Red Piranha
unified threat management

THREAT INTELLIGENCE REPORT

Sept 23 - 29, 2025

Report Summary:

- **New Threat Detection Added**
  - TA2726
- **Detection Summary**
  - **Threat Protections integrated into the Crystal Eye - 124**
  - **Newly Detected Threats - 67**

The following threats were added to Crystal Eye this week:

1. TA2726

TA2726 is another malicious actor using the QuickFix technique to trick users into downloading malware disguised as software updates. The Threat Actor also utilises a traffic distribution service (TDS) to redirect users to these updates. The threat actors' payloads operate on most major operating systems, including Windows, macOS, and Android.

Threats Protected: 1
Class Type: Malware
Rule Set Type (*https://attack.mitre.org/matrices/enterprise/*)**:**

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

Kill Chain:

Tactic	Technique ID	Technique Name
Command-and-Control	T1071.001	Application Layer Protocol: Web Protocols

Current Threat Summary

Known exploited vulnerabilities (Week 5 September 2025)

Vulnerability	CVSS	Description
CVE-2025-20362	6.5	Cisco Secure Firewall Adaptive Security Appliance (ASA), and Secure Firewall Threat Defence (FTD) Software VPN Web Server contain a vulnerability that can allow an unauthenticated remote attacker to gain access to the device without authorisation via a specially crafted HTTP request. This vulnerability has been actively exploited and can be chained with CVE-2025-20333 to further compromise the device.
CVE-2025-20333	9.9	Cisco Secure Firewall Adaptive Security Appliance (ASA), and Secure Firewall Threat Defence (FTD) Software VPN Web Server contain a buffer overflow vulnerability that can allow an authenticated remote attacker to execute code on the device via a specially crafted HTTP request. This vulnerability is known to be actively exploited and can be chained with CVE-2025-20362 to facilitate the initial access on the device.
CVE-2025-10585	8.8	Google Chromium contains a type-confusion vulnerability that could allow a remote attacker to execute code upon visiting a specially crafted HTML page. This vulnerability is within the V8 JavaScript and WebAssembly engine components of the browser and affects versions prior to 140.0.7339.185.

For more information, please visit the **Red Piranha Forum**:
https://forum.redpiranha.net/t/known-exploited-vulnerabilities-catalog-4th-week-of-september-2025/600

Updated Malware Signatures (Week 5 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.”

Ransomware Report

Ransomware Hits Last Week

Qilin led the ransomware ecosystem with 20.33% of reported incidents, confirming its role as a dominant operator in the current landscape. Its sustained momentum points toward a mix of affiliate-driven campaigns and opportunistic targeting across sectors.

Pear followed strongly at 13.01%, cementing itself as a significant threat actor with consistent victim disclosures. KillSec3 and Play each accounted for 9.76%, showing steady operations with mid-tier but impactful campaigns.

WorldLeaks was responsible for 5.69%, maintaining visibility in the leak-and-extort space. Inc Ransom and Miga both logged 4.88%, keeping their presence active across multiple regions.

Several groups registered 3.25% each, including BlackShrantac, Space Bears, Nova, Lynx, and DragonForce, indicating a cluster of operators maintaining sustained though smaller-scale activity.

Smaller actors such as Sarcoma (2.44%) and Akira (1.63%) remain relevant in niche campaigns, while Arachnal Leak (1.63%) added to the long-tail distribution of activity.

A wide range of groups, including Leaknet, Abyss-Data, The Gentlemen, Warlock, Radiant Group, Rhysida, J Group, Beast, Chaos, Qilin-Securotrop, and Anubis, each recorded 0.81% of incidents. While individually limited, their combined presence underscores the fragmented and diverse nature of ransomware operations, where many actors operate below mainstream visibility but still contribute to the overall threat landscape.

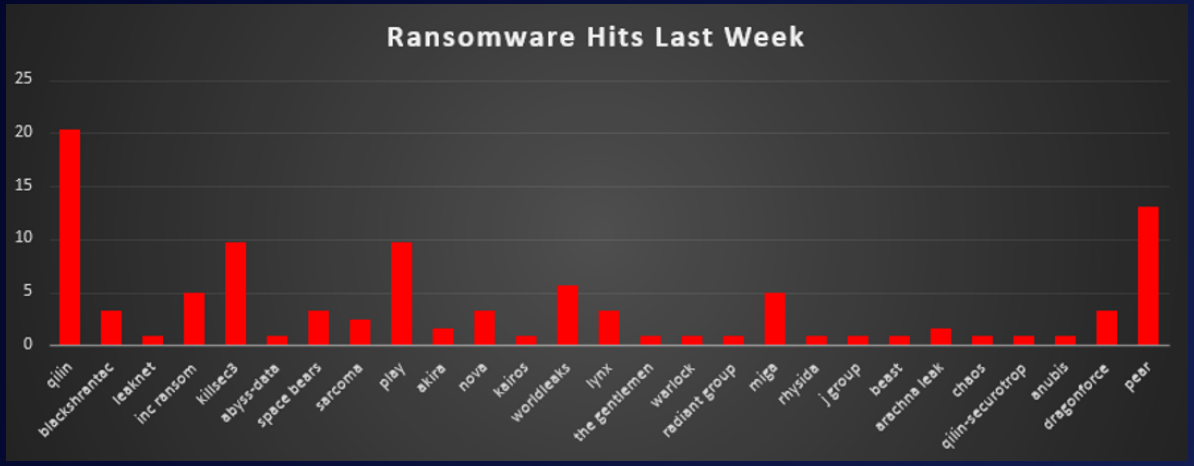


Figure 1: Ransomware Group Hits Last Week

Chaos Ransomware

Chaos" here refers to the new RaaS group active in 2025 (not the old Chaos/Yashma builder). The operation conducts classic big-game-hunting/double-extortion. Within Sep 20–28, 2025, multiple public sandboxes captured fresh Chaos encryptors and a new victim claim (AMS Fulfillment) on the group's data-leak site. These samples exhibit the same playbook: inhibit recovery (wbadmin, bcdedit), rename/encrypt files, drop a read_it.txt note, and, in some runs, touch browser credential stores.

Detailed TTPs

Initial Access
- Voice-phishing (helpdesk/social engineering) to coerce remote-assist access or MFA push approval.
- Compromised credentials (valid accounts) from stealer logs or prior breaches used on VPN/SSO/RDP.
- Opportunistic phishing with links to loader/launcher hosted on throwaway infra.

Detections: spikes in admin/SaaS logins from Tor/VPN ranges; anomalous MFA approvals; helpdesk tickets tied to "remote assist" requests; first-seen logins on RDP/VPN from atypical geos.

Execution
- Windows: LOLBIN-based scripts invoke recovery inhibition (bcdedit, wbadmin) and launch encryptor; batch/PowerShell wrappers.
- Linux/ESXi: shell scripts to stage and execute encryptor; parallelised worker threads for fast impact.

Detections: process-chains invoking bcdedit/wbadmin; unsigned executables launched from user profile/temp; unknown shell scripts on hypervisors; sudden high-entropy writes on datastores.

Persistence
- Startup folder drop of ransom note/launcher; registry Run/RunOnce keys.
- RMM tool abuse (ScreenConnect/AnyDesk) or added SSH keys on servers/hypervisors.

Detections: new binaries/shortcuts in Startup paths; fresh Run*/Scheduled Task entries; newly installed or side-loaded RMM agents; unexpected authorized_keys entries.

Privilege Escalation
- Use of already-privileged stolen creds; on Windows, attempts to dump LSASS or exploit local privesc to reach admin.

Detections: abnormal LSASS access; token/manipulation events; privilege assignment to unusual accounts; driver/service creation from non-IT users.

Discovery
- Environment scoping: AD group/user enumeration; share walks; vCenter/ESXi inventory queries; system/locale checks (for geo-fencing).

Detections: enumeration of domain admins from non-IT endpoints; aggressive SMB share listing; unusual vCenter API queries; registry reads of locale/geo keys.

Command-and-Control
- Short-lived VPS/Tor infrastructure for operator control and negotiation site access; occasional RMM backchannels.

Detections: egress to Tor directory/bridge IPs; first-seen TLS SNI/JA3 to low-reputation VPS ASNs; beacon-like RMM traffic from non-admin hosts.

Impact
- Inhibit recovery (delete backups, alter boot recovery) prior to encryption.
- Multi-threaded selective encryption; ransom note drop (e.g., read_it.txt), file rename/extension change, data-leak extortion.

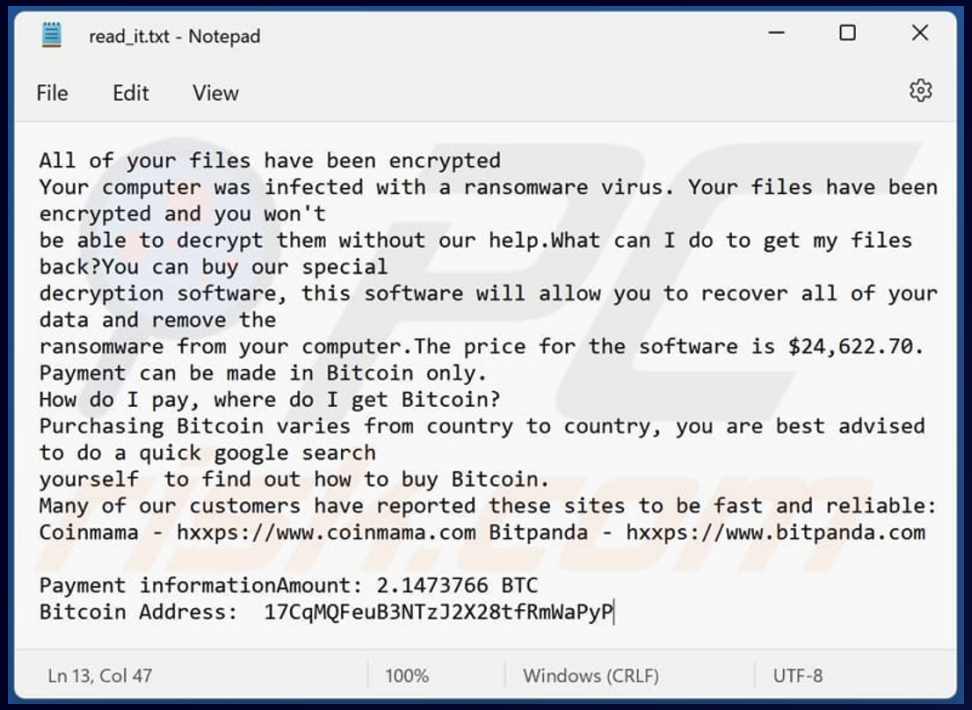
Detections: bcdedit/wbadmin/vssadmin telemetry; sharp spike in rename/write/entropy metrics; ransom note file creation in user and Startup paths; VM snapshot disablement on hypervisors.

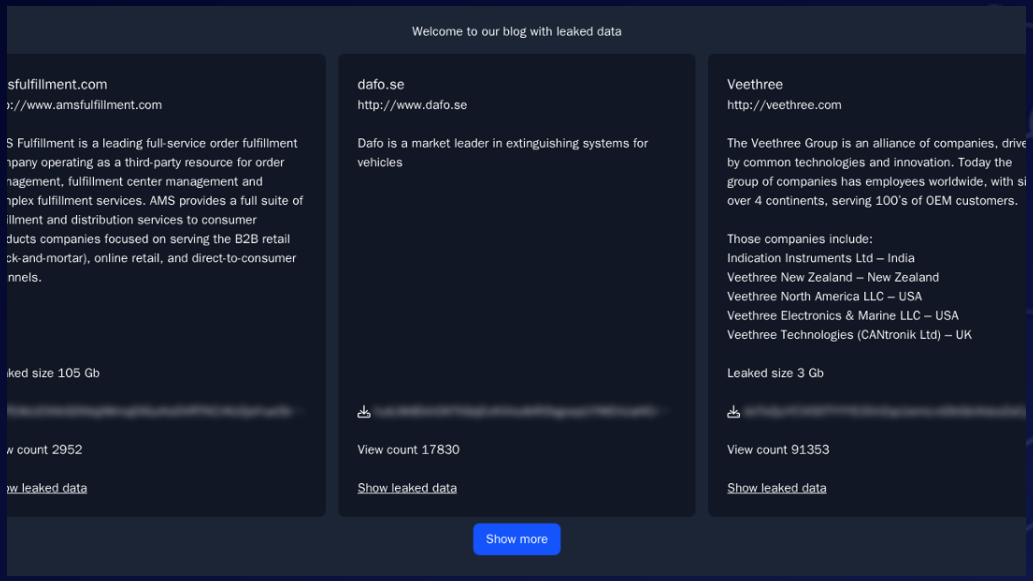
MITRE ATT&CK Mapping

Tactic	Technique (ID)	What it looks like	What it looks like
Initial Access	Phishing/Vishing (T1566)	User coerced to grant help/approve prompts	User coerced to grant help/approve prompts
Initial Access	Valid Accounts (T1078)	Stolen creds used on VPN/SSO	Stolen creds used on VPN/SSO
Execution	Cmd/PowerShell (T1059)	Scripts staging/running encryptor	Scripts staging/running encryptor
Execution	Remote Access Software (T1219)	AnyDesk/ScreenConnect/Quick Assist	AnyDesk/ScreenConnect/Quick Assist
Persistence	Startup/Run Keys (T1547.001)	Note/artifacts in Startup; autoruns	Note/artifacts in Startup; autoruns
Priv. Esc.	Privileged Accounts (T1078.004)	Elevated creds to push payloads	Elevated creds to push payloads
Discovery	Query Registry (T1012)	Locale/geo checks (e.g., Geo\Nation)	Locale/geo checks (e.g., Geo\Nation)
Discovery	System/Network (T1082/T1016)	Host/AD/share/VM enumeration	Host/AD/share/VM enumeration
Lateral Move	Remote Services: RDP/SMB (T1021.001/.002)	RDP, PsExec/WMI spread	RDP, PsExec/WMI spread
Def. Evasion	Impair Defences (T1562.001)	Stop AV/EDR; tamper services	Stop AV/EDR; tamper services
Def. Evasion / Impact	Inhibit Recovery (T1490)	wbadmin catalog delete; bcdedit tweaks	wbadmin catalog delete; bcdedit tweaks
Def. Evasion	Clear Logs / Delete (T1070.001/.004)	Log clears; cleanup	Log clears; cleanup
Collection	Data from Local (T1005)	Stage archives for leak	Stage archives for leak
Exfiltration	To Cloud/Web (T1567.002/.003)	Sync/HTTPS to leak infra	Sync/HTTPS to leak infra
C2	Proxy (T1090)	Tor/VPN relays, reverse tunnels	Tor/VPN relays, reverse tunnels
Impact	Encrypt for Impact (T1486)	Multithreaded encryption, renames	Multithreaded encryption, renames

Chaos Ransomware IOCs & Samples
SHA256
cd5df020000e93724880669c9daaeca26ecd56183667e630241aee095df16e1b
3082203c16b5c5459ae9fe55000b05a65dd143a4289934bc01dd773651698bc4
MD5
a64d9a528e1c5fc1d0a190c07d6d7571
fb6c58eb6d6ee199ad61a5b7f2f3d574
SHA1
955a91c639b2664bcf2f69c1f985136eeba5b401
b9678933f670d9c5e3b19bd974631605eb4f3853

Ransom note & artefacts
FILE: read_it.txt





Admin Server:
http://cdgi6zjox6zr5epk7k5rg673qduxy7dlkk7ws3n4vusspr5bmhx24aqd.onion/

PATHS:
C:\Users\<user>\Documents\read_it.txt
BTC ADDRESS:
bc1qlnzcep4l4ac0ttdrq7awxev9ehu465f2vpt9x0
Infrastructure / Leak
DLS (Tor):
hptqq2o2qjva7lcaaq67w36jihzivkaitkexorauw7b2yul2z6zozpqd.onion
amsfulfillment.com (discovered: 2025-09-24)
IP
144.172.103.42
45.61.134.36
107.170.35.225
File Server:
http://httj32vkww42kq3kjbsbuuv2izalkvswuyf5hepdodakrjq42ploe6ad.onion/
http://2yxf2ald2c67twt4663piypum2fu6yt4su453naxsdiilpd4m7pgu6qd.onion/
http://k6wtpxwq72gpeil5hqofae7yhbtxphbkyoe2g7rwmpx5sadc4sgsfvid.onion/

Worldwide Ransomware Victims

The United States continues to dominate the global ransomware landscape, accounting for 65.04% of all reported victims this week. This overwhelming concentration underscores its ongoing status as the most attractive target for threat actors due to its vast digital infrastructure, financial leverage, and interlinked supply chains.

Germany ranked second with 7.32%, highlighting its industrial strength and role as a key European hub for advanced manufacturing and critical sectors. Australia followed at 4.07%, maintaining its position as a consistent Asia-Pacific target. Canada also featured prominently with 3.25%, further reflecting the North American concentration of ransomware incidents.

Other notable nations included Brazil (2.44%), Italy (1.63%), Spain (1.63%), and France (0.81%), reinforcing Europe and Latin America as key secondary targets for ransomware groups.

A wide distribution of smaller-scale incidents (each 0.81%) was observed across Aruba, Turkey, Finland, Morocco, China, United Arab Emirates, New Zealand, Slovakia, Mexico, Cyprus, Singapore, Taiwan, United Kingdom, Dominican Republic, Barbados, India, and Argentina. While these countries contribute modestly to the global tally, they highlight ransomware's opportunistic reach, extending into both advanced economies and smaller nations.

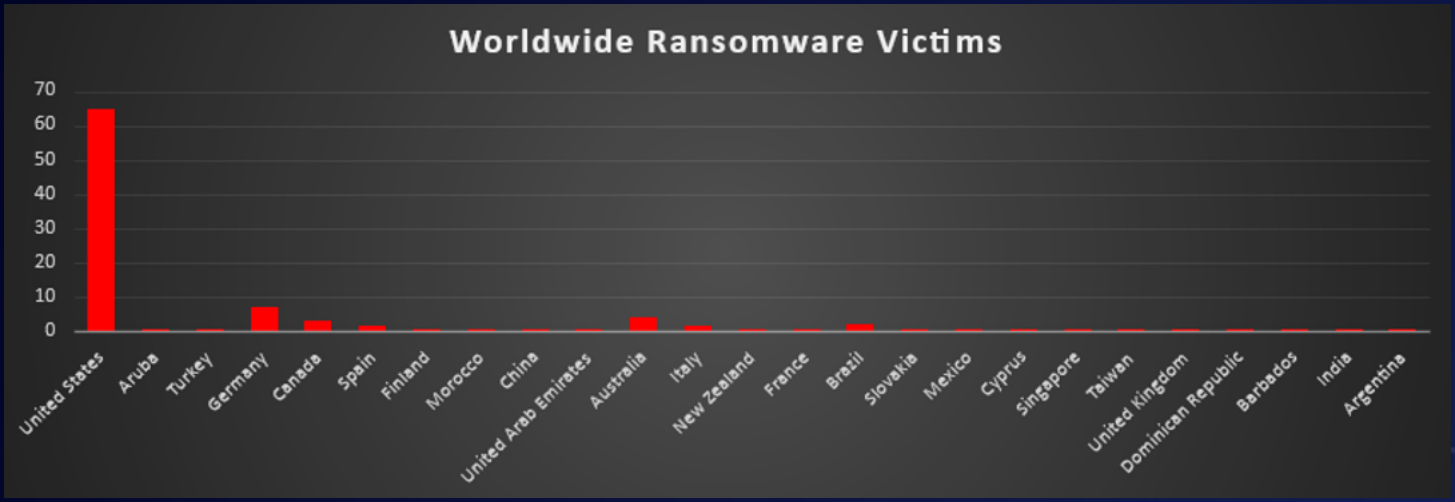


Figure 4: Ransomware Victims Worldwide

Industry-wide Ransomware Victims

Business Services once again led ransomware targeting this week, accounting for 20.33% of incidents. Its central role as a service provider across industries makes it a high-value entry point for attackers seeking widespread access.

Manufacturing followed with 8.94%, underscoring the sector's continued vulnerability due to legacy operational technologies, limited downtime tolerance, and its critical role in global supply chains. Retail ranked third at 9.76%, reflecting persistent exploitation of customer-facing operations and payment infrastructure.

Hospitality logged 10.57%, making it one of the most heavily impacted industries this week. Its reliance on digital reservations, point-of-sale systems, and customer data creates prime opportunities for extortion. Construction and Law Firms both reported 8.13%, reinforcing attackers' focus on industries where disruption directly impacts time-sensitive operations and highly sensitive legal or project data.

Mid-tier targeting was observed across Finance (6.5%), IT (4.88%), Federal (4.07%), Education (4.07%), and Real Estate (4.07%). These sectors remain attractive due to their concentration of sensitive data, regulatory exposure, and reliance on digital services.

Smaller but still notable incidents were reported in Transportation (2.44%), Organisations (2.44%), Energy (1.63%), Insurance (1.63%), Consumer Services (1.63%), and Agriculture (0.81%). Although individually less significant, these cases highlight ransomware's opportunistic spread across a wide range of verticals.

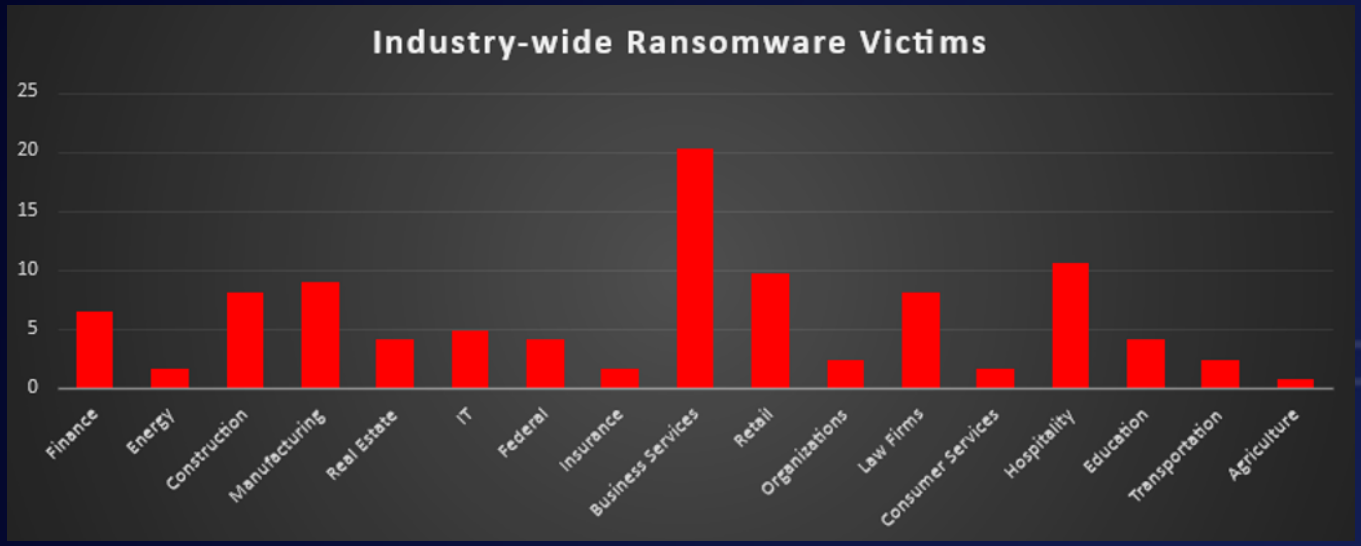


Figure 5: Industry-wide Ransomware Victims