
Red Piranha
unified threat management
THREAT INTELLIGENCE REPORT
Feb 21 - 27, 2023

Report Summary:

- **New Threat Detection Added** – 6 (DarkCloud Stealer, Qakbot malware, Orcus RAT, Doublezero Wiper Malware, OxtaRAT, and Clasiopa APT)
- **New Threat Protections**
- **Overall Weekly Observables Count**
- **Daily submissions by Observable Type**
- **New Ransomware Victims Last Week**

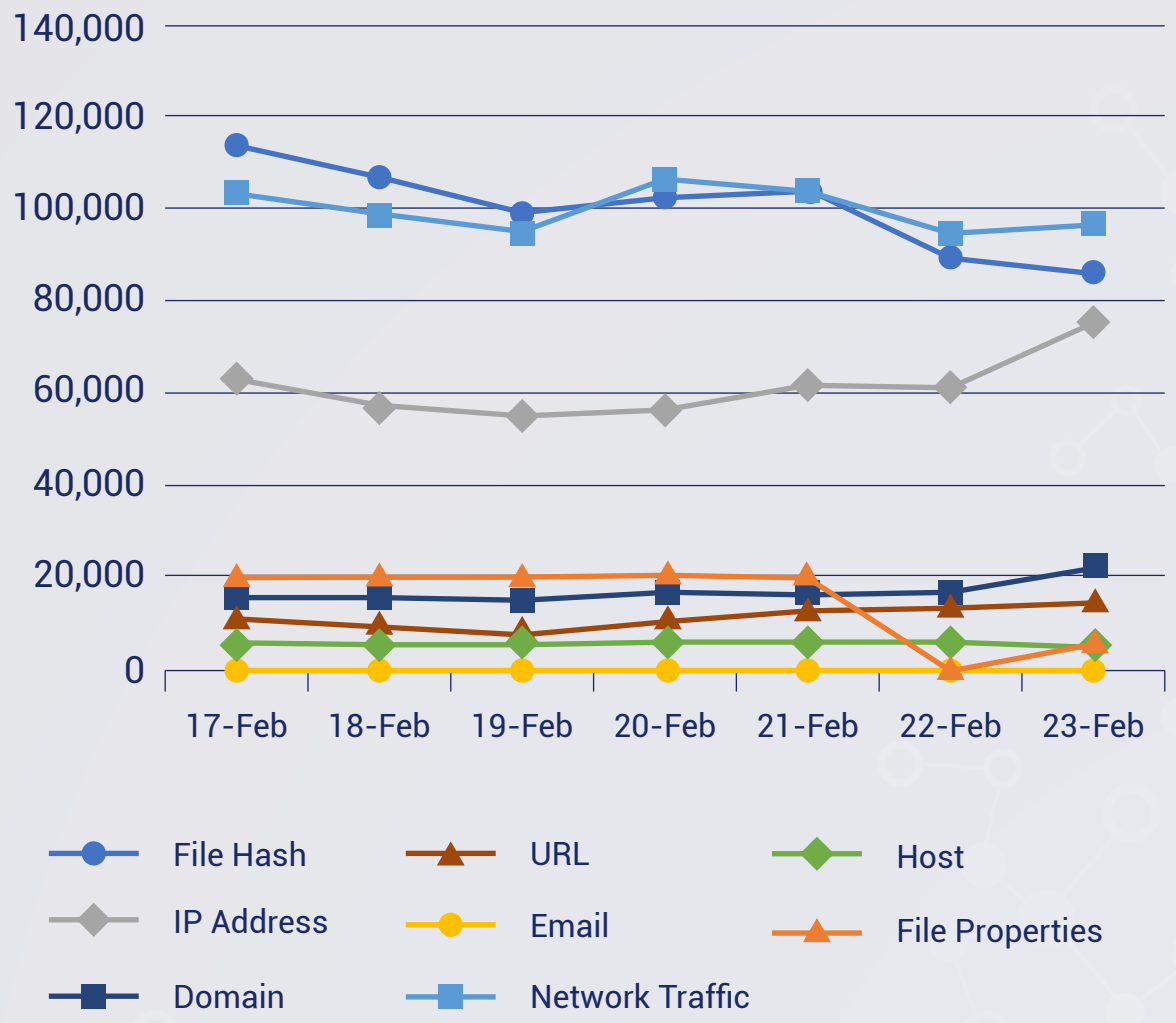
New Threat Protections (Week Ending 27/02/2023):

8

Overall Weekly Observables Count:

2,134,944

Daily Submissions by Observable Type:



Newly Detected Threats Added

1. DarkCloud Stealer

Throughout 2023, there have been reports of the DarkCloud Stealer appearing in numerous spam campaigns. This malware is capable of extracting sensitive data from compromised devices, such as credit card numbers, passwords, social security numbers, and other personal or financial information.

The DarkCloud Stealer operates through a multi-stage process that ultimately loads a final payload into the system's memory. Its data exfiltration capabilities are versatile and include the use of several communication channels, such as SMTP, Telegram, Web Panel, and FTP. Additionally, this advanced malware has the ability to customize its payload, enabling it to target different applications effectively and making it highly adaptable.

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 /T1053 - Persistence T1053 - Defence Evasion T1140 - Credential Access T1555/T1539/T1552/T1528 - Discovery T1087/T1518/T1057/T1007 - Command-and-ControlT1071

2. Qakbot malware

The Qakbot malware serves as a prime illustration of the ever-changing threat environment, emphasizing the criticality of maintaining a watchful eye in the cybersecurity realm. The malware's intricate architecture, far-reaching consequences, and pervasive prevalence stress the significance of taking pre-emptive and resilient security measures. The threat actors behind Qakbot exhibit considerable activity, frequently modifying their tactics to evade detection and increase their profits. They employ inventive attack methods such as OneNote attachments to showcase their level of sophistication and resourcefulness.

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: Initial Access T1566 - Execution T1204/T1059/T1218/T1059 - Defence Evasion T1140/T1564/T1055 - Credential Access T1555/T1056 - Discovery T1087/T1518/T1057/T1007 - Collection T1113/T1115 - Command-and-Control 1071/T1105

3. Orcus RAT

Orcus RAT is a type of malicious software program that enables remote access and control of computers and networks. It is a type of Remote Access Trojan (RAT) that has been used by attackers to gain access to and control computers and networks. Once downloaded onto a computer or network, it begins to execute its malicious code, allowing the attacker to gain access and control. It can steal data, conduct surveillance, and launch DDoS attacks. The malware is usually spread via malicious emails, websites, and social engineering attacks. It is also often bundled with other malicious software programs, such as Trojans, worms, and viruses.

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: Trojan
Kill Chain: Execution TA0002 - Execution TA0002 - Persistence TA0003 - Privilege Escalation TA0004 - Defence Evasion TA0005 - Credential Access TA0006 - Discovery TA0007 - Command-and-Control TA0011

4. Doublezero Wiper Malware

Doublezero is a data wiper malware, which destroys files, registry keys, and trees on the Victim machine. The malware is written in the .net programming language. It has customized obfuscation and a huge amount of junk code that makes malware reverse engineering harder to analyse these codes fully. The malware first enumerates the list of domain controllers connected to the infected host. When the malware is executed, it first checks if the compromised machine is one of the domain controllers. If this host is one of the domain controllers, the malware will not be executed.

Threat Protected: 01
Rule Set Type:

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

Class Type: Malware
Kill Chain: Initial Access TA0001 - Execution TA0002 - Privilege Escalation TA0004 - Defence Evasion TA0005 - Discovery TA0007 - Impact TA0040

5. OxtaRAT

OxtaRAT is an AutoIt-based malware for remote access. It is capable of remotely controlling its victim machines, searching and exfiltrating files, recording videos through the webcam and desktop, port scanning and more. The latest campaign is observed to be targeting human rights organisations and independent media from Azerbaijan and Armenia. The malware is being distributed as a document which appears to have a political context in the region. Once, opened, it drops an executable which executes scripts to run AutoIt. AutoIt is used to execute a code hidden in the attached image. The code installs a web shell, contacts its C&C, and downloads/uploads files.

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: Trojan-Activity
Kill Chain: Initial Access T1566 - Execution T1059 - Persistence T1053 - Command-and-Control T1102

6. Clasiopa

Clasiopa is a threat actor group that is known to target materials research organisations in Asia. Evidence gathered from Clasiopa reveals that they mostly gain access to their victim networks via brute force attacks. Toolsets used by Clasiopa are mostly distinct and customized. These tools include Atharvan, a custom remote access trojan; Lilith, which is used for modifying system processes; Thumbsender, which lists file names on a victim machine and sends them out 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 T1059/T1053 - Defence Evasion T1562 - Command-and-Control T1102

New Ransomware Victims Last Week: 61

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 61 new ransomware victim organisations in 27 different countries all over the world.

One particular ransomware group named LockBit3.0 tallied the greatest number of new victims (27), the locations of which are spread across different countries. This is followed by AlphV groups who hit 18 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	18
Avoslocker	1
LockBit 3.0	27
Lorenz	1
Mallox	1
Medusa	3
Play	1
Ragnarlocker	1
Ransomexx	1
Ransomhouse	2
Royal	4
V is Vendetta	1

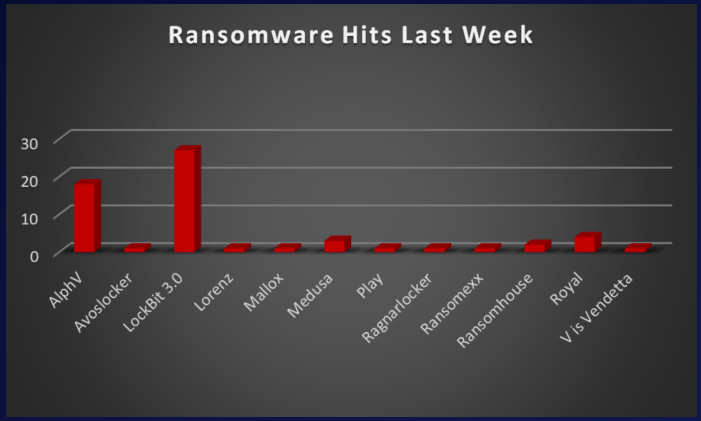


Figure 1: Ransomware Group Hits Last Week

If we look at the victims as per the country, we can say that the USA was once again the most affected country by ransomware groups where a total of 27 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
Argentina	1
Australia	1
Austria	1
Belgium	2
Bolivia	1
Brazil	4
Canada	4
China	1
Domingo	1
France	3
Germany	1
India	1
Indonesia	1
Iran	1
Italy	1
Mauritius	1
Mexico	1
Netherlands	1
New Zealand	1
Portugal	1
Taiwan	1
UK	4
USA	27

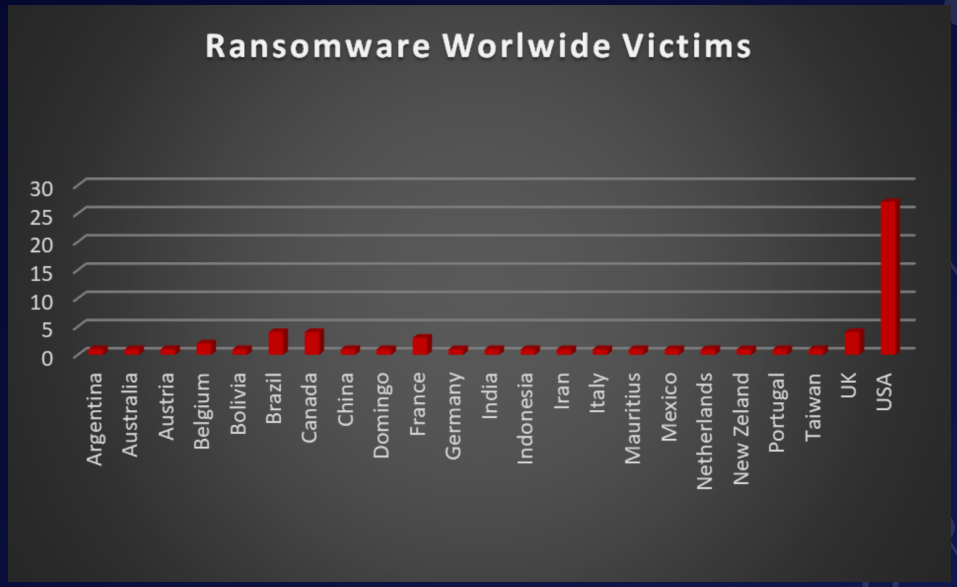


Figure 2: Ransomware Victims Worldwide

We conducted more research and discovered that 21 industries were affected globally by ransomware, with the manufacturing and Business Services sectors being struck with the loss of 11 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
Banking	2
Business Services	6
Construction	5
Consumer Services	2
Education	4
Electricity, Oil & Gas	2
Energy	1
Finance	1
Health Care	1
Hospitality	2
Insurance	2
IT	1
Legal Services	5
Manufacturing	11
Media & Internet	2
Organisations	4
Real State	2
Retail	3
Transportation	3
Unknown	1
Water Utility	1

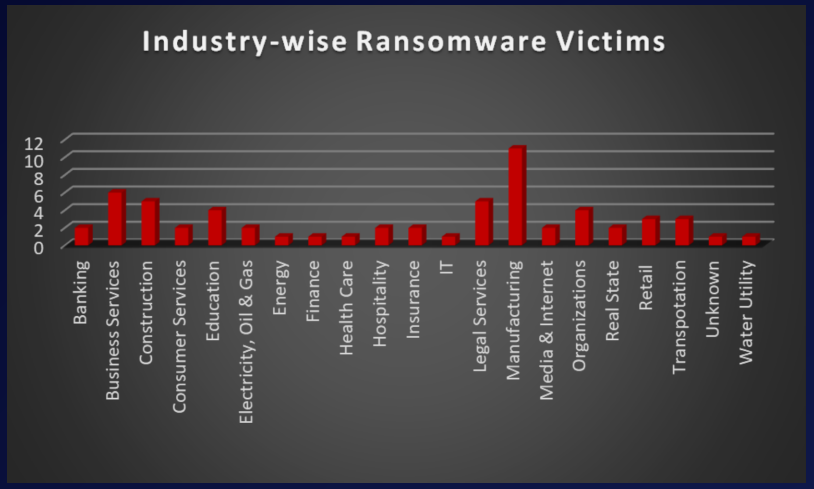


Figure 3: Industry-wise Ransomware Victims