Red Piranha
unified threat management

THREAT INTELLIGENCE REPORT

Oct 21 - 27, 2025

Report Summary:

- **New Threat Detection Added**
  - GlassWorm
  - Kamasers
- **Detection Summary**
  - **Threat Protections integrated into the Crystal Eye - 157**
  - **Newly Detected Threats - 8**

The following threats were added to Crystal Eye this week:

1. GlassWorm

GlassWorm is a new malware that targets Visual Studio Code, A popular software development IDE. The malware has been analysed to be a self-propagating worm that is 'invisible' to the eye. The malware was found in a VS Code extension called CodeJoy that can be found on OpenVSX, an open-source alternative to VS Code's marketplace.

The Malware's payload was made up of invisible Unicode characters that the extension would decode. It uses the Solana Blockchain as its C2 server, making it impossible to take down. The malware reads the blockchain for a specific address, then reads the memo to find its payload. It also uses Google Calendar as backup C2 infrastructure by hosting payload's locations on it.

The malware steals user credentials, such as GitHub, for propagation, and it looks for crypto wallets. It also deploys a SOCKS proxy and a VNC server to achieve remote access.

Threats Protected: 1
Class Type: Trojan-activity
Rule Set Type:

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

Kill Chain:

Tactic	Technique ID	Technique Name
Execution	T1059.007	Command and Scripting Interpreter: JavaScript
Persistence	T1112	Modify Registry
Lateral Movement	T1021.005	Remote Service: VNC
Collection	T1119	Automated Collection
Exfiltration	T1020	Automated Exfiltration

2. Kamasers

Kamasers is a DDOS botnet. The bot has backdoor capabilities as it connects to an attacker controller C2 server. This allows it to download files, receive commands, and execute files, allowing it to perform HTTP and DNS flooding attacks. The bot is also used to access sensitive files.

The bot has been seen to be communicating with third-party platforms such as Telegram, Discord, and GitHub, using these platforms as backup C2 servers.

Threats Protected: 2
Class Type: Command-and-Control
Rule Set Type:

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

Kill Chain:

Tactic	Technique ID	Technique Name
Exfiltration	T1041	Exfiltration Over C2 Channel

Current Threat Summary

Known exploited vulnerabilities (Week 3 October 2025)

Vulnerability	CVSS	Description
CVE-2025-54236	9.1	Adobe Commerce and Magento Open Source contain a deserialisation vulnerability that can allow an unauthenticated remote attacker to bypass authentication and execute code on the system.
CVE-2025-59287	9.8	Microsoft Windows Server Update Service (WSUS) contains a deserialisation vulnerability that can allow an unauthenticated remote attacker to execute code across the network, this vulnerability is a result of insufficient validation being applied upon decryption of the cookie used by the WSUS service. Since the WSUS service is often ran with high privileges, successful exploitation of this vulnerability can result in code being executed with SYSTEM level privileges.
CVE-2025-61932	9.3	Motex Landscope Endpoint Manager contains a vulnerability that can allow an unauthenticated remote attacker to execute code via a specially crafted packet, this vulnerability is a result of insufficient verification of the origin of the incoming requests sent to this service. Successfully exploitation of this vulnerability can result in an attacker gaining access to the system.
CVE-2022-48503	8.8	Multiple Apple products contain a vulnerability within the JavaScriptCore component of WebKit used on the devices which can result in arbitrary code execution upon processing a specially crafted web page.
CVE-2025-2746	9.8	Kentico Xperience CMS contains an authentication bypass vulnerability within the Staging Sync Server component that can allow an unauthenticated remote attacker to gain access to the system via the use of an empty SHA1 username. Further exploitation of additional vulnerabilities may result in an attacker executing code on the system.
CVE-2025-2747	9.8	Kentico Xperience CMS contains an authentication bypass vulnerability within the Staging Sync Server component that can allow an unauthenticated remote attacker to gain access to the system without a password. Further exploitation of additional vulnerabilities may result in an attacker executing code on the system.
CVE-2025-33073	8.8	Microsoft Windows SMB Client contains a vulnerability that can allow an authenticated attacker to escalate privileges to SYSTEM. This vulnerability can be exploited by coercing a target machine into authenticating back to the attacker's machine, which can enable an attacker to authenticate with NTLM against the target machine resulting in the ability to execute code in the context of SYSTEM.
CVE-2025-61884	7.5	Oracle E-Business Suite contains a server-side request forgery (SSRF) vulnerability within the Runtime component of the Oracle Configurator; this vulnerability can allow an unauthenticated remote attacker with network access to gain access to the system and execute code.

For more information, please visit the **Red Piranha Forum**:
https://forum.redpiranha.net/t/known-exploited-vulnerabilities-catalog-4th-week-of-october-2025/610

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

Qilin dominated the ransomware ecosystem this week, responsible for 29.3% of reported incidents. Its disproportionate activity highlights a major campaign surge, solidifying its role as the most aggressive actor in the current landscape.

Sinobi (7.01%) followed as the second-most active group, showing steady momentum in its operations. A cluster of groups, including Radar (5.73%), Clop (5.73%), and Genesis (5.73%), also stood out with elevated levels of activity, marking them as significant mid-tier contributors.

Other mid-level actors included Lynx (4.46%), SafePay (3.82%), Tengu (3.82%), and RansomHouse (3.18%), all of which maintained persistent visibility across multiple regions and industries. DragonForce (1.91%), Play (1.91%), BlackShrantac (1.91%), Kairos (1.91%), Nova (1.91%), and WorldLeaks (2.55%) formed another cluster of sustained but smaller campaigns.

Notable niche presences were observed from Akira (2.55%), Everest (2.55%), Medusa (3.26%), and Brain Cipher (1.27%), illustrating the continuing relevance of both established and emergent groups.

At the lower end, multiple groups logged isolated activity between 0.64–1.27%, including FulcrumSec, Space Bears, Pear, Obscura, Rhysida, Chaos, Kryptos, Beast, Inc Ransom, The Gentlemen, Anubis, and Handala. While individually minor, these actors collectively reinforce the fragmented and adaptive nature of the ransomware ecosystem.

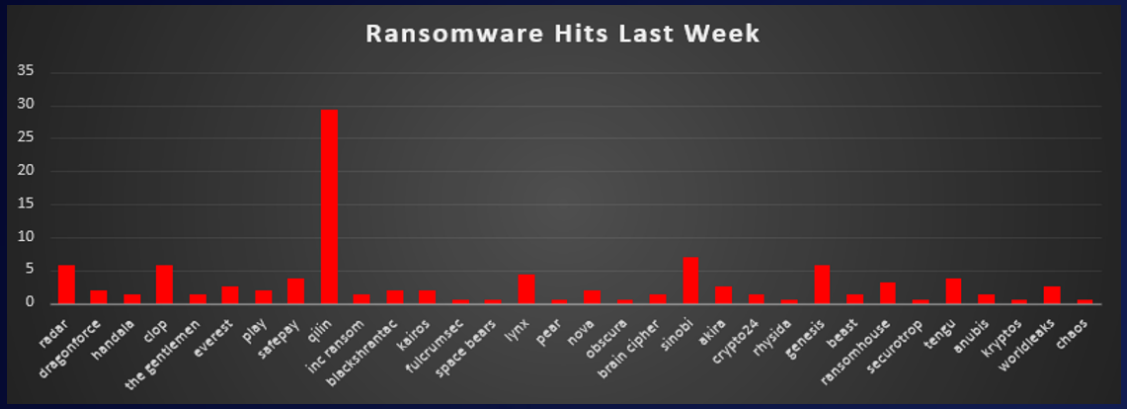


Figure 1: Ransomware Group Hits Last Week

Tengu Ransomware Overview

Tengu is a new RaaS operation first observed in October 2025. Tengu executed hands-on intrusions with double-extortion: data is exfiltrated before encryption; victims are directed to Tor portals for negotiation; and leak listings follow if payment stalls. Expect valid-account abuse, lateral movement, shadow-copy deletion, log tampering, and living-off-the-land execution.

Detailed TTPs

Initial Access

- Valid accounts / exposed remote services (RDP/VPN): Operator-driven intrusion leveraging stolen creds and remote access surfaces (ATT&CK: T1078, T1133).
- Public-facing app exploitation & targeted phishing (likely): Consistent with early-stage footholds seen in comparable RaaS ops (ATT&CK: T1190, T1566).

Execution

- LOLBins & script interpreters: powershell.exe, cmd.exe, rundll32.exe for proxy execution (ATT&CK: T1059, T1218).
- Operator tooling launch: Generic PE dropper then encryption module on endpoints (Windows), observed sample size ~534KB (likely .NET).

Privilege Escalation & Credential Access

- LSASS dumping/credential theft: Standard RaaS tradecraft during staging

Defence Evasion

- Service tamper & AV/EDR weakening:
  sc config wscsvc start= disabled
  sc config wuauserv start= disabled (ATT&CK: T1562).
- Log clearance: wevtutil cl *
- Living-off-the-land execution: rundll32, PowerShell to blend with admin activity (ATT&CK: T1218, T1059).

Discovery

- Network/service discovery & share enumeration to scope blast radius

Collection & Exfiltration (Double-Extortion)

- Staging + compression then bulk exfiltration using Rclone / WinSCP / cloud storage (e.g., MEGA) over encrypted channels (ATT&CK: T1074, T1041, T1567).

Host Artifacts (Correlated to TTPs)

- Dropped in C:\Windows\System32\: wraithnet_bot.exe, controller_gui.exe, controller_console.exe, wraithnet.log — used by/alongside the encryptor; good pivot points for hunts.

Ransom Note Workflow

- README-style note prefixed with [TENGU] and a Ticket ID; directs to live chat on onion site; explicitly states data exfiltration prior to encryption and threatens leaks/key destruction if non-payment (indicator of double-extortion stage completed).

MITRE ATT&CK Mapping

Tactic	Technique (ID)	What to expect
Initial Access	T1078 / T1133 / T1190 / T1566	Valid accounts; exposed remote services; public-facing app exploits; targeted phishing.
Execution	T1059 / T1218	PowerShell/CMD; signed-binary proxy (e.g., rundll32).
Persistence	T1547.001	Run/RunOnce keys (see WraithNet keys below).
Privilege Escalation / Cred. Access	T1003 / T1555	LSASS dumping; credential theft.
Defence Evasion	T1070 / T1562	Log clears; AV/EDR tamper; service disable.
Discovery	T1018 / T1046	Network/service discovery; AD recon (common RaaS tradecraft).
Lateral Movement	T1021	SMB/WMI/PsExec admin-share movement (operator-driven).
Exfiltration	T1041 / T1567	Staging + bulk outbound to cloud/FTP; Tor for comms.
Impact	T1486 / T1490	File encryption; recovery inhibition (shadow copy delete).

Indicators of Compromise (IOCs)

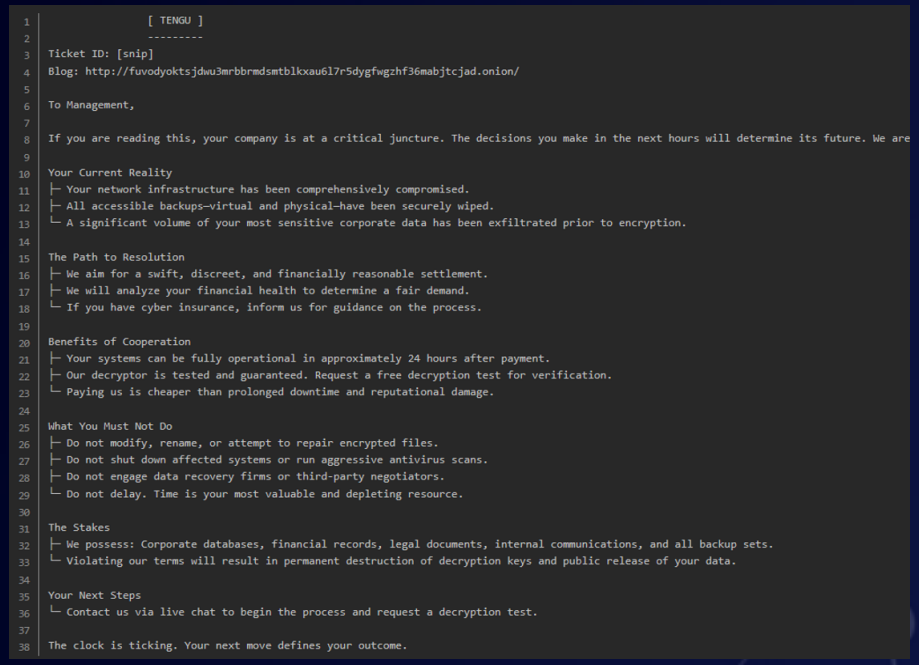
Malware Samples

- SHA-256: FAFB6C5E12DFEEFABA5AC8982D5BB13DD206CFCD328B9D36AA87257F762EE24A
- MD5: DFBC9412BE99B25137AB6AB575489A93

File/Note Artifacts

Encrypted extension: .tengu.

Ransom note filenames: TENGU_README.txt or <ID>-README.txt (e.g., 8F2Z-README.txt);



```
                [ TENGU ]
                ---------
Ticket ID: [snip]
Blog: http://fuvodyoktsjdwu3mrbbrmdsmtblkxau6l7r5dygfwgzhf36mabjtcjad.onion/

To Management,

If you are reading this, your company is at a critical juncture. The decisions you make in the next hours will determine its future. We are

Your Current Reality
├ Your network infrastructure has been comprehensively compromised.
├ All accessible backups—virtual and physical—have been securely wiped.
└ A significant volume of your most sensitive corporate data has been exfiltrated prior to encryption.

The Path to Resolution
├ We aim for a swift, discreet, and financially reasonable settlement.
├ We will analyze your financial health to determine a fair demand.
└ If you have cyber insurance, inform us for guidance on the process.

Benefits of Cooperation
├ Your systems can be fully operational in approximately 24 hours after payment.
├ Our decryptor is tested and guaranteed. Request a free decryption test for verification.
└ Paying us is cheaper than prolonged downtime and reputational damage.

What You Must Not Do
├ Do not modify, rename, or attempt to repair encrypted files.
├ Do not shut down affected systems or run aggressive antivirus scans.
├ Do not engage data recovery firms or third-party negotiators.
└ Do not delay. Time is your most valuable and depleting resource.

The Stakes
├ We possess: Corporate databases, financial records, legal documents, internal communications, and all backup sets.
└ Violating our terms will result in permanent destruction of decryption keys and public release of your data.

Your Next Steps
└ Contact us via live chat to begin the process and request a decryption test.

The clock is ticking. Your next move defines your outcome.
```

Tor Infrastructure
fuvodyoktsjdwu3mrbbrmdsmtblkxau6l7r5dygfwgzhf36mabjtcjad.onion

longcc4fqrfcqt5lzceutylaxir6h66fp6df3oin6mvwvz6pfdbxc6qd.onion

Anti-Recovery / Cleanup Commands
- vssadmin delete shadows /all /quiet (shadow copy deletion)
- wevtutil cl <LogName> (log clear)
- sc config wscsvc start= disabled and sc config wuauserv start= disabled (disable Security Center/Windows Update)

CE 5.5 Mitigations
- Eliminate WAN exposure to RDP/WinRM/SMB/admin UI and enforce MFA on VPN and all admin access.
- Block Tor (exits/bridges) and common exfil paths (MEGA/Dropbox/Syncthing) at CE firewall/DNS; Surge: disable QUIC and drop rclone/WinSCP traffic.
- Hard segment networks; deny East-West SMB/WMI/WinRM except via a jump-box; block PsExec/NTLM lateral movement.
- CE IDS baseline: Security=Alert; Surge: Alert+Drop for Tor/rclone/cloud SNI/JA3 and high-confidence mass-rename/encryption patterns.
- Ingest Sysmon + Windows logs into CE SIEM and auto-isolate hosts on hits for vssadmin, wevtutil, and Run-key persistence.
- Keep backups offline/immutable, block backup VLAN outbound to Internet, and verify restores on a fixed schedule.

Worldwide Ransomware Victims

The United States continued to dominate ransomware targeting, representing 57.32% of reported victims this week. This overwhelming concentration reinforces its position as the most attractive target for adversaries, driven by its expansive digital infrastructure, critical industries, and financial pressure points.

Canada (6.37%) and Australia (5.73%) followed as the most impacted outside the U.S., reflecting consistent targeting of Anglosphere economies. The United Kingdom (3.18%) also ranked prominently, highlighting the ongoing focus on European financial and service sectors.

Mid-tier victimisation was observed in Spain (1.91%), Singapore (1.91%), India (1.91%), and Qatar (1.91%), with Egypt, Saudi Arabia, Switzerland, Germany, Thailand, Brazil, and Japan each reporting 1.27%. These figures demonstrate ransomware's steady expansion across Europe, Asia, and the Middle East, targeting a mix of developed economies and emerging digital hubs.

A long tail of isolated incidents (0.64% each) spanned Peru, Dominican Republic, South Africa, Madagascar, Gabon, Finland, Mexico, Czech Republic, El Salvador, Indonesia, United Arab Emirates, France, Honduras, South Korea, China, Morocco, and Slovakia. While individually small, these cases illustrate ransomware's truly global footprint, impacting countries across every continent.

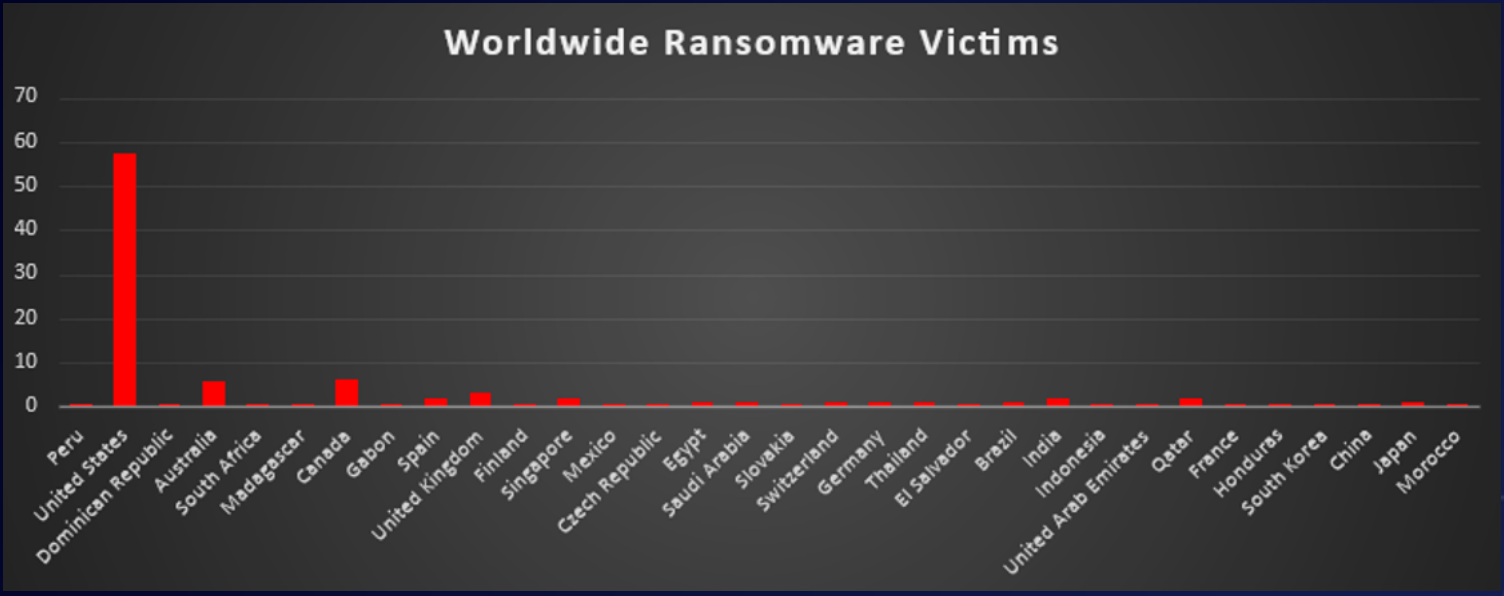


Figure 4: Ransomware Victims Worldwide

Industry-wide Ransomware Victims

Manufacturing was once again the most targeted sector, accounting for 19.11% of all reported ransomware incidents. Its reliance on operational technology, critical role in supply chains, and minimal tolerance for downtime make it one of the most consistently lucrative targets for threat actors.

Retail (13.38%) and Hospitality (11.46%) followed, highlighting adversaries' focus on customer-facing industries with high transaction volumes and sensitive data flows. Both sectors face persistent exposure through distributed digital systems and payment infrastructure.

Business Services (10.19%) ranked strongly as well, underscoring attackers' strategy of compromising IT, outsourcing, and consulting firms to gain leveraged access across multiple clients. Construction (7.01%) also featured prominently, reflecting adversary interest in industries with project-driven timelines and critical operational dependencies.

Mid-tier targeting included Law Firms (4.46%) and Organisations (4.46%), sectors attractive for their sensitive legal and administrative data. Transportation (3.18%), Insurance (2.55%), Consumer Services (2.55%), and Education (2.55%) also recorded steady levels of victimisation, showing ransomware's disruptive impact across essential service providers.

Smaller but notable activity was seen in Media & Internet (1.91%), Finance (1.91%), Telecommunications (1.91%), and Electronics (1.91%), reflecting targeted but limited campaigns. IT (1.27%), Energy (1.27%), and Federal (1.27%) each reported isolated but meaningful incidents, underlining that both public and private institutions remain exposed.

At the lower end, Minerals & Mining (0.64%) and Healthcare (0.64%) registered single incidents, but their inclusion reinforces ransomware opportunistic spread into critical and niche industries alike.

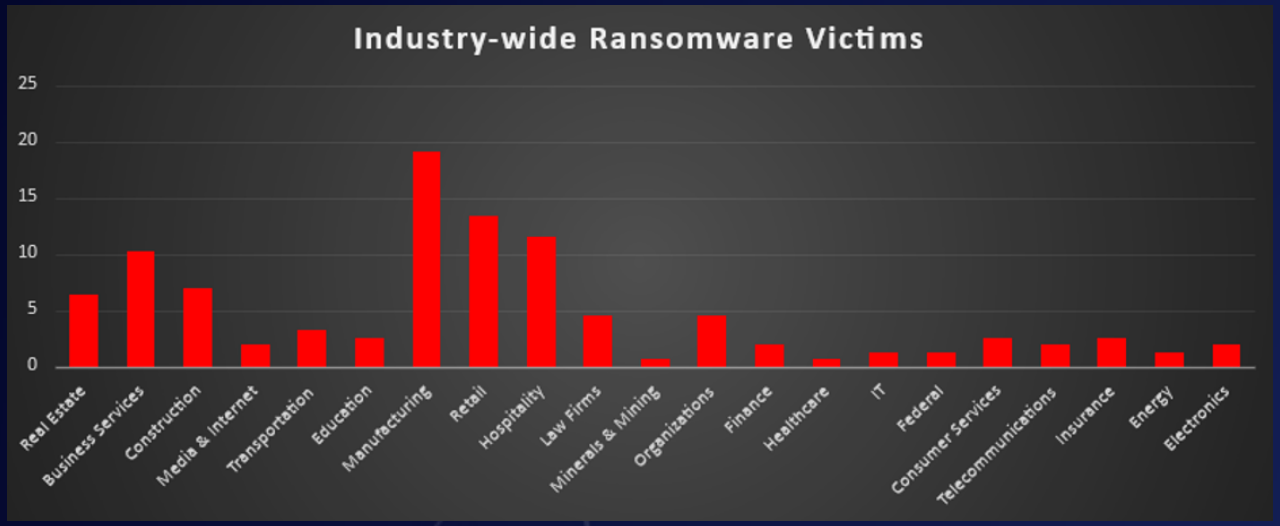


Figure 5: Industry-wide Ransomware Victims