Red Piranha
unified threat management

THREAT INTELLIGENCE REPORT

July 04 - 10, 2023

Report Summary:

- **New Threat Detection Added** – 4 (MacOS RustBucket Malware, Remcos RAT, Zeus Gameover, and JhoneRAT)
- **New Threat Protections**
- **New Ransomware Victims Last Week - 76**

Newly Detected Threats Added

1. MacOS RustBucket Malware

In an APT campaign discovered by researchers in April, macOS users were targeted with a sophisticated multi-stage malware, ultimately resulting in the RustBucket backdoor. This backdoor, attributed to the BlueNoroff APT group linked to Lazarus, has since evolved with additional variants, showcasing previously unseen persistence capabilities. RustBucket stands out for its diverse anti-evasion and anti-analysis measures observed throughout its stages. The attack commences with an Applet disguised as a PDF Viewer app, followed by subsequent stages that vary in payload language and architecture. The Stage 2 payloads, written in Swift or Objective-C, retrieve Stage 3 from a command-and-control server. Notably, the Stage 2 payload necessitates a specially crafted PDF to unlock the code and initiate the download of Stage 3, along with an XOR'd key for decoding the obfuscated C2 appended to the PDF's end.

Threat Protected: 02
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: Defence Evasion TA0005/ T1036.001/T1553.002 - Discovery TA0007/T1082 -Command-and-Control TA0011/T1573

2. Remcos RAT

Remcos RAT (Remote Control and Surveillance) has a notorious history in the world of cybercrime. Originally developed as a legitimate remote administration tool, it quickly became exploited by malicious actors for their nefarious purposes. Its capabilities are vast, allowing hackers to gain unauthorised access to compromised systems remotely. With features like keylogging, screen capturing, and file manipulation, Remcos RAT provides cybercriminals with complete control over infected machines. It has been involved in various high-profile attacks, including data breaches, financial fraud, and espionage activities. In recent years, Remcos RAT has been leveraged in sophisticated phishing campaigns, targeted attacks on businesses, and the distribution of other malware. Its evolving nature and advanced functionalities make it a constant threat, requiring vigilant cybersecurity measures to protect against its infiltration.

Threat Protected: 02
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/T1064 - Persistence TA0003/T1547.001 - Privilege Escalation TA0004/T1055/T1547.001 - Defence Evasion TA0005/T1036/T1055/T1064/T1497 - Credential Access TA0006/T1056 - Discovery TA0007/T1010/T1016T1018/T1082/T1083 - Collection TA0009/T1056 - Command-and-Control TA0011 /T1071/T1095

3. Zeus Gameover

Zeus Gameover, a notorious malware, infiltrates computer systems with a sophisticated workflow that wreaks havoc on unsuspecting victims. Through a stealthy combination of social engineering, exploit kits, and advanced encryption techniques, Zeus Gameover establishes control over infected machines, enabling cybercriminals to remotely access sensitive information, perform fraudulent transactions, and propagate further malware infections. With its intricate workflow, Zeus Gameover poses a significant threat to cybersecurity, demanding constant vigilance and robust defences to mitigate its devastating 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 T1012/T1590 - Weaponisation T1027 - Delivery T1566 - Exploitation T1203 - Installation T1059 – Command-and-Control T1043 - Actions on Objective T1003/T1005/T1039 - Exfiltration T1041 - Impact T1489

4. JhoneRAT

JhoneRAT, a sophisticated Remote Access Trojan (RAT), has emerged as a significant cyber threat in recent years. Operating across multiple platforms, including Windows, Linux, and macOS, JhoneRAT demonstrates advanced capabilities for espionage and unauthorised access. Its functionalities encompass keylogging, screen capturing, file exfiltration, and remote command execution, making it a versatile tool for malicious actors seeking to infiltrate and compromise targeted systems. With its evolving nature and potential for widespread impact, defending against JhoneRAT requires proactive cybersecurity measures and continuous monitoring to safeguard sensitive data and protect against unauthorised access.

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/T1591 - Weaponisation T1027 - Delivery T1566 Exploitation T1203 - Installation T1059 - Command-and-Control T1043 - Actions on Objective T1003/T1056/T1059 - Exfiltration T1041 - Impact T1490

Known exploited vulnerabilities (Week 1 July 2023):

Vulnerability	Description
CVE-2021-29256	Arm Mali GPU Kernel Driver Use-After-Free Vulnerability

Updated Malware Signatures (Week 1 July 2023)

Threat	Description
njRAT	A remote access trojan typically spread using phishing emails or social engineering tactics. It allows a threat actor to steal sensitive information, install additional malware, and control the victim's machine remotely.
Zusy	Zusy, alternatively referred to as TinyBanker or Tinba, is a trojan specifically designed to engage in man-in-the-middle attacks to pilfer banking data. Upon execution, it inserts itself into legitimate Windows processes like "explorer.exe" and "winver.exe." As the user visits a banking site, Zusy deceitfully presents a fraudulent form, aiming to deceive the user into providing personal information.
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.
Redline	A .NET-based information stealer malware.

New Ransomware Victims Last Week: 76

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 76 new ransomware victims from 21 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.

Clop, a specific ransomware, has affected the largest number of new victims (20) spread across various countries. Lockbit3 and Play groups follow closely with each hitting 13 and 11 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	2.63%
Akira	2.63%
Alphv	3.95%
Bianlian	3.95%
Black suit	1.32%
Blackbasta	1.32%
Blackbyte	2.63%
Clop	26.32%
Cyclops	3.95%
Karakurt	1.32%
Lockbit3	17.11%
Mallox	1.32%
Medusa	3.95%
Play	14.47%
Qilin	1.32%
Ragnarlocker	1.32%
Ransomexx	1.32%
Ransomware blog	2.63%
Rhysida	6.58%

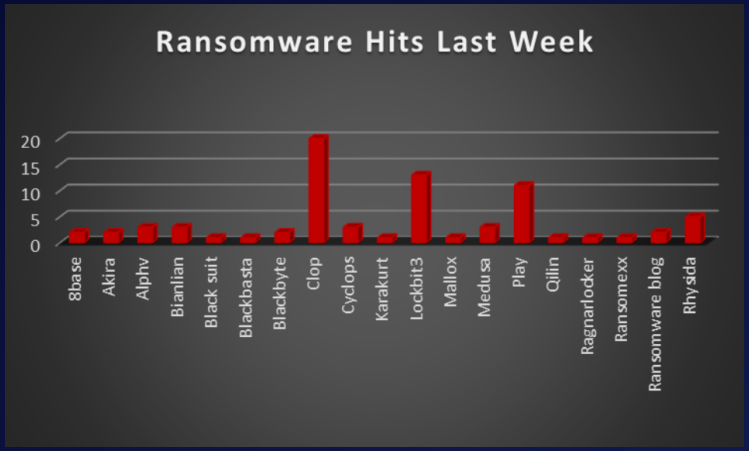

Figure 1: Ransomware Group Hits Last Week

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 44 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	2.63%
Bangladesh	1.32%
Canada	6.58%
Colombia	1.32%
Egypt	1.32%
France	1.32%
Germany	1.32%
Italy	5.26%
Japan	1.32%
Kenya	1.32%
Mexico	1.32%
Netherlands	2.63%
Poland	1.32%
Portugal	2.63%
Spain	2.63%
Switzerland	1.32%
Taiwan	1.32%
Thailand	1.32%
Turkey	1.32%
UK	2.63%
USA	57.89%

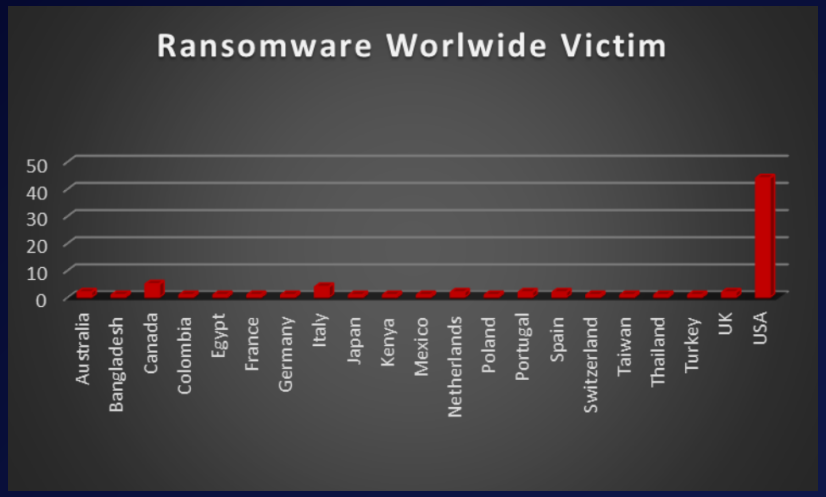

Figure 2: Ransomware Victims Worldwide

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 (%)
Automobile	1.32%
Banking	3.95%
Business Services	6.58%
Construction	3.95%
Consumer Services	2.63%
Electronics	1.32%
Energy	6.58%
Finance	6.58%
Government	3.95%
Healthcare	3.95%
Hospitality	6.58%
Insurance	1.32%
IT	13.16%
Legal Services	5.26%
Manufacturing	17.11%
Media	1.32%
Mining	2.63%
Organisations	1.32%
Real Estate	1.32%

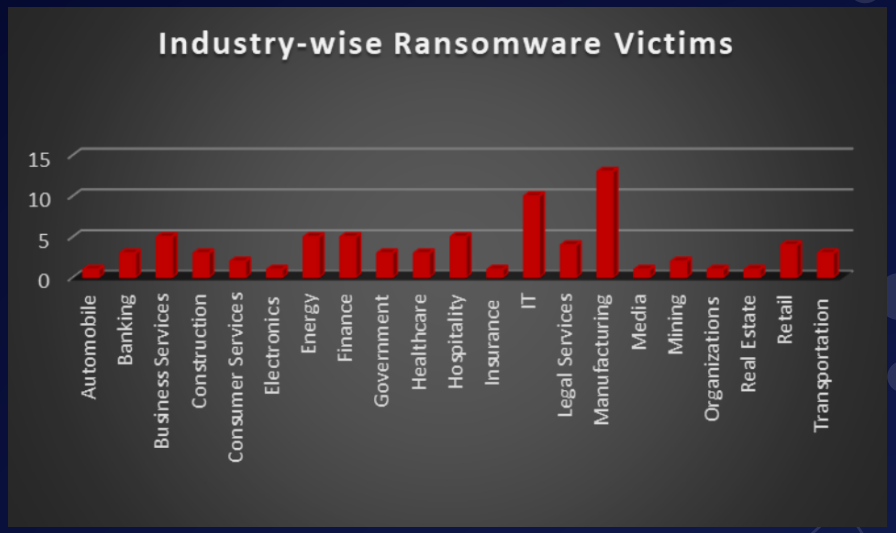

Figure 3: Industry-wise Ransomware Victims