Red Piranha
unified threat management

THREAT INTELLIGENCE REPORT

Nov 07 - 13, 2023

Report Summary:

- **New Threat Detection Added** – 3 (Bandit Stealer, FakeSG APT and Atlassian Confluence CVE-2023-22518)
- **New Threat Protections - 09**
- **New Ransomware Victims Last Week - 103**

Newly Detected Threats Added

1. Bandit Stealer

Bandit is a type of computer threat that steals important information like usernames and passwords. It targets web browsers, email programs, and even cryptocurrency wallets. The stolen info is then sent to a control server using Telegram. Bandit is smart and tries to avoid being detected by using different tricks when it is on a computer. People have been selling and buying Bandit on secret online forums since April 2023. The program is made using a coding language called Go, which is becoming more common among those who create harmful software.

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 T1047 - Defence Evasion T1027/T1036/T1497 - Credential Access T1003/T1056 - Discovery T1016/T1018/T1082/T1497 - Collection T1005/T1056 - Command-and-Control T1071/T1095/T1105

2. FakeSG APT

Over a couple of years back a campaign called FakeUpdates (SocGholish) was reported by the researchers. It tricks users into running a fake browser update on compromised websites, infecting computers with the NetSupport RAT. This allows hackers to access the victim's computer remotely and deliver more harmful software. Now, a new player called FakeSG has emerged, using a similar tactic on hacked WordPress sites. FakeSG distributes NetSupport RAT through zipped downloads or Internet shortcuts. Despite being a newcomer, FakeSG employs various layers of obfuscation, making it a serious threat that could compete with SocGholish.

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 T1059 - Privilege Escalation T1548 - Defence Evasion T1564/T1218/T1027/T1112/T1548/T1140 - Discovery T1082 - Command-and-Control T1071/T1571

3. Atlassian Confluence CVE-2023-22518

An improper authorisation vulnerability in the Atlassian Confluence Data Centre and Server may lead to substantial data loss when exploited by an unauthenticated attacker. It is important to note that there is no impact on confidentiality, as the attacker is unable to exfiltrate any data.

Threat Protected: 06
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: Web-application-activity
Kill Chain: Initial Access T1190

Known exploited vulnerabilities (Week 2 November 2023):

Vulnerability	Description
CVE-2023-29552	Service Location Protocol (SLP) Denial-of-Service Vulnerability
CVE-2023-22518	Atlassian Confluence Data Centre and Server Improper Authorization Vulnerability

Updated Malware Signatures (Week 2 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: 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 20 distinct industries across 30 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 (27) updates spread across various countries. Alphv and Blackbasta ransomware groups updated 10 victims each. Below are the victim counts (%) for these ransomware groups and a few others.

Name of Ransomware Group	Percentage of new Victims last week
8Base	3.88%
Abyss-Data	0.97%
Akira	7.77%
Alphv	9.71%
Blackbasta	9.71%
Cactus	2.91%
Ciphbit	0.97%
Cuba	1.94%
Hunters	1.94%
Inc Ransom	0.97%
Lockbit3	26.21%
Lorenz	2.91%
Medusa	5.83%
Monti	1.94%
NoEscape	5.83%
Play	9.71%
Qilin	0.97%
Ra Group	1.94%
Rhysida	3.88%

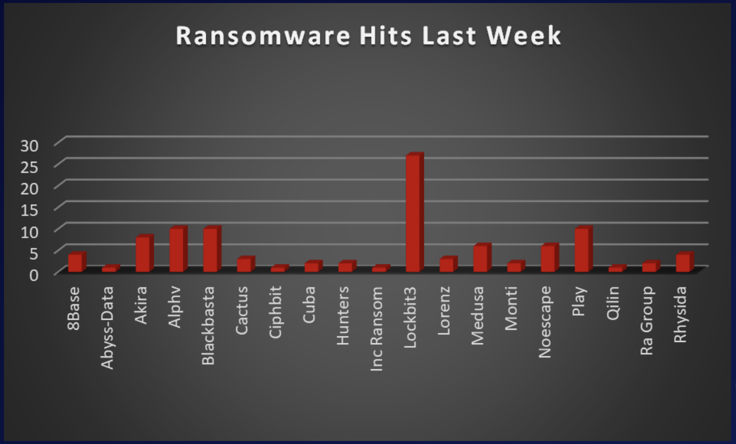

Figure 1: Ransomware Group Hits Last Week

When we examine the victims by country out of 30 countries around the world, we can conclude that the USA was once again the most ransomware-affected country, with a total of 49 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	0.97%
Belgium	0.97%
Brazil	1.94%
Canada	6.80%
Chile	0.97%
China	1.94%
Czech Republic	0.97%
Egypt	1.94%
France	2.91%
Germany	3.88%
India	0.97%
Indonesia	0.97%
Israel	1.94%
Italy	2.91%
Malaysia	0.97%
Mexico	0.97%
Namibia	0.97%
Netherlands	3.88%
Pakistan	0.97%
Philippines	0.97%
Poland	0.97%
Romania	0.97%
Saudi Arabia	0.97%
Singapore	1.94%
Slovenia	1.94%
Spain	0.97%
Taiwan	0.97%
Thailand	1.94%
UK	2.91%
USA	47.57%

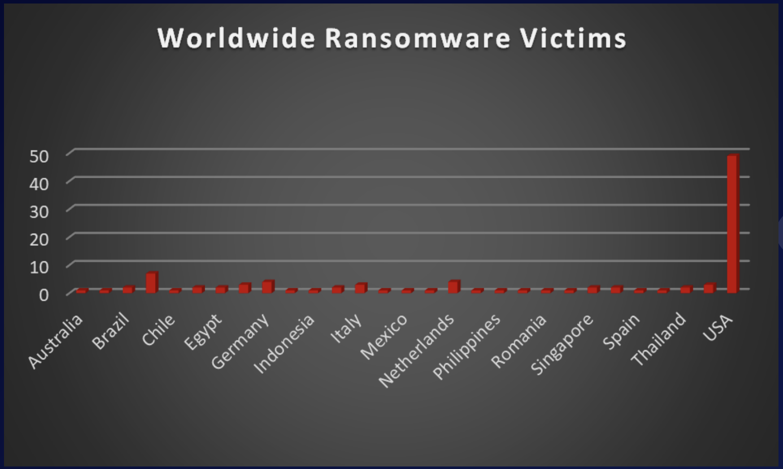

Figure 2: Ransomware Victims Worldwide

After conducting additional research, we found that ransomware has impacted 20 industries globally. Last week, the Manufacturing and Construction sectors were hit particularly hard, with 15% and 9% 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	4.85%
Construction	9.71%
Consumer Services	1.94%
Education	4.85%
Electricity, Oil & Gas	0.97%
Energy, Utilities & Waste Treatment General	1.94%
Finance	8.74%
Government	1.94%
Healthcare	8.74%
Hospitality	0.97%
Insurance	3.88%
IT	5.83%
Legal Services	6.80%
Manufacturing	14.56%
Metals & Mining	1.94%
Organisations	3.88%
Real Estate	0.97%
Retail	11.65%
Telecom	0.97%
Transportation	4.85%

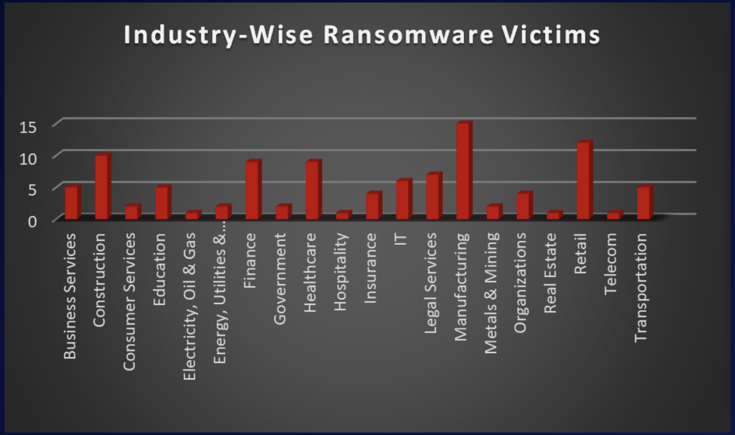

Figure 3: Industry-wise Ransomware Victims