Red Piranha
unified threat management

THREAT INTELLIGENCE REPORT

Feb 28 - Mar 06, 2023

Report Summary:

- **New Threat Detection Added** – 6 (ReverseRAT 3.0, R3NIN Sniffer Toolkit, WhiteSnake Stealer, 8220 Gang, S1deload Stealer, and Chaos RAT)
- **New Threat Protections**
- **Overall Weekly Observables Count**
- **Daily submissions by Observable Type**
- **New Ransomware Victims Last Week**

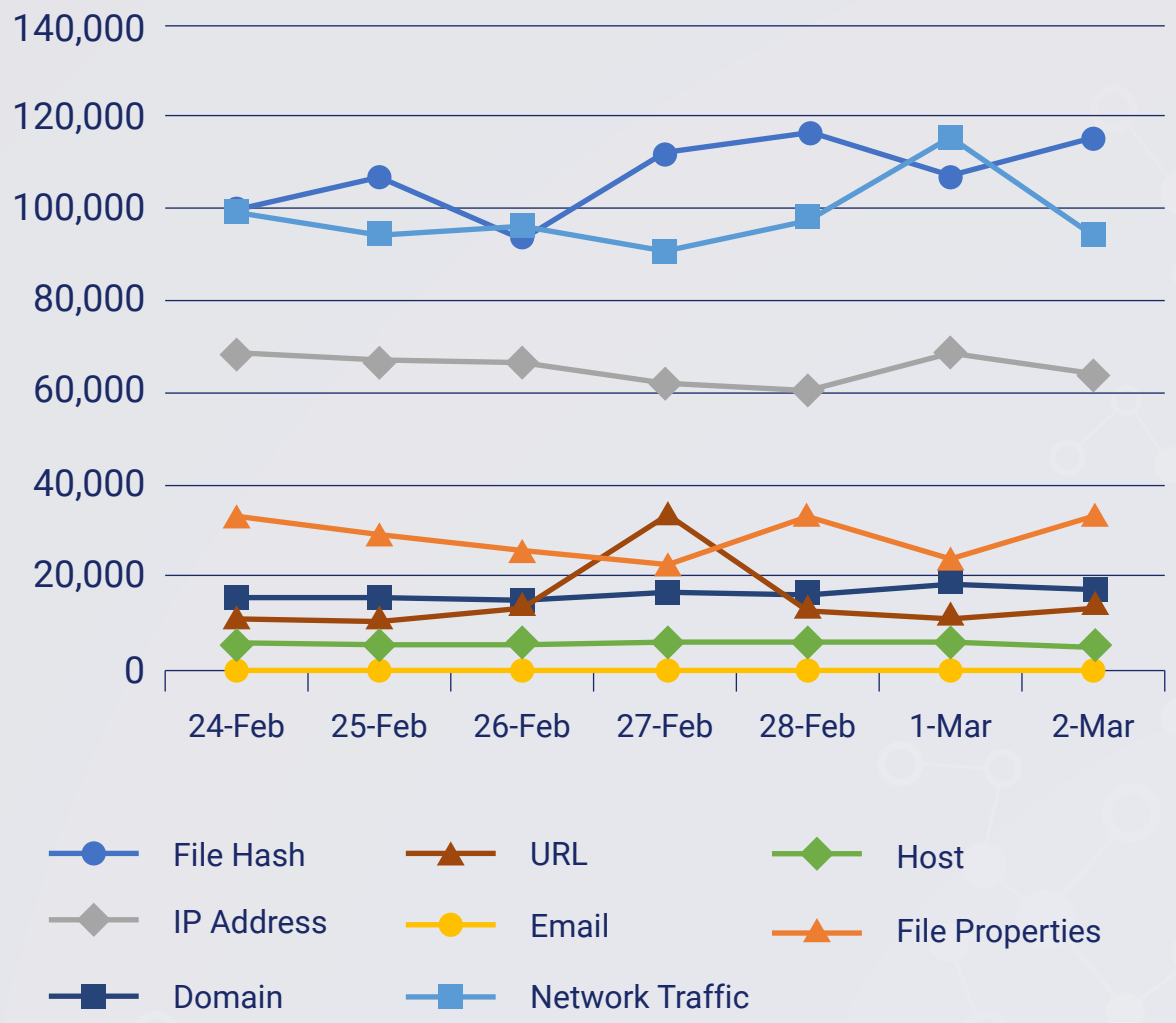
New Threat Protections (Week Ending 06/03/2023):

19

Overall Weekly Observables Count:

2,344,609

Daily Submissions by Observable Type:



Newly Detected Threats Added

1. ReverseRAT 3.0

An updated version of a backdoor called ReverseRAT has been observed targeting Indian government entities through spear phishing campaigns. The file masquerades as a fake advisory from India's Ministry of Communications about "Android Threats and Preventions." Once ReverseRAT gains persistence, it enumerates the victim's device, collects data, encrypts it using RC4, and sends it to the command-and-control (C&C) server. Some of its functions include taking screenshots, downloading and executing files, and uploading files to the C2 server.

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 - Persistence T1547 - Collection T1115 - Defence Evasion T1112 - Discovery T1057

2. R3NIN Sniffer Toolkit

The R3NIN Sniffer is a toolkit and panel that can be readily used to extract payment card data from e-commerce websites that have been compromised. This sniffer toolkit boasts several notable features, such as the ability to generate custom JavaScript codes for injection, the capability to exfiltrate compromised payment card data across different browsers, data management and analysis functions, BIN checks, and statistics generation.

On January 15, version 1.2 was released, which included features to fully obfuscate malicious scripts and conceal the URLs of the Command-and-Control (C&C) server. Another update was announced on January 26 that would add a keylogger to the sniffer module, enabling it to log input from multiple fields such as 'inputs,' 'selects,' and 'textareas' in a compromised website. On January 30, support for inline frames (iFrames) was added to the existing sniffer module.

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 T1064 - Defence Evasion T1027 - Credential Access T1003 - Discovery T1083 - Collection T1005 - Command-and-Control T1071/T1105

3. WhiteSnake Stealer

WhiteSnake Stealer is a relatively new type of Infostealer that has emerged in the cybercrime market. While there are already established and widely-used InfoStealers available, threat actors prefer to use new toolkits to stay ahead of antivirus detection and update their tactics, techniques, and procedures. In this particular instance, WhiteSnake Stealer has extended its reach by developing a Linux-based malware version alongside its Windows version. This strategic move enables it to target a broader range of users and potentially evade detection by security measures that may be more commonly deployed on Windows-based systems.

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 T1497 - Credential Access T1528 - Discovery T1010/T1518- Collection T1005 - Command-and-Control T1573

4. 8220 Gang

8220 Gang is a threat group known for attacking public cloud users with misconfigured applications and services. Their most prevalent attack technique is brute forcing accounts on these cloud servers. Once they have gained the initial foothold, they try and spread to other servers and infect them with miners.

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: Trojan-Activity
Kill Chain: Initial Access T1190/T1078 - Execution T1059 - Command-and-Control T1102

5. S1deload Stealer

S1deload Stealer is a malware which gathers user credentials on victim machines and uses the machines for cryptojacking and social media spamming. The initial distribution of this malware is through social engineering attacks where victims are encouraged to download an archive of photos. Upon execution, the malware starts sideloading its components as the legitimate process for defence evasion. It establishes a connection to its Command-and-Control server where the gathered credentials are imported. The threat actor then uses the social media accounts to sell boosting services for YouTube, Facebook, and other known social media platform.

Threat Protected: 10
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/T1106 - Defence Evasion T1564/T1574 - Credential Access T1555/T1539 - Command-and-Control T1071 - Exfiltration T1041

6. Chaos RAT

A cryptocurrency mining attack targeting the Linux operating system has recently included the use of an open-source remote access trojan known as CHAOS. The RAT alters /etc/crontab file, a UNIX task scheduler that downloads itself every 10 minutes from Pastebin to achieve persistence. Once downloaded and launched, it transmits system metadata to a remote server. It is GO Compiled with capabilities to carry out the following operations:

- Perform reverse shell,
- Download files,
- Upload files,
- Delete files,
- Take screenshots,
- Access file explorer,
- Gather operating system information,
- Restart the PC,
- Shutdown the PC, and
- Open a URL

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: Execution TA0002 - Persistence TA0003 - Privilege Escalation TA0004 - Defence Evasion TA0005 - Command-and-Control TA0011

New Ransomware Victims Last Week: 41

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 41 new ransomware victims from 13 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.

LockBit3.0, a specific ransomware, has affected the largest number of new victims (27) spread across various countries. Bianlian and Snatch groups follow closely with each hitting 03 new victims. Below is the victim counts for these ransomware groups and a few others.

Name of Ransomware Group	No of new Victims last week
Bianlian	3
LockBit 3.0	27
Medusa	1
Play	1
Ransomexx	1
Ransomhouse	2
Royal	1
Snatch	3
V is vendetta	1
Vicesociety	1

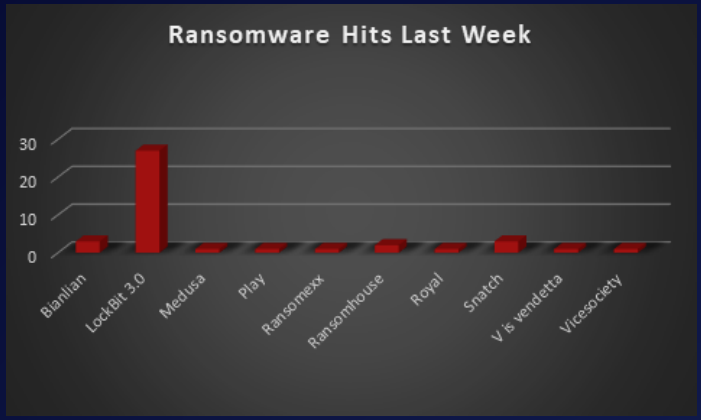


Figure 1: Ransomware Group Hits Last Week

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 13 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
Australia	1
Austria	1
Barbados	1
Brazil	1
Canada	2
China	1
France	2
Germany	1
Hong Kong	1
India	3
Italy	2
Japan	1
Kenya	1
Norway	1
Panama	1
Thailand	4
UK	4
USA	13

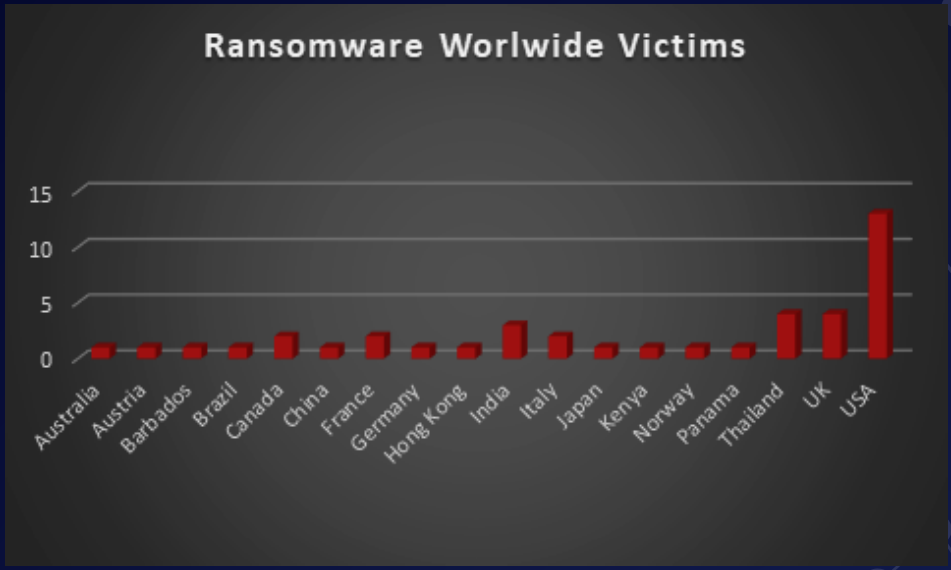


Figure 2: Ransomware Victims Worldwide

After conducting additional research, we found that ransomware has impacted 13 industries globally. Last week, the manufacturing and business services sectors were hit particularly hard, with the loss of four businesses in each sector. The table below presents the most recent ransomware victims sorted by industry.

Name of the affected Country	Number of Victims
Business Services	4
Construction	4
Education	2
Electricity, Oil & Gas	1
Finance	2
Government	2
Hospitality	3
IT	3
legal Services	2
Manufacturing	9
Organisations	2
Retail	4
Transportation	3

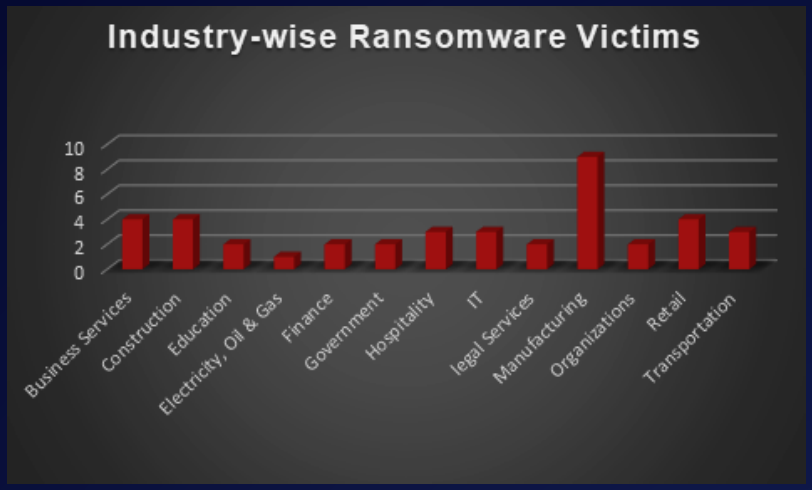


Figure 3: Industry-wise Ransomware Victims