Red Piranha
unified threat management

THREAT INTELLIGENCE REPORT

June 24 - 30, 2025

Report Summary:

- **New Threat Detection Added**
  - TransferLoader
  - KimJongRAT
- **Detection Summary**
  - **Threat Protections integrated into the Crystal Eye - 90**

The following threats were added to Crystal Eye this week:

1. TransferLoader

TransferLoader is a malware loader that has been active since at least February 2025 and consists of several components including a downloader, backdoor, and a loader and has been used to deploy the Morpheus ransomware as observed by ThreatLabz. TransferLoader includes several capabilities to remain undetected such as anti-debug, encryption and obfuscation, with utilising HTTP and IPFS for communication between the backdoor component and C2 server.

Threats Protected: 10
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	T1566.001	Spearphishing Attachment
Defence Evasion	T1622	Debugger Evasion
	T1497	Virtualisation/Sandbox Evasion
	T1027	Obfuscated Files or Information
	T1140	Deobfuscate/Decode Files or Information
Command-and-Control	T1071	Application Layer Protocols
	T1001	Data Obfuscation
	T1573	Encrypted Channel

2. KimJongRAT

KimJongRAT is classified as Remote Access Trojan, this family of malware has been around as early as 2013 and utilises a LNK file to facilitate downloading components such as the information stealer as well as a keylogger which are used in the malware. Apart from the information stealer capabilities, KimJongRAT does also include the functionality to execute commands on the infected system. As with most information stealers, sensitive information such as passwords, crypto wallets, and other web browser or system information is collected and sent to the remote C2 server, with commands and files encrypted via RC4 before transmission.

Threats Protected: 2
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
Execution	T1059.001	Command and Scripting Interpreter – PowerShell
	T1204.002	User Execution – Malicious File
Credential Access	T1555.003	Credentials from Password Stores – Credentials from Web Browsers
	T1056.001	Input Capture – Keylogging
Command-and-Control	T1071.001	Application Layer Protocol – Web Protocols
	T1573.001	Encrypted Channel – Symmetric Cryptography
Exfiltration	T1041	Exfiltration Over C2 Channel

Known exploited vulnerabilities (Week 4 June 2025)

Vulnerability	CVSS	Description
CVE-2019-6693	6.5 (Medium)	Fortinet FortiOS contains hard-coded credentials that are stored within the FortiOS configuration backup file. This can allow an attacker with access to the backup file to obtain sensitive data including user passwords, private key passwords, and high availability passwords. This may be valuable to an attacker when carrying out additional attacks.
CVE-2024-0769	9.8 (Critical)	D-Link DIR-859 routers contain a path traversal vulnerability that can allow an unauthenticated remote attacker to access sensitive files via a HTTP request that can result in the attacker gaining unauthorised access on the device. The D-Link DIR-859 is designated as End-of-life (EOL) so it's recommended to replace this device as it may no longer receive any security updates.
CVE-2024-54085	10.0 (Critical)	AMI MegaRAC SPx contains an authentication bypass vulnerability within the BMC component that can allow an attacker to gain access to the device via the Redfish Host Interface.

For more information, please visit the **Red Piranha Forum**:
https://forum.redpiranha.net/t/known-exploited-vulnerabilities-catalog-5th-week-of-june-2025/572

Updated Malware Signatures (Week 4 June 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

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

Qilin continues to dominate the ransomware landscape with 19.09% of total reported attacks this week. Its persistent high activity underscores its strong affiliate base and the effectiveness of its multi-phase operations.

Akira and Play each recorded 10.91%, confirming their positions as major players. These groups are known for their double extortion tactics, targeting both infrastructure-heavy sectors and professional service providers.

Handala maintains a significant share at 9.09%, suggesting ongoing focused campaigns, possibly targeting specific regions or verticals.

Lynx and DragonForce follow at 7.27% each, marking them as high-mid tier actors with growing visibility and impact.

Everest, Inc Ransom, and Kawa each accounted for 4.55%, continuing to remain active across a range of enterprise targets.

Groups like Interlock, WorldLeaks, and SafePay (each at 2.73%) maintain a steady presence, often engaging in opportunistic or smaller-scale campaigns.

Kairos and El Dorado reported 1.82%, while a wide range of smaller groups—Space Bears, NightSpire, Silent, TeamXXX, J Group, MetaEncryptor, Sarcoma, Stormous, Team Underground, Clop, and Cloak—each logged 0.91%. These actors, while individually low in volume, collectively represent the long tail of ransomware threats, contributing to the broader risk landscape through targeted or sporadic operations.

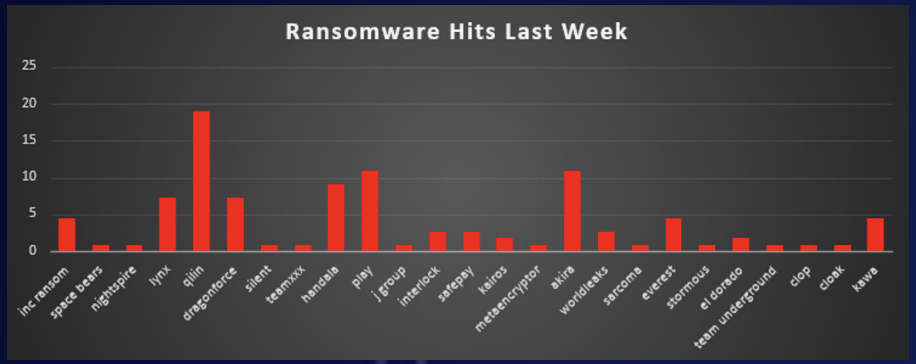


Figure 1: Ransomware Group Hits Last Week

Kawa4096 Ransomware

Kawa4096 (a.k.a. KaWaLocker) is a newly emerged ransomware group first observed publicly on June 27, 2025, when it launched its leak site on the dark web. The group employs double extortion tactics, encrypting victim files and threatening to publish stolen data unless a ransom is paid. Their operational style mirrors that of the Akira ransomware gang, especially in the design of their Tor-based leak portal, which features a retro terminal interface.

During the week of June 21 to June 27, Kawa4096 claimed responsibility for at least four confirmed breaches affecting organisations in the U.S. and Germany. While one breach occurred slightly earlier (June 20), it was disclosed within the week and is included in this analysis.

- No use of traditional clearnet infrastructure
- Communication solely over Tor, Tox, and OnionMail
- Initial access presumed via phishing and unauthorised RDP
- Strong focus on stealth, with ransomware binaries operating offline

Detailed TTPs
Initial Access – Spearphishing (T1566.001)
Victims received targeted phishing emails containing a malicious installer (shield.msi) or infected Office documents.

User Execution (T1204.002)
The user executed the payload (e.g., ran shield.msi), triggering the ransomware's entry point—reported by the same threat platforms.

Process Injection (T1055)
Kawa4096 spawned a helper process and injected malicious code into elevated system processes such as svchost.exe, maintaining stealth.

Persistence via Service/Task (T1543.003)
The malware created a Windows service or scheduled task to persist across reboots.

Privilege Escalation & Defence Evasion
Techniques used include:

- Process injection (again, T1055)
- Disabling AV or security tools (T1562.001)
- Deleting Volume Shadow Copies (T1490)
- Clearing Event Logs (T1070.001)

Ransomware Execution (Encryption + Optional Wiping)
Kawa4096 encrypted files using ChaCha20 with RSA key exchange (T1486) and optionally wiped file segments (T1561).

Ransom Note Deployment & Extortion Set-Up (T1486 Impact)
The malware dropped !!RestoreMyfileKavva.txt containing instructions and links to Tor leak site and Tox chat, guiding victims on how to contact attackers.

Detailed TTPs

Tactic	Technique (sub-technique)	TTP ID	Description
Initial Access	Phishing with Attachment	T1566.001	Malicious documents or executable loaders delivered via email
Execution	Command and Scripting Interpreter (PowerShell)	T1059.001	Execution of PowerShell payloads post-phishing
Persistence	Scheduled Task/Job	T1053.005	Used to maintain persistence post-compromise
Defence Evasion	Signed Binary Proxy Execution (e.g., mshta.exe)	T1218	Living off the land (LOLBins) to avoid detection
Credential Access	OS Credential Dumping	T1003	Attempted extraction of local administrator or cached credentials
Discovery	System Information Discovery	T1082	Local host discovery and drive enumeration
Exfiltration	Exfiltration Over C2 Channel (Tor)	T1041	Stolen data uploaded via anonymized channel (Tor hidden service)
Impact	Data Encrypted for Impact	T1486	Local files and mapped drives encrypted with AES-256 + RSA-4096
Impact	Data Destruction (Disk Wipe, Optional)	T1561	Some variants overwrite data prior to encryption (rare)

Indicators of Compromise (IOCs)
Domains and Onion Services:

Tor Leak Site

kawasa2qo7345dt7ogxmx7qmn6z2hnwaoi3h5aeosupozkddqwp6lqqd.onion
kawasax2ygoxytxtfjcy3a57vdyopj4k4c3m6rj5zht7io3t7g4wl3ad.onion

Delivery Filename: shield.msi
Ransom Note: !!Restore-My-file-Kavva.txt, referencing the Tor site and Tox

Contact Info:

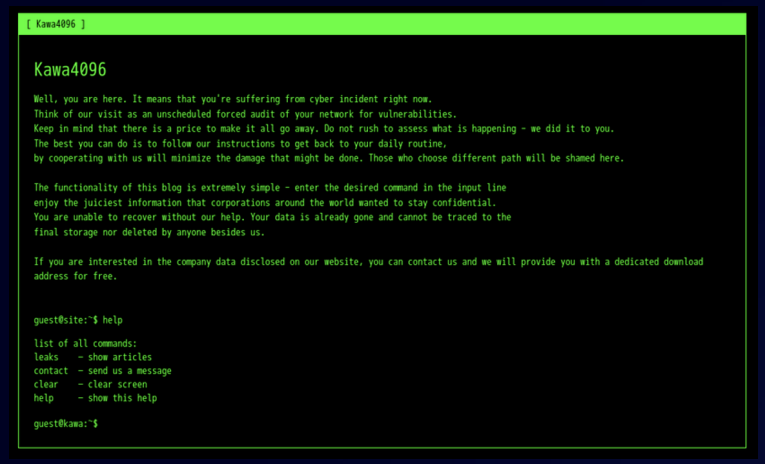
- Tox ID: 6A340207246B47E37F6D094D2236E5C6242B6E4461EEF8021FED2C9855240C3E11AEE886FAAF
- Email: kawa4096@onionmail.org

SHA256 hash: f3a6d4ccdd0f663269c3909e74d6847608b8632fb2814b0436a4532b8281e617

SHA3-384 hash:
cafd8e135dd873baa29218f17b55b44a83a1444afc380f94bfa5598a6ea00f0f60609658174ef40db963951cb8b1f2da

SHA1 hash: bd30c87774c083a1003c0b9fb0a922b702302272

MD5 hash: c3ce46d40b2893e30bf00fce72c2e1fa



Mitigation & Defensive Controls (with CE 5.0)

1. Email Gateway Hardening & User Awareness
   - Block .msi files and macro-enabled documents at the email gateway.
   - Educate users through phishing simulations and awareness campaigns.

2. Endpoint Behavioural Monitoring
   - Detect and alert on:
     - Malicious PowerShell or script activity
     - Process injection into system services like svchost.exe
     - Shadow copy deletion commands
     - Clearing of Windows event logs
   - Crystal Eye CE 5.0 uses host-based behaviour analytics and system call monitoring to identify these patterns in real-time.

3. Network Anomaly Detection & C2 Blocking
   - Block outbound traffic to anonymising networks like Tor and encrypted .onion domains.
   - CE 5.0's Network Detection & Response engine alerts on such traffic and can automatically block these channels.

4. Privilege Management & Persistence Prevention
   - Apply least-privilege principles to endpoints and servers.
   - Enforce MFA for remote access and admin accounts.
   - CE 5.0 monitors for unauthorised Windows service and scheduled task creation attempts (T1543.003).

5. Backup Strategy & Network Segmentation
   - Implement immutable, offline backups using the 3-2-1 rule.
   - Segment network zones to isolate critical systems.
   - CE 5.0 includes visibility into lateral movement attempts and ransomware propagation attempts.

6. Incident Response Integration
   - Ingest CE 5.0 alerts into SIEM/XDR solutions to automate containment and investigation workflows.
   - CE 5.0 enriches its detections with contextual indicators and mapped MITRE TTPs.

7. Threat Intelligence & Signature Updates
   - Crystal Eye CE 5.0 receives regular threat intelligence feeds and IDS/IPS signature updates to respond to new TTPs used by ransomware families like Kawa4096.

Worldwide Ransomware Victim

The United States continues to bear the brunt of global ransomware activity, accounting for an overwhelming 64.55% of all reported victims this week. This dominance reflects its vast digital infrastructure, high-value enterprise targets, and ongoing appeal to both ransomware-as-a-service (RaaS) operators and independent threat groups.

Israel and Canada each recorded 5.45%, marking them as high-interest targets—likely due to their advanced tech sectors, global business presence, and significant data holdings.

Germany followed with 3.64%, maintaining its status as a frequently targeted nation within Western Europe. The United Kingdom and Australia each saw 2.73%, indicating steady targeting of these well-connected economies.

Countries such as India, Spain, and Thailand each accounted for 1.82%, highlighting the global nature of ransomware operations and the increasing focus on Asia-Pacific and South Asia.

Meanwhile, a long list of nations—Turkey, Belgium, Argentina, Peru, Brazil, Serbia, Taiwan, Fiji, New Zealand, Sri Lanka, and United Arab Emirates—each reported 0.91% of total incidents. These figures emphasise that ransomware campaigns are far-reaching and increasingly opportunistic, impacting both major economies and smaller, less frequently targeted countries alike.

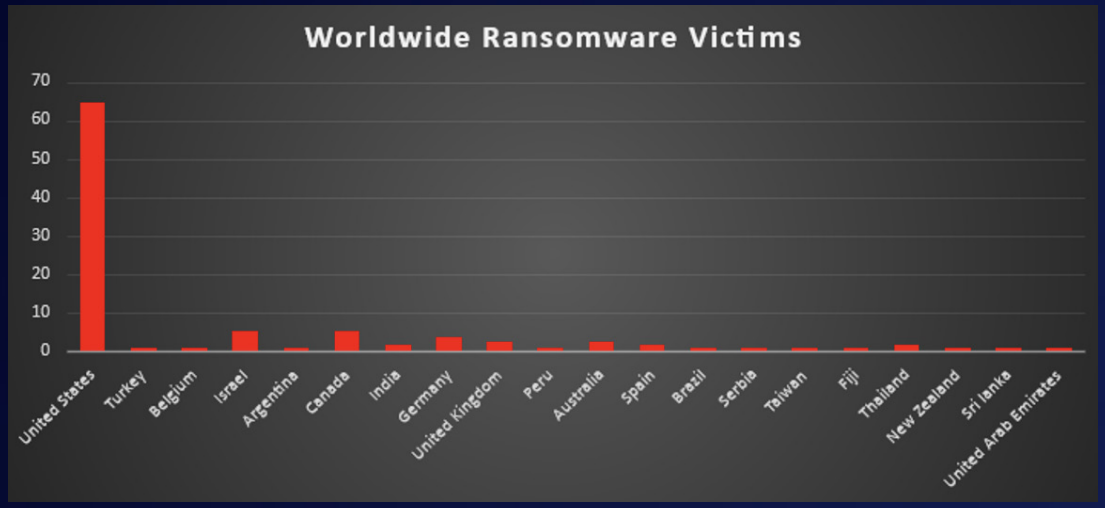


Figure 4: Ransomware Victims Worldwide

Industry-wide Ransomware Victims

Retail tops the list this week with 17.27% of all reported ransomware incidents. Its vast consumer data distributed digital environments, and reliance on uptime make it a high-value target, especially for extortion-based campaigns.

Business Services follows at 14.55%, continuing to be heavily exploited due to their access to multiple clients, sensitive data, and central roles in supply chains. Manufacturing remains a major victim, accounting for 12.73% of incidents. The sector's dependency on industrial control systems and minimal downtime tolerance makes it attractive to attackers aiming for maximum disruption.

Hospitality ranks fourth with 10%, driven by high volumes of customer data and online booking/payment platforms. Construction and Law Firms share 7.27% each, showing increased focus on sectors with valuable intellectual property and project-based financial flows.

Finance sits at 5.45%, maintaining its usual spot as a consistent target due to the nature of assets and regulatory pressure. Transportation comes in at 4.55%, likely linked to logistics operations, supply chain dependencies, and OT/IT convergence vulnerabilities.

Sectors like Education and Real Estate each report 3.64%, reflecting adversary interest in soft targets and data-rich environments.
Other impacted sectors include:

- Consumer Services and Organisations at 2.73%
- Healthcare, Federal, and Telecommunications at 1.82%
- IT, Insurance, and Electricity at 0.91%

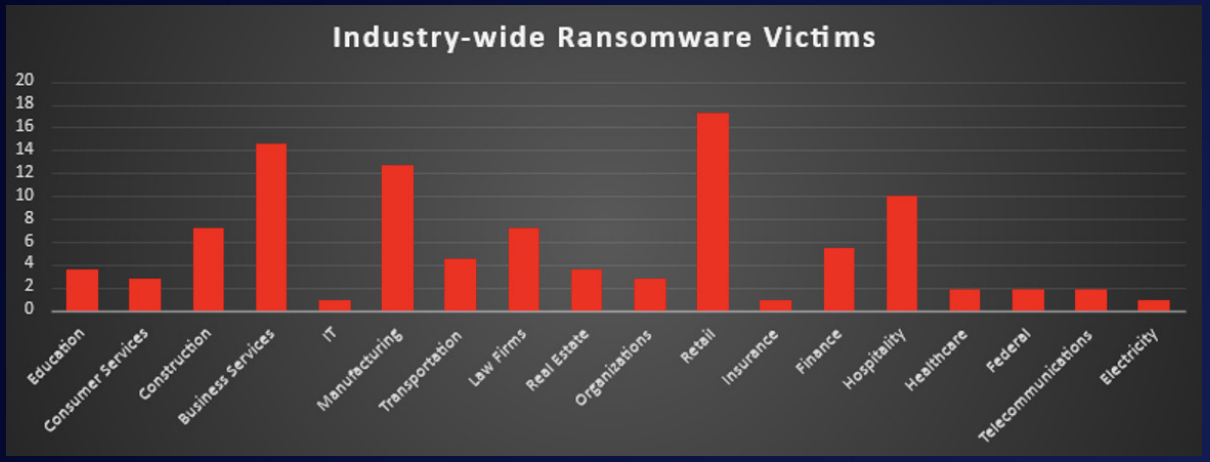


Figure 5: Industry-wide Ransomware Victims