Red Piranha
unified threat management

THREAT INTELLIGENCE REPORT

May 27 - June 02, 2025

Report Summary:

- **New Threat Detection Added**
  - Amatera Stealer
  - APT28 – Cherryspy

- **Detection Summary**
  - **Threat Protections integrated into the Crystal Eye - 116**
  - **Newly Detected Threats – 3**

The following threats were added to Crystal Eye this week:

1. Amatera Stealer

Amatera Stealer is classified as Maas (Malware-as-a-Service). This malware was initially named ACR Stealer but has since been rebranded as Amatera Stealer and is often spread via phishing campaigns or embedded in cracked software. Once infected by this malware, information, such as credentials or cryptocurrency wallets, is obtained, then added to a zip archive and exfiltrated to a C2 server.

Rules Created: 04
Rule Set Type:

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

Class Type: Trojan-Activity
Kill Chain:

Tactic	Technique ID	Technique Name
Defence Evasion	T1027	Obfuscated Files or Information
Credential Access	T1555.003	Credentials from Web Browsers
Collection	T1005	Data from Local System
Command-and-Control	T1071.001	Web Protocols
Exfiltration	T1041	Exfiltration over C2 Channel

2. APT 28 - Cherryspy

CHERRYSPY is a custom Python-based backdoor employed by the Russia-aligned threat group TAG-110 (also known as UAC-0063), which has been active since at least 2021. This malware is designed for cyber-espionage, focusing on data exfiltration and system monitoring across Central Asia, East Asia, and Europe. CHERRYSPY is typically deployed via a multi-stage attack chain involving the HATVIBE loader

Rules Created: 02
Rule Set Type:

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

Class Type: Trojan-activity

Kill Chain:

Tactic	Technique ID	Technique Name
Resource Development	T1583.003	Acquire Infrastructure: Virtual Private Server
Initial Access	T1566.001	Spearphishing Attachment
	T1190	Exploit Public-Facing Application
Execution	T1059.005	Command and Scripting Interpreter: Visual Basic
	T1204.002	User Execution: Malicious File
Persistence	T1053.005	Scheduled Task/Job
Defence Evasion	T1027.013	Encrypted/Encoded Files or Information
	T1218.005	System Binary Proxy Execution: Mshta
Command-and-Control	T1071.001	Application Layer Protocol: Web Protocols
Exfiltration	T1041	Exfiltration Over C2 Channel

Known exploited vulnerabilities (Week 5 - May 2025)

CISA hasn't added any known vulnerabilities in the last week.

Updated Malware Signatures (Week 5 - May 2025)

Threat	Description
Gholoader	GhoLoader is a malware loader often used to deploy follow-on payloads such as remote access trojans (RATs), info-stealers, and ransomware. It is typically delivered via phishing emails or malicious documents. Gh0Loader uses encrypted payloads, reflective loading, and living-off-the-land binaries (LOLBins) for stealth and evasion.
Lumma Stealer	Lumma Stealer is an infostealer sold as Malware-as-a-Service (MaaS), frequently seen exfiltrating browser credentials, crypto wallet data, and session tokens. The presence of Lumma-related C2 domains in traffic logs indicates active data exfiltration or beaconing from infected hosts. Domains may include dynamic DNS or obscure TLDs like .top, .xyz, or .onion.
Gamaredon	Gamaredon, a Russian-linked APT group, is known for using phishing to deliver macro-laced documents and RATs. Recent campaigns leverage the TryCloudFlare reverse proxy service to obfuscate real C2 infrastructure. This technique masks the attacker's server behind Cloudflare's CDN, making detection and takedown more difficult.

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 22.41% of total reported attacks. Its dominant presence highlights a strategic focus on either high-value infrastructure or sectors with lax security postures, suggesting operational maturity and efficient campaign execution.

Qilin follows with 18.97%, maintaining its trajectory as a persistent and aggressive operator. The sustained activity could be indicative of successful affiliate recruitment or consistent exploit reuse across targets.

Datacarry posted 7.76%, marking it as an emerging mid-tier threat actor worth monitoring. Meanwhile, Play continues to hold ground at 6.9%, signalling its continued relevance in targeting hybrid environments, especially MSPs and enterprise networks.

WorldLeaks accounted for 4.31% of hits, possibly reflecting either opportunistic breaches or targeted campaigns in niche sectors. DireWolf and El Dorado followed closely with 3.45% each, indicating a moderate but noticeable presence on the threat landscape.

A cluster of actors, including Devman, Arcus Media, Killsec3, Nova, Crypto24, and Hunters, each contributed 2.59%, suggesting coordinated or exploratory operations, possibly with new tooling or low-resourced affiliates.

Everest, Rhysida, Embargo, Inc Ransom, BlackSuit, and Ransomware Blog each reported 1.72% of activity, indicative of sustained but contained campaigns, often targeting soft or opportunistic assets.

The long tail of the ransomware ecosystem includes Nitrogen, 3AM, Ciphbit, Interlock, Space Bears, Lynx, Chaos, and Arkana Security, each contributing 0.86%. These groups, while individually small in reach, collectively emphasise the fragmented and distributed nature of ransomware threats, with numerous actors operating just below mainstream visibility.

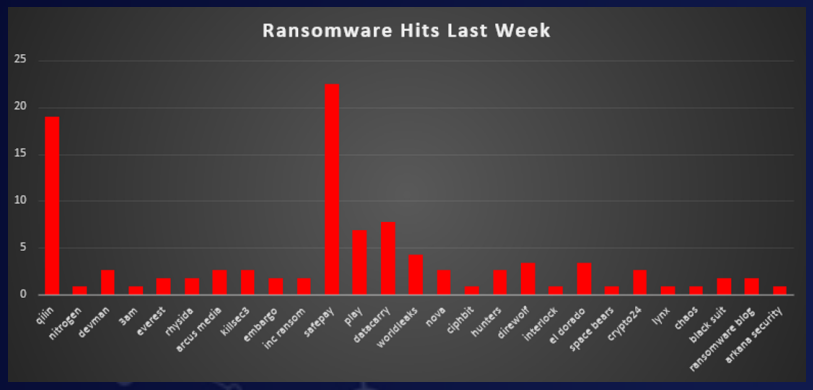


Figure 1: Ransomware Group Hits Last Week

EMBARGO Ransomware

EMBARGO is a relatively new ransomware group that emerged in 2024 and operates under a ransomware-as-a-service (RaaS) model. The group develops Rust-based ransomware payloads and provides them to affiliates (such as the threat actor tracked as Storm-0501) for execution. EMBARGO employs double-extortion tactics – stealing sensitive data before encrypting systems – to pressure victims into paying not only for decryption but also to prevent data leaks. The group maintains a Tor-based leak site to publish stolen data if ransoms are not paid, and claims to be an "international team without any political affiliations," focusing purely on criminal extortion.

Tactics, Techniques, and Procedures (TTPs):

Defence Evasion & Custom Tooling:
EMBARGO deploys a sophisticated toolkit featuring two Rust-based components, MDeployer (loader) and MS4Killer (EDR killer). MS4Killer is uniquely tailored per victim and abuses Safe Mode along with a "Bring Your Own Vulnerable Driver" (BYOVD) technique to disable AV/EDR at the kernel level, often leveraging outdated drivers like ProcMon.sys. It loops continuously to kill respawning security processes.

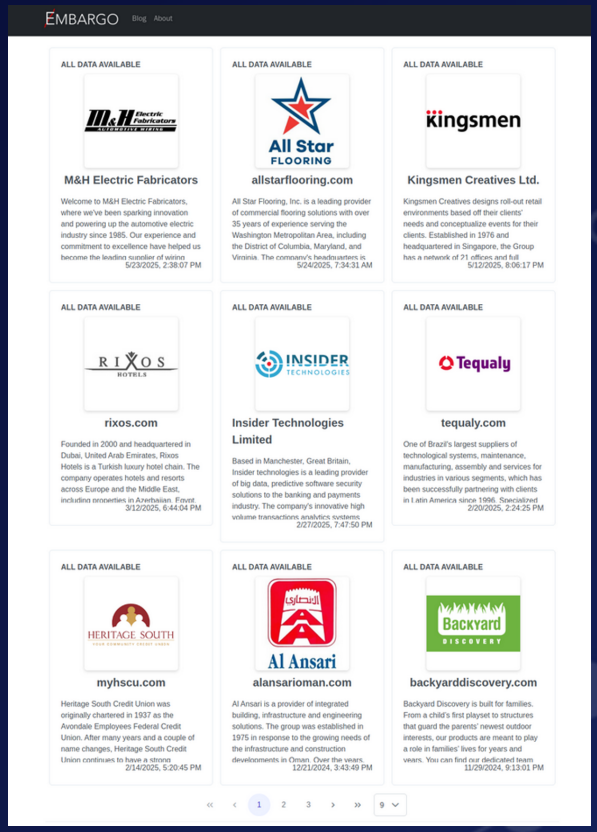
Advanced Evasion Tactics Include:

- Safe Mode Abuse (T1562.009) – Disables most defences by forcing boot into Safe Mode.
- BYOVD Exploits (T1211) – Drops vulnerable drivers for privileged access.
- Malicious WDAC Policy Abuse – Weaponises Microsoft's allowlisting to blind EDR.
- Self-deletion (T1070.004) – Ransomware removes itself post-execution.
- Obfuscated Code & Encrypted Strings (T1140) – Hinders reverse engineering.
- Living-off-the-Land – Uses tools like PowerShell, WMIC for stealth.

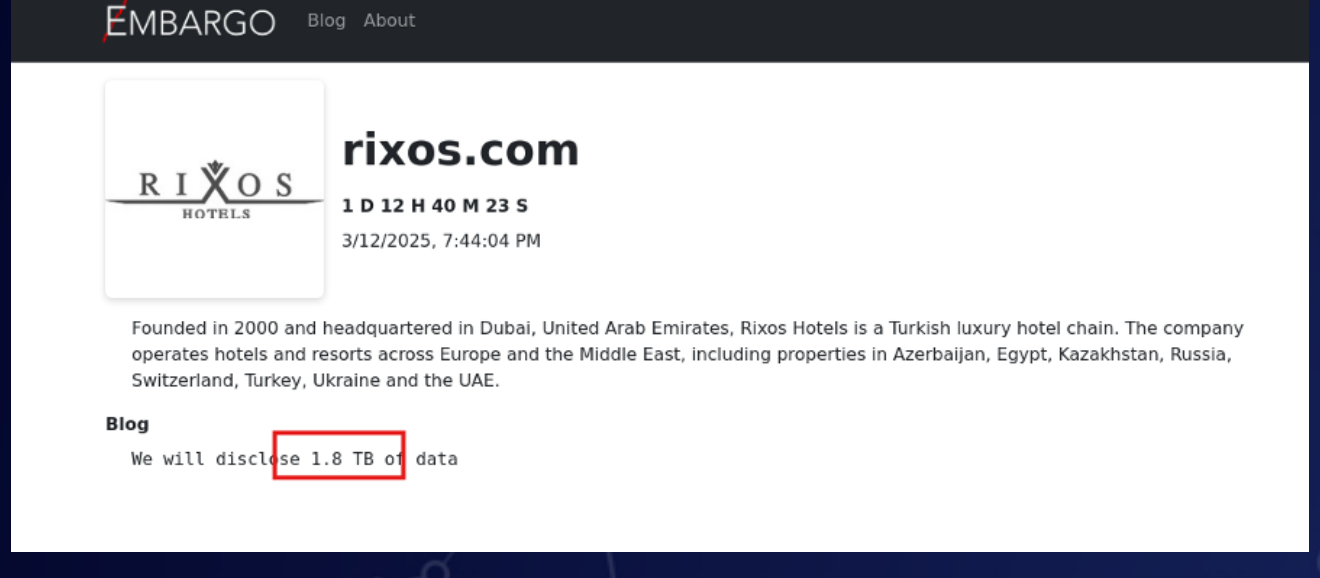
Initial Access & Lateral Movement:
Access vectors likely include phishing, stolen credentials, and MSP/supply-chain compromise. Once inside, EMBARGO conducts reconnaissance, dumps credentials, and moves laterally—typically achieving domain admin access before encryption.

Execution & Persistence:
Payloads are staged via MDeployer, which decrypts MS4Killer and the final ransomware payload in memory (e.g., pay.exe). Safe Mode boot configurations and registry run keys are used to maintain persistence across reboots.

Exfiltration & Impact:
EMBARGO exfiltrates sensitive data prior to encryption (e.g., via secure FTP/cloud). Data theft is followed by fast encryption using ChaCha20 with Curve25519 ECC keys. It disables Volume Shadow Copies (T1490) to prevent recovery. Victims are given 3–7 days before data is leaked, with ransom demands handled via Tor-based portals.



Tactic	Technique ID	Technique Name	Details
Initial Access	T1204.002	User Execution: Malicious File	Likely delivered via phishing attachments or links (requiring a user to open a malware-laced file).
Execution	T1059 / T1569	Command & Scripting Interpreter; System Services	Use of scripts or scheduled tasks to launch payloads (implied, not directly observed). MDeployer executes payloads and may install services for persistence.
Persistence	T1547.001	AutoStart (Registry)/Boot Configuration	Modifies boot settings (Safe Mode) and uses run keys or Startup folder for persistence in Safe Mode.
Privilege Escalation	T1068 / T1211	Exploitation for Privilege Escalation/Defence Evasion	Leverages a vulnerable driver to attain kernel-level code execution (BYOVD), enabling killing of security processes (requires admin access).
Defence Evasion	T1562.001	Disable or Modify Tools	Disables security software: e.g. applying malicious WDAC policy to turn off EDR; uses MS4Killer to kill AV/EDR processes.
Defence Evasion	T1562.009	Impair Defences: Safe Mode Boot	Forces system reboot into Safe Mode, preventing most defence tools from launching.
Defence Evasion	T1070.004	Indicator Removal on Host: File Deletion	Ransomware binary deletes itself after execution to hinder forensics.
Defence Evasion	T1140	Deobfuscate/Decode Files or Info	Ransomware payload has encrypted strings that are decoded at runtime (thwarts static analysis).
Discovery	T1083	File and Directory Discovery	Enumerates files/folders to decide what to encrypt (and possibly to locate sensitive data).
Discovery	T1135	Network Share Discovery	Scans and targets network shares (e.g. NAS, file servers) for encryption across the network.
Collection	T1560/T1005	Archive Data/Data from Local System	Gathers and archives sensitive files prior to encryption (for exfiltration). Specific tools are not public but likely use common archiving utilities.
Exfiltration	T1041	Exfiltration Over C2 or Symmetric Encrypted Channel	Sends stolen data to attacker-controlled servers (e.g. via Tor or cloud services) before ransomware deployment.
Impact	T1486	Data Encrypted for Impact	Encrypts files on victim systems using ChaCha20 encryption, rendering data inaccessible.
Impact	T1490	Inhibit System Recovery	Deletes or disables system backups and shadow copies to prevent easy recovery.
Impact	T1489	Service Stop (Denial of Service)	(Implicit) Likely stops critical services (databases, etc.) to ensure maximum file locking and to disrupt operations further.


EMBARGO
Blog
About
RIXOS
HOTELS
rixos.com
1 D 12 H 40 M 23 S
3/12/2025, 7:44:04 PM
Founded in 2000 and headquartered in Dubai, United Arab Emirates, Rixos Hotels is a Turkish luxury hotel chain. The company operates hotels and resorts across Europe and the Middle East, including properties in Azerbaijan, Egypt, Kazakhstan, Russia, Switzerland, Turkey, Ukraine and the UAE.
Blog
We will disclose 1.8 TB of data

IOCs.
TOX: 9500B1A73716BCF40745086F7184A33EA0141B7D3F852431C8FDD2E1E8FAF9277E9FDC117B47
URLs
http://embargobe3n5okxyzqphpmk3moinoap2snz5k6765mvtkk7hhi544jid.onion/api/blog/get
http://embargobe3n5okxyzqphpmk3moinoap2snz5k6765mvtkk7hhi544jid.onion

File servers
http://z2b75lk7xf6kme3zfvlmdmpwiaansnkcuhsojd23dgub5md24fhogcyd.onion/
http://wg55rcy2chmbpeh6pl5pftnveac2lqfxbletrtzanfjhhmvcjnn5tcqd.onion/

Tor v3 service – negotiation
http://76yl7gfmz2kkjglcevxps4tleyeqnqhfcxh6rnstxj27oxhoxird3hyd.onion
http://yj3eozlkkxkcsprc2fug7tolgtnllruyavuyyar3yzsccjdgvu2bl2yd.onion/
http://y6kyfs2unbfcyodzjrxadn4w5vyulhyotdi5dtiqulxbduujehupunqd.onion/
http://4q5tsu5o3msmv4am4dfhupwhzlyg7wv3lpswbvbhcrknr4ega7xetxad.onion/
http://5dw7bszmidrhpoltqbqmpixpz6mvgez3mr6xc7ktval2glrmbxkwopad.onion/
http://ec6edgevw2lzqy4ipafpbvjuu7r6ugqbljqokl3pvecc6c3a5ix3wgyd.onion/

Ransom Note Filename
HOW_TO_RECOVER_FILES.txt

Encrypted File Extension: .564ba1 (original variant); or 6-hex random (e.g. .b58eeb)
No latest malware sample was found publicly.

Associated Tools:
MDeployer, MS4Killer

Mitigation
Block/alert on the seven new onion hostnames at egress proxies, Tor gateways and DNS-layer firewalls.

1. Hunt for Safe-Mode reboots initiated from domain-admin-level accounts in Windows event logs — still the earliest reliable on-host sign of an impending EMBARGO detonation.
2. Driver block-rules: ensure Microsoft's vulnerable-driver blocklist (or equivalent EDR feature) is enabled to blunt MS4Killer's BYOVD payload (confirmed effective in Beazley's Feb 2025 incident).
3. Monitor WDAC policy pushes; any unsigned or suddenly restrictive policy appearing between 24 May and 2 Jun warrants immediate review.
4. Verify offline backups + immutable snapshots; shadow-copy deletion remains unchanged.

Worldwide Ransomware Victim

The United States remains the epicentre of ransomware activity, accounting for a staggering 52.59% of all reported victims last week. Its extensive digital infrastructure, complex supply chains, and vast economic influence continue to make it the most heavily targeted nation globally.

Canada follows at 7.76%, highlighting the persistent targeting of North American infrastructure, particularly organisations with deep technological integration and cross-border operations.

Australia ranks next with 5.17%, underscoring the country's position as a key economic player in the Asia-Pacific region and an increasingly attractive target for ransomware operators due to its strong adoption of cloud services and digital transformation.

Italy reported 4.31%, reflecting ongoing ransomware pressure on European nations with rich industrial and commercial ecosystems.

The United Kingdom and Germany each registered 2.59%, suggesting continued targeting of financial institutions, government entities, and professional services, often interconnected with U.S.-based networks.

Spain, Belgium, Mexico, and Taiwan each accounted for 1.72%, showing mid-level targeting across Western Europe, North America, and East Asia, regions often engaged in global trade and hosting critical business services.

A large group of countries, Slovenia, United Arab Emirates, Brazil, Argentina, Denmark, Switzerland, South Africa, Lithuania, Ireland, Philippines, Colombia, Thailand, India, Malaysia, Croatia, Czech Republic, South Korea, Indonesia, Peru, China, and Bulgaria, each experienced 0.86% of the total ransomware activity. This long-tail distribution reinforces ransomware's truly global footprint, reaching economies both large and small, and spanning every inhabited continent.

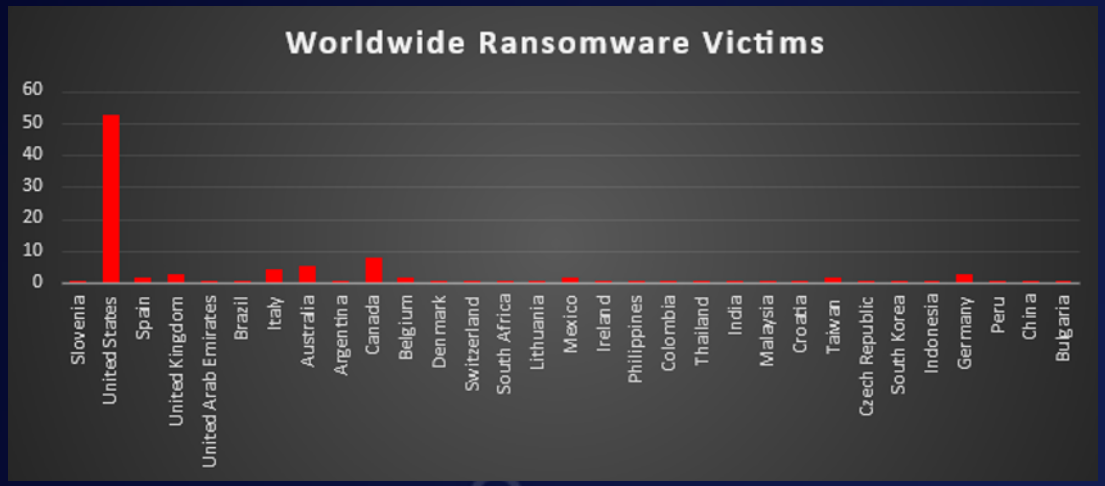


Figure 7: Ransomware Victims Worldwide

Ransomware Victims by Industry

Retail and Manufacturing sectors share the top spot this week, each accounting for 18.10% of all ransomware incidents. Their prominence reflects the ongoing exploitation of critical supply chains, widespread third-party dependencies, and often lagging cybersecurity maturity in operational environments.

Construction and Business Services followed with 11.21% each, showing sustained threat activity in sectors with complex vendor ecosystems and valuable project-based data. These industries often face challenges in securing distributed operations and contractor access points.

Education registered 5.17%, underscoring the continuous threat to academic institutions, which often balance accessibility with limited cybersecurity resources.

Law Firms and Finance each experienced 4.31%, likely driven by the sensitive nature of client data and financial assets housed within these sectors—both of which remain perennial ransomware targets.

A cluster of sectors, including Transportation, Healthcare, Hospitality, and Federal entities, each logged 3.45% of attacks, highlighting attackers' ongoing interest in sectors with mission-critical operations where downtime can generate urgency for ransom payment.

Consumer Services and Insurance were each hit in 1.72% of cases, indicating lower but still notable exposure in customer-facing service verticals.

Other sectors impacted, Organisations, Telecommunications (2.59% each), and Agriculture, Minerals & Mining, Energy, Real Estate, and Electronics (each at 0.86%), demonstrate the extensive breadth of industries targeted. Even traditionally lower-profile sectors are not immune, illustrating the indiscriminate nature of many modern ransomware campaigns.

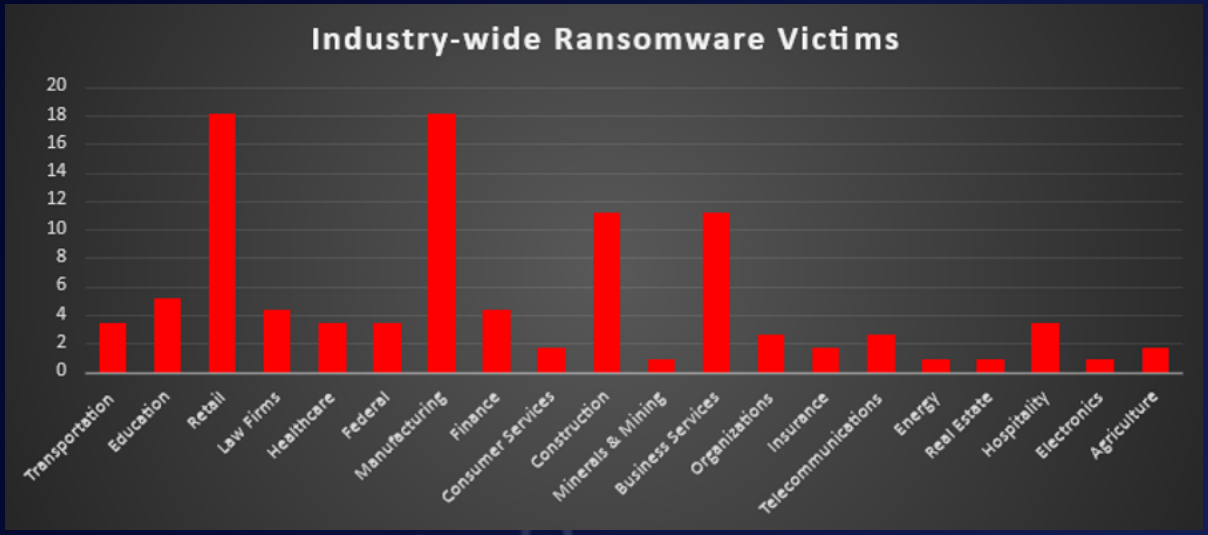


Figure 8: Industry-wide Ransomware Victims