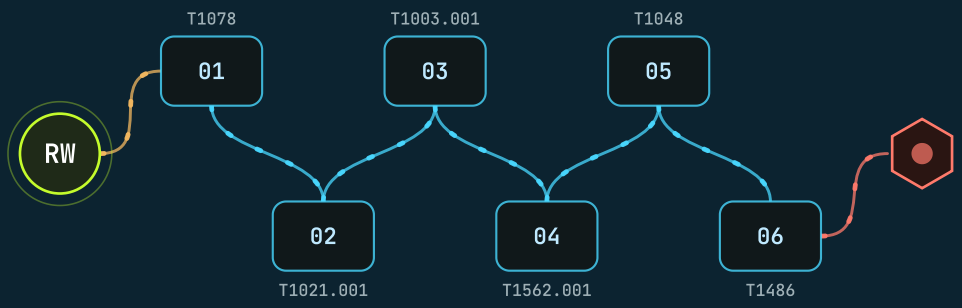


INTELLIGENCE BRIEF

Akira Is Still Breaking into SonicWall VPNs Two Years after the Patch

Akira is active in 2026 and still enters through SonicWall VPNs two years after the patch, and one affiliate now reboots into Safe Mode to blind EDR. Patch, reset VPN credentials, require MFA and watch failed logins.

EDITION
Fall/Winter 2026/2027 Edition
RW-04 · Ransomware group

PUBLISHED BY
Z7 Solutions LLC
Orlando, Florida

READ ONLINE
z7solutions.com
844-974-8669

01 At a Glance

STATUS

ACTIVE

Halcyon describes steady operations through the first half of 2026 and Huntress documented Akira intrusions in August and October 2026, although Qilin and The Gentlemen outpaced it in the second quarter. [11]

HEADLINE NUMBERS

$244.17M

ransomware proceeds Akira had claimed as of late September 2025 [1]

750

Akira leak-site claims in 2025 per the ransomware.live tracker, with 408 more through October 13, 2026 [17]

213,896

SonicWall VPN and management interfaces reachable online on August 24, 2026 [2]

7 minutes

from a VPN password spray to a successful login on an account with no MFA in August 2026 [3]

KEY FACTS

REPORTED STATUS

Active, with steady operations through the first half of 2026 [11]

INITIAL ACCESS

VPNs without MFA, reached with stolen or sprayed credentials or known Cisco and SonicWall flaws, plus spearphishing, RDP and SSH through routers [1]

KEY FLAW

SonicWall CVE-2024-40766, in CISA's Known Exploited Vulnerabilities catalog since September 9, 2024 with known ransomware use [6]

SPEED

Encryption within four hours of first access in almost all 2025 SonicWall intrusions Arctic Wolf analyzed; data theft in just over two hours in some cases [5]

PLATFORMS

Windows, VMware ESXi, Hyper-V and Nutanix AHV; the Rust-based Akira_v2 is the current encryptor [1]

PROCEEDS

About $244.17 million claimed as of late September 2025, per the FBI, CISA and partners [1]

02 What Happened

Akira is a ransomware-as-a-service operation that has hit organizations in North America, Europe and Australia since March 2023, and on November 13, 2025 the FBI, CISA and partners updated their warning to say it presents an imminent threat to critical infrastructure. Its 2025 surge came from mass abuse of SonicWall SSL VPNs, and that pattern continued into 2026. The front door has not changed: VPN accounts without MFA and a SonicWall flaw fixed in August 2024.

- The joint advisory update says Akira claimed about $244.17 million in proceeds as of late September 2025, encrypted Nutanix AHV virtual machine disks for the first time in June 2025, and has likely stopped using the older Megazord encryptor since 2024 in favor of the Rust-based Akira_v2.
- Arctic Wolf documented a SonicWall SSL VPN campaign that began on July 21, 2025, with logins from hosting-provider networks, internal scanning within five minutes and encryption in under four hours in almost all intrusions; SonicWall said it had high confidence the activity was not a zero-day and found significant correlation with CVE-2024-40766.
- ReliaQuest tied the incidents it analyzed to larger organizations that had acquired smaller ones, and counted more than 70 Akira victims in October 2025 alone from public-facing devices such as SonicWall SSL VPNs.
- On September 8, 2026 ThreatDown reported that its managed detection team handled multiple Akira cases involving a SonicWall device in recent weeks and counted 213,896 SonicWall interfaces reachable online on August 24, 2026.
- Huntress investigated an intrusion that began with a password spray on August 4, 2026 against a SonicWall SSL VPN with no MFA; a valid login landed within seven minutes, file shares were copied to cloud storage, the host was rebooted into Safe Mode to switch off EDR, and the encryptor then crashed on memory errors so no files were encrypted.

- A second Huntress case published on October 6, 2026 began with Remote Desktop access from a workstation the customer did not own, followed by stopped antivirus services, an LSASS memory dump, a GOST tunnel and Rclone exfiltration.

03 How It Works

01 Log in through an exposed VPN

MITRE ATT&CK T1078

Operators spray or reuse stolen credentials against VPNs that lack MFA and exploit flaws such as SonicWall CVE-2024-40766; Arctic Wolf saw the logins come from hosting-provider networks rather than home broadband. Spearphishing, RDP and unpatched Veeam servers are secondary routes.

02 Scan the network and move laterally

MITRE ATT&CK T1021.001

Within minutes of login operators scan with tools such as Advanced IP Scanner, NetExec and BloodHound, then move over RDP, SSH and SMB and add remote tools such as AnyDesk and RustDesk to blend in with administrators.

03 Create admin accounts, take credentials

MITRE ATT&CK T1003.001

Operators create domain accounts, in some cases named itadm, dump LSASS memory, run Mimikatz or LaZagne, and in one case copied domain controller disk files to extract the Active Directory database.

04 Blind the security tools

MITRE ATT&CK T1562.001

They uninstall or stop EDR, load vulnerable drivers (Arctic Wolf named rwdrv.sys and hlpdrv.sys), and in an August 2026 case rebooted a host into Safe Mode with Networking so EDR and Defender real-time protection did not start.

05 Steal data before encrypting

MITRE ATT&CK T1048

WinRAR gathers file shares and tools such as Rclone, WinSCP, FileZilla or s5cmd copy them to cloud storage or attacker servers, in some cases within about two hours of first access.

06 Encrypt and extort

MITRE ATT&CK T1486

Akira_v2 uses ChaCha20 with RSA, can encrypt only virtual machines or stop running ones, deletes shadow copies and drops fn.txt or akira_readme.txt; victims contact the group on a Tor site with a unique code and pay in Bitcoin.

04 Who Is at Risk

CISA says Akira mostly targets small and medium-sized businesses but also larger organizations, with a preference for manufacturing, educational institutions, information technology, healthcare, financial services and food and agriculture. Any organization with a SonicWall or other VPN that lacks MFA, or that kept old passwords after a firewall migration, is in scope.

- Schools and universities are named in CISA's list of preferred sectors.
- Manufacturing leads recent claims: 125 of the 408 Akira leak-site claims the ransomware.live tracker held for January 1 to October 13, 2026 were manufacturing, followed by professional services at 85 (a Z7 tally of the tracker's data, and the claims are the group's own).
- The United States is the most-listed country, with 216 of the 324 claims that carry a country tag in the same 2026 tracker data.
- Inherited or migrated VPN appliances are a repeat problem: ReliaQuest flags acquisitions, and SonicWall and ThreatDown flag local passwords that were not reset after a move from Gen 6 to Gen 7 firewalls.
- Managed service providers are exposed through customer VPNs: ThreatDown saw one MSP appear twice in its case data, hit through two separate customer environments.

Sectors in scope: manufacturing, education, information technology, healthcare and public health, financial services, food and agriculture, construction.

05 What Changed Since the Last Edition

EACH CHANGE WITH ITS SOURCE

01 SonicWall VPNs are still the main door two years after the fix. ThreatDown reported on September 8, 2026 that its managed detection team handled multiple Akira cases involving a SonicWall device in recent weeks and counted 213,896 SonicWall VPN portals and management interfaces reachable on August 24, 2026, against the 438,000 Bitsight figure the original edition quoted; the methods differ and reachable does not mean vulnerable.

SOURCE 2

02 A new defense evasion was documented. Huntress reported on August 12, 2026 an Akira affiliate who sprayed an SSL VPN with no MFA on August 4, logged in within seven minutes, copied file shares to a cloud bucket and rebooted into Safe Mode to disable EDR; the encryptor failed on memory errors, but the stolen data remains an extortion risk.

SOURCE 3

03 Another 2026 case started at Remote Desktop. Huntress (October 6, 2026) described Akira access over RDP from a workstation the customer did not own, followed by Bitdefender services stopped, an LSASS dump with procdump, a GOST tunnel and Rclone exfiltration to the cloud.

SOURCE 4

04 Akira is no longer the clear number two by leak-site volume. Check Point's Q2 2026 report names Qilin (279 victims) and The Gentlemen (269) as the top two, and the ransomware.live tracker shows 180 Akira claims in Q1 2026 and 124 in Q2, against 750 in all of 2025.

SOURCE 14

05 Incident-response data tells the same story. Coveware ranks Akira third with 9 percent of its Q2 2026 cases, down one place from Q1 2026.

SOURCE 12

06 A federal measure now exists beside the FBI's. FinCEN's December 2025 analysis of Bank Secrecy Act reports found Akira was the most-reported ransomware variant from 2022 to 2024, with 376 incidents and about $120.9 million in reported payments, a US-reported measure separate from the $244.17 million in claimed proceeds in the CISA advisory.

SOURCE 16

07 No arrest, takedown, sanction or indictment naming Akira was found. Halcyon's profile, updated July 27, 2026, lists no law enforcement action and describes steady operations through the first half of 2026.

SOURCE 11

06 What to Do Now

IN PRIORITY ORDER, HIGHEST IMPACT FIRST

01 DO FIRST **Require MFA on every VPN account, including local accounts on SonicWall and other firewalls, and alert on bursts of failed logins across many usernames from one source followed by a success.**

The August 2026 Huntress intrusion began with an MFA-less VPN account and a valid login seven minutes after the spray started.

02 **Update SonicWall firewalls to SonicOS 7.3.0 or later, then reset every local and Active Directory account that ever used the SSL VPN, including after any Gen 6 to Gen 7 migration.**

Patching does not undo credentials stolen earlier, and ThreatDown still ties Akira cases to the August 2024 flaw in September 2026.

03 **Disable SSL VPN if it is not needed, restrict management interfaces to trusted networks, and block or alert on VPN logins from hosting providers and countries where you do not operate.**

ThreatDown counted 213,896 SonicWall interfaces reachable online, and Arctic Wolf saw Akira logins arrive from hosting-provider networks.

04 **Run EDR with tamper protection on every server and endpoint, and alert on Safe Mode boots, msconfig or bcdedit changes, vulnerable driver loads and stopped security services.**

Akira uninstalls EDR, loads vulnerable drivers and in August 2026 used Safe Mode to switch protection off; Huntress noted its agent covered only a fraction of the hosts the attacker mapped.

05 **Alert on WinRAR archive creation across file shares, Rclone, s5cmd, FileZilla and large outbound transfers, and on unapproved remote tools such as AnyDesk, RustDesk, Ngrok and Cloudflare tunnels.**

Data theft comes first, often within hours of access, and a stopped encryptor still leaves stolen data to extort with.

06 **Patch Veeam Backup and Replication and VMware ESXi (CVE-2023-27532, CVE-2024-40711, CVE-2024-37085), keep backups offline and immutable, and test a restore of virtualized servers each quarter.**

CISA lists these flaws in Akira intrusions, and Akira encrypts ESXi, Hyper-V and Nutanix AHV virtual machines directly.

07 **After any acquisition or firewall migration, inventory every inherited VPN appliance and reset every credential before trusting it.**

ReliaQuest tied Akira's 2025 incidents to larger organizations that had acquired smaller ones, and migrated devices kept old local passwords.

08 **Decide in advance who declares a data breach and who talks to counsel and regulators, and treat any Akira indicator as a theft event even when nothing was encrypted.**

In the Safe Mode case the attacker had already stolen credentials and files, so extortion stayed possible; a 24/7 SOC, which Z7 Solutions™ provides for mid-size organizations, school districts and public agencies, is built to act in that early window.

07 Indicators

Indicators the sources publish, as they print them. Hunt with them, and check the source before you block.

FILE	Ransom notes named akira_readme.txt or fn.txt in C:\ and in each user's home directory [1]
FILE	Encrypted files ending in .akira, .powerranges, .akiranew or .aki [1]
BEHAVIOR	Domain administrative account named itadm created after initial access [1]
HASH	d2fd0654710c27dcf37b6c1437880020824e161dd0bf28e3a133ed777242a0ca (w.exe, Akira encryptor, SHA-256) [1]
HASH	3298d203c2acb68c474e5fdad8379181890b4403d6491c523c13730129be3f75 (Akira_v2, SHA-256) [1]
IP	38.114.123[.]167 (example SSL VPN login source published by Arctic Wolf, who also named hosting ASNs AS62240 and AS63023) [5]
BEHAVIOR	SSL VPN logins from virtual private server hosting networks rather than broadband providers [5]
FILE	Repackaged consent.exe used to load vulnerable drivers rwdrv.sys, churchill_driver.sys and hlpdrv.sys [5]
BEHAVIOR	Burst of failed VPN logins across many usernames from one source, followed by a success from the same address [3]
BEHAVIOR	msconfig.exe or bcdedit forcing a Safe Mode with Networking reboot; Kernel-Boot event 27 with SAFEBOOT:NETWORK and Kernel-General event 12 with BootMode 2 [3]
REGISTRY	AnyDesk added to the SafeBoot Network registry list before the reboot [3]

08 Sources

[1] **#StopRansomware: Akira Ransomware (AA24-109A, updated with new TTPs and IOCs)** CISA, FBI, DC3, HHS, Europol EC3 and international partners · April 18, 2024; updated November 13, 2025. https://www.cisa.gov/news-events/cybersecurity-advisories/aa24-109a

[2] **This SonicWall bug is 2 years old. Akira ransomware is still exploiting it.** ThreatDown (Malwarebytes) · September 8, 2026. https://www.threatdown.com/blog/this-sonicwall-bug-is-2-years-old-akira-ransomware-is-still-exploiting-it/

[3] **Akira Hits Safe Mode: Ransomware Rebooting Around EDR** Huntress · August 12, 2026. https://www.huntress.com/blog/akira-hits-safe-mode-ransomware-rebooting-around-edr

[4] **Up a Creek Without a Command Line: Mapping an Akira Ransomware Attack** Huntress · October 6, 2026. https://www.huntress.com/blog/mapping-akira-ransomware-attack

[5] **Smash and Grab: Aggressive Akira Campaign Targets SonicWall VPNs, Deploys Ransomware in an Hour or Less** Arctic Wolf Labs · September 26, 2025. https://arcticwolf.com/resources/blog/smash-and-grab-aggressive-akira-campaign-targets-sonicwall-vpns/

[6] **Known Exploited Vulnerabilities Catalog, entry for CVE-2024-40766 (SonicWall SonicOS)** CISA · added September 9, 2024; catalog feed released October 13, 2026. https://www.cisa.gov/known-exploited-vulnerabilities-catalog

[7] **CVE-2024-40766 record** NIST National Vulnerability Database · published August 23, 2024. https://nvd.nist.gov/vuln/detail/CVE-2024-40766

[8] **Akira ransomware exploiting critical SonicWall SSLVPN bug again** BleepingComputer · September 11, 2025. https://www.bleepingcomputer.com/news/security/akira-ransomware-exploiting-critical-sonicwall-sslvpn-bug-again/

[9] **Threat Spotlight: Akira Ransomware's SonicWall Campaign Creates Enterprise M&A Risk** ReliaQuest · November 25, 2025. https://reliaquest.com/blog/threat-spotlight-akira-ransomwares-sonicwall-campaign-creates-enterprise-m&a-risk/

[10] **Hitachi Vantara takes servers offline after Akira ransomware attack** BleepingComputer · April 28, 2025. https://www.bleepingcomputer.com/news/security/hitachi-vantara-takes-servers-offline-after-akira-ransomware-attack/

[11] **Threat group profile: Akira** Halcyon · updated July 27, 2026. https://www.halcyon.ai/threat-group/akira

[12] **Adverse cyber extortions are more common than commonly advised (Q2 2026 quarterly report)** Coveware by Veeam · July 29, 2026. https://coveware.com/2026/07/adverse-cyber-extortions-are-more-common-than-commonly-advised/

[13] **The State of Ransomware, Q1 2026** Check Point Research · May 11, 2026. https://research.checkpoint.com/2026/the-state-of-ransomware-q1-2026/

[14] **The State of Ransomware, Q2 2026** Check Point Research · August 13, 2026. https://research.checkpoint.com/2026/the-state-of-ransomware-q2-2026/

[15] **The State of Ransomware, Q3 2025** Check Point Research · November 13, 2025. https://research.checkpoint.com/2025/the-state-of-ransomware-q3-2025/

[16] **Financial Trend Analysis: Ransomware Trends in Bank Secrecy Act Data Between 2022 and 2024** FinCEN (US Treasury) · December 2025. https://www.fincen.gov/system/files/2025-12/FTA-Ransomware.pdf

[17] **Akira group victim records (public API, Z7 tally by discovery date)** ransomware.live · retrieved October 13, 2026. https://api.ransomware.live/v2/groupvictims/akira

NEXT STEP

What does this mean for your security?

Bring your questions about Akira, your environment and the controls you rely on. Talk through the most useful next step with Z7 Solutions LLC.

01 / Exposure

Bring one question about how this threat could affect your environment.

02 / Priorities

Bring your current safeguards, open gaps and budget questions.

ALSO IN THIS EDITION

- Qilin still tops most ransomware counts
  More from the edition · z7solutions.com/z7-cyber/qilin/
- Qilin still hits hospitals and infrastructure
  More from the edition · z7solutions.com/z7-cyber/qilin-part-2/
- LockBit 5.0 returns after Operation Cronos
  More from the edition · z7solutions.com/z7-cyber/lockbit/

CALL 844-974-8669

EMAIL sales@z7solutions.com

BOOK A SECURITY CONVERSATION — Book a Security Conversation ↗

Z7 Solutions™, Z7-Claw™ and Z7-Guard™ are trademarks of Z7 Solutions LLC.