Red Piranha
unified threat management

THREAT INTELLIGENCE REPORT

Aug 05 - 11, 2025

Report Summary:

- **New Threat Detection Added**
  - Stealerium
  - TinyLoader
- **Detection Summary**
  - **Threat Protections integrated into the Crystal Eye - 81**
  - **Newly Detected Threats - 22**

The following threats were added to Crystal Eye this week:

1. Stealerium

Stealerium is an open-source information stealer that's written in C# and has been known to be utilised in recent ClickFix-based campaigns. As with most stealer-based malware, Stealerium exfiltrates information stored in browsers, such as passwords, cookies, as well as cryptocurrency wallets and files. It also includes features such as a keylogger, webcam screenshots, as well as a "clipper", which replaces crypto wallet addresses when a cryptocurrency transaction is being made.

What sets Stealerium apart from standard infostealer-based malware is its ability to exfiltrate the information over Discord webhooks.

Threats Protected: 3
Class Type: Malware
Rule Set Type:

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

Kill Chain:

Tactic	Technique ID	Technique Name
Initial Access	T1566	Phishing
Execution	T1204.002	User Execution - Malicious File
	T1204.004	User Execution – Malicious Copy and Paste
	T1059.001	Command and Scripting Interpreter - PowerShell
Credential Access	T1555.003	Credentials from Password Stores – Web Browsers
Collection	T1056.001	Input Capture – Keylogging
	T1005	Data from Local System
Exfiltration	T1567.004	Exfiltration Over Web Service – Exfiltration Over Webhook

2. TinyLoader

XTinyLoader is a recently discovered modular loader and stealer-based malware that has been seen as early as July 2025 and has been seen to be distributed via fake cracked software.

Threats Protected: 3
Class Type: Malware
Rule Set Type:

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

Kill Chain:

Tactic	Technique ID	Technique Name
Execution	T1204.004	User Execution – Malicious File
Persistence	T1547.001	Boot or Logon AutoStart Execution – Registry Run Keys / Startup Folder
Defence Evasion	T1055.001	Process Injection – Dynamic-link Library Injection
	T1027.013	Obfuscated Files or Information – Encrypted/Encoded File
Collection	T1056.001	Input Capture – Keylogging
Command-and-Control	T1071.001	Application Layer Protocol – Web Protocols
Exfiltration	T1041	Exfiltration Over C2 Channel

Current Threat Summary

Known exploited vulnerabilities (Week 2 August 2025)

Vulnerability	CVSS	Description
D-Link DCS-2530L and DCS-2670L Devices	7.5 (High)	D-Link DCS-2530L and DCS-2670L IP cameras contain a vulnerability that can allow a remote unauthenticated attacker to obtain the Administrator password via an HTTP request. Both of these devices are end-of-life and may no longer receive security updates to mitigate against this vulnerability.
D-Link DCS-2530L and DCS-2670L Devices	8.8 (High)	D-Link DCS-2530L and DCS-2670L IP cameras contain a command injection vulnerability that can allow a remote authenticated attacker to execute operating system commands on the device via an HTTP request. Both of these devices are end-of-life and may no longer receive any security updates to mitigate against this vulnerability.
D-Link DNR-322L	8.8 (High)	D-Link DNR-322L contains a vulnerability that can allow a remote authenticated attacker to execute operating system commands via the backup restore functionality on the device. This device is end-of-life and may no longer receive security updates to address this vulnerability.

For more information, please visit the **Red Piranha Forum**:
https://forum.redpiranha.net/t/known-exploited-vulnerabilities-catalog-1st-week-of-august-2025/585

Updated Malware Signatures (Week 2 August 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.”
zgRAT	A Remote Access Trojan (RAT) used in cyberattacks that provides attackers with 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 – Weekly Overview

Qilin and Pear share the top position this week, each accounting for 13.53% of reported ransomware incidents. This high activity suggests well-coordinated campaigns, possibly driven by active affiliate networks and diversified targeting.

Black Nevas follows closely with 11.28%, indicating a strong operational tempo and potential expansion into new geographies or industries.

Walocker ranks next with 8.27%, showing a sustained presence and continued ability to disrupt victim operations.

Mid-tier activity comes from D4rk4rmy (6.77%), DragonForce and Play (6.02% each), groups known for a mix of opportunistic targeting and strategic campaigns.

Other active players include Lynx, Inc Ransom, WorldLeaks, and Everest (all at 3.01%), along with Fsociety and Interlock (2.26%). These actors maintain steady activity levels and remain persistent threats in their respective niches.

A broad set of lower-volume actors, Gunra, DireWolf, J Group, Devman2 and Sarcoma (1.5% each), are still engaging in smaller-scale or more targeted operations.

The long tail includes IMN Crew, Rhysida, Brain Cipher, Money Message, TeamXXX, Kairos, RansomedVC2, SafePay, Nitrogen, Qilin-Securotrop, Akira, Ransomware Blog, Space Bears, and Sinob (all at 0.75%). While individually small, collectively these represent a significant portion of the ecosystem's constant background activity.

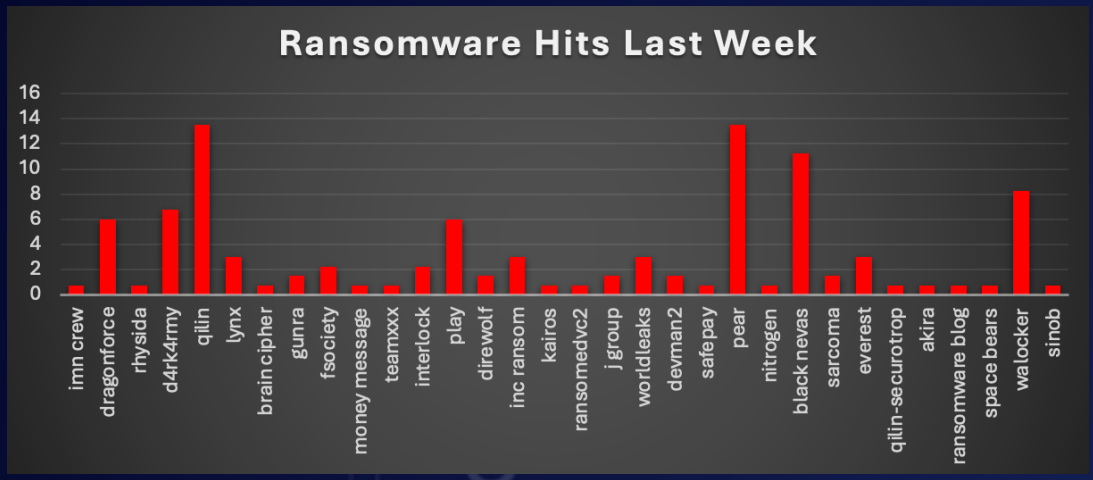


Figure 1: Ransomware Group Hits Last Week

PEAR Ransomware

PEAR (aka Pure Extraction And Ransom) emerged in June 2025 as a Tor-centric, data-broker operation. During 2–8 Aug, the group publicly listed its first batch of victims and brought multiple onion services online. Unlike "encrypt-first" crews, PEAR's playbook centres on data theft and extortion (direct, double, and occasional "free" leaks), all operational infrastructure observed is Tor-only.

Detailed TTPs

Initial Access

- Valid Accounts (T1078) – Confirmed (case-specific): ThinkBig's breach notice cites suspicious activity in an employee email account (O365/Exchange), indicating credentialed access rather than exploit-led encryption tooling. Confidence: High.
- Phishing (T1566) – Assessed (by analogy): Data-extortion actors frequently acquire creds via phishing or purchase from IABs before lateralising; no direct PEAR phish kit is public yet. Confidence: Low-Med, comparative to Karakurt/BianLian.

Discovery / Collection

- Email Collection (T1114) – Likely in ThinkBig case: Email account compromise suggests mailbox scraping. Confidence: Medium (victim notice + extortion content).
- Archive Collected Data (T1560.001) – Operators commonly compress before exfil; PEAR's proof bundles (ZIP/archives) in chats reinforce archiving behaviour. Confidence: Medium.
- Exfiltration to staging (T1074) – Data brokers stage data before leaks; PEAR maintains dedicated file-server onions for storage. Confidence: High.

Exfiltration

- Exfiltration Over Web Service (T1567) – Proof-of-data sent via limewire.com and ufile.io links during negotiations; full dumps are later hosted on PEAR's Tor services. Confidence: High.
- Exfiltration Over Unencrypted/Encrypted Channel (T1041) – Generic but applicable: data moved over HTTP(S) (third-party hosts) and Tor HS. Confidence: Medium. (Corroborated by chats + Tor-only infra.)

Command & Control / Communications

- Proxy/Anonymity Networks (T1090.003) – Tor hidden services for DLS/files; victim comms also via Tor; operator identifiers via onionmail/TOX. Confidence: High.

Impact/Extortion

- Data from Information Repositories (T1213) Leak/Extortion – Primary impact is exposure & coercion rather than encryption; WatchGuard explicitly lists Direct, Double, and Free Data Leaks. Confidence: High.

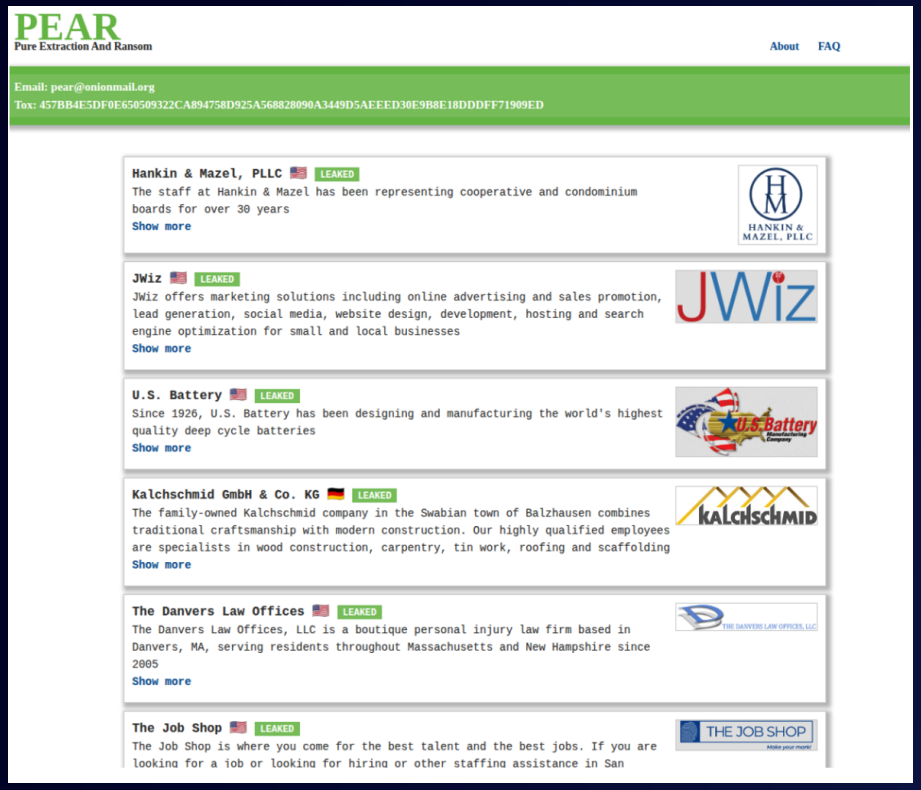
MITRE ATT&CK Matrix

Tactic	Technique ID	How PEAR manifests
Initial Access	Valid Accounts (T1078)	Compromised user email account used as a foothold; possible portal/VPN reuse
Initial Access	Phishing (T1566) (general)	Likely path to creds or IAB-sourced creds (no kit public)
Discovery	Email Collection (T1114)	Email/data store enumeration post-access
Collection	Archive Collected Data (T1560.001)	Mailbox scraping ahead of leaks
Collection	Exfiltration Over Web	Archive lists/samples before exfil
	Service (T1567)	Proof archives via limewire.com and ufile.io; bulk dumps to Tor file servers
Exfiltration	Exfiltration Over C2 Channel (T1041)	Data moved to PEAR-controlled Tor services
Exfiltration C2/Comms	Proxy: Tor (T1090.003)	DLS + file servers exclusively on .onion; contact via TOX/onionmail
Impact	Exfiltration-led Extortion (TA0040 context)	Publication pressure, "free leak" samples, no encryption

IOCs (campaign window context)

Onion Services:

- peargxn3oki34c4savcbcfqofjjwjnnyrlrbszfv6ujlx36mhrh57did.onion
- csxilwnl7orv6rwfjen5ye3tefk5shjtr4tysuykgxjsyngpvoqrvbid.onion
- etus2tmakckdlkyjpevoyciuao7er5fj3qm26aev3nch4fusptefiayd.onion
- yxwomyfmexm3bfcuumnugrzwluol5qwsw6pmne7jklgmzthkp35l2jqd.onion
- Pearsmob5sn44ismokiusuld34pnfwi6ctgin3qbvonpoob4lh3rmtqd.onion



Contact / Negotiation:

Email: pear@onionmail.org

TOX:
457BB4E5DF0E650509322CA894758D925A568828090A3449D5AEEED30E9B8E18DDDFF71909ED

Mitigation with CE 5.0

Email & Sandbox

- Block risky archives (ZIP/TAR/ISO) and enforce detonation for archives containing executables; auto-quarantine.
- Deny Tor/tor2web at DNS/HTTP(S) egress; alert on .onion host patterns in proxy logs.

Endpoint Protection

- HIPS rules to alert on Tor process invocation and unusual archiving at scale; watch for bulk read + archive from file servers (exfil staging).
- Detect credential dumping attempts and suspicious browser/session extractors where present.

Network Controls

- Egress ACLs: restrict outbound to approved destinations; TLS inspection where policy allows; block known Tor2Web domains.
- UEBA: alert on anomalous outbound volumes or first-time destinations from sensitive hosts.

Access Management

- MFA on all remote access; rotate credentials exposed in stealer logs; disable stale accounts.
- Geo/ASN-based conditional access for VPN/RDP.

Backup & Recovery

- Enforce immutable/offline backups; run table-top restore every 30 days; prioritise crown-jewel data sets.

Worldwide Ransomware Victims

The United States remains the overwhelming leader, with 46.62% of all reported ransomware victims this week. This continues to reflect its large attack surface, high-value targets, and heavy focus from ransomware operators globally.

Australia follows at 9.02%, marking a notable level of activity in the Asia-Pacific region. The United Kingdom ranks next at 6.02%, continuing to see consistent targeting of its financial, legal, and service-based industries.

Canada reported 3.76%, while Brazil and Germany each accounted for 3.01% of global incidents, both countries facing regular campaigns due to their industrial sectors and growing digital footprints.

Italy, India, Thailand, Japan, and Colombia each registered 2.26%, showing widespread targeting across Europe, Asia, and South America.

A mid-tier group, including Taiwan, Switzerland, Sweden, and South Korea-saw 1.5% each, reflecting smaller but still noteworthy attack levels.

The long tail includes numerous nations with 0.75% each: France, Vietnam, Nicaragua, Malaysia, Singapore, Mexico, Lithuania, Spain, Kenya, China, South Africa, Eswatini, Egypt, Cameroon, and the Czech Republic. These entries highlight ransomware's global reach, affecting both major economies and smaller nations.

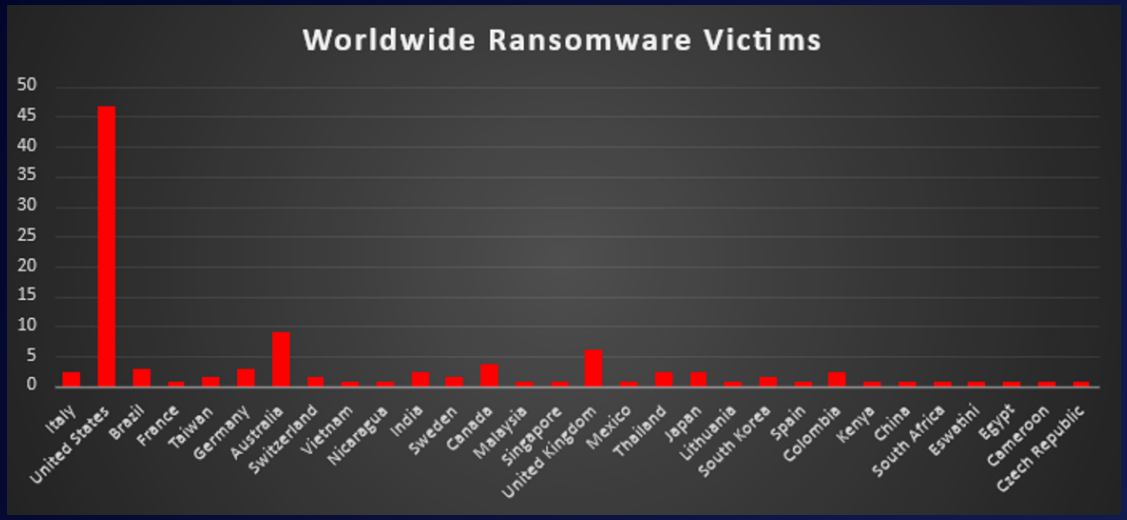


Figure 3: Ransomware Victims Worldwide

Industry-wide Ransomware Victims

Manufacturing remains the most targeted sector this week, representing 17.29% of all ransomware incidents. Its dependence on operational continuity, coupled with complex supply chains and legacy systems, makes it a consistent high-value target for threat actors.

Business Services follow at 11.28%, reflecting persistent campaigns against companies providing IT, consulting, and operational support, often serving as indirect access points to multiple industries.

Hospitality and Retail accounted for 9.77% and 9.02% respectively, showing that customer-facing sectors with large volumes of personal and payment data remain key targets.

Construction and Finance each reported 7.52%, with ransomware groups exploiting their contractual, project-based, and financial transaction systems.

Mid-tier sectors include Law Firms and Organisations (5.26% each), Agriculture, IT, and Education (4.51% each), all of which store valuable operational and proprietary information.

Other affected industries were:

- Energy (3.01%) - critical infrastructure under constant threat.
- Real Estate and Insurance (2.26% each) - sectors with sensitive contractual and financial data.
- Transportation, Federal, and Consumer Services (1.5% each) - vital services often targeted for maximum disruption.
- Healthcare and Media & Internet (0.75% each) - smaller shares this week, but historically high-value targets.

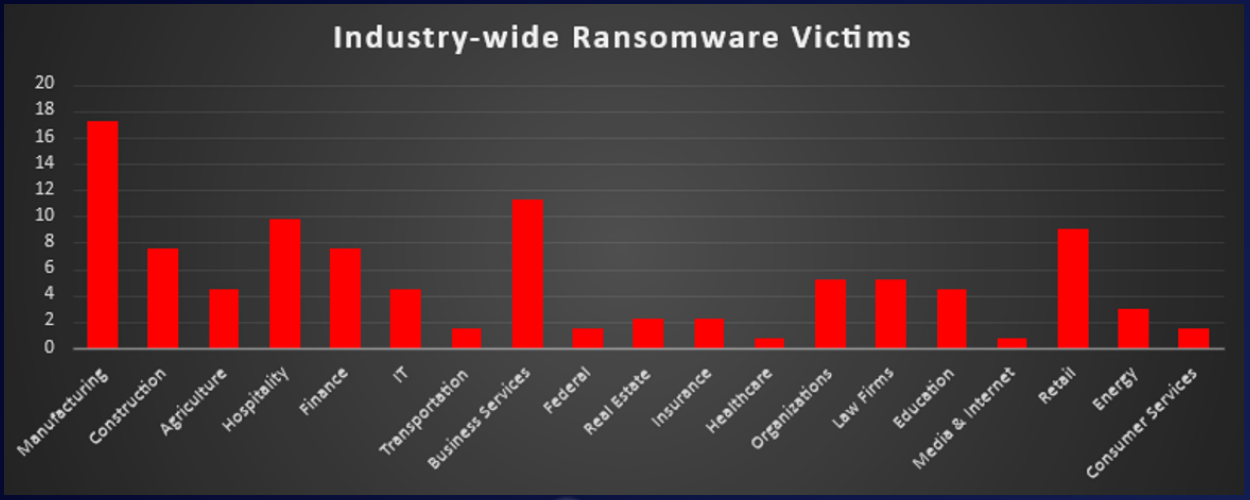


Figure 4: Industry-wide Ransomware Victims