Red Piranha
unified threat management

THREAT INTELLIGENCE REPORT

Jan 07 - 13, 2025

Report Summary:

- **New Threat Detection Added** – 2
  - Cyberhaven Chrome Extension Compromise
  - Tomiris
- **New Threat Protections - 389**

The following threats were added to Crystal Eye this week:

1. Cyberhaven Chrome Extension Compromise

In late December 2024, Cyberhaven, a cybersecurity firm specialising in Data Loss Prevention (DLP), experienced a significant security breach involving its Chrome browser extension. Attackers executed a phishing campaign targeting a Cyberhaven administrator, leading to unauthorised access to the company's Chrome Web Store account. This access allowed the attackers to upload a malicious version of the extension, which was automatically distributed to approximately 400,000 users. The compromised extension harvested sensitive data, including passwords and cookies, facilitating potential account takeovers. Cyberhaven detected the malicious activity within hours and promptly released a clean update to mitigate the threat. Further investigations revealed that this attack was part of a broader campaign affecting multiple Chrome extensions, collectively impacting over a million users.

Threats Protected: 120
Rule Set Type:

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

Class Type: Trojan-activity

Kill Chain:

Tactic	Technique ID	Technique Name
Initial Access	T1195	Supply Chain Compromise
Credential Access	T1555	Credentials from Password Stores

2. Tomiris

Tomiris is a Russian-speaking threat actor primarily focused on intelligence gathering within Central Asia, particularly targeting government and diplomatic entities in the Commonwealth of Independent States (CIS). Active since at least 2021, Tomiris is characterised by its rapid development and deployment of a diverse range of low sophistication "burner" implants written in various programming languages. These implants are often repeatedly deployed against the same targets using straightforward yet effective packaging and distribution techniques. Notably, Tomiris has experimented with unconventional delivery methods, such as DNS hijacking, and command-and-control (C2) channels, including the use of Telegram.

Threats Protected: 1
Rule Set Type:

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

Class Type: Trojan-activity

Kill Chain:

Tactic	Technique ID	Technique Name
Initial Access	T1566.002	Spearphishing Link
Execution	T1204.002	Malicious File
Persistence	T1547.001	Registry Run Keys / Startup Folder
Defence Evasion	T1027	Obfuscated Files or Information
Command-and-Control	T1095	Non-Application Layer Protocol

Known exploited vulnerabilities (Week 2 January 2024):

Vulnerability	CVSS	Description
CVE-2020-2883	9.8 (Critical)	Oracle WebLogic Server Unspecified Vulnerability
CVE-2024-55550	4.4 (Medium)	Mitel MiCollab Path Traversal Vulnerability
CVE-2024-41713	9.1 (Critical)	Mitel MiCollab Path Traversal Vulnerability
CVE-2025-0282	9.0 (Critical)	Ivanti Connect Secure, Policy Secure, and ZTA Gateways Stack-Based Buffer Overflow Vulnerability

For more information, please visit the **Red Piranha Forum**:
https://forum.redpiranha.net/t/known-exploited-vulnerabilities-catalog-2nd-week-of-january-2025/537

Updated Malware Signatures (Week 2 January 2024)

Threat	Description
Lumma Stealer	A type of malware classified as an information stealer. Its primary purpose is to steal sensitive information from infected systems, including but not limited to credentials, financial information, browser data, and potentially other personal or confidential information.
Mirai	A malware that turns networked devices running out-of-date Linux-based firmware—such as routers, IP cameras, and other Internet of Things (IoT) devices—into remotely controlled bots. These bots are then used as part of a botnet in large-scale Distributed Denial of Service (DDoS) attacks.

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 Group	Overall Percentage of total attack coverage
Apos	2.02%
FunkSec	2.02%
El Dorado	4.04%
Qilin	5.05%
Eraleign	25.25%
Eraleign (APT73)	5.05%
Rhysida	2.02%
LeakedData	3.03%
Hellcat	1.01%
Lynx	5.05%
Akira	16.16%
RansomHub	3.03%
SafePay	1.01%
8base	7.07%
Fog	1.01%
Morpheus	2.02%
Clop	2.02%
Abyss-data	1.01%
Termite	1.01%
Inc Ransom	2.02%
Space Bears	3.03%
Ransomware Blog	1.01%
Embargo	1.01%
Everest	3.03%
3AM	1.01%

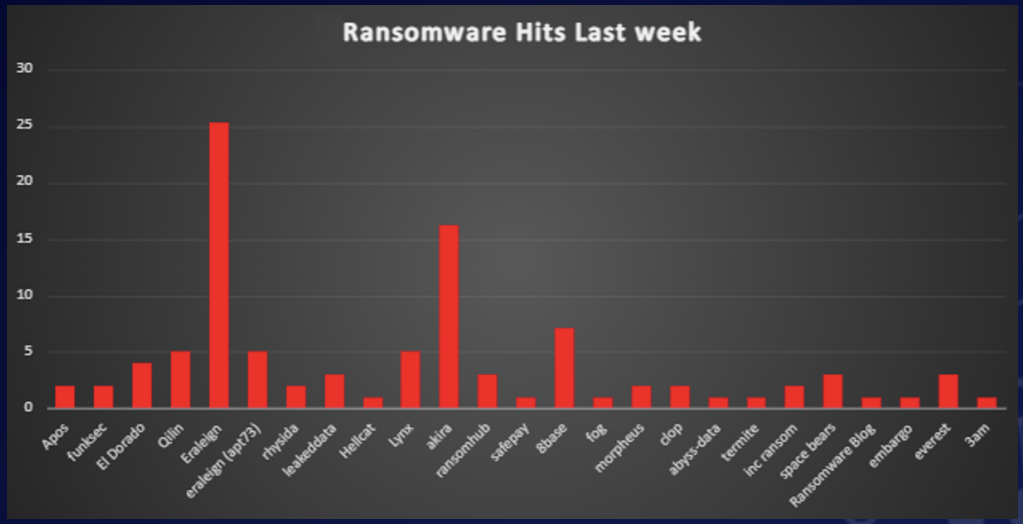

Figure 1: Ransomware Group Hits Last Week

FunkSec Ransomware

Group Emergence: FunkSec surfaced in late 2024, quickly claiming over 90+ victims since December.

Hacktivism-Cybercrime Blend: Some members have prior hacktivist links, and the group recycles data from older hacktivism campaigns, casting doubt on the authenticity of many leaks.

AI-Assisted Development: The group's custom ransomware, written in Rust, appears to be generated or heavily supported by AI tools, accelerating its iteration despite the apparent inexperience of its developers.

Low Ransom Demands: Demands as low as $10,000, coupled with discounted data sales, increase their visibility in cybercrime forums.

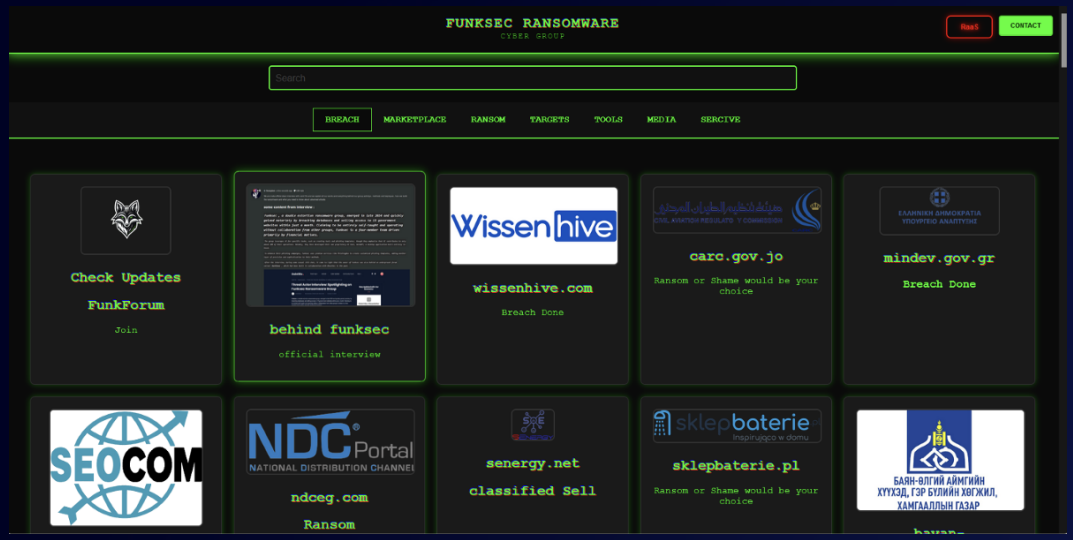

Figure 2: FunkSec Data Leak Site

Attack Methodology

- Double Extortion Tactics:
  - Data Theft: FunkSec steals sensitive files and threatens to publicly leak them.
  - File Encryption: The group encrypts victims' data using a Rust-based malware (with RSA/AES/ChaCha20 mechanisms).
  - Ransom Demand: Victims are pressured to pay to both unlock their data and prevent public leaks.
- Rapid Iteration & Publicity:
  - Their RaaS (Ransomware-as-a-Service) offering is updated frequently (new versions released days apart).
  - The group boasts about low antivirus detection by posting VirusTotal screenshots.
- Hacktivist-Style Messaging:
  - Despite typical cybercriminal behaviours, FunkSec's communications sometimes highlight political or ideological undertones, pointing to possible hacktivist elements.

Detailed TTPs

Initial Access & Privilege Escalation

- Uses various infiltration methods (not fully detailed in their statements) and checks for administrative rights using net session.
- When lacking privileges, the ransomware attempts to relaunch itself with elevated permissions (e.g., using PowerShell start-process -wait -Verb runas).

Defence Evasion

- Disables real-time monitoring in Windows Defender: Set-MpPreference -DisableRealtimeMonitoring $true
- Disables Security & Application event logging with wevtutil.
- Terminates processes/services (e.g., browsers, email clients, security tools) to prevent interference with encryption.

Once it has elevated privileges, the malware executes the following commands:

Command	Functionality
Set-MpPreference -DisableRealtimeMonitoring $true	Disable Windows Defender real-time protection.
wevtutil sl Security /e:false	Disable Security event logging.
wevtutil sl Application /e:false	Disable Application event logging.
Set-ExecutionPolicy Bypass -Scope Process -Force	Disable restrictions placed by the Powershell execution policy.
vssadmin delete shadows /all /quiet	predictably, delete shadow copy backups.

The terminate_processes function contains a hardcoded list of processes and services to terminate:

chrome.exe	firefox.exe	msedge.exe	explorer.exe	outlook.exe	vlc.exe
spotify.exe	skype.exe	discord.exe	steam.exe	java.exe	python.exe
node.exe	cmd.exe	powershell.exe	taskmgr.exe	wmplayer.exe	tscon.exe
notepad.exe	spooler	bits	dnsclient	lanmanworkstation	winmgmt
netsh	iphlpsvc	wuauserv	RemoteAccess	ShellHWDetection	SCardSvr
TrkWks	wscsvc	CryptSvc	msiserver	MpsSvc	defragsvc
upnphost	WindowsUpdate	srservice	wsmprovhost	AppIDSvc	AudioEndpointBuilder
Schedule	eventlog	PlugPlay	Netman	bthserv	ShellExperienceHost
SMB	WinDefend				

File Encryption Process
- Implements ChaCha20 (via Rust's orion.rs crate) for symmetric file encryption.
- Uses ephemeral keys generated by CryptGenRandom.
- Targets multiple drive letters and recursively encrypts files, appending .funksec extension.

Data Exfiltration & Publishing
- Steals data and hosts breach announcements on a data leak site (DLS).
- Threatens to sell or leak stolen data if victims refuse to pay.

Ransom Note Delivery
- Drops a ransom note (readme.me) with instructions for payment and contact.
- The note references FunkSec and, in some versions, Ghost Algeria—further indicating a developer based in Algeria.

AI-Enhanced Development
- Rust source code comments show signs of LLM-generated text.
- FunkSec released an AI chatbot using Miniapps to automate or assist malicious tasks (e.g., code suggestions, version updates).

IOCs
c233aec7917cf34294c19dd60ff79a6e0fac5ed6f0cb57af98013c08201a7a1c
66dbf939c00b09d8d22c692864b68c4a602e7a59c4b925b2e2bef57b1ad047bd
dcf536edd67a98868759f4e72bcbd1f4404c70048a2a3257e77d8af06cb036ac
b1ef7b267d887e34bf0242a94b38e7dc9fd5e6f8b2c5c440ce4ec98cc74642fb
5226ea8e0f516565ba825a1bbed10020982c16414750237068b602c5b4ac6abd
e622f3b743c7fc0a011b07a2e656aa2b5e50a4876721bcf1f405d582ca4cda22
20ed21bfdb7aa970b12e7368eba8e26a711752f1cc5416b6fd6629d0e2a44e5d
dd15ce869aa79884753e3baad19b0437075202be86268b84f3ec2303e1ecd966
7e223a685d5324491bcacf3127869f9f3ec5d5100c5e7cb5af45a227e6ab4603

Communication Via Session App:

Session
0538d726ae3cc264c1bd8e66c6c6fa366a3dfc589567944170001e6fdbea9efb3d
https://miniapps.ai/funksec

How to Mitigate:
- Deploy Robust Endpoint Security
- Implement Least Privilege & Access Controls
- Maintain Strict Patch Management
- Perform Frequent, Secure Backups
- Segment and Harden Networks
- Monitor and Log Key Events
- Secure Email & Web Gateways
- Leverage AI Defensively

Ransomware Victims Worldwide

A recent ransomware analysis reveals a striking 47.47% of global incidents targeted the United States, solidifying its position as the hardest-hit country by a significant margin. Trailing behind, the United Kingdom experienced 8.08% of attacks, followed by France at 5.05%.

Other significantly affected countries include Australia, Germany, Italy, and Canada, each accounting for 3.03% of reported attacks. Meanwhile, Argentina, Peru, and Brazil each reported 2.02% of the total incidents.

Nations such as India, Europe, Switzerland, Romania, Paraguay, Poland, Bolivia, Dominican Republic, Turkey, Kenya, Netherlands, Belgium, Sweden, Thailand, Armenia, South Africa, Oman, Ireland, Spain, Colombia, and Japan each reported 1.01% of the total ransomware incidents, indicating a widespread—albeit lower-level—impact across various regions.

This analysis underscores the global and persistent nature of ransomware threats, with North America and parts of Europe continuing to bear the brunt of the attacks, followed closely by multiple regions worldwide. These findings highlight the urgent need for heightened cybersecurity measures and proactive defences across all areas to combat the ever-evolving ransomware landscape.

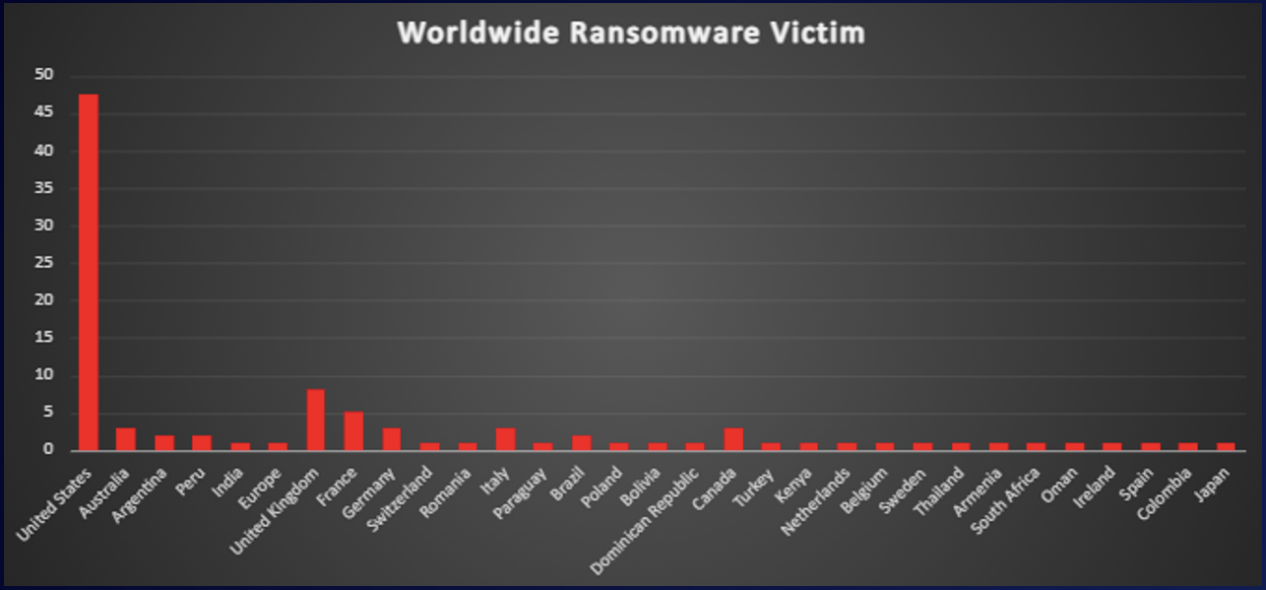

Figure 3: Ransomware Victims Worldwide

Ransomware Victims Industry-wide

A recent ransomware analysis highlights the Manufacturing sector as the most heavily targeted industry, accounting for 14.14% of total reported incidents. This underscores the critical vulnerability of essential production and supply chain operations to cyber threats.

Following Manufacturing, Business Services reported 13.13% of attacks, while Technology Services stood at 12.12%. Other heavily impacted sectors include Construction at 8.08%, Retail at 7.07%, and both Financial Services and Healthcare at 6.06% each.

Additional industries with notable impact include Media & Internet (3.03%) and Education (3.03%). Sectors such as Agriculture, Mining, IT, Law Firms, Transportation, Organisations, and Consumer Services each experienced 2.02% of the total incidents. Meanwhile, Food Services, Food, Logistics, Telecommunications, Entertainment, Government, Finance, Insurance, Energy, Real Estate, and Law Firms each reported 1.01% of attacks, indicating a more limited but still significant footprint.

This analysis underscores the broad and indiscriminate nature of ransomware threats, affecting a diverse range of industries worldwide. The findings highlight the urgent need for tailored cybersecurity strategies across both critical and emerging sectors to mitigate the ever-evolving ransomware landscape effectively.

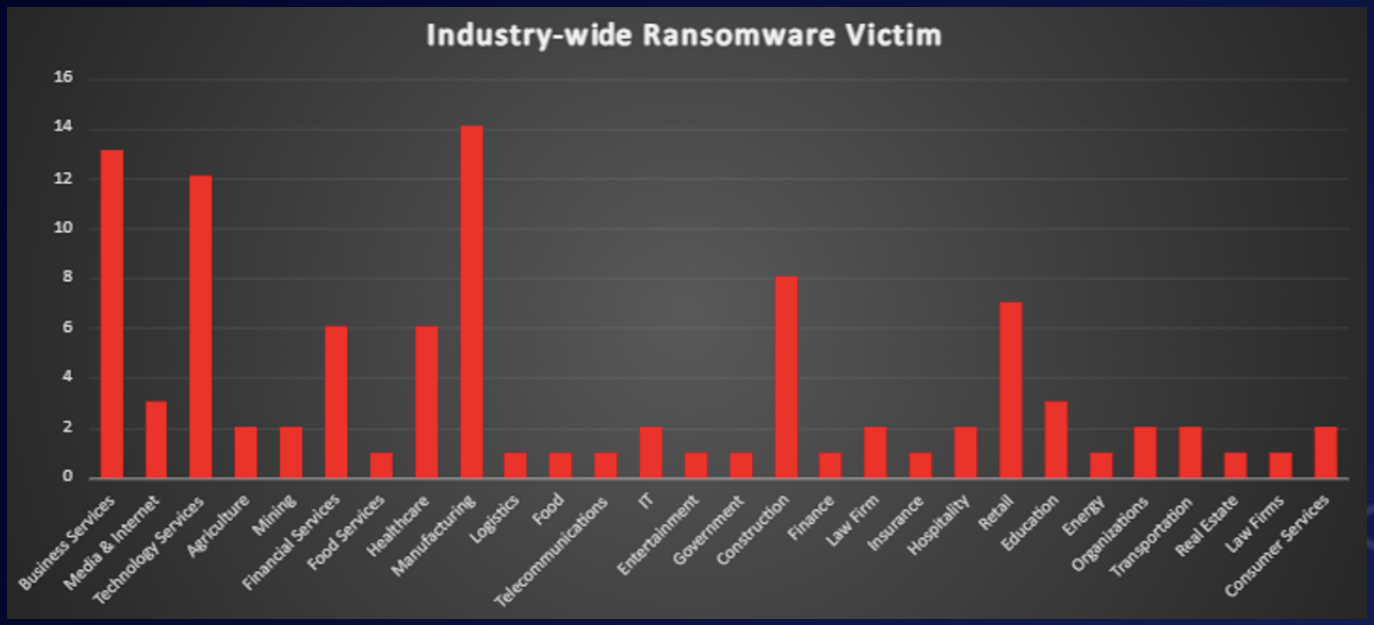

Figure 4: Industry-wide Ransomware Victims