Red Piranha
unified threat management

THREAT INTELLIGENCE REPORT

Feb 18 - 24, 2025

Report Summary:

- **New Threat Detection Added** – 2
  - Zyxel Telnet Default Credentials Vulnerability (CVE-2025-0890)
  - Ivanti Endpoint Manager Credential Coercion Vulnerabilities

- **New Threat Protections - 160**

The following threats were added to Crystal Eye this week:

1. Zyxel Telnet Default Credentials Vulnerability (CVE-2025-0890)

CVE-2025-0890 is a critical security vulnerability affecting legacy Zyxel Customer Premises Equipment (CPE) devices, specifically the VMG4325-B10A model running firmware version 1.00(AAFR.4) C0_20170615. This vulnerability arises from the use of insecure default credentials for the Telnet service, which, if unchanged by administrators, can allow unauthorised access to the device's management interface. The default accounts are:

- supervisor: zyad1234
- admin: 1234
- zyuser: 1234

The supervisor account, previously documented under CVE-2017-18371, possesses hidden privileges granting full system access. The zyuser account, though limited, can be leveraged in conjunction with other vulnerabilities, such as CVE-2024-40891, to achieve remote code execution. Despite these devices reaching end-of-life status and no longer receiving official support or patches from Zyxel, approximately 1,500 affected systems with internet-facing Telnet interfaces remain operational worldwide. This exposure underscores the critical need for users to change default credentials and consider replacing outdated hardware to maintain network security.

Threat Protected: 03
Rule Set Type:

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

Class Type: Attempted admin

Kill Chain:

Tactic	Technique ID	Technique Name
Initial Access	T1078	Valid Accounts
Execution	T1059.004	Command and Scripting Interpreter: Unix Shell
Persistence	T1078	Valid Accounts

2. Ivanti Endpoint Manager Credential Coercion Vulnerabilities

In October 2024, security researchers identified four critical vulnerabilities in Ivanti Endpoint Manager (EPM), which were subsequently patched in Ivanti's January 2025 update. These vulnerabilities allow unauthenticated attackers to coerce the EPM server's machine account credentials, enabling potential relay attacks that could compromise the server. The identified vulnerabilities are:

CVE-2024-10811: Credential Coercion in GetHashForFile
CVE-2024-13161: Credential Coercion in GetHashForSingleFile
CVE-2024-13160: Credential Coercion in GetHashForWildcard
CVE-2024-13159: Credential Coercion in GetHashForWildcardRecursive

These vulnerabilities reside in the WSVulnerabilityCore.dll component of the EPM server, specifically within the VulCore class, which exposes APIs related to vulnerability management. The affected methods (GetHashForFile, GetHashForSingleFile, GetHashForWildcard, and GetHashForWildcardRecursive) fail to validate user input properly, allowing attackers to supply crafted inputs that cause the server to access remote UNC paths. This behaviour can be exploited to coerce the server into authenticating against an attacker's system, facilitating relay attacks.

Threat Protected: 01
Rule Set Type:

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

Class Type: Attempted-admin

Kill Chain:

Tactic	Technique ID	Technique Name
Initial Access	T1190	Exploit Public-Facing Application
Execution	T1203	Exploitation for Client Execution
Credential Access	T1557	Adversary-in-the-Middle
Persistence	T1078	Valid Accounts

Known exploited vulnerabilities (Week 3 February 2024):

Vulnerability	CVSS	Description
CVE-2025-0108	8.8 (High)	Palo Alto Networks PAN-OS Authentication Bypass Vulnerability
CVE-2024-53704	9.8 (Critical)	SonicWall SonicOS SSLVPN Improper Authentication Vulnerability
CVE-2025-0111	7.1 (High)	Palo Alto Networks PAN-OS File Read Vulnerability
CVE-2025-23209	8.1 (High)	Craft CMS Code Injection Vulnerability
CVE-2025-24989	8.2 (High)	Microsoft Power Pages Improper Access Control Vulnerability

For more information, please visit the **Red Piranha Forum**:
https://forum.redpiranha.net/t/known-exploited-vulnerabilities-catalog-3rd-week-of-february-2025/547

Updated Malware Signatures (Week 3 February 2024)

Threat	Description
Lumma Stealer	A type of malware classified as an information stealer. Its primary purpose is to steal sensitive information from infected systems, including but not limited to credentials, financial information, browser data, and potentially other personal or confidential information.

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 Groups	Overall Percentage of total attack coverage
RansomHub	18.3%
Inc ransom	4.58%
Lynx	9.15%
Abyss-Data	0.65%
Embargo	1.31%
SafePay	3.27%
FunkSec	4.58%
Fsociety	2.61%
Cactus	7.84%
Hunters	0.65%
Akira	11.11%
Brain Cipher	1.96%
Qilin	5.88%
Fog	1.96%
Play	7.84%
Medusa	1.96%
BlackSuit	0.65%
Kairos	1.31%
Team Underground	0.65%
Rhysida	0.65%
Eraleign (APT73)	0.65%
Linkc	0.65%
RansomHouse	0.65%
Bianlian	0.65%
KillSec3	5.23%
Cloak	3.27%
Apos	0.65%
Termite	0.65%

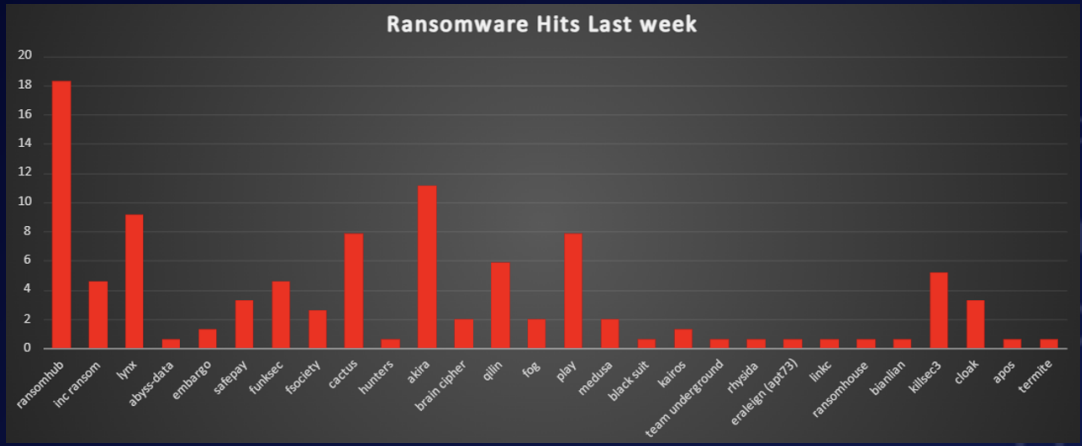

Figure 1: Ransomware Group Hits Last Week

Akira Ransomware Group

Overview

Ransomware threats continue to evolve, and among the latest variants making a significant impact in the cybersecurity landscape is Akira ransomware. Emerging in early 2023, Akira has actively targeted businesses across multiple industries, employing sophisticated encryption techniques to lock critical files and extort victims for ransom payments. This analysis explores Akira ransomware in-depth, covering its origins, attack methodology, encryption strategies, indicators of compromise (IOCs), and best practices for mitigation.

Origins and Background

Akira ransomware was first detected in March 2023 and quickly gained attention due to its ability to infiltrate both Windows and Linux environments. Researchers believe Akira operates under a Ransomware-as-a-Service (RaaS) model, wherein affiliates distribute the malware and share ransom proceeds with its developers.
Notably, Akira's developers are suspected to have prior experience in ransomware operations, possibly linked to the now-defunct Conti group. This hypothesis is based on similarities in source code, encryption methodologies, and attack tactics observed between Akira and past Conti campaigns.

Detailed Tactics, Techniques, and Procedures (TTPs)

Akira ransomware employs a well-defined attack methodology, systematically compromising targeted systems through multiple stages, including initial access, privilege escalation, lateral movement, data exfiltration, and file encryption.

Execution and Privilege Escalation

- System Services Execution (T1569, T1569.002): Akira leverages Windows Service Control Manager (services.exe) to maintain persistence and execute payloads.
- Privilege Escalation via Credential Dumping (T1003): Attackers use tools such as Mimikatz and PowerShell scripts to extract credentials.
- Remote Execution (T1021.002, T1078): Lateral movement is achieved via RDP, PsExec, and SSH (for Linux targets).

System Reconnaissance & Information Gathering

- System Information Discovery (T1082): Identifies machine configurations, domain details, and network topology.
- Registry Queries (T1012): Extracts system and user-specific configurations.
- Account Discovery (T1087): Harvests valid user credentials to escalate privileges.

Lateral Movement & Persistence

- Remote Desktop Protocol (RDP) Exploitation (T1021.001): Used for moving across the network.
- Windows Admin Shares (T1021.002): Attackers leverage compromised admin credentials to gain access to shared resources.
- Scheduled Task/Job Execution (T1053.005): Persistence through scheduled tasks that execute the ransomware payload.

Data Exfiltration & Impact

- Data Exfiltration (T1567.002): Utilises tools like Rclone and WinSCP to steal sensitive data before encryption.
- File Encryption for Impact (T1486): Akira encrypts files using a custom encryption algorithm and renames files with the .akira extension.
- Ransom Note Deployment (T1566): A ransom note (akira_readme.txt) is dropped with payment instructions.
- Double Extortion Model (T1653): Stolen data is used as leverage to coerce victims into ransom payments.

Targeted File Extensions

Akira selectively encrypts the following file types to maximise disruption while avoiding system crashes:
.docx, .xlsx, .pdf, .zip, .jpg, .png, .mp4, .sql, .db, .json, .php, .html
Critical system files like .exe, .dll, .sys are excluded to maintain system stability for ransom negotiations.

TTP Stage	Description	MITRE ATT&CK ID
Initial Access	Exploitation of unpatched VPN vulnerabilities, credential theft via phishing, brute-force attacks, or access through exposed remote services.	T1078, T1190
Privilege Escalation	Attackers leverage tools such as Mimikatz and PowerShell scripts to elevate privileges.	T1003, T1059
Lateral Movement	Movement through the network using RDP, PsExec (Windows), or SSH (Linux).	T1021, T1570
Data Exfiltration	Use of Rclone or WinSCP to extract sensitive data before encryption.	T1567
File Encryption & Ransom Deployment	Custom encryption algorithm applied to files, appending the .akira extension. Ransom notes (akira_readme.txt) are deployed with payment instructions.	T1486

Indicators of Compromise (IOCs)

Akira ransomware leaves distinct markers that security teams can monitor to detect and respond to infections.

- File Extensions and Ransom Note:
  - Encrypted files renamed with .akira extension.
  - Presence of akira_readme.txt in multiple directories.
- Command-and-Control (C2) Infrastructure:
  - Akira frequently changes its infrastructure, but known malicious IPs include:
    - 192.185.52.166
    - 185.141.63.120
  - Tor-based ransom payment and negotiation sites (updated on dark web monitoring platforms).

https://akiral2iz6a7qgd3ayp3l6yub7xx2uep76idk3u2kollpj5z3z636bad.onion/
https://akiral2iz6a7qgd3ayp3l6yub7xx2uep76idk3u2kollpj5z3z636bad.onion/l

- Chat Server:
  https://akiralkzxzq2dsrzsrvbr2xgbbu2wgsmxryd4csgfameg52n7efvr2id.onion/

Mitigation Strategies

Organisations can reduce their risk of Akira ransomware infections by implementing robust security measures:

- Enforce Multi-Factor Authentication (MFA) for VPN and RDP access.
- Regular Patching & Updates to software, firmware, and operating systems promptly.
- Disable unnecessary RDP access or enforce strict VPN controls with zero-trust policies.
- Implement Role-Based Access Control (RBAC) and limit administrative privileges.
- Deploy Advanced Endpoint Detection & Response (EDR) Solutions

Ransomware Victims Worldwide

A recent ransomware analysis highlights that the United States remains the most heavily impacted nation, accounting for a staggering 63.16% of global incidents, underscoring its ongoing vulnerability to ransomware threats. Following this, Canada reported 6.58% of attacks, reaffirming North America's status as a prime target.

Countries including Germany and the United Kingdom each accounted for 3.95% of incidents, reflecting notable exposure to ransomware attacks. Meanwhile, Sweden, France, and Taiwan each contributed 1.97%, further emphasising the widespread reach of these cyber threats.

A broader set of countries—including India, Australia, Netherlands, Malaysia, Spain, and Switzerland—each reported 1.32% of attacks, highlighting the diverse geographic footprint of ransomware activity. Additionally, nations such as the United Arab Emirates, Saudi Arabia, Singapore, Pakistan, Israel, Romania, Bulgaria, Bangladesh, Brazil, Finland, Nigeria, Colombia, Palau, and Ecuador each accounted for 0.66% of incidents, demonstrating the extensive global impact.

This analysis underscores the persistent and evolving nature of ransomware threats, with North America, Europe, and parts of Asia facing a significant portion of the impact. The findings emphasise the critical need for strengthened cybersecurity infrastructure, proactive defence strategies, and heightened vigilance across all sectors to mitigate the relentless rise of ransomware attacks worldwide.

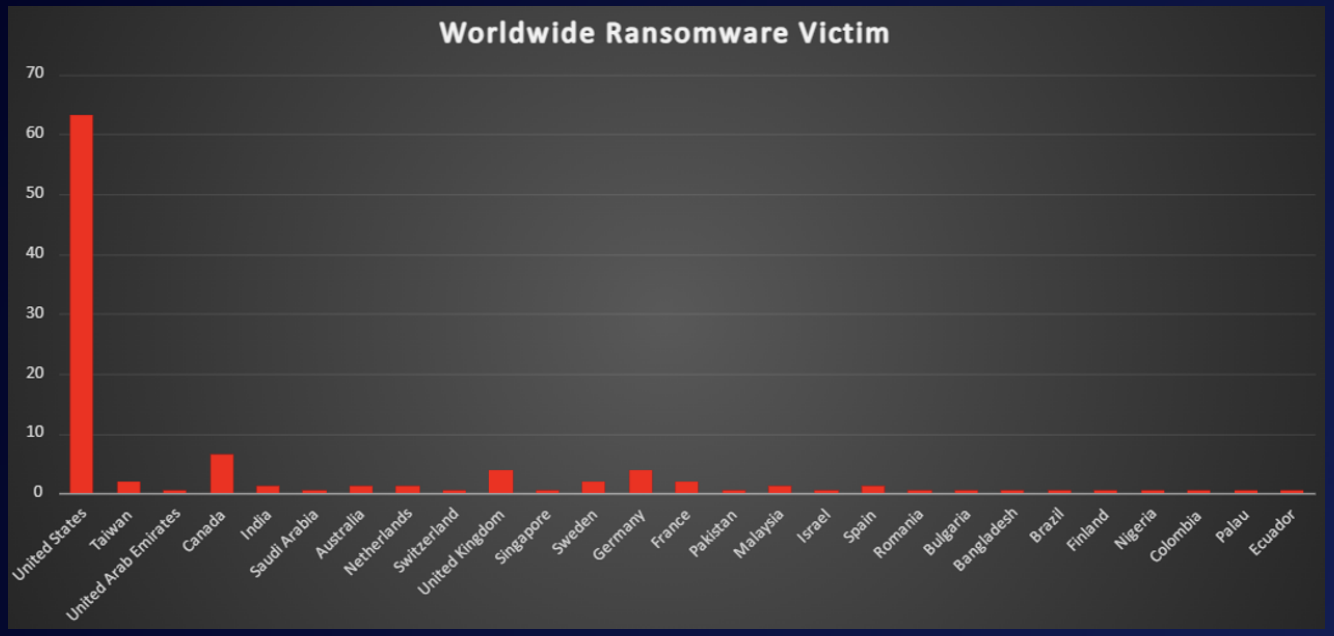

Figure 4: Ransomware Victims Worldwide

Ransomware Victims by Industry

A recent ransomware analysis highlights the Retail sector as the most targeted industry, accounting for 16.45% of total reported incidents. This underscores the sector's vulnerability due to its reliance on transactional systems and customer-facing operations.

Following closely, the Manufacturing sector reported 12.5% of ransomware attacks, emphasising the susceptibility of production and supply chain operations to cyber threats. The Business Services industry was also heavily impacted, making up 11.18% of incidents, while the Construction sector experienced 9.87%, demonstrating ongoing risks in infrastructure and project-based operations.

Sectors such as IT (7.89%), Healthcare (7.24%), and Federal Institutions (5.26%) also faced significant ransomware exposure, highlighting the persistent cyber threats across essential services and critical infrastructure. Meanwhile, Education (4.61%), Law Firms (3.95%), and Hospitality, Transportation, and Consumer Services (each 3.29%) also reported notable ransomware incidents.

Industries with a smaller, yet notable impact include Finance, Real Estate, Energy, and Insurance, each contributing 1.97%, while Agriculture, Minerals & Mining, and other organisations accounted for 0.66% of reported cases.

This analysis underscores the broad and indiscriminate nature of ransomware attacks, affecting industries across critical infrastructure, public services, and commercial enterprises. These findings reinforce the urgent need for tailored cybersecurity measures, stronger defences, and proactive risk management strategies to combat the ever-evolving ransomware landscape effectively.

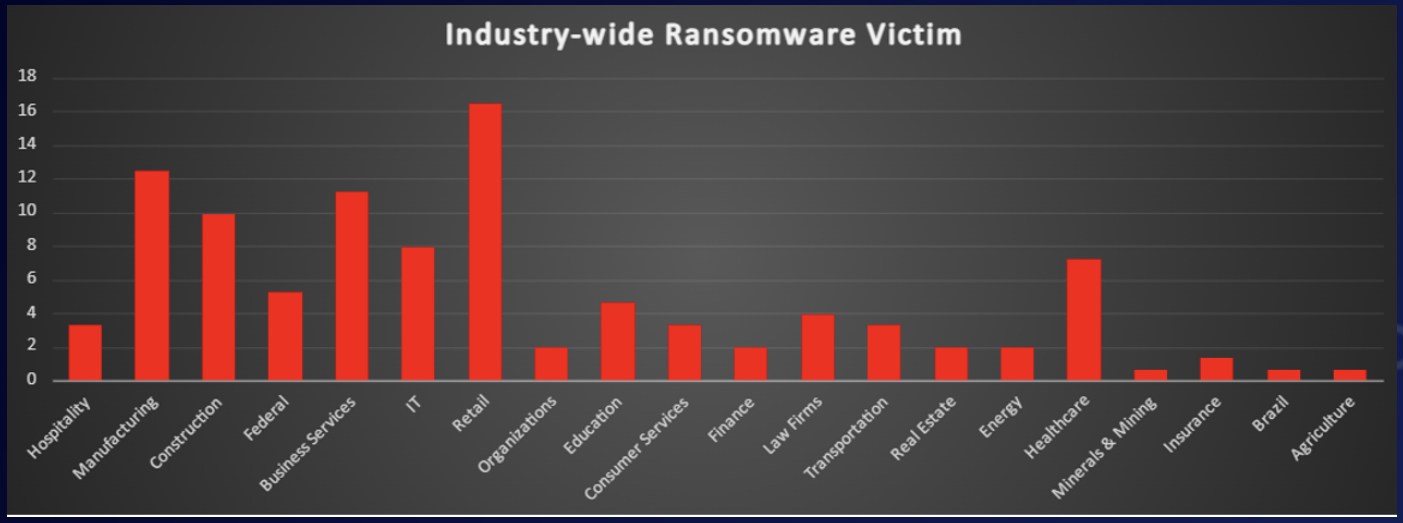

Figure 5: Industry-wide Ransomware Victims