Red Piranha
unified threat management

THREAT INTELLIGENCE REPORT

Mar 04 - 10, 2025

Report Summary:

- **New Threat Detection Added** – 2
  - PolarEdge IoT Botnet
  - OtterCookie Malware
- **New Threat Protections - 236**

The following threats were added to Crystal Eye this week:

1. PolarEdge IoT Botnet

PolarEdge is a recently identified botnet targeting Internet of Things (IoT) edge devices by exploiting the CVE-2023-20118 vulnerability. This botnet employs a stealthy Transport Layer Security (TLS) backdoor, allowing unauthorised access and control over compromised devices. The threat actors behind PolarEdge have constructed an extensive infrastructure to manage and expand their network of infected devices. The purpose of this botnet has not yet been determined. An objective of PolarEdge could be to control compromised edge devices, transforming them into Operational Relay Boxes for launching offensive cyber-attacks.

Threat Protected: 43
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	T1190	Exploit Public-Facing Application
Execution	T1059.004	Command and Scripting Interpreter: Unix Shell
Persistence	T1505.003	Server Software Component: Web Shell
Defence Evasion	T1027	Obfuscated Files or Information
Command-and-Control	T1071.001	Application Layer Protocol: Web Protocols
Impact	T1496	Resource Hijacking

2. OtterCookie Malware

OtterCookie is a newly identified malware associated with the Contagious Interview campaign, which is believed to be linked to North Korean threat actors. Unlike typical nation-state-sponsored attacks, this campaign appears financially motivated and targets a broader range of victims. First observed in November 2024, OtterCookie is primarily delivered through compromised Node.js projects or npm packages sourced from platforms like GitHub or Bitbucket. In some instances, applications developed using frameworks such as Qt or Electron have also been utilised as initial attack vectors. The malware employs loaders that download and execute JavaScript code from remote servers, often leveraging the cookie property within JSON data. Once executed, OtterCookie uses Socket.IO for communication, allowing it to receive commands to execute shell commands, steal host information, search for cryptocurrency wallet keys, and exfiltrate clipboard contents.

Threat Protected: 08
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	T1554	Compromise Software Supply Chain
Execution	T1059.007	Command and Scripting Interpreter: JavaScript
Credential Access	T1555	Credentials from Password Stores (Wallet Keys)
Collection	T1115	Clipboard Data
Command-and-Control	T1071.001	Application Layer Protocol: Web Protocols

Known exploited vulnerabilities (Week 1 March 2025):

Vulnerability	CVSS	Description
CVE-2024-4885	9.8 (Critical)	Progress WhatsUp Gold Path Traversal Vulnerability
CVE-2018-8639	7.8 (High)	Microsoft Windows Win32k Improper Resource Shutdown or Release Vulnerability
CVE-2022-43769	7.2 (High)	Hitachi Vantara Pentaho BA Server Special Element Injection Vulnerability
CVE-2022-43939	9.8 (Critical)	Hitachi Vantara Pentaho BA Server Authorization Bypass Vulnerability
CVE-2023-20118	7.2 (High)	Cisco Small Business RV Series Routers Command Injection Vulnerability
CVE-2025-22226	6.0 (Medium)	VMware ESXi, Workstation, and Fusion Information Disclosure Vulnerability
CVE-2025-22225	8.2 (High)	VMware ESXi Arbitrary Write Vulnerability
CVE-2025-22224	8.2 (High)	VMware ESXi and Workstation TOCTOU Race Condition Vulnerability
CVE-2024-50302	5.5 (Medium)	Linux Kernel Use of Uninitialized Resource Vulnerability

For more information, please visit the **Red Piranha Forum**:
https://forum.redpiranha.net/t/known-exploited-vulnerabilities-catalog-1st-week-of-march-2025/554

Updated Malware Signatures (Week 1 March 2025)

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.
AsyncRAT	A remote administration tool that was originally marketed as an open-source tool for legitimate remote system administration. However, it's often used for malicious purposes by cybercriminals due to its powerful features and stealthy behaviour.
XWorm	A Remote Access Trojan (RAT) and malware loader that's commonly used in cyberattacks to give attackers full remote control over a victim's system. It's part of a growing trend of commercialised malware sold or rented on dark web forums, often under the guise of a "legitimate tool."

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 Groups	Overall Percentage of total attack coverage
Inc ransom	2.11%
Medusa	2.82%
Clop	2.82%
Rhysida	1.41%
Play	5.63%
Lockbit3	0.7%
Monti	2.82%
KillSec3	1.41%
Cactus	11.97%
Lynx	6.34%
Fog	4.93%
Abyss-Data	0.7%
OX thief	0.7%
WikiLeaksv2	2.11%
Bianlian	4.93%
Akira	7.04%
Hunters	0.7%
RansomHub	12.68%
Qilin	5.63%
Apos	1.41%
Arcus Media	6.34%
Belsen Group	0.7%
FunkSec	0.7%
Kairos	1.41%
Secp0	1.41%
Skira Team	3.52%
SafePay	0.7%
Leaked Data	1.41%
Weyhro	3.52%
Interlock	0.7%
Sarcoma	0.7%

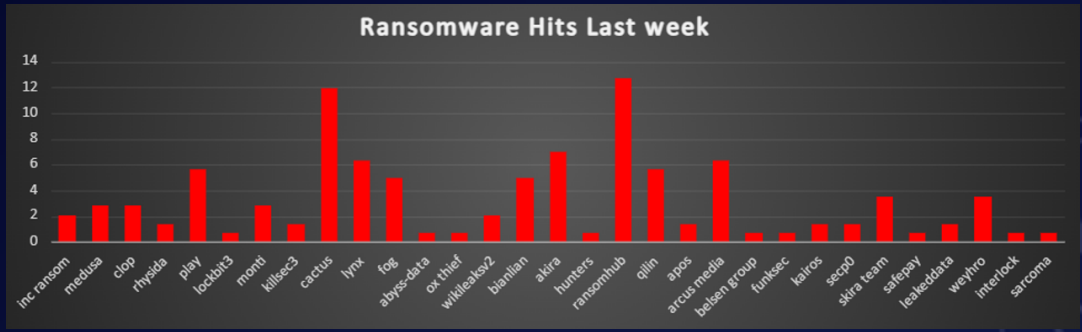
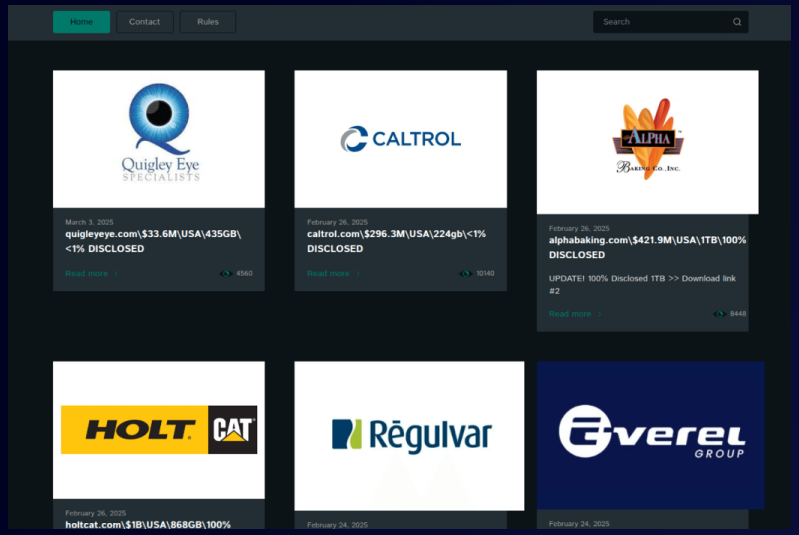


Figure 1: Ransomware Group Hits Last Week

Cactus Ransomware Group

Overview

The Cactus ransomware group has been observed utilising a multi-stage attack chain combining social engineering, lateral movement, ESXi hypervisor exploitation, and custom backconnect C2 implants. Red Piranha's detection and incident response efforts uncovered evolutionary changes in Cactus' tactics, techniques, and procedures (TTPs), emphasising a shift toward stealthier and more sophisticated lateral movement and persistence mechanisms. Although encryption was prevented in this case, attackers exhibited full kill chain completion readiness, including network traversal, privilege escalation, and ransomware delivery staging.



Detailed TTPs

Initial Access (TA0001)

- Phishing & Social Engineering (T1566):
  - Email bombing campaigns targeting victim inboxes.
  - Microsoft Teams impersonation from xxx@gamicalstudio.onmicrosoft.com, luring victims to accept Quick Assist remote sessions.

Execution (TA0002)

- User Execution (T1204):
  - Victim manipulated to download and extract malicious archives:
    - .bpx files concatenated into pack.zip, containing malicious DLLs and executables masquerading as legitimate OneDrive files.

Persistence (TA0003)

- Registry Modification (T1112):
  - Registry key HKCU\SOFTWARE\TitanPlus added to store BackConnect C2 IP addresses.

Privilege Escalation (TA0004)

- DLL Sideloading (T1574.002):
  - Placement of custom DLLs (e.g., wscapi.dll, libssl-3-x64.dll) in a trusted OneDrive directory for execution via OneDriveStandaloneUpdater.exe.

Defence Evasion (TA0005)

- Masquerading (T1036):
  - Use of OneDrive file names and directories to evade detection.
    - Disabling Security Tools (T1562):
  - On ESXi, disabled ExecInstalledOnly and firewall to run unauthorised binaries.

Credential Access (TA0006)

- Potential use of WinRM and SMB to harvest and reuse administrative credentials during lateral movement.

Lateral Movement (TA0008)

- SMB (T1021.002) and WinRM (T1021.006):
  - Network traversal using file shares and remote code execution via WinRM.

Command-and-Control (TA0011)

- BackConnect Implants (T1573):
  - Dynamic C2 registration via registry keys.
- WinSCP Deployment (T1105):
  - File transfer and exfiltration using WinSCP connecting to pumpkinrab.com.

Impact (TA0040)

- Ransomware Deployment (T1486):
  - Encryption attempt was interrupted, but ransom note delivered via email identifying as "Cactus Group

Tactic	Technique	Description
Initial Access	Phishing & Social Engineering (T1566.003)	Email bombing and Teams social engineering to gain access.
	Trusted Relationship Abuse (T1199)	Abuse of Teams for impersonation and remote access.
Execution	Malicious File Execution (T1204.002)	Download and execution of malicious .bpx archive files.
	Command Line (T1059.003)	Likely used for file manipulation and extraction.
Persistence	Registry Modification (T1547.001)	Registry key added for C2 communication (TitanPlus).
Privilege Escalation	DLL Sideloading (T1574.001)	Malicious DLLs loaded via OneDriveUpdater.exe.
Defence Evasion	Masquerading (T1036.005)	Files hidden in trusted OneDrive folders.
	Disable Firewall/Protections (T1562.004)	Disabled ESXi firewall and security settings.
Lateral Movement	SMB (T1021.002) and WinRM (T1021.006)	Spread through the network using shares and remote execution.
Command-and-Control (C2)	BackConnect C2 (T1071.001, T1571)	Communication with custom C2 via registry and HTTPS.
	WinSCP File Transfer (T1105)	WinSCP used for moving files and exfiltration.
Impact	Data Encryption (Planned) (T1486)	Ransomware prepared but stopped before execution.

Indicators of Compromise (IOCs)
Downloaded Files:
C:\Users\<user>\Downloads\kb153056-01.bpx
C:\Users\<user>\Downloads\kb153064-02.bpx

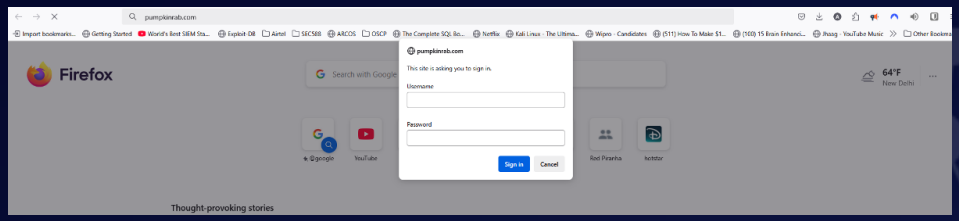
Extracted payloads (OneDrive masquerade):
C:\Users\<user>\AppData\Local\Microsoft\OneDrive\OneDriveStandaloneUpdater.exe
C:\Users\<user>\AppData\Local\Microsoft\OneDrive\wscapi.dll
C:\Users\<user>\AppData\Local\Microsoft\OneDrive\libssl-3-x64.dll
C:\Users\<user>\AppData\Local\Microsoft\OneDrive\vcruntime140.dll
C:\Users\<user>\AppData\Local\Microsoft\OneDrive\libcrypto-3-x64.dll

Registry Key:
HKCU\SOFTWARE\TitanPlus

C2 IP Addresses:

45.8.157.199
5.181.3.164
38.180.25.3
185.190.251.16
207.90.238.52
89.185.80.86

Domain and Associated IP:
Pumpkinrab.com -> 208.115.200.146



Communication:

TOX:
7367B422CD7498D5F2AAF33F58F67A332F8520CF0279A5FBB4611E0121AE421AE1D49ACEABB2
SONAR:
http://sonarmsng5vzwqezlvtu2iiwwdn3dxkhotftikhowpfjuzg7p3ca5eid.onion/contact/Cactus_Support
URLs
https://cactusbloguuodvqjmnzlwetjlpj6aggc6iocwhuupb47laukux7ckid.onion
https://cactus5dqnqkppa5ayckiyk6dttpqwczdqphv5mxh4dkk5ct544q5aad.onion/

File Server:

https://vhfd5qagh6j7qbisjqvly7eejqbv6z5bv77v6yuhctn77wmd3hjkyvad.onion
https://acfckf3l6l7v2tsnedfx222a4og63zt6dmvheqbvsd72hkhaqadrrsad.onion
https://6wuivqgrv2g7brcwhjw5co3vligiqowpumzkcyebku7i2busrvlxnzid.onion
https://truysrv2txxvobngtlssbgqs3e3ekd53zl6zoxbotajyvmslp5rdxgid.onion
https://jvtxo5gdcgloguty322ynfnpqkc2whe2jauc7ucm7bzmgct3k7ogr4yd.onion/

Mitigations
Initial Access Mitigation
- Implement phishing-resistant MFA (e.g., hardware tokens, FIDO2).
- Security awareness training on Quick Assist abuse and Microsoft Teams impersonation.
- Harden external communications; restrict Teams communications from external tenants.

Execution and Persistence Mitigation
- Block unsigned DLL loading via Windows Defender Application Control (WDAC).
- Monitor for unusual files in OneDrive directories and .bpx/.cab file downloads.
- Use group policy to disable Quick Assist if not required.

Lateral Movement Mitigation
- Restrict WinRM and SMB access using firewall rules and segmentation.
- Enforce LSA Protection to prevent credential theft.
- Monitor WinRM logs (Event ID 4688, 7045) and SMB share creation.

Ransomware Victims Worldwide

A recent ransomware analysis reveals that the United States remains the most heavily impacted nation, accounting for a staggering 61.27% of global incidents, highlighting its continued vulnerability to ransomware threats. Following this, Canada reported 5.63% of the attacks, emerging as another highly targeted region.

Brazil, India, and the United Kingdom also faced considerable exposure, each reporting 3.52% of ransomware incidents. Italy and Australia experienced 2.82% of attacks, indicating an ongoing risk in these regions. Spain, Japan, Germany, Switzerland, and France recorded 1.41% of global ransomware cases, reflecting notable, though comparatively lower, targeting.

Several other nations exhibited moderate levels of ransomware incidents, including Botswana, Argentina, Nigeria, Singapore, Malta, Indonesia, Austria, Portugal, Denmark, Turkey, Ukraine, Norway, Malaysia, South Africa, and Sweden, each reporting 0.7% of global ransomware cases.

This analysis underscores the persistent and widespread nature of ransomware attacks, with North America facing particularly high levels of risk. These findings highlight the critical need for robust cybersecurity measures, proactive defence strategies, and heightened vigilance across all sectors to counteract the increasing ransomware threat worldwide.

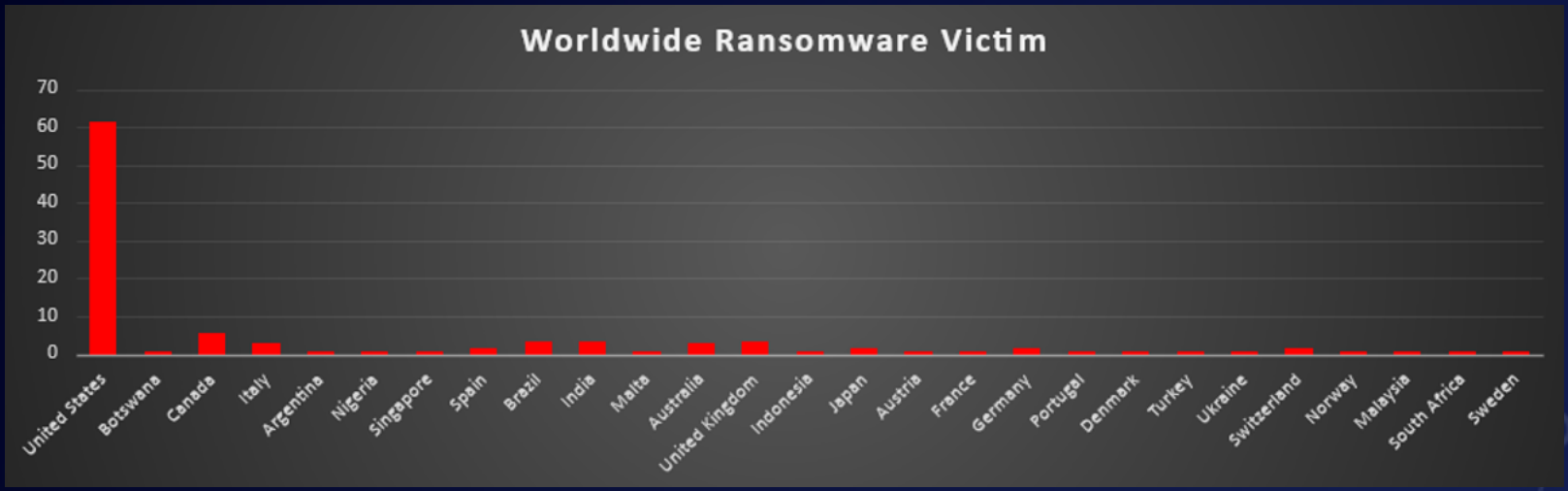


Figure 4: Ransomware Victims Worldwide

Ransomware Victims by Industry

A recent ransomware analysis highlights the Manufacturing sector as the most targeted industry, accounting for 24.65% of total reported incidents. This underscores the persistent threats faced by production processes and supply chain operations.

Following this, the Retail sector reported 13.38% of attacks, and Business Services accounted for 11.97%, emphasising the heightened risk to consumer-facing businesses and service-oriented organisations. The Healthcare industry also saw a significant impact, accounting for 5.63% of ransomware incidents.

Other heavily affected industries include Construction at 7.75% and IT services at 4.23%, reflecting ongoing security challenges in infrastructure development and technology operations. The Hospitality sector also recorded a notable 4.93%, indicating sustained ransomware pressure on businesses catering to public services.

Industries like Education, Finance, Federal, and Consumer Services each reported 3.52% of attacks, highlighting vulnerabilities in sectors that manage sensitive personal and financial data. Law Firms and Real Estate followed closely with 2.82%, signalling targeted attacks on industries involved in legal and property transactions.

Meanwhile, Insurance, Telecommunications, Transportation, and Organisations each accounted for 1.41% of ransomware incidents, while Energy, Electricity, and Media & Internet sectors each reported 0.7%, reflecting cybercriminals' continuing focus on critical infrastructure and essential services.

This analysis reinforces the indiscriminate and widespread nature of ransomware threats, impacting industries across critical infrastructure, public services, and commercial enterprises. The findings highlight the urgent need for industry-specific cybersecurity strategies, robust defence mechanisms, and proactive risk management to combat the evolving ransomware landscape.

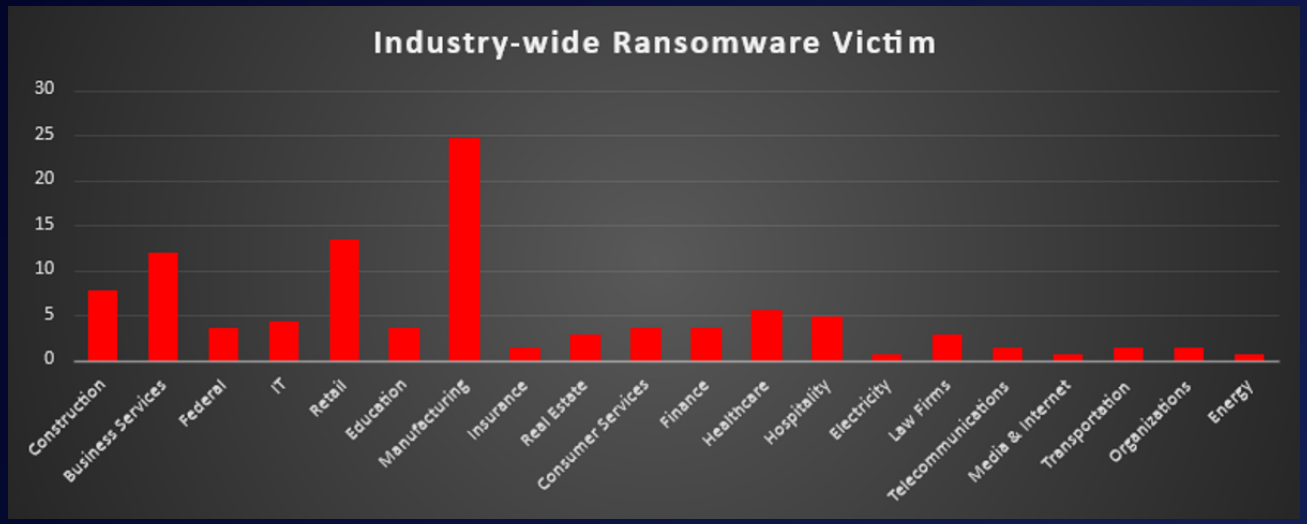


Figure 5: Industry-wide Ransomware Victims