Red Piranha
unified threat management

THREAT INTELLIGENCE REPORT

Sept 30 - Oct 6, 2025

Report Summary:

- **New Threat Detection Added**
  - BPFDoor
  - Klopatra
- **Detection Summary**
  - **Threat Protections integrated into the Crystal Eye - 105**
  - **Newly Detected Threats - 6**

The following threats were added to Crystal Eye this week:

1. BPFDoor

BPFDoor is a Linux backdoor malware used by a China-based threat actor. This malware has strong stealth capabilities, using Berkly Packet Filtering (BPF), which allows the malware to execute code into the Linux kernel. This allows the malware to hide its process ID, intercept syscalls, deal with network traffic, and hide kernel modules. The malware supports multiple protocols to interact with a C2 server, including TCP, UDP, and ICMP. All this stealth and communication functionality allows the threats to stealthily infect and laterally move within compromised networks.

Threats Protected: 14
Class Type: Command-and-Control
Rule Set Type:

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

Kill Chain:

Tactic	Technique ID	Technique Name
Execution	T1059.004	Command and Scripting Interpreter: Unix Shell
Persistence	T1205.002	Traffic Signalling: Socket Filters
Defence Evasion	T1480.002	Execution Guardrails: Mutal Exclusion
	T1564.011	Hide Artifacts: Ignore Process Interrupts
	T1562.004	Impair Defences: Disable or Modify System Firewall
	T1562.003	Impair Defences: Impair Command History Logging
	T1070.004	Indicator Removal: File Deletion
	T1070.006	Indicator Removal: Timestomp
	T1036.009	Masquerading: Break Process Trees
	T1036.011	Masquerading: Overwrite Process Arguments
Command-and-Control	T1205.002	Traffic Signalling: Socket Filters

2. Klopatra

Klopatra is a new Android-based Remote Access Trojan (RAT). It has been found to target financial institutions and their customers, primarily in Spain and Italy. This malware has strong stealth capabilities due to its use of a code protection system and uses native Android libraries, which reduces the visibility of analysis tools. Due to the language choices and C2 infrastructure, it is suspected that the malware was developed and used by Turkish-based threat actors.

The malware disguises itself as an app for IPTV (Internet based television platform) and once installed, it downloads the Klopatra malware and begins execution. The malware has full access to the entire system, from screen monitoring and input capture to action execution (Simulate taps and gestures).

Threats Protected: 6
Class Type: Domain-c2
Rule Set Type:

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

Kill Chain:

Tactic	Technique ID	Technique Name
Execution	T1204	User Execution
Persistence	T1653	Power Settings
Defence Evasion	T1564.012	Hide Artifacts: File/Path Exclusions
Command-and-Control	T1219	Remote Access Tools

Current Threat Summary

Known exploited vulnerabilities (Week 1 October 2025)

Vulnerability	CVSS	Description
CVE-2014-6278	8.8	GNU Bash contains an OS command injection vulnerability which allows remote attackers to execute arbitrary commands via a crafted environment. This vulnerability exists because of an incomplete fix for CVE-2014-6271, CVE-2014-7169, and CVE-2014-6277.
CVE-2017-1000353	9.8	Jenkins contains a remote code execution vulnerability. This vulnerability that could allowed attackers to transfer a serialised Java object to the remoting-based Jenkins CLI, this allow the existing blocklist-based protection mechanism to be bypassed.
CVE-2025-21043	8.8	Samsung mobile devices contain an out-of-bounds write vulnerability in libimagecodec.quram.so which allows remote attackers to execute arbitrary code.
CVE-2025-4008	8.7	Smartbedded Meteobridge contains a command injection vulnerability that could allow remote unauthenticated attackers to gain arbitrary command execution with elevated privileges (root) on affected devices. This is due to an unsafe eval call that is found at /cgi-bin/template.cgi.
CVE-2025-32463	9.3	Sudo contains an inclusion of functionality from untrusted control sphere vulnerability. This vulnerability could allow local attacker to leverage sudo's -R (–chroot) option to run arbitrary commands as root, even if they are not listed in the sudoers file.
CVE-2025-59689	6.1	Libraesva Email Security Gateway (ESG) contains a command injection vulnerability which allows command injection via a compressed e-mail attachment. This occurs due to an improper sanitisation during the removal of active code from files contained in some compressed archive formats.
CVE-2025-10035	10	Fortra GoAnywhere MFT contains a deserialisation of untrusted data vulnerability allows an actor with a validly forged license response signature to deserialise an arbitrary actor-controlled object, possibly leading to command injection.
CVE-2025-20352	7.7	Cisco IOS and IOS XE contains a stack-based buffer overflow vulnerability in the Simple Network Management Protocol (SNMP) subsystem that could allow for denial of service or remote code execution. A successful exploit could allow a low-privileged attacker to cause the affected system to reload, resulting in a DoS condition, or allow a high-privileged attacker to execute arbitrary code as the root user and obtain full control of the affected system.
CVE-2021-21311	7.2	Adminer contains a server-side request forgery vulnerability that, when exploited, allows a remote attacker to obtain potentially sensitive information.

For more information, please visit the **Red Piranha Forum**:
https://forum.redpiranha.net/t/known-exploited-vulnerabilities-catalog-1st-week-of-october-2025/601

Updated Malware Signatures (Week 1 October 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

Ransomware Hits Last Week

Scattered Lapsus$ Hunters dominated this week's ransomware activity, responsible for 19.9% of reported incidents. Its sudden prominence highlights either a large, coordinated campaign or a significant disclosure of past victim compromises.

Sinobi (10.95%) and Akira (10.45%) followed closely, showing sustained momentum and reaffirming their place among the top-tier operators. Qilin (6.97%), DevMan2 (7.46%), and Inc Ransom (5.47%) also reported significant activity, contributing to a mid-tier cluster of highly active threat groups.

Other notable contributors included Play (3.98%), Obscura (3.98%), J Group (3.48%), and Medusa (3.48%), suggesting focused but smaller-scale operations.

A broad range of groups each logged 1–2% of activity, including Coinbase Cartel, Securotrop, RansomHouse, The Gentlemen, Handala, Lynx, Nova, Space Bears, Anubis, and MyData. These actors remain visible but operate at lower volumes compared to leading players.

The long tail of groups accounted for 0.5% each, among them Rhysida, BlackShrantac, Sarcoma, Black Nevas, Chaos, Gunra, 3AM, LeakedData, Kairos, Sinob, WorldLeaks, Trinity, Crypto24, and Radar. While individually small, their collective footprint reinforces the fragmented nature of the ransomware landscape, where dozens of actors operate simultaneously at varying scales.

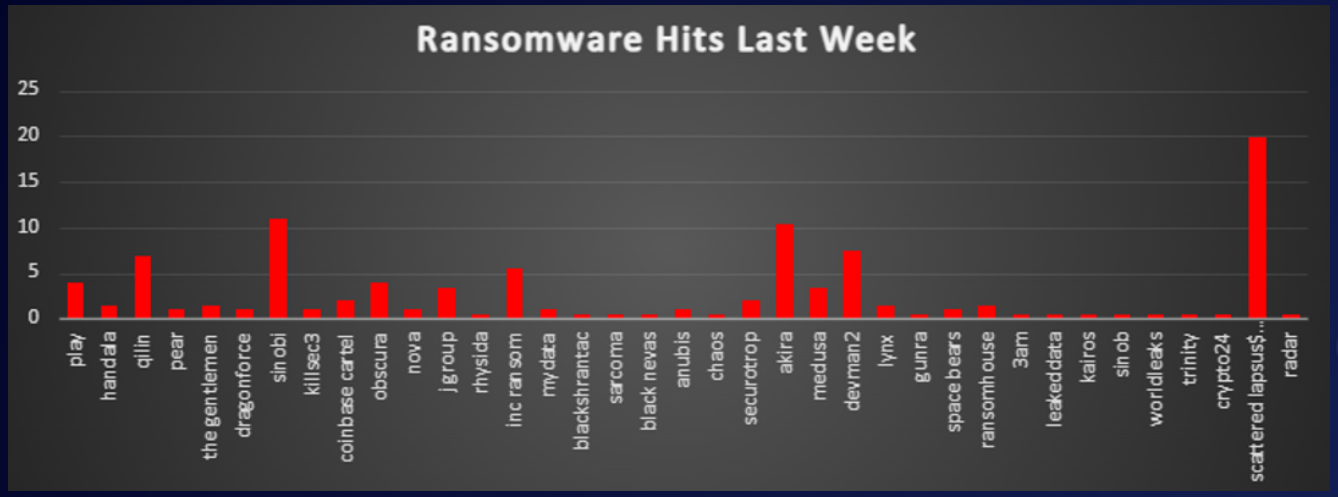


Figure 1: Ransomware Group Hits Last Week

Scattered LAPSUS$ Hunters Ransomware

Description
Scattered LAPSUS$ Hunters emerged with a coordinated extortion campaign leveraging stolen OAuth tokens and SaaS compromises, primarily targeting Salesforce customers. They published a new leak-site portal listing ~39 high-profile victims across finance, retail, aviation, and tech. The group demanded ransom with a strict deadline, threatening to leak nearly all data records if unpaid. This week marked a clear shift from individual victim extortion toward a SaaS-supply-chain-wide campaign.

Detailed TTPs

Initial Access
- Voice-phishing of helpdesk staff to authorise malicious Salesforce OAuth "Data Loader" apps.
- Supply-chain compromise of Salesloft GitHub repo to steal Salesforce/Google Workspace OAuth tokens.

Detections: New connected apps approved in Salesforce; anomalous MFA resets; GitHub repo access from unknown IP ranges.

Execution
- Abuse of Salesforce Data Loader via stolen tokens to query and pull bulk data.
- Legitimate SaaS APIs (SOQL queries) used to stage exfiltration.

Detections: Sudden high-volume Salesforce API queries; new OAuth client IDs in logs.

Persistence
- Continued use of refreshed OAuth tokens for long-term access.
- No malware persistence—relied on SaaS identity.

Detections: Tokens issued repeatedly from abnormal IP/ASN; OAuth apps persisting in tenant configs.

Privilege Escalation
- Use of already-admin stolen tokens to expand reach into Okta/Azure AD tenants.

Detections: First-time admin logins from suspicious IPs; token scope escalation events.

Defence Evasion
- Tor/VPN use for API calls; blending into legitimate SaaS activity.

Detections: Salesforce/Google Workspace traffic via Tor exit nodes; unusual geos for SaaS API requests.

Credential Access
- Theft of OAuth refresh tokens from Salesloft integration repos.

Detections: GitHub audit logs; token creation without customer initiation.

Discovery
- Enumeration of Salesforce objects (Accounts, Contacts, SSNs, AWS/Snowflake creds).

Detections: Abnormal SOQL query patterns; mass metadata enumeration in API telemetry.

Lateral Movement
- Pivot into Microsoft 365 and Okta via the same token set.

Detections: New admin sessions in AAD/Okta from Tor exit nodes.

Collection/Exfiltration
- Multi-TB exfiltration of Salesforce data via Tor hidden services.

Detections: Large SaaS exports (Drive, SharePoint, Salesforce) from user accounts.

Command & Control
- Leak-site onion portal for comms and extortion negotiations.
- Telegram channels are advertised on the portal.

Detections: Outbound to specific .onion hidden services; new Telegram handles in extortion comms.

Impact
- Threat of releasing ~1 billion Salesforce customer records.
- Victim cards published for Toyota, FedEx, Disney/Hulu, UPS, Aeroméxico, S&P Global, CIC Vietnam, and others.

Detections: Public appearance of victim data on leak portals/forums.

MITRE ATT&CK Mapping

Tactic	Technique (ID)	What it looks like	Fast detection
Initial Access	Valid Accounts (T1078)	Voice-phishing to approve Salesforce OAuth apps	New connected apps approved by end-users
Initial Access	Supply Chain (T1195.003)	Salesloft GitHub repo compromised for OAuth tokens	GitHub logs showing anomalous repo access
Credential Access	OAuth Token Theft (T1552)	OAuth refresh tokens stolen and reused	Token use from new IPs/geos
Execution	Command/Script (T1059)	Bulk SOQL queries run through Salesforce API	Sudden spikes in query logs
Persistence	Valid Accounts (T1078)	Reuse of long-lived OAuth tokens	Repeated token refresh without user action
Discovery	Account Discovery (T1087)	Enumeration of Salesforce objects, SSNs, keys	High-volume SOQL queries
Lateral Movement	Remote Services (T1021)	Token pivot into Okta/M365	First-time admin sessions in Okta/AAD
Exfiltration	Exfil over C2 (T1567.002)	Multi-TB SaaS data pulled via Tor/VPN	Large egress to Tor exit nodes
C2	Tor (T1572)	Use of Tor leak portal for negotiation	Tor traffic alerts
Impact	Data Exposure (T1490)	Threat to release ~1B Salesforce records	Leak-site monitoring

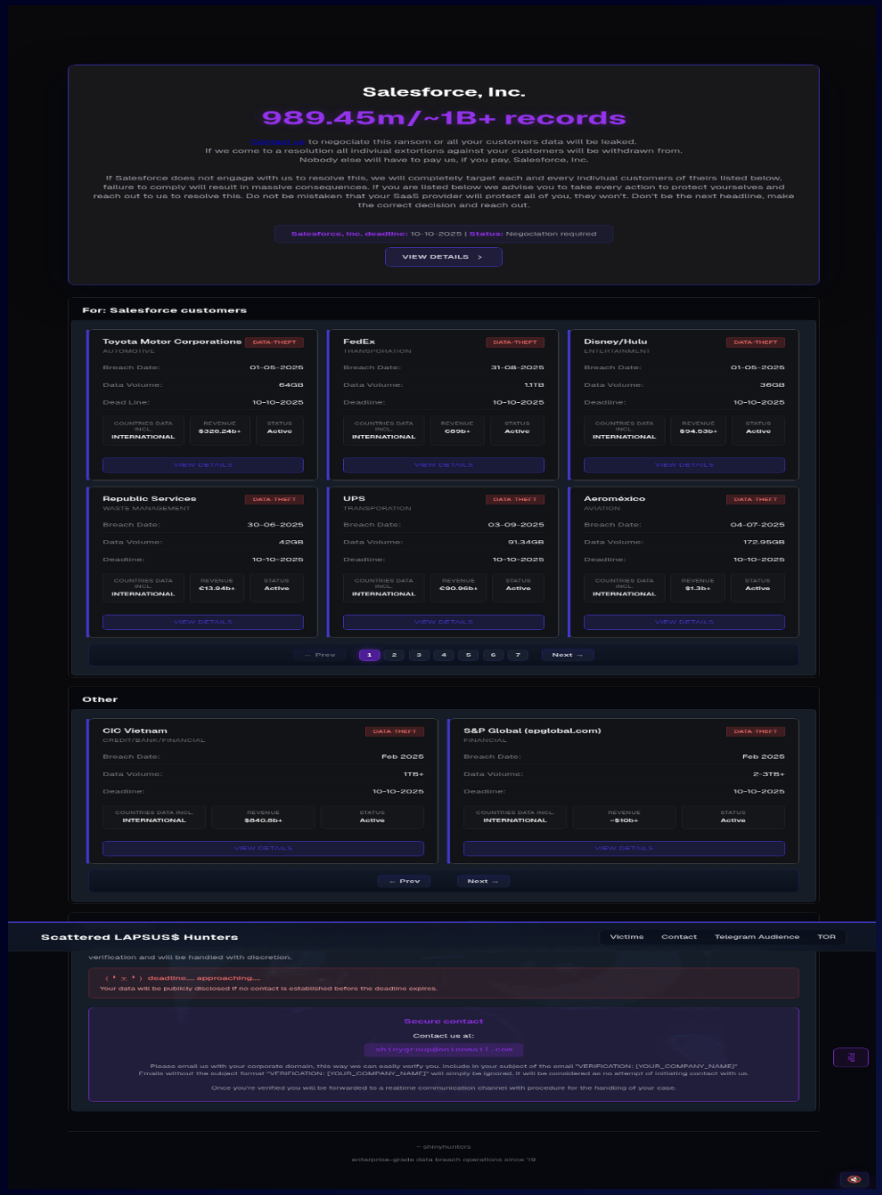
IOCs & Samples

Emails/Handles

- shinygroup@onionmail.com
- Telegram: t.me/sh1nygroup
- Telegram: t.me/SLSH6

Domains/Onion

- shinypogk4jjniry5qi7247tznop6mxdrdte2k6pdu5cyo43vdzmrwid.onion



Mitigation (CE 5.5)

- Endpoint: Auto-isolate on shadow-copy deletion/token theft; block new RMM installs.
- Identity: Enforce phishing-resistant MFA; disable legacy auth; revoke high-risk OAuth apps automatically.
- Network: Block Tor/VPN egress; alert on bulk SaaS exports (Salesforce, Drive, SharePoint).
- Detections: Look for first-time admin activity from helpdesk ranges; track “Reset MFA” spikes; monitor large Salesforce API query bursts.

Worldwide Ransomware Victims

The United States continues to dominate global ransomware activity, representing 57.71% of reported victims this week. Its vast digital infrastructure, financial leverage, and reliance on critical supply chains keep it firmly in the crosshairs of ransomware groups.

Australia followed with a significant 8.96%, reaffirming its position as one of the most heavily impacted Asia-Pacific nations. Canada (4.48%) and the United Kingdom (3.98%) also featured prominently, demonstrating steady targeting of North American and European enterprises.

Mid-tier victims included France (2.49%), Germany (1.99%), and the Netherlands (1.99%), alongside India, Spain, Denmark, Switzerland, and Israel (each between 1.49%–1.99%). These figures underscore the persistent targeting of Europe and Asia, particularly industrialised economies with advanced digital ecosystems.

Smaller-scale incidents (around 1%) were spread across Indonesia, Portugal, Mexico, Japan, and Austria, highlighting ransomware's opportunistic reach.

A broad long-tail of single incidents (0.5% each) was observed in South Korea, Thailand, the United Arab Emirates, Egypt, Ireland, Saudi Arabia, China, Singapore, Kenya, Brazil, Myanmar, Uruguay, and Vietnam. While individually minor, these attacks illustrate ransomware's ability to reach both mature and emerging markets, reinforcing its global scope.

This distribution once again demonstrates ransomware's dual targeting pattern: heavy concentration in high-value economies (U.S., Australia, Canada, U.K., Germany, France), paired with opportunistic strikes across a wide range of smaller nations.

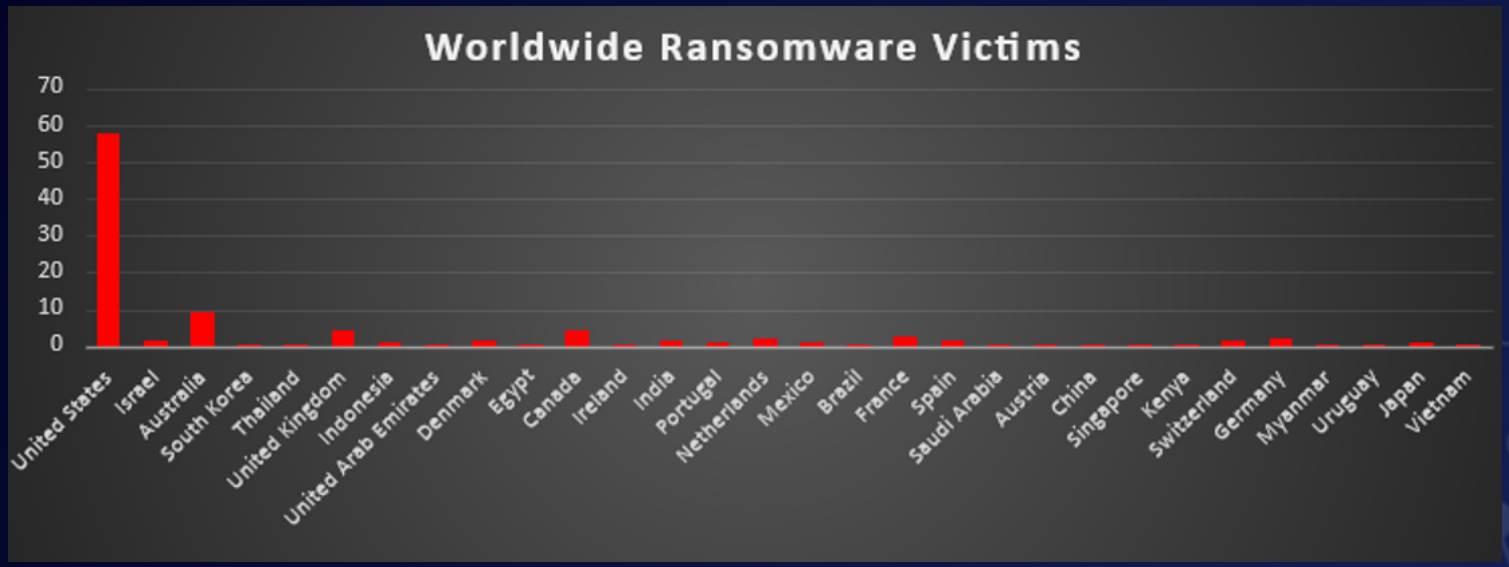


Figure 3: Ransomware Victims Worldwide

Industry-wide Ransomware Victims

Manufacturing remained the most targeted sector this week, representing 17.91% of incidents. Its reliance on legacy systems, operational technology, and intolerance for downtime make it a high-priority target for ransomware groups.

Retail followed closely at 15.92%, reflecting the sector's heavy reliance on customer-facing systems, payment data, and distributed operations, factors that create numerous vulnerabilities for attackers to exploit. Construction ranked third with 11.94%, a reminder of adversaries' focus on project-driven industries where operational disruption directly impacts contractual deadlines and financial flows.

Business Services (9.95%) and Hospitality (7.46%) both remained heavily targeted, underscoring attackers' preference for sectors handling sensitive client information, high transaction volumes, or customer-facing digital systems. Finance accounted for 5.47%, reaffirming its critical role as a high-value extortion target.

Mid-tier incidents were observed across Law Firms (4.98%), Transportation (4.48%), Federal (2.99%), IT (2.99%), Real Estate (1.99%), and Organisations (1.99%). Each of these sectors holds either sensitive legal, regulatory, or operational data, making them attractive despite their lower overall share.

Smaller but still noteworthy targeting included Telecommunications, Minerals & Mining, Media & Internet, Healthcare, Energy, and Consumer Services (each at 1.49%). Insurance reported 1%, while Agriculture registered 0.5%, highlighting ransomware's broad spread across industries regardless of digital maturity or sector size.

This week's distribution highlights ransomware's dual focus: sustained pressure on critical production and customer-facing sectors like manufacturing, retail, and construction, combined with opportunistic attacks across a wide array of industries, ensuring no vertical remains untouched.

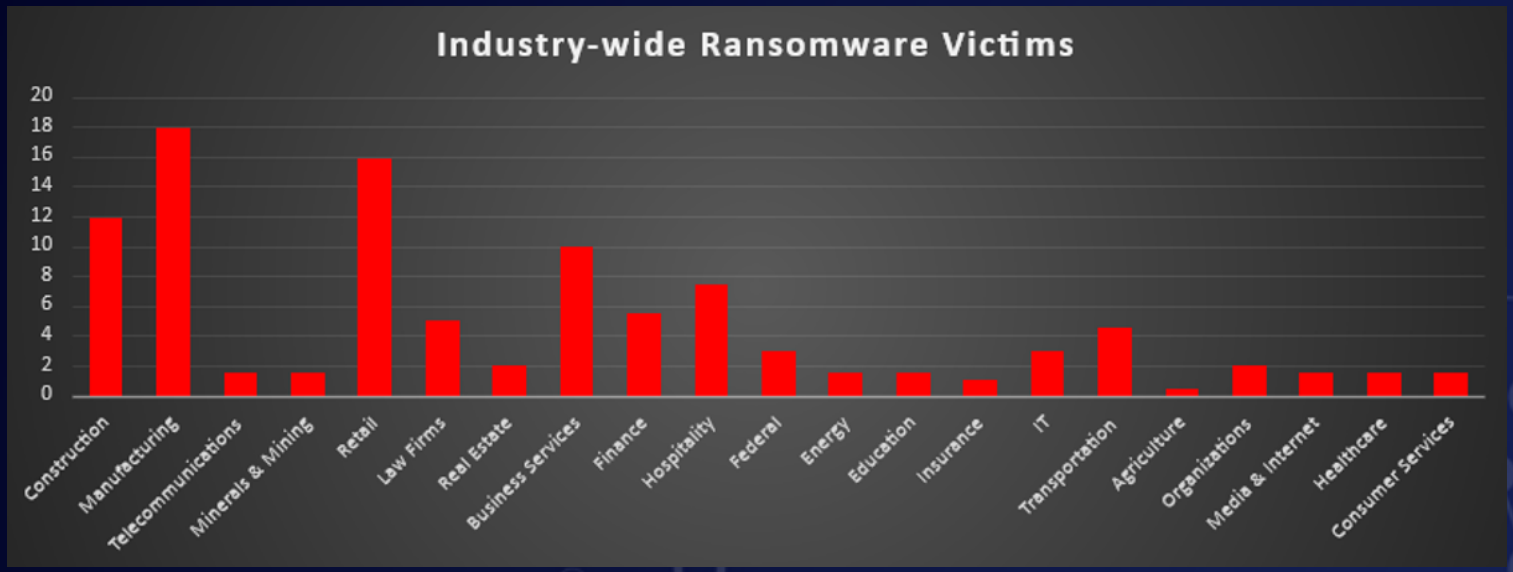


Figure 4: Industry-wide Ransomware Victims