Red Piranha
unified threat management

THREAT INTELLIGENCE REPORT

Nov 28 - Dec 04, 2023

Report Summary:

- **New Threat Detection Added** – 3 (MetaStealer Malware, Gh0st RAT, and Apache ActiveMQ Remote Code Execution (CVE-2023-46604))
- **New Threat Protections - 05**
- **New Ransomware Victims Last Week - 103**

Newly Detected Threats Added

1. MetaStealer

MetaStealer, a malware designed for Mac users, poses a serious threat by extracting sensitive information. Built with the Go programming language, it has surged in infostealers targeting macOS in 2023. Uniquely, it strategically targets business users through social engineering, using fake client personas to lure victims. The malware often arrives disguised as disk image bundles with business-related filenames, a distinctive approach for macOS threats. Its core executable includes obfuscated Go source code with functions for keychain exfiltration, password extraction, and file retrieval. MetaStealer's impact extends to disrupting business operations, compromising data, and posing the risks of identity theft and financial loss.

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-activity
Kill Chain: Execution T1047/T1059/T1129 - Privilege Escalation T1134 - Defence Evasion T1027/T1036/T1134/T1497 - Credential Access T1003/T1056 - Discovery T1010/T1012/T1018/T1033 - Collection T1005/T1056/T1115 - Command-and-Control T1071/T1095/T1102 - Impact T1529

2. Gh0st RAT

Gh0st RAT, a Trojan Remote Access Tool designed for the Windows Operating System, consists of crucial components the client and server. The client, a Windows application, oversees and manages remote Gh0st servers, enabling customised server installations. The server component, named SVCHOST.DLL, installs on compromised hosts as a Windows service. This DLL communicates with the Gh0st client, awaiting instructions. INSTALL.EXE, the dropper application, installs SVCHOST.DLL, while RESSDT.SYS, a kernel-level binary, resets the System Service Dispatch Table. The dropper, a comprehensive install program, initiates the Gh0st server installation and startup. Gh0st RAT empowers hackers with a range of capabilities, from screen control and keystroke logging to webcam access and remote shutdown authority.

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: Privilege Escalation T1055 - Defence Evasion T1027/T1055/T1622 - Credential Access T1056.004 - Discovery T1057/T1082/T1124/T1622 - Collection T1056 – Command-and-Control T1095/T1102

3. Apache ActiveMQ Remote Code Execution (CVE-2023-46604)

The OpenWire protocol marshaller in Java is susceptible to Remote Code Execution. This flaw could potentially enable a remote attacker, who has network access to a Java-based OpenWire broker or client, to execute arbitrary shell commands. The attack involves manipulating serialised class types within the OpenWire protocol, allowing the malicious actor to induce the instantiation of any class on the classpath in either the client or the broker, as appropriate.

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-Activity
Kill Chain: Initial Access T1190

Known exploited vulnerabilities (Week 5 November 2023):

Vulnerability	Description
CVE-2023-6345	Google Skia Integer Overflow Vulnerability
CVE-2023-49103	ownCloud graphapi Information Disclosure Vulnerability

Updated Malware Signatures (Week 5 November 2023)

Threat	Description
Remcos	Remcos functions as a remote access trojan (RAT), granting unauthorised individuals the ability to issue commands on the compromised host, record keystrokes, engage with the host's webcam, and take snapshots. Typically, this malicious software is distributed through Microsoft Office documents containing macros, which are often attached to malicious emails.
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.
Vidar	A stealer designed to collect sensitive data from infected machines. It usually targets Windows-based machines and is spread through email attachments or downloads from compromised websites.
Bifrost	A remote access trojan that enables its operator to take control of a victim machine and steal data. It is usually distributed through spam and phishing emails.
CoinMiner	This malicious software installs and runs cryptocurrency mining applications.

New Ransomware Victims Last Week: 103

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 103 new ransomware victims or updates in the few past victims from 19 distinct industries across 23 countries worldwide. This highlights the global reach and indiscriminate nature of ransomware attacks, which can affect organisations of all sizes and sectors.

LockBit3.0 and Play ransomware groups have affected the largest number of 12 victims, each update spread across various countries. Alphv ransomware group updated 11 new victims. Below are the victim counts (%) for these ransomware groups and a few others.

Name of Ransomware Group	Percentage of new Victims last week
3Am	0.97%
8Base	7.77%
Abyss-Data	0.97%
Akira	6.80%
Alphv	10.68%
Bianlian	0.97%
Black Suit	4.85%
Blackbasta	1.94%
Cactus	3.88%
Daixin	0.97%
Donutleaks	1.94%
Hunters	3.88%
Inc Ransom	0.97%
Knight	4.85%
Lockbit3	11.65%
Medusa	1.94%
Meow	1.94%
Metaencryptor	0.97%
Monti	2.91%
NoEscape	3.88%
Play	11.65%
Qilin	0.97%
Ra Group	0.97%
Ransomexx	0.97%
Ransomhouse	1.94%
Ransomware Blog	0.97%
Rhysida	3.88%
Snatch	3.88%

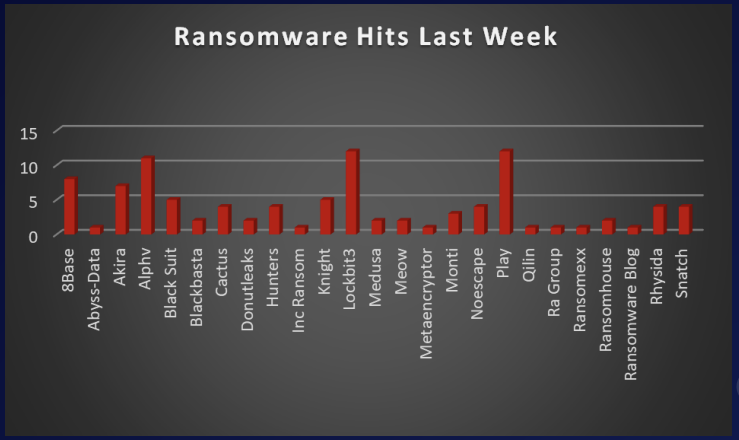

Figure 1: Ransomware Group Hits Last Week

When we examine the victims by country out of 23 countries around the world, we can conclude that the USA was once again the most ransomware-affected country, with a total of 58 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	2.91%
Belgium	0.97%
Canada	4.85%
China	1.94%
Costa Rica	0.97%
Croatia	0.97%
Egypt	0.97%
France	3.88%
Germany	4.85%
India	0.97%
Italy	2.91%
Malaysia	0.97%
Mexico	0.97%
Netherlands	0.97%
Poland	0.97%
Qatar	0.97%
Spain	1.94%
Sweden	0.97%
Switzerland	1.94%
Taiwan	0.97%
Thailand	0.97%
UK	5.83%
USA	56.31%

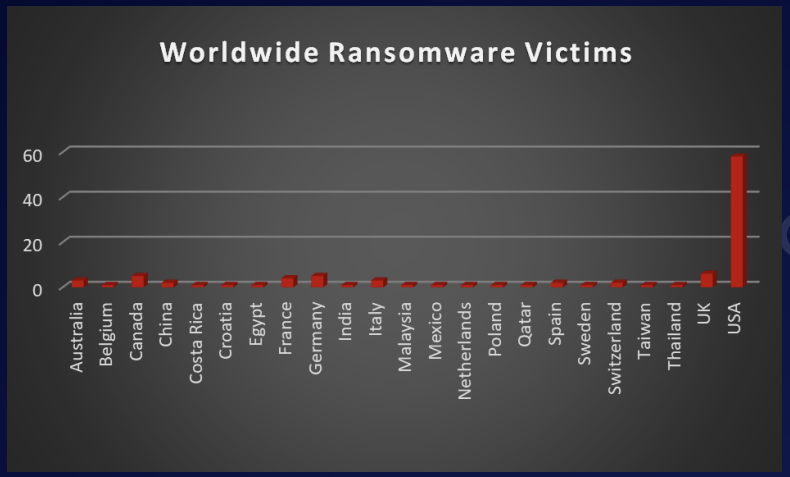

Figure 2: Ransomware Victims Worldwide

After conducting additional research, we found that ransomware has impacted 19 industries globally. Last week, the Manufacturing and Retail sectors were hit particularly hard, with 17% and 15% 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 (%)
Agriculture	1.94%
Business Services	11.65%
Construction	5.83%
Consumer services	1.94%
Education	5.83%
Energy, Utilities & Waste Treatment	3.88%
Finance	1.94%
Government	1.94%
Healthcare	6.80%
Hospitality	3.88%
Insurance	0.97%
IT	3.88%
Legal Services	7.77%
Manufacturing	17.48%
Organisations	3.88%
Real Estate	1.94%
Retail	15.53%
Telecom	0.97%
Transportation	1.94%

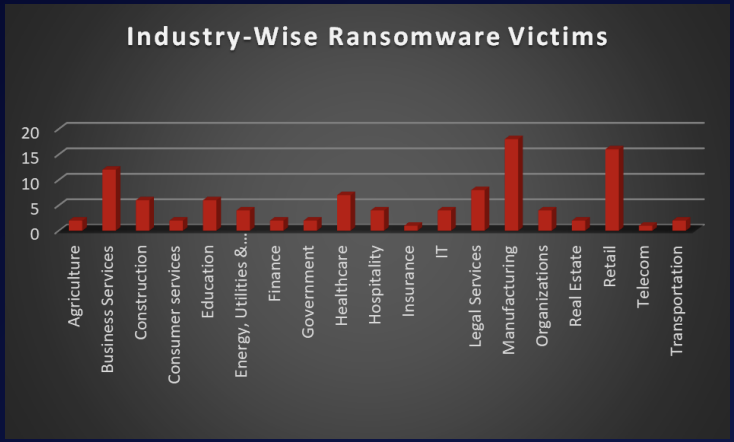

Figure 3: Industry-wise Ransomware Victims