Red Piranha
unified threat management

THREAT INTELLIGENCE REPORT

Jan 02 - 08, 2024

Report Summary:

- **New Threat Detection Added** – 2 (SmokeLoader Malware and TAG-63 Group)
- **New Threat Protections - 20**
- **New Ransomware Victims Last Week - 28**

Newly Detected Threats Added

1. SmokeLoader Malware

SmokeLoader, a backdoor malware, has served as a remote access tool and data thief since 2014. It infiltrates via Remote Desktop services, forming botnets for DDoS attacks and malware distribution. Operating across the Commonwealth of Independent States, it targets government entities using Kazakh currencies and languages. SmokeLoader employs stealth via obfuscation, operates stealthily, and evades antivirus programs. Priced at $1650, its compact size and annual updates enhance its capabilities. This malware extends beyond conventional backdoors by facilitating botnet commands and data theft. SmokeLoader diversifies propagation via emails, downloads, and exploitative tactics. Its obfuscated code thwarts analysis, complicating its detection and classification by antivirus software. SmokeLoader's collaboration with STOP/Djvu ransomware enhances its harmful potential.

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 T1053/T1129 - Persistence T1053 - Privilege Escalation T1053 -Discovery T1057/T1082/T1083

2. TAG-63 Group

An application found on a Telegram Channel linked to Hamas's supporters communicates with the group's Izz ad-Din al-Qassam Brigades website. Since Hamas' incursion into Israeli territory on October 7, 2023, the website has intermittently worked, facing attempts to evade takedowns or potential denial-of-service attacks. Infrastructure analysis reveals domains mimicking the tactics of the TAG-63 cyber group, linked to Hamas. The domains redirect to alqassam[.]ps and include a World Organisation Against Torture spoof. Increased network traffic at the incursion's start suggests informational dissemination. The application aims to boost Hamas's message, utilising shared Google Analytics codes and an apparent Iran nexus.

Threat Protected: 18
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: Command-and-Control T1071/T1095/T1573 - Defence Evasion T1406/T1447 - Credential T1409 - Access T1409 - Discovery T1421/T1422/T1424/T1426/T1430 - Impact T1447 - Collection T1409/T1430/T1507- Network Effects T1439

Known exploited vulnerabilities (Week 1 January 2024):

Vulnerability	CVSS	Description
CVE-2023-7101	N/A – undergoing NVD analysis	Spreadsheet::ParseExcel Remote Code Execution Vulnerability
CVE-2023-7024	8.8 High	Google Chromium WebRTC Heap Buffer Overflow Vulnerability

Updated Malware Signatures (Week 1 January 2024)

Threat	Description
Zeus	Also known as Zbot and is primarily designed to steal banking credentials.
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.
Trojan Miner	This malicious software installs and runs cryptocurrency mining applications.
XtremeRAT	A remote access trojan interacts with the infected machine via a remote shell, uploads/downloads files, and records from a webcam/microphone.

New Ransomware Victims Last Week: 28

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 28 new ransomware victims or updates in the few past victims from 13 distinct industries across 14 countries worldwide. This highlights the global reach and indiscriminate nature of ransomware attacks, which can affect organisations of all sizes and sectors.

LockBit3.0 and Hunter ransomware groups have affected the largest number of 4 victims each update spread across various countries. Blackbasta and Cactus ransomware groups updated 3 new 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
Alphv	10.71%
Bianlian	3.57 %
Black Suit	3.57%
Blackbasta	10.71%
Cactus	10.71%
Ciphbit	3.57%
Clop	3.57%
Hunters	14.29%
Inc Ransom	3.57%
Lockbit3	14.29%
Monti	3.57%
Play	7.14%
Ransomexx	3.57%
Ransomhouse	3.57%
Rhysida	3.57%

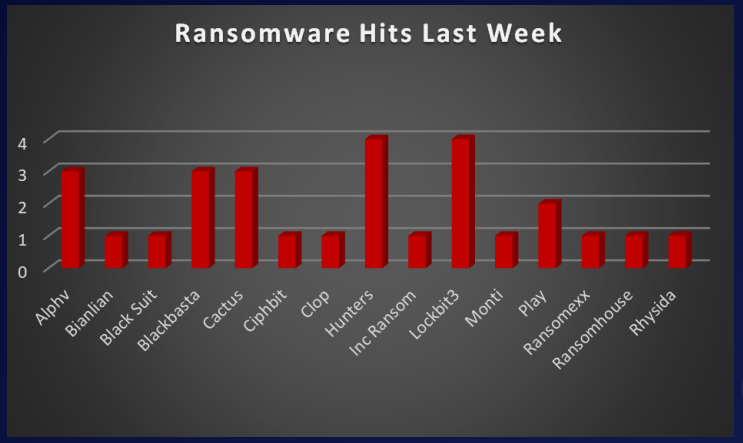

Figure 1: Ransomware Group Hits Last Week

When we examine the victims by country out of 14 countries around the world, we can conclude that the USA was once again the most ransomware-affected country, with a total of 13 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	7.14%
Canada	3.57%
Dominican Republic	3.57%
France	3.57%
Germany	3.57%
Kenya	3.57%
Netherlands	3.57%
New Zealand	3.57%
Philippines	3.57%
Saudi Arabia	3.57%
Spain	3.57%
Sweden	3.57%
UK	7.14%
USA	46.43%

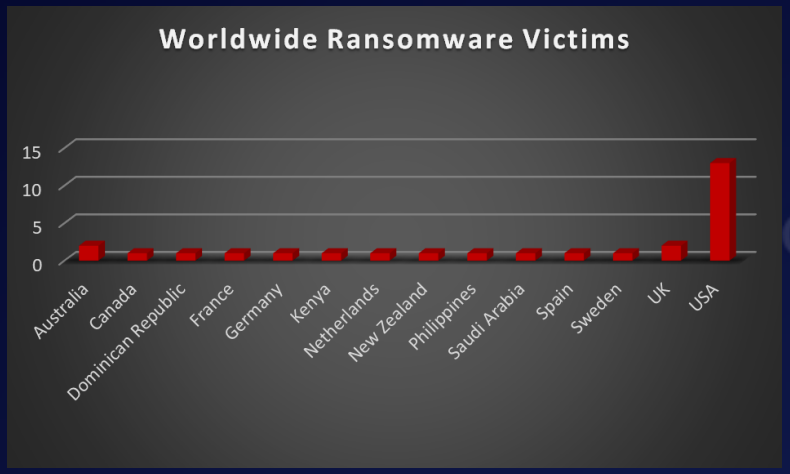

Figure 2: Ransomware Victims Worldwide

After conducting additional research, we found that ransomware has impacted 13 industries globally. Last week, the Retail and Transportation sectors were hit particularly hard, with 17% 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	7.14%
Construction	7.14%
Consumer Services	3.57%
Education	7.14%
Finance	7.14%
Healthcare	7.14%
Hospitality	3.57%
Legal Services	7.14%
Manufacturing	10.71%
Organisations	3.57%
Real Estate	3.57%
Retail	17.86%
Transportation	14.29%

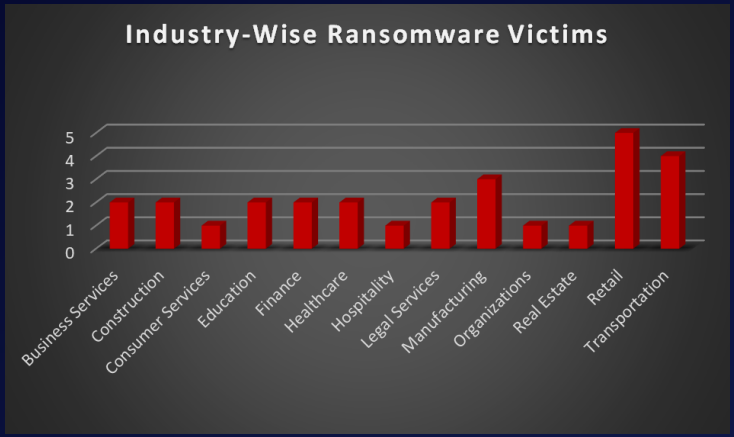

Figure 3: Industry-wise Ransomware Victims