Red Piranha
unified threat management

THREAT INTELLIGENCE REPORT

Mar 10 - 17, 2025

Report Summary:

- **New Threat Detection Added** – 2
  - Gholoader CnC (SocGholish)
  - CVE-2024-4577 – PHP CGI Argument Injection Vulnerability
- **New Threat Protections - 197**

The following threats were added to Crystal Eye this week:

1. Gholoader CnC (SocGholish)

SocGholish is a prevalent malware campaign that employs malicious JavaScript injections on legitimate websites to deliver fake browser update prompts. Unsuspecting users who follow these prompts download a .js file, often compressed within a .zip archive, leading to malware execution on their systems. The campaign operates through multiple stages:

- Stage 1: Compromise of legitimate websites to serve malicious JavaScript.
- Stage 2: Users visiting these sites receive fake browser update prompts, initiating the download of the malicious payload.
- Stage 3: Execution of the downloaded .js file, establishing command-and-control (C2) communication.

The malware has been observed deploying remote administration tools like NetSupport RAT and, in some cases, Cobalt Strike, indicating potential for further malicious activities, including ransomware deployment.

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	T1566.002	Phishing: Malicious Link
Execution	T1059.007	Command and Scripting Interpreter: JavaScript
Persistence	T1053.005	Scheduled Task/Job
Defence Evasion	T1027	Obfuscated Files or Information
Command-and-Control	T1071.001	Application Layer Protocol: Web Protocols

2. CVE-2024-4577 – PHP CGI Argument Injection Vulnerability

CVE-2024-4577 is a critical vulnerability affecting PHP versions 8.1.* before 8.1.29, 8.2.* before 8.2.20, and 8.3.* before 8.3.8, particularly when running in Common Gateway Interface (CGI) mode on Windows systems using Chinese and Japanese locales. Disclosed in June 2024, this flaw allows attackers to inject command-line arguments into the PHP process by exploiting how Unicode characters are converted into ASCII. Specifically, the misuse of soft hyphen characters (0xAD) enables threat actors to pass additional arguments that can lead to remote code execution (RCE). Within 24 hours of disclosure, active exploitation attempts were observed, including the deployment of malware such as Gh0st RAT and RedTail cryptominers.

Threat 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
Defence Evasion	T1027	Obfuscated Files or Information
Command-and-Control	T1071.001	Application Layer Protocol: Web Protocols

Known exploited vulnerabilities (Week 2 March 2025):

Vulnerability	CVSS	Description
CVE-2025-24201	8.8 (High)	Apple Multiple Products WebKit Out-of-Bounds Write Vulnerability
CVE-2025-21590	6.7 (Medium)	Juniper Junos OS Improper Isolation or Compartmentalization Vulnerability
CVE-2025-26633	7.0 (High)	Microsoft Windows Management Console (MMC) Improper Neutralization Vulnerability
CVE-2025-24983	7.0 (High)	Microsoft Windows Win32k Use-After-Free Vulnerability
CVE-2025-24984	4.6 (Medium)	Microsoft Windows NTFS Information Disclosure Vulnerability
CVE-2025-24985	7.8 (High)	Microsoft Windows Fast FAT File System Driver Integer Overflow Vulnerability
CVE-2025-24991	5.5 (Medium)	Microsoft Windows NTFS Out-Of-Bounds Read Vulnerability
CVE-2025-24993	7.5 (High)	Microsoft Windows NTFS Heap-Based Buffer Overflow Vulnerability
CVE-2025-25181	7.5 (High)	Advantive VeraCore SQL Injection Vulnerability
CVE-2024-57968	9.9 (Critical)	Advantive VeraCore Unrestricted File Upload Vulnerability
CVE-2024-13159	9.8 (Critical)	Ivanti Endpoint Manager (EPM) Absolute Path Traversal Vulnerability
CVE-2024-13160	9.8 (Critical)	Ivanti Endpoint Manager (EPM) Absolute Path Traversal Vulnerability
CVE-2024-13161	9.8 (Critical)	Ivanti Endpoint Manager (EPM) Absolute Path Traversal Vulnerability

For more information, please visit the **Red Piranha Forum**:
https://forum.redpiranha.net/t/known-exploited-vulnerabilities-catalog-2ndweek-of-march-2025/555

Updated Malware Signatures (Week 2 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
Stormous	0.56%
RansomHub	5.65%
FunkSec	3.95%
Lynx	5.65%
Arcus Media	1.69%
Inc ransom	4.52%
Fsociety	0.56%
Qilin	5.08%
Play	8.47%
Rhysida	1.13%
Embargo	1.13%
CrazyHunter Team	2.82%
Ransomexx	1.13%
Babuk-Bjorka	13.56%
Kairos	0.56%
Clop	1.13%
Medusa	1.13%
DragonForce	3.95%
Akira	11.3%
Cactus	7.34%
RansomHouse	1.69%
Nitrogen	0.56%
Hunters	0.56%
Fog	2.26%
SafePay	3.95%
KillSec3	1.13%
Nightspire	3.39%
Interlock	0.56%
WikiLeaksv2	1.13%
Trinity	2.82%

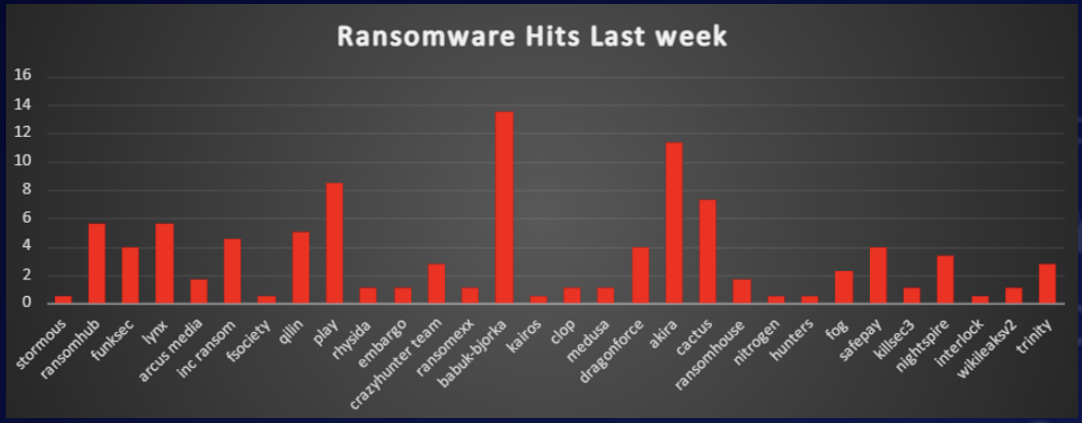
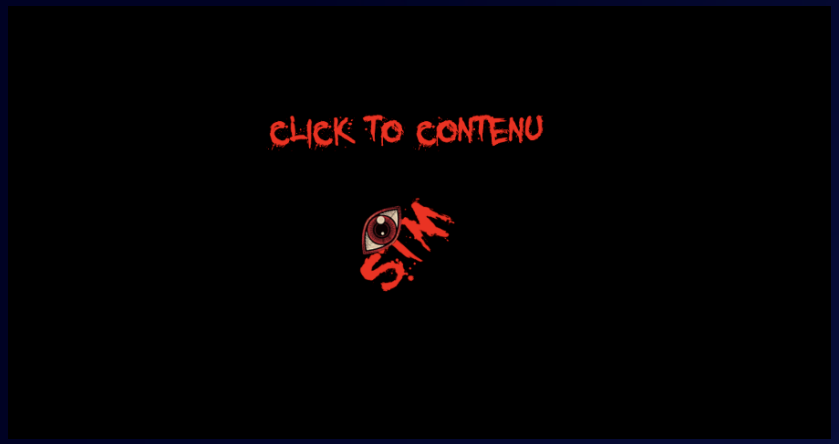


Figure 1: Ransomware Group Hits Last Week

Stormous ransomware

Stormous ransomware, operating in close collaboration with GhostSec, has evolved into a sophisticated and formidable threat actor. Their operations blend advanced intrusion techniques—including VPN credential compromise, lateral movement using legitimate tools, DLL sideloading, and exploitation of vulnerable drivers—with a double-extortion business model. This report details their attack chain, technical indicators (IOCs), and mitigation recommendations. It also highlights findings from recent threat intelligence (Red Piranha, May 7–May 13, 2024) and compares IOCs that show overlapping onion infrastructure between Stormous and GhostSec.



Overview

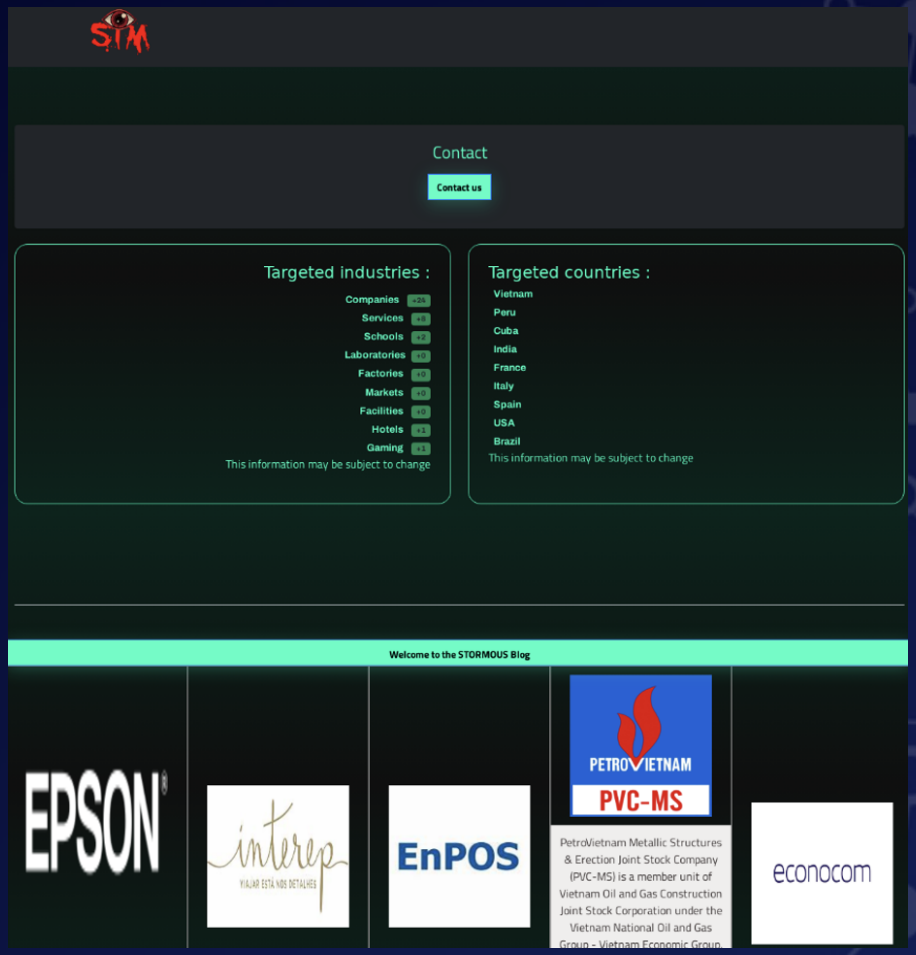
- Evolution & Collaboration:
  Stormous has recently aligned with GhostSec to launch a combined ransomware-as-a-service (RaaS) platform. This partnership facilitates a wider distribution of advanced payloads while using shared dark web infrastructure—most notably, common onion URLs for command-and-control (C2) and leak sites.
- Operational Tactics:
  The group gains initial access via compromised VPN credentials and escalates privileges using both legitimate administrative tools and covert techniques (e.g., DLL sideloading and vulnerable driver exploitation). Once inside, they encrypt files using robust AES-256 encryption and exfiltrate data, which is later used to pressure victims through public data leaks.
- Double-Extortion Model:
  In addition to encrypting victim files (typically appending a ".ghost" extension), Stormous exfiltrates sensitive data. If ransom demands are not met, the stolen data is published on dedicated leak sites, heightening the stakes for affected organisations.

Attack Chain Analysis

1. Initial Access
   - Technique: Credential Theft & VPN Compromise
   - Description:
     Attackers leverage stolen or weak VPN credentials to establish extended remote sessions. Long-duration sessions from atypical IP addresses are indicative of bypassed multifactor authentication and other security controls.
2. Execution & Lateral Movement
   - Technique: Remote Desktop Protocol (RDP) & Administrative Tools
   - Description:
     Post-compromise, attackers use RDP along with tools like PsExec and Windows Management Instrumentation (WMI) to spread laterally. This approach enables them to mimic legitimate user behaviour and remain undetected.
3. EDR Evasion & Privilege Escalation
   - Technique: DLL Sideloading and Exploitation of Vulnerable Drivers
   - Description:
     By replacing trusted DLLs (e.g., avupdate.dll) with malicious versions loaded by legitimate executables (such as upd.exe), the attackers bypass security checks. They further escalate privileges by exploiting a signed yet vulnerable driver (TPwSav.sys) to disable kernel-level security and remove EDR hooks.
4. Impact: Data Encryption & Exfiltration
   - Technique: AES-256 Encryption and Data Exfiltration
   - Description:
     After gaining control, the ransomware encrypts files (often appending a ".ghost" extension) and drops a ransom note (typically in HTML format) containing negotiation instructions. Simultaneously, sensitive data is exfiltrated to remote servers, which serves as a basis for subsequent public leaks if ransoms are not paid.

Detailed TTB Chart
Below is a table detailing the Tactics, Techniques, and Behaviours (TTB) used by Stormous in their attack chain:

Stage	Tactic	Technique
Initial Access	Credential Theft & VPN Compromise	Valid Accounts (T1078) / VPN Hijacking
Execution & Lateral Movement	Remote Desktop Protocol & Use of Legitimate Tools	RDP, PsExec, and WMI
EDR Evasion & Privilege Escalation	DLL Sideloading and Vulnerable Driver Exploitation	Sideloading via upd.exe and malicious replacement of avupdate.dll; exploitation of TPwSav.sys
Impact – Data Encryption & Exfiltration	Data Encryption and Exfiltration	AES-256 Encryption, File Renaming (.ghost extension), and Exfiltration
Command-and-Control (C2) Communication	Shared Dark Web Infrastructure (Onion URLs)	Tor-based C2 and Leak Sites



IOCs
Tox:
C286720F7592E5668A932F1D06EDEECBAFACB3BE369632C908F9511D072C142575BA8109CBC6

URLs
http://3slz4povugieoi3tw7sblxoowxhbzxeju427cffsst5fo2tizepwatid.onion
http://h3reihqb2y7woqdary2g3bmk3apgtxuyhx4j2ftovbhe3l5svev7bdyd.onion
http://h3reihqb2y7woqdary2g3bmk3apgtxuyhx4j2ftovbhe3l5svev7bdyd.onion/stm.html
http://pdcizqzjitsgfcgqeyhuee5u6uki6zy5slzioinlhx6xjnsw25irdgqd.onion

File servers
http://6sf5xa7eso3e3vk46i5tpcqhnlayczztj7zjktzaztlotyy75zs6j7qd.onion

Ransomware Victims Worldwide

A recent ransomware analysis reveals that the United States remains the most heavily impacted nation, accounting for a staggering 49.72% of global incidents, emphasising its continued vulnerability to ransomware threats.

Following the United States, India reported 5.65% of ransomware attacks, making it the second most targeted country in this period. Taiwan also experienced a high rate of incidents, contributing 5.08% to global cases. Canada reported 3.39% of attacks, emerging as another heavily targeted region.

Countries like the United Kingdom (4.52%), France (2.26%), Germany (2.26%), Italy (2.26%), Australia (2.26%), and China (2.82%) have also faced considerable ransomware exposure, underlining ongoing risks in these regions.

Nations such as Spain (1.13%), Brazil (1.69%), Poland (1.13%), Malaysia (1.13%), Peru (1.13%), Austria (1.13%), and Turkey (1.13%) experienced moderate ransomware activity, reflecting persistent but slightly lower levels of targeting.

Several other countries, including the United Arab Emirates, Denmark, Switzerland, Costa Rica, New Zealand, Slovakia, Dominican Republic, Pakistan, Argentina, Laos, Singapore, Thailand, Japan, Monaco, Norway, Egypt, Iraq, Ukraine, and Colombia, each recorded 0.56% of global ransomware cases, highlighting that the ransomware threat remains widespread and not confined to specific regions.

This analysis underscores the persistent and global nature of ransomware attacks, with North America and Asia facing particularly high levels of risk. These findings highlight the critical need for robust cybersecurity frameworks, proactive defence mechanisms, and heightened vigilance across all sectors to combat the evolving ransomware landscape worldwide.

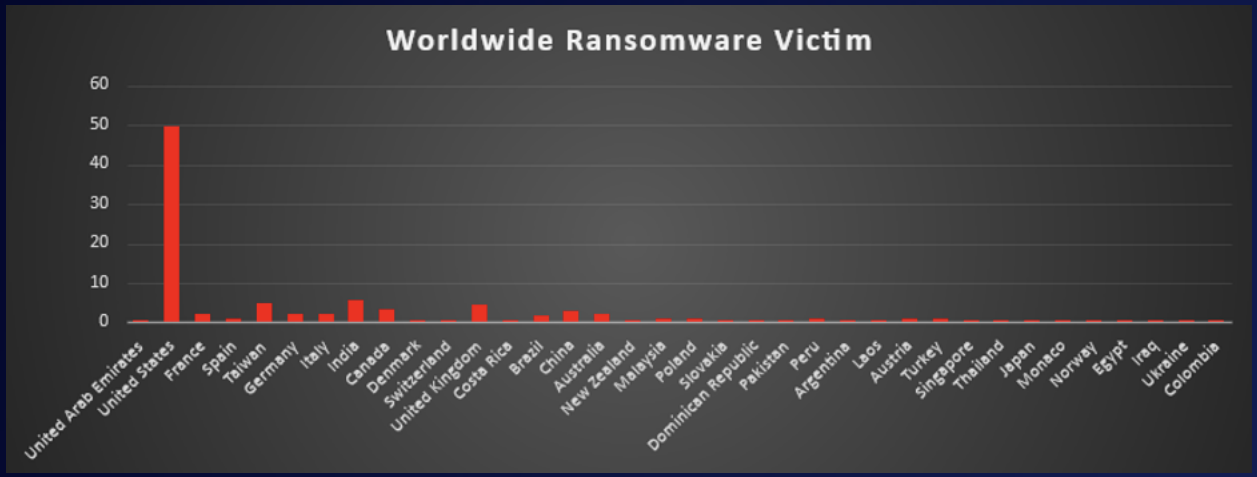


Figure 4: Ransomware Victims Worldwide

Ransomware Victims by Industry

A recent ransomware analysis highlights the Manufacturing sector as the most targeted industry, accounting for 21.47% of total reported incidents. This underscores the persistent threats faced by production processes, industrial operations, and supply chain networks.

Following this, Business Services accounted for 11.86% of ransomware attacks, emphasising the heightened risk to service-oriented organisations. The Healthcare industry also saw significant targeting, representing 7.91% of total incidents, reflecting the vulnerabilities within medical and patient data systems.

Other heavily impacted industries include Retail at 6.78%, Construction at 6.21%, and Education at 5.65%, indicating ongoing security challenges in consumer markets, infrastructure development, and academic institutions. The Transportation and Federal sectors each recorded 5.08% of ransomware incidents, showing that critical infrastructure and government entities remain key targets.

Industries such as Hospitality (3.95%), Consumer Services (4.52%), Law Firms (3.39%), and Finance (2.82%) also reported considerable exposure, highlighting the risks to sectors handling sensitive financial, legal, and consumer information.

Further, Telecommunications (2.82%), Real Estate (1.69%), Insurance (1.69%), Media & Internet (1.69%), and Organisations (1.69%) faced notable but relatively lower levels of ransomware incidents, reflecting cybercriminals' continued interest in essential service sectors and information management.

Meanwhile, industries like Technology (1.13%), IT (1.13%), and Law Firm (0.56%) (as a separate category from Law Firms) experienced targeted attacks, emphasising that professional and tech-based services are not immune. Other sectors, including Metals & Mining, Energy, Agriculture, and Electricity, each reported 0.56% of incidents, highlighting attacks against industrial and essential resource-based industries.

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 frameworks, proactive defence mechanisms, and continuous risk assessments to combat the ever-evolving ransomware landscape.

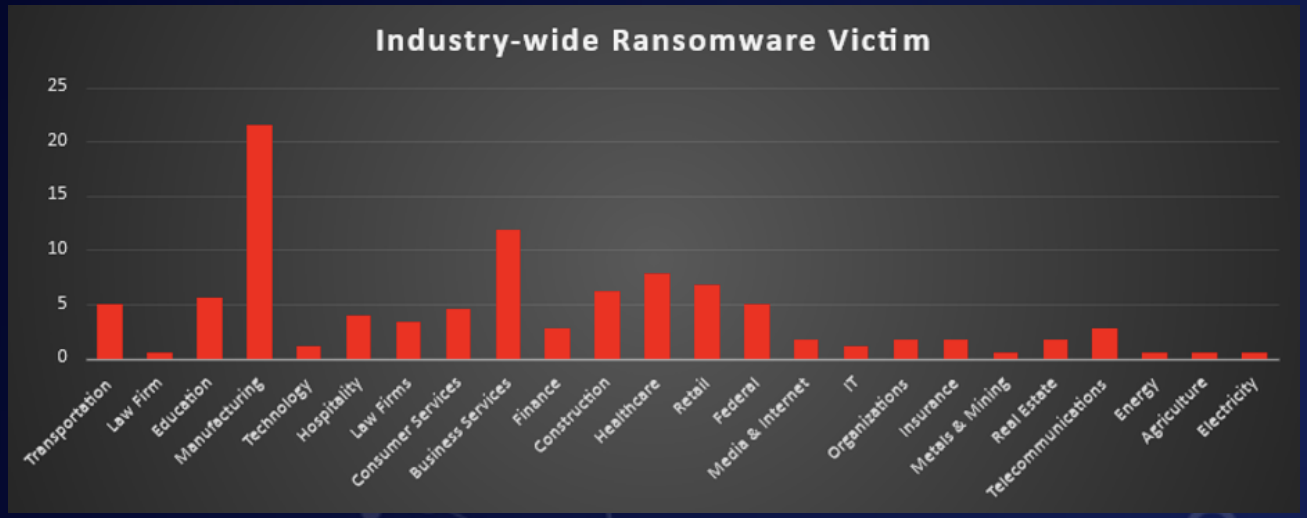


Figure 5: Industry-wide Ransomware Victims