Red Piranha
unified threat management

THREAT INTELLIGENCE REPORT

May 16 - 22, 2023

Report Summary:

- **New Threat Detection Added** – 5 (AndoryuBot, BlackSuit Ransomware, FSB Snake Malware, Symbiote, and PingPull Linux Variant)
- **New Threat Protections**
- **Overall Weekly Observables Count**
- **Daily submissions by Observable Type**
- **New Ransomware Victims Last Week - 48**

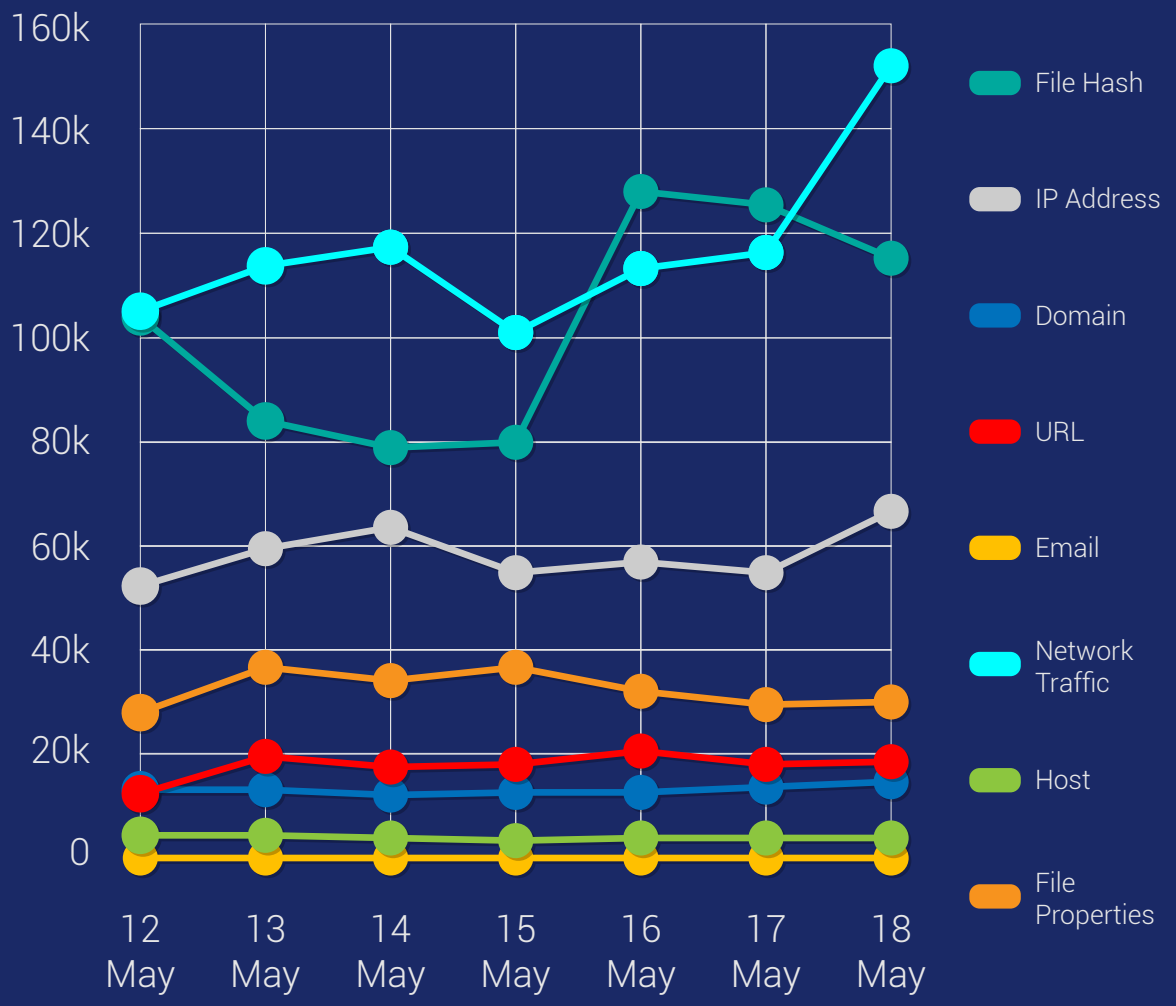
New Threat Protections (Week Ending 22/05/2023):

11

Overall Weekly Observables Count:

2,401,904

Daily Submissions by Observable Type:



Newly Detected Threats Added

1. AndoryuBot

Researchers have identified the active exploitation of CVE-2023-25717 and the deployment of a botnet called AndoryuBot, signalling that Threat Actors (TAs) are actively searching for vulnerable Ruckus assets to exploit. This vulnerability has a publicly available Proof of Concept (POC), indicating that TAs are likely to exploit it extensively. Fortinet released a blog on May 8th, 2023, confirming the distribution of AndoryuBot through the Ruckus vulnerability. On May 15th, 2023, the Cybersecurity, and Infrastructure Agency (CISA) included CVE-2023-25717 in their Known Exploited Vulnerability catalogue.

AndoryuBot is a new Botnet malware being sold on Telegram through a subscription model. TAs employ this malware to orchestrate large-scale distributed denial-of-service (DDoS) attacks, overwhelming targeted servers and infrastructure by inundating them with a high volume of traffic. Ruckus specializes in providing widely used networking solutions and services. However, the prevalence of these networking products has attracted the attention of TAs who actively exploit vulnerabilities for malicious purposes.

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: Execution T1059 - Defence Evasion T1140/T1480/T1036 - Privilege Escalation T1055 - Command-and-Control T1095

2. BlackSuit Ransomware

The rise in Linux-based ransomware groups, including Cylance and Royal ransomware, is directly linked to the extensive use of Linux as an operating system in various sectors, including enterprise environments and cloud computing platforms. The widespread adoption of Linux makes it an attractive target for ransomware groups, as a single attack can potentially compromise numerous systems.

Recently, researchers discovered a new ransomware group called BlackSuit. BlackSuit ransomware is designed to target users of both Windows and Linux operating systems. Researchers have observed that the code of the Linux variant of BlackSuit shares similarities with the Royal ransomware. It communicates with victims through an Onion site and, as of now, has not publicly disclosed any information about its victims.

Threat Protected: 01
Rule Set Type:

Class Type: Trojan- Activity
Kill Chain: Execution T1204/T1059 - Discovery T1057/T1082/T1083 - Impact T1486/T1490

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

3. FSB Snake Malware

A recently exposed malware from Russia's FSB. It is used for cyber espionage campaigns against various sensitive targets across 50 countries in Europe, Africa, Asia, Australia, North, and South America. The Snake malware targets sensitive intelligence information from high-priority targets such as research facilities, government organisations, journalists, critical infrastructure, and telecommunications among others. It created its own Peer-to-peer network of Snake implants which share all the information collected from their targets.

Threat Protected: 06
Rule Set Type:

Class Type: Trojan- Activity
Kill Chain: Initial Access T1566/T1078/T1190 - Execution T1059/T1569/T1106 - Persistence T1078/T1055/T1547 - Credential Access T1557/T1555 - Discovery T1087/T1040/T1135/T1518 - Command-and-Control T1001/T1573/T1071

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

4. Symbiote

A New, Nearly-Impossible-to-Detect Linux Threat termed Symbiote has been observed in the wild. The malware after infecting its target machine, hides itself and any other malware used by the threat actor. Live forensics of the infected machine might not be effective since all the files, processes, and network artefacts are hidden by the malware. The malware provides a backdoor for the threat actor, a rootkit facility, and the option to execute commands with the highest privileges. The packet capture tool on the infected machine is redundant as BPF bytecode is injected into the kernel that defines which packets should be captured. Symbiote adds its bytecode first so it can filter out network traffic that it does not want the packet-capturing software to see.

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: Malware
Kill Chain: Persistence TA0003 - Privilege Escalation TA0004 - Defence Evasion TA0005 - Discovery TA0007 - Command-and-Control TA0011

5. PingPull Linux Variant

Hackers are deploying new Linux malware variants in cyberespionage attacks, known as PingPull. PingPull is a Remote Access Trojan first used by the group Gallium, also known as Alloy Taurus. Upon execution, the malware is configured to communicate with the C2 domain over port 8443. It uses a statically linked OpenSSL (OpenSSL 0.9.8e) library to interact with the domain over HTTPS. The payload after running the command, will send the results back to the C2 server via an HTTPS request that resembles the beacon request but contains Base64 encoded ciphertext. The command handler supports functionality such as reading/writing files and folders, traversing through the directory and running commands.

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

Known exploited vulnerabilities (Week 3 May 2023):

Vulnerability	Description
CVE-2023-21492	Android ASLR Bypass – Memory-based vulnerability
CVE-2016-6415	Cisco IOS – Internet Key Exchange information disclosure vulnerability
CVE-2004-1464	Cisco IOS Telnet, SSH, and HTTP Denial-of-Service

Updated Malware Signatures (Week 3 May 2023)

Threat	Description
Kuluoz	A backdoor for a botnet. It executes commands from a remote malicious user.
Upatre	Upatre is also a malware dropper that downloads additional malware on an infected machine. It is usually observed to drop banking trojan after the initial infection.
Glupteba	A malware dropper that is designed to download additional malware on an infected machine.
PlasmaRAT	A remote access trojan designed for conducting denial-of-service attacks, cryptomining, and keylogging. Its source code is publicly available and has been leveraged by different threat groups.
Valyria	This Microsoft Word-based malware is used as a dropper for second-stage malware.
Razy	A stealer malware that collects sensitive information from victim machines, encrypts it and exfiltrates it to its Command-and-Control server.

New Ransomware Victims Last Week: 48

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 48 new ransomware victims from 20 distinct industries across 23 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. Alphv and Trigona groups follow closely with each hitting 10 and 04 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
Abyss-data	2.08%
Alphv	20.83%
Bianlian	2.08%
Blackbasta	2.08%
Blackbyte	2.08%
arakurt	2.08%
Lockbit3	33.33%
Malas	6.25%
Medusa	6.25%
Money message	2.08%
Play	2.08%
Ragnarlocker	2.08%
Royal	4.17%
Snatch	2.08%
Trigona	8.33%
Vicesociety	2.08%

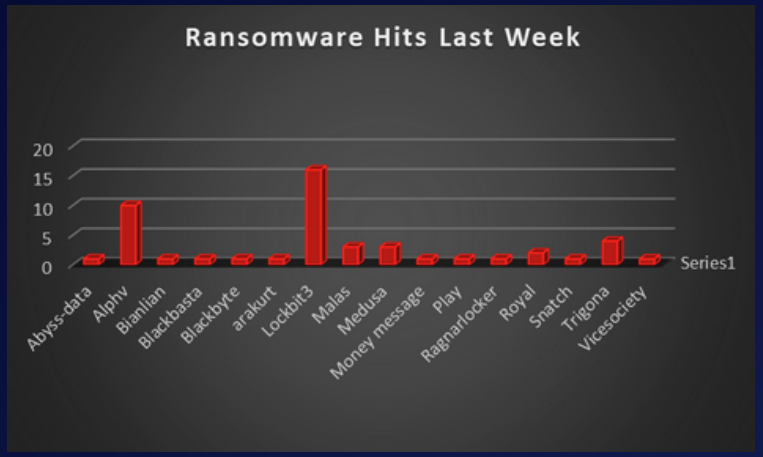


Figure 1: Ransomware Group Hits Last Week

When we examine the victims by country out of 23 countries around the world, we can conclude that the USA was once again the most ransomware-affected country, with a total of 19 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
Angola	2.08%
Argentina	2.08%
Canada	2.08%
China	2.08%
Colombia	2.08%
Czech Republic	2.08%
Finland	2.08%
Germany	4.17%
India	2.08%
Indonesia	4.17%
Italy	2.08%
Korea	2.08%
Macedonia	2.08%
Malaysia	2.08%
Mexico	4.17%
Philippines	2.08%
Russia	2.08%
South Africa	2.08%
Spain	6.25%
Taiwan	2.08%
UK	6.25%
USA	39.58%

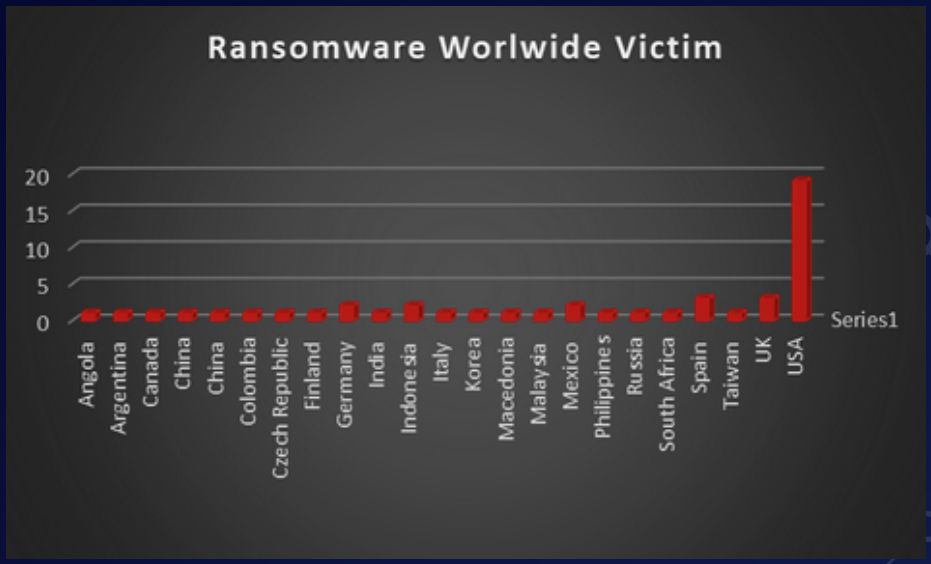


Figure 2: Ransomware Victims Worldwide

After conducting additional research, we found that ransomware has impacted 20 industries globally. Last week, the Manufacturing and Business Services sectors were hit particularly hard, with the loss of 10 and 06 businesses in each sector respectively. The table below presents the most recent ransomware victims sorted by industry.

Industry	Victims Count (%)
Agriculture	2.08%
Business Services	12.50%
Construction	2.08%
Consumer Services	2.08%
Education	6.25%
Energy	6.25%
Finance	6.25%
Healthcare	8.33%
Hospitality	2.08%
Insurance	4.17%
IT	2.08%
Manufacturing	20.83%
Media & Internet	2.08%
Metals & Mining	2.08%
Minerals & Mining	2.08%
Organisations	2.08%
Real Estate	2.08%
Retail	4.17%
Telecommunications	8.33%
Transportation	2.08%

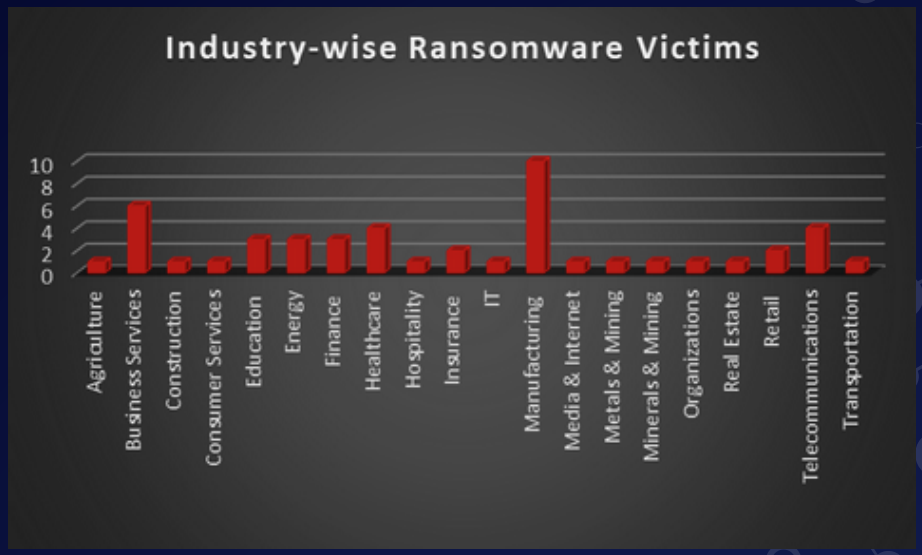


Figure 3: Industry-wise Ransomware Victims