Red Piranha
unified threat management

THREAT INTELLIGENCE REPORT

Mar 14 - 20, 2023

Report Summary:

- **New Threat Detection Added** – 6 (GoatRAT, Emotet, Winter Vivern APT, Prometei Botnet, Clop Ransomware, and Parallax RAT)
- **New Threat Protections**
- **Overall Weekly Observables Count**
- **Daily submissions by Observable Type**
- **New Ransomware Victims Last Week**

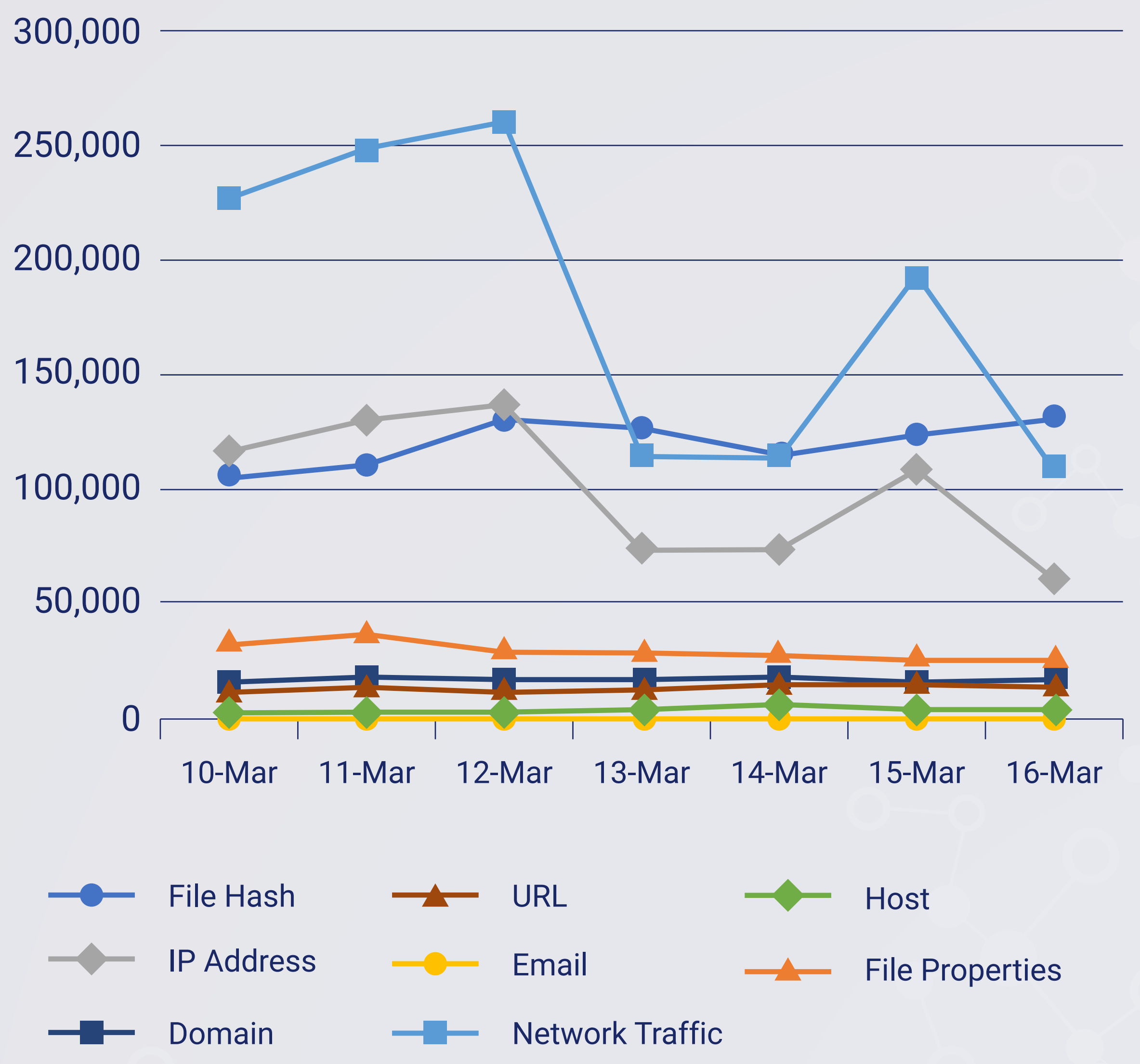
New Threat Protections (Week Ending 20/03/2023):

17

Overall Weekly Observables Count:

3,201,210

Daily Submissions by Observable Type:



Newly Detected Threats Added

1. GoatRAT

Recently, there has been a surge in the usage of Android Banking Trojans that specifically target Brazilian banks utilising the PIX instant payment platform. A fresh iteration of GoatRAT has been discovered, which exclusively utilises the ATS framework to conduct deceitful money transactions. Notably, GoatRAT lacks other traditional features of banking Trojans, such as stealing authentication codes or incoming SMS messages and solely relies on the Accessibility service to execute the ATS framework, which suffices to execute fraudulent financial transactions. This new version of GoatRAT underlines the increased risk of cyberattacks in the present technological landscape, which may not necessitate numerous permissions or advanced Banking Trojan features to execute financial fraud.

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: Initial Access T1476 - Initial Access T1444 - Discovery T1418 - Impact T1516

2. Emotet

Emotet is a Banking Trojan that spreads through spam emails containing malicious attachments, and once downloaded, it can receive commands from a remote server and steal victims' emails and contacts. It was once the most widespread malware, but its activity has been declining. However, after three months of inactivity, the Emotet botnet has resurfaced and resumed sending malicious emails to infect devices worldwide. The new spam campaign uses Epoch4 servers and large document attachments, and the botnet's activity has been observed in over 16 countries by the researchers.

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: Initial Access T1566 - Execution T1204/T1059/T1218 - Defence Evasion T1140/T1564/T1112 - Persistence T1547 - Discovery T1082/T1083/T1007 - Command-and-Control T1071/T1105

3. Winter Vivern

Winter Vivern is a threat actor group that is known to conduct espionage using simple yet effective techniques. Recent campaigns revealed that different government organisations have been targeted such as Poland, Ukraine, Italy, and India.

Rules are deployed on Crystal Eye devices to detect and prevent attacks that are attributed to the Winter Vivern.

Threat Protected: 09
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 - Command-and-Control T1102

4. Prometei Botnet

Prometei is a botnet that was first discovered in 2020. Through continuous monitoring, it was revealed that Prometei kept on improving its infrastructure and capabilities. One of its techniques includes the installation of Apache with a web shell to gain access to their victims' machines accessible. The botnet was also observed to have a self-updating feature. Based on sinkhole data, it is also assessed with high confidence that the Prometei botnet has more than 10,000 infected systems worldwide.

Threat Protected: 04
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: Resource Development T1584 - Persistence T1505 - Evasion T1027/T1036 - Lateral Movement T1210 - Command-and-Control T0884

5. Clop Ransomware

A ransomware has been observed appending its encrypted file with the extension ".ClOP". The CLOP Ransomware has been seen targeting a victim's network instead of their systems in their attacks' allowing them to persist even after the endpoints are cleaned up. The delivery of the said malware is being done through phishing campaigns. The loader sent in these campaigns in turn downloads software like SDBOT, FlawedAmmyy, and Cobalt Strike to set the stage for deployment of the malware.

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: Initial Access TA0001 - Execution TA0002 - Persistence TA0003 - Privilege Escalation TA0004 - Defence Evasion TA0005 - Command-and-Control TA0011

6. Parallax RAT

Attackers are using Parallax RAT to gain access to their victims with functionality such as upload and download files as well as record keystrokes and screen captures. The first payload is a Visual C++ malware that employs the process hollowing technique to inject Parallax RAT into a legitimate Windows component called pipanel.exe. Parallax RAT, besides gathering system metadata, is also capable of accessing data stored in the clipboard and even remotely rebooting or shutting down the compromised machine. One notable aspect of the attacks is the use of the Notepad utility to initiate conversations with the victims and instruct them to connect to an actor-controlled Telegram channel.

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 TA0002 - Defence Evasion TA0005 - Discovery TA0007

New Ransomware Victims Last Week: 67

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 67 new ransomware victims from 15 distinct industries across 16 countries worldwide. This highlights the global reach and indiscriminate nature of ransomware attacks, which can affect organisations of all sizes and sectors.

LockBit 3.0, a specific ransomware, has affected the largest number of new victims (30) spread across various countries. Blackbasta and Play groups follow closely with each hitting 10 and 06 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
Blackbasta	14.92%
BlackByte	4.47%
Clop	7.46%
Everest	2.98%
LockBit 3.0	44.77%
Lorenz	2.98%
Medusa	2.98%
Monti	2.98%
Play	8.95%
Ransomhouse	2.98%
Royal	1.49%
Vicesociety	2.98%

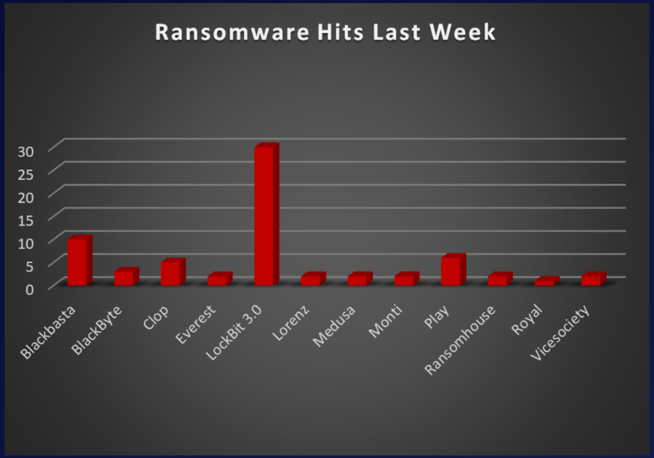


Figure 1: Ransomware Group Hits Last Week

When we examine the victims by country out of 16 countries around the world, we can conclude that the USA was once again the most ransomware-affected country, with a total of 41 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
Belgium	1.49%
Brazil	2.98%
Canada	4.47%
China	1.49%
Colombia	1.49%
Germany	4.47%
Indonesia	1.49%
Italy	5.97%
Lebanon	1.49%
Malaysia	1.49%
Netherlands	1.49%
Saudi Arabia	2.98%
Taiwan	1.49%
UAE	1.49%
UK	4.47%
USA	61.19%

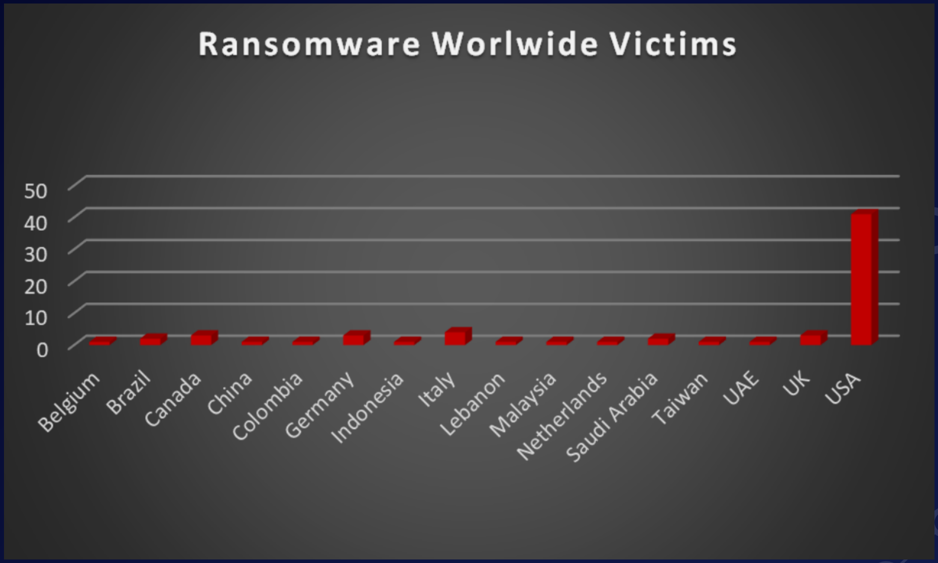


Figure 2: Ransomware Victims Worldwide

After conducting additional research, we found that ransomware has impacted 15 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 most recent ransomware victims sorted by industry.

Industry	Victims Count (%)
Business Services	10.44%
Consumer Services	4.47%
Education	7.46%
Electricity, Oil & Gas	2.98%
Finance	4.47%
Government	1.49%
Healthcare	4.47%
IT	7.46%
Legal Services	10.44%
Manufacturing	17.91%
Mining	1.49%
Real Estate	4.47%
Retail	13.43%
Telecommunication	2.98%
Transportation	5.97%

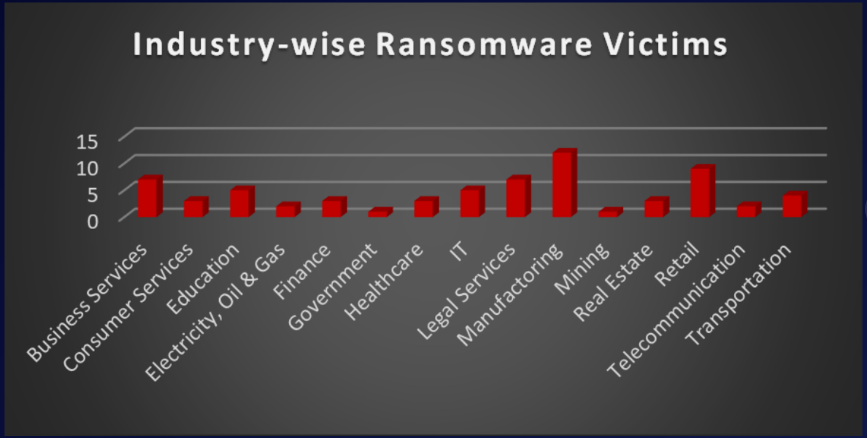


Figure 3: Industry-wise Ransomware Victims