Red Piranha
unified threat management

THREAT INTELLIGENCE REPORT

April 8 - 14, 2025

Report Summary:

- **New Threat Detection Added** – 2
  - MinIO Incomplete Signature Validation for Unsigned-Trailer Uploads (CVE-2025-31489)
  - PostgreSQL Authenticated Remote Code Execution (CVE-2025-2945)

- **New Threat Protections - 197**

The following threats were added to Crystal Eye this week:

1. MinIO Incomplete Signature Validation for Unsigned-Trailer Uploads CVE-2025-31489

The Signature component of the authorisation may be invalid which will allow clients with some knowledge and access (Bucket information and WRITE permissions) to upload random objects to the instance.

Threat Protected: 01
Rule Set Type:

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

Class Type: Web-application-activity

Kill Chain:

Tactic	Technique	Description
Initial Access	T1078	Valid Accounts
Execution	T1059.009	Command and Scripting Interpreter: Cloud API
Collection	T1530	Data from Cloud Storage

2. PostgreSQL Authenticated Remote Code Execution CVE-2025-2945

This vulnerability allows remote code execution via unsafe parameters in two pgAdmin endpoints. The POST endpoints /sqleditor/query_tool/download (query_command parameter) and /cloud/deploy (high_avaliability parameter) use parameters that are unsafely passed through a Python eval() function allowing the RCE.

Threat Protected: 02
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: Web-application-attack

Kill Chain:

Tactic	Technique	Description
Initial Access	T1078	Valid Accounts
Execution	T1059.009	Command and Scripting Interpreter: Cloud API

Known exploited vulnerabilities (Week 2 April 2025):

Vulnerability	CVSS	Description
CVE-2024-53197 CVE-2024-53150	7.8 (High)	Linux Kernel contains a vulnerability in the USB-audio driver that allows an attacker with physical access to the system to use a malicious USB device to potentially manipulate system memory, escalate privileges, or execute arbitrary code.
CVE-2025-30406	9.8 (Critical)	Gladinet CentreStack contains a use of hard-coded cryptographic key vulnerability in the way that the application manages keys. Successful exploitation allows an attacker to created payloads for server-side deserialisation, allowing for remote code execution.
CVE-2025-29824	7.8 (High)	Microsoft Windows Common Log File System (CLFS) Driver contains a use-after-free vulnerability that allows an authorised attacker to elevate privileges locally.
CVE-2025-31161	9.8 (Critical)	CrushFTP contains an authentication bypass vulnerability in the HTTP authorisation header that allows a remote unauthenticated attacker to authenticate to any known or guessable user account.

For more information, please visit the **Red Piranha Forum**:
https://forum.redpiranha.net/t/known-exploited-vulnerabilities-catalog-3rd-week-of-april-2025/560

Updated Malware Signatures (Week 2 April 2025)

Threat	Description
ClipBanker	Is an information stealer and spy trojan, it aims to steal information such as Browser History, Cookies, Outlook data, Skype, Telegram and searches for cryptocurrency wallets. It is usually distributed through phishing emails and social media posts.
Grandoreiro Stealer	Is a Banking trojan, that allows threat actors to perform fraudulent banking operations on the victim's computer to bypass banking security. This trojans is usually delivered through phishing 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 Groups	Overall Percentage of total attack coverage
Space Bears	1.46%
Hellcat	2.93%
Hunters	2.93%
Sarcoma	2.44%
Leaked Data	6.34%
Cicada3301	0.98%
Qilin	13.66%
Play	6.83%
DragonForce	8.78%
Lockbit3.0	2.44%
Devman	3.41%
Bert	0.98%
Akira	20.98%
Rhysida	0.49%
RansomHouse	0.98%
KillSec3	1.46%
Morpheus	0.98%
Interlock	0.98%
Kairos	0.98%
Crypto24	2.93%
Medusa	1.46%
MetaEncryptor	0.49%
Inc ransom	3.41%
Team Underground	0.49%
NightSpire	3.41%
Chaos	0.49%
Lynx	1.46%
Run Some Wares	0.49%
RAlord	0.49%
3AM	3.9%
Termite	0.49%
Brain Cipher	0.49%

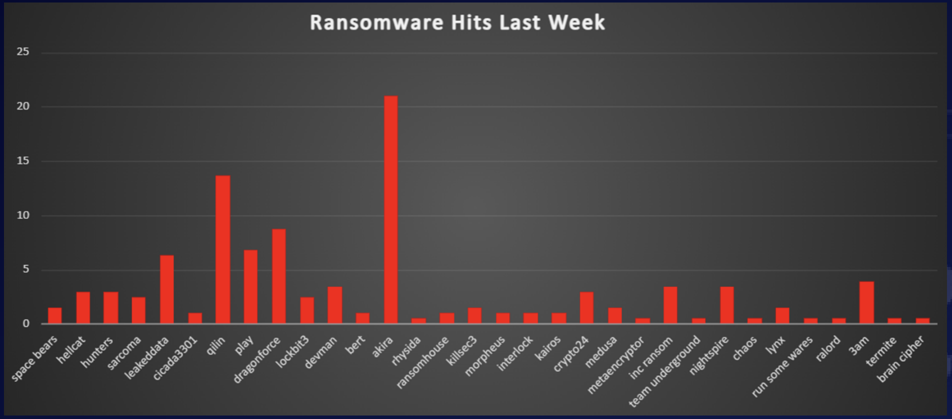


Figure 1: Ransomware Group Hits Last Week

NightSpire Ransomware Group

NightSpire is an emerging ransomware operation that surfaced in early 2025. While it shares characteristics with established Ransomware-as-a-Service (RaaS) models, NightSpire exhibits signs of inexperience, such as operational security lapses and the use of mainstream communication channels. Despite this, the group has rapidly expanded its victimology, targeting small to medium-sized enterprises across various sectors.

Attack Chain Analysis

Initial Access
- Exploits vulnerabilities in external-facing services, notably the FortiOS zero-day CVE-2024-55591, allowing unauthorised super-admin access to FortiGate firewalls.

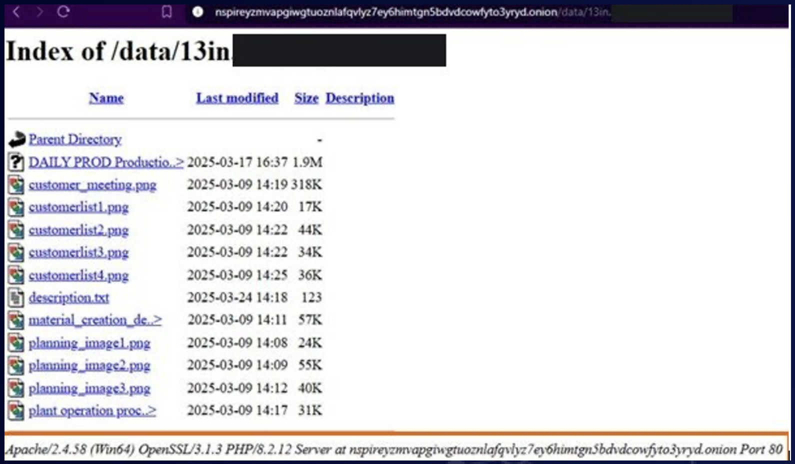
Lateral Movement
- Utilises native Windows utilities such as PsExec, WMI, and RDP to traverse networks.

Execution
- Deploys payloads using PowerShell scripts and obfuscated binaries.

Defence Evasion
- Employs "living off the land" techniques, using legitimate system tools to avoid detection.

Data Exfiltration and Impact
- Implements a double extortion model: exfiltrates data using tools like MEGAcmd and WinSCP, then encrypts files, threatening to leak data if ransoms aren't paid.

Stage	Tactic	Technique ID	Technique Description	Details
Initial Access	Exploit Public-Facing Application	T1190	Exploitation of CVE-2024-55591	Gains unauthorised super-admin access to FortiGate firewalls.
Execution	Command and Scripting Interpreter	T1059	PowerShell and Batch Script Execution	Deploys ransomware payloads and scripts.
Persistence	Scheduled Task/Job	T1053	Creation of Scheduled Tasks	Ensures persistence across system reboots.
Privilege Escalation	Exploitation for Privilege Escalation	T1068	Exploits for Privilege Escalation	Leverages system vulnerabilities to gain higher privileges.
Defence Evasion	Obfuscated Files or Information	T1027	Obfuscation Techniques	Uses obfuscated code and legitimate tools to evade detection.
Credential Access	OS Credential Dumping	T1003	LSASS Memory Dumping	Extracts credentials using tools like Mimikatz.
Lateral Movement	Remote Services	T1021	Use of SMB, RDP, and PsExec	Moves laterally within networks using valid credentials.
Impact	Data Encrypted for Impact	T1486	File Encryption	Encrypts data using symmetric encryption algorithms.
Exfiltration	Exfiltration Over Web Service	T1567.002	Data Exfiltration via MEGAcmd and WinSCP	Transfers stolen data to cloud storage services like Mega.nz.

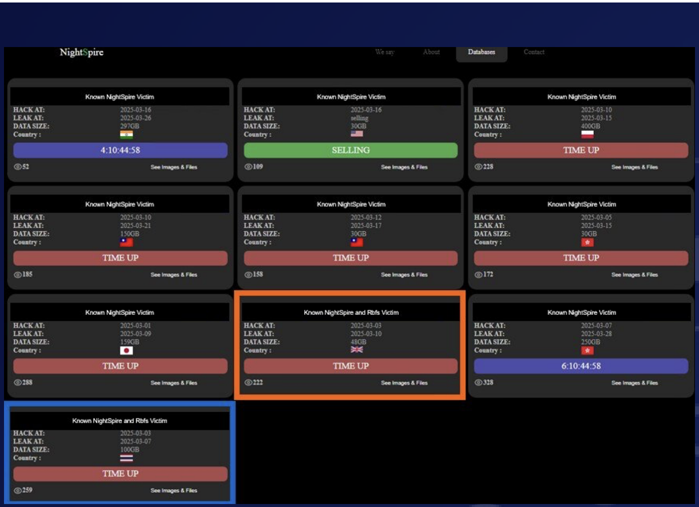


nspireyzmvapgiwgtuoznlafqvlyz7ey6himtgn5bdvdcowfyto3yryd.onion/data/13in.[redacted]

Index of /data/13in[redacted]

```
   Name                         Last modified     Size  Description
   Parent Directory                                  -
   DAILY PROD Productio..>      2025-03-17 16:37  1.9M
   customer_meeting.png         2025-03-09 14:19  318K
   customerlist1.png            2025-03-09 14:20   17K
   customerlist2.png            2025-03-09 14:22   44K
   customerlist3.png            2025-03-09 14:22   34K
   customerlist4.png            2025-03-09 14:25   36K
   description.txt              2025-03-24 14:18   123
   material_creation_de..>      2025-03-09 14:11   57K
   planning_image1.png          2025-03-09 14:08   24K
   planning_image2.png          2025-03-09 14:09   55K
   planning_image3.png          2025-03-09 14:12   40K
   plant operation proc..>      2025-03-09 14:17   31K
```

Apache/2.4.58 (Win64) OpenSSL/3.1.3 PHP/8.2.12 Server at nspireyzmvapgiwgtuoznlafqvlyz7ey6himtgn5bdvdcowfyto3yryd.onion Port 80



Known NightSpire Victim
HACK AT: 2025-03-16
LEAK AT: 2025-03-26
DATA SIZE: 297GB
Country : 🇮🇳
4:10:44:58
52 See Images & Files

Known NightSpire Victim
HACK AT: 2025-03-16
LEAK AT: selling
DATA SIZE: 30GB
Country : 🇺🇸
SELLING
109 See Images & Files

Known NightSpire Victim
HACK AT: 2025-03-10
LEAK AT: 2025-03-15
DATA SIZE: 400GB
Country : 🇵🇱
TIME UP
228 See Images & Files

Known NightSpire Victim
HACK AT: 2025-03-10
LEAK AT: 2025-03-21
DATA SIZE: 150GB
Country : 🇹🇼
TIME UP
185 See Images & Files

Known NightSpire Victim
HACK AT: 2025-03-12
LEAK AT: 2025-03-17
DATA SIZE: 30GB
Country : 🇹🇼
TIME UP
158 See Images & Files

Known NightSpire Victim
HACK AT: 2025-03-05
LEAK AT: 2025-03-15
DATA SIZE: 30GB
Country : 🇻🇳
TIME UP
172 See Images & Files

Known NightSpire Victim
HACK AT: 2025-03-01
LEAK AT: 2025-03-09
DATA SIZE: 159GB
Country : 🇯🇵
TIME UP
288 See Images & Files

Known NightSpire and Rbfs Victim
HACK AT: 2025-03-03
LEAK AT: 2025-03-10
DATA SIZE: 48GB
Country : 🇬🇧
TIME UP
222 See Images & Files

Known NightSpire Victim
HACK AT: 2025-03-07
LEAK AT: 2025-03-28
DATA SIZE: 250GB
Country : 🇻🇳
6:10:44:58
328 See Images & Files

Known NightSpire and Rbfs Victim
HACK AT: 2025-03-03
LEAK AT: 2025-03-07
DATA SIZE: 100GB
Country : 🇹🇭
TIME UP
259 See Images & Files

Indicator	Description	SHA256
MEGAcmd	Mega-related tool, used by NightSpire for data transfer as part of data exfiltration.	Hash was not retrievable.
Everything.exe	Voidtools' Everything	35cefe4bc4a98ad73dda4444c700aac9
	Tool filename, used by NightSpire for scanning directories and file enumeration.	f749efde8f9de6a643a57a5b605bd4e7
WinSCP-6.3.7-Setup.exe	Tool used by NightSpire for data exfiltration activities.	
7z2408-x64.exe, 7zG.exe, 7z.exe	Filenames of 7zip executables, used by NightSpire to compress data prior to exfiltration activities.	
WINDOWS-DTX-8GB, XDRAGON-SERVER1	Hostnames of devices used by NightSpire to conduct their attacks.	
14.139.185.60	WinSCP remote server IP address associated with NightSpire's infrastructure.	
WINDOWS-DTX-8GB, XDRAGON-SERVER1	Hostnames of devices used by NightSpire to conduct their attacks.	
14.139.185.60	WinSCP remote server IP address associated with NightSpire's infrastructure.	

IP Addresses
14.139.185.60: Associated with WinSCP remote server used by NightSpire.

Hostnames
XDRAGON-SERVER1: Hostname observed in NightSpire attacks, linked to the operator alias 'xdragon128'.

File Artifacts
7z2408-x64.exe, 7zG.exe, 7z.exe: 7-Zip executables used to compress data prior to exfiltration.

Communication Channels
Gmail Addresses: Utilised for victim communication, indicating a lack of operational security
Tor-Based Leak Site: Hosts stolen data to pressure victims into paying ransoms.

Onion URLs
nspireyzmvapgiwgtuoznlafqvlyz7ey6himtgn5bdvdcowfyto3yryd.onion
nspireyzmvapgiwgtuoznlafqvlyz7ey6himtgn5bdvdcowfyto3yryd.onion
Nspireyzmvapgiwgtuoznlafqvlyz7ey6himtgn5bdvdcowfyto3yryd.onion

Ransomware Victims Worldwide

A recent ransomware threat landscape analysis reveals that the United States remains the most significantly impacted nation, accounting for a substantial 52.2% of global incidents. This highlights the persistent targeting of US-based organisations by increasingly sophisticated ransomware operations.

Canada emerges as the second-most affected country, reporting 5.85% of global incidents, followed by India at 3.9%, and Germany, Italy, and Australia, each contributing 2.93%. These figures signal an intensifying focus on key global economies across North America, Europe, and Asia-Pacific.

Several other countries have experienced moderate levels of ransomware activity, including Japan and Singapore (2.44% each), as well as the United Kingdom, France, and Taiwan (1.95% each), reflecting a broader geographic distribution of ransomware attacks across the globe.

Nations reporting 1.46% of incidents each include Mexico, Brazil, China, and Spain — suggesting that even well-defended or geographically distant nations are not immune to these threats. Similarly, countries like Egypt, Saudi Arabia, Malaysia, and Poland each reported 0.98% of cases.

A number of countries recorded lower yet notable percentages of ransomware activity, each contributing 0.49% of global incidents. These include The Netherlands, Austria, China, Israel, Colombia, Indonesia, Argentina, Japan, Ireland, Switzerland, Sweden, Egypt, Iran, Ukraine, New Zealand, Greece, Turkey, Thailand, South Korea, South Africa, Peru, Portugal, Romania, Luxembourg, Czech Republic, Malta, Jordan, Hungary, and Cyprus.

This global distribution of ransomware incidents underscores the widening scope and international scale of cybercriminal operations. The findings highlight the urgent need for coordinated cybersecurity efforts, including cross-border intelligence sharing, robust threat detection capabilities, and resilient incident response plans to mitigate the escalating risk posed by ransomware threats.

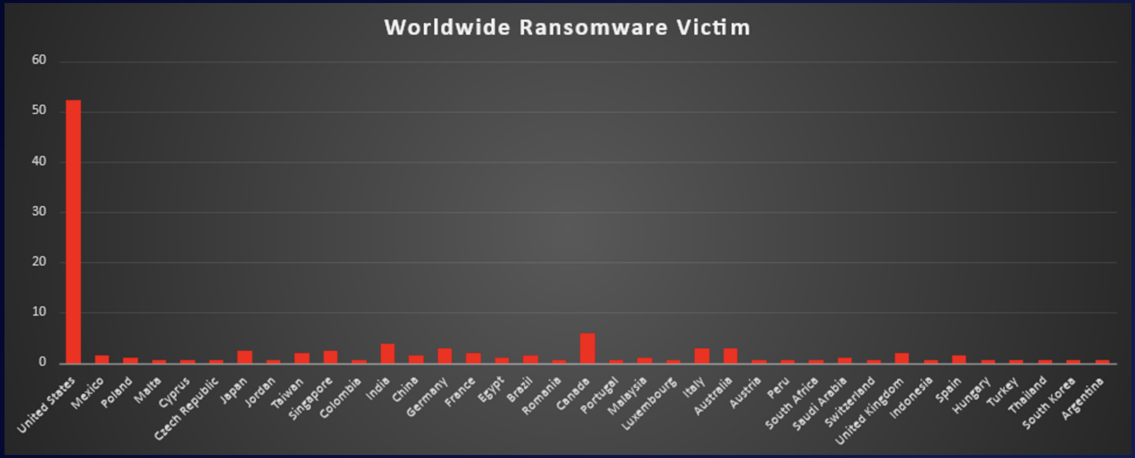


Figure 4: Ransomware Victims Worldwide

Ransomware Victims by Industry

In the most recent industry-specific analysis of ransomware activity, the Manufacturing sector has emerged as the most targeted, accounting for 19.51% of global incidents. This continues to highlight the pressing vulnerabilities in industrial control systems, production infrastructure, and interconnected supply chains.

Business Services followed closely with 17.07%, signaling sustained ransomware focus on service-based and consulting organisations that handle large volumes of client data. The Construction industry ranked third, with 12.2% of incidents, reflecting ongoing exposure among engineering, infrastructure, and development firms.

Other heavily impacted sectors include Retail (9.76%) and Hospitality (5.85%), underscoring the targeting of consumer-focused industries and public-facing enterprises. Law Firms accounted for 5.37%, highlighting the attractiveness of legal firms that manage sensitive contractual and litigation data.

Sectors such as Healthcare (3.41%), Finance (2.93%), Telecommunications (2.44%), Transportation (2.44%), Real Estate (2.44%), IT (2.44%), Electronics (2.44%), and Education (2.44%) all reported comparable levels of ransomware incidents. These numbers reflect the growing attack surface presented by essential service providers and technology-reliant sectors.

Emerging concerns were observed in Insurance (1.95%), Consumer Services (1.95%), Minerals & Mining (1.46%), and Energy (1.46%), indicating ransomware operators' increasing interest in sectors with valuable operational or financial data.

Lower but still notable targeting was seen in Federal (0.98%), Electricity (0.49%), Media & Internet (0.49%), and Organisations (0.49%), showing that even smaller or niche sectors remain exposed to opportunistic ransomware threats.

This analysis affirms that ransomware attacks remain indiscriminate and opportunistic, affecting both critical infrastructure and commercial enterprises. The growing breadth of targeted sectors reinforces the necessity for industry-specific cybersecurity frameworks, enhanced intrusion detection mechanisms, and robust incident response plans to combat these evolving threats.

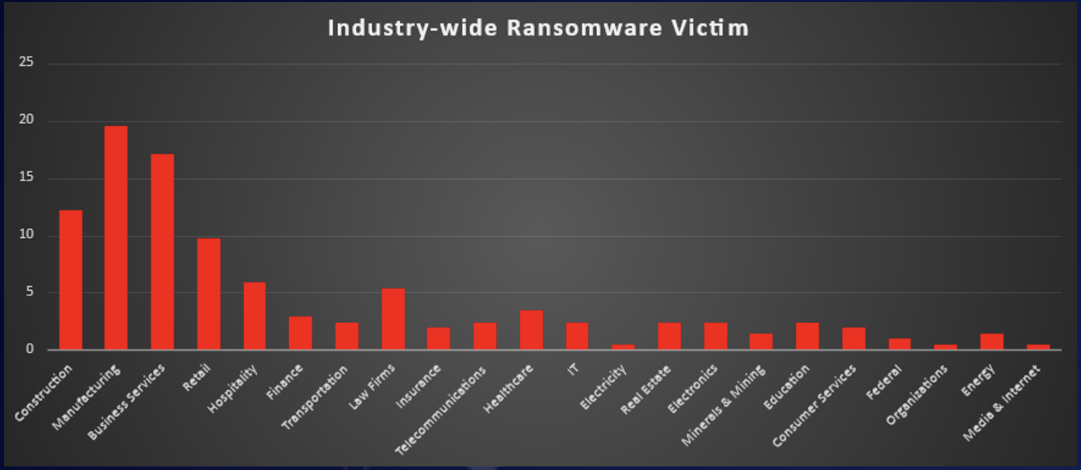


Figure 5: Industry-wide Ransomware Victims