Red Piranha
unified threat management

# THREAT INTELLIGENCE REPORT

Mar 07 - 13, 2023

# Report Summary:

- **New Threat Detection Added** – 6 (ImBetter Stealer, SYS01 Stealer, Parallax RAT, Hiatus, Blind Eagle, and MQsTTang Backdoor)
- **New Threat Protections**
- **Overall Weekly Observables Count**
- **Daily submissions by Observable Type**
- **New Ransomware Victims Last Week**

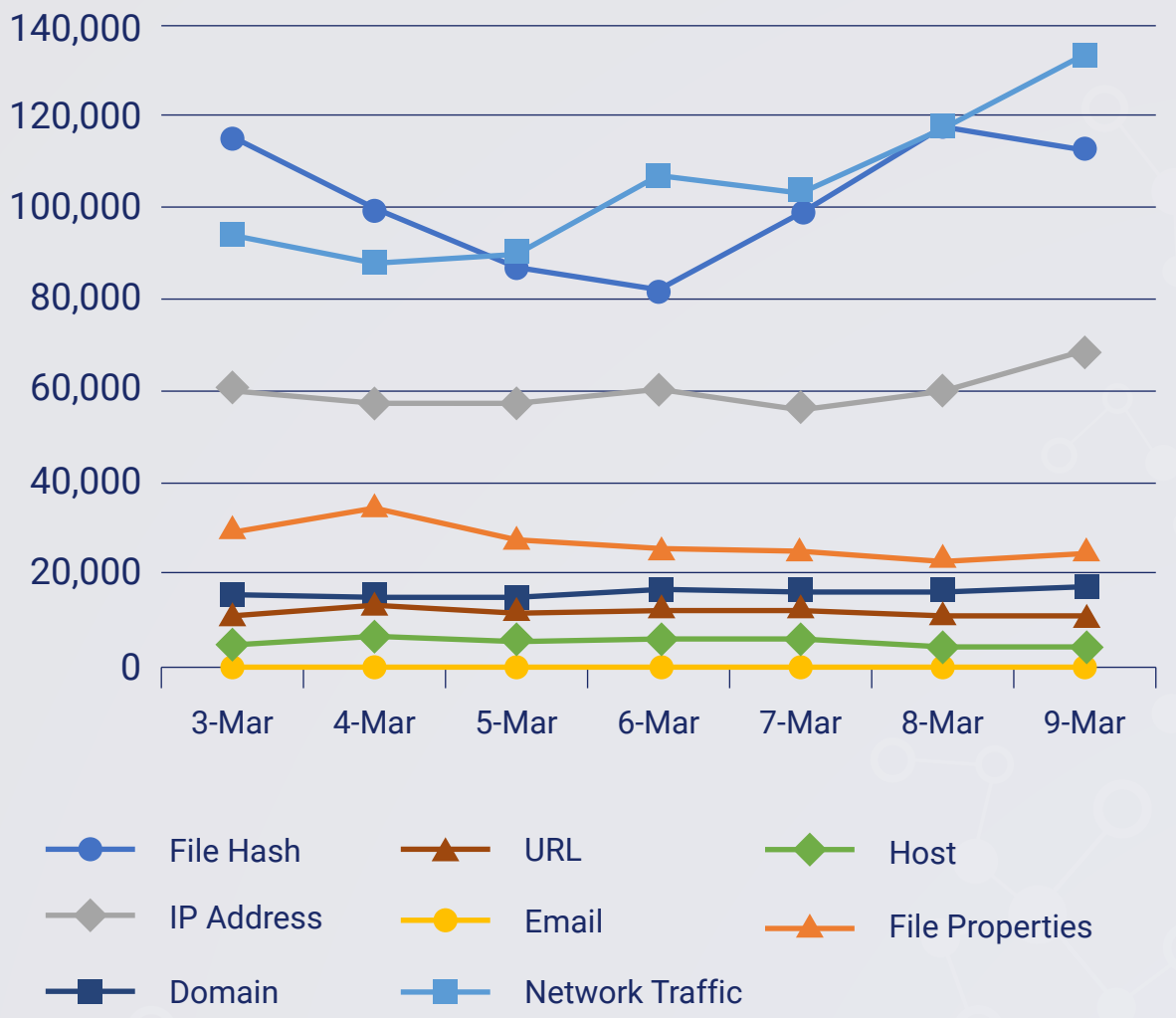
## New Threat Protections (Week Ending 13/03/2023):

**9**

## Overall Weekly Observables Count:

**2,246,821**

## Daily Submissions by Observable Type:



# Newly Detected Threats Added

## 1. ImBetter Stealer

ImBetter Stealer is a type of malware created specifically to extract confidential information from computer systems and internet browsers. This information includes sensitive data like Login credentials, Cookies, User profiles, and Wallet extensions. The use of this malware can be particularly risky as it can allow cybercriminals to gain unauthorized access to victims' online accounts and crypto wallets, leading to the loss of valuable digital assets or personal information.

**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-activity
**Kill Chain:** Execution T1204 - Defence Evasion T1027 - Credential Access T1528 -Discovery T1010/T1083 - Collection T1005 - Command-and-Control T1071

## 2. SYS01 Stealer

SYS01 Stealer has been observed targeting critical government infrastructure employees, manufacturing companies, and other industries. The attackers behind this campaign are focusing on Facebook business accounts, utilizing Google ads and fake Facebook profiles to promote content such as games, adult material, and pirated software. These tactics are aimed at enticing victims to download a malicious file. Once downloaded, the malware is designed to steal sensitive information, including login credentials, cookies, as well as Facebook ad and business account data.

**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 T1059/T1064 - Execution T1059/T1059 - Privilege Escalation T1055/T1134 -Defence Evasion T1036/T1055 - Discovery T1033/T1083 - Impact T1496/T1529

## 3. Parallax RAT

ParallaxRAT is a malware known to be distributed through spam and phishing emails. Like any other remote access trojan, it is capable of stealing credentials, keylogging, and completely taking over a victim's computer. It has been observed lately that this malware is being used to target cryptocurrency organisations.

**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:** Trojan- Activity
**Kill Chain:** Initial Access T1566 - Execution T1059 - Persistence T1037 - Command-and-Control T1102

## 4. Hiatus

Hiatus is a remote access trojan targeting routers and network devices. It targets enterprise routers and where it deploys its malicious binaries. Once a device is infected, the threat actor converts the device into a proxy. It also monitors traffic on ports that are associated with email and file transfer.

**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-Activity
**Kill Chain:** Initial Access T1190 - Execution T1059 - Defence Evasion T1205 - Command-and-Control T1090/T1205

## 5. Blind Eagle

Blind Eagle, also known as APT-C-36 has recently been observed using an advanced toolset comprising Meterpreter payloads that are being delivered by spear phishing attachments. The emails generally include a URL redirecting to a PDF file which in turn deploys malware on the targeted system, effectively launching the infection chain. A malicious RAT is installed on the targeted machine, enabling the threat actor to access and run commands on the said machine at any point in time they desire to do so.

**Threat Protected:** 03
**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:** Backdoor
**Kill Chain:** Initial Access T1566.001 - Execution T1204.001, T1204.002, T1059.005, T1059.001, T1059.003 - Persistence T1053.005, T1547.001 - Defence Evasion T1218.009

## 6. MQsTTang Backdoor

MQsTTang is a barebones backdoor that allows the attacker to execute arbitrary commands on a victim's machine and get the output. Even so, it does present some interesting characteristics. Chief among these is its use of the MQTT protocol for C&C communication. MQTT is typically used for communication between IoT devices and controllers, and the protocol hasn't been used in many publicly documented malware families.

**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:** Backdoor
**Kill Chain:** Resource Development T1583.003/T1583.004/T1587.001/T1588.002/T1608.001/T1608.002 - Initial Access T1566.002 - Execution T1106/T1204.002 - Defence Evasion T1036.004 - Command-and-Control T1071/T1102.002/T1132.001/T1573.001 - Exfiltration T1041

## New Ransomware Victims Last Week: 71

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 71 new ransomware victims from 19 distinct industries across 26 countries worldwide. This highlights the global reach and indiscriminate nature of ransomware attacks, which can affect organisations of all sizes and sectors.

Royal, a specific ransomware, has affected the largest number of new victims (17) spread across various countries. LockBit 3.0 and AlphV groups follow closely with each hitting 13 and 11 new victims respectively. Below are the victim counts in per cent for these ransomware groups and a few others.

| Name of Ransomware Group | Percentage of new Victims last week |
|---|---|
| AlphV | 15.49% |
| Blackbyte | 2.82% |
| Clop | 9.86% |
| Dark Power | 14.08% |
| LockBit 3.0 | 18.31% |
| Mallox | 4.23% |
| Medusa | 5.63% |
| Monti | 1.41% |
| Royal | 23.94% |
| Vicesociety | 4.23% |

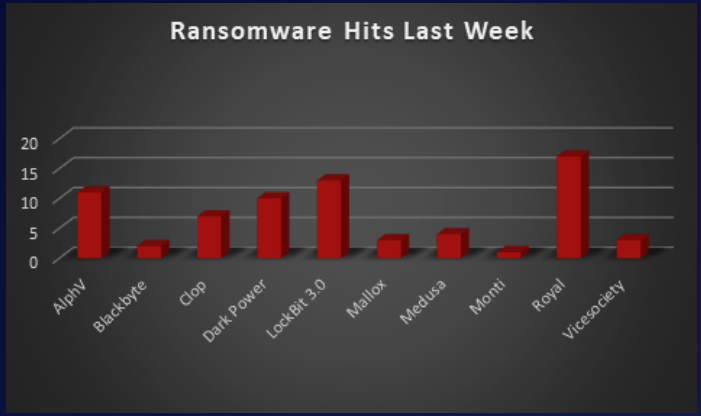



*Figure 1: Ransomware Group Hits Last Week*

When we examine the victims by country out of 26 countries around the world, we can conclude that the USA was once again the most ransomware-affected country, with a total of 32 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 |
|---|---|
| Algeria | 1.41% |
| Argentina | 1.41% |
| Australia | 4.23% |
| Brighton | 1.41% |
| Canada | 5.63% |
| Czech Republic | 1.41% |
| Denmark | 1.41% |
| Egypt | 1.41% |
| France | 2.82% |
| Germany | 5.63% |
| Hungary | 1.41% |
| India | 4.23% |
| Indonesia | 1.41% |
| Israel | 1.41% |
| Lima | 1.41% |
| Luxembourg | 1.41% |
| Pakistan | 1.41% |
| Poland | 1.41% |
| Puerto Rico | 1.41% |
| Singapore | 1.41% |
| Spain | 2.82% |
| Turkey | 2.82% |
| UAE | 2.82% |
| UK | 1.41% |
| USA | 45.07% |
| Venezuela | 1.41% |

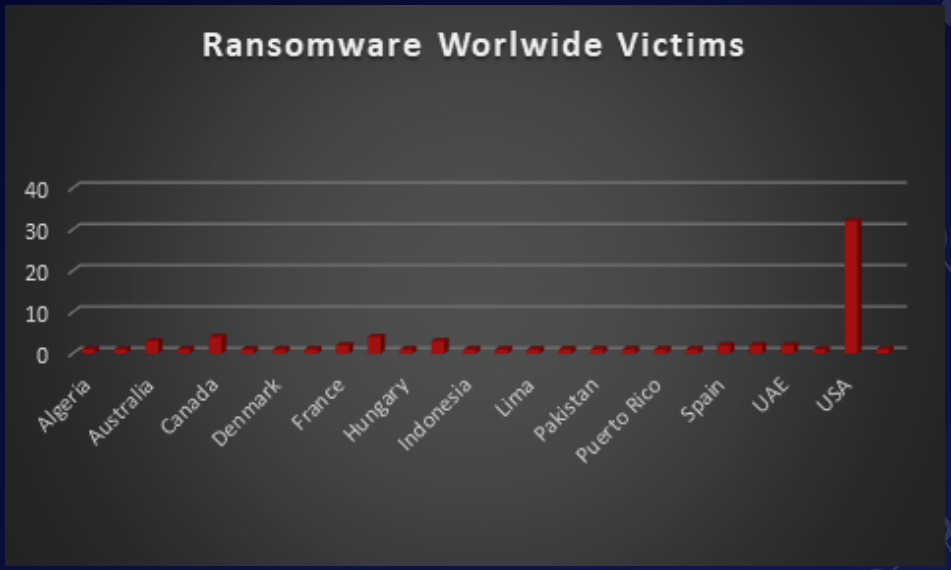



*Figure 2: Ransomware Victims Worldwide*

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

| Industry | Victims Count (%) |
|---|---|
| Business Services | 9.76% |
| Construction | 9.76% |
| Education | 4.88% |
| Electricity, Oil & Gas | 2.44% |
| Finance | 4.88% |
| Government | 4.88% |
| Hospitality | 7.32% |
| IT | 7.32% |
| legal Services | 4.88% |
| Manufacturing | 21.95% |
| Organisations | 4.88% |
| Retail | 9.76% |
| Transportation | 7.32% |

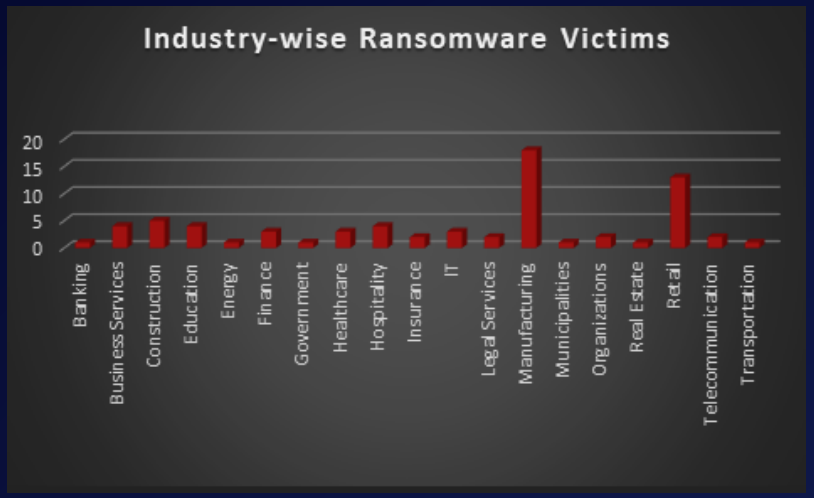



*Figure 3: Industry-wise Ransomware Victims*