
Red Piranha
unified threat management
THREAT INTELLIGENCE REPORT
Feb 14 - 20, 2023

Report Summary:

- **New Threat Detection Added** – 6 (Dalbit APT, Frebniis Backdoor, NewsPenguin, MalVirt malware, SparkRAT, and SHARPEXT)
- **New Threat Protections**
- **Overall Weekly Observables Count**
- **Daily submissions by Observable Type**
- **New Ransomware Victims Last Week**

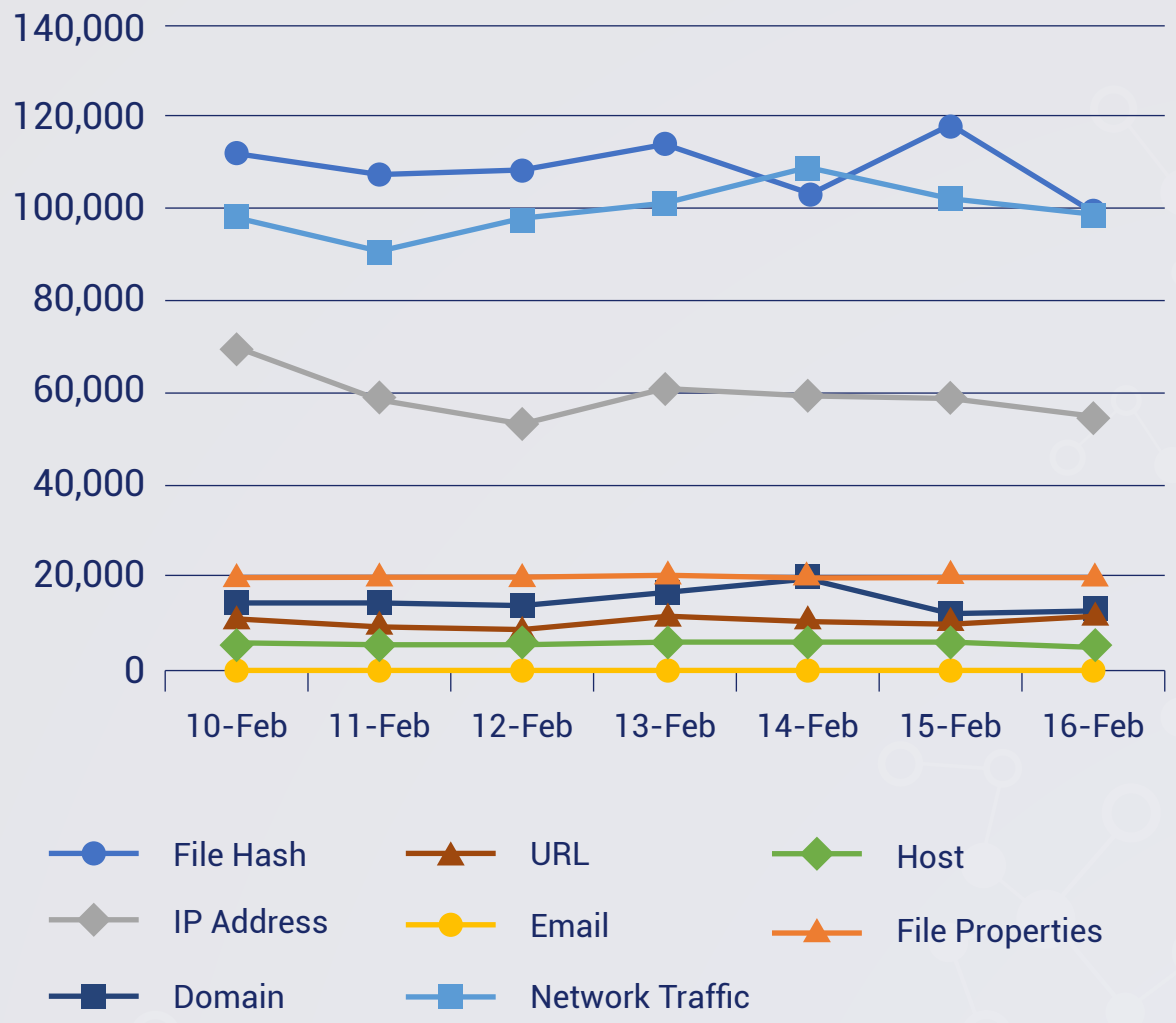
New Threat Protections (Week Ending 20/02/2023):

9

Overall Weekly Observables Count:

2,208,222

Daily Submissions by Observable Type:



Newly Detected Threats Added

1. Dalbit APT

Dalbit is a threat actor group recently discovered to have targeted Korean organisations. Their usual tactic is to target SQL and Web Servers with exploits to upload web shells. Through these web shells, additional tools such as binaries for privilege escalation, proxy tools, and scanning tools are downloaded. Upon initial foothold, FRP (Fast Reverse Proxy) is deployed to connect back to their Command-and-Control server or another victim's server via RDP. It appears that the end goal is to eventually deploy ransomware on their victims.

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 T1190 - Execution T1059 - Command-and-Control T1105

2. Frebniis Backdoor

Frebniis is a newly observed malware that abuses IIS to deploy a backdoor onto systems. The threat actor or group behind this is still unknown and no attribution has been made yet. Microsoft's IIS feature (iisfreb.dll) used to troubleshoot web requests is injected with a malicious code. This code allows the malware to monitor HTTP requests and recognize specially formatted HTTP requests allowing for remote code execution. However, the attacker needs to gain access to the actual target by other means.

Threat Protected: 02
Rule Set Type:

Class Type: Trojan- Activity
Kill Chain: Execution T1559/T1129

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

3. NewsPenguin

A new cyber threat actor, NewsPenguin, has been discovered targeting organisations in Pakistan using a sophisticated method of payload delivery. The attacker is using a targeted phishing campaign with a weaponized document, disguised as an exhibitor manual for the upcoming Pakistan International Maritime Expo & Conference (PIMEC-2023), to trick their victims. The document contains embedded malicious VBA macro code, which leads to the final payload execution. The final payload is an advanced espionage tool encrypted with a unique "penguin" encryption key.

Threat Protected: 02
Rule Set Type:

Class Type: Trojan-activity
Kill Chain: Initial Access T1566.001 - Execution T1204.002, T1059.005, T1059.003, T1203, T1047, T1059.001, T1559.001 - Privilege Escalation T1055, T1055.002- Defence Evasion T1480, T1221, T1027, T1140, T1070.004, T1564.001, T1221, T1112, T1036 - Command-and-Control T1105, T1071.001, T1132.001, T1573.001 - Exfiltration T1041, T1029 - Discovery 1083, T1057, T1082, T1497.003

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

4. MalVirt malware

Researchers have discovered a new cluster of virtualised malware loaders called MalVirt, which utilises the KoiVM virtualizing protector for obfuscating their implementation and execution. They distribute payloads that include the Formbook family of infostealer malware, with an unusual amount of applied anti-analysis and anti-detection techniques. The use of alternative malware distribution methods, such as malvertising and ISO files, is on the rise, as Office macros in documents from the Internet are blocked by Microsoft. The Formbook family is a feature-rich infostealer malware that is used by threat actors with cybercrime motivations but has also been observed in attacks with potentially political motivations. The intricate loader suggests an attempt to co-opt cybercriminal distribution methods to load more targeted second-stage malware onto specific victims after initial validation.

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: aT1543.003/T1547.001/T1547.008/T1574.002 - Privilege Escalation T1055/T1543.003 /T1547.001 - Defence Evasion T1112/T1497 - Credential Access T1003/T1056 - Discovery T1012/T1057 - Collection T1005/T1056/T1114 - Command-and-Control T1071/T1095

5. SparkRAT

A Chinese-speaking hacking group tracked as 'DragonSpark' was observed employing Golang source code interpretation to evade detection while launching espionage attacks against organisations in East Asia. It has been observed that the intrusion vector is vulnerable to MySQL database servers exposed online. The threat actors access vulnerable MySQL and web server endpoints by deploying web shells through SQL injection, cross-site scripting, or web server vulnerabilities. Then, the attackers deploy SparkRAT, a Golang-based open-source tool that can run on Windows, macOS, and Linux, offering feature-rich remote access functionality. SparkRAT uses the WebSocket protocol to communicate with the C2 server, and can automatically upgrade itself, constantly adding new features.

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
Kill Chain: Initial Access T1566.001- Execution T1204.002 – Command-and-Control T1071 - Impact T1565

6. SHARPEXT

SHARPEXT is a malicious browser extension deployed by SharpTongue following the successful compromise of a target system. In the first versions of SHARPEXT investigated by Volexity, the malware only supported Google Chrome. The latest version (3.0 based on the internal versioning) supports three browsers:

Chrome, Edge, Whale

Prior to deploying SHARPEXT, the attacker manually exfiltrates the files required to install the extension (explained below) from the infected workstation. SHARPEXT is then manually installed by an attacker-written VBS script.

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 - Execution T1204 – Command-and-Control T1071 - Impact T1565

New Ransomware Victims Last Week: 84

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 84 new ransomware victim organisations from 26 different countries all over the world.

One particular ransomware group named LockBit3.0 tallied the greatest number of new victims (38), the locations of which are spread across different countries. This is followed by Medusa groups who hit 14 new victims. Victim counts these ransomware groups, and a few others are listed below.

Name of Ransomware Group	No of new Victims last week
0mega	1
AlphV	5
Avoslocker	9
Bianlian	4
BlackByte	1
Daixin	1
LockBit3.0	38
Mallox	3
Medusa	14
Play	2
Ransomhouse	1
Royal	4
V is vendetta	1

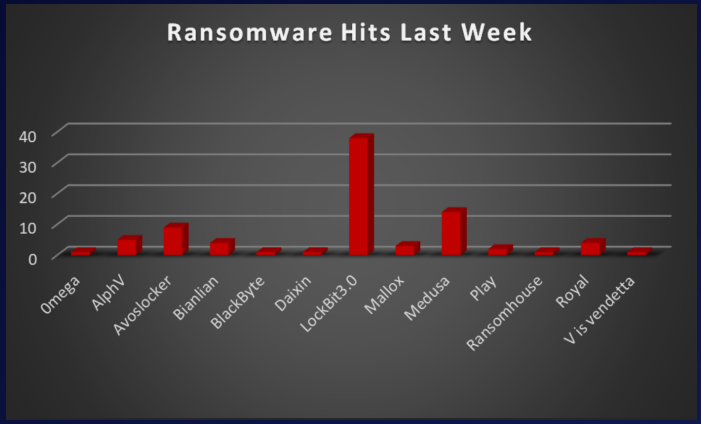


Figure 1: Ransomware Group Hits Last Week

If we look at the victims as per the country, we can say that the USA was once again become the most affected country by ransomware groups where a total of 41 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	4
Austria	1
California	1
Canada	5
France	3
Germany	1
India	2
Indonesia	1
Ireland	2
Italy	5
Korea	1
Malaysia	1
Mali	1
Netherlands	1
Pakistan	1
Singapore	1
Spain	1
Switzerland	2
Thailand	1
Tonga	1
UK	2
Uruguay	1
USA	41
Victoria	1
Vietnam	2

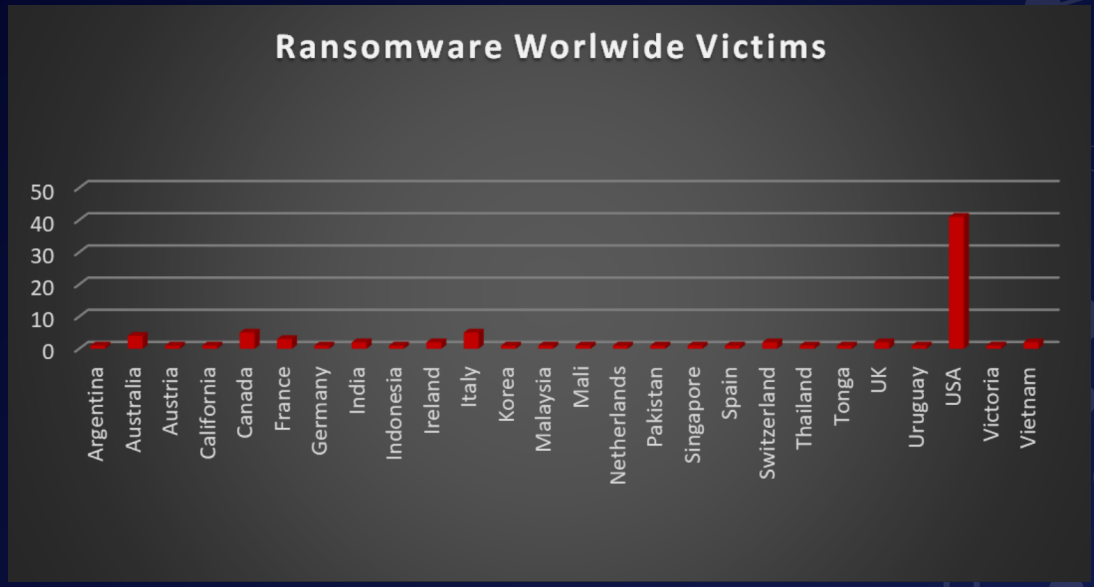


Figure 2: Ransomware Victims Worldwide

We conducted more research and discovered that 21 industries were affected globally by ransomware, with the manufacturing and Construction sectors being struck with the loss of 24 and 8 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	1
Business Services	8
Construction	8
Consumer Services	3
Education	2
Energy	4
Finance	2
Financial Services	1
Government	2
Health Care	6
Hospitality	4
Insurance	1
IT	1
Legal Services	2
Manufacturing	24
Mining	2
Organisation	1
Real States	3
Retail	5
Telecommunication	1
Transportation	3

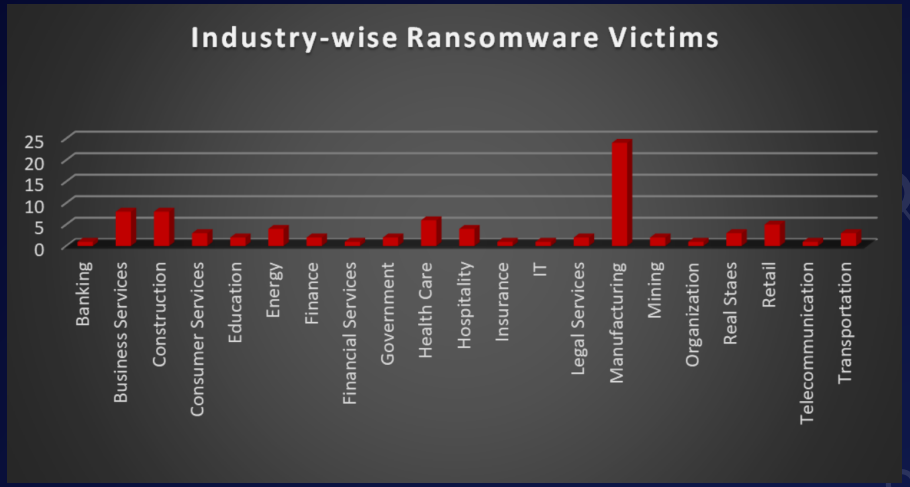


Figure 3: Industry-wise Ransomware Victims