Red Piranha
unified threat management

THREAT INTELLIGENCE REPORT

Oct 7 - 13, 2025

Report Summary:

- **New Threat Detection Added**
  - Temperedchef
- **Detection Summary**
  - **Threat Protections integrated into the Crystal Eye - 109**
  - **Newly Detected Threats - 3**

The following threats were added to Crystal Eye this week:

1. TemperedChef

TemperedChef is part of a malware campaign primarily targeting European organisations. The campaign uses an advertising campaign and a malware-infected PDF Editor. The PDF Editor installer utilises a technique that makes it look and feel legitimate; it contains 'auto updates' and even an EULA that the user must agree to. Once installed, the application sets an autorun to maintain persistence.

The PDF Editor application is an election application, so it has full access to executed bundled JavaScript. The JavaScript that it executes is used for the malicious activity. The activity remains dormant to get installed on as many devices as possible, before it begins to steal browser credentials and upload them to an attacker-controlled server (Remained dormant for around ~3-4 months).

Threats Protected: 4
Class Type: Trojan-Activity
Rule Set Type:

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

Kill Chain:

Tactic	Technique ID	Technique Name
Execution	T1059.007	Command and Scripting Interpreter: JavaScript
Persistence	T1547.001	Registry Run Keys / Startup Folder
Collection	T1119	Automated Collection
Exfiltration	T1020	Automated Exfiltration

Current Threat Summary

Known exploited vulnerabilities (Week 2 October 2025)

Vulnerability	CVSS	Description
CVE-2021-43798	7.5	Grafana contains a path traversal vulnerability that can allow an unauthenticated remote attacker to read files on the system, this vulnerability affects versions 8.0.0-beta1 to 8.3.0 and was fixed in version 8.3.1. Exploitation of this vulnerability may allow an attacker to compromise the system further.
CVE-2025-27915	5.4	Synacor Zimbra Collaboration Suite (ZCS) contains a cross-site scripting vulnerability within the Classic Web Client that can allow a remote attacker to execute code when accessing an email containing a malicious calendar invitation file (.ics). This vulnerability is due to insufficient sanitisation of HTML content when the client parses the ICS file, and as it's executed within the context of the Zimbra session it can enable unauthorised actions being performed within the account such as reading emails, contacts and changing settings including email forwarding.
CVE-2021-22555	8.3	Linux Kernel contains a heap out-of-bounds write vulnerability that can allow an attacker with local access to a system to escalate privileges to root. This vulnerability is made possible due to a use-after-free vulnerability within the Netfilter component of the Linux Kernel.
CVE-2010-3962	8.1	Microsoft Internet Explorer contains a use-after-free vulnerability that can result in an unauthorised remote attacker to execute code on a system upon accessing a webpage containing malicious code.
CVE-2021-43226	7.8	Microsoft Windows Common Log File System Driver contains a vulnerability that can allow a local attacker to escalate privileges on the system.
CVE-2013-3918	8.8	Microsoft Windows contains an out-of-bound write vulnerability that can allow a remote attacker to execute code on the system upon visiting a webpage containing malicious code. This vulnerability affects the ActiveX InformationCardSigninHelper component used by Internet Explorer.
CVE-2011-3402	8.8	Microsoft Windows Kernel contains a vulnerability within the TrueType font parsing engine component in win32k.sys that can allow a remote attacker to execute arbitrary code on a system upon visiting a malicious webpage or opening a word document. This vulnerability is due to improper validation of a specially crafted TrueType font file and can enable execution of code in kernel-mode or with SYSTEM level privileges.
CVE-2010-3765	9.8	Multiple Mozilla Products Firefox, SeaMonkey and Thunderbird contain a memory corruption vulnerability that can allow a remote attacker to execute arbitrary code upon visiting a specially crafted webpage.
CVE-2025-61882	9.8	Oracle E-Business Suite contains several vulnerabilities that when chained together can result in an unauthenticated remote attacker to gain access to the system, this vulnerability affects versions 12.2.3 through to 12.2.14.

For more information, please visit the **Red Piranha Forum**:
https://forum.redpiranha.net/t/known-exploited-vulnerabilities-catalog-2nd-week-of-october-2025/605

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 Hits Last Week

KillSec3 dominated this week's activity, responsible for a staggering 50% of all reported ransomware incidents. This overwhelming presence signals either a large, coordinated campaign or a surge in disclosures tied to its affiliates, making it the most significant actor by far.

Trailing behind, Qilin (7.14%), Akira (5.65%), and Sinobi (5.36%) stood out as major contributors, each sustaining visible operations across multiple sectors. Together, these groups represented nearly a fifth of global incidents, highlighting a broadening ecosystem of persistent mid-tier players.

Other groups with notable activity included DevMan2 (2.08%), Brotherhood (2.38%), Safepay (2.38%), and Toufan (2.98%). Scattered Lapsus$ Hunters (2.98%) also maintained relevance, showing the continued activity of data-leak-focused groups.

Clusters of activity in the 1–2% range came from Inc Ransom, DragonForce, Chaos, WorldLeaks, Radiant Group, Kryptos, Beast, and Nova, underscoring the mid-level presence of diverse operators leveraging opportunistic campaigns.

A long tail of smaller groups contributed 0.3–0.6% each, including The Gentlemen, Play, Kairos, Anubis, Space Bears, Leaknet, LeakedData, Sarcoma, PayoutsKing, Interlock, Radar, Tengu, Lynx, Nasir Security, NullBulge, MyData, BlackShrantac, Black Nevas, and Securotrop. While individually minor, their combined activity reflects the fragmented nature of the ransomware ecosystem, where many actors run lower-volume but persistent operations.

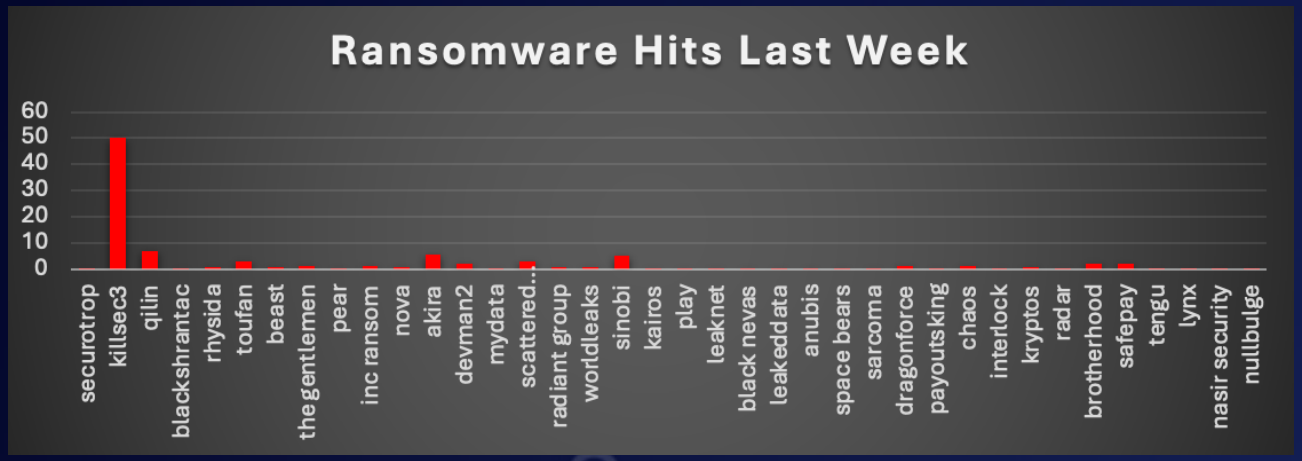

Figure 1: Ransomware Group Hits Last Week

KillSec3 Ransomware

KillSec3 is a financially motivated RaaS born from earlier hacktivist tooling. Its affiliates typically:

- Gain access via phishing, RDP, exposed services and supply-chain vectors.
- Perform credential theft / lateral movement, exfiltrate sensitive data (examples: large Brazilian healthcare dataset via open S3), then encrypt files or directly extort using leaked data.
- Use tor-hosted leak portals and Telegram channels for negotiations and public shaming.
- Employ Windows Defender disabling, shadow-copy deletion, scheduled tasks, and possible LSASS/registry hive access for credential harvesting.

Detailed TTPs

Initial access

- Phishing (malicious attachments / credential harvest). Detect: Email gateway flags for macro/HTML attachments, anomalous logins after email click.
- RDP brute-force / exposed RDP / unpatched remote services.

Detect: Failed login spike, atypical source IPs, new external connections to RDP ports.

Execution

- Dropper runs (EXE/installer) that invokes Windows Crypto APIs (bcrypt) to perform file encryption.

Detect: New process spawning patterns invoking encryption routines, unusual file I/O patterns.

Persistence

- Registry Run keys, scheduled tasks, service creation.

Detect: New Run keys under HKLM/HKCU, Event ID 4698/4702 for scheduled tasks.

Privilege escalation

- Use of valid accounts, credential reuse and local privilege escalation via tools.

Detect: Unusual admin account use, new accounts created, LSASS memory access.

Defence evasion

- Disable Defender real-time (registry change), stop/kill AV services, delete shadow copies (vssadmin / diskshadow / wmic).

Detect: Registry write to HKLM\SOFTWARE\Policies\Microsoft\Windows Defender\Real-Time Protection\DisableRealtimeMonitoring, execution of vssadmin/diskshadow, process termination of security services.

Credential access

- Exporting SAM/SEC hives, LSASS memory harvest (mimikatz or similar), dumping saved credentials.

Detect: Suspicious reg.exe saves, lsass dump creation, use of debugging tools.

Discovery / Lateral movement

- SMB/Windows admin shares, RDP pivoting, use of WMI/PSExec.

Detect: New SMB sessions, administrative RPC calls, and lateral movement scanning.

Collection & Exfiltration

- Bulk staging to cloud storage (S3 misconfigurations observed), exfil over Tor/C2, and use of legitimate cloud APIs to export large volumes.

Detect: Large outbound uploads to cloud endpoints, unusual S3 PUT activity, Tor egress.

Impact

- File encryption (.killsec or randomised extension), ransom note drop (README.txt, !KillSec_Instructions.txt), and publication of stolen data on Tor leak sites.

Detect: Sudden file extension changes, presence of ransom notes, outbound connections to Tor hidden services.

MITRE ATT&CK Mapping

Tactic	Technique (ID)	Observed behaviour / detection hint
Initial Access	Phishing (T1566)	Malicious emails with attachments/links
Initial Access	External Remote Services / RDP (T1021)	Brute force, exposed RDP sessions
Execution	Command/Script (T1059)	PowerShell/cmd to run payload
Persistence	Scheduled Task (T1053.005) / Registry Run Keys (T1547.001)	New scheduled tasks / Run entries
Priv Esc	Valid Accounts (T1078)	Compromised credentials used for escalation
Credential Access	OS Credential Dumping (T1003)	LSASS/reg hive dumps
Defence Evasion	Disable Defender (T1562.001) / Delete Shadow Copies (T1490)	Registry writes / vssadmin execution
Exfiltration	Exfil over C2 (T1041) / Transfer to Cloud Storage (T1567.002)	Large uploads to S3 / Tor egress
Impact	Data Encrypted (T1486) / Data Destruction (T1485)	Mass encryption; shadow copy deletion

Indicators of Compromise (IOCs)

Hashes (examples)

- SHA256: 8cee3ec87a5728be17f838f526d7ef3a842ce8956fe101ed247a5eb1494c579d
- SHA1: e014c9e5f712775e771c7f36d2a580d8d290c9ad
- MD5: 12b818950d749c378aabd81a0bac9742

Domains / Tor / C2

- Tor leak portal (example): ks5424y3wpr5zlug5c7i6svvxweinhbdcqcfnptkfcutrncfazzgz5id.onion
- Tor file server: xo4o2o2ezgydykywn6zkyqx7toio6z5rzvmjyakgtgkk22vv7223jmqd.onion
- Known IPs observed as Tor/C2 endpoints: 82.147.84.98, 77.91.77.187, 93.123.39.65
- Telegram negotiation channel (example): t.me/killsecc

File/artifact names

- Ransom notes: README.txt, !KillSec_Instructions.txt
- Encrypted file extensions: .killsec or randomised alphanumeric extension.

Registry & commands

- Registry: HKLM\SOFTWARE\Policies\Microsoft\Windows Defender\Real-Time Protection\DisableRealtimeMonitoring = 1
- Shadow deletion commands: vssadmin.exe delete shadows /all /quiet, diskshadow.exe, wmic shadowcopy delete
- Presence of unexpected Run keys or scheduled tasks invoking unknown binaries.

Detection & Mitigation

- Alert on registry writes to Defender real-time keys where the source process is non-trusted.
- Detect vssadmin / diskshadow / wmic shadowcopy delete executed by non-admin scheduled tasks or unfamiliar processes.
- Notify on mass file rename patterns matching encryption I/O (high file entropy writes across many file types).
- Monitor for large outbound uploads to cloud storage APIs (S3/Drive) from unusual hosts.
- Flag outbound connections to Tor exit nodes /.onion resolvers or known Tor IPs.
- Correlate new scheduled tasks / Run keys with suspicious parent processes.

Immediate containment

- Isolate infected hosts from network segmentation (air-gapped if possible).
- Block known Tor/C2 IPs at the perimeter and stop egress to public cloud endpoints until validated.
- Revoke exposed credentials and rotate service/service-account keys (especially for cloud storage).
- Enforce phishing-resistant MFA, disable legacy auth, and rotate admin credentials.
- Block/monitor RDP on internet-facing hosts; require VPN and conditional access.
- Implement EDR policies to prevent process injection and LSASS dumping; enable tamper protection.
- Enforce least privilege for cloud buckets and enable MFA delete / S3 block public access.

Worldwide Ransomware Victims

The United States dominated ransomware victimisation this week, accounting for 52.38% of global incidents. This concentration reflects attackers' continued preference for US-based targets due to their large digital ecosystems, economic value, and operational pressure points.

India (5.95%) and Canada (5.65%) followed as the most impacted outside the U.S., underscoring their growing presence in the ransomware threat landscape. The United Kingdom also featured prominently with 4.46%, showing continued targeting of European financial, legal, and service-based industries.

Australia (2.98%), France (2.38%), and the United Arab Emirates (2.38%) formed the next tier, highlighting adversaries' sustained campaigns across both Western economies and Middle Eastern hubs. Germany (2.08%) added further evidence of consistent ransomware impact in Europe.

A broad set of mid-level activity was seen across Italy (1.19%), Brazil (1.79%), Denmark (0.89%), Japan (0.89%), China (0.89%), and Mexico (0.89%), with each country hosting multiple reported victims. These attacks illustrate ransomware's spread into both advanced industrial economies and rapidly digitising emerging markets.

Smaller but noteworthy cases (0.3–0.6% each) were distributed widely across Argentina, Peru, the Philippines, Israel, Romania, Spain, Thailand, Venezuela, Botswana, Mongolia, and Indonesia, among others. Countries such as Zimbabwe, South Africa, Vietnam, Croatia, Austria, Chile, Nigeria, Morocco, Iraq, Malaysia, and New Zealand also reported isolated incidents, underscoring ransomware's truly global reach.

This geographic spread reinforces a dual trend: ransomware remains heavily concentrated in core economies (U.S., India, Canada, U.K., Australia), while opportunistic attacks continue to strike globally, ensuring no nation is immune from its impact.

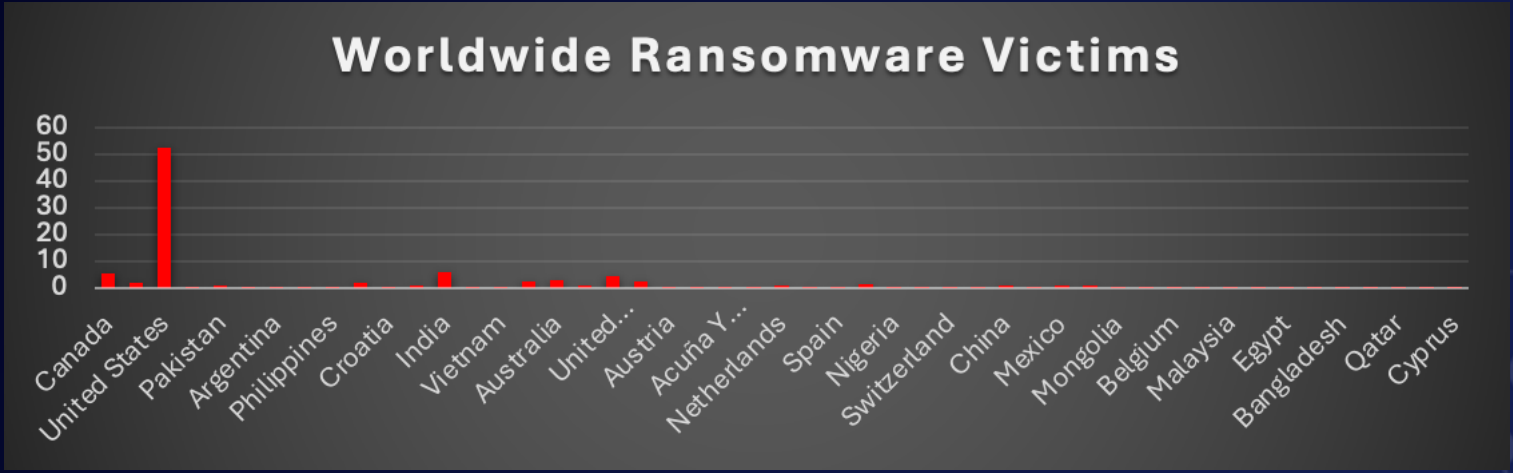

Figure 2: Ransomware Victims Worldwide

Industry-wide Ransomware Victims

Business Services led the ransomware victim landscape this week with 8.33% of reported incidents. Its role as a backbone for IT, consulting, and outsourcing makes it a lucrative target, offering attackers potential access to multiple downstream clients through a single compromise.

Manufacturing (7.44%) and Construction (7.14%) followed closely, underscoring ransomware's continued focus on industries with time-sensitive operations and minimal tolerance for downtime. These sectors remain vulnerable due to reliance on legacy systems and fragmented supply chains.

Retail (6.85%) and Hospitality (5.65%) also featured prominently, reflecting adversaries' interest in customer-facing verticals with high transaction volumes and valuable payment data. The combination of widespread digital exposure and operational dependency makes these industries attractive targets for extortion.

Mid-tier sectors included Law Firms (3.27%), Finance (2.98%), and Organisations (2.68%), all of which store sensitive or high-value data. Transportation, IT, and Healthcare (each 2.08%) added further diversity to ransomware campaigns, emphasising attackers' willingness to exploit both operational and data-rich environments.

Lower-level but consistent targeting was observed in Insurance and Consumer Services (1.79%), Real Estate (1.19%), and Energy, Education, and Media & Internet (each 0.89%). Niche industries such as Telecommunications and Minerals & Mining (0.6% each), along with Federal and Agriculture (0.3% each), reported isolated but notable incidents, reminding us that no vertical is exempt.

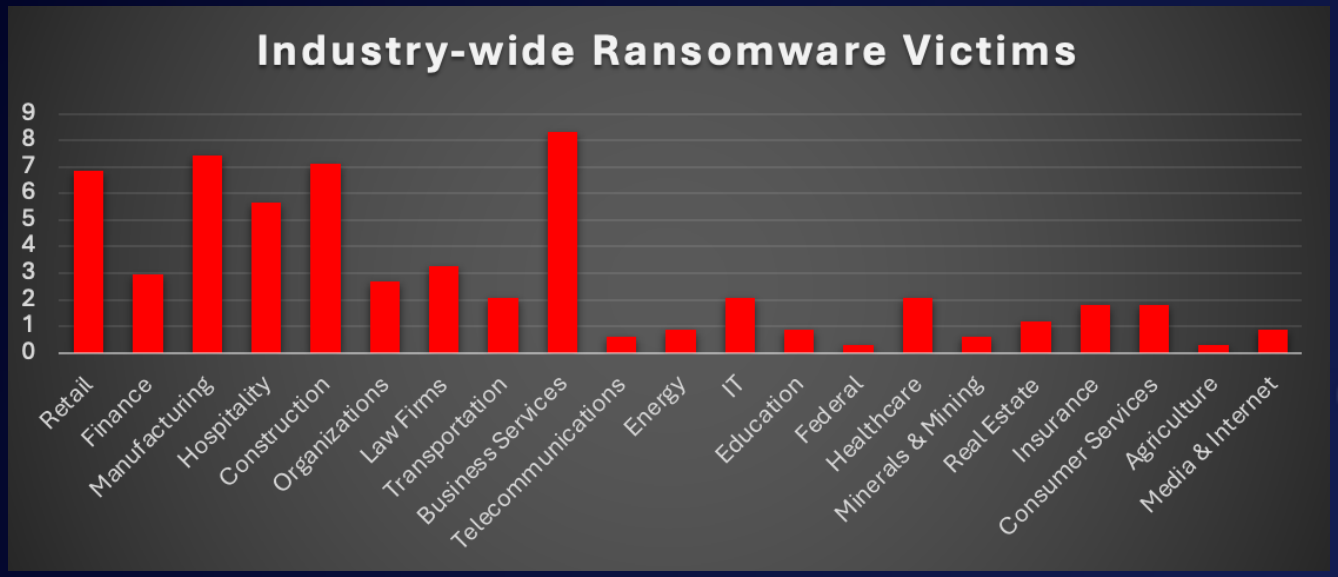

Figure 3: Industry-wide Ransomware Victims