Red Piranha
unified threat management

THREAT INTELLIGENCE REPORT

Dec 24 - 30, 2024

Report Summary:

- **New Threat Detection Added** – 2
  - Craft CMS Template Path Injection RCE (CVE-2024-56145)
  - LandUpdate808 Fake Update Variant
- **New Threat Protections - 133**

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

1. Craft CMS Template Path Injection RCE (CVE-2024-56145)

A critical vulnerability has been identified in Craft CMS, a widely used PHP-based content management system with over 150,000 installations globally. The issue arises from the misuse of the register_argc_argv PHP configuration directive, which, when enabled, allows attackers to pass command-line arguments via the URL query string. This can lead to unauthorised inclusion of remote templates through the –templatesPath parameter, resulting in remote code execution (RCE). The vulnerability affects Craft CMS versions prior to 4.13.1 and 5.5.1. Administrators are strongly advised to update to the latest versions to mitigate this risk.

Threats Protected: 01
Rule Set Type:

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

Class Type: Attempted-admin

Kill Chain:

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

2. LandUpdate808 Fake Update Variant

LandUpdate808 is a recently identified fake update malware variant that deceives users into downloading malicious payloads by presenting fraudulent software update prompts. Unlike other fake update malware such as SocGholish, LandUpdate808 employs a distinct delivery mechanism involving specific URI patterns like /p/land.php and /wp-content/uploads/update.php. The malware's payloads are typically named following the pattern update_DD_MM_YYYY_####### and have been observed with .js, .exe, or .msix extensions. The initial infection vector involves injecting malicious scripts into compromised websites, which then display fake update pages to visitors, prompting them to download and execute the malicious payload.

Threats Protected: 14
Rule Set Type:

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

Class Type: Trojan-activity

Kill Chain:

Tactic	Technique ID	Technique Name
Initial Access	T1566.002	Spearphishing Link
Execution	T1059.001	Command and Scripting Interpreter
Defence Evasion	T1218.010	System Binary Proxy Execution: Regsvr32
Command-and-Control	T1071.001	Web Protocols

Known exploited vulnerabilities (Week 4 December 2024):

Vulnerability	CVSS	Description
CVE-2021-44207	8.1 (High)	Acclaim Systems USAHERDS Use of Hard-Coded Credentials Vulnerability

For more information, please visit the **Red Piranha Forum**:
https://forum.redpiranha.net/t/known-exploited-vulnerabilities-catalog-4th-week-of-december-2024/534

Updated Malware Signatures (Week 4 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.
Nanocore	The Nanocore trojan, built on the .NET framework, has been a subject of multiple source code leaks, resulting in its widespread accessibility. Similar to other remote access trojans (RATs), Nanocore empowers malicious actors with complete system control, enabling activities such as video and audio recording, password theft, file downloads, and keystroke logging.

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
KillSec3	18.1%
Abyss-Data	0.95%
FunkSec	13.33%
Monti	0.95%
8Base	0.95%
RA group	5.71%
Hunters	2.86%
Cactus	2.86%
Eraleign (APT73)	3.81%
RansomHub	4.76%
Fog	5.71%
Akira	11.43%
Everest	1.9%
Lockbit3	2.86%
Qilin	2.86%
Sarcoma	3.81%
Lynx	0.95%
El Dorado	0.95%
Hellcat	1.9%
SafePay	2.86%
Handala	0.95%
Rhysida	0.95%
Bianlian	0.95%
Ciphbit	0.95%
Interlock	0.95%
Inc ransom	2.86%
RansomHouse	2.86%

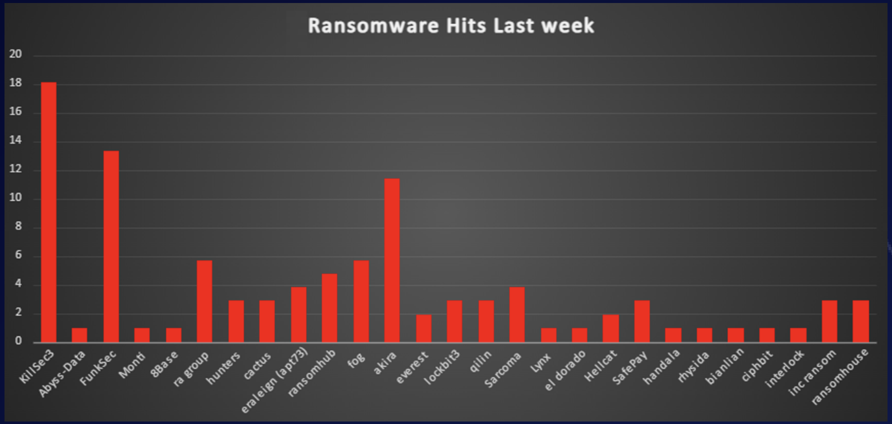


Figure 1: Ransomware Group Hits Last Week

Abyss Locker Ransomware Analysis

Overview

Abyss Locker ransomware operations, in their current form, emerged in March 2023, aggressively targeting VMware ESXi environments. Abyss Locker functions as a multi-extortion group, leveraging a TOR-based website to list victims and exfiltrated data if ransom demands are unmet.

Historical Background

- In January 2023, a threat actor named "infoleak222" shared data on the now-defunct Breached forums, correlating with data on the Abyss Locker website.
- Previous Abyss variants, including a Windows variant, date back to 2019.

Attack Methodology

Initial Access

- Exploitation of weak SSH configurations (via SSH brute-force attacks) is a common entry point.

Payload and Execution

- Abyss Locker payloads for Linux are derived from the Babuk codebase.
- The ransomware uses a command-line interface requiring specific arguments for encryption:
  Usage: %s [-m (5-10-20-25-33-50) -v -d] Start Path
  m: Encryption mode or percentage
  v: Verbose mode
  d: Daemon (persistence)

Targeting VMware ESXi

Abyss Locker uses "esxcli" commands to manage and encrypt virtual machines:

- esxcli vm process list
- esxcli vm process kill -t=force -w=%d
- esxcli vm process kill -t=hard -w=%d
- esxcli vm process kill -t=soft -w=%d

Encrypted files carry the ".crypt" extension, and directories contain ransom notes named ".README_TO_RESTORE".

Detailed TTPs

Abyss Locker ransomware employs a variety of Tactics, Techniques, and Procedures (TTPs) across the attack lifecycle:

1. Initial Access (T1078)
   - Exploitation of exposed SSH services through brute-force attacks.
   - Vulnerability exploitation in ESXi hypervisors.
2. Execution (T1059)
   - Deployment of Babuk-derived ransomware payloads.
   - Manual execution of encryption commands using the CLI.
3. Persistence (T1078.004)
   - Daemon mode enabled for long-term presence.
4. Privilege Escalation (T1068)
   - Exploiting misconfigurations in ESXi permissions.
5. Defence Evasion (T1070.004)
   - Disabling security tools and services on ESXi servers.
   - Use of legitimate tools (e.g., esxcli) to blend malicious activities.
6. Credential Access (T1552)
   - Harvesting credentials from compromised SSH sessions.
7. Discovery (T1083)
   - Scanning for virtual machines and active services.
8. Lateral Movement (T1021.004)
   - Moving across hypervisor systems within the network.
9. Impact (T1486)
   - Encryption of virtual machine data.
   - Deployment of ransom notes.

IOCs (Indicators of Compromise)

FileHash-MD5:

- 18baedf43f4a68455e8d36b657aff03c (Ransom:Win32/Babuk.SIB!MTB)
- 89d397164f57d3d0731c7c577b8e5be4 (is__elf)
- f29980170738505583547d8203838888 (Ransom:Win32/Babuk.SIB!MTB)

FileHash-SHA1:

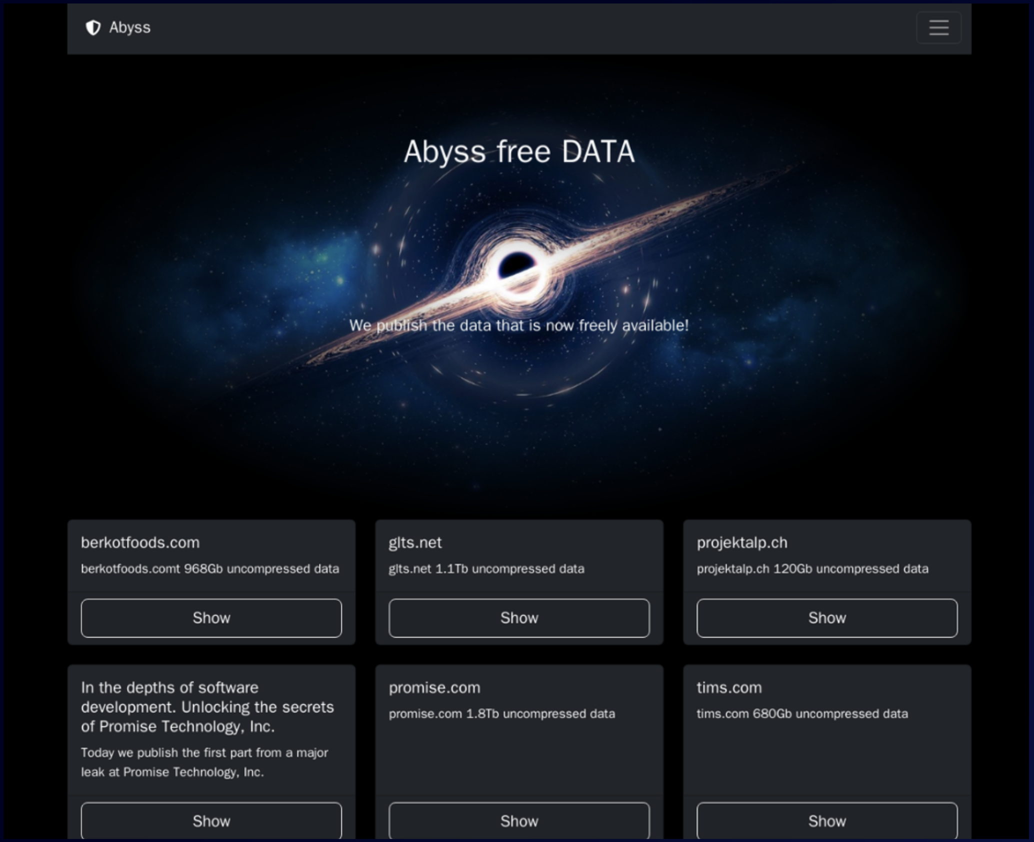
- 40ceb71d12954a5e986737831b70ac669e8b439e (is__elf)
- 4402a8888ee408f39dd51135ca1b69819916c0af (Ransom:Win32/Babuk.SIB!MTB)
- 5770b7c3931f6ed12650ad27b7fb2bf0752b80dc (Ransom:Win32/Babuk.SIB!MTB)

FileHash-SHA256:

- 056220ff4204783d8cc8e596b3fc463a2e6b130db08ec923f17c9a78aa2032da
- 0763e887924f6c7afad58e7675ecfe34ab615f4bd8f569759b1c33f0b6d08c64 (Ransom:Win32/Babuk.SIB!MTB)
- 1a31b8e23ccc7933c442d88523210c89cebd2c199d9ebb88b3d16eacbefe4120
- 1d04d9a8eeed0e1371afed06dcc7300c7b8ca341fe2d4d777191a26dabac3596

How to Mitigate:

1. Anti-Malware Tools: Use software capable of detecting ransomware through signatures, heuristics, and machine learning.
2. Network Traffic Monitoring: Look for unusual traffic patterns and connections to known command-and-control servers.
3. Security Audits: Regular vulnerability assessments.
4. Employee Training: Educate staff on recognising phishing emails and suspicious activity.
5. Backup and Recovery Plan: Ensure robust backup strategies for rapid recovery.



Abyss

Abyss free DATA

We publish the data that is now freely available!

berkotfoods.com

berkotfoods.comt 968Gb uncompressed data

Show

glts.net

glts.net 1.1Tb uncompressed data

Show

projektalp.ch

projektalp.ch 120Gb uncompressed data

Show

In the depths of software development. Unlocking the secrets of Promise Technology, Inc.

Today we publish the first part from a major leak at Promise Technology, Inc.

Show

promise.com

promise.com 1.8Tb uncompressed data

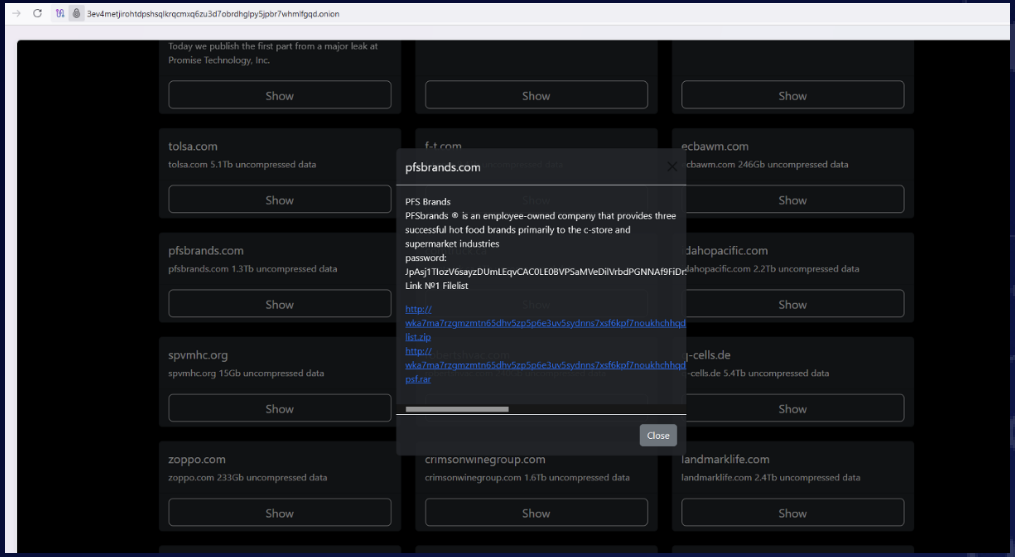
Show

tims.com

tims.com 680Gb uncompressed data

Show

Leaked Data:



3ev4metjirohtdpshsqlkrqcmxq6zu3d7obrdhglpy5jpbr7whmlfgqd.onion

Today we publish the first part from a major leak at Promise Technology, Inc.

Show

Show

Show

tolsa.com

tolsa.com 5.1Tb uncompressed data

Show

f-t.com

ecbawm.com

ecbawm.com 246Gb uncompressed data

Show

pfsbrands.com

pfsbrands.com 1.3Tb uncompressed data

Show

idahopacific.com

idahopacific.com 2.2Tb uncompressed data

Show

spvmhc.org

spvmhc.org 15Gb uncompressed data

Show

q-cells.de

q-cells.de 5.4Tb uncompressed data

Show

pfsbrands.com

PFS Brands
PFSbrands ® is an employee-owned company that provides three successful hot food brands primarily to the c-store and supermarket industries
password:
JpAsj1TlozV6sayzDUmLEqvCAC0LE0BVPSaMVeDilVrbdPGNNAf9FiDr
Link №1 Filelist

http://wka7ma7rzgmzmtn65dhv5zp5p6e3uv5sydnns7xsf6kpf7noukhchhqd
list.zip
http://wka7ma7rzgmzmtn65dhv5zp5p6e3uv5sydnns7xsf6kpf7noukhchhqd
psf.rar

Close

zoppo.com

zoppo.com 233Gb uncompressed data

Show

crimsonwinegroup.com

crimsonwinegroup.com 1.6Tb uncompressed data

Show

landmarklife.com

landmarklife.com 2.4Tb uncompressed data

Show

Ransomware Victims Worldwide

A recent ransomware analysis reveals a striking 53.33% of global incidents targeted the United States, solidifying its position as the hardest-hit country by a significant margin. Trailing behind, Canada experienced 5.71% of attacks, while Argentina and Israel each reported 3.81% of the total incidents.

Other significantly affected countries include Brazil and Australia, each accounting for 2.86% of reported attacks. Following them, nations such as UAE, Spain, Egypt, Algeria, Indonesia, and Mexico each reported 1.9% of the total ransomware incidents.

Meanwhile, a diverse group of nations, including United Kingdom, Germany, Greece, Latvia, Taiwan, France, South Africa, India, El Salvador, Finland, Turkey, Switzerland, Chile, Italy, Netherlands, and China, each experienced a limited impact, representing just 0.95% of the total incidents.

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

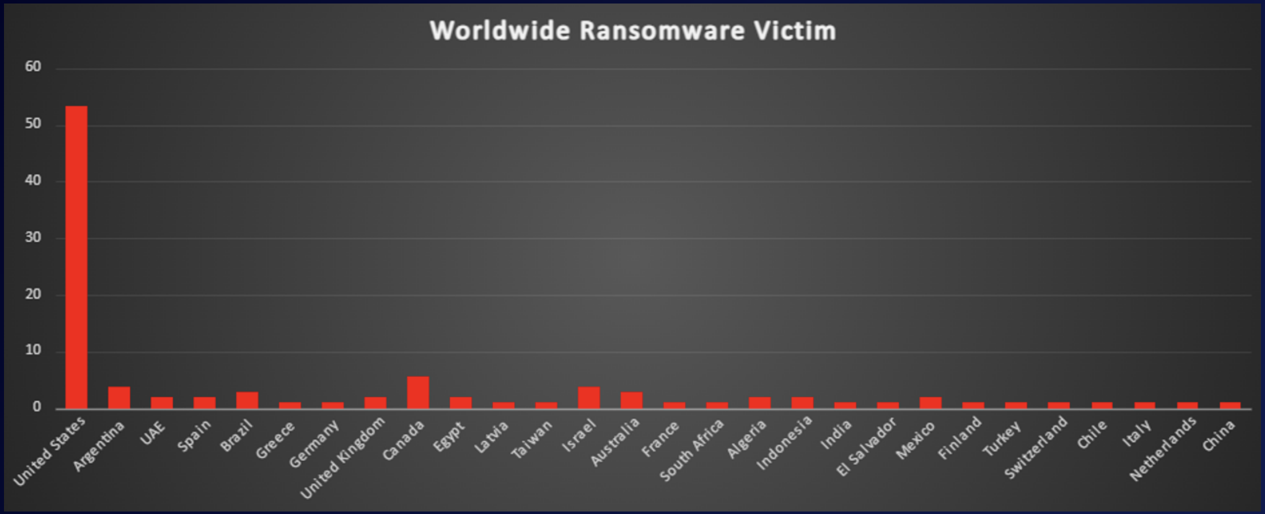


Figure 4: Ransomware Victims Worldwide

Ransomware Victims Industry-wide

A recent ransomware analysis highlights the Manufacturing sector as the most heavily targeted industry, accounting for a significant 27.62% of total reported incidents. This underscores the critical vulnerability of essential production and supply chain operations to cyber threats.

Following Manufacturing, Business Services reported 8.57% of attacks, while Retail accounted for 7.62%. Other heavily impacted sectors include Construction, Healthcare, and Law Firms, each experiencing 5.71% of the total incidents. The Hospitality industry followed closely with 4.76%, while Food, Transportation, Finance, and Consumer Services each faced 3.81% of attacks.

Sectors such as Electricity, Real Estate, Automotive, IT, and Education each reported 1.9% of ransomware incidents.

Meanwhile, industries experiencing a more limited impact, each representing 0.95% of the total attacks, include Chemical Manufacturing, Logistics, IT Services, Car Rental Services, Financial Services, Telecommunications, Government, Organisations, Federal, and Media & Internet.

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

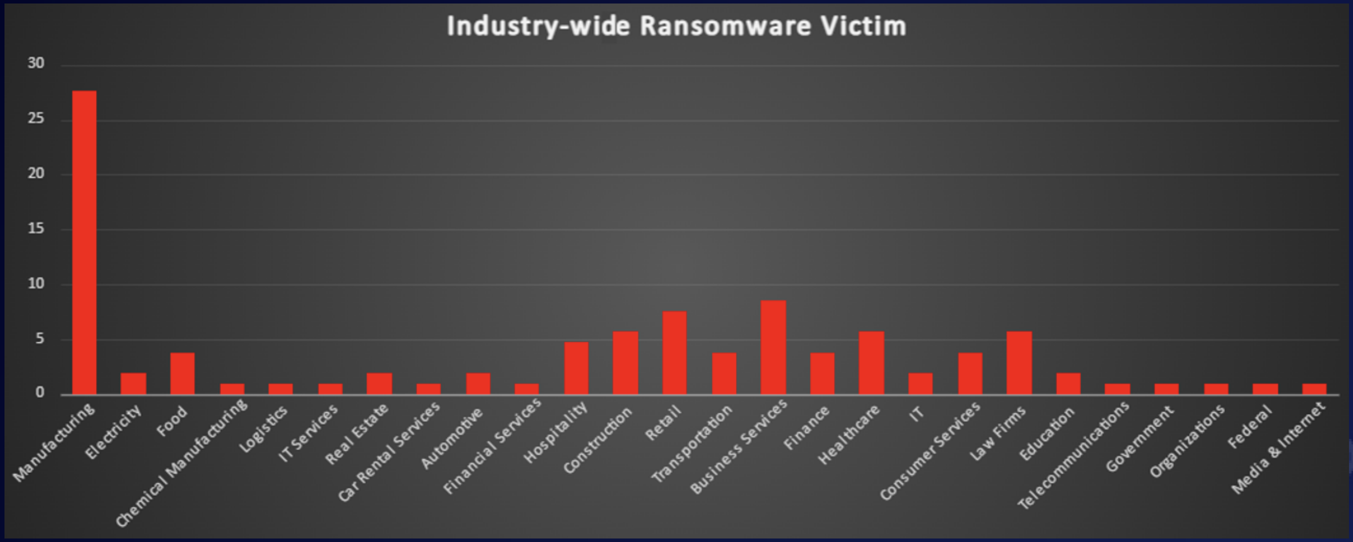


Figure 5: Industry-wide Ransomware Victims