Red Piranha
unified threat management

THREAT INTELLIGENCE REPORT

Oct 14 - 20, 2025

Report Summary:

- **New Threat Detection Added**
  - iMonitor
  - Cobalt Strike
- **Detection Summary**
  - **Threat Protections integrated into the Crystal Eye - 84**
  - **Newly Detected Threats - 4**

The following threats were added to Crystal Eye this week:

1. iMonitor

iMonitor appears to be a new malware that appears to mimic employee 'spyware'. This malware is based on Gh0strat, a Remote Access Tool (RAT) that has been used by multiple threat actors since 2009. It's been used to infect critical infrastructure such as energy organisations and telecommunications.

The RAT has the ability to capture keystrokes, monitor webcams and microphones, deploy more malware, and have full access to the infected system via a remote shell.

iMonitor is known to send system information to attacker controlled C2 servers, and initiate RDP connections.

Threats Protected: 9
Class Type: Command-and-Control
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
Persistence	T1547.001	Registry Run Keys / Startup Folder
Privilege Escalation	T1543.003	Create or Modify System Process: Windows Service
Defence Evasion	T1562.004	Impair Defences: Disable or Modify System Firewall
Collection	T1119	Automated Collection
Exfiltration	T1020	Automated Exfiltration

2. Cobalt Strike

Cobalt Strike is a commercial Remote Access Tool (RAT) that is advertised as simulation software designed to execute attacks and emulate post-exploitation techniques used by Threat Actors. Because of the features that Cobalt Strike has included, it is used by threat actors as well.

There have been many threat actors found to be using cobalt strike for malicious purpose such as TA group Leviathan, a Chinse state-sponsored group that has targeted various sectors such as government, healthcare and defence. There has been a ransomware group identified to be using cobalt strike, Play uses their own encryption software called Playcrypt that has been used in government, healthcare and other critical infrastructure.

Threats Protected: 6
Class Type: Command-and-Control
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
Exfiltration	T1041	Exfiltration Over C2 Channel

Current Threat Summary

Known exploited vulnerabilities (Week 3 October 2025)

Vulnerability	CVSS	Description
CVE-2025-54253	10	Adobe Experience Manager Forms contains an authentication bypass vulnerability that can allow an unauthenticated remote attacker to gain access to the system, this vulnerability affects versions before 6.5.23.0 and was fixed in version 6.5.0-0108. The vulnerability itself is primarily an authentication bypass, however, due to struts devmode being enabled this can result in code execution on the system.
CVE-2025-47827	4.6	IGEL OS contains a vulnerability within the cryptographic signature verification of the igel-flash-driver module that can allow for a Secure Boot bypass resulting in the ability to mount a filesystem from an unverified SquashFS image.
CVE-2025-24990	8.3	Microsoft Windows Agere Modem Driver contains an untrusted pointer dereference vulnerability within the ltmdm64.sys driver that can result in an attacker with local access to escalate privileges.
CVE-2025-59230	8.1	Microsoft Windows contains a privilege escalation vulnerability within the Windows Remote Access Connection Manager that can allow for an attacker with local access to escalate privileges to SYSTEM.
CVE-2025-6264	7.8	Rapid7 Velociraptor contains a privilege escalation vulnerability that can allow for command execution, this vulnerability is a result of incorrect default permissions which can enable users with COLLECT_CLIENT permissions the ability to execute commands on endpoints.
CVE-2016-7836	8.8	SKYSEA Client View contains a vulnerability within the management console that can allow an unauthenticated remote attacker to bypass authentication and execute code on the system.

For more information, please visit the **Red Piranha Forum**:
https://forum.redpiranha.net/t/known-exploited-vulnerabilities-catalog-3rd-week-of-october-2025/608

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

Qilin overwhelmingly dominated ransomware activity this week, responsible for 45.11% of all reported incidents. This outsized share highlights either a coordinated surge in operations or significant disclosure of victim cases, reaffirming Qilin's position as one of the most aggressive and persistent groups currently active.

A mid-tier cluster of activity followed at much lower volumes. Akira (5.43%) and Coinbase Cartel (5.43%) stood out as notable operators, continuing to demonstrate steady victimisation across multiple industries. Sinobi (4.35%), DragonForce (3.8%), Nova (3.8%), Medusa (3.26%), and Play (3.26%) also maintained visibility, underscoring the persistence of established groups in the ecosystem.

Additional actors with moderate presence included Rhysida (2.72%), DevMan2 (2.72%), Everest (1.63%), Interlock (1.63%), and BlackShrantac (1.63%). These groups continue to operate at smaller scales but represent ongoing risk due to their opportunistic targeting strategies.

A wide range of groups accounted for 0.54-1.09% each, including WorldLeaks, Anubis, Handala, Scattered Lapsus$ Hunters, BqtLock, Brotherhood, Direwolf, Inc Ransom, Pear, The Gentlemen, KillSec3, Obscura, Radiant Group, RansomHouse, 3AM, Kraken, Lynx, MyData, and Black Nevas. While their activity levels were relatively minor, their collective presence illustrates the fragmented nature of the ransomware threat landscape, where dozens of smaller actors remain active alongside dominant players.

This week's distribution reflects a clear imbalance: ransomware activity was heavily concentrated under Qilin's banner, while a broad mix of secondary and fringe groups sustained the ecosystem's diversity and unpredictability.

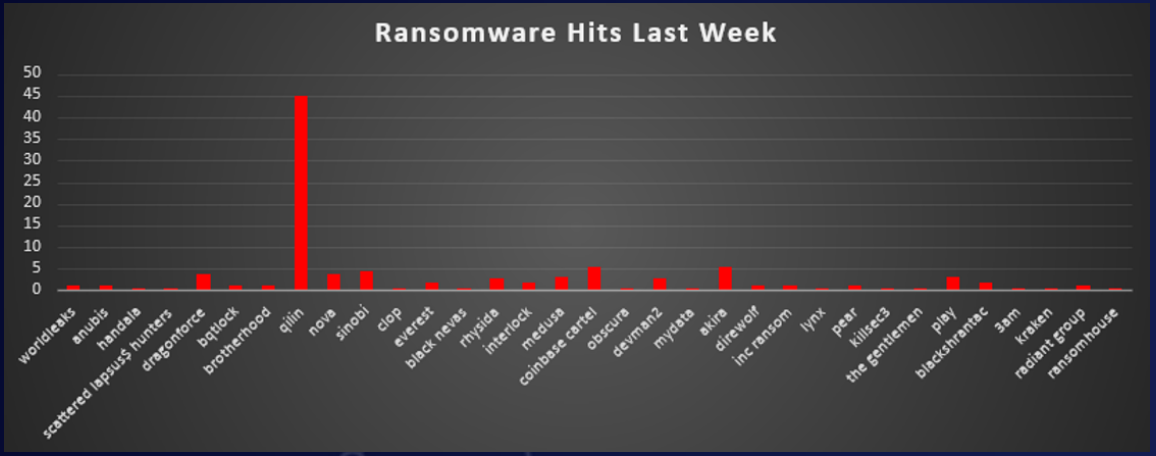

Figure 1: Ransomware Group Hits Last Week

Qilin Ransomware Overview

Qilin, also known as Agenda, operates a professional RaaS platform with distinct Windows and Linux/ESXi binaries. Affiliates receive tailored builds, often password-protected to thwart sandboxing, and deploy double-extortion strategies leveraging encrypted files and exfiltrated data.

Leak and Extortion Tactics: Qilin maintains a Tor-based leak site for naming victims and publishing stolen data. Affiliates may also auction data to third parties if initial extortion fails. The group has expanded into triple extortion, threatening DDoS and media exposure.

High-Profile Target: Asahi Group Holdings (Japan) suffered significant disruption from Qilin during this period. Negotiation efforts failed, and 27GB of sensitive data were publicly leaked. Other victims announced this week include France's Paris Retina Vision and Spain's Tax Agency.

Detailed TTPs

Initial Access
- Spearphishing with malicious attachments (e.g., LNK, ZIP, ISO).
- Credential harvesting and brute-force against RDP/VPN endpoints.
- Exploitation of Citrix ADC, Fortinet VPN, and VMware ESXi flaws.
- Abuse of initial access brokers (IABs) for compromised accounts.
- MFA bombing and session hijacking to bypass identity protections.

Execution
- Deployment of ransomware via PsExec, WMI, and GPO.
- Safe Mode reboots to bypass security tools (using bcdedit, AutoLogon).
- Use of LOLBins: rundll32, mshta, cmd, and PowerShell.
- Packed binaries (Themida, UPX) evade static detection.

Persistence
- Creation of new local admin accounts.
- Scheduled tasks and service creation for payload delivery.
- Registry modifications: HKLM Run keys and boot configurations.
- Deployment of remote access tools (e.g., AnyDesk, MeshCentral).

Privilege Escalation
- Use of Mimikatz and LSASS dumping for token stealing.
- BYOVD attacks: deployment of vulnerable drivers (TPwSav.sys).
- Exploitation of UAC bypass techniques.
- Token impersonation and process injection.

Defence Evasion
- Windows Defender tampering: DisableRealtimeMonitoring = 1.
- Shadow copy deletion via vssadmin, wbadmin, diskshadow.
- Event log clearance with wevtutil and PowerShell.
- File renaming and timestamp modification to avoid detection.
- Packing and code obfuscation to hinder reverse engineering.

Credential Access
- LSASS memory scraping with direct system calls.
- Credential dumping via reg save of SAM/SECURITY hives.
- Browser credential harvesting (Chrome, Firefox, Edge).
- NTDS.dit extraction for domain-wide credential capture.

Discovery
- AD enumeration using built-in tools and AdFind.
- Network scanning (Nmap, AngryIP, SoftPerfect).
- Identification of backup systems and NAS devices.
- Software inventory via WMI and registry analysis.

Lateral Movement
- Use of PsExec and WMI for remote command execution.
- GPO abuse for ransomware deployment across domains.
- RDP sessions using stolen credentials.
- SSH access to ESXi hosts for Linux variant deployment.

Collection & Exfiltration
- Data aggregation into staging directories.
- Compression with 7-Zip, WinRAR, often encrypted.
- Exfiltration to cloud storage (MEGA, Dropbox) via Rclone.
- Use of FTP/SFTP servers controlled by threat actors.

Impact
- AES-CTR file encryption with RSA-4096 key wrapping.
- Ransom notes: QILIN-ReadMe.txt, _RECOVER.txt.
- Encrypted file extensions: .MmXReVIxLV, .X0aMJ, unique per target.
- Public shaming via leak sites and threat of data sale.

MITRE ATT&CK Mapping

Tactic	Technique (ID)	Description
Initial Access	T1566, T1190, T1078	Phishing, exposed RDP/VPN, valid accounts
Execution	T1059, T1053.005, T1569.002	PowerShell, scheduled task, service creation
Persistence	T1547.001, T1053.005	Registry keys, Safe Mode auto-login
Priv Esc	T1003, T1543, T1068	LSASS dump, BYOVD, system service abuse
Defence Evasion	T1070.001, T1562.001, T1490	Log clearing, AV disable, shadow deletion
Credential Access	T1003, T1555, T1552.001	LSASS + browser credentials, SAM dumping
Discovery	T1087, T1046, T1069	Account, network, group discovery
Lateral Movement	T1021.002, T1021.001, T1484.001	SMB, RDP, GPO push
Exfiltration	T1041, T1567.002	FTP/Cloud exfiltration
Impact	T1486, T1490	File encryption, recovery inhibition

Indicators of Compromise (IOCs)

Hashes:
- 31c3574456573c89d444478772597db40f075e25c67b8de39926d2faa63ca1d8
- c9707a3bc0f177e1d1a5587c61699975b1153406962d187c9a732f97d8f867c5
- a7f2a21c0cd5681eab30265432367cf4b649d2b340963a977e70a16738e955ac
- 13cda19a9bf493f168d0eb6e8b2300828017b0ef437f75548a6c50bfb4a42a09
- 9e1f8165ca3265ef0ff2d479370518a5f3f4467cd31a7b4b006011621a2dd752

IPs:
- 193.106.175.107
- 45.134.140.69
- 184.174.96.70
- 184.174.96.74
- 180.131.145.73
- 188.34.188.7
- 185.208.156.157
- 185.196.10.19

C2 & Leak Infrastructure:
- ftp://dataShare:nX4aJxu3rYUMiLjCMtuJYTKS@85.209.11.49
- ftp://dataShare:2bTWYKNn7aK7Rqp9mnv3@188.119.66.189
- hxxp://catcompany[.]info
- 80.64.16.87
- 176.113.115.97
- 176.113.115.209

Artifacts:
- Ransom notes: _RECOVER.txt, QILIN-ReadMe.txt
- Encrypted extensions: .MmXReVIxLV, .X0aMJ, custom per attack
- Suspicious files: avupdate.dll, IPScanner.ps1, logon.bat, main.exe, setlang.exe, vcredist_x86.exe, tniwinagent.exe

Registry & Config Changes:
- HKLM\SOFTWARE\Microsoft\Windows Defender\Real-Time

Protection\DisableRealtimeMonitoring = 1
- Safe Mode: HKLM\SYSTEM\CurrentControlSet\Control\SafeBoot\Option
- AutoLogon Keys: DefaultUserName, DefaultPassword, AutoAdminLogon

Tools Used:
Rclone, WinRAR, 7-Zip, PsExec, AdFind, AnyDesk, Mimikatz, PowerView, Process Hacker

Detection & Mitigation Recommendations
- Alert on registry edits to Defender policies.
- Monitor vssadmin / wbadmin / diskshadow usage.
- Detect encryption-like file activity spikes.
- Monitor Rclone uploads and unknown FTP connections.
- Watch for Safe Mode boot flag modifications.
- EDR policy: block LSASS dumps, enable tamper protection.
- Segment ESXi access and disable unused management interfaces.
- Enforce MFA, disable legacy protocols.
- Flag creation of new admin accounts and GPO changes.
- Block unapproved software: WinRAR CLI, Rclone, AdFind.

Worldwide Ransomware Victims

The United States remained the primary global ransomware target this week, accounting for 56.52% of reported victims. It's overwhelming share underscores adversaries' continued prioritisation of U.S.-based organisations due to their extensive digital infrastructure, high-value industries, and pressure to rapidly resolve disruptions.

France (5.43%) emerged as the second most impacted country, reflecting concentrated targeting of Western Europe. Canada (4.89%), Spain (3.26%), and Italy, Germany, and the United Kingdom (each 2.17%) followed, reinforcing Europe and North America's ongoing position at the centre of ransomware operations.

Other notable nations included Japan (1.63%), Australia (1.63%), India (1.09%), Switzerland (1.09%), Brazil (1.09%), South Korea (1.09%), Malaysia (1.09%), United Arab Emirates (1.09%), and the Netherlands (1.09%). These mid-tier figures point to the breadth of ransomware's reach across both industrialised Asia-Pacific economies and high-value European hubs.

A long tail of countries reported isolated cases (0.54% each), including Bulgaria, Norway, Venezuela, Colombia, Denmark, Indonesia, Pakistan, Austria, Thailand, Cyprus, Taiwan, Mexico, South Africa, Kenya, Greece, Ghana, Poland, Nigeria, and Morocco. While individually small, these incidents highlight ransomware's opportunistic exploitation of victims worldwide, spanning every continent.

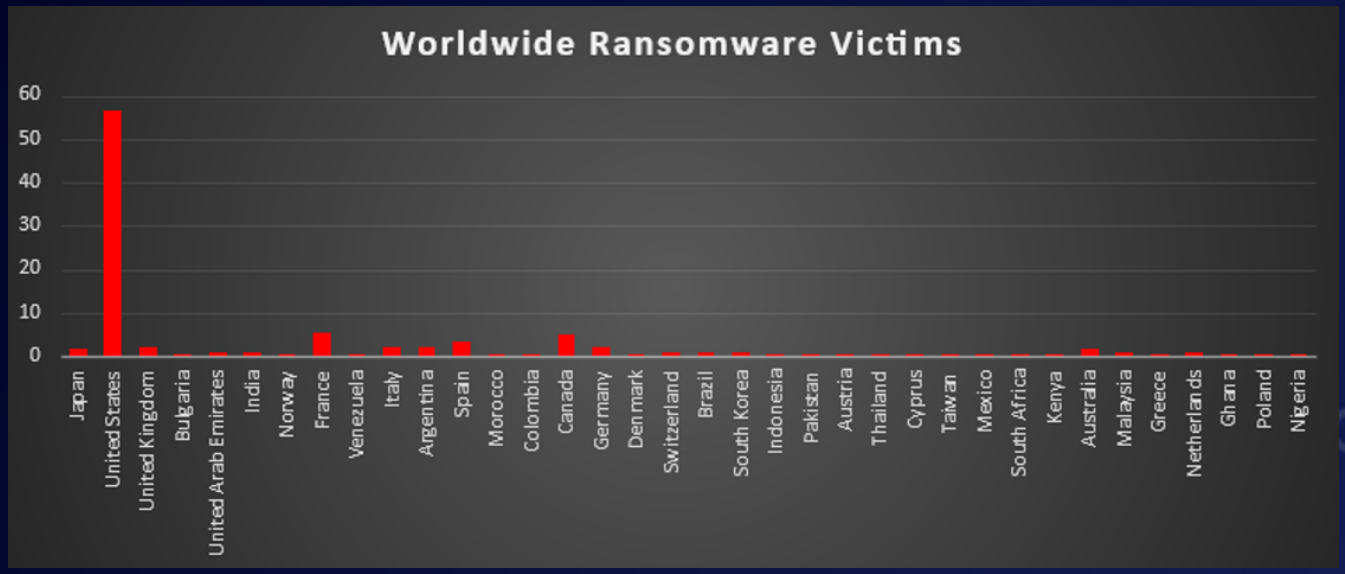

Figure 2: Ransomware Victims Worldwide

Industry-wide Ransomware Victims

Manufacturing was the most heavily impacted sector this week, accounting for 21.2% of incidents. Its reliance on operational technology, limited tolerance for downtime, and integration into global supply chains continue to make it one of ransomware's most lucrative targets.

Business Services (10.87%) ranked second, reflecting adversaries' sustained focus on outsourcing, IT, and consulting firms. By compromising these providers, attackers gain leveraged access into multiple downstream client environments.

Other heavily targeted verticals included Retail (8.15%), Construction (7.61%), and Hospitality (6.52%), all industries with customer-facing operations and complex supply chains that are highly sensitive to disruption. Law Firms (5.43%) and IT (5.43%) also saw elevated targeting, underscoring ransomware's appeal in data-rich environments that hold sensitive client, legal, or digital assets.

The Energy sector (4.35%) and Federal entities (4.89%) also featured prominently, showing attackers' intent to pressure critical infrastructure and public institutions. Transportation (3.8%), Finance (2.72%), Education (2.72%), and Consumer Services (2.72%) formed a mid-tier cluster, all sectors where operational or data disruption directly affects large populations.

Smaller but still notable victimisation was recorded in Organisations (2.17%), Electronics (2.17%), Real Estate (2.17%), and Insurance (2.17%), sectors often targeted for their financial or operational leverage. Meanwhile, Healthcare (1.63%), Minerals & Mining (1.09%), Media & Internet (1.09%), and Telecommunications (0.54%) continued to face lower but consistent levels of targeting. Agriculture (0.54%) rounded out this week's activity with isolated incidents.

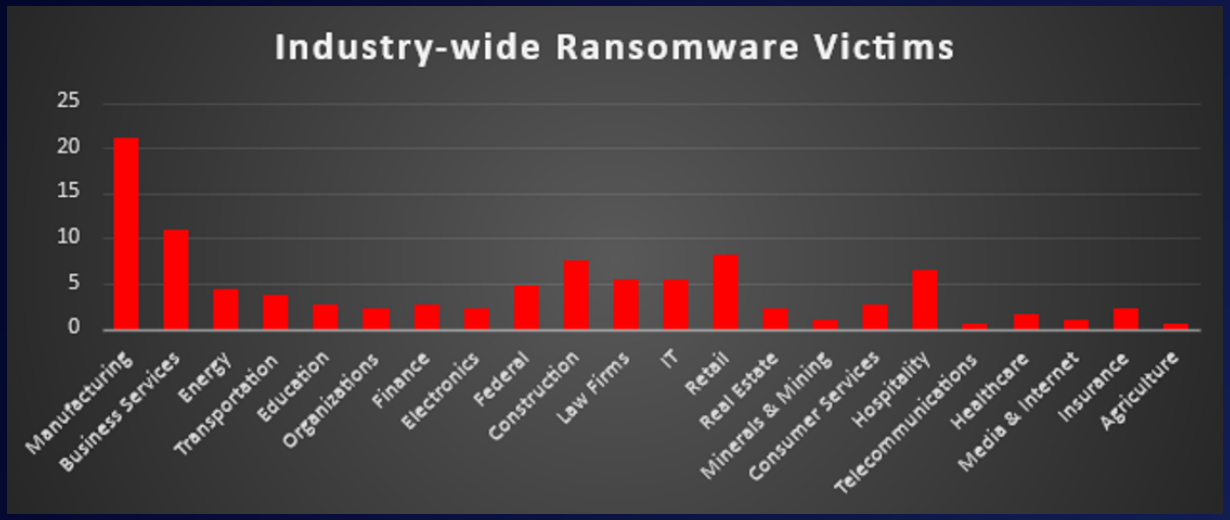

Figure 3: Industry-wide Ransomware Victims