Red Piranha
unified threat management

THREAT INTELLIGENCE REPORT

Dec 02 - 08, 2025

Report Summary:

- **New Threat Detection Added**
  - TA2726
- **Detection Summary**
  - **Threat Protections integrated into the Crystal Eye - 202**
  - **Newly Detected Threats - 2**

The following threats were added to Crystal Eye this week:

1. TA2726

TA2726 is a threat actor group that acts as a traffic distribution system (TDS) to redirect user traffic to malicious payloads. A TDS redirects or filters web traffic, typically used for targeted advertisement or geolocation tracking. TA2726 is using the TDS to direct unsuspecting users to malicious payloads such as JavaScript injections or malware downloads.

Threats Protected: 4
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
Resource Development	T1583.001/2/4/8	Acquire Infrastructure:
		Domains
		DNS Server
		Server
		Malvertising

Current Threat Summary

Known exploited vulnerabilities (Week 1 December 2025)

Vulnerability	CVSS	Description
CVE-2025-55182	10	Meta React Server Components contain a deserialisation vulnerability that can allow an unauthenticated remote attacker to execute code on the system. This vulnerability affects several components including react-server-dom-webpack, react-server-dom-parcel, react-server-dom-turbopack, and due to the opensource nature this vulnerability also affects other frameworks including next, react-router, waku, @parcel/rsc, @vitejs/plugin-rsc, and rwsdk.
CVE-2021-26828	8.8	OpenPLC ScadaBR contains a vulnerability that can allow a remote authenticated attacker to upload an execute an arbitrary file which can result in code execution on the server via the uploading of a webshell. This vulnerability affects versions through 0.9.1 on Linux, and versions through 1.12.4 on Windows.
CVE-2025-48572	Pending	Android Framework contains an unspecified vulnerability within the MediaButtonReceiverHolder and MediaSessionService components that can result in privilege escalation on the device without user interaction.
CVE-2025-48633	Pending	Android Framework contains an unspecified vulnerability within the DevicePolicyManagerService component that can result in information disclosure from the device, potentially leading to privilege escalation without user interaction.

For more information, please visit the **Red Piranha Forum**:
https://forum.redpiranha.net/t/known-exploited-vulnerabilities-catalog-1st-week-of-december-2025/625

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

Qilin led this week's activity, responsible for 20.86% of all reported incidents. This made it the single most dominant operator in the ecosystem, suggesting a concentrated campaign window or a bulk release of victim disclosures that put Qilin clearly ahead of every other group.

A powerful second tier was formed by Akira (13.9%) and LockBit 5 (12.3%), both continuing to operate as large, mature ecosystems with steady victim intake and multi-region targeting. TridentLocker (5.35%) sat just behind them, indicating an increasingly relevant presence and hinting at a growing pipeline of compromises.

A mid-tier cluster, DevMan2 (4.81%), Inc Ransom (4.28%), SafePay (4.28%), DragonForce (3.74%), Play (3.21%), RansomHouse (2.67%), Genesis (2.67%), Sinobi (2.67%), and Everest (2.14%), maintained a steady operational tempo. These crews collectively contributed a substantial share of cases, combining data theft, double extortion, and opportunistic intrusions across multiple industries.

Smaller but persistent operators, including Root (1.6%), alongside BlackShrantac, Handala, Anubis, Chaos, Rhysida, Nitrogen, Nightspire, Interlock, Space Bears, and Nova (each 1.07%), sustained a low- to mid-volume presence. Their activity reflects ongoing campaigns that may not dominate headlines individually but keep the overall pressure high across regions and sectors.

At the long tail, low-frequency brands such as The Gentlemen, Radar, Crypto24, Ciphbit, Benzona, Securotrop, Coinbase Cartel, Lynx, and LockBit 3 (each 0.53%) appeared only sporadically but still contributed to ecosystem fragmentation and churn. While each represents a small fraction of total incidents, their combined footprint underscores how diversified and resilient the ransomware landscape remains.

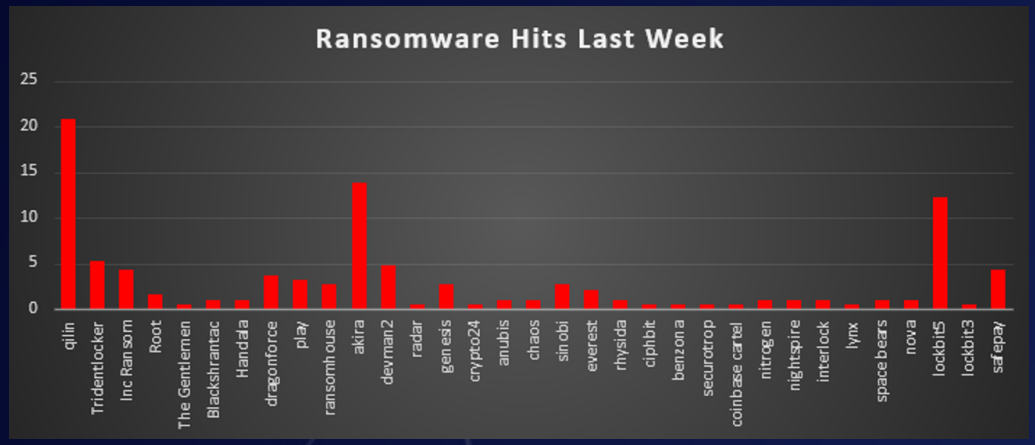


Figure 1: Ransomware Group Hits Last Week

LockBit 5.0

LockBit 5.0 is the newest iteration of the long-running LockBit RaaS operation and represents a major upgrade rather than a simple version bump. First seen in September 2025, this version expands LockBit's cross-platform focus with hardened payloads for Windows, Linux, and ESXi, supported by a more stealth-capable loader and extensive anti-analysis mechanisms.

The malware uses heavy packing, encrypted strings, dynamic API hashing, and process hollowing to avoid EDR visibility. Its two-stage execution model, where a loader injects the encryptor into defrag.exe, allows near fileless deployment, making detection significantly harder. LockBit 5.0 also patches ETW logging, reloads clean copies of system DLLs to defeat EDR hooks, and kills over 60+ security and backup services during execution.

Encrypted files receive a random 16-character extension, making automated recovery more difficult. The ransomware drops a ransom note (typically ReadMeForDecrypt.txt) directing victims to Tor negotiation portals and the LockBit leak site. This version continues to avoid execution on Russian / CIS language systems, consistent with LockBit's origin.

LockBit 5.0's resurgence follows the gang's internal leak in early 2025 and law-enforcement pressure under Operation Cronos. Despite setbacks, this version demonstrates the group's enhanced technical sophistication, faster encryption engine, and a more aggressive affiliate ecosystem.

Detailed TTPs (Short)

Initial Access

- Delivered by affiliates via phishing, unpatched public-facing apps, or compromised RDP/VPN credentials.
- Attackers establish persistence, escalate privileges, then manually deploy the payload.

Execution & Payload

- Two-stage loader injects the encryptor into defrag.exe for stealthy execution.
- Supports invisible/visible modes, selective encryption, delays, and network-wide targeting.
- Uses XChaCha20 + Curve25519 for fast and strong encryption across Windows, Linux, and ESXi.

Privilege Escalation & Lateral Movement

- Affiliates dump credentials (LSASS/SAM) using Mimikatz, ProcDump, or built-in Windows utilities.
- Spread using PsExec, SMB admin shares, PowerShell remoting, WMI, or GPO startup scripts.

Defence Evasion

- Packed/obfuscated loader, encrypted strings, dynamic API hashing.
- Unhooks security DLLs, patches ETW to kill event logging, deletes shadow copies, wipes logs.
- Skips Russian/CIS systems based on locale.

Collection & Exfiltration

- Uses StealBit or Rclone to exfiltrate sensitive data before encryption.
- Large outbound HTTPS/uploads to attacker infrastructure or cloud storage.

Impact

- Encrypts local and network data; ESXi variant can knock out entire VM clusters.
- Appends random 16-char extensions; drops ReadMeForDecrypt.txt.
- Deletes backups, shadow copies, and disables security tools to maximise impact.

MITRE ATT&CK TTPs:

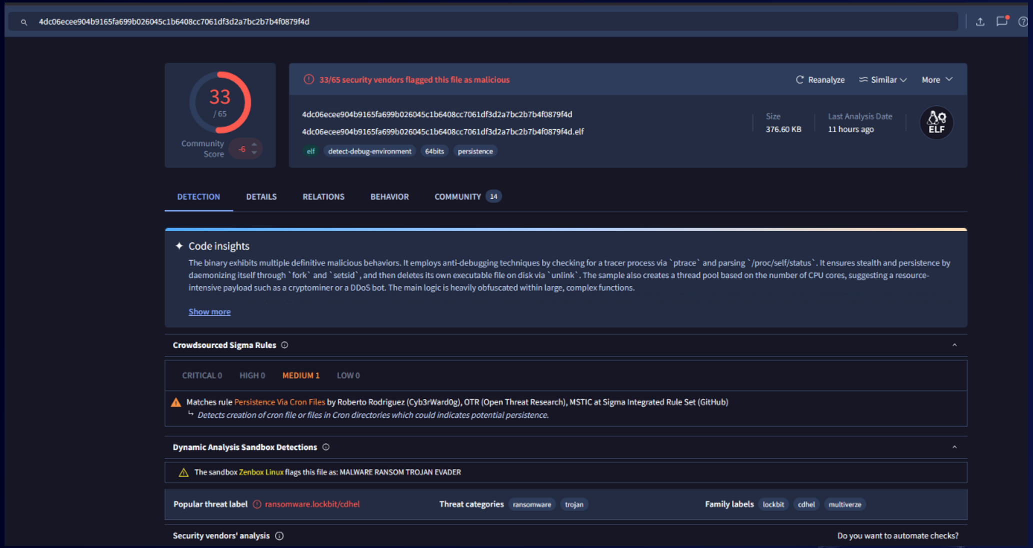
Tactic	Technique	ID	Summary
Initial Access	Phishing, Exploit Public-Facing Apps, Valid Accounts	T1566 / T1190 / T1078	Affiliates use emails, vulnerable VPN/servers, or stolen RDP/VPN creds.
Execution	PowerShell/MSHTA, Process Hollowing (defrag.exe)	T1059 / T1055.012	Fileless loader injects encryptor into trusted processes.
Persistence	None (operationally deployed once)	—	Attackers persist manually; LockBit itself doesn't.
Privilege Escalation	Credential Dumping, Valid Accounts	T1003 / T1078	LSASS/SAM dump domain admin mass deployment.
Defence Evasion	Obfuscation, API Hashing, Unhooking, ETW Patch, Kill Security Tools	T1027 / T1562	Loader heavily obfuscated; system telemetry disabled.
Credential Access	LSASS dumping	T1003	Tooling used pre-deployment for lateral movement.
Discovery	Network Share Discovery	T1135	Prepare for broad encryption.
Lateral Movement	PsExec, WMI, SMB	T1021 / T1047	Rapid spread across domain.
Collection	Data staging before exfiltration	T1560	Archives created pre-encryption.
Exfiltration	Rclone / StealBit to cloud or attacker infra	T1567	Data stolen for double extortion.
Impact	Encrypt Data, Inhibit Recovery	T1486 / T1490	XChaCha20 encryption + deletion of backups.

Indicators of Compromise (IOCs)

Malware Hashes

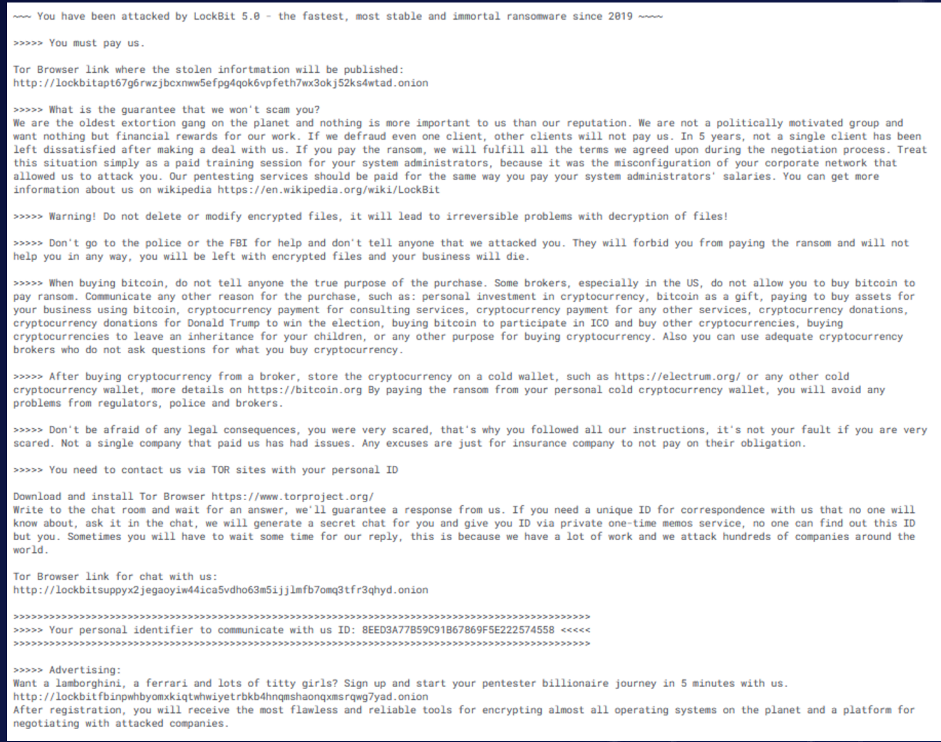
Known LockBit 5.0 samples include:

- 7ea5afbc166c4e23498aa9747be81ceaf8dad90b8daa07a6e4644dc7c2277b82
- 180e93a091f8ab584a827da92c560c78f468c45f2539f73ab2deb308fb837b38
- 4dc06ecee904b9165fa699b026045c1b6408cc7061df3d2a7bc2b7b4f0879f4d
- 90b06f07eb75045ea3d4ba6577afc9b58078eafeb2cdd417e2a88d7ccf0c0273
- 98d8c7870c8e99ca6c8c25bb9ef79f71c25912fbb65698a9a6f22709b8ad34b6



Ransom Notes

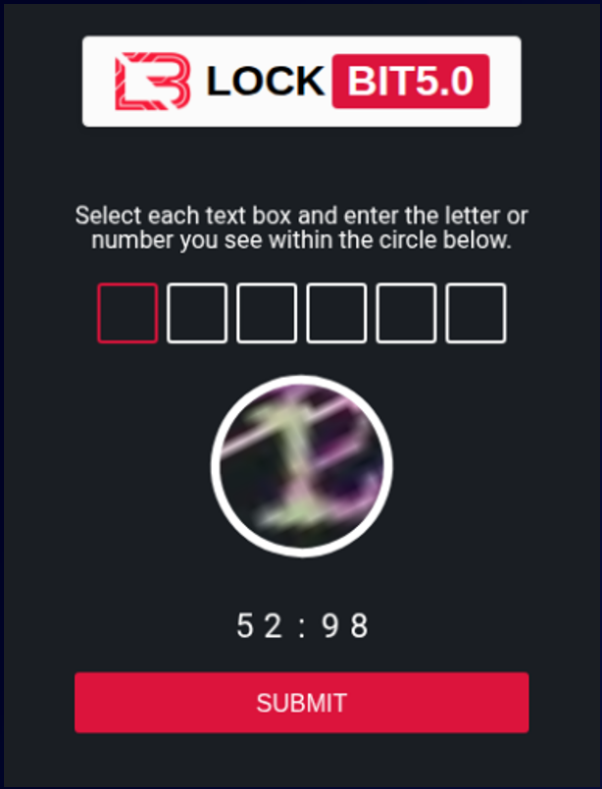
- ReadMeForDecrypt.txt



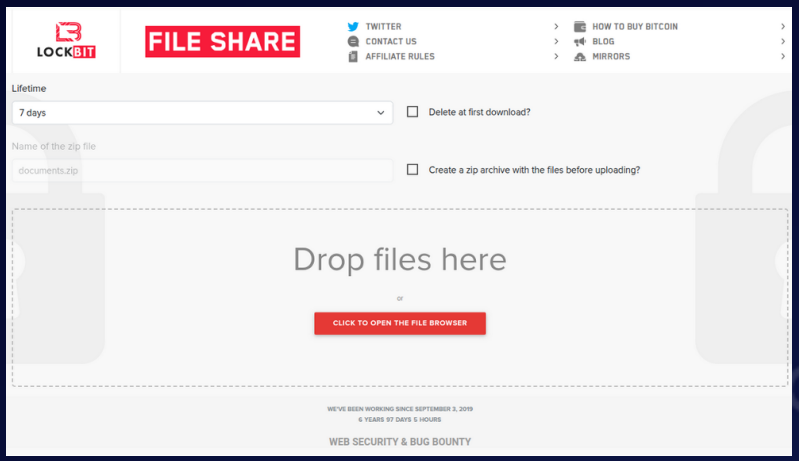
```
~~~ You have been attacked by LockBit 5.0 - the fastest, most stable and immortal ransomware since 2019 ~~~~

>>>>> You must pay us.

Tor Browser link where the stolen infortmation will be published:
http://lockbitapt67g6rwzjbcxnww5efpg4qok6vpfeth7wx3okj52ks4wtad.onion

>>>>> What is the guarantee that we won't scam you?
We are the oldest extortion gang on the planet and nothing is more important to us than our reputation. We are not a politically motivated group and
want nothing but financial rewards for our work. If we defraud even one client, other clients will not pay us. In 5 years, not a single client has been
left dissatisfied after making a deal with us. If you pay the ransom, we will fulfill all the terms we agreed upon during the negotiation process. Treat
this situation simply as a paid training session for your system administrators, because it was the misconfiguration of your corporate network that
allowed us to attack you. Our pentesting services should be paid for the same way you pay your system administrators' salaries. You can get more
information about us on wikipedia https://en.wikipedia.org/wiki/LockBit

>>>>> Warning! Do not delete or modify encrypted files, it will lead to irreversible problems with decryption of files!

>>>>> Don't go to the police or the FBI for help and don't tell anyone that we attacked you. They will forbid you from paying the ransom and will not
help you in any way, you will be left with encrypted files and your business will die.

>>>>> When buying bitcoin, do not tell anyone the true purpose of the purchase. Some brokers, especially in the US, do not allow you to buy bitcoin to
pay ransom. Communicate any other reason for the purchase, such as: personal investment in cryptocurrency, bitcoin as a gift, paying to buy assets for
your business using bitcoin, cryptocurrency payment for consulting services, cryptocurrency payment for any other services, cryptocurrency donations,
cryptocurrency donations for Donald Trump to win the election, buying bitcoin to participate in ICO and buy other cryptocurrencies, buying
cryptocurrencies to leave an inheritance for your children, or any other purpose for buying cryptocurrency. Also you can use adequate cryptocurrency
brokers who do not ask questions for what you buy cryptocurrency.

>>>>> After buying cryptocurrency from a broker, store the cryptocurrency on a cold wallet, such as https://electrum.org/ or any other cold
cryptocurrency wallet, more details on https://bitcoin.org By paying the ransom from your personal cold cryptocurrency wallet, you will avoid any
problems from regulators, police and brokers.

>>>>> Don't be afraid of any legal consequences, you were very scared, that's why you followed all our instructions, it's not your fault if you are very
scared. Not a single company that paid us has had issues. Any excuses are just for insurance company to not pay on their obligation.

>>>>> You need to contact us via TOR sites with your personal ID

Download and install Tor Browser https://www.torproject.org/
Write to the chat room and wait for an answer, we'll guarantee a response from us. If you need a unique ID for correspondence with us that no one will
know about, ask it in the chat, we will generate a secret chat for you and give you ID via private one-time memos service, no one can find out this ID
but you. Sometimes you will have to wait some time for our reply, this is because we have a lot of work and we attack hundreds of companies around the
world.

Tor Browser link for chat with us:
http://lockbitsuppyx2jegaoyiw44ica5vdho63m5ijjlmfb7omq3tfr3qhyd.onion

>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>
>>>>> Your personal identifier to communicate with us ID: 8EED3A77B59C91B67869F5E222574558 <<<<<
>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>

>>>>> Advertising:
Want a lamborghini, a ferrari and lots of titty girls? Sign up and start your pentester billionaire journey in 5 minutes with us.
http://lockbitfbinpwhbyomxkiqtwhwiyetrbkb4hnqmshaonqxmsrqwg7yad.onion
After registration, you will receive the most flawless and reliable tools for encrypting almost all operating systems on the planet and a platform for
negotiating with attacked companies.
```

File Extensions
- Random 16-character extensions (unique per infection).

Onion Infrastructure
- LockBit 5.0 Support/Chat: lockbitsuppyx2jegaoyiw44ica5vdho63m5ijjlmfb7omq3tfr3qhyd.onion
- Affiliate Panel: lockbitfbinpwhbyomxkiqtwhwiyetrbkb4hnqmshaonqxmsrqwg7yad.onion



- Leak Site: lockbitapt67g6rwzjbcxnww5efpg4qok6vpfeth7wx3okj52ks4wtad.onion
- Data Storage Server: lockbitfss2w7co3ij6am6wox4xcurtgwukunx3yubcoe5cbxiqakxqd.onion



Tox
3085B89A0C515D2FB124D645906F5D3DA5CB97CEBEA975959AE4F95302A04E1D14E41080A105

Crystal Eye 5.5 Mitigation

1. Secure External Access
   - Enforce MFA on RDP/VPN; patch exposed apps; block legacy protocols.
2. 2. Privilege Management
   - Rotate admin/MSP creds; disable unused accounts; monitor privilege escalation in CE SIEM.
3. Backup & Recovery Protection
   - Use offline/immutable backups; restrict access to backup servers; detect shadow-copy deletion.
4. Execution Control
   - CEASR: block unknown binaries from %TEMP%, %APPDATA%; restrict PsExec and WMI remoting.
5. Exfiltration & Tor Detection
   - Monitor large outbound uploads; block Tor entry nodes and LockBit Onion domains.
6. Endpoint Hardening
   - Enable EDR tamper protection; enforce Sysmon-style logging; monitor suspicious defrag.exe behaviour.
7. Network Segmentation
   - Isolate AD, ESXi hosts, file servers, and critical infra.
8. IR Playbook
   - Automate SOAR actions for LockBit IOCs; isolate hosts; block hashes/Onion URLs; rotate credentials.

Worldwide Ransomware Victims

The United States overwhelmingly dominated this week's ransomware landscape, accounting for 59.89% of all identified victims. This level of concentration again confirms that the US is the primary hunting ground for most major ransomware operations, driven by its large enterprise footprint, higher disclosure rates, and the perceived willingness/ability of victims to pay.

Canada (5.88%) emerged as the second most impacted country, placing it firmly behind the U.S. but still in a clearly high-risk bracket. Together, the US and Canada represented over 65% of all observed victims, underlining how strongly threat actors continue to prioritize North American targets.

A notable mid-tier group included Germany (4.28%), Australia (3.21%), and Italy (combined 3.20%), followed by France and the United Kingdom (each 2.14%). These mature economies consistently appear in victim datasets, reflecting both sizable digital infrastructures and regular reporting of incidents.

Below this, a broader band of activity was seen across China, Malaysia, and Brazil (each 1.60%), with Taiwan, Vietnam, Switzerland, Portugal, Singapore (each 1.07%), and Newer single-digit presences like Argentina, Indonesia, Israel, Philippines, Jordan, Sweden, Belgium, Japan, Peru, Croatia, Spain, Thailand, Barbados, Mexico, Zambia, Egypt, and India (each 0.53%) forming the long tail. While these countries show relatively low individual volumes, their combined footprint reinforces a key trend: ransomware remains a global problem, with opportunistic and campaign-driven attacks touching almost every region rather than being confined to a small set of geographies.

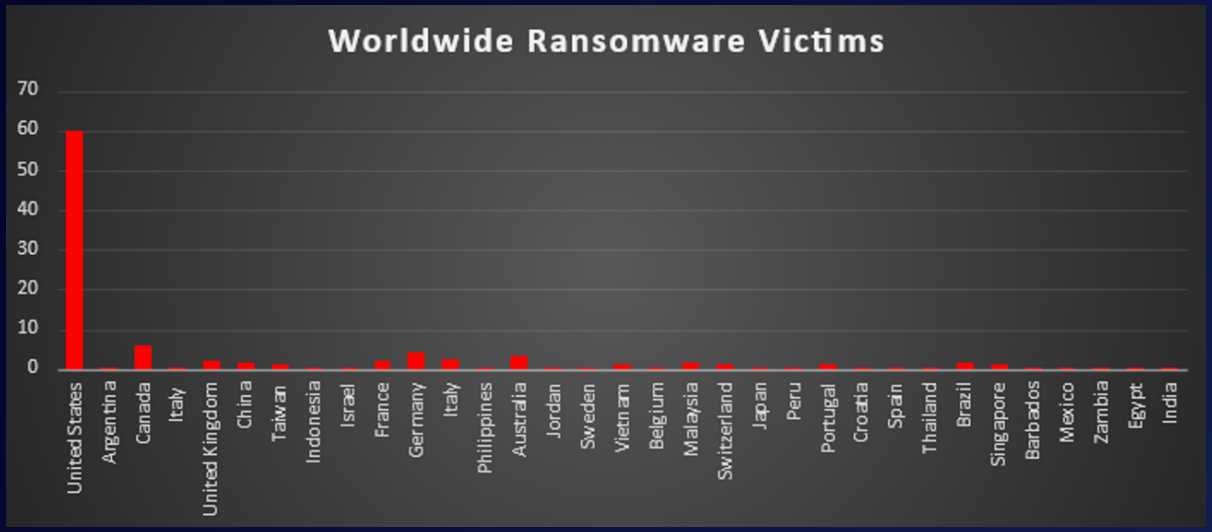


Figure 6: Ransomware Victims Worldwide

Industry-wide Ransomware Victims

Manufacturing remained the most heavily targeted sector this week, accounting for 18.18% of all identified ransomware victims. This keeps it firmly at the top of the risk ladder, reflecting how production-critical environments and supply-chain dependencies continue to make manufacturers highly attractive extortion targets.

A strong second tier was formed by Construction (13.9%), Business Services (12.83%), and Retail (9.63%). Together, these industries represent a broad mix of project-driven, service-oriented, and consumer-facing organisations, all of which handle high-value contracts, payments, and operationally sensitive timelines that ransomware operators routinely exploit to increase leverage during negotiations.

A diverse mid-band followed with Law Firms and IT (each 5.35%), Hospitality (4.81%), Education and Finance (each 3.74%), and Energy and Transportation (each 3.21%), supported by Electronics and Federal entities (each 2.67%), as well as Real Estate and Telecommunications (each 2.14%). This layer underscores that both private and public sectors — from legal and professional services to infrastructure, government, and critical business operations — remain regular fixtures in victim disclosures.

Lower-volume but still active verticals included Insurance (1.6%), and Media & Internet, Healthcare, and Consumer Services (each 1.07%), with Minerals & Mining and general Organisations (each 0.53%) forming the long tail. While individually small, this distribution shows that ransomware activity is not confined to a handful of headline sectors; nearly any industry with digitised operations and monetisable data remains within the threat envelope. (One entry labelled “Peru” appears to be a misclassified data point and is not treated as a separate industry in this breakdown.)

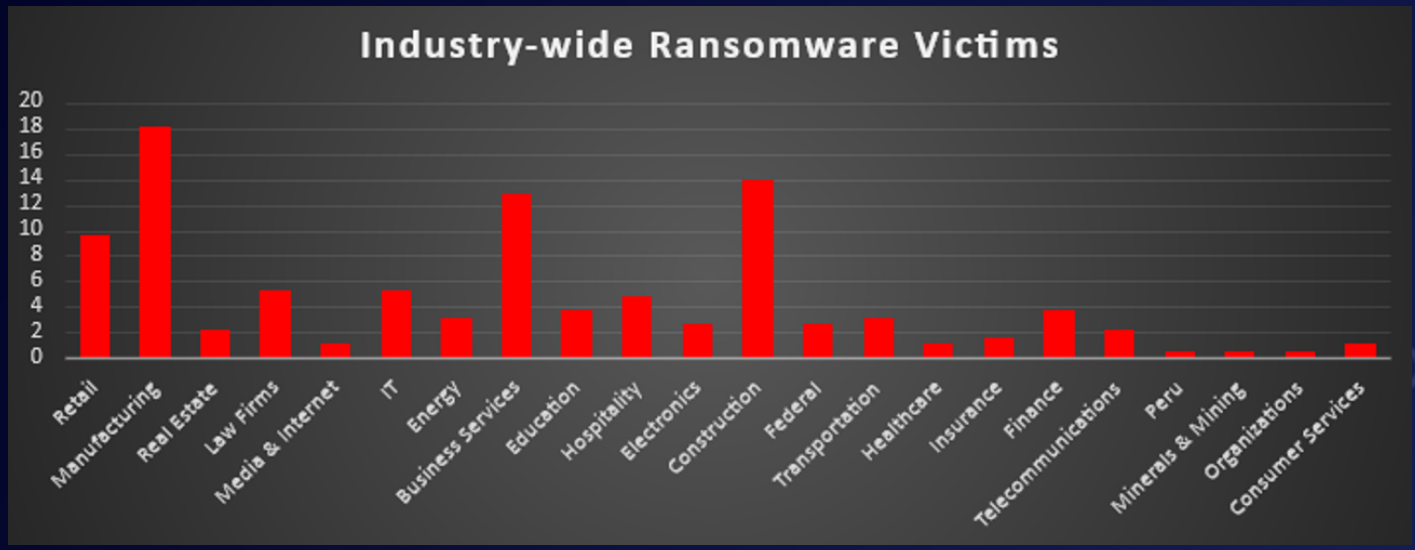


Figure 7: Industry-wide Ransomware Victims