems were compromised, a circumstance that initially fueled the hypothesis of a new zero-day exploit.

Another critical element concerns **SonicWall's OTP MFA** : attackers were able to authenticate even with accounts protected by this feature, increasing the severity of the campaign.

Techniques and tools used

Once they gain access via SSL VPN, the attackers:

- initiate internal network scanning to identify exposed ports such as **SMB (445), RPC (135), and SQL (1433)** ;
- use reconnaissance and lateral movement tools including **Impacket, SoftPerfect Network Scanner, and Advanced IP Scanner** ;
- create new administrative accounts and raise the privileges of existing ones;
- install remote access software such as **AnyDesk, TeamViewer, and RustDesk** to ensure persistence;
- establish hidden connections via **reverse SSH and Cloudflare Tunnels** .

To reduce the chance of detection, threat actors attempt to disable endpoint security solutions, such as **Windows Defender** and EDR.

In some cases, they use the **BYOVD (bring your own vulnerable driver)** technique to compromise systems at the kernel level and delete shadow volume copies to prevent any restores.

From data collection to ransomware release

Before starting the encryption, the attackers *exfiltrate sensitive information: the files are compressed with **WinRAR** and extracted using tools like **rclone** and **FileZilla*** . They then distribute the **Akira** ransomware, via executable files named *akira.exe* or *locker.exe* , encrypting network drives and launching the ransom note.

Recommendations for organizations

Arctic Wolf experts urge all organizations using SonicWall appliances to take immediate action.

In particular, it is recommended to **reset SSL VPN credentials** , including Active Directory-linked accounts, especially if systems have previously run firmware vulnerable to CVE-2024-40766. Simply applying patches is not considered sufficient if credentials have already been compromised.

Redazione
The editorial team of Red Hot Cyber consists of a group of individuals and anonymous sources who actively collaborate to provide early information and news on cybersecurity and computing in general.

Lista degli articoli