Red Piranha
unified threat management

THREAT INTELLIGENCE REPORT

Dec 17 - 23, 2024

Report Summary:

- **New Threat Detection Added** – 2
  - FortiWLM Unauthenticated SQL Injection (CVE-2023-34991)
  - Operation Crimson Palace - XiebroC2 CnC
- **New Threat Protections - 178**

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

1. FortiWLM Unauthenticated SQL Injection (CVE-2023-34991)

Fortinet's Wireless LAN Manager (FortiWLM) has been found to contain several critical security vulnerabilities that could allow remote attackers to fully compromise the system. These vulnerabilities include unauthenticated command injection (CVE-2023-34993), unauthenticated SQL injection (CVE-2023-34991), and unauthenticated arbitrary file read (CVE-2023-42783). Exploiting these flaws could lead to unauthorised command execution, database manipulation, and access to sensitive files, respectively. FortiWLM is commonly deployed in large enterprise environments, making these vulnerabilities particularly concerning. Fortinet has released patches to address these issues, and it is strongly recommended that affected organisations apply these updates promptly.

Threats Protected: 01
Rule Set Type:

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

Class Type: Attempted-admin

Kill Chain:

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

2. Operation Crimson Palace - XiebroC2 CnC

Operation Crimson Palace is a sophisticated cyberespionage campaign attributed to Chinese state-sponsored actors, targeting government agencies and public service organisations in Southeast Asia. The campaign employs advanced tactics, including DLL sideloading, to deploy custom malware such as "TattleTale," a previously undocumented keylogger. The attackers have demonstrated adaptability by shifting to open-source tools and varying their command-and-control (C2) channels to evade detection. Notably, compromised infrastructure within the same verticals has been leveraged to stage malware and relay C2 communications, indicating a strategic approach to blending into the targeted environments.

Threats Protected: 05
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
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 3 December 2024):

Vulnerability	CVSS	Description
CVE-2024-35250	7.8 (High)	Microsoft Windows Kernel-Mode Driver Untrusted Pointer Dereference Vulnerability
CVE-2024-20767	7.4 (High)	Adobe ColdFusion Improper Access Control Vulnerability
CVE-2024-55956	9.8 (Critical)	Cleo Multiple Products Unauthenticated File Upload Vulnerability
CVE-2021-40407	9.8 (Critical)	Reolink RLC-410W IP Camera OS Command Injection Vulnerability
CVE-2019-11001	7.2 (High)	Reolink Multiple IP Cameras OS Command Injection Vulnerability
CVE-2022-23227	9.8 (Critical)	NUUO NVRmini 2 Devices Missing Authentication Vulnerability
CVE-2018-14933	9.8 (Critical)	NUUO NVRmini Devices OS Command Injection Vulnerability
CVE-2024-12356	9.8 (Critical)	BeyondTrust Privileged Remote Access (PRA) and Remote Support (RS) Command Injection Vulnerability

For more information, please visit the **Red Piranha Forum**:
https://forum.redpiranha.net/t/known-exploited-vulnerabilities-catalog-3rd-week-of-december-2024/533

Updated Malware Signatures (Week 3 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
Funksec	14.47%
Bianlian	3.14%
RansomHub	8.81%
El Dorado	3.77%
Killsec3	4.4%
Cicada3301	1.26%
Handala	0.63%
Akira	9.43%
Team Underground	0.63%
Fog	7.55%
Eraleign (APT73)	1.89%
Argonauts Group	0.63%
Dragonforce	2.52%
Leaked Data	1.26%
Lynx	1.89%
Qilin	3.77%
Kairos	1.26%
Play	4.4%
Stormous	0.63%
Everest	3.77%
Interlock	1.89%
Hunters	3.77%
Nitrogen	1.89%
3AM	0.63%
Brain Cipher	1.26%
Bluebox	1.89%

Ransomware Group	Overall Percentage of total attack coverage
Rhysida	0.63%
Cactus	0.63%
Nullbulge	0.63%
Blackbasta	3.14%
Clop	1.26%
Money Message	0.63%
Medusa	2.52%
Cloak	1.26%
Abyss-data	0.63%
Lockbit3	0.63%
Space Bears	0.63%

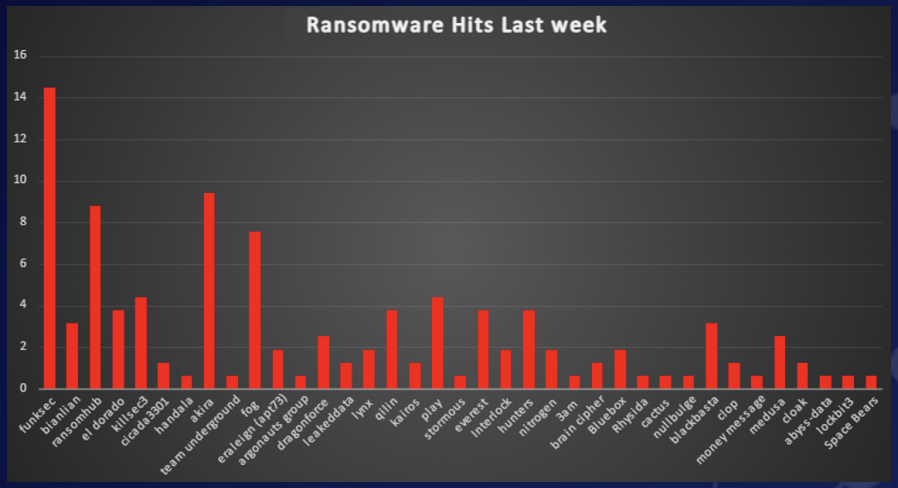


Figure 1: Ransomware Group Hits Last Week

Fog Ransomware Group

Fog Ransomware emerged in April 2024, targeting both Windows and Linux endpoints. It operates as a multi-pronged extortion operation, utilising a TOR-based Data Leak Site (DLS) to publicly list victims and host exfiltrated data from those who refuse to meet ransom demands.
This ransomware is part of the modern ransomware-as-a-service (RaaS) ecosystem, with customiable payloads tailored to disrupt operations in targeted environments.

Detailed TTPs
Initial Access and Foothold Establishment:

- Primary Initial Access Methods:
  - o Exploitation of known vulnerabilities in public-facing systems.
  - o Use of compromised credentials purchased from Initial Access Brokers (IABs).
- Post-Access Lateral Movement: Systematic traversal across network endpoints using valid credentials.

Cross-Platform Payloads:

- Windows Variant: Focuses on shadow copy deletion, service termination, and extensive configuration capabilities.
- Linux Variant: Targets virtual environments (e.g., VMSD and VMDK files) and employs tailored commands for environment disruption.

```
@1.6
@1.8OC1C6VPEEYOD9GLCFUUQAUMS
@1.1ndVo4q
@1.5/tmp/0987890
@1.2.fog
@1.3.vmem,.log,.vmdk,.vmem,.vswp,.vmsn,.vmsd
```

Fog Ransomware supports multiple command-line parameters. These include:

Parameter	Description
--help	Display all available syntax
--offvm	Force termination of VM-related processes
--size	Specify file encryption percentage (e.g., 70%)
--target	Define specific paths or directories for encryption
--id	Provide ID/password for execution (required)
--fork	Run without terminal, daemon mode
--log (file)	Enable logging (to terminal by default)
--nomutex	Skip checks for existing running processes
--showtalkid	Display campaign ID without encryption
--processallfiles	Encrypt all files, ignoring default extensions
--thread	Specify the number of threads for encryption

File Encryption Behavior:
File Extensions: .fog, .Fog, .FLOCKED
Windows Shadow Copy Deletion Command:
vssadmin.exe delete shadows /all /quiet

Windows Configuration: JSON-based configuration enabling:

- Custom encrypted file extensions.
- Ransom note filename configuration.
- Service and process termination lists.
- RSA public key embedding for encryption operations.

Readme.txt

```
If you are reading this, then you have been the victim of a cyber attack. We call ourselves
Fog and we take responsibility for this incident. We are the ones who encrypted your data and
also copied some of it to our internal resource. The sooner you contact us, the sooner we can
resolve this incident and get you back to work.
To contact us you need to have Tor browser installed:
1. Follow this link: xql562evsy7njcsngacphc2erzjfecwotdkobn3m4uxu2gtqh26newid.onion
2. Enter the code: O62V5NYWBJ3QB420IXRT9KL6
3. Now we can communicate safely.
If you are decision-maker, you will get all the details when you get in touch. We are waiting
for you.
```

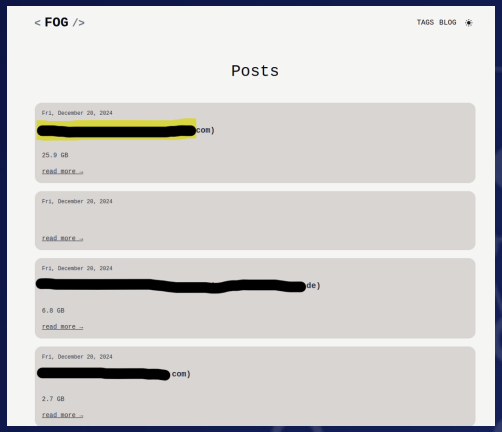
Fog Data Leak Site (DLS):
First Observed: July 2024

- Access Method: TOR-only

https://xql562evsy7njcsngacphc2erzjfecwotdkobn3m4uxu2gtqh26newid.onion/
http://xbkv2qey6u3gd3qxcojynrt4h5sgrhkar6whuo74wo63hijnn677jnyd.onion
http://xbkv2qey6u3gd3qxcojynrt4h5sgrhkar6whuo74wo63hijnn677jnyd.onion/posts
http://hlbqbuy2bo3onn6h6eq7pbci24kughiaw4rkxrewidnqma3hwwgt2ead.onion

Ransom Note:

- File Name: readme.txt
- Content: Instructions for victim communication via a TOR-based victim portal.



IOCs
FOG SAMPLES: MD5
==========
bef7a4725f55879af412d32f0b3b06bb
64433a8a138c62661da2ccf552483c33
7cc06e17a31673726f8fb94789252a93
8f052170eb9c8cda872d07888753c5e7
240eb6d3415de2284e03ba8a586ed724
868d8f2e942dd73b8ba9022fe7676032
6e48a67e0005cd6299d585314830af69
c18dd6b7d1acf12d39ebb017a21a4a3e
3226adfad6c5d31065347fbd2bda10e2
1a0a919dff09f63366f27f5e4c865d75
9bfa6efef31916adcb6d447b48434be5
b1094be42cf05bdd38951c8bf5c83cfd
f63c17d6753abb95d876f5c02dc57ad5
25a14b8104eb50d56c46df79b0df37bf
617d79c02ebac68b613d5b7cdbf001fd
07c6b4756715d73304ec0ebc951dddad

Mutex Name
==========
0m0bHYzntKuADHQz1YX0MPCjS26b7asN
voMcpdnwArrBIyzahjp7uJVceOsCFLIl
xtbpOtQCBF9KY5QMq33HdOjNW80pJYJ1
gWUK6AReEbhPFd2Z0OT8I1TLYBBkZVJE
Y0VCgFJ8FD7Twhdwuxk0VYGqUiYmzbPu
wpONYDTEXGEv2X5mvCgIs618ltuvnAdh
oBEIreRh5nFhUlymJvREJtSU1DXxAJJ2
524XGJTL4UK3kHgtljv41na68DtBWhlu
NfmNPlDMYMgQ70aY8fhAAwsHOK5Lne0V
D8l7rENCnQE5Sl7JoGa5Rc3TYaj2Q9fN
bKBcfMqrZXqjg35X9dg1MgDiqOrGWF8j
jBgB4ZHxUhNdJL9mz61WFXxI0GUXPAxw
DtcUAP6CtuupgWeFtVPGC54S0CUwThWZ
yPkZKkz7eRZuvAjYe18tTIs6TYvr3P5F
mPDJFFp1i358nAY53VS8Xqyo83UT71Gb
7oxTzmnLPJ9TKPrGJ7PZad9UfKGlsEzE

FOG RANSOMWARE HOSTNAMES
==========
DESKTOP-7G1IC87
DESKTOP-ET51AJO
KHSVMREP2022

IP ADDRESSES
==========
5.230.33.178
5.230.46.107

How to Mitigate Fog Ransomware

1. Employee Education:
   - Conduct regular cybersecurity awareness training.
   - Educate staff on phishing attack identification and reporting suspicious activity.
2. Implement Strong Authentication Controls:
   - Enforce strong password policies.
   - Enable Multi-Factor Authentication (MFA) for all remote and administrative access.
3. Network Hardening:
   - Restrict RDP and SSH Access:
     - Use VPNs for secure access.
     - Enforce MFA on remote access portals.
   - Implement network segmentation to prevent lateral movement.
4. System and Software Updates:
   - Regularly apply security patches and updates to operating systems, software, and firmware.
   - Disable unnecessary services and protocols.
5. Backup and Disaster Recovery:
   - Perform frequent, encrypted backups of critical systems and data.
   - Store backups in offline, air-gapped environments.
   - Regularly test data recovery processes.
6. Endpoint Protection:
   - Deploy advanced endpoint detection and response (EDR) solutions.
   - Enable real-time monitoring and alerting for suspicious activities.
7. Network Monitoring and Logging:
   - Enable network anomaly detection tools.
   - Monitor log files for early indicators of compromise (IOCs).

Ransomware Victims Worldwide

A recent ransomware analysis reveals a striking 55.97% of global incidents targeted the United States, making it the hardest-hit country by far. Trailing behind, Canada experienced 5.66% of attacks, while Australia, France, Brazil, and India each reported 3.14%.

Other significantly affected countries include Germany at 2.52%, followed by the United Kingdom at 1.89%. Nations such as China, Italy, Poland, Sweden, and Indonesia each reported 1.26% of the total attacks.

Meanwhile, a diverse group of nations, including Mexico, Netherlands, Nigeria, Mongolia, Thailand, Israel, Saudi Arabia, Poland, Greece, Ukraine, Belgium, Ecuador, Sri Lanka, Hong Kong, Jamaica, Vietnam, Spain, Argentina, Egypt, and Botswana, each saw a limited impact, representing just 0.63% of the total incidents.

This analysis underscores the global and persistent nature of ransomware threats, with North America bearing the brunt of the attacks, followed by Europe and parts of Asia. These numbers emphasise the critical need for enhanced cybersecurity measures across all regions to combat the ever-evolving ransomware threat landscape.

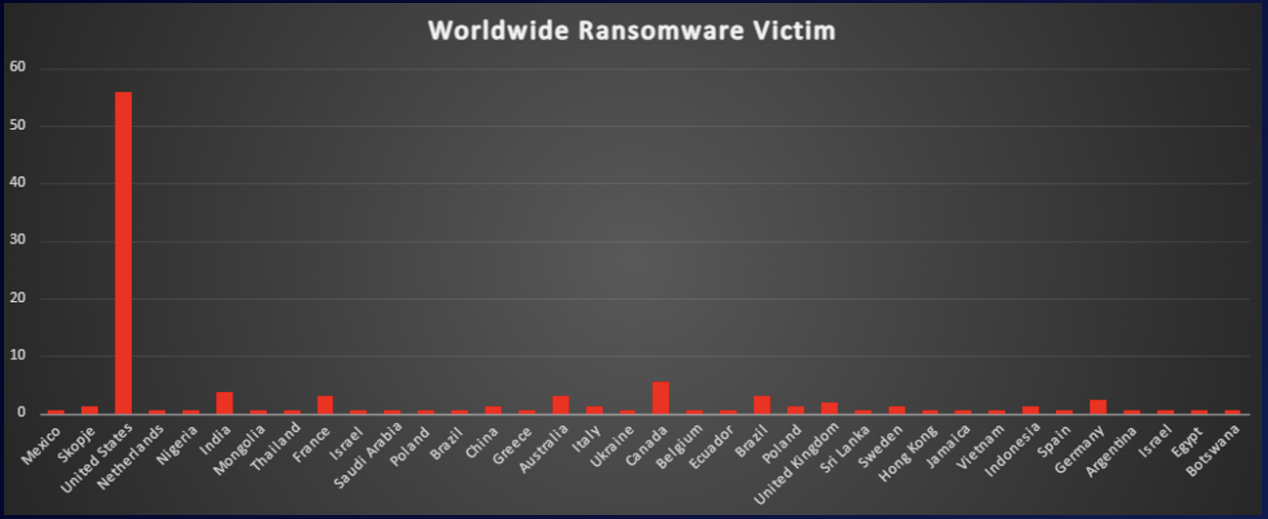


Figure 5: Ransomware Victims Worldwide

Ransomware Victims Industry-wide

Ransomware attacks continue to disrupt industries across the board, with the Manufacturing sector emerging as the hardest hit, accounting for a significant 18.24% of all incidents. Trailing closely behind, the Business Services sector faced 11.95%, while Retail reported 11.32% of attacks, highlighting their vulnerability to cyber threats.

The Healthcare sector follows with 7.55%, emphasising its critical exposure to ransomware disruptions. Construction also experienced notable impacts, representing 8.18% of total incidents. Meanwhile, Finance recorded 6.29%, reflecting its continued attractiveness as a target due to high-value data.

Sectors such as Law Firms (4.4%), Media & Internet (3.77%), Federal (3.14%), Telecommunications (3.14%), Education (3.14%), Hospitality (3.14%), Organisations (3.14%), and Consumer Services (3.14%) have all faced mid-level impacts from ransomware operations.

Smaller, yet significant, shares of attacks were observed in IT (2.52%), Insurance (1.89%), Electricity (1.89%), and Energy (1.26%), indicating ongoing risks in infrastructure-critical sectors.

Lower incidence rates were reported in Transportation (0.63%), Logistics (0.63%), and Real Estate (0.63%), though no industry can claim immunity from ransomware threats.

These numbers paint a clear picture: ransomware attacks are indiscriminate, targeting critical infrastructure, public services, and corporate entities alike. This broad distribution across industries highlights the urgent need for proactive cybersecurity strategies, tailored risk assessments, and incident response plans to mitigate the escalating threat of ransomware worldwide.

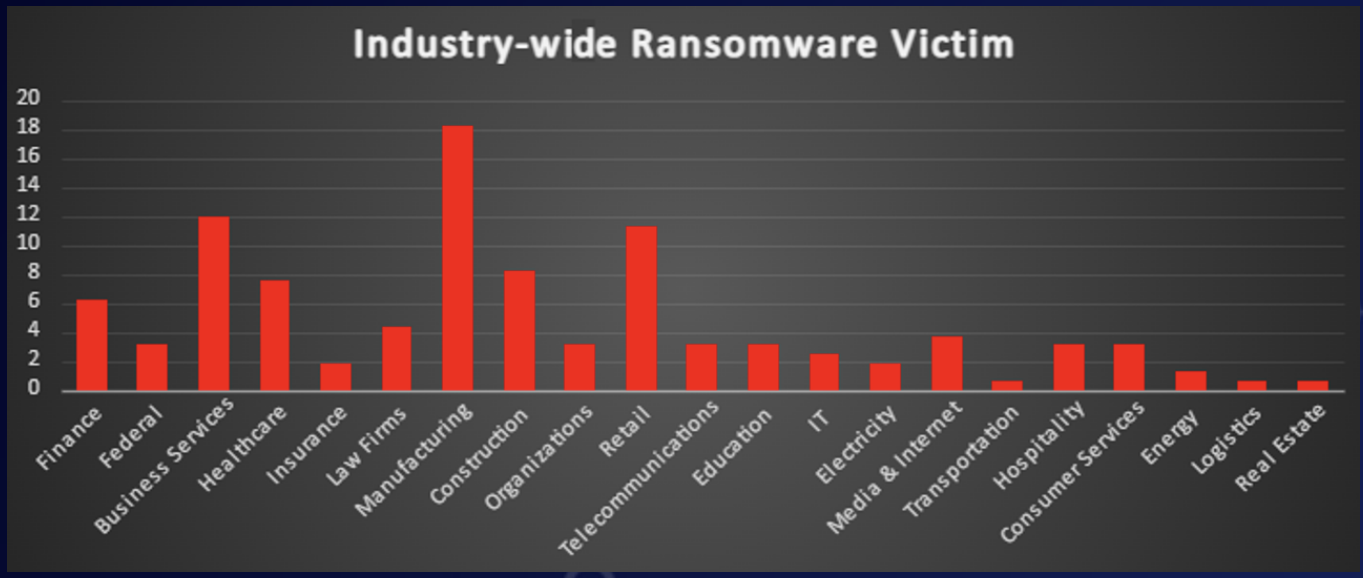


Figure 6: Industry-wide Ransomware Victims