THREAT INTELLIGENCE REPORT

February 03 - 09, 2026

Red Piranha
unified threat management

Report Summary:

New Threat Detection Added

- PulsarRAT
- Chrysalis Backdoor

The following threats were added to Crystal Eye this week:

1. PulsarRAT

PulsarRAT is a remote access tool (RAT) that is built on Quasar RAT, an open-source RAT that has been around since 2014. Threat actors have used this software as a base for their malware with PulsarRAT being a new iteration. PulsarRAT has new built-in functions that assist threat actors in performing data theft on the infected host. It supports keylogging, info stealing (credentials, cookies, crypto wallets, session files), and remote shells.

Threats Protected: 1
Class Type: Trojan-activity
Rule Set Type:

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

Kill Chain:

Tactic	Technique ID	Technique Name
Collection	T1119	Automated Collection
Command-and-Control	T1071.001	Application Layer Protocol: Web Protocols

2. Chrysalis Backdoor

Chrysalis Backdoor is a custom malware which has been attributed to the Lotus Blossom, a Chinese APT. Chrysalis was packed into Notepad++ due to a compromise of the hosting platform that Notepad++ was using to distribute the software. Chrysalis uses legitimate binaries/programs to sideline the malicious DLL. Chrysalis uses custom hashing to hide its C2 logic in the DLL. The malware sets persistence via service or registry edits; it can also keep an instance of itself in the background.

Threats Protected: 5
Class Type: Domain-c2
Rule Set Type:

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

Kill Chain:

Tactic	Technique ID	Technique Name
Persistence	T1543.003 T1547.001	Create or Modify System Process: Windows Service Boot or Logon AutoStart Execution: Registry Run Keys / Startup Folder
Command-and -Control	T1071.001	Application Layer Protocol: Web Protocols

Current Threat Summary

Known Exploited Vulnerabilities (Week 1 - February 2026)

Vulnerability	CVSS	Description
React Native Community CLI	9.8	React Native Community CLI contains a command injection vulnerability that can allow an unauthenticated attacker to send a HTTP request to the Metro Development Server. This server is created when using @react-native-community/cli which by default binds the development server to all interfaces. Exploitation of this vulnerability can result in the execution of operating system commands on this server.
SmarterTools SmarterMail	9.3	SmarterTools SmartMail contains a vulnerability within the ConnectToHub API method that can allow an unauthenticated remote attacker to execute operating system commands.
GitLab Community and Enterprise	6.8	GitLab Community and Enterprise Editions contain a server-side request forgery vulnerability that can allow an unauthenticated attacker to send requests on the server's behalf via the CI Lint API.
Sangoma FreePBX OS	8.6	Sangoma FreePBX Endpoint Manager contains an OS command injection vulnerability that can allow an authenticated remote attacker to execute operating system commands on the system.
Sangoma FreePBX OS	9.8	Sangoma FreePBX contains an authentication bypass vulnerability that can allow an unauthenticated remote attacker to log into the system as an admin user. Exploitation of this vulnerability could allow an attacker to carry out further attacks which may result in unauthorised access to the system.
SolarWinds Web Help Desk	9.8	SolarWinds Web Help Desk contains a deserialisation vulnerability that can allow an unauthenticated remote attacker to execute code on the system.

For more information, please visit the Red Piranha Forum:
https://forum.redpiranha.net/t/known-exploited-vulnerabilities-catalog-1st-week-of-february-2026/639

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

0APT overwhelmingly dominated this week's ransomware activity, responsible for 44.74% of all reported incidents. This is a massive share for a single actor and strongly suggests either a large, coordinated campaign window or a substantial dump of backlogged victim disclosures that pushed 0apt far ahead of every other group in the ecosystem.

A strong second tier was led by Qilin (9.4%), Akira (6.77%), and Everest (5.64%), with Inc Ransom (3.76%), DragonForce (3.38%), and The Gentlemen (3.01%) close behind. Together, this band of established crews formed a sizeable secondary block of activity, reflecting sustained multi-industry targeting and regular leak-site publishing beneath the shadow of 0APT's surge.

A mid-tier cluster included Play (2.63%), PayoutsKing (2.63%), and Sinobi (2.26%), along with Coinbase Cartel (1.88%), and a group of operators, each contributing 1.13% of cases, Rhysida, Anubis, Medusa, and RansomHouse. These actors did not approach 0apt's scale individually, but collectively they represented a meaningful slice of global ransomware pressure and helped maintain a diverse threat mix across regions and sectors.

Smaller but persistent operators, such as Tengu, The Green Blood Group, Linkc, DevMan2, Lynx, ShinyHunters (each 0.75%), maintained a visible but lower-volume presence, continuing to add background noise to the ecosystem through sporadic yet recurring victim disclosures.

At the long tail, a wide spread of fringe groups, Pear, Interlock, Genesis, Leaknet, Termite, Worldleaks, Space Bears, KillSec3, Nitrogen, Bravox, Beast, TridentLocker (each 0.38%), appeared in very small numbers but still contributed to the overall fragmentation and churn. While individually minor, their collective footprint underscores how crowded and resilient the ransomware ecosystem remains, even in weeks where one family like 0apt clearly dominates the statistics.

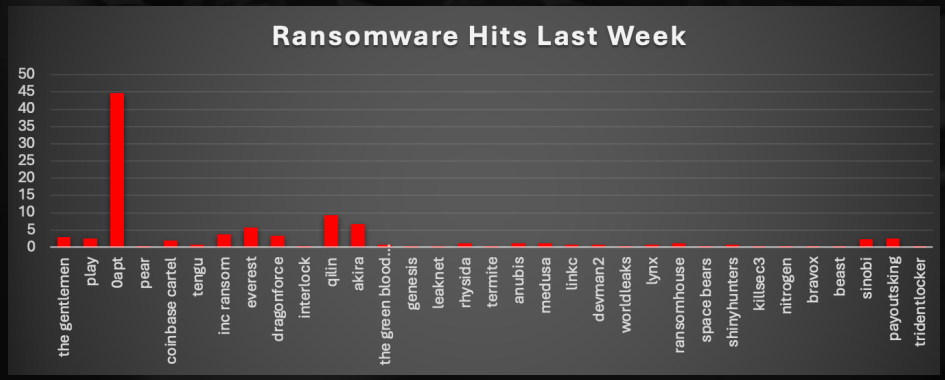


Figure 1: Ransomware Group Hits Last Week

The Green Blood Group Ransomware

The Green Blood Group is a newly emerged ransomware operation first observed in late January 2026. The group operates a double-extortion model - encrypting victim files while exfiltrating sensitive data to maximise ransom pressure. The Green Blood Group maintains a Tor-based Data Leak Site (DLS) where victim profiles are published alongside a staged countdown/holding message mechanism. The group has claimed victims across India, Belgium, Egypt, Senegal, and Colombia, targeting sectors including Government/Public Sector, Manufacturing, and Industrial operations.

Based on infrastructure observations and malware analysis, The Green Blood Group appears to be an entirely new, standalone ransomware operation rather than a rebrand of a known legacy group. The targeting pattern suggests a deliberate focus on regions where incident response maturity and ransomware disclosure requirements vary, potentially increasing the likelihood of successful extortion. Notably, on 4-5 February 2026.

Technical Profile
Ransomware Payload: The Green Blood Group operates a Golang-based encryption framework compiled with go1.24.2 and AMD64-specific assembly optimisations:

- Encryption Engine: ChaCha8 (a faster, 8-round variant of the ChaCha20 stream cipher), chosen for speed on modern CPUs capable of encrypting hundreds of GB/hour. Internal Go crypto library method names (.State.Init, .Refill64, .Reseed, .Next,. block) and source path /usr/local/go/src/internal/chacha8amd64.s confirm vetted cryptographic primitives with AMD64 assembly optimisations.
- File Extension: Appends .tgbg to encrypted files (e.g., document.pdf document.pdf.tgbg).
- Ransom Note: !!!READ_ME_TO_RECOVER_FILES!!!.txt dropped in encrypted directories.
- Binary Characteristics: Fully statically linked Go executable (not obfuscated at the compiler level). The .data section contains go_buildinfo_ref, go_buildinfo, and runtime_buildVersion_str-confirming it is a native Go binary rather than a wrapper or loader. All Go runtime symbols (runtime_morestack, sync.WaitGroup, channels) are fully readable.
- Platform Support: Windows (Win64/AMD64 confirmed). Cross-platform potential inherent to Golang compilation.
- Extortion Types: Direct Extortion, Double Extortion, and Free Data Leaks (three concurrent models per WatchGuard).

Detailed Tactics, Techniques, and Procedures (TTPs)

1. Initial Access (Multi-Vector Delivery)
The Green Blood Group gains initial access through multiple delivery mechanisms typical of modern ransomware operations. Primary access methods include phishing emails containing malicious attachments or links designed to trick users by mimicking legitimate communications, exploitation of vulnerabilities in outdated software and public-facing applications to deploy the ransomware silently, compromised websites and malicious advertisements serving drive-by downloads, pirated software, cracking tools, and key generators used as trojanised delivery vehicles, and infected USB drives and peer-to-peer file-sharing networks. The group's targeting pattern focuses on organisations in regions with lower incident response maturity (India, Senegal, Egypt, Colombia, Belgium), suggesting affiliates or operators may also leverage Initial Access Brokers (IABs) for pre-compromised network access.

2. Execution & Encryption Engine
Upon achieving access, the Golang-compiled binary is executed on the victim system. The ransomware immediately initialises its KeyManager-a lean 56-byte container carrying the 32-byte ChaCha8 encryption key as a byte slice, a recovery token string (only provided upon ransom payment), and a unique machineID to tag each infected host. The main encryption orchestrator struct spans 120 bytes, containing a pointer to the KeyManager, a pool of worker channels for parallel encryption, two sync.WaitGroups to track file processing and overall progress, a mutex-protected statistics block, and the fileQueue channel that feeds victim file paths to the encryption workers. The Go-idiomatic design enables concurrent workers to race through directories in parallel, with keys generated once and reused, progress silently tallied-built to scale across dozens or hundreds of CPU cores.

3. Reconnaissance & Discovery
The Green Blood Group performs systematic filesystem traversal to identify high-value targets before encryption. The ransomware traverses C:\Users\ and all mounted drives, queuing every discoverable file for ChaCha8 encryption. A file evaluation gatekeeper uses DMORD (likely a custom hash or magic-byte check) that scans 32+ offsets across each file header. Files are evaluated against a blacklist/exclusion list including .exe files and critical system paths to avoid system instability and maximise successful extortion. The malware does not blindly encrypt everything-it deliberately weighs file traits against exclusion criteria before queueing, ensuring the operating system remains functional while data files are rendered inaccessible. System Information Discovery is performed via the machineID generation mechanism, which uniquely fingerprints each infected host for victim identification and ransom tracking.

4. Defence Evasion
The Green Blood Group employs several evasion characteristics inherent to its design. The use of Golang naturally complicates reverse engineering due to non-standard calling conventions, massive function tables, and the large binary size typical of statically linked Go executables. However, Foresiet's analysis confirms the binary is NOT obfuscated at the compiler level-all Go runtime symbols (runtime_morestack, sync.WaitGroup, channels) are readable, and the go_buildinfo confirms the go1.24.2 toolchain. Communication infrastructure exclusively uses Tor (.onion services) and OnionMail to avoid attribution and takedown.

5. Data Collection & Exfiltration (Double-Extortion Preparation)
Before encryption is triggered, data is exfiltrated to support the double-extortion model. The scale of exfiltration is evidenced by the Senegal DAF breach, where the group claims to have stolen 139 TB of data-including biometric records, identity documents, electoral data, and immigration files for the entire Senegalese population. According to SENTV cybersecurity experts, this volume suggests a structured, prolonged operation requiring internal access, privilege escalation, and progressive data exfiltration over weeks or months. Data from the local system is harvested across sensitive directories, staged for efficient transfer, and exfiltrated over attacker-controlled channels. This data theft is central to the double-extortion model-even if a victim successfully restores from backups, the threat of leaking sensitive data provides secondary leverage to demand payment.

6. Encryption & Impact (Ransomware Deployment)
The Green Blood Group employs a modern, speed-optimised encryption scheme. Files are encrypted using ChaCha8, an 8-round variant of the ChaCha20 stream cipher, compiled with AMD64-specific assembly optimisations (/usr/local/go/src/internal/chacha8amd64.s). This is not borrowed crypto code-it is a deliberate, tuned implementation using standard Go crypto library internals chosen for maximum throughput on modern CPUs, consistent with 2025-2026 ransomware families that encrypt hundreds of GB/hour. Encrypted files receive the .tgbg extension. The ransom note !!!READ_ME_TO_RECOVER_FILES!!!.txt is deployed in affected directories containing a Recovery ID (format: GREEN-BLOOD--<ID>), Machine ID, and contact details directing victims to thegreenblood@proton.me with payment inquiry instructions. Encrypted files are not trivially recoverable without the correct key material. No free decryptor is currently available.

7. Inhibit System Recovery
As is standard with modern ransomware operations, The Green Blood Group is expected to destroy recovery options before or during encryption. While the specific shadow copy deletion commands have not been independently extracted from the binary, this behaviour is nearly universal among ransomware families and consistent with the group's professional design approach. The deliberate exclusion of .exe files and system-critical paths from encryption further supports an operator philosophy of maintaining system bootability while denying data access-maximising pressure on victims to pay rather than simply reimage.

8. Command & Control/Negotiation/Data Leak

The Green Blood Group maintains Tor-based infrastructure for operations and victim communications. The leak site operates at scbrksw5fgjtujc2ah42roo6bij2unr2tggfcynpbql5a7yp3s22taid.oni on on port 8000, running a Python SimpleHTTP 0.6 server on Python 3.9.2. The site was last confirmed active on 2026-02-08 10:31:57 UTC. Instead of immediately listing victims, the site displays a staged countdown-style holding message indicating that victim names and stolen data are temporarily withheld. This tactic allows victims time to negotiate before identities are exposed, signals credibility without prematurely burning leverage, and avoids premature exposure that could disrupt negotiations. Victim communication is conducted via two email channels: thegreenblood@proton.me (in ransom notes) and thegreenblood@onionmail.org (on leak site infrastructure), plus a Tox ID for P2P encrypted chat. The staged disclosure model has become increasingly common among ransomware groups seeking to balance operational security with maximum extortion impact.

9. Operational Model & Attribution

The Green Blood Group currently appears to operate as a standalone group rather than a Ransomware-as-a-Service (RaaS) with visible affiliate recruitment. No evidence of affiliate dashboards, recruitment posts on darknet forums, or RaaS pricing has been observed. The group's geographical origin and potential affiliations remain unknown. Cyble notes that while the group has not yet publicly named specific victims on some tracking platforms, it claims affected organisations are located in India, Senegal, and Colombia. The professionally engineered payload, structured key management, and dedicated Tor infrastructure indicate deliberate design choices rather than experimental development-suggesting experienced operators behind the operation.

MITRE ATT&CK TTP Matrix

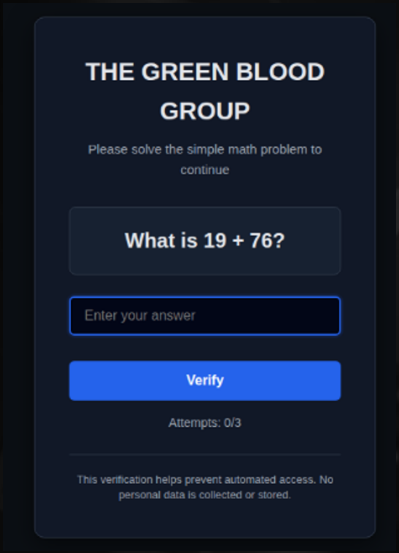
The table below summarises The Green Blood Group's tactics and techniques mapped to the MITRE ATT&CK framework:

Tactic	Technique (ID)	Green Blood Implementation
Initial Access	Phishing (T1566)	Malicious email attachments/links mimicking legitimate communications
	Drive-by Compromise (T1189)	Compromised websites, malicious advertisements
Initial Access	Replication via Removable Media (T1091)	Infected USB drives, P2P file-sharing networks
Execution	User Execution: Malicious File (T1204.002)	User executes Golang-compiled binary
Discovery	File & Directory Discovery (T1083)	Traverses C:\Users\ and mounted drives via DMORD file evaluation
	System Info Discovery (T1082)	machineID generation to fingerprint each infected host
Collection	Data from Local System (T1005)	File evaluation and queueing against exclusion criteria via DMORD
Exfiltration	Exfil Over C2 Channel (T1041)	139 TB data theft in DAF case; data staged before encryption
Defence Evasion	Obfuscated Files or Information (T1027)	Go binary complexity (though not compiler-level obfuscation)
Impact	Data Encrypted for Impact (T1486)	ChaCha8 encryption with .tgbg extension; parallel worker threads
	Inhibit System Recovery (T1490)	Likely VSS deletion (standard ransomware behaviour)
	Financial Theft/Extortion (T1657)	Ransom demand via email and Tox for decryption key
C2	App Layer Protocol: Web (T1071.001)	Tor-based leak site and C2 communication
	Proxy: Multi-hop (T1090.003)	Tor .onion for anonymisation of leak site infrastructure
Resource Dev.	Acquire Infrastructure (T1583.001)	Tor .onion site, OnionMail, and Proton.me services

Indicators of Compromise (IOCs)
Infrastructure/C2:

- TOR Leak Site: scbrksw5fgjtujc2ah42roo6bij2unr2tggfcynpbql5a7yp3s22taid.onion:8000

Full URL: http://scbrksw5fgjtujc2ah42roo6bij2unr2tggfcynpbql5a7yp3s22taid.onion[:]8000[/]sqdkhqskdhqskdjqsgdhfh.html



Server Fingerprint: SimpleHTTP 0.6 / Python 3.9.2
Communication Identifiers:

- Email (Ransom Note): thegreenblood@proton.me
- Email (Leak Site): thegreenblood@onionmail.org
- Tox: F97A512AA18917444315510B107AB8B46166CAC4E79DB76B849FFE48A67A4B621AB7CC9A1EFB

Malware Samples:

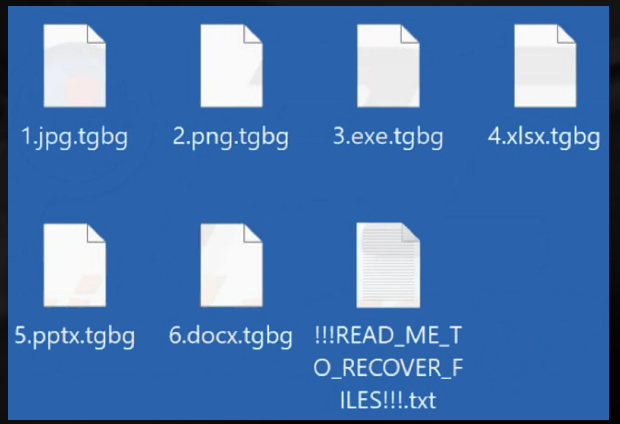
- SHA-256: 12bba7161d07efcb1b14d30054901ac9ffe5202972437b0c47c88d71e45c7176

AV Detection Names:

Vendor	Detection
Avast	FileRepMalware [Ransom]
Bkav Pro	W64.AIDetectMalware
ESET-NOD32	Generik.DWXINLW Trojan
Kaspersky	Trojan-Ransom.Win32.Encoder.afyu
Microsoft	Ransom:Win32/Avaddon.P!MSR

File Indicators:

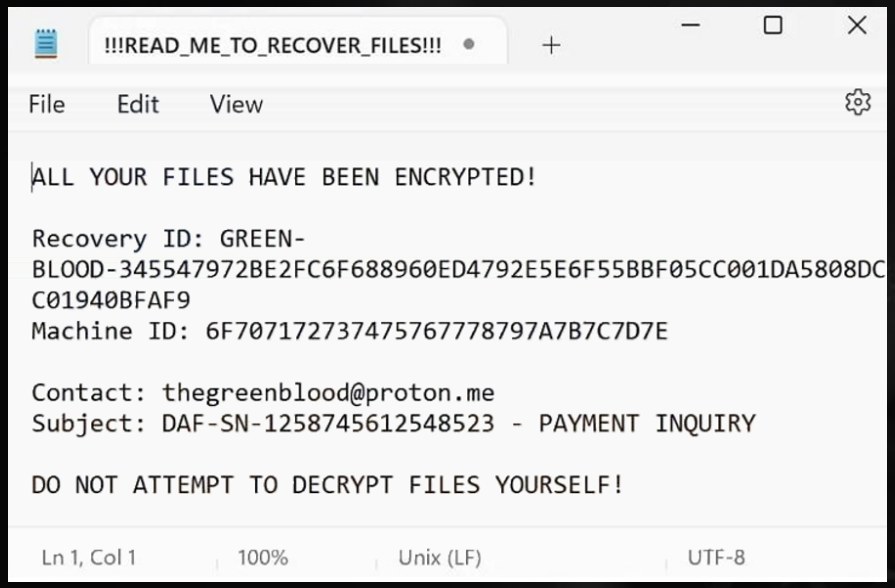
- Extension: .tgbg
- Ransom Note: !!!READ_ME_TO_RECOVER_FILES!!!.txt
- Recovery ID Format: GREEN-BLOOD--<RecoveryID>
- Go Build Version: go1.24.2 (from go_buildinfo in .data section)
- Binary Type: Golang, statically linked, AMD64, Win64



Crypto Library Strings (YARA Hunting):

- .State.Init
- .Refill64
- .Reseed
- .Next
- .block
- /usr/local/go/src/internal/chacha8amd64.s
- go_buildinfo_ref
- runtime_buildVersion_str

Ransom Note Content:



Mitigation Strategies

Recommended CE 5.5 Configuration Actions

- Block Green Blood Infrastructure (CE SWG): Add the known .onion address (scbrksw5fgjtujc2ah42roo6bij2unr2tggfcynpbql5a7yp3s22taid.onion) and OnionMail/Proton.me contact addresses to the Crystal Eye Unified Secure Web Gateway (SWG) blocklists. Leverage Deep Packet Inspection (DPI) to identify and block outbound Tor traffic at the perimeter.
- Deploy IDPS Threat Hunting Rules (CE IDPS / Threat Hunt Dashboard)
- Enforce CEASR Application Allowlisting (CEASR Endpoint): Deploy the Crystal Eye Attack Surface Reduction (CEASR) application to all Windows endpoints. Enable application allowlisting policies aligned to ASD Essential Eight Maturity Level 3 to block execution of unknown or unauthorised Golang-compiled binaries from user-writeable directories (Downloads, Temp, AppData).
- Monitor for Go-Based Ransomware Binaries (CEASR + CE EDR): Configure CEASR behavioural monitoring to alert on execution of unknown statically linked Go binaries. Use CE EDR host-based sensors to detect go_buildinfo sections in PE headers as a high-confidence indicator of Golang-compiled malware.
- Activate Red Piranha MDR & Incident Response (CESOC / DFIR): Enable Red Piranha's Managed Detection and Response (MDR) services and CESOC 24×7 SOC escalation for rapid response to Green Blood indicators. Utilise the integrated SOAR response playbooks for automated containment of low-risk alerts and coordinated human-machine teaming for high-risk ransomware incidents.

Worldwide Ransomware Victims

The United States remained the primary epicentre of ransomware activity, accounting for 47.74% of all identified victims. In other words, nearly half of all known cases this period hit U.S.-based organisations, keeping it far ahead of any other single country in terms of observable exposure.

A strong second tier consisted of the United Kingdom (6.39%), Canada (4.89%), Switzerland (3.38%), and Sweden (3.01%). Together, this block represents a substantial share of non-U.S. activity, reflecting mature digital infrastructures, high levels of online services, and regular disclosure of security incidents, all factors that make these markets attractive to extortion operators.

A broader mid-band followed, led by France and Japan (each 2.63%), Australia and Germany (each 2.26%), and a cluster of key economies at 1.88%, India, United Arab Emirates, and Italy. Just behind them, China, Singapore, and Taiwan (each 1.5%), along with Spain and Finland (each 1.13%), show that ransomware is deeply embedded across Europe and the Asia-Pacific region, not just in North America.

Below this sits a long tail of lower-volume geographies, including Austria, Indonesia, Liberia, Mexico, Denmark (each 0.75%), and a wide spread of single-incident countries such as Armenia, Tanzania, Brazil, Lithuania, Myanmar, Egypt, Dominican Republic, Cambodia, Chile, Bahrain, Malaysia, Thailand, Saudi Arabia, Ireland, Norway, Turkey, Argentina, Senegal, Romania, Netherlands, South Korea, Portugal (each 0.38%). Individually, these contribute only a small fraction of total volume, but collectively they reinforce the same pattern seen week after week: ransomware is a global problem, touching dozens of countries rather than being confined to a handful of headline markets.

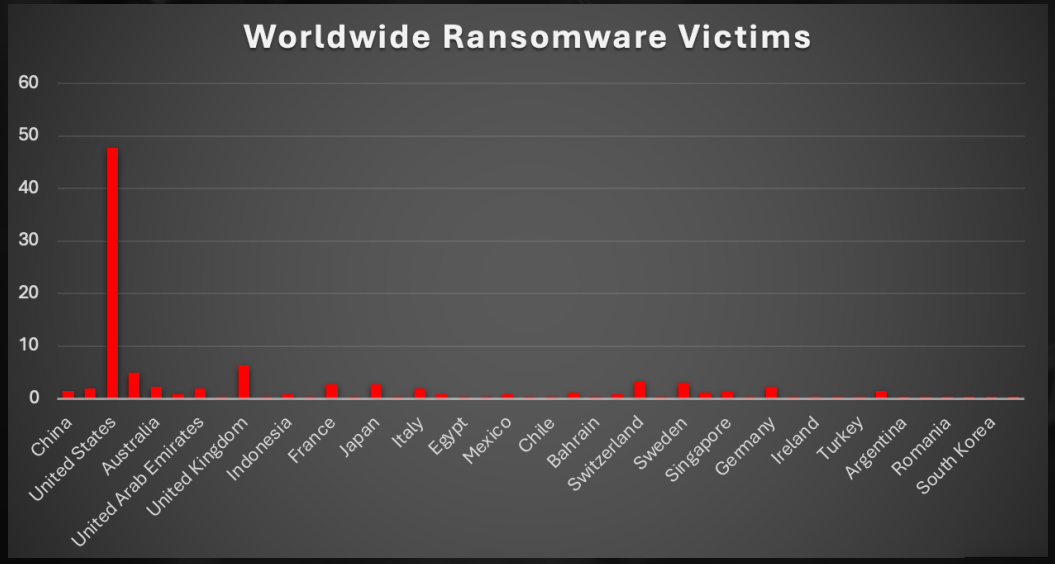


Figure 6: Ransomware Victims Worldwide

Industry-wide Ransomware Victims

Manufacturing was by far the most heavily targeted sector, accounting for 31.2% of all identified ransomware victims. Nearly one in three recorded incidents hit manufacturing, keeping production environments and supply-chain–critical operations right at the top of the risk ladder where downtime instantly translates into financial loss and strong extortion leverage.

A powerful second tier consisted of Business Services (10.53%), Healthcare (9.77%), Retail (7.89%), and Construction (6.39%). Together, these four sectors formed a large concentration of cases across service-heavy, patient-facing, consumer-facing, and project-driven environments, all of which rely on continuous operations, complex logistics, and sensitive data, making them ideal pressure points for ransomware actors.

A broad mid-band followed with Electronics (4.51%), Energy and Education (each 3.38%), and a cluster of Federal, Transportation, Law Firms, and IT organisations (each 2.63%), supported by Finance (1.88%). This layer shows that both critical services (power, transport, government, finance) and knowledge-/data-centric sectors are now routine fixtures in victim datasets rather than occasional outliers.

Lower-volume but still active categories included Real Estate (1.5%), Hospitality, Telecommunications, Media & Internet, Organisations, and Consumer Services (each 1.13%), along with Agriculture and Insurance (each 0.75%), and Minerals & Mining (0.38%) forming the long tail. Individually small but collectively meaningful, this spread underlines how ransomware pressure is now highly diversified across industries: any organisation with digitised operations and monetisable data sits somewhere inside this threat surface.

(The entries labelled Senegal, Taiwan, and Canada at 0.38% clearly belong to the geography dimension and appear as misclassified rows rather than distinct industry sectors.)

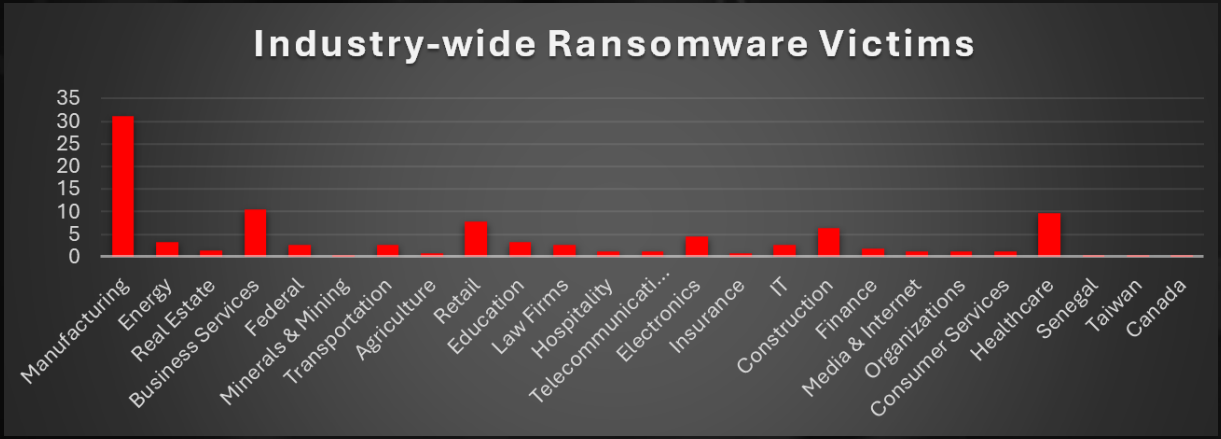


Figure 7: Industry-wide Ransomware Victims