Red Piranha
unified threat management

THREAT INTELLIGENCE REPORT

Dec 03 - 09, 2024

Report Summary:

- **New Threat Detection Added** – 2 (Earth Kasha APT – LODEINFO malware and Zabbix SQL Injection (CVE-2024-42327))
- **New Threat Protections - 195**

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

1. Earth Kasha APT – LODEINFO malware

Since 2019, the cyber-espionage group Earth Kasha has been deploying LODEINFO malware, primarily targeting Japanese organisations. In early 2023, their operations expanded to include entities in Taiwan and India, focusing on advanced technology sectors and government agencies. The group has diversified its initial access methods, now exploiting public-facing applications such as SSL-VPNs and file storage services. LODEINFO facilitates unauthorised access, data exfiltration, and prolonged persistence within compromised networks.

Threats Protected: 3
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	T1566.001	Spearphishing Attachment
Persistence	T1574.002	DLL Side Loading
Execution	T1204.002	Malicious File
Command-and-Control	T1071.001	Application Layer Protocol: Web Protocols

2. Zabbix SQL Injection (CVE-2024-42327)

A critical SQL injection vulnerability has been identified in Zabbix, an open-source monitoring tool. This flaw, designated as CVE-2024-42327 with a CVSS score of 9.9, allows non-administrator users with API access to execute arbitrary SQL queries. Successful exploitation of this vulnerability could grant attackers full control over affected Zabbix instances. Affected versions include 6.0.0 to 6.0.31, 6.4.0 to 6.4.16, and 7.0.0. It is strongly recommended that the latest patched versions be updated to mitigate the associated risks.

Threats Protected: 01
Rule Set Type:

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

Class Type: Trojan-activity

Kill Chain:

Tactic	Technique ID	Technique Name
Initial Access	T1190	Exploit Public-Facing Application

Known exploited vulnerabilities (Week 1 December 2024):

Vulnerability	CVSS	Description
CVE-2024-11667	9.8 (Critical)	Zyxel Multiple Firewalls Path Traversal Vulnerability
CVE-2024-11680	9.8 (Critical)	ProjectSend Improper Authentication Vulnerability
CVE-2023-45727	7.5 (High)	North Grid Proself Improper Restriction of XML External Entity (XXE) Reference Vulnerability
CVE-2024-51378	9.8 (Critical)	CyberPanel Incorrect Default Permissions Vulnerability

For more information, please visit the **Red Piranha Forum**:
https://forum.redpiranha.net/t/known-exploited-vulnerabilities-catalog-1st-week-of-december-2024/529

Updated Malware Signatures (Week 1 December 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.
Remcos	Remcos functions as a remote access trojan (RAT), granting unauthorised individuals the ability to issue commands on the compromised host, record keystrokes, engage with the host's webcam, and take snapshots. Typically, this malicious software is distributed through Microsoft Office documents containing macros, which are often attached to malicious emails.

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
Trinity	0.82%
Dragonforce	1.64%
Sarcoma	7.38%
Eraleign (APT73)	5.74%
Embargo	0.82%
RansomHub	19.67%
Inc ransom	0.82%
Bianlian	2.46%
Qilin	4.1%
Medusa	4.1%
Brain Cipher	2.46%
Hunters	1.64%
Daixin	1.64%
Darkvault	0.82%
8base	4.92%
Lynx	2.46%
Fog	1.64%
Handala	0.82%
Rhysida	0.82%
Funksec	9.02%
Blackbasta	8.2%
Lockbit3	0.82%
Cloak	0.82%
RA Group	1.64%
3AM	0.82%
Killsec3	0.82%
Nitrogen	0.82%
Space Bears	0.82%
RansomHouse	2.46%
Play	3.28%
SafePay	1.64%
Abyss-data	0.82%
Termite	0.82%
Everest	0.82%
Interlock	0.82%
Kairos	0.82%

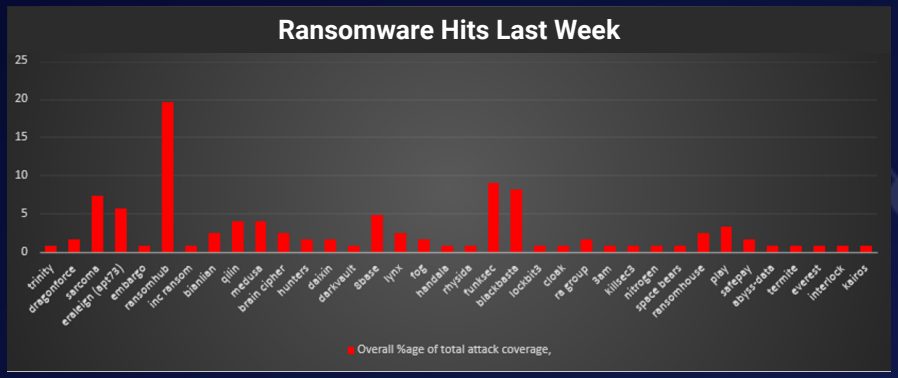

Figure 1: Ransomware Group Hits Last Week

Funksec Ransomware Group

Funksec Ransomware based on the latest analysis conducted in December 2024, researchers identified a novel ransomware variant named Funksec ransomware, marking its entry into the threat landscape. This extortion-focused operation leverages a unique approach by creating a Tor-based data-leak site (DLS) to centralise its ransomware activities. Funksec ransomware employs a double-extortion strategy, exfiltrating sensitive data and threatening public exposure if demands are unmet. Key characteristics of Funksec ransomware include its emphasis on victim-shaming through data leaks and its operational rhetoric of leveraging DDoS tools for additional extortion.

Detailed TTPs

Initial access methods for Funksec ransomware are currently unknown, but ransomware groups often employ techniques such as vulnerability exploitation, brute-forcing credentials, or purchasing access from Initial Access Brokers (IABs). Tools and methods associated with Funksec operations include:

- Development of a custom DDoS tool for additional leverage.
- Hosting breach information on a Tor-based DLS.
- Posting victim details, leaked data, and tool downloads on its DLS.

The DLS includes three main pages:

- BREACH: Displays victim listings with breach statuses and downloadable leaked data.
- TOOLS: Offers a free DDoS tool written in Python, capable of HTTP and UDP floods.

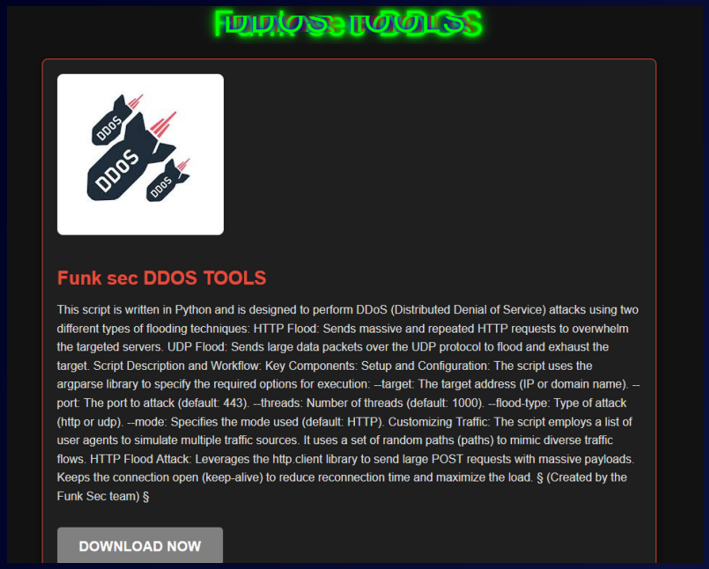

Figure 2: DDoS tool page on Funksec's DLS

- RANSOM: Currently under construction, expected to host ransom payment details and further attack information.

Indicator Of Compromise (IOCs)

- Known Tor DLS links:
  - http://7ixfdvqb4eaju5lzj4gg76kwlrxg4ugqpuog5oqkkmgfyn33h527oyyd.onion
  - http://pke2vht5jdeninupk7i2thcfvxegsue6oraswpka35breuj7xxz2erid.onion
  - http://ykqjcrptcai76ru5u7jhvspkeizfsvpgovton4jmreawj4zdwe4qnlid.onion
- DDoS tool download link: Active as of December 2024 on gofile.io.
- Latest IOCs:
  - IPv4: 181.224.231.148
  - IPv4: 207.180.201.194
  - FileHash-MD5: 9b9b18360d7bae6349cb828f0eb22306
  - FileHash-MD5: c21b18ab9db3f180927d4fe82d82ec60
  - FileHash-SHA1: 3e38b20b5a1f43f7a0720403857e220338377037
  - FileHash-SHA1: 7726d70eb75a66c4cf1bd74576108bfb5753d4a6
  - SHA256: 1a7ac94f8a2cbbcad2cb25a1aaf16cfe1e1156445e859a1822c834b21b564dfb
  - SHA256: e7c5a3df933efa32853ef85a22b55c9e99d10feb5b929ae514096106c63228c4
  - IPv4: 51.77.140.4
  - URL: http://181.224.231.148/verificativa.sql

Threat Assessment Funksec ransomware appears to have significant technical capabilities and a structured approach to ransomware operations, leveraging a Tor-based DLS to enhance its visibility and impact. With its multi-extortion methods and custom tool development, the group presents a growing threat to organisations globally.

Mitigations:

1. **Employee Training**: Provide regular training to employees to recognise phishing attempts and avoid actions that could lead to initial access by threat actors.
2. **Monitor Dark Web Activity**: Actively monitor threat intelligence feeds and dark web forums for indicators related to your organisation or industry.
3. **Restrict Access**: Limit user privileges and employ multi-factor authentication to reduce the risk of credential compromise.
4. **Develop an Incident Response Plan**: Establish and regularly test a detailed incident response plan to mitigate the impact of ransomware incidents.
5. **Enhance Network Security Measures**: Implement advanced firewalls, intrusion detection systems, and endpoint protection to monitor and block malicious activities.

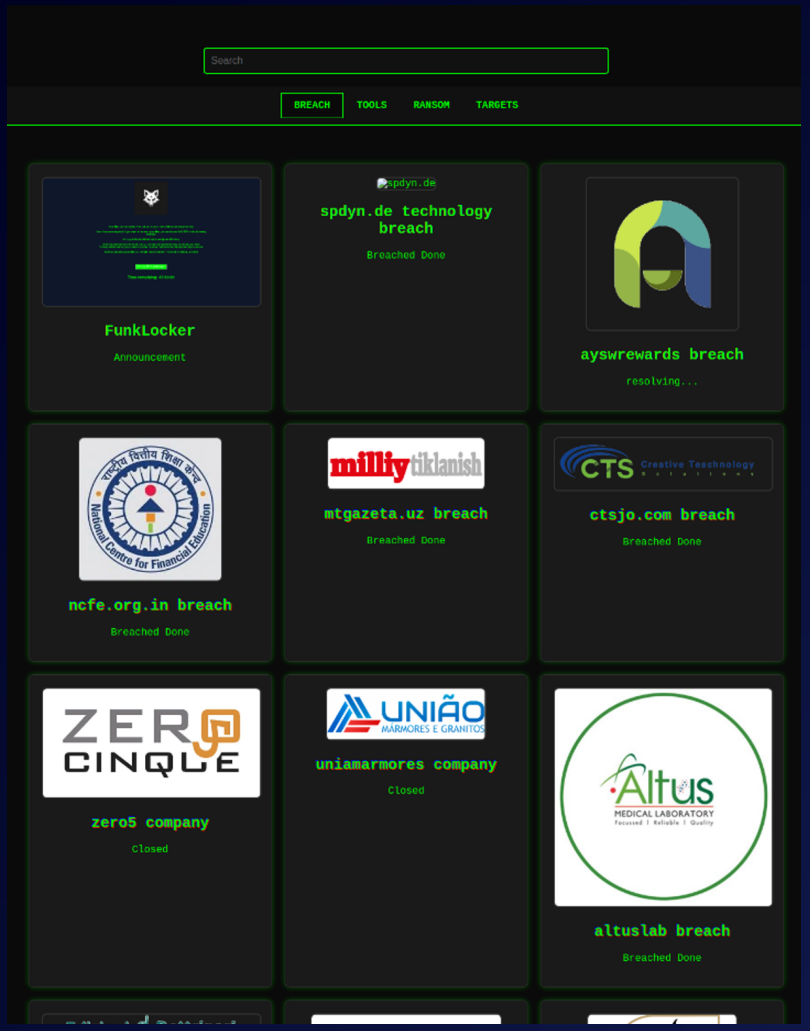

Figure 3: Victim listings on the Funksec DLS

Ransomware Victims Industry-wise

Based on the analysis of ransomware attacks across various industries, the data highlights notable trends in attack distribution:

- Manufacturing (13.93%) emerged as the most targeted sector during the specified period. This is indicative of the criticality of the manufacturing industry and the potential impact of disruptions in supply chains.
- Retail (9.84%) and Construction (9.84%) were also heavily impacted, highlighting the vulnerability of industries with significant operational dependencies and customer-facing services.
- Business Services (8.2%) experienced a substantial share of attacks, emphasising the persistent threat to organisations offering a broad range of professional services.
- Finance (4.1%) and sectors like Hospitals (3.28%), Telecommunications (3.28%), Transportation (3.28%), and Accounting Services (3.28%) also faced significant risks, underscoring the expansive reach of ransomware threats across essential service providers.

Smaller but critical industries such as Federal (1.64%), Agriculture (1.64%), and Law Firms (1.64%) were not spared, reflecting the diverse and pervasive nature of these attacks.

This analysis highlights the extensive reach of ransomware across industries, emphasising the urgent need for cross-sector collaboration, enhanced threat detection, and robust incident response plans. The broad targeting patterns demonstrate that all industries, regardless of size or digital reliance, must prioritise cybersecurity to mitigate risks effectively.

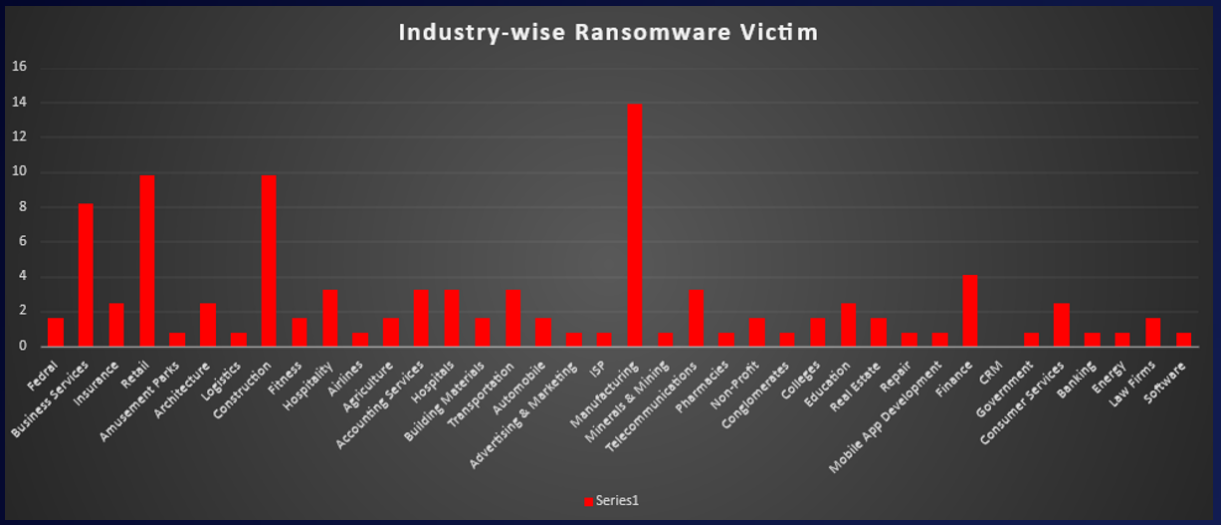

Figure 4: Industry-wise Ransomware Victims

Ransomware Victims Worldwide

A recent ransomware analysis reveals a striking 52.46% of global incidents targeted the United States, making it the hardest-hit country by far. Trailing behind, the United Kingdom experienced 6.56% of attacks, while Canada reported 3.28%. Australia, Italy, France, and Germany each faced 3.28% to 4.1% of the attacks, reflecting notable vulnerabilities in these regions.

Brazil (5.74%) saw a significant percentage of incidents, highlighting its exposure to ransomware threats. Meanwhile, countries such as Spain, India, and Japan contributed 1.64% or less of total incidents, demonstrating a broader geographical reach. Other countries like Saudi Arabia, Pakistan, and South Korea each reported 0.82%, emphasising the far-reaching nature of these attacks.

This analysis demonstrates the widespread nature of ransomware attacks, with North America and Europe bearing the brunt of these persistent threats. These numbers emphasise the urgent need for enhanced cybersecurity measures across these heavily targeted regions, especially in the United States, which remains the prime focus of attackers.

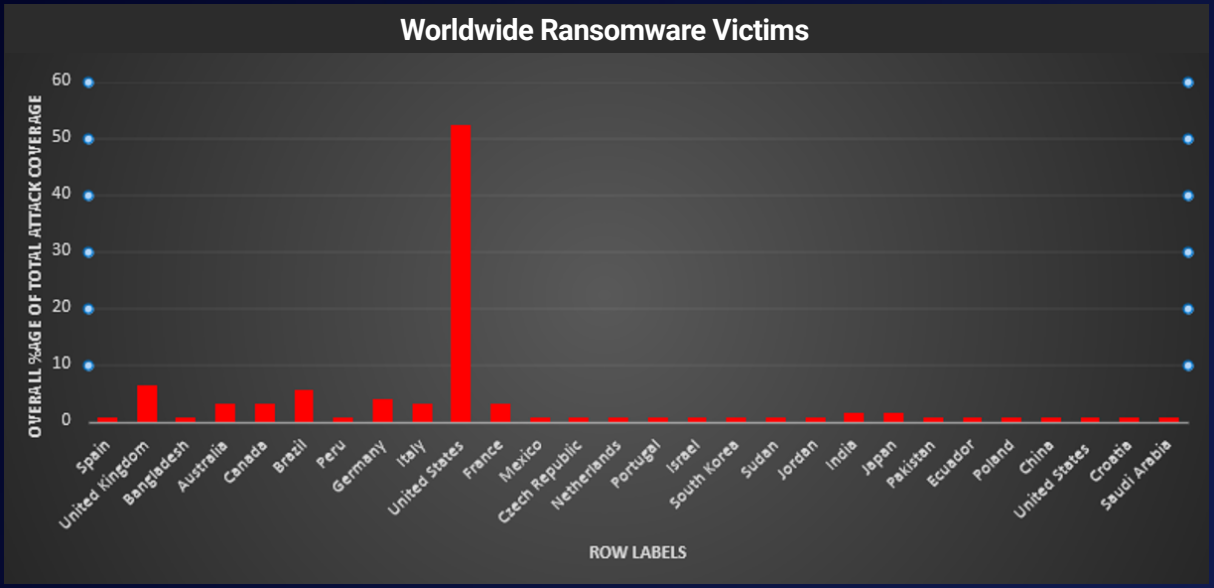

Figure 5: Ransomware Victims Worldwide