

# Cyber - Akira Ransomware

Akira ransomware has emerged in recent years as one of the more serious cyber threats to businesses and organisations.

This Loss document is intended to provide guidance on protecting against an Akira ransomware attack.

# Cyber – Akira Ransomware

## Introduction

Ransomware cyber-attacks are a growing risk to businesses and organisations, and the threat is increasing with more frequent and targeted attacks being reported.

The open-source intelligence site [Ransomware.live](https://ransomware.live) reported over 5,000 successful attacks across the world from January to September 2025.

Akira is a prominent strain of ransomware that operates primarily as a Ransomware-as-a-service model (RaaS) targeting corporate entities, with the team behind it effectively partnering with hacking outfits. The hackers breach company systems, steal data, and then deploy Akira ransomware to encrypt digital estates, leveraging a double extortion method to pressure organisations into paying up.

This Loss Prevention Standard provides an in-depth look at the Akira ransomware group's background, their tactics and techniques, the types of organisations at risk, and proactive measures recommended by security authorities (such as the UK's National Cyber Security Centre and the U.S. Cybersecurity and Infrastructure Security Agency (CISA) to mitigate this threat.

## Background

Akira first emerged in early 2023 and quickly became a significant player in the ransomware space. The group behind the model is believed to be highly experienced, with some researchers noting clear overlaps with the infamous Conti group (a now-defunct ransomware group). Code analysis and even cryptocurrency wallet records suggest Akira's developers may include former Conti members. This lineage indicates that Akira's operators have a sophisticated pedigree, reusing proven techniques and software routines from past high-profile campaigns.

Akira will publish stolen data if victims refuse to pay. Their unique site on the dark web allows visitors (including the victims and media) to navigate via typed commands and see lists of "hacked companies" and upcoming data releases.

Akira has expanded rapidly. Within months of their first attacks, they developed versions of their malware for Windows, Linux and VMware ESXi systems, enabling them to encrypt virtual infrastructure as well as ordinary PCs. By early 2024, the group had hit over 250 organisations worldwide, causing estimated losses of at least \$42 million USD in ransom payments. Law enforcement agencies across the US and Europe (including the FBI, CISA, Europol, and the Netherlands' NCSC) have issued joint alerts about Akira, underscoring the threat's severity. Security analysts classify Akira as a RaaS operation, meaning the core group provides the ransomware malware and leak site, while affiliates (criminal partners) carry out the intrusions and share in the profits.



This business model has lowered the barrier to entry for cybercrime – even relatively young or less-skilled hackers (commonly referred to as Script Kiddies) can inflict major damage by leasing Akira’s tools.

## **Akira Tactics, Techniques and Procedures**

### **Initial Intrusion**

Most Akira incidents begin with the attackers gaining unauthorised access to a victim’s network, often by exploiting weak remote access security. A common entry point is through Virtual Private Network (VPN) services or Remote Desktop Protocol (RDP) access points that are not secured with multifactor authentication. In practice, this means if an organisation’s VPN or remote login accepts just a password, and that password is weak (easily guessed) or has been leaked, Akira’s affiliates can readily break in.

Akira actors have also been observed exploiting known software vulnerabilities in internet-facing systems to gain entry. For example, they have targeted flaws in VPN and networking products such as Cisco ASA and Fortinet appliances. In 2023, Cisco disclosed that Akira was actively abusing a then-unknown zero-day exploit (CVE-2023-20269) in Cisco’s VPN software to acquire valid credentials and establish remote access. Unpatched VPN servers and other exposed applications are essentially open doors for these attackers.

Phishing emails with malicious attachments or links have also been used to trick employees and steal their login details. In some cases, Akira may even purchase stolen credentials from underground markets (via “initial access brokers”) to speed up the break-in.

Overall, the group’s initial access techniques rely on taking advantage of poor authentication practices and unpatched security holes, routes that can often be prevented with basic cyber hygiene risk management.

### **Gaining a Foothold**

Once inside a network, the Akira attackers often move swiftly to establish persistence and prepare the ground for ransomware deployment. One tactic is to create new user accounts (or use stolen ones) with administrative privileges. By having admin-level access, the attackers can then disable security tools and explore the network freely. Akira is known to disable or uninstall antivirus and other endpoint protections to avoid detection. In one investigation, researchers saw the attackers exploit a vulnerable driver to shut down security processes, a stealthy bring-your-own-vulnerable-driver trick to evade defences. They may also use legitimate remote administration tools (like AnyDesk or natively available PowerShell scripts) to blend in with normal IT activity.

Next, the intruders gather intel via reconnaissance and perform lateral movements across the digital estate. They scan the network to identify other systems, servers, and accessible backups. Publicly available admin tools are known to be repurposed for this stage: for example, Akira operators have been seen running Active Directory queries to map out user accounts, computers, and trust relationships. They also deploy network scanners such as SoftPerfect Network Scanner and Advanced IP Scanner to locate additional machines and open ports.

During this discovery phase, the attackers will hunt for high-value targets like file servers and domain controllers, as well as any accessible backup systems.

Akira is known to harvest credentials aggressively to expand their reach: using tools like Mimikatz and LaZagne to dump passwords from memory, stealing password hashes or Kerberos tickets, and even extracting entire Active Directory databases from domain controllers. With a trove of credentials, they can then move laterally, using stolen admin accounts to log in via RDP to other servers, or using remote execution tools to push malware across machines.

By this point, the attackers effectively control the IT environment: This ensures that even if one access route is discovered and cut off by defenders, the attackers have alternate channels to maintain their foothold.

Akira's operators focus on evasion detection during these stages. Beyond disabling security software, they may hide their tracks by modifying system settings. Researchers noted instances of Akira affiliates tampering with Windows Registry settings to hide newly created users from the logon screen and to allow remote RDP logins without re-entering credentials. Akira actors have been observed creating a virtual machine (VM) within the victim's network to run their tools in isolation, attempting to conceal malicious actions under the guise of a legitimate VM.

### **Data Exfiltration and Ransomware Deployment**

After exploring the network and gaining control, the Akira group proceeds to steal sensitive data and then encrypt systems, two steps of their double-extortion scheme. Data theft (exfiltration) usually occurs before ransomware is triggered. Akira attackers take time to gather confidential files: databases, financial records, client data, and any intellectual property they can find. To export this, they use trusted tools and channels.

They might compress large data archives using WinRAR and then transfer them out via FileZilla or WinSCP (FTP/SFTP clients) or through cloud storage sync tools like Rclone (often configured to upload to Mega cloud drives). In some cases, they have leveraged their installed backdoors (such as AnyDesk or an SSH/RDP session) to exfiltrate data directly. The use of common IT utilities for exfiltration makes it harder for automated defences to distinguish malicious transfers from normal network operations.

With the valuable data safely in their possession, the attackers execute the ransomware encryption across the network. The Akira ransomware is a sophisticated malware that uses strong encryption to lock files. Encrypted files are renamed with an ".akira" extension (or in some newer cases ".powerranges", referencing a variant of the malware dubbed "Megazord"). On Windows systems, Akira also runs commands to delete backup shadow copies. They have similarly targeted popular enterprise backup solutions, using tools to locate and wipe Veeam backups and snapshots in one reported incident. In effect, they try to remove any recovery options the victim might have.

Once encryption is complete, the ransomware leaves a plain-text ransom note (often named akira\_readme.txt or fn.txt) in directories, containing a brief message and a unique code or link for contacting the attackers via a Tor hidden service (onion site). Akira's note typically does not specify an amount or deadline upfront; instead, victims are instructed to initiate contact and await further instructions. This tactic forces the victim to engage with the criminals if they want to negotiate, at which point the attackers will set an amount in private. According to reports, [Akira's ransom demands have ranged from around \\$200,000 up to \\$4 million \(USD\)](#), depending on the victim's size and the value of data stolen.

If a victim refuses to pay for decryption, the gang will threaten to publish or sell the stolen data. Akira maintains a dark web leaks blog where they name victims and post sample data to prove the validity of the breach. To increase pressure, Akira's team has been known to call companies directly to exert further pressure on paying the ransom and the consequences of a data leak. Unlike some groups, Akira has reportedly offered victims a choice: they can pay to decrypt files or (for a separate fee) pay to delete the stolen data. In other words, if a company has good backups and doesn't need the decryption key, Akira might still extort money solely for the promise of not leaking data (although entrusting criminals to delete stolen data is a risk in itself).

Payments are typically demanded in cryptocurrency (usually Bitcoin) to maintain anonymity. If the victim pays, the attackers supply a decryption tool and agree to destroy their copy of the data. If the victim refuses, Akira will often publish the data on their site which other criminals can use to exploit. Therefore, even organisations with reliable data backups may find themselves paying to avoid public breaches of confidentiality.

### **Target Organisations**

Akira's operations have been indiscriminate in terms of industry and geography, putting many types of organisations at risk. In their first year of activity, Akira impacted companies across North America, the UK, Europe, and the Asia-Pacific region. It appears they are willing to target any organisation that might afford a ransom, whether in the private sector or critical infrastructure. A US government alert in 2024 noted Akira attacks spanning a "wide range of businesses and critical infrastructure entities", from small professional firms to larger industrial companies and schools.

Akira appears to be relatively sector agnostic, but the healthcare sector has been frequently hit; both US and UK authorities have warned hospitals and health services to be on guard, as Akira's leak site has listed multiple health sector victims. The group's willingness to go after hospitals, schools, and critical services underscores their ruthlessness - these are sectors where outages can be life-threatening or hugely disruptive.

Other reported Akira victims have included municipalities, law firms, and educational institutions. The overarching common thread is that the organisation targeted had some vulnerability - whether human (e.g. an employee falling for a phishing email or using a poor password) or technical (an unpatched VPN gateway, an exposed RDP port, etc.) that opened the door to attackers. No organisation is truly "too small" or "too niche" to be targeted; Akira's affiliate model means multiple threat actors are each seeking out opportunities, and they will pursue any network they can monetise. Ransomware has become a booming criminal industry, with a low barrier to entry, rather than the realm of a few elite hackers. Groups utilising Akira are part of this criminal ecosystem and have shown willingness to target everything from local businesses to critical national infrastructure. Therefore, all organisations should consider themselves at risk and ensure they are prepared.

### **Proactive Mitigations and Defensive Measures**

Defending against Akira and similar ransomware groups/strains is possible through strong fundamental cybersecurity practices. Both industry experts and national security agencies have published guidance to help organisations reduce the risk of a devastating attack. Below are key mitigation measures drawn from the UK NCSC, U.S. CISA/FBI advisories, and security research.

## **Strengthen Access Controls**

Implement multi-factor authentication on all remote access services (VPNs, RDP, email, etc.) and any critical accounts. MFA adds an extra login step (such as a one-time code or mobile app approval) that dramatically reduces the chance of an attacker using stolen or guessed passwords.

Ensure strong, unique passwords are used – ideally enforced via policy and supplemented with user education about creating passphrases (the UK NCSC recommends the [three random words](#) technique for memorable but strong passwords).

All default passwords on systems should be changed, and password reuse across different accounts must be avoided to prevent credential stuffing attacks. It's also advisable to monitor for leaked credentials (through threat intelligence or services) so you can reset any that become exposed.

## **Patch Known Vulnerabilities Promptly**

Keep your systems and software up to date with security patches, especially for internet-facing servers and devices. Many Akira intrusions leveraged known vulnerabilities in VPN appliances and other software that had updates available. Prioritise patching any “high” or “critical” severity flaws that attackers are known to exploit (CISA provides a public catalogue of [Known Exploited Vulnerabilities](#) that is a good reference).

If legacy systems cannot be patched immediately, consider temporary workarounds such as segmentation and removing external access or increased monitoring on those assets until they can be updated. Timely patching is repeatedly cited by experts as one of the most cost-effective steps to prevent ransomware incidents.

## **Lock Down Remote Access**

Evaluate and harden any remote access points into your network. Disable unused RDP or other remote desktop ports, or at least restrict them behind a VPN or firewall. If VPN is used, require MFA and consider adding user IP/address restrictions if possible.

Regularly review configurations for VPNs, cloud admin portals, and email access to ensure they follow security best practices (e.g. using modern encryption, no default creds, etc.). Misconfigured or exposed remote services are like an open door for attackers, so they should be tightly controlled or closed altogether when not needed.

## **Segment and Limit Network Access**

Use network segmentation to prevent an intruder from freely roaming across your entire IT environment. For example, sensitive servers should be on separate VLANs or sub-networks with strict access rules. If an accounting system has no need to talk to the factory floor network, enforce that separation. This way, even if one part of the network is breached, ransomware cannot easily spread to all systems.

Applying the principle of least privilege for user accounts is also crucial: employees (and their credentials) should only have access to the systems and data necessary for their job. Regularly audit accounts and remove any unnecessary admin privileges, limiting what hackers can do if they compromise a single account.

## **Deploy Detection and Response Tools**

Invest in modern endpoint detection and response (EDR) and network monitoring solutions that can spot suspicious activity. There are a number of open source tools available to assist with this, one of which is Wazuh. These tools can alert on unusual patterns, such as an unknown program trying to disable antivirus, or a user account suddenly accessing large amounts of data at odd hours.

According to CISA, using an EDR can help detect lateral movement and command-and-control channels by flagging uncommon connections on hosts.

Set up centralised logging and security information and event management (SIEM) so that you have visibility across the network – and make sure someone is tasked to review alerts. It’s also wise to configure alerts for specific indicators of compromise tied to Akira’s known tactics (e.g. alerts if a new account named “itadm” is created on a domain, or if tools like AdFind.exe or Rclone.exe are executed on servers). While false positives can occur, tuning your detection to known threat behaviours can dramatically improve early warning of an attack in progress.

### **Protect and Backup Your Data**

Maintain offline, encrypted, immutable backups of critical data and systems, and test your restore procedures regularly. “Offline” means the backup is stored in a way that is not constantly connected to your main network – for example, on external drives that are plugged in only for backups, or in secure cloud storage with separate credentials. This protects backups from being encrypted or deleted by ransomware that gains domain-wide access. Having reliable backups can dramatically impact recovery time however, the risk of data leak extortion would remain.

### **Disaster Recovery Plan**

In addition to backing up, ensure you have disaster recovery plans for quickly restoring operations, and consider keeping some spare hardware or cloud failover options if your primary systems are hit. The faster you can recover independently, the less pressure to pay a ransom.

### **Implement Email and Web Protections**

Since phishing is a common initial vector, deploy robust email security filters to catch malicious attachments or links. Many attacks start with an innocent-looking email, so spam filters and attachment sandboxing can stop malware before it reaches users.

Train staff to recognise phishing attempts and social engineering – for instance, by running periodic phishing simulation tests and interactive training. Web browsing protections (DNS filtering, blocking access to known malicious sites) can also prevent users from accidentally visiting the attackers’ infrastructure (e.g. if they click a bad link).

### **Harden Your Infrastructure**

Take inventory of all your IT assets and ensure they are configured securely. Turn off or uninstall any unneeded services or software (reducing the attack surface). Disable default admin shares or at least rename the default administrator accounts, so attackers can’t guess them easily.

Apply recommended hardening guidelines for operating systems (such as enabling controlled folder access, securing PowerShell, and requiring signed scripts where possible). Also, close unnecessary ports and enforce host-based firewalls – for example, if a workstation never needs to act as a server, it shouldn’t accept incoming connections at all. These measures can stall an attacker’s lateral movement.

## Prepare an Incident Response Plan

Despite best efforts, assume a breach could happen and have a plan ready. Develop and practice a cyber incident response plan that covers detection, containment, eradication, recovery, and communication steps. This should include:

- Who to call (internal teams, external specialists, legal counsel, cyber insurance etc.),
- How to isolate infected systems (e.g. network isolation procedures), and
- How to safely restore from backups.

Having a playbook means faster and more coordinated response, which can significantly limit damage if an attack occurs.

Include a plan for external communications (notifying customers or regulators if data is compromised – this is crucial for compliance and managing reputational damage).

Also, engage with threat intelligence and law enforcement as appropriate; for instance, UK organisations can reach out to the [NCSC](#) or regional police cyber units for guidance, and worldwide there's [StopRansomware.gov](#) resources and contacts.

Reporting incidents can help authorities track the attackers and potentially aid in recovery efforts (in some cases decryption tools or keys have been obtained by law enforcement for certain ransomware).

## Regular Training and Auditing

Cultivate a security aware culture. Conduct regular staff training on cybersecurity basics, especially focusing on phishing awareness, safe password practices, and the importance of reporting unusual IT issues promptly. Simulate attacks (like red-team exercises or table-top exercises) to test your organisation's readiness and improve your team's response. Additionally, perform routine security audits and risk assessments, ideally by independent experts, to uncover any weaknesses before attackers do.

Additionally, perform routine security audits and risk assessments, ideally by independent experts, to uncover any weaknesses before attackers do.

In the United Kingdom, frameworks such as [Cyber Essentials](#) or [ISO 27001: Information security, cybersecurity and privacy protection - Information security management systems - Requirements](#) can provide structured guidance on best practices and help demonstrate your commitment to cyber resilience.

## Summary

Defending against Akira is not about any one silver bullet, but rather a layered approach combining technology, process, and people. Basic cyber hygiene – like up-to-date systems, strong authentication, limited privileges, and monitored networks – forms the foundation that can thwart most of Akira's known tactics.

As the UK's NCSC and partners stress, organisations should assume that threat actors will find the weakest link, so it's critical to shore up all areas of your cyber defences simultaneously. By implementing the measures above, a company makes itself a much harder target and potentially prevent a cyber ransomware event.

## Specialist Partner Solutions

Aviva Risk Management Solutions can offer access to a wide range of risk management products and services at preferential rates via our network of Specialist Partners.

Business Continuity - [Horizonscan](#)

Cyber Security Awareness Training [Phishing Tackle](#)

For more information please visit: [Aviva Risk Management Solutions – Specialist Partners](#)

## Sources and Useful Links

- CISA Stop Ransomware Site - [Stop Ransomware | CISA](#)
- CISA KEV catalogue - [Known Exploited Vulnerabilities](#)
- CISA - [#StopRansomware: Akira Ransomware](#)
- [Ransomware Live](#)
- [FBI Healthcare Advisory](#)
- [Qualys Akira Article](#)
- [Weightmans Akira Advisory](#)
- [Trend Micro Advisory - Ransomware Spotlight - Akira](#)
- [US Health Sector Cybersecurity Coordination Centre: HC3 Akira Software](#)
- [Qualys Community - Akira Ransomware Analysis Origins, Tactics and Detection Strategies](#)
- [Qualys - What is Akira Ransomware: An Overview](#)
- [Trend Micro - Ransomware Spotlight: Akira](#)
- [CISA #StopRansomware: Akira Ransomware - Summary](#)

## Additional Information

Relevant Aviva Loss Prevention Standards include:

- **Cyber Security: Top 12 Tips to Protect Against Cyber Attacks.**
- **Cyber Security: Respond and Recover.**
- **Cyber Security: The Internet of Things**
- **Ransomware – Cyber Loss Prevention Standard**
- **Cyber Essentials – Accreditation**
- **Cyber – Respond and Recover**
- **Cyber – Incident Response Process**
- **Cyber – Homeworking Security**

To find out more, please visit [Aviva Risk Management Solutions](#) or speak to one of our advisors.

Email us at [riskadvice@aviva.com](mailto:riskadvice@aviva.com) or call 0345 366 6666.\*

\*The cost of calls to 03 prefixed numbers are charged at national call rates (charges may vary dependent on your network provider) and are usually included in inclusive minute plans from landlines and mobiles. For our joint protection telephone calls may be recorded and/or monitored.

## **Please Note**

This document contains general information and guidance only and may be superseded and/or subject to amendment without further notice. Aviva has no liability to any third parties arising out of ARMS' communications whatsoever (including Loss Prevention Standards), and nor shall any third party rely on them. Other than liability which cannot be excluded by law, Aviva shall not be liable to any person for any indirect, special, consequential or other losses or damages of whatsoever kind arising out of access to, or use of, or reliance on anything contained in ARMS' communications. The document may not cover every risk, exposure or hazard that may arise, and Aviva recommend that you obtain specific advice relevant to the circumstances.

14<sup>th</sup> November 2025

Version 1.1

ARMSGI3422025

Aviva Insurance Limited, Registered in Scotland Number SC002116. Registered Office: Pitheavlis, Perth PH2 0NH.  
Authorised by the Prudential Regulation Authority and regulated by the Financial Conduct Authority and the Prudential Regulation Authority.