THREAT INTELLIGENCE REPORT

February 24 - March 02, 2026

Red Piranha
unified threat management

Report Summary:

New Threat Detection Added

- PureLogs Stealer

Detection Summary

- New Threat Protection: 86
- Newly Detected Threats: 12

The following threats were added to Crystal Eye this week:

1. PureLogs Stealer

PureLogs Stealer is a .NET based infostealer that's available within the Pure Malware-as-a-Service offerings. It's often spread via phishing campaigns and is the final stage of a sophisticated multi-stage execution chain where the initial loader is embedded in a PNG image.

As with most infostealers, it targets credentials and sensitive information from instant messaging and email clients, browsers, and crypto wallets. Due to the modularity of this malware, the capabilities may evolve over time. Once data has been collected, it's encrypted and exfiltrated to the C2 server.

Threats Protected: 7
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
Initial Access	T1566.001	Phishing: Spearphishing Attachment
Execution	T1204.002	User Execution: Malicious File
	T1059.007	Command and Scripting Interpreter: JavaScript
	T1059.001	Command and Scripting Interpreter: PowerShell
Defence Evasion	T1027.003	Obfuscated Files or Information: Steganography
	T1027.014	Obfuscated Files or Information: Polymorphic Code
Collection	T1055.012	Process Injection: Process Hollowing
	T1555.003	Credentials from Password Stores: Credentials from Web Browsers
	T1115	Clipboard Data
	T1560.002	Archive Collected Data: Archive via Library
	T1113	Screen Capture
Command-and -Control	T1573.001	Encrypted Channel: Symmetric Cryptography
Exfiltration	T1041	Exfiltration Over C2 Channel

Current Threat Summary

Known Exploited Vulnerabilities (Week 4 - February 2026)

Vulnerability	CVSS	Description	Affected Version	Fixed Version
Cisco SD-WAN (CVE-2022-20775)	7.8	**Authenticated Privilege escalation via Path Traversal** Cisco SD-WAN CLI contains a path traversal vulnerability that can allow an authenticated attacker with local access to the device to escalate their privileges to root. This vulnerability affects multiple Cisco products if they are running a vulnerable version of the SD-WAN software.	< 18.4 20.8 19.2 20.3 20.6 20.7	20.6.3 20.7.2 20.8.1
Cisco Catalyst SD-WAN Controller and Manager (CVE-2026-20127)	10	**Authentication Bypass** Multiple Cisco products contain an authentication bypass vulnerability that can allow an unauthenticated remote attacker to gain access to the system. This vulnerability affects the peering authentication mechanism and if exploited can result in an attacker gaining administrative access to the device, which can enable accessing and modifying the SD-WAN network configuration.	< 20.9 20.14 20.9 20.15 20.11 20.16 20.12 20.18 20.13	20.9.8.2 20.12.6.1 20.12.5.3 20.12.6.1 20.15.4.2 20.18.2.1
Soliton Systems K.K FileZen (CVE-2026-25108)	8.7	**Authenticated Command Injection** Soliton Systems K.K FileZen contains a command injection vulnerability that can allow an authenticated attacker to execute arbitrary operating system commands on the system. Exploitation of this vulnerability requires the FileZen Antivirus Check Option to be enabled, allowing an attacker to execute arbitrary commands via a specially crafted HTTP request.	4.2.1 - 5.0.10	5.0.11

For more information, please visit the Red Piranha Forum:
https://forum.redpiranha.net/t/known-exploited-vulnerabilities-catalog-4th-week-of-february-2026/643

Updated Malware Signatures (Week 4 - February 2026)

Threat	Description
XWorm	A Remote Access Trojan (RAT) and malware loader that's commonly used in cyberattacks to give attackers full remote control over a victim's system. It's part of a growing trend of commercialised malware sold or rented on dark web forums, often under the guise of a "legitimate tool."
TrustConnect	Malware-as-a-Service (MaaS) platform operating as a Remote Access Trojan (RAT) masquerading as a legitimate Remote Monitoring Management (RMM) tool that's commonly spread through phishing campaigns.

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 led this week's activity, accounting for 17.24% of all reported incidents. That placed it clearly at the top of the ecosystem, reflecting a sustained campaign tempo and consistent victim disclosures.

A strong second tier was formed by The Gentlemen (12.07%) and Vect (9.77%), followed by Inc Ransom (6.9%), Akira (6.32%), and Play (5.75%). Together, this cluster represented a substantial share of total weekly activity, showing that multiple established crews were operating on a meaningful scale rather than a single group dominating outright.

A solid mid-tier band included Nightspire (5.17%), and a group at 3.45% each CipherForce, DragonForce, and Coinbase Cartel. These actors maintained steady publishing rhythms, contributing materially to overall pressure across industries and regions.

Below that, a broad lower-mid segment consisting of ShinyHunters, Anubis, Payload, Beast, Termite, and Insomnia (each 1.72%), alongside KillSec3, LeakedData, Everest, Leaknet, Tengu, Pear, Chaos, and RansomHouse (each 1.15%). While individually modest, collectively represent a diversified layer of active extortion operations.

At the long tail, a series of fringe operators Rhysida, AtomSilo, Nova, Medusa, Cloak, PayoutsKing, Handala, KittyKatKrew, Blackout, Abyss-data, and Linkc (each 0.57%) appeared in small volumes. Individually minor but collectively persistent, this tail highlights the continued fragmentation and churn within the ransomware ecosystem, where numerous smaller crews remain active even when larger brands capture the bulk of headlines.

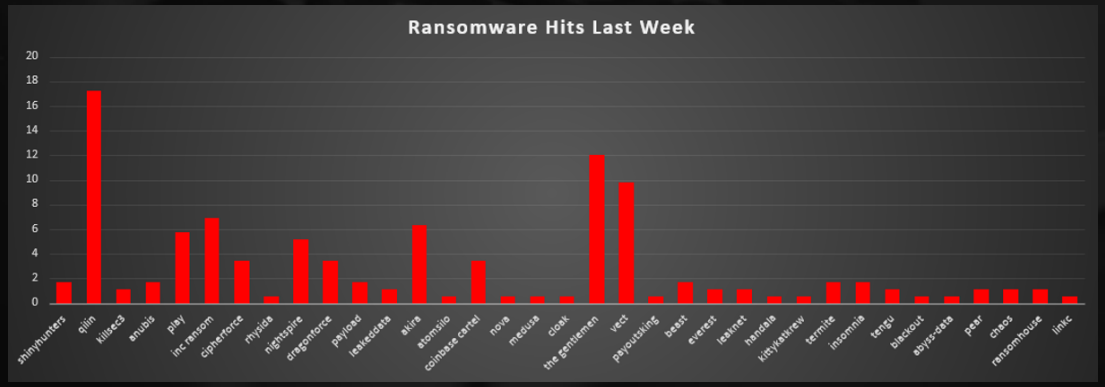


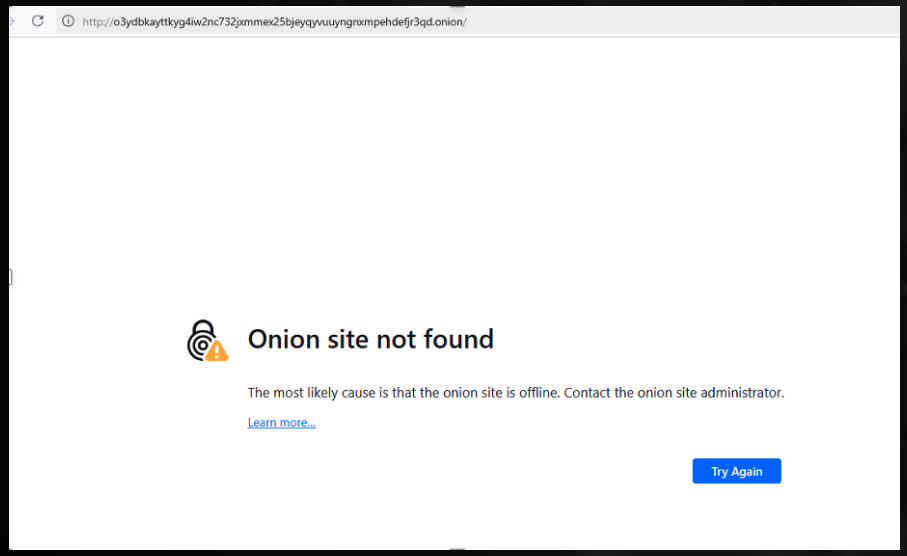
Figure 1: Ransomware Group Hits Last Week

CipherForce Ransomware

CipherForce is a newly observed doubleextortion ransomware group that began publishing victims around 23 February 2026 and operates a Torhosted leak site at o3ydbkayttkyg4iw2nc732jxmmex25bjeyqyvuuyngnxmpehdefjr3qd.onion. It is operated by TeamPCP a cloud-native cybercrime collective, active since late 2025.

Key Group Attributes:

- First public presence: 23 February 2026
- Operating model: Double-extortion (data exfiltration + ransomware)
- Actively recruiting affiliates as of reporting period
- Self-linked to prior activity as TeamPCP and Shellforce
- DLS is intermittently offline - unstable, low uptime (~14% over 30 days)



- Negotiation contact via Session messenger (encrypted)

Tactics, Techniques & Procedures (TTPs)

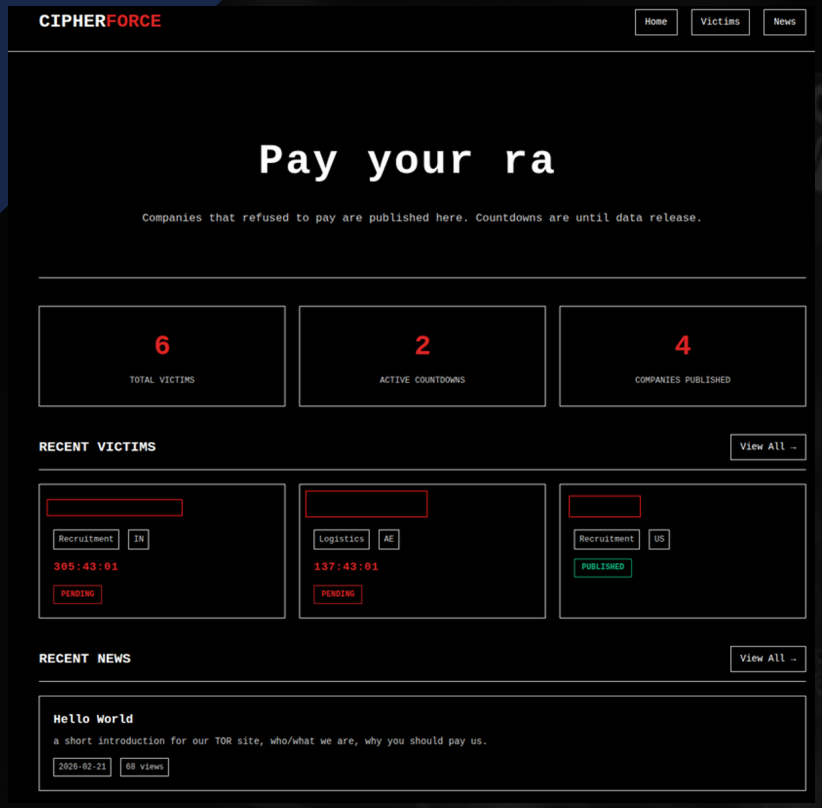
No independent technical analysis has been published by any victim. The TTPs below are limited to what is directly observable from DLS posts and group communications.

Observable Behaviour	Evidence / Source
Double extortion model	DLS posts threaten data leak AND destruction of decryption keys if ransom not paid.
Data exfiltration prior to encryption	Victim data previewed/published on DLS before ransom deadline
Data available for download (with password)	Archive password @shellforce used.
Ransom deadline imposed	1-week payment deadline stated explicitly in DLS post
Affiliate recruitment	DLS self-description states group is actively seeking affiliates

No validated technical attribution exists to map to MITRE ATT&CK framework. Including speculative mappings would be misleading.

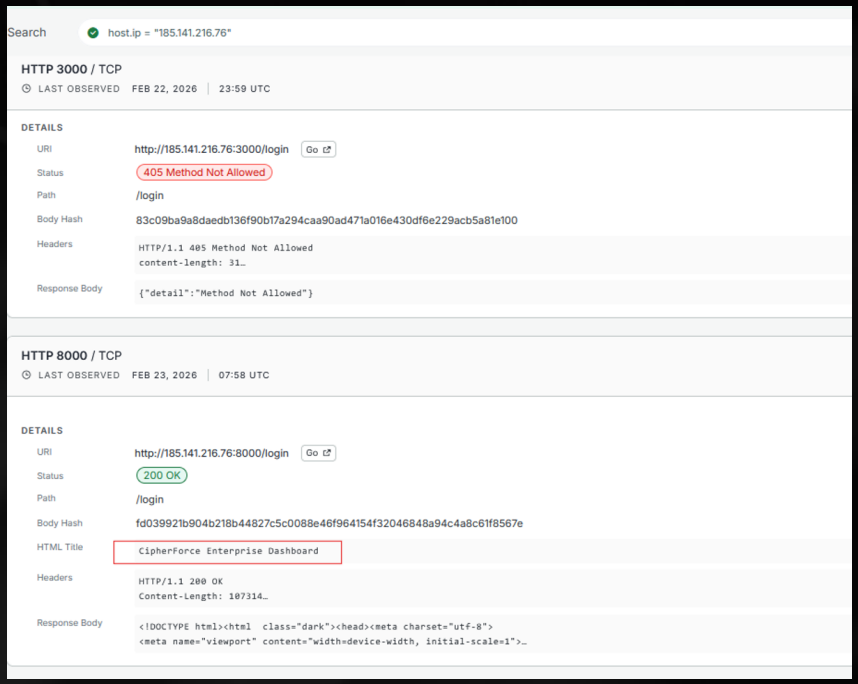
Indicators Of Compromise (IoCs)

Type	Value
Full URL	http://o3ydbkayttkyg4iw2nc732jxmmex25bjeyqyvuuyngnxmpeh-defjr3qd.onion/



IP / Web Panel

Type	Value
Web Panel URL	http://185.141.216.76:5000/
Login Page	http://185.141.216.76:8000/login



Communication Channels

Platform	Value / Handle
Session ID	05a04c7c548c39e903c5913973dd55b6f3d9c1a10d346-ca9d49d10b9428095823e
Telegram	https://t.me/team_pcp
Telegram	https://t.me/Persy_PCP
Telegram	https://t.me/+fQrXQuy77Ng2YzBh
Telegram Bot	https://t.me/fbi_open_door_911_Bot

Worldwide Ransomware Victims

The United States remained the dominant ransomware target, accounting for 47.4% of all identified victims. Nearly one in two recorded incidents hit US-based organisations, keeping it firmly at the center of global ransomware activity.

A clear second tier consisted of Canada (4.62%), Brazil (4.05%), and China (3.47%), followed by India, Italy, France, and Thailand (each 2.89%). These countries represent the bulk of non-US activity, reflecting large digital economies, broad enterprise footprints, and high-value organisational targets.

A mid-band followed with United Kingdom and Germany (each 2.31%), and a cluster at 1.73% Australia and United Arab Emirates. Several countries contributed 1.16% each, including Switzerland, Singapore, Colombia, Panama, South Korea, Belgium, Malaysia, and Japan. This layer shows ransomware activity is consistently distributed across North America, Europe, the Middle East, and Asia Pacific.

Below that sits a long tail of single-incident geographies, Mexico, Namibia, Viet Nam, Netherlands, Turkey, Ecuador, Poland, Israel, Czech Republic, Romania, Venezuela, Argentina, Jamaica, Luxembourg, Saudi Arabia, Greece, Hong Kong, Taiwan, Spain, Portugal (each 0.58%). Individually small, but collectively wide-ranging, this distribution reinforces the same structural pattern seen week after week, ransomware is not regionally contained it is globally dispersed, with both major economies and smaller markets regularly appearing in victim datasets.

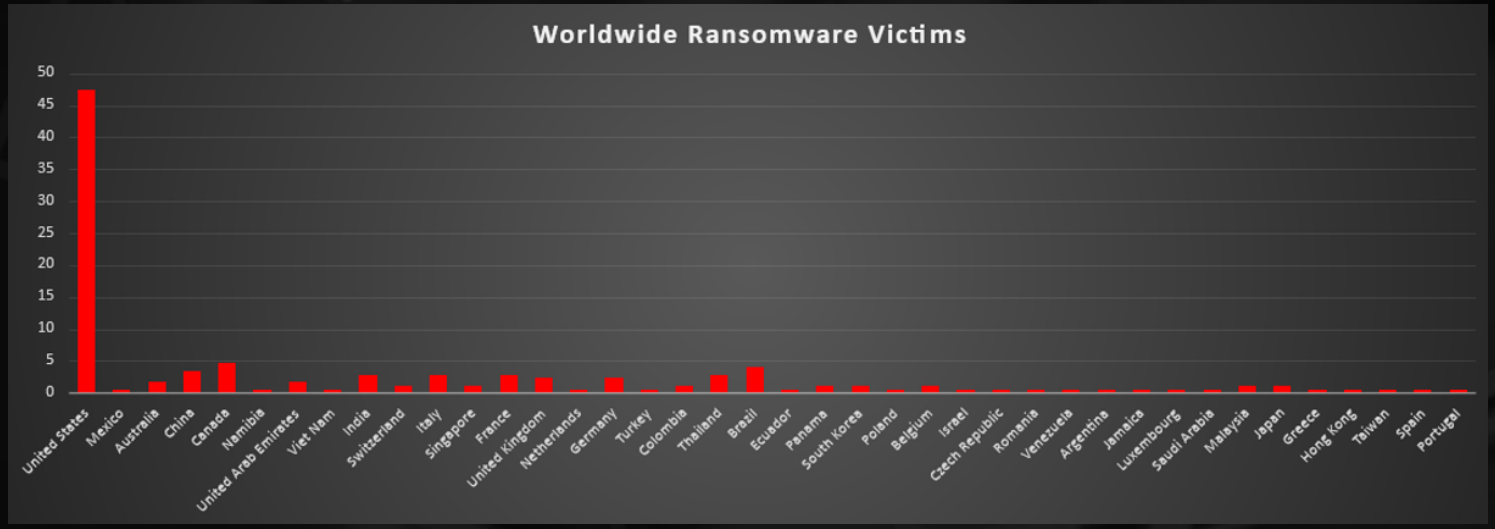


Figure 5: Ransomware Victims Worldwide

Industry-wide Ransomware Victims

Manufacturing led all sectors, accounting for 14.45% (25 incidents) of total ransomware activity. Business Services followed closely at 13.29% (23 incidents), reinforcing the continued targeting of service-layer organisations that often provide access to multiple downstream clients.

IT ranked third at 9.25% (16 incidents), underscoring the ongoing strategic value of technology providers as high-leverage targets. Finance and Healthcare were tied at 8.67% (15 incidents each), maintaining their consistent presence due to sensitive data holdings and operational criticality. Retail was close behind at 8.09% (14 incidents).

Mid-tier exposure included Construction (5.78%), Law Firms (5.2%), and Transportation (3.47%). These sectors typically hold contractual, infrastructure, or regulatory-sensitive data, making them opportunistic but valuable targets.

Lower-frequency sectors included Energy and Hospitality (each 2.89%), Federal and Telecommunications (each 2.31%), and smaller shares across Architecture, Electronics, Real Estate, Agriculture, Education, Media & Internet, Minerals & Mining, Organisations, and Consumer Services (each under 2% individually).

Ransomware actors continue concentrating on operationally critical and supply-chain-connected industries in Manufacturing, Business Services, IT, Finance, and Healthcare while maintaining broad diversification across nearly every economic sector.

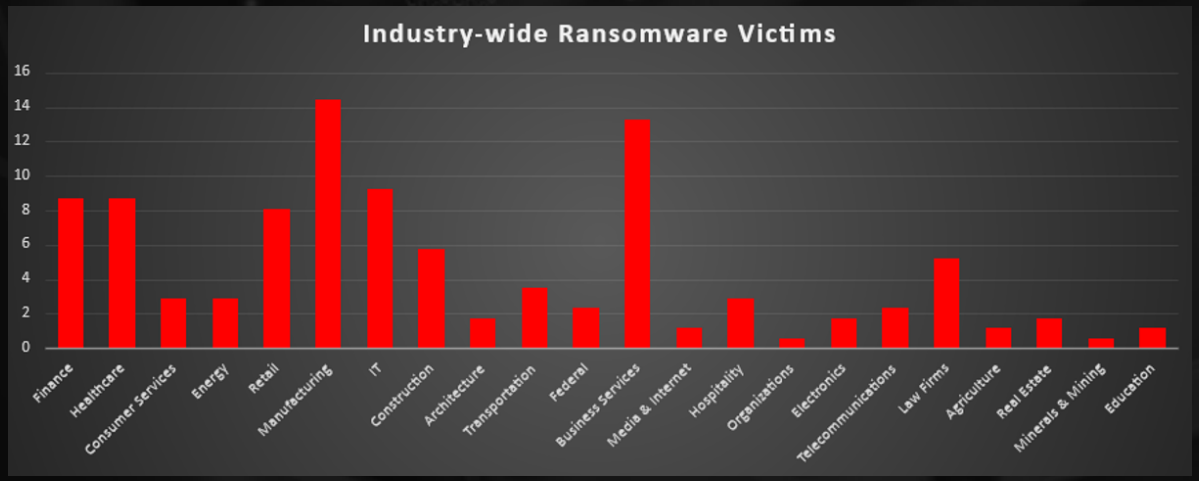


Figure 6: Industry-wide Ransomware Victims