Red Piranha
unified threat management

THREAT INTELLIGENCE REPORT

Mar 21 - 27, 2023

Report Summary:

- **New Threat Detection Added** – 6 (Royal Ransomware, Bad magic APT, Xaview Stealer Malware, SOMNIRECORD, Muggle Stealer, and FakeGPT)
- **New Threat Protections**
- **Overall Weekly Observables Count**
- **Daily submissions by Observable Type**
- **New Ransomware Victims Last Week**

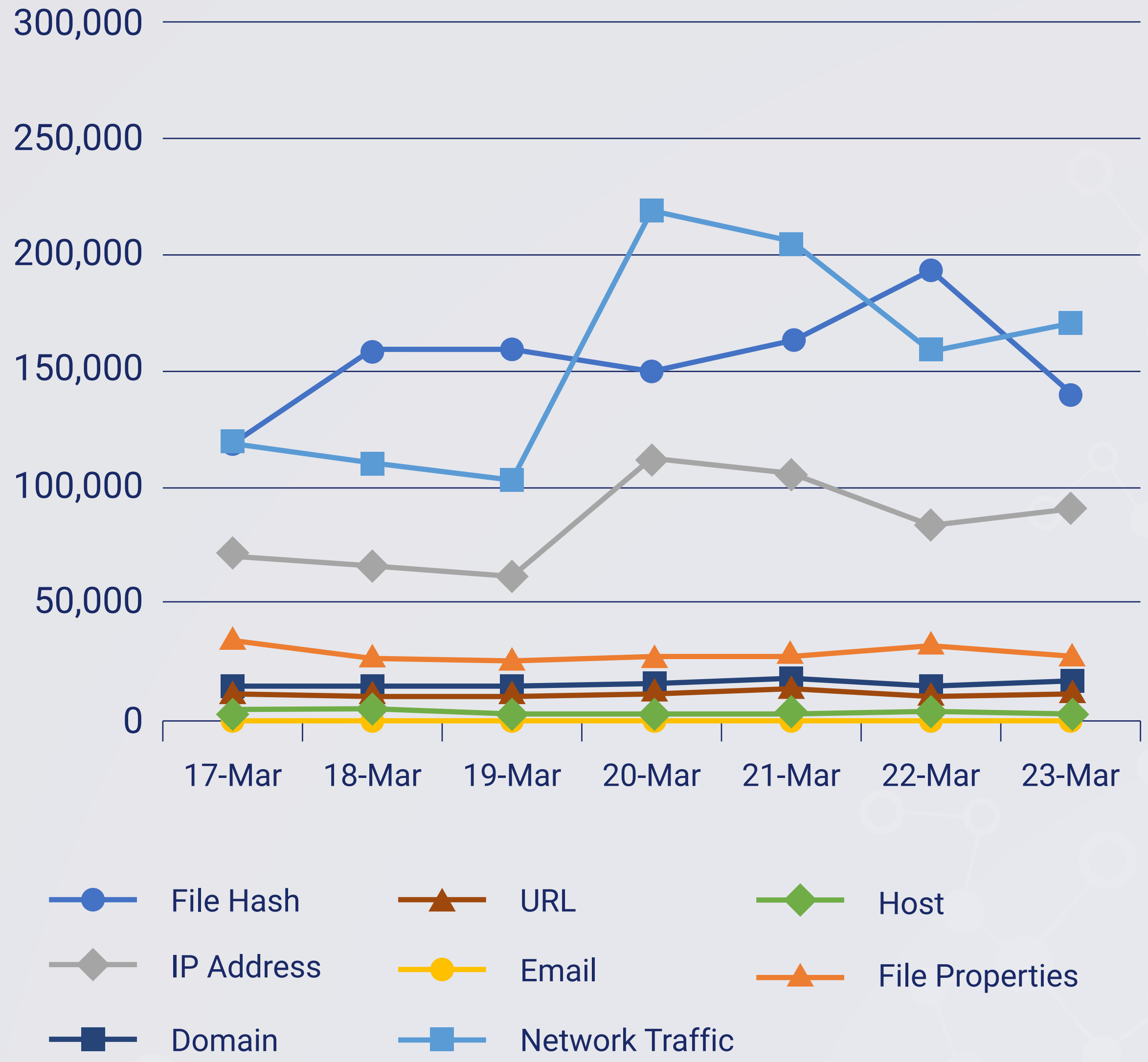
New Threat Protections (Week Ending 27/03/2023):

14

Overall Weekly Observables Count:

3,170,268

Daily Submissions by Observable Type:



Newly Detected Threats Added

1. Royal Ransomware

Royal Ransomware has been observed approaching its victims through phishing campaigns and using common threat loaders such as BATLOADER and Qbot. The threat loader then downloads a Cobalt Strike payload to continue the malicious operation within the infected environment. Other ransomware operations like Qbot and BlackBasta have been noted using the same technique. The ransomware has been gaining momentum in its no of victims beating some of the top ransomware groups.

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: Discovery TA0005/TA0007 - Impact TA0040 - Execution TA0002

2. Bad magic APT

A sophisticated advanced persistent threat (APT) group has been active since at least, 2016 and has targeted multiple organisations in various countries. The group, which the researchers refer to as "Bad magic," uses a variety of tactics and techniques, including spear-phishing emails, custom malware, and strategic web compromises, to gain access to their targets' networks and exfiltrate sensitive data.

According to the researchers, Bad magic has a particular interest in telecommunications, financial services, and government organisations, and they suspect that the group may be state-sponsored. The group's malware is highly sophisticated and its advanced evasion techniques and anti-analysis measures avoid detection. The researchers also note that Bad magic is highly skilled and adaptable, constantly evolving its tactics and techniques in response to new security measures.

Threat Protected: 02
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: Initial Access T1091 - Execution T1047/T1053/T1059/T1064 -Persistence T1053 - Privilege Escalation T1053/T1055 - Defence Evasion T1036/T1055 - Discovery T1010/T1018/T1083 - Lateral Movement T1091

3. Xaview Stealer Malware

Xaview Stealer is a type of malware that is designed to steal sensitive information from an infected device. This malware is a type of Trojan, which means that it disguises itself as a legitimate file or application to deceive users into downloading and installing it. Once Xaview Stealer is installed on a device, it starts to collect a wide range of information, including browser history, cookies, usernames and passwords, credit card information, and more. This information is then sent back to the attacker's server, where it can be used for malicious purposes such as identity theft or financial fraud. One of the main ways that Xaview Stealer is distributed is through spam email campaigns. These emails often contain malicious attachments or links that, when clicked on, download, and install the malware onto the victim's 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- Activity
Kill Chain: Initial Access T1476 - Initial AccessT1444 - Discovery T1418 - Impact T1516

4. SOMNIRECORD

SOMNIRECORD is a malware written in C++. It acts as a backdoor and masquerades its traffic as DNS as a form of evasion. It makes a DNS query to retrieve its commands from a hardcoded domain in the binary. Its commands allow the attacker to execute any software from the victim machine, list processes, and deploy a webshell.

Threat Protected: 04
Rule Set Type:

Class Type: Trojan-Activity
Kill Chain: Execution T1059 - Defence Evasion T1036

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

5. Muggle Stealer

Muggle Stealer is a malware that collects Windows and browser passwords, collects information, and takes screenshots of victim machines. The collected data is then uploaded to a Chinese IP. There is not enough data yet on how this stealer is commonly distributed and is not currently attributed to any threat actor.

Rules have been deployed on Crystal Eye devices that will detect and prevent this traffic.

Threat Protected: 04
Rule Set Type:

Class Type: Trojan-Activity
Kill Chain: Execution T1059 - Collection T1005/T1113/T1056 - Command-and-Control T1102

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

6. FakeGPT

It has been observed that the fake ChatGPT Chrome extension is being used as Facebook Ads account stealer. The malicious extension named Chat GPT for Google intends to steal Facebook session cookies and compromise accounts at go. The cookies are, subsequently, sent to the attackers' server via a GET request. The cookie list is AES-encrypted and attached to the X-Cached-Key HTTP header value. This ensures that the cookies could be pilfered without any deep packet inspection mechanisms raising alarms.

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 T1189 - Resource Development T1583/ T1586 - Lateral Movement T1550 - Command-and-Control T1102

New Ransomware Victims Last Week: 188

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 188 new ransomware victims from 26 distinct industries across 34 countries worldwide. This highlights the global reach and indiscriminate nature of ransomware attacks, which can affect organisations of all sizes and sectors.

Clop, a specific ransomware, has affected the largest number of new victims (105) spread across various countries. LockBit 3.0 and AlphV groups follow closely with each hitting 27 and 15 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	2.65
Alphv	7.97
Avoslocker	2.65
Blackbasta	2.12
Blackbyte	0.53
Clop	55.85
Everest	0.53
Karakurt	0.53
Lockbit3	14.36
Medusa	2.12
Monti	2.12
Play	3.72
Ransomhous	0.53
Ransomhouse	1.06
royal	2.65
vicesociety	0.53

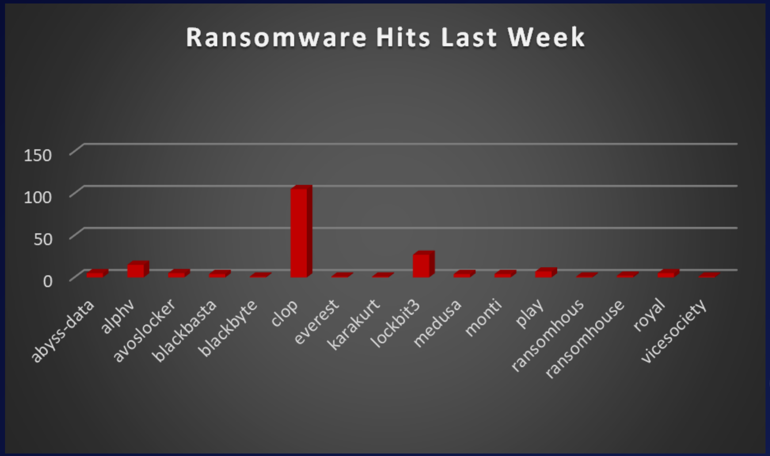


Figure 1: Ransomware Group Hits Last Week

When we examine the victims by country out of 34 countries around the world, we can conclude that the USA was once again the most ransomware-affected country, with a total of 108 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
Kuwait	0.53
Argentina	1.59
Australia	1.06
Austria	1.06
Bavaria	0.53
Canada	1.06
Chile	0.53
Czech Republic	0.53
Denmark	0.53
France	4.25
Germany	1.06
India	3.72
Indonesia	0.53
Italy	1.06
Japan	1.06
Mexico	0.53
New Zealand	0.53
Norway	0.53
Panama	0.53
Philippines	0.53
Pakistan	0.53
Poland	0.53
Puerto Rico	1.06
Saudi Arabia	1.06
Singapore	0.53
South Africa	3.19
Switzerland	1.06
Taiwan	0.53
Thailand	1.06
Turkey	1.06
UAE	1.06
UK	7.97
USA	57.44

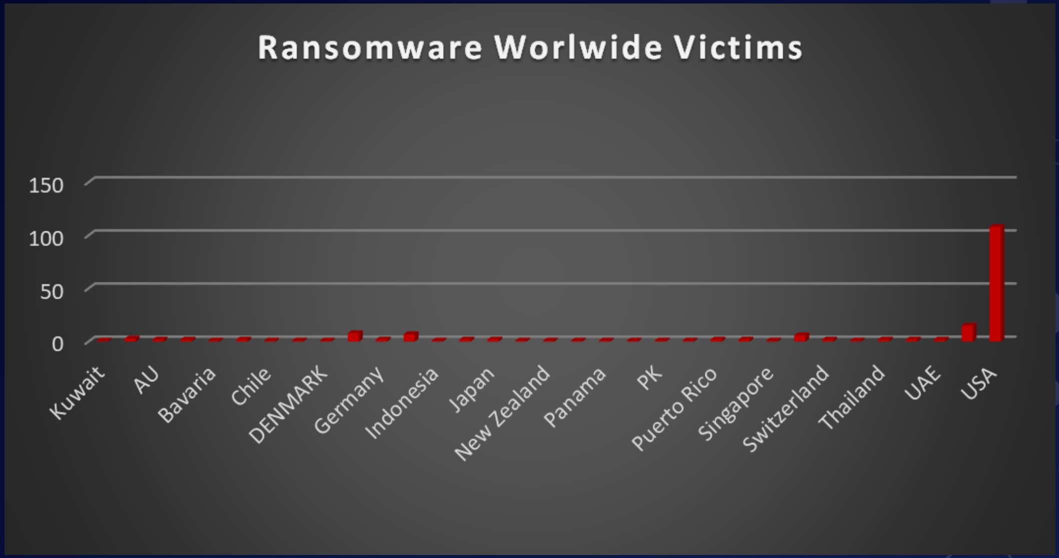


Figure 2: Ransomware Victims Worldwide

After conducting additional research, we found that ransomware has impacted 26 industries globally. Last week, the manufacturing and Business Services sectors were hit particularly hard, with the loss of 27 and 26 businesses in each sector, respectively. The table below presents the most recent ransomware victims sorted by industry.

Industry	Victims Count (%)
Architecture, Engineering & Design	0.53
Business Services	13.83
Construction	7.45
Consumer Services	2.66
Education	2.13
Electricity, Oil & Gas	0.53
Energy, Utilities & Waste Treatment	2.13
Finance	2.66
Government	4.26
Healthcare	3.19
Hospitality	2.13
Insurance	3.72
IT	7.98
Legal Services	3.72
Manufacturing	14.36
Media & Internet	2.66
Membership Organisations	0.53
Metals & Mining	1.06
Municipalities	1.06
Oil & energy	0.53
Organisations	1.60
Real Estate	2.66
Retail	5.85
Telecommunications	3.72
Transportation	8.51
Turkey	0.53

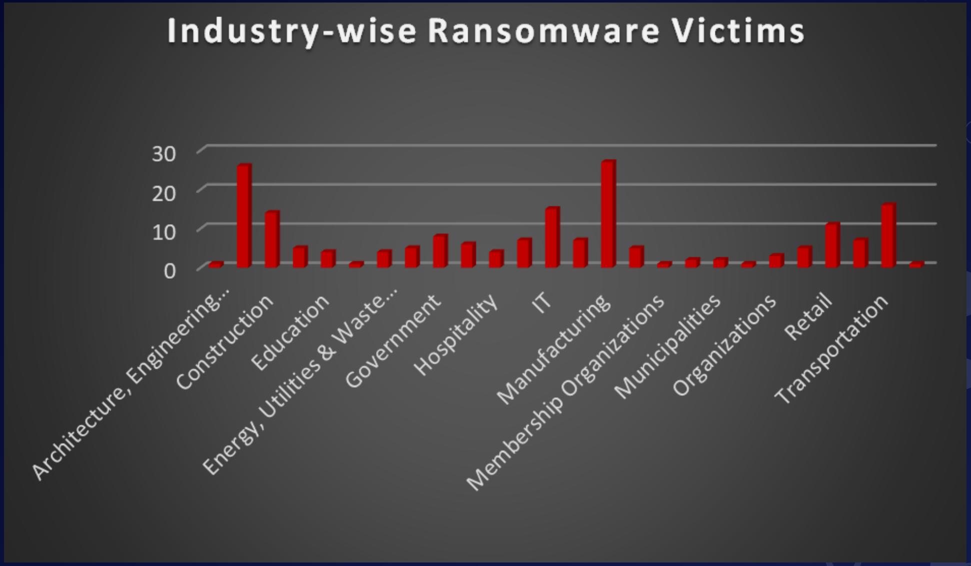


Figure 3: Industry-wise Ransomware Victims