Red Piranha
unified threat management

THREAT INTELLIGENCE REPORT

May 23 - 29, 2023

Report Summary:

- **New Threat Detection Added** – 4 (SharpPanda APT, Invicta Stealer, SeroXen RAT, and Fanxgiao)
- **New Threat Protections**
- **Overall Weekly Observables Count**
- **Daily submissions by Observable Type**
- **New Ransomware Victims Last Week - 66**

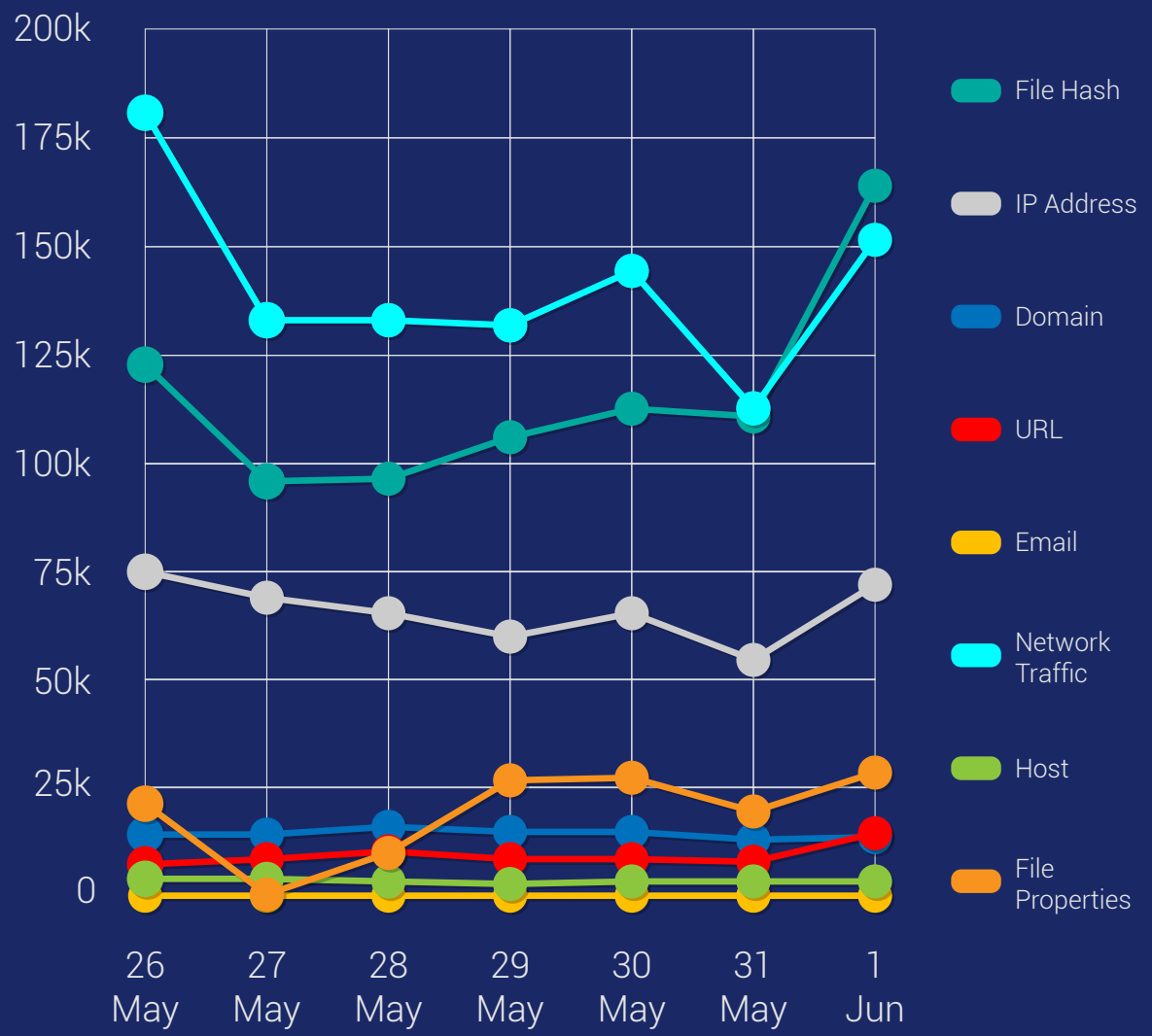
New Threat Protections (Week Ending 05/06/2023):

6

Overall Weekly Observables Count:

2,168,277

Daily Submissions by Observable Type:



Newly Detected Threats Added

1. SharpPanda APT

The SharpPanda APT group comprises exceptionally sophisticated cyber threat actors who carry out targeted and prolonged attacks against specific entities, including governments, organisations, and industries. Their objectives encompass espionage, disruption, and financial gain. SharpPanda has been linked to multiple cyber espionage campaigns, employing tactics such as spear-phishing, social engineering manipulation, and exploiting zero-day vulnerabilities to illicitly access networks.

Previously, the group primarily targeted government officials, particularly in Southeast Asian countries. However, as evidenced in their recent campaign, they have shifted their focus to high-level government officials from G20 countries across Europe, North America, and South Asia. This APT group consistently adapts its techniques and incorporates new tools into its arsenal as it evolves.

Threat Protected: 01
Rule Set Type:

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

Class Type: Trojan-activity
Kill Chain: Initial Access T1566 - Execution T1204/T1203 - PersistenceT1053 - Defence Evasion T1497/T1027 - Discovery T1082/T1518/T1016 - Collection T1006 - Command-and-Control - T1065/T1071/T1105

2. Invicta Stealer

We have recently encountered a new type of malware called Invicta Stealer, which has caught our attention due to the activities of its developer on social media platforms. The developer actively promotes this information-stealing malware and highlights its dangerous capabilities. In the current landscape, there is a growing trend among malware developers to create and offer various types of stealers to potential buyers and affiliates. Among these, Invicta Stealer stands out as an exceptionally formidable threat. Its unique strength lies in its ability to target a wide range of highly sensitive information found in numerous applications and web browsers. The stolen data can be exploited by attackers for financial gains or to launch further attacks on individuals and organisations by taking advantage of the compromised information. It is crucial to recognise the severity of this threat and take appropriate measures to safeguard against such malicious activities.

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 - Defence Evasion T1027 - Credential Access T1528/T1555 - Discovery T1010/T1083 - Collection T1005 - Command-and-Control T1071

3. SeroXen RAT

A fileless RAT dubbed SeroXen has become the preferred tool for cybercriminals to target gamers. It has excellent detection evasion capabilities on static and dynamic analysis. Based on a combination of different open-source projects, including r77-rootkit, Quasar RAT, and NirCmd, its capabilities get further enhanced, making it a powerful RAT. The delivery of the RAT takes place through RAT is delivered either via phishing emails or Discord channels. SeroXen RAT is a sophisticated Remote Access Trojan that boasts several powerful features. It is designed to remain undetected by antivirus software, providing fully undetectable functionality both during scanning and while running. It includes features like HVNC (Hidden Virtual Network Computing), primarily used for penetration testing, LOTL (Living Off the Land) techniques to operate in a fileless manner, and a rootkit to conceal its presence.

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 TA0002 - Persistence TA0003 - Privilege Escalation TA0004 - Defence Evasion TA0005 - Discovery TA0007

4. Fanxgiao

Fanxgiao uses various strategies to maintain anonymity: most of its infrastructure is protected behind CloudFlare, and domain names are changed regularly and quickly. Users arrive at a Fangxiao-controlled site through a link sent in a WhatsApp message, which in turn sends them to a landing domain impersonating a well-known, trusted brand. Companies affected include Emirates, Singapore's Shopee, Unilever, Indonesia's Indomie, Coca-Cola, McDonald's and Knorr.

Victims are then redirected to a main survey domain. When they click the link, they are sent through a series of advertising sites to one of a set of constantly changing destinations. A click on the "Complete registration" button with an Android user-agent will sometimes result in a download of the Triada malware. As victims are invested in the scam, keen to get their "reward," and the site tells them to download the app, this has likely resulted in a significant number of infections.

Threat Protected: 03
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: Command-and-Control TA0011/ T1071/T1571/ T1573

Known exploited vulnerabilities (Week 1 June 2023):

Vulnerability	Description
CVE-2023-34362	MOVEit Transfer – SQL Injection
CVE-2023-28771	Zyxel – Command Injection vulnerabilities on multiple firewall products

Updated Malware Signatures (Week 1 June 2023)

Threat	Description
Qakbot	A malware designed to acquire valuable data such as banking credentials and is also capable of stealing FTP credentials and spreading across a network by utilising SMB.
Tofsee	A malware that is used to send spam emails, and conduct click frauds as well as cryptomining
Glupteba	A malware dropper that is designed to download additional malware on an infected machine.
Upatre	A malware dropper that downloads additional malware on an infected machine. It is usually observed to drop banking trojan after the initial infection.
Bifrost	A remote access trojan that enables its operator to take control of a victim machine and steal data. It is usually distributed through spam and phishing emails.
DarkKomet	A remote access trojan that can take full control over an infected machine.

New Ransomware Victims Last Week: 66

Red Piranha proactively gathers information about organisations impacted by ransomware attacks through various channels, including the Dark Web. In the past week, our team identified a total of 66 new ransomware victims from 18 distinct industries across 21 countries worldwide. This highlights the global reach and indiscriminate nature of ransomware attacks, which can affect organisations of all sizes and sectors.

Lockbit3, a specific ransomware, has affected the largest number of new victims (16) spread across various countries. Play and Royal groups follow closely with each hitting 11 and 10 new victims respectively. Below are the victim counts (%) for these ransomware groups and a few others.

Name of Ransomware Group	Percentage of new Victims last week
8base	1.52%
Akira	10.61%
AlphaV	4.55%
Bianlian	3.03%
Blackbasta	1.52%
Darkrace	3.03%
Lockbit3	24.24%
Medusa	3.03%
Monti	1.52%
Play	16.67%
RA Group	7.58%
Ragnarlocker	1.52%
Ransomhouse	1.52%
Royal	15.15%
Trigona	3.03%
Vicesociety	1.52%

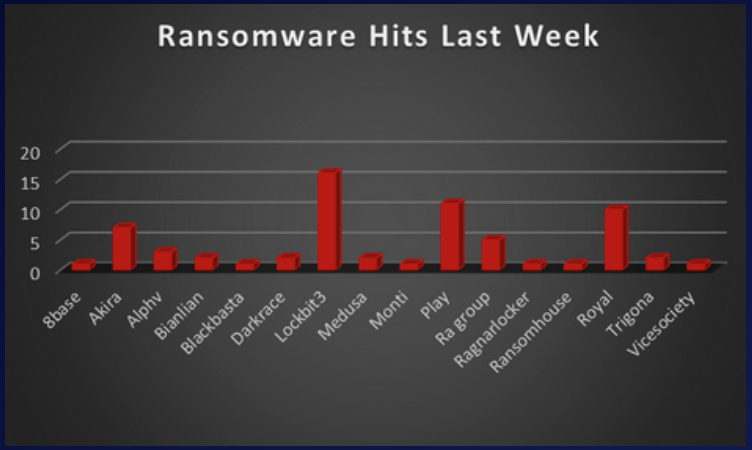


Figure 1: Ransomware Group Hits Last Week

When we examine the victims by country out of 21 countries around the world, we can conclude that the USA was once again the most ransomware-affected country, with a total of 31 new victims reported last week. The list below displays the number (%) of new ransomware victims per country.

Name of the affected Country	Number of Victims
Argentina	1.52%
Australia	1.52%
Austria	1.52%
Canada	10.61%
Colombia	3.03%
Czech Republic	3.03%
Denmark	1.52%
France	3.03%
Germany	1.52%
Italy	3.03%
Japan	3.03%
Korea	1.52%
Netherlands	1.52%
Paraguay	1.52%
Spain	1.52%
Sweden	1.52%
Switzerland	1.52%
Taiwan	1.52%
Turkey	1.52%
UK	7.58%
USA	46.97%

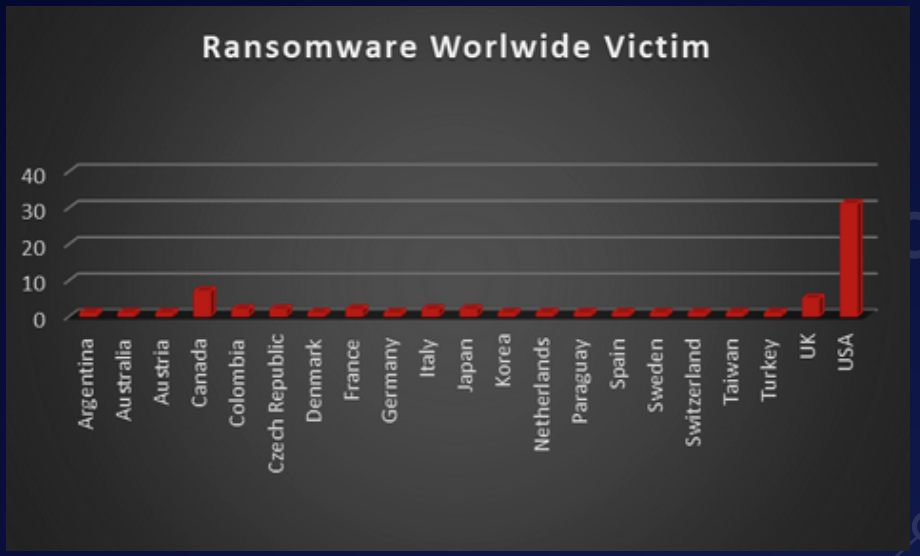


Figure 2: Ransomware Victims Worldwide

After conducting additional research, we found that ransomware has impacted 18 industries globally. Last week, the Manufacturing and Business Services sectors were hit particularly hard, with the loss of 14 and 09 businesses in each sector respectively. The table below presents the most recent ransomware victims sorted by industry.

Industry	Victims Count (%)
Business Services	13.64%
Construction	6.06
Consumer Services	1.52%
Education	6.06%
Energy	1.52%
Finance	10.61%
Government	1.52%
Healthcare	1.52%
Hospitality	3.03%
Insurance	1.52%
IT	7.58%
Legal Services	3.03%
Manufacturing	21.21%
Media	1.52%
Organisations	3.03%
Real Estate	4.55%
Retail	7.58%
Transportation	4.55%

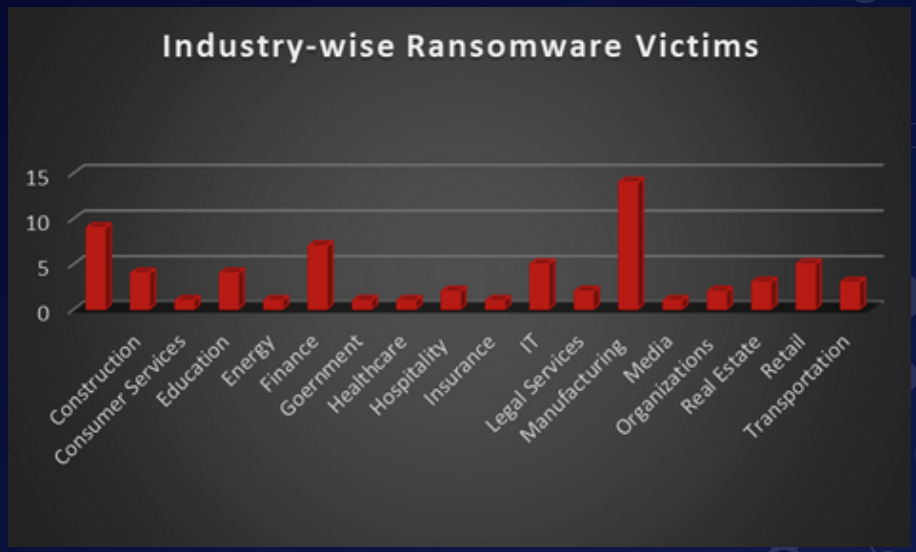


Figure 3: Industry-wise Ransomware Victims