Red Piranha
unified threat management

# THREAT INTELLIGENCE REPORT

Dec 09 - 15, 2025

# Report Summary:

- **New Threat Detection Added**
  - PeerBlight
- **Detection Summary**
  - **Threat Protections integrated into the Crystal Eye - 171**
  - **Newly Detected Threats - 6**

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

## 1. PeerBlight

PeerBlight is a new malware created as a backdoor for Linux systems. It infects systems using React Server Components due to the new vulnerability dubbed React2Shell (CVE-2025-55182). This vulnerability makes it trivial to execute code on the affected systems. The malware maintains persistence via a custom systemd service, which always starts when the infected system is booted. The malware deploys cryptomining on the infected system via a bash script it pulls from GitHub. The malware creates a backdoor via BitTorrent DHT Distributed Hash Table) which is a decentralised network system for connecting multiple peers usually for torrenting, the backdoor is also more resistant than traditional C2 connections, as the C2 domain can be modified in case of a domain takedown.

**Threats Protected: 4**
**Class Type:** Malware
**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 |
|---|---|---|
| Initial Access | T1190 | Exploit Public-Facing Application |
| Execution | T1059 | Command and Scripting Interpreter |
| Persistence | T1543.002 | Create or Modify System Process: Systemd Service |
| Command-and-Control | T1095 | Non-Application Layer Protocol |

# Current Threat Summary

## Known exploited vulnerabilities (Week 2 December 2025)

| Vulnerability | CVSS | Description |
|---|---|---|
| CVE-2018-4063 | 8.8 | Sierra Wireless AirLink ALEOS contains a vulnerability that can allow an authenticated remote attacker to upload an arbitrary file that can result in an attacker gaining access to the device. This vulnerability affects versions 4.9.3 and as this device is end-of-life it may no longer receive future security updates. |
| CVE-2025-14174 | 8.8 | Google Chromium contains a memory corruption vulnerability within the ANGLE component of the browser that can allow an attacker to access out of bounds memory via a specially crafted HTML page, this vulnerability may affect other browsers that utilise Chromium. |
| CVE-2025-58360 | 8.2 | OSGeo GeoServer contains an XML External Entity (XXE) vulnerability that can allow an unauthenticated remote attacker to send a request containing a specially crafted XML that can result in an attacker accessing files on the filesystem or sending requests from the context of the server. This vulnerability was fixed in versions 2.25.6, 2.26.3 and 2.27.0. Exploitation of this vulnerability may allow an attacker to carry out further attacks against the system. |
| CVE-2025-6218 | 7.8 | RARLAB WinRAR contains a path traversal vulnerability that can allow an unauthenticated remote attacker to execute code on the system upon opening a specially crafted archive. |
| CVE-2025-62221 | 7.8 | Microsoft Windows contains a Use After Free vulnerability within the Cloud Files Mini Filter Driver that can allow an authenticated local attacker to escalate their privileges to SYSTEM. |
| CVE-2022-37055 | 9.8 | D-Link Routers GO-RT-AC750 contains a buffer overflow vulnerability that can allow an unauthenticated remote attacker to execute code on the device. This vulnerability affects an end-of-life device and may no longer receive future security updates. |
| CVE-2025-66644 | 7.2 | Array Networks ArrayOS AG contains a vulnerability within the DesktopDirect component that can allow an unauthenticated remote attacker to execute operating system commands on the device, this vulnerability affects versions 9.4.5.8 and earlier. Exploitation of this vulnerability can result in an attacker gaining access to the device. |

For more information, please visit the **Red Piranha Forum**:
https://forum.redpiranha.net/t/known-exploited-vulnerabilities-catalog-2nd-week-of-december-2025/626

## 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.

This report provides a detailed analysis of Kazu, an emerging data extortion group that has rapidly expanded operations targeting healthcare, government, and critical infrastructure sectors.

## Ransomware Hits Last Week

Qilin led this week's activity, responsible for 18.53% of all reported incidents. This made it the single most dominant operator in the ecosystem, pointing to a focused campaign window or a concentrated batch of victim disclosures that pushed Qilin well ahead of the rest of the field.

A strong second tier was formed by DevMan2 (14.66%), followed by Coinbase Cartel and Akira (each 8.19%), and LockBit 5 (6.9%). Together, these crews represent a large, highly active bloc of operations, with enough volume to rival Qilin collectively and signalling sustained, multi-region targeting and regular leak-site publishing.

A mid-tier cluster, Sinobi (5.6%), DragonForce and Inc Ransom (each 3.45%), Worldleaks (2.59%), and Everest, Rhysida, Space Bears, and KillSec3 (each 2.16%) maintained a steady operational tempo and consistent victim disclosures. This band reflects a set of crews that may not dominate weekly totals individually but collectively make up a significant portion of global ransomware pressure.

Smaller but persistent operators, including Nova and Stormous (each 1.72%), as well as Nightspire, Lynx, Root, Chaos, and Genesis (each 1.29%), continued to appear in lower volumes while keeping a visible footprint across multiple sectors and regions.

At the long tail, a wide range of brands, Kazu, Handala, SafePay, Anubis, Tengu, Brotherhood, Toufan (each 0.86%), plus Embargo, Benzona, Datacarry, Securotrop, Leaknet, Interlock, The Gentlemen, Abyss-data, Pear (each 0.43%), each accounted for only a small share of activity. Individually, they are minor, but together they highlight the fragmentation, churn, and long-tail resilience of the broader ransomware ecosystem.

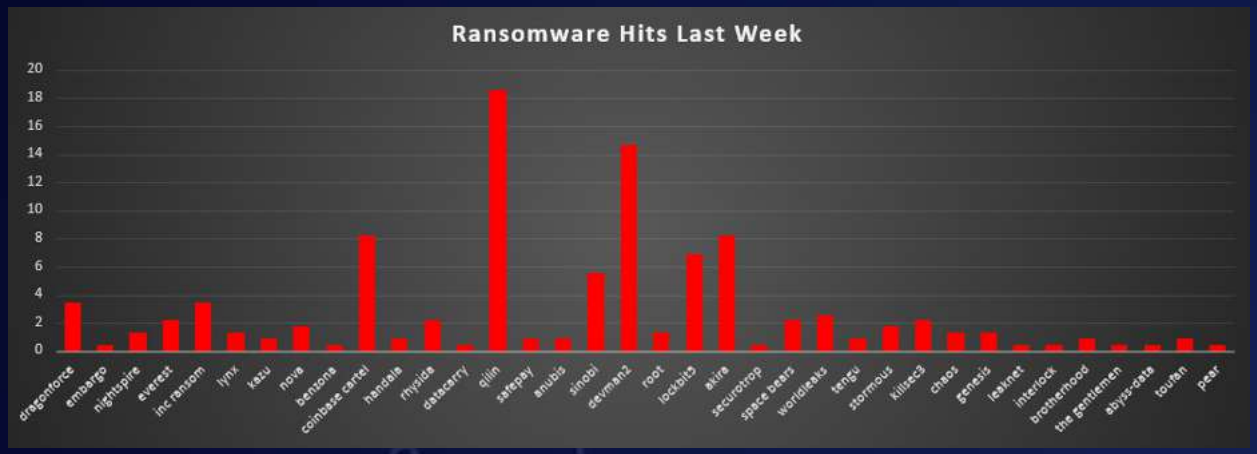



*Figure 1: Ransomware Group Hits Last Week*

## Kazu Ransomware

Kazu is a relatively new ransomware and data extortion group that emerged around mid-2025. Despite its recent appearance, Kazu quickly became active by targeting organisations worldwide, notably in Southeast Asia, the Middle East, Latin America, and parts of Europe. The group primarily targets government agencies, public-sector institutions, healthcare providers, financial services, and other data-rich organisations.

Early victims included multiple government bodies (e.g., in Colombia, Mexico, Thailand), insurance and healthcare companies, and even NGOs. For example, in late 2025, Kazu claimed attacks on a U.K. dental imaging center (CT Dent Ltd) and a Nigerian insurance firm (Leadway Assurance), threatening to leak stolen data unless their ransom demands were met. Kazu's modus operandi closely follows the double-extortion model: infiltrating networks, exfiltrating large volumes of sensitive data, then encrypting files and demanding payment under threat of publishing the stolen data.

Kazu operates a Tor-hidden leak site where it lists victims and ransom demands, often with a countdown timer before data release. The group typically posts proof samples of the data (or at least descriptive summaries) on this site to pressure victims. For instance, in a November 2025 incident, Kazu advertised 353 GB of data (over 1.24 million files) stolen from Doctor Alliance (a US healthcare IT platform), demanding $200,000 and threatening to leak the data by a set deadline.

Detailed Tactics, Techniques, and Procedures (TTPs)

Kazu often gains a foothold through weakly secured remote services or stolen credentials. Investigations indicate the group exploits exposed Remote Desktop Protocol (RDP) services and unpatched internet-facing applications to penetrate networks. In some cases, phishing emails or malware-laced documents have likely been used to deliver malware that helps establish access.

- Exploits public-facing web applications, portals, and web-enabled services (T1190) – Security researcher analysis indicates "there appears to be a strong focus on web portals and web-enabled services," suggesting exploitation of web application or web hosting platform vulnerabilities to gain unauthorised access directly from web applications.
- Valid Accounts & Credential Abuse (T1078) – Analysts note that Kazu may leverage credentials obtained from infostealer logs or dark web markets (reusing passwords from previous breaches). One report noted approximately 60% of Kazu victims had prior infostealer infections, supporting this attack vector.
- Phishing: Spear Phishing Attachment (T1566.001) – Malicious emails with weaponised attachments may be used to deliver initial loader malware. In early December 2025, a malware sample linked to Kazu's activity was identified as SmokeLoader (aka "Dofoil"), a known loader trojan used to execute follow-on payloads.
- External Remote Services (T1133) – Exploitation of exposed RDP/VPN services for initial network access. One confirmed victim indicated the breach occurred via a "legacy vulnerability that has since been patched."
- Initial Loader Deployment – Once access is obtained, Kazu may deploy SmokeLoader to download/install ransomware or other tools while establishing persistence on infected hosts. SmokeLoader communicates with C2 servers over HTTP and serves as a backdoor for additional payloads.

Execution & Payload Deployment

Reports suggest Kazu uses a custom or borrowed ransomware payload that shows technical links to LockBit. In particular, a ransomware sample tied to Kazu attacks was identified as a new LockBit 5.0 variant. This payload, once executed on victim systems, proceeds to encrypt files using robust encryption algorithms.

- Command and Scripting Interpreter (T1059) – PowerShell and CMD scripts used for execution, lateral movement preparation, and payload deployment across the network.
- Native API (T1106) – Malware using Windows API calls directly for execution, enabling more sophisticated and stealthy operations.

- Process Hollowing (T1055.012) – Two-stage loader injects the encryptor into legitimate processes (such as defrag.exe) for stealthy execution, allowing near-fileless deployment and making detection significantly harder.
- Service Execution (T1569.002) – Creating or using Windows services to run malicious payloads, establishing execution persistence across system reboots.
- Encryption Capabilities – The LockBit-derived payload supports invisible/visible modes, selective encryption, delays, and network-wide targeting. Uses XChaCha20 + Curve25519 (or AES + RSA in some variants) for fast and strong encryption across Windows, Linux, and ESXi environments.

Persistence Mechanisms

While Kazu's ransomware itself may not establish long-term persistence (operating as a single deployment), the initial access tools and loaders used by the group do maintain persistence to ensure continued access during the attack lifecycle.

- Create or Modify System Process: Windows Service (T1543.003) – Installing malicious services for persistence, ensuring the loader or backdoor survives system reboots.
- Boot or Logon AutoStart Execution (T1547) – Placing malware in startup locations to maintain access. SmokeLoader and similar loaders commonly use this technique.
- Scheduled Tasks (T1053) – Using Windows scheduled tasks to execute malware at specified intervals or trigger points, maintaining operational persistence.
- Note: Attackers typically persist manually through the compromised network; the LockBit-derived ransomware itself is operationally deployed once during the final attack phase and doesn't require long-term persistence.

Privilege Escalation & Credential Access

After gaining entry, Kazu moves to strengthen its hold on the network. The attackers seek out administrator credentials or other ways to escalate privileges, for example, by dumping password hashes and tokens from compromised machines or by exploiting privilege escalation vulnerabilities.

- OS Credential Dumping (T1003) – Using tools like Mimikatz, ProcDump, or built-in Windows utilities to dump LSASS memory and extract password hashes, Kerberos tickets, and plaintext credentials. This enables domain admin access for mass deployment.
- SAM Database Extraction – Extracting local account credentials from the Security Account Manager (SAM) database on compromised systems.
- Abuse Elevation Control Mechanism: Bypass User Account Control (T1548.002) – Techniques to bypass UAC and gain administrative rights without triggering security prompts.
- •Process Injection (T1055) – Ransomware injecting into legitimate processes to evade defences while operating with elevated privileges.
- Valid Accounts Abuse (T1078) – Once credentials are obtained, using legitimate admin accounts for further access, making detection more difficult as activities appear legitimate.

Lateral Movement

With elevated access, Kazu operators map out the network and move laterally to critical servers. According to incident analyses, Kazu frequently targets backup servers, file shares, and database servers during lateral movement, preparing to maximise damage and data capture.

- Remote Services: Remote Desktop Protocol (T1021.001) – Using RDP with stolen credentials to access servers and workstations across the network, providing interactive access for manual operations.
- Remote Services: SMB/Windows Admin Shares (T1021.002) – Moving laterally via shared drives (C$, ADMIN$) to deploy malicious binaries or scripts on multiple machines simultaneously.
- PsExec & Remote Execution Tools – Using PsExec, WMI (T1047), PowerShell remoting, or GPO startup scripts to execute payloads across domain-joined systems rapidly.
- Living-off-the-Land Techniques – The group has been observed using native Windows utilities and admin tools during lateral movement – using Windows utilities, scheduled tasks, PowerShell, and WMI to execute payloads and propagate while evading detection.
- Network Share Discovery (T1135) – Identifying accessible network shares to prepare for broad encryption and data exfiltration operations.

## Defence Evasion

Kazu employs multiple techniques to avoid detection by security tools and analysts. The malware uses heavy packing, encrypted strings, dynamic API hashing, and process hollowing to avoid EDR visibility.

- Obfuscated Files or Information (T1027) – Packed/obfuscated loader with encrypted strings and dynamic API hashing to prevent static analysis and signature-based detection.
- Impair Defences (T1562) – LockBit 5.0 patches ETW (Event Tracing for Windows) logging, reloads clean copies of system DLLs to defeat EDR hooks, and kills over 60+ security and backup services during execution.
- Unhooking Security DLLs – The ransomware actively unhooks security monitoring DLLs to bypass endpoint detection and response solutions.
- Indicator Removal: Clear Windows Event Logs (T1070.001) – Deleting or clearing Windows event logs to remove evidence of malicious activity and hinder forensic investigation.
- Locale-Based Execution Guard – The ransomware skips execution on Russian/CIS language systems based on locale detection, consistent with LockBit's origin and common among Russian-linked ransomware operations.
- Tor & Encrypted Communications – Exclusive use of Tor for leak site operations and multiple encrypted communication channels (Signal, Session, Telegram) for victim communications, preventing interception.

## Discovery

Before data collection and ransomware deployment, Kazu operators conduct extensive reconnaissance within the compromised environment to identify high-value targets and map the network infrastructure.

- System Information Discovery (T1082) – Identifying host configuration, domain information, installed software, and system roles to prioritise targets.
- File and Directory Discovery (T1083) – Searching file shares, databases, and local systems for valuable data, including PII, financial records, healthcare data, and confidential documents.
- Software Discovery: Security Software Discovery (T1518.001) – Identifying installed antivirus, EDR, and security tools to plan evasion strategies and determine which defences need to be disabled.

## Data Collection & Exfiltration

A hallmark of Kazu's operations is the mass exfiltration of sensitive data prior to ransomware deployment. Once they have access to file servers and databases, Kazu operators identify and aggregate valuable data for extraction.

- Archive Collected Data: Archive via Utility (T1560.001) – Compressing large datasets into archives (ZIP, RAR, 7z) for easier transfer. In the Colombian CNSC breach, the stolen ~2.9 TB of files were compressed into encrypted archives before exfiltration.
- Automated Collection (T1119) – Automated scripts crawling file shares and databases to gather files. The sheer volume of data stolen is often enormous (hundreds of GB to multiple TB), indicating automated processes.
- Data Types Targeted – Employee records, customer/client PII, financial documents, database dumps, emails, healthcare records (patient names, DOB, Medicare numbers, diagnoses, medications), insurance data, and government HR databases.
- Exfiltration Over Alternative Protocol: Encrypted Channel (T1048.003) – Data exfiltrated over encrypted channels (SSL/TLS, Tor, VPN tunnels) to attacker-controlled infrastructure, reducing the chance of interception.
- Exfiltration Over C2 Channel (T1041) – Sending stolen data via malware's C2 connections. May use tools like Rclone for cloud storage exfiltration or custom SFTP/FTP transfers.
- Exfiltration Over Web Service (T1567) – StealBit or Rclone used to upload sensitive data to attacker infrastructure or cloud storage services. Large outbound HTTPS uploads were observed during attacks.

Volume Examples from Known Incidents:

- Doctor Alliance (USA): 353 GB, 1.24 million files, 1.2 million patient records
- Colombian CNSC: 2.9 TB of government files
- Dubai PCFC: 1.94 TB, 13 million files
- M-TIBA Kenya: 4.8 million patient records, 2.15 TB
- Vidal Health India: 472 GB, 326,865 files
- Kuwaiti Construction Company: 18 TB (offered for sale)

Command-and-Control

Kazu operates through decentralised communication infrastructure rather than traditional centralised C2 servers, leveraging anonymisation networks and encrypted messaging platforms.

- Ingress Tool Transfer (T1105) – Downloading additional tools or malware (such as the ransomware payload) into the compromised network after initial access is established.
- Application Layer Protocol: Web Protocols (T1071.001) – Using HTTPS/TLS for C2 communications and data exfiltration, blending with legitimate traffic.
- Non-Standard Port (T1571) – Using unusual network ports for C2 or exfiltration to evade detection and bypass firewall rules.
- Tor-Based Infrastructure – Primary leak site operates as a Tor hidden service. Victim negotiations are conducted through Tor-based portals or encrypted messaging apps.
- Multi-Channel Communications – Telegram channels (@kazu_breach, @kazu_21) for public announcements, Signal (@kazu.517) and Session messenger for direct victim contact, providing redundancy and anonymity.

Impact

With data in hand, Kazu launches the final phase to maximise pressure on victims through both encryption (when deployed) and data exposure threats.

- Data Encrypted for Impact (T1486) – When ransomware is deployed, files on local and network drives are encrypted using robust algorithms (AES + RSA or XChaCha20 + Curve25519). The payload appends a unique 16-character random extension to encrypted files.
- Inhibit System Recovery (T1490) – Deleting shadow copies (vssadmin delete shadows), backup catalogs, and disabling recovery options to prevent easy restoration without paying the ransom.
- Service Stop (T1489) – Stopping or killing processes like databases, mail servers, and security tools (60+ services) prior to encryption to release file locks and maximise damage.
- Ransom Notes – Drops ransom note (typically ReadMeForDecrypt.txt) on each system, directing victims to Tor negotiation portals. Example message: "Your company has been compromised by Kazu. All data will be leaked if no action is taken."
- ESXi Impact – ESXi variant capabilities can knock out entire VM clusters, causing widespread operational disruption in virtualised environments.

Extortion & Victim Communications

Kazu's final phase is the extortion negotiation, where they leverage the stolen data and encryption to demand payment. The group maintains multiple redundant communication channels for victim engagement.

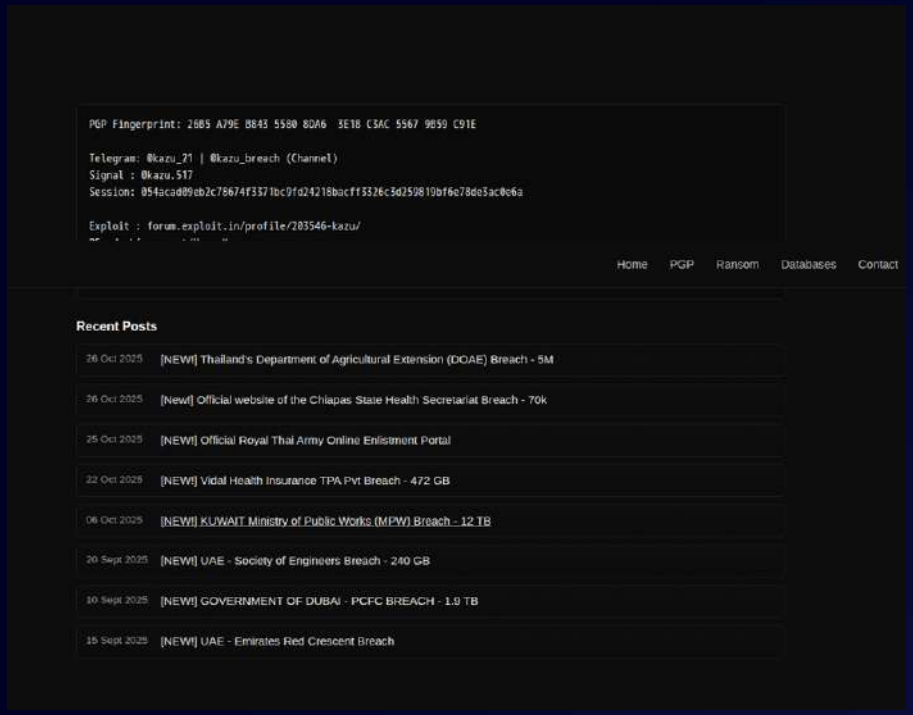
- Tor Leak Site Operations – Primary platform where Kazu lists each victim with data volume, screenshots/file trees as proof, ransom amount, and countdown timer. Approximately 33% uptime observed.
- Telegram Broadcasting – @kazu_breach channel used to announce new victims and leak releases to followers, amplifying pressure through public exposure.
- Direct Negotiation Channels – Victims directed to contact via Telegram (@kazu_21), Signal (@kazu.517), or Session messenger for ransom negotiations.
- Underground Forum Activity – Active profiles on Exploit.in and DarkForums are used for data sales, network access auctions, and reputation building within the cybercriminal community.
- Ransom Demand Structure – Tiered pricing based on victim size and data value. Observed demands: $100-$600 (small targets), $2,000-$8,000 (mid-range), $40,000-$300,000 (large government/corporate). Commonly $100,000-$300,000 for major victims.
- Sample Leaking – Kazu releases data samples on hacker forums to pressure victims (e.g., 200 MB sample from Doctor Alliance containing patient records). Full leaks or data sales follow if ransom deadlines lapse.

MITRE ATT&CK TTPs:

| Tactic | Technique | ID | Summary |
|---|---|---|---|
| Initial Access | External Remote Services | T1133 | Exploiting exposed RDP/VPN for access |
| Initial Access | Exploit Public-Facing Application | T1190 | Unpatched NAS, web apps, portals |
| Initial Access | Phishing: Spear Phishing Attachment | T1566.001 | Malicious emails delivering SmokeLoader |
| Initial Access | Valid Accounts | T1078 | Stolen/compromised credentials from infostealers |
| Execution | Command and Scripting Interpreter | T1059 | PowerShell/CMD used in scripts |
| Execution | Native API | T1106 | Malware using Windows API calls |
| Execution | Service Execution | T1569.002 | Windows services to run payloads |
| Persistence | Create/Modify System Process | T1543.003 | Installing services for persistence |
| Persistence | Boot or Logon AutoStart | T1547 | Malware in startup locations |
| Priv Escalation | Process Injection | T1055 | Ransomware injecting into processes |
| Priv Escalation | Bypass UAC | T1548.002 | Gaining admin rights without prompts |
| Credential Access | OS Credential Dumping | T1003 | Mimikatz, LSASS/SAM dump for hashes |
| Discovery | System Information Discovery | T1082 | Host config, domain info enumeration |
| Discovery | File and Directory Discovery | T1083 | Searching shares for valuable data |
| Discovery | Security Software Discovery | T1518.001 | Checking for AV/EDR presence |
| Lateral Movement | Remote Desktop Protocol | T1021.001 | RDP for lateral movement |
| Lateral Movement | SMB/Windows Admin Shares | T1021.002 | Moving via shared drives |
| Collection | Archive Collected Data | T1560.001 | Compressing stolen files into archives |
| Collection | Automated Collection | T1119 | Scripts gathering files from servers |
| C2 | Ingress Tool Transfer | T1105 | Downloading tools/malware into network |
| C2 | Web Protocols | T1071.001 | HTTPS/TLS for C2 and exfiltration |
| C2 | Non-Standard Port | T1571 | Unusual ports for C2/exfil |
| Exfiltration | Exfil Over Alternative Protocol | T1048.003 | Data over SSL/TLS or Tor |
| Exfiltration | Exfil Over C2 Channel | T1041 | Stolen data via malware's C2 |
| Impact | Data Encrypted for Impact | T1486 | File encryption with ransomware |
| Impact | Inhibit System Recovery | T1490 | Deleting backups and shadow copies |
| Impact | Service Stop | T1489 | Killing databases, AV, backup services |

Indicators of Compromise (IOCs)

Kazu Ransomware Payload (LockBit variant)
SHA-256: 7ea5afbc166c4e23498aa9747be81ceaf8dad90b8daa07a6e4644dc7c2277b82
MD5: 95daa771a28eaed76eb01e1e8f403f7c
Malware Loader (Initial Access Tool)
MD5: e818a9afd55693d556a47002a7b7ef31
Reported SmokeLoader (Dofoil) malware hash, observed on Dec 6, 2025. Used to deploy additional payloads (ransomware) and establish backdoor access. Communicates with C2 servers over HTTP.
Kazu Leak Site (Tor URL)
http://6czlbd2jfiy6765fbnbnzuwuqocg57ebvp3tbm35kib425k4qnmiiiqd[.]onion




Kazu Communications

Telegram Channel: hxxps://t[.]me/kazu_breach – Public breach announcements
Telegram Contact: hxxps://t[.]me/kazu_21 – Direct victim contact
Signal: @kazu.517 – Encrypted negotiations
Session Messenger ID: 054acad09eb2c78674f3371bc9fd24218bacff3326c3d259819bf6e78de3ac0e6a
Hacker Forum Profiles: Exploit[.]in (profile ID 203546), DarkForums[.]st (user "Kazu") – Used for data sales and network access auctions
LockBit 5.0 Infrastructure (Related IOC)
IP: 205.185.116[.]233 (AS53667 - PONYNET/FranTech Solutions)
Domain: karma0[.]xyz

Crystal Eye 5.5 Mitigation

1. Secure External Access
   - Enforce MFA on RDP/VPN; patch exposed apps; block legacy protocols.
   - Deploy WAF rules to detect SQL injection, authentication bypass, and API abuse on web applications.
2. Privilege Management
   - Rotate admin/MSP creds; disable unused accounts; monitor privilege escalation in CE SIEM.
   - Implement least-privilege access for web application service accounts and database connections.
3. Backup & Recovery Protection
   - Use offline/immutable backups; restrict access to backup servers; detect shadow-copy deletion attempts.
4. Execution Control
   - CEASR: block unknown binaries from %TEMP%, %APPDATA%; restrict PsExec and WMI remoting.
5. Data Loss Prevention & Exfiltration Detection
   - Monitor large outbound uploads; block Tor entry nodes and Kazu Onion domains.
   - Implement DLP policies for PII, healthcare records (HIPAA), and financial data.
6. Endpoint Hardening
   - Enable EDR tamper protection; enforce Sysmon-style logging; monitor for suspicious process behaviour.
7. Network Segmentation
   - Isolate AD, ESXi hosts, file servers, database servers, and critical infra from the general network.
8. IR Playbook
   - Automate SOAR actions for Kazu IOCs; isolate hosts; block hashes/Onion URLs; rotate credentials.
   - Develop a specific playbook for data extortion scenarios; prepare breach notification procedures for healthcare/government targets.

## Worldwide Ransomware Victims

The United States again dominated the ransomware landscape, accounting for 42.67% of all identified victims. This concentration makes the U.S. the primary hunting ground for threat actors, reflecting both its huge enterprise footprint and the high rate of disclosed incidents compared to most other regions.

A clear second tier consisted of France (5.17%), the United Kingdom (4.74%), and Canada and the United Arab Emirates (each 4.31%). Together, these countries form a substantial non-US hotspot where mature economies and digitally dependent organisations continue to be repeatedly exposed to ransomware operations.

A broader mid-band included Japan, India, Germany (each 2.59%), Italy (2.16%), as well as Switzerland and Brazil (each 1.72%), followed by the Philippines (1.72%), and a cluster of Singapore, Thailand, Israel, Denmark, and Australia (each 1.29%). These numbers show that ransomware is entrenched across both developed and fast-growing economies, especially where digital services, manufacturing, and finance are heavily concentrated.

Below that, a long tail of countries, such as Turkey, South Africa, Poland, Vietnam, Mexico, Spain, Colombia, Netherlands (each 0.86%), and numerous others including Ghana, Jordan, Lebanon, Portugal, Saudi Arabia, Bolivia, Dominican Republic, Cambodia, Oman, Paraguay, Chile, Peru, China, Belgium, South Korea, Egypt, Nigeria, Tunisia, Malaysia, Bulgaria, Sweden, and Ireland (each 0.43%) - appeared at low individual volumes.

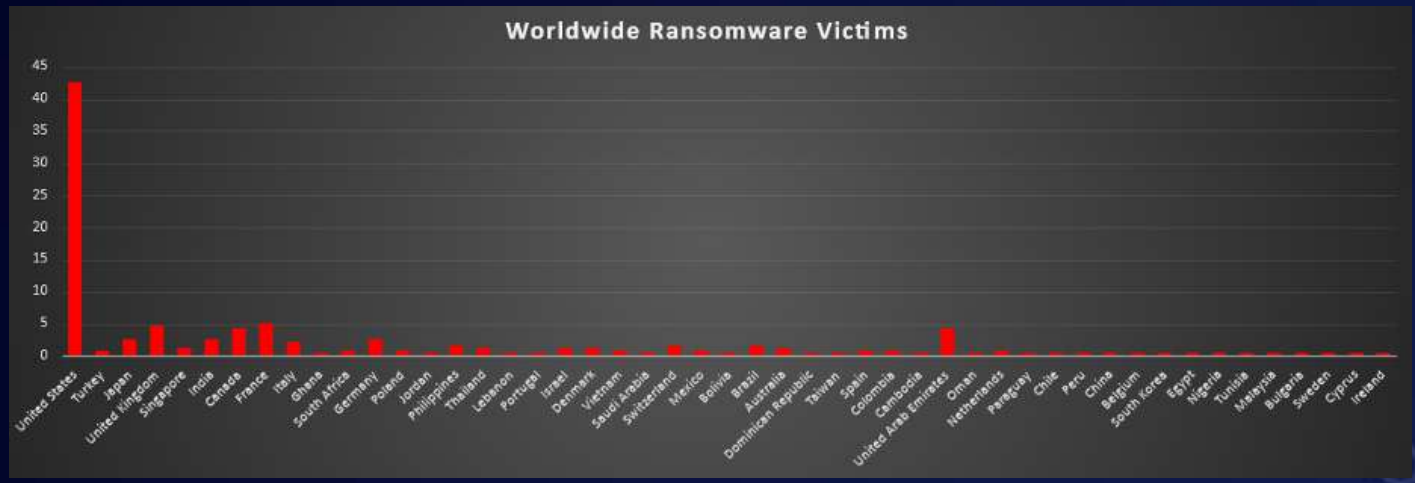



*Figure 3: Ransomware Victims Worldwide*

## Industry-wide Ransomware Victims

Business Services was the most heavily targeted sector this week, accounting for 15.52% of all ransomware victims identified. This reinforces how attractive service-driven organisations are to attackers, given their central role in handling client data, third-party integrations, and outsourced business processes.

A strong second tier consisted of Hospitality (11.64%), Construction (11.64%), and Manufacturing (11.21%), followed closely by Retail (9.48%). Together, these operationally intensive industries represent a highly exposed band where even short disruptions can directly impact revenue, supply chains, and customer experience, a leverage that ransomware operators aggressively exploit during extortion.

A broad mid-band followed, led by Real Estate (5.6%), Finance (4.31%), and Law Firms, Consumer Services (each 3.45%), alongside Federal entities (3.02%). Beneath that, Electronics and Media & Internet (each 2.59%), plus Transportation, Healthcare, and Energy (each 2.16%), showed that both critical services and knowledge-based sectors remain regular fixtures in victim disclosures rather than edge cases.

Lower volume but still active verticals included Telecommunications, Insurance, and general “Organisations” (each 1.72%), as well as IT (1.29%), Education, Agriculture (each 0.86%), and Minerals & Mining, Architecture (each 0.43%), forming the long tail. While individually small, this distribution makes it clear that ransomware pressure extends across almost every major industry, with no single vertical able to consider itself outside the threat envelope.

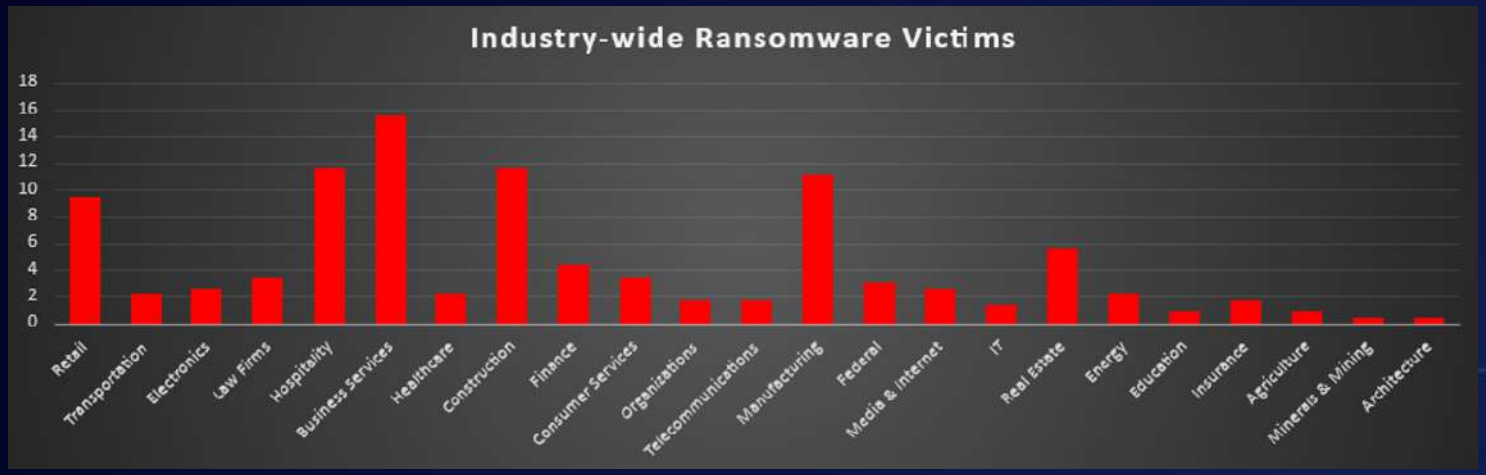



*Figure 4: Industry-wide Ransomware Victims*