Red Piranha
unified threat management

THREAT INTELLIGENCE REPORT

Jan 21 - 27, 2025

Report Summary:

- **New Threat Detection Added** – 2
  - CreateRCE
  - Progress WhatsUp Gold Path Traversal Vulnerability CVE-2024-12105

- **New Threat Protections - 313**

The following threats were added to Crystal Eye this week:

1. CreateRCE

A critical vulnerability in Microsoft Windows, designated as CVE-2023-35628 has been identified. This flaw resides in the CreateUri function, which is responsible for parsing Uniform Resource Identifiers (URIs). An attacker can exploit this vulnerability by sending a specially crafted email to an Outlook client or by persuading a user to navigate to a folder containing a malicious file in File Explorer. Successful exploitation allows for remote code execution without user interaction, making it a zero-click vulnerability. Microsoft addressed this issue in the December 2023 Patch Tuesday update. Systems updated with this patch are protected against this vulnerability.

Threat Protected: 01
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	T1204.001	User Execution: Malicious Link or Email
Execution	T1204.003	Execution via Malicious File
Defence Evasion	T1027	Obfuscated Files or Information
Privilege Escalation	T1068	Exploitation for Privilege Escalation
Command-and-Control	T1102.001	Web Services: C2 Communications Over HTTPS

2. Progress WhatsUp Gold Path Traversal Vulnerability CVE-2024-12105

A path traversal vulnerability, identified as CVE-2024-12105, has been discovered in Progress WhatsUp Gold version 24.0.1 Build 2177, Total Plus Edition. This vulnerability exists in the handling of SnmpExtendedActiveMonitor requests. An authenticated attacker can exploit this flaw by sending a specially crafted HTTP request, leading to unauthorised information disclosure. The issue arises from improper validation of user-supplied input, allowing attackers to access files and directories outside the intended directory structure.

Threat 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

Known exploited vulnerabilities (Week 4 January 2024):

Vulnerability	CVSS	Description
CVE-2020-11023	6.1 (Medium)	JQuery Cross-Site Scripting (XSS) Vulnerability
CVE-2025-23006	9.8 (Critical)	SonicWall SMA1000 Appliances Deserialisation Vulnerability

For more information, please visit the **Red Piranha Forum**:
https://forum.redpiranha.net/t/known-exploited-vulnerabilities-catalog-4th-week-of-january-2025/540

Updated Malware Signatures (Week 4 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.
Tofsee	A malware that is used to send spam emails, conduct click frauds as well as crypto mining.
Upatre	Upatre is also a malware dropper that downloads additional malware on an infected machine. It is usually observed to drop banking trojan after the initial infection.

Ransomware Report

The Red Piranha Team conducts ongoing surveillance of the dark web and other channels to identify global organisations impacted by ransomware attacks. From January 18th January to 24th, 2024, 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
Wikileaksv2	3.87%
Clop	36.77%
Bianlian	1.94%
Qilin	3.87%
Money message	0.65%
Rhysida	1.29%
Kairos	0.65%
Eraleign (apt73)	1.29%
Medusa	5.16%
Lynx	4.52%
Sarcoma	2.58%
Handala	0.65%
Fsociety	1.29%
Hunters	0.65%
SafePay	2.58%
RansomHub	9.03%
Everest	0.65%
FunkSec	3.87%
Cloak	1.94%
Space Bears	3.87%
Killsec3	1.29%
Inc ransom	1.29%
Akira	2.58%
Monti	0.65%
El Dorado	1.29%
Lockbit3	0.65%
Fog	1.94%
Leaked Data	0.65%
8base	0.65%
GD LockerSec	1.94%

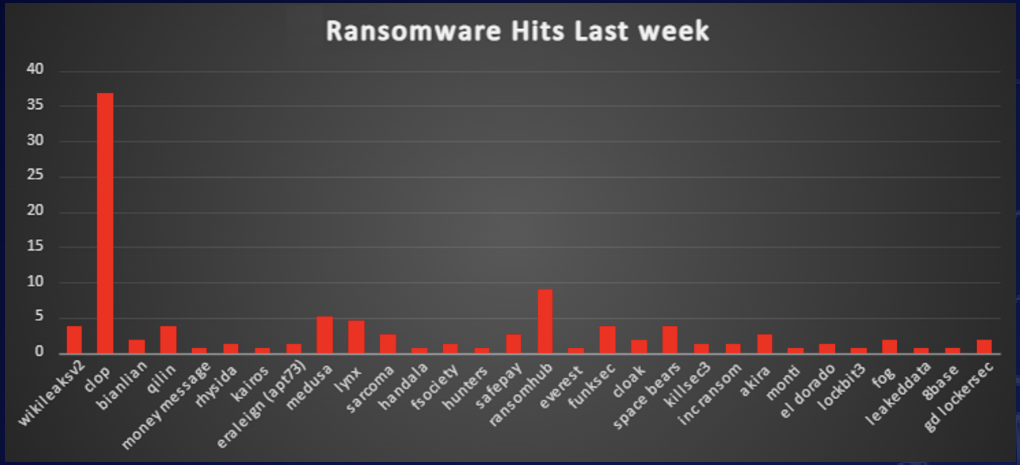
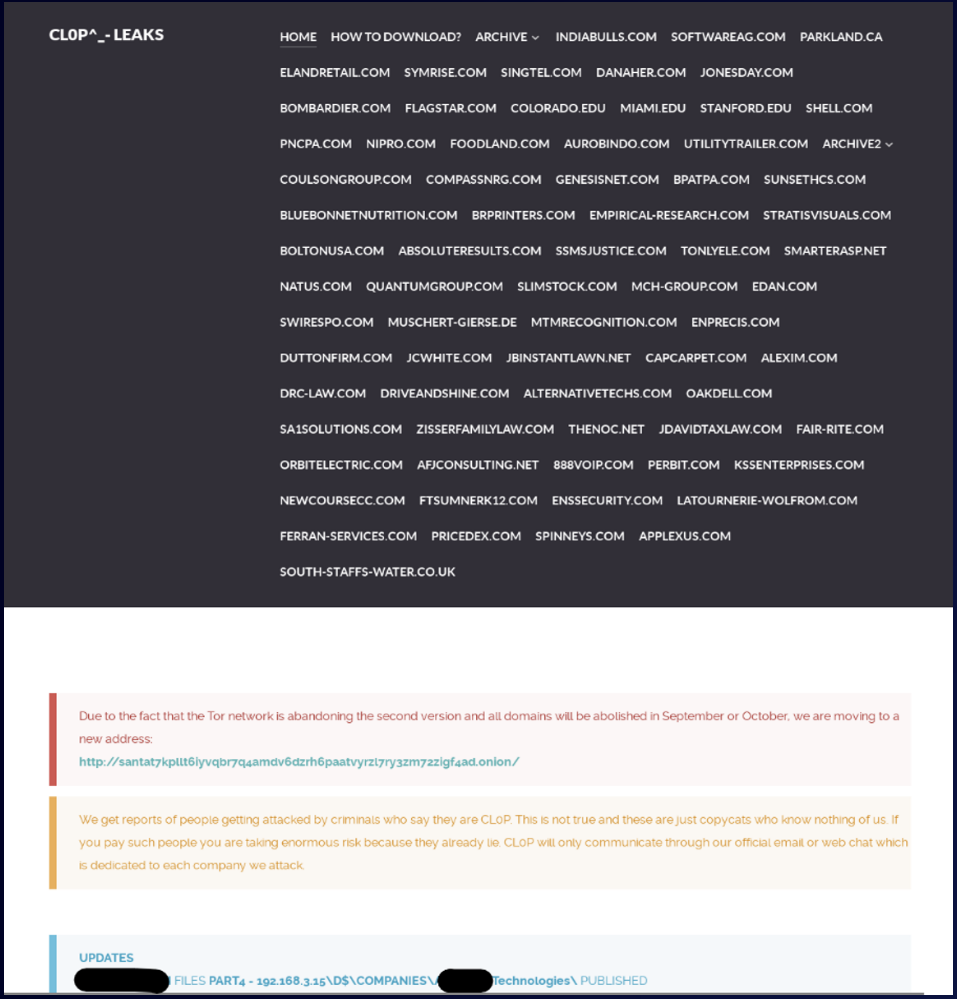


Figure 1: Ransomware Group Hits Last Week

Cl0p Ransomware

Cl0p ransomware has emerged as one of the most persistent and financially damaging cyber threats in recent years. Known for targeting organisations in a variety of industries—most notably finance and government - Cl0p leverages a combination of advanced exploitation techniques and sophisticated encryption methods to extort its victims. The ransomware is infamous for its "double extortion" model: encrypting a victim's files while also threatening to leak sensitive data if a ransom isn't paid. By adapting to new vulnerabilities, Cl0p remains a dynamic and dangerous adversary.



Due to the fact that the Tor network is abandoning the second version and all domains will be abolished in September or October, we are moving to a new address:
http://santat7kpllt6iyvqbr7q4amdv6dzrh6paatvyrzl7ry3zm72zigf4ad.onion/

We get reports of people getting attacked by criminals who say they are CLOP. This is not true and these are just copycats who know nothing of us. If you pay such people you are taking enormous risk because they already lie. CLOP will only communicate through our official email or web chat which is dedicated to each company we attack.

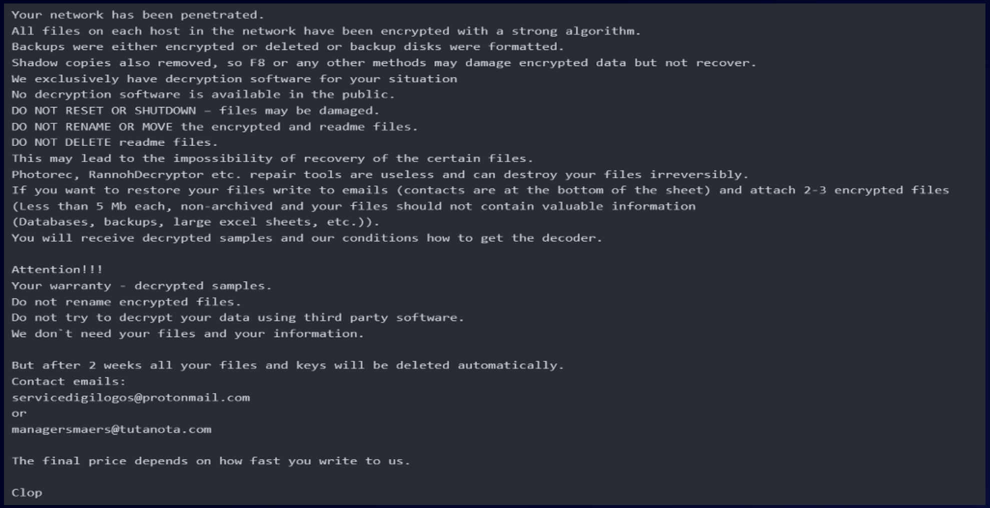
UPDATES
[redacted] FILES PART4 - 192.168.3.15\D$\COMPANIES\ [redacted] Technologies\ PUBLISHED

Detailed TTPs (Tactics, Techniques, and Procedures)

1. Initial Access:
    - Exploiting publicly known vulnerabilities in widely used software.
    - Phishing campaigns using targeted social engineering.
2. Execution:
    - Leveraging malicious dropper files that execute PowerShell scripts.
    - Executing unsigned binaries to establish persistence.
3. Persistence:
    - Maintaining access through encrypted backdoors and custom malware strains.
    - Using stolen credentials to re-enter compromised networks.
4. Privilege Escalation:
    - Identifying and exploiting configuration flaws or weak permissions.
    - Abusing legitimate administrative tools to escalate access.
5. Data Exfiltration and Encryption:
    - Stealing sensitive data before encryption (double extortion).
    - Encrypting files with advanced cryptographic algorithms.
6. Impact:
    - Rendering critical systems and data inaccessible.
    - Threatening reputational harm by leaking stolen data.

MITRE ATT&CK ID	Technique
T1082	System Information Discovery
T1190	Exploit Public-Facing Application
T1083	File and Directory Discovery
T1204	User Execution
T1059.001	PowerShell
T1566	Phishing
T1027	Obfuscated Files or Information
T1486	Data Encrypted for Impact
T1573	Encrypted Channel
T1105	Ingress Tool Transfer
T1490	Inhibit System Recovery

Ransomware Note:



```
Your network has been penetrated.
All files on each host in the network have been encrypted with a strong algorithm.
Backups were either encrypted or deleted or backup disks were formatted.
Shadow copies also removed, so F8 or any other methods may damage encrypted data but not recover.
We exclusively have decryption software for your situation
No decryption software is available in the public.
DO NOT RESET OR SHUTDOWN - files may be damaged.
DO NOT RENAME OR MOVE the encrypted and readme files.
DO NOT DELETE readme files.
This may lead to the impossibility of recovery of the certain files.
Photorec, RannohDecryptor etc. repair tools are useless and can destroy your files irreversibly.
If you want to restore your files write to emails (contacts are at the bottom of the sheet) and attach 2-3 encrypted files
(Less than 5 Mb each, non-archived and your files should not contain valuable information
(Databases, backups, large excel sheets, etc.)).
You will receive decrypted samples and our conditions how to get the decoder.

Attention!!!
Your warranty - decrypted samples.
Do not rename encrypted files.
Do not try to decrypt your data using third party software.
We don`t need your files and your information.

But after 2 weeks all your files and keys will be deleted automatically.
Contact emails:
servicedigilogos@protonmail.com
or
managersmaers@tutanota.com

The final price depends on how fast you write to us.

Clop
```

IOCs (Indicators of Compromise)
Vulnerabilities:

- CVE-2023-0669
- CVE-2023-34362
- CVE-2024-45195
- CVE-2024-50623
- CVE-2024-55956

IP Addresses:

- 103.140.62.43
- 146.190.133.67
- 162.240.110.250
- http://ekbgzchl6x2ias37.onion
- http://santat7kpllt6iyvqbr7q4amdv6dzrh6paatvyrzl7ry3zm72zigf4ad.onion
- http://3ws3t4uo7fehnn4qpmadk3zjrxta5xlt3gsc5mx4sztrsy7ficuz5ayd.onion/
- http://amnwxasjtjc6e42siac6t45mhbkgtycrx5krv7sf5festvqxmnchuayd.onion/
- http://qahjimrublt35jlv4teesicrw6zhpwhkb6nhtonwxuqafmjhr7hax2id.onion/
- http://l4rdimrqyonulqjttebry4t6wuzgjv5m62rnpjho3q22a6maf6d5evyd.onion/
- http://npkoxkuygikbkpuf5yxte66um727wmdo2jtpg2djhb2e224i4r25v7ad.onion
- http://6v4q5w7di74grj2vtmikzgx2tnq5eagyg2cubpcnqrvvee2ijpmprzqd.onion/remote0

Mail:
SUPPORT@IN2PAY.COM
UNLOCK@GOTO-PAY.COM
support@he1p-center.com
unlock@cl-leaks.com
unlock@he1p-me.com

File Extensions:

- .cl0p (renamed encrypted files)

Observed Malware Behaviour:
•Files encrypted with RC4, RSA-1024 wrapping the encryption keys.
•Obfuscated payloads and scripts to evade detection.

Mitigations

1. Apply Security Patches Promptly:
   - Regularly update software, particularly those known to have been exploited by Cl0p (e.g., file transfer solutions).
2. Implement a Strong Backup Strategy:
   - Maintain offline or immutable backups of critical data.
   - Regularly test backups to ensure they are accessible and complete.
3. Enhance Network Segmentation and Access Control:
   - Segregate sensitive data and systems from regular user access.
   - Apply the principle of least privilege (PoLP).
4. Conduct Regular Security Awareness Training:
   - Educate employees about phishing attacks and social engineering techniques.
   - Emphasise the importance of scrutinising unsolicited emails and links.
5. Deploy Advanced Threat Detection and Response Solutions:
   - Use Endpoint Detection and Response (EDR) to identify suspicious behaviour early.
   - Monitor network traffic for signs of data exfiltration or unauthorised encryption attempts.
6. Establish a Clear Incident Response Plan:
   - Define roles and responsibilities for responding to ransomware attacks.
   - Conduct tabletop exercises to prepare for a rapid response.

By employing these proactive measures, organisations can significantly reduce the risk of Cl0p ransomware infections and minimise the impact of an attack.

Ransomware Victims Worldwide

A recent ransomware analysis reveals that the United States remains the most heavily impacted nation, accounting for a staggering 56.77% of global incidents—underscoring its continued vulnerability to ransomware threats. Canada follows with 8.39% of recorded attacks, highlighting significant challenges in North America. Meanwhile, Australia, the United Kingdom, and India contribute 5.81%, 3.87%, and 3.87% of global incidents respectively, reflecting ongoing risks in both Asia-Pacific and Europe.

Other countries such as France (1.29%), Germany (2.58%), Pakistan (2.58%), and Italy (1.29%) also show notable levels of ransomware activity. The Netherlands, Mexico, and Bangladesh each recorded 1.94% of global incidents, signalling the broad geographic spread of ransomware threats.

Lower but still notable percentages come from nations like Vietnam, Kuwait, and Denmark, which contribute 0.65% each. Countries including Israel, Switzerland, Malaysia, Portugal, Philippines, Japan, and Morocco also reflect small yet significant parts of the worldwide ransomware landscape.

This distribution illustrates the global and persistent nature of ransomware threats, with North America continuing to bear the brunt of attacks. The findings further emphasise the critical need for strengthened cybersecurity measures, proactive defence strategies, and heightened vigilance across all sectors to counter the unrelenting rise in ransomware incidents worldwide.

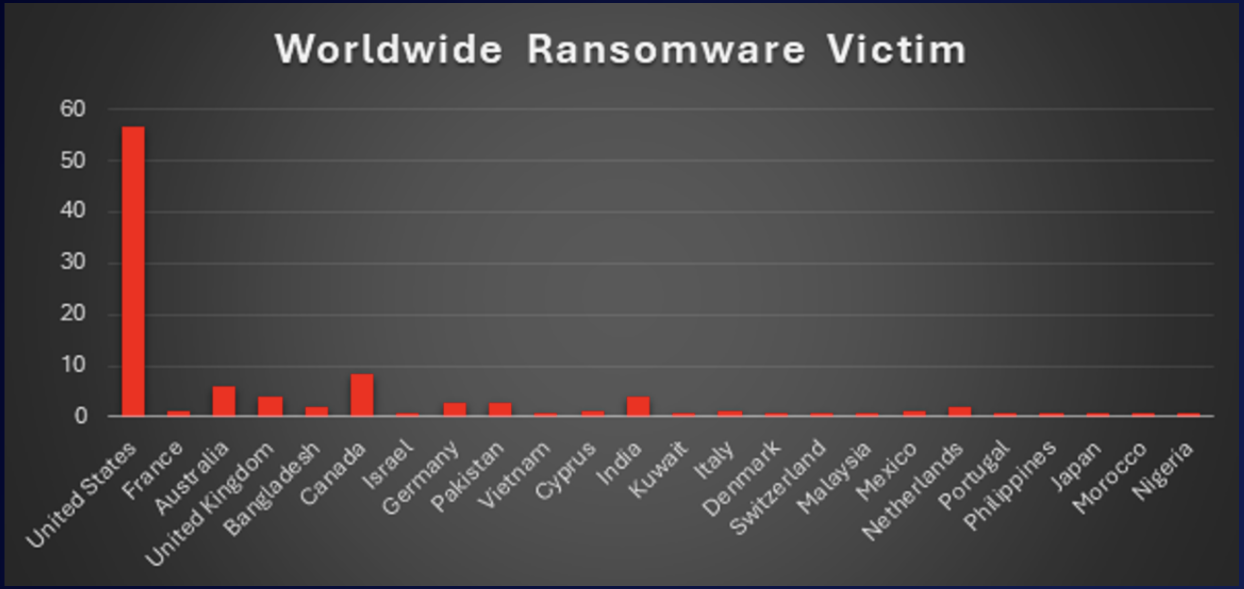


Figure 4: Ransomware Victims Worldwide

Ransomware Victims by Industry

A recent ransomware analysis reveals Manufacturing as the most targeted sector, accounting for 26.96% of the total reported incidents. Next in line is Retail at 20.87%, followed by IT and Business Services, each at 13.04%. The Transportation sector stands at 11.3%, illustrating the widespread nature of ransomware threats across multiple key industries.

Healthcare reported 6.96% of attacks, while Education recorded 6.09%. Construction showed 9.57%, underscoring the persistent risk levels across these industries. Finance reported 7.83%, highlighting consistent exposure within the financial arena.

Further down the list, Hospitality and Telecommunications each contributed 1.74% of incidents. Federal entities, Energy, and Consumer Services recorded 4.35%, 4.35%, and 0.87% respectively. Real Estate and Law Firms also reported smaller percentages of ransomware attacks, showing that no sector is immune.

This analysis underscores the pervasive and indiscriminate nature of ransomware, cutting across critical infrastructure, public services, and commercial enterprises alike. Organisations must adopt robust cybersecurity frameworks, invest in proactive threat detection, and develop effective incident response strategies to mitigate the evolving ransomware landscape effectively.

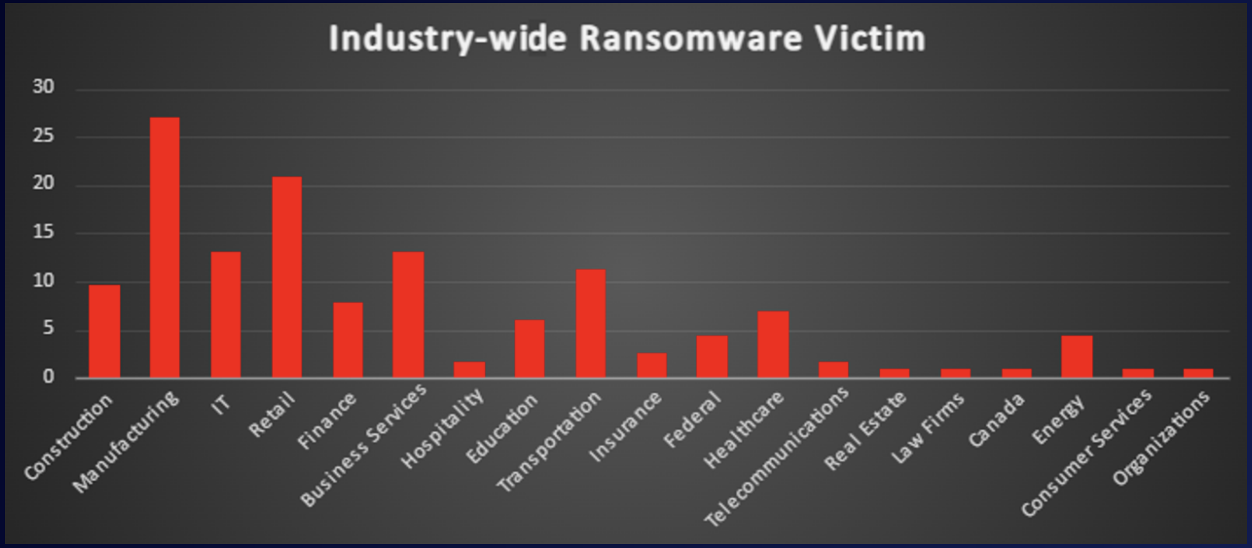


Figure 5: Industry-wide Ransomware Victims