Red Piranha
unified threat management

THREAT INTELLIGENCE REPORT

Mar 25 - 31, 2025

Report Summary:

- **New Threat Detection Added** – 5
  - Arechclient2
  - SocGholish
  - Specter Insight
  - Lumma Stealer
  - SvcStealer

- **New Threat Protections - 159**

The following threats were added to Crystal Eye this week:

1. Arechclient2

Arechclient2 is a .NET RAT reported to have numerous capabilities including multiple stealth functions. We observed the acquired malicious executable profiling victim systems, stealing information such as browser and crypto-wallet data, and launching a hidden secondary desktop to control browser sessions, which aligns closely with reports from others such as the Center for Internet Security (CIS).

Threat Protected: 01
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	Description
Initial Access	T1204.002 – User Execution (Malicious File)	Victim runs a malicious executable disguised as a legitimate file.
	T1566.001 – Spearphishing Attachment	Often delivered via phishing emails with infected attachments.
Execution	T1059.005 – .NET Execution	Runs as a .NET binary, sometimes unpacked in memory.
Persistence	T1547.001 – Registry Run Keys	Adds itself to registry to auto-start on reboot.
Defence Evasion	T1027 – Obfuscation	Uses obfuscation and anti-VM checks to avoid detection.
Credential Access	T1555.003 – Steal Browser Credentials	Extracts saved passwords from browsers.
Discovery	T1082 – System Information Discovery	Collects system details like OS, hardware, and software.
Collection	T1113 – Screen Capture	Takes screenshots to monitor user activity.
	T1056.001 – Keylogging	Logs keystrokes silently.
Command-and-Control	T1071.001 – C2 over HTTPS	Communicates with the attacker's server via encrypted web traffic.
Impact	T1490 – Inhibit System Recovery	Can be used to delete recovery data if other malware is deployed.

2. SocGholish Malware

SocGholish, also known as FakeUpdates, is a JavaScript-based malware framework primarily used for initial access in sophisticated cyberattacks. It's heavily used by cybercriminals (especially initial access brokers) to compromise corporate environments

Threat Protected: 15
Rule Set Type:

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

Class Type: Exploit Kit

SocGholish is a social engineering-based malware that:

- Disguises itself as fake browser or software updates, hence the alias "FakeUpdates."
- Is delivered through compromised websites, often legitimate ones.
- Deploys JavaScript to infect the system, typically without downloading a visible file.
- Is used to load additional malware payloads (like Cobalt Strike, remote access trojans, or ransomware).

Initial Access (via SEO poisoning or compromised websites)

- Victim visits a compromised legitimate website (often via search engine).
- The site shows a pop-up saying something like "Your browser is out of date. Please update."
- The update link actually downloads a malicious JavaScript.

Execution

- The JavaScript runs in memory or drops a loader, which may connect to a command-and-control (C2) server.
- Attackers can then deliver follow-on payloads (remote shells, info stealers, ransomware, etc.).

Post-exploitation

- Tools like Cobalt Strike, RATs, or even ransomware like Clop or BlackCat have been seen as next-stage payloads.
- In some cases, SocGholish is used in access-as-a-service models to sell access to ransomware groups.

Tactic	Technique	Description
Initial Access	[T1189] Drive-by Compromise	Compromised websites serve fake browser updates to trick users into downloading JavaScript payloads.
	[T1190] Exploit Public-Facing Application	Sometimes uses known vulnerable WordPress plugins to compromise websites.
	[T1566.002] Spearphishing Link	Occasionally delivered via links in emails or search-engine optimised (SEO) results.
Execution	[T1059.007] JavaScript	Malicious JavaScript is executed after download under the guise of a browser update.
	[T1204.002] User Execution: Malicious File	Relies heavily on user interaction (downloading and running fake updates).
Persistence	[T1547.001] Registry Run Keys/Startup Folder	May establish persistence by modifying registry keys for startup.
Privilege Escalation	[T1055] Process Injection	Injects malicious code into legitimate processes (if additional payloads like Cobalt Strike are used).
Defence Evasion	[T1027] Obfuscated Files or Information	Uses heavily obfuscated JavaScript to avoid detection.
	[T1140] Deobfuscate/Decode Files or Info	Payloads deobfuscate on execution in memory.
Command-and-Control	[T1071.001] Application Layer Protocol: Web	C2 communication via HTTP(S) using fake domains.
	[T1105] Ingress Tool Transfer	Downloads additional payloads like remote access tools or ransomware.
Credential Access	[T1003.001] LSASS Memory	(If chained with tools like Cobalt Strike) can dump credentials from memory.
Discovery	[T1082] System Information Discovery	Post-compromise tools may gather system info.
Lateral Movement	[T1021.002] SMB/Windows Admin Shares	If additional malware is delivered, may move laterally in the network.
Impact	[T1486] Data Encrypted for Impact	Final stage may involve ransomware deployment (REvil, Clop, etc.).

3. Specter Insight

Specter Insight C2 is a sophisticated, cross-platform command-and-control (C2) framework designed for red team engagements, threat emulation, and training. It integrates seamlessly with existing infrastructure, making detection challenging for security systems. The framework supports multiple listeners and protocols, manages implants, and facilitates data exfiltration. Its adaptability enhances the effectiveness of hacking campaigns, particularly those employing tactics like ClickFix to exploit software vulnerabilities or user behaviour.

Threat Protected: 01
Rule Set Type:

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

Class Type: Exploit Kit
Initial Access:

- T1566.001 – Spearphishing Attachment: Attackers send emails with malicious attachments to deliver the Specter Insight C2 implant.
- T1190 – Exploit Public-Facing Application: Utilising tactics like ClickFix, attackers exploit vulnerabilities in software configurations to gain unauthorised access. GBHackers Security

Execution:

- T1059.005 – Command and Scripting Interpreter: Visual Basic: The implant executes scripts to establish communication with the C2 server. Practical Security Analytics LLC

Persistence:

- T1547.001 – Registry Run Keys / Startup Folder: Modifies registry keys or startup folders to maintain persistence across system reboots.

Privilege Escalation:

- T1055 – Process Injection: Injects malicious code into legitimate processes to escalate privileges.

Defence Evasion:

- T1027 – Obfuscated Files or Information: Employs obfuscation techniques to evade detection by security tools.

Credential Access:

- T1555 – Credentials from Password Stores: Harvests credentials stored in browsers and other applications.

Discovery:

- T1082 – System Information Discovery: Gathers detailed information about the infected system's hardware and software.

Lateral Movement:

- T1021.001 – Remote Desktop Protocol: Utilises RDP to move laterally within the network.

Collection:

- T1113 – Screen Capture: Captures screenshots of the user's desktop to gather intelligence.

Tactic	Technique	Description
Initial Access	T1566.001 – Spearphishing Attachment T1190 – Exploit Public-Facing Application	Delivers malicious implants via phishing emails with attachments. Leverages software misconfigurations (e.g., ClickFix) to gain access.
Execution	T1059.005 – Command and Scripting Interpreter: VB	Executes scripts to initiate implant communication.
Persistence	T1547.001 – Registry Run Keys / Startup Folder	Adds registry entries or startup scripts to persist across reboots.
Privilege Escalation Defence Evasion	T1055 – Process Injection T1027 – Obfuscated Files or Information	Injects code into legitimate processes to escalate privileges. Uses obfuscated code and file structures to evade detection.
Credential Access	T1555 – Credentials from Password Stores	Extracts saved credentials from browsers and password managers.
Discovery	T1082 – System Information Discovery	Collects host, OS, and software information.
Lateral Movement Collection	T1021.001 – Remote Desktop Protocol (RDP) T1113 – Screen Capture	Moves laterally using RDP within the internal network. Takes screenshots from victim machines.
Command-and-Control	T1071.001 – Application Layer Protocol: Web	Maintains C2 via HTTP/S communications.
Exfiltration	T1041 – Exfiltration Over C2 Channel	Exfiltrates stolen data over the same channel used for C2.
Impact	T1489 – Service Stop	Terminates system services to degrade system defences.

3. Lumma Stealer

Lumma Stealer (also known as LummaC2) is a high-speed, modular information-stealing malware sold on underground forums as Malware-as-a-Service (MaaS). It is known for exfiltrating credentials, session cookies, crypto wallet data, and system information. Written in C, it is highly obfuscated and often delivered via phishing or malicious advertising (malvertising). Lumma uses a custom C2 infrastructure and is regularly updated to evade detection.

Threat Protected: 39
Rule Set Type:

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

Class Type: domain-c2
Initial Access:
- T1566.002 – Spearphishing Link: Delivered via phishing emails containing links to malicious downloads.
- T1189 – Drive-by Compromise: Victims are redirected through malicious ads or compromised websites to download the stealer.

Execution:
- T1204.002 – User Execution: Malicious File: Victims manually execute a disguised Lumma payload, often packed in a ZIP or disguised as a legitimate installer.

Persistence:
- T1547.001 – Registry Run Keys/Startup Folder: Modifies registry keys or startup folders to maintain persistence across system reboots.
- T1053.005 – Scheduled Task: Creates scheduled tasks to ensure malware re-executes after a reboot.

Privilege Escalation:
- T1055 – Process Injection: Injects malicious code into legitimate processes to escalate privileges and evade detection.

Defence Evasion:
- T1027 – Obfuscated Files or Information: Uses code obfuscation and string encryption to hide functionality from antivirus tools.
- T1497 – Virtualisation/Sandbox Evasion: Checks for virtual environments to avoid analysis and evade detection.

Credential Access:
- T1555.003 – Credentials from Web Browsers: Extracts saved credentials from Chrome, Firefox, and Edge.
- T1555.004 – Credentials from Password Managers: Attempts to steal login data from locally stored password manager vaults.

Discovery:
- T1082 – System Information Discovery: Gathers host information including OS version, architecture, and installed software.

Collection:
- T1113 – Screen Capture: Takes screenshots of the desktop or browser activity.
- T1552.001 – Steal Encrypted Wallets: Extracts local crypto wallet data like MetaMask and Electrum.

- T1512 – Credentials from Web Cookies: Steals session cookies to enable account hijacking.
- T1560.001 – Archive Collected Data: Compresses and prepares stolen data for exfiltration.

Command-and-Control:

- T1071.001 – Application Layer Protocol: HTTPS: Communicates with remote attacker-controlled servers using encrypted HTTP/S.
- Custom Protocol: Uses a proprietary C2 protocol in some versions for stealth and reliability.

Exfiltration:

- T1041 – Exfiltration Over C2 Channel: Sends stolen data over the same encrypted communication channel used for C2.

Tactic	**Technique**	**Description**
Initial Access	T1566.002 – Spearphishing via Link	Victims lured through phishing links or fake installers.
	T1189 – Drive-by Compromise	Delivered through fake software or ads (malvertising).
Execution	T1204.002 – User Execution: Malicious File	User manually runs the downloaded Lumma executable.
Persistence	T1547.001 – Registry Run Keys / Startup Folder	Ensures the stealer runs on system startup.
	T1053.005 – Scheduled Task	Uses scheduled tasks to maintain persistence.
Defence Evasion	T1027 – Obfuscation	Highly obfuscated payloads to evade AVs.
	T1497 – Virtualisation/Sandbox Evasion	Checks for analysis environments before executing.
Credential Access	T1555.003 – Steal Browser Credentials	Steals saved login credentials from Chrome, Edge, Firefox.
	T1555.004 – Credentials from Password Managers	Targets password managers and browser vaults.

5. SvcStealer

SvcStealer is a stealthy information-stealing malware designed to exfiltrate browser credentials, Discord tokens, and system information from infected machines. It is often distributed via malicious executables disguised as cracked software or utility tools, primarily targeting Windows systems. Known for its lightweight structure and simple C2 communication, SvcStealer is typically used in low-sophistication, high-volume campaigns.

Threat Protected: 02
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:
Initial Access:
- T1204.002 – User Execution: Malicious File: Delivered as a disguised EXE, often bundled with cracked software or shared on forums.

Execution:
- T1059.003 – Command and Scripting Interpreter: Windows Command Shell: Executes commands and initiates malicious activity using PowerShell or batch scripts.

Persistence:
- T1547.001 – Registry Run Keys/Startup Folder: Writes itself to the startup folder or adds a registry entry to persist across reboots.

Defence Evasion:
- T1027 – Obfuscated Files or Information: The binary is packed or obfuscated to evade antivirus detection.

Credential Access:
- T1555.003 – Credentials from Web Browsers: Steals login credentials stored in Chromium-based browsers.
- T1555.005 – Steal Application Access Tokens: Extracts Discord tokens for account hijacking.

Discovery:
- T1082 – System Information Discovery: Gathers basic system info such as hostname, OS, CPU, and user account data.

Collection:
- T1113 – Screen Capture (variant-dependent): Some versions may capture screenshots to gather additional visual intel.
- T1560.001 – Archive Collected Data: Archives all harvested data before exfiltration.

Command-and-Control:
- T1071.001 – Application Layer Protocol: HTTPS: Sends exfiltrated data over HTTP or HTTPS to a hardcoded C2 URL.

Exfiltration:
- T1041 – Exfiltration Over C2 Channel: Transmits stolen data directly through the established C2 link.

Tactic	Technique	Description
Initial Access	T1204.002 – User Execution: Malicious File	SvcStealer is commonly distributed as an EXE file disguised as cracked software or cheat tools. Users are tricked into executing it manually.
Execution	T1059.003 – Command and Scripting Interpreter: Cmd/Powershell	Executes via Windows Command Shell or PowerShell, depending on how it's deployed or if it's dropped by another loader.
Persistence	T1547.001 – Registry Run Keys / Startup Folder	Adds itself to the Windows startup folder or creates registry keys (e.g., HKCU\Software\Microsoft\Windows\CurrentVersion\Run) to auto-start on boot.
Privilege Escalation	T1027 – Obfuscated Files or Information	Uses simple obfuscation or packing to evade static analysis and antivirus detection. May also use uncommon file names to avoid suspicion.
Defence Evasion	T1555.003 – Credentials from Web Browsers	Extracts saved login credentials from Chromium-based browsers like Chrome, Brave, and Edge.
Credential Access	T1555.005 – Steal Application Access Tokens	Steals Discord authentication tokens directly from local storage to hijack user sessions.
	T1082 – System Information Discovery	Gathers host details including hostname, OS version, user name, and sometimes hardware info to profile victims.
Discovery	T1113 – Screen Capture (variant-dependent)	Some builds include functionality to capture the screen, helping attackers observe victim activity.
	T1560.001 – Archive Collected Data	Collected credentials and system info are zipped before transmission to the attacker's C2 server.

Known exploited vulnerabilities (Week 4 March 2025):

Vulnerability	CVSS	Description
CVE-2024-20439	9.8 (High)	Cisco Smart Licensing Utility contains a static credential vulnerability that allows an unauthenticated, remote attacker to log in to an affected system and gain administrative credentials.
CVE-2025-2783	8.4 (High)	Google Chromium Mojo on Windows contains a sandbox escape vulnerability caused by a logic error, which results from an incorrect handle being provided in unspecified circumstances
CVE-2019-9874	7.5 (High)	Sitecore CMS and Experience Platform (XP) Deserialisation Vulnerability
CVE-2019-9875	8.6 (High)	Sitecore CMS and Experience Platform (XP) Deserialisation Vulnerability
CVE-2025-30154	9.3 (Critical)	reviewdog/action-setup GitHub Action Embedded Malicious Code Vulnerability

Updated Malware Signatures (Week 4 March 2025)

Threat	Description
zgRAT	This threat is a classic remote access trojan that allows its operator to gain remote control of a compromised machine, perform keylogging, steal sensitive data, and also upload/execute other threats. Note zgRAT is also capable of spreading via USB drives
ClipBanker	Trojan.ClipBanker is Malwarebytes' detection name for a type of Trojan that tries to steal currencies from the affected system by stealing or manipulating the data on the Windows clipboard.
XWorm	XWorm is a relatively new versatile tool that was discovered in 2022. It enables attackers to carry out a variety of functions, which include a ccessing sensitive information, gaining remote access, and deploying additional malware.

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
Bianlian	0.67%
Play	3.36%
Cicada3301	1.34%
KillSec3	2.68%
SafePay	1.34%
Babuk-Bjorka	11.41%
Interlock	1.34%
Inc ransom	3.36%
Lynx	4.03%
CrazyHunter Team	0.67%
Qilin	6.04%
Frag	18.12%
Medusa	2.68%
RansomHub	17.45%
Hellcat	1.34%
NightSpire	4.03%
LockBit3	2.01%
Akira	0.67%
Arkana Security	1.34%
Rhysida	1.34%
Zerolockersec	1.34%
Ransomware blog	0.67%
Ralord	3.36%
Everest	0.67%
Sarcoma	4.7%
VanHelsing	0.67%
RansomHouse	0.67%
Abyss-Data	0.67%
Stormous	0.67%
Leaked Data	0.67%

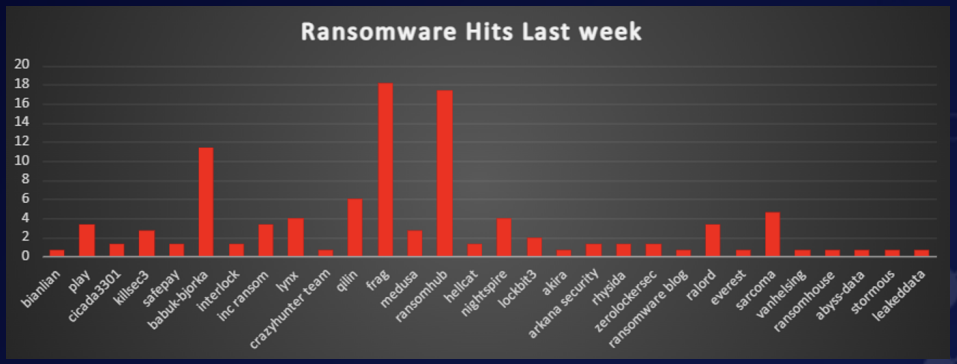

Figure 1: Ransomware Group Hits Last Week

Latrodectus Ransomware

Latrodectus is a sophisticated Windows-based malware loader first identified in October 2023. Designed to infiltrate systems stealthily, it facilitates the deployment of additional malicious payloads, including ransomware, remote access trojans, and information stealers. Its advanced evasion techniques and ability to execute code within legitimate process memory make it particularly dangerous, enabling activities such as data theft, remote system control, and disruption of critical operations. By masquerading legitimate files and employing complex obfuscation methods, Latrodectus poses a significant threat to the cybersecurity of both individuals and organisations.

Detailed Tactics, Techniques, and Procedures (TTPs):

- Initial Access and Execution:
  - Latrodectus is primarily distributed through phishing emails containing malicious attachments or links. These emails often masquerade as legitimate communications, enticing recipients to open attachments or click on links that initiate the infection chain.
- Defence Evasion:
  - The malware employs various techniques to evade detection, including:
    - Debugger Evasion (T1622): Detects the presence of debugging tools to thwart analysis.
    - Deobfuscation/Decode Files or Information (T1140): Deobfuscates encrypted strings to conceal its true functionality.
- Persistence Mechanisms:
  - Latrodectus establishes persistence through:
    - Boot or Logon Autostart Execution via Registry Run Keys/Startup Folder (T1547.001): Modifies registry keys to ensure execution upon system startup.
    - Scheduled Tasks (T1053.005): Creates tasks to execute malicious payloads at specified intervals.
- Command-and-Control (C2) Communication:
  - Utilises standard application layer protocols for C2 communication, including:
    - Application Layer Protocol: Web Protocols (T1071.001): Sends registration information to C2 servers via HTTP POST requests.
    - Data Encoding: Standard Encoding (T1132.001): Employs Base64 encoding for data transmitted to C2 servers.
- Discovery and Information Gathering:
  - Conducts various discovery activities to gather system information:
    - Account Discovery: Domain Account (T1087.002): Identifies domain administrator accounts by executing commands like net group "Domain Admins" /domain.
    - System Information Discovery (T1082): Collects data on system configurations and settings.
- Impact:
  - Capable of downloading and executing additional payloads, leading to:
    - Data Encrypted for Impact (T1486): Facilitates ransomware deployment to encrypt critical data.
    - Inhibit System Recovery (T1490): Disables system recovery features to prevent restoration of encrypted files.

Indicators of Compromise (IOCs):
File Hashes (MD5):

- 0a2b923be8aefb8e3cd0d2787183ef35
- 1f4f7c5154d73bbcfb88dbfd0a7b131c
- 1fd0fffa9b17a3351ed277c1cae23305
- 24740f0f2d658a5d863e93ab33029a41
- 2a14c25eff6022168936b847354335cf
- 2ec5ce52d41c58ec86bd6448c557d298
- 3b67ecc2f2ade1f1865aa384ed8de227
- 47aff6fc736afa4f4d677a776fcad230
- 51a202e07a388762720ff5d21da7996c
- 524a8891a7df50aa9ced2da9ef379929

Mitigation Strategies:

- Email Security:
  - Advanced Filtering: Implement sophisticated email filtering solutions to detect and block phishing emails containing malicious attachments or links.
  - User Awareness Training: Educate employees on recognising phishing attempts and the dangers of interacting with unsolicited attachments or links.
- Endpoint Protection:
  - Antivirus and Anti-malware: Deploy robust endpoint detection and response (EDR) solutions to identify and mitigate malicious activities associated with Latrodectus. Regularly update antivirus definitions to detect and remove known Latrodectus variants.
  - Application Control: Restrict the execution of unauthorised applications and scripts to prevent malware installation.
- Network Security:
  - Traffic Monitoring: Monitor network traffic for signs of command-and-control (C2) communication, particularly unusual HTTP POST requests or Base64-encoded data transmissions.
  - Intrusion Detection and Prevention Systems (IDPS): Implement IDPS to block known indicators of compromise (IOCs) and suspicious activities.
- System Hardening:
  - Regular Patching: Keep operating systems and applications up to date with the latest security patches to mitigate vulnerabilities exploited by Latrodectus.
  - Access Controls: Enforce the principle of least privilege, ensuring users have only the access necessary for their roles.
- Backup and Recovery:
  - Regular Backups: Conduct regular backups of critical data and ensure backups are stored securely and are not accessible from the main network.
  - Recovery Planning: Develop and regularly update incident response and disaster recovery plans to quickly address infections and restore operations.

By implementing these strategies, organisations can enhance their defences against Latrodectus and similar malware threats.

Ransomware Victims Worldwide

A recent ransomware analysis reveals that the United States continues to be the most heavily impacted nation, accounting for a staggering 56.38% of global incidents. This underscores the ongoing vulnerability of US-based entities across various sectors to sophisticated ransomware threats.

Canada follows as the second-most affected country, reporting 5.37% of incidents, while France accounts for 4.70%, highlighting growing ransomware risks across North America and Western Europe. The United Kingdom (3.36%), India (2.01%), Australia (2.01%), and Japan (2.01%) also reported notable incident volumes, reflecting a broadening global threat footprint.

Other nations with a moderate percentage of ransomware incidents include Spain (2.01%), Italy (2.01%), Turkey (2.01%), Germany (2.01%), and Brazil (1.34%). Countries such as Pakistan, Argentina, Colombia, China, Thailand, Mexico, Hungary, and Iraq each reported between 0.67% and 1.34% of global cases.

Additional countries impacted include Netherlands, Singapore, Slovakia, Chile, Korea, Egypt, Morocco, Malaysia, Israel, Dominican Republic, Sweden, and Antigua and Barbuda, each contributing 0.67% of global ransomware cases.

This analysis underscores the increasingly global nature of ransomware attacks, with a continued focus on North America, Europe, and Asia. The findings emphasise the urgent need for proactive cybersecurity defences, cross-border threat intelligence sharing, and resilient recovery planning to mitigate these growing threats.

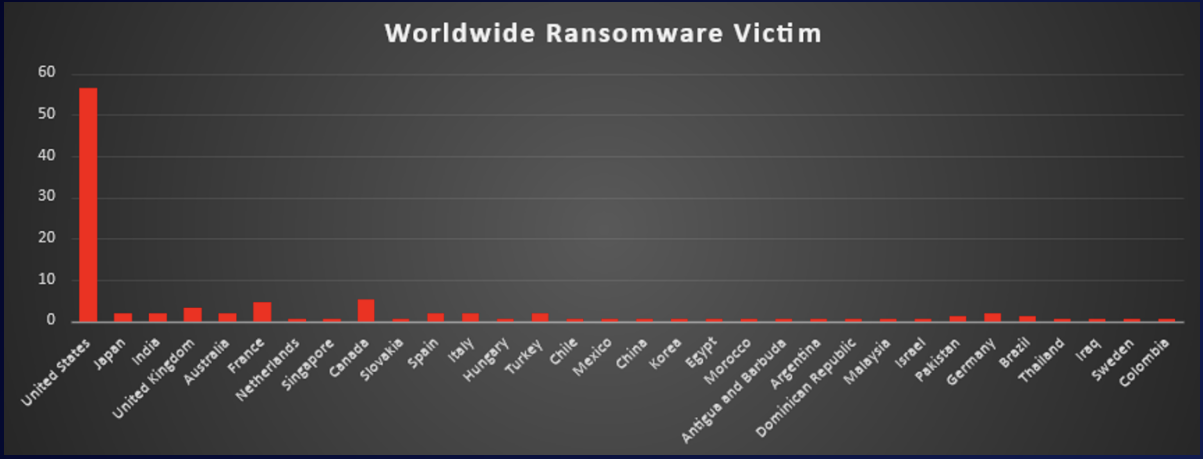

Figure 2: Ransomware Victims Worldwide

Ransomware Victims by Industry

In the most recent industry-specific analysis of ransomware incidents, the Manufacturing sector once again emerged as the top target, accounting for 13.42% of global attacks. This highlights persistent vulnerabilities in industrial networks, production systems, and supply chain ecosystems.

Business Services followed closely at 12.08%, indicating the high risk to service-oriented and consulting sectors. The Construction industry reported 9.40% of incidents, underscoring continued exposure among infrastructure and development firms.

Other significantly affected industries include Retail (8.05%), Healthcare (6.04%), and Education (6.04%), illustrating the risks to sectors dealing with sensitive consumer, patient, and student data. Transportation, Finance, and Organisations each reported 4.70% of total ransomware incidents, while Hospitality accounted for 4.03%, reflecting cybercriminals' focus on public-facing services and essential logistics.

Sectors like Law Firms (3.36%), Federal (3.36%), Energy (3.36%), and Real Estate (2.68%) also experienced notable targeting, showing attackers' interests in sensitive legal, operational, and strategic data.

Emerging trends show ransomware also targeting IT (2.01%), Telecommunications (2.01%), and Minerals & Mining (2.01%). Industries like Electronics, Consumer Services, Agriculture, and Insurance each saw 1.34% or less, indicating that no vertical is immune.

This analysis confirms that ransomware remains an indiscriminate threat, affecting both critical infrastructure and private enterprises. It highlights the urgent need for industry-specific threat modeling, enhanced detection frameworks, and resilience strategies to counteract ransomware's evolving tactics.

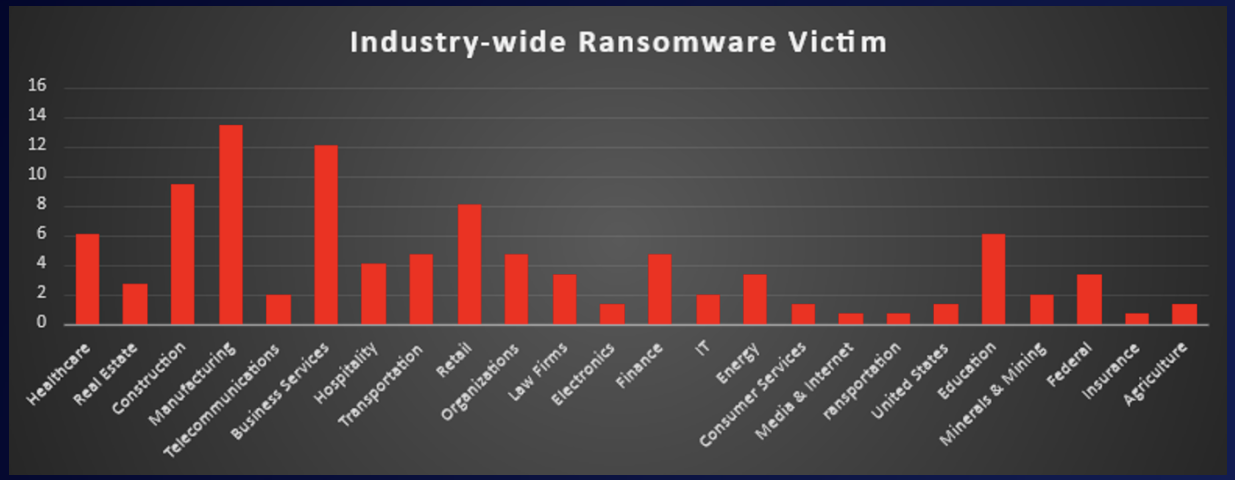

Figure 3: Industry-wide Ransomware Victims