Red Piranha
unified threat management

THREAT INTELLIGENCE REPORT

Nov 04 - 10, 2025

Report Summary:

- **New Threat Detection Added**
  - IcedID
  - TA569
- **Detection Summary**
  - **Threat Protections integrated into the Crystal Eye - 81**
  - **Newly Detected Threats - 8**

The following threats were added to Crystal Eye this week:

1. IcedID

Aka BokBot, IcedID is a malware originally classified as banking malware that was first observed in 2017. It also acts as a loader for other malware, including ransomware. The well-known IcedID version consists of an initial loader that contacts a Loader C2 server, downloads the standard DLL Loader, which then delivers the standard IcedID Bot. IcedID is developed and operated by the actor named LUNAR SPIDER.

Threats Protected: 1
Class Type: Malware
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
Discovery	T1087.002	Account Discovery: Domain Account
Command-and-Control	T1071.001	Application Layer Protocol: Web Protocols
Persistence, Privilege Escalation	T1547.001	Boot or Logon AutoStart Execution: Registry Run Keys / Startup Folder

2. TA569

TA569 is a prolific group that engages in a variety of financial cybercrimes. They are a well-funded and well-organised group that may operate in Russia or Eastern Europe. Their attacks typically include phishing, website injections, and malware (such as bank trojans) to steal financial information from individuals and/or organisations. Their main attack tools include a web loader called SocGholish, the bank Trojan Chthonic, and the remote-control software NetSupport.

Threats Protected: 16
Class Type: Malware
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
Discovery	T1082	System Information Discovery
Execution	1204.001	User Execution: Malicious Link
Initial Access	T1566.002	Phishing: Spearphishing Link
Defence Evasion	T1036.005	Masquerading: Match Legitimate Resource Name or Location

Current Threat Summary

Known exploited vulnerabilities (Week 5 October 2025)

Vulnerability	CVSS	Description
CVE-2025-48703	9	CWP Control Web Panel contains a vulnerability within the filemanager module of the software that can allow an unauthenticated remote attacker to execute operating system commands on the system via a HTTP request, this vulnerability affects versions prior to 0.9.8.1205.
CVE-2025-11371	7.5	Gladinet CentreStack and Triofox contains a vulnerability that can allow an unauthenticated remote attacker to read files on the filesystem and affects all versions up to 16.7.10368.56560. Exploitation of this vulnerability may allow an attacker to gain further access on the system.

For more information, please visit the **Red Piranha Forum**:
https://forum.redpiranha.net/t/known-exploited-vulnerabilities-catalog-1st-week-of-november-2025/616

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 led global ransomware activity this week with 17.39 % of reported incidents, maintaining its position as one of the most aggressive and persistent groups operating across multiple regions and sectors.

Akira (15.22 %) followed closely, continuing to expand its victim base through opportunistic targeting and affiliate-driven campaigns. Inc Ransom (9.42 %) and Clop (9.42 %) both registered strong presences, marking a sustained resurgence of mid-tier actors leveraging known exploits and data-extortion tactics.

A mid-range cluster of activity came from Play (5.8 %), Nightspire (4.35 %), WorldLeaks (2.9 %), Nova (2.9 %), and Interlock (2.9 %), reflecting continuous diversification within active leak-site operations.

Several other groups maintained moderate visibility, including DragonForce (2.17 %), RansomHouse (2.17 %), MyData (2.17 %), Leaknet (2.17 %), Rhysida (2.17 %), and Stormous (2.17 %), each sustaining multi-target campaigns at smaller scales.

Lower-level but consistent activity (0.72–1.45 %) was observed from Anubis, Coinbase Cartel, The Gentlemen, Medusa, Space Bears, Black Nevas, Genesis, RansomHouse, SafePay, Sinobi, Nitrogen, Brotherhood, Kryptos, Everest, and Handala.

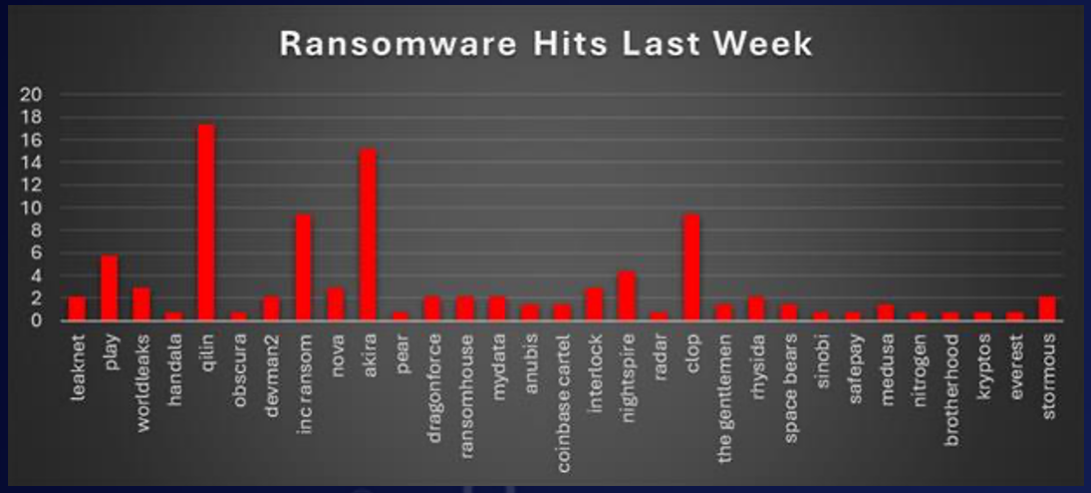


Figure 1: Ransomware Group Hits Last Week

Handala Ransomware

Handala began as a politically-motivated hacktivist collective and has evolved into a destructive wiper-capable ransomware operator since late 2023. During the Nov 1–7 window, the group emphasised public data dumps and doxxing, continuing its regular weekend disclosures and maintaining pressure on targeted organisations rather than publishing new, large-scale exploit activity.

Detailed TTPs (narrative)

1. Initial access — Targeting via spearphishing attachments and credential harvesting; in some cases, exploitation of public-facing services to drop first-stage loaders. Attachments frequently masquerade as utilities or update installers (example: F5UPDATER.exe).
2. Staging & loader behaviour — Multi-stage chain: lightweight downloader/loader Delphi/packed second-stage in-memory unpacking that writes and executes wiper modules. Loaders often use signed legitimate binaries as proxies to bypass naive allowlists.
3. Execution & persistence — Uses scheduled tasks and Run keys for persistence; leverages valid credentials and lateral movement tools (PsExec-like behaviour) to spread; frequently removes shadow copies, modifies BCD/boot settings and overwrites MBR/partition metadata to disable recovery.
4. Obfuscation & anti-forensics — Heavy string/base64 obfuscation, custom packing, and anti-VM/sandbox checks. Wiper components include routines to zero out key file types and to corrupt filesystem metadata.
5. Data discovery & exfiltration — Automated collection of high-value documents and database dumps. Exfiltration occurs over encrypted HTTPS to anomalous hosts and via cloud storage/Telegram endpoints; JA3/TLS fingerprinting and non-standard ports are observed.
6. Impact phase — Wipe-first actions remove backups and recovery artifacts, then selective encryption or public data dump. Public extortion/doxxing via onion sites and Telegram channels follows, pressuring victims and increasing reputational damage.
7. Post-compromise interaction — Use of Tor hidden services for victim communication and leak sites; actor maintains a cadence of disclosures to amplify impact.

MITRE ATT&CK Mapping Table

Tactic	Technique ID	Technique Name
Initial Access	T1566.001	Spearphishing Attachment
Initial Access	T1190	Exploit Public-Facing Application
Execution	T1059.005	Command & Scripting Interpreter (VB / AutoIt / bash)
Execution	T1218	Signed Binary Proxy Execution
Persistence	T1547.001	Registry Run Keys / Scheduled Tasks
Privilege Escalation	T1078	Valid Accounts
Defence Evasion	T1027	Obfuscated Files or Information
Defence Evasion	T1562	Impair Defences (AV/EDR Tampering)
Discovery	T1083	File and Directory Discovery
Collection	T1005 / T1119	Data from Local System / Automated Collection
Exfiltration	T1041	Exfiltration over C2 Channel
Impact	T1561	Disk Wipe
Impact	T1486	Data Encrypted for Impact

IOCs & C2 Infrastructure

File / Artifact Indicators

- F5UPDATER.exe - Loader (SHA256: fe07dca68f288a4f6d7cbd34d79bb70bc309635876298d4fde33c25277e30bd2)
- Handala.exe - Secondary Delphi loader (SHA256: 454e6d3782f23455875a5db64e1a8cd8eb743400d8c6dadb1cd8fd2ffc2f9567)
- Hatef.exe - Windows wiper (SHA256: e28085e8d64bb737721b1a1d494f177e571c47aab7c9507dba38253f6183af35)
- Hamsa.sh - Linux base64-obfuscated bash wiper (SHA256: 6f79c0e0e1aab63c3aba0b781e0e46c95b5798b2d4f7b6ecac474b5c40b840ad)
- Extensions: .NBA observed
- Ransom notes: READ_ME.txt, readme.txt, READ_ME_.TXT

C2 & Network Infrastructure

Active IPs/Ports:

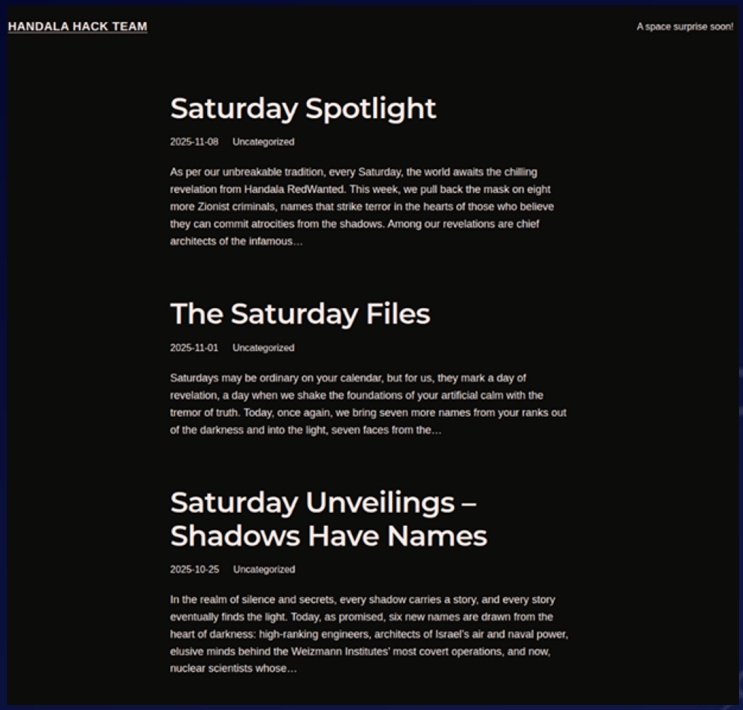
- 185.216.70.236:8443
- 194.180.48.149:8443
- 194.180.48.18:10443
- 171.22.28.245:41337
- 194.169.175.132
- 193.42.33.29

Domains:

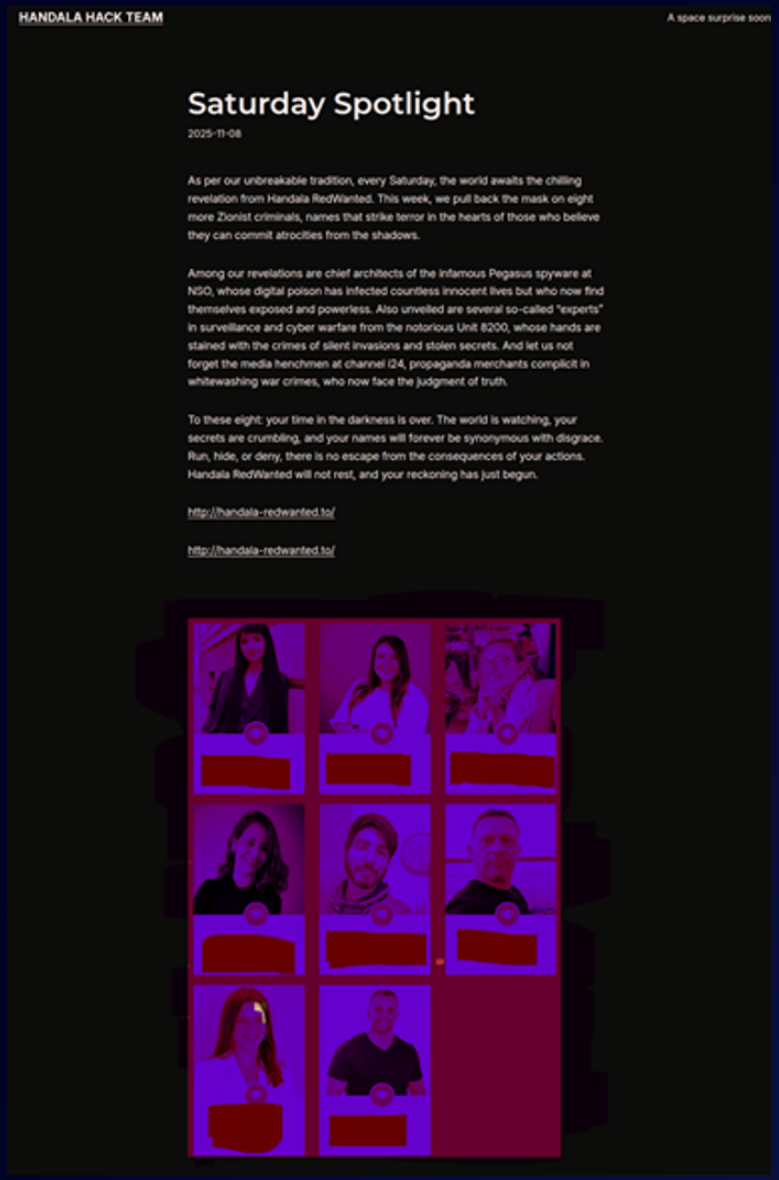
- xn--wnscp-tsa[.]net – fake WinSCP domain
- Exfil endpoints: HTTPS/Tor, Telegram bots, cloud storage (Storj/S3-like)

Onion Links:

- http://vmjfieomxhnfjba57sd6jjws2ogvowjgxhhfglsikqvvrnrajbmpxqqd[.]onion
- https://handala[.]to/
- http://handala-redwanted[.]to



- http://handala-hack[.]to
- supporthandala[.]onion – chat interface for victims



Crystal Eye 5.5 Mitigation

1. Email/Web Filtering: Block executable attachments, ISO files, and spoofed domains; enable content disarm.
2. EDR Correlation: Detect bcdedit, vssadmin, and PsExec execution chains; alert on AV service stops.
3. Network Controls: Block C2 IPs/domains; restrict outbound HTTPS to unknown IPs.
4. Segmentation: Limit SMB/WinRM; isolate admin workstations.
5. Backup Hardening: Enforce immutable, offline backups and periodic restore verification.
6. Response Playbook: Rapid isolate, collect volatile data, rotate credentials, and alert SOC/PR.

Worldwide Ransomware Victims

The United States continued to dominate ransomware targeting this week, accounting for 55.07% of all reported victims. This overwhelming concentration highlights the country's persistent vulnerability due to its extensive enterprise ecosystem, critical infrastructure, and high-value digital operations.

India (5.07%) ranked second, reflecting a steady increase in attacks on the nation's growing IT, business outsourcing, and manufacturing sectors. The United Kingdom (4.35%), France (2.9%), Germany (2.9%), and Australia (2.9%) followed, reinforcing the trend of sustained activity across major Western economies.

Mid-tier targeting included Japan (2.17%), Singapore (2.17%), and the United Arab Emirates (2.17%), demonstrating ransomware's widening geographic footprint across both the Asia-Pacific and Middle Eastern regions.

Smaller but recurring incidents were observed in Spain, Mexico, Switzerland, Vietnam, Brazil, and Canada (each 1.45%), while isolated attacks (each 0.72%) were recorded in Sweden, Austria, China, Malaysia, Thailand, Argentina, Slovenia, Zambia, Sri Lanka, Netherlands, Egypt, Ukraine, Indonesia, Morocco, and Italy.

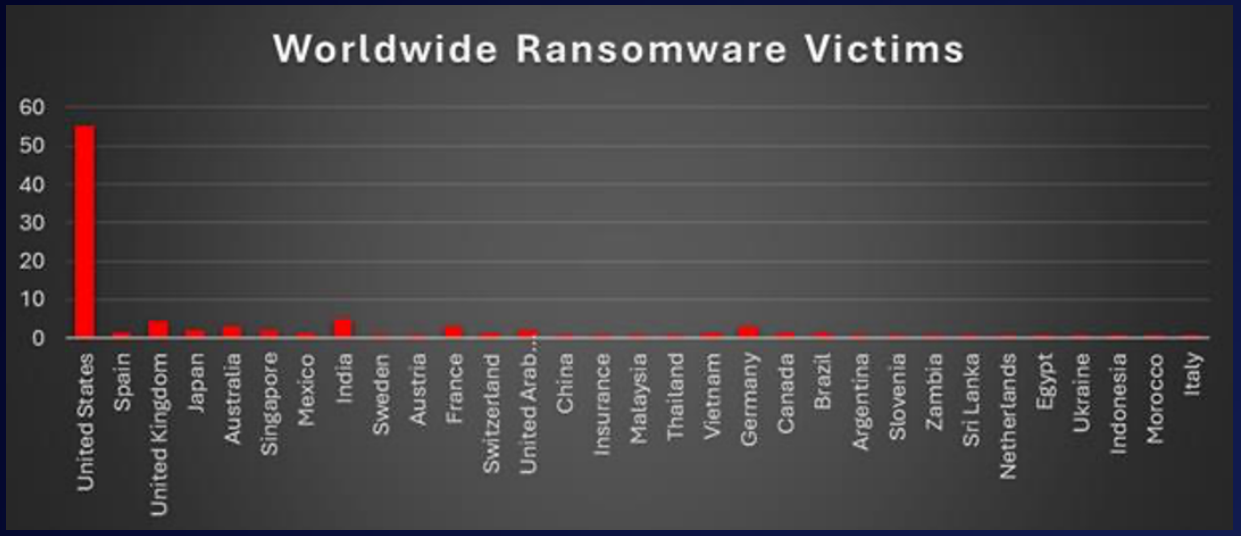


Figure 4: Ransomware Victims Worldwide

Industry-wide Ransomware Victims

Manufacturing was the most heavily impacted sector this week, representing 21.74 % of total incidents. Its critical supply-chain role, reliance on legacy operational systems, and minimal tolerance for downtime continue to make it ransomware's top-value target.

Business Services (14.49 %), Construction (9.42 %), and Retail (7.97 %) followed, underscoring attackers' preference for industries with extensive digital exposure, vendor interdependencies, and constant financial throughput. These sectors provide multiple entry points and strong leverage for extortion.

Hospitality (7.97 %) remained a high-risk vertical, driven by attacks on reservation systems, payment platforms, and customer data repositories. Law Firms (5.8 %) and Transportation (5.07 %) also featured prominently, reflecting the appeal of legal and logistics data to financially motivated actors.

Mid-tier targeting spanned Media & Internet (4.35 %), Finance (3.62 %), and Healthcare (2.9 %), where disruption and data sensitivity provide strong ransom pressure. Consumer Services (2.17 %), Education (2.17 %), Real Estate (2.17 %), Insurance (2.17 %), and Federal entities (2.17 %) showed steady but moderate exposure.

Smaller yet recurring incidents were observed in Energy (1.45 %), Electronics (1.45 %), Telecommunications (0.72 %), Minerals & Mining (0.72 %), and Organisations (0.72 %), demonstrating that even niche sectors are not immune.

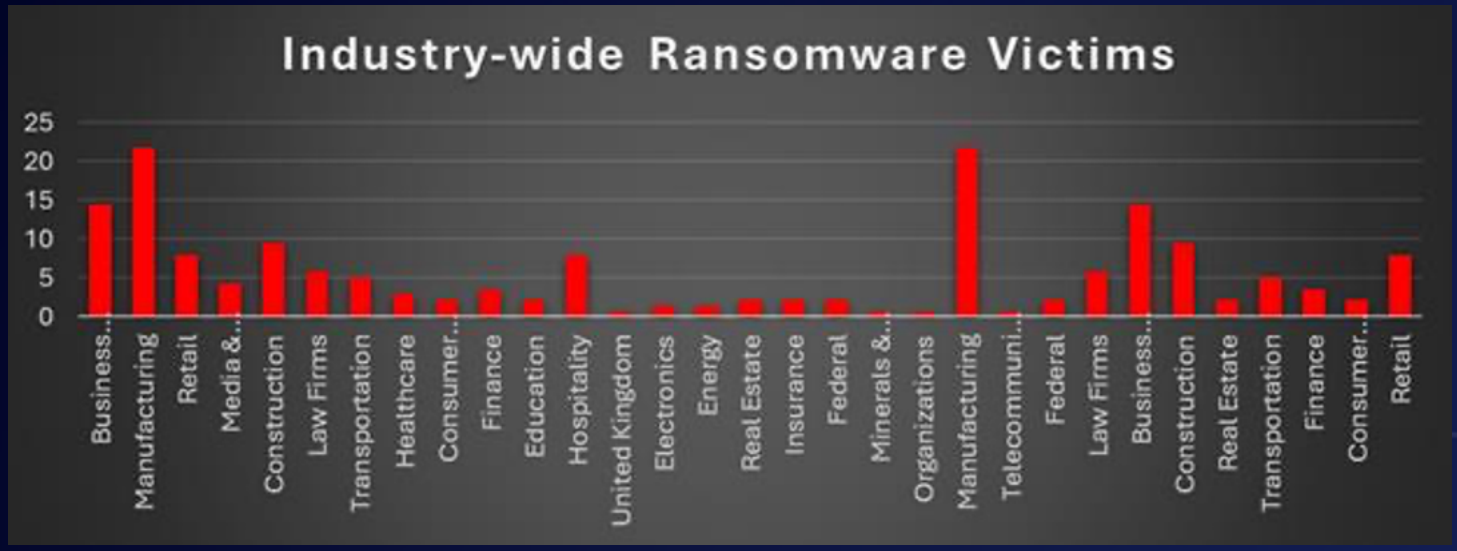


Figure 5: Industry-wide Ransomware Victims