Red Piranha
unified threat management

THREAT INTELLIGENCE REPORT

Apr 29 - May 05, 2025

Report Summary:

- **New Threat Detection Added** – 2
  - ClickFix
  - Lumma Stealer

- **New Threat Protections - 205**

The following threats were added to Crystal Eye this week:

1. ClickFix

ClickFix is a social engineering attack technique that creates pop-ups alerting the user that if something has gone wrong on their computer then they can fix it by clicking buttons labelled “Fix It” or “Copy Fix”. By pressing these buttons, it saves a malicious command to the user clipboard, and they are instructed to open PowerShell and paste it in, this then executes a payload that comprises the user’s system.
The initial infection that causes the “pop-ups” to occur is usually delivered through phishing emails.

Threat Protected: 08
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: Malware

MITRE ATT&CK:

Tactic	Technique ID	Description
Initial Access	T1566.001 T1566.002	Phishing: Spear phishing Attachment Phishing: Spear phishing Link
Execution	T1059.001 T1204.001 T1204.004	Command and Scripting Interpreter: PowerShell User Execution: Malicious Link User Execution: Malicious Copy and Paste

2. Lumma Stealer

Lumma Stealer has been around since 2022 and has grown to be one of the most prominent “info stealer” malware. Lumma Stealer uses the MaaS (Malware-as-a-Service) model and primarily targets Cryptowallets, User Credentials and Multifactor Authentication Web browser extensions for users on Windows systems as payloads are delivered in EXE, DLL and PowerShell formats.

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: Domain-c2

Kill Chain:

Tactic	Technique ID	Description
Initial Access	T1566.001 T1566.002	Phishing: Spear phishing Attachment Phishing: Spear phishing Link
Execution	T1059.001 T1204.001	Command and Scripting Interpreter: PowerShell User Execution: Malicious Link
Credential Access	T1555.003 T1555.004 T1555.005	Credentials from Password Stores: Web Browsers, Password Managers
Exfiltration	T1041	Exfiltration Over C2 Channel

Known exploited vulnerabilities (Week 1 - May 2025)

CISA (https://www.cisa.gov/known-exploited-vulnerabilities-catalog)

Vulnerability	CVSS	Description
CVE-2025-31324	10.0 (Critical)	SAP NetWeaver Unrestricted File Upload Vulnerability
CVE-2024-38475	9.1 (Critical)	Apache HTTP Server Improper Escaping of Output Vulnerability
CVE-2023-44221	7.2 (High)	SonicWall SMA100 Appliances OS Command Injection Vulnerability
CVE-2025-34028	10.0 (Critical)	Commvault Command Center Path Traversal Vulnerability
CVE-2024-58136	9.8 (Critical)	Yiiframework Yii Improper Protection of Alternate Path Vulnerability

For more information, please visit the **Red Piranha Forum**:
https://forum.redpiranha.net/t/known-exploited-vulnerabilities-catalog-1st-week-of-may-2025/562

Updated Malware Signatures (Week 1 - 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

Qilin tops the list with 17.27%. Nova follows at 16.36%, continuing its rise from a mid-tier outfit into a true “big game” player.

Play sits close behind on 14.55%; the group’s fast-moving Linux/VMware lockers keep MSPs and industrial targets in its sights.

J Group accounts for 8.18%. While smaller, its opportunistic hit list shows wide geographic spread.

Rhysida posts 7.28% (two separate listings in the raw feed). Their hallmark is hands-on-keyboard intrusions that end in quick ESXi or Windows encryption.

A solid 40%+ of all observed attacks stem from these top three families alone, underscoring a highly concentrated threat environment. Mid-packed actors such as Lynx and Devman (each at 5.45%) plus Medusa, Hunters, and Inc Ransom round out the top ten, reinforcing the long-tail of persistent but less prolific gangs.

Victims continue to span every vertical—from manufacturing and professional services to healthcare—highlighting that defensive priorities must remain industry-agnostic: patch velocity, credential hygiene, and robust off-network backups are still the best universal shields against this concentrated onslaught.

Ransomware Groups	Overall Percentage of total attack coverage
Rhysida	3.64%
Dunghill	0.91%
Qilin	17.27%
Gunra	1.82%
RAlord	0.91%
NightSpire	0.91%
Medusa	4.55%
Rhysida	3.64%
Hunters	3.64%
Play	14.55%
Nova	16.36%
Secp0	0.91%
Lynx	5.45%
Termite	0.91%
Akira	1.82%
Bert	0.91%
Inc Ransom	2.73%
Leaked Data	0.91%
Devman	5.45%
Interlock	0.91%
Skira Team	0.91%
RansomHouse	0.91%
Everest	1.82%
Lockbit3.0	2.73%
Stormous	0.91%
J Group	8.18%

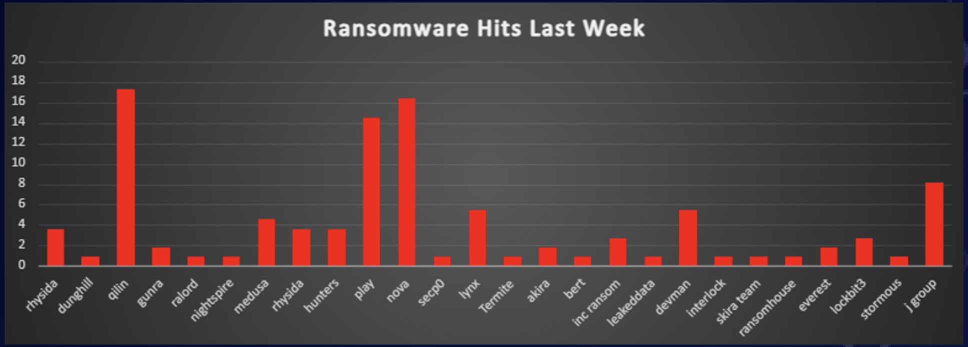
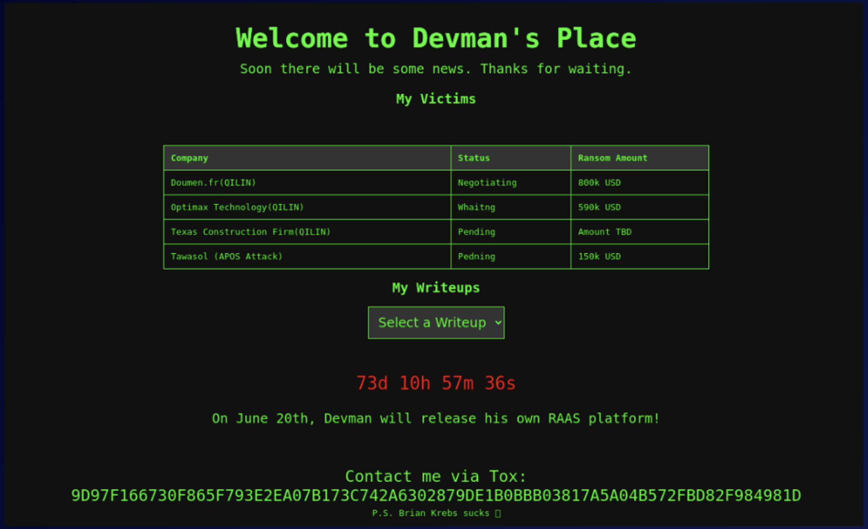


Figure 1: Ransomware Group Hits Last Week

Devman Ransomware Group

Devman burst onto the scene in mid-April 2025, appearing on the dark web leak markets with an initial wave of more than a dozen victims. Early chatter on threat-intel forums suggests the operator is a former affiliate of the Qilin/Agenda RaaS who has split off to launch a brand-new franchise while still collaborating on some jobs. Public breach posts credited jointly to “Qilin & Devman” (e.g., the Feel Four S.L. retail attack) confirm that the newcomer is already comfortable partnering with established crews.

From the start, Devman has embraced a double-extortion business model: data is stolen first, then systems are encrypted, and finally the victim is pressured with public disclosure on a leak portal if payment is refused. Victims span retail, construction, healthcare, manufacturing, and IT services across Asia, Europe, Africa, and North America, underscoring an opportunistic, RaaS-style targeting philosophy rather than a single-sector focus.



Welcome to Devman's Place

Soon there will be some news. Thanks for waiting.

My Victims

Company	Status	Ransom Amount
Doumen.fr(QILIN)	Negotiating	800k USD
Optimax Technology(QILIN)	Whaitng	590k USD
Texas Construction Firm(QILIN)	Pending	Amount TBD
Tawasol (APOS Attack)	Pedning	150k USD

My Writeups

73d 10h 57m 36s

On June 20th, Devman will release his own RAAS platform!

Contact me via Tox:
9D97F166730F865F793E2EA07B173C742A6302879DE1B0BBB03817A5A04B572FBD82F984981D
P.S. Brian Krebs sucks □

Detailed TTPs

Devman ransomware campaigns begin by exploiting vulnerable perimeter services such as unpatched VPN gateways or ESXi hosts. A 64-bit payload runs with administrator privileges, leveraging native APIs and command-line execution. Persistence and lateral spread rely on scheduled services, Run-key hijacking, and PsExec-driven SMB propagation. The malware escalates privileges through service abuse, then disables security products and wipes Windows or ESXi logs. It enumerates shares and domains, stages stolen data, and exfiltrates archives through encrypted channels. Negotiations use peer-to-peer Tox while a public leak site amplifies pressure. Finally, robust encryption and snapshot deletion cripple recovery, forcing ransom payments from victims worldwide.

Stage	Techniques Observed
Initial Access	• Exploit of exposed services / un-patched web apps (e.g., VPN, ESXi). (Lockbit Decryptor)
Execution	• 64-bit payload executed with admin rights. • Native API & command-line invocation (T1106/T1059).
Persistence & Lateral Movement	• Scheduled services or modified Run keys (T1543). • PsExec/SMB for cross-host propagation (T1021).
Privilege Escalation	• Abuse of service installs/token privileges (T1548).
Defence Evasion	• Stops AV/backup services & clears Windows/ESXi logs (T1562).
Discovery	• Network share and domain discovery to maximise impact (T1135).
Exfiltration	• Bulk file staging then exfiltration over encrypted channels (T1041).
Command-and-Control	• Negotiation via peer-to-peer Tox messenger; leak-site for pressure (T1071.001). (Ransomware.live)
Impact	• Data-Encrypted-for-Impact (T1486). • Inhibit System Recovery – deletes shadow copies & ESXi snapshots (T1490). (Lockbit Decryptor)

TTP Chart

Tactic (ID)	Technique	Technique ID	Description
Initial Access	Exploit Public-Facing Application	T1190	Weaponises un-patched VPN/ESXi services
Execution	Native API	T1106	Runs encryption routines directly via Win32 APIs
Persistence	Create/Modify System Process	T1543	Installs malicious service for re-launch
Priv-Esc	Abuse Elevation Control Mechanism	T1548	Uses built-in admin tokens
Defence Evasion	Impair Defences	T1562	Terminates security & backup processes
Discovery	Network Share Discovery	T1135	Enumerates shares before encryption
Lateral Move	Remote Services (PsExec/SMB)	T1021	Spreads to adjacent hosts
Exfiltration	Exfiltration Over C2 Channel	T1041	Sends archives to TA-controlled servers
C2	Application-Layer Protocol (Tor/Tox)	T1071.001	Negotiation & leak-site hosting
Impact	Data Encrypted for Impact	T1486	Encrypts files with AES + RSA
Impact	Inhibit System Recovery	T1490	Deletes snapshots/shadow copies

Indicator Type	Value
Onion URL	qljmlmp4psnn3wqskkf3alqquatymo6hntficb4rhq5n76kuogcv7zyd.onion
Clearnet IP	83.217.209.210
File Extension	.devman
Ransom Note	recover_files.txt
ESXi Target Path	/vmfs/volumes/*
Negotiation Channel	Tox messenger ID (unique per victim)

Other Indicators

- Surge in CPU/Disk utilisation as w.exe (or similarly named binary) spawns across servers.
- Sudden stop of backup/AV services (vss, sql, vmware-hostd, etc.).
- Large outbound traffic burst to Tor relay IPs just before encryption.

Ransomware Victims Worldwide

A fresh review of public victim-site postings for the current period confirms that the United States remains the epicentre of ransomware activity, absorbing an outsized 44.55% of all known incidents. The figure is even higher than last period's 39.62%, underscoring the country's unmatched concentration of high-value infrastructure and data-rich enterprises that continue to attract both profit-driven and geopolitically motivated actors.

Canada emerges as a distant—but still notable—second with 6.36% of global cases, signalling a steady rise in attacks across North America outside the US mainland. Germany follows at 4.55%, reflecting the persistent targeting of Europe's industrial and manufacturing heartland. A trio of nations each record 3.64% of incidents: Italy, Australia, and China. Italy's presence highlights sustained Southern-European exposure, while concurrent activity in Australia and China points to the Asia-Pacific theatre's growing importance for threat actors seeking both Western and regional targets.

The mid-tier impact is visible in the United Kingdom (2.73%) and Saudi Arabia (2.73%), alongside Argentina and South Africa (each 2.73%). These numbers suggest that both established economies and key emerging markets remain firmly on adversaries' radar. Nations posting 1.82% of incidents include Malaysia, Georgia, Japan, and Singapore—an indicator of ransomware's reach into South-East Asian, Caucasian, and East-Asian digital ecosystems.

A broad long-tail of countries each account for 0.91% of reported cases—among them Brazil, Portugal, Taiwan, The Netherlands, Spain, Malta, Jordan, Thailand, Hungary, Peru, France, Luxembourg, Vietnam, India, Costa Rica, New Zealand, and the island nation of Fiji. Although individual volumes are low, the sheer geographic diversity of these sightings underlines ransomware's truly transnational footprint.

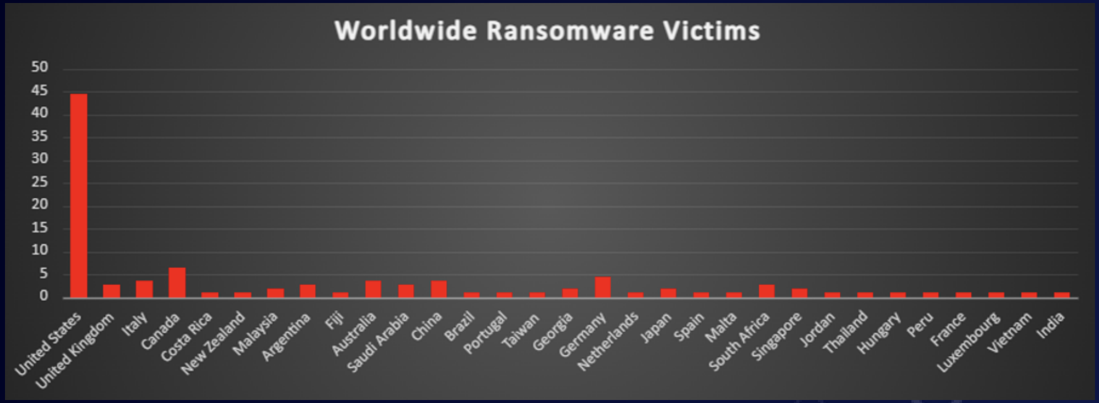


Figure 3: Ransomware Victims Worldwide

Countries	Worldwide Ransomware Victims
United States	44.55%
United Kingdom	2.73%
Italy	3.64%
Canada	6.36%
Costa Rica	0.91%
New Zealand	0.91%
Malaysia	1.82%
Argentina	2.73%
Fiji	0.91%
Australia	3.64%
Saudi Arabia	2.73%
China	3.64%
Brazil	0.91%
Portugal	0.91%
Taiwan	0.91%
Georgia	1.82%
Germany	4.55%
The Netherlands	0.91%
Japan	1.82%
Spain	0.91%
Malta	0.91%
South Africa	2.73%
Singapore	1.82%
Jordan	0.91%
Thailand	0.91%
Hungary	0.91%
Peru	0.91%
France	0.91%
Luxembourg	0.91%
Vietnam	0.91%
India	0.91%

Ransomware Victims by Industry

The Manufacturing sector remains the most targeted, accounting for 20% of ransomware attacks, highlighting its reliance on industrial systems and the high cost of operational downtime. Business Services follow at 16.36%, as threat actors exploit their access to sensitive client data and widespread integration in supply chains.

The Retail sector ranks third with 8.18%, frequently targeted due to high transaction volumes and customer data. Construction follows with 7.27%, reflecting risks tied to disrupted project timelines and infrastructure operations.

Sectors like Education, Transportation, Healthcare, and Consumer Services each report 4.55%, showing consistent pressure on institutions that manage personal data or critical services. Hospitality, Law Firms, and IT each see 3.64% of attacks, pointing to the exploitation of availability and legal or technical data.

Energy, Telecommunications, Finance, Federal, and Media & Internet each account for 2.73%, while Insurance and Organisations report 1.82%. Even niche industries like Minerals & Mining and Agriculture, each at 0.91%, are now on the radar.

This broad impact underscores ransomware's cross-industry reach. Regardless of size or sector, all organisations must adopt tailored defences, ensure regular backups, and maintain response readiness to counter the ever-evolving ransomware threat.

Industries	Industry-wide Ransomware Victims
Business Services	16.36%
Education	4.55%
Manufacturing	20%
Hospitality	3.64%
Energy	2.73%
Telecommunications	2.73%
Law Firms	3.64%
Federal	2.73%
Construction	7.27%
Transportation	4.55%
Retail	8.18%
IT	3.64%
Finance	2.73%
Insurance	1.82%
Minerals & Mining	0.91%
Consumer Services	4.55%
Agriculture	0.91%
Healthcare	4.55%
Media & Internet	2.73%
Organisations	1.82%

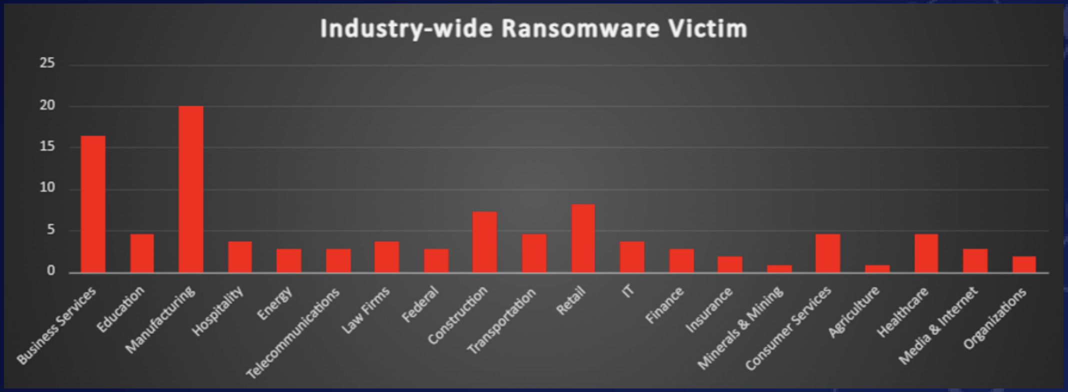


Figure 4: Industry-wide Ransomware Victims