Red Piranha
unified threat management

THREAT INTELLIGENCE REPORT

Sept 16 - 22, 2025

Report Summary:

- **New Threat Detection Added**
  - Shai-Hulud
  - Oyster Backdoor

- **Detection Summary**
  - **Threat Protections integrated into the Crystal Eye - 197**
  - **Newly Detected Threats - 20**

The following threats were added to Crystal Eye this week:

1. Shai-Hulud

Windows malware loader delivered via phishing (ISO/ZIP+LNK) or trojanised installers. Uses PowerShell/WSH to fetch a second stage over HTTPS, sets persistence (Run keys / Scheduled Tasks), does basic discovery + credential theft, and can stage data exfil or ransomware.

Threats Protected: 1
Class Type: Malware
Rule Set Type:

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

Kill Chain:

Tactic	Technique ID	Technique Name
Initial Access	T1566.001	Phishing: Attachment
	T1195.002	Supply Chain Compromise: Installer
Execution	T1204.002	User Execution: Malicious File
	T1059.001	Command & Scripting: PowerShell
Persistence	T1547.001	Registry Run Keys / Startup Folder
	T1053.005	Scheduled Task
Privilege Escalation	T1068	Exploitation for Privilege Escalation
Defence Evasion	T1027	Obfuscated/Compressed Files & Info
	T1112	Modify Registry
	T1562.001	Impair Defences: Disable AV/EDR
Credential Access	T1003.001	LSASS Memory
	T1555.004	Credentials from Web Browsers
Discovery	T1082	System Information Discovery
	T1069.002	Permission Groups Discovery: Domain
Lateral Movement	T1021.002	SMB/Windows Admin Shares
	T1047	WMI
Command & Control	T1071.001	Web Protocols (HTTPS)
Exfiltration	T1041	Exfiltration Over C2 Channel
Impact	T1490	Inhibit System Recovery
	T1486	Data Encrypted for Impact

2. Oyster Backdoor

Cross-platform backdoor used for remote command execution, file ops, and data exfiltration. Typically delivered via phishing or trojanised installers, establishes HTTPS-based C2, sets persistence (services/registry on Windows; cron/systemd on Linux), and may perform basic discovery and credential theft prior to lateral movement.

Threats Protected: 31
Class Type: Malware
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	T1566.001	Phishing: Attachment
Initial Access	T1195.002	Supply Chain Compromise: Compromised Software
Execution	T1059.003	Command and Scripting Interpreter: Windows Command Shell
Execution	T1059.004	Command and Scripting Interpreter: Bash
Persistence	T1547.001	Boot or Logon AutoStart Execution: Registry Run Keys / Startup Folder
Persistence	T1053.003	Scheduled Task/Job: Cron
Persistence	T1543.003	Create or Modify System Process: Windows Service
Privilege Escalation	T1068	Exploitation for Privilege Escalation
Defence Evasion	T1027	Obfuscated/Compressed Files and Information
Credential Access	T1003.001	OS Credential Dumping: LSASS Memory
Credential Access	T1555.003	Credentials from Password Stores: Credentials from Web Browsers
Discovery	T1082	System Information Discovery
Discovery	T1046	Network Service Discovery
Lateral Movement	T1021.002	Remote Services: SMB/Windows Admin Shares
Lateral Movement	T1021.001	Remote Services: Remote Desktop Protocol
Command & Control	T1071.001	Application Layer Protocol: Web Protocols (HTTPS)
Command & Control	T1008	Fallback Channels
Exfiltration	T1041	Exfiltration Over C2 Channel
Impact	T1490	Inhibit System Recovery

Current Threat Summary

Updated Malware Signatures (Week 3 September 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.”

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 the ransomware ecosystem this week with 19.59% of reported incidents, reinforcing its dominance as one of the most aggressive and persistent threat actors.

Play followed at 10.14%, continuing to demonstrate steady operations, particularly against organisations with weaker security postures. Inc Ransom matched this activity with 9.46%, showing consistent campaigns and reinforcing its position as a key mid-tier operator.

Akira accounted for 7.43%, while Coinbase Cartel registered 6.76%, both maintaining momentum with sustained targeting across multiple industries. SafePay also contributed significantly at 5.41%, reflecting its stable role in the current ransomware ecosystem.

Other notable presences included Warlock (4.73%) and Everest (4.05%), while Sarcoma (2.7%), BlackShrantac (2.7%), and The Gentlemen (2.03%) each logged meaningful mid-level activity. Lynx, Radar, Kairos, Arcus Media, and WorldLeaks all recorded 2.03% apiece, maintaining visibility in the mid-tier landscape.

A long tail of smaller actors, including KillSec3, Devman2, Obscura, Datacarry, Medusa, Ransomware Blog, Metaencryptor, Lunalock, DragonForce, Beast, IMN Crew, Termite, Brain Cipher, MyData, Space Bears, Crypto24, Securotrop, Sinobi, and Anubis, each accounted for 0.68–1.35%. While their activity is individually limited, their collective presence illustrates the fragmented and diverse nature of the ransomware threat landscape.

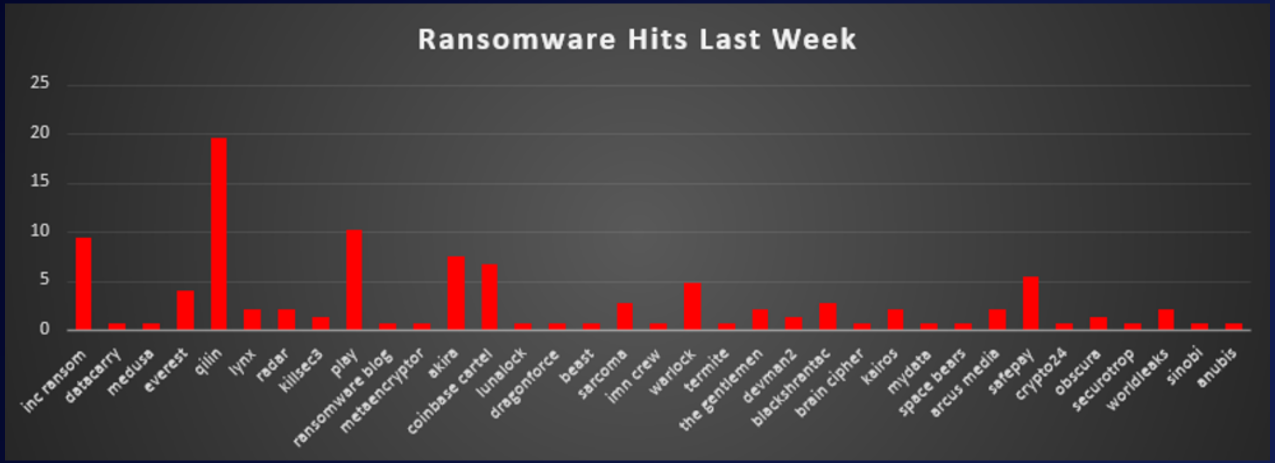


Figure 1: Ransomware Group Hits Last Week

Coinbase Cartel Ransomware

Red Piranha assesses Coinbase Cartel as a financially motivated extortion collective operating since mid-2025, formed from ShinyHunters, Scattered Spider, and Lapsus$ affiliates. While their leak site currently emphasises data exfiltration only, intelligence indicates the group is actively developing the shinysp1d3r ESXi-targeted RaaS, suggesting an imminent transition to double-extortion ransomware operations.

Detailed TTPs

Initial Access

Coinbase Cartel gains entry through insider recruitment and bribery of third-party contractors, abuse of valid accounts, and vishing techniques that trick users into authorising malicious OAuth applications.
Detections: sudden administrative logins from Tor/VPN IPs; anomalous OAuth approvals; employee reports of bribery or coercion.

Execution

In cloud environments, custom Python scripts mimic Salesforce Data Loader to mass-exfiltrate data. On-premises, the shinysp1d3r loader executes in memory via shell scripts on ESXi hosts, retrieving the encryptor and launching parallel VMDK encryption while disabling snapshots.
Detections: unknown shell script execution on ESXi; rapid high-entropy file writes to datastore paths; snapshot disablement events.

Persistence

Persistence is achieved through long-lived OAuth tokens, malicious connected apps, or by adding SSH keys and hidden accounts on servers.
Detections: unrecognised admin users; anomalous SSH authorized_keys entries; OAuth apps not deployed by IT.

Privilege Escalation

Privilege escalation relies primarily on compromised admin credentials. In enterprise environments, escalation may also involve credential dumping or leveraging unpatched privilege escalation flaws.
Detections: abnormal LSASS access attempts; use of escalation binaries or drivers; privilege assignment to unusual accounts.

Defence Evasion

The group clears and disables logs on ESXi, disguises malicious applications as legitimate tools, and uses Tor/VPN infrastructure for anonymity.
Detections: syslog forwarding disabled; mass log truncation; newly created apps with names mimicking Salesforce Data Loader.

Discovery

Discovery includes enumeration of VMware datastores, virtual machines, Active Directory objects, and file shares to locate high-value data.
Detections: unusual vCenter API queries; enumeration of domain admin groups from non-IT accounts; aggressive SMB share enumeration.

Lateral Movement

Movement between systems is achieved using SSH with root credentials across ESXi hosts and potentially RDP or PsExec in Windows environments.
Detections: new SSH sessions between hypervisors; PsExec activity from accounts outside IT; abnormal RDP logons from Tor/VPN IPs.

Collection & Exfiltration

Data is staged and exfiltrated via cloud APIs, encrypted channels, or third-party storage. Archives are created to compress large data sets prior to transfer.
Detections: creation of large compressed archives; abnormal high-volume API exports; outbound encrypted transfers to Tor nodes.

Impact

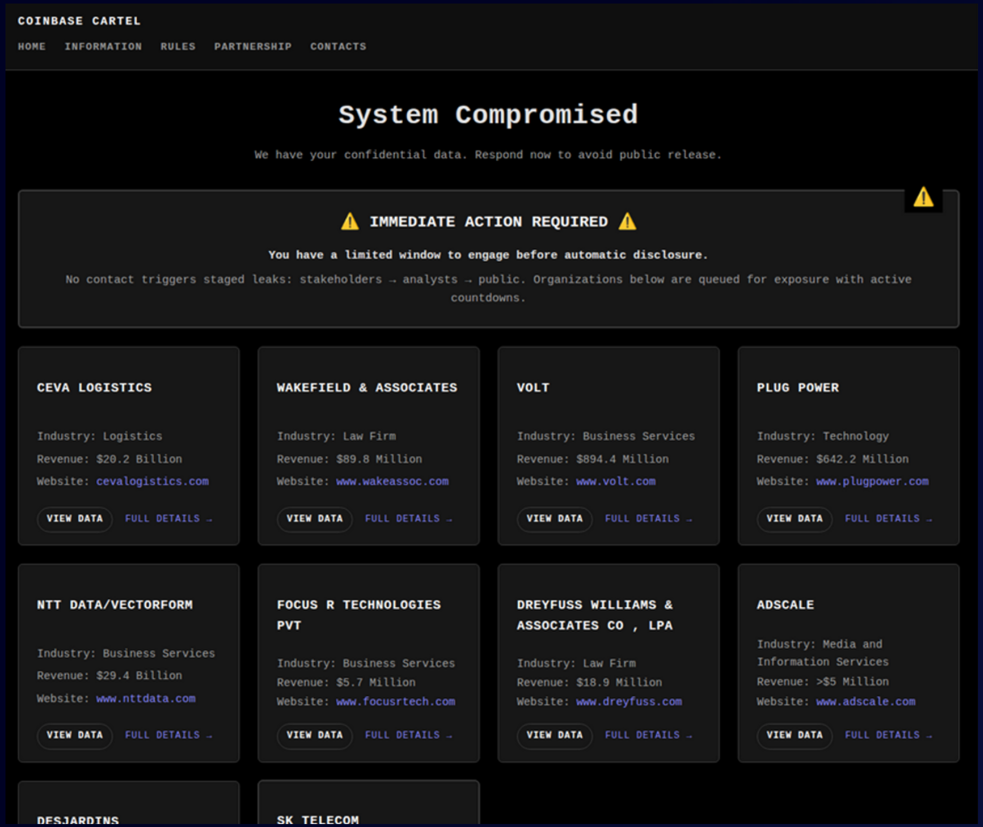
Current operations emphasise data disclosure and extortion without encryption. With shinysp1d3r active, expected impact will include mass ESXi encryption resulting in enterprise-wide disruption.
Detections: VM snapshot disablement; datastore file renaming; ransom note artifacts once shinysp1d3r is deployed.

MITRE ATT&CK Mapping

Tactic	**Technique ID**	**How it appears for** Gentlemen
Initial Access	Valid Accounts (T1078); Trusted Relationship (T1199); Vishing (T1566.004)	Bribery, stolen creds, voice phishing for OAuth/SSO approvals
Execution	Unix Shell (T1059.004); Memory-resident loader - encryptor	Shell scripts on ESXi, Python data dump scripts
Persistence	Create Account (T1136); Valid Tokens (T1078)	OAuth tokens, malicious apps, hidden SSH accounts
Privilege Escalation	Privileged Credentials (T1078.004); OS Credential Dumping (T1003)	Use of admin creds; possible LSASS dumps
Defence Evasion	Clear Logs (T1070); Disable Logging (T1562.002); Proxy/Tor (T1090.003)	Log clearing on ESXi; Tor/VPN for exfiltration
Discovery	Cloud Service Discovery (T1580); Remote System Discovery (T1018)	Enumerates vCenter, AD, file shares
Lateral Movement	SSH (T1021.004); RDP (T1021.001)	SSH across ESXi; RDP/PsExec in Windows
Collection	Data from Information Repositories (T1213); Automated Collection (T1119)	Bulk CRM/API exports; staging archives
Exfiltration	Exfil to Cloud Storage/API (T1567.002); Exfiltration Over C2 (T1041)	Encrypted transfers via APIs, Tor, or cloud storage
Impact	Data Encrypted for Impact (T1486)	Projected shinysp1d3r ESXi encryption

IOCs

Leak Site: fjg4zi4opkxkvdz7mvwp7h6goe4tcby3hhkrz43pht4j3vakhy75znyd.onion
C2/Infrastructure: affiliateshinysp1d3r[.]com (payload fetch server)
Email: shinycorp@tuta[.]com, shinygroup@tuta[.]com



System Compromised

We have your confidential data. Respond now to avoid public release.

⚠ **IMMEDIATE ACTION REQUIRED** ⚠

You have a limited window to engage before automatic disclosure.

No contact triggers staged leaks: stakeholders → analysts → public. Organizations below are queued for exposure with active countdowns.

CEVA LOGISTICS
Industry: Logistics
Revenue: $20.2 Billion
Website: cevalogistics.com
VIEW DATA FULL DETAILS →

WAKEFIELD & ASSOCIATES
Industry: Law Firm
Revenue: $89.8 Million
Website: www.wakeassoc.com
VIEW DATA FULL DETAILS →

VOLT
Industry: Business Services
Revenue: $894.4 Million
Website: www.volt.com
VIEW DATA FULL DETAILS →

PLUG POWER
Industry: Technology
Revenue: $642.2 Million
Website: www.plugpower.com
VIEW DATA FULL DETAILS →

NTT DATA/VECTORFORM
Industry: Business Services
Revenue: $29.4 Billion
Website: www.nttdata.com
VIEW DATA FULL DETAILS →

FOCUS R TECHNOLOGIES PVT
Industry: Business Services
Revenue: $5.7 Million
Website: www.focusrtech.com
VIEW DATA FULL DETAILS →

DREYFUSS WILLIAMS & ASSOCIATES CO , LPA
Industry: Law Firm
Revenue: $18.9 Million
Website: www.dreyfuss.com
VIEW DATA FULL DETAILS →

ADSCALE
Industry: Media and Information Services
Revenue: >$5 Million
Website: www.adscale.com
VIEW DATA FULL DETAILS →

DESJARDINS

SK TELECOM

Mitigation Summary — Coinbase Cartel / shinysp1d3r

- Harden Access: Enforce MFA everywhere (cloud, VPN, vCenter). Limit contractor access with the least privilege and strict monitoring.
- Protect ESXi & Cloud: Disable ESXi SSH by default, push logs to secure syslog, and restrict OAuth app creation in SaaS platforms.
- Detect Early: Monitor for unusual CRM exports, OAuth approvals, large archive creation, and syslog/service tampering on ESXi. Flag logins from Tor/VPN nodes.
- Prepare Response: Maintain ransomware-specific IR playbooks, isolate compromised accounts/hosts quickly, and pre-stage regulator/customer comms.
- Backup & Recovery: Keep offline/immutable backups and regularly test ESXi restore drills to ensure rapid recovery.
- Awareness & Training: Train staff and contractors to resist bribery and vishing tactics.

Worldwide Ransomware Victims

The United States dominated the ransomware landscape this week, accounting for 52.03% of all reported victims. Its dominance highlights the continuing preference of threat actors to focus on high-value targets in North America, where the digital footprint is vast and enterprises are often pressured into ransom negotiations due to operational criticality.

Germany (4.73%) and Australia (4.73%) followed as the next most impacted nations. Both countries remain frequent targets due to their advanced industrial bases, highly digitised infrastructures, and roles as global supply chain hubs. Canada also reported 4.05%, reinforcing its steady presence among top-targeted nations.

Mid-tier targeting was observed in Italy (3.38%), France (2.7%), South Korea (2.7%), and the United Kingdom (2.7%), underscoring Europe and Asia's continued exposure to ransomware campaigns. Additional notable activity was recorded in Sweden, Spain, Netherlands, and China (each at 2.03%).

A long tail of countries reported isolated incidents (each at 0.68–1.35%), including Thailand, Japan, Brazil, Dominican Republic, Portugal, Chile, Denmark, Singapore, Turkey, Egypt, Taiwan, Pakistan, India, Kenya, Greece, United Arab Emirates, and Namibia. While individually small, these figures emphasise ransomware's global reach, extending beyond core Western economies into Latin America, Africa, and Asia-Pacific.

This distribution reflects ransomware's dual strategy: a heavy concentration of attacks in the U.S. and major European economies, paired with opportunistic exploitation of smaller or emerging markets where defences may be less mature.

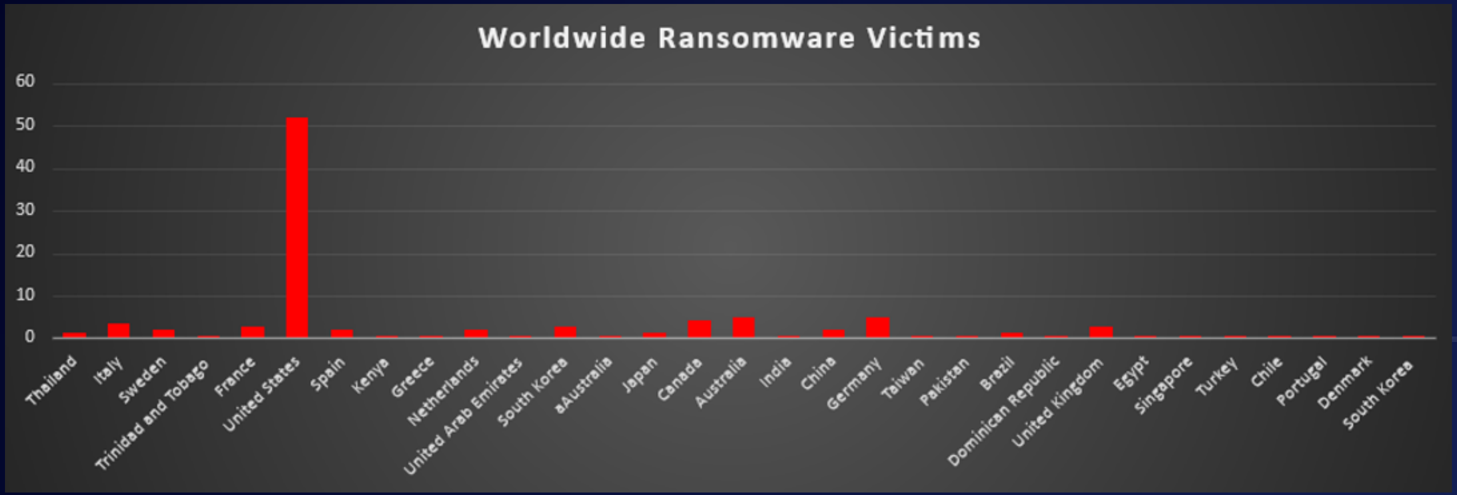


Figure 3: Ransomware Victims Worldwide

Industry-wide Ransomware Victims

Business Services topped the list this week with 16.78% of ransomware incidents, reflecting adversaries' continued focus on IT, consulting, and outsourcing firms. These organisations serve as gateways to multiple client environments, amplifying the impact of a single compromise.

Manufacturing followed at 14.09%, reaffirming its position as one of the most consistently targeted sectors due to its operational criticality and low tolerance for downtime. Finance also ranked high with 13.42%, highlighting attackers' interest in institutions that handle sensitive data and liquidity pressure points, often forcing quicker ransom negotiations.

Construction logged 9.4%, demonstrating adversary preference for industries with complex supply chains and decentralised digital infrastructures. Retail accounted for 8.72%, underscoring its persistent vulnerabilities tied to customer payment systems and distributed operations.

Mid-tier victims included Hospitality (4.7%), Energy (4.03%), Law Firms (3.36%), Telecommunications (3.36%), and Real Estate (3.36%). Each of these verticals presents unique high-value data and operational leverage points attractive to extortion-driven campaigns.

Sectors with moderate but notable impact were IT (2.01%), Transportation (2.01%), Insurance (2.01%), Media & Internet (2.01%), Healthcare (2.68%), Federal (2.68%), Consumer Services (2.01%), and Organisations (1.34%), reflecting ransomware's wide net across both private enterprises and public entities.

At the lower end, Education (0.67%) and Agriculture (0.67%) registered small shares of reported incidents. Though their numbers are limited, these sectors remain vulnerable due to typically weaker cyber defences and growing digitisation.

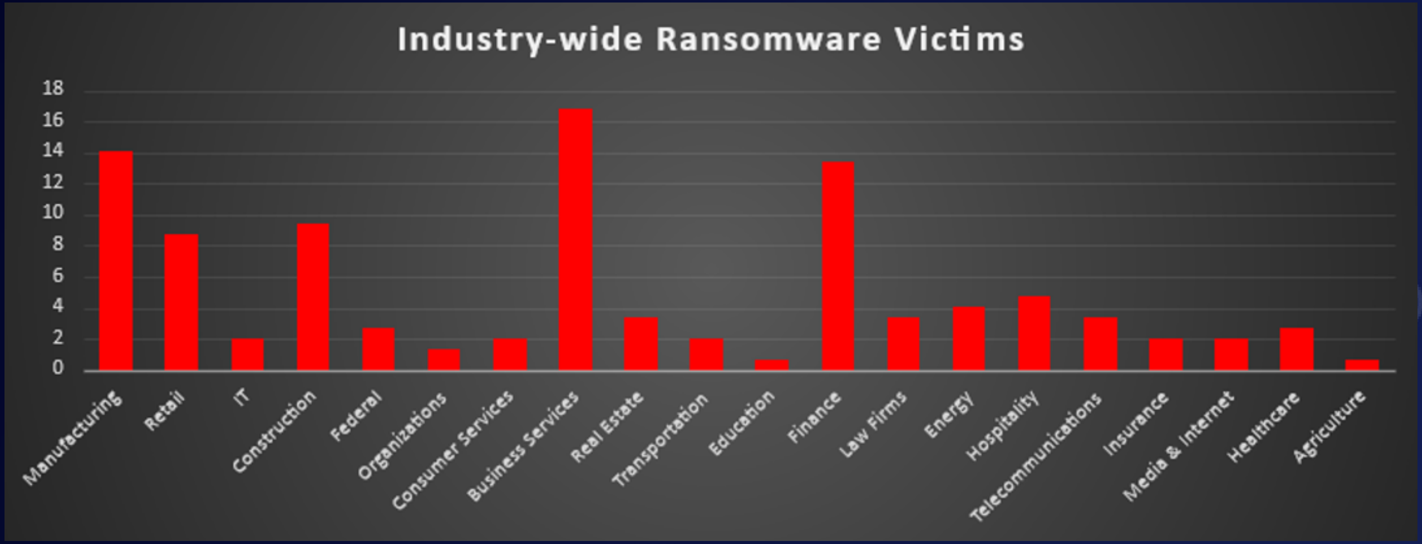


Figure 4: Industry-wide Ransomware Victims