Red Piranha
unified threat management

THREAT INTELLIGENCE REPORT

Aug 22 - 28, 2023

Report Summary:

- **New Threat Detection Added** – 3 (CollectionRAT Malware, XLoader Malware, and Ferest Smuggler)
- **New Threat Protections**
- **New Ransomware Victims Last Week - 142**

Newly Detected Threats Added

1. CollectionRAT

CollectionRAT presents a repertoire of standard Remote Access Trojan (RAT) functionalities, encompassing command execution and file management on compromised endpoints. The core implant is crafted from a Microsoft Foundation Class (MFC) library-based Windows binary. This binary dynamically decrypts and executes the actual malware code, employing MFC's intricate object-oriented framework. The choice of MFC, primarily used for crafting user interfaces in Windows apps, adds layers of complexity that obscure malware analysis. However, CollectionRAT utilises MFC solely as a wrapper for decrypting malicious code.

Upon infiltration, CollectionRAT initiates by gathering system data, crafting a unique fingerprint for the infected environment. This fingerprint is communicated to the Command-and-Control (C2) server. Subsequently, commands flow from the C2 server, triggering diverse tasks on the compromised system. Among these tasks, CollectionRAT's prowess is manifested in its capacity to establish a reverse shell. This shell empowers the malware to execute arbitrary commands seamlessly. It extends its influence further, allowing the reading, writing, and manipulation of files on the disk, as well as spawning new processes. This versatility equips it to procure and deploy supplementary payloads as needed. Interestingly, the implant possesses an evasive function, permitting its removal from the endpoint under C2 directives.

In essence, CollectionRAT deftly wields a varied arsenal of capabilities within its seemingly intricate MFC framework. Its fusion of RAT functionalities with a sophisticated decryption mechanism showcases its adaptability and the intricacies that veil its core operations.

Threat Protected: 03
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/T1497 - Discovery TA0007/T1010/T1018/T1082/T1497 - Command-and-Control TA0011/T1071/T1105/T1573

2. XLoader Malware

XLoader, a long-standing malware-as-a-service infostealer and botnet, has maintained its presence since 2015. Its enduring existence has witnessed numerous iterations, each evolving to adapt to the changing cybersecurity landscape.

In 2021, XLoader expanded its scope to include macOS platforms. Notably, its initial macOS variant was distributed as a Java program. However, its efficacy was hindered by the absence of the Java Runtime Environment as a default macOS component post-Snow Leopard. This constraint limited its reach to systems where Java was selectively installed.

Presently, XLoader emerges anew, shedding its previous dependencies. This resurgence is marked by a transformation in its programming foundation. The malware has transitioned to being natively coded in C and Objective C languages, a shift that affords it enhanced autonomy and versatility.

XLoader's latest incarnation employs a ruse to cloak its malicious intent. It has adopted the guise of an innocuous office productivity application named 'OfficeNote'. Remarkably, it is now signed with an Apple developer signature, lending it an appearance of legitimacy.

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: Execution TA0002/T1064 - Persistence TA0003/T1547.011 - Privilege Escalation TA0004/T1547.011 - Defence Evasion TA0005/T106 - Discovery TA0007/T1082 - Command-and-Control TA0011/T1071/T1105

3. Ferest Smuggler

Ferest Smuggler is a credential harvesting campaign that leads to Business Email Compromise fraud. This phishing campaign was observed in August 2023 targeting a municipal government on the US West Coast. The attackers spoofed the domain of the Visa-owned payment processor, Authorise.net. By employing a domain with null MX records, they successfully evaded email filters, allowing the malicious email to reach its intended recipients.

A business email compromise (BEC) threat actor only requires an account that has no multi-factor authentication (MFA) protection to gain access to a staff member's inbox. Once in possession of this email inbox, especially if it belongs to an employee in departments like accounting or human resources (HR), the threat actor gains access to a wide array of potential targets. These targets are extracted from the contacts and entities found within the stolen emails. Operating under the guise of the original victim organisation, the threat actor can target clients, companies, or partners listed in the compromised email archive. This enables them to execute actions such as requesting wire transfers as typically done by the victim organisation.

Threat Protected: 02
Rule Set Type:

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

Class Type: Trojan-activity
Kill Chain: Initial Access T1566

Known exploited vulnerabilities (Week 4 August 2023):

Vulnerability	Description
CVE-2023-26359	Adobe ColdFusion Deserialisation of Untrusted Data Vulnerability
CVE-2023-27532	Veeam Backup & Replication Cloud Connect Missing Authentication for Critical Function Vulnerability
CVE-2023-38035	Ivanti Sentry Authentication Bypass Vulnerability
CVE-2023-32315	Ignite Realtime Openfire Path Traversal Vulnerability
CVE-2023-38831	RARLAB WinRAR Code Execution Vulnerability

Updated Malware Signatures (Week 4 August 2023)

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

New Ransomware Victims Last Week: 142

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 142 new ransomware victims from 18 distinct industries across 30 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 (58) spread across various countries. Cloak and LockBit3.0 hit 18 & 14 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	7.75%
Akira	0.70%
Alphv	5.63%
Arvinclub	4.23%
Bianlian	0.70%
Blackbyte	0.70%
Cloak	12.68%
Clop	40.85%
Cuba	0.70%
LockBit3.0	9.86%
Medusa	1.41%
Noescape	2.82%
Play	5.63%
Ransomed	3.52%
Rhysida	2.11%
Snatch	0.70%

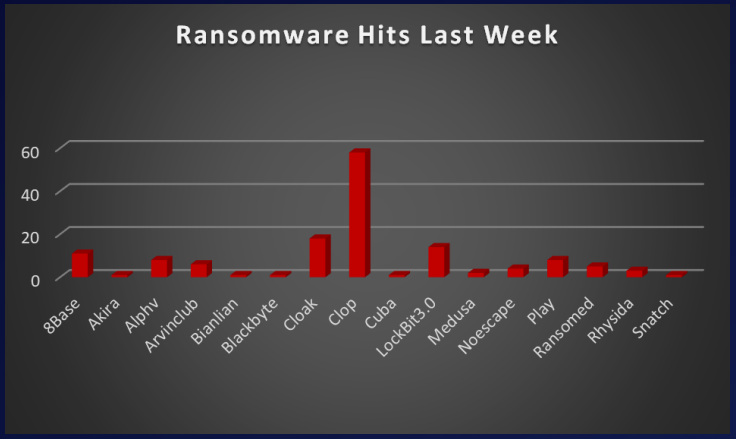

Figure 1: Ransomware Group Hits Last Week

When we examine the victims by country out of 30 countries around the world, we can conclude that the USA was once again the most ransomware-affected country, with a total of 77 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	1.41%
Austria	0.70%
Bahamas	0.70%
Bermuda	0.70%
Brazil	2.82%
Canada	3.52%
China	0.70%
France	2.82%
Germany	2.82%
Guatemala	1.41%
India	2.11%
Iran	2.11%
Ireland	0.70%
Israel	0.70%
Italy	2.82%
Japan	1.41%
Mexico	2.11%
Moldova	0.70%
Netherlands	2.11%
Philippines	0.70%
Saint Vincent and the Grenadines	0.70%
Singapore	0.70%
South Africa	1.41%
Spain	0.70%
Switzerland	2.82%
Taiwan	0.70%
Thailand	0.70%
UAE	0.70%
UK	4.23%
USA	54.23%

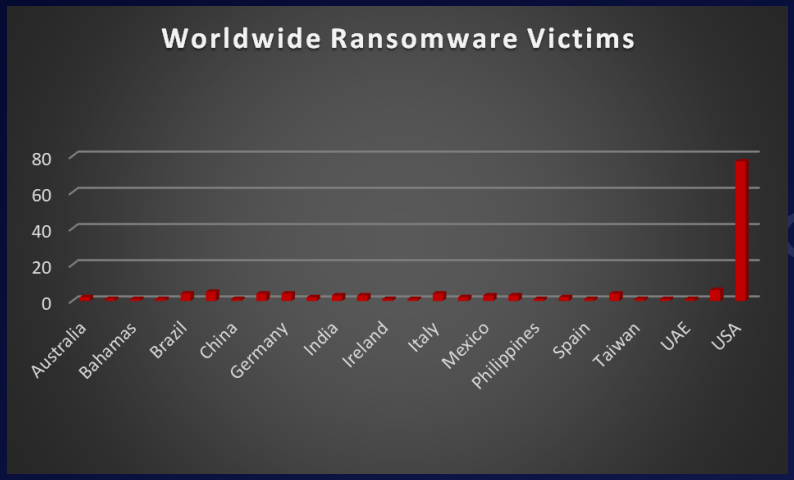

Figure 2: Ransomware Victims Worldwide

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 16% and 10% of the total ransomware victims belonging to each of those sectors respectively. The table below presents the most recent ransomware victims sorted by industry.

Industry	Victims Count (%)
Banking	7.04%
Business Services	10.56%
Construction	7.04%
Consumer Services	2.82%
Education	7.04%
Finance	5.63%
Government	1.41%
Healthcare	4.23%
Hospitality	4.93%
Insurance	6.34%
IT	9.86%
Legal Services	4.93%
Manufacturing	16.90%
Media & Internet	2.82%
Organisations	2.11%
Retail	2.82%
Telecom	1.41%
Transportation	2.11%

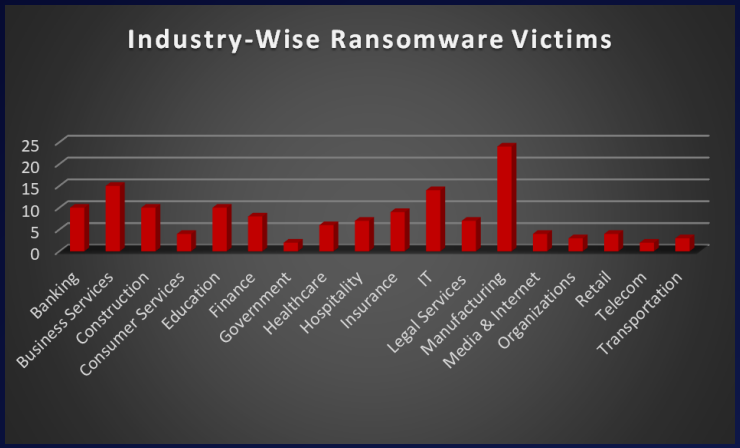

Figure 3: Industry-wise Ransomware Victims