THREAT INTELLIGENCE REPORT

February 17 - 23, 2026

Red Piranha
unified threat management

Report Summary:

New Threat Detection Added

- TrustConnect
- MoonRise

Detection Summary

- New Threat Protection: 183
- Newly Detected Threats: 139

The following threats were added to Crystal Eye this week:

1. TrustConnect

TrustConnect is a Malware-as-a-Service (MaaS) platform discovered in early 2026 that operates as a Remote Access Trojan (RAT) masquerading as a legitimate Remote Monitoring Management (RMM) tool, allowing threat actors to gain unauthorised access to company systems. The attackers use social engineering and often deliver via phishing lures. Campaigns observed in late January and early February 2026 used fake business, government, and document-sharing themes.

Threats Protected: 9
Class Type: Trojan-activity
Rule Set Type:

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

Kill Chain:

Tactic	Technique ID	Technique Name
Initial Access	T1566.001	Phishing: Spearphishing Attachment
Resource Development	T1583.003	Acquire Infrastructure: Virtual Private Server
Execution	T1204.002 T1059.001	User Execution: Malicious File Command and Scripting Interpreter: PowerShell
Command-and-Control	T1071.001	Application Layer Protocol: Web Protocols

2. MoonRise

MoonRise is a sophisticated Remote Access Tool (RAT) written in the GO (Golang) programming language and is known for its extensive surveillance capabilities and cross-platform potential. This frequently masquerades as a legitimate system process (such as svchost.exe or moonrise-client.exe). This is also able to modify the Windows Registry to run keys that establish persistence, ensuring it restarts with the computer. This primarily focuses on surveillance and data theft, including real-time streaming, webcam/microphone access, and keystroke logging. MoonRise is often distributed via phishing emails, software cracks, and malvertising.

Threats Protected: 1
Class Type: Command-and-Control
Rule Set Type:

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

Kill Chain:

Tactic	Technique ID	Technique Name
Command-and-Control	T1071.001	Application Layer Protocol: Web Protocols
Initial Access	T1566.001	Phishing: Spearphishing Attachment
Execution	T1204.002	User Execution: Malicious File
Persistence, Privilege Escalation	T1547.001	Boot or Logon AutoStart Execution: Registry Run Keys / Startup Folder
Defence Evasion	T1553.002	Subvert Trust Controls: Code Signing

Current Threat Summary

Known Exploited Vulnerabilities (Week 3 - February 2026)

Vulnerability	CVSS	Description
CVE-2025-49113	9.9	RoundCube Webmail contains a PHP object deserialisation vulnerability that can allow an authenticated attacker to execute code on the system. This vulnerability affects versions before 1.5.10 and before 1.6.11.
CVE-2025-68461	7.2	RoundCube Webmail contains a cross-site scripting vulnerability within the animate tag of an SVG document, this can allow an unauthenticated attacker to execute JavaScript if a user opens an email containing a malicious SVG attachment.
CVE-2021-22175	6.8	GitLab contains a server-side request forgery vulnerability that can allow an unauthenticated remote attacker to send requests in the context of the server to internal networks via webhooks.
CVE-2026-22769	10	Dell RecoverPoint for Virtual Machines (RP4VMs) contains a vulnerability relating to the use of hard-coded credentials that can allow an unauthenticated remote attacker to authenticate to the underlying system with root level privileges.
CVE-2020-7796	9.8	Synacor Zimbra Collaboration Suite (ZCS) contains a server-side request forgery vulnerability within the WebEx zimlet component that can allow an unauthenticated remote attacker to send requests in the context of the server and may allow for further attacks against the system.
CVE-2024-7694	7.2	TeamT5 ThreatSonar Anti-Ransomware contains a vulnerability that can allow an authenticated remote attacker to upload files containing malicious code which can result in an attacker gaining access to the underlying system.
CVE-2008-0015	8.8	Microsoft Windows Video ActiveX Control contains a vulnerability that can allow an unauthenticated remote attacker to execute code on a device upon visiting a specially crafted web page.
CVE-2026-2441	8.8	Google Chromium CSS contains a use-after-free vulnerability that can allow an unauthenticated remote attacker to execute arbitrary code upon visiting a specially crafted HTML page, this vulnerability affects versions prior to 145.0.7632.75.

For more information, please visit the Red Piranha Forum:
https://forum.redpiranha.net/t/known-exploited-vulnerabilities-catalog-3rd-week-of-february-2026/642

Updated Malware Signatures (Week 3 - February 2026)

Threat	Description
NanoCore CnC Checkin	This detects CnC (C2) check-ins performed by the NanoCore malware. CnC checks are used to let the malware operators know which and how many systems they have available to accept commands from.

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

Ransomware activity this week was dominated by NightSpire, accounting for 19.35% of total disclosures, marking it as the most aggressive operator in the current reporting cycle. LockBit 5, following closely behind, at 13.71%, signalled continued evolution and sustained operational scale under the LockBit brand. The Gentlemen followed up ith 8.47%, while Qilin maintained strong activity at 7.26%. DragonForce also remained highly active, contributing 6.05%.

A second tier of notable actors included Akira (4.84%), Play (4.03%), and INC Ransom (3.63%). Everest and Lynx each represented 3.23%, demonstrating steady operational continuity. Meanwhile, Genesis accounted for 2.82%, and both Sinobi and Space Bears stood at 2.42%.

Moderate-to-lower activity bands included ShinyHunters (2.02%), Payload (1.61%), and Medusa (1.61%). Groups contributing 1.21% included Coinbase Cartel, WorldLeaks, Eraleign (APT73), and Tengu.

Smaller contributors at 0.81% included Interlock, Securotrop, LeakNet, Beast, and Insomnia. Single-disclosure actors at 0.4% included Kairos, Bravox, Nova, KillSec3, Rhysida, PayoutsKing, Anubis, Nitrogen, RansomHouse, Cloak, and Brain Cipher.

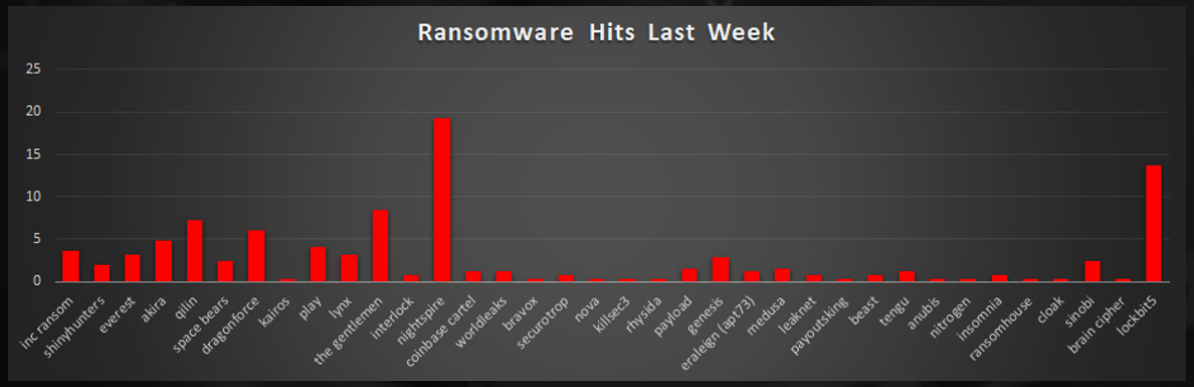


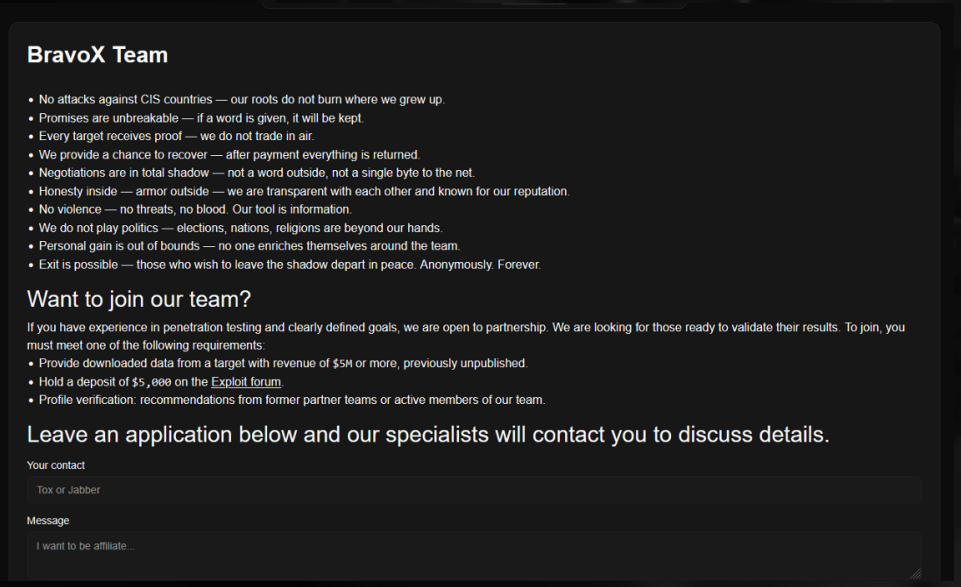
Figure 1: Ransomware Group Hits Last Week

BravoX Ransomware

Description

BravoX is a newly emerged Ransomware-as-a-Service (RaaS) operation that first announced itself publicly on 23 January 2026 by posting a Tor-based Data Leak Site (DLS) address.
BravoX operates a double-extortion model, combining file encryption with bulk data exfiltration. Confirmed exfiltration volumes published on the DLS range from 460 GB to over 3.1 TB per victim, indicating systematic collection from enterprise file stores. The group threatens progressive data publication on its DLS if ransom demands are not met.

Affiliate recruitment criteria observed prior to the RAMP forum seizure specify a minimum target revenue threshold of USD 5 million and explicitly exclude Commonwealth of Independent States (CIS) countries, a restriction consistent with Russian-speaking threat actors seeking to avoid domestic law enforcement attention. The affiliate revenue split was not confirmed in open-source reporting prior to the forum seizure.



BravoX Team

- No attacks against CIS countries — our roots do not burn where we grew up.
- Promises are unbreakable — if a word is given, it will be kept.
- Every target receives proof — we do not trade in air.
- We provide a chance to recover — after payment everything is returned.
- Negotiations are in total shadow — not a word outside, not a single byte to the net.
- Honesty inside — armor outside — we are transparent with each other and known for our reputation.
- No violence — no threats, no blood. Our tool is information.
- We do not play politics — elections, nations, religions are beyond our hands.
- Personal gain is out of bounds — no one enriches themselves around the team.
- Exit is possible — those who wish to leave the shadow depart in peace. Anonymously. Forever.

Want to join our team?

If you have experience in penetration testing and clearly defined goals, we are open to partnership. We are looking for those ready to validate their results. To join, you must meet one of the following requirements:

- Provide downloaded data from a target with revenue of $5M or more, previously unpublished.
- Hold a deposit of $5,000 on the Exploit forum.
- Profile verification: recommendations from former partner teams or active members of our team.

Leave an application below and our specialists will contact you to discuss details.

Your contact

Tox or Jabber

Message

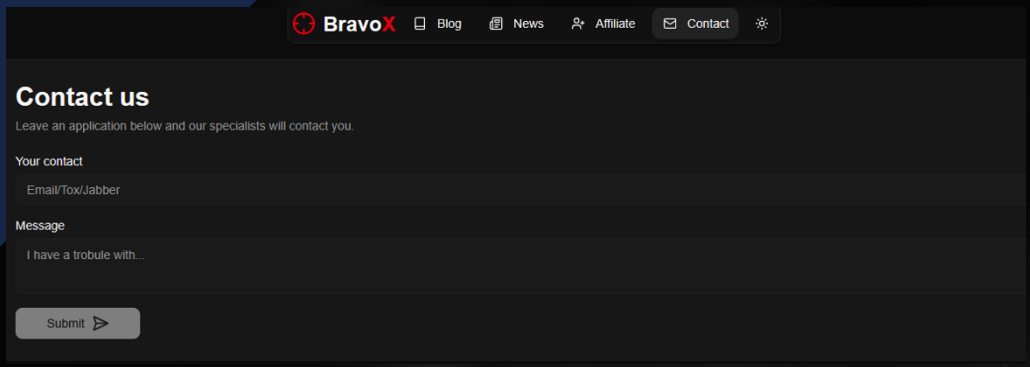
I want to be affiliate...

Technical Profile

As of 20 February 2026, no BravoX encryptor binary, file hash of any type, ransom note, encrypted file extension, or any other malware artefact has been recovered, submitted to any analysis platform, or published by any threat intelligence vendor or researcher. No technical analysis of the BravoX payload has been conducted or published.

Data Leak Site Infrastructure (Confirmed via Red Piranha DLS Analysis):

- Technology Stack: Vue 3.5.25 (JavaScript SPA framework), Vite build toolchain, Pinia state management, Vue Router (history mode), Axios 1.13.2 HTTP client, Tailwind CSS, Sonner notification library. Confirmed through Red Piranha source enumeration of the DLS.
- Site Structure: Seven routes identified: blog, individual blog posts, news, individual news articles, victim data explorer (/explorer/:id), affiliate management portal (/affiliate), and ransom negotiation contact form (/contact).
- Authentication: Cookie-based session authentication is enforced sitewide. Unauthenticated requests to gated content are redirected to a verification gate (/verify). Victim data is not accessible without an authenticated session.
- Real-Time Capability: Server-Sent Events (SSE) streaming implemented in DLS codebase, indicating live operational monitoring by BravoX operators.
- Affiliate Panel: Dedicated /affiliate route confirms the RaaS model is operationally implemented on the platform, not solely claimed in recruitment posts.
- Negotiation Channel: Ransom negotiation conducted via a dedicated /contact module embedded in the DLS. No email, TOX messenger, or other external communication channels have been observed for BravoX.



Detailed TTPs (Tactics, Techniques, and Procedures)

No detailed TTPs have been documented for BravoX by any threat intelligence vendor, researcher, or open-source platform as of 20 February 2026.

The only phases that can be confirmed from operational evidence are Data Collection/Exfiltration and Impact, and even these are confirmed only through the group's own DLS publications rather than through independent incident response analysis or forensic evidence.

Confirmed Operational Activity

Data Exfiltration (Confirmed - DLS Evidence): Large-scale data exfiltration is confirmed across all seven claimed victims through proof-of-data volumes published on the DLS. Confirmed volumes per victim are: Fusion Hill (US, Marketing/Advertising) - 3.1 TB; OEC Bretagne (France, Food Processing) - 859.7 GB; Vatier & Associes (France, Legal) - 463.1 GB. The remaining four victim data volumes are not fully specified in open-source reporting. Exfiltration tooling, protocol, staging mechanism, and timeline have not been confirmed in any published source.

Ransom Extortion via DLS (Confirmed): Staged data leak publication via two active Tor .onion DLS addresses is confirmed. Victim profiles are published with data volume claims and progressive disclosure timelines. Negotiation is conducted exclusively through the DLS /contact module.

RaaS Affiliate Infrastructure (Confirmed): Affiliate management portal confirmed as an active module in the DLS platform. Affiliate recruitment occurred on the RAMP forum prior to its seizure on 28 January 2026, with confirmed criteria of USD 5 million minimum target revenue and CIS country exclusion.

Unknown Attack Chain Phases

The following attack chain phases remain entirely undocumented for BravoX: Initial Access, Execution, Persistence, Privilege Escalation, Defence Evasion, Credential Access, Discovery, Lateral Movement, and Command-and-Control (beyond the Tor-based DLS). These gaps cannot be filled through inference without introducing unverified analytical assumptions. Red Piranha will update this section as confirmed incident response data or payload analysis becomes available.

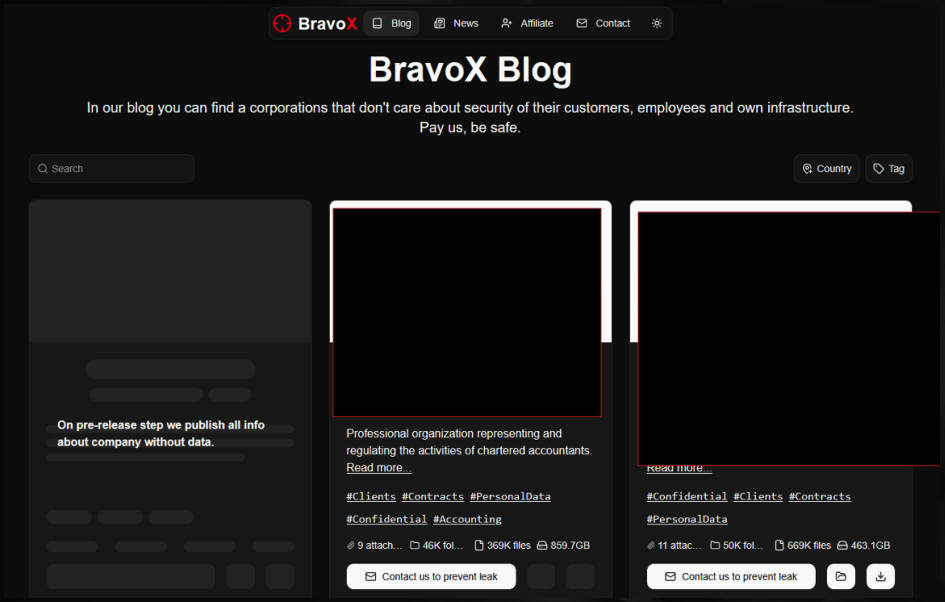
MITRE ATT&CK TTP Matrix

The table below maps only confirmed or operationally evidenced BravoX activity to the MITRE ATT&CK framework. No entries are included for phases that are unknown. This mapping will be significantly expanded upon the recovery of an encryptor sample or the publication of incident response findings.

Tactic	Technique (ID)	BravoX Implementation
Initial Access	Unknown	No initial access vector confirmed. No incident response data or payload analysis is available.
Execution	Unknown	No encryptor binary has been recovered. Execution model, parameters, and delivery method unknown.
Persistence	Unknown	No persistence mechanisms are documented.
Privilege Escalation	Unknown	No escalation techniques are documented.
Defence Evasion	Unknown	No evasion techniques documented. No binary recovered for analysis.
Discovery / Lateral Movement	Unknown	No discovery tooling or lateral movement methods are documented.
Command-and-Control	Unknown (beyond DLS infrastructure)	No C2 IP addresses, clear web domains, or operational C2 channels are identified. Victim negotiation via Tor DLS confirmed. Ransomware payload C2 unknown.

Indicators of Compromise (IOCs)
Infrastructure / C2:

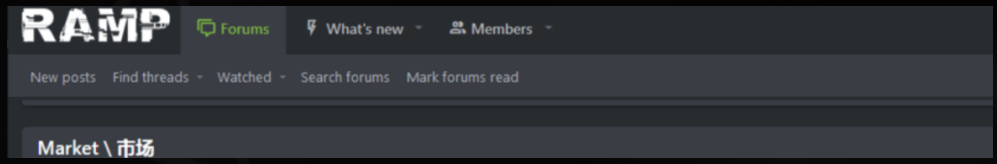
- TOR Data Leak Site (Primary, ONLINE): bravoxxtrmqeeevhl7gdh2yzvlrjxajr66d33c7ozosrccx4cz7cepad.onion
- TOR Data Leak Site (Secondary, ONLINE): bravoxxwcfz5qk43ychgveprpd5mw5hvxfs4a2uz2okx7mumiht4fzyd.onion



Note: Both .onion addresses confirmed operationally active as of 20 February 2026. No C2 IP addresses, clear-web domains, or other network-layer IOCs have been published by any source for BravoX. Any IP addresses attributed to BravoX in third-party feeds should be independently verified before actioning.

Communication Identifiers:

- RaaS Recruitment Forum: RAMP cybercriminal forum - account active September 2025 to 28 January 2026 (date of seizure). The forum is no longer operational.



Victim Profile Reporting Period Activity

One new victim was added to the BravoX DLS during the 14–20 February 2026 reporting period:

- OEC Bretagne (France | Food Processing / Chartered Accountants | Published approx. 16 February 2026 | 859.7 GB claimed data including client information, professional contracts, and personal data)

Mitigation Strategies
Recommended CE 5.5 Configuration Actions

- Block BravoX Infrastructure (CE SWG): Add both confirmed .onion addresses (bravoxxtrmqeeevhl7gdh2yzvlrjxajr66d33c7ozosrccx4cz7cepad.onion and bravoxxwcfz5qk43ychgveprpd5mw5hvxfs4a2uz2okx7mumiht4fzyd.onion) to the Crystal Eye Unified Secure Web Gateway (SWG) blocklists
- Deploy IDPS Exfiltration Detection Rules (CE IDPS / Threat Hunt Dashboard): In the absence of file-based IOCs, IDPS alerting should focus on exfiltration precursor behaviours consistent with BravoX's confirmed operational profile: bulk data staging events, large-volume transfers to unusual external endpoints, unexpected compression utility execution (7-Zip, WinRAR, tar) in sensitive directories, and anomalous use of encrypted file transfer clients.
- Enforce CEASR Application Allowlisting (CEASR Endpoint): Deploy Crystal Eye Attack Surface Reduction (CEASR) application allowlisting policies aligned to ASD Essential Eight Maturity Level 3.
- Activate Red Piranha MDR & Incident Response (CESOC / DFIR): Enable Red Piranha Managed Detection and Response (MDR) services and CESOC 24×7 SOC escalation. Organisations in Healthcare, Legal, Professional Services, Food Processing, and Marketing in the United States, France, and Canada should be prioritised as elevated-risk environments.

Ransomware Victims by Geography

The United States continues to dominate the ransomware landscape, accounting for 47.98% of worldwide victims. The concentration of attacks reflects its economic scale, digital infrastructure maturity, and the financial leverage threat actors can extract from impacted organisations.

A second cluster of heavily targeted countries includes Italy (4.03%), along with Canada, India, Germany, the United Kingdom, and Brazil, each recording 3.23%. Taiwan followed at 2.82%, while Japan stood at 2.42%. Spain and Thailand each contributed 2.02%, indicating consistent multinational targeting across Europe and Asia-Pacific.

Countries contributing 1.61% to 1.21% included Chile, Poland, Indonesia, Egypt, and Mexico, demonstrating ransomware's reach across emerging and mid-sized economies.

Several countries recorded 0.81% of total activity, including Turkey, France, China, South Africa, Sweden, United Arab Emirates, Kuwait, Argentina, and Romania.

A broader long tail of countries, each represented 0.4% of global victims, including Hong Kong, Fiji, Puerto Rico, South Korea, Austria, Israel, Hungary, Belgium, Denmark, Peru, Sudan, Saudi Arabia, New Zealand, Netherlands, Morocco, Ukraine, Mauritius, Australia, Colombia, Turks and Caicos Islands, Norway, and Korea.

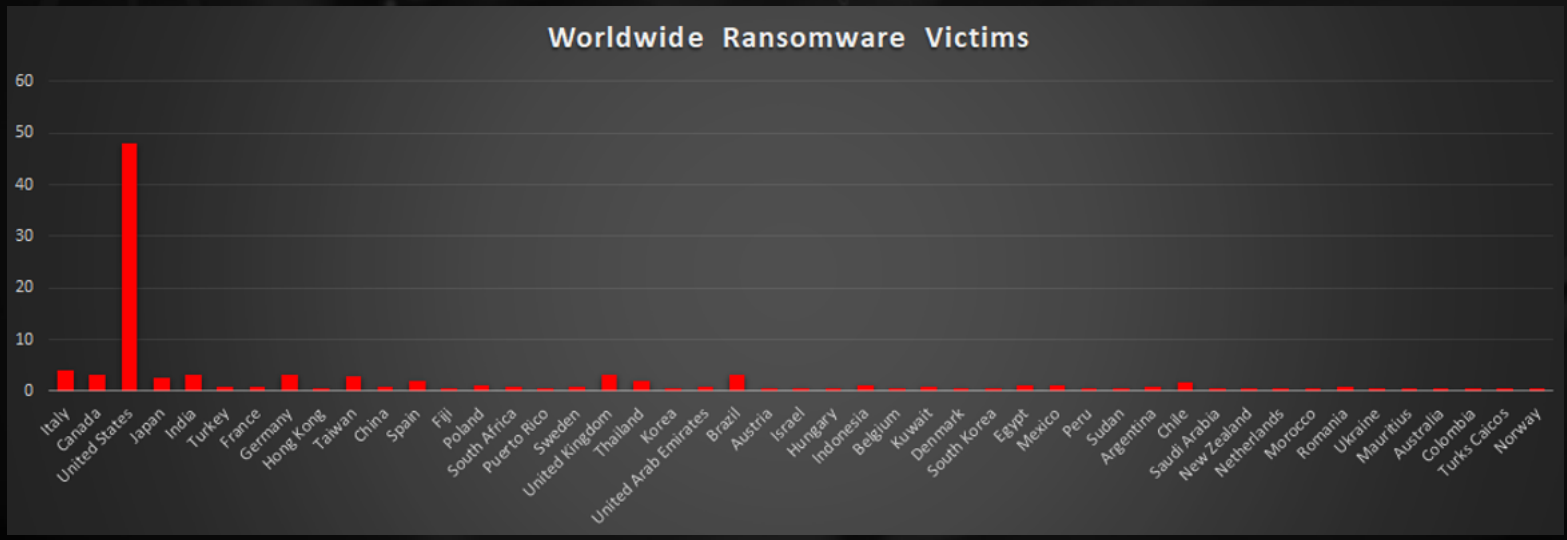


Figure 6: Ransomware Victims Worldwide

Industry-wide Ransomware Victims

Ransomware activity is most heavily concentrated in the Manufacturing sector, which accounts for 16.94% of industry-wide victims, making it the most targeted industry in the dataset. Business Services follows at 14.11%, reinforcing that operationally critical and service-oriented organisations remain prime targets due to their dependence on uptime and client data integrity.

Retail represents 8.87% of victims, while Hospitality and Construction each account for 7.66%. These sectors rely heavily on continuous operations and transactional systems; increasing the leverage of attackers can be applied during disruptions. IT stands at 6.45%, and Transportation at 6.05%, both of which are infrastructure-enabling industries that can create cascading operational impacts if compromised.

Healthcare accounts for 5.24% of victims, and Finance represents 4.03%. Despite strong regulatory environments, both sectors remain attractive due to sensitive data holdings and high urgency to restore operations. Law Firms and Education each contribute 3.63%, while Architecture represents 3.23%, reflecting consistent targeting of professional services handling proprietary or confidential information.

Consumer Services makes up 2.82% of victims. Federal and Agriculture, each accounting for 2.02%, while Insurance stands at 1.61%. Real Estate and Organisations, each representing 1.21%. Electronics and Energy are the least represented sectors in this dataset at 0.81% each.

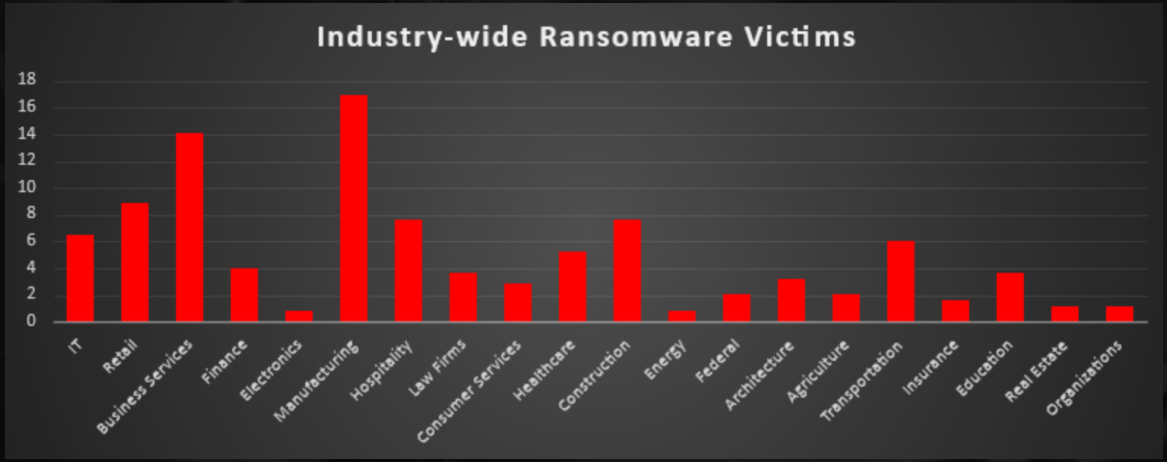


Figure 7: Industry-wide Ransomware Victims