Red Piranha
unified threat management

# THREAT INTELLIGENCE REPORT

May 09 - 15, 2023

# Report Summary:

- **New Threat Detection Added** – 4 (DarkWatchman RAT, Akira Ransomware, Snake Infostealer Malware, and DEV - 1028 BOTNET)
- **New Threat Protections**
- **Overall Weekly Observables Count**
- **Daily submissions by Observable Type**
- **New Ransomware Victims Last Week**

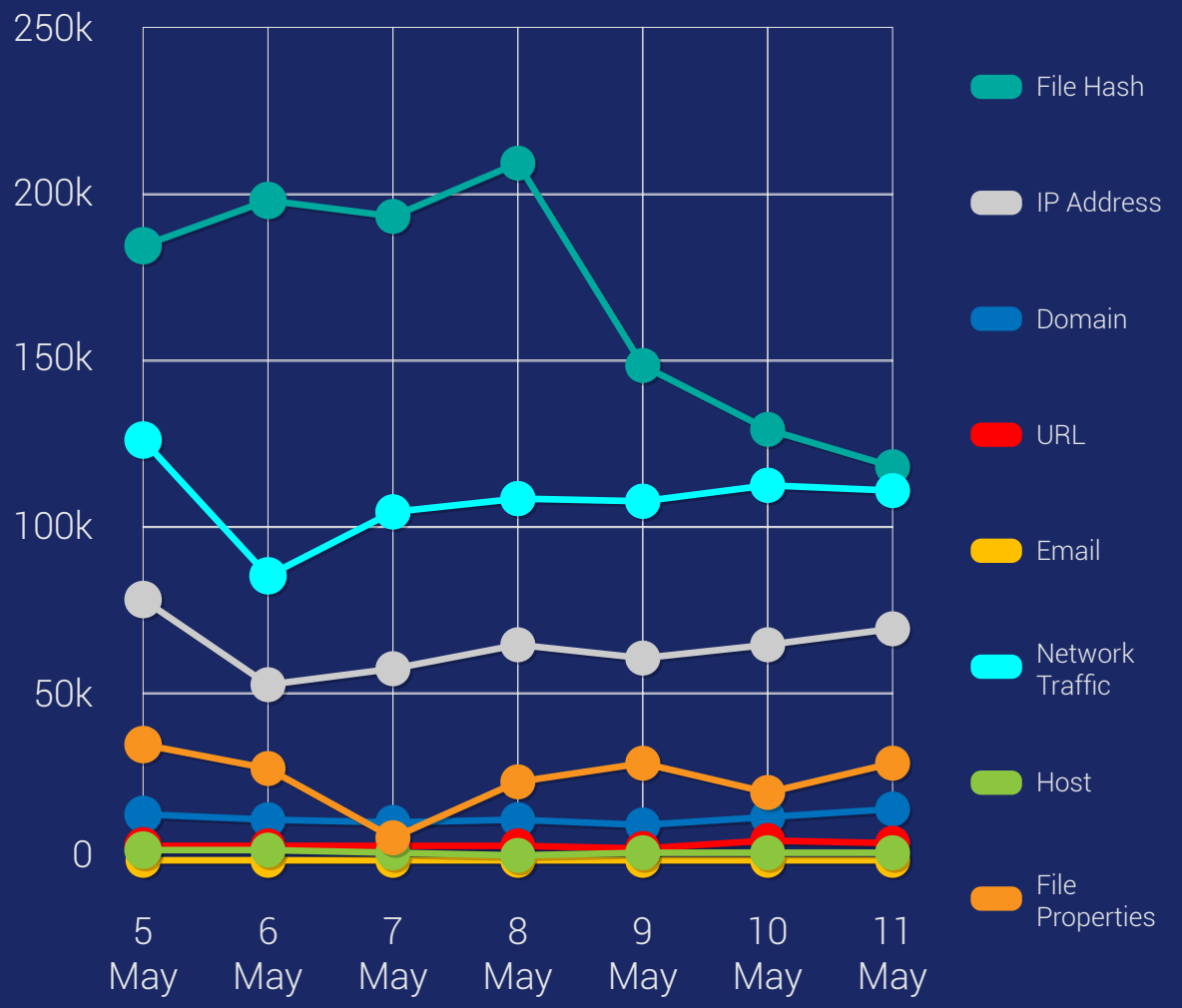
## New Threat Protections (Week Ending 15/05/2023):

**05**

## Overall Weekly Observables Count:

**2,718,844**

## Daily Submissions by Observable Type:



# Newly Detected Threats Added

## 1. DarkWatchman RAT

The DarkWatchman Remote Access Trojan (RAT) has recently been observed utilizing a novel phishing technique to propagate itself, underscoring the persistent innovation employed by threat actors to compromise systems. The growing frequency of DarkWatchman sightings in the wild suggests that this malware may become an increasingly prevalent feature of future cyberattacks.

Moreover, the use of the Windows Registry as a storage medium for fileless malware is a notable development, as it can effectively evade detection by traditional antivirus solutions that depend on file scanning. The keylogging functionality of DarkWatchman serves as a representative example of such fileless malware capable of bypassing detection measures.

**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 - Execution T1059/T1204/T1218/T1059 - Defence Evasion T1140/T1564 - Persistence T1053 - Discovery T1012/T1087/T1082 - Input Capture T1056.001 - Command-and-Control T1071

## 2. Akira Ransomware

A recently detected ransomware variant dubbed "Akira" is currently targeting multiple organisations and jeopardizing the confidentiality of their sensitive data. To increase the probability of receiving payment from the victims, the Akira ransomware uses a double-extortion tactic, which involves both exfiltrating and encrypting the data. The threat actors behind the ransomware then threaten to publicize or sell the stolen data on the dark web if the ransom is not paid to decrypt the data.

Akira ransomware was first observed in April 2023 and has already affected more than 15 publicly disclosed victims, with a majority of them located in the United States. The victims hail from diverse industries, including but not limited to BFSI, Construction, Education, Healthcare, and Manufacturing.

The Akira ransomware is a recently identified strain of ransomware that has been predominantly impacting organisations in the United States and Canada. This ransomware group is actively targeting businesses and demanding a substantial amount of money in exchange for the decryption keys.

As organisations ramp up their defences against ransomware attacks, there is a corresponding increase in the number of new ransomware groups emerging. These groups continually refine their strategies and expand their operations to maximize their profits.

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

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

**Class Type:** Trojan- Activity
**Kill Chain:** Execution T1204/T1047/T1059 - Defence Evasion T1497/T1027 - Discovery T1057/T1012/T1082/T1083 - Impact T1486/T1490

## 3. Snake Infostealer Malware

The Snake malware is an information-stealing malware that is implemented in the .NET programming language.  It is a feature-rich information-stealing malware that has keystroke logging as well as clipboard data, screenshot, and credential theft capabilities. Snake can steal credentials from over 50 applications, which include File Transfer Protocol (FTP) clients, email clients, communication platforms, and web browsers. Snake can exfiltrate stolen data through a variety of protocols, such as FTP, Simple Mail Transfer Protocol (SMTP), and Telegram.

**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:** Malware
**Kill Chain:** Execution TA0002 - Persistence TA0003 - Privilege Escalation TA0004 - Defence Evasion TA0005 - Credential Access TA0006 - Discovery TA0007 - Collection TA0009 - Command-and-Control TA0011

## 4. DEV - 1028 BOTNET

A new cross-platform botnet has been found originating from malicious software downloads on Windows devices and succeeds in infecting Linux-based devices like Minecraft servers. The botnet spreads by enumerating default credentials on internet-exposed Secure Shell (SSH)-enabled devices. IoT devices with remote configuration enabled and configured with potentially insecure settings are at risk of attacks like this botnet. The botnet's spreading mechanism makes it uniquely interesting. While the malware can be removed from the infected source PC, it could persist on unmanaged IoT devices in the network and continue to operate as part of the botnet.

**Threat Protected:** 02
**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:** Malware
**Kill Chain:** Execution TA0002 - Privilege Escalation TA0004 - Defence Evasion TA0005 - Discovery TA0007 - Command-and-Control TA0011

## Known exploited vulnerabilities (Week 2 May 2023):

| Vulnerability | Description |
|---|---|
| CVE-2023-29336 | Microsoft Win32K Privilege Escalation Vulnerability |
| CVE-2016-8735 | Apache Tomcat Remote Code Execution Vulnerability |
| CVE-2016-3427 | Oracle Java SE and JRockit Unspecified Vulnerability |
| CVE-2015-5317 | Jenkins User Interface (UI) Information Disclosure Vulnerability |
| CVE-2010-3904 | Linux Kernel Improper Input Validation Vulnerability |
| CVE-2014-0196 | Linux Kernel Race Condition Vulnerability |
| CVE-2021-3560 | Red Hat Polkit Incorrect Authorization Vulnerability |
| CVE-2023-25717 | Multiple Ruckus Wireless Products CSRF and RCE Vulnerability |

Updated Malware Signatures (Week 2 May 2023)

| Threat | Description |
|---|---|
| Kuluoz | A backdoor for a botnet. It executes commands from a remote malicious user. |
| Upatre | Upatre is also a malware dropper that downloads additional malware on an infected machine. It is usually observed to drop banking trojan after the initial infection. |
| Glupteba | A malware dropper that is designed to download additional malware on an infected machine. |

## New Ransomware Victims Last Week: 86

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 86 new ransomware victims from 19 distinct industries across 18 countries worldwide. This highlights the global reach and indiscriminate nature of ransomware attacks, which can affect organisations of all sizes and sectors.

Akira, a specific ransomware, has affected the largest number of new victims (19) spread across various countries. Lockbit3 and Bianlian groups follow closely with each hitting 18 and 16 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 |
|---|---|
| Abyss-data | 3.49% |
| Akira | 22.09% |
| Alphv | 9.30% |
| Avoslocker | 1.16% |
| Bianlian | 18.60% |
| Blackbyte | 1.16% |
| Cuba | 1.16% |
| Karakurt | 1.16% |
| Lockbit3 | 20.93% |
| Medusa | 2.33% |
| Monti | 3.49% |
| Play | 3.49% |
| Ra group | 6.98% |
| Royal | 1.16% |
| Trigona | 2.33% |
| Vicesociety | 1.16% |

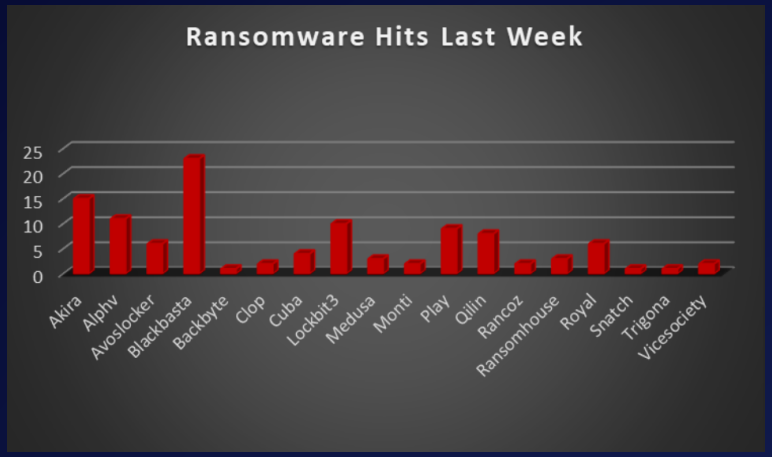



*Figure 1: Ransomware Group Hits Last Week*

When we examine the victims by country out of 18 countries around the world, we can conclude that the USA was once again the most ransomware-affected country, with a total of 51 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 |
|---|---|
| Austria | 1.16% |
| Brazil | 2.33% |
| Canada | 8.14% |
| Chile | 2.33% |
| Germany | 4.65% |
| India | 1.16% |
| Italy | 2.33% |
| Korea | 2.33% |
| Libya | 1.16% |
| Mexico | 1.16% |
| Namibia | 1.16% |
| Poland | 1.16% |
| Slovakia | 1.16% |
| South Africa | 1.16% |
| Switzerland | 1.16% |
| UK | 6.98% |
| USA | 59.30% |
| Viet Nam | 1.16% |

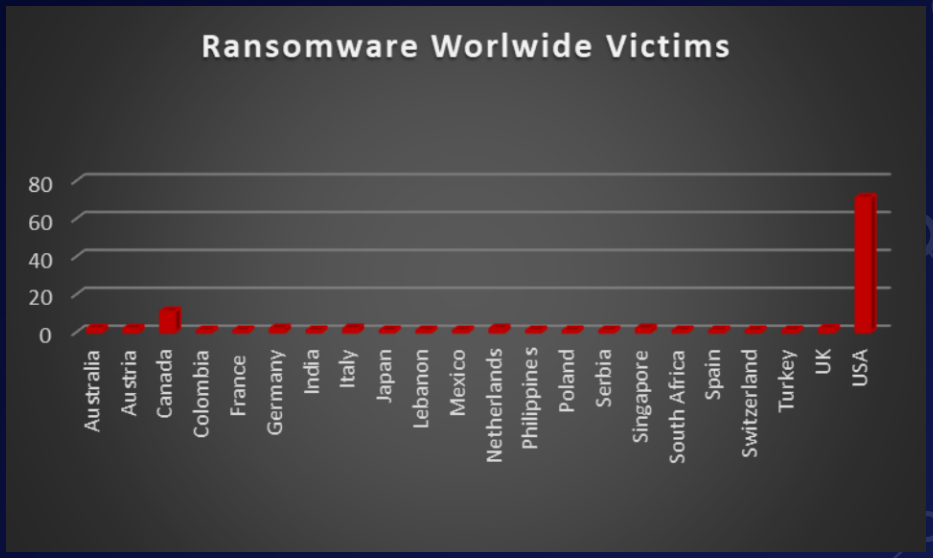



*Figure 2: Ransomware Victims Worldwide*

After conducting additional research, we found that ransomware has impacted 19 industries globally. Last week, the manufacturing and Education sectors were hit particularly hard, with the loss of 10 businesses in each sector respectively. The table below presents the most recent ransomware victims sorted by industry.

| Industry | Victims Count (%) |
|---|---|
| Agriculture | 1.16% |
| Business Services | 9.30% |
| Construction | 8.14% |
| Consumer Services | 2.33% |
| Education | 11.63% |
| Energy | 1.16% |
| Finance | 5.81% |
| Health care | 5.81% |
| Hospitality | 2.33% |
| Insurance | 3.49% |
| IT | 6.98% |
| Legal Services | 4.65% |
| Manufacturing | 11.63% |
| Metals & Mining | 1.16% |
| Organisations | 2.33% |
| Real Estate | 4.65% |
| Retail | 10.47% |
| Telecommunication | 3.49% |
| Transportation | 3.49% |

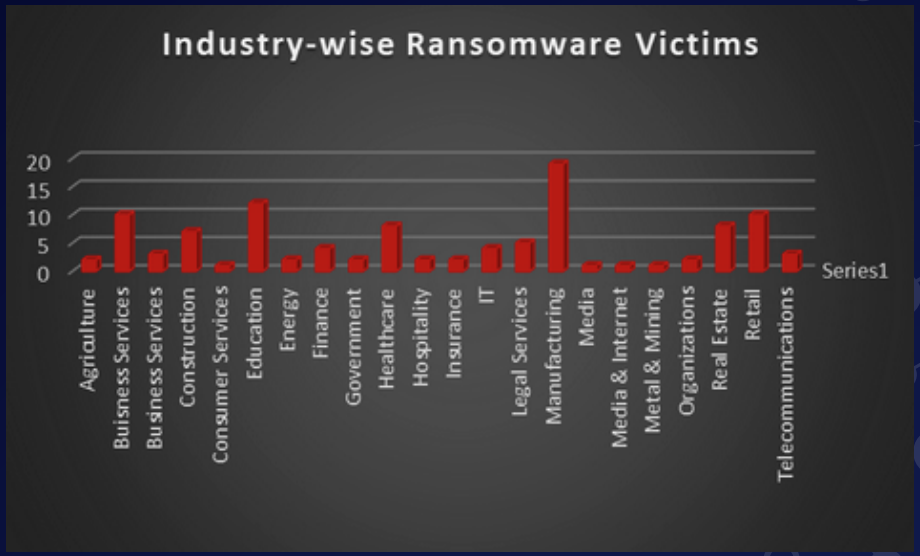



*Figure 3: Industry-wise Ransomware Victims*