Red Piranha
unified threat management

THREAT INTELLIGENCE REPORT

Dec 19 - 25, 2023

Report Summary:

- **New Threat Detection Added** – 2 (1xxbot Malware and Kraken Ransomware)
- **New Threat Protections - 3**
- **New Ransomware Victims Last Week - 89**

Newly Detected Threats Added

1. 1xxbot Malware

1xxbot, also known as Sectop is a remote access trojan (RAT) discovered by researchers recently. This malware allows remote control of infected devices, creating serious risks. Once installed, it can either record the desktop or create an invisible one, enabling hackers to monitor users' activities. It manipulates browsers like Chrome, Firefox, and Explorer, modifying settings and disabling security measures. 1xxbot can force visits to harmful sites, further infecting the system and boosting web traffic for profit. It gathers device and OS details and injects an executable file into system locations. While incomplete, 1xxbot poses a significant threat, potentially leading to privacy breaches, financial harm, and 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 T1129/T1203 - Persistence T1543.003 - Privilege Escalation T1055/T1574.002 - Defence Evasion T1027/T1036/T1055/T1222/T1497 - Credential Access T1003 - Discovery T1010/T1012/T1018 - Collection T1005/T1185 - Command-and-Control T1071

2. Kraken Ransomware

The Kraken ransomware, named after the legendary sea creature, emerged posing as SuperAntiSpyware, a legitimate app. McAfee's research team revealed its recent rise, delivered through the Fallout Exploit kit, the same tool used for GandCrab ransomware. Kraken employs Ransomware-as-a-Service (RaaS), a hacker toolkit, that holds computer data hostage for ransom. However, Kraken also wipes files, making recovery almost impossible. It's stealthy, producing new versions to avoid detection and has an exclusion list hinting at its origins. Kraken aims to attract more cybercriminals, reducing profits for affiliates. Battling this malware proves challenging due to its ever-evolving tactics.

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 - Persistence T1574.002 - Privilege Escalation T1055/T1574.002 - Defence Evasion T1036/T1055/T1140/T1497 - Discovery T1018/T1057/T1082/TT1083 - Collection T1560 - Command-and-Control T1071/T1095/T11055 - Impact T1486

Known exploited vulnerabilities (Week 3 December 2023):

Vulnerability	CVSS	Description
CVE-2023-49897	8.8 High	FXC AE1021, AE1021PE OS Command Injection Vulnerability
CVE-2023-47565	8.8 High	QNAP VioStor NVR OS Command Injection Vulnerability

Updated Malware Signatures (Week 3 December 2023)

Threat	Description
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.
CoinMiner	This malicious software installs and runs cryptocurrency mining applications.
Glupteba	A malware dropper that is designed to download additional malware on an infected machine.

New Ransomware Victims Last Week: 89

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 89 new ransomware victims or updates in the few past victims from 19 distinct industries across 20 countries worldwide. This highlights the global reach and indiscriminate nature of ransomware attacks, which can affect organisations of all sizes and sectors.

LockBit3.0 ransomware group has affected the largest number of 14 victims' updates spread across various countries. Werewolves and Cactus ransomware groups updated 12 and 11 new 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	10.11%
Alphv	3.37%
Bianlian	2.25%
Blackbasta	6.74%
Cactus	12.36%
Clop	1.12%
Dragonforce	3.37%
Hunters	1.12%
Inc Ransom	2.25%
Knight	1.12%
Lockbit3	15.73%
Medusa	2.25%
Meow	2.25%
Play	11.24%
Ra Group	7.87%
Rhysida	1.12%
Snatch	2.25%
Werewolves	13.48%

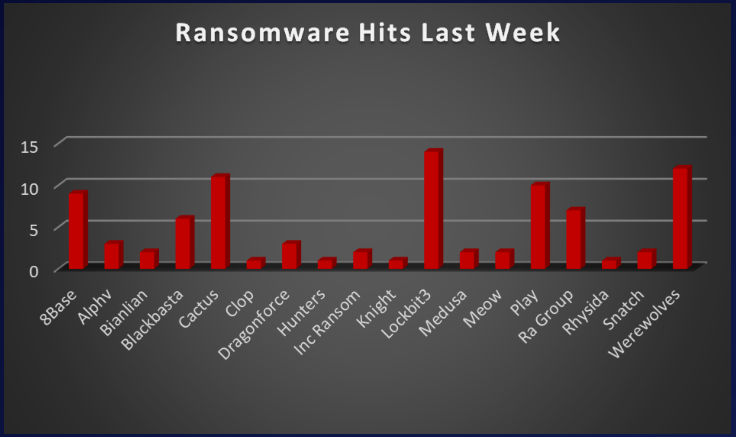

Figure 1: Ransomware Group Hits Last Week

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 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
Australia	3.37%
Belgium	1.12%
Canada	3.37%
Denmark	2.25%
France	3.37%
Germany	6.74%
India	3.37%
Italy	1.12%
Lithuania	1.12%
Luxembourg	2.25%
Macedonia	1.12%
Netherlands	2.25%
Poland	1.12%
Russia	5.62%
Serbia	1.12%
Singapore	1.12%
South Africa	1.12%
Spain	1.12%
UK	10.11%
USA	47.19%

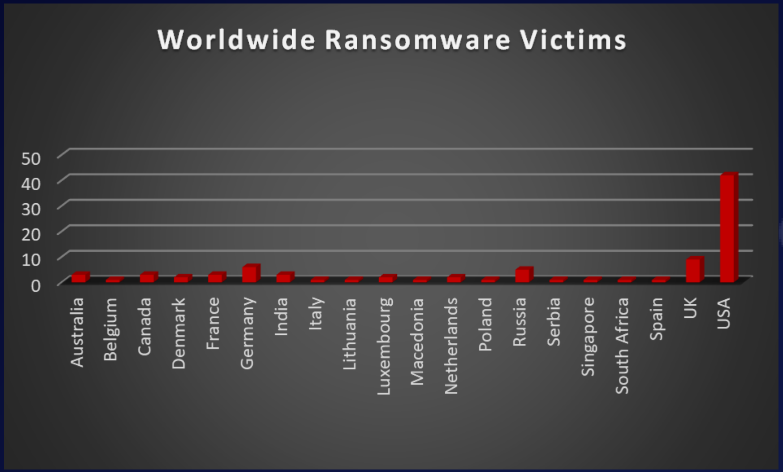

Figure 2: Ransomware Victims Worldwide

After conducting additional research, we found that ransomware has impacted 19 industries globally. Last week, the Manufacturing and Business Services sectors were hit particularly hard, with 17% and 13% 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	1.12%
Construction	1.12%
Consumer Services	13.48%
Education	8.99%
Energy, Utilities & Waste Treatment	3.37%
Finance	6.74%
Government	2.25%
Healthcare	4.49%
Hospitality	1.12%
IT	7.87%
Legal Services	5.62%
Manufacturing	1.12%
Media & Internet	2.25%
Metals & Mining	17.98%
Organisations	3.37%
Real Estate	3.37%
Retail	10.11%
Telecom	3.37%
Transportation	2.25%

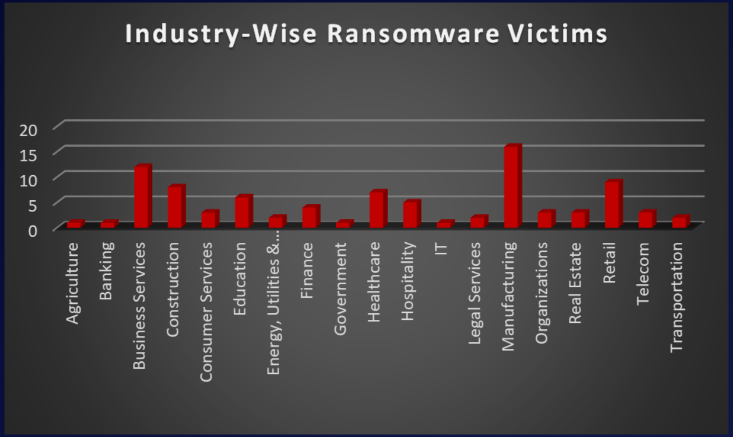

Figure 3: Industry-wise Ransomware Victims