Red Piranha
unified threat management

THREAT INTELLIGENCE REPORT

June 17 - 23, 2025

Report Summary:

- **New Threat Detection Added**
  - Predator Spyware
  - Adaptix
- **Detection Summary**
  - **Threat Protections integrated into the Crystal Eye - 153**
  - **Newly Detected Threats – 2**

The following threats were added to Crystal Eye this week:

1. Predator Spyware

Predator Spyware is developed by Intellexa (formally Cytrox), a company based in North Macedonia. This spyware has been used on politicians, businessmen, and journalists. The Predator has several features that make it a nightmare for anyone who's a target. It has real-time monitoring capabilities, data collection for items such as call logs, messages, location data, and more. It also contains C2 capabilities which allows the attacker to force video and microphone usage.

Predator has a stealth mode to allow it to be very hard to detect and is cross-platform compatible. It is compatible with Android and iOS devices.

The spyware usually makes its way onto unsuspecting victims' devices through unpatched and zero-day vulnerabilities. Vulnerabilities in Google Chrome, Linux, and Android were used in the past.

Threats Protected: 02
Rule Set Type:

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

Class Type: Malware
Kill Chain:

Tactic	Technique ID	Technique Name
Initial Access	T1190	Exploit Public-Facing Application
Collection	T1123	Audio Capture
	T1005	Data from Local System
	T1113	Screen Capture
	T1125	Video Capture
Command-and-Control	T1665	Hide Infrastructure
	T1219	Remote Access Tools
Exfiltration	T1041	Exfiltration Over C2 Channel

2. Adaptix

Adaptix is an open-source C2 framework that is used for post-exploitation for pentesters. This tool is being used by Fog ransomware to maintain persistence on victims.

Adaptix contains features such as File and Process browser, Socks Proxy support, local and reverse port forwarding, and Cross-platform development, so it has agent support and monitoring support for Windows, Linux and MacOS. It also supports first and third-party plugins.

Threats Protected: 02
Rule Set Type:

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

Class Type: Trojan-activity

Kill Chain:

Tactic	Technique ID	Technique Name
Command-and-Control	T1573	Encrypted Channel
	T1071	Application Layer Protocol
	T1573	Encrypted Channel
	T1572	Port Tunnelling
	T1090	Proxy
	T1219	Remote Access Tools

Known exploited vulnerabilities (Week 3 June 2025)

Vulnerability	CVSS	Description
CVE-2023-0386	7.8 (High)	Linux Kernel contains a privilege escalation vulnerability within the OverlayFS subsystem that can allow a locally authenticated attacker to escalate privileges on the system.
CVE-2023-33538	8.8 (High)	Multiple TP-Link routers contain a vulnerability within the web management interface that can allow remote authenticated attackers to execute OS commands on the system via a specially crafted HTTP request. This vulnerability affects TP-Link TL-WR940N V2/V4, TL-WR841N V8/V10, TL-WR740N V1/V2 devices, and as these are end-of-life it's recommended to replace these products as they may no longer receive security fixes to address the issue.
CVE-2025-43200	4.8 (Medium)	Multiple Apple devices contain an unspecified vulnerability that occurs when processing a specially crafted photo or video when shared via an iCloud link.

For more information, please visit the **Red Piranha Forum**:
https://forum.redpiranha.net/t/known-exploited-vulnerabilities-catalog-4th-week-of-june-2025/570

Updated Malware Signatures (Week 3 June 2025)

Threat	Description
zgRAT	A Remote Access Trojan (RAT) used in cyberattacks that provides attackers 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 Worldwide

DragonForce leads this week's ransomware activity with 15.18% of total reported attacks, signalling a sharp surge and possibly indicating either the start of a new campaign or aggressive targeting of vulnerable sectors.

SafePay follows closely at 14.29%, continuing its steady climb across recent weeks and reaffirming its position as a high-volume actor, likely due to either effective affiliate expansion or targeting under-defended enterprise environments.

Qilin maintains a strong presence with 13.39%, remaining one of the most persistent threats with an international footprint and consistent hit rate, often leveraging advanced tactics and wide-reaching infrastructure.

Akira, Play, and Handala each contributed 7.14%, marking them as active mid-tier operators this week. Their operations typically combine encryption with exfiltration, putting additional pressure on victims through double extortion.

Inc Ransom accounted for 8.04%, continuing to be a disruptive force in ransomware circles with strategic data leak threats and targeted campaigns.

Groups like WorldLeaks, Sarcoma, Medusa, and J Group each logged 2.68%, indicating steady, lower-volume campaigns likely targeting smaller enterprises or less-defended verticals.

A wide cluster of groups, including Killsec3, Rhysida, Lynx, Nova, Kairos, Direwolf (all at 1.79%), and Interlock, IMN Crew, Stormous, Space Bears, Anubis, and NightSpire (all at 0.89%), represent the fragmented tail of the ransomware ecosystem. These actors often execute niche or opportunistic attacks, yet their presence contributes to the overall complexity and unpredictability of the ransomware threat landscape.

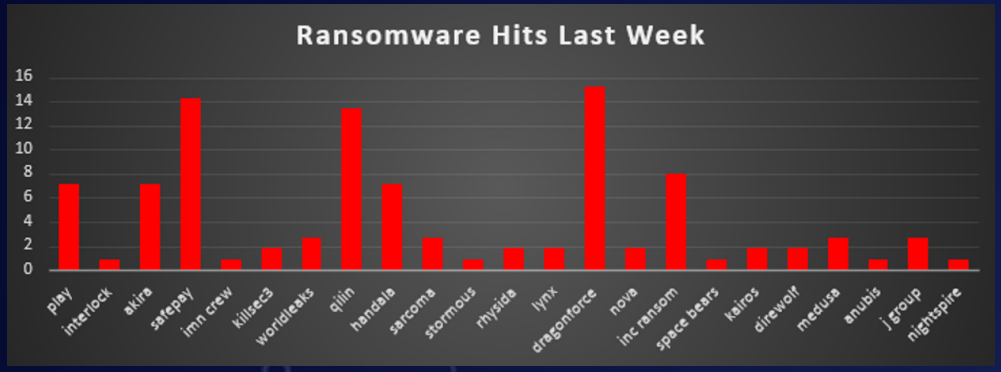

Figure 1: Ransomware Group Hits Last Week

Handala Ransomware

Description
Between 14 and 20 June 2025, the politically motivated Handala group deployed a hybrid ransomware-and-wiper toolkit in targeted "digital solidarity" attacks against Israeli infrastructure. Their malware operates in two phases:

1. Wiper Phase: Immediately upon execution, the malware overwrites critical files with random data in small chunks—rendering them irrecoverable by conventional recovery tools. It also corrupts MBR/partition tables on key hosts to maximise disruption.
2. Ransomware Phase: After the wiper routines are complete, any remaining files are encrypted with AES-256. Each victim is assigned a unique decryption key that Handala holds hostage. Victims see a desktop ransom note (READ_ME.txt) with:
    - A unique victim ID
    - Payment instructions (usually in cryptocurrency)
    - Links to both clearnet and Tor sites where stolen data is or will be publicly leaked

By combining destructive wiping with strong encryption, Handala ensures that even if victims restore from backups, any files not recovered prior to wiping remain permanently lost. This dual approach amplifies operational downtime, pressures victims to pay, and fuels public embarrassment through data leaks.

Detailed TTPs

Spear-phishing Delivery (T1566.001)
Targeted emails impersonate IT/security teams, urging recipients to install a "critical security update." An attached installer, when executed, initiates the attack without visible UI.

Stage-1 Loader Execution (T1059.005)
The installer drops an AutoIt-based loader that waits (30–90 s) to evade sandboxes, then quietly gathers system details (hostname, user, OS version).

Reconnaissance & Profiling (T1590, T1016)
The loader fetches the victim's public IP and local network configuration, building a profile for tailored follow-on actions.

Configuration & C2 Setup (T1071.001)
A small config file from a clearnet portal provides:
- A Telegram Bot API endpoint for exfiltration
- A Tor hidden-service URL for payload download

Data Exfiltration over Telegram (T1041)
System profile and sample files are sent to the attacker's Telegram channel, bypassing conventional defences.

Payload Download via Tor (T1071.001)
The loader retrieves the full wiper/encryptor payload from a .onion address, safeguarding hosting resilience and attacker anonymity.

In-Memory Deployment & Defence Evasion (T1218, T1140)
Using a trusted utility (e.g., certutil), the loader decodes and injects the payload into a legitimate process (such as svchost.exe), leaving minimal disk artefacts.

Disk Wipe & File Encryption (T1561, T1486)
- Wiper: Overwrites files in small random-data chunks, rendering them irrecoverable.
- Encryptor: Applies AES-256 encryption to remaining files, denying access and setting up for extortion.

Persistence via Scheduled Task (T1547.001)
A recurring task (every 15 minutes) ensures the loader re-launches automatically, surviving reboots or partial cleanup.

Ransom Note Deployment (T1486)
A "READ_ME.txt" note on the desktop contains a unique ID, payment instructions, and links to both clearnet and Tor leak sites hosting stolen data.

Detailed TTPs

Tactic	Technique (sub-technique)	ID
Initial Access	Spearphishing Attachment	T1566.001
	Exploit Public-Facing App	T1190
Execution	AutoIt Scripting	T1059.005
	Data Manipulation (file overwrite)	T1565.001
Persistence	Scheduled Task	T1547.001
Defence Evasion	Signed-Binary Proxy Execution (certutil, etc.)	T1218
	Deobfuscate/Decode Files	T1140
Credential Access	Credentials from Config Files	T1555
Discovery	System Network Configuration Discovery	T1016
Collection	Archive Collected Data (7-Zip)	T1560.001
Command-and-Control	Application Layer Protocol (Telegram, Tor)	T1071.001
Exfiltration	Exfiltration Over C2 (Telegram API)	T1041
Impact	Data Encryption	T1486
	Disk Wipe	T1561

Indicators of Compromise (IOCs)

• Clearnet Leak Portals:

- handala-hack.to
- handala.cx
- handala.to

IP:

- 67.195.228.56

• Tor Hidden Service:

- vmjfieomxhnfjba57sd6jjws2ogvowjgxhhfglsikqvvrnrajbmpxqqd.onion

• Telegram Channels & Bots:

- t.me/Handala_Backup
- Bot endpoints embedded in loader config

• Alternative Channels:

- Tox ID: 02C75E60211314F4A69C323A3CE334D75C72CD8C742F3ED168447405C541DF057294365D6C1E
- Twitter: twitter.com/Handala_Hack
- https://t.me/Handala_hack
- https://t.me/Handala_Channel
- BreachForums: breachforums.cx/User-Handala

Sample Hashes:

- 6f79c0e0e1aab63c3aba0b781e0e46c95b5798b2d4f7b6ecac474b5c40b840ad
- 96dec6e07229201a02f538310815c695cf6147c548ff1c6a0def2fe38f3dcbc8
- Fe07dca68f288a4f6d7cbd34d79bb70bc309635876298d4fde33c25277e30bd2

Mitigation & Recommendations

- Deploy advanced email sandboxing; simulate spear-phishing exercises regularly.
- Rapidly remediate VPN and web-application vulnerabilities; enforce MFA on remote access.
- Monitor for scheduled task creation, unusual use of certutil/AutoIt, and in-memory injection behaviours.
- Alert on TOR and Telegram API traffic; block known leak-site domains and onion-to proxies.
- Implement a 3-2-1 strategy with immutable, offline snapshots to withstand wiper activity.
- Isolate critical assets; limit lateral movement protocols (e.g., SMB, RDP).
- Leverage CE 5.0 integrated threat intelligence feeds, automated IOC ingestion, and real-time wiper/ransomware detection to rapidly identify and contain Handala-style attacks.

By incorporating CE 5.0 alongside best practices for phishing defence, patching, EDR, network monitoring, backups, and segmentation, you'll significantly enhance both your detection capabilities and your resilience against dual wiper-ransomware threats like Handala.

Worldwide Ransomware Victim

The United States continues to dominate global ransomware victim reports, accounting for 56.25% of all incidents this week. This substantial share highlights its persistent attractiveness to threat actors due to its vast digital infrastructure, high-value targets, and interconnected enterprise systems.

Australia comes in second with 8.04%, reflecting a notable spike in targeted attacks within the Asia-Pacific region. This could indicate focused campaigns on Australian businesses or public-sector institutions.

Both Canada and the United Kingdom reported 7.14% of total ransomware attacks, maintaining their positions as frequent targets—likely due to mature economies, reliance on cloud services, and strong financial and healthcare infrastructures.

Germany followed with 4.46%, confirming Western Europe's continued exposure to high-impact ransomware campaigns.

Countries such as Israel, Thailand, Brazil, Italy, and France each recorded 1.79%, representing strategic interest in regions hosting critical data or infrastructure.

A broad group of nations—including South Africa, Colombia, Turkey, Belgium, Norway, Tanzania, Taiwan, and India—each reported 0.89% of incidents. These figures reflect the truly global reach of ransomware, where even lower-profile or geographically dispersed countries are not spared.

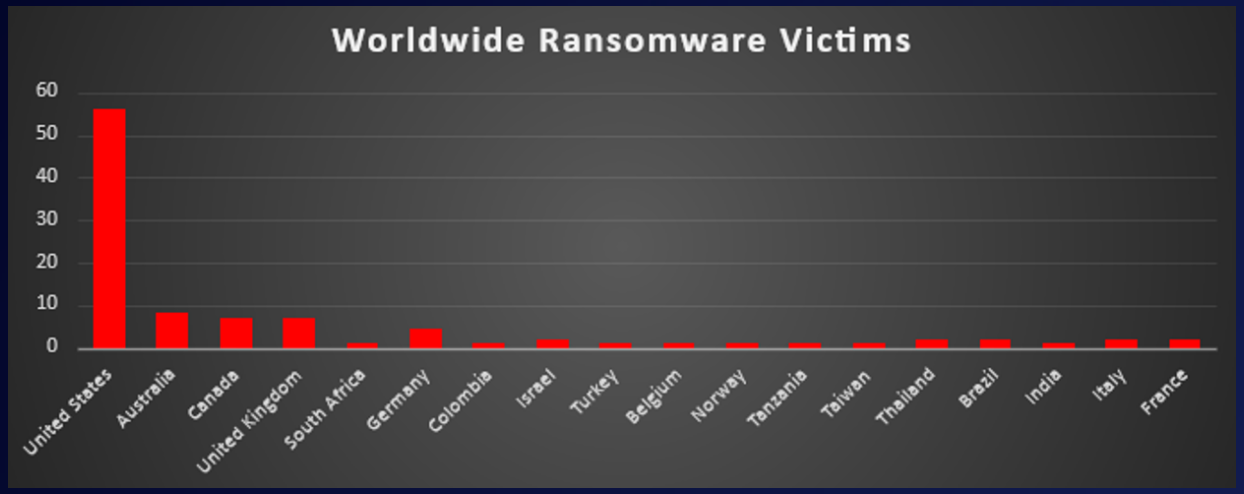

Figure 4: Ransomware Victims Worldwide

Industry-wide Ransomware Victims

Manufacturing remains the most heavily targeted industry this week, accounting for 14.29% of all reported ransomware incidents. Its complex infrastructure, operational dependencies, and often outdated systems make it a prime target for threat actors seeking to disrupt supply chains.

Business Services follows closely with 13.39%, as attackers continue to focus on consultancy, legal support, and third-party vendors that often serve as stepping stones into larger enterprise networks.

Construction and Hospitality sectors recorded 11.61% and 10.71%, respectively highlighting a surge in targeting of operational sectors with fragmented digital defences and high-value operational data.

Retail stands at 7.14%, likely driven by customer data-rich environments and seasonal transaction peaks that heighten extortion pressure.
A mid-tier cluster—Transportation, Education, Finance, Federal, and IT—each reported 4.46% of incidents. These sectors are routinely targeted due to their sensitive data, public dependencies, and reliance on always-available systems.

Insurance, Consumer Services, and Real Estate each accounted for 3.57%, showing consistent interest in sectors where financial data, contracts, and customer records are central.

Lower-volume attacks were reported in Electricity, Telecommunications, and Organisations (1.79% each), pointing to opportunistic targeting or sector-specific campaigns.

Smaller industry verticals—including Agriculture, Law Firms, Media & Internet, and Energy—each registered 0.89%, reminding us that no industry is immune, even if not a primary focus of widespread campaigns.

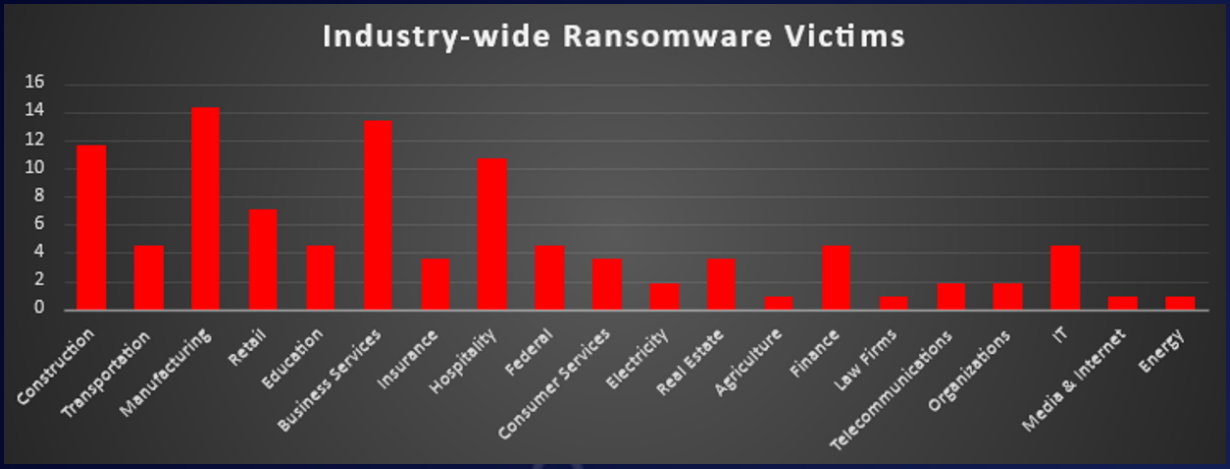

Figure 5: Industry-wide Ransomware Victims