Red Piranha
unified threat management

THREAT INTELLIGENCE REPORT

Jan 28 - Feb 03, 2025

Report Summary:

- **New Threat Detection Added** – 2
  - Nosviak C2
  - Progress WhatsUp QNAP QTS/QuTS File Upload CVE-2024-53691
- **New Threat Protections - 182**

The following threats were added to Crystal Eye this week:

1. Nosviak C2

Nosviak is a botnet command-and-control (C2) system that supports various callback communication protocols, including those used by Mirai and Qbot. Over the past seven months, there has been an increase in hosts tagged as Nosviak. Researchers have identified a network of over 150 interconnected hosts across 20 countries, operating modified versions of Nosviak. These systems offer Distributed Denial-of-Service (DDoS) and proxy services under the guise of "stress testing" tools. The storefronts associated with this network often share identical HTML templates, differentiated only by unique branding, names, and pricing structures. Many of these services utilise Nosviak's branding API to apply distinct themes while potentially operating on shared infrastructure.

Threat Protected: 14
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
Command-and-Control	T1071.001	Application Layer Protocol: Web Protocols

2. QNAP QTS/QuTS File Upload CVE-2024-53691

A critical path traversal vulnerability, identified as CVE-2024-53691, has been discovered in QNAP Network Attached Storage (NAS) devices running QTS 5.1.x and QuTS hero h5.1.x. This vulnerability allows authenticated users with file upload permissions to upload a ZIP file containing a symbolic link (symlink). By exploiting the encrypt/decrypt functionality, an attacker can achieve arbitrary file write, leading to remote code execution with root privileges. QNAP has addressed this issue in QTS 5.2.0.2802 build 20240620 and later, and QuTS hero h5.2.0.2802 build 20240620 and later.

Threat Protected: 03
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	T1078	Valid Accounts
Execution	T1059.004	Command and Scripting Interpreter: Unix Shell

Known exploited vulnerabilities (Week 5 January 2024):

Vulnerability	CVSS	Description
CVE-2025-24085	7.8 (High)	Apple Multiple Products Use-After-Free Vulnerability

For more information, please visit the **Red Piranha Forum**:
https://forum.redpiranha.net/t/known-exploited-vulnerabilities-catalog-5th-week-of-january-2025/542

Updated Malware Signatures (Week 5 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.

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
Abyss-data	0.49%
GD LockerSec	1.47%
DragonForce	5.88%
Killsec3	0.98%
FunkSec	3.43%
Space Bears	0.49%
SafePay	3.43%
RansomHouse	0.49%
Lynx	5.88%
Akira	3.43%
Babuk-Bjorka	31.86%
Inc ransom	6.37%
Qilin	3.43%
Everest	0.49%
Metaencryptor	0.49%
Rhysida	1.47%
Cloak	1.96%
Monti	3.92%
RansomHub	0.98%
Play	5.39%
Cactus	3.43%
Fog	0.98%
Handala	0.49%
Kairos	0.49%
Leaked Data	2.94%
Eraleign (APT73)	1.47%
3AM	0.49%
Termite	0.49%
Fsociety	0.49%
8Base	0.49%
Medusa	5.88%

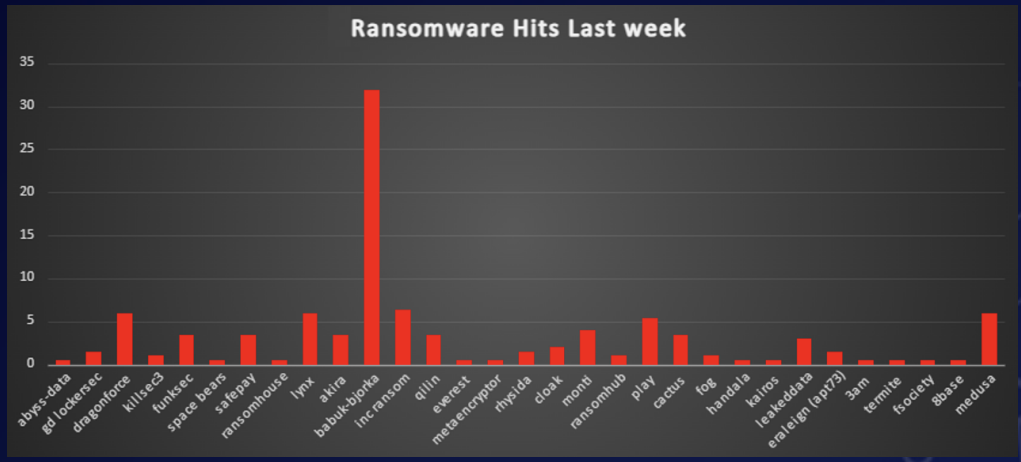

Figure 1: Ransomware Group Hits Last Week

Babuk-Bjorka Ransomware

1. Overview

The Red Piranha Team conducts ongoing surveillance of the dark web and other channels to track global organisations impacted by ransomware. In late 2021, our monitoring highlighted the rising dominance of multiple ransomware families, including Babuk, RansomHouse, and others targeting enterprise-level systems. Recently, we uncovered Babuk 2 or Babuk-Bjorka, a threat actor leveraging the Babuk name to inflate credibility and extort victims by recycling previously leaked data from other groups.

Our initial deep-dive analysis suggests that Babuk 2 is not an official or revived branch of the original Babuk group. Rather, the group appears to be engaging in double-extortion posturing—much like other ransomware collectives—but without any definitive evidence of actual, large-scale deployments. Instead, Babuk 2 is posting victims claimed by multiple existing threat groups, implying they are fabricating or exaggerating their attack history.

2. Key Findings

1. High Incidence of Recycled Victim Claims:
   - Over 90% of the listed victims on the Babuk 2 Data Leak Site (DLS) were previously posted by groups like FunkSec, RansomHub, LockBit, and Meow. This strongly indicates Babuk 2 is opportunistically republishing old breaches.
2. Unverified Encryption Operations:
   - Unlike RansomHouse, which aggressively encrypts data using tools like Mario ESXi and automates attacks with MrAgent, Babuk 2 has not demonstrated tangible deployment or specialised tools.
   - The group is, instead, mimicking double-extortion tactics by threatening to release data unless a ransom is paid.
3. Potential Exploitation of Leaked Babuk Code:
   - The original Babuk source code was leaked in 2021 and subsequently integrated by various groups. Babuk 2 may be using—or falsely claiming to use—this leaked code to bolster their perceived capabilities.

3. Babuk 2 Tools and Techniques (Hypothesised)

Note: While the original Babuk group's leaked source code is available online, Babuk 2's exact tooling remains unverified.

3.1 Claimed Ransomware Locker

•Background: Babuk 2 references the old Babuk source code.

•Observations: No confirmed samples or hashes have been attributed to Babuk 2's locker.

3.2 Data Leak Site (DLS) Operations

- Method:
  - Babuk 2 has posted over 64 alleged victims, most of which match historical breaches by other groups.
  - The DLS content suggests a double-extortion approach, but there is no direct evidence of fresh data exfiltration.

4. Tactics, Techniques, and Procedures (TTPs)

Tactic	Technique	ID	Description
Initial Access	Valid Accounts	T1078.002	There is no evidence of new account compromises directly tied to Babuk 2.
Impact	Data Encrypted for Impact	T1486	Babuk 2's DLS references encryption, but no confirmed incidents exist.
Impact	Data Manipulation (Extortion)	T1565.002	Babuk 2 recycles older breach data in posted victim claims.
Command-and-Control	Unverified / Unclear	—	Babuk 2's infrastructure remains undefined.
Exfiltration	Exfiltration Over Web Service	T1567.002	Posted data is consistent with older leaks, with no proven new exfiltration.

5. Observed Indicators of Compromise (IOCs)

- Babuk 2 Ransom Note (Text Sample):
  - A single sample uploaded from Croatia on January 10, 2025, containing text nearly identical to multi-group ransom notes.
- Victim Listings:
  - Over 64 organisations listed, with 90%+ duplication from other groups' historical claims.

No unique file hashes, network indicators, or command-and-control details specific to Babuk 2 have been confirmed.

Email Addresses

- locksupport@onionmail.org

Telegram Handles

- @babuklockberOffice
- @bjorkanesiaaaa

Tox IDs

022A7EEB83B648F55DA7A6BEFD130C2156C74F3501A31D853234EC2D18E77A1E5BEC7F602011

552653D2E9A5701EA30612EAE77345293F2E35C5D29DB196BB62395BE71BB25F

Cryptocurrency Wallets

- BTC: 1JdvS63gBEFH3auYStgeSB3Q2xMdi5cZiF
- XMR: 84aZsdYquVxDCVn49UDS8K89bhKyRzAqBMef4XxZ7QQ7eSuSPxnpD1oKbhZpE6pqPSG25V6Z3oRNkfXLuxqxYPzYL4xQPKV
- ETC: 0xFd8Cd01BAB931c9aF6a99A5F969a9052bBee6fd7
- ETH: 0x9e2f075d3fff657695dc4661f42115588ee13263

Onion URLs

- http://7dikawx73goypgfi4zyo5fcajxwb7agemmiwqax3p54aey4dwobcvcyd.onion
- http://gtmx56k4hutn3ikv.onion/
- http://xeuvs5poflczn5i5kbynb5rupmidb5zjuza6gaq22uqsdp3jvkjkciqd.onion/
- http://fpwwt67hm3mkt6hdavkfyqi42oo3vkaggvjj4kxdr2ivsbzyka5yr2qd.onion/
- http://57mphyfkxoj5lph2unswd23akewz3jtj7mb6wignwmyto32ghp2visid.onion/

Ransomware Victims Worldwide

A recent ransomware analysis reveals that the United States remains the most heavily impacted nation, accounting for a staggering 49.02% of global incidents, highlighting its continued vulnerability to ransomware threats. Following this, the United Kingdom reported 6.86% of the attacks, emerging as another notable target. Several countries exhibit considerable exposure to ransomware threats, including Canada at 4.41%, as well as Australia and India at 3.92% each. Meanwhile, Germany and Brazil both reported 3.43% of ransomware incidents, indicating an ongoing risk in these regions.

A number of nations registered moderate impact levels, such as Spain and Indonesia (1.96% each), alongside Sweden, Colombia, Italy, and France (1.47% each). Other countries, including Norway, Netherlands, Egypt, Japan, and Argentina, each experienced 0.98% of the reported attacks.

A broader set of countries—Romania, Paraguay, Mexico, Kenya, Macedonia, Zambia, China, Turkey, Malaysia, Slovakia, El Salvador, Honduras, South Korea, Uganda, Singapore, Israel, Vietnam, Bangladesh, Thailand, Portugal, and Finland—each contributed 0.49% to the overall ransomware landscape, underscoring the far-reaching, global nature of these threats.

This analysis underlines the persistent and worldwide scope of ransomware attacks, with North America showing particularly high vulnerability. The findings emphasise the critical need for robust cybersecurity measures, proactive defence strategies, and heightened vigilance across all sectors to combat the relentless growth of ransomware threats.

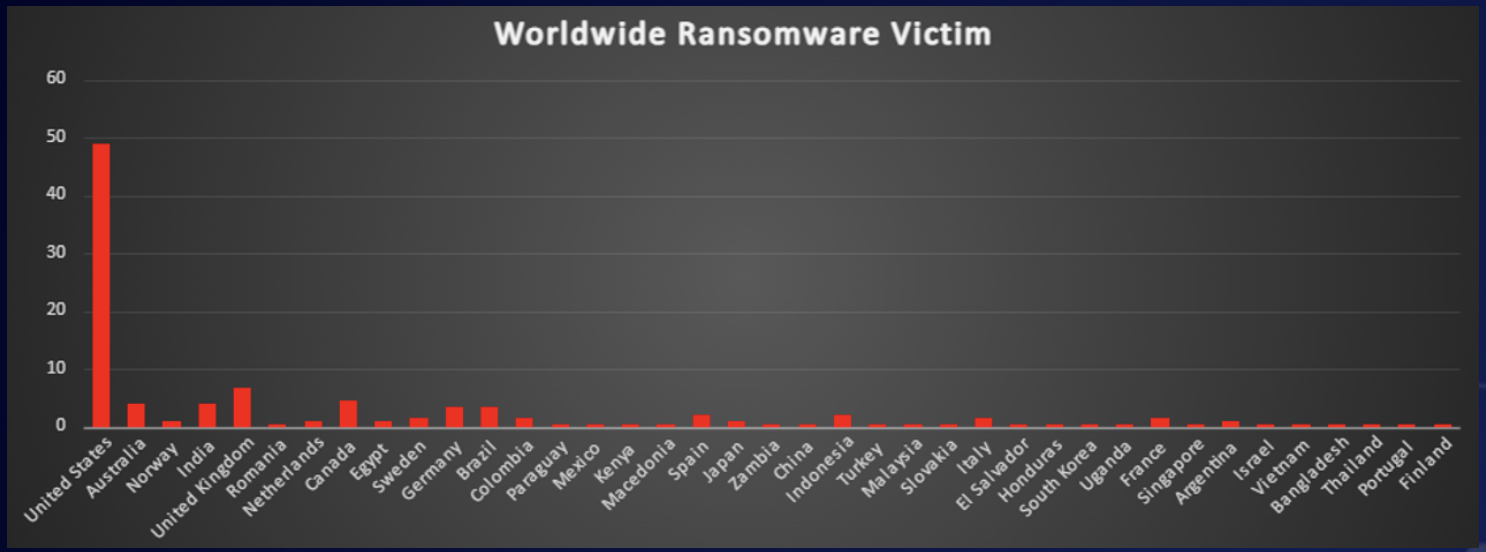

Figure 2: Ransomware Victims Worldwide

Ransomware Victims by Industry

A recent ransomware analysis highlights the Retail sector as the most targeted industry, accounting for 15.69% of total reported incidents. This underscores the heightened risk posed to consumer-facing operations and payment systems.

Close behind are the Manufacturing sector at 11.76% and Business Services at 11.27%, emphasising the persistent threats faced by production processes and service-oriented organisations. Other significantly affected industries include Education at 6.86% and Healthcare at 6.37%, reflecting ongoing vulnerabilities in sectors handling sensitive data and critical services.

Meanwhile, Construction reports 5.88% of attacks, followed by IT and Transportation at 4.41% each. Finance and Hospitality each account for 3.92% of reported incidents, while Law Firms and Federal institutions both see 3.43%. Lower, yet notable shares of ransomware activity appear in Media & Internet and Telecommunications (2.94% each), Energy, Organisations, and Consumer Services (2.45% each), as well as Real Estate and Insurance (1.96% each). Agriculture records 0.98% of incidents, and Minerals & Mining shows a minimal but noteworthy 0.49%.

This analysis underscores the pervasive and indiscriminate nature of ransomware threats, impacting industries across critical infrastructure, public services, and commercial enterprises. The findings highlight the urgent need for sector-specific cybersecurity strategies, robust defences, and proactive risk management to effectively combat the evolving ransomware landscape.

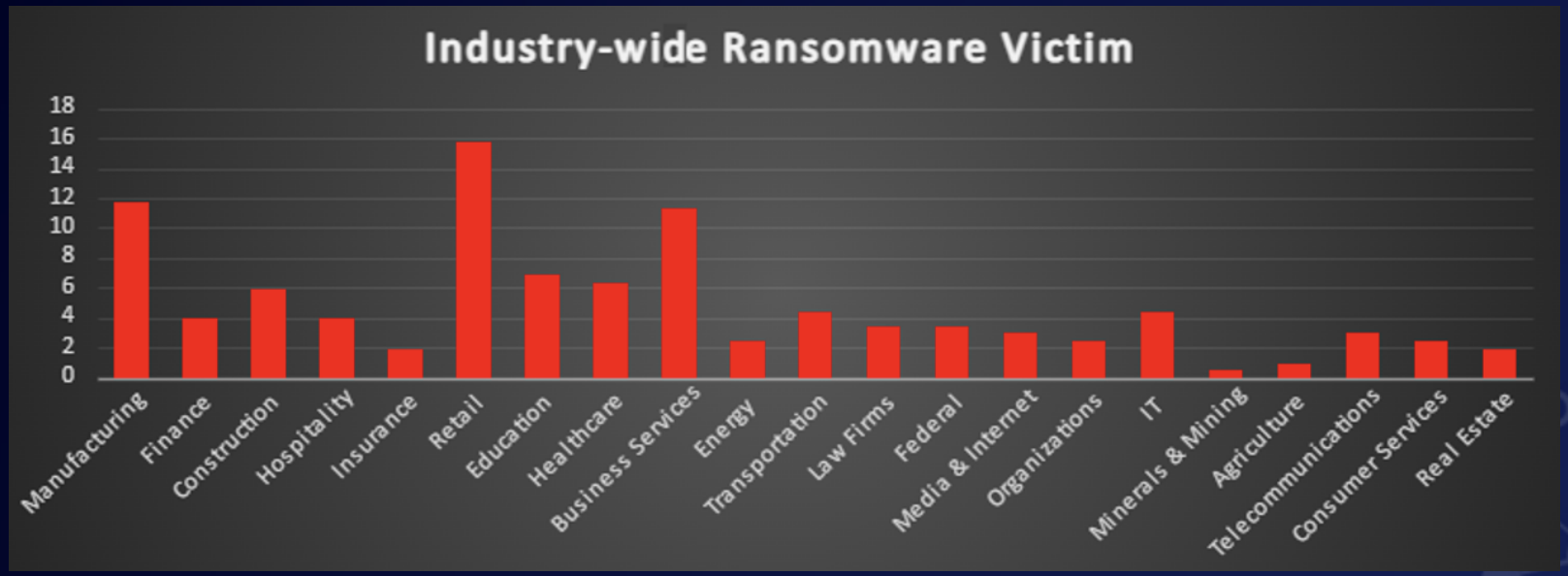

Figure 3: Industry-wide Ransomware Victims