Red Piranha
unified threat management

THREAT INTELLIGENCE REPORT

Nov 14 - 20, 2023

Report Summary:

- **New Threat Detection Added** – 3 (BunnyLoader Malware, Mars Stealer Malware and SysAid Traversal Attack CVE-2023-47246)
- **New Threat Protections - 06**
- **New Ransomware Victims Last Week - 114**

Newly Detected Threats Added

1. BunnyLoader Malware

BunnyLoader, a newly emerged Malware-as-a-Service (MaaS) threat, surfaced across underground forums. This sophisticated tool is more than just troublesome; it is equipped with multiple capabilities, from downloading and running additional harmful software to stealing browser data and system credentials. But what truly sets BunnyLoader apart is its use of a keylogger to capture keystrokes and a clipper to monitor the clipboard, substituting legitimate cryptocurrency wallet addresses with those controlled by cybercriminals.

Threat Protected: 04
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. Mars Stealer Malware

Beware if you store crypto in a digital wallet—a notorious crypto hack, once known as Oski Trojan, has resurfaced as Mars Stealer with enhanced tactics. Unlike its predecessor, it bypasses 40+ browser-based wallet security measures, even defying two-factor authentication (2FA), posing a grave threat. It is available for less than $200 on the Dark Web and infiltrates systems through phishing emails or disguised downloads. Once in your system, it targets browser extensions, gathering private crypto keys and wallet info, enabling hackers to drain your wallet unnoticed. This malware selectively avoids certain regions and erases its traces, leading to financial loss, privacy breaches, and potential identity theft.

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/T1053 - Persistence T11053 - Privilege Escalation T1053 - Defence Evasion T1027/T1036/T1562/1620 - Credential Access T1003 - Discovery T1010/T1012/T1082 - Collection T1005/T1056 - Command-and-Control T1071/T1095/1105

3. SysAid Traversal Attack CVE-2023-47246

On November 2nd, the SysAid team detected a potential vulnerability in their SysAid Server (On-Prem) software. The investigation conclusively revealed the presence of a zero-day vulnerability in the SysAid on-premises software. The threat actors identified as DEV-0950 (Lace Tempest) have successfully exploited the vulnerability by uploading a WAR archive containing a WebShell and other payloads into the webroot of the SysAid Tomcat web service.

The WebShell granted the attacker unauthorised access and control over the compromised system. The attackers employed a PowerShell script, deployed via the WebShell, to execute a malware loader named 'user.exe' on the compromised host. This loader was utilised to inject the GraceWire trojan into one of the running processes. It also executes a second-stage PowerShell script that removes evidence from the victim machine.

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: Attempted-admin
Kill Chain: Initial Access T1190

Known exploited vulnerabilities (Week 3 November 2023):

Vulnerability	Description
CVE-2023-47246	SysAid Server Path Traversal Vulnerability
CVE-2023-36844	Juniper Junos OS EX Series PHP External Variable Modification Vulnerability
CVE-2023-36845	Juniper Junos OS EX Series and SRX Series PHP External Variable Modification Vulnerability
CVE-2023-36846	Juniper Junos OS SRX Series Missing Authentication for Critical Function Vulnerability
CVE-2023-36847	Juniper Junos OS EX Series Missing Authentication for Critical Function Vulnerability
CVE-2023-36851	Juniper Junos OS SRX Series Missing Authentication for Critical Function Vulnerability
CVE-2023-36033	Microsoft Windows Desktop Window Manager (DWM) Core Library Privilege Escalation Vulnerability
CVE-2023-36025	Microsoft Windows SmartScreen Security Feature Bypass Vulnerability
CVE-2023-36036	Microsoft Windows Cloud Files Mini Filter Driver Privilege Escalation Vulnerability
CVE-2023-36584	Microsoft Windows Mark of the Web (MOTW) Security Feature Bypass Vulnerability
CVE-2023-1671	Sophos Web Appliance Command Injection Vulnerability
CVE-2020-2551	Oracle Fusion Middleware Unspecified Vulnerability

Updated Malware Signatures (Week 3 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: 114

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 114 new ransomware victims or updates in the few past victims from 21 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 (31) updates spread across various countries. Alphv and Play ransomware groups updated 13 and 12 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	7.02%
Abyss-Data	1.75%
Alphv	11.40%
Bianlian	1.75%
Black Suit	0.88%
Blackbasta	7.89%
Cuba	1.75%
Hunters	5.26%
Inc Ransom	4.39%
Lockbit3	27.19%
Lorenz	0.88%
Medusa	1.75%
NoEscape	5.26
Play	10.53%
Qilin	0.88%
Ra Group	4.39%
Ransomexx	0.88%
Ransomhouse	0.88%
Rhysida	0.88%
Snatch	4.39%

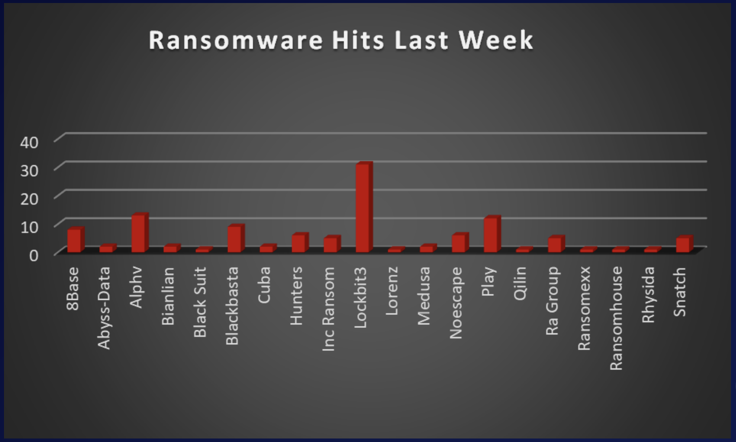

Figure 1: Ransomware Group Hits Last Week

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 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	0.88%
Canada	6.14%
Denmark	1.75%
Ecuador	0.88%
Finland	0.88%
France	1.75%
Germany	8.77%
Greece	0.88%
India	2.63%
Italy	2.63%
Japan	0.88%
Malaysia	0.88%
Maldives	0.88%
Mexico	1.75%
Netherlands	0.88%
Philippines	0.88%
Romania	0.88%
Singapore	1.75%
South Africa	0.88%
Spain	2.63%
Sweden	0.88%
Taiwan	2.63%
UK	6.14%
USA	50.88%

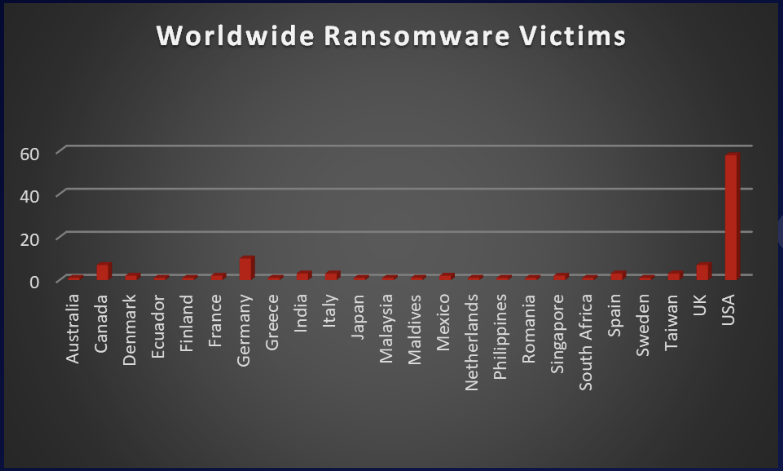

Figure 2: Ransomware Victims Worldwide

After conducting additional research, we found that ransomware has impacted 21 industries globally. Last week, the Manufacturing and Business Services sectors were hit particularly hard, with 18% 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 (%)
Agriculture	1.75%
Business Services	14.91%
Construction	4.39%
Consumer Services	0.88%
Cultural	0.88%
Education	3.51%
Energy, Utilities & Waste Treatment	2.63%
Finance	6.14%
Government	3.51%
Healthcare	5.26%
Hospitality	4.39%
Insurance	0.88%
IT	3.51%
Legal Services	1.75%
Manufacturing	18.42%
Media & Internet	1.75%
Metals & Mining	3.51%
Real Estate	3.51%
Retail	8.77%
Telecom	1.75%
Transportation	7.89%

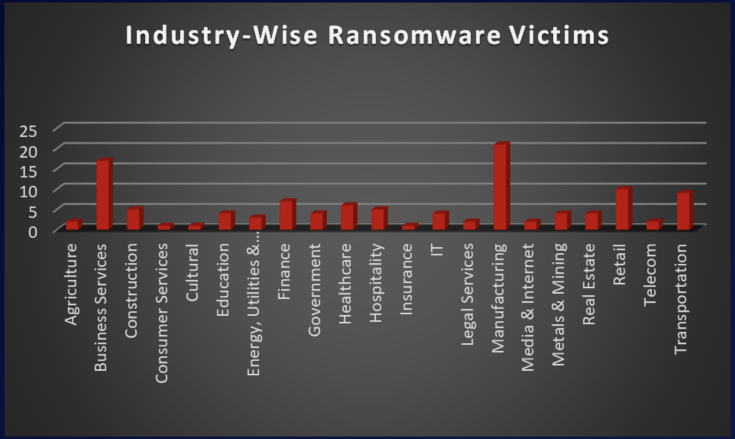

Figure 3: Industry-wise Ransomware Victims