Red Piranha
unified threat management

THREAT INTELLIGENCE REPORT

July 01 - 07, 2025

Report Summary:

- **New Threat Detection Added**
  - BitterAPT
  - Myth Stealer

- **Detection Summary**
  - **Threat Protections integrated into the Crystal Eye - 83**
  - **Newly Detected Threats - 4**

The following threats were added to Crystal Eye this week:

1. BitterAPT

BitterAPT is suspected to be a group originating from South Asia. They have targeted governments, energy and energy organisations. BitterAPT usually infiltrates these organisations through spear phishing. Once the attachment has been opened (.chm (Compiled HTML help file)) it creates a scheduled task to gain persistence on the device. This task will also download a malicious script and execute it.

BitterAPT uses this to collect various file types from the infected PC and send them to their C2 server.

Threats Protected: 07
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
Initial Access	T1566.001	Spearphishing Attachment
Execution	T1053.005	Scheduled Task
Persistence	T1053.005	Scheduled Task
Collection	T1119	Automated Collection
Command-and-Control	T1102.002	Bidirectional Communication
Exfiltration	T1041	Exfiltration Over C2 Channel

2. Myth Stealer

Myth Stealer is a rust based InfoStealer. Myth Stealer has been distributing its infostealer through fake gaming websites. Users believe they are downloading the game but are instead downloading malware that when executed extracts sensitive information such as password and cookies from the installed browsers. The malware is also regularly updated to evade EDR solutions.

Threats Protected: 16
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
Initial Access	T1566	Phishing
Execution	T1204	User Execution
Collection	T1119	Automated Collection

Known exploited vulnerabilities (Week 1 July 2025)

Vulnerability	CVSS	Description
CVE-2025-6554	8.1 (High)	Google Chromium V8 contains a vulnerability that can allow a remote attacker to execute code via a specially crafted HTML page. This vulnerability affects versions prior to 138.0.7204.96 and may affect other web browsers that are based upon Chromium.
CVE-2025-48927 CVE-2025-48928	5.3 (Medium)	TeleMessage TM SGNL contains multiple vulnerabilities that relate to an exposed endpoint containing the Spring Boot Actuator heapdump. The contents of the heap dump contained sensitive information including passwords that were sent over HTTP and was accessible until 2025-05-05.
CVE-2025-6543	9.2 (Critical)	Citrix NetScaler ADC and Gateway contain a buffer overflow vulnerability that can result in an unauthenticated remote attacker gaining access to the system or causing a denial of service. This vulnerability affects versions 14.1 to 14.1-47.46, 13.1 to 13.1-59.19 and 13.1-FIPS and NDcPP to 13.1-37.236.

For more information, please visit the **Red Piranha Forum**:
https://forum.redpiranha.net/t/known-exploited-vulnerabilities-catalog-1st-week-of-july-2025/573

Updated Malware Signatures (Week 1 July 2025)

Threat	Description
UNC_MachoMan	MachoMan or Mach-O is a malware specifically designed for MacOS. It is a designed infostealer, so it looks for sensitive information such as browser content, keychain content and even data stored in notes.

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 dominates the ransomware landscape this week with 21.74% of all reported incidents, highlighting its sustained and aggressive campaigns likely supported by an active affiliate network and evolving toolset.

Kraken follows with 8.70%, marking a significant presence and possibly indicating the launch of a new wave of operations or partnerships with RaaS affiliates.

Akira and Play both recorded 6.52%, reinforcing their reputations as high-volume actors known for targeting professional services, infrastructure-heavy environments, and mid-sized enterprises.

Handala held a solid 5.43%, while Nova, NightSpire, and Inc Ransom each accounted for 4.35%, suggesting consistent targeting from mid-tier operators or smaller, focused campaigns.

DragonForce and SafePay each posted 3.26%, continuing their visibility across multiple regions and sectors.

A variety of actors—including El Dorado, Sarcoma, Space Bears, Everest, and SatanLock—each made up 2.17% of reported activity, contributing to a broad mid-tier threat profile.

Numerous smaller groups, including 3AM, Rhysida, Global, Kawa, Kairos, Daixin, Nitrogen, IMN Crew, and Interlock, each contributed 1.09%, reflecting the fragmented nature of the ransomware ecosystem where dozens of actors contribute to overall threat volume, even if operating below the radar.

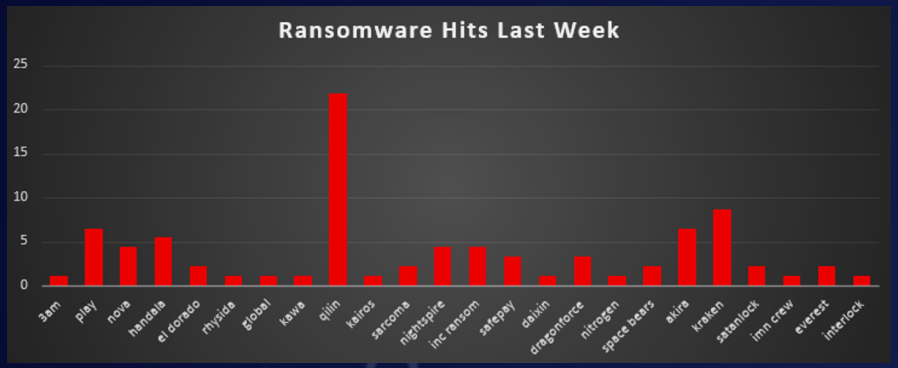


Figure 1: Ransomware Group Hits Last Week

3AM Ransomware

3AM (aka “ThreeAM”) is a Rust-based ransomware strain first observed in September 2023 when Conti affiliates - thwarted in a LockBit deployment - pivoted to this new payload. Since then, 3AM has operated as a lean double-extortion RaaS, linked to former Conti/Royal operators. It leverages highly targeted social-engineering (email-bombing + vishing), novel VM-based loaders, and “living-off-the-land” tradecraft to steal data before encryption. Confirmed victims include a U.S. packaging firm (mid-2023), multiple enterprises through 2024, and a Sophos-protected customer in Q1 2025, where strong MFA and EDR limited impact to a single unprotected server.

Key Facts

- First Seen: September 2023 (fallback after LockBit failure)
- Affiliation: Conti BlackSuit/Royal lineage (shared infrastructure, leaks)
- Leak Site: Tor portal (double-extortion) launched Q4 2023

Detailed TTPs

- Initial Access
  - Email-Bombing + Vishing: Flood inbox - spoofed IT support call - Quick Assist session (no payload on disk)
  - Malicious Archive (ZIP VBS dropper): Delivered via lookalike domain (msquick[.]link), extracting a QEMU VM and VBScript loader
  - Traditional Phishing/RDP: Spear-phish with macro docs or stolen VPN/RDP creds (Storm-1811 pattern)

- Execution & Deployment
  - VM-in-VM Loader: QEMU launches a hidden Windows 7 VM running QDoor backdoor (C2 over port 443)
  - Cobalt Strike & Tooling: Beacon stagers, credential stealers, and WMIC/PowerShell for remote execution

- Persistence
  - Account Manipulation: New local admin (“SupportUser”); domain service-account compromises
  - RMM Agents: XEOXRemote and Syncro installs for stealthy long-term access
  - Backdoors: QDoor binaries (vol.exe, svchost.exe) dropped on servers

- Privilege Escalation
  - Credential Dumping: Likely LSASS dumps (inferred from rapid DA compromise)
  - Token Impersonation/Valid Accounts: Use of stolen domain admin credentials

- Defence Evasion
  - Service/EDR Kill: net stop dozens of AV/backup services; EDR-killer tools
  - Shadow-Copy Deletion: vssadmin delete shadows /all /quiet; wbadmin delete systemstate
  - Sandbox Evasion: Loader requires -k <access_key> and modes (-m local|net) to run

- Discovery & Lateral Movement
  - WMI & Admin Shares: wmic /node:<host> process calls; pushing ransomware via \\host\c$
  - RDP Enablement: Registry and firewall tweaks (d.bat) to allow RDP across network

- Data Exfiltration
  - GoodSync Backblaze B2: 868 GB stolen over 3 days in Q1 2025
  - FTP (Wput): Early case using FTP for exfil in 2023

- Impact
  - Double-Extortion: Files encrypted (.threeamtime), data threatened for leak on Tor site
  - Partial Encryption Mode: -s switch to speed up attacks by encrypting file segments

Stage	Technique	TTP ID
Initial Access	Spearphishing Attachment	T1566.001
	Phone-based Social Engineering (vishing)	(Social Eng.)
Execution	Deploy Container (VM-in-VM)	T1610
	Command and Scripting Interpreter	T1059
Persistence	Create Account: Local	T1136.001
	Remote Access Software (RMM agents)	T1219
Privilege Escalation	OS Credential Dumping	T1003
	Valid Accounts	T1078
Defence Evasion	Disable or Modify Tools	T1562.001
	Inhibit System Recovery (Shadow Copy Delete)	T1490
Discovery	Network Share Discovery	T1135
	System Information Discovery	T1082
Lateral Movement	SMB/Windows Admin Shares	T1021.002
	Remote Services (RDP)	T1021.001
Exfiltration	Exfiltration Over Cloud Storage (Backblaze)	T1567.002
Impact	Data Encrypted for Impact	T1486
	Data Destruction (Optional Wiping)	T1561

Indicators of Compromise (IOCs)

- File Artifacts:
  - Ransomware samples (SHA-256):
    - 307a1217aac33c4b7a9cd923162439c19483e952c2ceb15aa82a98b46ff8942e
    - 079b99f6601f0f6258f4220438de4e175eb4853649c2d34ada72cce6b1702e22
  - Encrypted extension: *.threeamtime
  - Ransom note: RECOVER-FILES.txt (starts with “Hello. ‘3 am’ The time of mysticism…”)

```
========== RECOVER-FILES ==========
Hello. "3 am," the time of mysticism, isn't it?
All your files are encrypted with 3AM's strongest cipher.
Backups and shadow copies have been deleted.
Violation of our terms will result in public data exposure.

To recover your files and negotiate:
1. Open Tor Browser.
2. Navigate to:
   threeamkelxicjsaf2czjyz2lc4q3ngqkxhhlexyfcp2o6raw4rphyad.onion/recovery
3. Enter your access key:
   <your-unique-access-key>

Contact us on Tor or email:
3amnight@inbox.ru
==================================
```

  - VM dropper files:
    - C:\ProgramData\UpdatePackage_exic\Update.vbs
    - …\wexe (QEMU binary)
    - …\Update_excic.acow2 (VM image)
  - Backdoor binaries: vol.exe, svchost.exe in ProgramData

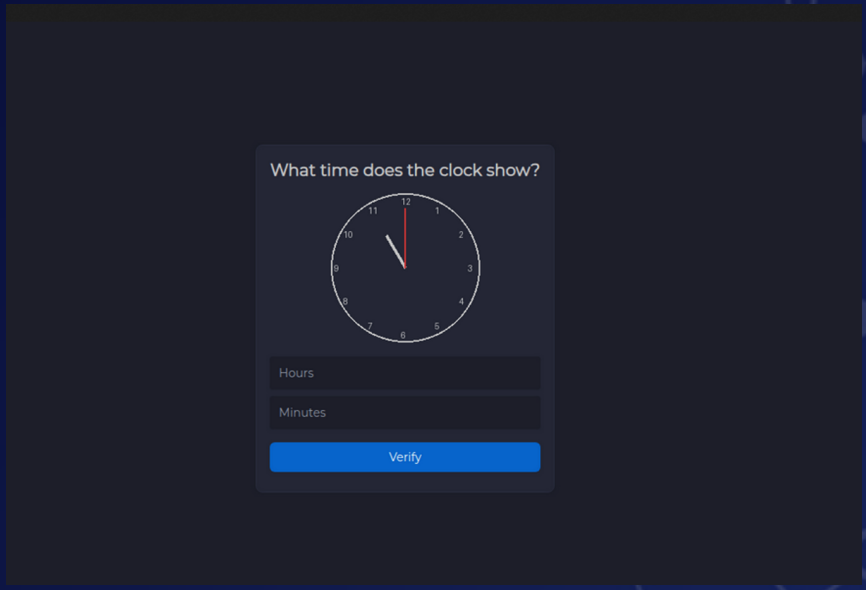
- Registry & Scheduled Tasks:
  - RDP enablement via HKLM\SYSTEM\…\Terminal Server\fDenyTSConnections = 0
  - Scheduled Task WindowsSensor15 uninstalling Duo MFA

- Network Indicators:
  - Backdoor C2 IPs: 88.118.167.239:443, 172.86.121.134
  - Conti-linked servers: 185.202.0.111, 212.18.104.6, 85.159.229.62
  - Phishing domain: msquick.link 1ty.me Google Drive download

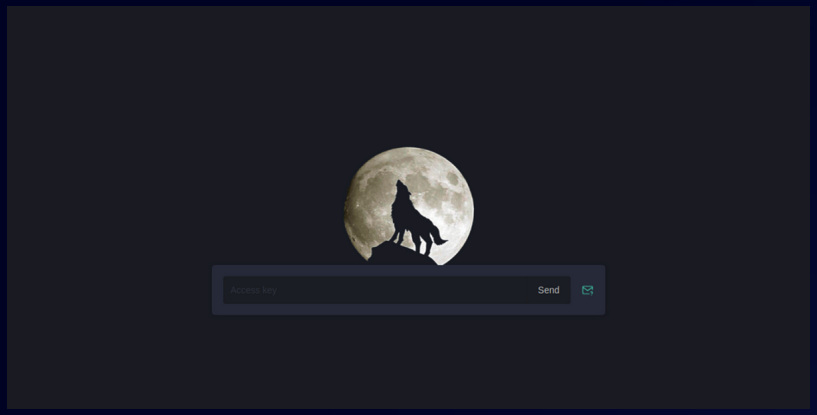
- Tor leak site:

Their Captcha Page.

threeam7fj33rv5twe5ll7gcrp3kkyyt6ez5stssixnuwh4v3csxdwqd.onion



threeamkelxicjsaf2czjyz2lc4q3ngqkxhhlexyfcp2o6raw4rphyad.onion/recovery



o Contact email: 3amnight@inbox.ru, threeam@onionmail.org

Mitigation & Defensive Controls (with CE 5.0)

1. Email Gateway & User Training
   - o Block .msi attachments, macros; simulate email-bombing scenarios
   - o Train staff on vishing red flags (unsolicited IT calls)

2. Endpoint Hardening & Behaviour Analytics
   - o Enforce application control: block QEMU, GoodSync, Wput on endpoints
   - o Detect mass service-stop commands and shadow-copy deletions
   - o Monitor for new RECOVER-FILES.txt drop events

3. Network Filtering & Monitoring
   - o Block/alert on outbound to known C2 IPs and Tor exit/hidden service traffic
   - o Segment network to restrict SMB and RDP access

4. Identity & Access Management
   - o Apply MFA on all remote access (RDP, VPN, admin portals)
   - o Audit and remove unauthorised local/domain admin accounts

5. Backup & Recovery
   - o Maintain immutable, offline backups (3-2-1 rule)
   - o Test restoration procedures regularly

6. Incident Response Orchestration
   - o Automate containment via EDR integration (isolate infected hosts)
   - o Triage via memory captures for key extraction; ingest CE 5.0 alerts into SIEM/XDR

7. Threat Intelligence Sharing
   - o Share new IOCs on OTX/MISP; subscribe to Conti-family intel feeds
   - o Monitor dark-web leak sites for mentions of “3AM” or victim names

Worldwide Ransomware Victims

The United States continues to dominate the global ransomware threat landscape, accounting for 56.52% of all reported victims this week. This consistent trend highlights its vast digital attack surface, high-value enterprise targets, and persistent prioritisation by threat actors across the ransomware ecosystem.

Spain and Canada follow at 5.43% each, reflecting ongoing targeting of critical infrastructure, government, and commercial sectors within these countries.

India and the United Kingdom each recorded 3.26%, underlining their prominence as key victims due to rapidly expanding digital footprints and international business integration.
Countries such as Italy, Australia, Germany, Sweden, Thailand, and Israel each saw 2.17% of incidents, showing that Western Europe and Asia-Pacific regions remain highly targeted zones, especially for mid- to high-tier ransomware operators.

A long tail of nations—including Belgium, Taiwan, Malaysia, Croatia, Portugal, Saudi Arabia, Colombia, Denmark, Panama, Bangladesh, Argentina, and Ecuador—each accounted for 1.09% of global ransomware activity. This reflects the truly global nature of ransomware campaigns, which increasingly affect smaller economies and emerging markets alongside their larger counterparts.

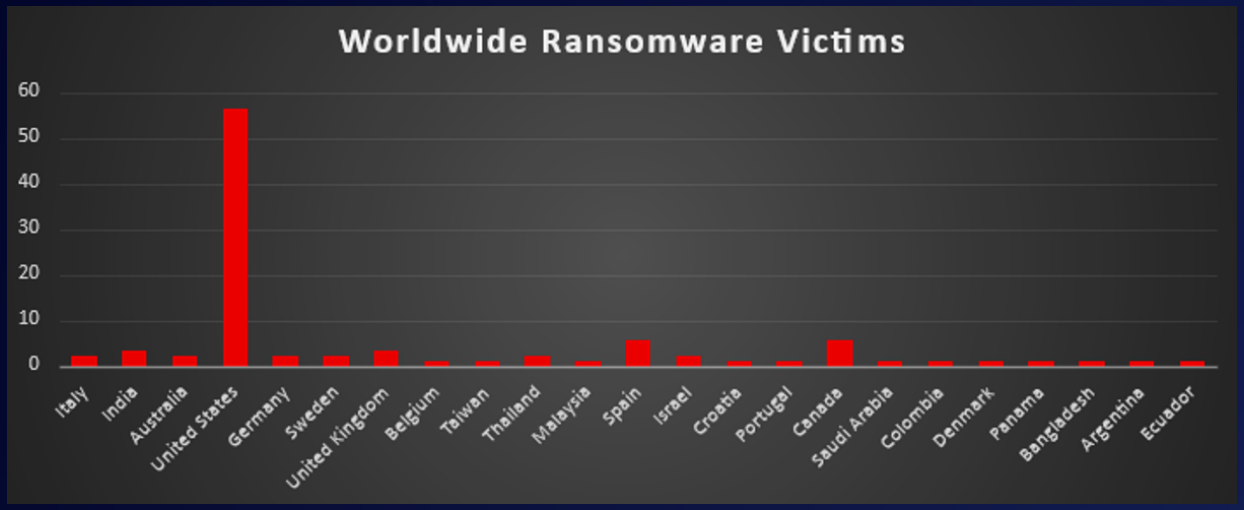


Figure 5: Ransomware Victims Worldwide

Industry-wide Ransomware Victims

Business Services leads the ransomware impact chart this week with 15.22% of all reported incidents. This sector's interconnectedness and access to third-party data make it a high-value target for attackers seeking lateral access to broader networks.

Manufacturing remains a close second at 14.13%, a reflection of its operational criticality and vulnerability due to legacy systems and complex supply chains.

Both Retail and Construction report 13.04% each, emphasising the continuing threat to industries with high transaction volumes, customer data, and often inconsistent cybersecurity practices.

Hospitality registered 10.87%, reflecting ongoing exploitation of the sector's heavy reliance on digital booking, payments, and personal data processing.

Telecommunications saw 5.43%, indicating increased attacker interest in infrastructure providers—especially those enabling internet, mobile, or data services across regions.
Finance and Organisations each accounted for 4.35%, highlighting continued pressure on sectors dealing with sensitive data and mission-critical operations.

Mid-tier targets include Federal, Law Firms, Education (3.26% each), and Transportation, Consumer Services, IT (2.17% each), representing sectors with essential services and varying degrees of cybersecurity maturity.

Sectors like Media & Internet, Insurance, and Energy recorded 1.09% of incidents each—illustrating ransomware's broad reach, even into less frequently targeted industries.

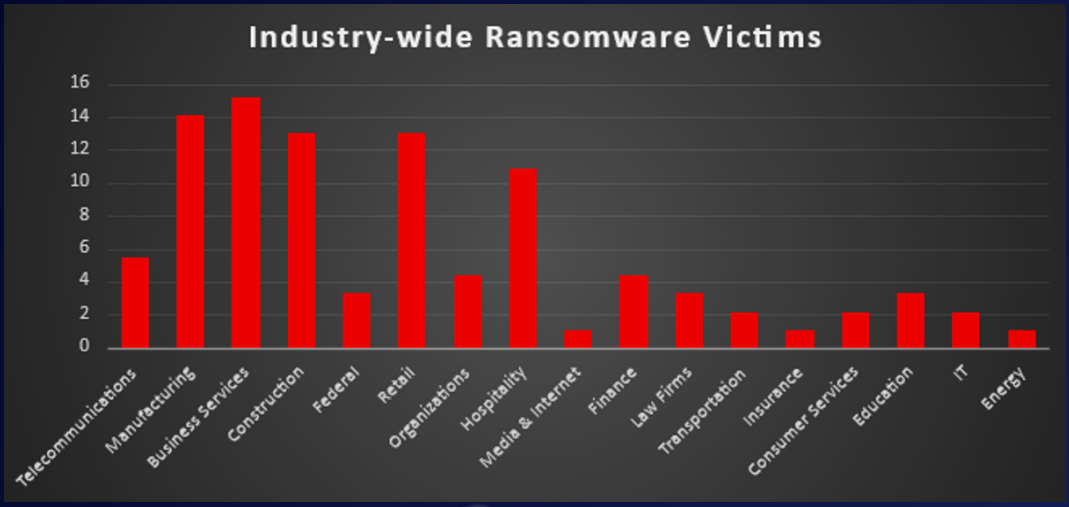


Figure 6: Industry-wide Ransomware Victims