Red Piranha
unified threat management

# THREAT INTELLIGENCE REPORT

July 15 - 21, 2025

# Report Summary:

- **New Threat Detection Added**
  - SillyRAT
  - Phantom Remote

- **Detection Summary**
  - **Threat Protections integrated into the Crystal Eye - 174**
  - **Newly Detected Threats - 38**

# The following threats were added to Crystal Eye this week:

## 1. SillyRat

SillyRAT is an open-source RAT written in pure Python. It is capable of cross-platform infection back to a central C2 server. It is currently built to allow for command execution, keylogging, screenshots, and system dumps.

**Threats Protected: 07**
**Rule Set Type:**

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

**Class Type:** Command-and-Control

**Kill Chain:**

| Tactic | Technique ID | Technique Name |
|---|---|---|
| Enterprise | TA0011 | Command-and-Control |
| Enterprise | T1095 | Non-Application Layer Protocol |

## 2. Phantom Remote

Phantom Remote is a custom built backdoor used by the Russian hacktivist group “Rainbow Hyena”, delivered through phishing. PhantomRemote is a PE32+ DLL file created in C++ collects information about the infected target, loads other executables, and runs commands from the C2 server.

**Threats Protected: 02**
**Rule Set Type:**

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

**Class Type:** Trojan-Activity

**Kill Chain:**

| Tactic | Technique ID | Technique Name |
|---|---|---|
| Enterprise | TA0011 | Command-and-Control |
| Enterprise | T1071 | Application Layer Protocol |

## Known exploited vulnerabilities (Week 3 July 2025)

| Vulnerability | CVSS | Description |
|---|---|---|
| CVE-2025-53770 | 9.8 (Critical) | Microsoft SharePoint Server on-premises contains a deserialisation vulnerability that allows the remote unauthenticated attacker to execute code on the system. |
| CVE-2025-25257 | 9.6 (Critical) | Fortinet FortiWeb contains an SQL Injection vulnerability that can allow a remote unauthenticated attacker to execute SQL commands on the system via a HTTP request, exploitation of this vulnerability can result in the ability to gain access to the system. |
| CVE-2025-47812 | 10 (Critical) | Wing FTP Server contains a vulnerability that can allow a remote unauthenticated attacker to execute code on the system and can result in the ability to execute operating system commands in the context of the FTP service. |

For more information, please visit the **Red Piranha Forum**:
https://forum.redpiranha.net/t/known-exploited-vulnerabilities-catalog-3rd-week-of-july-2025/577

## Updated Malware Signatures (Week 3 July 2025)

| Threat | Description |
|---|---|
| Win32/XWorm | A windows trojan malware |

## 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

Inc Ransom and Qilin lead the ransomware activity this week, each accounting for 13.45% of reported incidents. Their continued dominance suggests persistent campaigns, likely fueled by aggressive affiliate models and wide-scale targeting.

Akira follows with 9.24%, maintaining strong momentum as one of the most active ransomware groups, often focusing on sectors such as healthcare, education, and professional services.

SafePay and DragonForce each logged 6.72% and 5.88%, respectively, while WorldLeaks and Cicada3301 also registered 5.88% and 5.04%, showing consistent targeting mid-tier groups leveraging double extortion and leak site pressure tactics.

BlackByte and Devman2 both accounted for 4.2%, with Play, Nova, Crypto24, and Lynx each contributing 3.36%—indicating smaller, focused campaigns targeting key industries or regions.

NightSpire and Interlock followed at 2.52%, maintaining a presence just below the mainstream radar but still capable of inflicting significant operational damage.

Actors like Everest, PayoutsKing, Gunra, and Nitrogen each recorded 1.68%. While a long tail of groups—including Stormous, Sarcoma, Kairos, Global, Rhysida, Fsociety, Money Message, and Kraken—each made up 0.84% of all activity. These represent opportunistic or highly targeted attacks typical of lower-tier or emerging threat actors.

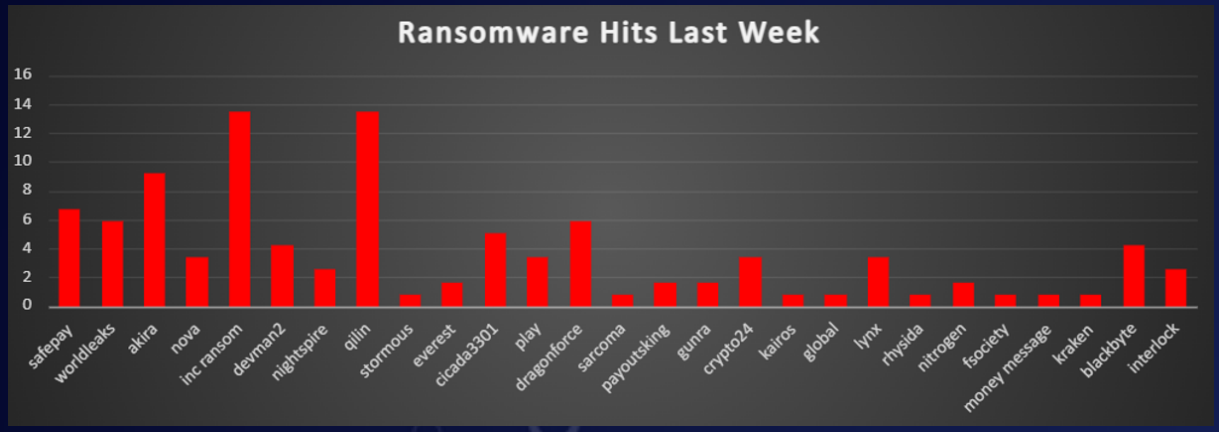



*Figure 1: Ransomware Group Hits Last Week*

# Cicada3301 Ransomware

Cicada3301 is a rapidly evolving Rust-based Ransomware-as-a-Service (RaaS) platform that leverages a double-extortion model: encrypt first, then threaten data leakage via Tor-hosted leak sites. Affiliates gain access to an admin panel where they assemble payloads, choose target platforms (Windows, Linux, ESXi), and interact with victims through built-in chat functions. Between 12 July 2025 and 18 July 2025, Cicada3301 carried out at least five confirmed attacks spanning life sciences, public services, construction, and gaming industries. Key characteristics of this week's activities include opportunistic RDP/phishing access, data exfiltration of up to 2.5 TB, and deployment of segment-based ChaCha20 encryption. Below is a concise breakdown of their Tactics, Techniques & Procedures (TTPs), followed by detailed MITRE mapping, and finally the most up-to-date Infrastructure & IOCs for swift integration into your defences.

Detailed TTPs

Initial Access

- RDP Credential Abuse via brute-forcing or leaked credentials
- Phishing ZIP/ISO Attachments delivering a small Rust loader

Payload Execution

- Reflective Injection of the main encryptor to avoid disk writes
- Service Shutdown commands (net stop CrowdStrikeSensorService) to disable EDRs

File Encryption & Exfiltration

- ChaCha20-Poly1305 for per-file encryption and authentication, suffixing files with random 7-char extensions (e.g., .jtu5s6r)
- Data Exfiltration of sensitive archives (up to 2.5 TB) prior to encryption

Defence Evasion & Persistence

- UPX Packing with custom headers to foil signature detection
- Scheduled Task creation (CicadaPersist) for restart-survival

TTP Mapping to MITRE ATT&CK

| Stage | Technique | ATT&CK ID |
|---|---|---|
| Initial Access | Valid Accounts (RDP) / Phishing | T1078, T1566 |
| Execution | Command and Scripting Interpreter | T1059 |
| Persistence | Scheduled Task | T1053 |
| Privilege Escalation | Service Installation | T1543 |
| Defence Evasion | Obfuscated Files or Information / Disable Security Tools | T1027, T1562 |
| Credential Access | Credential Dumping (memory) | T1003 |
| Lateral Movement | Remote Service Execution (SMB / WMI) | T1021 |
| Collection | Data from Network Shared Drive | T1039 |
| Exfiltration | Exfiltration Over C2 Channel | T1041 |
| Impact | Data Encrypted for Impact | T1486 |

Infrastructure & IOCs

http://cicadabv7vicyvgz5khl7v2x5yygcgow7ryy6yppwmxii4eoobdaztqd.onion/
http://cicadacnft7gcgnveb7wjm6pjpjcjcsugogmlrat7u7pcel3iwb7bhyd.onion/
http://cicadafhqpjwm2sblkfbuwn7sglbibuejr3m7fildpqpjv3hghlhb4id.onion/
http://zf6bl4dczp5z7uaba2lhm5wrhrpflwvzsx2nhf7zyf63tpsfzc54tbad.onion/
http://hgannromwuui7n2jvphpteposc3gioqkuo2ncb6fzopasgcq7ixcjeqd.onion/
http://osd6tsgegts2xaqo3o2hrpqatwlslqfyc3msvyksad4iucauif3oqqad.onion/
http://uds75egfqi7mfpxckf2un742qsj6rh3kfrydqaldwgkrqp2a37lk6fyd.onion/
http://wuyfbttjjzsmr5ghl5hoi75ytse3bwrqgk63c6guv3lhw7hwtxbgveid.onion/
http://bmfyfxl74qb6rsukgwymv7e22ua4uvhszsamqwx7jmj57qkamxwlhbid.onion/
http://yaoehn32c2s5pwsuzhaa4lsu2a4seycpwyvn5gfz3bn4i74t2jo3frad.onion/
http://5atqn4dwosjauijzj445mm7t6bqrcvzlzcylpmpnx243jxvlimyb6aid.onion/

File servers

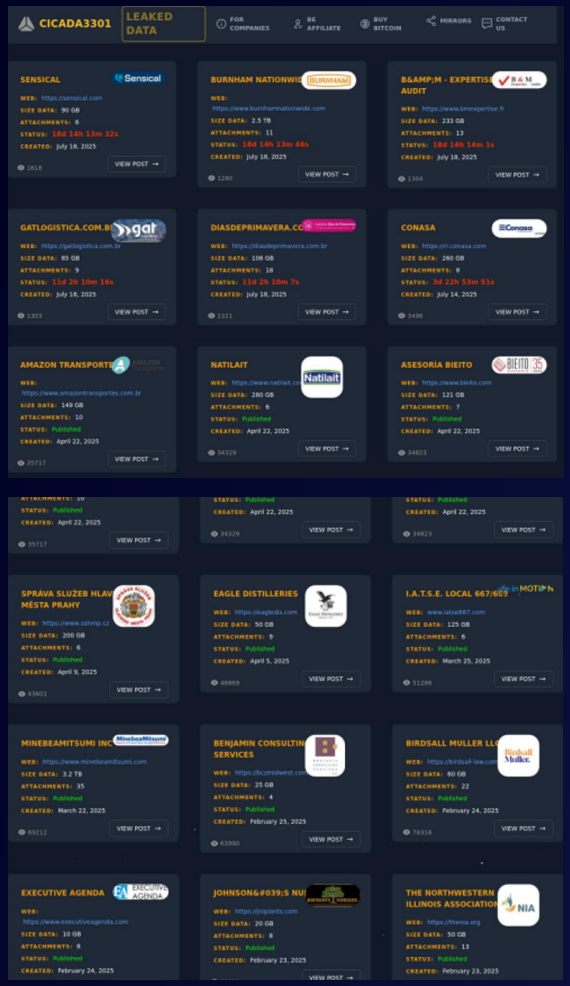
http://ruzislhpcuvfzw3t2xfqu7gog3gs5j2u65ysaq3ybqkzri3hjddaqgad.onion/
http://leakshrlgof456tiw4ww5moiqlnrcork7q7r3cjgmsvex6zazpluhlad.onion/ec49pw6bi
8xc2mk3j89kkiaa4ikdrf4wnq2nas4cseciagbw5pq63th7cqajky3c/

Chat servers

http://cicadaxousmk6nbntd3ucxefmfgt2drhtfdvh7gmdeh3ttvudam6f2ad.onion

Malware Sample Hashes

- SHA-256: 20fc3cf1afcad9e6f19e9abebfc9daf374909801d874c3d276b913f12d6230ec (Windows loader)
- SHA-256: ebffc9ced2dba66db9aae02c7ccd2759a36c5167df5cd4adb151b20e7eab173c (ESXi build)




Mitigation Strategy Using CE 5.0

1. Email Protection & User Training
   - Block ZIP, ISO, and macro-laced files via the Email Protection Module
   - Run phishing simulations and educate users on impersonation tactics

2. Endpoint Hardening & Behaviour Analytics
   - Use HIPS to block tools like psexec0.exe and batch scripts
   - Detect ransom behaviors (net stop, vssadmin, ransom note drops) via TAE

3. Firewall & Network Threat Defence
   - Block Cicada3301 C2 IPs and Tor traffic via Threat Feeds
   - Monitor .onion activity and apply ASN blocks for attacker infrastructure

4. Identity & Access Controls
   - Enforce MFA for all remote/admin access
   - Audit and remove unnecessary admin accounts with IAM + AD Watchdog

5. Backup & Recovery Assurance
   - Use CE's Backup module for immutable, versioned backups
   - Regularly test restore scenarios with ransomware simulations

## Worldwide Ransomware Victims

The United States remains the most heavily impacted nation, accounting for 47.9% of all reported ransomware attacks this week. Its massive digital ecosystem and concentration of high-value enterprises make it the top target for threat actors globally.

Canada and Australia each reported 5.88%, maintaining their positions as key targets in the North American and Asia-Pacific regions. The United Kingdom follows with 5.04%, with frequent targeting of its financial, legal, and public service sectors.

Italy and Spain saw 4.2% and 3.36% respectively, reinforcing the ongoing focus on Western European countries.

Germany and Brazil each reported 2.52%, while a cluster of nations, including Romania, Singapore, New Zealand, France, Switzerland, and Luxembourg, registered 1.68%. These figures reflect a distributed threat landscape with growing geographical diversity in targeting.

A long tail of countries, Lebanon, Uganda, Algeria, United Arab Emirates, Namibia, Kenya, India, Egypt, South Africa, Argentina, Belgium, Croatia, Ireland, Guatemala, and Indonesia, each accounted for 0.84% of global ransomware incidents. These figures demonstrate that ransomware operators are targeting both highly digitised economies and developing regions, exploiting vulnerabilities wherever possible.

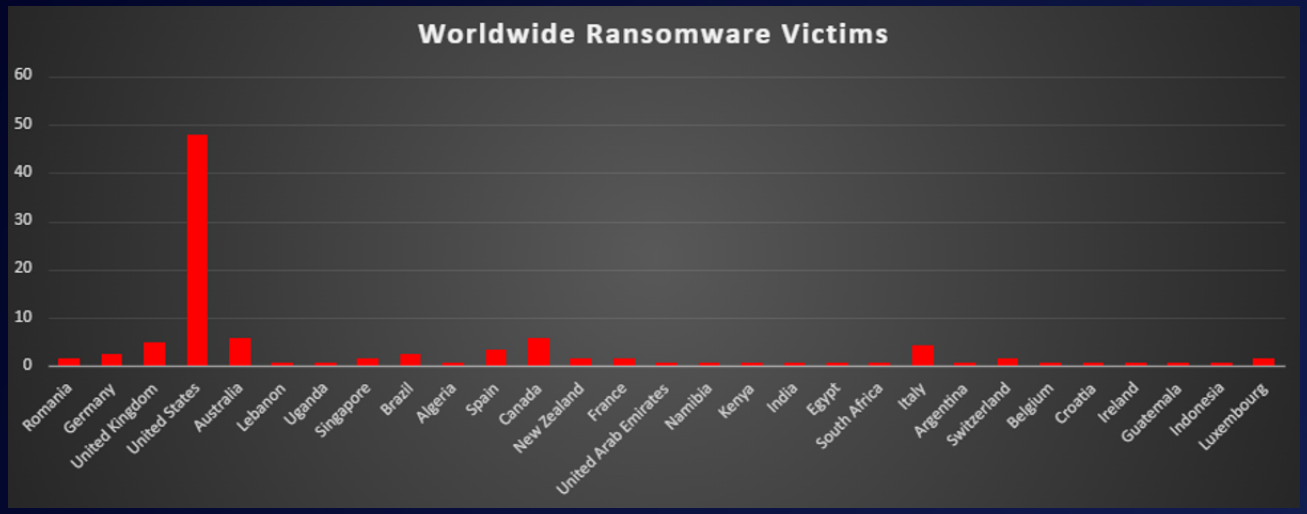



*Figure 4: Ransomware Victims Worldwide*

## Industry-wide Ransomware Victims

Business Services and Manufacturing share the top spot this week, each accounting for 18.49% of ransomware incidents. These sectors continue to be prime targets due to their critical roles in supply chains, vendor ecosystems, and the valuable data they process.

Retail follows with 11.76%, consistently targeted for its customer data, payment infrastructure, and widespread digital operations.

Law Firms and Construction both reported 8.4%, reflecting continued interest in sectors handling sensitive intellectual property, project-based finances, and often fragmented cybersecurity controls.

Education contributed 7.56%, reaffirming its vulnerability due to open access environments, aging infrastructure, and limited security budgets.

Federal organisations accounted for 4.2%, indicating sustained targeting of public institutions, often as part of politically or financially motivated campaigns.

Mid-tier sectors include Hospitality (3.36%), and a group of industries, Finance, Consumer Services, Real Estate, and Organisations, each at 2.52%, representing core service and economic sectors increasingly in the crosshairs of ransomware operators.

A smaller but notable share of incidents impacted Insurance, Healthcare, Telecommunications, and Energy (each at 1.68%), followed by Transportation, Media & Internet, and IT (each at 0.84%). These figures emphasise that ransomware is far from industry-specific; threat actors continue to exploit vulnerabilities wherever digital transformation outpaces security maturity.

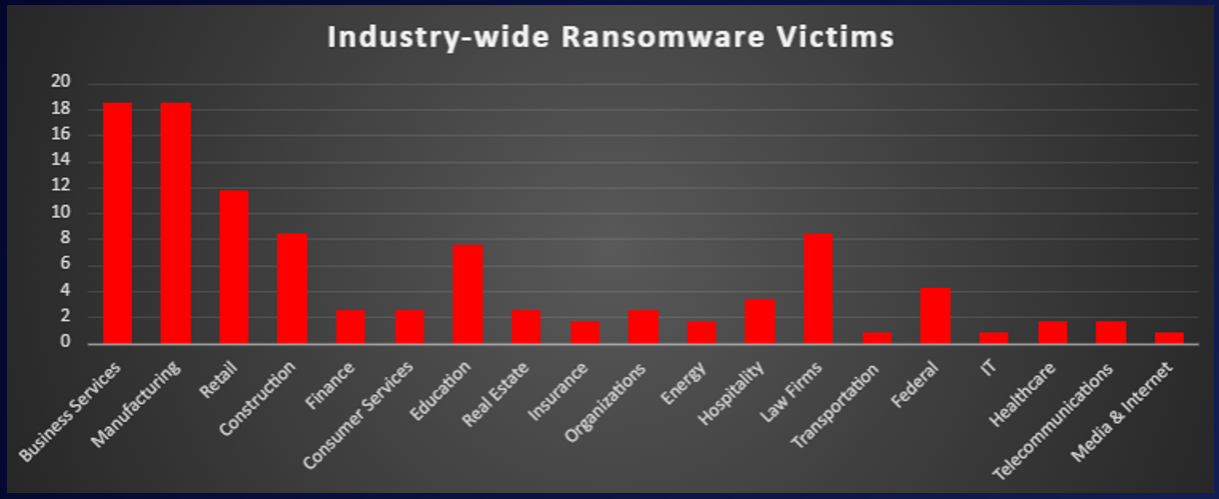



*Figure 5: Industry-wide Ransomware Victims*