
Red Piranha
unified threat management
THREAT INTELLIGENCE REPORT
Oct 03 - 09, 2023

Report Summary:

- **New Threat Detection Added** – 3 (BunnyLoader Malware, CrimsonRAT Malware and Agniane Stealer)
- **New Threat Protections - 9**
- **New Ransomware Victims Last Week - 75**

Newly Detected Threats Added

1. BunnyLoader Malware

In early September, cybersecurity researchers made a concerning discovery – a new Malware-as-a-Service (MaaS) threat named BunnyLoader surfaced on several underground forums. This insidious tool offers a range of capabilities, including downloading and executing a second-stage payload, pilfering browser credentials and system data, and more. What makes BunnyLoader particularly alarming is its utilisation of a keylogger to record keystrokes and a clipper to monitor the clipboard, replacing cryptocurrency wallet addresses with those controlled by malicious actors.

After collecting this sensitive data, BunnyLoader efficiently packages it into a ZIP archive and transmits it to a Command-and-Control (C2) server. This recently spotted this malicious loader, written in C/C++, is being peddled on the dark web for $250. It is noteworthy that BunnyLoader is rapidly evolving, receiving frequent feature updates and bug fixes. Moreover, it employs various anti-sandbox techniques to evade detection while performing actions like downloading and executing a second-stage payload, keylogging, data theft, and remote command execution.

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: 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. CrimsonRAT Malware

CrimsonRAT is a dangerous remote access tool (RAT) constructed using the Java programming language, and it is important to note that it is malicious, not a legitimate application. Cybercriminals wield this RAT as a sinister means to take control of compromised computers and execute a range of malicious actions. With CrimsonRAT, malicious actors gain the capability to manipulate and erase files on the compromised system, making it a potent tool for their destructive purposes. It also serves as a "backdoor" for injecting additional malware into the infected system, typically ransomware and data-stealing trojans. Ransomware encrypts data and extorts payments for decryption, while data stealers harvest personal information for illicit profit. Beyond this, CrimsonRAT can be employed to disseminate adware and browser hijackers, resulting in unwanted redirects, intrusive ads, and privacy breaches. Its presence can lead to permanent data loss, severe privacy violations, diminished online experiences, and various other issues.

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 T1047 - Privilege Escalation T1134 - Defence Evasion T1222 - Discovery T1016 - Collection T1005 - Command-and-Control T1071/T1095

3. Agniane Stealer

Agniane Stealer acquires login credentials, system particulars, and ongoing browsing sessions from browsers, tokens, and file transfer tools. It focuses on cryptocurrency extensions and wallets. This stolen data is relayed to Command-and-Control C&C servers, where malicious actors can exploit the information they have obtained.

The Agniane Stealer is linked to the Malware-as-a-Service (MaaS) platform known as the Cinoshi Project, which was first uncovered in early 2023. Agniane Stealer's code framework closely mirrors that of the Cinoshi Project. This close association indicates that Agniane Stealer has been offered for purchase on multiple dark web forums. The threat actors behind Agniane Stealer employ packers to sustain and regularly update the malware's functionalities and evasion capabilities.

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: Initial Access T1566/T1190 - Execution T1059 - Defence Evasion T1622 - Collection T1005 - Command-and-Control T1071/T1102 - Exfiltration T1567

Known exploited vulnerabilities (Week 1 October 2023):

Vulnerability	Description
CVE-2023-5217	Google Chrome libvpx Heap Buffer Overflow Vulnerability
CVE-2023-4211	Arm Mali GPU Kernel Driver Use-After-Free Vulnerability
CVE-2023-28229	Microsoft Windows CNG Key Isolation Service Privilege Escalation Vulnerability
CVE-2023-42793	JetBrains TeamCity Authentication Bypass Vulnerability
CVE-2023-42824	Apple iOS and iPadOS Kernel Privilege Escalation Vulnerability
CVE-2023-40044	Progress WS_FTP Server Deserialisation of Untrusted Data Vulnerability
CVE-2023-22515	Atlassian Confluence Data Center and Server Privilege Escalation Vulnerability

Updated Malware Signatures (Week 1 October 2023)

Threat	Description
Redline	A .NET-based information stealer malware
Nymeria	A remote access trojan written in the AutoIT language designed for automation. This trojan is designed to steal information and upload the contents to its command-and-control server.
MacStealer	A remote access trojan enables its operator to take control of a victim machine and steal data. It is usually distributed through spam and phishing emails.
Upatre	Upatre is also a malware dropper that downloads additional malware on an infected machine. It is usually observed to drop banking trojan after the initial infection.
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.

New Ransomware Victims Last Week: 75

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 75 new ransomware victims or updates in the few past victims from 19 distinct industries across 26 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 (17) updates spread across various countries. Play and Alphv ransomware groups updated 8 & 6 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
0Mega	1.33%
8Base	2.67%
Akira	2.67%
Alphv	8.00%
Arvinclub	2.67%
Bianlian	1.33%
Blackbyte	1.33%
Cactus	2.67%
Cuba	1.33%
Knight	1.33%
Lockbit3	22.67%
Lorenz	1.33%
Mallox	1.33%
Medusa	5.33%
Money Message	4.00%
Monti	5.33%
Noescape	6.67%
Play	10.67%
Qilin	1.33%
Ragnarlocker	6.67%
Ransomed	4.00%
Rhysida	4.00%
Trigona	1.33%

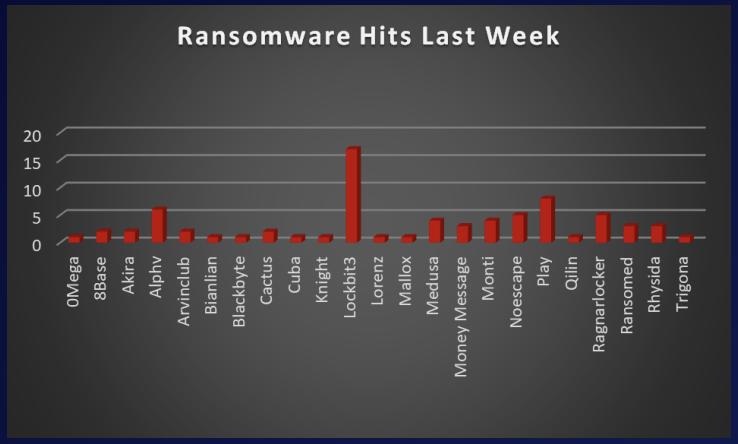

Figure 1: Ransomware Group Hits Last Week

When we examine the victims by country out of 26 countries around the world, we can conclude that the USA was once again the most ransomware-affected country, with 35 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	1.33%
Australia	1.33%
Brazil	2.67%
Bulgaria	1.33%
Canada	2.67%
Czech Republic	2.67%
Dominican Republic	1.33%
France	4.00%
Germany	2.67%
Guatemala	1.33%
Hungary	1.33%
India	2.67%
Iran	1.33%
Italy	4.00%
Japan	2.67%
Mexico	1.33%
Miami	1.33%
Netherlands	1.33%
Norway	1.33%
Portugal	1.33%
Singapore	1.33%
Spain	4.00%
Taiwan	1.33%
Thailand	1.33%
UK	5.33%
USA	46.67%

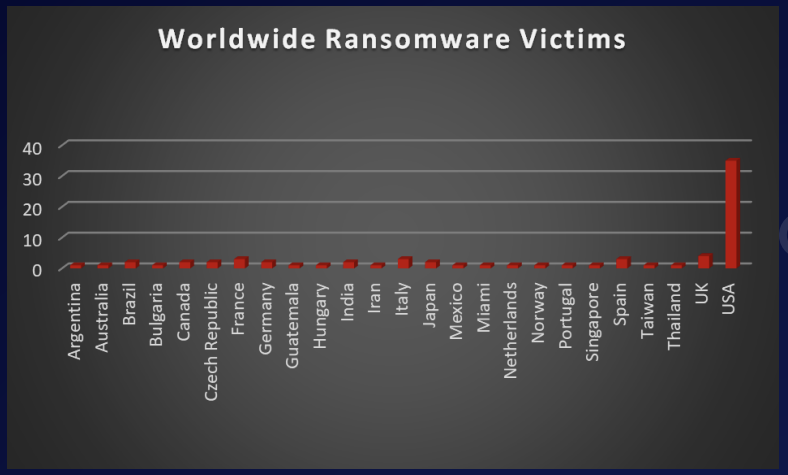

Figure 2: Ransomware Victims Worldwide

After conducting additional research, we found that ransomware has impacted 19 industries globally. Last week, the Manufacturing and Hospitality sectors were hit particularly hard, with 16% and 12% 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	4.00%
Chambers of Commerce	1.33%
Construction	8.00%
Consumer Services	1.33%
Education	4.00%
Finance	4.00%
Government	6.67%
Healthcare	12.00%
Hospitality	12.00%
IT	5.33%
Legal Services	1.33%
Manufacturing	16.00%
Media & Internet	1.33%
Metals & Mining	1.33%
Organisation	1.33%
Real Estate	1.33%
Retail	9.33%
Telecom	4.00%
Transportation	5.33%

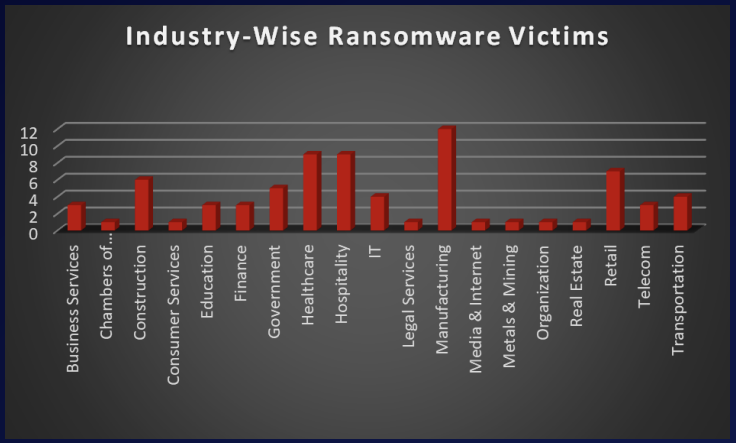

Figure 3: Industry-wise Ransomware Victims