Akira Ransomware bypasses MFA on SonicWall VPNs

Data: 2025-09-29 11:01:51

Autor: Inteligência Against Invaders

Akira Ransomware bypasses MFA on SonicWall VPNs

Akira ransomware is targeting SonicWall SSL VPNs, bypassing OTP MFA on accounts, likely using stolen OTP seeds.

Since July 2025, Akira ransomware has exploited SonicWall SSL VPNs, likely using credentials obtained from the exploitation of the CVE-2024-40766 vulnerability, bypassing OTP MFA. Attacks spread quickly across sectors, with rapid post-login activity and short dwell times, making early detection crucial.

The Akira ransomware campaign, active since July 21, 2025, is targeting SonicWall NSA and TZ series devices running SonicOS 6–8, including recent 7.3.0 builds. The experts pointed out that despite SonicWall releasing updates to harden against brute force and MFA attacks, intrusions continue, even on patched devices. Researchers believe the attacks stem from credentials stolen during earlier exploitation of CVE-2024-40766, because it remains valid across firmware upgrades.

“Although the credential-based mitigations suggested by SonicWall are reasonable from a best practices standpoint, we are still not able to explain how threat actors were able to successfully bypass MFA. We will demonstrate this bypass below.” reads the report published by Arctic Wolf.

The Akira ransomware campaign shows initial access via malicious SSL VPN logins from VPS providers, which is unusual compared to typical broadband or SD-WAN logins. In some attacks, threat actors also used privacy VPNs. Both local and LDAP-synced accounts were targeted, including AD sync accounts not configured for VPN use. Over half of the intrusions involved OTP MFA accounts, with attackers successfully authenticating. Evidence suggests valid credentials, possibly from CVE-2024-40766 exploitation or stolen OTP seeds, though the MFA bypass method is still unclear.

The experts noticed that some intrusions showed evenly timed logins across multiple accounts from the same VPN IP, suggesting scripted automated access, though most cases involved 1–2 accounts.

After SSL VPN access, attackers moved rapidly, typically scanning the internal network within five minutes using tools like SoftPerfect and Advanced IP Scanner, targeting RPC/NetBIOS/SMB/SQL ports. They used Impacket (SMB sessions, WMIExec-style quser redirection) and RDP for lateral movement, and deployed AD enumeration with nltest, dsquery, Get-ADUser/Get-ADComputer, SharpShares, BloodHound, ldapdomaindump and related tools. The attackers saved outputs and reconnaissance files to C:ProgramData or Temp and sometimes opened in Notepad, indicating systematic discovery before further compromise.

Threat actors searched for VM storage/backups to access sensitive data and domain credentials,

though admins were often obtained by other means before extraction. They used sqlcmd and a novel PowerShell tool (supports MSSQL/Postgres) to extract and decrypt Veeam 11/12 credentials, retrieving DPAPI secrets and salts and temporarily altering PostgreSQL config (with a dated comment) to permit loopback connections. Attackers created local and domain admin accounts (e.g., sqlbackup, veean), added users to groups like “ESX Admins,” and installed RMMs (AnyDesk, TeamViewer, RustDesk). To maintain persistence, attackers used SSH reverse tunnels and Cloudflare Tunnel (cloudflared) installed as a service, OpenSSH opened to 0.0.0.0, and scripted installers using Invoke-WebRequest/Start-BitsTransfer.

Attackers used multiple techniques to evade detection, including disabling RMMs and deleting Volume Shadow Copies, turning off UAC for local accounts, and attempting to disable Defender/EDR. They used a BYOVD technique; they repackaged Microsoft’sconsent.exeand ran it from directories disguised as legitimate EDR software.

Threat actors installed WinRAR on servers and domain controllers, often placing the binary in ProgramData, to package files for exfiltration. They extracted and ran rclone (from ProgramData) or installed FileZilla (fzsftp.exe) to transfer RAR archives over SFTP/SSH to VPS hosts. Ransomware (akira/locker/w.exe) was deployed to multiple locations (e.g., C:lock, C:ProgramData) with per-drive options (-p, -s), usually encrypting environments within four hours, sometimes as fast as 55 minutes after access.

“The most crucial mitigation to this threat is to reset all SSL VPN credentials on SonicWall devices that have ever run firmware vulnerable to CVE-2024-40766, as well as Active Directory credentials on accounts used for SSL VPN access and LDAP synchronization.” concludes the report.

Follow me on Twitter:@securityaffairsandFacebookandMastodon

PierluigiPaganini

(SecurityAffairs–hacking,ransomware attack)