THREAT INTELLIGENCE REPORT

January 13 – January 19, 2026

Red Piranha
unified threat management

Report Summary:

New Threat Detection Added

- GhostPenguin
- EtherRAT

Detection Summary

- New Threat Protection: 126
- Newly Detected Threats: 6

The following threats were added to Crystal Eye this week:

1. GhostPenguin

GhostPenguin is a C++-based backdoor developed for the Linux platform. It provides remote access to the infected system via a remote shell and includes functionality for retrieving system information, modifying files, directories, and timestamps, as well as exfiltration. Communication is done via UDP with RC5 encryption.

Threats Protected: 1
Class Type: Trojan-Activity
Rule Set Type:

Ruleset	IDS: Action	IPS: Action
Balanced	Reject	Drop
Security	Reject	Drop
WAF	Disabled	Disabled
Connectivity	Alert	Alert
OT	Reject	Drop

Kill Chain:

Tactic	Technique ID	Technique Name
Execution	T1059.004	Command and Scripting Interpreter: Unix Shell
Defence Evasion	T1070.006 T1070.004	Indicator Removal: Timestomp Indicator Removal: File Deletion
Discovery	T1082 T1083	System Information Discovery File and Directory Discovery
Collection	T1119 T1005	Automated Collection Data from Local System
Command-and-Control	T1573.001 T1095	Encrypted Channel: Symmetric Cryptography Non-Application Layer Protocol
Exfiltration	T1041	Exfiltration Over C2 Channel

2. EtherRAT

EtherRAT is a new malware payload affecting React Servers. Due to the recent CVE-2025-55182, which details a Remote Code Execution (RCE) vulnerability which affects various components of the React Server ecosystem and has a CVSS score of 10.0 - the highest risk score possible. The React Server Ecosystem has been targeted heavily by the impact and ease of exploitation from the CVE. Many threat actors have been deploying malware on the affected systems, including EtherRAT.

EtherRAT differs from the usual malware that captures data and sets up basic C2 connections for control and persistence. EtherRAT combines multiple techniques to maintain persistence and control of the infected system. It uses Ethereum Smart Contracts (ESC) for C2 communication. The ESC is used to post commands and URLs for the malware to read and use because the blockchain is immutable; these transactions can't be removed.
EtherRAT also has five methods to maintain persistence on the infected system, such as using systemd services, cron jobs, and auto-execution via .bashrc config. EtherRAT also does not automatically harvest credentials on install.

Threats Protected: 3
Class Type: Trojan-Activity
Rule Set Type:

Ruleset	IDS: Action	IPS: Action
Balanced	Reject	Drop
Security	Reject	Drop
WAF	Disabled	Disabled
Connectivity	Alert	Alert
OT	Reject	Drop

Kill Chain:

Tactic	Technique ID	Technique Name
Initial Access	T1190	Exploit Public-Facing Application
Execution	T1059.007	Command and Scripting Interpreter: JavaScript
Persistence	T1547.013 T1543.002 T1053.003 T1546.004	Boot or Logon AutoStart Execution: XDG AutoStart Entries Create or Modify System Process: Systemd Service Scheduled Task/ Job: Cron Event Triggered Execution: Unix Shell Configuration Modification
Command -and-Control	T1071.001	Application Layer Protocol: Web Protocol

Current Threat Summary

Known Exploited Vulnerabilities (Week 3 - January 2026)

Vulnerability	CVSS	Description
CVE-2026-20805	5.5	Microsoft Windows Desktop Windows Manager contains an information disclosure vulnerability that can allow an attacker with local access to disclose the section address of a remote ALPC port in user-mode memory. The ALPC (Advanced Local Procedure Call) is used in inter-process communication, the disclosure of this address may assist an attacker in bypassing ASLR (Address Space Layout Randomisation) to facilitate the development of additional exploits.
CVE-2025-8110	8.7	Gogs contains a path traversal vulnerability within the PutContents API that can result in local code execution as a result of improper Symbolic link handling which can allow overwriting files outside the repository directory.

For more information, please visit the Red Piranha Forum:
https://forum.redpiranha.net/t/known-exploited-vulnerabilities-catalog-3rd-week-of-january-2026/633

Updated Malware Signatures (Week 3 - January 2026)

Threat	Description
XWorm	A Remote Access Trojan (RAT) and malware loader that's commonly used in cyberattacks to give attackers full remote control over a victim's system. It's part of a growing trend of commercialised malware sold or rented on dark web forums, often under the guise of a “legitimate tool.”

Ransomware Report

The Red Piranha Team conducts ongoing surveillance of the dark web and other channels to identify global organisations impacted by ransomware attacks. In the past week, our monitoring revealed multiple ransomware incidents across diverse threat groups, underscoring the persistent and widespread nature of these cyber risks. Presented below is a detailed breakdown of ransomware group activities during this period.

Ransomware Hits Last Week

Qilin led this week's activity, responsible for 16.2% of all reported incidents. This put it clearly at the top of the ecosystem, reflecting a concentrated campaign phase or a batch of delayed victim disclosures that pushed Qilin ahead of every other active group.

A strong second tier was formed by Akira (14.79%), alongside Sinobi (9.15%), Orion (9.15%), Inc Ransom (7.04%), and The Gentlemen (5.63%). Together, this block of actors represented a substantial share of global ransomware pressure, with sustained multi-sector targeting and regular leak-site publications.

A solid mid-tier cluster, Everest, Obscura, and DevMan2 (each 4.23%), followed by Genesis, Tengu, and Beast (each 2.82%), and Play, Nova, Clop, Direwolf, and DragonForce (each 2.11%), maintained a steady operational tempo. These crews did not individually rival Qilin or Akira but collectively contributed a large portion of weekly incidents through ongoing double-extortion and data-theft activity.

Smaller but active operators, KillSec3, Anubis, and Nightspire (each 1.41%), continued to appear at low but consistent volumes, keeping a visible footprint across regions and industries.

At the fringe, Securotrop and MS13-089 (each 0.7%) accounted for only a sliver of total incidents, but together with the broader mid- and low-volume actors, they illustrate the same pattern as prior weeks: a few dominant brands driving the bulk of disclosures, backed by a wide base of smaller crews that preserve the fragmentation and resilience of the ransomware ecosystem.

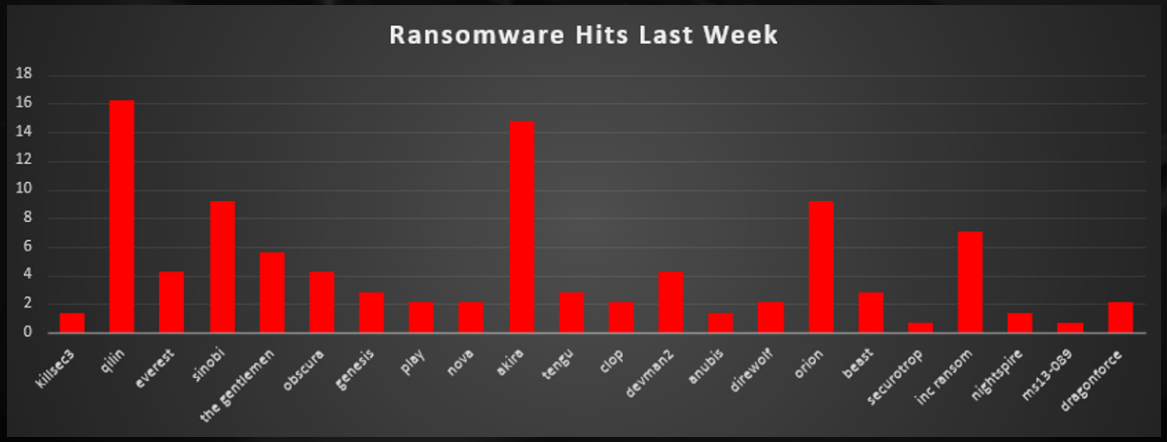


Figure 1: Ransomware Group Hits Last Week

Akira Ransomware

Akira is a ransomware-as-a-service (RaaS) group that emerged in March 2023, quickly rising to prominence by targeting organisations worldwide. The gang employs double-extortion tactics – stealing sensitive data before encrypting systems – to pressure victims into paying. By January 2024, Akira had hit over 250 organisations (primarily in North America) and earned an estimated $42 million in ransoms. Their operations expanded further through 2025: as of late September 2025, they accrued $244 million USD in proceeds and claimed hundreds of victims across sectors, including manufacturing, education, IT, healthcare, finance, and more. Akira is believed to have ties to the defunct Conti cartel – code overlap and blockchain analysis suggest Akira's developers and affiliates include former Conti members. This heritage gave Akira a headstart with sophisticated tools, seasoned negotiators, and a network of initial access brokers.

Akira's branding is notable: their Tor data-leak site features a retro 'green-screen' terminal interface, where visitors must type commands (like leaks, news, contact) to navigate. This old-school aesthetic is a psychological ploy to reinforce the 'elite hacker' persona and unsettle victims. Akira initially coded its ransomware in C++ for Windows (appending '.akira' to encrypted files) but introduced a new Rust-based variant in August 2023 (dubbed 'Megazord') that appends '.powerrangers' to files. Both versions continue to be used interchangeably. Akira primarily targeted Windows networks at first, then added a Linux/ESXi locker in April 2023 for VMware environments.

In mid-2025, Akira actors demonstrated a further evolution by encrypting Nutanix AHV virtual machine disks – achieved by exploiting a SonicWall SSL-VPN vulnerability (CVE-2024-40766) to broaden access beyond VMware/Hyper-V hosts. This adaptive strategy highlights Akira's willingness to invest in new capabilities to bypass defences and target critical infrastructure. During January 10-16, 2026, the group posted 15+ new victims to their leak site, demonstrating sustained high operational tempo with lifetime ransom proceeds exceeding $244 million.

Security vendors track this group under multiple names: PUNK SPIDER (CrowdStrike), Storm-1567 (Microsoft), Howling Scorpius (Unit 42), and GOLD SAHARA (Secureworks). MITRE assigns them the identifier G1024. The group currently operates four primary variants: Akira (C++, .akira extension), Megazord (Rust, .powerranges extension), Akira Linux (C/C++, .akira extension for Linux/ESXi), and Akira_v2 (Rust, .akiranew extension for ESXi and Nutanix AHV systems).

Detailed Tactics, Techniques, and Procedures (TTPs)

1. Initial Access (Compromised VPN & Exploited Vulnerabilities)
Akira predominantly gains access through compromised VPN credentials lacking multi-factor authentication, specifically targeting Cisco ASA, SonicWall SSL-VPN, and Fortinet VPN appliances. In mid-2025, Akira mass-exploited CVE-2024-40766 (SonicWall VPN flaw) to steal credentials and gain illicit access. Additional exploited vulnerabilities include CVE-2023-20269 (Cisco ASA/FTD zero-day), CVE-2024-40711 (Veeam Backup RCE), CVE-2023-48788 (FortiClientEMS SQL injection), CVE-2024-37085 (VMware ESXi authentication bypass), and CVE-2020-3259 (Cisco ASA information disclosure). Secondary access methods include spearphishing campaigns delivering credential-harvesting links, RDP brute forcing, and purchasing access from initial access brokers.

2. Privilege Escalation & Persistence
Once inside networks, Akira establishes persistence through creating new domain administrator accounts (commonly named 'itadm'), deploying legitimate remote access tools like AnyDesk, RustDesk, LogMeIn, and MeshCentral/MeshAgent, and maintaining access via stolen valid credentials. The group escalates privileges primarily through harvested domain administrator credentials and exploitation of additional vulnerabilities within compromised environments. They bypass User Account Control by disabling Remote UAC via registry modifications to allow elevated commands to be run remotely without prompts.

3. Reconnaissance & Discovery
Akira performs extensive network discovery using Advanced IP Scanner, MASSCAN, SoftPerfect Network Scanner, and command-line tools (nltest, net, ipconfig) to map the network. They enumerate Active Directory information using AdFind and PowerShell scripts, identify network shares with tools like SharpShares, and run BloodHound for AD reconnaissance to identify high-value targets. The attackers systematically identify file servers, backup locations, virtualisation storage (VHD/VMDK files), and critical services to terminate before encryption.

4. Defence Evasion (Advanced Techniques)
Akira employs sophisticated evasion methods, including Bring Your Own Vulnerable Driver (BYOVD) attacks using the Zemana antimalware driver and Intel ThrottleStop driver (rwdrv.sys) to terminate security processes and disable kernel callbacks. Additional techniques include disabling Windows Defender via PowerShell (Set-MpPreference -DisableRealtimeMonitoring $true), clearing Windows Event Logs, using Ngrok for encrypted C2 tunnelling, and deploying their own virtual machines to bypass host-based security controls. They modify system settings like disabling remote User Account Control restrictions in the registry to ease lateral movement.

5. Credential Access (Aggressive Harvesting)
Akira operators aggressively pursue credential access using Mimikatz and the DonPAPI toolkit to harvest passwords from Windows credentials, cached browser passwords, RDP/VNC logins, LSASS memory dumps, SAM database extraction, and NTDS.dit copying from domain controllers. They employ Kerberoasting attacks against service accounts and have been observed targeting Veeam backup software to extract saved passwords from configuration files. LaZagne and PCHunter are also deployed for comprehensive credential extraction.

6. Lateral Movement (Enterprise Spread)
Lateral movement relies heavily on Remote Desktop Protocol (RDP), SMB/Windows Admin Shares (ADMIN$, C$), and SSH connections to ESXi hosts. Tools include PsExec for remote execution, WMI/WMIC for distributed commands, and Impacket for protocol manipulation. With valid domain credentials in hand, attackers pivot across the network, deploying tools and payloads for mass deployment across the enterprise environment.

7. Data Exfiltration (Double-Extortion Preparation)
Before deploying ransomware, Akira exfiltrates large volumes of data (typically hundreds of gigabytes) from victim systems to use as leverage for extortion. The group archives stolen data using WinRAR or 7-Zip, then transfers it via RClone to cloud storage (particularly MEGA), WinSCP, and FileZilla. Data exfiltration can begin as quickly as two hours after initial compromise. In some cases, they set up Cloudflare Tunnel (cloudflared.exe) or Ngrok to create encrypted outbound tunnels for covert C2 and data exfiltration through benign cloud infrastructure.

8. Process/Service Termination (Pre-Encryption Preparation)
Akira terminates database services (SQL Server, MySQL, Oracle), backup processes (Veeam, Commvault, Acronis), and security software to release file locks and ensure successful encryption. They use the Windows Restart Manager to identify and close processes holding file handles. This is executed immediately before deploying the encryption payload.

9. Inhibit System Recovery (Backup Destruction)
As a final destructive step, the ransomware deletes system backups and shadow copies via vssadmin (vssadmin delete shadows /all /quiet) and WMI commands (wmic shadowcopy delete) to prevent recovery. They also execute wbadmin delete catalogue -quiet to remove Windows backup catalogues. This maximises pressure on victims to either pay the ransom or face both data leak and prolonged downtime.

10. Encryption & Impact (Ransomware Deployment)

When ready to execute, Akira actors deploy the encryptor across targeted systems (often overnight or during weekends to evade notice). The malware encrypts files using hybrid encryption, combining ChaCha8/ChaCha20 with RSA on Windows and AES/CAMELLIA with RSA on Linux systems. Akira skips encrypting Windows system folders (Recycle Bin, System Volume Information, Boot, Windows, ProgramData) and critical file extensions (.exe, .dll, .sys) to avoid system crashes. Encrypted files receive extensions: .akira (original), .powerrangers (Megazord), or .akiranew (v2). Ransom notes (akira_readme.txt, powerranges.txt, or akiranew.txt) are dropped in each directory, directing victims to their Tor negotiation portal.

11. Command-and-Control / Negotiation / Data Leak

Akira maintains TOR-based infrastructure, including a negotiation portal (akiralkzxzq2dsrzsrvbr2xgbbu2wgsmxryd4csgfameg52n7efvr2id.onion) where victims communicate with operators, and a data leak site (akiral2iz6a7qgd3ayp3l6yub7xx2uep76idk3u2kollpj5z3z636bad.onion) with a retro 1980s-aesthetic green-screen terminal interface. If victims refuse to pay, Akira threatens to publish stolen data on their leak site. The gang regularly publishes batches of victim data; in November 2024, they listed 30 new victims in a single day, indicating surge activity. Command-and-control infrastructure increasingly leverages Ngrok tunnelling for encrypted sessions alongside traditional remote access tools.

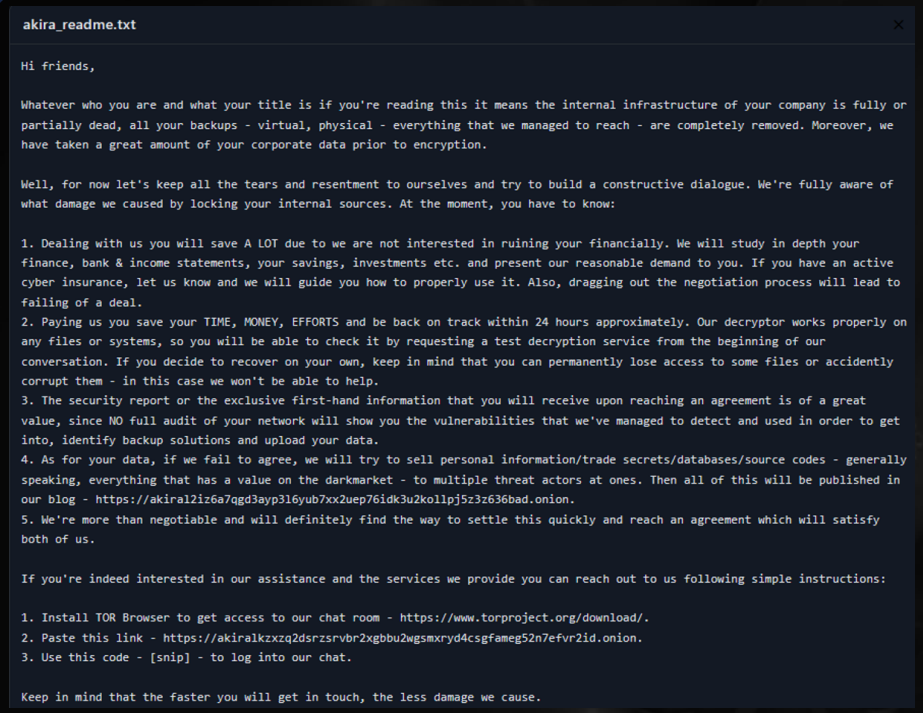
MITRE ATT&CK TTP Matrix

The table below summarises Akira's tactics and techniques mapped to the MITRE ATT&CK framework:

Tactic	Technique (ID)	Akira Implementation
Initial Access	External Remote Services (T1133)	Compromising exposed VPN/remote access services (SonicWall, Cisco ASA) using stolen credentials
Initial Access	Valid Accounts (T1078)	Logging in with valid but illicit credentials obtained via broker or brute-force
Initial Access	Exploit Public-Facing Application (T1190)	CVE-2024-40766 (SonicWall), CVE-2023-20269 (Cisco), CVE-2024-40711 (Veeam)
Persistence	Create Account (T1136)	Creating new domain admin accounts (e.g., "itadm") to maintain access
Persistence	Remote Access Software (T1219)	Installing AnyDesk, RustDesk, LogMeIn, MeshCentral for persistent access
Defence Evasion	Disable or Modify Tools (T1562.001)	Disabling Windows Defender, uninstalling EDR, BYOVD attacks with Zemana/Intel drivers
Defence Evasion	Indicator Removal (T1070.001)	Clearing Windows Event Logs to hide activity
Defence Evasion	Protocol Tunnelling (T1572)	Ngrok/Cloudflare Tunnel for encrypted C2 sessions bypassing perimeter monitoring
Credential Access	OS Credential Dumping (T1003)	Mimikatz, LaZagne, DonPAPI for LSASS memory, SAM, NTDS.dit, browser credentials
Credential Access	Kerberoasting (T1558)	Kerberoasting attacks against service accounts
Discovery	Network Service Discovery (T1046)	Advanced IP Scanner, MASSCAN, SoftPerfect for network scanning
Discovery	Domain Trust Discovery (T1482)	Nltest, AdFind, BloodHound for Active Directory enumeration
Lateral Movement	Remote Services (T1021)	RDP (T1021.001), SMB admin shares (T1021.002), SSH to ESXi (T1021.004), PsExec, WMI
Collection	Archive Collected Data (T1560)	WinRAR/7-Zip compression before exfiltration
Exfiltration	Exfiltration to Cloud (T1567.002)	RClone to MEGA, WinSCP, FileZilla via cloud storage/FTP/SFTP
Impact	Data Encrypted for Impact (T1486)	ChaCha20/RSA hybrid encryption with .akira/.powerrangers/.akiranew extensions
Impact	Inhibit System Recovery (T1490)	Deleting Volume Shadow Copies via vssadmin-/WMI, wbadmin catalogue deletion
Impact	Service Stop (T1489)	Terminating database, backup, and security services before encryption

Indicators of Compromise (IOCs)
Infrastructure / C2:

- IP Addresses (C2/Exfiltration): 66.165.243.39, 54.37.204.180, 13.107.42.12, 148.72.168.13, 141.95.84.40, 185.205.209.206, 16.1.0.106
- Domains: cybertrolls.cloud, on3cx.de, dynsys.is-a-guru.com, samaerx.ddnsfree.com, foxn1.sells-it.net, 51-83-136-132.xyz, s1-filecr.xyz



akira_readme.txt

Hi friends,

Whatever who you are and what your title is if you're reading this it means the internal infrastructure of your company is fully or partially dead, all your backups - virtual, physical - everything that we managed to reach - are completely removed. Moreover, we have taken a great amount of your corporate data prior to encryption.

Well, for now let's keep all the tears and resentment to ourselves and try to build a constructive dialogue. We're fully aware of what damage we caused by locking your internal sources. At the moment, you have to know:

1. Dealing with us you will save A LOT due to we are not interested in ruining your financially. We will study in depth your finance, bank & income statements, your savings, investments etc. and present our reasonable demand to you. If you have an active cyber insurance, let us know and we will guide you how to properly use it. Also, dragging out the negotiation process will lead to failing of a deal.
2. Paying us you save your TIME, MONEY, EFFORTS and be back on track within 24 hours approximately. Our decryptor works properly on any files or systems, so you will be able to check it by requesting a test decryption service from the beginning of our conversation. If you decide to recover on your own, keep in mind that you can permanently lose access to some files or accidently corrupt them - in this case we won't be able to help.
3. The security report or the exclusive first-hand information that you will receive upon reaching an agreement is of a great value, since NO full audit of your network will show you the vulnerabilities that we've managed to detect and used in order to get into, identify backup solutions and upload your data.
4. As for your data, if we fail to agree, we will try to sell personal information/trade secrets/databases/source codes - generally speaking, everything that has a value on the darkmarket - to multiple threat actors at ones. Then all of this will be published in our blog - https://akiral2iz6a7qgd3ayp3l6yub7xx2uep76idk3u2kollpj5z3z636bad.onion.
5. We're more than negotiable and will definitely find the way to settle this quickly and reach an agreement which will satisfy both of us.

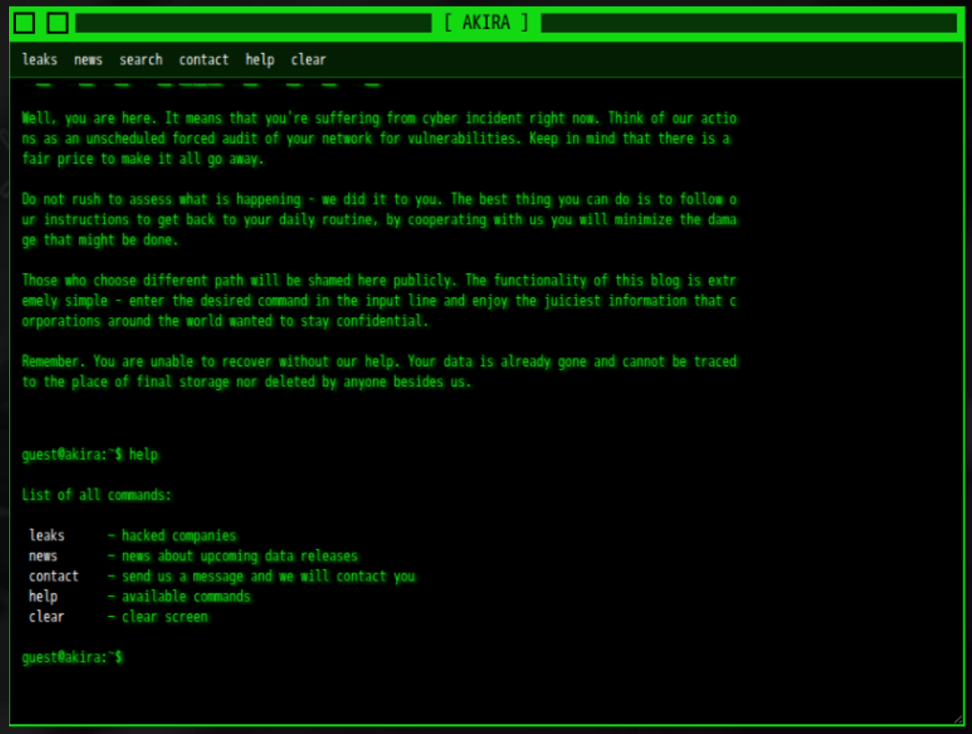
If you're indeed interested in our assistance and the services we provide you can reach out to us following simple instructions:

1. Install TOR Browser to get access to our chat room - https://www.torproject.org/download/.
2. Paste this link - https://akiralkzxzq2dsrzsrvbr2xgbbu2wgsmxryd4csgfameg52n7efvr2id.onion.
3. Use this code - [snip] - to log into our chat.

Keep in mind that the faster you will get in touch, the less damage we cause.

- TOR Onion Addresses: akiral2iz6a7qgd3ayp3l6yub7xx2uep76idk3u2kollpj5z3z636bad.onion (Data Leak Site)

akiralkzxzq2dsrzsrvbr2xgbbu2wgsmxryd4csgfameg52n7efvr2id.onion (Negotiation Portal)



Malware Samples (SHA-256 Hashes):

- Akira Windows Encryptors:

d2fd0654710c27dcf37b6c1437880020824e161dd0bf28e3a133ed777242a0ca

337d21f964091417f22f35aee35e31d94fc3f35179c36c0304eef6e4ae983292

dcfa2800754e5722acf94987bb03e814edcb9acebda37df6da1987bf48e5b05e

bfd5fc6cd3dea74738ac7025fa14ea844f400708df2293572796568f65bd6b61

- Akira_v2 Variant:

3298d203c2acb68c474e5fdad8379181890b4403d6491c523c13730129be3f75

0ee1d284ed663073872012c7bde7fac5ca1121403f1a5d2d5411317df282796c

- Megazord Rust Variant:

ffd9f58e5fe8502249c67cad0123ceeeaa6e9f69b4ec9f9e21511809849eb8fc

dfe6fddc67bdc93b9947430b966da2877fda094edf3e21e6f0ba98a84bc53198

131da83b521f610819141d5c740313ce46578374abb22ef504a7593955a65f07

- Linux/ESXi Samples:

e1321a4b2b104f31aceaf4b19c5559e40ba35b73a754d3ae13d8e90c53146c0f

74f497088b49b745e6377b32ed5d9dfaef3c84c7c0bb50fabf30363ad2e0bfb1

Tools & Artefacts Associated with Akira:

- Remote Access Tools: AnyDesk, RustDesk, LogMeIn, MeshCentral/MeshAgent
- Credential Dumpers: Mimikatz, LaZagne, DonPAPI, PCHunter
- Network Discovery: Advanced IP Scanner, SoftPerfect Network Scanner, MASSCAN, AdFind, BloodHound, SharpShares
- Tunnelling: cloudflared.exe (Cloudflare Tunnel), Ngrok
- Data Exfiltration: Rclone.exe, WinSCP, FileZilla, WinRAR, 7-Zip
- Post-Exploitation: Cobalt Strike, PsExec, Impacket
- BYOVD Drivers: Zemana antimalware driver, Intel ThrottleStop (rwdrv.sys)

File Indicators:

- Encrypted File Extensions: .akira (original), .powerrangers (Megazord), .akiranew (v2)
- Ransom Note Filenames: akira_readme.txt, powerranges.txt, akiranew.txt
- Common Staging Paths: C:\ProgramData\, C:\Windows\Temp\, C:\PerfLogs\, C:\Users\<username>\AppData\

Exploited Vulnerabilities (CVEs):

- CVE-2024-40766: SonicWall SonicOS SSL-VPN (Improper access control)
- CVE-2023-20269: Cisco ASA/FTD VPN (Zero-day)
- CVE-2024-40711: Veeam Backup (Remote code execution)
- CVE-2023-48788: FortiClientEMS (SQL injection)
- CVE-2024-37085: VMware ESXi (Authentication bypass)
- CVE-2020-3259: Cisco ASA (Information disclosure)

Crystal Eye 5.5 Mitigation Strategies

- Perimeter Control: Block known Akira IP addresses, TOR nodes, and malicious domains. Restrict internet-facing RDP. Enforce VPN with MFA for all remote access.
- Network Segmentation: Separate workstations, servers, and virtualisation environments. Block SMB/WinRM east-west traffic to prevent lateral movement.
- Vulnerability Management: Immediately patch CVE-2024-40766 (SonicWall), CVE-2023-20269 (Cisco), CVE-2024-40711 (Veeam). Use Crystal Eye IPS virtual patching for critical vulnerabilities.
- Endpoint Hardening: Enable EDR tamper protection. Prevent unauthorised process/service termination. Implement application allowlisting to block unauthorised binaries.
- Access Governance: Enforce MFA everywhere. Implement strong password policies. Apply least privilege principles. Use Privileged Access Workstations (PAWs) for administrators. Remove stale and excessive privileged accounts.
- Backup Resilience: Implement a 3-2-1 backup strategy with offline/immutable storage. Isolate backup networks from production. Test restore procedures quarterly with documented runbooks.
- SIEM Correlation: Alert on vssadmin/wbadmin shadow copy deletions, mass file encryption patterns, abnormal service stops, suspicious logons, TOR traffic, and Ngrok/Cloudflare Tunnel usage.
- Behavioural Analytics: Monitor for execution of credential dumping tools (Mimikatz, LaZagne), installation of unauthorised remote access software, unusual archive/compression activity followed by large data transfers, and BYOVD driver loading attempts.

Worldwide Ransomware Victims

The United States overwhelmingly dominated ransomware exposure this period, accounting for 59.15% of all identified victims. Roughly three out of every five known cases were U.S.-based, keeping it firmly established as the primary hunting ground for most major ransomware operations.

A clear second tier consisted of the United Kingdom (7.04%), Canada (4.23%), Malaysia (2.82%), and India and the United Arab Emirates (each 2.11%). Together, these countries formed the bulk of non-U.S. activity, reflecting mature digital ecosystems, regular incident disclosure, and organisational profiles that attackers see as highly monetisable.

A mid-band followed, including Romania, France, Turkey, Thailand, Spain, Germany, and Sweden (each 1.41%), which collectively represent a spread of European and Asian economies where ransomware is now a persistent and visible threat rather than an occasional anomaly.

Below this, a long tail of single-incident geographies, Japan, Peru, Philippines, Iraq, Greece, Czech Republic, Australia, Italy, Brazil, Ecuador, Chile, Croatia, Egypt, Argentina, China, Colombia, Mozambique (each 0.7%), appeared at low individual volumes. While each contributes only a small fraction of total activity, their combined footprint reinforces the same pattern seen in previous weeks: ransomware remains a global problem, touching dozens of countries across every region, not just a handful of headline markets.

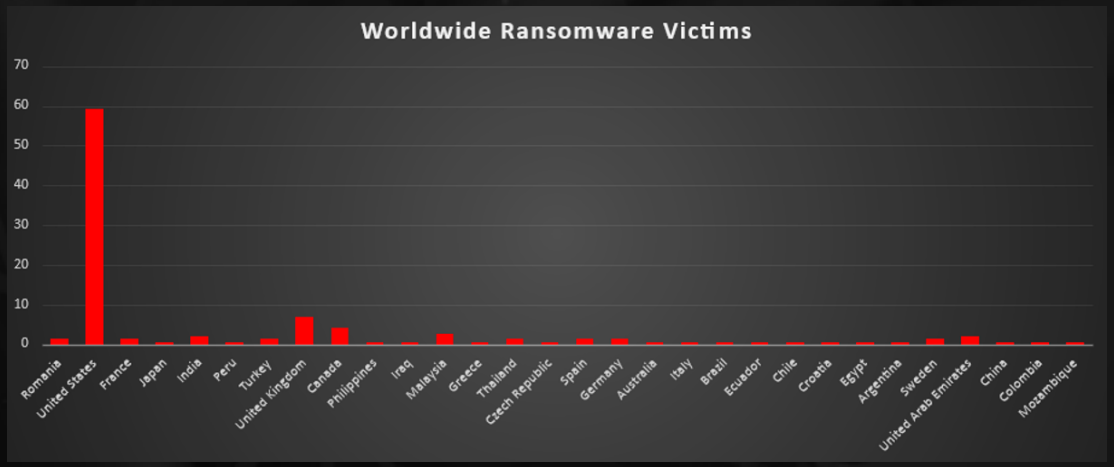


Figure 5: Ransomware Victims Worldwide

Industry-wide Ransomware Victims

Business Services was the most heavily impacted sector this period, accounting for 9.86% of all identified ransomware victims. This keeps service-heavy organisations, handling client operations, outsourcing, and third-party workflows, right at the centre of attacker focus, where disruption to service delivery and contractual obligations creates immediate leverage.

A strong second tier consisted of Construction Management (5.63%), Manufacturing (4.93%), Industrial Machinery & Equipment (4.23%), and Law Firms (4.23%), with Hospitals & Physicians Clinics, Banking, and Electronics (each 3.52%) close behind. Together, these sectors span project execution, core production, heavy industry, legal services, frontline healthcare, and financial operations, all areas where downtime and data loss can rapidly turn into regulatory, safety, or revenue crises.

A broad mid-band followed, including Finance, Education, Building Materials, Electricity, and Food & Beverage (each 2.82%), alongside Government, Architecture, Chemicals & Related Products, Hospitality, Real Estate, Advertising Networks, Home Improvement & Hardware Retail (each 2.11%). This layer shows how both public-sector entities and critical commercial verticals, from utilities and construction supply chains to education and retail-adjacent services, are now routine fixtures in ransomware datasets.

Lower-volume but still active categories were widely spread, covering Telecommunications, Energy, Apparel & Accessories Retail, Civil Engineering Construction, Insurance, Grocery Retail, Appliances, Transportation, ERP providers (each 1.41%), plus a long tail of niche and specialised segments such as Healthcare Technology, Office Products Distribution, Agriculture, Automotive Dealers and Service, Freight & Logistics, Department Stores, Grocery and Furniture sub-verticals, Media & Internet, Broadcasting, Membership Organisations, Holding Companies, Airlines, and various retail/consumer service bands (each 0.7%). Individually small but collectively significant, this long-tail distribution reinforces the same pattern seen in geography data: ransomware pressure is highly diversified across industries, and any organisation with digital operations and monetisable data sits somewhere inside the threat surface.

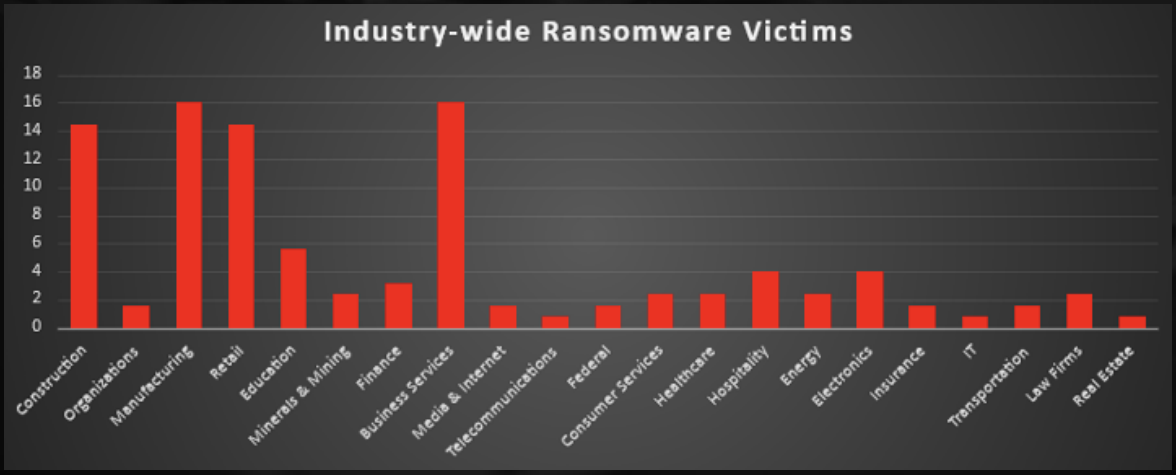


Figure 6: Industry-wide Ransomware Victims