Red Piranha
unified threat management

THREAT INTELLIGENCE REPORT

May 13 - 19, 2025

Report Summary:

- **New Threat Detection Added** – 2
  - DollyWay
  - RATatouille (I2PRAT)

- **Threat Protections integrated into the Crystal Eye - 178**

The following threats were added to Crystal Eye this week:

1. DollyWay

DollyWay has been around since 2016 and focuses on comprising WordPress sites. Since 2016 they have successfully compromised over 20,000 sites. Once a site is compromised, it redirects users to a malicious site when they visit a compromised site. DollyWay is currently using a traffic direction system (TDS) to redirect users, this also generates revenue as users are sent to scam sites.

Rules Created: 02
Rule Set Type:

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

Class Type: Trojan-activity
Kill Chain:

Tactic	Technique ID	Technique Name
Initial Access	T1190	Exploit Public-Facing Application
Execution	T1059	Command and Scripting Interpreter
Persistence	T1505	Server Software Component
Command-and-Control	T1568	Dynamic Resolution

2. RATatouille (I2PRAT)

I2PRAT is a multistage Remote Access Trojan (RAT). This malware is deployed via a technique called ClickFix which has been covered in the past. ClickFix technique impersonates known websites, or browser updates and tricks the user into copying and pasting a PowerShell script into their terminal. Once the I2PRAt malware executes it goes through various stages to disable Microsoft Defender and deobfuscate itself to perform persistence and connect to the attacker-owned C2 server.

Rules Created: 06
Rule Set Type:

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

Class Type: Trojan-activity

Kill Chain:

Tactic	Technique ID	Technique Name
Execution	T1059.001	Command and Scripting Interpreter - PowerShell
Persistence	T1574.001	Hijack Execution Flow - DLL
Privilege Escalation	T1548	Abuse Elevation Control Mechanism
Defence Evasion	T1622 T1140	Debugger Evasion Deobfuscate/Decode Files or Information
Command-and-Control	T1568	Dynamic Resolution

Known exploited vulnerabilities (Week 3 - May 2025)

Vulnerability	CVSS	Description
CVE-2025-42999	9.1 (Critical)	SAP NetWeaver contains a vulnerability within the Visual Composer Metadata Uploader component of the application that can allow an authenticated remote attacker to upload files that when deserialised by the application can result in the attacker gaining access to the host system.
CVE-2024-12987	9.8 (Critical)	Multiple DrayTek routers contain a vulnerability within the web management interface that can allow an attacker to execute OS commands.
CVE-2025-4664	4.3 (Medium)	Google Chromium contains a vulnerability that can result in a leakage of cross-origin data when loading a remote img via a specially crafted HTML page.
CVE-2025-32756	9.6 (Critical)	Multiple Fortinet products contain a vulnerability that can allow an unauthenticated remote attacker to execute arbitrary code or commands via an HTTP request that can result in an attacker gaining access to the system. This vulnerability affects FortiCamera, FortiMail, FortiNDR, FortiRecorder and FortiVoice.
CVE-2025-32709	7.8 (High)	Microsoft Windows Ancillary Function Driver for WinSock contains a vulnerability that can allow an authenticated attacker to escalate privileges to the administrator.
CVE-2025-30397	7.5 (High)	Microsoft Windows Scripting Engine contains a vulnerability that can allow a remote attacker to execute code over a network resulting in gaining unauthorised access to the system.
CVE-2025-32706	7.8 (High)	The Driver used in the Microsoft Windows Common Log File System (CLFS) contains a privilege escalation vulnerability that can allow a local attacker to elevate to SYSTEM-level privileges.
CVE-2025-32701	7.8 (High)	Microsoft Windows Common Log File System (CLFS) Driver contains a privilege escalation vulnerability that can allow a local attacker to elevate to SYSTEM-level privileges.
CVE-2025-32400	7.8 (High)	The DWM Core Library in Microsoft Windows contains a privilege escalation vulnerability that can allow a local attacker to elevate to SYSTEM-level privileges.
CVE-2025-47729	4.9 (Medium)	The TeleMessage archiving backend contains a vulnerability that results in cleartext messages being archived on the remote service. The intended functionality of this application is to archive the end-to-end encrypted messages, however, due to this flaw the cleartext messages are archived instead.

For more information, please visit the **Red Piranha Forum**:
https://forum.redpiranha.net/t/known-exploited-vulnerabilities-catalog-3rd-week-of-may-2025/564

Updated Malware Signatures (Week 3 - May 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.”
UNK_MachoMan	A North Korean Created Python Malware. They impersonate LinkedIn Recruiters and send potential target questions to answer in the form of coding assessment, and this requires the victims to pull and set up a Docker Image that looks legitimate but configures a connection to a C2 Server.

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

SafePay has surged ahead this week, accounting for 22.32% of all reported ransomware incidents. Its sharp rise signals either a large-scale campaign or expansion in tooling and targeting scope—especially noteworthy given its relatively low visibility in the past weeks.

Qilin comes in second at 11.61%, continuing its aggressive streak and demonstrating increasing technical maturity across sectors. Inc Ransom follows closely with 8.04%, sustaining pressure on a wide victim base, often leveraging double-extortion tactics.

Kraken also makes a prominent showing at 7.14%, a significant jump from its usual low-profile activity, suggesting an operational uptick or a successful exploitation campaign.

J Group and LeakedData each contribute 4.46%, pointing to continued activity from mid-tier actors maintaining a foothold across various industries. A trio—Medusa, Stormous, and Weyhro—register 3.57% each, reflecting persistent campaigns with evolving infrastructure and payload variants.

Devman (2.68%) and LockBit3.0 (1.79%) show reduced momentum this week compared to past prominence yet still retain enough reach to disrupt operations across enterprise systems.

Meanwhile, a group of persistent mid-volume threats—including Bert, DragonForce, WorldLeaks, RansomHouse, and Lynx (each at 1.79%)—illustrate the noisy baseline of ransomware threats that continue to test defensive perimeters.

Play, though historically dominant, drops to 6.25%, indicating a potential tactical pivot or diminished campaign activity. Notably, operators like Nova, Monti, Gunra, Clop, Kairos, NightSpire, Rhysida, Everest, Embargo, El Dorado, Space Bears, and BlackSuit each contribute 0.89%, underscoring the diversity of lesser-known groups still actively exploiting the global attack surface.

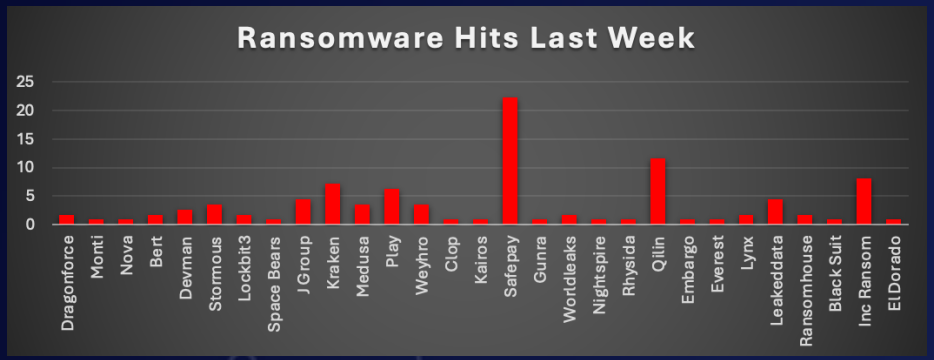
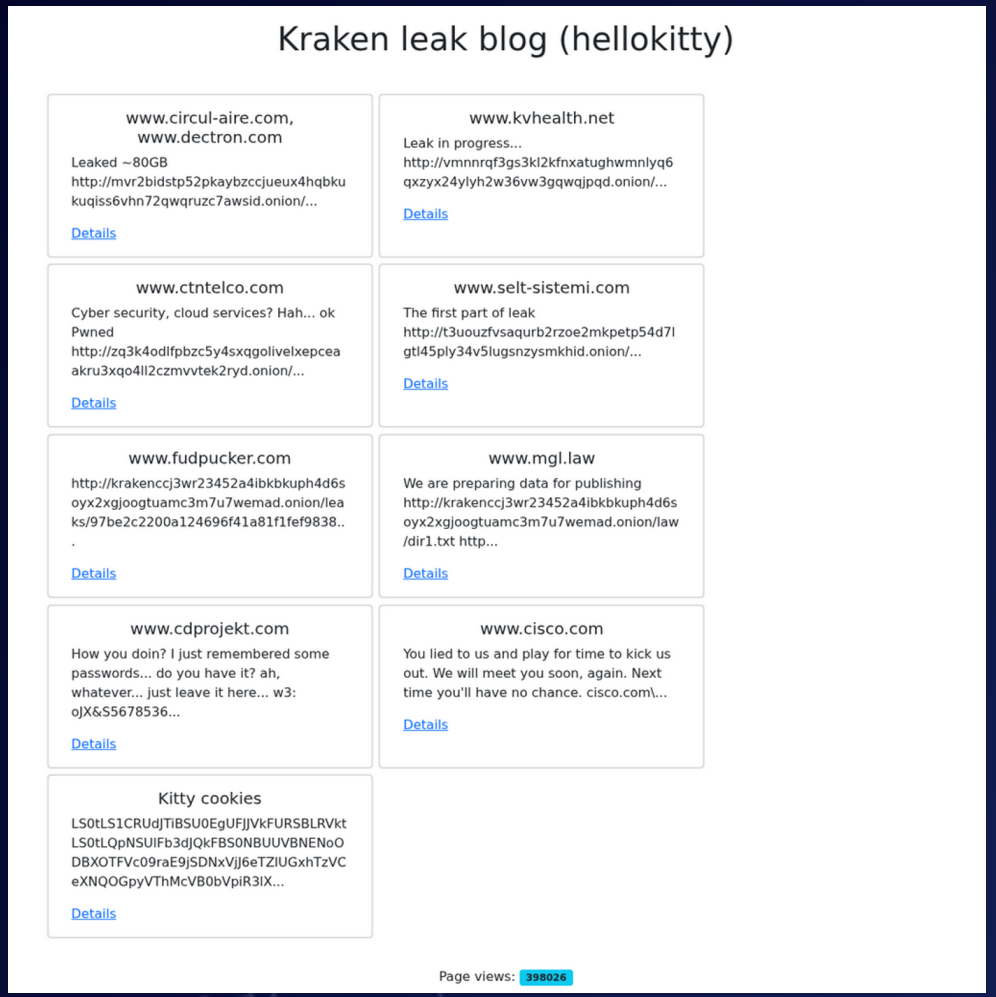


Figure 1: Ransomware Group Hits Last Week

Kraken Ransomware

Description
Kraken is a ransomware group believed to be a rebranding of the HelloKitty/HelloGookie operation. It emerged in February 2025 and has since targeted multiple industries including technology, healthcare, legal services, and hospitality. Kraken follows a double-extortion model, stealing sensitive data before encrypting victim systems and threatening public disclosure via a Tor-based data leak site.

Kraken's tactics mirror those used by its predecessor HelloKitty, including rapid exploitation of vulnerabilities, privilege escalation, and aggressive encryption. While many of their earlier leaks re-used data from previous breaches, newly confirmed victims, including Klickitat Valley Health (KVH), indicate active and ongoing operations.



Detailed TTPs

Initial Access:

- Exploiting public-facing applications (e.g., Apache ActiveMQ RCE CVE-2023-46604).
- Use of stolen credentials acquired via phishing, bypassing MFA.

Privilege Escalation & Lateral Movement:

- Credential dumping via Mimikatz and similar tools.
- Using valid accounts and remote desktop protocols for movement across the network.

Defence Evasion:

- Disabling or killing processes related to security, databases, and backups.
- Deleting shadow copies via vssadmin and WMI commands.

Discovery:

- Enumerating processes and files.
- Discovering network shares, system information, and user sessions.

Execution & Command-and-Control:

- Manual execution of ransomware via cmd or batch scripts.
- Use of built-in Windows shell commands, no active C2 during encryption.

Exfiltration:

- Sensitive data staged and exfiltrated, likely via tools like rclone or SFTP.
- Used as leverage for ransom through a Tor-based leak site.

Impact:

- File encryption with .crypted extension.
- Deletion of backups and delivery of custom ransom notes.

Kraken Ransomware – IOCs

Domains & URLs

- Tor Leak Site:

krakenccj3wr23452a4ibkbkuph4d6soyx2xgjoogtuamc3m7u7wemad.onion

- Legacy Contact Email Domain (HelloKitty era):

hellokittycat[.]online

File Indicators

- Encrypted File Extension:

.crypted

(Files renamed to include this extension after encryption.)

- Ransom Note Filenames:

Typically dropped as readme.txt, HOW_TO_DECRYPT.txt, or similar in each directory.

Malware Hashes

- Representative Ransomware Sample Hash (HelloKitty/Kraken variant):

SHA-256:
501487B025F25DDF1CA32DEB57A2B4DB43CCF6635C1EDC74B9CFF54CE0E5BCFE

(Note: New samples will likely vary, but similar imphash and behaviour.)

Tools Used

- mimikatz.exe – Credential dumping
- lsass.DMP – LSASS memory dump for credential harvesting
- vssadmin.exe – Deletion of Volume Shadow Copies
- taskkill.exe – Termination of AV/database/backup processes
- Batch scripts executed via cmd.exe

Command Patterns (Detection Signatures)

- vssadmin delete shadows /all /quiet
- taskkill /F /IM <process_name> (e.g., sqlservr.exe, veeam.exe)
- net stop <service_name> (e.g., backup, antivirus)

Index of /

../		
FTP/	14-Feb-2025 19:30	-
FTP_ATT/	14-Feb-2025 19:26	-
PROFILES/	13-Feb-2025 00:03	-
SCANNED_DOCS/	12-Feb-2025 16:59	-
SHARED_DOCS/	15-Feb-2025 11:32	-

Index of /

../		
AEROSPACE MATERIALS MANAGEMENT Srl/	20-Feb-2025 12:27	-
LEONARDO SpA - div.ne Elicotteri Vergiate VA/	20-Feb-2025 12:23	-
LEONARDO SpA - div.ne elettronica Bacoli NA/	20-Feb-2025 12:27	-
LEONARDO SpA - div.ne elettronica Nerviano MI/	20-Feb-2025 12:26	-
LEONARDO SpA - div.ne elettronica Ronchi dei Le..>	20-Feb-2025 12:26	-
LEONARDO SpA - div.ne elettronica San Maurizio ..>	20-Feb-2025 12:25	-
LEONARDO SpA - div.ne elettronica presso Campi ..>	20-Feb-2025 12:26	-
LEONARDO SpA - div.ne elicotteri Cascina Costa ..>	20-Feb-2025 12:24	-
LEONARDO SpA - div.ne elicotteri Sesto Calende VA/	20-Feb-2025 12:23	-
LEONARDO SpA - div.ne velivoli presso Aeroporto..>	20-Feb-2025 12:23	-
LEONARDO SpA - div.ne velivoli presso Lonate Po..>	20-Feb-2025 12:22	-
LEONARDO SpA - div.ne velivoli presso San Mauri..>	20-Feb-2025 12:21	-
LEONARDO SpA - div.ne velivoli presso Venegono ..>	20-Feb-2025 12:20	-
Mecaer Aviation Group S.p.A/	20-Feb-2025 12:19	-
NOVE S.r.l/	20-Feb-2025 12:19	-
POLITECNICO DI TORINO/	20-Feb-2025 12:19	-
TELESPAZIO/	20-Feb-2025 12:19	-
TELESPAZIO Belgium Srl/	20-Feb-2025 12:19	-
THALES ALENIA SPACE ITALIA S.p.A - Gorgonzola/	20-Feb-2025 12:18	-
UR Holding S.p.A/	20-Feb-2025 12:18	-
REGISTRO DDT e FT ATTIVE 25.xlsx	10-Feb-2025 16:56	39426

Ransomware Victims Worldwide

The United States remains the most targeted nation globally, accounting for a staggering 43.75% of all ransomware victims last week. With its extensive digital infrastructure, high concentration of critical industries, and interconnected networks, the US continues to present lucrative opportunities for both targeted and mass exploitation ransomware operations.

Germany follows as a distant second with 8.04%, indicating that Western Europe's industrial and manufacturing hubs remain in the crosshairs of ransomware groups seeking disruption and financial gain.

Canada ranks third with 8.04% as well (combined from 5.36% and 2.68%), reflecting the country's strong economic ties to the US and its susceptibility through shared supply chains and digital service providers.

Australia is next at 4.47% (1.79% + 2.68%), reaffirming its strategic importance in the Asia-Pacific region, particularly given its high cloud adoption rates and expanding managed service ecosystems.

Japan (combining 0.89% and 3.57%) contributes 4.46%, highlighting renewed ransomware activity in the region. Similarly, Brazil and the United Kingdom each accounted for 3.58%, suggesting sustained targeting of Latin American and Western European networks.

Notably, Spain, France, Singapore, and Taiwan each reported 1.79% of global ransomware incidents, showing distributed attacks across European and Southeast Asian nations.

A broad spectrum of countries—including India, South Africa, Italy, Netherlands, Switzerland, Philippines, Belgium, Poland, Guatemala, Jamaica, Peru, Romania, Cyprus, and Pakistan—each experienced 0.89% of total incidents, a reminder that even lower-profile or emerging economies are not exempt from global ransomware activity.

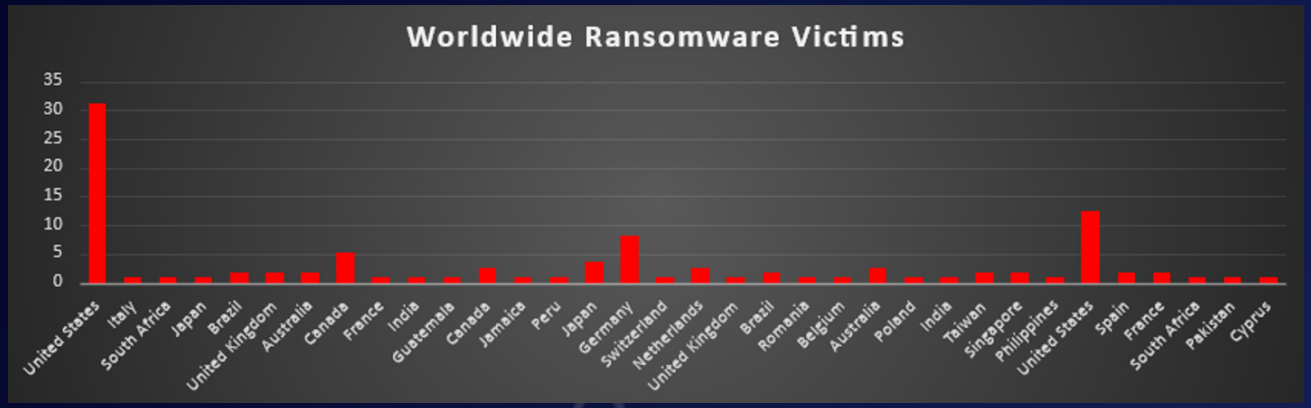


Figure 4: Ransomware Victims Worldwide

Ransomware Victims by Industry

The Manufacturing sector continues to bear the brunt of ransomware activity, accounting for 17.86% of total incidents this week. Its reliance on uptime, legacy systems, and often-overlooked cybersecurity investments make it a persistent high-value target for disruption-based extortion.

Construction follows at 11.61%, indicating growing adversary interest in infrastructure-heavy industries. The sector's increasing digitisation, coupled with often limited cybersecurity resources, makes it a soft target for attackers aiming to halt critical operations.

Retail stands at 8.93%, remaining attractive due to its rich customer data, integrated point-of-sale systems, and high dependency on digital transactions. Meanwhile, Business Services—which include consulting, BPO, and professional support—saw 8.04% of attacks, reinforcing their role as high-value intermediary targets.

Finance, Transportation, and Hospitality each reported 6.25%, reflecting how sectors tied to economic infrastructure and public service are facing parallel waves of targeted intrusions.

Healthcare and Education experienced 4.46% each, highlighting continued attacker interest in sectors with high-impact service models and time-sensitive operations. Consumer Services and Law Firms were hit with 3.57% each—both representing sectors where the value of data confidentiality and uptime creates high leverage for extortion.

A cluster of industries—including Media & Internet, Real Estate, Federal, and Telecommunications—each reported 2.68%, suggesting broader targeting of data-rich and connectivity-focused verticals.

The IT and Energy sectors each accounted for 1.79%, while Organisations (unspecified entities) also shared this rate, reinforcing that attackers continue to pursue targets irrespective of organisational size or specialisation.

Finally, Minerals & Mining and Insurance each contributed 0.89% of incidents, with the inclusion of Insurance reaffirming that even cyber-risk managers themselves are not beyond reach.