THREAT INTELLIGENCE REPORT

March 03 - 09, 2026

Red Piranha
unified threat management

Report Summary:

New Threat Detection Added

- DefendNot
- TrustConnect

Detection Summary

- New Threat Protection: 111
- Newly Detected Threats: 11

The following threats were added to Crystal Eye this week:

1. DefendNot

DefendNot is an open-source tool designed to disable Windows Defender by telling the Windows Security Center (WSC) service that there is a different anti-virus/anti-malware application running, the WSCs turns off windows defender in this scenario to avoid compatibility and conflicting issues.

This tool is used by threat actors to disable EDR on endpoint systems to allow their malware to bypass detection and execute correctly. The tool can also be installed in the autorun folder to keep defender from running on boot up.

This tool does not affect Windows Server as the WSC service does not exist on Windows Server operating systems.

Threats Protected: 5
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	T1204.002 T1059.001	User Execution: Malicious File Command and Scripting Interpreter: PowerShell
Defence Evasion	T1562.001	Impair Defences: Disable or Modify Tools
Persistence	T1547.001	Boot or Logon AutoStart Execution: Registry Run Keys/ Startup Folder

Current Threat Summary

Known Exploited Vulnerabilities (Week 1 - March 2026)

Vulnerability	CVSS	Description	Affected Version	Fixed Version
Hikvision Multiple Products	10	Authentication Bypass Multiple Hikvision devices contain an authentication bypass vulnerability that can allow an unauthenticated remote attacker to gain access to the device by appending a base64 string in a URL parameter.	Check vendor advisory for affected products and versions	
Rockwell Multiple Products	9.8	Authentication Bypass Multiple Rockwell products contain an authentication bypass vulnerability that can allow an unauthenticated remote attacker to obtain a cryptographic key which can be used in communication with the Logix controllers, allowing for modification of configuration and application code.	Check vendor advisory for affected products and versions	
Apple Multiple Products	8.8	Remote Code Execution via WebKit Multiple Apple products contain a use-after-free vulnerability within WebKit that can allow an unauthenticated remote attacker to execute code on the devices upon visiting a specially crafted web page.	MacOS: < 13.5 iOS, iPadOS, Safari: < 16.6	13.5 16.6
Apple Multiple Products	8.8	Remote Code Execution via WebKit Multiple Apple products contain an integer overflow vulnerability within WebKit that can allow an unauthenticated remote attacker to execute code on the device upon visiting a specially crafted web page.	iOS, iPadOS, tvOS: < 15.2 MacOS: <= 12.0 watchOS: < 8.3	15.2 12.1 8.3
Apple iOS and iPadOS	7.8	Privilege Escalation Apple iOS and iPadOS devices contain a use-after-free vulnerability that may allow an application to execute arbitrary code with elevated kernel privileges.	iOS, iPadOS: < 17	17
Broadcom VMware Aria Operations	8.1	Unauthenticated Command Injection Broadcom VMware Aria Operations contain a command injection vulnerability that can allow an unauthenticated remote attacker to execute arbitrary commands on the system while a support-assisted product migration is in progress.	Check vendor advisory for affected products and versions	
Qualcomm Multiple Chipsets	7.8	Integer Overflow Multiple Qualcomm chipsets contain an integer overflow vulnerability within the KGSL (Kernel Graphics Support Layer) kernel driver, this driver is used as an interface between the operating system and the GPU hardware.	Check vendor advisory for affected chipsets and versions	

For more information, please visit the Red Piranha Forum:
https://forum.redpiranha.net/t/known-exploited-vulnerabilities-catalog-1st-week-of-march-2026/645

Updated Malware Signatures (Week 1 - March 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."

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 ransomware activity this week with 18.52% (45 incidents), maintaining its position as the most active operator in the ecosystem. Its sustained publishing cadence and wide targeting footprint continue to place it at the top of weekly victim disclosures.

A strong second tier included DragonForce (10.7%) and Inc Ransom (9.88%), followed by AiLock (7.41%) and Play (7%). These groups collectively represent a large portion of weekly activity and demonstrate steady operational tempo across multiple sectors.

Another notable cluster consisted of Akira (6.58%), Nightspire (6.17%), and The Gentlemen (4.94%), with Lapsus$ (4.12%) also showing a visible presence in victim disclosures. This group reflects a mix of long-standing ransomware brands and actors maintaining consistent leak-site activity.

Mid-tier activity included Handala (2.88%), Everest (2.47%), Vect (2.47%), and smaller contributions from Pear (1.65%), Payload (1.23%), Tengu (1.23%), ShinyHunters (1.23%), SafePay (1.23%), and KillSec3 (1.23%).

At the lower end of the distribution were a number of sporadic operators including Coinbase Cartel, Anubis, PayoutsKing, Brain Cipher (each 0.82%), alongside several single-incident groups such as MyData, Lynx, Linkc, Rhysida, Bravox, Insomnia, Beast, Termite, Kairos, MetaEncryptor, XP95, Crypto24, TridentLocker, and Chaos (each 0.41%).

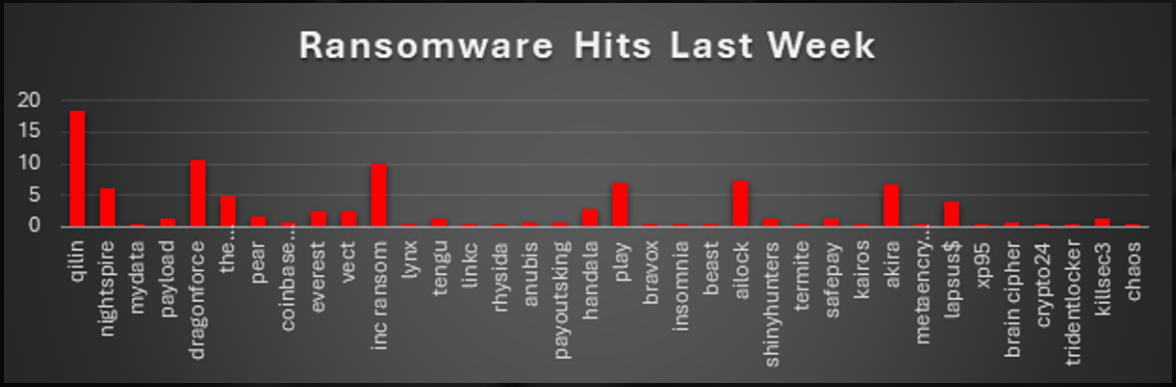
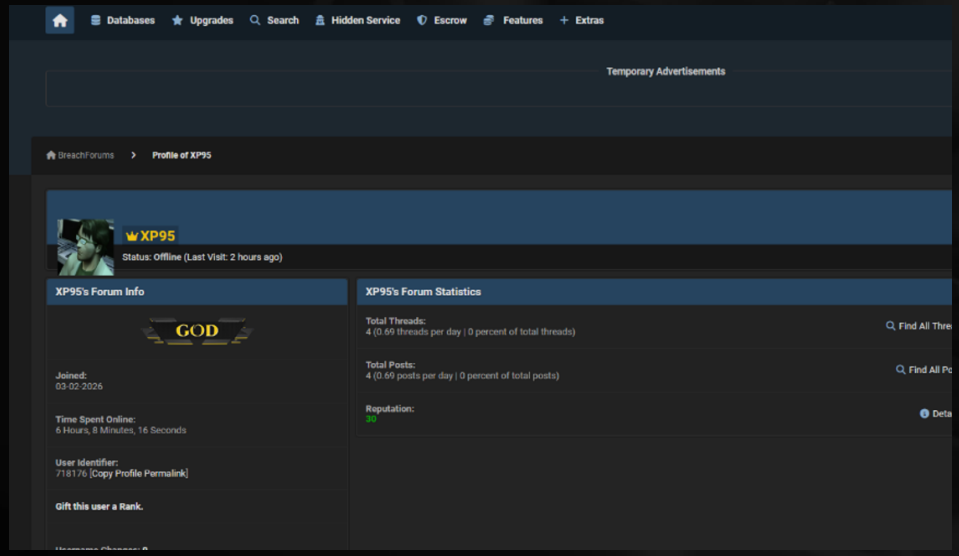


Figure 1: Ransomware Group Hits Last Week

XP95 Ransomware

Red Piranha's threat intelligence team identified XP95 as a newly emerged data-extortion actor, first observed on 4 March 2026. Unlike conventional ransomware operators, XP95 does not deploy encryption malware. The group operates a pure exfiltration-and-extortion model: sensitive data is stolen from the victim environment, a proof-of-compromise sample is published on a Tor-hosted Data Leak Site (DLS) and cross-posted to BreachForums, and a ransom demand is issued with a hard payment deadline. Failure to pay results in full public release or sale of the stolen dataset. XP95's sole confirmed victim within the 28 February – 6 March 2026 reporting window is Eholo Health, a Spanish mental-health SaaS platform serving over 10,000 psychologists across Spain and Andorra. The actor's BreachForums profile was freshly created at the time of first appearance, with no prior references in threat intelligence reporting linking XP95 to any known organised group or prior campaigns.



Tactics, Techniques & Procedures (TTPs)

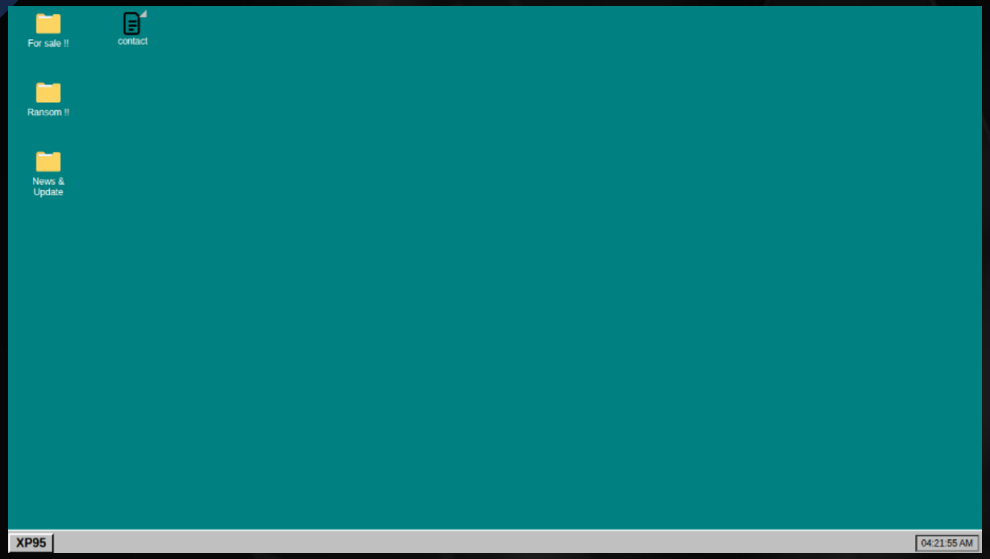
No validated technical TTPs have been published by any threat intelligence source. No security vendor, incident-response firm, or government agency has released a technical analysis of XP95's intrusion methods, tooling, or infrastructure. The TTPs below are limited to what is directly observable from DLS posts, BreachForums activity, and public breach reporting.

Observable Behaviour	Evidence / Source
Pure data extortion (no encryption)	No encryption binary, ransom note file, or decryptor referenced in any victim communication or DLS post
Data exfiltration prior to extortion	Victim data previewed/published on DLS and biteblob.com before ransom deadline
Data offered for download (password-protected)	Victim data archives hosted at biteblob.com with direct download links in DLS post
Ransom deadline imposed	15 March 2026 payment deadline stated explicitly in DLS post for Eholo Health
Data simultaneously posted to BreachForums	XP95 BreachForums profile active; victim claim cross-posted alongside DLS
Privacy-hardened negotia-tion channels	Session messenger (ID published), Signal (link published), Keybase profile - no email contact
High-sensitivity sector targeting	Healthcare SaaS platform targeted; stolen data includes 1.14M+ psychological clinical notes

No validated MITRE ATT&CK mapping exists for XP95. No published threat intelligence source has attributed specific MITRE technique IDs to this actor. A mapping will only be possible if/when a technical incident response report or malware sample analysis is published. Speculative mappings have been intentionally omitted.

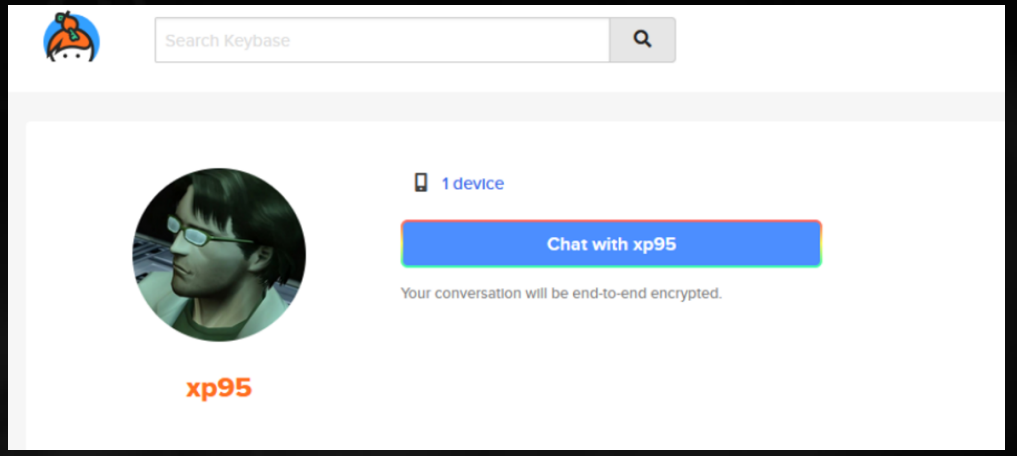
Indicators of Compromise (IoCs)
Tor Data Leak Site

Type	Value
Full URL (currently DOWN)	http://37lfmtakhknzx5t6k57ieijkiqrc4c3kpimfvrmafva25ut2tkn-vw3yd.onion/



Communication Channels

Platform	Value / Handle
Session ID	05d3d75e8370cfc72c7a563c9880995eaf4c33f1bd42a5d4e9cd65e713b190c934
Signal	https://signal.me/#eu/CdaTwdWhKF5rFNGSks8HIHyoBJsU0IAC-jVAaYtW2p4wFoKk4xxRLUKnGCbHsWO9i
Keybase	https://keybase.io/XP95



Data Sample Hosting (biteblob.com)

Archive	URL
Medical notes sample (.zip)	https://biteblob.com/Information/YNlNvLRPhA0F3W/#samples_notes.zip
PII records sample (.zip)	https://biteblob.com/Information/caYuDi8i5XnzS1/#samples_pii.zip

CE 5.5 Mitigation Recommendations

The following mitigations are mapped to Cyber Essentials (CE) 5.5 controls and are directly applicable to the XP95 threat profile. Given that XP95 operates as a pure data-exfiltration actor - with no encryption component - defences must prioritise preventing unauthorised access to sensitive data repositories, detecting large-volume outbound data transfers, and securing privileged account pathways. Healthcare and SaaS providers are the current primary target profile.

- Enforce role-based access control (RBAC) across all data repositories and SaaS management interfaces. Limit access to clinical records and PII to verified, business-justified users only. Audit and revoke excess permissions quarterly.
- Mandate phishing-resistant MFA (FIDO2/hardware token) for all privileged accounts, VPN gateways, and SaaS admin portals. SMS-based MFA is insufficient; replace with authenticator apps or hardware keys for high-risk roles.
- Deploy DLP (Data Loss Prevention) controls to monitor and alert bulk transfers of sensitive data. Establish baselines for normal egress traffic volume and alert on anomalous outbound transfers exceeding threshold, particularly to file-sharing platforms (e.g. biteblob.com).
- Ensure documented IR playbooks cover pure data-exfiltration scenarios (not only ransomware encryption). Confirm GDPR/NIS2 notification timelines are met (72 hours to supervisory authority). Engage DPA (e.g. AEPD for Spain) and relevant national police immediately upon confirmed exfiltration.

Worldwide Ransomware Victims

The United States remained the dominant target this period with 53.5% (130 incidents) of all recorded ransomware victims. This means more than half of all known attacks occurred against US-based organisations, continuing the long-standing pattern of North America being the primary focus of ransomware operations.

A second tier of countries accounted for much smaller but still notable shares. Germany represented 5.76%, followed by Canada (4.94%), United Kingdom (4.53%), and France (4.12%). Australia also recorded a significant presence with 3.7% of victims. Together, these countries make up the majority of activity outside the United States and reflect regions with large digital economies and extensive enterprise infrastructure.

A mid-range group included South Korea, India, and Spain (each 2.06%), along with Italy, Israel, and Turkey (each 1.65%). These figures indicate continued ransomware exposure across both European and Asia-Pacific markets.

Several countries recorded smaller but recurring activity at 0.82%, including Singapore, Malaysia, Brazil, Netherlands, United Arab Emirates, and Thailand.

The remainder of the dataset forms a long tail of single-incident countries at 0.41% each, including Greece, Russia, Portugal, Japan, Mexico, Switzerland, Austria, China, Norway, Philippines, Belgium, Georgia, Romania, Lebanon, Pakistan, Egypt, and Madagascar.

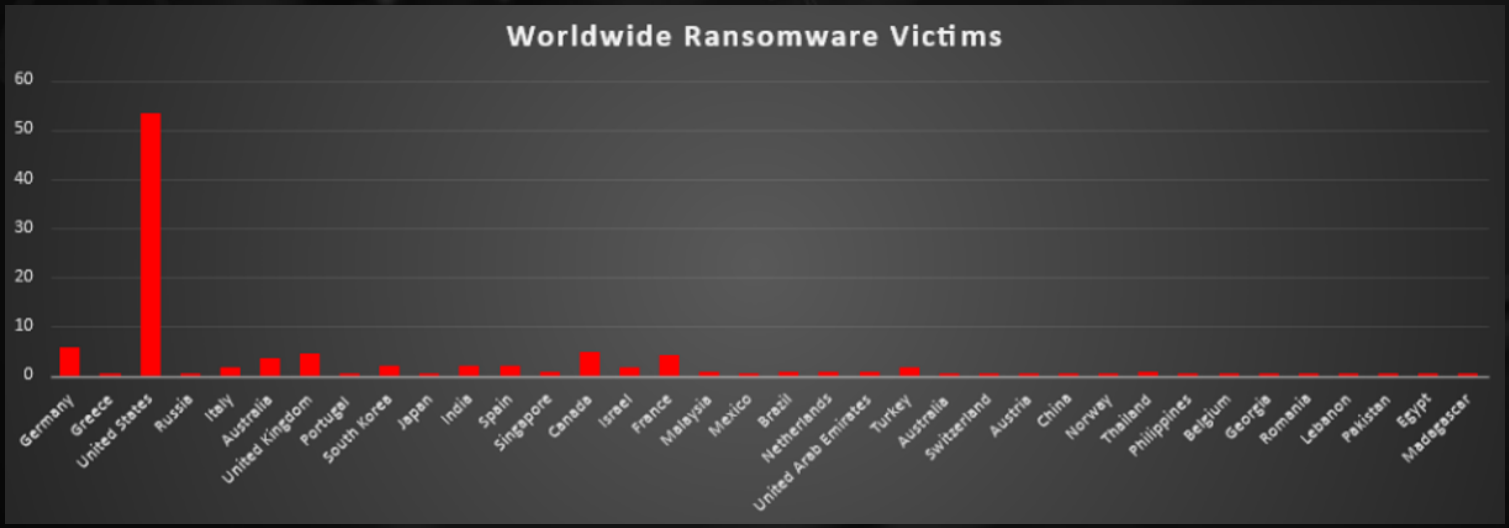


Figure 6: Ransomware Victims Worldwide

Industry-wide Ransomware Victims

Manufacturing remained the most heavily targeted sector, accounting for 17.28% (42 incidents) of all ransomware victims. The industry's reliance on continuous production, supply chains, and operational technology environments continues to make it a high-leverage target where downtime quickly translates into financial pressure.

Close behind was Business Services at 15.23% (37 incidents). Organisations in this category often provide outsourced services or operational support to multiple clients, meaning a single compromise can disrupt numerous downstream businesses. Law Firms (9.88%) and Retail (9.05%) formed the next tier, reflecting the value of sensitive legal data and the operational pressure associated with customer-facing commerce platforms.

A strong mid-tier included Construction (6.17%) and Architecture (5.35%), industries closely tied to infrastructure and project delivery cycles. Hospitality (4.12%), along with Transportation and IT (each 3.7%), also showed notable exposure, highlighting how service continuity and logistics operations remain attractive leverage points for ransomware groups.

Several sectors appeared with moderate activity, including Healthcare, Telecommunications, and Education (each 2.88%), Energy and Finance (each 2.47%), and Federal organisations and general Organisations (each 2.06%). These sectors often contain critical services or sensitive data, making them frequent but not always top-volume targets.

Lower-frequency industries included Insurance and Consumer Services (each 1.65%), Media & Internet (1.23%), and Real Estate, Minerals & Mining, Agriculture, and Electronics (each 0.82%).

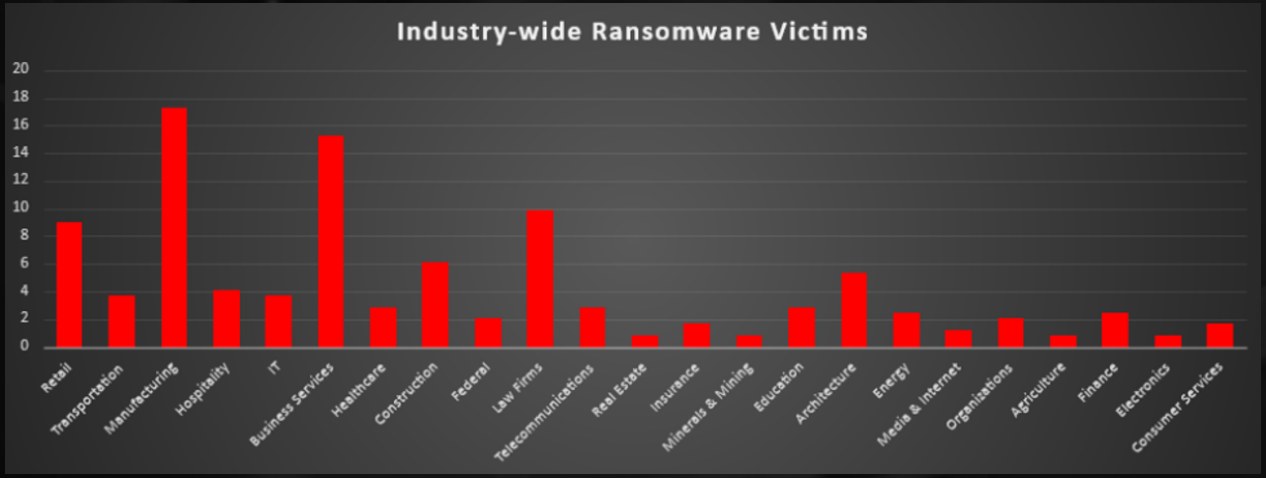


Figure 7: Industry-wide Ransomware Victims