Red Piranha

unified threat management

THREAT INTELLIGENCE REPORT

Jan 31 - Feb 6, 2023

Report Summary:

- **New Threat Detection Added** – 6 (SpyMax, Amadey Bot Malware, Titan Stealer Malware, STOP/DJVU ransomware, Ice Breaker APT, and GCleaner Malware)
- **New Threat Protections**
- **Overall Weekly Observables Count**
- **Daily submissions by Observable Type**
- **New Ransomware Victims Last Week**

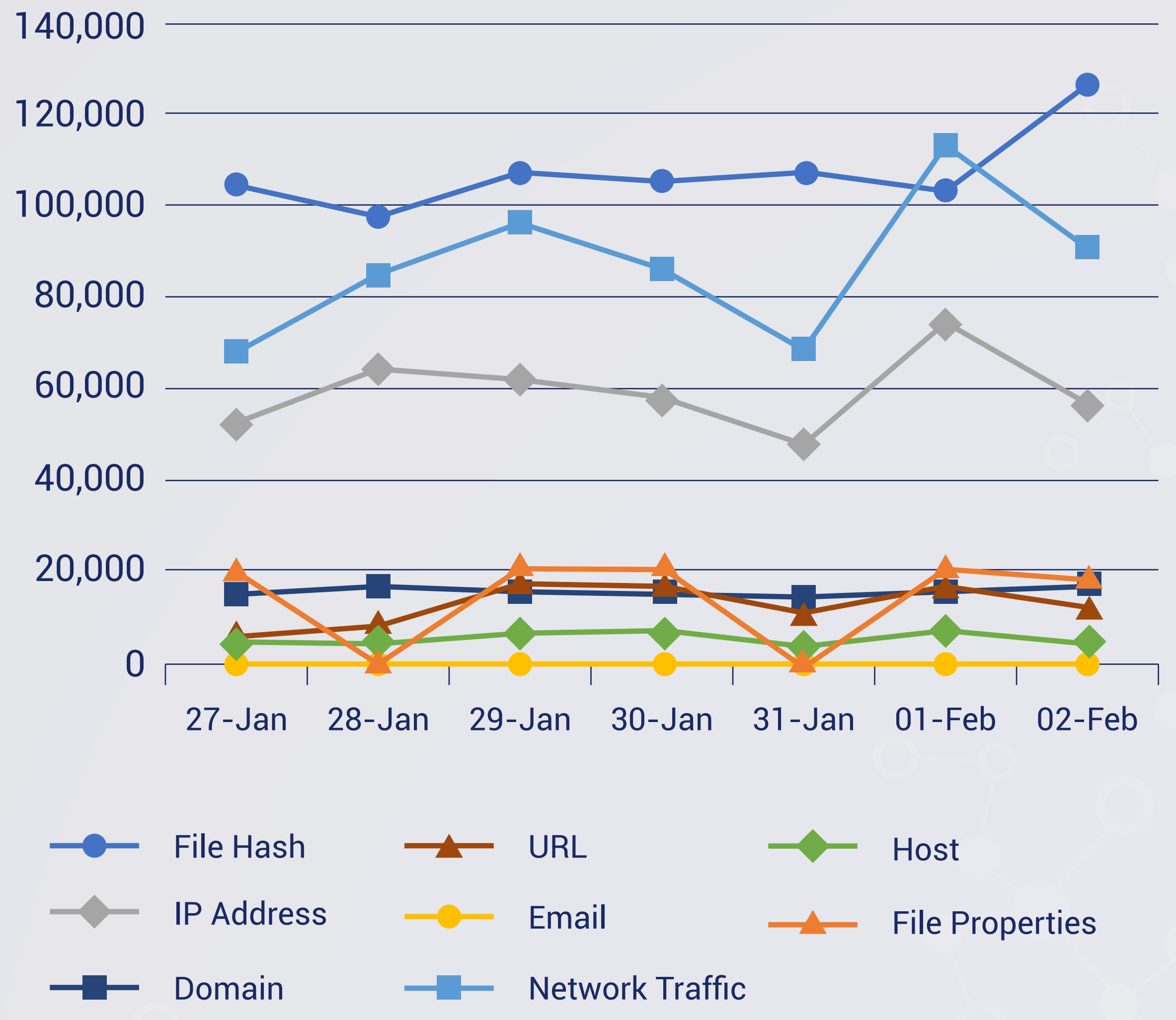
New Threat Protections (Week Ending 06/02/2023):

15

Overall Weekly Observables Count:

2,084,946

Daily Submissions by Observable Type:



Newly Detected Threats Added

1. SpyMax

A powerful form of Android malware known as SpyMax is in the highlight trying to steal bank details and passwords, as well as social media pages. The latest version of the SpyMax has been openly directed at banking apps. SpyMax typically masquerades as a legitimate banking app as a part of the phishing attack, drawing users into downloading fake versions that install straight onto their Android devices. The app presents a bogus login page that looks identical to the bank's login, and using a keylogger, tracks the usernames and passwords entered. After installation the malware escalates itself to gain admin privileges, making it a task for the users to uninstall it.

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: Malware
Kill Chain: Initial Access T1566 - Privilege Escalation T1548 - Credential Access T1056 - Command-and-Control T1071

2. Amadey Bot Malware

The Amadey bot is a Trojan that is used to steal private data from infected devices. It was first identified in 2018. It was initially discovered to be distributed through exploit kits, and Threat Actors (TAs) used it to spread malware like the Flawed Ammyy Remote Access Trojan and the GrandCrab ransomware. LOCKBIT affiliates used the Amadey bot in 2022 to spread ransomware to the victims. The appearance and functionality of bots have significantly improved in recent years.

Amadey is an example of a bot that comes fully loaded with features like system reconnaissance, information theft, malware download and execution, data exfiltration, and even clipper functionalities in its most recent version. Threat actors are able to do this in order to steal login, payment, and personal information from web browsers, which they can then use for a variety of fraudulent activities. Due to their extensive capabilities, this type of malware poses a serious threat to a wide range of potential victims.

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/T1218/T1047/T1106 - Persistence T1547/T1053 - Defence Evasion T1027/T1497 - Credential Access T1003/T1552/T1552/T1056 - Discovery T1082/T1518/T1083/T1087 - Collection T1005/T1213 - Command-and-Control T1071/T1095

3. Titan Stealer

One such malware, known as Titan Stealer, was recently discovered by researchers. The numerous Command-and-Control (C&C) infrastructures connected to this Stealer's attack on new victims were also found. A recent example of TAs using Golang is Titan Stealer. There were 94 entries in the panel, which suggests that the malware may have infected several systems and may have activated multiple Command-and-Control servers.

A system's IP address, country, city, username, screen size, CPU model name, threads, and GPU are all extracted by Titan Stealer. The stealer searches the victim's computer for various cryptocurrency wallets. The related files are taken and sent to the C&C server if the stealer is able to identify the wallets installed on the victim's computer. The stealer first checks wallets and then scans the system for installed software before sending a list of that software to its C&C server. The hacker then looks for installed web browsers to extract various browser data, including passwords, session cookies, autofill, and more. Text and document files that are on the computer are listed and taken by the stealer.

The stealer now targets FTP clients and steals FTP server credentials from FileZilla and GHISLER. Along with enumerating and grabbing text and document files, the thief also targets and steals stored Telegram data. The data thief then zips up the stolen information, turns it into a Base64-encoded string, and sends it to its Command-and-Control server.

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 - Credential Access T1003/T1552 - Discovery T1082/T1518/T1083/T1087 - Collection T1005 - Command-and-Control T1071/T1095

4. STOP/DJVU ransomware

The DJVU variants include several layers of obfuscation, which aim to slow verification by researchers as well as automated analysis tools. STOP/DJVU uses RSA encryption, one of the most commonly used ransomware groups, focusing on Windows operating systems. STOP/Djvu infection can happen through multiple approaches - Pirate software and torrents, Fake .exe, Malicious scripts or Spam. The ransomware has no pre-set infection method which makes it even harder to detect the initial sign of compromise.

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: Persistence TA0003 - Boot or Logon Autostart Execution T1547 - Privilege Escalation TA0004 - Data Encrypted for Impact T1485 - System Information Discovery T1082 - Process Injection T1055

5. Ice Breaker APT

A recently tracked threat actor dubbed as Ice Breaker has been targeting the online gaming/casino industry. The context of their social engineering attack is that the threat actors would falsely request technical support from the casino/gaming representative. Upon initial conversation, the threat actor would send links to the LNK/Zipped images of their supposed issue. Upon successful execution of the files from the victim, credentials will be harvested, and a shell will be opened for the next series of attacks.

Threat Protected: 06
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/T1204 - Persistence T1547 - Defence Evasion T1218 - Command-and-Control T1071

6. GCLeaner Malware

GCleaner is a trojan malware that disguises itself as a system/cache cleaner and even a file recovery software for computers. It claims to clean a computer's cache, delete unnecessary files, clean out disk storage, etc. However, GCleaner has been exposed as a Pay-per-Install malware where they sell access to their victims' computers to drop other types of malware. In essence, the threat actors behind GCleaner would sell their victims' computers to other threat actors. Hence, it is observed that different types of malware are discovered on computers that have a GCleaner installation. Malware such as Redline, SmokeLoader, RacoonStealer are just some of the ones that are dropped.

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: Initial Access T1189 - Execution T1059 - Discovery T1012/T1082 - Command-and-Control T1102

New Ransomware Victims Last Week: 52

Red Piranha regularly collects information about organizations hit by ransomware from different sources including the Dark Web. During the previous week, Red Piranha identified a total of 52 new ransomware victim organizations in 22 different countries all over the world.

One particular ransomware group named LockBit3.0 tallied the greatest number of new victims (39), the locations of which are spread across different countries. This is followed by AlphV and Royal groups who hit 4 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	4
Bianlian	1
LokBit3.0	39
Play	1
Royal	4
ViceSociety	3

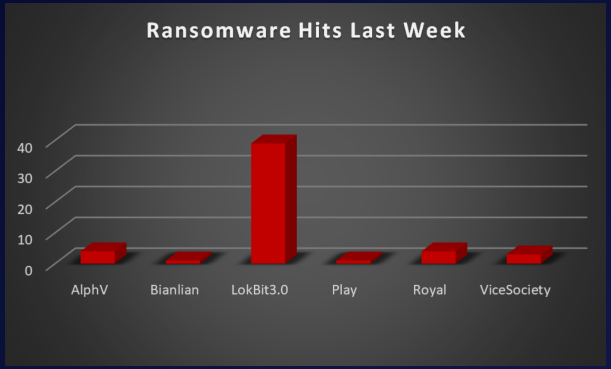


Figure 1: Ransomware Group Hits Last Week

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 19 new victims were reported last week followed by the United Kingdom with 4 new victims reported. The number of new ransomware victims per country is listed below:

Name of the affected Country	Number of Victims
Albania	1
Australia	1
Belgium	1
Brazil	1
Canada	3
China	1
Czech Republic	1
Denmark	1
Egypt	1
France	3
Germany	2
Greece	1
Israel	1
Italy	3
Japan	1
Mexico	3
Portugal	1
Romania	1
Thailand	1
UK	4
USA	19
Western Sahara	1

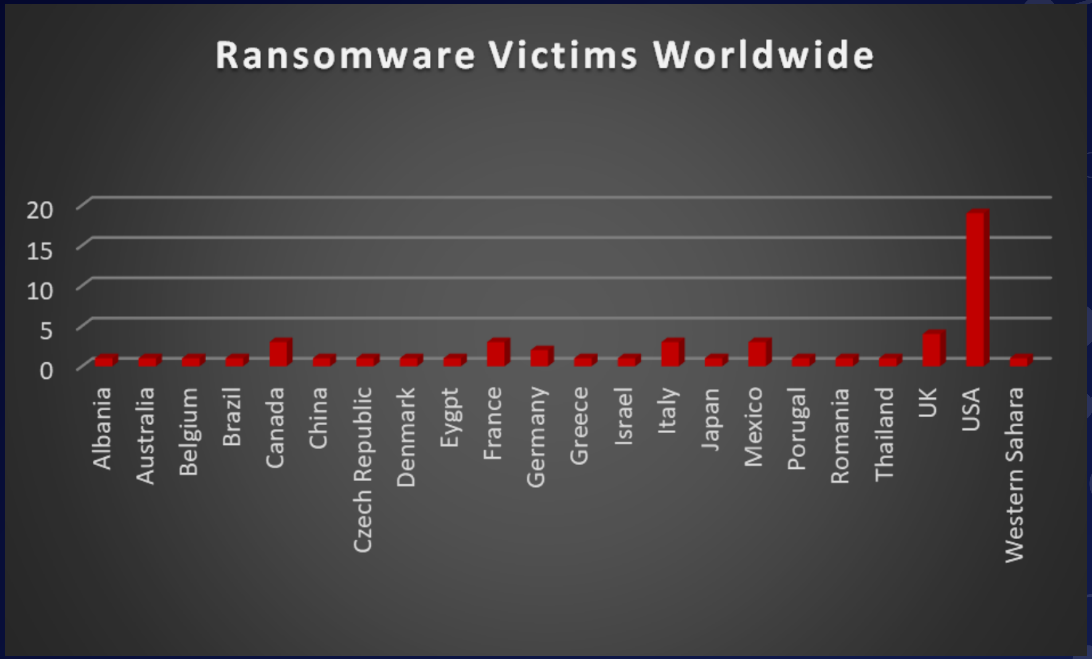


Figure 2: Ransomware Victims Worldwide

We conducted more research and discovered that 16 industries were affected globally by ransomware, with the manufacturing and IT sectors being struck with the loss of 12 and 6 new businesses respectively just last week. The following table lists the latest ransomware victims by sector:

Name of the affected Country	Number of Victims
Automobile	1
Business Services	4
Construction	1
Education	3
Electricity, Oil & Gas	1
Finance	2
Government	3
Healthcare	3
Hospitality	2
Insurance	1
IT	6
Legal Services	5
Manufacturing	12

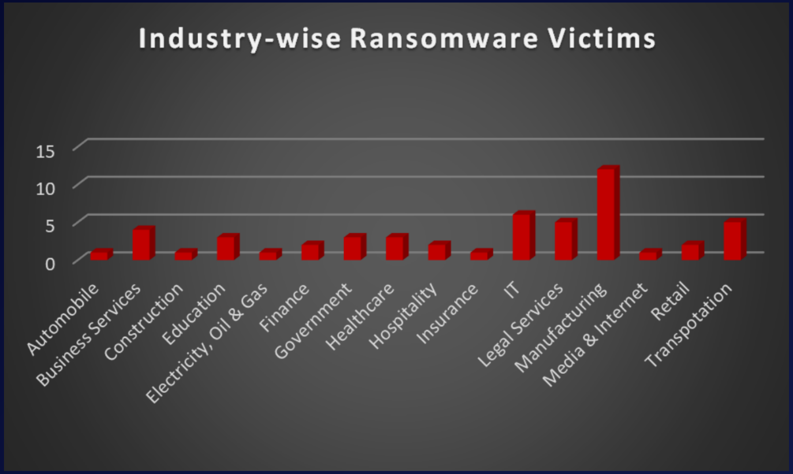


Figure 3: Industry-wise Ransomware Victims