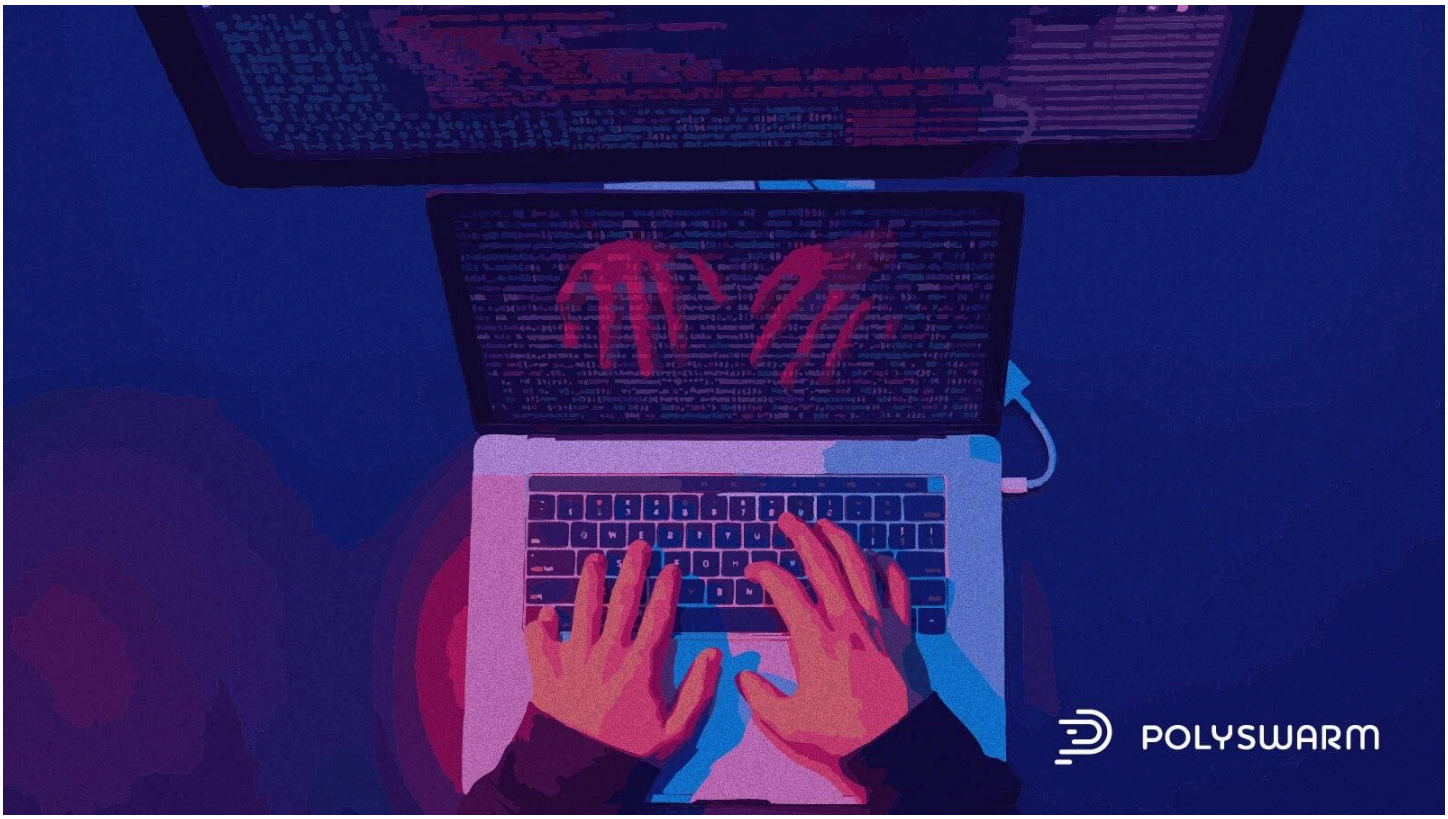
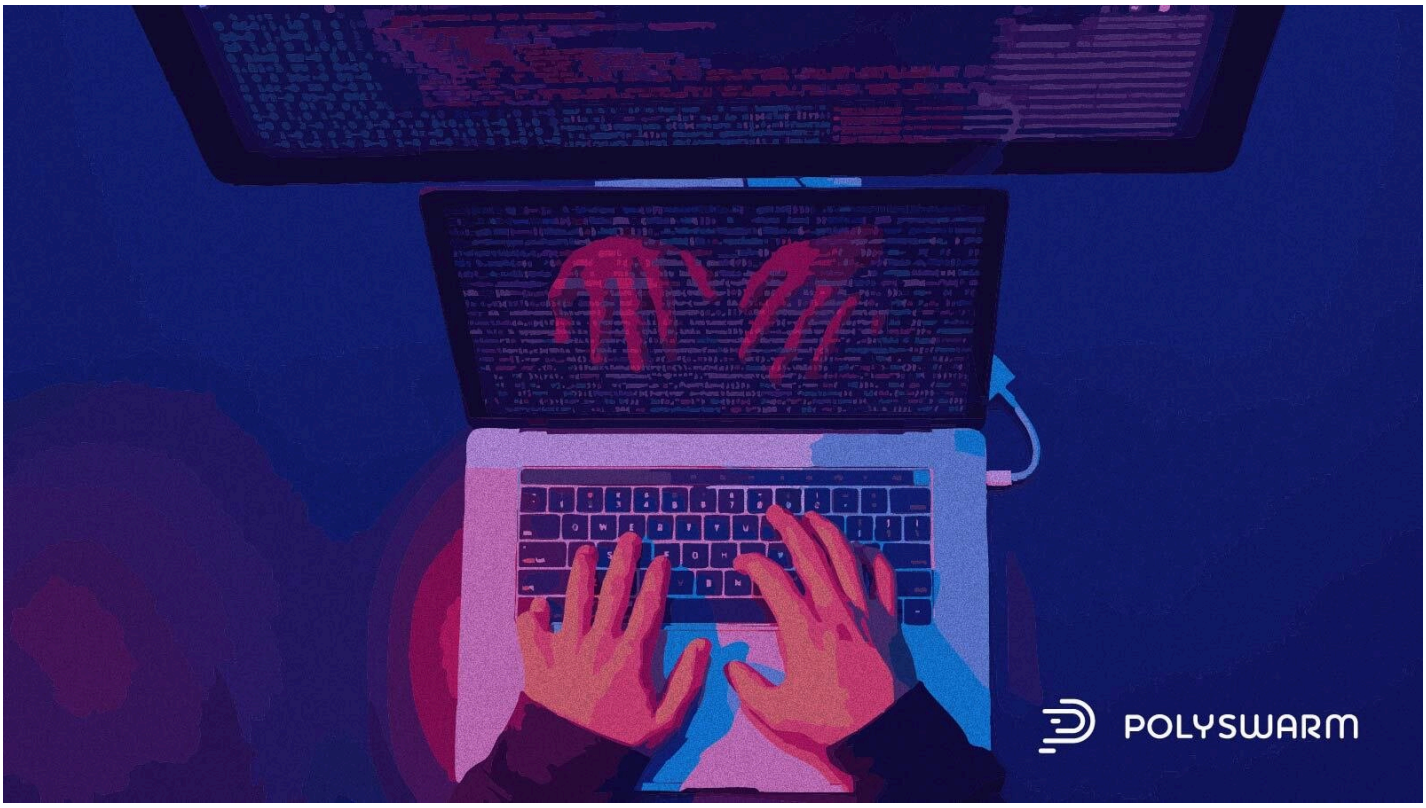
The PolySwarm Blog



Akira Reloaded

Oct 7, 2025 1:04:01 PM / by The Hivemind



Verticals Targeted: Real Estate, Insurance, Energy, Manufacturing, Legal Services, Healthcare, Construction, Retail, Agriculture, Finance, Business Services, Transportation, Software, Hospitality, Government, Telecommunications
Regions Targeted: US, Europe, South America, Australia, Canada, India, Africa

Executive Summary

A surge in Akira ransomware attacks since July 2025 exploits SonicWall VPNs via CVE-2024-40766, enabling rapid credential-based intrusions with dwell times as short as 55 minutes. Threat actors leverage stolen credentials, bypass MFA, and deploy tools such as Impacket and WinRAR for lateral movement and data exfiltration, targeting organizations across various sectors.

Key Takeaways

- Akira ransomware is deployed within hours, with some intrusions completed in under 55 minutes, emphasizing the need for swift detection and response.
- Threat actors exploit CVE-2024-40766, an improper access control vulnerability in SonicWall firewalls, to harvest credentials for malicious SSL VPN logins.
- Threat actors' use of Impacket for SMB-based discovery, WinRAR for data staging, and RMM tools like AnyDesk and RustDesk for persistence highlights a sophisticated attack chain.

- Successful authentication against MFA-enabled accounts suggests advanced credential theft techniques, though the exact method remains unclear.

Akira's Recent Surge in Activity

Since late July 2025, industry analysts have tracked a relentless Akira ransomware campaign targeting SonicWall SSL VPNs, exploiting a known vulnerability to deliver devastating attacks in under an hour. This campaign, ongoing as of September 2025, demonstrates a highly aggressive and opportunistic approach, compromising organizations across multiple sectors with alarming efficiency. Leveraging CVE-2024-40766, an improper access control flaw in SonicWall firewalls, threat actors gain initial access through malicious SSL VPN logins, often bypassing multi-factor authentication (MFA) with stolen credentials. The rapid execution of this attack chain underscores the critical need for robust detection and response mechanisms to protect enterprise environments. Arctic Wolf reported on this activity.

The campaign begins with malicious logins originating from virtual private server (VPS) hosting providers, a hallmark of this operation. These logins frequently target accounts synchronized with Active Directory via LDAP, including those with OTP-based MFA enabled. Notably, threat actors have achieved successful authentication within minutes, raising concerns about the efficacy of MFA in this context. While the precise method of bypassing MFA remains elusive, evidence suggests the use of previously harvested credentials, potentially stolen during earlier exploitation of CVE-2024-40766 in 2024. Affected SonicWall devices include NSA and TZ series running SonicOS versions 6 and 7, with some intrusions observed on recently patched firmware, indicating that patching alone is insufficient without credential resets.

Post-compromise, the attack chain is swift and methodical. Within five minutes of access, threat actors initiate internal network scanning using tools like SoftPerfect Network Scanner and Advanced IP Scanner, targeting ports such as 135 (RPC), 445 (SMB), and 1433 (SQL). The Python-based Impacket library facilitates discovery and lateral movement through anomalous SMBv2 session setup requests, often from hostnames like "kali" or "WIN." Active Directory enumeration follows, employing tools such as nltest, dsquery, and PowerShell cmdlets like Get-ADUser to map network assets.

Data exfiltration is a key objective, with WinRAR used to archive sensitive files, including text, PDF, and Office documents, into 3 GB chunks for transfer via tools like Rclone or FileZilla to VPS infrastructure. A novel PowerShell script was observed extracting credentials from Veeam Backup & Replication databases, supporting both MSSQL and PostgreSQL backends. This script decrypts credentials using DPAPI and Base64-encoded formats, targeting virtual machine backups to access sensitive data. Persistence is maintained through local and domain account creation, often masquerading as legitimate services, alongside remote management tools such as AnyDesk, RustDesk, and Cloudflared for command-and-control (C2).

To evade defenses, attackers disable endpoint detection and response (EDR) tools and Windows Defender using bring-your-own-vulnerable-driver (BYOVD) techniques, leveraging repackaged Microsoft binaries. Geofencing restricts ransomware execution in Eastern European and Central Asian locales, a common tactic

to avoid regional scrutiny. The ransomware, deployed as akira.exe or locker.exe, encrypts drives and network shares within hours, appending the .akira extension and employing a double-extortion model to coerce ransom payments. PolySwarm analysts consider Akira to be an evolving threat.

Targeting

In recent months, Akira has been observed targeting a variety of verticals and locales. Targeted verticals have included real estate, insurance, energy, manufacturing, legal services, healthcare, construction, retail, agriculture, finance, business services, transportation, software, hospitality, government, telecommunications, and others. Targets have included entities in the US, Europe, South America, Australia, Canada, India, and Africa.

Akira's RaaS and Affiliate Program Growth

In addition to exploitation of CVE-2024-40766, Akira's evolution as a Ransomware-as-a-Service operation and growing affiliate program has also contributed to its surge in activity. Emerging initially in 2023, the group has adapted by shifting tactics, including double extortion, and maintaining a high volume of campaigns across multiple industries.

Akira operates as a RaaS platform, meaning the core developers provide the ransomware toolkit, including encryptors, infrastructure, and leak sites, to independent affiliates who carry out attacks in exchange for a cut of the profits. This is typically 70-80% for affiliates, with 20-30% going to the core group. This model incentivizes rapid scaling, as affiliates handle the operational "heavy lifting" of initial access, lateral movement, and ransom negotiations, allowing Akira to amplify its impact without centralizing risk.

Why the Akira Affiliate Program Is Growing

Low Barrier to Entry for Affiliates

Akira's toolkit is versatile, supporting Windows, Linux, and VMware ESXi environments, which broadens its appeal to affiliates targeting diverse systems. The group provides user-friendly tools, including cross-platform encryptors and pre-configured attack chains, enabling even less-skilled cybercriminals to participate. This lowers the technical barrier, attracting a wider pool of affiliates, from seasoned operators to opportunistic newcomers.

Lucrative Profit-Sharing Model

The typical 70-80% profit split is competitive within the RaaS ecosystem, drawing affiliates away from disrupted groups. Akira’s affiliate payouts are among the highest, with ransoms often ranging from $500,000 to $2 million per victim, incentivizing aggressive campaigns. This financial allure has fueled affiliate recruitment.

Capitalizing on Ecosystem Gaps

The ransomware landscape in 2025 has seen fragmentation due to law enforcement actions and internal conflicts in other groups. Akira has filled this vacuum, absorbing disaffected affiliates from competitors.

Operational Efficiency for Affiliates

Akira's streamlined attack pipeline, exploiting vulnerabilities like CVE-2024-40766 in SonicWall appliances, paired with stolen credentials or weak MFA, enables affiliates to execute attacks quickly with a short dwell time. This speed reduces detection risks and appeals to affiliates seeking high-volume, low-dwell-time operations. The group's double-extortion tactics further increase ransom success rates, making it a preferred choice.

Impact of Affiliate Growth on the Surge in Attacks

Increased Attack Volume

The influx of affiliates has led to a surge in campaigns, with over 40 confirmed incidents in July-August 2025 and continued activity into September. Sectors like construction, manufacturing, and law firms have been hit hardest, reflecting affiliates' focus on high-payout targets.

Geographic Expansion

Affiliates are targeting new regions beyond North America, including Germany, Spain, Italy, and Canada, driven by Akira's global infrastructure and localized extortion tactics.

Diverse Attack Vectors

Affiliates leverage Akira's toolkit to exploit a range of entry points, from SonicWall VPN flaws (CVE-2024-40766) to Cisco VPN vulnerabilities (CVE-2023-20269) and misconfigured RDP. This flexibility allows affiliates to hit unpatched or poorly secured systems, often opportunistically, across multiple industries.

Leak Site Activity

Akira's data leak site has seen unprecedented posting volumes in 2025, with an approximate 30% increase in victim listings since Q1. This reflects affiliates' success in extorting payments and their use of public shaming to pressure victims.

IOCs

PolySwarm has multiple samples of Akira. The following are hashes of some of our most recent Akira samples, as of the time of writing.

a610ef0e37af408aa49c7296d238796c57ac45aa8b0809ce72bc4d75b23fdf4f

e9e0c53a59e00827c6e904d8d32ffc23bb9e2f45fa41d6acdc00533bfe151c62

26841db9c5f0aa186c07462709984a15ff7d867e7cb635d270442cfef3868354

ba6c0aa1b0ff6651b843de22cc83010addbb27f7c2d53db81a87d52b2fc32999

e8c7ceb1a023c5f69b3ad9146c1a674088b7471cdcfb936fd5afba4f45aabac1

dd0f8a5d991b5ceda51e74ea52604d6f601eb59053a9c5a01974f011a34572ca

a5a4ee68bfdd7449b11289b8af200ff1d146deda40d23913059ed2a941cf7a5b

392bbfa9a1526428e2db1c5bd6fda098ee0303a8ebf2831e66fd68d54f5977ed

8cc602098466734f49a2207af9cff47a9999756de600c703fb2405bf067d268f

b5dfd4fb5e17d304c15d42a1d2404ff7a578b618f996f5cb6b2762cd9a6d0c53

bca1fa9761692b63182acb87c43aa5f4297b237396cd95444b7bc398f1ae338b

1db5fba5f0310225d842c9bdc05c027143335fa397b109232711510f64960968

401f99900f2a95a9841678308609b7b2dba88fd7248645f81ec2d9308463025a

0942a5df0ab3f0278cdc5b3eb11c899dcaf0dda34238de71000626e220c92e07

9e56d7b5621fc6fd6b966923447988d06e48f6211461de532b71023588e0c95b

aac26c298a11e3d5b5ce409f7290ab108d9f98e1f819291e143fe12fb8537466

fa57f2c1c3b2a8a75bbce65bc59b81c0b39c75ba9857bbfe32d60862a1847978

096281571085fe6bc80d50e8d8510379ac8481c56f9bc53a001c8156e7e764d3

0195f7d41644e87291092aff91770f0eca1ab775562b56791a31f409793499e4

d5d55ab3e29faa76ec513f9b32112cf4dff67f8911786a2916d6b951150cd722

You can use the following CLI command to search for all Akira samples in our portal:

$ polyswarm link list -f Akira

Don't have a PolySwarm account? Go here ***to sign up for a free Community plan or subscribe.***

Contact us **at** hivemind@polyswarm.io **|** ***Check out our*** **blog** **|** Subscribe ***to our reports.***

Topics: Threat Bulletin, Data Exfiltration, credential theft, SonicWall VPN, Ransomware Campaign, Akira Ransomware, CVE-2024-40766, SSL VPN

Written by The Hivemind