Red Piranha
unified threat management

THREAT INTELLIGENCE REPORT

May 20 - 26, 2025

Report Summary:

- **New Threat Detection Added** – 2
  - BunnyLoader
  - APT28 Russia Macro Loader

- **Detection Summary**
  - **Threat Protections integrated into the Crystal Eye - 144**
  - **Newly Detected Threats – 8**

The following threats were added to Crystal Eye this week:

1. BunnyLoader

BunnyLoader is classified as MaaS (Malware-as-a-Service). This malware is constantly being updated for new functionality and EDR evasion. This includes changing delivery methods and obfuscation methods to evade detection. This malware is capable of stealing information such as credentials and cryptocurrency. It also has the ability to deploy other malware as well.

Rule Set Type:

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

Class Type: Malware

Kill Chain:

Tactic	Technique ID	Technique Name
Defence Evasion	T1027.013	Encrypted/Encoded File
	T1027.011	Fileless Storage
	T1027.002	Software Packing
Collection	T1005	Data from Local System

2. APT28 – Macro Loader

APT28 is identified as a Russian threat actor that has been attributed to Russia's GRU (Main Intelligence Directorate). TAG-110, a group with ties to APT28 has created a macro embedded in Microsoft Word template files (.dotm). When the macro is executed, it places itself in the Word startup folder to gain persistence (\Users\[User name]\AppData\Roaming\Microsoft\Word\STARTUP). Once the document has been added to the startup folder, it will automatically run. This collects information about the system such as Computer Name, Username, Region and System Version. It will then send this information to a C2 server. This C2 server can be used to deploy malware directly on the infected system.

Rules Created: 04
Rule Set Type:

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

Class Type: Trojan-activity
Kill Chain:

Tactic	Technique ID	Technique Name
Initial Access	T1566.001	Phishing: Spearphishing Attachment
Execution	T1059.005	Visual Basic
Command-and-Control	T1071.001	Web Protocols
Persistence	T1547.001	Registry Run Keys/Startup Folder
Collection	T1005	Data from Local System

Known exploited vulnerabilities (Week 4 - May 2025)

Vulnerability	CVSS	Description
CVE-2025-4632	9.8 (Critical)	Samsung MagicINFO 9 Server contains a vulnerability that can allow an unauthenticated remote attacker to write files to an arbitrary location, this vulnerability affects versions 21.1050.0 and earlier and can result in an attacker executing code on the system.
CVE-2023-38950	7.5 (High)	ZKTeco BioTime contains a vulnerability that can allow an unauthenticated remote attacker to read arbitrary files on this system. This vulnerability affects versions 8.5.5 and earlier, and if chained with CVE-2023-38951 and CVE-2023-38952, it may result in an attacker gaining access to the system.
CVE-2024-27443	7.2 (High)	Synacor Zimbra Collaboration Suite contains a vulnerability that can allow an attacker to execute arbitrary JavaScript. This vulnerability can be exploited simply by sending an email with a calendar header, resulting in JavaScript being executed once viewed.
CVE-2025-27920	7.2 (High)	Srimax Output Messenger contains a vulnerability that can allow an authenticated remote attacker to read or write arbitrary files, this vulnerability affects versions before 2.0.63 and can result in an attacker viewing files on the system.
CVE-2024-11182	6.1 (Medium)	MDaemon Email Server contains a vulnerability that can allow a remote attacker to execute arbitrary JavaScript via an email. This vulnerability affects versions before 24.5.1c and results in JavaScript being executed when viewing an email.
CVE-2025-4428	7.2 (High)	Ivanti Endpoint Manager Mobile contains a vulnerability that can allow a remote authenticated attacker to execute code via a crafted API request. This vulnerability may result in an attacker executing code on the system.
CVE-2025-4427	5.3 (Medium)	Ivanti Endpoint Manager Mobile contains a vulnerability that can allow an unauthenticated remote attacker to gain access to the API without authentication. This vulnerability affects versions 12.5.0.0 and earlier, and when combined with CVE-2025-4428 can result in an attacker gaining access to the system.

For more information, please visit the **Red Piranha Forum**:
https://forum.redpiranha.net/t/known-exploited-vulnerabilities-catalog-4th-week-of-may-2025/565

Updated Malware Signatures (Week 4 - May 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 Victims Worldwide

SafePay leads the ransomware landscape this week with 19.15% of total reported attacks. Its consistent growth in activity underscores its operational maturity and possible targeting of high-value infrastructure or poorly defended enterprise networks.

Akira closely follows with 18.09%, continuing its aggressive campaign across both professional service providers and infrastructure-heavy verticals. The group's sustained momentum suggests deep automation or effective affiliate operations.

Stormous makes a strong appearance with 9.57%, possibly reflecting a burst campaign or new victim disclosures. Play also maintains relevance at 8.51%, retaining its status as a high-volume actor known for targeting MSPs and hybrid environments.

Qilin accounts for 7.45%, further cementing its reputation as a persistent mid-tier operator showing steady international reach. Meanwhile, Arcus Media and Devman (each at 5.32%) appear to be ramping up operations, potentially testing new tooling or expanding affiliate networks.

A noticeable cluster of actors including Lynx, Interlock, and Inc Ransom (each at 3.19%) represent the mid-range of current campaigns—active enough to remain on the radar but not dominating the threat landscape.

Rhysida, Kairos, and Space Bears each posted 2.13%, maintaining pressure in niche sectors or geographies. Several smaller groups—Morpheus, RansomHouse, IMN Crew, Killsec3, WorldLeaks, Arkana Security, Bert, Everest, and LeakedData—each contributed 1.06%, a reminder of the long-tail nature of ransomware where many actors operate just below mainstream visibility.

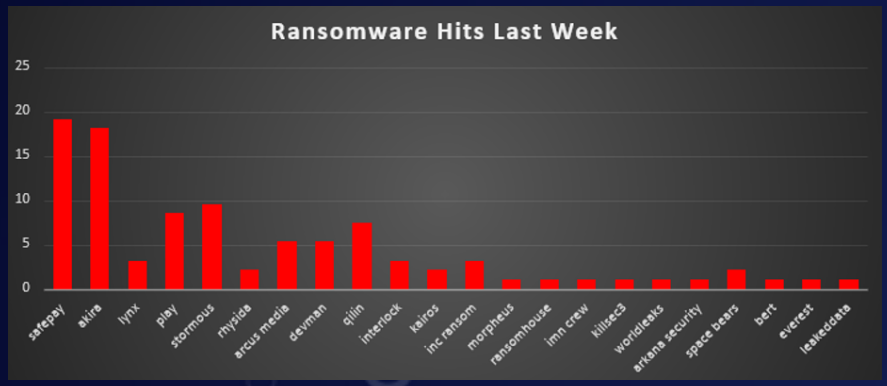


Figure 1: Ransomware Group Hits Last Week

Stormous Ransomware

Stormous is a politically charged, pro-Russian ransomware crew that mixes hacktivist messaging with straightforward profit motives. It is one-fifth of "The Five Families" collective (Stormous, GhostSec, ThreatSec, Blackforums, SiegedSec). In March 2024 the gang partnered with GhostSec to launch the STMX GhostLocker RaaS, giving affiliates both Python (StormCry) and Golang (GhostLocker 2.0) lockers and a dark-web management panel. Between 17 and 23 May 2025, Stormous Leaked a credential dump for multiple French-government agencies (AFD, ARS Île-de-France, Cour des Comptes, etc.). Although the ~70 k credentials were MD5-hashed and partly dated, they pose a phishing/credential-reuse risk.

Breached the hospitality supply chain by attacking HyperGuest's hotel-booking API. Data exfiltrated from partner property Jpark Island Resort & Waterpark included ≥ 30 k plaintext card records, reservation logs and internal docs, obtained via a trusted-relationship entry point instead of an exploit.

Tactics, Techniques, and Procedures (TTPs)

Stormous and its affiliates conduct multi-stage attacks combining both "living off the land" techniques and custom malware. The group's operations mirror those of many modern ransomware crews, with a typical progression from initial intrusion and reconnaissance, through lateral movement and data theft, to final encryption and extortion. Below is a breakdown of observed TTPs, mapped to the MITRE ATT&CK framework:

Initial access: Weak & reused creds are the golden key. They smash exposed RDP/VPN portals with brute-force and credential-stuffing, launch spear-phishing lures tied to their political storylines, and pop unpatched web apps/CVEs. When convenient, they simply ride in on a partner's legitimate API (HyperGuest case) — mapping to Valid Accounts and Trusted Relationship techniques.

Execution & Persistence: Living-off-the-Land meets custom tooling. PowerShell & cmd spawn their Python-built StormCry encryptor (EXE via PyInstaller). Persistence comes from Scheduled Tasks, Run key, rogue Windows services, or a "stormous.php" web shell that doubles as defacer + on-demand encryptor.

Privilege Escalation & Lateral Movement: UAC bypass tricks plus any local vuln they can grab get them admin. Cobalt Strike beacons and built-in PowerShell enumeration fan out, while stolen creds hop over SMB/RDP. They'll even pivot across cloud or partner APIs once domain-level control is in sight.

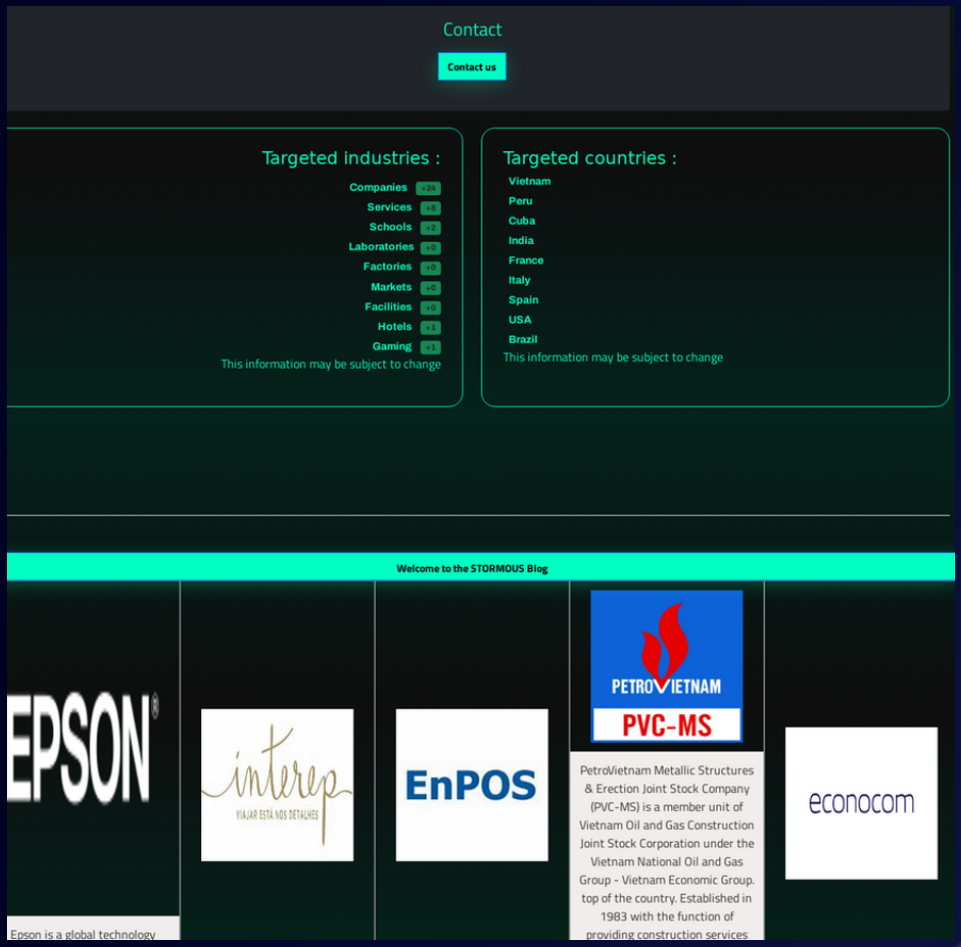
Defence Evasion: Heavy obfuscation, packed binaries, renamed system tools, process/service killing, and shadow-copy wipes. The Python- -EXE wrapper alone dodges some AV heuristics, and web-shell defacements distract blue teams mid-encryption.

Collection & Exfiltration: Double-extortion playbook: zip/7z key datasets, then exfil over HTTPS or straight through already-legit APIs. Cloud storage drops—or direct API queries—keep traffic blend-in low-noise.

Impact & Extortion: StormCry / GhostLocker encrypts with AES-256 + RSA wrapper; adds .stormous, .F5, or .ghost extensions. HTML/TXT ransom notes funnel victims to @StormousBot or TOX, give 3–7-day deadlines, and threaten Tor-site leaks. Ransoms range from a few hundred USD (smaller "Dragon RaaS" ops) to six-figure asks for big-game targets. Proof-of-life file decryption and "discounts" sweeten negotiations—non-payers get doxxed on the "Stormous Blog."

Stage	Tactic	Description
Reconnaissance	Active Scanning (T1595)	Scans for vulnerable servers and exposed RDP/VPN endpoints.
Resource Development	Obtain Capabilities: Tool (T1588.002)	Acquires or develops tools like custom ransomware ("StormCry") and uses leaked tools (Cobalt Strike).
Initial Access	Phishing (T1566)	Sends spear-phishing emails with malicious links or attachments to gain entry.
	Exploit Public-Facing Application (T1190)	Exploits known vulnerabilities in web servers or applications (e.g., SQLi, Log4j) to breach networks.
	Valid Accounts (T1078)	Leverages stolen or default credentials to access RDP/VPN and cloud accounts.
	Trusted Relationship (T1199)	Exploits connections between organisations (partner access) to infiltrate targets (e.g., HyperGuest API abuse).
Execution	Command and Scripting Interpreter (T1059)	Runs commands via PowerShell and cmd.exe to execute payloads and admin tasks.
	User Execution: Malicious File (T1204.002)	Relies on users opening a malware dropper (e.g. enabling a macro or running an EXE) delivered via phish or drive-by.
	Server Software Component: Web Shell (T1505.003)	Deploys web shells (e.g.,stormous.php) on web servers to enable remote code execution and encryption on websites.
Persistence	Scheduled Task/Job (T1053)	Creates scheduled tasks to re-execute malware (for example, to maintain ransomware foothold).
	Boot/Logon AutoStart – Registry Run Keys (T1547.001)	Adds registry Run entries for malware to start at user login.
	Create or Modify System Process – Windows Service (T1543.003)	Installs malicious services for persistence or to launch payloads as SYSTEM.
Privilege Escalation	Abuse Elevation Control Mechanism – UAC Bypass (T1548.002)	Escalates privileges by bypassing User Account Control, often via registry or scripts, to run ransomware as admin (seen in Stormous affiliate toolkit).
Defence Evasion	Obfuscated Files or Information (T1027)	Uses packed or PyInstaller-wrapped binaries, script obfuscation, and string encryption to evade AV detection.
	Disable/Modify Tools – Kill Processes (T1562.001)	Terminates security and backup software processes prior to encryption to avoid interference (e.g., kills databases, AV).
	Indicator Removal on Host (T1070)	Deletes logs or shadow copies to remove evidence and hinder system recovery.
Credential Access	OS Credential Dumping (T1003) [Likely]	(Not directly observed in public reports for Stormous, but likely used) – could use tools like Mimikatz or built-in methods to dump hashes for lateral movement.
Discovery	File and Directory Discovery (T1083)	Enumerates file shares and directories for valuable data prior to exfiltration.
	Network Service Scanning (T1046)	Discovers open ports/services in the network (e.g., scanning for additional RDP/SMB targets); inferred from attacker behaviour.
Lateral Movement	Remote Services: Remote Desktop (T1021.001)	Spreads through the network using RDP with stolen credentials to access other systems.
	Remote Services: SMB/Windows Admin Shares (T1021.002)	Copies or executes tools over SMB (e.g., using PsExec or admin shares to deploy ransomware across hosts).
Collection	Archive Collected Data (T1560)	Compresses and packages stolen data (e.g., into ZIP or 7z archives) prior to exfiltration.
Exfiltration	Exfiltration Over C2 Channel (T1041)	Transfers stolen data out over encrypted channels (HTTPS, TOR). In one case, used Pastebin and APIs as exfil conduits for notes and data.
	Exfiltration Over Web Service (T1567.002)	Uses third-party services (cloud storage, file-sharing sites) or web APIs to exfiltrate data (e.g., pulling records via a partner API).
Impact	Data Encrypted for Impact (T1486)	Deploys ransomware to encrypt files on victim systems using AES-256 + RSA (files renamed with .stormous, .F5, .ghost, etc.).
	Inhibit System Recovery (T1490)	Deletes backups and shadow copies, and may disable recovery services, to prevent victim from restoring data without paying.
	Disk Wipe/Delete (T1487)	(Possibly in some cases) Threat actors might wipe or corrupt certain data after exfiltration to increase pressure, though the primary motive is encryption rather than destruction.

Stormous Ransomware – IOCs
Tor leak sites:
http://3slz4povugieoi3tw7sblxoowxhbzxeju427cffsst5fo2tizepwatid.onion
http://h3reihqb2y7woqdary2g3bmk3apgtxuyhx4j2ftovbhe3l5svev7bdyd.onion
http://h3reihqb2y7woqdary2g3bmk3apgtxuyhx4j2ftovbhe3l5svev7bdyd.onion/stm.html
http://pdcizqzjitsgfcgqeyhuee5u6uki6zy5slzioinlhx6xjnsw25irdgqd.onion



Telegram support bot: @StormousBot, @STORMOUS_HACKER
TOX ID: C286720F7592E5668A932F1D06EDEECBAFACB3BE369632C908F9511D072C142575BA8109CBC6
File Indicators:
stormous.php: PHP web shell that doubles as defacer + encryptor.
Ransom notes: README.txt / README.html – HTML variant often pulls content from Pastebin URL at runtime

File servers:
http://6sf5xa7eso3e3vk46i5tpcqhnlayczztj7zjktzaztlotyy75zs6j7qd.onion

Malware Hashes:
StormCry Windows locker hash 501487b025f25ddf1ca32deb57a2b4db43ccf6635c1edc74b9cff54ce0e5bcfe
Stormous PHP web shell – aa62afd6a48d3c42ed66d4f5b9189be847ec055b
Tools Used
- vssadmin.exe delete shadows /all /quiet (shadow-copy removal)
- taskkill /F /IM <proc> (SQL, Veeam, AV)
- Cobalt Strike beacon or other post-exploitation loaders.

Command-Pattern Detections
- taskkill /F /IM sqlservr.exe
- wmic process call create "cmd /c <locker>.exe"
- Archive staging: 7za a -t7z exfil.7z <dir>

Worldwide Ransomware Victim

The United States continues to be the epicentre of ransomware activity, accounting for a commanding 45.74% of all reported victims last week. Its vast digital footprint, interconnected supply chains, and critical infrastructure make it a prime and persistent target for threat actors across the ransomware spectrum.

Germany follows at 8.51%, reinforcing its position as one of Europe's most frequently attacked economies—driven by its industrial base, robust technology sector, and role in global manufacturing.

The United Kingdom accounts for 5.32%, reflecting ongoing targeting of financial, legal, and professional services, many of which maintain operational ties with U.S.-based entities. France trails closely at 4.26%, further solidifying Western Europe as a favoured region for ransomware operators.

Other notable nations include Canada, Spain, and Turkey (each at 3.19%), where attacks reflect strategic attention to NATO-aligned economies and service providers.

Singapore, Australia, Kenya, and Malaysia each registered 2.13% of attacks, highlighting continued adversary focus on the Asia-Pacific and African regions. These nations represent a mix of financial hubs, cloud-driven economies, and growing digital infrastructures—factors that make them attractive to ransomware groups.

A broad swath of countries—including Italy, Romania, Brazil, Philippines, Maldives, Vietnam, Japan, Greece, Austria, Botswana, Thailand, Czech Republic, Netherlands, Ecuador, South Africa, and Sweden—each experienced 1.06% of attacks. This long-tail distribution confirms the truly global reach of ransomware, where no region is immune, and even smaller or geographically distant economies face increasing risk.

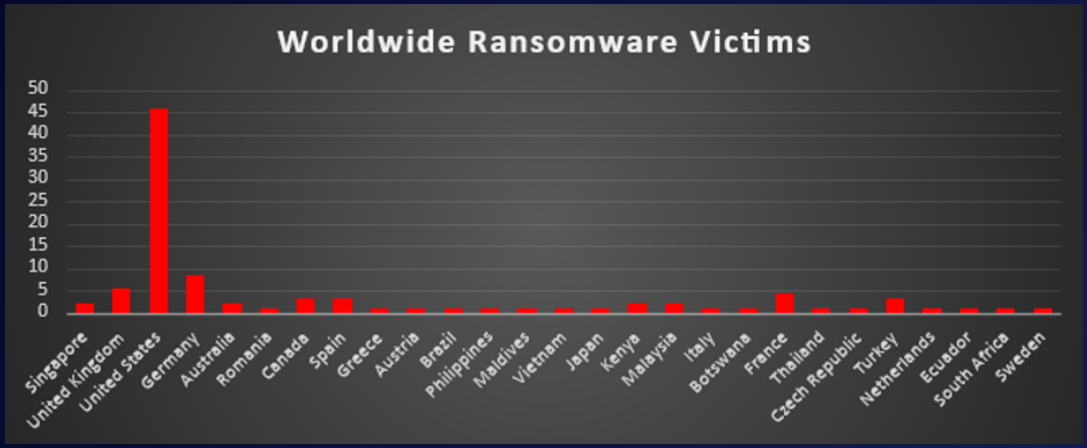


Figure 5: Ransomware Victims Worldwide

Ransomware Victims by Industry

Manufacturing remains the most heavily impacted sector this week, accounting for 15.96% of ransomware incidents. The industry's reliance on uninterrupted operations, coupled with legacy systems and often delayed cybersecurity modernisation, makes it a persistent and attractive target for attackers.

Construction comes in next at 13.83%, reflecting a continued focus on infrastructure-dependent sectors. With growing digitisation in construction logistics and project management systems, this sector presents new vulnerabilities—particularly for smaller firms with limited security staff.

Business Services represents 10.64% of attacks, underscoring the risks associated with third-party service providers, consultancy firms, and outsourcing partners—who often serve as gateways to broader enterprise environments.

Hospitality saw 9.57% of incidents, likely driven by the industry's reliance on centralised booking systems, customer databases, and point-of-sale networks—making it a rich source of both financial and PII data.

Both Retail and Law Firms experienced 7.45% of attacks each. Retail continues to be exploited for its transactional nature and supply chain complexity, while law firms remain high-value targets due to the sensitive legal documents and reputational leverage available to attackers.

A second tier of frequently targeted sectors includes Education, Healthcare, Consumer Services, and Real Estate (each at 4.26%). These industries share common traits such as large user bases, legacy IT infrastructure, and time-sensitive operations—making them attractive to ransomware actors.

Finance and Organisations followed with 3.19% each, while Energy, Telecommunications, and Transportation each experienced 2.13% of reported incidents—highlighting continued threat activity in critical infrastructure and public-facing service sectors.

Lower frequency, but still notable attacks were observed in the Federal, Media & Internet, Minerals & Mining, and Insurance sectors, each accounting for 1.06% of total incidents. Their inclusion illustrates that ransomware actors continue to probe across a wide industry spectrum for gaps in cyber defences.

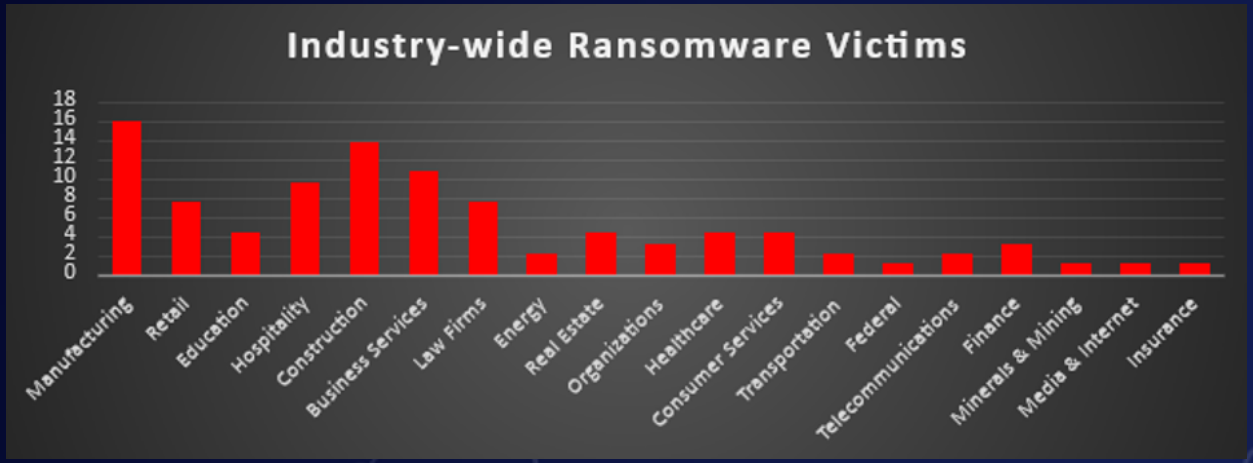


Figure 6: Industry-wide Ransomware Victims