AKIRA RANSOMWARE: OPERATIONAL EVOLUTION AND GLOBAL IMPACT

Vairav Cyber Security Report

Date: April 18, 2025

Vairav Cyber Threat Intelligence Team

Vairav Technology Security Pvt. Ltd.

Thirbam Sadak 148
Baluwatar, Kathmandu

Phone: +977 4541540
Mobile: +977-9820105900
Email: sales@vairavtech.com

EXECUTIVE SUMMARY

Akira Ransomware has rapidly evolved into a prominent ransomware threat actor, leveraging a double extortion model. The group targets organizations across North America, Europe, and Australia, stealing sensitive data before encrypting it and threatening to publish it on their Data Leak Site (DLS) if ransom demands are unmet. By January 2024, Akira had affected over 250 organizations and claimed over USD 42 million in ransom payments. Operating under a Ransomware-as-a-Service (RaaS) model, Akira actors gain initial access through compromised credentials. Technical artifacts link Akira to previously known malware such as Conti, and their toolset includes both Windows and Linux variants, the latter focused on VMware ESXi environments.

KEY FINDINGS

- **First Identified:** March 2023
- **Access Vector:** Compromised credentials, initial access often via VPN without MFA
- **Extortion Strategy:** Double extortion (data exfiltration + encryption)
- **Notable Tools & Variants:**
  - .akira extension (C++ version)
  - .powerranges via Megazord (Rust-based variant)
- **Akira_v2** was observed in recent investigations
- **Linux Variant:** Targets VMware ESXi hosts
- **Record Activity:** Over 30 victims leaked in a single day (Nov 13–14, 2023)
- **Ransom Proceeds:** Over USD 42 million (as of Jan 1, 2024)
- **Known Associations:** Links to Conti, GOLD SAHARA, and PUNK SPIDER

CAMPAIGN OVERVIEW

Threat Actor: Akira Ransomware Group (RaaS)

Campaign Objective: Financial extortion via data theft and ransomware encryption,

Industries Targeted: Business services, Education, Manufacturing, Finance, Healthcare, Construction, Retail, Technology, and Critical Infrastructure

Regions Targeted: United States, Canada, Europe (UK, Germany, Denmark, Sweden, Czech Republic), Australia, Nigeria, and Uruguay

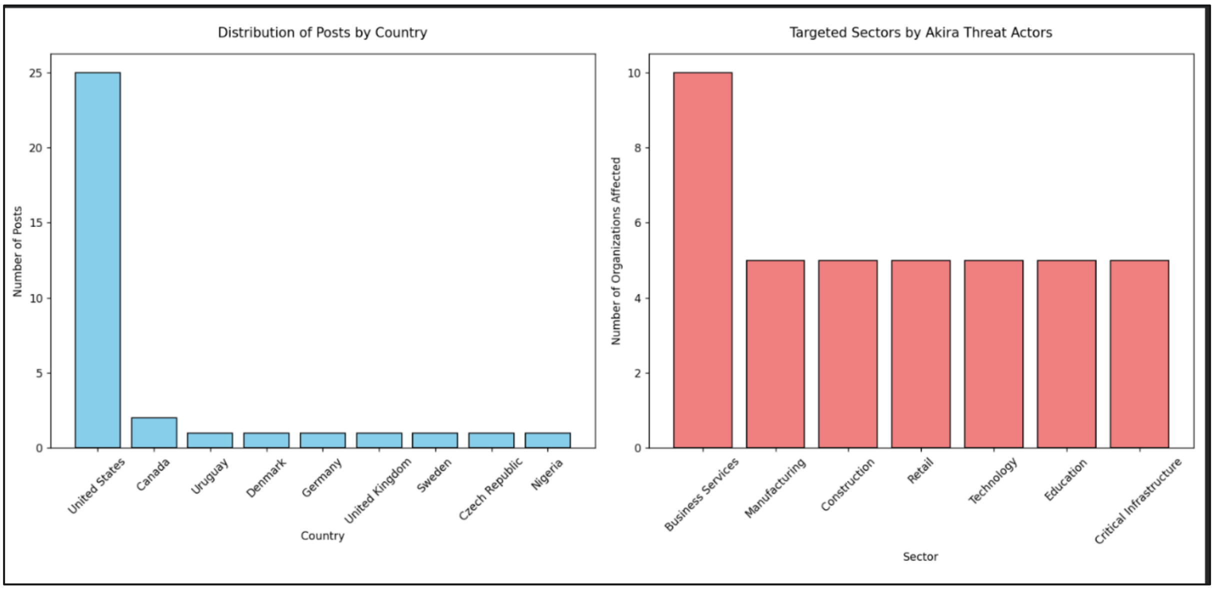
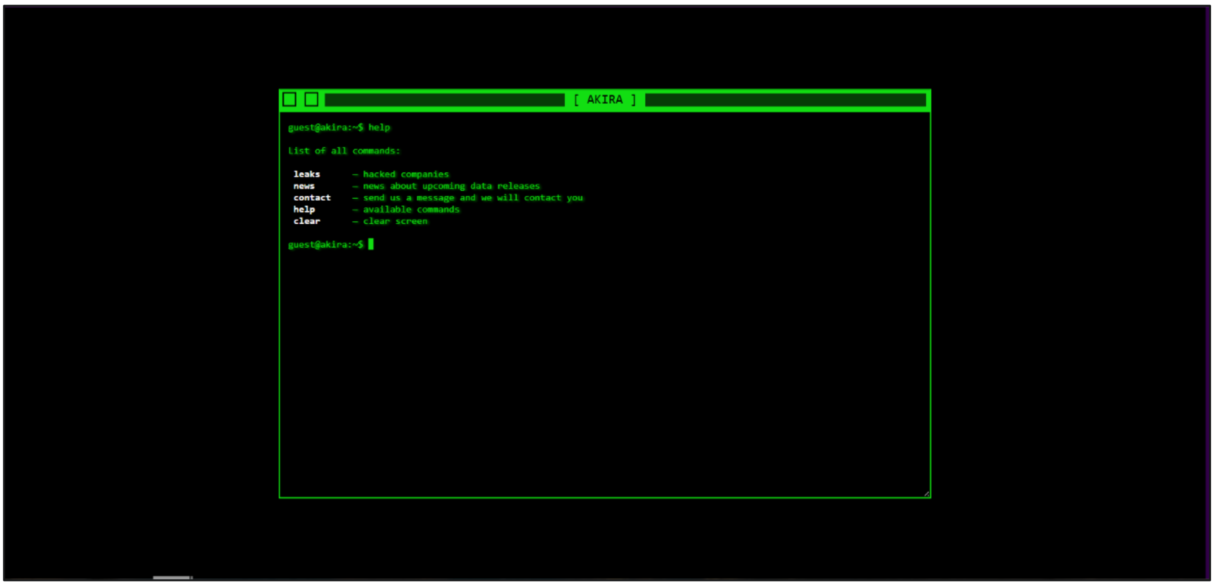


Figure 1: Regions/Industries targeted

BACKGROUND

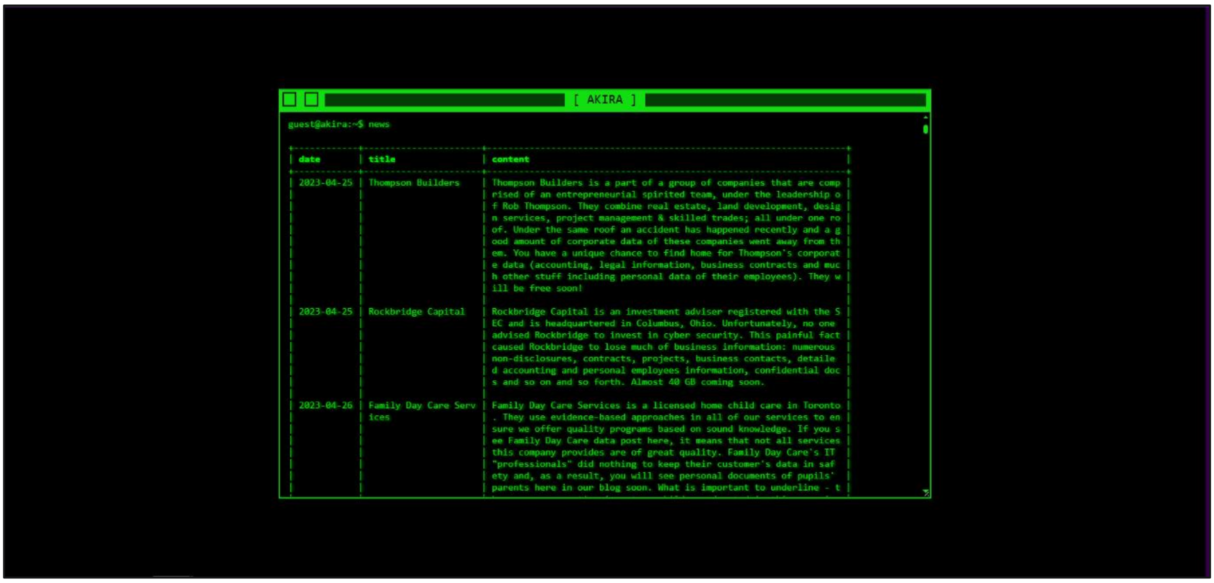
The Akira ransomware group's data leak site is divided into five sections. The "Leaks" section displays victims who declined to pay the ransom, resulting in the public release of their stolen data. The "News" section features newly compromised organizations, likely still involved in ransom negotiations.



```
guest@akira:~$ help

List of all commands:

 leaks      — hacked companies
 news       — news about upcoming data releases
 contact    — send us a message and we will contact you
 help       — available commands
 clear      — clear screen

guest@akira:~$
```

Figure 2: Akira ransomware data leak site

Recently, three victims previously listed in the "News" section appeared in the "Leaks" section, indicating they did not pay. Additionally, 29 entirely new victims were added to "Leaks," and three more were introduced in "News," bringing the total number of newly listed victims to 32, with three confirmed non-payments.



```
guest@akira:~$ news

+------------+----------------------+--------------------------------------------------------------+
| date       | title                | content                                                      |
+------------+----------------------+--------------------------------------------------------------+
| 2023-04-25 | Thompson Builders    | Thompson Builders is a part of a group of companies that are comp |
|            |                      | rised of an entrepreneurial spirited team, under the leadership o |
|            |                      | f Rob Thompson. They combine real estate, land development, desig |
|            |                      | n services, project management & skilled trades; all under one ro |
|            |                      | of. Under the same roof an accident has happened recently and a g |
|            |                      | ood amount of corporate data of these companies went away from th |
|            |                      | em. You have a unique chance to find home for Thompson's corporat |
|            |                      | e data (accounting, legal information, business contracts and muc |
|            |                      | h other stuff including personal data of their employees). They w |
|            |                      | ill be free soon!                                            |
|            |                      |                                                              |
| 2023-04-25 | Rockbridge Capital   | Rockbridge Capital is an investment adviser registered with the S |
|            |                      | EC and is headquartered in Columbus, Ohio. Unfortunately, no one |
|            |                      | advised Rockbridge to invest in cyber security. This painful fact |
|            |                      | caused Rockbridge to lose much of business information: numerous |
|            |                      | non-disclosures, contracts, projects, business contacts, detaile |
|            |                      | d accounting and personal employees information, confidential doc |
|            |                      | s and so on and so forth. Almost 40 GB coming soon.          |
|            |                      |                                                              |
| 2023-04-26 | Family Day Care Serv | Family Day Care Services is a licensed home child care in Toronto |
|            | ices                 | . They use evidence-based approaches in all of our services to en |
|            |                      | sure we offer quality programs based on sound knowledge. If you s |
|            |                      | ee Family Day Care data post here, it means that not all services |
|            |                      | this company provides are of great quality. Family Day Care's IT |
|            |                      | "professionals" did nothing to keep their customer's data in saf |
|            |                      | ety and, as a result, you will see personal documents of pupils' |
|            |                      | parents here in our blog soon. What is important to underline - t |
```

Figure 3: Data leak site news section

KNOWN EXPLOITED CVES

CVE-2023-20269 (CVSS: 5.0, Medium)

A flaw in Cisco ASA and FTD's remote access VPN allows attackers to perform brute-force attacks to discover valid credentials or establish unauthorized VPN sessions due to improper AAA separation.

CVE-2020-3259 (CVSS: 7.5, High)

A vulnerability in Cisco ASA and FTD's web services interface allows unauthenticated attackers to access sensitive memory data by sending crafted GET requests. This mainly affects devices with specific AnyConnect or WebVPN configurations.

KNOWN ASSOCIATIONS

PUNK SPIDER

Identified in April 2023, PUNK SPIDER is believed to be the primary Big Game Hunting (BGH) adversary behind the development and operation of Akira ransomware and its dedicated leak site (DLS). The group leverages legitimate software and open-source penetration tools in their attacks.

GOLD SAHARA

A cybercrime group actively deploying Akira ransomware, GOLD SAHARA, is known for using public tools and built-in Windows utilities. Their tactics include:

- Initial Access via compromised VPN credentials

- Network Discovery using Advanced IP Scanner and SoftPerfect Network Scanner
- Domain Enumeration with Nltest
- Remote Access through AnyDesk and PuTTY
- Data Staging with WinRAR and exfiltration using Rclone
- Extortion via access to SharePoint files
- Disruption by deleting admin accounts before ransomware deployment

TACTICS, TECHNIQUES, AND PROCEDURES (TTPs)

PLATFORM TARGETED: Windows

INITIAL ACCESS

Akira threat actors typically gain their initial foothold through virtual private network (VPN) services that lack Multi-Factor Authentication (MFA). In many incidents, actors exploited known vulnerabilities in Cisco ASA devices, such as CVE-2023-20269 and CVE-2020-3259, to gain access using stolen or brute-forced credentials. Beyond VPN exploitation, Akira also uses spear-phishing and phishing emails, Remote Desktop Protocol (RDP) exposure, and abuse of valid credentials to breach external-facing services and infiltrate networks.

PERSISTENCE AND DISCOVERY

After gaining access, the actors focus on establishing persistence and mapping the environment. They often create new domain accounts, one commonly observed example is an admin-level account named itadm to maintain long-term access. To escalate privileges, they deploy credential access techniques such as Kerberoasting to extract service account hashes and leverage tools like Mimikatz and LaZagne for credential scraping. For reconnaissance, Akira uses SoftPerfect Network Scanner and Advanced IP Scanner to identify active hosts and open ports. They also utilize native Windows commands like net and nltest to identify domain controllers and assess domain trust relationships within the environment.

DEFENSE EVASION

Akira threat actors use multiple defense evasion techniques to disable security tools and maintain stealth during operations. A notable method includes abusing the Zemana

AntiMalware driver via PowerTool to disable endpoint protection solutions. In some sophisticated attacks, the group has deployed two ransomware payloads in the same breach, Megazord (targeting Windows systems) and Akira_v2 (targeting Linux/ESXi systems), demonstrating coordinated multi-platform capabilities. The group typically avoids placing an initial ransom note, forcing victims to initiate contact through a Tor-based leak site using a unique victim-specific code.

EXFILTRATION AND IMPACT

Before encrypting files, Akira exfiltrates sensitive data to leverage for extortion. The group uses a variety of tools such as WinRAR to archive files, and FileZilla, WinSCP, and RClone to transfer data out of the victim's network. To establish command and control (C2) channels, they rely on remote access and tunneling tools, including AnyDesk, RustDesk, MobaXterm, Ngrok, and Cloudflare Tunnel. These tools allow them to move data using protocols like FTP and SFTP or cloud services such as Mega. Once data is exfiltrated, the group issues ransom demands via a hidden service on the Tor network. Victims are given no upfront ransom amount instead; they must contact Akira through the provided link. In some cases, Akira actors have even made follow-up phone calls to pressure organizations into paying.

ENCRYPTION

Akira uses a hybrid encryption technique that combines the ChaCha20 stream cipher with RSA public-key cryptography. This combination allows for fast file encryption while securely exchanging keys. The ransomware is capable of both full and partial encryption, depending on the file type and size. Encrypted files are typically renamed with a .akira extension in early variants or .powerranges in newer Megazord-based attacks. To prevent recovery, the encryptor (w.exe) uses PowerShell commands to delete Volume Shadow Copies (VSS). A ransom note named fn.txt is dropped in the root directory (C:\) and each user's home folder (C:\Users\).

AKIRA_V2 ENHANCEMENTS

The Akira_v2 variant, developed in the Rust programming language, incorporates advanced features and obfuscation. It accepts runtime arguments that allow attackers to customize the attack options, including specifying encryption paths (-p), network shares (-

s), and encryption percentage (-n), as well as spawning child processes with --fork to optimize CPU usage. Akira_v2 also includes anti-analysis protections, such as requiring a valid Build ID to execute, and virtualization-specific commands like vmonly to target only virtual machines and stopvm to shut down active VMs. On Linux/ESXi systems, encrypted files may use the akiranew extension, and a ransom note titled akiranew.txt is dropped in affected directories.

CONCLUSION

Since its emergence in March 2023, Akira ransomware has become a major cyber threat, impacting over 250 organizations. The group exploits VPNs without MFA, abuses Cisco vulnerabilities, and leverages tools like AnyDesk, RClone, and WinSCP for lateral movement and data exfiltration. Its shift from C++ to Rust-based variants reflects efforts to enhance encryption speed and evade detection. Targeting a wide range of sectors, Akira’s adaptable tactics underscore the need for strong cyber hygiene, patch management, and proactive threat detection to defend against this evolving threat.

MITRE ATT&CK TECHNIQUES

Tactics	Techniques (ID)
Initial Access	Valid Accounts (T1078) Exploit Public-Facing Application (T1190) External Remote Services (T1133) Phishing (T1566) • Spearphishing Attachment (T1566.001) • Spearphishing Link (T1566.002)
Credential Access	OS Credential Dumping (T1003) • LSASS Memory (T1003.001)
Discovery	System Network Configuration Discovery (T1016) System Information Discovery (T1082) Domain Trust Discovery (T1482) Process Discovery (T1057) Permission Groups Discovery (T1069) • Local Groups (T1069.001) • Domain Groups (T1069.002) Remote System Discovery (T1018)
Persistence	Create Account (T1136) • Domain Account (T1136.002)
Defense Evasion	Impair Defenses (T1562) • Disable or Modify Tools (T1562.001)
Command and Control	Remote Access Software (T1219) Proxy (T1090)
Collection	Archive Collected Data (T1560) • Archive via Utility (T1560.001)
Exfiltration	Exfiltration Over Alternative Protocol (T1048) Transfer Data to Cloud Account (T1537) Exfiltration Over Web Service (T1567) • Exfiltration to Cloud Storage (T1567.002)

Impact	Data Encrypted for Impact (T1486) Inhibit System Recovery (T1490) Financial Theft (T1657)

INDICATORS OF COMPROMISE (IOCs)

File name	Hashes
w.exe	*d2fd0654710c27dcf37b6c1437880020824e161dd0bf28e3a133ed7772*
Win.exe	*dcfa2800754e5722acf94987bb03e814edcb9acebda37df6da1987bf48*
Anydesk.exe	*dcfa2800754e5722acf94987bb03e814edcb9acebda37df6da1987bf48*
Gcapi.dll	*73170761d6776c0debacfbbc61b6988cb8270a20174bf5c049768a264*
Sysmon.exe	*1b60097bf1ccb15a952e5bcc3522cf5c162da68c381a76abc2d5985659*
Rclone.exe	*aaa647327ba5b855bedea8e889b3fafdc05a6ca75d1cfd98869432006d*
Winscp.rnd	*7d6959bb7a9482e1caa83b16ee01103d982d47c70c72fdd03708e2b7f*
WinSCP-6.1.2-Setup.exe	*36cc31f0ab65b745f25c7e785df9e72d1c8919d35a1d7bd4ce8050c8c0*
Akira_v2	*3298d203c2acb68c474e5fdad8379181890b4403d6491c523c1373012* *0ee1d284ed663073872012c7bde7fac5ca1121403f1a5d2d5411317df2*
Megazord	*ffd9f58e5fe8502249c67cad0123ceeeaa6e9f69b4ec9f9e21511809849* *dfe6fddc67bdc93b9947430b966da2877fda094edf3e21e6f0ba98a84bc* *131da83b521f610819141d5c740313ce46578374abb22ef504a759395* *9f393516edf6b8e011df6ee991758480c5b99a0efbfd68347786061f0e0* *9585af44c3ff8fd921c713680b0c2b3bbc9d56add848ed62164f7c9b9f2* *2f629395fdfa11e713ea8bf11d40f6f240acf2f5fcf9a2ac50b6f7fbc7521c8* *7f731cc11f8e4d249142e99a44b9da7a48505ce32c4ee4881041beedd* *95477703e789e6182096a09bc98853e0a70b680a4f19fa2bf86cbb9280* *0c0e0f9b09b80d87ebc88e2870907b6cacb4cd7703584baf8f2be1fd94* *C9c94ac5e1991a7db42c7973e328fceeb6f163d9f644031bdfd4123c7b*
VeeamHax.exe	*aaa6041912a6ba3cf167ecdb90a434a62feaf08639c59705847706b9f4*
Veeam-Get-Creds.ps1	*18051333e658c4816ff3576a2e9d97fe2a1196ac0ea5ed9ba386c46def*
PowershellKerberosTicketDumper	*5e1e3bf6999126ae4aa52146280fdb913912632e8bac4f54e98c58821a*
sshd.exe	*8317ff6416af8ab6eb35df3529689671a700fdb61a5e6436f4d6ea8ee00*
ipscan-3.9.1-setup.exe	*892405573aa34dfc49b37e4c35b655543e88ec1c5e8ffb27ab8d1bbf90*

VAIRAV RECOMMENDATIONS

To reduce the risk and impact of Akira ransomware attacks, organizations are strongly advised to:

1. **Implement Multi-Factor Authentication (MFA)**: Apply MFA to all remote access services, especially VPNs, to prevent unauthorized access via compromised credentials.
2. **Patch Vulnerabilities Promptly**: Prioritize patching known vulnerabilities, particularly in Cisco ASA/FTD products (e.g., CVE-2023-20269, CVE-2020-3259), and ensure security appliances are regularly updated.
3. **Restrict External Access**: Limit and monitor access to RDP, VPN, and other exposed services. Enforce the least privilege access controls.
4. **Deploy Network Segmentation and EDR Solutions**: Use endpoint detection and response (EDR) and segment critical infrastructure to reduce lateral movement opportunities.
5. **Monitor for Suspicious Tool Usage**: Detect and alert on the use of remote tools like AnyDesk, RClone, MobaXterm, and PowerShell abuse, especially if they appear in unexpected contexts.
6. **Regularly Back Up and Isolate Critical Data**: Maintain encrypted, offline backups of essential systems and validate their restoration regularly to ensure operational continuity post-incident.
7. **Conduct Security Awareness Training**: Educate employees on phishing, credential hygiene, and recognizing suspicious activities to reduce social engineering success.
8. **Engage in Threat Hunting and Intelligence Sharing**: Proactively hunt for indicators of compromise (IOCs) and share intelligence with trusted ISACs or national CERTs to improve collective defense.

CONTACT US

Vairav Technology Security Pvt. Ltd.

Cyber Defender from the land of Gurkha

Thirbam Sadak 148, Baluwatar

Kathmandu, Nepal

Phone: +977-01-4541540

Mobile: +977-9820105900

Email: sales@vairavtech.com

Website: https://vairavtech.com