Red Piranha
unified threat management

THREAT INTELLIGENCE REPORT

Aug 12 - 18, 2025

Report Summary:

- **New Threat Detection Added**
  - CastleLoader
  - Vidar Stealer

- **Detection Summary**
  - **Threat Protections integrated into the Crystal Eye - 67**
  - **Newly Detected Threats - 4**

The following threats were added to Crystal Eye this week:

1. CastleLoader

CastleLoader distributes various kinds of malware, such as info-stealers and RATs, through Cloudflare-themed ClickFix attacks. They also use fake GitHub repositories that are masqueraded as legitimate applications.

CastleLoader first appeared in early 2025 and has quickly evolved into a formidable foe. CastleLoader has deployed numerous C2 servers, which resulted in nearly 500 successful infections. Most of these infections were of critical targets, including government entities.

Threats Protected: 5
Class Type: 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
Initial Access	T1566	Phishing
Execution	T1059.001	Command and Scripting Interpreter - PowerShell
Command-and-Control	T1071.001	Application Layer Protocol – Web protocols
Exfiltration	T1020	Automated Exfiltration

2. Vidar Stealer

Vidar is an info-stealer-based malware. It collects a variety of sensitive information from an infected device, including OS Data, browser history, cookies, and stored credentials. It also looks for payment details such as Credit Card data.
Vidar Stealer also sells access to infected machines to ransomware gangs for profit and further compromise.

Threats Protected: 3
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

Current Threat Summary

Known exploited vulnerabilities (Week 3 August 2025)

Vulnerability	CVSS	Description
N-able N-Central	9.4 (Critical)	N-able N-Central contains a vulnerability that can allow an authenticated remote attacker to execute operating system commands, which can result in the ability to gain access to the system.
N-able N-Central	9.4 (Critical)	N-able N-Central contains a deserialization vulnerability that can allow an authenticated remote attacker to execute code, which can result in an attacker gaining access to the system.
RARLAB WinRAR	8.4 (High)	RARLAB WinRAR contains a vulnerability that affects the Windows versions of the software, WinRAR, UnRAR, and UnRAR.dll. This vulnerability relates to how the software handles alternative data streams and can enable files to be written to an unintended location via path traversal, resulting in the execution of arbitrary code upon opening a malicious archive.
Microsoft Office	8.8 (High)	Microsoft Office Excel contains a vulnerability that can allow an unauthenticated remote attacker to execute arbitrary code via a specially crafted Excel file. This vulnerability affects Microsoft Excel 2000, XP, 2003, and 2004 for Mac, and may impact additional Office products.
Microsoft Internet Explorer	8.8 (High)	Microsoft Internet Explorer contains a memory corruption vulnerability that can allow an unauthenticated remote attacker to execute code via JavaScript, exploitation of this vulnerability can occur upon visiting a website containing the malicious code.

For more information, please visit the **Red Piranha Forum**:
https://forum.redpiranha.net/t/known-exploited-vulnerabilities-catalog-2nd-week-of-august-2025/586

Updated Malware Signatures (Week 3 August 2025)

Threat	Description
XWorm	A Remote Access Trojan (RAT) and malware loader that's commonly used in cyberattacks to give attackers full remote control over a victim's system. It's part of a growing trend of commercialised malware sold or rented on dark web forums, often under the guise of a "legitimate tool."
zgRAT	A Remote Access Trojan (RAT) used in cyberattacks that provides attackers with remote access to a machine. Commonly spread in malware loaders and through phishing emails.

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 Victims – Weekly Overview

Qilin dominated the ransomware landscape this week, accounting for 21.3% of all reported incidents. Its aggressive campaigns reflect ongoing operations against diverse industries and geographies, consolidating its role as one of the most persistent actors.

Play and Sinobi both followed closely at 10.19% each, highlighting their growing foothold in the ransomware ecosystem. Their simultaneous rise suggests coordinated or opportunistic campaigns across multiple regions.

Akira was also prominent, responsible for 8.33% of cases. This group continues to build momentum through disruptive operations targeting organisations with weaker endpoint protections.

Everest and SafePay each registered 6.48%, marking them as significant mid-tier players. Both groups have maintained consistent activity in recent weeks, often striking smaller enterprises and critical supply chain partners.

Cloak contributed 4.63%, and Inc Ransom accounted for 3.7%, underscoring their steady, targeted campaigns. Meanwhile, Interlock, Direwolf, and Beast each logged 2.78%, showing renewed attention from these actors after quieter periods.

Several other groups, including Rhysida, Worldleaks, Weyhro, Crypto24, Anubis, and Team Underground, hovered at 1.85% each, signalling diversified activity across mid-tier ransomware families.

Finally, Bqtlock, Medusa, Lynx, D4rk4rmy, Arcus Media, J Group, Apos, Datacarry, Sarcoma, and Handala each represented 0.93% of incidents, demonstrating that smaller and emerging ransomware variants continue to probe for opportunities and expand their footprint.

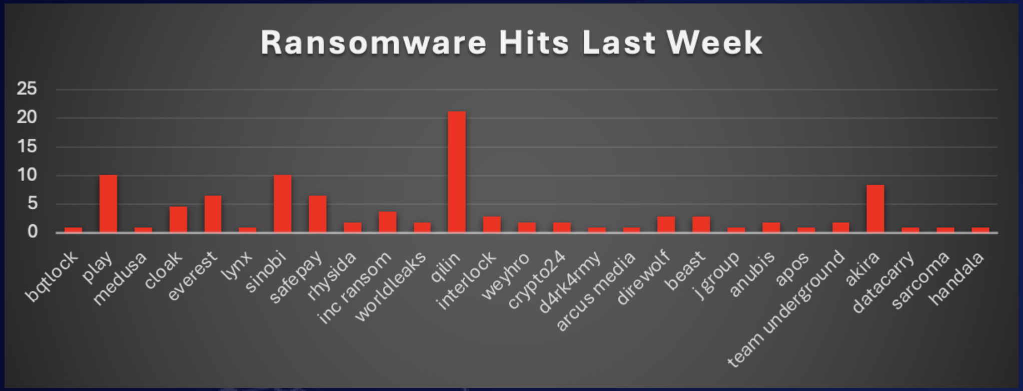


Figure 1: Ransomware Group Hits Last Week

SINOBI Ransomware

SINOBI is a mid-2025 extortion outfit that operates primarily as a data-broker (steal-and-leak), while some reports also note an encrypting variant that drops a README.txt ransom note and may append .SINOBI to files. The crew runs multiple Tor leak and chat portals and occasionally uses clearnet "mirror" sites for victim onboarding, but their core infrastructure is Tor-only, so reliable public C2 IPs are uncommon. Targeting appears broad across sectors, with initial access likely via stolen credentials or phishing, followed by bulk collection, archiving, and exfiltration to their services before public shaming on the leak site. Detection tends to focus on .onion portal access, ransom-note artefacts, and unusual archiving/egress activity rather than fixed IPs.

Detailed TTPs & ATT&CK mappings

Initial Access

- Valid Accounts (T1078) – Assessed: Data-broker operations frequently originate from stolen credentials or IAB hand-offs; several affected org types (insurance, construction, education) match typical cred-abuse targeting
- Phishing (T1566) – Assessed: Common precursor to mailbox or VPN compromise; no SINOBI-specific phishing kit is public yet.

Discovery / Collection

- Email Collection (T1114) – Assessed: Victim sectors and extortion narratives suggest mailbox and file-share scraping pre-leak.
- Archive Collected Data (T1560.001) – Bundling data before transfer and proof-packs is standard; ransom notes reference negotiation portals post-collection.

Exfiltration

- Exfiltration Over Web Service (T1567) – Use of Tor file servers/DLS and occasional third-party shares during negotiations (pattern seen across brokers).
- Exfiltration Over C2 Channel (T1041) – Transfer to SINOBI-controlled .onion endpoints observed (DLS and possible file areas).

Command-and-Control / Comms

- Proxy/Anonymity Networks: Tor (T1090.003) – All public infra (DLS, login/chat) is Tor-only; no validated clearnet C2 IPs during the window.

Impact / Extortion

- Data Exposure & Coercion (TA0040 / T1657) – Primary effect is publication pressure via DLS; WatchGuard lists Direct/Double/Free leak modalities. Confidence: High. WatchGuard
- File Encryption (T1486) – Contested: Some reports on a malware called "Sinobi" show encryption (.SINOBI, README.txt) and Tor-chat negotiation; not consistently evidenced across Aug 11–17 postings.

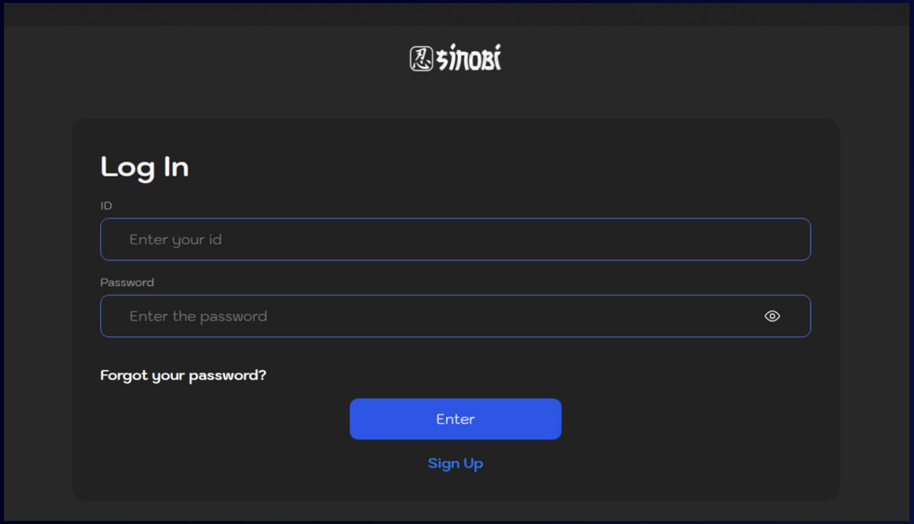
MITRE ATT&CK Matrix

Tactic	Technique	How it shows up for SINOBI this week	Confidence / Evidence
Initial Access	T1078 Valid Accounts	Likely stolen creds/IAB; sector mix & lag to claims typical for brokers	Medium (pattern)
Initial Access	T1566 Phishing	Plausible path to creds; no kit published	Low-Med (analogue)
Discovery	(General)	Enumeration of shares/mailboxes before exfil	Low (inferred)
Collection	T1114 Email Collection	Mailbox/file scraping ahead of leak	Medium (pattern + sectors)
Collection	T1560.001 Archive Data	Bundled "proof" and dumps	Medium (ransom note flow)
Exfiltration	T1567 Over Web Service	Uploads to Tor DLS/files; occasional 3rd-party shares	High
Exfiltration	T1041 Over C2	Movement to SINOBI onion infra	Med-High
C2/Comms	T1090.003 Tor	DLS and chat portals on .onion only	High
Impact	TA0040/T1657 Data Exposure	Leak-led extortion; "Direct/Double/-Free"	High
Impact	T1486 Encryption	.SINOBI extension, README.txt (contested vs. group tracker)	Low-Med

IOCs

Leak/DLS onions (7)

sinobi6ftrg27d6g4sjdt65malds6cfptlnjyw52rskakqjda6uvb7yd.onion,
sinobi6rlec6f2bgn6rd72xo7hvds4a5ajiu2if4oub2sut7fg3gomqd.onion,
sinobi6ywgmmvg2gj2yygkb2hxbimaxpqkyk27wti5zjwhfcldhackid.onion,
sinobi7l3wet3uqn4cagjiessuomv75aw3bvgah4jpj43od7xndb7kad.onion,
sinobi7sukclb3ygtorysbtrodgdbnrmgbhov45rwzipubbzhiu5jvqd.onion,
sinobi23i75c3znmqqxxyuzqvhxnjsar7actgvc4nqeuhgcn5yvz3zqd.onion,
sinobia6mw6ht2wcdjphessyzpy7ph2y4dyqbd74bgobgju4ybytmkqd.onion.


Log In

ID

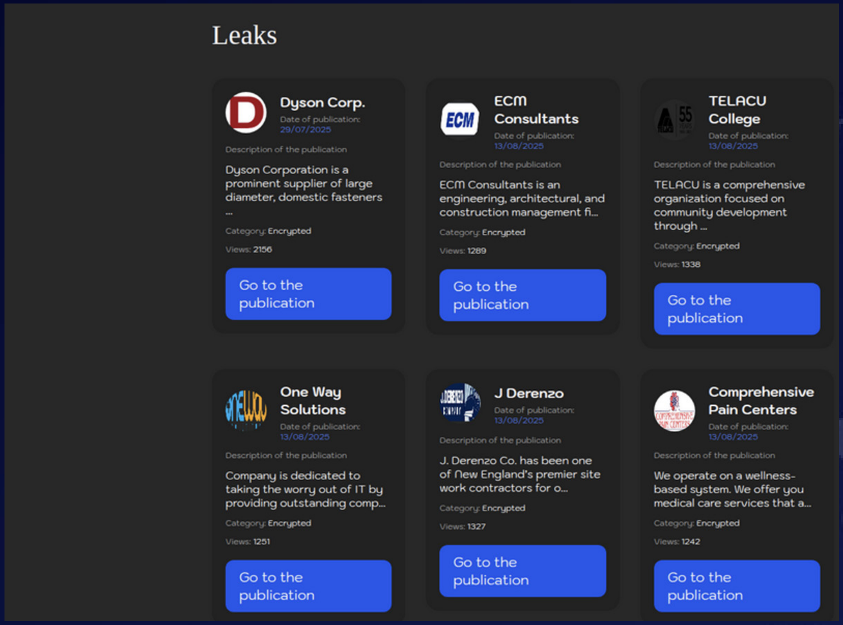
Enter your id

Password

Enter the password

Chat/negotiation onions (7)

sinobi7yuoppj76qnkwiobwfc2qve2xkv2ckvzyyjblwd7ucpptl62ad.onion/login,
sinobi57mfegeov2naiufkidlkpze263jtbldokimfjqmk2mye6s4yqd.onion/login,
sinobibdvzohujkliofkxiz3ueyedfh6bed2lzjz2z6pafw5jeoptsid.onion/login,
sinobibjqytwqxjw24zuerqcjyd3hoow6zia7z6kzvwawivamu7nqayd.onion/login,
sinobicrh73ongfuxjajmlyyhalvkhlcgttxkxaxz3gvsgdcgf76uiqd.onion/login,
sinobidxodgt4jsr3tlmf2rr4okjvvwfp5gh3lrqxnowomcx62ssrhqd.onion/login,
sinobiea4snfqtkc43paumapo4oi7vxcy5vjzfoalunsnvzehozfhpyd.onion/login


Leaks

Dyson Corp.
Date of publication: 29/07/2025
Description of the publication
Dyson Corporation is a prominent supplier of large diameter, domestic fasteners ...
Category: Encrypted
Views: 2156

ECM Consultants
Date of publication: 13/08/2025
Description of the publication
ECM Consultants is an engineering, architectural, and construction management fi...
Category: Encrypted
Views: 1289

TELACU College
Date of publication: 13/08/2025
Description of the publication
TELACU is a comprehensive organization focused on community development through ...
Category: Encrypted
Views: 1338

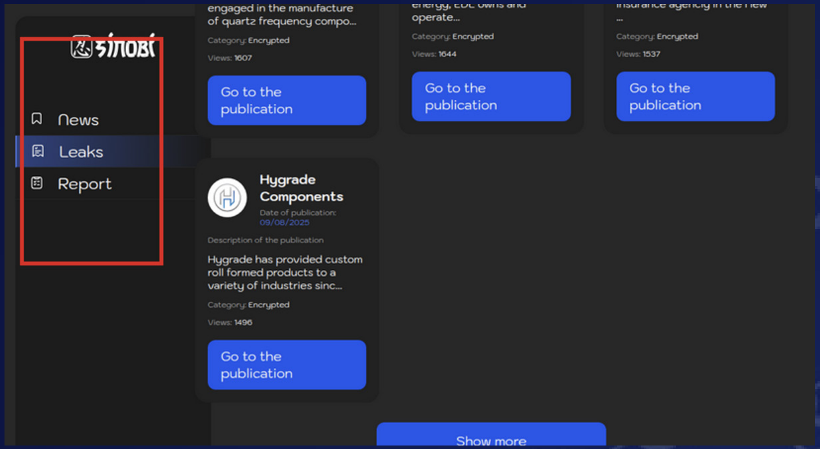
One Way Solutions
Date of publication: 13/08/2025
Description of the publication
Company is dedicated to taking the worry out of IT by providing outstanding comp...
Category: Encrypted
Views: 1251

J Derenzo
Date of publication: 13/08/2025
Description of the publication
J. Derenzo Co. has been one of New England's premier site work contractors for o...
Category: Encrypted
Views: 1327

Comprehensive Pain Centers
Date of publication: 13/08/2025
Description of the publication
We operate on a wellness-based system. We offer you medical care services that a...
Category: Encrypted
Views: 1242

Clearnet mirrors:

blog.sinobi.us.org,
chat.sinobi.us.org,
cdn.sinobi.us.org.


engaged in the manufacture of quartz frequency compo...
Category: Encrypted
Views: 1607

operate...
Category: Encrypted
Views: 1644

...
Category: Encrypted
Views: 1537

Hygrade Components
Date of publication: 09/08/2025
Description of the publication
Hygrade has provided custom roll formed products to a variety of industries sinc...
Category: Encrypted
Views: 1496

Mitigation with CE 5.0

Email & Identity

- Enforce MFA on VPN/O365/SSO; monitor for unusual OAuth grants and inbox rule creation (T1078/T1114).
- Phishing controls & sandboxing for archive-type attachments; auto-quarantine suspicious ZIP/ISO/TAR.

Endpoint / EDR

- HIPS rules for mass archiving and Tor client execution; detect large file reads from shares followed by compression (T1560/T1567).
- If encryption behaviour is suspected at a site, enable canaries and file-rename heuristics (*.SINOBI).

Network / Proxy / DNS

- Block/alert on .onion in SNI/Host/URI and common tor2web domains (T1090.003, T1567).
- Restrict outbound to approved destinations; instrument UEBA for abnormally large egress.

Backups & DR

- Maintain immutable/offline backups; quarterly restore tests for high-value datasets.

Worldwide Ransomware Victims

The United States continues to dominate as the most heavily impacted country, reporting 56.48% of all global ransomware victims this week. This figure reaffirms its position as the top target for ransomware operators, largely due to its expansive digital infrastructure, higher ransom payment capabilities, and the large number of enterprises across critical industries.

Germany follows with 6.48%, reflecting its strong industrial and manufacturing base, which remains attractive to cybercriminals. The United Kingdom and Australia each account for 5.56%, underscoring their recurring exposure to ransomware incidents targeting sectors like finance, healthcare, and education.

Canada contributes 1.85% of total victims, similar to Poland's 1.85%, indicating steady but moderate targeting. France and South Korea both stand at 2.78%, pointing to the continued pressure on European and Asian economies. Italy also registered 2.78%, reflecting ongoing attacks against its growing digital ecosystem.

Other notable entries include Turkey, The Netherlands, Brazil, Thailand, Belgium, Israel, and several smaller economies such as Luxembourg, Algeria, Morocco, and the United Arab Emirates, each reporting 0.93% of global cases. While individually minor, these incidents highlight the wide geographic spread of ransomware campaigns.

Overall, ransomware activity remains highly concentrated in Western economies but demonstrates persistent global reach, with incidents affecting North America, Europe, Asia, the Middle East, and Africa alike.

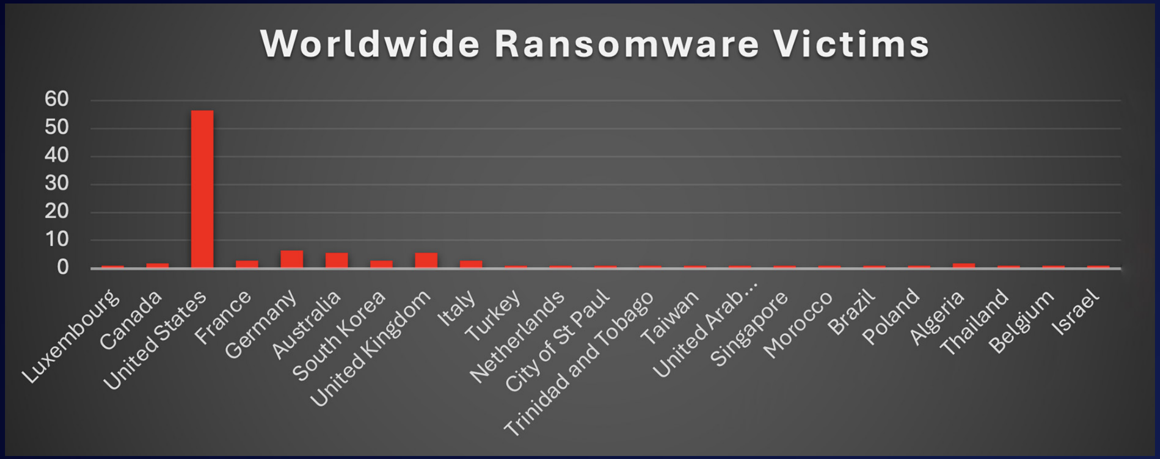


Figure 5: Ransomware Victims Worldwide

Industry-wide Ransomware Victims

Business Services lead this week's ransomware tally, accounting for 17.59% of total incidents. Their broad role as intermediaries for IT, consulting, and operational support makes them a lucrative entry point into multiple industries at once.

Manufacturing follows closely at 14.81%, reflecting the sector's critical role in supply chains. Attackers continue exploiting operational technology (OT) dependencies, legacy systems, and the fact that downtime here translates into severe financial and logistical disruptions.

Retail reported 12.04% of incidents, highlighting the sector's ongoing vulnerability due to widespread point-of-sale systems, digital payment ecosystems, and customer data repositories.

Construction saw 10.19%, driven by decentralised vendor management and project-based IT setups, making consistent security controls a challenge.

Hospitality was hit with 8.33%, reflecting attackers' preference for guest management systems, payment data, and 24/7 operations that leave little room for system shutdowns.

Law Firms accounted for 5.56%, showing consistent targeting due to their sensitive client records, legal filings, and case data with high extortion potential.

Finance came in at 4.63%, as ransomware actors seek to leverage immediate liquidity pressure on financial institutions to force faster payouts.

Education, IT, and Transportation each logged 3.7%, sectors that rely heavily on digital infrastructure but often have mixed security maturity levels.

Real Estate and Consumer Services followed with 2.78% apiece, both handling critical customer data yet often lagging in robust cyber defences.

Federal, Energy, Insurance, Agriculture, and Minerals & Mining each reported 1.85%, underlining that even heavily regulated or resource-driven sectors are not immune.

Finally, Telecommunications accounted for 0.93%, a reminder that while large telecoms may have strong defences, niche operators remain vulnerable.

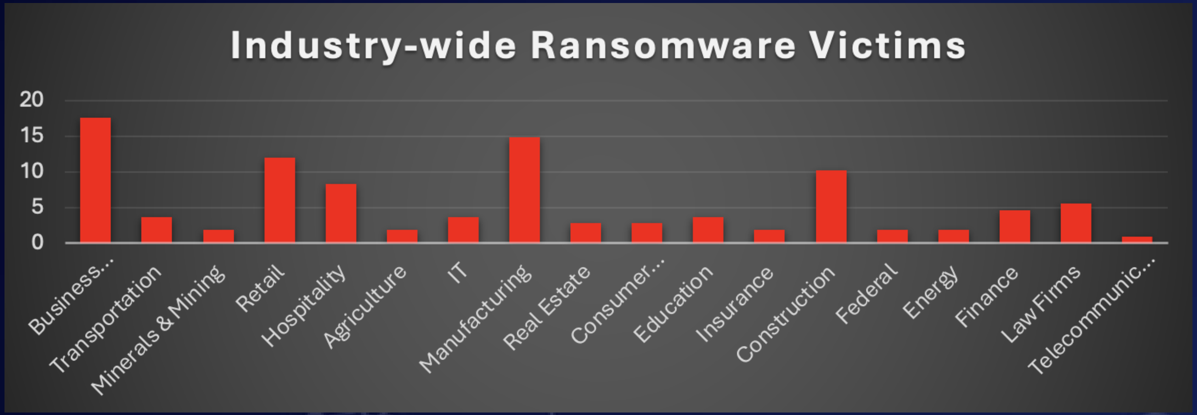


Figure 6: Industry-wide Ransomware Victims