Red Piranha
unified threat management

THREAT INTELLIGENCE REPORT

Oct 31 - Nov 06, 2023

Report Summary:

- **New Threat Detection Added** – 3 (BunnyLoader Malware, Earth Lusca APT, and Apache ActiveMQ CVE-2023-46604)
- **New Threat Protections - 09**
- **New Ransomware Victims Last Week - 104**

Newly Detected Threats Added

1. BunnyLoader Malware

Cybersecurity experts found a new and worrisome threat known as BunnyLoader on underground forums. This malicious tool does some concerning things like downloading harmful software, stealing your web browser login information, and more. What's alarming is that BunnyLoader uses a keylogger to record what you type and a clipper to watch your clipboard, so it can replace cryptocurrency wallet addresses with ones controlled by bad actors. After collecting this sensitive information, BunnyLoader neatly packages it into a ZIP file and sends it to a Command-and-Control server. This sneaky program, written in C/C++, is being sold on the dark web for $250. It is important to note that BunnyLoader is always getting updated and improved to avoid getting caught by security systems while carrying out its actions like downloading harmful software, recording keystrokes, stealing data, and taking remote commands.

Threat Protected: 05
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 - Persistence T1547.001 - Privilege Escalation T1547.001 - Defence Evasion T1027/T1036/T1497 - Discovery T1010/T1016/T1018 - Collection T1005 - Command-and-Control T1071/T1095

2. Earth Lusca APT

A cyber threat group called Earth Lusca APT has been found targeting countries in Southeast Asia, Central Asia, Latin America, and Africa. They are mainly interested in government agencies involved in foreign affairs, technology, and telecommunications. Their focus has shifted to exploiting vulnerabilities in their target's exposed servers. Notably, they are using new and unknown vulnerabilities (0-day) in these servers. They are using a malicious program called SprySOCKS Trojan, which can perform various standard actions like gathering system information, creating a virtual connection, checking network connections, creating a proxy, and transferring files. It also supports basic file operations like listing, deleting, renaming, and creating directories.

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 - Execution T1059 - Collection T1005 - Command-and-Control T1090

3. Apache ActiveMQ CVE-2023-46604

Apache ActiveMQ is vulnerable to Remote Code Execution. The vulnerability may allow a remote attacker with network access to a broker to run arbitrary shell commands by manipulating serialised class types in the OpenWire protocol to cause the broker to instantiate any class on the classpath. Users are recommended to upgrade to version 5.15.16, 5.16.7, 5.17.6, or 5.18.3, which fixes this issue.

Threat Protected: 03
Rule Set Type:

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

Class Type: Attempted-admin
Kill Chain: Execution T1059 - Privilege Escalation T1068

Known exploited vulnerabilities (Week 1 November 2023):

Vulnerability	Description
CVE-2023-46747	F5 BIG-IP Configuration Utility Authentication Bypass Vulnerability
CVE-2023-46748	F5 BIG-IP Configuration Utility SQL Injection Vulnerability
CVE-2023-46604	Apache ActiveMQ Deserialization of Untrusted Data Vulnerability

Updated Malware Signatures (Week 1 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: 104

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 104 new ransomware victims or updates in the few past victims from 19 distinct industries across 24 countries worldwide. This highlights the global reach and indiscriminate nature of ransomware attacks, which can affect organisations of all sizes and sectors.

LockBit3.0, a specific ransomware, has affected the largest number of victims (24) updates spread across various countries. Play and Blackbasta ransomware groups updated 19 & 13 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	6.73%
Akira	0.96%
Alphv	7.69%
Bianlian	1.92%
Black Suit	0.96%
Blackbasta	12.50 %
Daixin	0.96%
Inc Ransom	1.92%
Knight	8.65%
Lockbit3	23.08%
Medusa	2.88%
Metaencryptor	0.96%
Noescape	10.58%
Play	18.27%
Rhysida	0.96%
Snatch	0.96%

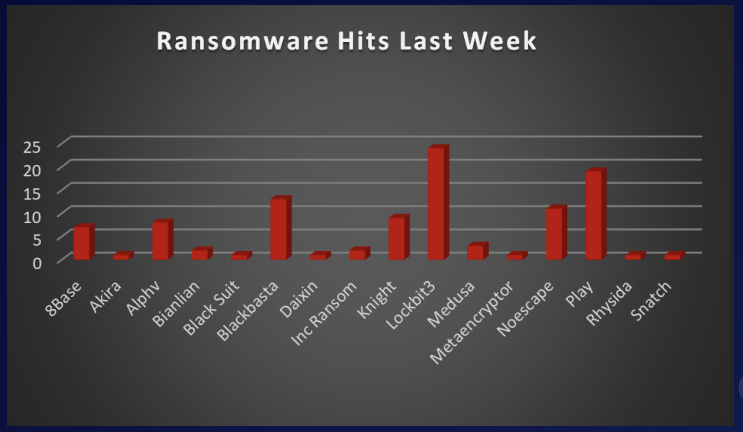

Figure 1: Ransomware Group Hits Last Week

When we examine the victims by country out of 24 countries around the world, we can conclude that the USA was once again the most ransomware-affected country, with a total of 55 victims updates last week. The list below displays the number (%) of new ransomware victims per country.

Name of the affected Country	Number of Victims
Argentina	0.96%
Australia	2.88%
Belgium	0.96%
Brazil	0.96%
Canada	1.92%
Chile	0.96%
France	3.85%
Germany	2.88%
India	0.96%
Italy	8.65%
Japan	0.96%
Jordan	0.96%
Mexico	0.96%
Myanmar	0.96%
Netherlands	3.85%
Philippines	0.96%
Poland	0.96%
Saudi Arabia	0.96%
Senegal	0.96%
Spain	0.96%
Thailand	0.96%
UAE	0.96%
UK	7.69%
USA	52.88%

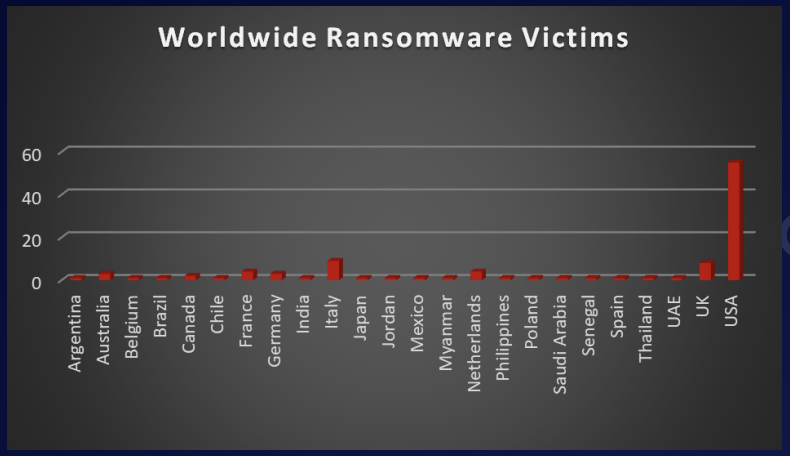

Figure 2: Ransomware Victims Worldwide

After conducting additional research, we found that ransomware has impacted 19 industries globally. Last week, the Manufacturing and Construction sectors were hit particularly hard, with 125% and 14% 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 (%)
Business Services	8.65%
Cities, Towns & Municipalities	0.96%
Construction	12.50 %
Consumer Services	1.92%
Education	3.85%
Electricity, Oil & Gas	0.96%
Finance	2.88%
Government	0.96%
Healthcare	5.77%
Hospitality	6.73%
Insurance	1.92%
Legal Services	3.85%
Manufacturing	25.96%
Media & Internet	1.92%
Organisations	5.77%
Real Estate	0.96%
Retail	9.62%
Telecom	3.85%
Transportation	0.96%

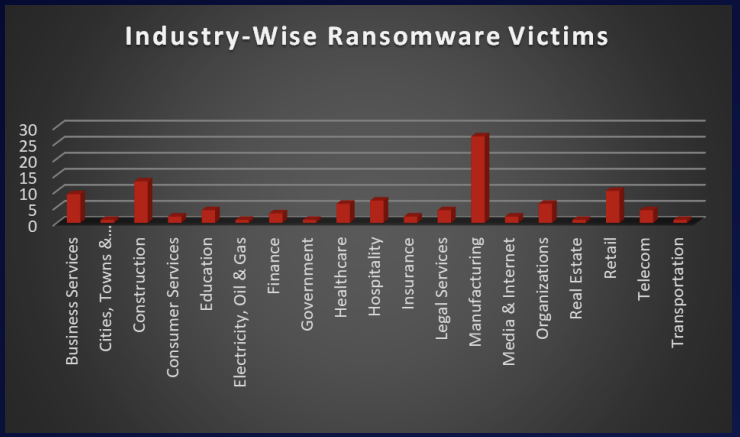

Figure 3: Industry-wise Ransomware Victims