Red Piranha
unified threat management

THREAT INTELLIGENCE REPORT

Feb 7 - 13, 2023

Report Summary:

- **New Threat Detection Added** – 4 (Medusa Botnet, New BATLoader malware, Andariel APT, and Fortra RCE CVE-2023-0669)
- **New Threat Protections**
- **Overall Weekly Observables Count**
- **Daily submissions by Observable Type**
- **New Ransomware Victims Last Week**

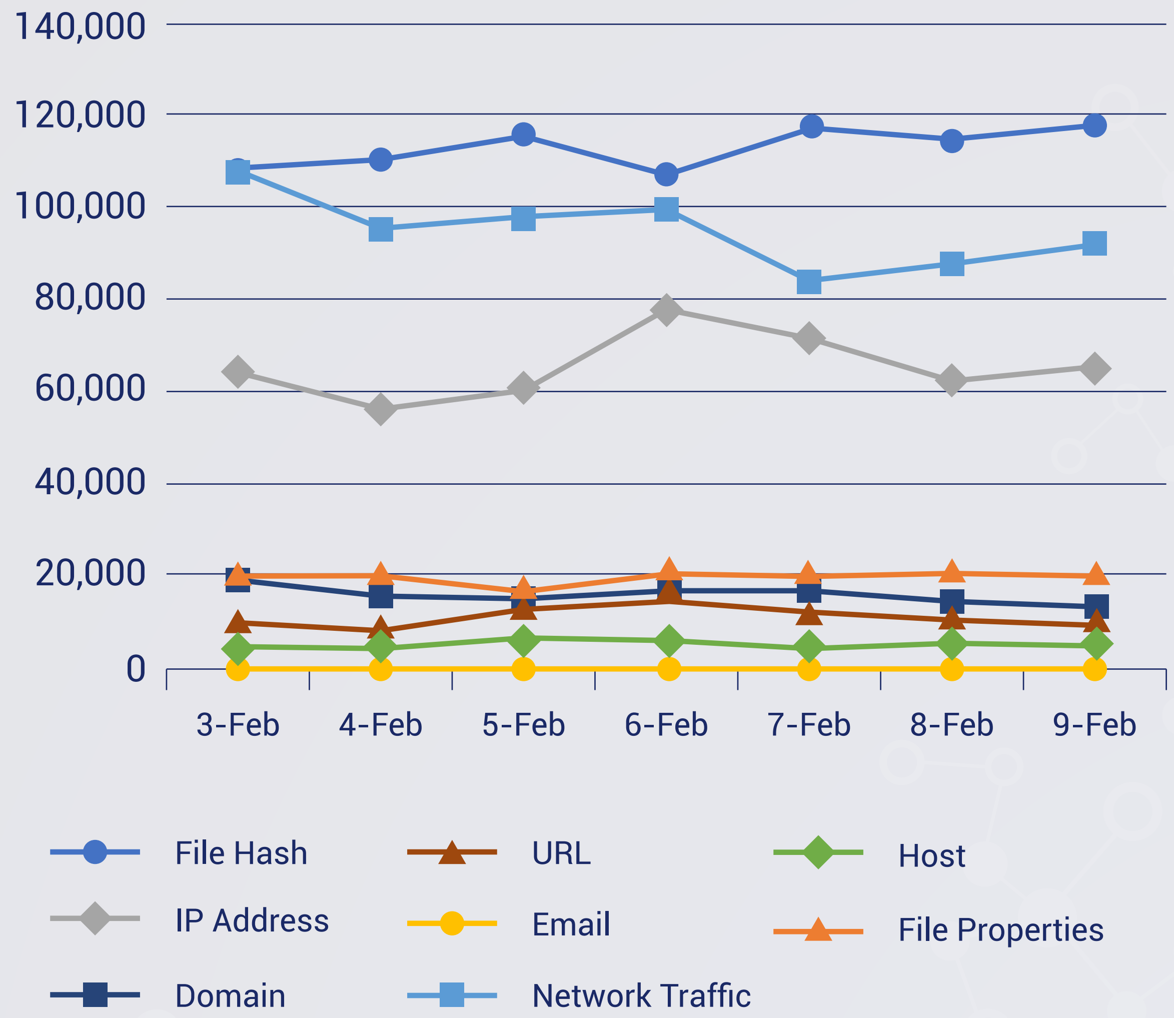
New Threat Protections (Week Ending 13/02/2023):

10

Overall Weekly Observables Count:

2,243,920

Daily Submissions by Observable Type:



Newly Detected Threats Added

1. Medusa Botnet

Researchers have discovered a new variant of the Mirai botnet that can spread and download the Medusa Botnet. Upon execution, the Mirai botnet connects to its command-and-control server to retrieve the Medusa stealer file, which it then executes on Linux machines. The Medusa Botnet has the potential to launch devastating Distributed Denial of Service (DDoS) attacks at various levels of the network hierarchy, and can also carry out ransomware attacks on target systems. Additionally, it can conduct brute force attacks on Telnet services, collecting information such as system specifications, IP address, and unique identifier and sending it back to the 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: Discovery T1518.001 - Command-and-Control T1071/T1095

2. BATLoader malware

Researchers have uncovered a new and sophisticated form of BAT loader, a type of malware used to spread various RATs and Stealer malware families. This new variant of BAT loader is distinct in its method of delivering the malicious payload to the user's system and has been seen in multiple malware families. According to our research, this BAT loader is being utilised by OneNote Attachment, which spreads through spam emails. The infection techniques of the BAT loader and its payload delivery mechanism highlight its adaptability and challenges. This loader is known for employing malspam and social engineering tactics to gain access to target networks through batch and PowerShell scripts, making it a complicated threat to detect. Its ability to evolve and adapt makes the BAT loader a persistent and dangerous type of malware.

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/T1064/T1047/T1059 - Persistence T1053 - Privilege Escalation T1055 - Defence Evasion T1222/T1564/T1036 - Discovery T1082 - Command-and-Control T1071

3. Andariel APT

Andariel is a threat group that is also closely attributed to APT38 and Lazarus. A campaign from the APT group has been recently discovered. The group has utilised the exploitation of the Zimbra Mail vulnerability (CVE-2022-27925 and CVE-2022-37042). Upon initial exploitation, the threat actors installed tunnelling tools to create a connection to a second server that is directly connected to their Command-and-Control server.

Rules to detect the Zimbra Mail exploit that this APT group utilised, as well as the backdoor activity attributed to this APT group are deployed in the Crystal Eye.

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 T1190 - Execution T1059 - Persistence T1136/T1053 - Command-and-Control T1102

4. Fortra RCE CVE-2023-0669

Fortra has released a security advisory for a remote code execution vulnerability found in their GoAnywhere file transfer solution. The vulnerability lies in the Licensing component servlet. As of writing, there is no patch available, but Fortra has released steps on how to disable the licensing service. A network access level is also required for the exploit to work.

Crystal Eye has deployed rules to detect the required parameter for this traffic.

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: Attempted-admin
Kill Chain: Initial Access T1190

New Ransomware Victims Last Week: 39

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 39 new ransomware victim organisations from 16 different countries all over the world.

One particular ransomware group named LockBit3.0 tallied the greatest number of new victims (18), the locations of which are spread across different countries. This is followed by Play group that hit 6 new victims. Victim counts these ransomware groups, and a few others are listed below.

Name of Ransomware Group	No of new Victims last week
AlphV	3
Biianlian	4
BlackByte	1
LockBit3.0	18
Lorenz	1
Play	6
Ransomhouse	2
Royal	3
Vicesociety	1

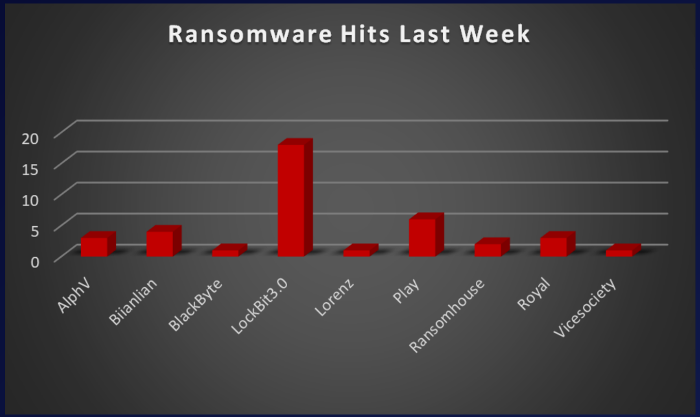


Figure 1: Ransomware Group Hits Last Week

If we look at the victims as per the country, we can say that the USA again became the most affected country by ransomware groups, where 21 new victims were reported last week. The number of new ransomware victims per country is listed below:

Name of the affected Country	Number of Victims
Afghanistan	1
Canada	1
Colombia	1
France	2
Germany	1
Indonesia	1
Italy	2
Jordan	1
Singapore	1
Spain	1
Switzerland	1
Taiwan	1
UAE	1
UK	2
USA	21
Vatican City	1

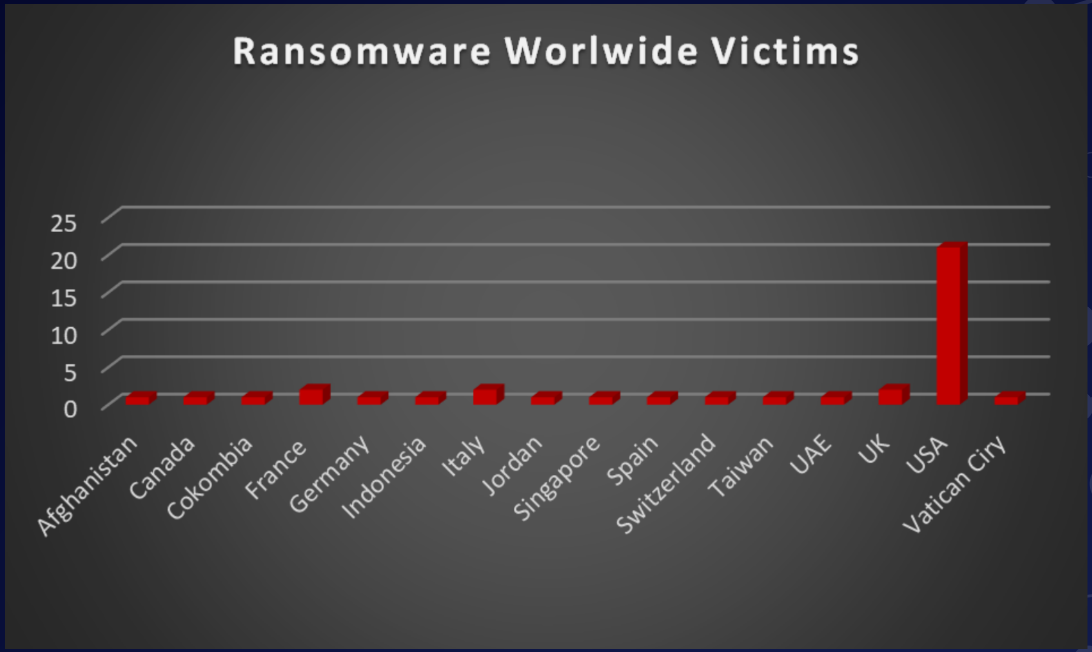


Figure 2: Ransomware Victims Worldwide

We conducted more research and discovered that 15 industries were affected globally by ransomware with the manufacturing and IT sectors being struck with the loss of 7 and 4 new businesses respectively just last week. The sector/industry of three new victims was not recognised. The following table lists the latest ransomware victims by sector:

Name of the affected Country	Number of Victims
Business Services	3
Construction	4
Education	3
Finance	2
Government	1
Healthcare	2
Hospitality	1
IT	4
Legal Services	1
Manufacturing	7
Media & Internet	1
Organisations	1
Real State	2
Retail	2
Transportation	2
Unknown	3

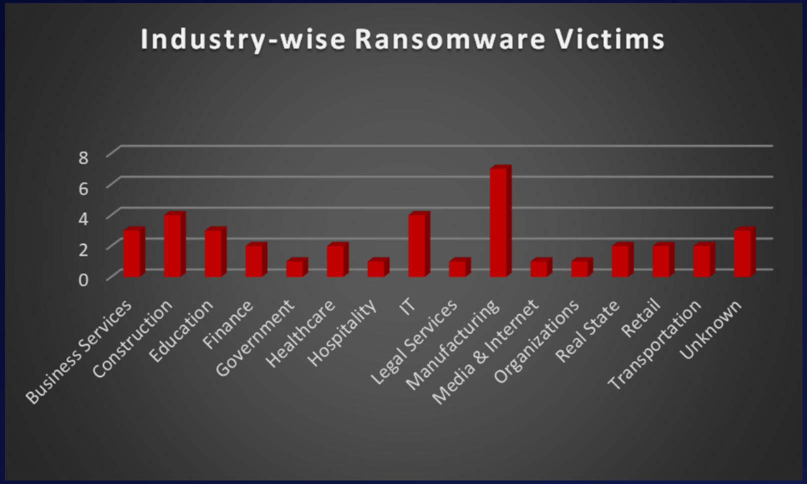


Figure 3: Industry-wise Ransomware Victims