Red Piranha
unified threat management

THREAT INTELLIGENCE REPORT

Nov 21 - 27, 2023

Report Summary:

- **New Threat Detection Added** – 2 (WailingCrab Malware and SOVA Malware)
- **New Threat Protections - 05**
- **New Ransomware Victims Last Week - 70**

Newly Detected Threats Added

1. WailingCrab Malware

Researchers monitored the evolution of the WailingCrab malware family, particularly its Command-and-Control (C2) communication methods, which now exploit the Internet of Things (IoT) protocol MQTT. WailingCrab, aka WikiLoader, is a complex malware often distributed by the initial access broker Hive0133. First seen in December 2022, it targets Italian entities with Gozi backdoor through email campaigns. The malware prioritizes stealth, utilizing legitimate websites for C2 communication and employing well-known platforms like Discord for payloads. WailingCrab's recent adoption of the MQTT protocol enhances its evasion tactics, as this protocol is rarely used by malware, allowing it to operate discreetly.

Threat Protected: 03
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-activity
Kill Chain: Persistence T1574.002 - Privilege Escalation T1574.002 - Defense Evasion T1070.006/T1218.010/T1218.011/T1497/T1574.002 - Discovery T1018/T1082/T1497

2. SOVA Malware

This year, we've seen a surge in Android banking malware due to increased mobile payment use amid the global pandemic. Threat actors are capitalizing on this shift, exploiting evolving tech and behaviours enter SOVA a new, sophisticated Android malware. While in early stages, it boasts standard features like other banking malware but aims for more. SOVA's creator actively tests and plans advanced functions like overlay attacks, keylogging, hiding notifications, and modifying crypto wallets. Planned features include on-device fraud, DDoS, ransomware, making SOVA a potentially extensive Android malware, setting a new standard for banking trojans targeting financial institutions.

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: Trojan-activity
Kill Chain: Execution T1053 - Privilege Escalation T1053 - Defence Evasion T1036/T1620 Discovery T1012/T1082 – Collection T1056 - Command-and-Control T1071/T1095/1105.

Known exploited vulnerabilities (Week 4 November 2023):

Vulnerability	Description
CVE-2023-4911	GNU C Library Buffer Overflow Vulnerability

Updated Malware Signatures (Week 4 November 2023)

Threat	Description
Razy	A stealer malware that collects sensitive information from victim machines, encrypts it and exfiltrates it to its Command-and-Control server.
Zeus	Also known as Zbot and is primarily designed to steal banking credentials
Glupteba	A malware dropper that is designed to download additional malware on an infected machine.
Valyria	A Microsoft Word-based malware which is used as a dropper for second-stage malware.
Tofsee	A malware that is used to send spam emails, conduct click frauds and cryptomining.
Trojan Miner	This malicious software installs and runs cryptocurrency mining applications.

New Ransomware Victims Last Week: 70

Red Piranha proactively gathers information about organizations impacted by ransomware attacks through various channels, including the Dark Web. In the past week, our team identified a total of 70 new ransomware victims or updates in few past victims from 18 distinct industries across 18 countries worldwide. This highlights the global reach and indiscriminate nature of ransomware attacks, which can affect organizations of all sizes and sectors.

LockBit3.0, a specific ransomware, has affected the largest number of victims (16) updates spread across various countries. Alphv and Meow ransomwares updated 9 and 8 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
3Am	1.43%
8Base	10%
Akira	4.29%
Alphv	12.86%
Bianlian	4.29%
Blackbasta	4.29 %
Cactus	4.29%
Clop	1.43%
Hunters	1.43%
Inc Ransom	10%
Lockbit3	22.86%
Medusa	1.43%
Meow	11.43%
Noescape	4.29%
Play	2.86%
Rhysida	2.86%

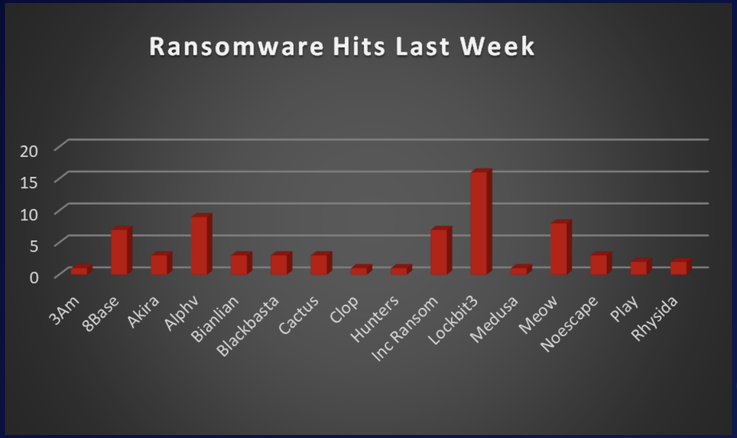

Figure 1: Ransomware Group Hits Last Week

When we examine the victims by country out of 18 countries around the world, we can conclude that the USA was once again the most ransomware affected country, with a total of 40 victims updates last week. The list below displays the number (%) of new ransomware victims per country.

Name of the affected Country	Number of Victims
Australia	7.14%
Belgium	1.43%
Canada	2.86%
Denmark	1.43%
France	1.43%
Germany	2.86%
India	2.86%
Indonesia	1.43%
Italy	5.71%
Luxembourg	1.43%
Morocco	2.86%
Netherlands	1.43%
Nigeria	1.43%
Norway	1.43%
Singapore	1.43%
Spain	1.43%
UK	4.29%
USA	57.14%

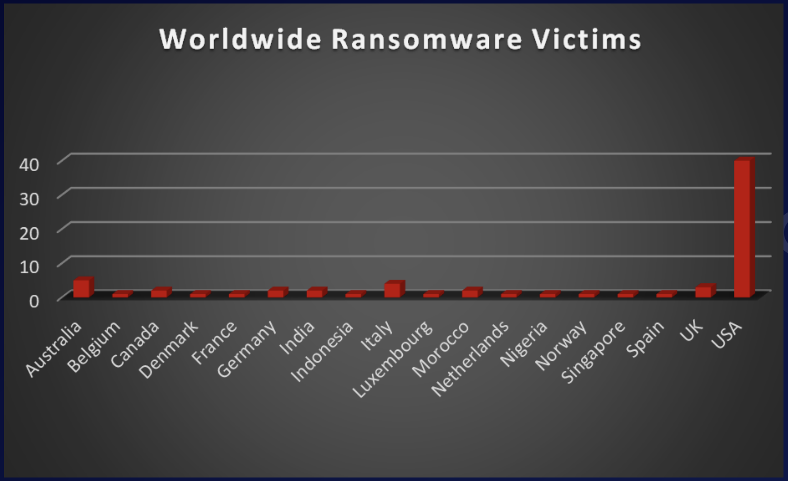

Figure 2: Ransomware Victims Worldwide

After conducting additional research, we found that ransomware has impacted 18 industries globally. Last week, the Manufacturing and Construction sectors were hit particularly hard, with 30% and 11% of the total ransomware victims belonged in each of those sectors respectively. The table below presents the most recent ransomware victims sorted by industry.

Industry	Victims Count (%)
Agriculture	1.43%
Banking	1.43%
Business Services	2.86%
Construction	11.43%
Consumer Services	2.86%
Education	2.86%
Finance	2.86%
Healthcare	8.57%
Hospitality	1.43%
Insurance	2.86%
IT	5.71%
Legal Services	4.29%
Manufacturing	30.00%
Media & Internet	2.86%
Organizations	2.86%
Real Estate	1.43%
Retail	7.14%
Transportation	7.14%

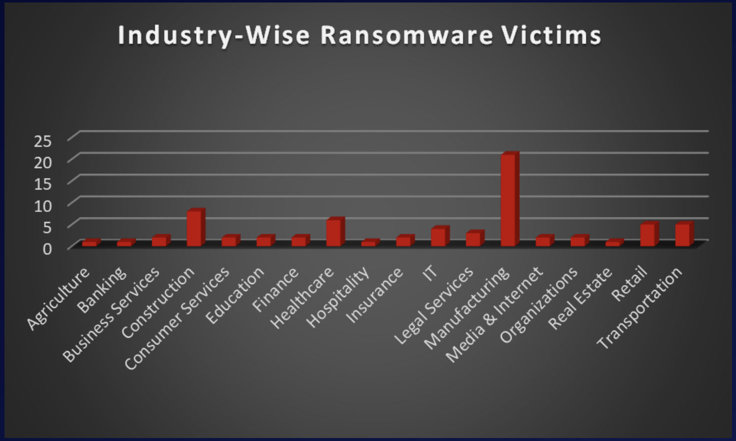

Figure 3: Industry-wise Ransomware Victims