Red Piranha
unified threat management

THREAT INTELLIGENCE REPORT

Jan 24 - 30, 2023

Report Summary:

- **New Threat Detection Added** – 6 (Gigabud RAT, Aurora Stealer, PY#RATION RAT, Obsidium Stealer, Lexmark Printer Exploit, and Witchetty)
- **New Threat Protections**
- **Overall Weekly Observables Count**
- **Daily submissions by Observable Type**
- **New Ransomware Victims Last Week**

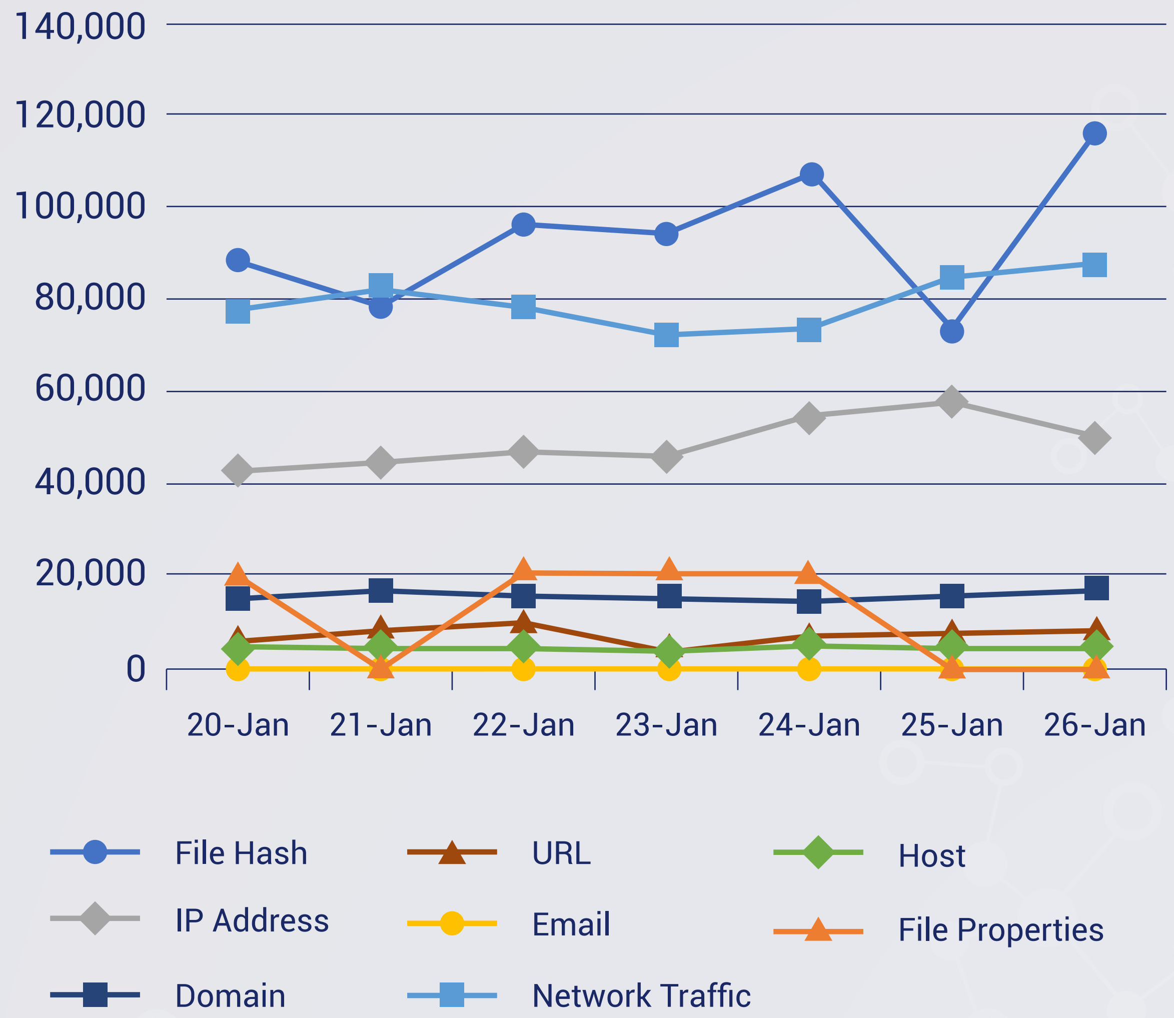
New Threat Protections (Week Ending 30/01/2023):

17

Overall Weekly Observables Count:

1,818,084

Daily Submissions by Observable Type:



Newly Detected Threats Added

1. Gigabud RAT

The analysis shows that the campaign has been actively running by the Threat Actor since July 2022 which mainly targeting Thailand. The campaign expanded to target victims in other countries like Peru and the Philippines later. The TA has used unique techniques to evade detection and sustain the campaign for an extended period. It also noticed that the Gigabud RAT instead of using HTML overlay attacks utilizes screen recording as a primary method for gathering sensitive information. The RAT also abuses the Accessibility service, like other banking trojans. The Threat Actor behind the Gigabud RAT is continuously developing new variants of the malware intending to target different countries.

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 Access T1444 -Discovery T1418 - Collection T1513 - Credential Access T1411 - Impact T1582 - Command-and-Control T1436 - Exfiltration T1567

2. Aurora Stealer

Aurora is a malware that aims to steal personal information. It targets data from web browsers, crypto wallets, browser extensions, Telegram, and specific user directories. The malware continues its data collection by searching for FTP client software, Telegram, Discord, and Steam applications in the victim's machine and steals important information from their config and session data files. The malware also grabs specific files from directories like the Desktop and Documents and takes screenshots of the victim's system. After gathering all the necessary information, it saves the data in JSON format, compresses it using GZIP, and converts it into Base64 encoding format before sending it to the Command-and-Control (C&C) server.

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/T1059/T1047 - Defence Evasion T1027/T1497 - Credential Access T1003/T1056/T1552 - Discovery T1082/T1518/T1083/T1087 - Collection T1005 - Command-and-Control T1071/T1095

3. PY#RATION RAT

A new Python-based attack campaign is leveraging a Python-based remote access trojan (RAT) to gain control over compromised systems. The malware comes with a host of capabilities that allows the threat actor to harvest sensitive information. Later versions of the backdoor also sport anti-evasion techniques, suggesting that it's being actively developed and maintained. The attack commences with a phishing email containing a ZIP archive, which, in turn, harbours two shortcut (.LNK) files that masquerade as front and back side images of a seemingly legitimate UK driver's license.

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 T1566.001 - Execution T1204.002 - Persistence T1547.001 - Command-and-Control T1071 - Collection T1115 - Credential Access T1555.003

4. Obsidium Stealer

Obsidium Stealer is a malware that is designed to capture data from infected devices. It targets crypto-wallets, web browser cookies, passwords stored from authentication apps, and general computer information. It will zip/compress this data and send it to its Command-and-Control server. It also has anti-analysis behaviour in that it sends meaningless functions when run over a debugger. Red Piranha's Crystal Eye has rules in place to detect potential exfiltration of these data.

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 - Execution T1059 - Collection T1119/T1005/T1185 - Command-and-Control T1132 - Exfiltration T1041

5. Lexmark Printer Exploit

A researcher from the recently concluded Pwn2Own Toronto 2022 has publicly released a working exploit for the 'MC3224adwe' Lexmark Printer/Copier. It is not clear as to which other products are affected as it was only tested on the 'MC3224adwe' with a firmware version of 'CXLBL.081.225'. Lexmark has not provided any fix for this at the moment.

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: Attempted-admin
Kill Chain: Initial Access T1190 - Execution T1059.006

6. Witchetty

The Witchetty espionage group (aka LookingFrog) has been progressively updating its toolset, using new malware in attacks on targets in the Middle East and Africa. Among the new tools being used by the group is a backdoor Trojan (Backdoor.Stegmap) that employs steganography, a rarely seen technique where malicious code is hidden within an image. While the group has continued to use the LookBack backdoor, several new pieces of malware appear to have been added to its toolset. Backdoor.Stegmap which leverages steganography to extract its payload from a bitmap image. Although rarely used by attackers, if successfully executed, steganography can be leveraged to disguise malicious code in seemingly innocuous-looking image files.

Threat Protected: 07
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 T1444 - Discovery T1418 - Collection T1513 - Credential Access T1411 - Command-and-Control T1436

New Ransomware Victims Last Week: 27

Red Piranha regularly collects information about organisations hit by ransomware from different sources including the Dark Web. During the previous week, Red Piranha identified a total of 27 new ransomware victim organisations from 11 different countries all over the world.

One particular ransomware group named LockBit3.0 tallied the greatest number of new victims (6), the locations of which are spread across different countries. This is followed by AlphV and Bianlian groups who hit 5 new victims each. Victim counts these ransomware groups, and a few others are listed below:

Name of Ransomware Group	No of new Victims last week
AlphV	5
bianlian	5
LockBit3.0	6
Mallox	3
Play	2
Royal	5
vicesociety	1

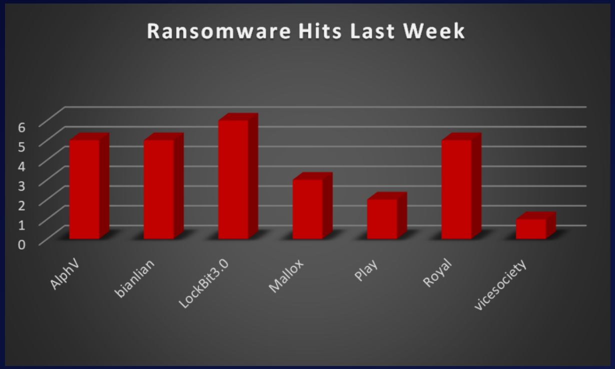


Figure 1: Ransomware Group Hits Last Week

If we look at the victims as per the country, we can say that the USA was once again become the most affected country by ransomware groups where a total of 13 new victims were reported last week followed by Australia with 3 new victims reported. The number of new ransomware victims per country is listed below:

Name of the affected Country	Number of Victims
Australia	3
Austria	2
Canada	1
France	1
Germany	1
India	2
Portugal	1
Singapore	1
Sweden	1
UK	1
USA	13

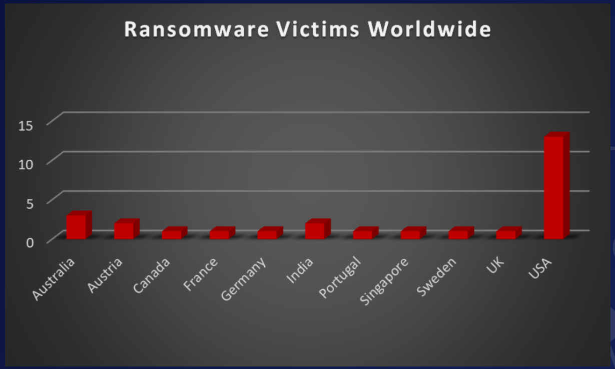


Figure 2: Ransomware Victims Worldwide

We conducted more research and discovered that 13 industries were affected globally by ransomware, with the manufacturing and retail sectors being struck with the loss of six new businesses globally just last week. The following table lists the latest ransomware victims by sector:

Name of the affected Country	Number of Victims
Business Services	3
Construction	1
Education	1
Energy	1
Engineering	1
Finance	1
Healthcare	2
Hospitality	2
Insurance	1
IT	1
Manufacturing	6
Municipalities	1
Retail	6

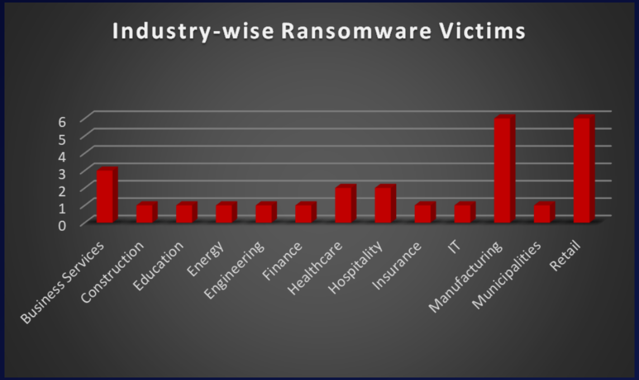


Figure 3: Industry-wise Ransomware Victims