Red Piranha
unified threat management

THREAT INTELLIGENCE REPORT

Dec 27, 2022 - Jan 02, 2023

Report Summary:

- **New Threat Detection Added** – 04 (YouTube Bot, GodFather Returns, STRRat Malware, and Drokbk Malware)
- **New Threat Protections**
- **Overall Weekly Observables Count**
- **Daily submissions by Observable Type**
- **New Ransomware Victims Last Week**

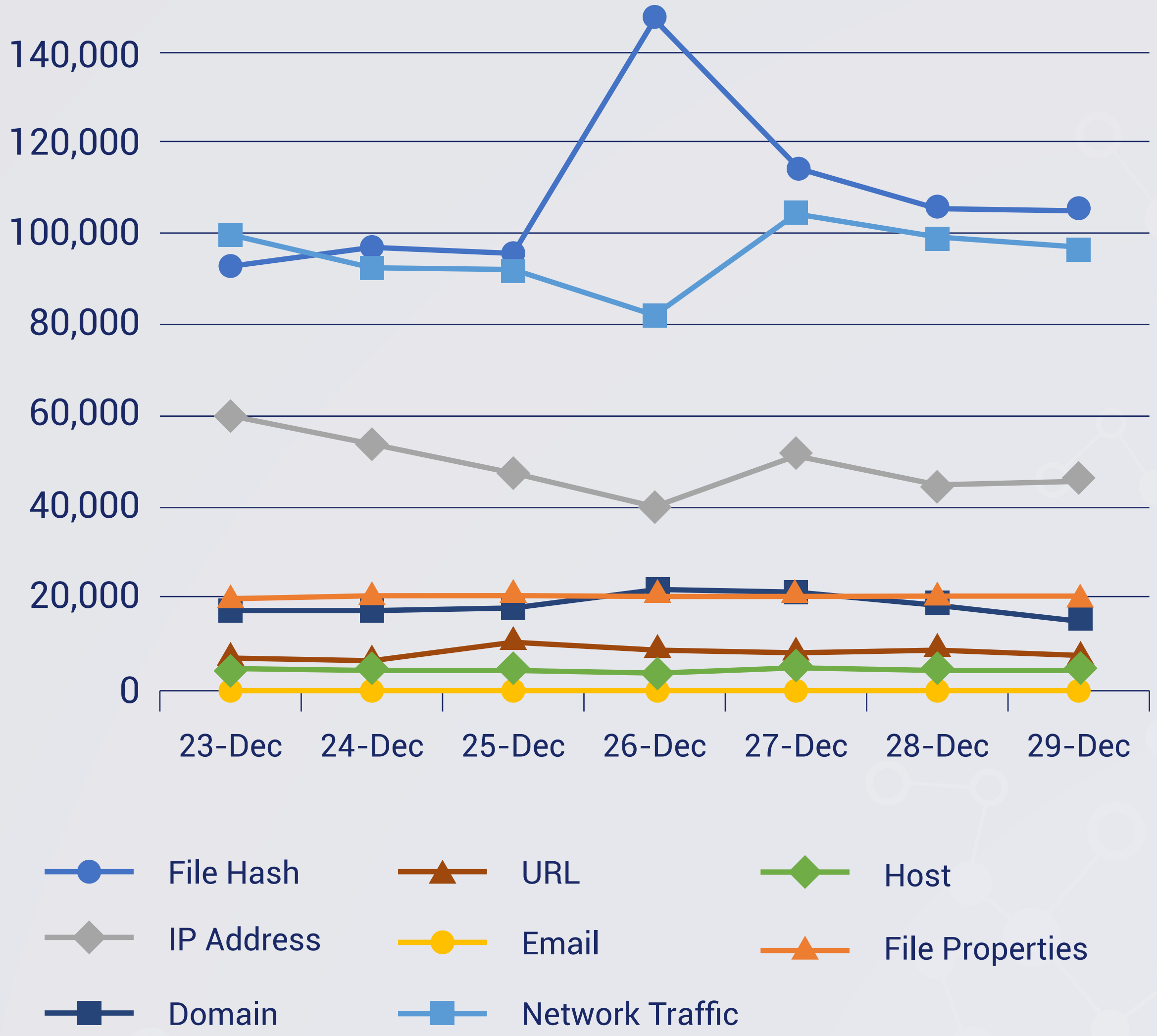
New Threat Protections (Week Ending 02/01/2023):

08

Overall Weekly Observables Count:

2,104,132

Daily Submissions by Observable Type:



Newly Detected Threats Added

1. YouTube Bot Malware

Recently, a new YouTube bot malware was discovered that can watch, like, and comment on YouTube videos. Additionally, it can steal private data from browsers and function as a bot that takes instructions from a command-and-control (C&C) server to carry out additional nefarious deeds. It was created as a 32-bit executable file using the .NET compiler. The malware first determines whether it is running in a managed environment, like VMware or VirtualBox, before executing. To enhance the number of likes, comments, and views on their YouTube videos in this scenario, The Threat Actors (TAs) deploy specially crafted YouTube bots. Additionally, the YouTube bot can harvest passwords, cookies, AutoFill data, and other sensitive information from its victims.

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/T1047/T1059 - Persistence T1053 - Privilege Escalation T1055 - Defense Evasion T1036/T1562/T1497 - Credential Access T1003 - Discovery T1057/T1082/T1518 - Collection T1005 - Command-and-Control T1071/T1105

2. GodFather Malware Returns

GodFather is a well-known Android banking virus that mostly targets consumers in European nations. Recently, multiple Android samples for GodFather that were posing as MYT applications were discovered. The name of this application is MYT Müzik, and it is written in Turkish. As a result, it is believed that this application targets Turkish Android users. After successfully being installed on the victim's device, the GodFather Android virus collects private data like SMSs, basic device information like loaded app data, and the phone number of the device. In addition to these features, it can also route incoming calls from the victim's device, inject banking URLs, and control the device screen using VNC.

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 T1476 - Initial Access T1444 - Execution T1575 - Collection T1513 - Command-and-Control T1436/T1616

3. STRRat Malware

STRRAT is a Java-based remote access trojan (RAT) that provides threat actors with full remote control of infected Windows endpoints. STRRAT focuses on stealing credentials from browsers and email clients like Microsoft Edge, Google Chrome, Mozilla Firefox, Microsoft Outlook, Mozilla Thunderbird, and Foxmail. It also steals credentials by recording keystrokes of infected endpoints. STRRat also has the capability of mimicking a ransomware attack. No files are encrypted; the malware appends the file - extension ".crimson" while opening Notepad to display a false ransom note.

Threat Protected: 03
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: Discovery TA0007

4. Drokbk Malware

The Dead Drop Resolver is a technique where a legitimate cloud service is exploited to host the information that points to the command-and-control infrastructure. A recent example is the latest campaign Using Drokbk Malware. Drokbk is deployed post-intrusion alongside other access mechanisms as an additional form of persistence within the victim's environment. The Drokbk dropper checks for the existence of the c:\programdata\SoftwareDistribution directory and creates the directory if it does not exist. The dropper then writes all bytes from an internal resource to c:\users\public\pla. This is a temporary step; the extracted file (pla) is then copied to c:\programdata\SoftwareDistribution\SessionService.exe.

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: Malware
Kill Chain: Execution TA0002 - Persistence TA0003 - Command-and-Control TA0011

New Ransomware Victims Last Week: 30

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 30 new ransomware victim organisations from 13 different countries all over the world.

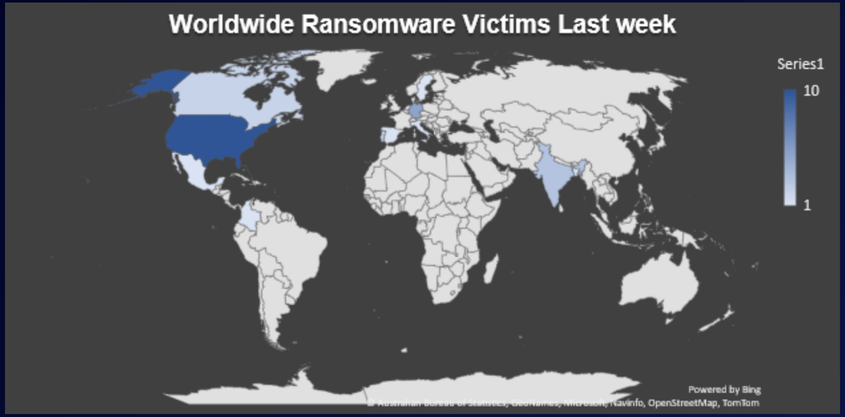

Worldwide Ransomware Victims Last week
Series1
10
1
Powered by Bing
© Australian Bureau of Statistics, GeoNames, Microsoft, Navinfo, OpenStreetMap, TomTom

Figure 1: Ransomware Victims Worldwide

One particular ransomware group named Royal tallied the greatest number of new victims (09), the locations of which are spread across different countries. This is followed by AlphV and Snatch groups with 06 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	6
Bianlian	3
Hive	1
LockBit	3
Play	1
RansomHouse	1
Royal	9
Snatch	6

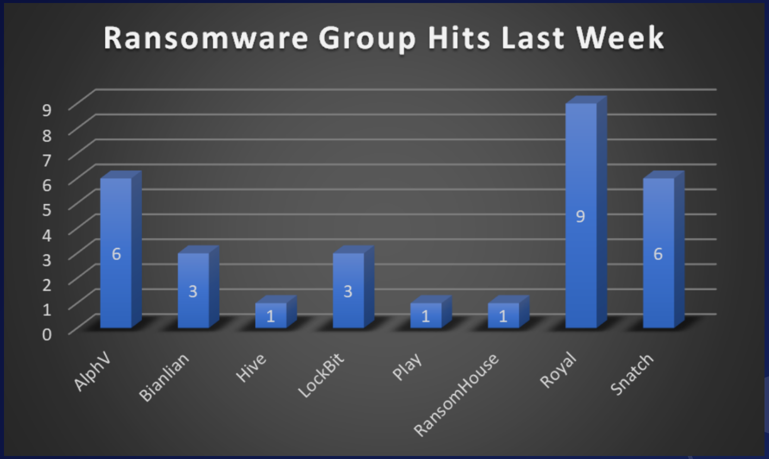


Figure 2: Ransomware Hits last Week

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 10 new victims were reported last week followed by Germany and India where 5 and 3 new victims respectively were reported. The number of new ransomware victims per country is listed below:

Name of the effected Country	Number of Victims
Bangladesh	1
Canada	2
Colombia	1
Germany	5
India	3
Italy	1
Mexico	1
Portugal	2
Rome	1
Spain	1
Sweden	1
USA	10
Vanuatu	1

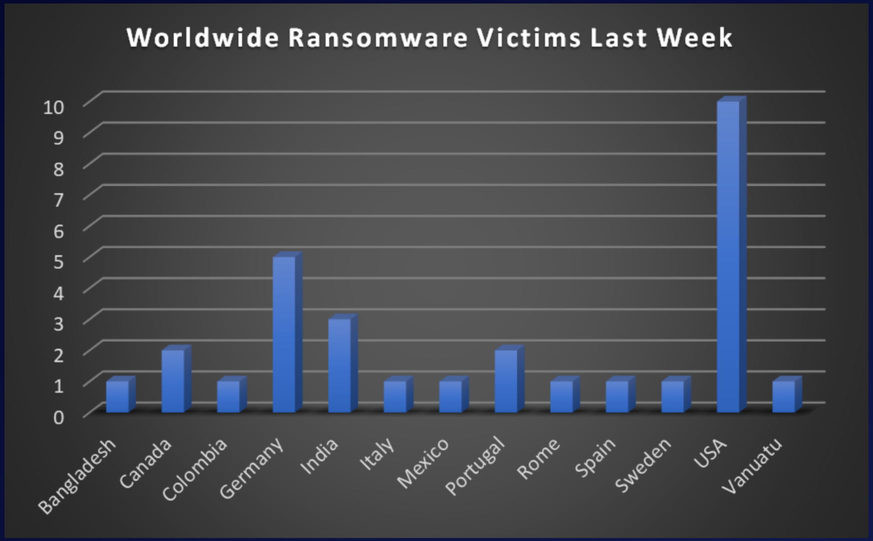


Figure 3: Country-wise Ransomware Victims