Red Piranha
unified threat management

THREAT INTELLIGENCE REPORT

Sept 02 - 08, 2025

Report Summary:

- **New Threat Detection Added**
  - Rungan
- **Detection Summary**
  - **Threat Protections integrated into the Crystal Eye - 166**
  - **Newly Detected Threats - 34**

The following threats were added to Crystal Eye this week:

1. Rungan

Rungan is a passive C++ backdoor used by a new threat actor dubbed “GhostRedirector” to keep access to at least 65 Windows Servers in Brazil, Thailand, and Vietnam. While Rungan is used to maintain access, its main purpose is to deploy “Gamshen,” which is a native IIS module that can manipulate search engine results to boost the page ranking of a preconfigured target website.

Rungan plants a register to a plaintext hardcoded URL “http://+:80/v1.0/8888/sys.html” into the compromised server, which bypasses normal IIS restrictions by using the HTTP Server API. The backdoor then waits for a request that matches the URL and executes the received commands on the compromised server.

More specifically, Rungan uses the “action” parameter to select between a list of predefined commands, which includes registering new backdoor URLs, creating local users, and arbitrary code execution.

Threats Protected: 4
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	Alert	Alert
OT	Disabled	Disabled

Kill Chain:

Tactic	Technique ID	Technique Name
Initial Access	T1659	Content Injection
Execution	T1059.001	Command and Scripting Interpreter – Powershell & Windows Command Shell
	T1059.003	
Persistence	T1136.001	Create Account – Local Account
	T1505.004	Server Software Component – IIS Components
Command-and-Control	T1071.001	Application Layer Protocol – Web Protocols
Exfiltration	T1567	Exfiltration Over Web Service

Current Threat Summary

Known exploited vulnerabilities (Week 2 September 2025)

Vulnerability	CVSS	Description
CVE-2025-38352	7.4 (High)	Linux Kernel contains a race condition vulnerability within the POSIX CPU component that may result in the elevation of privileges.
CVE-2025-48543	8.1 (High)	Android Runtime contains a use-after-free vulnerability that can facilitate a chrome sandbox escape that can lead to local privilege escalation without user interactivity.
CVE-2025-53690	9.0 (Critical)	Multiple Sitecore products contain a deserialisation vulnerability that can result in unauthenticated remote attackers to execute code on the system. This vulnerability affects Experience Manager (XM), Experience Platform (XP), Experience Commerce (XC) and Managed Cloud products. This vulnerability is due to a misconfiguration where sample machine keys were used during deployment.
CVE-2023-50224	6.5 (Medium)	TP-Link TL-WR841N contains an authentication bypass vulnerability that can allow an attacker within the same network as the router to gain access to the device by sending a HTTP request that results in the disclosure of stored credentials.
CVE-2025-9377	8.6 (High)	TP-Link Archer C7(EU) and TL-WR841N/ND(MS) contain a vulnerability that can allow an authenticated attacker to execute operating system commands on the device via the Parental Control component of the devices. These devices are designated as End-of-life, and although they did receive patches for this vulnerability, it is recommended to replace these devices as they may not receive additional updates in the future.
CVE-2020-24363	8.8 (High)	TP-link TL-WA855RE contains an authentication bypass vulnerability that can allow an unauthenticated attacker on the same network to gain access to the device. This vulnerability occurs due to a missing authentication on the factory reset and reboot endpoint which can enable setting a new administrative password upon reset.
CVE-2025-55177	5.4 (Medium)	Meta Platforms WhatsApp contains a vulnerability that could allow a remote unauthenticated attacker to send a request to a user that would enable the processing of the content from an arbitrary URL. This vulnerability has been known to be combined with CVE-2025-43300 which enabled execution of code on Apple devices.

For more information, please visit the **Red Piranha Forum**:
https://forum.redpiranha.net/t/known-exploited-vulnerabilities-catalog-1st-week-of-september-2025/595

Updated Malware Signatures (Week 2 September 2025)

Threat	Description
TA4903	TA4903 is a financially motivated threat actor known as “Magnet Goblin”. This threat actor typically uses one-day vulnerabilities against publicly facing services as an initial infection vector. Magnet Goblin does not use a specific malware but is known to use, WARPWIRE, Ligolo, and a custom version of NerbianRAT.
TA406	TA406 is a Democratic People's Republic of Korea (DPRK) state-sponsored actor that has been targeting Ukrainian government bodies. They have been utilising phishing credential-stealing and malware components in their attacks. TA406 uses malicious HTML, ZIP, and LNK files that execute PowerShell scripts to exfiltrate information.

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

Lynx emerged as the most active group this week, responsible for 15.6% of all reported ransomware incidents. Its sharp rise suggests concentrated campaigns and possibly expanded affiliate activity.

Qilin followed with 13.76%, reinforcing its position as one of the ecosystem's most consistent and aggressive players. Inc Ransom and Akira both logged 10.09%, underscoring their steady presence as high-impact operators across multiple regions and industries.

SafePay accounted for 7.34%, while DragonForce and Obscura each contributed 6.42%. These groups continue to demonstrate mid-tier but consistent levels of targeting, particularly in opportunistic campaigns.

3AM added 2.75%, while Desolator and Play each registered 3.67%, showing moderate but notable levels of activity.

A cluster of smaller actors, including Warlock, Medusa, Devman2 (all at 1.83%), and a long tail of groups such as Black Nevas, Sinobi, Anubis, Everest, Lunalock, Chaos, WorldLeaks, Gunra, PayoutsKing, Kraken, Nova, Cicada3301, MyData, LeakedData, Rhysida, and Yurei (all at 0.92%) reflect the fragmented nature of the ransomware ecosystem. While individually minor, these actors collectively account for a significant share of global activity and highlight ransomware's decentralised structure.

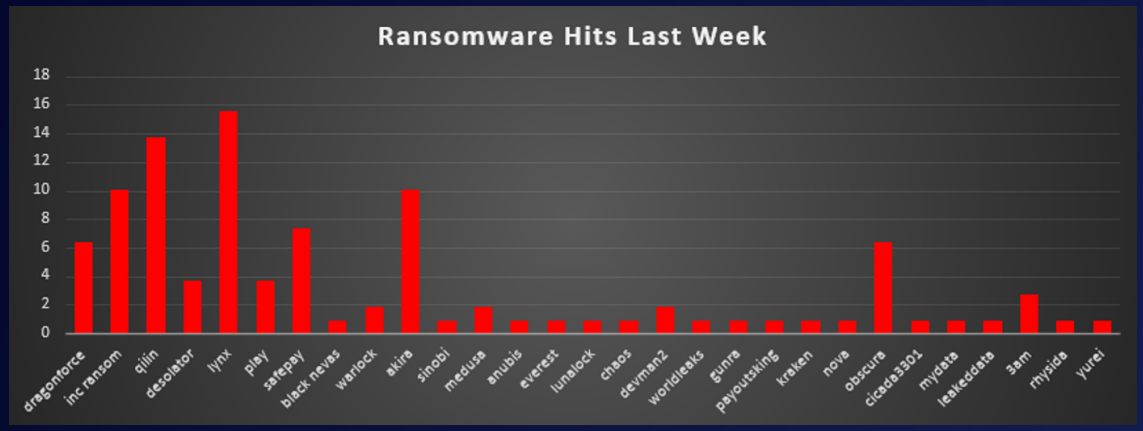


Figure 1: Ransomware Group Hits Last Week

Obscura Ransomware

Red Piranha assesses Obscura as a new, financially motivated ransomware operation. It aims to halt day-to-day work, leverage the risk of reputational and regulatory harm via alleged data theft, and drive fast negotiations under time pressure. Organisations should be prepared for firm deadlines and extortionate messaging.

Obscura is a newly identified Go-based ransomware.

Key points:
- Deployed from the domain controller's NETLOGON share via scheduled tasks (e.g., SystemUpdate), resulting in rapid enterprise-wide propagation.
- Requires administrative privileges; exits if not elevated.
- Disables recovery (vssadmin delete shadows) and kills security/backup/database processes prior to encryption.
- Implements XChaCha20 file encryption with Curve25519 (X25519) key exchange; appends a 64-byte footer containing the string "OBSCURA!", a 32-byte public key, and a 24-byte nonce.
- Excludes core system and boot files from encryption to maintain OS stability.

Detailed TTPs

Initial Access
- Status: Unknown (insufficient telemetry).
- Likely techniques (contextual):
  - T1078 – Valid Accounts (use of domain context and DC staging suggests pre-existing privileged access).
  - T1133 – External Remote Services (later RDP enablement hints at remote-access reliance, but initial vector remains unconfirmed).

Detections/alerts: failed/successful logons to admin groups; anomalous DC logons; first-seen admin from unusual source IPs.

Execution
- T1053.005 – Scheduled Task/Job: Scheduled Task
  - Observed: Enterprise-wide scheduled task "SystemUpdate" executed the payload from NETLOGON.
- T1059.003 – Command Shell
  - Observed: cmd.exe used as the container for follow-on commands (e.g., VSS deletion, firewall change).
- T1480.001 – Execution Guardrails: Environmental Keying
  - Observed: DAEMON environment variable gates encryption vs. prep stages.

Artifacts/commands:
- Task names: SystemUpdate (multiple hosts).
- cmd.exe /c ... wrappers for host-prep commands.

Detections/alerts: new scheduled tasks on multiple hosts; task creation from DC context; command interpreter spawned by task scheduler.

Persistence
- T1053.005 – Scheduled Task/Job: Scheduled Task
  - Observed: Scheduled tasking provided reliable re-execution across the estate.

Detections/alerts: persistence baselining; new/modified tasks post-logon; tasks pointing to SYSVOL/NETLOGON paths.

Privilege Escalation
- Status: Not observed (hard requirement on admin, no built-in elevation).
- Guardrail: Binary exits if not running with administrative rights (token membership check).

Detections/alerts: processes exiting with explicit "not admin" logic; programs relaunching only under elevated tokens.

Defence Evasion
- T1036.003 – Masquerading: Rename System Utilities / Domain-Themed Naming
  - Observed: Binary named to mimic the domain to blend with DC assets.
- T1562.001 – Impair Defences: Disable or Modify Tools
  - Observed: Large process kill list targeting EDR/AV/backup/DB/monitoring/virtualisation agents.
- T1490 – Inhibit System Recovery
  - Observed: VSS snapshot removal: vssadmin delete shadows /all /quiet.
- T1562.004 – Impair Defences: Disable or Modify System Firewall
  - Observed: Task “iJHcEkAG” enabling RDP through Windows Firewall: cmd.exe /C netsh firewall set service type=remotedesktop mode=enable > \Windows\Temp\... 2>&1
- T1027 – Obfuscated/Compressed Files and Information
  - Observed: Ransom note stored base64-encoded within the binary (decoded at runtime).

Detections/alerts:
- Sudden termination of multiple security/backup processes; VSS deletions; firewall rule changes enabling RDP; first-seen executables with domain-like names under SYSVOL.

Discovery
- T1082 – System Information Discovery
  - Observed: CPU core count via system APIs; host role checks.
- T1083 – File and Directory Discovery
  - Observed: Enumeration of all storage devices and capacities to plan encryption coverage.
- (Windows domain awareness) Domain role checks via system APIs to print role-specific messages.

Detections/alerts: unusual volume enumeration by non-backup processes; frequent device/volume queries; domain-role API usage by non-system binaries.

Lateral Movement / Distribution
- T1021.002 – Remote Services: SMB/Windows Admin Shares (distribution vector via domain share)
  - Observed: Payload placed in C:\WINDOWS\sysvol\sysvol\[domain].local\scripts\ (NETLOGON) — replicated across DCs.
- T1053.005 – Scheduled Task (Domain-wide)
  - Observed: Tasking leveraged to fan-out execution to multiple endpoints.

Detections/alerts: new binaries in SYSVOL\scripts; unexpected replication of non-script executables; scheduled task creation sourced from DCs.

Command-and-Control
- Status: Not evidenced (no standalone C2 channel observed in telemetry).
- Operator comms (extortion phase): [claimed] Contact via TOX and onion site in the ransom note.

Detections/alerts: Tor/TOX egress attempts from servers; first-seen outbound to Tor nodes.

Collection & Exfiltration
- Status: [claimed] data theft in note; not directly evidenced in observed host activity.

Detections/alerts: server-side transfers to cloud storage/Tor; large anomalous SMB reads from file servers; egress volume spikes.

Impact
- T1486 – Data Encrypted for Impact
  - Observed: File encryption across enumerated storage; ransomware note dropped to C:\README-OBSCURA.txt; encrypted files marked with .obscura and a per-file footer (identifier + public key + nonce).
- T1489 – Service Stop
  - Observed: Stopping/killing databases, backup agents, logging, and security services prior to encryption.

MITRE ATT&CK Matrix

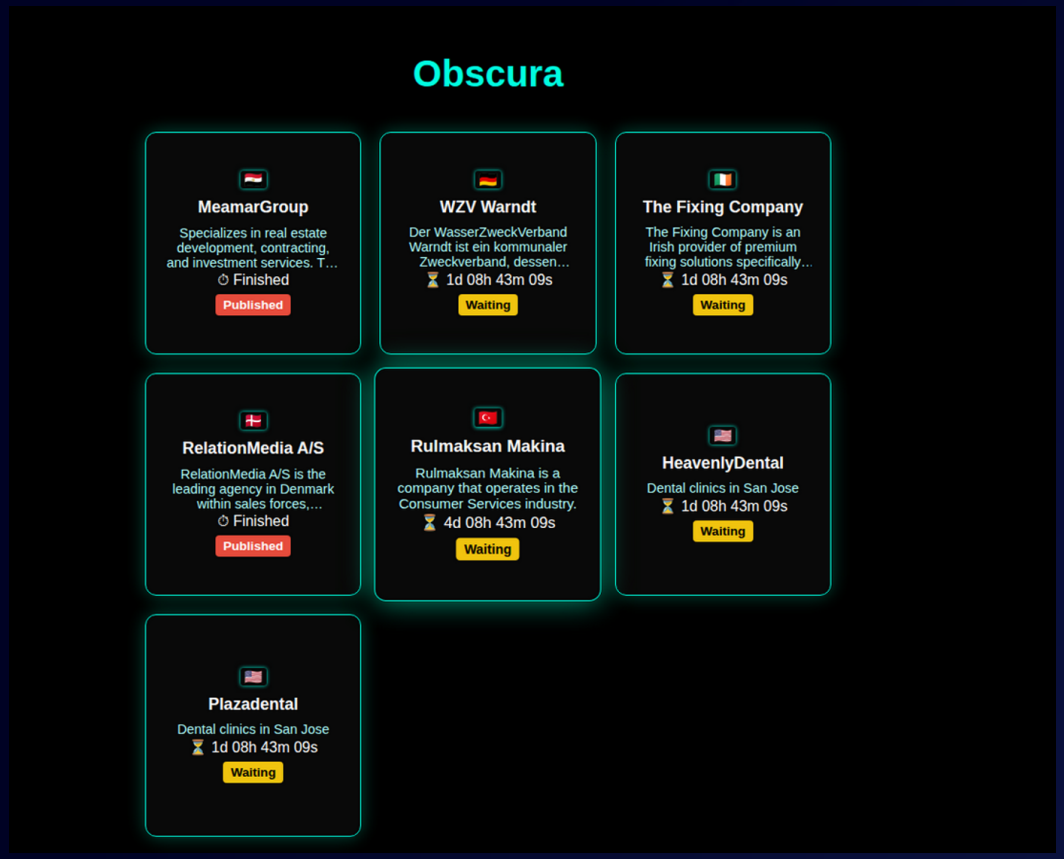
Tactic	Technique	How it appears for Obscura
Initial Access	T1078 Valid Accounts / T1133 External Remote Services (suspected)	Initial vector not directly observed; environment suggests domain-wide execution from DC NETLOGON.
Execution	T1053.005 Scheduled Task / T1204 User Execution (possible)	Scheduled task "SystemUpdate" across hosts; task "iJHcEkAG" modifying firewall.
Privilege Escalation	— (requires admin already)	Exits if not admin; relies on existing admin context.
Defence Evasion	T1562.001 Disable Security Tools / T1490 Inhibit System Recovery / T1480 Execution Guardrails	Kills EDR/backup/DB processes; deletes VSS; DAEMON gating for staged execution.
Discovery	T1082 System Information Discovery	Enumerates CPU cores and storage devices.
Credential Access	—	No direct capability observed.
Lateral Movement	—	No explicit code beyond DC-based distribution; implied via DC role messages.
Impact	T1486 Data Encrypted for Impact	XChaCha20 encryption with Curve25519 key exchange; exclusion list to maintain stability.

IOCs
[company name].exe à Ransomware executable (placed on DC NETLOGON share)
SHA256:
c00a2d757349bfff4d7e0665446101d2ab46a1734308cb3704f93d20dc7aac23
README_Obscura.txt

```
Good day! Your company has failed a simple penetration test.

>> Your network has been completely encrypted by our software.

Our ransomware virus uses advanced cryptography technology that will make it very difficult for you to recover

>> All information has been stolen.
We have stolen all information from all devices on your network, including NAS. The data includes but is not li

>> You have about 240 hours to respond.
If there is no response, all stolen information will be distributed.
We are waiting for you to decide to write to us, and we will be happy to negotiate a ransom price with you. By
1) a report on how we infiltrated your network
2) instructions + software that decrypts all files
3) our assistance in recovery, if needed.

>> They will not help you; they are your enemies.
Recovery agencies, the police, and other services will NOT HELP you. Agencies want your money, but they do not

If you think you can restore your infrastructure from external backups that we did not access, we warn you:
1) The laws of any country impose huge fines on companies for information leaks.
2) Playing against us will not work in your favor. We will gladly wipe every one of your servers and computers.

When you write to us, we expect to hear from you who you are and what your relationship to the company is.
Your ID: [REDACTED]
TOX: [REDACTED]
Blog: http://obscurad3aphckihv7wptdxvdnl5emma6t3vikcf3c5oiiqndq6y6xad.onion/
Obscura. 2025.
```

C:\WINDOWS\sysvol\sysvol\[domain].local\scripts\ à Threat actor ops folder

http://obscurad3aphckihv7wptdxvdnl5emma6t3vikcf3c5oiiqndq6y6xad.onion/



Detection & Mitigation

- Identity & Exposure

Enforce MFA on RDP/VPN/SSO; remove direct internet-exposed RDP; restrict DC admin access.

- Endpoint (CE-EDR / CE-XDR)

Alert on execution from NETLOGON paths; creation of enterprise-wide scheduled tasks; vssadmin shadow deletions; bulk process kills of EDR/backup/DB services; base64 decode routines writing to C:\README-OBSCURA.txt.

- Network (CE-NGFW / CE-SOAR)

Monitor SMB traffic to NETLOGON shares; alert on unusual replication artifacts; restrict Tor/MEGA access from servers.

- Backup & Recovery

Maintain immutable/offline backups; monitor VSS states; routinely test restores.

- Hardening & Monitoring

Audit DCs for new/modified GPOs and scripts; baseline scheduled tasks; monitor for netsh firewall modifications enabling RDP.

Worldwide Ransomware Victims

The United States remains the overwhelming leader in ransomware victimisation, representing 60.55% of all reported cases this week. This concentration underscores its persistent attractiveness for threat actors due to its large digital footprint, high-value enterprises, and critical infrastructure sectors.

Canada followed with 5.5%, reflecting a steady rise in incidents, while Germany logged 4.59%, highlighting sustained pressure on Europe's largest economy. Australia accounted for 2.75%, maintaining its status as a notable Asia-Pacific target.

A mid-tier group of nations—including Spain, Mexico, France, Ireland, India, and the United Kingdom—each reported 1.83% of incidents. These figures illustrate the consistent focus on Western and emerging economies with highly interconnected supply chains.

The long tail of countries, each registering 0.92%, reflects ransomware's global reach. This includes Vietnam, Colombia, Austria, Argentina, Switzerland, Belgium, Thailand, Taiwan, China, South Korea, Singapore, Turkey, Egypt, Japan, Sri Lanka, and Denmark. While these numbers are individually small, collectively they demonstrate ransomware's opportunistic spread across regions with varying levels of cybersecurity maturity.

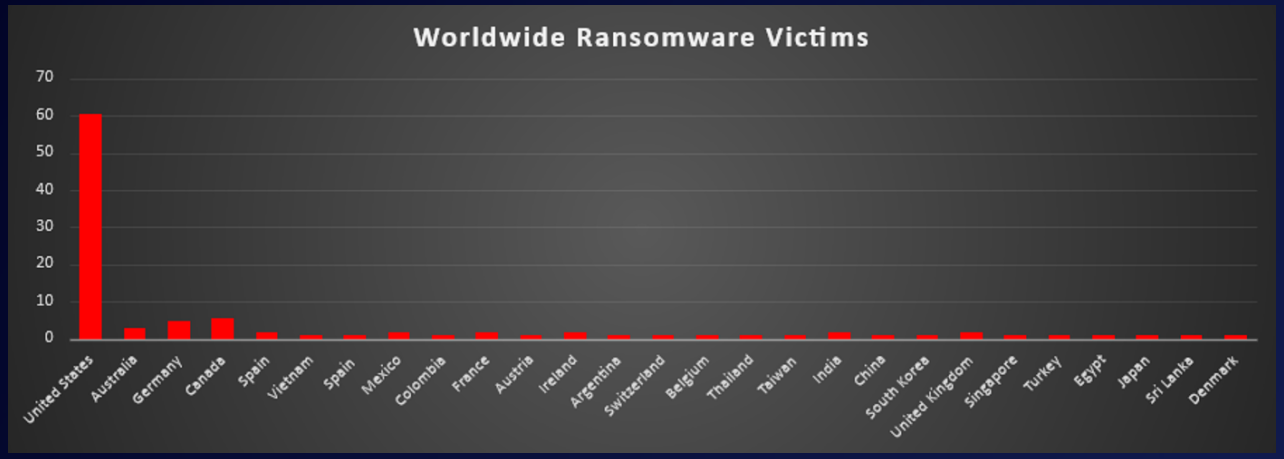


Figure 4: Ransomware Victims Worldwide

Industry-wide Ransomware Victims

Manufacturing remains the hardest-hit sector this week, representing 19.27% of all reported ransomware incidents. Its heavy reliance on operational continuity and legacy infrastructure continues to make it a high-value target where downtime creates significant leverage for attackers.

Business Services followed closely at 15.6%, reflecting adversaries' strategic targeting of firms that provide IT, consulting, and back-office support across multiple industries. Compromising these entities often creates ripple effects that extend far beyond a single victim organisation.

Hospitality reported 12.84%, highlighting its vulnerability due to centralised booking systems, payment infrastructure, and reliance on always-on operations. Construction and Retail also saw high levels of activity at 11.93% and 11.01% respectively—both sectors often managing decentralised supply chains and sensitive financial records, making them ripe for disruption.

Mid-tier targeting was observed in Education (4.59%), Real Estate (3.67%), and Finance (3.67%), all sectors where proprietary information and sensitive customer data offer significant extortion value.

A secondary cluster of incidents included Consumer Services, Agriculture, and Media & Internet (each at 2.75%), alongside Law Firms, Telecommunications, and Federal institutions (each at 1.83%). These figures reinforce ransomware's opportunistic spread into both critical and commercial verticals.

Smaller but noteworthy activity was also seen in IT, Healthcare, and Transportation (all at 0.92%), reminding us that even industries with comparatively fewer reports are far from exempt from ransomware exposure.

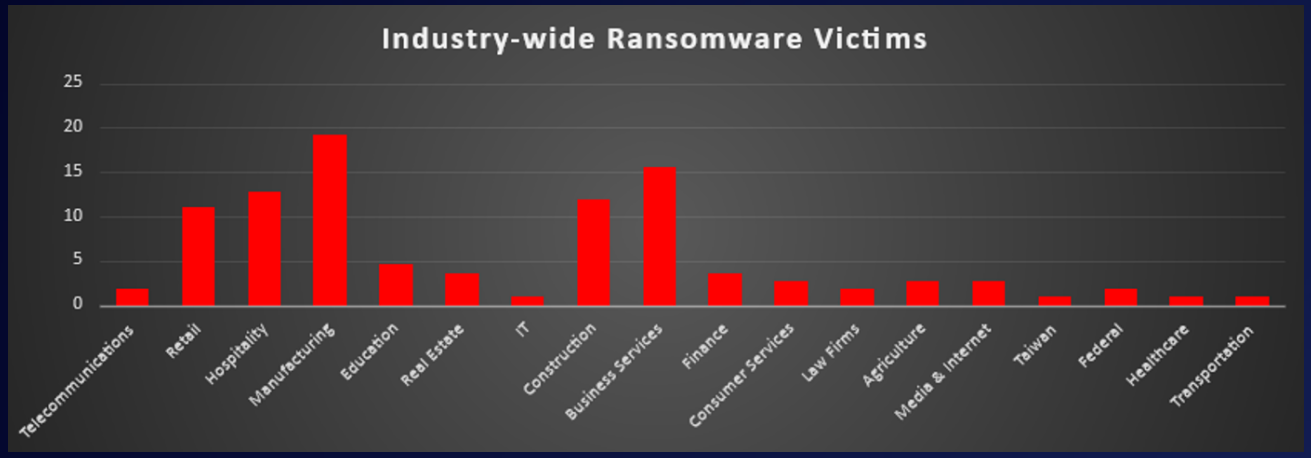


Figure 5: Industry-wide Ransomware Victims