Red Piranha
unified threat management

THREAT INTELLIGENCE REPORT

June 20 - 26, 2023

Report Summary:

- **New Threat Detection Added** – 4 (Mallox Ransomware Predator Malware, WispRider Malware, and SeroXen RAT)
- **New Threat Protections**
- **Overall Weekly Observables Count**
- **Daily submissions by Observable Type**
- **New Ransomware Victims Last Week - 110**

Newly Detected Threats Added

1. Mallox Ransomware

A new variant of the Mallox ransomware has been discovered, introducing a change in its file extension from ".mallox" to ".malox" for encrypted files. The ransomware utilises BatLoader, a tool previously associated with the distribution of RATs (Remote Access Trojans) and stealers. The Mallox ransomware group has integrated BatLoader into their operations, employing it to extract and inject the ransomware payload. This loader bears similarities to the one observed in the distribution of various malware families such as Quasar RAT, Async RAT, Redline Stealer, and DC RAT. Unlike the previous method of infection, this new technique eliminates the need for a downloader to retrieve the ransomware payload from a remote server. Instead, the ransomware payload is contained within a batch script, which is then injected into an executable file without being saved on the disk. The adoption of these novel infection techniques indicates that the threat actors responsible for Mallox ransomware are actively modifying their tactics, techniques, and procedures (TTPs), highlighting their ongoing efforts to improve evasiveness and sustain their malicious activities.

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 T1204 - Defence Evasion T1140/T1562/T1222 - Discovery T1082/T1083 – Command-and-Control T1071 - Impact T1486

2. Predator Malware

Predator, a malicious spyware designed for Android devices, emerged as a significant threat between August and October 2021. During this period, the attackers took advantage of zero-day vulnerabilities targeting Chrome and the Android operating system to implant Predator spyware on Android devices, even those that were fully updated.

Based on a high-confidence assessment, it is believed that the exploits used in these attacks were packaged by a single commercial surveillance firm named Cytrox. Subsequently, these exploits were sold to various government-backed actors who employed them in at least three distinct campaigns. The government-backed threat actors, originating from countries including Armenia, Côte d'Ivoire, Egypt, Greece, Indonesia, Madagascar, Serbia, and Spain, acquired and leveraged these exploits to deploy Predator spyware on their Android targets. In all the campaigns, the targeted Android users were deceived with one-time links sent via email. These links were cleverly disguised to mimic URL shortener services, adding to the effectiveness and deceptive nature of the attacks.

Threat Protected: 03
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: Initial Access T1476/T1444 - Collection   T1512//T1412/T1533/T1417 - Discovery
T1418 - Impact T1510

3. WispRider Malware

WispRider malware is a highly sophisticated and insidious software that poses a grave threat to computer systems and networks. As an advanced persistent threat (APT), WispRider has gained notoriety for its ability to stealthily infiltrate and persistently operate within compromised systems. This malware is designed to gain unauthorised access to sensitive information by exploiting vulnerabilities and employing various techniques, such as social engineering and spear-phishing. Once inside a target system, WispRider establishes a backdoor, allowing the attacker to remotely control the compromised machine and carry out malicious activities undetected. With its advanced evasion capabilities, WispRider can bypass traditional security measures, making it essential for organisations to adopt comprehensive security practices to defend against this formidable threat.

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 T1043 - Actions on Objective T1028 - Persistence T1547 - Defence Evasion T1565 - Exfiltration T1041

4. SeroXen RAT

SeroXen RAT is a highly potent remote access trojan (RAT) that poses a significant threat to computer systems and networks. This sophisticated malware grants unauthorised individuals the ability to gain remote control and conduct covert surveillance on compromised devices. SeroXen RAT can be deployed through various means, including phishing emails or malicious downloads, and once it infiltrates a system, it establishes a persistent foothold, allowing the attacker extensive control over the infected device. With features like keylogging, screen capturing, and file manipulation, SeroXen RAT presents a grave security concern, necessitating robust cybersecurity measures to detect, mitigate, and prevent its impact on both individuals and organisations.

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 T1043 - Actions on Objective T1028 - Persistence T1547 - Defence Evasion T1565 - Exfiltration T1041

Known exploited vulnerabilities (Week 4 June 2023):

Vulnerability	Description
CVE-2016-0165	Microsoft Win32k Privilege Escalation Vulnerability
CVE-2016-9079	Mozilla Firefox, Firefox ESR, and Thunderbird Use-After-Free Memory Vulnerability
CVE-2021-44026	Roundcube Webmail SQL Injection Vulnerability
CVE-2020-12641	Roundcube Webmail Remote Code Execution Vulnerability
CVE-2020-35730	Roundcube Webmail Cross-Site Scripting (XSS) Vulnerability
CVE-2023-20887	Vmware Aria Operations for Networks Command Injection Vulnerability
CVE-2023-20867	VMware Tools Authentication Bypass Vulnerability
CVE-2023-27992	Zyxel Multiple NAS Devices Command Injection Vulnerability
CVE-2023-32439	Apple Multiple Products WebKit Type Confusion Memory Vulnerability
CVE-2023-32435	Apple iOS and iPadOS WebKit Memory Corruption Vulnerability
CVE-2023-32434	Apple Multiple Products Integer Overflow Vulnerability

Updated Malware Signatures (Week 4 June 2023)

Threat	Description
Upatre	A malware dropper that downloads additional malware on an infected machine. It is usually observed to drop banking trojan after the initial infection.
Nanocore	The Nanocore trojan, built on the .NET framework, has been the subject of multiple source code leaks, resulting in its widespread accessibility. Similar to other remote access trojans (RATs), Nanocore empowers malicious actors with complete system control, enabling activities such as video and audio recording, password theft, file downloads, and keystroke logging.
Ramnit	A banking trojan used to steal online banking credentials.
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: 110

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 110 new ransomware victims from 20 distinct industries across 29 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 (27) spread across various countries. Alphv and 8base groups follow closely with each hitting 14 and 12 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	10.91%
Akira	5.45%
Alphv	12.73%
Bianlian	1.82%
Black suit	2.73%
Blackbasta	1.82%
Clop	24.55%
Dunghill	1.82%
Karakurt	0.91%
Lockbit3	6.36%
Mallox	1.82%
Medusa	1.82%
Noescape	5.45%
Play	10.91%
Qilin	1.82%
Ra group	1.82%
Rhysida	4.55%
Snatch	1.82%
Vicesociety	0.91%

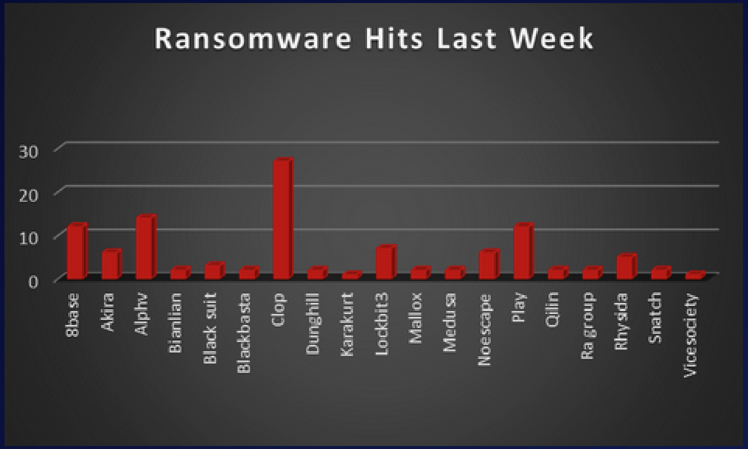

Figure 1: Ransomware Group Hits Last Week

When we examine the victims by country out of 29 countries around the world, we can conclude that the USA was once again the most ransomware-affected country, with a total of 62 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
Austria	1.82%
Belgium	0.91%
Brazil	0.91%
Canada	0.91%
China	2.73%
Czech	0.91%
France	2.73%
Gabon	0.91%
Germany	2.73%
India	0.91%
Ireland	1.82%
Japan	1.82%
Korea	1.82%
Lebanon	0.91%
Mexico	0.91%
Nicaragua	0.91%
Pakistan	0.91%
Peru	0.91%
Portugal	0.91%
Qatar	0.91%
South Africa	0.91%
Spain	2.73%
Switzerland	1.82%
Taiwan	0.91%
Thailand	0.91%
Tokyo	0.91%
Turkey	0.91%
UK	7.27%
USA	56.36%

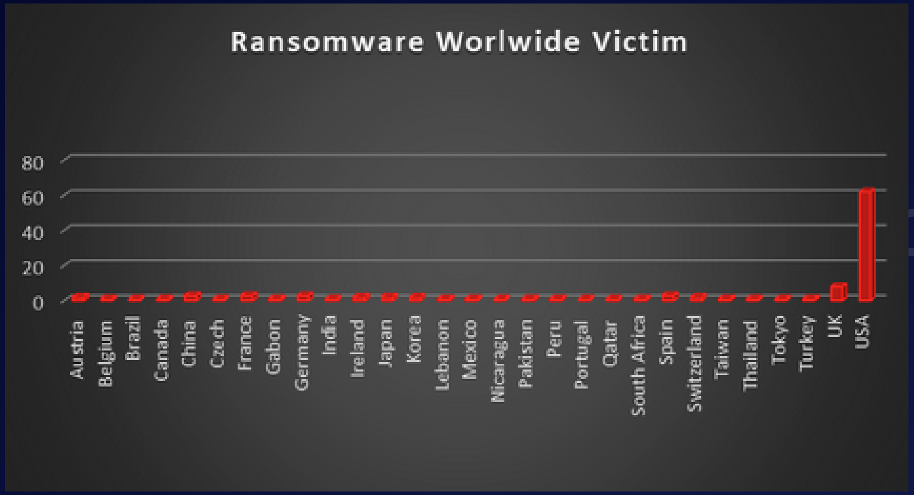

Figure 2: Ransomware Victims Worldwide

After conducting additional research, we found that ransomware has impacted 20 industries globally. Last week, the Business Services and Manufacturing sectors were hit particularly hard, with the loss of 21 and 18 businesses in each sector respectively. The table below presents the most recent ransomware victims sorted by industry.

Industry	Victims Count (%)
Agriculture	0.91%
Automotive	0.91%
Business Services	19.09%
Construction	9.09%
Consumer Services	4.55%
Education	4.55%
Energy	0.91%
Finance	7.27%
Government	0.91%
Healthcare	3.64%
Hospitality	1.82%
Insurance	2.73%
IT	6.36%
Legal Services	2.73%
Manufacturing	16.36%
Media	0.91%
Organisation	0.91%
Real Estate	0.91%
Retail	10.00%
Transportation	5.45%

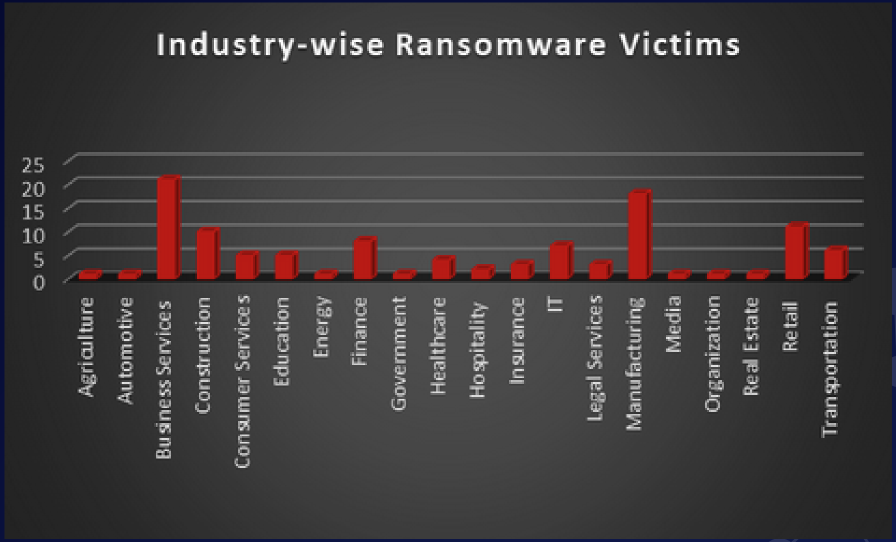

Figure 3: Industry-wise Ransomware Victims