Red Piranha
unified threat management

THREAT INTELLIGENCE REPORT

Oct 28 - Nov 3, 2025

Report Summary:

- **New Threat Detection Added**
  - TA455
  - Amadey

- **Detection Summary**
  - **Threat Protections integrated into the Crystal Eye - 222**
  - **Newly Detected Threats - 6**

The following threats were added to Crystal Eye this week:

1. TA455

TA455 is an Iranian Threat Actor group that is most known for targeting the aerospace industry with advance spear phishing techniques. The group used well-known and trusted services such as Cloudflare and GitHub to route and disguise their C2C traffic.

Victims were contacted via email and LinkedIn and lured to a 'Dream Job'. All they had to do was check a few files and documents. These files and documents contain malware to infect and take control of the victim's device. The malware was also getting flagged as a North Korean malware, this was most likely to throw off attribute to Iran.

Threats Protected: 13
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
Initial Access	T1566	Phishing
Execution	T1204.002	User Execution: Malicious File
Collection	T1119	Automated Collection
Exfiltration	T1020	Automated Exfiltration

2. Amadey

Amadey has been active since 2018 and continues to maintain a botnet infrastructure. Amadey is a trojan malware that maintains persistence on infected hosts and allows for full control of the system via C2 communications. It maintains persistence through registry and scheduled tasks.

It also uses a lot of techniques from other known malware groups such as Lockbit and Redline for privilege escalation and execution mechanisms.

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
Execution	T1059.001	Command and Scripting Interpreter: PowerShell
Persistence	T1547.001	Boot or Logon AutoStart Execution: Registry Run Keys/ Startup Folder
	T1053.005	Scheduled Task/Job: Scheduled Task
Privilege Escalation	T1548	Abuse Elevation Control Mechanism
Command-and-Control	T1071	Application Layer Protocol

Current Threat Summary

Known exploited vulnerabilities (Week 5 October 2025)

Vulnerability	CVSS	Description
CVE-2025-41244	7.8	Broadcom VMware Aria Operations and VMware Tools contain a vulnerability that can allow an attacker with access to a virtual machine to escalate privileges within the virtual machine, exploitation of this vulnerability requires VMware Tools to be installed and to be managed by Aria Operations with SDMP enabled. The vulnerability itself comes down to a regex used by the service discovery feature, simply renaming a specially crafted binary to match this regex can result in this binary being executed in an elevated context.
CVE-2025-24893	9.8	XWiki Platform contains a vulnerability that can allow an unauthenticated remote attacker to execute arbitrary code by sending a specially crafted request to SolrSearch, exploitation of this vulnerability can result in an attacker gaining access to the system.
CVE-2025-6204	8.0	Dassault Systèmes DELMIA Apriso contains a vulnerability that can allow a remote attacker to execute code on the system by accessing a file or webshell that's been uploaded via the file upload API. This vulnerability affects versions from Release 2020 through to Release 2025, and when combined with the unauthenticated account creation vulnerability (CVE-2025-6205) can result in an attacker gaining access to the system.
CVE-2025-6205	9.1	Dassault Systèmes DELMIA Apriso contains a vulnerability that can allow an unauthenticated remote attacker to create a user with administrative privileges on the system. This vulnerability affects version from Release 2020 through to Release 2025. This vulnerability can be used with the code execution vulnerability (CVE-2025-6204) to gain access to the system.

For more information, please visit the **Red Piranha Forum**:
https://forum.redpiranha.net/t/known-exploited-vulnerabilities-catalog-5th-week-of-october-2025/611

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 global ransomware activity this week, accounting for 16.02% of all observed incidents. Its consistent dominance underscores its continued expansion and highly organised affiliate structure, driving steady victim disclosures across sectors.

Akira (13.59%) followed closely, marking a major operational surge that reaffirms its aggressive tactics and persistent presence in both enterprise and mid-market environments. Stormous (9.22%) also recorded strong activity, maintaining its reputation as a disruptive and opportunistic group targeting a mix of industries and geographies.

A mid-tier cluster of actors, including Sinobi (4.85%), Play (5.34%), Everest (3.88%), Medusa (3.88%), Inc Ransom (3.88%), and Ciphbit (2.91%), continued steady campaigns, representing the core of ongoing ransomware operations. Groups such as Nightspire (2.91%), BlackShrantac (2.91%), Clop (2.91%), and PayoutsKing (1.94%) also contributed to the overall activity with targeted, lower-volume operations.

Smaller but persistent presences were observed from Rhysida (1.94%), Coinbase Cartel (1.94%), Genesis (1.46%), DragonForce (1.46%), Brain Cipher (1.46%), Black Nevas (1.46%), and RansomHouse (0.49%), each maintaining operational continuity despite limited public exposure.

A wide spectrum of fringe groups, including Handala, Toufan, Brotherhood, Obscura, MetaEncryptor, Nitrogen, Radiant Group, Chaos, SafePay, MyData, Nova, Interlock, Lynx, Pear, Beast, DevMan2, Sarcoma, and The Gentlemen, each accounted for less than 1% of total incidents, yet their collective footprint reinforces the decentralised, adaptive, and volatile nature of the global ransomware landscape.

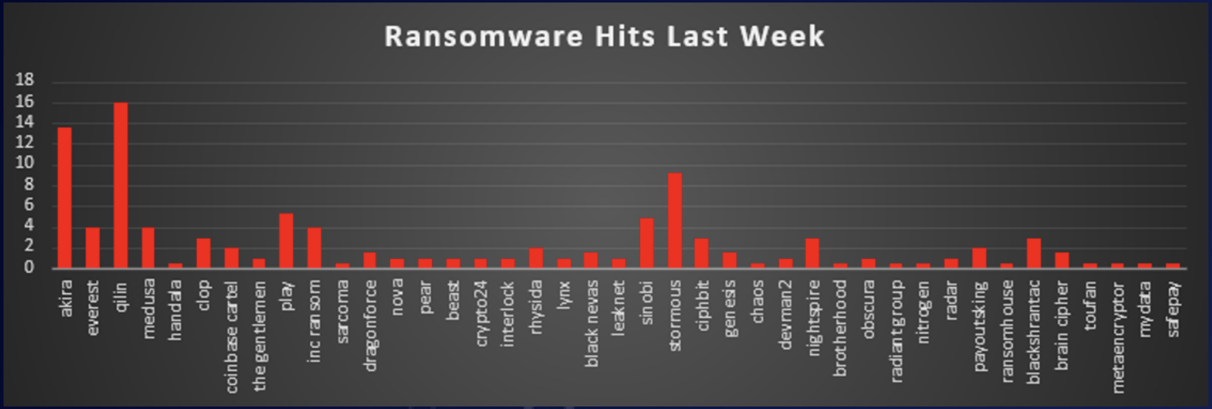


Figure 1: Ransomware Group Hits Last Week

Nitrogen Ransomware

Threat Summary

Nitrogen ransomware is a double-extortion threat group active since mid-to-late 2024. The group became notorious for exploiting malvertising vectors to deliver payloads that disable security tooling and encrypt systems using the .NBA extension. As of 31 October 2025, Nitrogen had claimed over 34 publicly named victims on its dark web leak site. It continues to target organizations across financial, manufacturing, legal, and IT sectors.

Tactics, Techniques, and Procedures (TTPs)

Initial Access

- T1189 - Drive-by Compromise: Poisoned Google/Bing ads impersonate software like WinSCP, AnyDesk, etc.
- T1583.008 - Acquire Infrastructure: Malvertising: Threat actors create fake download portals mimicking legitimate software.
- T1204.002 - User Execution: Malicious File: Victim executes ISO-packaged installer leading to DLL sideloading.

Execution

- T1218 - Signed Binary Proxy Execution: DLL sideloading via legitimate software like Advanced_IP_Scanner.exe.
- T1059 - Command and Scripting Interpreter: Malicious Python execution via bundled pythonw.exe.

Persistence

- T1053 - Scheduled Task/Job: Registry keys or scheduled tasks created for payload execution.
- T1547.001 - Registry Run Keys/Startup Folder: Persistence using Windows Run keys.

Privilege Escalation

- T1068 - Exploitation for Privilege Escalation: Use of known vulnerable drivers.

Defence Evasion

- T1562.001 - Disable or Modify Tools: Uses truesight.sys to terminate AV/EDR.
- T1562.009 - Safe Mode Boot Modification: Executes bcdedit.exe to disable Safe Boot.
- T1027 - Obfuscated Files or Information: Obfuscated Python and sideloaded components.

Credential Access

- T1003.001 - LSASS Memory: Harvesting credentials from memory.

Discovery

- T1057 - Process Discovery: Enumerates processes for EDR detection.
- T1007 - System Service Discovery

Lateral Movement

- T1021.002 - SMB/Windows Admin Shares
- T1021.001 - Remote Services: RDP

Command and Control

- T1071.001 - Web Protocols: HTTP/S over non-standard ports (e.g., 8443, 10443).

Exfiltration

- T1041 - Exfiltration Over C2 Channel: Exfiltration of sensitive files before encryption.

Impact

- T1486 - Data Encrypted for Impact: Ransomware encrypts data using .NBA extension.
- T1490 - Inhibit System Recovery: Deletes shadow copies and disables recovery.

MITRE ATT&CK Mapping Table

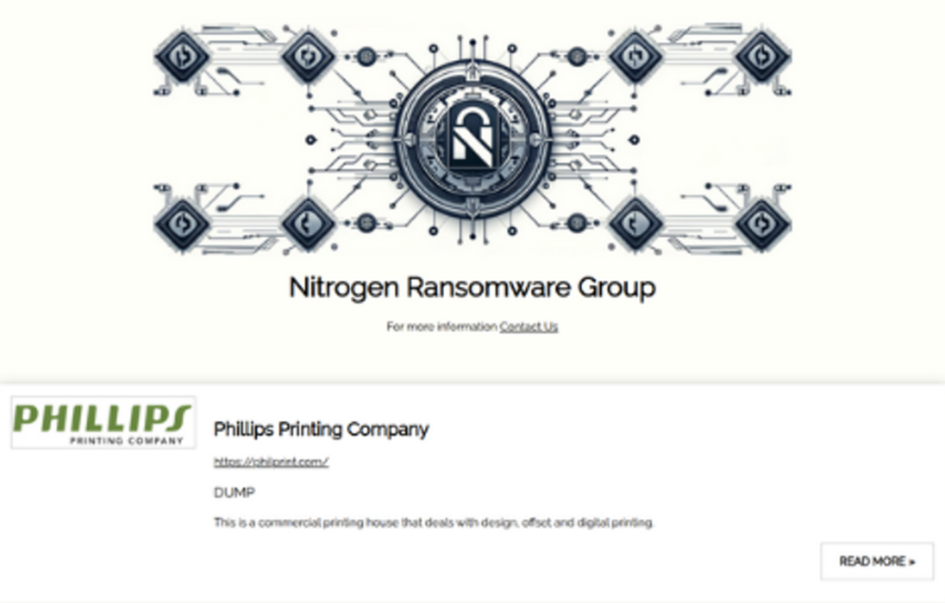
Tactic	Technique	ID	Description
Initial Access	Drive-by Compromise	T1189	Fake software ads lead to malicious downloads.
	Acquire Infrastructure: Ads	T1583.008	Paid search engine ads mimic popular software.
	User Execution	T1204.002	Victim executes trojanised installer.
Execution	DLL Sideloading via Signed Binary	T1218	Malicious DLL loaded by legitimate EXE.
	Command Scripting	T1059	Python scripts for payload execution.
Persistence	Scheduled Task	T1053	Ensures repeat execution.
	Registry Run Keys	T1547.001	Payload auto-launch at boot.
Privilege Escalation	Exploitation for Privilege Escalation	T1068	Uses vulnerable driver for kernel access.
Defence Evasion	AV/EDR Kill via Driver	T1562.001	truesight.sys kills security software.
	Disable Safe Boot	T1562.009	Executes bcdedit.exe for recovery prevention.
	Obfuscation	T1027	Scripts and loaders are obfuscated.
Credential Access	Credential Dumping via LSASS	T1003.001	Steals user credentials.
Discovery	Process Discovery	T1057	Identifies running security software.
	System Service Discovery	T1007	Maps service-based targets.
Lateral Movement	SMB Share Movement	T1021.002	Propagates across network.
	Remote Desktop Protocol	T1021.001	Possible use for access expansion.
Command & Control	Web Protocols	T1071.001	Beacons to HTTP/S over ports 8443, 10443.
Exfiltration	C2 Exfiltration	T1041	Sends stolen data to remote server.
Impact	Encrypt Files	T1486	Encrypts with .NBA extension.
	Delete Recovery	T1490	Deletes shadow copies.

Indicators of Compromise (IOCs)

- File Extensions: .NBA
- Ransom Note: readme.txt, READ_ME_.TXT
- Mutex: nvxkjcv7yxctvgsdfjhv6esdvsx
- Tox IDs:
  - 46CA5EEC55A16767B7F8293DB18F753D1BF60C536747EFD115035DDA40948427E1DDFD107F03
  - 088B7708F2C1557B6023B1102FFC5C36C023FF4883CB073F26A33B73832C9268993ED58B817E
- Hashes:
  - 55f3725ebe01ea19ca14ab14d747a6975f9a6064ca71345219a14c47c18c88be
- C2 Infrastructure IPs/Ports:
  - 185.216.70.236:8443
  - 194.180.48.149:8443
  - 194.180.48.18:10443
  - 171.22.28.245:41337
  - 194.169.175.132
  - 193.42.33.29

- Malicious Domains:
  - xn--wnscp-tsa[.]net (homograph for WinSCP)
- Tor Comm Links

http://nitrogenczslprh3xyw6lh5xyjvmsz7ciljoqxxknd7uymkfetfhgvqd.onion



Nitrogen Ransomware Group

For more information Contact Us

Phillips Printing Company

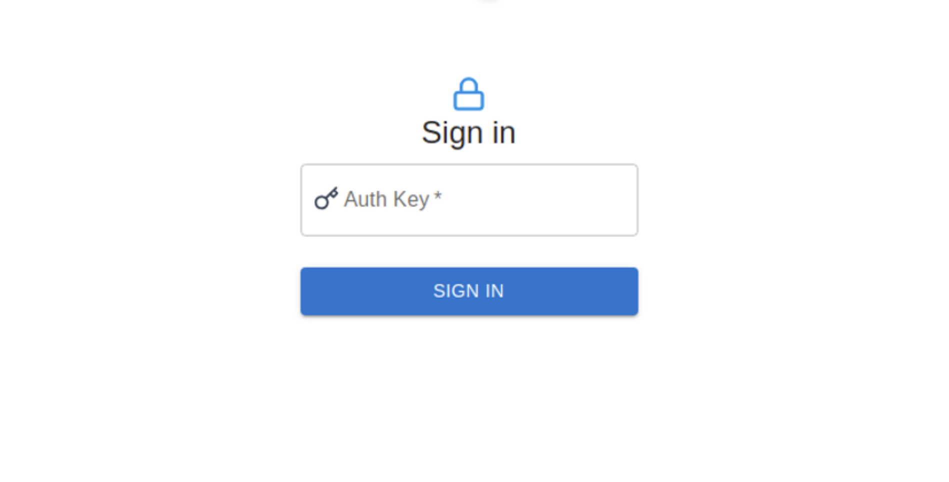
https://philprint.com/

DUMP

This is a commercial printing house that deals with design, offset and digital printing.

Support Chat

http://ws6uapok34o3uvn3v6nru574urlvlbn5u3pi2xzyg765vpv2fixcm4ad.onion



Sign in

Crystal Eye 5.5 Mitigation Strategy

1. Initial Access Mitigations
   - Block ads and unauthorised browser install on endpoints.
   - Monitor for ISO execution from downloads folder.
   - Prevent drive-by downloads using browser hardening and policy restrictions.
2. Persistence & Lateral Movement
   - Implement CE segmentation policies: restrict SMB/WinRM/PsExec to jump boxes only.
   - Log scheduled task and Run key creation to CE SIEM with alerting.
3. Defence Evasion & Recovery Inhibition
   - Block known vulnerable driver hashes and verify code signing.
   - Monitor for bcdedit.exe commands disabling Safe Boot.
   - Isolate hosts on vssadmin or wevtutil execution.
4. Command & Control/Exfiltration
   - Disable QUIC, monitor JA3/SNI for rclone/WinSCP and suspicious TLS tunnels.
   - Block exfil services (MEGA, Dropbox, Syncthing) at DNS/Surge layers.
5. Backup & Recovery
   - Keep backups offline/immutable with no Internet egress.
   - Verify restores quarterly under test conditions.

Worldwide Ransomware Victims

The United States once again dominated global ransomware targeting this week, accounting for 55.83% of all reported victims. Its massive digital footprint, economic value, and concentration of critical industries continue to make it the world's most targeted region.

The United Kingdom (5.83%) and Canada (5.34%) followed as the next most affected nations, reaffirming persistent targeting across North America and Western Europe. These countries remain attractive due to high data density and the likelihood of ransom negotiations.

France (4.37%) and Germany (2.91%) represented the top European mainland targets, followed by Spain (2.43%) and the United Arab Emirates (2.43%), demonstrating ransomware's balanced focus across Western economies and strategic Middle Eastern hubs.

Other mid-tier victims included Australia (1.46%), Malaysia (1.94%), Turkey (1.46%), Italy (0.97%), Netherlands (0.97%), India (0.97%), and Singapore (0.97%), illustrating sustained campaigns against digitally advanced Asia-Pacific nations.

A broad long-tail of isolated incidents (each 0.49%) extended across Saudi Arabia, Brazil, South Korea, China, Japan, New Zealand, Mexico, Israel, Poland, Vietnam, Indonesia, Nigeria, Colombia, Ecuador, Ukraine, Kuwait, Sweden, Finland, Morocco, and Konsise. While these numbers are individually small, they highlight ransomware's continued global expansion and opportunistic victimisation across every continent.

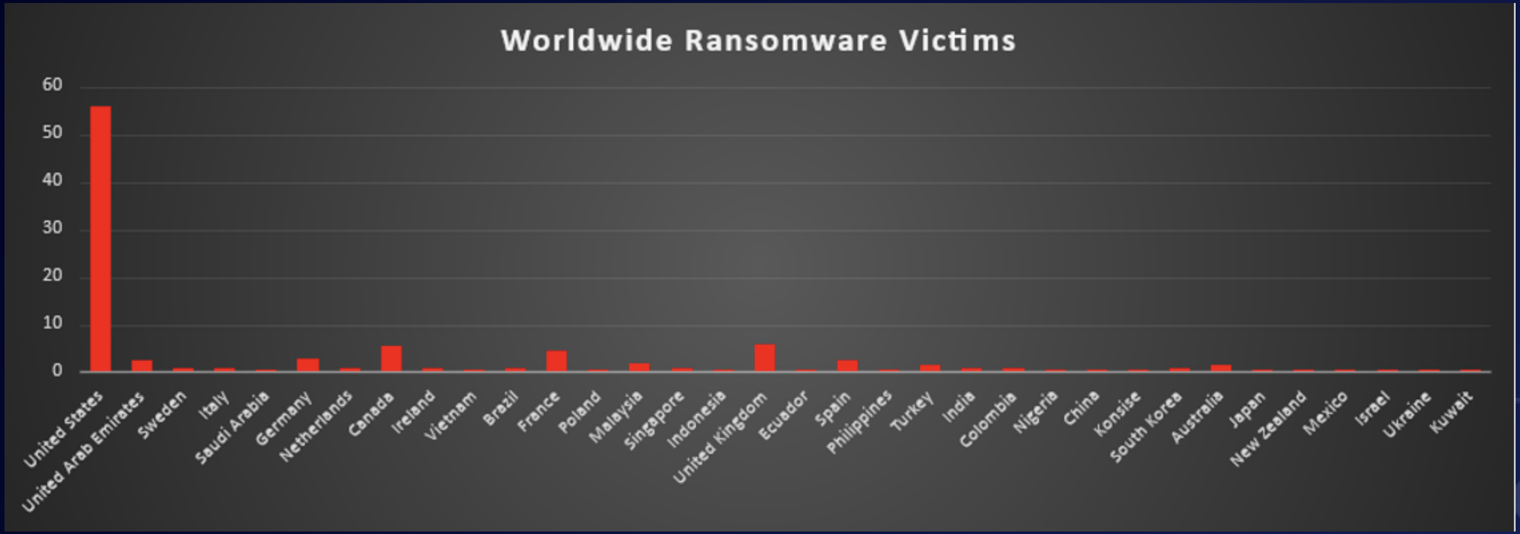


Figure 4: Ransomware Victims Worldwide

Industry-wide Ransomware Victims

Manufacturing continued to lead ransomware targeting this week, accounting for 16.5% of all reported incidents. Its dominance underscores attackers' sustained focus on operational sectors where downtime directly translates to financial loss and supply chain disruption.

A strong wave of activity was observed across Construction (12.62%), Retail (12.62%), and Business Services (12.14%). These industries remain prime targets due to their reliance on interconnected systems, third-party vendors, and high transaction volumes, all of which increase the likelihood of exploitation and extortion. Hospitality (9.22%) also featured prominently, reflecting persistent campaigns aimed at data-rich, customer-facing environments where service disruption has immediate reputational and financial impact.

Mid-tier targeting included Law Firms (5.83%), Energy (3.4%), Transportation (3.4%), Finance (3.4%), and Real Estate (3.4%), indicating ransomware operators' ongoing focus on sectors that handle critical operational and financial data.

Further activity was recorded in Healthcare (2.91%), Insurance (2.91%), and IT (2.43%), highlighting adversaries' continued exploitation of sectors holding sensitive personal or digital assets.

At the lower end, Consumer Services (1.94%), Telecommunications (1.94%), and Media & Internet (1.46%) saw limited but notable incidents. Isolated cases were also reported in Federal (1.46%), Organisations (0.97%), and niche verticals like Minerals & Mining (0.49%), Agriculture (0.49%), and Education (0.49%), reinforcing ransomware's opportunistic spread across all industries.

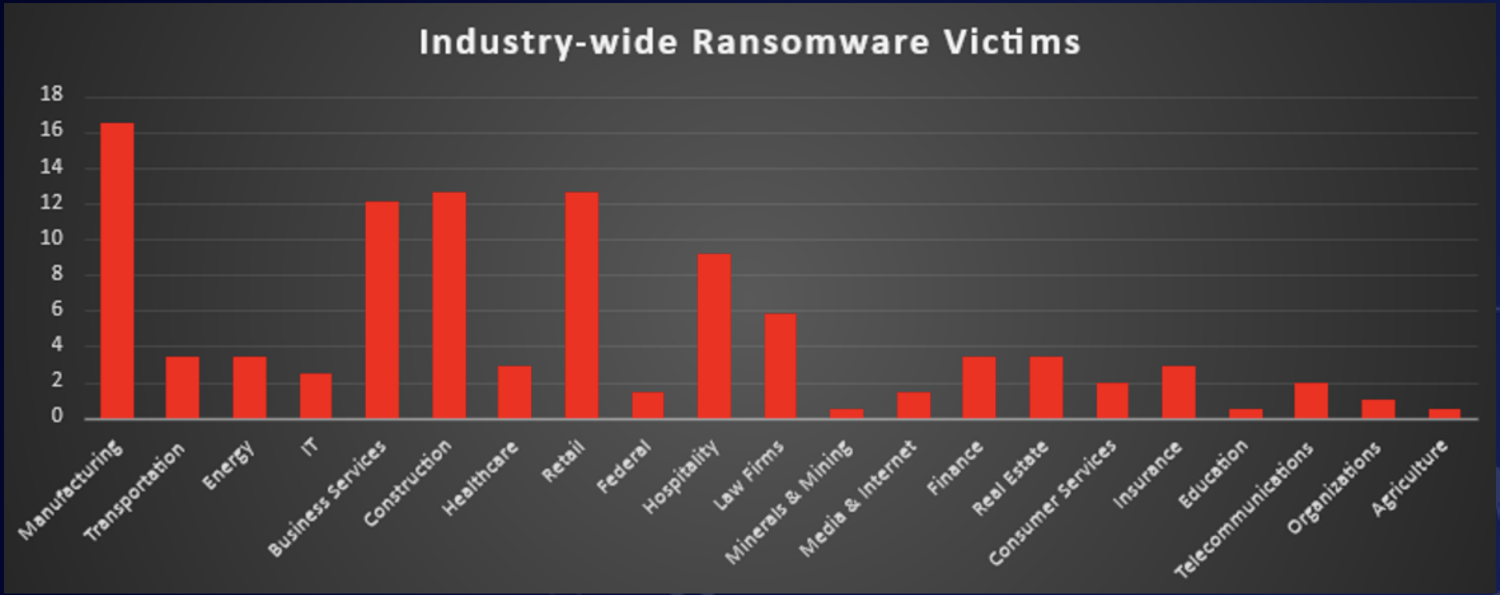


Figure 5: Industry-wide Ransomware Victims