Red Piranha
unified threat management

THREAT INTELLIGENCE REPORT

Jan 10 - 16, 2023

Report Summary:

- **New Threat Detection Added** – 6 (LummaC2 Stealer, Turla Malware, SugarCRM Auth Bypass, BlindEagle APT, Ginp Malware, and Linux.Backdoor.WordPressExploit.1)
- **New Threat Protections**
- **Overall Weekly Observables Count**
- **Daily submissions by Observable Type**
- **New Ransomware Victims Last Week**

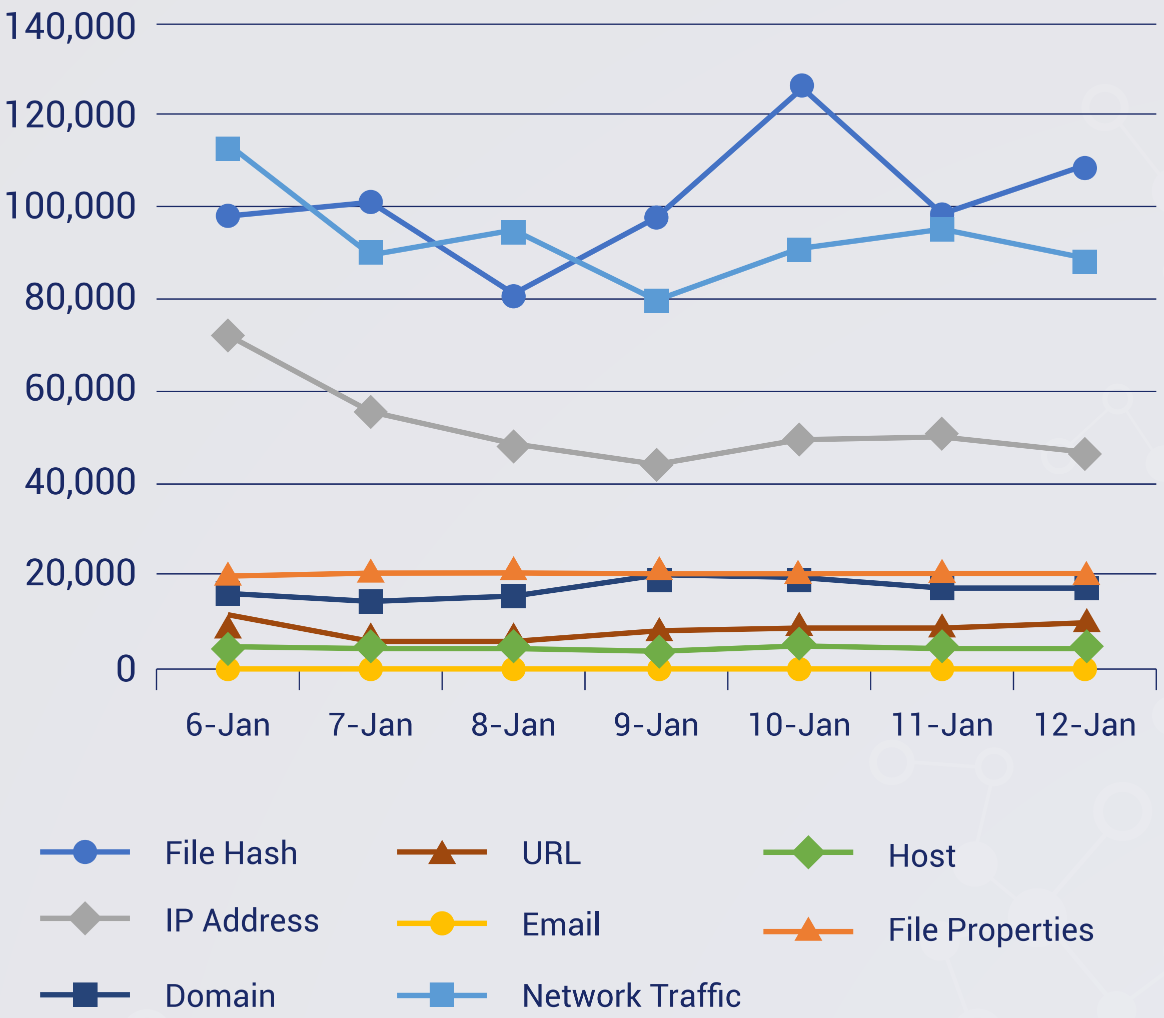
New Threat Protections (Week Ending 16/01/2023):

12

Overall Weekly Observables Count:

2,054,912

Daily Submissions by Observable Type:



Newly Detected Threats Added

1. LummaC2 Stealer

Like the other stealer malware, LummaC2 Stealer has the ability to steal sensitive information from the victim's computer as well as their operating system. This Stealer can gather data from web browsers and target 2FA extensions and cryptographic wallets. Login credentials, personally identifiable information (PII), and financial information are just a few examples of the extra data kept on web browsers that can also be used to steal by the LummaC2 Stealer. Threat actors can use the stolen data for making money: they may sell the stolen data to other threat actors, or they can use it to steal cryptocurrency from the victim's wallets.

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: Defence EvasionT1140/T1562 - DiscoveryT1082/T1083- Collection T1119/T1005 -Command-and-ControlT1071- ExfiltrationT1020

2. Turla Malware

It has been observed that the suspected Turla malware is targeting Ukrainian entities since the onset of the invasion. The campaign's operational tactics appear consistent with Turla's considerations for planning and advantageous positioning to achieve initial access to the victim systems, as the group has leveraged USBs and conducted extensive victim profiling in the past.

The extensive profiling achieved since January possibly allowed the group to select specific victim systems and tailor their follow-on exploitation efforts to gather and exfiltrate information of strategic importance to inform Russian priorities.

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: Defence Evasion T1027/T1055/T1112/T1622 - Persistence T1547.001 - Discovery T1010/T1012/T1033/T1049/T1057/T1082/T1083/T1518 - Collection T1584 - Resource Development T1584 - Command-and-Control T1071.001/T1573.002 - Impact T1529

3. SugarCRM Auth Bypass

An Auth Bypass and RCE exploit has been publicly disclosed by a security researcher that affects SugarCRM's Sell, Serve, Enterprise, Professional, and Ultimate software solutions. The vulnerability relies on a missing authentication check in the loadUser() method of one of SugarCRM's components. Two hotfix patches have been released by SugarCRM which are automatically deployed on SugarCRM's cloud and managed hosting instances. The patches are also available for download for instances outside of SugarCloud and SugarCRM-managed hosting. Red Piranha's Crystal Eye have deployed rules to detect these exploit attempts.

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: Attempted-user
Kill Chain: Initial Access T1190

4. BlindEagle APT

Ongoing campaigns by a threat group that usually targets countries from South America have been observed. Their usual tactic is to send phishing emails pretending to be from the government. These emails contain malicious documents or links where the recipients have to download a file. The malware within these documents is revealed to be QuasarRAT. QuasarRAT is an open-source trojan that is easily publicly available from multiple sources like Github. It leverages PowerShell, Python and 'Living-off-the-land' binaries.

Threat Protected: 03
Rule Set Type:

Class Type: Trojan-activity
Kill Chain: Initial Access T1190 - Execution T1059 - Command-and-Control T1102

Ruleset	IDS: Action	IPS: Action
Balanced	Reject	Drop
Security	Reject	Drop
WAF	Disabled	Disabled
Connectivity	Alert	Alert
OT	Disabled	Disabled

5. Ginp Malware

The Ginp mobile banking malware, which emerged in late 2019, is one of the top most prevalent Android banking malware families today. It started as an SMS stealer and rapidly evolved into one of the most advanced actors in the financial fraud landscape. Ginp has primarily targeted Spanish banks, but recent evidence suggests the malware has changed or may change its targeting strategy in the near future to focus on Turkey. New Ginp overlay pages are intended for overlay attacks on mobile devices residing on the malware's command-and-control (C&C) servers. These overlay pages are spoofs of legitimate banking pages, meant to deceive mobile device users into sharing confidential banking and other information. Several of these fake overlays mimic banks in Turkey, suggesting that malware operators intend to use these pages in future campaigns to target customers of Turkish banks.

Threat Protected: 02
Rule Set Type:

Class Type: Malware
Kill Chain: Command-and-Control TA0011 - Defense Evasion TA0030 - Credential Access TA0031 - Impact TA0034

Ruleset	IDS: Action	IPS: Action
Balanced	Reject	Drop
Security	Reject	Drop
WAF	Disabled	Disabled
Connectivity	Alert	Alert
OT	Disabled	Disabled

6. Linux.Backdoor.WordPressExploit.1

A previously unknown Linux malware has been exploiting 30 vulnerabilities in multiple outdated WordPress plugins and themes to inject malicious JavaScript. The trojan can hack websites based on a WordPress CMS and inject a script into their web pages. The trojan uses known vulnerabilities in WordPress plugins and website themes to do so. Initially, the trojan contacts its C&C server and receives the address of the site it is to infect. Once it has the information, Linux.BackDoor.WordPressExploit.1 successively tries exploiting vulnerabilities in the various outdated plugins and themes that can be installed on a website.

Threat Protected: 03
Rule Set Type:

Ruleset	IDS: Action	IPS: Action
Balanced	Alert	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 - Defense Evasion TA0005 – Command-and-Control TA0011

New Ransomware Victims Last Week: 49

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 49 new ransomware victim organisations from 17 different countries all over the world.

One particular ransomware group named LockBit3.0 tallied the greatest number of new victims (14), the locations of which are spread across different countries. This is followed by AlphV group 10 new victims. Victim counts these ransomware groups, and a few others are listed below.

Name of Ransomware Group	No of new Victims last week
Omega	1
AlphV	10
Avoslocker	3
Hive	2
Karakurt	1
LockBit3.0	14
Lorenz	3
Mallox	1
Play	2
Ransomhouse	2
Royal	5
Snatch	1
Vicesociety	4

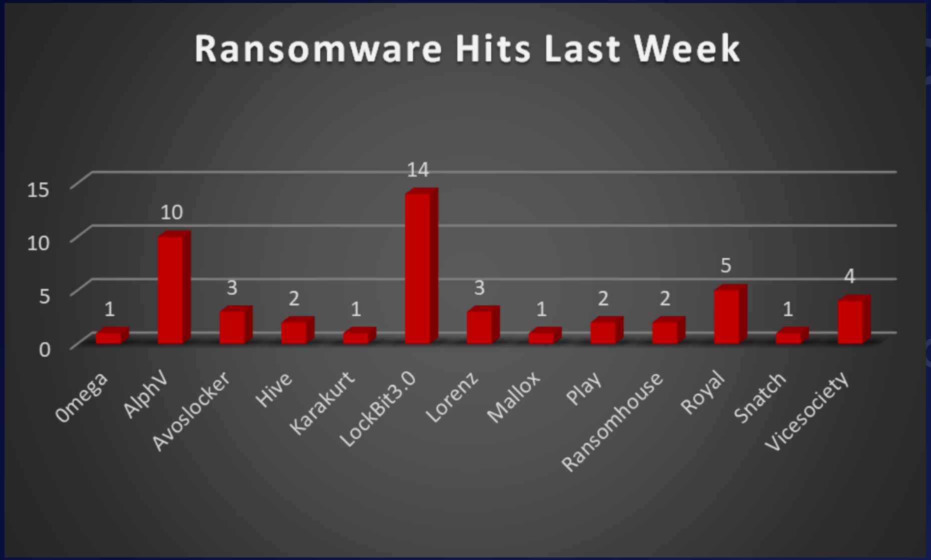


Figure 1: Ransomware Group Hits Last Week

If we look at the victims as per the country, we can say that the USA has once again become the most affected country by ransomware groups where a total of 18 new victims were reported last week followed by the UK with 9 new victims reported. The number of new ransomware victims per country is listed below:

Name of the effected Country	Number of Victims
Australia	2
Florida	1
France	1
Germany	2
India	1
Indonesia	1
Italy	1
Japan	1
Maldives	1
Mexico	3
Netherlands	2
Singapore	1
Switzerland	2
Thailand	2
United Kingdom	9
USA	18

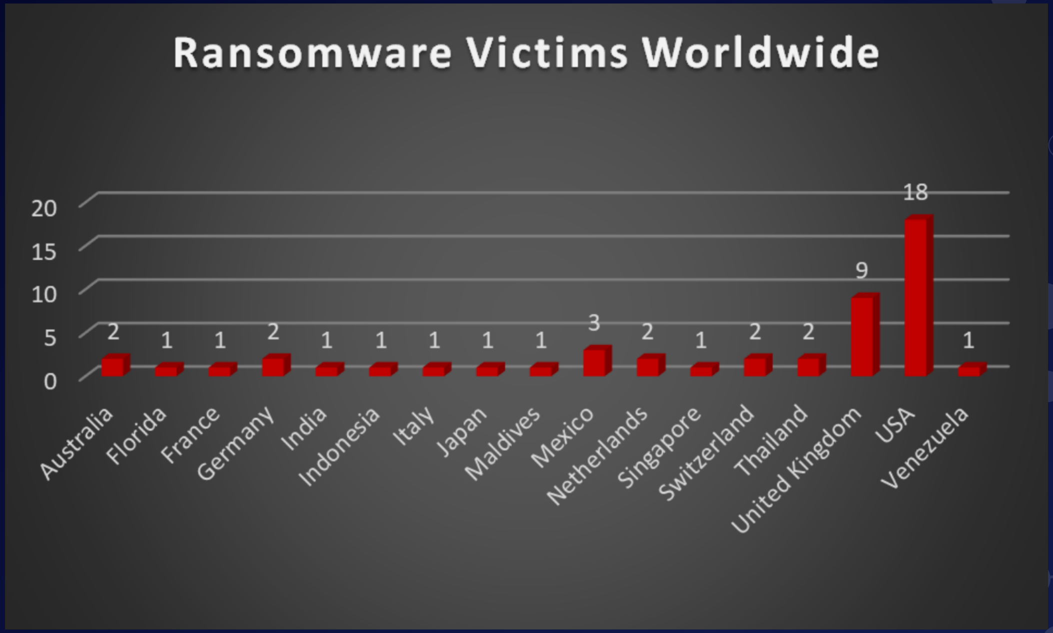


Figure 2: Ransomware Victims Worldwide