Red Piranha
unified threat management

THREAT INTELLIGENCE REPORT

July 08 - 14, 2025

Report Summary:

- **New Threat Detection Added**
  - NordDragonScan
  - Keitaro TDS

- **Detection Summary**
  - **Threat Protections integrated into the Crystal Eye - 113**
  - **Newly Detected Threats - 8**

The following threats were added to Crystal Eye this week:

1. NordDragonScan

NordDragonScan is a new infostealer created for Windows. The malware leverages HTA files (HTML Application) to deliver malicious payloads to the victim. It also propagates through the network by scanning the local network for reachable and vulnerable systems. Like many other infostealers, it looks for sensitive information such as credentials, user profiles (Chrome, Firefox data), and documents. These are then exfiltrated to an attacker-controlled C2 server.

Threats Protected: 05
Rule Set Type:

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

Class Type: Malware

Kill Chain:

Tactic	Technique ID	Technique Name
Execution	T1059	Command and Scripting Interpreter
Persistence	T1112	Modify Registry
Collection	T1119	Automated Collection
Exfiltration	T1041	Exfiltration Over C2 Channel

2. Keitaro TDS

It is a commercial TDS (Traffic Distribution System) platform that is being abused by threat actors for malvertising. This TDS system is used to bypass content filtering as it is a legitimate service. The TDS redirects users to legitimate sites, but I can also (under certain conditions) send users to malicious download sites. Keitaro is an Estonian company founded in 2009.

Threats Protected: 04
Rule Set Type:

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

Class Type: Malware

Known exploited vulnerabilities (Week 2 July 2025)

Vulnerability	CVSS	Description
Citrix NetScaler ADC and Gateway	9.3 (Critical)	Citrix NetScaler ADC and Gateway contains a vulnerability that can allow a remote unauthenticated attacker to obtain data from memory via an HTTP request. The information obtained through exploitation of this vulnerability can include credentials, session tokens, and other information that can be used to facilitate further attacks.
Synacor Zimbra Collaboration Suite (ZCS)	7.5 (High)	Synacor Zimbra Collaboration Suite (ZCS) contains a vulnerability that can allow a remote unauthenticated attacker to send requests on the server's behalf through the means of a Server-Side Request Forgery vulnerability.
Rails Ruby on Rails	7.5 (High)	Ruby on Rails contains a vulnerability that can allow a remote unauthenticated attacker to read arbitrary files on the webserver.
PHP PHPMailer	9.8 (Critical)	PHPMailer contains a vulnerability that can allow a remote unauthenticated attacker to execute commands on the system.
Looking Glass Multi-Router Looking Glass (MRLG)	9.8 (Critical)	Multi-Router Looking Glass (MRLG) contains a buffer overflow vulnerability that can result in an unauthenticated attacker executing code on the system.

For more information, please visit the **Red Piranha Forum**:
https://forum.redpiranha.net/t/known-exploited-vulnerabilities-catalog-2nd-week-of-july-2025/576

Updated Malware Signatures (Week 2 July 2025)

Threat	Description
NetSupport Rat	NetSupport Rat is a Remote Access Tool capable of avoiding EDR while maintaining persistence and performing data exfiltration. It also has info stealer capabilities.

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

Devman2 dominates the ransomware landscape this week with a staggering 23.63% of all reported attacks, indicating an aggressive and possibly highly automated campaign. This surge may reflect targeted operations against vulnerable infrastructures or the emergence of a large affiliate operation.

PayoutsKing and SafePay each recorded 6.59%, reinforcing their rise in the ransomware-as-a-service (RaaS) scene. Their high activity levels suggest ongoing or recently launched campaigns likely focused on data theft and rapid encryption-based extortion.

Play sits at 5.49%, consistent with its sustained presence across multiple verticals, known for its double extortion strategy and hybrid targeting methods.

Inc Ransom and WorldLeaks both posted 4.95%, further establishing themselves as persistent mid-tier threats leveraging leak sites and pressure tactics.

Qilin and D4rk4rmy followed at 4.4%, signalling active operations, possibly targeting industry-specific victims or exploiting recent vulnerabilities.

Groups such as Kraken, Kawa, Crypto24, and DireWolf (each at 2.75%) continue to conduct smaller yet steady campaigns that contribute to overall ecosystem noise.

DragonForce, Lynx, and Handala were also active this week, each responsible for 2.2–3.3% of attacks, suggesting renewed or sustained low-visibility operations.

A broad array of lower-activity actors—including Arcus Media, Nova, Medusa, RansomedVC2, and Everest (1.65%); Fsociety, SatanLock, Cloak, Sarcoma, Embargo, Cicada3301, TeamXXX (1.1%); and Sinobi, Clop, Rhysida, Blackout, Global, J Group, and LockBit3 (0.55%)—illustrates the long tail of the ransomware landscape. These groups, while individually responsible for fewer attacks, collectively represent the persistent, decentralised threat actors capable of launching targeted or opportunistic operations.

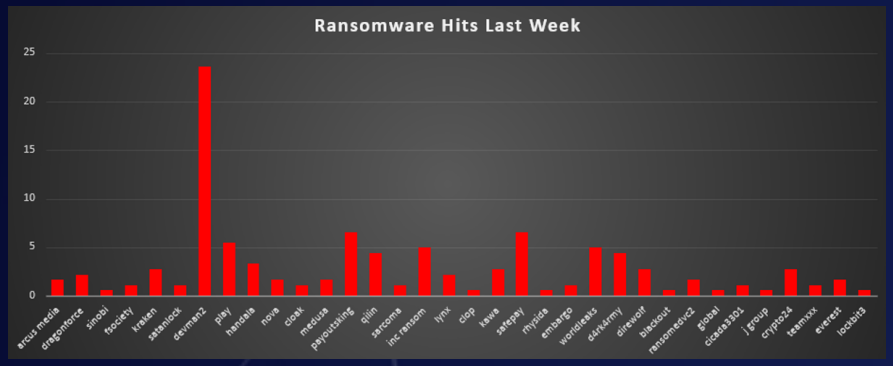


Figure 1: Ransomware Group Hits Last Week

DevMan2 Ransomware

DevMan, a rapidly evolving ransomware group, has continued its silent but strategic expansion across critical global sectors. Initially emerging as a splinter operation of Qilin and APOS threat actors, DevMan now operates a dedicated infrastructure, dark web leak site, and affiliate distribution model.

Recent incidents between July 5–13, 2025, confirm targeted strikes against the manufacturing, professional services, and IT services sectors across North America, Europe, and India. The group's increasing visibility, refined infrastructure, and adoption of Tor-proxyed admin servers underline a pivot toward sustained operations, characteristic of a maturing threat actor.

Detailed TTP

Initial Access

- Phishing campaigns with malicious ZIP attachments
- Exploitation of exposed RDP/VPN services (weak credentials or unpatched Fortinet instances)
- Supply chain entry via compromised IT/consulting partners

Payload Execution

- Custom loader (iamdidy.exe) deployed via PowerShell/WMIC
- Loads Qilin-influenced PE ransomware binary
- Avoids dropping to disk in select variants via reflective injection

File Encryption

- Partial encryption technique observed (segment-based AES-256 with RSA-wrapped session keys)
- Adds a custom extension: .devman2locked
- Drops ransom note: DEV_RESTORE_INFO.txt containing Tor URL and Tox ID for negotiation

Anti-Analysis & Evasion

- Heavy obfuscation via Themida + manual code virtualisation
- Injects into explorer.exe or svchost.exe to avoid EDRs
- Kills EDR and AV services: net stop CrowdStrikeSensorService, taskkill /F /IM SentinelAgent.exe

TTP Mapping to MITRE ATT&CK

Stage	Technique	ID
Initial Access	Phishing Attachment / RDP Exploitation	T1566.001 / T1133
Execution	Command and Script Interpreter	T1059
Persistence	Registry Run Keys / Service Installation	T1547.001
Privilege Escalation	OS Credential Dumping	T1003
Defence Evasion	Disable/Bypass Security Tools	T1562.001
Lateral Movement	SMB Admin Shares + Token Impersonation	T1021.002 / T1134
Exfiltration	Encrypted RClone traffic to Backblaze / Mega	T1567.002
Impact	Data Encryption for Impact	T1486

Infrastructure & IOCs

Tor Leak Site

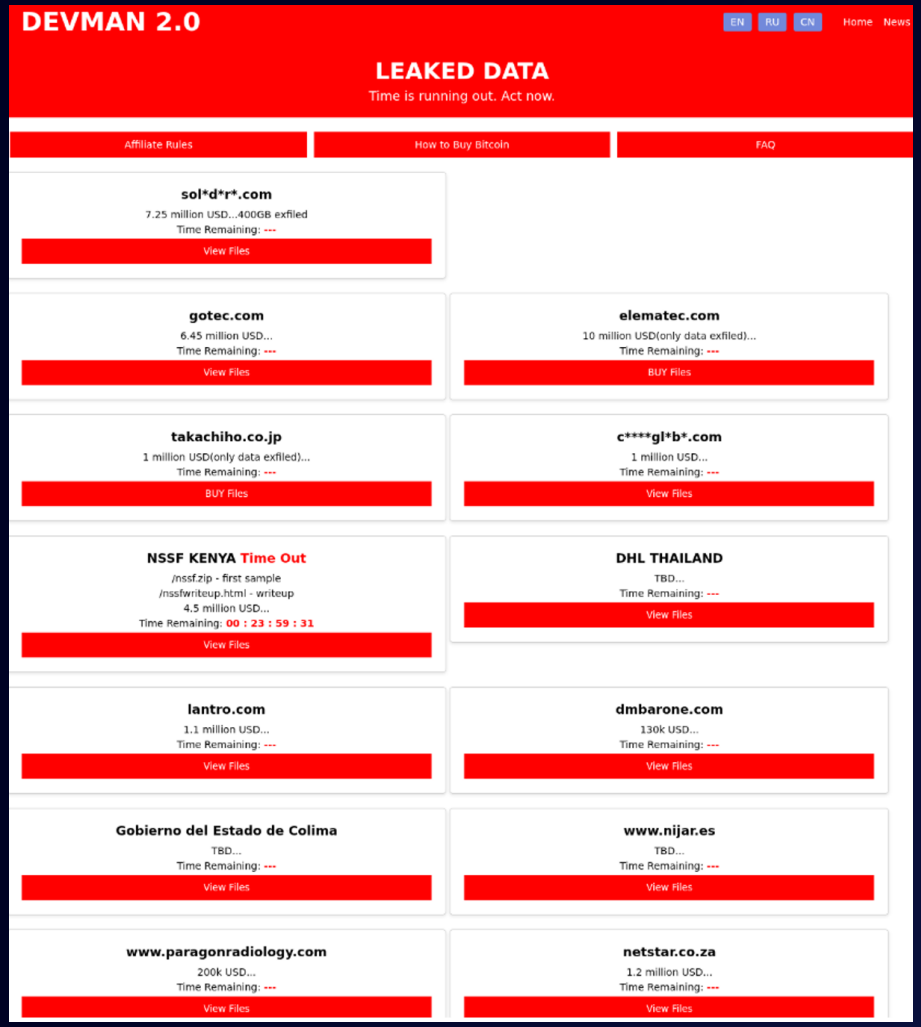
- qljmlmp4psnn3wqskkf3alqquatymo6hntficb4rhq5n76kuogcv7zyd.onion (Active as of July 13 – leaks include manufacturing and IT firms)

C2 / Admin Servers

- 38.132.122.213 - Active C2 Gateway (ASN 9009 – M247 Europe SRL)
- 38.132.122.214 - Admin interface proxy for Tor leak site
- 83.217.209.210 - Legacy DevMan C2 server (deprecated)

Other Artifacts

- Tox ID: 9D97F166730F865F793E2EA07B173C742A6302879DE1B0BBB03817A5A04B572FBD82F984981D
- Ransomware SHA-256:
  - ab2fd6a735c1420987465e7d90e107f2fa1fc0f986f410f3a083c39a24cf28fc



Mitigation Strategy Using CE 5.0

1. Email Protection & User Training
   - Block risky attachments (ZIP, MSI, macro docs) in the Email Protection Module.
   - Simulate vishing/email-bombing via Phishing Simulation.
   - Educate users on IT impersonation and social engineering red flags.

2. Endpoint Hardening & Behaviour Analytics
   - Use HIPS to block execution of tools like iamdidy.exe, QEMU, Rclone, and GoodSync.
   - Detect behavioural anomalies such as net stop, vssadmin delete, or ransom note drops with the Threat Analytics Engine (TAE).

3. Firewall & Network Threat Defence
   - Block known DevMan C2 IPs (38.132.122.213, .214) and Tor traffic via Firewall & Threat Feeds.
   - Add ASN blocks (ASN 9009 & 215826) and monitor outbound .onion activity.

4. Identity & Access Controls
   - Enforce MFA across all RDP, VPN, and administrative access.
   - Audit and remove unauthorised local/domain admin accounts via IAM + AD Watchdog.

5. Backup & Recovery Assurance
   - Configure immutable, versioned backups with CE's Backup module.
   - Regularly test restore scenarios using ransomware simulation.

6. Incident Response & Threat Sharing
   - Enable automated host isolation, YARA scans, and memory triage via CE's SOAR tools.
   - Share IOCs with MISP/OTX and subscribe to Conti/Qilin/APOS threat feeds through the Threat Intelligence Hub.

Worldwide Ransomware Victims

The United States remains the epicentre of global ransomware attacks, accounting for a commanding 45.05% of all reported incidents this week. This reflects the continued targeting of U.S. organisations across healthcare, education, government, and enterprise sectors due to their high-value data and complex infrastructure.

The United Kingdom follows with 4.95%, highlighting its ongoing vulnerability due to its strong digital economy and cross-sector digital dependencies. Italy registered 4.4%, maintaining its place as a high-priority European target, while Australia and South Africa each logged 3.85%, showing elevated threat levels in both the Asia-Pacific and African regions.

Germany, Japan, and Brazil each reported 3.3%, continuing a trend of steady ransomware activity targeting Western and industrialised economies. Singapore (2.75%) and Canada (2.2%) also faced notable threats, underlining their position as major regional hubs and attractive ransomware targets.

A broad mid-tier group—including Spain, Thailand, United Arab Emirates, and China—each registered 1.65%, with other countries like Mexico, South Korea, Kenya, Malaysia, France, and Taiwan all reporting 1.1% of global ransomware activity.

Finally, a diverse range of nations—Indonesia, Vietnam, Sri Lanka, Philippines, Croatia, Jordan, Luxembourg, Greece, Cayman Islands, Poland, India, Switzerland, Peru, New Zealand, Azerbaijan, and Colombia—each logged 0.55%. This long tail illustrates the decentralised and global nature of ransomware, where both large and small economies remain susceptible to opportunistic or targeted attacks.

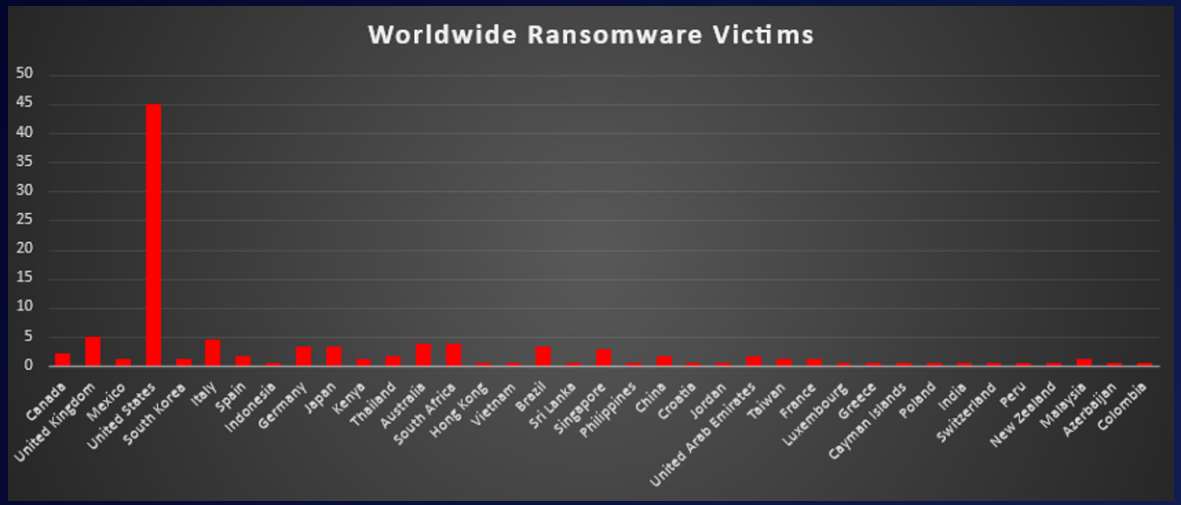


Figure 3: Ransomware Victims Worldwide

Industry-wide Ransomware Victims

Manufacturing continues to be the most heavily impacted sector, accounting for 16.48% of all reported ransomware incidents this week. Its essential role in global supply chains and reliance on legacy systems make it a persistent and lucrative target.

Business Services follows at 14.29%, reflecting attackers' preference for third-party providers who often serve multiple high-value clients and may act as access vectors into larger enterprise ecosystems.

Retail ranks third with 12.64%, driven by its heavy reliance on digital transactions and the rich customer data it processes, ideal for double extortion tactics.

Construction and Hospitality each reported 8.79%, highlighting an increased threat actor focus on operational industries that depend on real-time systems and often lack enterprise-grade defences.

Law Firms saw 5.49%, confirming ongoing targeting of sectors handling confidential, high-stakes data. Both Media & Internet and Organisations followed with 4.4%, showing growing interest in content-driven and non-profit entities.

Sectors such as Education (3.85%), Healthcare (3.3%), Federal, Telecommunications, and Energy (each 2.75%) remain consistent mid-tier targets—each holding critical infrastructure or sensitive data attractive to ransomware operators.

Lower-volume incidents were reported in Finance (2.2%), Consumer Services, Transportation, Insurance (each 1.65%), IT (1.1%), and Agriculture (0.55%). These figures demonstrate that no sector is exempt, and opportunistic targeting continues across a wide range of industries.

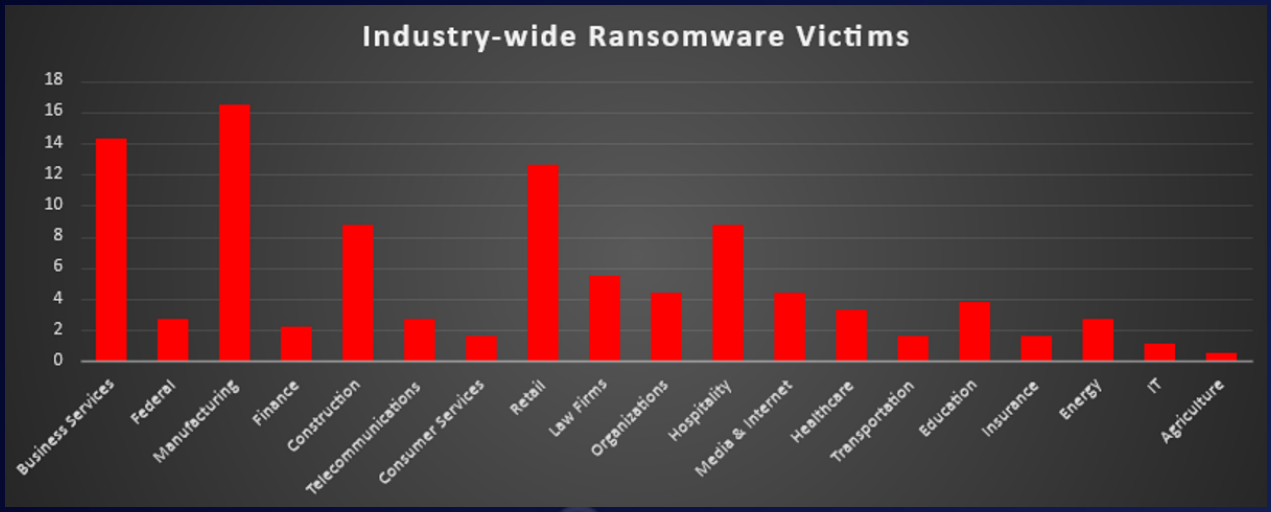


Figure 4: Industry-wide Ransomware Victims