Red Piranha
unified threat management

THREAT INTELLIGENCE REPORT

Dec 05 - 11, 2023

Report Summary:

- **New Threat Detection Added** – 3 (DarkIRC Bot, BlackTech APT and ownCloud Vulnerabilities (CVE-2023-41093 - CVE-2023-49105))
- **New Threat Protections - 09**
- **New Ransomware Victims Last Week - 96**

Newly Detected Threats Added

1. DarkIRC Bot

DarkIRC is a versatile botnet reported recently in the wild. It functions as a browser stealer, keylogger, and can even execute distributed denial-of-service attacks. This malicious tool also operates as a bitcoin clipper, altering bitcoin wallet addresses to steal transactions. In one campaign, it targets vulnerable WebLogic servers via an “HTTP GET” request, executing a PowerShell script to download a binary file. DarkIRC avoids virtual environments from VMware, VirtualBox, and others, using anti-sandbox tactics. Upon infiltration, it persists by installing within a Chrome file, enabling autorun commands for continued operation.

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/T1059/T1129 - Privilege Escalation T1134 - Defence Evasion T1027/T1036/T1134/T1497 - Credential Access T1003/T1056 - Discovery T1010/T1012/T1018/T1033 - Collection T1005/T1056/T1115 - Command-and-Control T1071/T1095/T1102 - Impact T1529

2. BlackTech APT

BlackTech, a cyber espionage group focused on East Asia, particularly Taiwan, Japan, and Hong Kong, is driven by the goal of stealing technology from its targets. Analysing their tactics revealed a common thread connecting three seemingly unrelated campaigns: PLEAD, Shrouded Crossbow, and Waterbear. PLEAD, active since 2012, specialises in information theft, targeting Taiwanese government agencies and private organisations. Their toolset includes the PLEAD backdoor and DRIGO exfiltration tool, delivered through spear-phishing emails. PLEAD actors employ a router scanner to identify vulnerable routers, enabling them to establish virtual servers for command-and-control or malware delivery.

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: Defence Evasion T1027/T1497 - Credential Access T1056 - Discovery T1012/T1018/T1082/T1497 - Collection T1056 - Command-and-Control T1071/T1095/T11573

3. ownCloud Vulnerabilities (CVE-2023-41093 - CVE-2023-49105)

The ownCloud graphapi is susceptible to an information disclosure vulnerability, which could expose sensitive data stored in phpinfo() through GetPhpInfo.php, potentially revealing administrative credentials.

An issue was discovered in ownCloud owncloud/core before 10.13.1. An attacker can access, modify, or delete any file without authentication if the username of a victim is known, and the victim has no signing-key configured. This occurs because pre-signed URLs can be accepted even when no signing-key is configured for the owner of the files. The earliest affected version is 10.6.0.

Threat Protected: 05
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 T1190

Known exploited vulnerabilities (Week 1 December 2023):

Vulnerability	Description
CVE-2023-42917	Apple Multiple Products WebKit Memory Corruption Vulnerability
CVE-2023-42916	Apple Multiple Products WebKit Out-of-Bounds Read Vulnerability
CVE-2023-33107	Qualcomm Multiple Chipsets Integer Overflow Vulnerability
CVE-2023-33106	Qualcomm Multiple Chipsets Use of Out-of-Range Pointer Offset Vulnerability
CVE-2023-33063	Qualcomm Multiple Chipsets Use-After-Free Vulnerability
CVE-2022-22071	Qualcomm Multiple Chipsets Use-After-Free Vulnerability
CVE-2023-41266	Qlik Sense Path Traversal Vulnerability
CVE-2023-41265	Qlik Sense HTTP Tunneling Vulnerability

Updated Malware Signatures (Week 1 December 2023)

Threat	Description
Remcos	Remcos functions as a remote access trojan (RAT), granting unauthorised individuals the ability to issue commands on the compromised host, record keystrokes, engage with the host's webcam, and take snapshots. Typically, this malicious software is distributed through Microsoft Office documents containing macros, which are often attached to malicious emails.
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.
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.
Bifrost	A remote access trojan that enables its operator to take control of a victim machine and steal data. It is usually distributed through spam and phishing emails.
CoinMiner	This malicious software installs and runs cryptocurrency mining applications.

New Ransomware Victims Last Week: 96

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 96 new ransomware victims or updates in few past victims from 20 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 ransomwares, has affected the largest number of 19 victims' updates spread across various countries. Play and Alphv ransomware groups updated 13 and 9 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
3Am	2.08%
8Base	5.21%
Abyss-Data	1.04%
Akira	6.25%
Alphv	9.38%
Bianlian	4.17%
Black Suit	3.13%
Blackbasta	2.08%
Cactus	2.08%
Cloak	7.29%
Dunghill	1.04%
Hunters	1.04%
Inc Ransom	2.08%
Lockbit3	19.79%
Medusa	5.21%
Metaencryptor	2.08%
Monti	2.08%
NoEscape	2.08%
Play	13.54%
Qilin	4.17%
Ransomware Blog	1.04%
Rhysida	2.08%
Snatch	1.04%

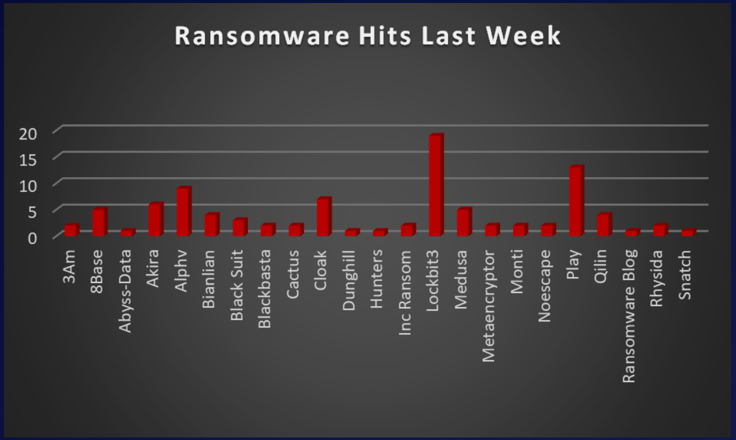

Figure 1: Ransomware Group Hits Last Week

When we examine the victims by country out of 20 countries around the world, we can conclude that the USA was once again the most ransomware-affected country, with a total of 53 victims updates last week. The list below displays the number (%) of new ransomware victims per country.

Name of the affected Country	Number of Victims
Canada	9.38%
Chian	1.04%
Curacao	1.04%
France	3.13%
Germany	4.17%
India	2.08%
Italy	4.17%
Japan	1.04%
Netherlands	1.04%
Nicaragua	1.04%
Panama	1.04%
Singapore	1.04%
South Africa	1.04%
South Korea	1.04%
Spain	3.13%
Sri Lanka	1.04%
Taiwan	1.04%
UK	6.25%
USA	55.21%
Vietnam	1.04%

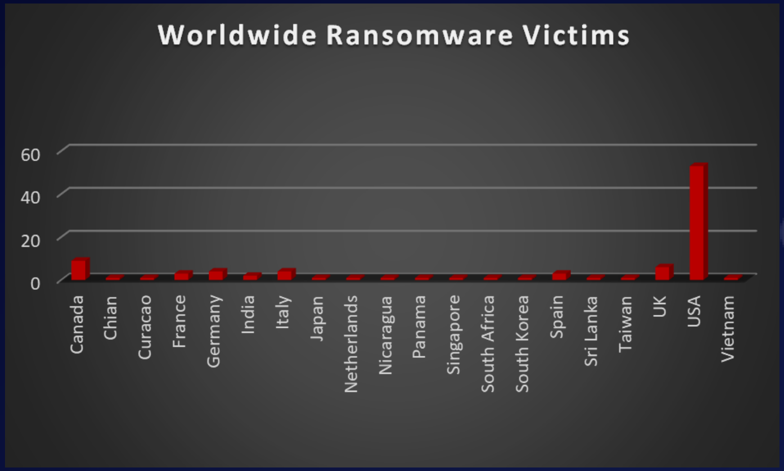

Figure 2: Ransomware Victims Worldwide

After conducting additional research, we found that ransomware has impacted 20 industries globally. Last week, the Manufacturing and Retail sectors were hit particularly hard, with 21% 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 (%)
Agriculture	1.04%
Business Services	8.33%
Cities, Towns & Municipalities	1.04%
Construction	8.33%
Consumer Services	1.04%
Education	3.13%
Energy, Utilities & Waste Treatment	8.33%
Finance	5.21%
Government	1.04%
Healthcare	5.21%
Hospitality	4.17%
Insurance	1.04%
IT	7.29%
Legal Service	4.17%
Manufacturing	21.88%
Media & Internet	1.04%
Real Estate	2.08%
Retail	9.38%
Telecom	2.08%
Transportation	4.17%

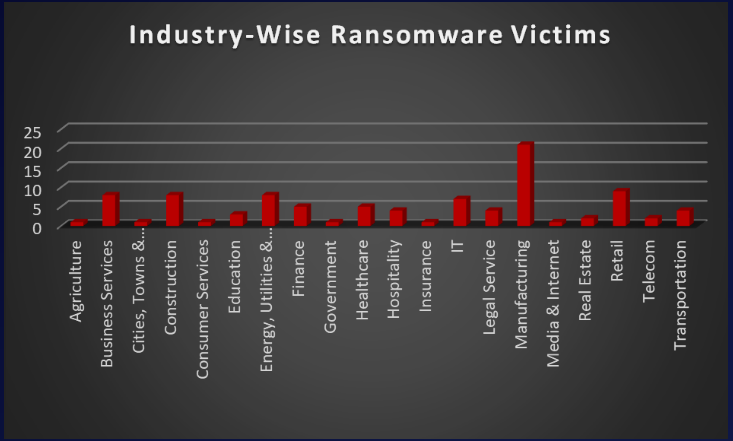

Figure 3: Industry-wise Ransomware Victims