Red Piranha
unified threat management

THREAT INTELLIGENCE REPORT

Apr 22 - 28, 2025

Report Summary:

- **New Threat Detection Added** – 5
  - LandUpdate808
  - Gamaredon APT
  - Zyxel AMG1302-T10B
  - Commvault Pre-Auth RCE
  - BentoML Unauthenticated Remote Command Execution

- **New Threat Protections - 174**

The following threats were added to Crystal Eye this week:

1. LandUpdate808

LandUpdate808 is a malicious downloader campaign that delivers malware disguised as fake browser updates. Victims are lured through compromised websites that display deceptive upgrade notices (e.g., Chrome update prompts). Once clicked, a script or executable loader is dropped, further deploying remote access tools like NetSupport RAT. The campaign uses cookie tracking to avoid reinfection and aggressively rotates file types (JavaScript, EXE, MSIX) to evade detection. Its objective is to establish remote control on victim systems for further exploitation.

Threat Protected: 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: Exploit Kit

Kill Chain:

Tactic	Technique	Description
Initial Access	T1189 – Drive-by Compromise	The victim is tricked into visiting a fake update page and downloading a malicious file.
Execution	T1204.002 – User Execution: Malicious File	The fake installer is executed, triggering malware download and installation.
Discovery	T1082 – System Information Discovery	Collects OS and hardware details for payload tailoring.
Command-and-Control	T1071.001 – Application Layer Protocol: HTTPS	Communicates with attacker-controlled C2 servers over HTTPS.
Impact	T1490 – Inhibit System Recovery	Delivered RAT establishes persistence for ongoing access.

2. Gamaredon APT

Gamaredon (also known as Armageddon or Shuckworm) is a Russian-aligned APT group specialising in cyber-espionage against Ukrainian and governmental organisations. The group uses phishing emails with malicious attachments to implant lightweight but persistent backdoors such as Pterodo. Their tactics include heavy obfuscation, credential harvesting, lateral movement via infected USBs, and fast flux C2 domains. The primary goal is long-term surveillance and confidential data exfiltration.

Threat Protected: 15
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: Domain-c2

Kill Chain:

Tactic	Technique	Description
Initial Access	T1566.001 – Spearphishing Attachment	Weaponised Word documents with malicious macros.
Execution	T1059.005 – Command and Scripting Interpreter: Visual Basic	Macros download and execute payloads via PowerShell.
Persistence	T1547.001 – Registry Run Keys/Startup Folder	Maintains access via autorun registry entries.
Defence Evasion	T1027 – Obfuscated Files or Information	Scripts and binaries are heavily obfuscated.
Discovery	T1082 – System Information Discovery	Collects hostnames, OS versions, and drives information.
Credential Access	T1555 – Credentials from Password Stores	Harvests browser and system stored credentials.
Lateral Movement	T1021.002 – SMB/Windows Admin Shares	Moves laterally via file shares or infected USBs.
Collection	T1119 – Automated Collection	Recursively gathers targeted documents.
Command-and-Control	T1071.001 – C2 over HTTPS	Maintains encrypted communication with attacker C2.
Exfiltration	T1041 – Exfiltration Over C2 Channel	Sends collected documents to remote servers.

3. Zyxel AMG1302-T10B Directory Traversal Attempt (CVE-2025-3577)

A directory traversal vulnerability in Zyxel AMG1302-T10B router web interfaces allow authenticated administrators to access arbitrary files outside the web root. Exploiting this flaw can leak sensitive information such as system credentials, WLAN keys, and internal configuration files. While it requires an admin login to exploit, it drastically expands an attacker's capabilities post-authentication.

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: Web-application-attack
Kill Chain:

Tactic	Technique	Description
Initial Access	T1190 – Exploit Public-Facing Application	Exploits admin access to perform directory traversal.
Discovery	T1083 – File and Directory Discovery	Enumerates file system contents beyond the intended scope.
Credential Access	T1552.001 – Steal Credentials from Config Files	Extracts stored credentials from configuration files.
Impact	T1531 – Device Lockout (Potential)	Possible unauthorised modification or lockout via recovered credentials.

4. Commvault Pre-Auth RCE (CVE-2025-34028)

A critical pre-authentication remote code execution vulnerability in the Commvault Command Center allows unauthenticated attackers to execute arbitrary code by uploading crafted ZIP archives. Exploitation can lead to full compromise of backup servers, exfiltration of sensitive data, or lateral movement within the network. Proof-of-concept exploits are already circulating, making unpatched systems extremely high risk.

Threat Protected: 02
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: Domain-c2
Kill Chain:

Tactic	Technique	Description
Initial Access	T1190 – Exploit Public-Facing Application	Uploads malicious ZIP archive without authentication.
Execution	T1505.003 – Server Software Component: Web Shell	Executes embedded web shell after ZIP unpack.
Persistence	T1053.005 – Scheduled Task/Job (Potential)	Establishes foothold with cron jobs or new user creation.
Privilege Escalation	T1068 – Exploitation for Privilege Escalation	Achieves SYSTEM/root access upon successful code execution.
Command-and-Control	T1071.001 – C2 over HTTPS	Communicates via normal HTTPS traffic to external servers.
Impact	T1485 – Data Destruction	Attackers may wipe or encrypt backup archives.

5. BentoML Unauthenticated Remote Command Execution via Insecure Deserialisation

An insecure deserialisation vulnerability in BentoML's model-serving platform allows remote unauthenticated code execution. By sending a specially crafted serialised object to exposed BentoML API endpoints, attackers can execute arbitrary Python code on the server. This attack can lead to a complete host takeover, manipulation of machine learning models, and pivoting to other internal systems.

Threat Protected: 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	Description
Initial Access	T1190 – Exploit Public-Facing Application	Sends malicious serialised payload to API endpoint.
Execution	T1059.006 – Python Command Execution	Arbitrary Python code execution via deserialisation.
Persistence	T1546.007 – Application Implant	May implant backdoors or modify application code.
Privilege Escalation	T1068 – Exploitation for Privilege Escalation	Gains full host privileges if service runs as root.
Defence Evasion	T1222 – File and Directory Permissions Modification	Clears logs or plants stealthy modules.
Impact	T1499 – Endpoint Denial of Service (Potential)	Disrupts ML operations or manipulates data.

Known exploited vulnerabilities (Week 4 - April 2025)

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

Vulnerability	CVSS	Description
CVE-2025-34028	10.0 (Critical)	Commvault Command Center Innovation Release contains a path traversal vulnerability that allows an unauthenticated remote attacker to upload a ZIP archive which upon extraction can result in Remote Code Execution. This vulnerability affects versions 11.38.0 through 11.38.19 and was fixed in versions 11.38.20 and 11.38.25, no other versions are affected.
CVE-2025-42599	9.8 (High)	Qualitia Active! Mail contains a stack-based buffer overflow vulnerability that can allow an unauthenticated remote attacker to send a specially crafted request that can allow for remote code execution or denial of service. This vulnerability affects versions 6.60.05008561 and earlier and is fixed in version 6.60.06008562. This vulnerability is currently under active exploitation.
CVE-2025-1976	8.6 (High)	Broadcom Brocade Fabric OS contains a code execution vulnerability that allows for an authenticated user with admin privileges to execute commands with full root privileges. This vulnerability affects the IP Address validation functionality of the Fabric OS, and although root access was removed in version 9.1.0, it can be exploited to execute existing Fabric OS commands and can also be used to modify the Fabric OS itself. This affects versions 9.1.0 through 9.1.1.d6 and is known to be actively exploited in the wild. This vulnerability was fixed in Faric OS version 9.1.1d7 and does not affect versions 9.2.0+, Brocade ASCG or Brocade SANnav.

Updated Malware Signatures (Week 4 - April 2025)

Threat	Description
WordPress Social Warfare Plugin Exploit Related Domain	Attackers are exploiting vulnerabilities in outdated versions of the Social Warfare WordPress plugin to gain unauthorised access, execute code, or redirect site traffic. Domains associated with these exploits are often used to host malicious payloads or serve as C2 infrastructure for follow-on attacks. Targeted exploitation may lead to full site compromise or redirection to phishing/malware sites.
PhantomNet C2 Domain	PhantomNet is a stealthy command-and-control (C2) framework used by threat actors to manage compromised machines across global networks. PhantomNet-related domains are leveraged to deliver commands, exfiltrate stolen data, and deploy secondary payloads. Its infrastructure emphasises evasion through frequent domain changes and encrypted communications.
Arkei/Vidar/Mars S tealer Variant Data Exfiltration	Arkei, Vidar, and Mars Stealer are modular infostealers designed to harvest browser credentials, cryptocurrency wallets, and system data. Recent variants rapidly exfiltrate collected information to attacker-controlled servers shortly after infection. The malware prioritises stealth, using encrypted channels and compression techniques to minimise detection during data theft.

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 Groups	Overall Percentage of total attack coverage
Nightspire	3.14%
RALord	2.52%
Devman	3.14%
Sarcoma	1.26%
Qilin	3.14%
Hunters	2.52%
Lockbit3.0	1.26%
RansomHouse	1.26%
Akira	8.18%
Cicada3301	1.89%
Lynx	8.18%
Inc Ransom	1.89%
Medusa	0.63%
Rhysida	1.26%
Play	4.4%
Satanlock	41.51%
Kairos	1.26%
Anubis	0.63%
DragonForce	0.63%
Gunra	1.89%
Silent	2.52%
Crypto24	0.63%
Interlock	1.26%
AzzaSec	1.89%
BlackSuit	1.26%
Nitrogen	1.26%

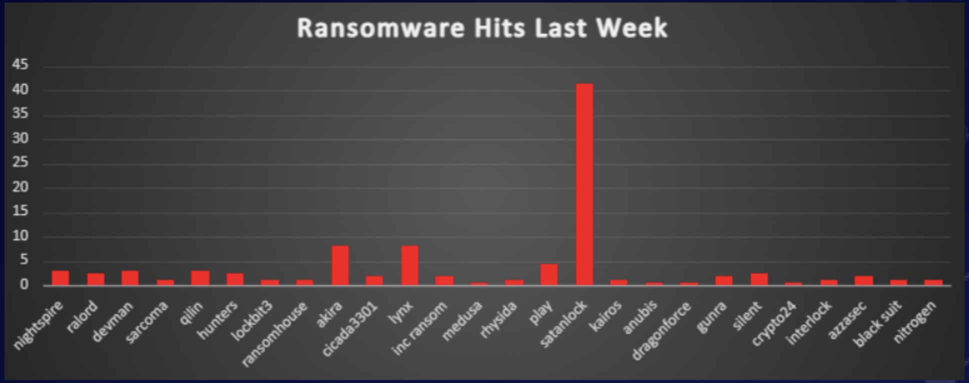

Figure 1: Ransomware Group Hits Last Week

RALord Ransomware Group

RALord is an emerging ransomware threat group identified in 2025. Operating under the Nova RaaS (Ransomware-as-a-Service) model, the group provides affiliates with a ready-made payload and retains 15% of ransom proceeds. RALord's operations revolve around double-extortion tactics — encrypting data and threatening to publish stolen information on their Tor-based leak site. The group primarily uses two ransomware variants: one written in Rust (appending ".RALord") and the Nova-based variant (appending ".nova"). Victims are instructed to contact operators through encrypted messaging services like qTox and Session. Notably, RALord has claimed to exempt schools and non-profits, though it continues to target a wide range of sectors globally.

Detailed TTPs

Initial Access

- Exploits vulnerable public-facing applications (e.g., VPNs, firewalls, RDP)
- May use spear-phishing or stolen credentials

Persistence & Lateral Movement

- Persistence achieved via Hijack Execution Flow (T1574)
- Affiliates use tools like Cobalt Strike for lateral movement

Execution

- Executed manually with administrative privileges
- Rust-based 64-bit payload invokes conhost.exe to run encryption logic

Encryption Behaviour

- Encrypts files with RC4 stream cipher
- Appends ".RALord" or ".nova" extensions
- Drops ransom note (README-.txt) in each folder

Command-and-Control

- No active C2 in binary
- Victims contact operators via:
- Tox ID: 0C8E5B45C57AE244E9C904C5BC74F73306937469D9CEA22541CA69AC162B8D42A20F4C0382AC

•Session ID: 054f55ec93aca9bac362b9d91eff36a7ce451e7caba47c0b2e004ba429f9529c79

Impact

- Encrypts and steals data for extortion
- Causes operational downtime, data breach risks, and reputational damage

Tactic	Technique	ID	Description
Initial Access	Exploit Public-Facing Application	T1190	Exploits VPNs, firewalls, RDP
Execution	Native API	T1106	Runs conhost.exe and invokes encryption logic
Persistence	Hijack Execution Flow	T1574	Registry/DLL hijack for persistence
Privilege Escalation	Hijack Execution Flow	T1574	Used to elevate privileges
Defence Evasion	Impair Defences	T1562	Terminates AV, disables backups
Discovery	Network Share Discovery	T1135	Maps and encrypts shared folders
Lateral Movement	Remote Services (PsExec, SMB)	T1021	Manual propagation via admin tools
Exfiltration	Exfiltration Over C2 Channels	T1041	Data stolen pre-encryption via secure channels
C2	Application Layer Protocol	T1071.001	Tor, Tox, Session for comms
Impact	Data Encrypted for Impact	T1486	Files encrypted using RC4
Impact	Inhibit System Recovery	T1490	Deletes shadow copies, backup services

IOCs

File Extensions

- .RALord
- .nova

File Hashes

- SHA-256: 456B9ADAABAE9F3DCE2207AA71410987F0A571CD8C11F2E7B41468501A863606
- MD5: be15f62d14d1cbe2aecce8396f4c6289

File Names

- README-.txt

C2 Indicators

- Tor Sites:
    - ralord3htj7v2dkavss2hjzviviwgsf4anfdnihn5qcjl6eb5if3cuqd.onion
    - ralordqe33mpufkpsr6zkdatktlu3t2uei4ught3sitxgtzfmqmbsuyd.onion
    - ralordt7gywtkkkkq2suldao6mpibsb7cpjvdfezpzwgltyj2laiuuid.onion

Other Artifacts

- conhost.exe spawns on execution
- Suspicious registry Run entries
- Use of expand.exe during unpacking

Mitigation Strategies

- Apply patches to VPNs, RDP, and firewall appliances
- Implement MFA and strong access controls
- Segment networks and enforce the least privilege
- Deploy EDR and monitor for bulk file encryption patterns
- Backup data securely and keep backups offline
- Disable unnecessary services and script engines
- Train staff on phishing and ransomware awareness
- Monitor for use of Tox, Session, and Tor applications
- Search for ransom notes and encrypted file extensions as early detection indicators

Ransomware Victims Worldwide

A recent analysis of the global ransomware threat landscape highlights that the United States remains the most heavily impacted nation, accounting for a significant 39.62% of all reported ransomware incidents. This continued dominance underscores the country's high-value target status among financially and politically motivated threat actors, driven by its vast digital infrastructure and critical industry base.

Brazil ranks second with 6.29% of incidents, reflecting growing ransomware activity in Latin America and signalling increased attention from cybercriminal groups toward emerging economies. Italy follows with 5.66%, while Canada reports 5.03%, and the United Kingdom comes close behind at 4.4%. These figures suggest a sustained threat presence in both Southern Europe and North America.

Germany experienced 3.77% of global attacks, indicating its continued exposure as a key player within the European industrial and technological landscape. Spain and India each accounted for 2.52%, highlighting a broader targeting of both Western and South Asian nations. Other countries with notable activity include Japan, Australia, Belgium, and Indonesia, each contributing 1.89% of global ransomware cases, reflecting a diversification in threat actor targeting strategies.

Several countries reported 1.26% of incidents each, including Taiwan, China, Mexico, and Colombia, suggesting that cybercriminals are actively expanding their focus to East Asian and Latin American regions. A wide range of countries reported 0.63% of global ransomware cases, including South Africa, Tunisia, Chile, Sweden, Paraguay, Kenya, Macedonia, Zambia, Georgia, Turkey, Malaysia, Slovakia, El Salvador, Norway, Honduras, South Korea, Argentina, Panama, Singapore, Finland, Luxembourg, Saudi Arabia, Zimbabwe, Pakistan, and Portugal. Though individually lower in volume, these instances underscore the global sprawl of ransomware operations.

This widespread and uneven distribution of ransomware activity reinforces the transnational and indiscriminate nature of cybercrime today. It calls for coordinated global defence strategies, including robust intelligence sharing, public-private sector cooperation, and investment in proactive cybersecurity infrastructure to mitigate the evolving ransomware threat across geopolitical and economic boundaries.

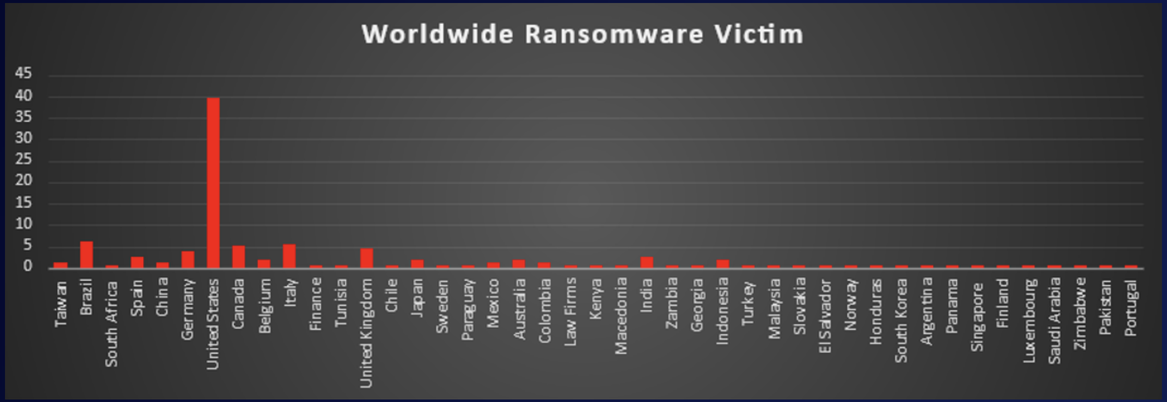

Figure 2: Ransomware Victims Worldwide

Ransomware Victims by Industry

In the most recent industry-specific analysis of ransomware activity, the Business Services sector has emerged as the most targeted, accounting for 12.58% of global incidents. This reflects the growing threat landscape for consulting, outsourcing, and professional service providers, who often serve as gateways to sensitive client data and broader supply chains.

The Retail sector follows closely, representing 11.95% of ransomware cases. The high volume of customer transactions, personal data, and seasonal sales cycles make retail organisations attractive to ransomware operators seeking maximum disruption. Manufacturing ranks third at 10.69%, emphasising the sector's ongoing exposure due to its reliance on industrial control systems and tightly integrated production lines.

Both the Construction and Transportation sectors each reported 8.18% of incidents, indicating that infrastructure-heavy industries remain high-value targets. The operational disruption caused by ransomware in these sectors can have cascading effects across national supply chains and public utilities.

The Healthcare and Finance industries each accounted for 6.29% of cases. These sectors continue to draw attention due to the high-value data they handle—be it patient records or financial transactions—and their critical need for uptime. Meanwhile, the Education and Hospitality sectors, each with 4.4% of incidents, highlight the vulnerability of institutions catering to the public and managing vast stores of personally identifiable information.

Sectors such as Law Firms, Federal, Organisations, and Energy each faced 3.14%–3.77% of the attacks, showcasing how ransomware operators value legal, governmental, and utility-related data. Consumer Services and Insurance industries also reported meaningful levels of activity at 2.52% each, underscoring the continued diversification of targets.

At the lower end of the spectrum, Agriculture, Real Estate, and Telecommunications each accounted for 1.26%, while Media & Internet and IT stood at 1.89%. These figures demonstrate that no industry—regardless of size or public profile—is beyond the reach of ransomware campaigns.

Minerals & Mining reported 0.63%, but even such niche sectors are being probed by cybercriminals, highlighting the opportunistic nature of modern ransomware actors. This industry-wide distribution emphasises the cross-sector impact of ransomware and the urgent need for tailored security strategies, cyber hygiene awareness, and sector-specific resilience plans. Whether dealing with digital infrastructure, client-facing operations, or national interests, every industry must treat ransomware as a critical operational risk in today's interconnected threat environment.

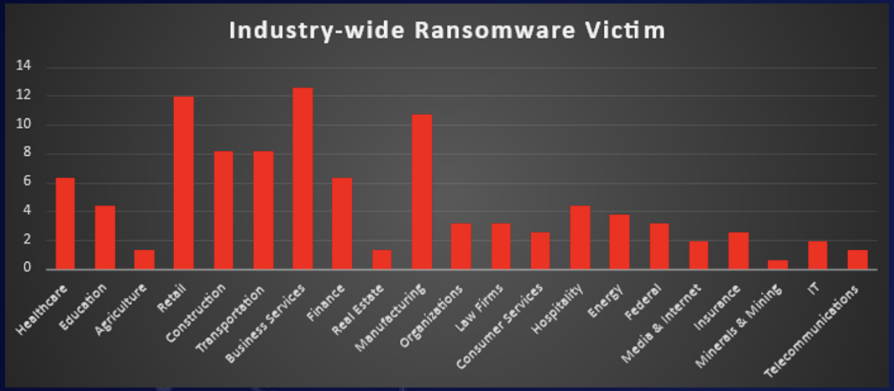

Figure 3: Industry-wide Ransomware Victims