



# **THREAT INTELLIGENCE REPORT**

**Aug 26 - Sept 01, 2025**

# Report Summary:

## ■ New Threat Detection Added

- KoiStealer

## ■ Detection Summary

- Threat Protections integrated into the Crystal Eye - 107
- Newly Detected Threats - 5



# The following threats were added to Crystal Eye this week:

## 1. Koi Stealer

KoiStealer is an infostealer that is suspected of being created by North Korean threat actors. There have been a few attack vectors of compromise linked to this malware. The most common technique used is for the threat actor group to pose as legitimate job recruiters for software developers. Through this process, they infect the victim by exchanging emails, with one of the emails containing the malicious file. Another method is by sending out benign emails to strike up a conversation, and if someone replies, they will send the malicious link to them.

This infostealer has two variants, one for MacOS and another for windows environments, this will focus on the Windows variant. Once the malware is running, it will run a script that creates a PowerShell process that will download another script. This will also create another PowerShell process that will further download more payloads. During this process, it will check the environment to ensure that it's not running in a sandbox to disrupt analysis, and it will also set up a scheduled task to maintain persistence on the system.

Once the malware has gone through its setup, it will then begin to steal information such as device information, crypto wallets, web browser data such as saved credentials and cookies, and it will also steal credentials to applications such as SSH and WinAuth. All this information will be sent to the same C2 server that downloaded all the initial payloads.

**Threats Protected: 2**  
**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           | Disabled    | Disabled    |

### Kill Chain:

| Tactic              | Technique ID | Technique Name                                 |
|---------------------|--------------|--|
| Initial Access      | T1566        | Phishing                                       |
| Execution           | T1059.001    | Command and Scripting Interpreter –            |
|                     | T1059.007    | PowerShell & JavaScript                        |
|                     | T1204.001    | User Execution – Malicious Link                |
| Persistence         | T1053.005    | Scheduled Task/ Job – Scheduled Task           |
| Defence Evasion     | T1497.001    | Virtualisation/Sandbox Evasion - System Checks |
| Collection          | T1119        | Automated Collection                           |
| Command-and-Control | T1071.001    | Application Layer Protocol Web Protocols       |
| Exfiltration        | T1041        | Exfiltration Over C2 Channel                   |



## Current Threat Summary

### Known exploited vulnerabilities (Week 1 September 2025)

| Vulnerability            | CVSS           | Description   |
|--------------------------|----------------|---|
| Sangoma FreePBX          | 10 (Critical)  | Sangoma FreePBX contains a vulnerability that can allow a remote unauthenticated attacker to bypass the authentication and gain access to the system. Exploitation of the vulnerability can lead to further attacks including SQL Injection as well as the ability to execute code.             |
| Citrix NetScaler         | 9.2 (Critical) | Citrix NetScaler ADC and NetScaler Gateway contain a memory corruption vulnerability that can allow a remote unauthenticated attacker to execute code on the system. Exploitation of this vulnerability can result in an attacker gaining access to the system or to cause a denial of service. |
| Git                      | 8.1 (High)     | Git contains a vulnerability that can allow a remote unauthenticated attacker to execute code on a device upon cloning a malicious git repository with the “--recursive” tag.   |
| Citrix Session Recording | 5.1 (Medium)   | Citrix Session Recording contains a vulnerability that can allow escalation of privileges to a NetworkService Account from an authenticated user that’s in the same Windows Active Directory domain as the session recording server.  |
| Citrix Session Recording | 5.1 (Medium)   | Citrix Session Recording contains a deserialisation vulnerability that can allow an attacker within the same intranet of the session recording server to execute code with the privileges of a NetworkService Account.  |

For more information, please visit the **Red Piranha Forum**:

<https://forum.redpiranha.net/t/known-exploited-vulnerabilities-catalog-4th-week-of-august-2025/588>

### Updated Malware Signatures (Week 1 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 with 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 Victims – Weekly Overview

[SafePay](#) led this week’s activity, responsible for 16.52% of all reported incidents. Its continued rise highlights sustained campaigns against enterprises, leveraging both encryption and data theft for maximum extortion pressure.

[Qilin](#) and [Cephalus](#) followed closely at 14.78% each, cementing their positions among the most aggressive operators. Qilin’s consistency suggests strong affiliate participation, while [Cephalus](#)’ activity indicates a possible surge of new campaigns.

[Inc Ransom](#) accounted for 6.96%, maintaining its role as a mid-tier but disruptive actor.

[WorldLeaks](#), [DragonForce](#), and [Akira](#) each reported 5.22%, underscoring their ability to remain relevant with steady campaigns across various geographies and industries.

[Direwolf](#) and [Play](#) both contributed 4.35%, demonstrating persistent though moderate activity. [Interlock](#) followed with 3.48%, while [Lynx](#) registered 2.61% of total incidents.

Smaller but notable activity came from [Kairos](#), [Medusa](#), and [Rhysida](#) (each at 1.74%), suggesting probing attacks or targeted operations.

Finally, a wide group of actors—including [RansomHouse](#), [Metaencryptor](#), [Warlock](#), [Beast](#), [LockBit3](#), [Sinobi](#), [Chaos](#), [Sarcoma](#), [Leaknet](#), [Anubis](#), [Black Nevas](#), [Everest](#), and [LeakedData](#)—each represented 0.87% of activity. While individually limited, these groups collectively reflect the long-tail of the ransomware ecosystem, where smaller crews and splinter operators maintain a steady global presence.

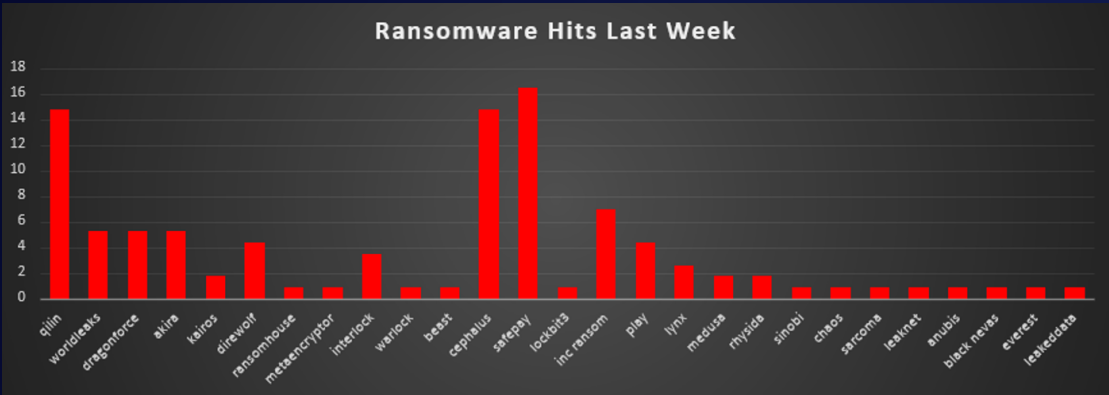


Figure 1: Ransomware Group Hits Last Week



# Cephalus Ransomware

Red Piranha observed two Cephalus intrusions in mid-August. In both cases the threat actor authenticated over RDP with compromised credentials without MFA, staged data via MEGA (MEGAcmd), then attempted to execute ransomware through DLL sideloading:

SentinelBrowserNativeHost.exe   SentinelAgentCore.dll   data.bin  
(encryptor)

One deployment failed due to Microsoft Defender quarantine; the other succeeded, dropping a note that begins “We’re Cephalus”, to increase pressure, and provides TOX/Email contact plus a proof-of-theft link.

```
We're Cephalus, 100% financial motivated. We're sorry to tell you that your intranet has been compromised by us, and we have stolen confidential data from your intranet, including your confidential clients, contacts and cases etc.

We've taken down your whole domain control, all your past and ongoing matters and client list are in our hands.
Before 08/15/2025 you should contact us , the earlier you contact us , the smaller the problem will be.
After that your data will be uploaded, your competitors, partners, clients, authorities, tax agensis and lawyer would be able to access it. We will start mailing and calling your clients.
Those who didn't follow our orders have already be in trouble , check your peer SSKRPLAW and other companies as you search us with "Cephalus data leak" or just simply pay a visit to those news website:
https://www.hendryadrian.com/sherman-silverstein-data-leak-5gb-of-sensitive-client-and-firm-information-allegedly-exposed/
https://insecureweb.com/massive-bar-architects-data-breach-by-cephalus/
Or that will not happen, If we will close this deal in time!!!
```

## Detailed TTPs

### Initial Access

- Vector: Valid-account RDP (no MFA).
- Staging: MEGAcmd used to move archives to MEGA prior to encryption. Observed command line (example):

C:\Users\[user]\AppData\Local\MEGAcmd\MEGAcmdUpdater.exe  
--normal-update --do-not-install --version 2010100

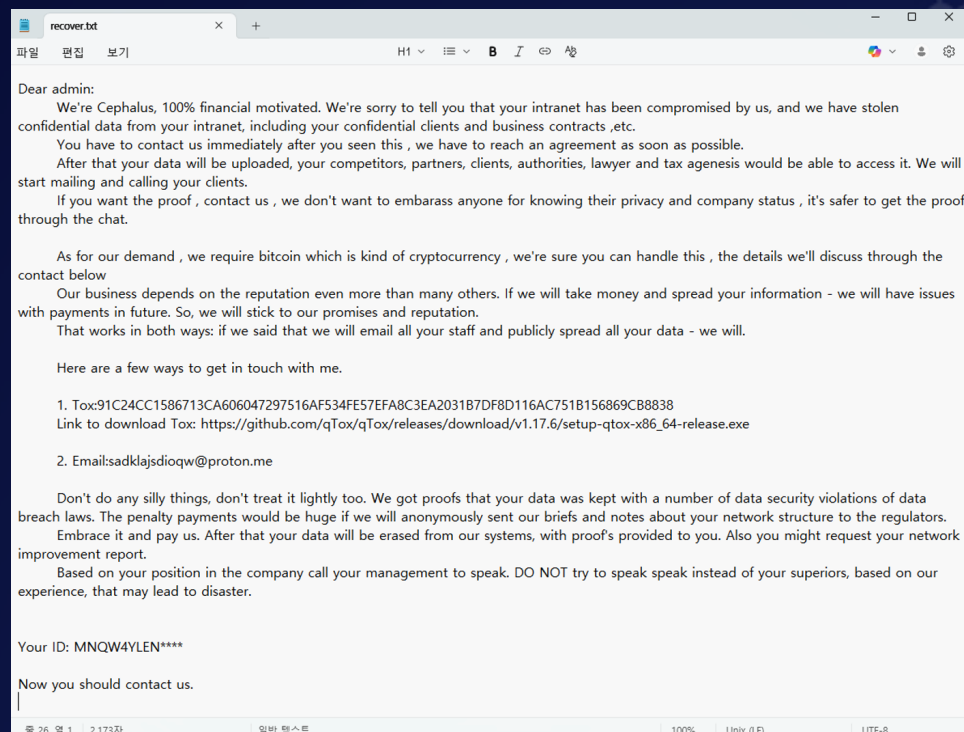
### Execution Tradecraft: DLL Sideload

- Actor placed SentinelBrowserNativeHost.exe in Downloads, which loaded a rogue SentinelAgentCore.dll.
- The DLL then loaded data.bin containing the ransomware code.
- This is signed-binary proxy execution / DLL sideloading to blend with legitimate EDR tooling.

## Defence Evasion

Child activity of the sideload chain included:

- Inhibit recovery:  
vssadmin delete shadows /all /quiet
- Tamper with Microsoft Defender:  
Add-MpPreference (exclusions for paths/extensions/processes).  
Registry policy edits:  
HKLM\SOFTWARE\Policies\Microsoft\Windows Defender\\* (e.g., DisableRealtimeMonitoring, DisableBehaviorMonitoring, DisableOnAccessProtection, DisableAntiSpyware).  
Service control: stop/disable WinDefend, WdNisSvc, Sense, SecurityHealthService.
- Ransom note & extension: recover.txt; encrypted files observed with .sss.



recover.txt

파일 편집 보기 H1 H2 H3 B I U A

Dear admin:

We're Cephalus, 100% financial motivated. We're sorry to tell you that your intranet has been compromised by us, and we have stolen confidential data from your intranet, including your confidential clients and business contracts ,etc.

You have to contact us immediately after you seen this , we have to reach an agreement as soon as possible.

After that your data will be uploaded, your competitors, partners, clients, authorities, lawyer and tax agensis would be able to access it. We will start mailing and calling your clients.

If you want the proof , contact us , we don't want to embarrass anyone for knowing their privacy and company status , it's safer to get the proof through the chat.

As for our demand , we require bitcoin which is kind of cryptocurrency , we're sure you can handle this , the details we'll discuss through the contact below

Our business depends on the reputation even more than many others. If we will take money and spread your information - we will have issues with payments in future. So, we will stick to our promises and reputation.

That works in both ways: if we said that we will email all your staff and publicly spread all your data - we will.

Here are a few ways to get in touch with me.

1. Tox:91C24CC1586713CA606047297516AF534FE57EFA8C3EA2031B7DF8D116AC751B156869CB8838  
Link to download Tox: [https://github.com/qTox/qTox/releases/download/v1.17.6/setup-qtox-x86\\_64-release.exe](https://github.com/qTox/qTox/releases/download/v1.17.6/setup-qtox-x86_64-release.exe)

2. Email:sadklajsdioqw@proton.me

Don't do any silly things, don't treat it lightly too. We got proofs that your data was kept with a number of data security violations of data breach laws. The penalty payments would be huge if we will anonymously sent our briefs and notes about your network structure to the regulators.

Embrace it and pay us. After that your data will be erased from our systems, with proof's provided to you. Also you might request your network improvement report.

Based on your position in the company call your management to speak. DO NOT try to speak speak instead of your superiors, based on our experience, that may lead to disaster.

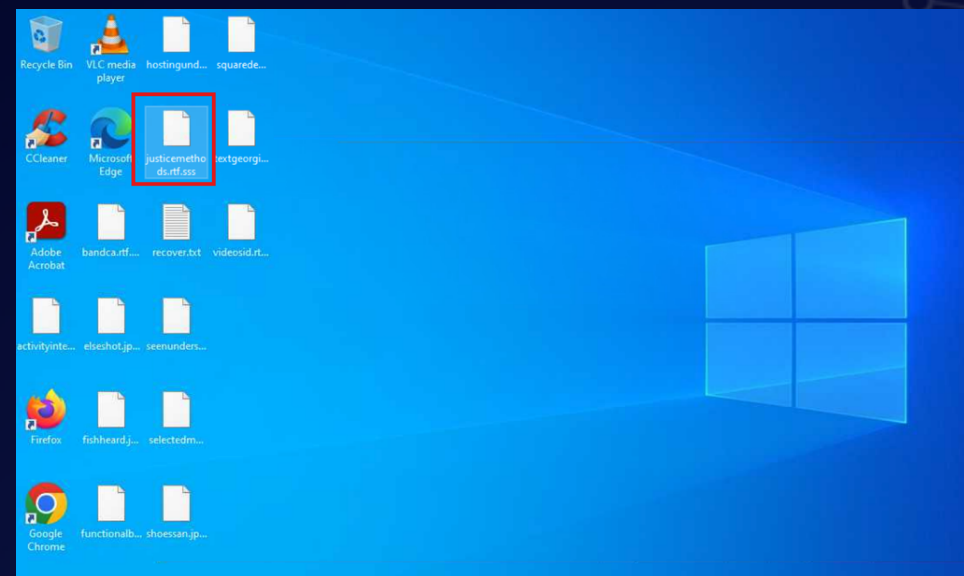
Your ID: MNQW4YLEN\*\*\*\*

Now you should contact us.

줄 26, 열 1 2,173자 일반 텍스트 100% Unix (LF) UTF-8

## MITRE ATT&CK Matrix

| Tactic         | Technique  | How it appears for Cephalus  |
|----------------|--|--|
| Initial Access | T1133 External Remote Services / T1078 Valid Accounts    | RDP login with stolen creds, no MFA  |
| Initial Access | T1218 Signed Binary Proxy Exec                           | Launch of SentinelBrowserNativeHost.exe from Downloads                                   |
| Collection     | T1053.005 Scheduled Task                                 | MEGAcmd updater scheduled in user context  |
| Collection     | T1574.002 DLL Side-Loading                               | Rogue SentinelAgentCore.dll loaded by Sentinel binary                                    |
| Exfiltration   | T1112 Modify Registry / T1562.001 Disable Security Tools | Defender policies flipped; services disabled<br><br>Not primary focus in observed window |
| Exfiltration   | (n/a evidence-lite)                                      |  |
| C2/Comms       | T1567.002 Exfiltration to Cloud Storage                  | MEGA / MEGAcmd prior to encryption   |
| Impact         | T1490 Inhibit System Recovery / T1486 Data Encrypted for | vssadmin deletions; encryption follows   |



## Indicators of Compromise (IOCs)

### File/Artifact Names

- SentinelBrowserNativeHost.exe (unusual when executed from C:\Users\[user]\Downloads\)
- SentinelAgentCore.dll (sideload DLL)
- data.bin (encryptor payload)
- recover.txt (ransom note)
- Encrypted extension: .sss

### Hashes:

- SentinelBrowserNativeHost.exe à

SHA256:0d9dfc113712054d8595b50975efd9c68f4cb8960eca010076b46d2fba3d2754

- SentinelAgentCore.dll à

SHA256:  
82f5fb086d15a8079c79275c2d4a6152934e2dd61cc6a4976b492f74062773a7

SHA256:  
a34acd47127196ab867d572c2c6cf2fccffa3a7a87e82d338a8efed898ca722

IP: 51.145.123.29

Associated domain à ntp6.n-helix[.]com , http://ntp17.dn.n-helix[.]com/

Tor URL

http://cephalus6oiypuwumqlwurvbwmwsfglg424zjdmywfgqm4iehkqivsjyd[.]ion

Evidence:

<https://gofile.io/d/fixCg7> - proofs.



```

jpp-server
  eXpd8
    eXpd8 DB
      Expd8_Data.MDF
      Expd8_Log.LDF
    Install
      eXpd8 Server Prerequisites
        R5.0.14
          Citrix
            0x0409.ini
            Autorun.inf
            CitrixClientVD.msi
            Data1.cab
            setup.exe
            Setup.ini
          DSSProR5
            0x040a.ini
            0x040c.ini
            0x0407.ini
            0x0409.ini
            0x0410.ini
            0x0419.ini
            1031.mst
            1033.mst
            1034.mst
            1036.mst
            1040.mst
            1049.mst
            Data1.cab
            Data2.cab
            DSSPlayer.msi
            instmsi30.exe
            setup.bmp
            setup.exe
            Setup.ini
  ..
  ..

```

## Mitigation & Detection with CE 5.0

### Identity & Access (CE-IAM/Email Security)

- Enforce MFA on RDP/VPN/SSO; disable direct internet-exposed RDP.
- Alert on suspicious mailbox rules / OAuth grants (if O365/Google Workspace present).

### Endpoint (CE-EDR / CE-XDR)

- Block/Alert when SentinelBrowserNativeHost.exe executes from Downloads/Temp/Desktop.
- Detections for:
  - o vssadmin shadow deletion
  - o PowerShell Add-MpPreference / Set-MpPreference
  - o Registry edits to Defender policy hives
  - o Service stop/disable for Defender components
  - o MEGAcmd execution and network egress

### Network (CE-NGFW / CE-SOAR)

- Restrict egress to approved destinations; flag connections to MEGA endpoints from servers.
- Block/alert Tor/tor2web where feasible (actors sometimes reference dark-web content in notes).

### Backup & Recovery

- Maintain immutable/offline backups; validate restores quarterly.
- Monitor for backup share access + VSS manipulation.

**Cephalus**  
Cephalus Hack You

**16** ACTIVE LEAKS | **8** DATA SOURCES

**Cooperation**  
tox : 02E5E0E64D2A4C87C0CEE437B1F399B3225E0B9BA080D067D7C925D4682A87A7FF7816165B9

Search domains, com [ SEARCH ] [ RESET ]

**ALL DOMAINS** Explore our database of 16 domains

|  |   |   |
|--|---|---|
| <b>CARESTL</b><br>CareSTL Health<br><b>carestlhealth.org</b><br>> CareSTL Health DATA Leak   900+GB   KAWA4096 STEALED our data<br>[ ACCESS DATA ] | <b>SYSTEM-EXE</b><br>SystemExec Co., Ltd.<br><b>system-exe.co.jp</b><br>> SystemExec Co., Ltd. (システムエグゼ) GitHub naked repo leak   30G+<br>[ ACCESS DATA ] | <b>BARARCH</b><br>BAR Architects & Interiors<br><b>bararch.com</b><br>> BAR Architects & Interiors DATA LEAK   1.5T+<br>[ ACCESS DATA ] |
| <b>KSTRATEGIE</b><br>K. Strategies Marketing and Public Relations  | <b>BALANCEDSO</b><br>LPL Financial  | <b>GMLLP</b><br>Guerrero Pears LLP  |



# Worldwide Ransomware Victims

The United States continues to dominate the global ransomware landscape, reporting 52.17% of all incidents this week. Its high concentration of critical infrastructure, financial institutions, and enterprises ensures it remains the top target for ransomware groups.

Canada accounted for 9.57%, reflecting a significant increase in targeting compared to prior weeks. This spike underscores attackers' preference for North American organisations, exploiting similar supply chain dependencies and digital infrastructures.

Germany and the United Kingdom each registered 6.09%, reinforcing their roles as key European hotspots. These mature economies remain attractive due to valuable intellectual property and business data.

Australia reported 4.35%, while Italy followed with 3.48%, indicating steady ransomware activity across both regions.

Spain, France, Brazil, and Mexico each accounted for 1.74%, signaling a dispersed but consistent targeting pattern across Southern Europe and Latin America.

Several countries—including Finland, Singapore, Greece, Mauritius, Indonesia, Japan, Denmark, Georgia, Costa Rica, Sweden, India, Peru, and Ireland—each logged 0.87% of global incidents. While individually small, this long tail highlights ransomware's increasingly globalised reach, with operators probing diverse geographies for vulnerable entry points.

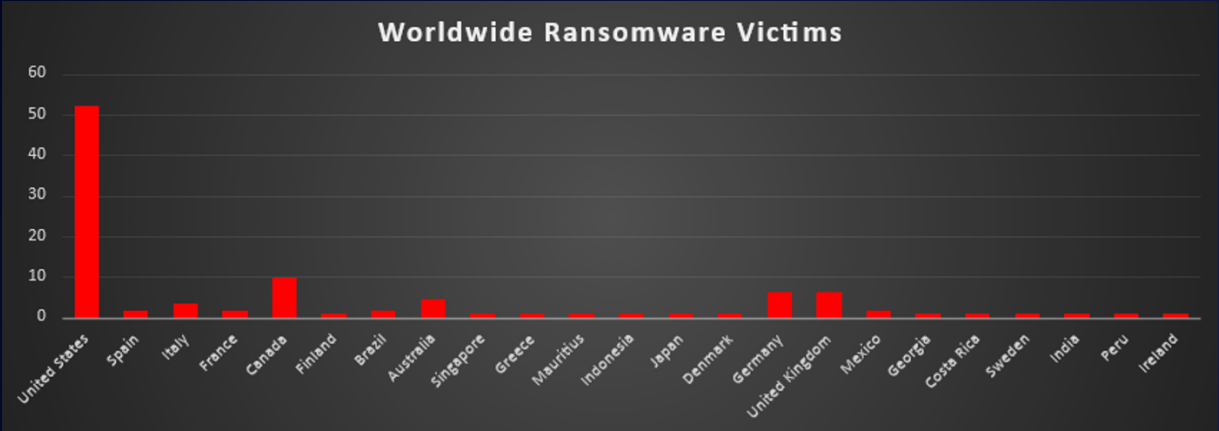


Figure 7: Ransomware Victims Worldwide



## Industry-wide Ransomware Victims

Manufacturing continues to be the most targeted sector this week, accounting for 24.35% of reported incidents. Its critical operational role, reliance on legacy systems, and limited tolerance for downtime make it a perennial focus for ransomware operators.

Construction and Business Services both followed at 11.3% each. Construction firms, with their complex vendor ecosystems and high-value projects, remain lucrative targets. Business Services, which often act as IT, consulting, and operational support providers to multiple industries, represent a key gateway for attackers into larger networks.

Hospitality registered 9.57%, reflecting steady exploitation of customer-centric sectors that manage significant volumes of sensitive personal and payment data.

Law Firms, Retail, Education, and Finance each recorded 6.96%, highlighting attackers' continued interest in industries rich in sensitive intellectual property, consumer records, financial data, and institutional trust.

Mid-tier victims included Organisations (3.48%), Transportation, Media & Internet, and Consumer Services (each at 2.61%), sectors that, while less frequently targeted, still face substantial disruption risks due to their role in public services and customer engagement.

Smaller incidents were observed in Insurance and Real Estate (1.74% each), along with Federal entities (0.87%), underscoring ransomware's wide reach across both public and private sector verticals, even when volumes remain comparatively low.

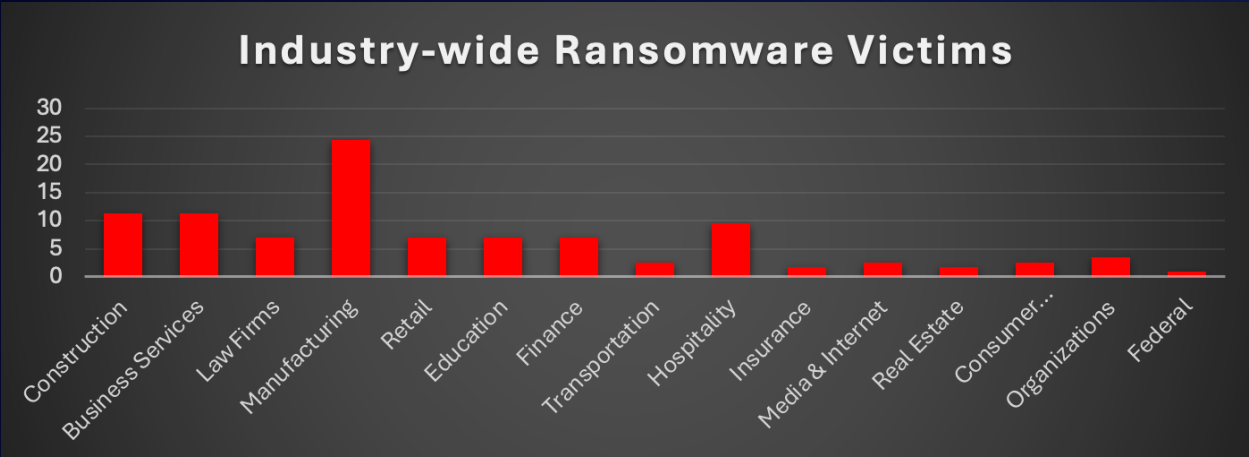


Figure 8: Industry-wide Ransomware Victims

