Red Piranha
unified threat management

THREAT INTELLIGENCE REPORT

Nov 11 - 17, 2025

Report Summary:

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

- **Detection Summary**
  - **Threat Protections integrated into the Crystal Eye - 80**
  - **Newly Detected Threats - 7**

The following threats were added to Crystal Eye this week:

1. PikaBot

PikaBot is a malicious backdoor and has been active since early 2023. PikaBot usually gets in via phishing and maintains persistence and is known for widely deployed loader malicious actors utilized to distribute payloads such as Cobalt strike or ransomware.

Rules Created: 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	T1059.001	Command and Scripting Interpreter: PowerShell
Persistence, Privilege Escalation, Defense Evasion	T1574	Hijack Execution Flow
Initial Access	T1566.002	Phishing: Spearphishing Link

2. Lumma Stealer

Lumma Stealer is type of malware that belongs to the information stealer malware family and has been in use since at least 2022. This is a Malware as a Service (MaaS) where the capture data is being sold in criminal markets to Initial Access Brokers. The attackers are using phishing email or fake CAPTCHA verification and exploiting legitimate applications to deliver the Lumma Stealer.

Threats Protected: 2
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
Command and Control	T1071.001	Application Layer Protocol: Web Protocols
Collection	T1119	Automated Collection
Persistence, Privilege Escalation	T1547.001	Boot or Logon Autostart Execution: Registry Run Keys / Startup Folder
Discovery	T1217	Browser Information Discovery

Current Threat Summary

Known exploited vulnerabilities (Week 2 November2025)

For more information, please visit the **Red Piranha Forum**:

Vulnerability	CVSS	Description
CVE-2025-21042	8.8	Samsung Mobile Devices contains Out-of-Bounds Write Vulnerability that could allow remote attackers to execute arbitrary code in libimagecodc.quram.so.
CVE-2025-12480	9.1	Gladinet Triofox contains vulnerability that allows unauthenticated remote attackers to access the initial setup pages even after the setup is complete.
CVE-2025-62215	9.1	Microsoft Windows Kernel Contains a race condition vulnerability that allows a local attacker with low-level privileges to escalate privileges. When the exploitation of this vulnerability is successful, the attacker could enable to gain SYSTEM-level access
CVE-2025-9242	9.3	WatchGuard Firebox contains an out-of-bounds write vulnerability that allows remote attacker to execute arbitrary code. This affects both the Mobile User VPN with IKEv2 and the Branch Office VPN using IKEv2 when configured with a dynamic gateway peer. The affects the following Fireware OS 11.10.2 up to and including 11.12.4_Update1, 12.0 up to and including 12.11.3 and 2025.1.
CVE-2025-64446	9.1	Fortinet FortiWeb contains a relative path traversal vulnerability that can allow an unauthenticated remote attacker to execute administrative commands on the system via crafted HTTP or HTTPS Request.

Ransomware Report

The Red Piranha Team conducts ongoing surveillance of the dark web and other channels to identify global organizations 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

Kazu dominated this week's ransomware activity, responsible for 17.45% of all reported incidents. This continued surge reinforces its growing influence as one of the most aggressive and rapidly expanding threat groups in the ecosystem.

Inc Ransom (10.38%) and Clop (10.38%) followed closely, forming a strong second tier. Both groups continue to run high-volume, high-impact campaigns that leverage data-extortion pressure and opportunistic exploitation across multiple industries.

A mid-tier cluster included Qilin (8.49%), Akira (6.6%), RansomHouse (4.72%), Play (4.25%), and Everest (4.25%), each maintaining consistent operational tempo and multi-region targeting. Coinbase Cartel (2.83%), Safepay (2.83%), BlackShrantac (2.83%), Nightspire (2.36%), and Brotherhood (2.36%) also registered steady presence.

Smaller but active operators—Genesis, Sinobi, DragonForce, Beast, WorldLeaks (each 1.89%)—continued to contribute to the mid-lower tier of campaigns. Additional lower-volume actors such as Anubis (1.42%), Direwolf (1.42%), Nova (0.94%), DevMan2 (0.94%), Rhysida (0.94%), Chaos (0.94%) kept the long-tail activity steady.

A wide range of fringe groups each accounted for 0.47% of total incidents, including Handala, Securotrop, J Group, Sarcoma, Crypto24, PayoutsKing, Leaknet, Kraken, Space Bears, and others. While individually small, collectively they highlight the fragmentation and persistence of the ransomware ecosystem.

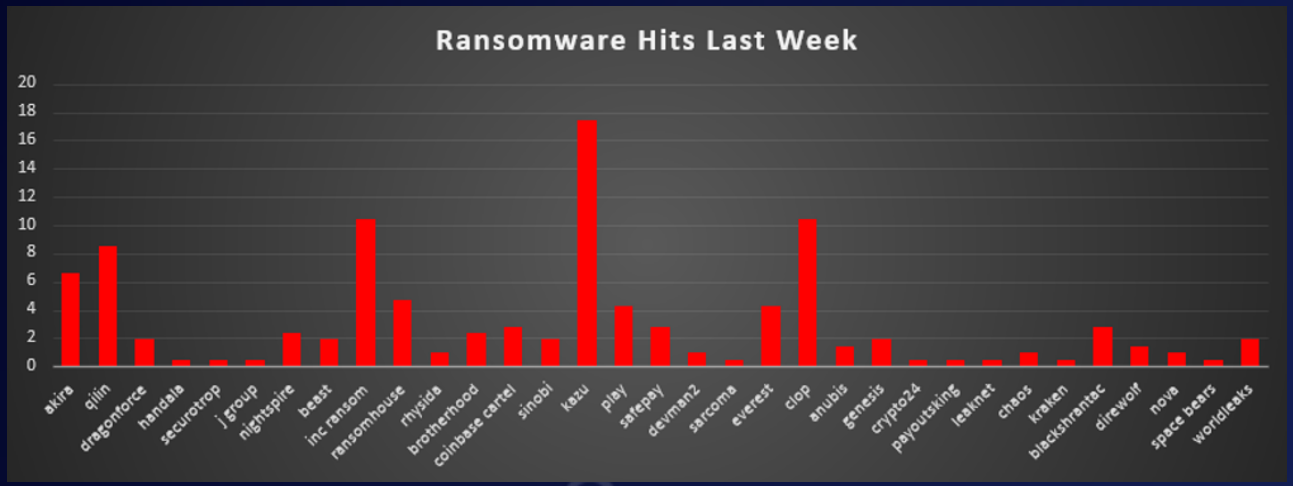


Figure 1: Ransomware Group Hits Last Week

J Group ransomware

J Group ransomware emerged in February 2025 as a double extortion operation with a critical twist: when ransom negotiations fail, they auction stolen data to competitors and malicious actors on underground forums. The group follows a doubleextortion model: attackers infiltrate a network, exfiltrate sensitive data, and then encrypt systems, threatening to publicly leak the stolen data if the ransom is not paid. In its first year J Group has claimed dozens of victims worldwide - from manufacturing and engineering firms to aerospace suppliers and even defence contractors. Recent attacks include a massive breach of German airambulance provider FAI Aviation (nearly 3 TB stolen). In one Australian defense supplychain incident, J Group even claimed “a treasure trove of sensitive military information” after 5 months in the network.

Detailed TTPs

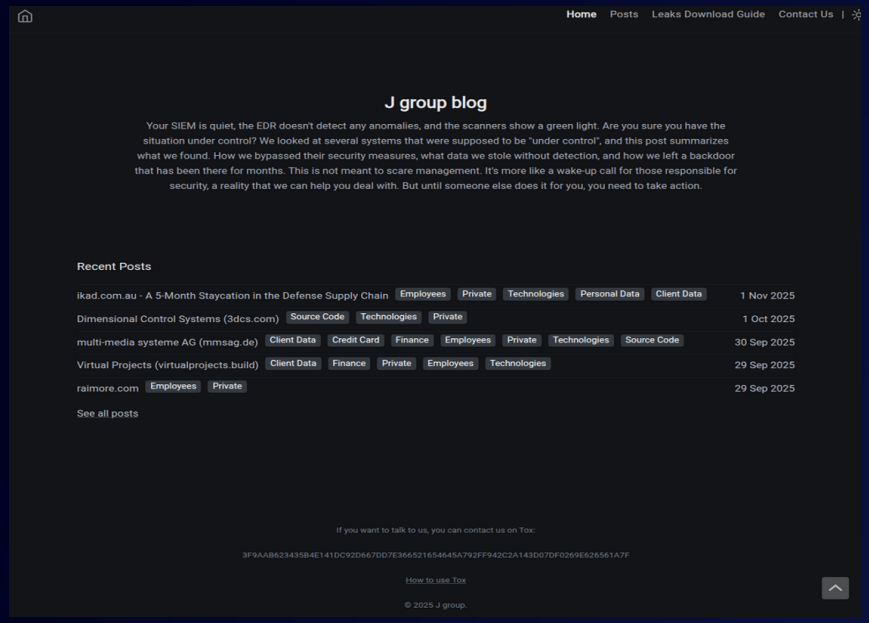
1. External Reconnaissance
   Identify exposed VPN, RDP, web apps, and misconfigured services on internet-facing assets using automated scanners and OSINT.
2. Target Profiling
   Map victim’s industry, technology stack, subsidiaries, and high-value systems to prioritize impactful data and maximize extortion leverage.
3. Initial Access – Phishing
   Deliver tailored spearphishing emails with weaponized documents or links exploiting unpatched client-side vulnerabilities for initial foothold.
4. Initial Access – Credential Abuse
   Use purchased, leaked, or brute-forced VPN/RDP credentials to log in directly, bypassing perimeter protections and usual detection.
5. Initial Foothold Hardening
   Drop simple loaders or web shells, disable logging where possible, and verify persistence before deeper environment exploration begins.
6. Privilege Escalation
   Leverage misconfigurations or local/kernel exploits, combined with credential dumping, to obtain domain admin or equivalent privileged access.
7. Credential Dumping and Expansion
   Dump LSASS, browser passwords, and cached credentials to expand access across servers, databases, and backup management consoles.
8. Domain and Network Discovery
   Enumerate domain controllers, file shares, backup servers, EDR/XDR components, and business-critical applications using built-in admin tools.
9. Host and Data Discovery
   Systematically search for file servers, engineering repositories, finance shares, defense documents, and backups containing sensitive regulated information.
10. Evasion and Tool Masking
    Prefer LOLbins, renamed admin tools, and signed binaries; tamper with logs, avoid noisy scanners, and blend into legitimate traffic.
11. Persistence Establishment
    Create new privileged accounts, scheduled tasks, or services; sometimes modify RDP, VPN, or domain policies for reliable re-entry.
12. Data Collection and Staging
    Aggregate targeted data into staging directories, then compress and split archives to bypass size limits and simplify high-volume exfiltration.
13. Data Exfiltration
    Exfiltrate archives via HTTPS, SFTP, or TOR proxies to attacker-controlled infrastructure, VPS storage, or dedicated leak servers.
14. Backup and Recovery Destruction
    Delete Volume Shadow Copies, target backup agents, snapshots, and accessible NAS backups to severely limit victim recovery options.
15. Ransomware Payload Deployment
    Distribute ransomware binary through Group Policy, PsExec, or remote management tools for near-simultaneous execution across many endpoints.
16. File Encryption and System Impact
    Encrypt business-critical data while generally preserving basic OS functionality, ensuring systems remain bootable but operationally crippled.
17. Ransom Note Delivery
    Drop ransom notes across encrypted systems with victim ID, TOR portals, communication instructions, deadlines, and threats of public exposure.
18. Double-Extortion and Public Pressure
    Threaten leaks, gradually publish stolen data on J Group’s TOR leak site, and amplify pressure through public listings and media.
19. Negotiation and Payment Handling
    Conduct negotiations exclusively via TOR-based chat portals, offer “proof of deletion,” demand cryptocurrency, and may threaten repeated leaks.
20. Post-Incident Re-Entry Potential
    If all access paths aren’t eradicated, reuse leftover credentials, implants, or misconfigurations to re-extort or resell access.

MITRE ATT&CK TTPs:

Tactic	Technique (ID)	Notes/Examples
Initial Access	Phishing (T1566), Valid Accounts (T1078)	Likely compromise via phishing emails or stolen credentials.
Execution	Command-Line (T1059), Malware Execution (T1204)	Launching ransomware payloads, possibly via PowerShell or CMD.
Persistence	Account Manipulation (T1098) or Scheduled Task (T1053)	(Possible but unconfirmed; typical for maintaining access.)
Privilege Escalation	Exploitation of Vulnerability (T1068), Credential Dumping (T1003)	May use known exploits or tools (Mimikatz etc.) to gain higher rights.
Defense Evasion	Indicator Removal (T1070)	Deletes backups/shadow copies; may disable security tools.
Credential Access	OS Credential Dumping (T1003)	(Likely to harvest admin passwords for lateral movement.)
Discovery	System Network Connections Discovery (T1016), System Information (T1082)	(Probable network and host enumeration post-compromise.)
Lateral Movement	Remote Services (T1021)	Using RDP/SMB to spread; possible abuse of VPN or remote admin tools.
Collection	Data from Local System (T1005)	Aggregating files, compressing data before exfiltration.
Exfiltration	Exfiltration Over C2 (T1041)	Data stolen (e.g. 3 TB from FAI) likely uploaded to attacker servers.
Impact	Data Encrypted for Impact (T1486)	Files are encrypted on disk (double-extortion); denial of access.

IOCs

- Onion Leak Sites: Two Tor hidden-service addresses are known for J Group leak blogs:
  twniiyed6mydtbe64i5mdl56nihl7atfaqtpww6gqyaiohgc75apzpad.onion
  w4d5aqmdxkcsc2xwcz7w7jo6wdmvmakgy3y6mfmdtzmyvxe77cjkfbad.onion



TOX ID:
3F9AAB623435B4E141DC92D667DD7E366521654645A792FF942C2A143D07DF0269E626561A7F

Mal names:

- mal2.exe
- jlockr-c7153bdffa0a2de5771193dedd0e4985d08d9497e1b6f97d9beb6a3e54ae48b9.exe
- c7153bdffa0a2de5771193dedd0e4985d08d9497e1b6f97d9beb6a3e54ae48b9.exe
- Other Domains: The group also uses a sharing domain (https:[//]share[.]jtor[.]xyz/torrents/ as seen in leaked torrent links).
- File Indicators: A ransomware sample bPxc3J3BaZ.exe was flagged as malicious and contained the above onion URL. This sample explicitly ran vssadmin.exe deleteshadows /all /quiet

Mitigations Crystal Eye XDR 5.5:

1. Harden remote access with CE SD-WAN & VPN stack
   Use IPSec VPN / SSL VPN / WireGuard only; block direct RDP/SMB from internet via Advanced Firewall, and enforce MFA on all remote access.
2. Filter email and web via Secure Web Gateway
   Enable Email Scanning Gateway + Secure Web Gateway (Anti-phishing, Anti-malware File Scanner, Antivirus, Web Filter, Application/Protocol Filter) to block macro docs, executables, and malicious / newly registered domains.
3. Segment the network using Security Zones & VLANs
   Use Hosts & Groups, Custom Security Zones, and VLAN interfaces to isolate user, server, backup and management networks; allow only required ports between zones.
4. Detect and block exploit / lateral TTPs with IDPS
   Turn on Intrusion Protection & Detection with updated signatures; tune rules for RDP/VPN brute-force, SMB abuse, C2 beacons, and anomalous lateral movement.
5. Protect identities and reduce attack surface
   Use Account Manager / Account Roles for least privilege; pair with Crystal Eye Attack Surface Reduction (CEASR) and OS hardening to restrict PowerShell/CMD, LOLbins, and unsigned tools.
6. Secure and isolate backups using Network Backup
   Use Backup PC / Database Backup to store backups in separate zones; restrict access, apply immutability where possible, and regularly test restores.
7. Monitor, hunt and log with SIEM + Forensics
   Enable Incident and Event Services SIEM, Forensic Logging, PCAP SNAP, and Threat / Security Dashboards to detect unusual logins, privilege changes, bulk exfiltration, and TOR/proxy usage.
8. Prepare CE-centric incident response playbooks
   Define runbooks that use Crystal Eye to: isolate hosts (firewall rules/zones), block IOCs, pull logs/PCAP, rotate credentials, and restore from known-good backups after eradication.

Worldwide Ransomware Victims

The United States remained the primary global ransomware target this week, accounting for 49.06% of all reported victims. This sustained concentration reflects continued large-scale targeting of U.S. enterprises, public services, and supply-chain–linked organizations.

Mexico (5.66%) showed a notable spike, highlighting a sharp rise in attacks across Latin America. Canada (3.3%) and Australia (3.3%) followed, maintaining consistent pressure across the Anglosphere.

Mid-tier targeting included United Kingdom (2.36%), Colombia (2.36%), Italy (1.89%), Japan (1.89%), Argentina (1.89%), United Arab Emirates (1.89%), and Singapore (1.89%)—all digitally mature economies experiencing sustained ransomware interest.

A wide set of countries recorded moderate but recurring victimization (0.94% each) Peru, Saudi Arabia, Costa Rica, Germany, Indonesia, Spain, Sweden.

A long tail of isolated single-incident cases (0.47% each) spread across every region:
Nigeria, South Africa, Nepal, Jordan, Sri Lanka, Venezuela, Iran, Kuwait, Vietnam, Belgium, Egypt, Ireland, Finland, Philippines, Malta, Czech Republic, Korea, Bulgaria, Turkey, Israel, Malaysia, Qatar.

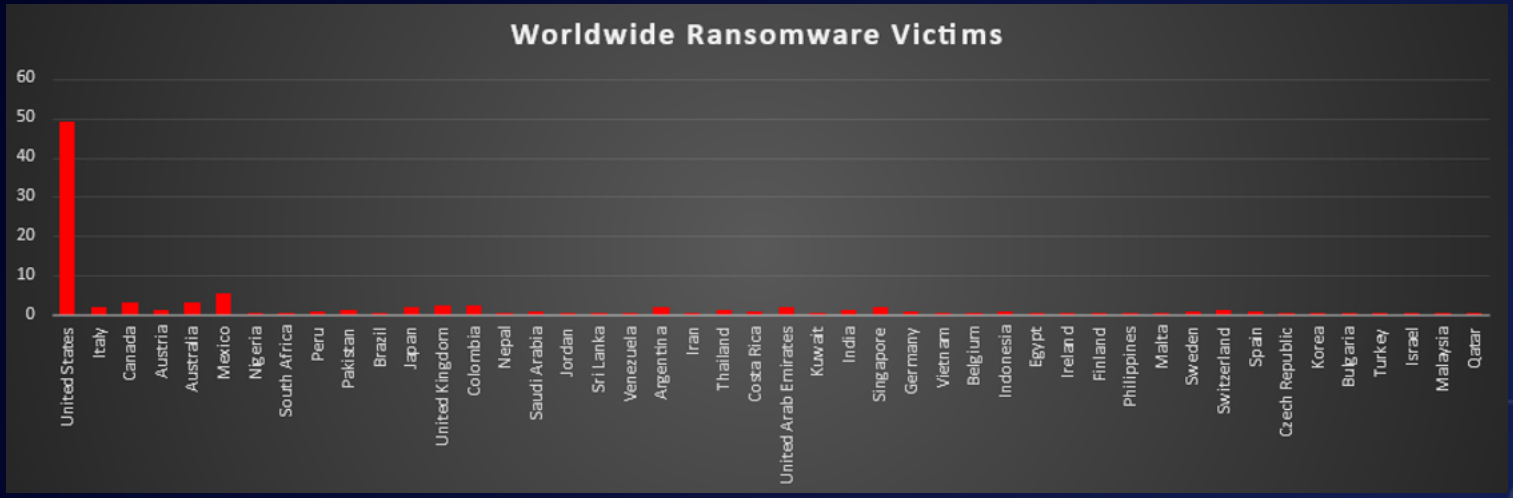


Figure 5: Ransomware Victims Worldwide

Industry-wide Ransomware Victims

Manufacturing remained the most targeted sector this week with 11.79% of incidents. Its combination of legacy OT infrastructure, complex supply chains, and costly downtime keeps it a priority target for extortion-driven threat actors.

Federal entities (8.49%) saw elevated activity, signaling sustained pressure on government networks where operational disruption provides significant leverage. Business Services (6.13%), Construction (5.66%), and Hospitality (5.19%) formed the next high-impact tier—industries with major customer-facing operations, extensive vendor reliance, and valuable data assets.

Mid-level victimization included Organizations (4.25%), Consumer Services (2.83%), Retail (2.83%), Energy (2.83%), Finance (2.36%), Law Firms (2.36%), Education (2.36%), and Insurance (1.89%). These verticals face steady targeting due to their regulatory exposure, sensitive data, and operational dependencies.

Lower-volume but consistent cases were reported across Transportation (1.42%), IT (0.94%), Telecommunications (0.94%), Real Estate (0.94%), and a group of niche sectors—Media & Internet, Electronics, Agriculture, and Healthcare (each 0.47%). These represent opportunistic attacks where even single compromises can provide high-leverage data or operational impact.

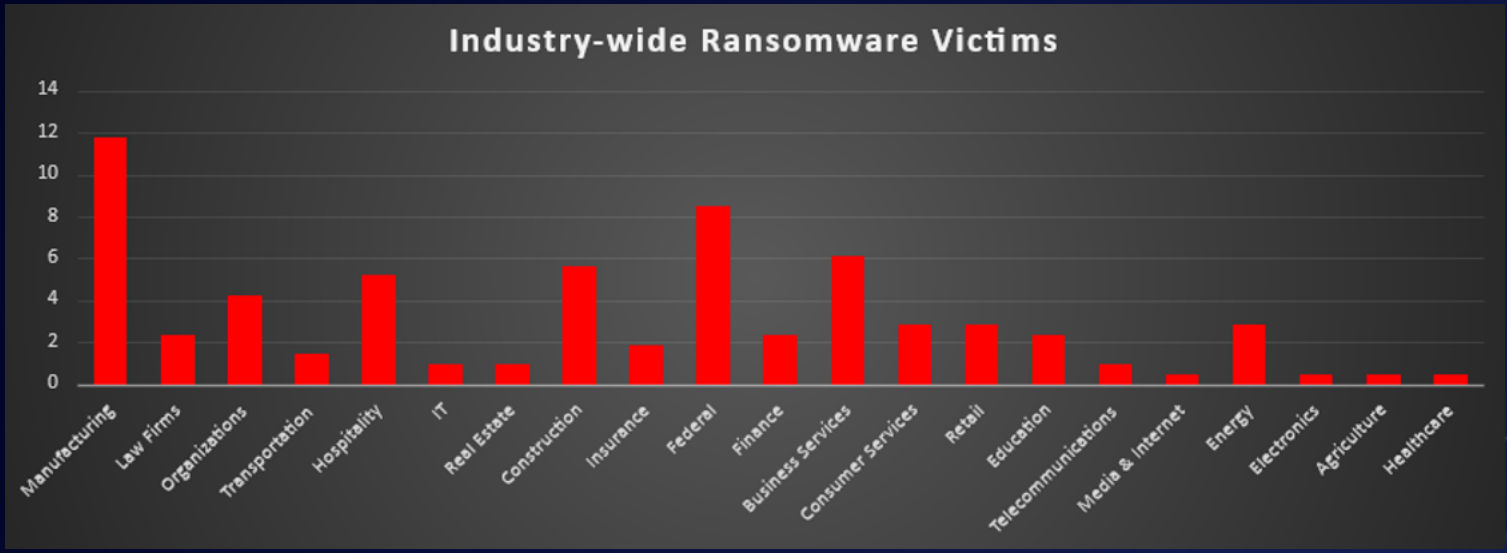


Figure 6: Industry-wide Ransomware Victims