Red Piranha
unified threat management

# THREAT INTELLIGENCE REPORT

May 23 - 29, 2023

# Report Summary:

- **New Threat Detection Added** – 4 (Delta Stealer CVE-2023-2571, AhRat Android Malware, and Vultur)
- **New Threat Protections**
- **Overall Weekly Observables Count**
- **Daily submissions by Observable Type**
- **New Ransomware Victims Last Week**

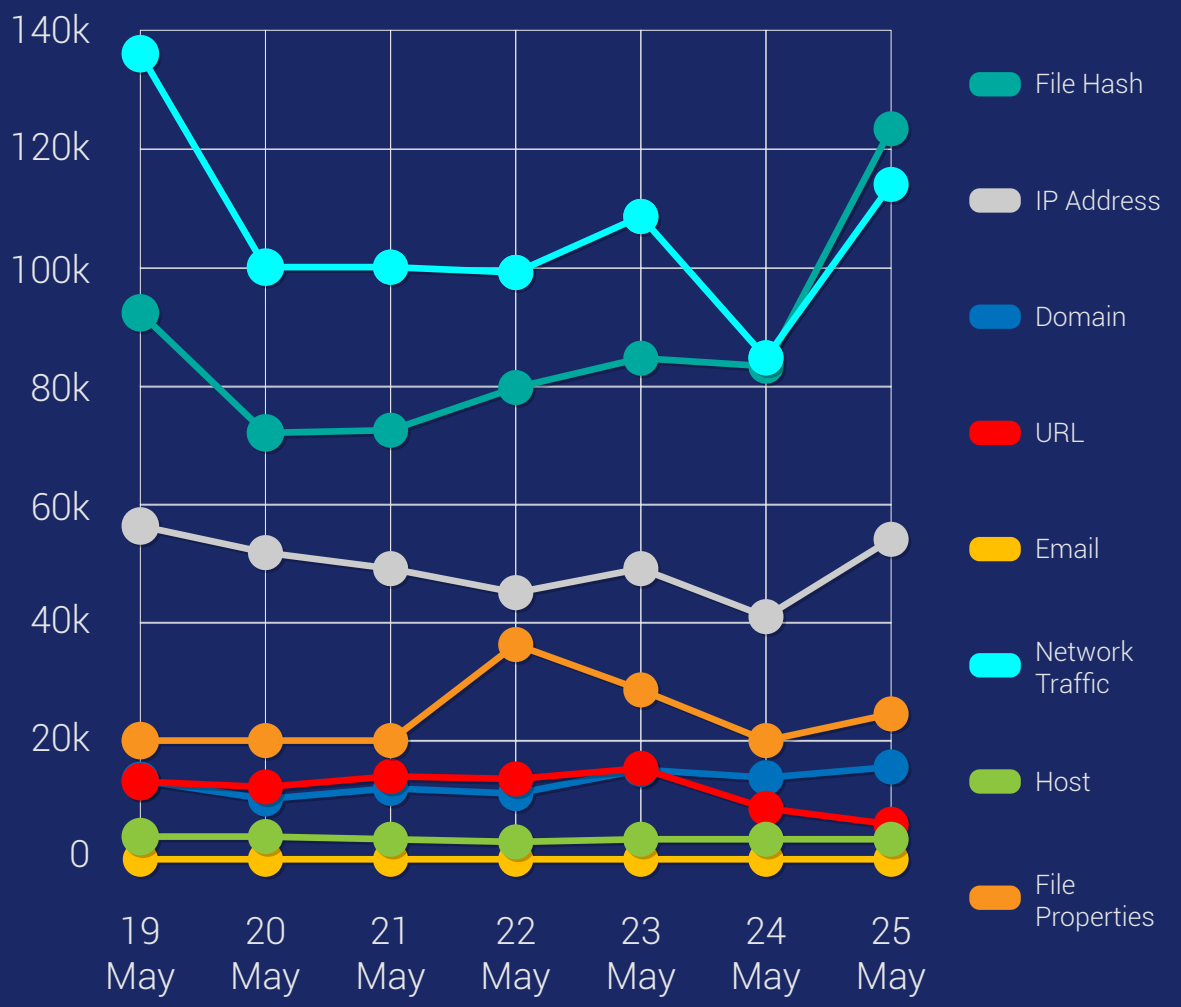
## New Threat Protections (Week Ending 29/05/2023):

4

## Overall Weekly Observables Count:

2,094,855

## Daily Submissions by Observable Type:



# Newly Detected Threats Added

## 1. Delta Stealer

Delta Stealer is a type of malware that has gained attention in the cybersecurity landscape. It is an information-stealing Trojan designed to target users' sensitive data, such as login credentials, financial information, and cryptocurrency wallets. Delta Stealer has been observed leveraging the popular Rust programming language, making it an example of the growing adoption of Rust for malicious purposes. The malware's name, "Delta Stealer," stems from the fact that it was initially discovered and analysed by the cybersecurity firm, Kaspersky, in 2019. Since then, it has undergone several evolutions and updates to enhance its capabilities and evade detection by security software.

One notable characteristic of Delta Stealer is its use of GitHub Codespaces, a cloud-based development environment, to host and distribute its payload. This method allows the attackers to leverage the legitimate infrastructure provided by GitHub, making it more challenging for security solutions to identify and block the malware. The Delta Stealer primarily spreads through phishing campaigns, where unsuspecting users are tricked into downloading and executing malicious files. These files may be disguised as legitimate software installers, documents, or other enticing content. Once executed, Delta Stealer starts its operation by establishing communication with command-and-control (C&C) servers, enabling the attackers to remotely control the infected machines and exfiltrate stolen data.

The malware is capable of stealing various types of sensitive information from infected systems. This includes web browser credentials, email credentials, FTP client credentials, instant messenger login data, cryptocurrency wallets, and other stored data. Delta Stealer achieves this by employing techniques such as keylogging, capturing screenshots, and scanning the system for relevant files and configurations.

**Threat Protected:** 01
**Rule Set Type:**

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

**Class Type:** Trojan-activity
**Kill Chain:** Initial Access T1566/T1078/T1190 - Execution T1059/T1569/T1106 - Persistence T1078/T1055/T1547 - Credential Access T1557/T1555 - Discovery T1087/T1040/T1135/T1518 - Command-and-Control T1001/T1573/T1071

## 2. CVE-2023-25717

The Ruckus Wireless Admin Remote Code Execution Attempt, identified by the CVE-2023-25717 vulnerability, is a security issue that poses a significant risk to the Ruckus Wireless Admin interface. This vulnerability allows remote attackers to execute arbitrary code on the affected system, potentially leading to unauthorized access, data breaches, and system compromise. Exploiting this vulnerability requires an attacker to send specially crafted requests to the vulnerable system, bypassing security measures and gaining control over the device. To mitigate the risk, it is crucial for organisations using Ruckus Wireless Admin to apply the necessary patches and updates provided by the vendor promptly.

**Threat Protected:** 01
**Rule Set Type:**

**Class Type:** Trojan- Activity
**Kill Chain:** Privilege Escalation TA0004 - Defence Evasion TA0005

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

## 3. AhRat Android Malware

A new, previously unidentified remote access trojan (RAT) has been noticed within an Android screen recording app, available for download on the Google Play Store and already gained more than thousands of installations. The 'iRecorder – Screen Recorder' app, initially introduced in 2021, was potentially compromised through a malicious update in 2022. The threat actor utilized its name to deceive users by requesting audio recording and file access permissions under the guise of a legitimate screen recording application. The RAT is based on an open-source Android RAT known as AhMyth.

**Threat Protected:** 01
**Rule Set Type:**

**Class Type:** Trojan- Activity
**Kill Chain:** Command-and-Control TA0011 - Defence Evasion TA0030 - Credential Access TA0031 - Discovery TA0032

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

## 4. Vultur

A new RAT, unlike others, has been observed to be active in the banking sector. Vultur is prone to using screen recording based on VNC to obtain all the PII (Personal Identifiable Information). After installation on the target, the dropper uses advanced evasion techniques, including steganography, file deletion and code obfuscation, in addition to multiple checks before downloading the malware. Once it has been downloaded the trojan gives a threat actor a clear view of everything that is happening on the compromised device.

**Threat Protected:** 01
**Rule Set Type:**

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

**Class Type:** Trojan
**Kill Chain:** Defence Evasion T1564 - Command-and-Control T1071 - Impact T1640

## Known exploited vulnerabilities (Week 4 May 2023):

| Vulnerability | Description |
|---|---|
| CVE-2023-32373 | Apple – WebKit Use-After-Free code execution vulnerability |
| CVE-2023-28204 | Apple – WebKit Out-of-Bounds Read vulnerability – Information disclosure |
| CVE-2023-32409 | Apple – WebKit Sandbox Escape Vulnerability |
| CVE-2023-2868 | Barracuda Networks – Input Validation vulnerability leading to code execution |

Updated Malware Signatures (Week 4 May 2023)

| Threat | Description |
|---|---|
| Ramnit | A banking trojan used to steal online banking credentials. |
| Qakbot | A malware designed to acquire valuable data such as banking credentials and is also capable of stealing FTP credentials and spreading across a network by utilizing SMB. |
| Tofsee | A malware that is used to send spam emails, and conduct click frauds as well as cryptomining. |
| Valyria | A Microsoft Word-based malware used as a dropper for second-stage malware. |
| Zeus | Also known as Zbot and is primarily designed to steal banking credentials. |
| njRAT | A remote access trojan typically that is spread using phishing emails or social engineering tactics. It allows a threat actor to steal sensitive |
| | information, install additional malware, and control the victim's machine remotely. |
| TeslaCrypt | A ransomware that started in the year 2015. It is usually distributed through spam email campaigns, malicious attachments, and exploit kits. |

## New Ransomware Victims Last Week: 141

Red Piranha proactively gathers information about organisations impacted by ransomware attacks through various channels, including the Dark Web. In the past week, our team identified a total of 141 new ransomware victims from 21 distinct industries across 32 countries worldwide. This highlights the global reach and indiscriminate nature of ransomware attacks, which can affect organisations of all sizes and sectors.

8base, a specific ransomware, has affected the largest number of new victims (62) spread across various countries. Lockbit3 and Royal groups follow closely with each hitting 21 and 10 new victims respectively. Below are the victim counts (%) for these ransomware groups and a few others.

| Name of Ransomware Group | Percentage of new Victims last week |
|---|---|
| 8base | 43.97% |
| Akira | 1.42% |
| Alphv | 5.67% |
| Bianlian | 2.13% |
| Blackbasta | 0.71% |
| Blackbyte | 0.71% |
| Cuba | 0.71% |
| Karakurt | 0.71% |
| Lockbit3 | 14.89% |
| Medusa | 4.26% |
| Play | 7.09% |
| Qilin | 2.84% |
| Royal | 7.09% |
| Snatch | 4.96% |
| Trigona | 2.13% |
| Vicesociety | 0.71% |

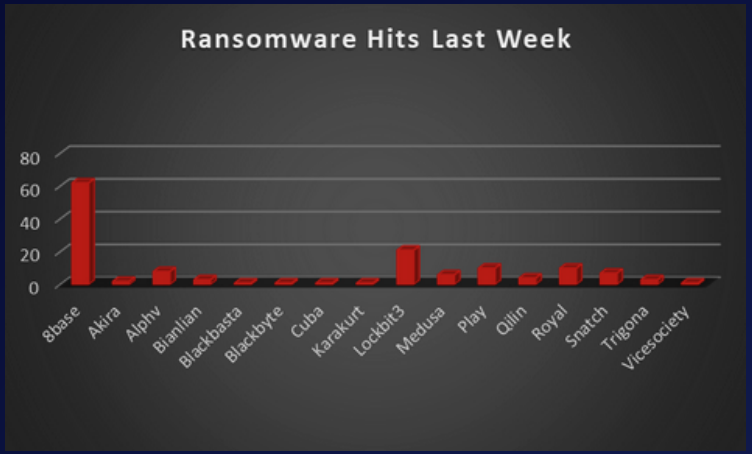



*Figure 1: Ransomware Group Hits Last Week*

When we examine the victims by country out of 32 countries around the world, we can conclude that the USA was once again the most ransomware-affected country, with a total of 69 new victims reported last week. The list below displays the number (%) of new ransomware victims per country.

| Name of the affected Country | Number of Victims |
|---|---|
| Argentina | 0.71% |
| Australia | 3.55% |
| Belgium | 1.42% |
| Brazil | 4.26% |
| Canada | 4.26% |
| Chile | 0.71% |
| China | 0.71% |
| Czech Republic | 0.71% |
| Denmark | 0.71% |
| Egypt | 0.71% |
| France | 1.42% |
| Germany | 5.67% |
| Guatemala | 0.71% |
| India | 3.55% |
| Indonesia | 0.71% |
| Italy | 1.42% |
| Jamaica | 0.71% |
| Mexico | 1.42% |
| New Zealand | 0.71% |
| Peru | 0.71% |
| Poland | 0.71% |
| Portugal | 0.71% |
| Singapore | 1.42% |
| South Africa | 1.42% |
| Spain | 2.13% |
| Sri Lanka | 0.71% |
| Taiwan | 0.71% |
| Trinidad | 1.42% |
| Turkey | 0.71% |
| UAE | 1.42% |
| UK | 4.96% |
| USA | 48.94% |

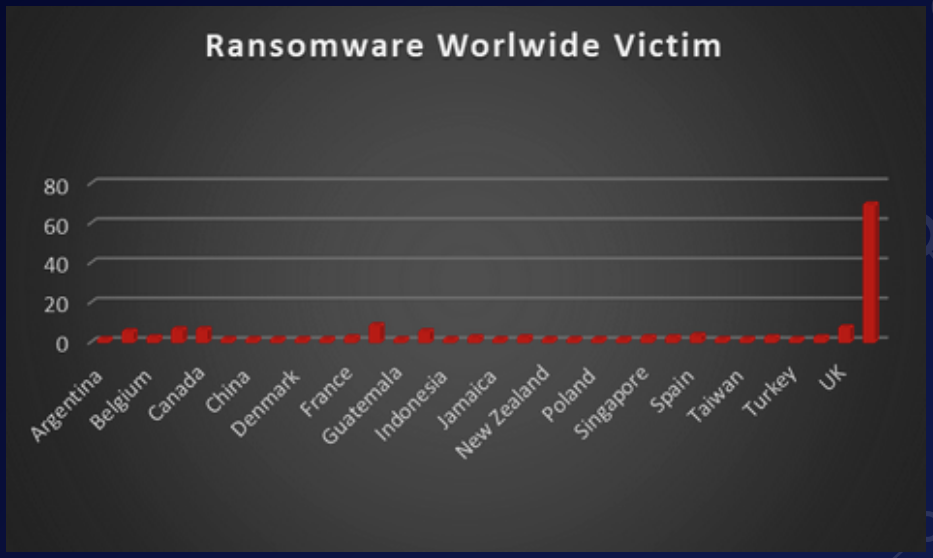



*Figure 2: Ransomware Victims Worldwide*

After conducting additional research, we found that ransomware has impacted 21 industries globally. Last week, the Manufacturing and Business Services sectors were hit particularly hard, with the loss of 25 and 23 businesses in each sector respectively. The table below presents the most recent ransomware victims sorted by industry.

| Industry | Victims Count (%) |
|---|---|
| Agriculture | 1.42% |
| Business Services | 16.31% |
| Construction | 7.80% |
| Consumer Services | 4.26% |
| Education | 5.67% |
| Energy | 0.71% |
| Finance | 4.96% |
| Government | 1.42% |
| Healthcare | 6.38% |
| Hospitality | 4.96% |
| Insurance | 2.13% |
| IT | 4.26% |
| Legal Services | 4.26% |
| Manufacturing | 17.73% |
| Media | 2.84% |
| Metals & Mining | 0.71% |
| Organisations | 1.42% |
| Real Estate | 2.13% |
| Retail | 6.38% |
| Telecommunication | 0.71% |
| Transport | 3.55% |

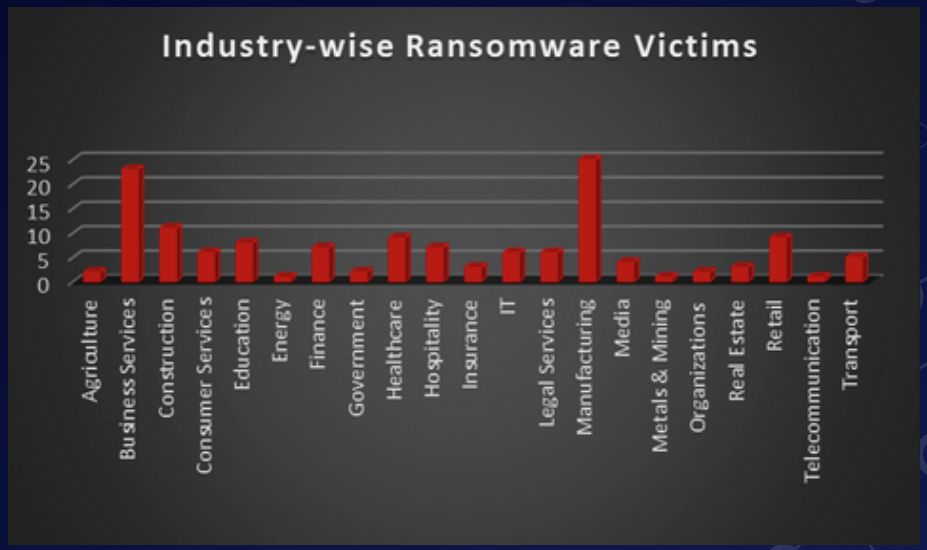



*Figure 3: Industry-wise Ransomware Victims*