Red Piranha
unified threat management

THREAT INTELLIGENCE REPORT

May 06 - 12, 2025

Report Summary:

- **New Threat Detection Added** – 2
  - ZPHP
  - Interlock Ransomware
- **New Threat Protections - 135**

The following threats were added to Crystal Eye this week:

1. ZPHP

ZPHP is a malware that is distributed through malicious websites or compromised websites in the form of JavaScript. When visiting one of these sites it makes it appear as if the user requires a browser update. This attempts to trick the user into downloading a malicious payload that while disguised as a Browser Update.

Threat Protected: 08
Rule Set Type:

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

Class Type: Exploit-kit

MITRE ATT&CK:

Tactic	Technique ID	Technique Name
Initial Access	T1189	Drive-by Compromise

2. Interlock Ransomware

Interlock Ransomware deploys a multi-stage attack chain to deliver its malicious payload to networks and users. They start by compromising public-facing websites and presenting the user with a fake browser update (This is very similar to ZPHP). By masquerading as a browser update, they trick the user by copying a malicious PowerShell script and pasting it into their terminal. This executes multiple tools such as pyinstaller. This ultimately leads to the user's device having ransomware installed.

Threat Protected: 01
Rule Set Type:

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

Class Type: Trojan-activity

MITRE ATT&CK:

Tactic	Technique ID	Technique Name
Initial Access	T1189 T1190	Drive-by Compromise Exploit Public-Facing Application
Execution	T1059.001	Command and Scripting Interpreter: PowerShell
Impact	T1486	Data Encrypted for Impact

Known exploited vulnerabilities (Week 2 - May 2025)

Vulnerability	CVSS	Description
CVE-2024-6047 CVE-2024-11120	9.8 (Critical)	Certain end-of-life GeoVision devices contain a vulnerability that can allow an unauthenticated remote attacker to execute operating system commands. These devices are no longer being maintained and receiving security updates, it is recommended to replace the affected products.
CVE-2025-27363	CVSS 8.1 (High)	FreeType contains a vulnerability within the subglyph parsing functionality relating to TrueType GX and variable font files, this vulnerability can result in an arbitrary write which can allow for code execution on the affected device or software that utilises this component
CVE-2025-3248	CVSS 9.8 (Critical)	Langflow contains a vulnerability that can allow an unauthenticated remote attacker to execute arbitrary code via an HTTP request that can result in remote code execution on the affected servers. This vulnerability is a result of an API endpoint that was missing authentication and affects versions prior to 1.3.0.

For more information, please visit the **Red Piranha Forum**:
https://forum.redpiranha.net/t/known-exploited-vulnerabilities-catalog-2nd-week-of-may-2025/563

Updated Malware Signatures (Week 2 - May 2025)

Threat	Description
Lumma Stealer	A type of malware classified as an information stealer. Its primary purpose is to steal sensitive information from infected systems, including but not limited to credentials, financial information, browser data, and potentially other personal or confidential information.
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

Play once again leads the ransomware landscape, responsible for 19.28% of total attacks last week. Known for its swift, high-impact operations—particularly against MSPs and hybrid environments—Play continues to operate with precision and volume.

Akira follows with 14.46%, maintaining its aggressive campaign across professional services and infrastructure-heavy targets. Qilin accounts for 9.64%, showing growing sophistication and a broader international victim base.

IMN Crew makes a strong appearance at 8.43%, suggesting rapid operational scaling, while Brain Cipher registers 7.23%, consistent with its methodical targeting patterns.

A cluster of mid-level operators—Rhysida, LockBit3, Everest, and Devman (each at 3.61%)—continue to target ESXi and enterprise Windows environments with a blend of persistence and precision.

Smaller but more persistent actors such as Sarcoma (4.82%), RansomHouse, Hunters, Lynx, and Interlock (each at 2.41%) reflect the long-tail activity that keeps defenders under pressure across industries.

Meanwhile, lesser-known but active threats like Monti, Gunra, Silent, Cloak, Killsec3, Termite, Orca, and Bert—each contributing 1.2%—demonstrate how the ransomware ecosystem remains noisy, crowded, and opportunistic.

Interestingly, Nova, previously seen climbing the charts, fell to 1.2%, hinting at a temporary pause or tactical regrouping.

This distribution reaffirms the dominance of a few high-volume actors while highlighting the steady drumbeat of activity from emerging and niche groups. The ransomware threat remains dynamic and distributed, demanding continuous visibility, threat intelligence integration, and resilience planning.

Ransomware Groups	Overall Percentage of total attack coverage
Monti	2.41%
Brain Cipher	7.23%
Rhysida	3.61%
Bert	1.2%
Interlock	2.41%
Silent	1.2%
Sarcoma	4.82%
Gunra	1.2%
Lynx	2.41%
Devman	3.61%
RansomHouse	2.41%
Play	19.28%
Hunters	2.41%
LockBit3.0	3.61%
Everest	3.61%
IMN crew	8.43%
Qilin	9.64%
Cloak	1.2%
KillSec3	1.2%
Termite	1.2%
Orca	1.2%
Akira	14.46%
Nova	1.2%

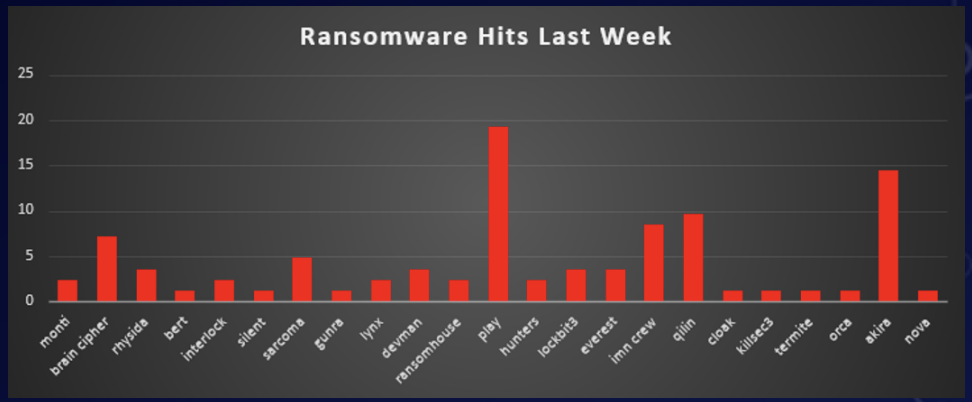


Figure 1: Ransomware Group Hits Last Week

Gunra Ransomware Group

Gunra is a newly emergent ransomware family identified in April 2025. Based on leaked Conti source code, it represents a new wave of double-extortion ransomware that combines encryption with sensitive data theft. Victims are pressured into negotiations through a bespoke Tor-based portal and warned that exfiltrated data will be published if no contact is made within 5 days.

Gunra has already hit organisations in Japan, Egypt, Italy, Argentina, and Panama, and early indicators show targeting across healthcare, pharmaceuticals, manufacturing, and real estate. The ransomware adds the ".ENCRT" extension to encrypted files and drops a ransom note titled "R3ADM3.txt" into each affected directory. The note provides instructions for contacting the operators- who refer to themselves as the "Manager"- via a private chat hosted on the Tor network.

Gunra uses advanced evasion techniques including process injection, sandbox detection via IsDebuggerPresent, and Windows Management Instrumentation (WMI) commands to destroy backups and limit recovery. Its binary is heavily obfuscated, minimising detection. While no worm capabilities have been confirmed, the ransomware's precision suggests a manual affiliate model targeting high-value entities.

Detailed TTPs
Gunra operators likely initiate attacks through spear-phishing emails containing malicious attachments or links. This method allows attackers to bypass perimeter defences and gain an initial foothold without relying on exploits. Given Gunra's Conti-based lineage, phishing is the preferred method due to its simplicity and high success rate in targeting human vulnerabilities.

Once inside the target environment, Gunra executes its payload using Windows Management Instrumentation (WMI) and native Windows API calls. This dual-layer execution helps evade detection by masquerading as legitimate system behaviour. The use of WMI for shadow copy deletion ensures critical backups are destroyed before encryption begins, while API calls like FindNextFileExW and TerminateProcess facilitate recursive file targeting and neutralisation of defensive processes.

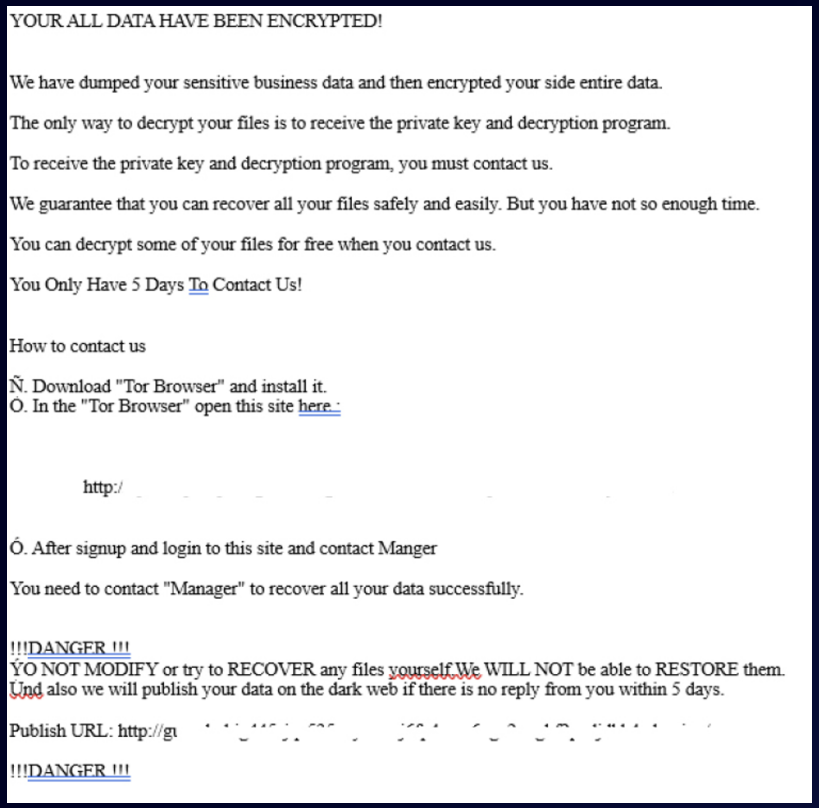
To maintain access and potentially spread within the environment, Gunra leverages process injection- executing malicious code within legitimate processes to remain undetected. The malware's potential bootkit-level persistence implies deep system embedding, possibly modifying system startup behaviour to reload after reboots. Although no worm behaviour has been confirmed, its structure may support manual lateral movement by operators.

To maximise impact, Gunra escalates privileges by interacting with process tokens using APIs like GetCurrentProcess and OpenProcess. These allow it to impersonate or hijack higher-privileged sessions, facilitating access to sensitive files, deletion of backups, and disabling security features- all critical for successful system-wide encryption.

Gunra employs anti-analysis strategies to avoid detection in sandbox and forensic environments. It uses functions such as IsDebuggerPresent to identify virtual or debugged execution contexts and may alter behaviour or terminate execution when analysis is detected. Furthermore, the binary is heavily packed and obfuscated, thwarting static analysis by antivirus engines and increasing time-to-detection.

In line with double-extortion practices, Gunra stages data locally and exfiltrates it via encrypted communication channels. By transferring sensitive data before encryption, the attackers gain leverage to extort victims not just through file encryption but also by threatening public exposure on their Tor-based leak site.

Gunra forgoes traditional C2 infrastructure in favour of anonymous, encrypted communication through Tor hidden services. Victims are instructed to visit .onion addresses to negotiate with the attackers, often identified as "Manager." This decentralisation complicates attribution and takedown efforts by defenders and law enforcement.



YOUR ALL DATA HAVE BEEN ENCRYPTED!

We have dumped your sensitive business data and then encrypted your side entire data.

The only way to decrypt your files is to receive the private key and decryption program.

To receive the private key and decryption program, you must contact us.

We guarantee that you can recover all your files safely and easily. But you have not so enough time.

You can decrypt some of your files for free when you contact us.

You Only Have 5 Days To Contact Us!

How to contact us

Ñ. Download "Tor Browser" and install it.
Ó. In the "Tor Browser" open this site here.:

http:/

Ó. After signup and login to this site and contact Manger

You need to contact "Manager" to recover all your data successfully.

!!!DANGER !!!
ÝO NOT MODIFY or try to RECOVER any files yourself.We WILL NOT be able to RESTORE them.
Und also we will publish your data on the dark web if there is no reply from you within 5 days.

Publish URL: http://g

!!!DANGER !!!

TTP Chart

Tactic (ID)	Technique	Technique ID	Description
Initial Access	Phishing	T1566.001	Delivery via malicious email content.
Execution	Native API Execution	T1106	Uses Win32 APIs and WMI for file operations.
Persistence	Create/Modify System Process	T1543	May install boot-level persistence.
Priv-Esc	Abuse Elevation Mechanism	T1548	Token impersonation for admin rights.
Defence Evasion	Impair Defences	T1562	AV and backup termination via process kill.
Discovery	System Info Discovery	T1082	Uses system APIs to profile infected host.
Exfiltration	Encrypted Channel (Tor)	T1041	Sends stolen data before encryption.
C2	Onion/Tor Protocol	T1071.001	Negotiation through .onion site.
Impact	Data Encrypted for Impact	T1486	Files encrypted with AES/RSA and .ENCRT extension.
Impact	Inhibit System Recovery	T1490	Deletes VSS and local backups via WMI.

IOCs

Onion URL: apdk7hpbbquomgoxbhutegxco6btrz2ara3x2weqnx65tt45ba3sclyd.onion
Leak Site: gunrabxbig445sjqa535uaymzerj6fp4nwc6ngc2xughf2pedjdhk4ad.onion
File Extension: .ENCRT
Ransom Note: R3ADM3.txt
SHA-256: 854e5f77f788bbbe6e224195e115c749172cd12302afca370d4f9e3d53d005fd
MD5: 9a7c0adedc4c68760e49274700218507
Behavioural IOCs: Surge in file renames, VSS deletions via wmic shadow copy delete

Ransomware Victims Worldwide

The United States continues to dominate the global ransomware victim landscape, accounting for 52.38% of all reported attacks last week. Its concentration of high-value targets, digital dependency, and extensive business infrastructure make it a perennial Favorite for both targeted and opportunistic ransomware campaigns.

Australia ranks second with 9.52%, indicating that attackers are maintaining a strategic focus on the APAC region—particularly where cloud adoption and managed services are widespread.

Canada follows at 5.95%, once again underlining its vulnerability due to tightly connected supply chains and digital dependencies with US organisations.

Other impacted nations include the United Kingdom (3.57%), Spain and Japan (each at 2.38%), demonstrating continued threat activity across Europe and Asia.

A wide range of countries—including India, Portugal, Colombia, Italy, Singapore, Germany, Dominican Republic, Belgium, Croatia, Indonesia, France, Austria, Philippines, Switzerland, Brazil, UAE, Nigeria, and Thailand—each reported 1.19% of total ransomware victims, reflecting the increasingly global reach of threat actors.

This distribution reinforces the notion that no region is immune. Attackers continue to exploit weak points across borders, industries, and organisational sizes. To combat this global threat, security teams must prioritise continuous risk assessment, invest in international threat intelligence collaboration, and enforce resilient data recovery strategies across all geographic locations.

Countries	Worldwide Ransomware Victims
United States	52.38%
India	1.19%
Spain	2.38%
Portugal	1.19%
Canada	5.95%
Colombia	1.19%
United Kingdom	3.57%
Italy	1.19%
Australia	9.52%
Japan	2.38%
Singapore	1.19%
Germany	1.19%
Dominican Republic	1.19%
Canada	1.19%
Belgium	1.19%
Croatia	1.19%
Indonesia	1.19%
France	1.19%
Austria	1.19%
Philippines	1.19%
Switzerland	1.19%
Brazil	1.19%
United Arab Emirates	1.19%
Nigeria	1.19%
Thailand	1.19%

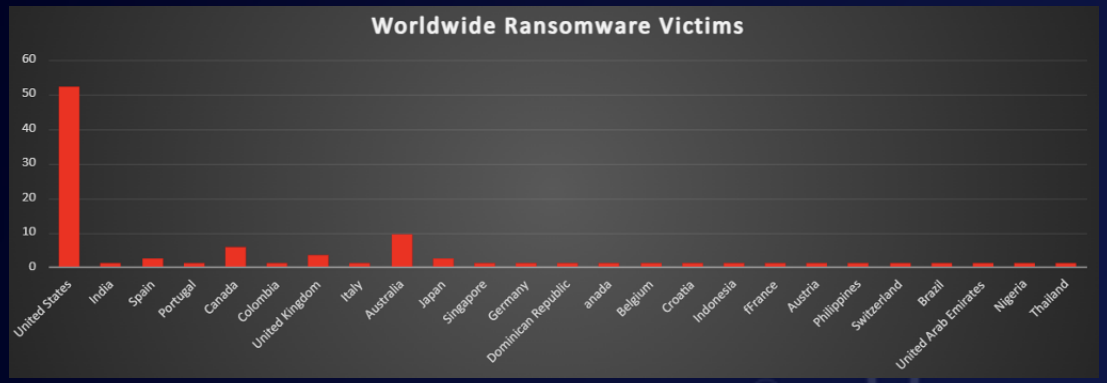


Figure 3: Ransomware Victims Worldwide

Ransomware Victims by Industry

The Manufacturing and Business Services sectors are tied at the top this week, each accounting for 16.87% of all ransomware incidents. Manufacturing remains a perennial target due to its mission-critical operations and traditionally underfunded cybersecurity layers. Meanwhile, Business Services—including consulting, outsourcing, and professional support—face sustained pressure as intermediaries with access to broader client environments.

Construction emerges prominently at 12.05%, a notable uptick suggesting an increased focus on infrastructure and logistics-driven enterprises—many of which may lack dedicated cybersecurity teams.

Law Firms (8.43%) and Retail (7.23%) remain high on attackers' lists. For law firms, the risk of data exposure and legal liability makes them ideal extortion targets. Retail, with its rich stores of customer data and financial workflows, continues to be exploited through both network breaches and third-party access points.
The Insurance sector accounted for 6.02% of attacks—an important reminder that even cybersecurity policy underwriters and risk managers are not immune to threat actor focus.

Lower, but consistent targeting was observed in Transportation (4.82%), Healthcare, Finance, Hospitality, and Consumer Services (each ranging between 3.61% and 4.82%), highlighting how ransomware groups continue to diversify their targeting across critical and public-facing verticals.

A wide tail of sectors—including Education, IT, Federal, Media & Internet, Energy, Real Estate, Agriculture, and Minerals & Mining—each experienced 1.2–2.41% of the total attacks, reflecting the broad and opportunistic nature of current campaigns.

These patterns once again underscore the industry-agnostic nature of ransomware. Regardless of sector, organisations must prioritise patch velocity, access control, and well-isolated backups to mitigate the expanding operational and reputational risks tied to ransomware.

Industries	Industry-wide Ransomware Victims
Transportation	4.82%
Consumer Services	3.61%
Insurance	6.02%
Hospitality	3.61%
Manufacturing	16.87%
Construction	12.05%
Education	1.2%
Retail	7.23%
Law Firms	8.43%
Business Services	16.87%
Minerals & Mining	1.2%
Finance	3.61%
Healthcare	3.61%
IT	2.41%
Federal	2.41%
Media & Internet	2.41%
Energy	1.2%
Real Estate	1.2%
Agriculture	1.2%

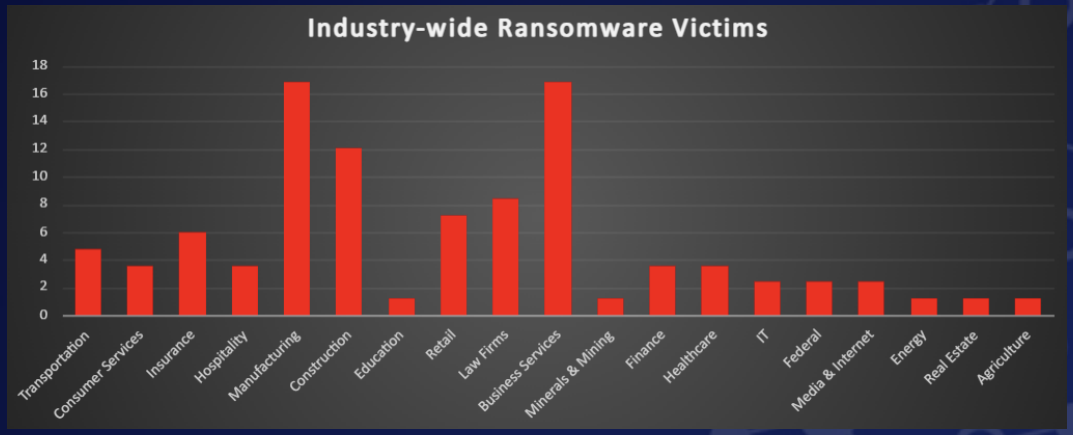


Figure 4: Industry-wide Ransomware Victims