Red Piranha
unified threat management

THREAT INTELLIGENCE REPORT

Sept 09 - 15, 2025

Report Summary:

- **New Threat Detection Added**
  - TinyNuke

- **Detection Summary**
  - **Threat Protections integrated into the Crystal Eye - 219**
  - **Newly Detected Threats - 78**

The following threats were added to Crystal Eye this week:

1. TinyNuke

TinyNuke (otherwise known as Nuclear Bot) is a well-developed banking trojan that includes a HiddenDesktop/VNC server and a reverse socks4 server. After aggressive promotion by the developer, the source code was published on GitHub, which led to ancestors such as XBot.

As TinyNuke has been distributed since 2016, it is not limited to any specific threat actor, and such initial attack vectors can be those of social engineering, zero days, and weak credentials.

Threats Protected: 5
Class Type: Trojan-Activity
Rule Set Type: (https://attack.mitre.org/matrices/enterprise/)

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

Kill Chain:

Tactic	Technique ID	Technique Name
Exfiltration	T1567	Exfiltration Over Web Service
Command-and-Control	T1090.003	Multi-hop Proxy
	T1219.002	Remote Desktop Software
Collection	T1119	Automated Collection

Current Threat Summary

Known exploited vulnerabilities (Week 3 September 2025)

Vulnerability	CVSS	Description
CVE-2025-5086	9 (Critical)	Dassault Systèmes DELMIA Apriso contains a deserialisation vulnerability that can allow an unauthenticated remote attacker to execute code and gain access to the system. This vulnerability affects a wide range of versions from Release 2020 to Release 2025. As DELMIA Apriso is a Manufacturing Operations Management (MOM) and Manufacturing Execution System (MES) solution, production and manufacturing environments have a high risk of being impacted by this vulnerability.

For more information, please visit the **Red Piranha Forum**:
https://forum.redpiranha.net/t/known-exploited-vulnerabilities-catalog-2nd-week-of-september-2025/596

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.”
zgRAT	A Remote Access Trojan (RAT) used in cyberattacks that provides attackers remote access to a machine. Commonly spread in malware loaders and through phishing emails.

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

The Gentlemen dominated this week's ransomware landscape, responsible for 21.09% of observed incidents. Their surge highlights the group's aggressive targeting strategy and continued expansion across multiple geographies.

KillSec3 and Akira each accounted for 10.88% of incidents, underscoring their persistence and adaptability in exploiting diverse entry points. Meanwhile, Play followed closely with 10.2%, continuing its role as one of the more disruptive mid-tier ransomware operators.

Securotrop registered 7.48% of total hits, marking an uptick in their operations. Qilin contributed 6.12%, maintaining its consistent presence in global victimisation trends.

Several groups posted mid-level activity: Inc Ransom (4.08%), Radar (3.4%), Everest (2.72%), Lynx (2.72%), and SafePay (2.72%), reflecting steady campaigns across business services, retail, and manufacturing sectors.

Smaller but noteworthy activity was observed from Beast, Black Nevas, Medusa, MyData, Yurei, Worldleaks, and others (each between 1.36–1.36%), while fringe actors like Cloak, Dragonforce, Warlock, Space Bears, Rhysida, Ransomhouse, Abyss-Data, and Nitrogen appeared at 0.68% each.

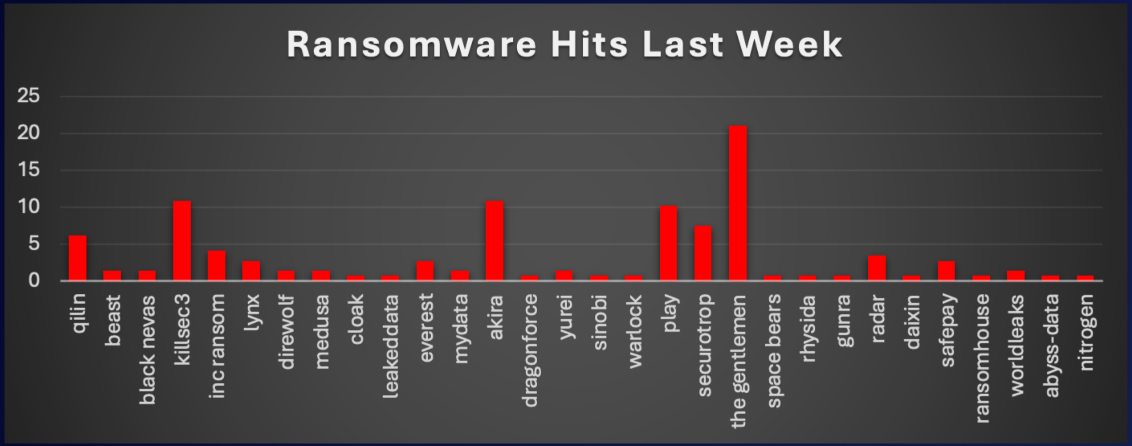


Figure 1: Ransomware Group Hits Last Week

The Gentlemen Ransomware

Red Piranha assesses The Gentlemen as a new, financially motivated ransomware operation active since July 2025. This group demonstrates advanced tradecraft, including the use of vulnerable signed drivers, Group Policy abuse, and double extortion. They have impacted victims across at least 17 countries and multiple industries.
The group appends the extension ".7mtzhh" to encrypted files and drops the ransom note README-GENTLEMEN.txt. Their operations emphasise disabling defences, exfiltrating sensitive data, and then encrypting systems enterprise-wide.

Detailed TTPs
Initial Access
The Gentlemen gain entry through compromised VPN gateways and the use of valid admin credentials. The reliance on FortiGate appliances suggests the exploitation of unpatched vulnerabilities or credential stuffing against exposed services. The use of domain accounts highlights prior credential theft or purchase.
Detections: sudden administrative logons from unusual IPs; anomalous VPN activity.

Execution
Execution is multi-layered: PowerShell scripts disable security tools, while PsExec and Group Policy deliver payloads across the estate. The ransomware binary requires a runtime password to activate its encryption routine, adding an environmental guardrail.
Detections: new domain-wide scheduled tasks; suspicious PowerShell disabling Defender; password-parameterised binary launches.

Persistence
Persistence is maintained via AnyDesk installation, scheduled tasks from GPO, and registry modifications to enable RDP. Attackers may also create hidden admin accounts.
Detections: unexpected AnyDesk installations; new/modified scheduled tasks; registry changes enabling RDP services.

Privilege Escalation
Privilege escalation is not heavily built into the malware itself, but is achieved by tools like PowerRun.exe and the exploitation of signed drivers. These allow SYSTEM-level execution and termination of otherwise protected processes.
Detections: loading of unusual drivers; SYSTEM processes launched by non-system binaries.

Defence Evasion
The hallmark of Gentlemen is impairing defences. Through All.exe/Allpatch2.exe, they load ThrottleBlood.sys to kill AV/EDR processes at kernel level. PowerShell disables Microsoft Defender, exclusions are added, shadow copies removed, logs cleared.
Detections: mass process/service termination; Defender exclusion additions; vssadmin execution.

Discovery
The group maps networks using tools like Advanced IP Scanner and Nmap, and enumerates AD accounts, groups, and domain controllers.
Detections: network scanning from unusual hosts; enumeration of Domain Admins; queries to identify PDC.

Lateral Movement
Propagation is domain-wide through the NETLOGON share and PsExec. Group Policy ensures simultaneous delivery of the ransomware across all machines.
Detections: non-script executables placed in NETLOGON; PsExec launched by non-IT accounts.

Collection & Exfiltration
Files are staged in C:\ProgramData\data before exfiltration via WebDAV or WinSCP. Stolen data is later used for extortion on leak sites.
Detections: anomalous creation of large archives; unusual outbound encrypted transfers.

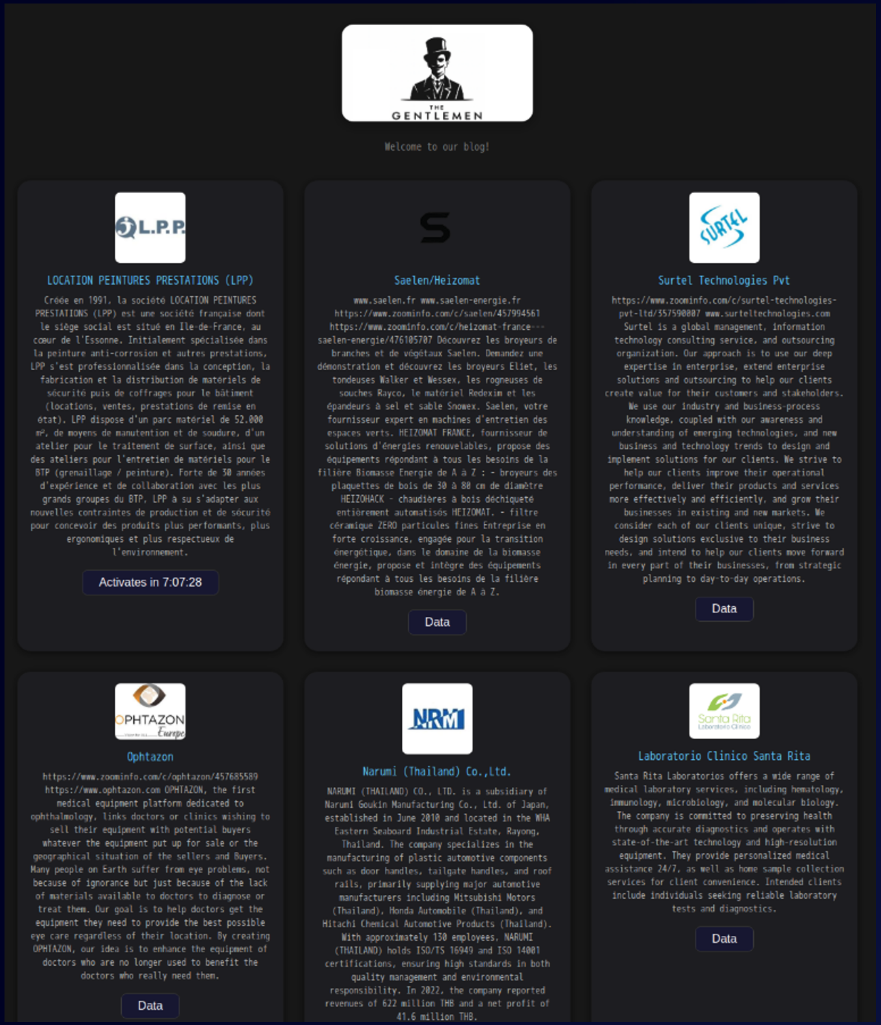
Impact
Encryption halts business operations. Files receive .7mtzhh extension, ransom note README-GENTLEMEN.txt dropped. Services are stopped (backup, database, AV) and recovery inhibited by deleting VSS and logs. A batch file then self-deletes the ransomware binary.
Detections: sudden file renaming to .7mtzhh; ransom notes across directories; shadow copy deletions.

MITRE ATT&CK Mapping

Tactic	**Technique ID**	**How it appears for** Gentlemen
Initial Access	T1133 External Remote Services	Exploitation of FortiGate VPN appliances for entry.
	T1059.001 PowerShell	Defender disabled, exclusions added, system info gathered.
Execution	T1053.005 Scheduled Task	GPO tasks deploy ransomware across domain.
	T1569.002 Service Execution	PsExec is used for remote payload launch.
	T1053.005 Scheduled Task	Scheduled tasks from GPO for persistence.
Persistence	T1136 Create Account	Possible hidden admin accounts created.
	T1547 Boot/Logon AutoStart	Registry edits enabling RDP services.
	T1068 Exploitation for Privilege Escalation	PowerRun.exe executes with SYSTEM privileges.
Privilege Escalation	T1548.002 Abuse Elevation Control Mechanism	Kernel driver abuse (ThrottleBlood.sys) bypasses protection.
	T1562.001 Disable Security Tools	Killing EDR/AV, Defender disabled.
Defence Evasion	T1490 Inhibit System Recovery	Deletion of shadow copies.
	T1562.006 Indicator Blocking	Event logs cleared.
	T1036.005 Masquerading	Tools renamed to blend in (e.g., domain-themed file names).
	T1087 Account Discovery	Enumerates AD users, groups, Domain Admins.
Discovery	T1046 Network Service Scanning	Advanced IP Scanner, Nmap used.
	T1018 Remote System Discovery	Identifies domain controllers and key servers.
	T1021.002 SMB/Windows Admin Shares	NETLOGON share propagation.
Lateral Movement	T1077 Windows Admin Shares	PsExec for lateral execution.
	T1560 Archive Collected Data	Sensitive files are staged in ProgramData folder.
Collection	T1041 Exfiltration Over C2 Channel	Files exfiltrated via WebDAV/WinSCP.
Exfiltration	T1486 Data Encrypted for Impact	.7mtzhh appended, ransom notes dropped.
Impact	T1489 Service Stop	Backup/DB/AV processes killed.
	T1561.001 Disk Wipe: Data Destruction	Shadow copies deleted, logs cleared.

IOCs

- File extension: .7mtzhh
- Ransom note: README-GENTLEMEN.txt
- Hashes:
  - c12c4d58541cc4f75ae19b65295a52c559570054 (Ransomware payload)
  - c0979ec20b87084317d1bfa50405f7149c3b5c5f (All.exe – AV killer)
  - df249727c12741ca176d5f1ccba3ce188a546d28 (Allpatch2.exe – updated AV killer)
  - e00293ce0eb534874efd615ae590cf6aa3858ba4 (PowerRun.exe)
- Driver: ThrottleBlood.sys (abused vulnerable driver)
- C2/Leak site: Onion site http://tezwsse5czllksjb7cwp65rvnk4oobmzti2znn42i43bjdfd2prqqkad.onion/
- Contact: TOX ID F8E24C7F5B12CD69C44C73F438F65E9BF560ADF35EBBDF92CF9A9B84079F8F04060FF98D098E



Welcome to our blog!

LOCATION PEINTURES PRESTATIONS (LPP)

Créée en 1991, la société LOCATION PEINTURES PRESTATIONS (LPP) est une société française dont le siège social est situé en Ile-de-France, au cœur de l'Essonne. Initialement spécialisée dans la peinture anti-corrosion et autres prestations, LPP s'est professionnalisée dans la conception, la fabrication et la distribution de matériels de sécurité puis de coffrages pour le bâtiment (locations, ventes, prestations de remise en état). LPP dispose d'un parc matériel de 52.000 m², de moyens de manutention et de soudure, d'un atelier pour le traitement de surface, ainsi que des ateliers pour l'entretien de matériels pour le BTP (grenaillage / peinture). Forte de 30 années d'expérience et de collaboration avec les plus grands groupes du BTP, LPP à su s'adapter aux nouvelles contraintes de production et de sécurité pour concevoir des produits plus performants, plus ergonomiques et plus respectueux de l'environnement.

Saelen/Heizomat

www.saelen.fr www.saelen-energie.fr https://www.zoominfo.com/c/saelen/457994561 https://www.zoominfo.com/c/heizomat-france---saelen-energie/476105707 Découvrez les broyeurs de branches et de végétaux Saelen. Demandez une démonstration et découvrez les broyeurs Eliet, les tondeuses Walker et Wessex, les rogneuses de souches Rayco, le matériel Redexim et les épandeurs à sel et sable Snowex. Saelen, votre fournisseur expert en machines d'entretien des espaces verts. HEIZOMAT FRANCE, fournisseur de solutions d'énergies renouvelables, propose des équipements répondant à tous les besoins de la filière Biomasse Energie de A à Z : - broyeurs des plaquettes de bois de 30 à 80 cm de diamètre HEIZOHACK - chaudières à bois déchiqueté entièrement automatisés HEIZOMAT. - filtre céramique ZERO particules fines Entreprise en forte croissance, engagée pour la transition énergétique, dans le domaine de la biomasse énergie, propose et intègre des équipements répondant à tous les besoins de la filière biomasse énergie de A à Z.

Surtel Technologies Pvt

https://www.zoominfo.com/c/surtel-technologies-pvt-ltd/357590807 www.surteltechnologies.com Surtel is a global management, information technology consulting service, and outsourcing organization. Our approach is to use our deep expertise in enterprise, extend enterprise solutions and outsourcing to help our clients create value for their customers and stakeholders. We use our industry and business-process knowledge, coupled with our awareness and understanding of emerging technologies, and new business and technology trends to design and implement solutions for our clients. We strive to help our clients improve their operational performance, deliver their products and services more effectively and efficiently, and grow their businesses in existing and new markets. We consider each of our clients unique, strive to design solutions exclusive to their business needs, and intend to help our clients move forward in every part of their businesses, from strategic planning to day-to-day operations.

Ophtazon

https://www.zoominfo.com/c/ophtazon/457685589 https://www.ophtazon.com OPHTAZON, the first medical equipment platform dedicated to ophthalmology, links doctors or clinics wishing to sell their equipment with potential buyers whatever the equipment put up for sale or the geographical situation of the sellers and Buyers. Many people on Earth suffer from eye problems, not because of ignorance but just because of the lack of materials available to doctors to diagnose or treat them. Our goal is to help doctors get the equipment they need to provide the best possible eye care regardless of their location. By creating OPHTAZON, our idea is to enhance the equipment of doctors who are no longer used to benefit the doctors who really need them.

Narumi (Thailand) Co.,Ltd.

NARUMI (THAILAND) CO., LTD. is a subsidiary of Narumi Goukin Manufacturing Co., Ltd. of Japan, established in June 2010 and located in the WHA Eastern Seaboard Industrial Estate, Rayong, Thailand. The company specializes in the manufacturing of plastic automotive components such as door handles, tailgate handles, and roof rails, primarily supplying major automotive manufacturers including Mitsubishi Motors (Thailand), Honda Automobile (Thailand), and Hitachi Chemical Automotive Products (Thailand). With approximately 130 employees, NARUMI (THAILAND) holds ISO/TS 16949 and ISO 14001 certifications, ensuring high standards in both quality management and environmental responsibility. In 2022, the company reported revenues of 622 million THB and a net profit of 41.6 million THB.

Laboratorio Clinico Santa Rita

Santa Rita Laboratorios offers a wide range of medical laboratory services, including hematology, immunology, microbiology, and molecular biology. The company is committed to preserving health through accurate diagnostics and operates with state-of-the-art technology and high-resolution equipment. They provide personalized medical assistance 24/7, as well as home sample collection services for client convenience. Intended clients include individuals seeking reliable laboratory tests and diagnostics.

Detection & Mitigation

Identity & Exposure

- Patch and harden FortiGate VPN appliances; enforce MFA on VPN/RDP/SSO.
- Restrict Domain Controller administrative access.
- Crystal Eye IDM and Crystal Eye SOAR can baseline privileged logins and trigger alerts on anomalies.

Endpoint (Crystal Eye EDR / Crystal Eye XDR)

- Detect and alert on unusual driver loads (ThrottleBlood.sys), mass process kills, or tamper attempts on Defender.
- Monitor for suspicious PowerShell disabling AV or adding blanket exclusions.
- Crystal Eye EDR policies can flag attempts to terminate backup/AV processes or clear logs.

Network (Crystal Eye NGFW / Crystal Eye SOAR)

- Monitor SMB traffic to NETLOGON shares and detect placement of non-script executables.
- Alert on unexpected replication artifacts or GPO script modifications.
- Crystal Eye NGFW can restrict Tor/TOX egress attempts, while Crystal Eye SOAR workflows escalate such events to SOC analysts.

Backup & Recovery

- Maintain immutable/offline backups; test restores routinely.
- Monitor VSS states for deletion events (vssadmin delete shadows).
- Crystal Eye XDR backup monitoring modules can generate early alerts if backup services are stopped.

Hardening & Monitoring

- Enable Windows vulnerable driver blocklist to prevent BYOVD (ThrottleBlood.sys) abuse.
- Enforce tamper protection in endpoint security.
- Audit DCs for new/modified GPOs and logon scripts.
- Crystal Eye XDR’s configuration monitoring can baseline scheduled tasks and flag unauthorised persistence mechanisms.

Worldwide Ransomware Victims

The United States continues to dominate the global ransomware victim landscape, accounting for 54.42% of reported cases this week. This overwhelming share highlights the nation's persistent vulnerability, driven by its large digital economy, diverse industry targets, and lucrative victim profiles.

Canada (4.76%) and Australia (4.08%) represent the next highest concentrations, reaffirming their position as prime targets in the Anglosphere. Both countries have critical industries—energy, healthcare, and business services—that attract threat actors due to their economic importance and frequent reliance on outsourced IT.

The United Kingdom (3.4%) and France (3.4%) also remain in the top tier of impacted nations, alongside Germany (2.72%) and Spain (2.72%), demonstrating ransomware's continued impact across Western Europe. These countries often face double extortion campaigns, where stolen data is weaponised to pressure negotiations.

A middle cluster of victimisation includes Argentina (2.04%), Colombia (2.04%), and the United Arab Emirates (2.04%), reflecting ransomware operators' spread into Latin America and the Middle East. Poland, India, Indonesia, Thailand, and Venezuela each logged 1.36%, signaling a broadening distribution into emerging economies.

Lower-level but still significant incidents were recorded in Brazil, Taiwan, Switzerland, Nigeria, Russia, Panama, Kuwait, El Salvador, Morocco, Sweden, Oman, Japan, South Korea, and Namibia, each registering 0.68% of cases. These isolated but recurring entries underscore ransomware's global reach, affecting both advanced and developing economies across multiple continents.

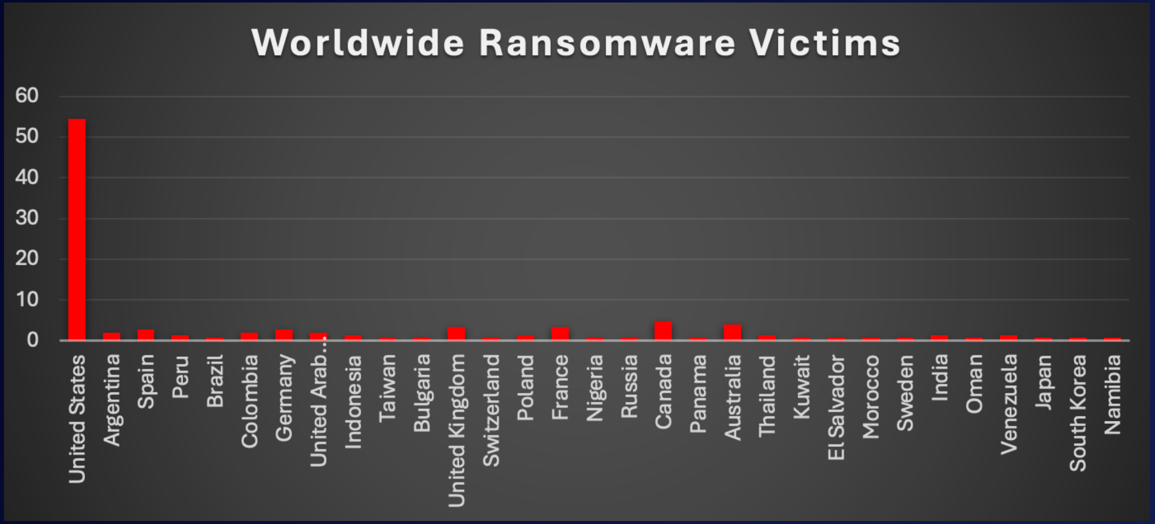


Figure 3: Ransomware Victims Worldwide

Industry-wide Ransomware Victims

Manufacturing continues to be the most heavily targeted sector, accounting for 21.77% of reported ransomware incidents. Its operational criticality, reliance on legacy technologies, and minimal downtime tolerance make it a consistent focal point for ransomware groups.

Business Services follow with 14.97%, reflecting ongoing exploitation of consulting, IT, and outsourcing firms, which often provide attackers indirect access into multiple client environments. Retail ranks third at 11.56%, underscoring its vulnerability due to large transaction volumes, distributed operations, and often inconsistent security standards.

Construction saw 10.88% of incidents, highlighting adversaries' focus on project-driven industries that depend on continuous operational flow. Hospitality registered 6.8%, with attacks likely driven by access to customer payment data and high reliance on digital booking systems. Healthcare came in at 5.44%, reaffirming the sector's ongoing risk due to sensitive patient data and its limited ability to withstand downtime.

Mid-tier victims included IT (4.08%), Finance (2.72%), Energy (2.72%), Transportation (2.72%), and Education (2.72%), each reflecting the high-value or sensitive data they manage. Organisations, Agriculture, Real Estate, and Federal each reported 2.04%, while Law Firms, Telecommunications, Consumer Services, and Insurance each accounted for 1.36% of incidents.

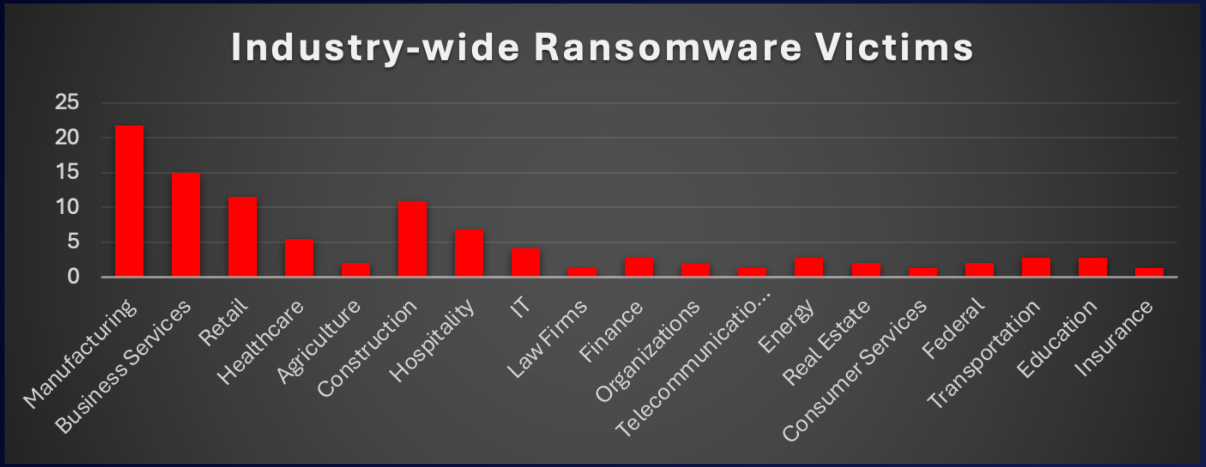


Figure 4: Industry-wide Ransomware Victims