Red Piranha
unified threat management

THREAT INTELLIGENCE REPORT

Feb 11 - 17, 2025

Report Summary:

- **New Threat Detection Added** – 2
  - Winos4.0 Malware Campaign
  - SonicWall SSL VPN Session Hijacking (CVE-2024-53704)
- **New Threat Protections - 144**

The following threats were added to Crystal Eye this week:

1. Winos4.0 Malware Campaign

Winos4.0 is an advanced malicious framework, evolved from Gh0strat, featuring modular components for comprehensive functionality and stable architecture. It has been deployed in various attack campaigns, including Silver Fox. Researchers have identified multiple samples of Winos4.0 concealed within gaming-related applications, such as installation tools, speed boosters, and optimisation utilities. Analysis of the decoded DLL file indicates potential targeting of the education sector, as evidenced by its file description, “校园政⊠” (Campus Administration).

Threat Protected: 05
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: Trojan activity

Kill Chain:

Tactic	Technique ID	Technique Name
Initial Access	T1195.001	Supply Chain Compromise: Compromise Software Supply Chain
Execution	T1059.005	Command and Scripting Interpreter: Visual Basic
Persistence	T1547.001	Boot or Logon AutoStart Execution: Registry Run Keys / Startup Folder
Defence Evasion	T1027	Obfuscated Files or Information
Command-and-Control	T1071.001	Application Layer Protocol: Web Protocols

2. SonicWall SSL VPN Session Hijacking (CVE-2024-53704)

CVE-2024-53704 is a critical authentication bypass vulnerability affecting the SSL VPN component of unpatched SonicWall firewalls. This flaw allows remote, unauthenticated attackers to hijack active SSL VPN sessions, granting unauthorised access to internal networks. Exploiting this vulnerability enables attackers to:

- Access Virtual Office bookmarks
- Obtain NetExtender client configuration profiles
- Establish VPN tunnels
- Terminate user sessions

The vulnerability affects SonicOS versions 7.1.x (7.1.1-7058 and earlier), 7.1.2-7019, and 8.0.0-8035. SonicWall released patches addressing this issue on January 7, 2025. Organisations are strongly advised to apply these updates promptly to mitigate potential exploitation.

Threat Protected: 02
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	T1133	External Remote Services
Execution	T1203	Exploitation for Client Execution
Persistence	T1078	Valid Accounts
Defence Evasion	T1036	Masquerading
Credential Access	T1557	Adversary-in-the-Middle

Known exploited vulnerabilities (Week 2 February 2024):

Vulnerability	CVSS	Description
CVE-2024-40891	8.8 (High)	Zyxel DSL CPE OS Command Injection Vulnerability
CVE-2024-40890	8.8 (High)	Zyxel DSL CPE OS Command Injection Vulnerability
CVE-2025-21418	7.8 (High)	Microsoft Windows Ancillary Function Driver for WinSock Heap-Based Buffer Overflow Vulnerability
CVE-2025-21391	7.1 (High)	Microsoft Windows Storage Link Following Vulnerability
CVE-2025-24200	6.1 (Medium)	Apple iOS and iPadOS Incorrect Authorisation Vulnerability
CVE-2024-41710	Ongoing Analysis	Mitel SIP Phones Argument Injection Vulnerability
CVE-2024-57727	7.5 (High)	SimpleHelp Path Traversal Vulnerability

For more information, please visit the **Red Piranha Forum**:
https://forum.redpiranha.net/t/known-exploited-vulnerabilities-catalog-2nd-week-of-february-2025/546

Updated Malware Signatures (Week 2 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 Group	Overall Percentage of total attack coverage
Hunters	0.77%
Fsociety	1.15%
SafePay	0.77%
Rhysida	1.15%
Ransomexx	0.38%
Kraken	2.3%
Qilin	3.07%
RansomHub	10.34%
Fog	2.3%
Handala	0.38%
Cicada3301	0.38%
Lockbit3	0.38%
Akira	5.75%
Lynx	1.53%
Medusa	6.13%
Wikileaksv2	0.77%
Sarcoma	2.68%
Killsec3	3.07%
Clop	36.4%
Eraleign (apt73)	0.38%
Bianlian	3.07%
DragonForce	0.77%
Monti	0.77%
Inc ransom	0.38%
Everest	0.38%
Cactus	0.77%
Termite	0.38%
Ransomware blog	0.38%
3AM	0.77%
Play	4.98%
Ciphbit	0.38%
FunkSec	6.51%
Embargo	0.38%

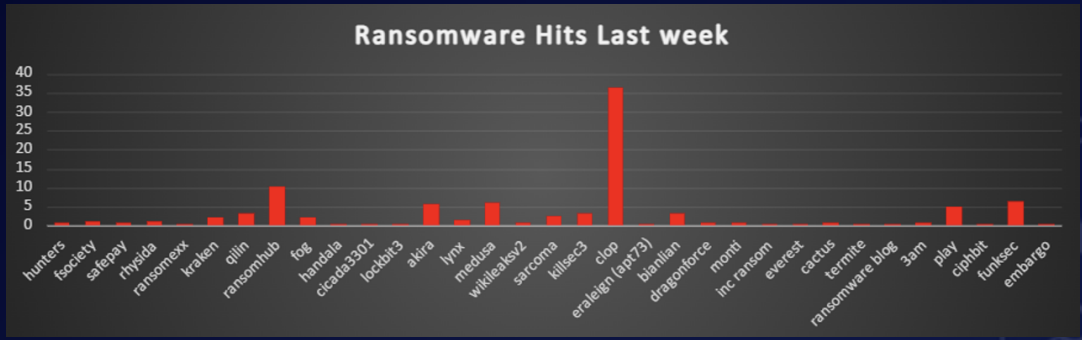


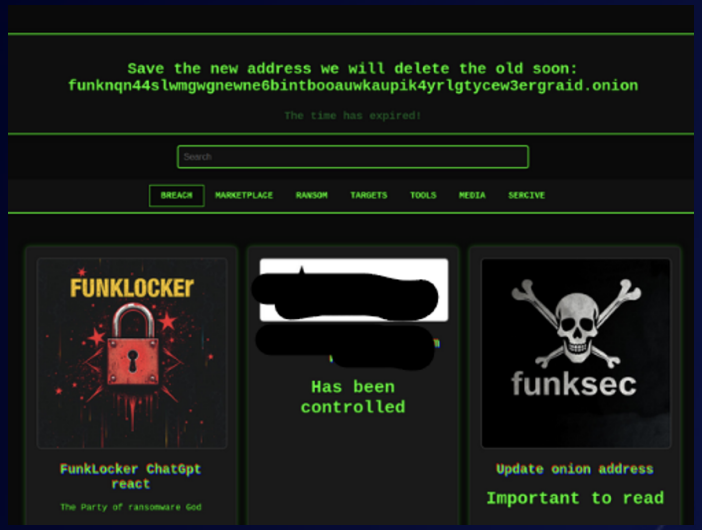
Figure 1: Ransomware Group Hits Last Week

FunkSec Ransomware Group

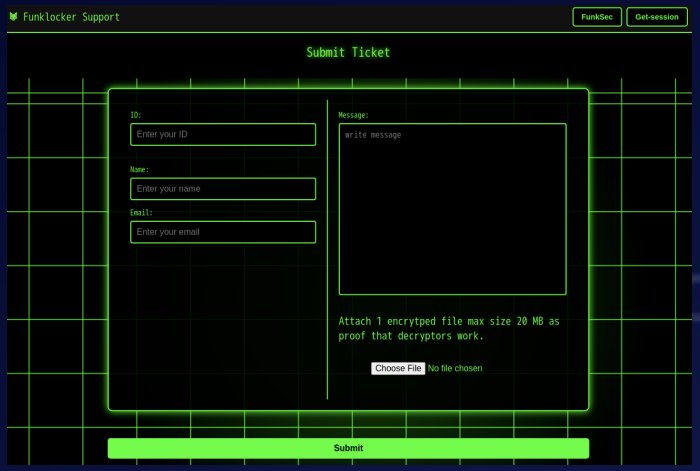
Overview

The Red Piranha team conducted an analysis and discovered that this ransomware variant exhibits advanced evasion techniques, including hiding itself in the Windows Recycle Bin, disabling Windows Defender, and encrypting a wide range of file types. The malware utilises PowerShell to bypass execution policies and load the BitLocker module, potentially leveraging it for encryption. Additionally, the ransomware is linked to phishing campaigns using fake login portals and malicious executables. It appends the .funksec extension to encrypted files and drops ransom notes in the affected directories.

THE DATA LEAK SITE



Contact Form - FunkLocker Support



Detailed Tactics, Techniques, and Procedures (TTPs)
This ransomware arrives on a system as a file dropped by other malware or as a file unknowingly downloaded by users when visiting malicious websites.

Once executed, it drops the following file:

{malware filepath}\IMAGENAME.jpg – Sets this image as the desktop wallpaper after encryption, likely as part of its intimidation tactics.

1. Initial Access

- Phishing Links & Malicious Downloads
  - Fake software installers and disguised document files (setup-avast-premium-x64.exe, document pdf.exe, Agent381.msi)
  - Malicious URLs that impersonate legitimate services (employeeportal.net-login.com, gmail.net-login.com).

2. Execution

- Execution via Malicious PowerShell Scripts
  - The malware bypasses execution policies using the command:

File Path	Cmdline
C:\Windows\System32\net.exe	"net" session
C:\Windows\System32\tasklist.exe	"tasklist" /fi "IMAGENAME eq vmware"
C:\Windows\System32\WindowsPower-Shell\v1.0\powershell.exe	"powershell" -Command "Set-MpPreference -DisableRealtimeMonitoring $true"
C:\Windows\System32\WindowsPower-Shell\v1.0\powershell.exe	"powershell" -Command "wevtutil sl Security /e:false"
C:\Windows\System32\WindowsPower-Shell\v1.0\powershell.exe	"powershell" -Command "wevtutil sl Application /e:false"
C:\Windows\System32\WindowsPower-Shell\v1.0\powershell.exe	"powershell" -Command "Set-ExecutionPolicy Bypass -Scope Process -Force"

3. Persistence & Defence Evasion

- Hiding in the Recycle Bin
  - The malware creates files in the Recycle Bin to avoid detection:

Source: C:\Users\user\Desktop\setup-avast-premium-x64.exe

File created:
C:\$Recycle.Bin\S-1-5-21-2246122658-3693405117-2476756634-1000\desktop.ini.funksec

- Windows Defender Tampering
  - Modifies Defender settings to disable real-time monitoring:

Set-MpPreference -DisableRealtimeMonitoring $true

- Use of BitLocker Module
  - Loads the BitLocker PowerShell module, possibly for encryption purposes:

Source: C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
File opened: C:\Windows\system32\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psd1

4. Impact (Ransomware Encryption)

- Encrypts files with the following extensions:
  - Documents, scripts, archives, databases, media files, and executables.
  - Appends .funksec to encrypted files.
- Drops ransom notes in the format:
  {malware filepath}\README-{10 random alphanumeric}.md

Tactic	Technique	Details	TTP ID
Initial Access	Phishing with Malicious Attachments	Malicious executables and scripts disguised as legitimate files.	T1566.001
Initial Access	Malicious Downloads	Fake software installers and phishing links used for malware delivery.	T1189
Execution	Execution via PowerShell	PowerShell scripts executed to manipulate system settings and execute payloads.	T1059.001
Execution	Execution Policy Bypass	PowerShell execution policy bypassed to allow unrestricted script execution.	T1548.002
Persistence & Evasion	Hiding in Recycle Bin	Creates hidden files in C:$Recycle.Bin to evade detection.	T1564.001
Persistence & Evasion	Disabling Windows Defender	Uses PowerShell to disable real-time monitoring and tamper with security settings.	T1562.001

Indicators of Compromise (IOCs)

File Hashes

- MD5: e099255ea4aa8eb41e26e5d94737fc26
- SHA1: 2c13d842e788e6c981b2fae65834b1220d55f5a8
- SHA256: 89b9f7499d59d0d308f5ad02cd6fddd55b368190c37f6c5413c4cfcd343eeff3

Malicious Filenames

setup-avast-premium-x64.exe
ZipThis.exe
document pdf.exe
fiyati_teklif 615TBI507_ ON-SAN Vakum san tic_ Sipari#U015fi jpeg docx.exe
anrek.mp4.hta
title.mp4.hta
Agent381.msi
Setup.exe
yxU3AgeVTi.exe

Malicious URLs

https://report-scam.malwarebouncer.com/XcUR2TnV2VTlXT0s0Z0NYa01KSGt3dUtWMWNiblBrc29mMlpZUU1WdThBSjdDdTlRQTVDV1ZZd0pDeWRmUU5rQ1QvVDNiSlBNYWd2bTd0eTRkZW5jT0hrYTBKWHFiVUc4TVZBOGpiNkh4VG9OTm9zNTVUWHNmNWVydHpqbzhlc1llSzdzTHZ0dENVNWRLZy9BbCsyVDRMSGRHOThUWnV5QUxPU0RZL1dPalNYTmUzMTVoRzI5bmk1ZVZRPT0tLUdVYnJkMC9GazI3MWlxYmotLUpFOURyOWkzK1I6Vy9BYTVOVDBVNkE9PQ==?cid=2346401253

---

https://pwv95gp5r-xn--r3h9jdud-xn----c1a2cj-xn----p1ai.translate.goog/sIQKSvTC/b8KvU/uoTt6?ZFhObGNpNXBiblp2YkhabGJXVnVkRUJ6YjNWMGFHVnliblJ5ZFhOMExtaHpZMjVwTG01bGRBPT06c1JsOUE+&_x_tr_sch=http&_x_tr_sl=hrLWHGLm&_x_tr_tl=bTtllyql

---

https://covid19.protected-forms.com/XQTNkY0hwMkttOEdiZmZ0V2RRTHpDdDNqUTROanhES0NBYmdFOG1KTGRSTUtrK3VMMzlEN1JKVVFXNUxaNGJOQmd1YzQ3ajJMeVdZUDU3TytRbGtlaFhWRkxnT0lkeTZhdy9xWEhjeFBoRXRTb2hxdjlVbi9iSk1qZytLQ0JxRjd4UmpOS3VUQ2lpOEZneTRoVmpzY2dyekR1WlhYOWVteVcrUXg0a2Y2aEU2ZEZwMVNId3R0U01RK3N3PT0tLVR0bDl1WEFUelg3K2VzTystLUxaMkFrZnU0UmJXRkR3aE5NRE9BOEE9PQ==?cid=2351432832

---

https://employeeportal.net-login.com/XL0pFWEloTnBYUmM5TnBUSmVpbWxiSUpWb3BBL1lPY1hwYU5uYktNWkd5ME82bWJMcUhoRklFUWJiVmFOUi9uUS81dGZ4dnJZYkltK2NMZG5BV1pmbFhqMXNZcm1QeXBXTXI4R090NHo5NWhuL2I4TXdxNlY4VlZxWHVPNTdnc1M3aU4xWjhFTmJiTEJWVUYydWVqZjNPbnFkM3M5T0FNQ2lRL3EySjhvdVVDNzZ2UHJQb0xQdlhZbTZRPT0tLTJaT0Z2TlJ3S0NMTTZjc2ktLTZGNUlwRnVkbFRTTHR2dUFITkcxVFE9PQ==?cid=2341891188

---

https://gmail.net-login.com/Xb1Rnb3pKRC9CUEdpbldIVTREbHhIK1Vza1NvaWlrblBlbkN4aUdCZUt0Y2NlSGJiWmZ2d0M1dTB5dEpRbnRoVDdBVkFTcEJqWGowNVZycWJNWHlIUHlLOG1qS0FvemVPSXpFRFhGcUhmaVU1ekQwMklrVmM0QjVpNmhLaDdoY1I4UlhMcFo1TTJaSFhtaWpiWWFqWGZ5WEg4TnBiOUl4MDI1RFMyWStQRFoyNFo5UFZNUUpmWXBtaUg0Y0FjUG1jejdSVnFVOXJQL2VzdmNLM1lEaWtmRkZnZEk2Vi0tVHFIeU0vOWxTN01YVEtXbS0tTTh5Skh1eEtsc0xTT0J5Rzg2Q2ZJQT09?cid=2330416057%3EOpen

---

https://en.newsnowbangla.com/archives/69912

---

https://mail.donotreply.biz/XWW04VVZpU2JyWTFmVy96T2RUOUEvcEhyMWhFSm5uZElnVUlmb2dTZEdMRFdGSU1UV2V3S3RUNGdrNmNQRFJ4WTFPRHdYYlkraDV3S1YyVVpuU3E3K2p1bWowcEt3M24ySVBLanRDUkwyYitYWExuYTB5YlhVTUhySWZKbGJCTE9oRHl2RCtjR29BbEk3ZEwxZFJaNmNoK29ESk0vTGcxSmtyK0FWTExLWTdxYlQ1Yys1bjNiTUczY0RnPT0tLTU2R0pFM1VwZFRnVndZSWktLXptU2lWOHlQdjR0eGI1K09OQVZtRnc9PQ==?cid=2315575162

---

https://mail.donotreply.biz/XWW04VVZpU2JyWTFmVy96T2RUOUEvcEhyMWhFSm5uZElnVUlmb2dTZEdMRFdGSU1UV2V3S3RUNGdrNmNQRFJ4WTFPRHdYYlkraDV3S1YyVVpuU3E3K2p1bWowcEt3M24ySVBLanRDUkwyYitYWExuYTB5YlhVTUhySWZKbGJCTE9oRHl2RCtjR29BbEk3ZEwxZFJaNmNoK29ESk0vTGcxSmtyK0FWTExLWTdxYlQ1Yys1bjNiTUczY0RnPT0tLTU2R0pFM1VwZFRnVndZSWktLXptU2lWOHlQdjR0eGI1K09OQVZtRnc9PQ==?cid=2315575162

IP

199.232.192.193 (Fastly CDN - potential C2 communication)

Mitigations:

Email & Web Filtering

- Implement Email Filtering (M1031) to block phishing emails and malicious attachments.
- Use Web Content Filtering (M1035) to prevent access to known malicious sites.

Execution Prevention & PowerShell Security

- Enforce Execution Prevention (M1038) to block unauthorised script execution.
- Enable PowerShell Logging (M1045) and PowerShell Constrained Language Mode to monitor suspicious activity.

User Access & System Hardening

- Use User Account Control (M1052) to limit administrative privileges.
- Apply Application Control (M1038) to restrict execution of unauthorised applications.

File & Directory Security

- Set File and Directory Permissions (M1022) to prevent unauthorised modifications.
- Regularly Monitor the Recycle Bin for hidden malware artifacts.

Endpoint Protection & Network Security

- Deploy Antivirus/Endpoint Protection (M1049) to detect and block malware.
- Use Network Segmentation (M1030) to prevent ransomware from spreading across systems.

Data Protection & Integrity Monitoring

- Maintain Regular Data Backups (M1053) to restore lost files without paying ransom.
- Implement File Integrity Monitoring (M1044) and Endpoint Detection & Response (M1040) to detect unauthorised file changes.

Ransomware Victims Worldwide

A recent ransomware analysis reveals that the United States remains the most heavily impacted nation, accounting for a staggering 64.75% of global incidents, highlighting its continued vulnerability to ransomware threats. Following this, Canada reported 6.9% of the attacks, emerging as another highly targeted region.

The United Kingdom and Australia also faced considerable exposure, reporting 3.83% of ransomware incidents each. India experienced 2.68% of attacks, indicating an ongoing risk in the region. Meanwhile, Germany recorded 2.3% of global ransomware cases, followed by Sweden and Mexico at 1.15% each.

Several other nations exhibited moderate levels of ransomware incidents, including Japan at 1.53%, Italy, France, Romania, Taiwan, and Poland each reporting 0.77% of global ransomware cases. Additionally, Israel, the Philippines, Ukraine, Greece, Ireland, Portugal, Zambia, Morocco, South Africa, Chile, the Netherlands, New Zealand, Indonesia, Malaysia, Belarus, Brazil, Saudi Arabia, and Kenya each reported 0.38% of global ransomware incidents.

This analysis underscores the persistent and widespread nature of ransomware attacks, with North America facing particularly high levels of risk. These findings highlight the critical need for robust cybersecurity measures, proactive defence strategies, and heightened vigilance across all sectors to counteract the increasing ransomware threat worldwide.

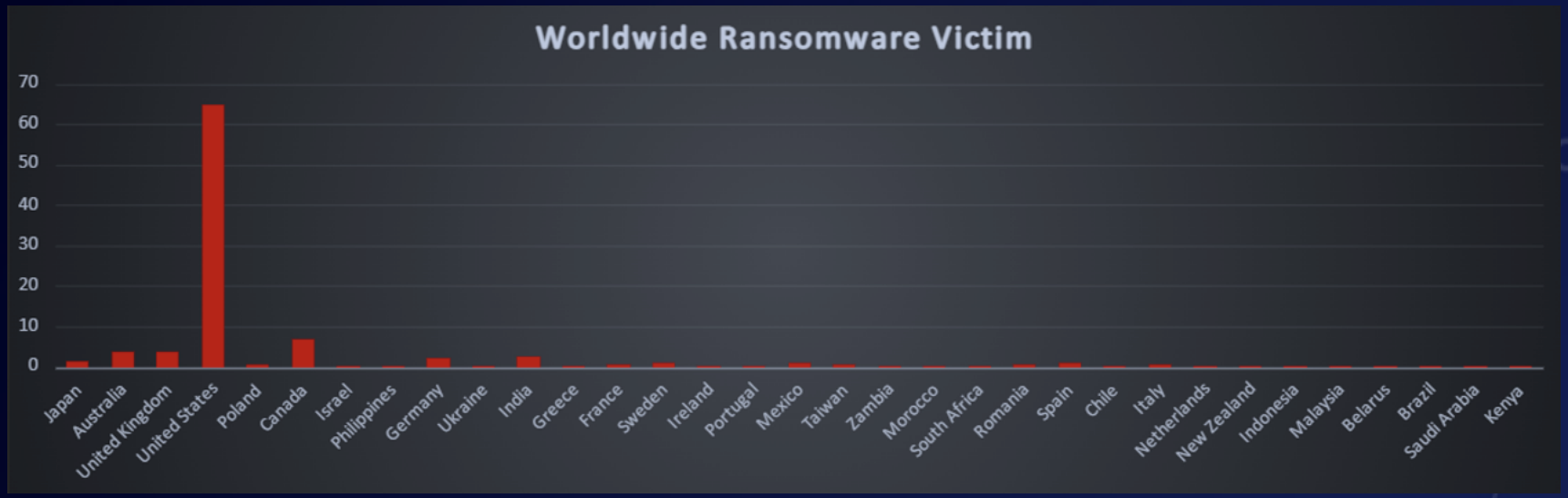


Figure 5: Ransomware Victims Worldwide

Ransomware Victims by Industry

A recent ransomware analysis highlights the Manufacturing sector as the most targeted industry, accounting for 21.84% of total reported incidents. This underscores the persistent threats faced by production processes and supply chain operations.

Following this, the Retail sector reported 15.33% of attacks, emphasising the heightened risk to consumer-facing businesses. Business Services also faced significant exposure, recording 11.49% of incidents. The Transportation sector saw a notable impact, accounting for 7.66% of ransomware incidents.

Other heavily affected industries include Construction at 6.13% and IT and Telecommunications, each reporting 4.21%, reflecting ongoing security challenges in infrastructure development and technology services. Education also recorded 4.21% of attacks, followed by Consumer Services and Finance, each at 3.83%, and Healthcare at 3.07%, highlighting vulnerabilities in sectors handling sensitive data.

Meanwhile, Real Estate and Law Firms each accounted for 2.3% of reported ransomware incidents. The Hospitality industry faced 3.83%, indicating cybercriminals' focus on service-oriented businesses. Federal institutions and Organisations each recorded 1.15%, while Energy and Media & Internet sectors saw 0.77% of attacks. Insurance also faced 0.77% of incidents, underscoring the diverse impact of ransomware across industries.

Lower, yet notable, shares of ransomware activity were recorded in Agriculture (1.15%), showcasing the widespread reach of ransomware across sectors.

This analysis reinforces the indiscriminate nature of ransomware threats, impacting industries across critical infrastructure, public services, and commercial enterprises. The findings highlight the urgent need for sector-specific cybersecurity strategies, robust defences, and proactive risk management to mitigate the evolving ransomware landscape.

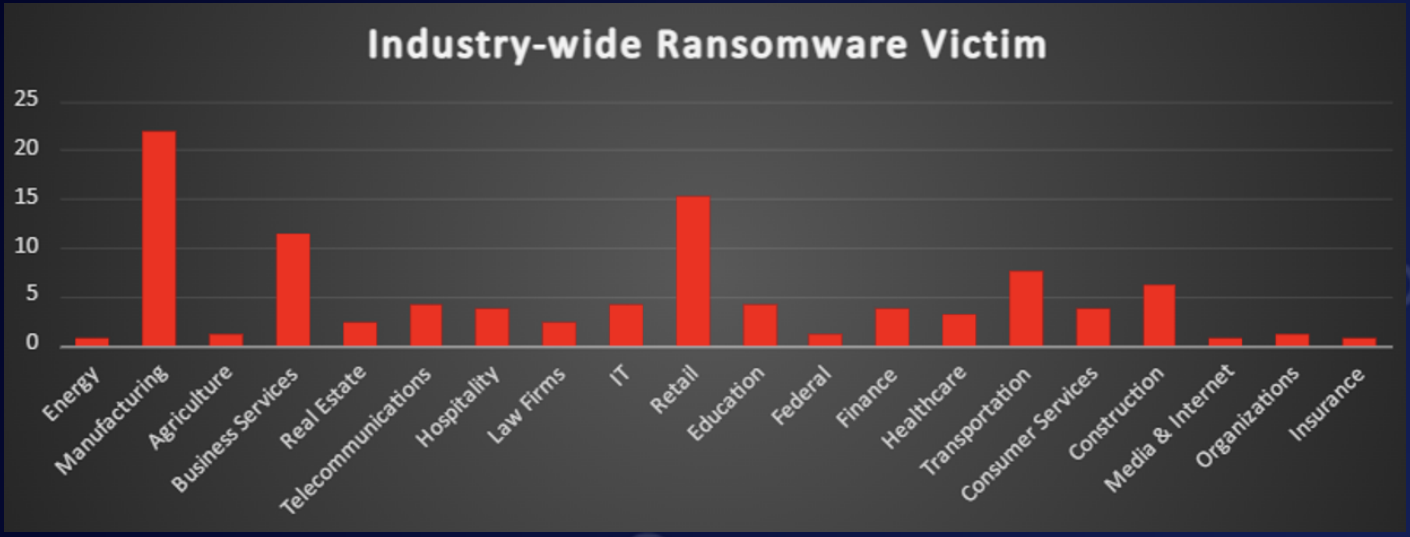


Figure 6: Industry-wide Ransomware Victims