Red Piranha
unified threat management

THREAT INTELLIGENCE REPORT

Nov 25 - Dec 01, 2025

Report Summary:

- **New Threat Detection Added**
  - LummaStealer
  - SocGholish
- **Detection Summary**
  - **Threat Protections integrated into the Crystal Eye - 54**
  - **Newly Detected Threats - 4**

The following threats were added to Crystal Eye this week:

1. LummaStealer

Lumma Stealer (a.k.a. Lumma or LummaC2) is part of an information stealer malware family in use since 2022. This is a Malware as a Service (MaaS) where stolen data is being sold on the dark web. This is being distributed through social engineering tactics, including phishing emails, fake CAPTCHA Challenges, and malicious links. LummaStealer also uses the Fake Update technique to get users to download or run malicious code/scripts.

Threats Protected: 16
Class Type: Malware
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
Collection	T1119	Automated Collection
Persistence, Privilege Escalation	T1547.001	Boot or Logon AutoStart Execution: Registry Run Keys / Startup Folder
Discovery	T1217	Browser Information Discovery
Execution	T1059.001	Command and Scripting Interpreter: PowerShell

2. SocGholish

SocGholish is a JavaScript-based loader malware that has been used since at least 2017. They are known for using fake software updates to trick users into gaining access to the system. If the user downloads and executes the alleged update, then the malware is installed on the computer. Once it is installed, the downloader can execute other types of malware, such as RAT and other malicious payloads.

Threats Protected: 6
Class Type: Malware
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
Execution	T1059.007	Command and Scripting Interpreter: JavaScript
Execution	T1047	Windows Management Instrumentation
Command-and-Control	T1102	Web Service
Execution	T1204.001	User Execution: Malicious Link
Discovery	T1033	System Owner/User Discovery

Current Threat Summary

Known exploited vulnerabilities (Week 4 November2025)

Vulnerability	CVSS	Description
CVE-2021-26829	5.4	OpenPLC ScadaBR contains a stored cross-site scripting vulnerability within the 'system_settings.shtm' component of the system and affects versions through 0.9.1 on Linux and through 1.12.4 on Windows. This vulnerability can allow an authenticated attacker to add malicious code, resulting in the code being executed upon visiting the page.

For more information, please visit the **Red Piranha Forum**:
https://forum.redpiranha.net/t/known-exploited-vulnerabilities-catalog-4th-week-of-november-2025/621

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 22.22% of all reported incidents. This made it the single most dominant operator in the ecosystem, indicating either a concentrated campaign window or a batch of delayed victim disclosures hitting in one go and pushing Qilin clearly ahead of all competitors.

A strong second tier was formed by Akira (15%), The Gentlemen (7.78%), DragonForce (7.22%), and Everest (6.67%), all of which sustained multi-industry targeting and regular leak-site publishing. Their combined footprint shows that, beyond a single dominant actor, multiple well-established crews are simultaneously running sizeable pipelines of intrusions and extortion cases.

A mid-tier cluster, Inc Ransom (5.56%), Sinobi (5%), Benzona (2.78%), Play (2.22%), and Rhysida (2.22%), maintained a steady operational tempo, combining data theft, double-extortion, and opportunistic targeting across regions. These crews did not individually rival Qilin or Akira but collectively represented a significant share of observed ransomware pressure.

Smaller yet persistent operators, including PayoutsKing, Nova, Nightspire, Root, and Embargo (each 1.67%), together with Worldleaks, Tengu, Interlock, SafePay, Coinbase Cartel, Medusa, Anubis, and KillSec3 (each 1.11%), contributed to the continuous background noise of the ecosystem. Their activity highlights how many mid-to-low-volume brands remain active at any given time.

At the long tail, low-frequency groups such as Lynx, Securotrop, Pear, Handala, Beast, RansomHouse, Chaos, 3AM, Ciphbit, Toufan, and Brotherhood (each 0.56%) appeared only sporadically but still added to the overall fragmentation and churn. While individually minor, their continued presence underlines the resilience and constant regeneration of the ransomware landscape.

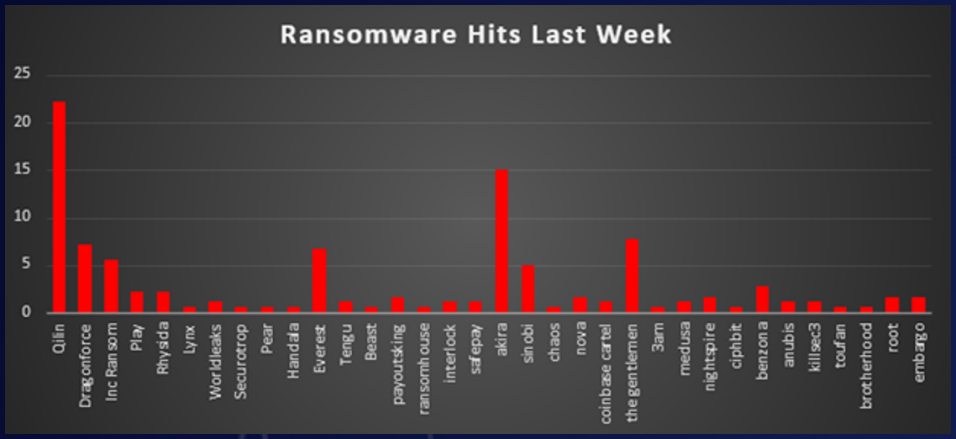


Figure 1: Ransomware Group Hits Last Week

Benzona Ransomware

Benzona is a newly emerged double-extortion ransomware group first observed in late November 2025. On 26 November 2025, the group simultaneously listed at least five victims on its Tor leak site, including multiple Romanian automotive dealerships (Suzuki, Mazda, Dacia in Ploiești) and a healthcare nonprofit in Côte d'Ivoire. This coordinated disclosure strongly suggests a shared entry vector or common third-party/supplier access across several related environments. Once inside a network, Benzona deploys a Windows ransomware payload that encrypts data and appends the extension .benzona to victim files (e.g. report.pdf report.pdf.benzona). A ransom note named RECOVERY_INFO.txt is dropped into affected directories to initiate the extortion phase.

The note tells victims their files have been encrypted and data exfiltrated, warns that manual recovery attempts may cause "irreversible data loss," and gives a 72-hour deadline to contact the operators via a Tor-based negotiation portal. A separate "News public" Onion URL is used as a leak blog where victims and stolen data are published if negotiations fail or payment is refused. In one documented incident, the actors demanded around USD 90,000 with a leak deadline four days after the breach. No free decryptor exists at the time of writing, and paying remains high-risk: as with other groups, there is no guarantee decryption or deletion of stolen data will actually occur.

Benzona follows a classic double-extortion model – enterprise environments are disrupted via encryption while large volumes of sensitive data (internal documents, financial records, emails, client data, etc.) are stolen to maximise pressure. Early victimology points to corporate targets in automotive, manufacturing, and healthcare, with at least ~200 GB of data claimed stolen in the Poliserv case alone. AV telemetry shows detections such as Ransom:Win32/Avaddon.P!MSR, hinting at code reuse or lineage from older ransomware families like Avaddon. The group operates a dedicated Tor leak site, a separate Tor chat portal for negotiations, and publishes a PGP key and Tox ID as alternative secure contact channels – behaviour consistent with a mature, well-organised ransomware operation.

Detailed TTPs (Short)

Initial Access

- Likely a mix of spear-phishing, exposed services (RDP/VPN/web apps) and/or compromised third-party platforms, which explains multiple related victims hit in one wave.
- Suspected use of valid credentials from an earlier compromise or password reuse.

Execution & Encryption

- Windows payload (~9–10 MB) runs on hosts, then enumerates local disks and shares.
- Encrypts data and appends .benzona, drops RECOVERY_INFO.txt with Tor links and a 72-hour deadline.
- Probably stops AV/backup services and deletes shadow copies before or during encryption.

Lateral Movement & Privilege Escalation

- Likely credential dumping on key servers (LSASS / SAM) and use of domain/admin accounts.
- Movement via RDP, SMB, and admin shares rather than noisy exploits.

Defence Evasion

- Packed/obfuscated binary to evade signatures.
- Attempts to disable security tools, logging and backup agents to slow detection and recovery.

Collection & Exfiltration

- Targets file servers and business shares; bundles large data sets into archives (tens–hundreds of GB).
- Exfiltrates over encrypted channels (HTTPS) to attacker infrastructure and/or cloud storage before triggering encryption.

Command-and-Control & Impact

- Uses Tor for negotiation and leak site; PGP/Tox as backup channels.
- Impact is classic double extortion: operational outage via encryption + regulatory and reputational damage via data theft and public leaks.

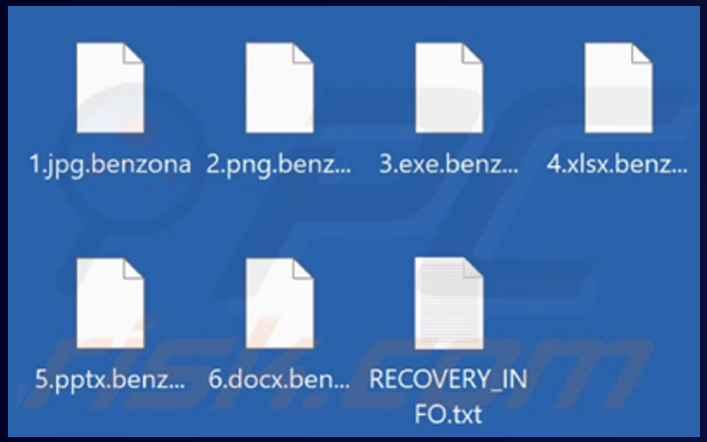
MITRE ATT&CK TTPs:

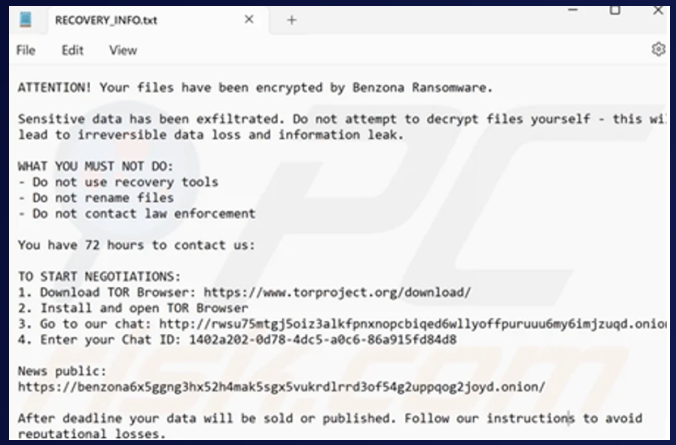
Tactic	Technique	ID	Observed / Assessed Use by Benzona
Initial Access	Spear-phishing Attachment	T1566.001	Likely used to deliver the initial Benzona payload via malicious documents or links.
Initial Access	Exploit Public-Facing Application	T1190	Suspected exploitation of shared vulnerable services / third-party platforms to simultaneously breach multiple related organisations.
Initial Access	Valid Accounts (Domain/Enterprise)	T1078.002	Use of stolen or pre-compromised credentials for RDP/VPN and internal access is highly probable.
Execution	User Execution: Malicious File	T1204.002	Execution of the Benzona EXE (benzona_rans.exe, ~9.7 MB) by users, scheduled tasks or admin tools.
Persistence	Boot/Logon AutoStart via Registry	T1547	Possible registry Run/RunOnce entries or scheduled tasks to ensure execution on reboot (not yet fully confirmed).
Privilege Escalation	OS Credential Dumping	T1003	Likely credential dumping (e.g. LSASS scraping) to obtain admin/service credentials and spread laterally.
Defence Evasion	Impair Defences/ Disable Security Tools	T1562.001	Disabling AV/EDR, killing backup agents and deleting shadow copies to block detection and recovery.
Defence Evasion	Inhibit System Recovery	T1490	Deletion of Volume Shadow Copies and tampering with system restore mechanisms to prevent file restoration.
Discovery	Network Share Discovery	T1135	Scanning and enumeration of file servers and network shares to locate bulk sensitive data.
Lateral Movement	Remote Services (SMB/Admin Shares)	T1021.002	Use of valid credentials over SMB and admin shares to push payloads and move between systems.
Collection	Archive Collected Data	T1560	Aggregation and compression of large data sets (~200 GB in one case) before exfiltration.
Exfiltration	Exfiltration Over C2 Channel	T1041	Upload of archives over encrypted channels (HTTPS) to attacker-controlled infrastructure (e.g. 179.43.139.126).
Exfiltration	Exfiltration to Cloud Storage	T1567.002	Plausible use of third-party cloud/file-sharing services for large data transfers (inferred, not yet fully attributed).
Command-and-Control	Encrypted Channel (Tor)	T1573	Tor-based negotiation and possible C2 channels, leveraging .onion services for anonymity.
Impact	Data Encrypted for Impact	T1486	File system encryption using strong crypto and appending .benzona extension across affected systems.
Impact	Data Manipulation / Data Exposure	T1565 / TA0040	Public leak/auction of stolen data on the Benzona Onion blog to maximise extortion pressure.

Indicators of Compromise (IoCs)

Ransomware Artefacts

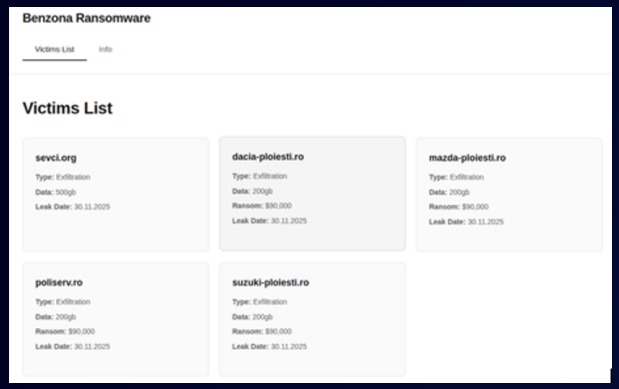
- File extension: .benzona (added to all encrypted files, strong indicator of infection)
- Ransom note: RECOVERY_INFO.txt dropped in encrypted directories containing victim ID and Tor URLs\



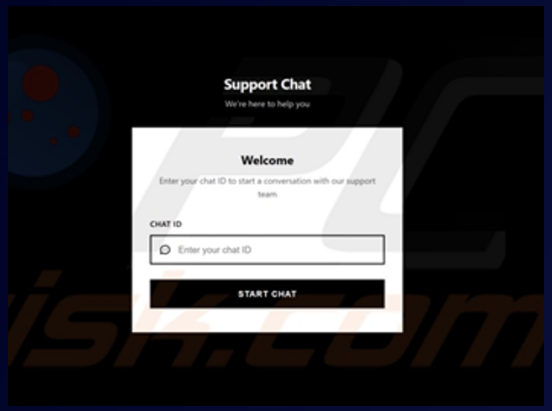


Malware Hashes
- SHA-256: 09f7432834ce15e701aa7fcc84a9c2441c1c7e0a9cb66a6211845be73d2597cc
- MD5: 6e2189ab11f130ead644b1d5bd00f1ac

Onion Infrastructure
- Leak site: benzona6x5ggng3hx52h4mak5sgx5vukrdlrrd3of54g2uppqog2joyd.onion



- Negotiation / support portal: rwsu75mtgj5oiz3alkfpnxnopcbiqed6wllyoffpuruuu6my6imjzuqd.onion



Network IOC
- IP address: 179.43.139.126 (Switzerland) – observed in association with Benzona infrastructure. Treat any communication to/from this IP as highly suspicious.

Communication Handles
- Tox ID: 7308E8CFE8AA18D718B5EF44C34A2E5E2C90B7FDB150FA2EC31E995F5F4B23044A98802A4DF0
- PGP public key: RSA 2048-bit key published on the Benzona leak site (fingerprint and full block available there) for encrypted communications and authenticity verification.

Known Victim Domains (Late Nov 2025)
- suzuki-ploiesti.ro
- dacia-ploiesti.ro
- mazda-ploiesti.ro
- poliserv.ro
- sevci.org

These domains confirm active Benzona compromise; organisations with operational or third-party ties to them should consider increased monitoring and threat hunting for Benzona-like behaviours.

Mitigations – Crystal Eye 5.5

1. Harden External Access
   - Enforce MFA on VPN/RDP/portals, restrict admin access by IP, and aggressively patch internet-facing services. Block legacy protocols at Crystal Eye 5.5 perimeter.
2. Control Privileged & Vendor Accounts
   - Apply least-privilege, rotate admin and MSP/vendor credentials, and alert in CE SIEM on new privileged accounts or abnormal logins.
3. Secure Backups & Recovery
   - Maintain offline/segregated backups, no direct RDP/SMB from user LANs. Monitor and block shadow-copy deletion and destructive PowerShell patterns.
4. Contain Ransomware Execution
   - Use CEASR to block unknown binaries from user-writeable paths and restrict remote admin tools. Detect mass file changes and suspicious archive creation on servers.
5. Monitor Exfiltration & Tor
   - On CE SWG/IDS, detect large outbound uploads, unusual destinations, and Tor/Onion traffic. Block known Benzona IPs and Onion addresses.
6. Prepare a Benzona IR Playbook
   - Pre-define SOAR actions for .benzona / RECOVERY_INFO.txt (isolate host, push IOCs, rotate keys), then re-image, restore from clean backups and treat all accessible data as potentially breached.

Worldwide Ransomware Victims

The United States remained the clear epicentre of ransomware activity, accounting for 40.56% of all identified victims. This outsized concentration shows that, once again, the U.S. is bearing the brunt of targeting, reflecting both its large enterprise surface area and high visibility of public disclosures.

Canada emerged as the second most impacted country with a combined 10% share of reported victims, putting it firmly in the high-risk bracket alongside the US. Together, North America (US + Canada) represented over half of all observed ransomware victims, underlining how strongly threat actors continue to focus on this region.

A notable mid-tier layer included Australia (3.89%), Romania (3.33%), and Germany (2.78%), followed by Spain, Brazil, France, and India (each 2.22%). These figures show that while no single country in this band approaches U.S.-level exposure, several mature and emerging economies are consistently appearing as repeat victims.

Below this, a broader spread of activity was observed across New Zealand and the United Kingdom (each 1.67%), as well as Singapore, Switzerland, and Mexico (each 1.11%). A long tail of countries, including Vietnam, Egypt, the Netherlands, the United Arab Emirates, Portugal, Iraq, Colombia, Thailand, and Japan (each 0.56%), appeared at low individual volumes but collectively highlight that ransomware remains a global, not regional, problem, with opportunistic targeting reaching into diverse geographies.

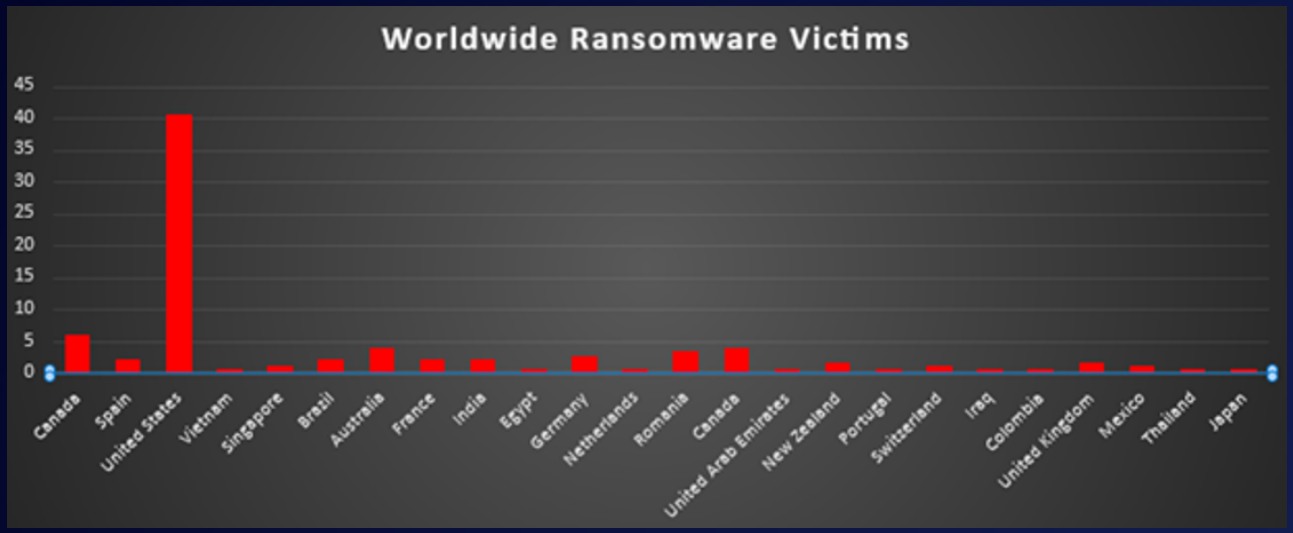


Figure 6: Ransomware Victims Worldwide

Industry-wide Ransomware Victims

Manufacturing was the most heavily impacted sector this week, accounting for 18.33% of all identified ransomware victims. This once again confirms how attractive production environments and supply-chain–critical businesses are to extortion operators, where operational disruption directly translates into strong pressure to pay.

A strong second tier consisted of Retail (12.22%), Business Services (11.11%), Hospitality (9.44%), and Construction (8.89%). Together, these consumer- and service-facing industries represent a broad mix of organisations that handle payments, customer data, and time-sensitive operations — all conditions that attackers routinely exploit to maximise leverage during negotiations.

A diverse mid-band followed, led by Education (5%), Finance (4.44%), Healthcare and Law Firms (each 3.33%), then Real Estate, Federal, Consumer Services, and IT (each 2.78%), plus Transportation and General Organisations (each 2.22%). This layer shows that critical services, public-sector entities, and knowledge-driven industries all remain in regular fixtures on ransomware leak sites rather than outliers.

Lower volume but still active categories included Energy (1.67%), Minerals & Mining and Insurance (each 1.11%), and a long tail of Telecommunications, Media & Internet, and Agriculture (each 0.56%). While individually small, this long-tail distribution demonstrates that ransomware operators are not confined to any single vertical; virtually any sector with digital operations and monetisable data continues to face measurable exposure.

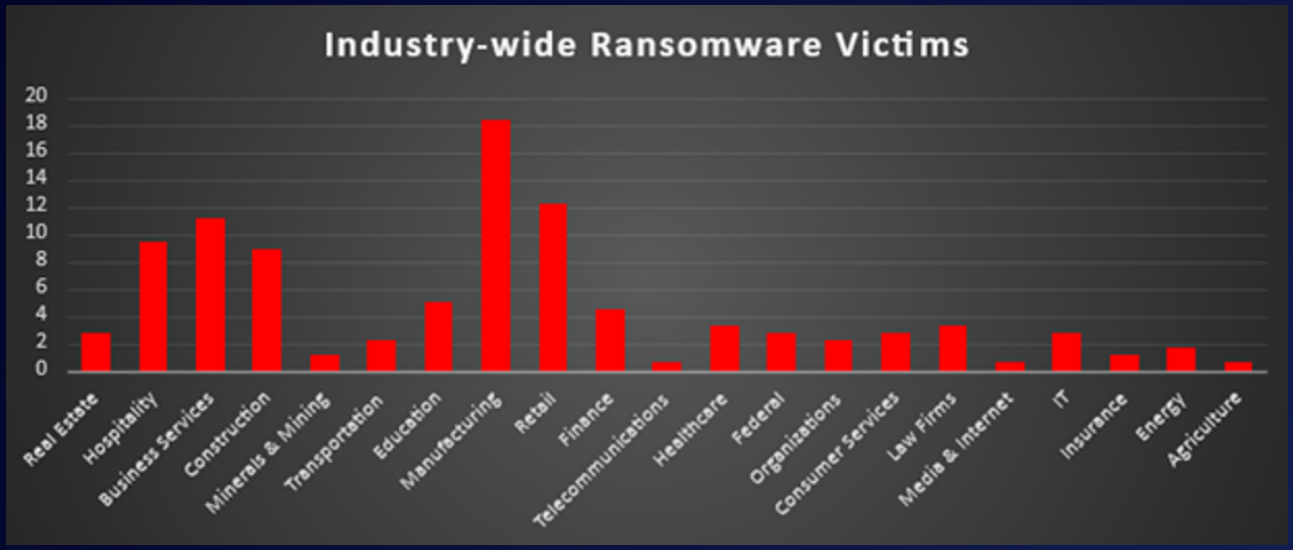


Figure 7: Industry-wide Ransomware Victims