THREAT INTELLIGENCE REPORT

February 10 - 16, 2026

Red Piranha
unified threat management

Report Summary:

New Threat Detection Added

- ROKRAT
- MacSync

Detection Summary

- New Threat Protection: 314
- Newly Detected Threats: 10

The following threats were added to Crystal Eye this week:

1. ROKRAT

ROKRAT is specialised malware created by North Korea-backed APT 37, also known as ScarCruft. The malware is known to be delivered via spear phishing attacks to mainly South Korean victims. The malware is delivered in various forms such as documents, LNK files, and ZIP files.

The most recent versions of ROKRAT are being delivered in a zip file. Once unzipped, it contains a LNK file (Shortcut) that's disguised as a PDF and docx file. The malicious LNK file contains obfuscated batch commands and C# that execute PowerShell to execute the malicious custom PowerShell script.

The script decodes the initial C# Code that loads the first stage of malware into memory while also removing malicious code from the decoy documents.

The malware does various checks for sandbox/vm detection and collects victim information while preparing the second loader. The second loader downloads autoit3.exe (automation tool) to execute a custom script, installing a backdoor to the victims' devices that are linked to a C2 host.

Threats Protected: 1
Class Type: Domain-C2
Rule Set Type:

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

Kill Chain:

Tactic	Technique ID	Technique Name
Initial Access	T1566.001	Phishing: Spearphishing Attachment
Execution	T1204.002	User Execution: Malicious File
Defence Evasion	T1140 T1070	Deobfuscate/Decode Files or Information Indicator Removal
Discovery	T1497	Virtualisation/Sandbox Evasion
Collection	T1119	Automated Collection

2. MacSync

MacSync is a malware targeting macOS environments. The malware abuses code-signing and the notarisation process (Apple's process for checking third-party apps for malicious components) to bypass macOS Gatekeeper protections (Ensures only trusted software is able to run).

MacSync contains various defence functions such as decoy files, execution-chain clean up and sandbox detection to avoid analysis and detection. The malware harvests credentials and exfiltrates the data.

Threats Protected: 4
Class Type: Trojan-Activity
Rule Set Type:

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

Kill Chain:

Tactic	Technique ID	Technique Name
Execution	T1059	Command and Scripting Interpreter
Defence Evasion	T1553.001	Subvert Trust Controls: Gatekeeper Bypass
	T1553.002	Subvert Trust Controls: Code Signing
	T1497	Virtualisation/Sandbox Evasion
Collection	T1005	Data from Local System
Exfiltration	T1041	Exfiltration Over C2 Channel

Current Threat Summary

Known Exploited Vulnerabilities (Week 2 - February 2026)

Vulnerability	CVSS	Description
BeyondTrust Remote Support (RS) and Privileged Remote Access (PRA)	9.9	BeyondTrust Remote Support (RS) and Privileged Remote Access (PRA) contain a command injection vulnerability that can allow an unauthenticated remote attacker to execute operating system commands in the context of the site user via a specially crafted WebSocket request.
Apple	7.8	Multiple Apple devices contain a buffer overflow vulnerability that can allow an attacker with memory write capabilities to execute code on the devices, this vulnerability was fixed in versions 26.3
Microsoft Configuration Manager	9.8	Microsoft Configuration Manager contains an SQL injection vulnerability that can allow an unauthenticated remote attacker to execute operating system commands on the system via a specially crafted SQL query.
Notepad++	7.7	Notepad++ when using the WinGUp updater, contains a download of code without integrity check vulnerability that could allow an attacker to intercept or redirect update traffic to download and execute an attacker-controlled installer. This could lead to arbitrary code execution with the privileges of the user.
SolarWinds Web Help Desk	9.8	SolarWinds Web Help Desk contains a security control bypass vulnerability that could allow an unauthenticated attacker to execute arbitrary commands within the WHD application allowing PowerShell to be utilised.
Microsoft	8.8	Microsoft MSHTML Framework contains a protection mechanism failure vulnerability that could allow an unauthorised attacker to bypass a security feature over a network. The MSHTML Framework is used by applications such as the Office Suite and Explorer.
Microsoft	6.2	Microsoft Windows Remote Access Connection Manager contains a NULL pointer dereference that could allow an unauthorised attacker to deny service locally.
Microsoft	8.8	Microsoft Windows Shell contains a protection mechanism failure vulnerability that could allow an unauthorised attacker to bypass Smart Screen prompts. Smart Screen is used to warn the user that they are trying to launch an unsigned or unrecognised application.
Microsoft	7.8	Microsoft Windows Remote Desktop Services contains an improper privilege management vulnerability that could allow an authorised attacker to elevate privileges locally to SYSTEM.
Microsoft	7.8	Microsoft Desktop Windows Manager (DWM) contains a type of confusion vulnerability that could allow an authorised attacker to elevate privileges locally.
Microsoft	7.8	Microsoft Office Word contains a reliance on untrusted inputs in a security decision vulnerability that could allow an authorised attacker to elevate privileges locally. The vulnerability allows a malicious document to bypass Object Linking & Embedding (OLE) mitigations.

For more information, please visit the Red Piranha Forum:
https://forum.redpiranha.net/t/known-exploited-vulnerabilities-catalog-2nd-week-of-february-2026/640

Current Threat Summary

Updated Malware Signatures (Week 2 - February 2026)

Threat	Description
Proxy Applications/ Browser Extensions	There are several application and web browser extensions that allows your device/network to access a proxy for other users (Major distributed network). They are usually advertised as a way to make passive income by allowing their network to act as a proxy. Access to these proxies is sold to allow the buyers to have access to a 'Residential IP' as opposed to a VPS IP. These networks have been seen to scanned web application/websites for vulnerabilities and other bot activities such as a data scraping/crawling.

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

Ransomware activity this week was led by The Gentlemen, accounting for 18.5% of total reported activity. Close behind was Qilin at 16.74%, followed by Clop with 15.42%. These three groups dominated the landscape, driving a significant share of global ransomware disclosures.

A second tier of active operators included Insomnia (8.81%) and Play (7.49%), both maintaining consistent operational momentum. Mid-level contributors such as INC Ransom (4.41%) and LeakedData (3.52%) continued to demonstrate steady campaign activity. Meanwhile, Akira, Sinobi, and DragonForce each contributed 2.64%, reflecting a sustained but comparatively moderate presence.

Lower-percentage actors included Anubis (1.76%), along with SafePay, Beast, and Space Bears at 1.32% each. Groups contributing 0.88% included Nova, Bravox, Pear, Tengu, WorldLeaks, CiphBit, and Kairos.

Single-incident contributors, each representing 0.44% of weekly activity, included Crypto24, KillSec3, Chaos, Medusa, Reynolds, Nitrogen, LeakNet, Everest, Rhysida, ShinyHunters, Genesis, and Interlock.

Overall, activity remains heavily concentrated among a small group of dominant operators, while a broad long tail of smaller actors continues to contribute to persistent and distributed ransomware campaigns globally.

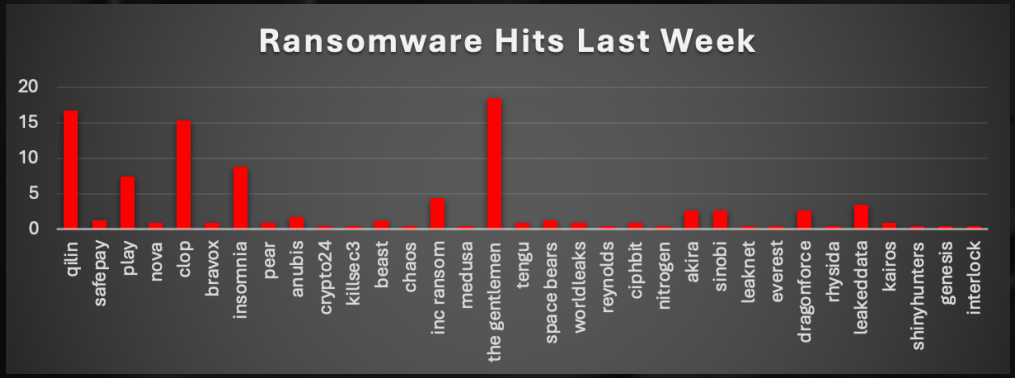


Figure 1: Ransomware Group Hits Last Week

The Gentlemen Ransomware

The Gentlemen is a ransomware operation first observed in mid-2025. The group operates a double-extortion model, encrypting victim files while exfiltrating sensitive data to maximise ransom pressure. The Gentlemen maintains a Tor-based Data Leak Site (DLS) where victim profiles are published alongside a staged countdown mechanism and direct TOX messenger negotiation channels.

The targeting pattern indicates a deliberate focus on medium-to-large enterprises with complex Active Directory environments and high-value data assets.

Detailed Tactics, Techniques, and Procedures (TTPs)

1. Initial Access (Internet-Facing Service Exploitation)
The Gentlemen gains initial access primarily through exploitation of internet-facing services, specifically FortiGate firewall admin panels and VPN interfaces, as well as through the use of compromised administrative credentials. No evidence of mass phishing campaigns or drive-by download delivery has been publicly documented for this group.

2. Reconnaissance & Discovery
Upon achieving access, The Gentlemen performs systematic Active Directory and network reconnaissance. Advanced IP Scanner is deployed for network mapping and infrastructure enumeration. A custom batch script enumerates user accounts, including domain admins, enterprise admins, custom privilege groups (itgateadmin), and VMware administrator groups. This targeted enumeration of virtualisation management groups is consistent with preparation for ESXi-specific encryption deployment. Domain trust discovery is performed to map trust relationships across the domain.

3. Privilege Escalation
Privilege escalation is achieved through two primary mechanisms. First, PowerRun.exe, a legitimate privilege escalation utility, is used to bypass UAC and gain SYSTEM-level privileges. Second, CVE-2025-7771, a high-severity code execution and privilege escalation vulnerability in the ThrottleStop driver, is exploited for kernel-level access.

Defence Evasion (BYOVD & AV/EDR Termination)
The Gentlemen employs a sophisticated Bring Your Own Vulnerable Driver (BYOVD) technique as its primary defence evasion mechanism. ThrottleStop.sys, a legitimate but vulnerable driver, is renamed to ThrottleBlood.sys and loaded to exploit CVE-2025-7771.

Our analysis confirmed that the tools were adapted mid-campaign based on the victim's specific security stack, Allpatch2.exe dynamically targets specific security agents rather than using a static kill list.

Additionally, Windows Defender is disabled via PowerShell and exclusions are added globally across all volumes. No compiler-level obfuscation has been reported in the ransomware binary itself; defence evasion relies on the password-protected execution model and kernel-level AV termination rather than binary obfuscation.

5. Lateral Movement
Lateral movement is achieved through multiple channels. PsExec is deployed over SMB admin shares for remote command execution. AnyDesk is installed as a persistent Windows service providing a remote access backdoor. PuTTY is used for SSH-based lateral movement, particularly relevant for reaching Linux and ESXi infrastructure. RDP sessions are enabled by modifying Windows Firewall rules and setting the DisableRestrictedAdmin registry key to 0. The combination of RDP, SSH, and legitimate remote management tools demonstrates an operator philosophy of leveraging trusted administrative channels to blend with normal network activity.

6. Data Collection & Exfiltration (Double-Extortion Preparation)
Before encryption is triggered, data is exfiltrated to support the double-extortion model. Data from the local system and network shares is harvested across sensitive directories and staged locally before exfiltration. WinSCP is used for encrypted data transfers over SFTP/SCP channels. The specific volume of data exfiltrated per victim has not been independently quantified in public reporting. The exfiltration phase is assessed to occur over a period of days to weeks, depending on network size and data volume, though this timeline has not been confirmed by incident response reports and should be treated as an analytical estimate based on comparable RaaS operations.

MITRE ATT&CK TTP Matrix

The table below summarises The Gentlemen's tactics and techniques mapped to the MITRE ATT&CK framework:

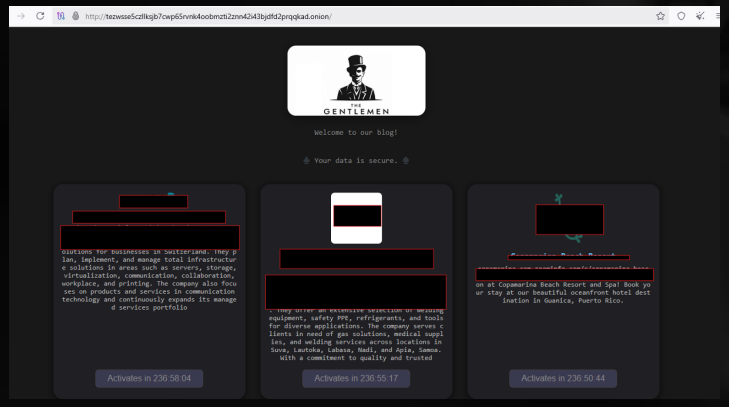
Tactic	Technique (ID)	Gentlemen Implementation
Initial Access	Exploit Public-Facing Application (T1190)	Exploitation of exposed FortiGate admin panels, VPN interfaces, and other internet-facing services to gain initial foothold
	Valid Accounts (T1078)	Use of compromised administrative credentials, including domain accounts (T1078.002), for entry into enterprise environments
Execution	PowerShell (T1059.001)	PowerShell used to disable Defender, add exclusions across all drives, enumerate volumes, and modify ICACLS permissions
Execution	Windows Command Shell (T1059.003)	Batch scripts (1.bat) for mass account enumeration across 60+ user accounts including domain admins, enterprise admins, and VMware groups
Persistence	Boot or Logon AutoStart Execution (T1547)	Self-restart and run-on-boot functionality observed in latest January/February 2026 variants
	Create or Modify System Process (T1543)	Installation of AnyDesk as a Windows service for persistent remote access backdoor
Privilege Escalation	Exploitation for Privilege Escalation (T1068)	Abuse of PowerRun.exe to bypass UAC and gain SYSTEM privileges; CVE-2025-7771 kernel-level escalation via ThrottleStop driver
Defence Evasion	Impair Defences: Disable or Modify Tools (T1562.001)	BYOVD technique using ThrottleBlood.sys (renamed ThrottleStop.sys) with All.exe/Allpatch2.exe to terminate AV/EDR processes at kernel level
	Obfuscated Files or Information (T1027)	Password-protected ransomware payloads (mandatory --password parameter) to prevent automated sandbox analysis and accidental detonation
	Domain Policy Modification: Group Policy Modification (T1484.001)	GPO manipulation to deploy ransomware domain-wide via NETLOGON shares, enabling centralised mass deployment
Discovery	Network Service Discovery (T1046)	Advanced IP Scanner for network mapping and infrastructure enumeration across compromised environments
	Account Discovery: Domain Account (T1087.002)	AD enumeration of domain admins, enterprise admins, custom privilege groups (itgateadmin), and VMware groups via batch scripts
Lateral Movement	Remote Services: SMB/Windows Admin Shares (T1021.002)	PsExec over SMB admin shares for remote command execution and ransomware deployment
	Remote Services: RDP (T1021.001)	RDP sessions across compromised systems; firewall rules and registry (DisableRestrictedAdmin=0) modified to enable access
	Remote Services: SSH (T1021.004)	PuTTY used for SSH-based lateral movement across Linux/ESXi infrastructure
Collection	Data from Network Shared Drive (T1039)	Collection from network shares across the domain; data staged locally before exfiltration
Exfiltration	Exfiltration Over Alternative Protocol (T1048.001)	WinSCP used for encrypted data exfiltration over SFTP/SCP channels
Com-	Remote Access Software (T1219)	AnyDesk installed as a persistent remote access backdoor; Tor-based communication for victim negotiations
mand-and-Control	Application Layer Protocol: Web Protocols (T1071.001)	C2 over HTTP/HTTPS; all victim communication routed through Tor .onion infrastructure

Indicators of Compromise (IOCs)

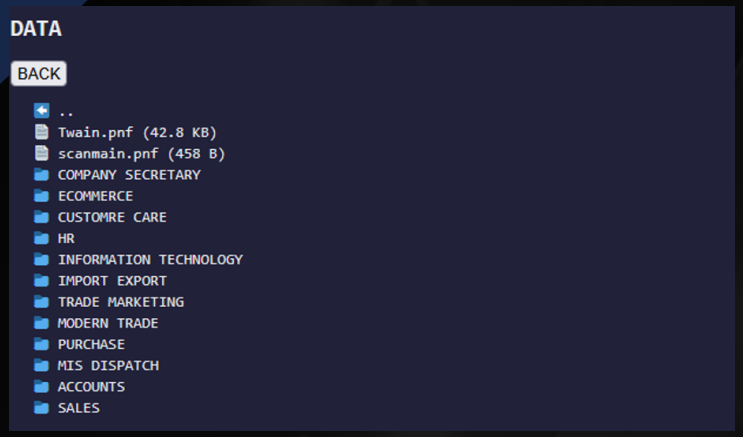
Infrastructure / C2:

- TOR Leak Site (Negotiation):

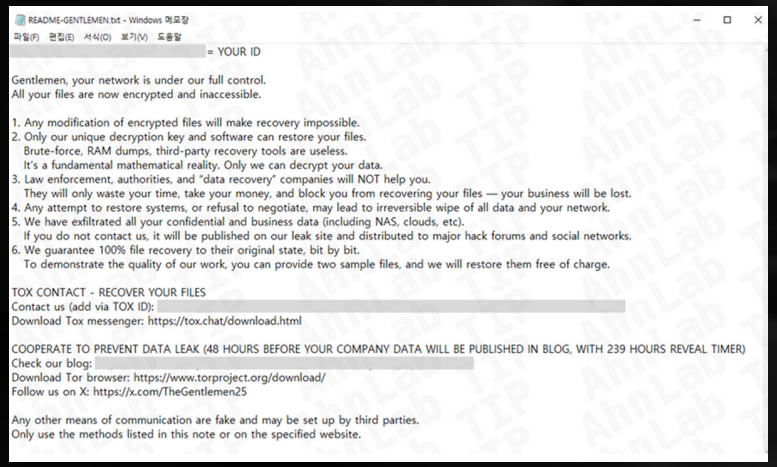
tezwsse5czllksjb7cwp65rvnk4oobmzti2znn42i43bjdfd2prqqkad.onion



- TOR Data Leak Site (DLS): 25swr3rgce7elyedjmmhdw4ourgtxc72mj2cynsrqz6wwitestfpiiyd.onion



Communication Identifiers:
- TOX ID: F8E24C7F5B12CD69C44C73F438F65E9BF560ADF35EBBDF92CF9A9B84079F8F04060FF98D098E
- Extension: .7mtzhh (primary); .ojuopo (observed in separate campaigns)
- Ransom Note: README-GENTLEMEN.txt


README-GENTLEMEN.txt - Windows 메모장
파일(F) 편집(E) 서식(O) 보기(V) 도움말
= YOUR ID

Gentlemen, your network is under our full control.
All your files are now encrypted and inaccessible.

1. Any modification of encrypted files will make recovery impossible.
2. Only our unique decryption key and software can restore your files.
Brute-force, RAM dumps, third-party recovery tools are useless.
It's a fundamental mathematical reality. Only we can decrypt your data.
3. Law enforcement, authorities, and "data recovery" companies will NOT help you.
They will only waste your time, take your money, and block you from recovering your files — your business will be lost.
4. Any attempt to restore systems, or refusal to negotiate, may lead to irreversible wipe of all data and your network.
5. We have exfiltrated all your confidential and business data (including NAS, clouds, etc).
If you do not contact us, it will be published on our leak site and distributed to major hack forums and social networks.
6. We guarantee 100% file recovery to their original state, bit by bit.
To demonstrate the quality of our work, you can provide two sample files, and we will restore them free of charge.

TOX CONTACT - RECOVER YOUR FILES
Contact us (add via TOX ID):
Download Tox messenger: https://tox.chat/download.html

COOPERATE TO PREVENT DATA LEAK (48 HOURS BEFORE YOUR COMPANY DATA WILL BE PUBLISHED IN BLOG, WITH 239 HOURS REVEAL TIMER)
Check our blog:
Download Tor browser: https://www.torproject.org/download/
Follow us on X: https://x.com/TheGentlemen25

Any other means of communication are fake and may be set up by third parties.
Only use the methods listed in this note or on the specified website.

- BYOVD Driver: ThrottleBlood.sys (renamed from ThrottleStop.sys; exploits CVE-2025-7771)
- AV Killer Tools: All.exe, Allpatch2.exe
- Privilege Escalation: PowerRun.exe
- Recon Script: 1.bat
- Binary Type: Golang, cross-platform (Windows/Linux/ESXi/NAS/BSD)

Mitigation with CE 5.5

1. Block Tor traffic and .onion IOCs at CE SWG perimeter using DPI to sever all Gentlemen C2 communication channels.
2. Enforce CEASR application allowlisting to block unsigned Golang binaries and ThrottleStop/ThrottleBlood kernel driver loads on endpoints.
3. Deploy CE IDPS hunting rules targeting -- password execution patterns, .7mtzhh file writes, and mass service termination events.
4. Activate CESOC 24×7 MDR escalation with SOAR playbooks for automated containment of BYOVD and ransomware deployment indicators.

Ransomware Victims by Geography

The United States remains overwhelmingly the most targeted country, accounting for 59.03% of worldwide ransomware victims. This reflects a continued strategic focus on large, digitally mature economies with high revenue potential and broad attack surfaces. Canada follows at 6.61%, reinforcing North America as the primary hotspot for ransomware operations.

In Europe, the United Kingdom recorded 3.96% while France accounted for 2.64%. Other European nations, including Germany, Italy, Spain, Sweden, Switzerland, Ireland, Portugal, Austria, Luxembourg, the Czech Republic, and Denmark, each contributed smaller but notable shares, highlighting persistent ransomware exposure across the European region.

In the Asia-Pacific region, activity was distributed across multiple economies. India represented 2.2%, while Japan, Australia, and Thailand each stood at 1.32%. Additional activity was observed in Singapore, Malaysia, New Zealand, South Korea, the Philippines, Indonesia, Taiwan, and China, demonstrating the widening geographic footprint of ransomware campaigns across the region.

In the Middle East and surrounding regions, the United Arab Emirates and Turkey each accounted for 1.76%, while Saudi Arabia also registered activity. Across Latin America, victims were reported in Brazil, Mexico, Chile, Colombia, Peru, and Ecuador, indicating sustained targeting beyond North America and Europe.

African nations, including South Africa, Nigeria, and Ghana, also recorded incidents, reflecting ransomware's continued global penetration.

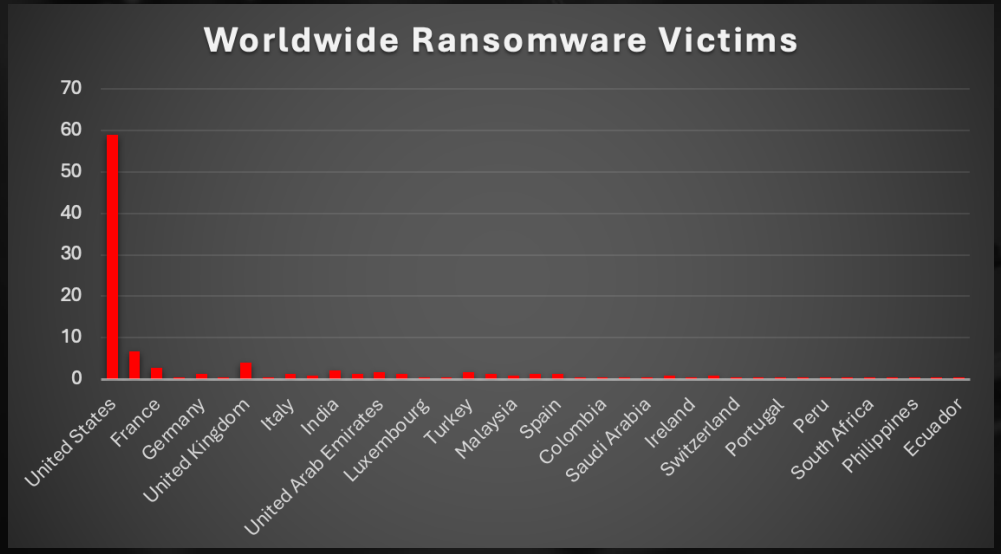


Figure 5: Ransomware Victims Worldwide

Industry-wide Ransomware Impact

Ransomware activity this week was most heavily concentrated in Business Services, which accounted for 18.06% of total victims, reinforcing its position as a primary target due to its broad client exposure and data-rich environments. Manufacturing followed closely at 15.86%, continuing its long-standing trend as a high-value sector frequently targeted for operational disruption leverage.

A second tier of impacted industries included Construction (8.81%) and Hospitality (8.37%), both reflecting consistent exposure to ransomware operations. Law Firms represented 7.93%, highlighting ongoing targeting of legal entities where sensitive contractual and litigation data can be exploited. Retail also recorded notable activity at 7.05%, underscoring the continued risk to customer data and payment ecosystems.

Mid-level impact was observed across Finance (5.73%), Electronics (3.52%), Healthcare (3.08%), and IT (3.08%). These sectors remain strategically attractive due to their critical infrastructure role, regulatory pressures, and potential for rapid ransom payments. Real Estate and Education each accounted for 2.64%, while Federal, Transportation, Consumer Services, and Energy each represented 2.2%, indicating steady but comparatively moderate targeting.

Lower-frequency sectors included Organisations (1.76%) and Insurance (1.32%), while Media & Internet (0.88%) and Agriculture (0.44%) recorded limited activity.

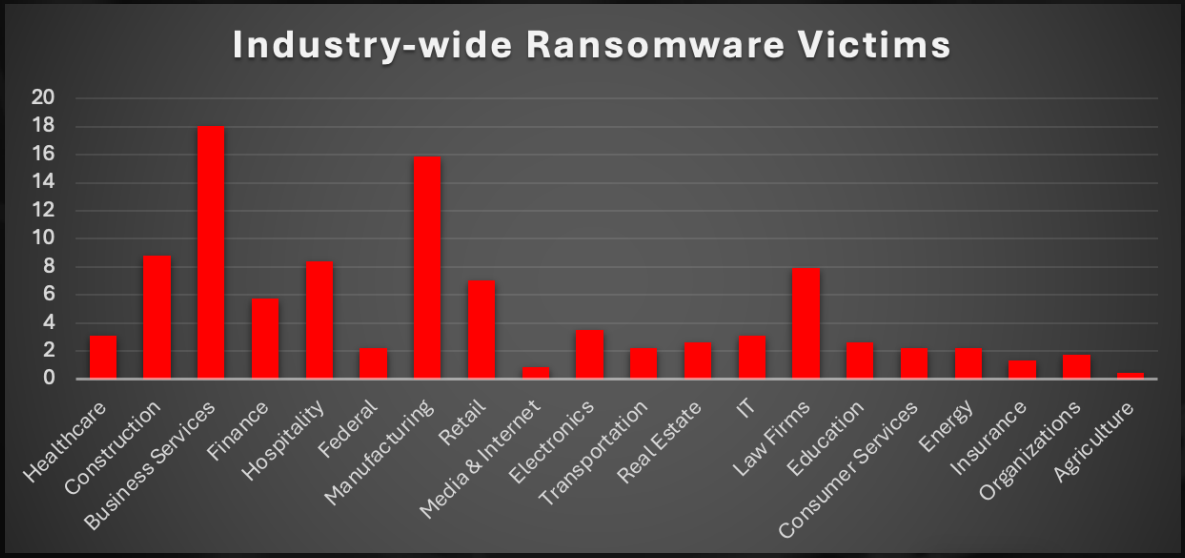


Figure 6: Industry-wide Ransomware Victims