Red Piranha
unified threat management

THREAT INTELLIGENCE REPORT

June 27 - July 03, 2023

Report Summary:

- **New Threat Detection Added** – 4 (Akira Ransomware, Wagner Ransomware, EarlyRAT, and Warzone RAT)
- **New Threat Protections**
- **New Ransomware Victims Last Week - 89**

Newly Detected Threats Added

1. Akira Ransomware

Researchers have recently unveiled significant insights into the operations of a newly discovered ransomware group called "Akira." This group is actively engaging in a relentless pursuit of various organisations, compromising their invaluable data. Notably, Akira ransomware has broadened its scope to encompass the Linux platform. Since its emergence in April 2023, Akira ransomware has already infiltrated and victimised 46 entities that have been publicly disclosed, with an additional 30 victims identified subsequent to our previous blog post. The majority of these victims are situated in the United States. Akira ransomware has targeted a diverse array of industries, spanning Education, Banking, Financial Services and Insurance (BFSI), Manufacturing, Professional Services, and others. Initially focusing on Windows systems, Akira ransomware has now expanded its repertoire to include Linux platforms. This strategic shift exemplifies an emerging trend among ransomware groups, indicating an imminent upsurge in assaults aimed at Linux environments. The fact that a formerly Windows-centric ransomware group has redirected its focus towards Linux highlights the growing vulnerability of these systems to cyber threats.

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

2. Wagner Ransomware

A new ransomware variant known as Wagner has emerged in the cybersecurity landscape, believed to be a derivative of the Chaos ransomware. What sets this ransomware apart is its ransom note, which deviates from the usual demand for money and instead encourages users to join the PMC Wagner.

The ransom note intriguingly begins with the phrase "Official Wagner PMCs Employment Virus." PMC Wagner refers to the Wagner Group, a Russian paramilitary organisation recognised as a private military company consisting of mercenaries. The ransomware sample was initially submitted from Russia, and the ransom note itself is written in Russian, indicating a possible focus on targets within Russia. The intentions of this ransomware appear to be centred around spreading messages of rebellion and incitement against the Russian authorities.

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 - Persistence T1547 - Discovery T1082/T1083/T1057 - Impact T1486 /T1490

3. EarlyRAT

EarlyRAT is a remote access trojan (RAT) that has emerged as a sophisticated and stealthy malware threat. Initially identified in 2020, EarlyRAT is designed to infiltrate systems and gain unauthorised access, enabling attackers to remotely control infected machines and steal sensitive information. Known for its advanced evasion techniques and modular architecture, EarlyRAT poses a significant risk to organisations and individuals, highlighting the need for robust cybersecurity measures to detect, prevent, and mitigate its impact.

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: Malware
Kill Chain: Reconnaissance T1590 - Weaponisation T1588 - Delivery T1566 Exploitation T1203 - Installation T1059 – Command-and-Control T1090 - Lateral Movement T1071 - Data Exfiltration T1041 - Persistence T1060 - Evasion T1027

4. Warzone RAT

Warzone RAT is a remote access trojan (RAT) that has gained notoriety for its potent capabilities and malicious intent. Operating stealthily in the background, Warzone RAT infiltrates systems undetected and establishes a covert connection between the attacker and the compromised machine. By providing remote control access, Warzone RAT enables threat actors to execute malicious commands, exfiltrate sensitive data, and carry out various malicious activities, making it a significant cybersecurity threat. Its advanced features and evasive techniques highlight the critical need for robust security measures to protect against such sophisticated RAT attacks.

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: Reconnaissance T1590 - Weaponisation T1588 - Delivery T1566 - Exploitation T1203 - Installation T1059 - Command-and-Control T1090 - Lateral Movement T1071 - Collection T1119 - Exfiltration T1048 - Impact T1499

Known exploited vulnerabilities (Week 5 June 2023):

Vulnerability	Description
CVE-2021-25372	Samsung Mobile Devices Improper Boundary Check Vulnerability
CVE-2021-25371	Samsung Mobile Devices Unspecified Vulnerability
CVE-2021-25395	Samsung Mobile Devices Race Condition Vulnerability
CVE-2021-25394	Samsung Mobile Devices Race Condition Vulnerability
CVE-2021-25489	Samsung Mobile Devices Improper Input Validation Vulnerability
CVE-2021-25487	Samsung Mobile Devices Out-of-Bounds Read Vulnerability
CVE-2019-20500	D-Link DWL-2600AP Access Point Command Injection Vulnerability
CVE-2019-17621	D-Link DIR-859 Router Command Execution Vulnerability

Updated Malware Signatures (Week 5 June 2023)

Threat	Description
Kuluoz	A backdoor for a botnet. It executes commands from a remote malicious user.
Tofsee	A malware that is used to send spam emails, conduct click frauds as well as cryptomining.
XtremeRAT	A remote access trojan interacts with the infected machine via a remote shell, uploads/downloads files, and records from a webcam/microphone.
Zeus	Also known as Zbot and is primarily designed to steal banking credentials.
Valyria	A Microsoft Word-based malware which is used as a dropper for second stage malware.

New Ransomware Victims Last Week: 89

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 89 new ransomware victims from 21 distinct industries across 34 countries worldwide. This highlights the global reach and indiscriminate nature of ransomware attacks, which can affect organisations of all sizes and sectors.

Clop, a specific ransomware, has affected the largest number of new victims (33) spread across various countries. Akira and 8base groups follow closely with each hitting 11 and 7 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	7.87%
Akira	12.36%
Alphv	4.49%
Bianlian	5.62%
Blackbasta	3.37%
Clop	37.08%
Karakurt	3.37%
Lockbit3	3.37%
Mallox	3.37%
Medusa	2.25%
Play	4.49%
Ra group	2.25%
Ransomexx	1.12%
Ransomware blog	3.37%
Rhysida	5.62

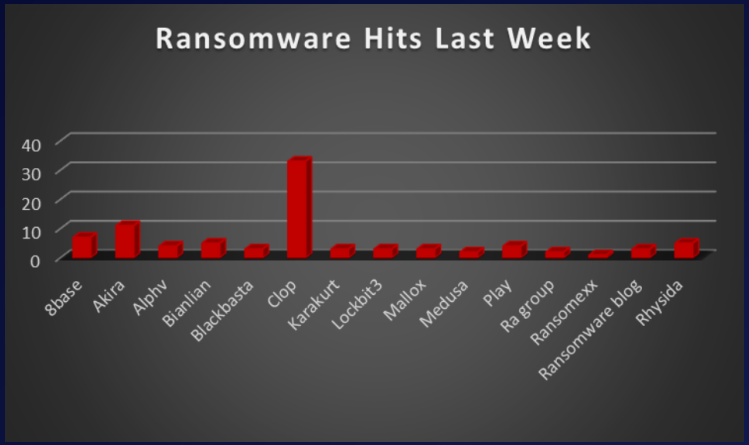

Figure 1: Ransomware Group Hits Last Week

When we examine the victims by country out of 34 countries around the world, we can conclude that the USA was once again the most ransomware affected country, with a total of 45 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
Australia	2.25%
Bahamas	2.25%
Bermuda	1.12%
Canada	4.49%
Egypt	1.12%
France	2.25%
Germany	4.49%
Hungary	1.12%
India	3.37%
Ireland	1.12%
Israel	1.12%
Italy	4.49%
Japan	1.12%
Korea	1.12%
Netherlands	1.12%
Portugal	1.12%
Serbia	1.12%
Singapore	1.12%
Slovakia	1.12%
South Africa	1.12%
Spain	1.12%
Switzerland	1.12%
Taiwan	1.12%
Thailand	2.25%
UK	5.62%
USA	50.56%

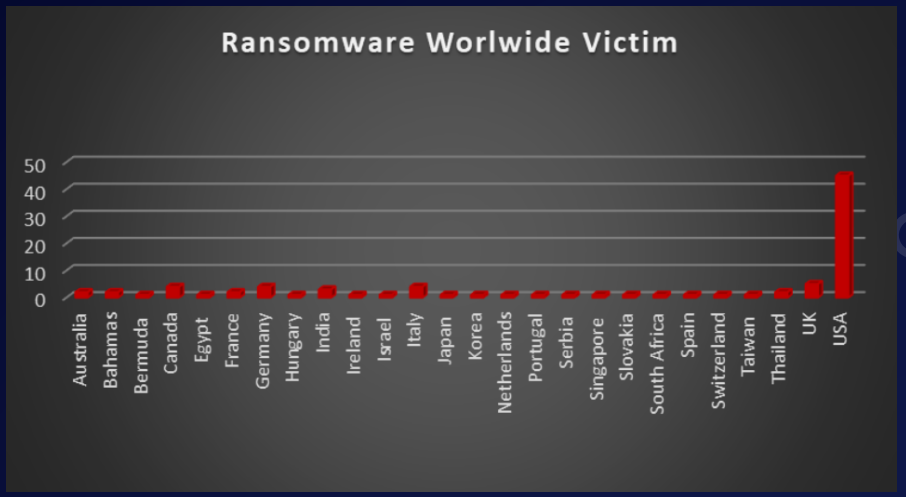

Figure 2: Ransomware Victims Worldwide

After conducting additional research, we found that ransomware has impacted 21 industries globally. Last week, the Business Services and Insurance sectors were hit particularly hard, with the loss of 11 and 10 businesses in each sector respectively. The table below presents the most recent ransomware victims sorted by industry.

Industry	Victims Count (%)
Business Services	12.36%
Construction	5.62%
Education	7.87%
Electronics	2.25%
Energy	1.12%
Finance	6.74%
Healthcare	4.49%
Holding Companies	1.12%
Hospitality	5.62%
Insurance	11.24%
IT	5.62%
Legal Services	5.62%
Manufacturing	10.11%
Media	1.12%
Real Estate	1.12%
Retail	6.74%
Telecommunications	3.37%
Transportation	7.87%

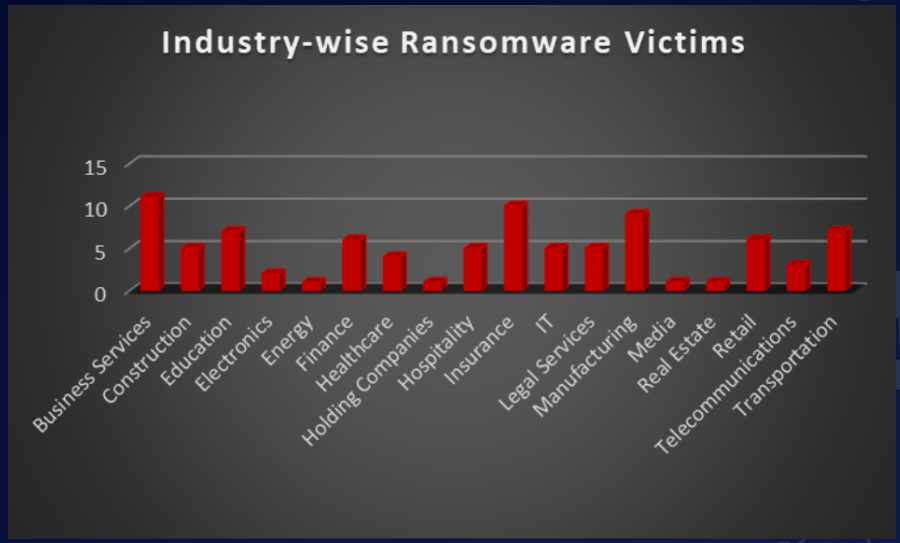

Figure 3: Industry-wise Ransomware Victims