Red Piranha
unified threat management

THREAT INTELLIGENCE REPORT

May 02 - 08, 2023

Report Summary:

- **New Threat Detection Added** – 5 (CVE-2023-21932, DarkCloud Stealer, Shellbot, Tsunami Malware, and RokRAT)
- **New Threat Protections**
- **Overall Weekly Observables Count**
- **Daily submissions by Observable Type**
- **New Ransomware Victims Last Week**

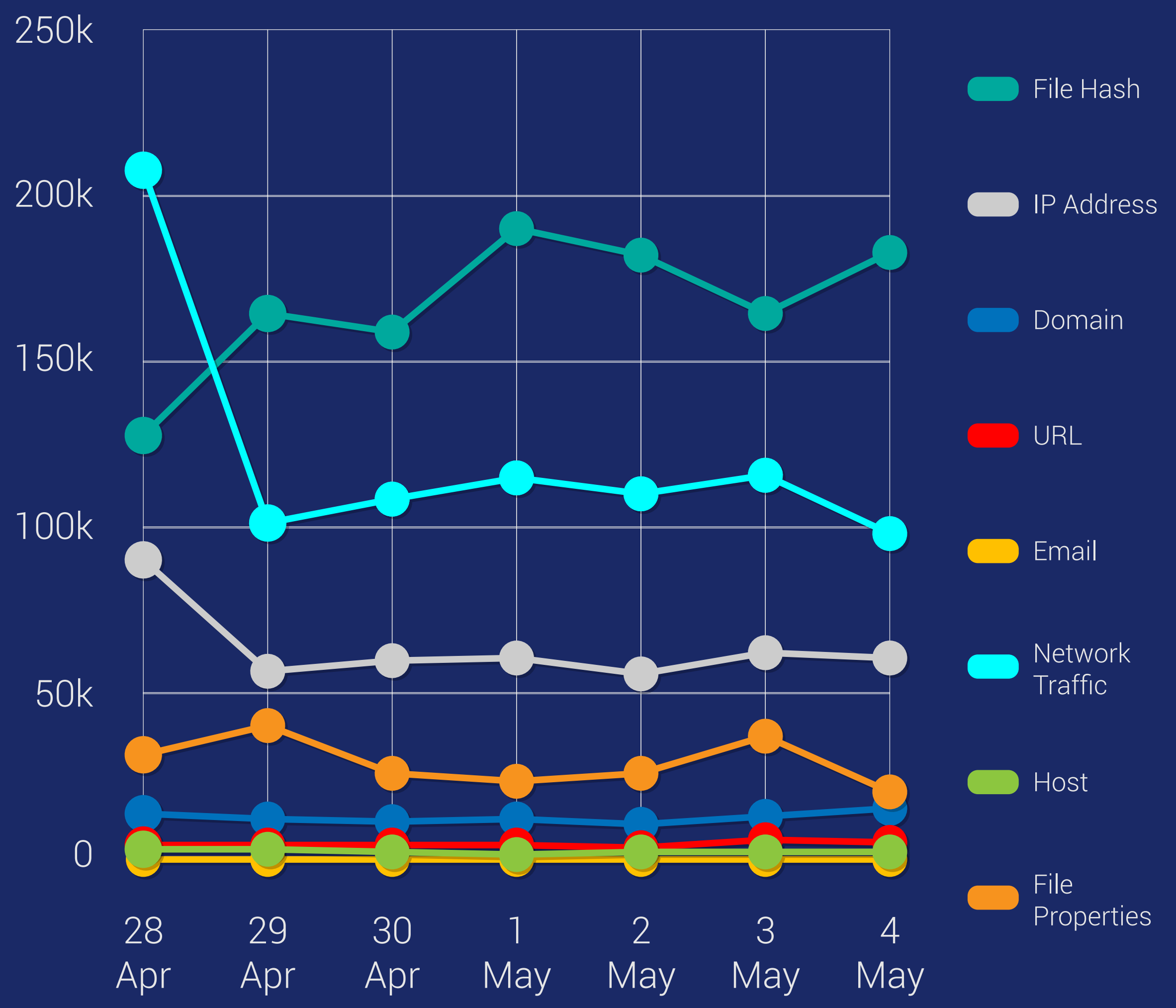
New Threat Protections (Week Ending 08/05/2023):

12

Overall Weekly Observables Count:

2,796,453

Daily Submissions by Observable Type:



Newly Detected Threats Added

1. Exploit for CVE-2023-21932

The Oracle Opera property management system was reported vulnerable to multiple exploits, including the ability for attackers to obtain the JNDI connection name through servlets that leak information. The system's weak hardcoded cryptography also makes it possible for attackers to create encrypted payloads and execute remote commands without authentication. Attackers can upload a web shell, leading to arbitrary command execution and potential lateral privilege escalation. Versions of Oracle Hospitality Opera 5 Property Services 5.6 and below are affected. A solution to this vulnerability is upgrading to the latest version of Opera, version 5.6 or higher.

Threat Protected: 01
Rule Set Type:

Ruleset	IDS: Action	IPS: Action
Balanced	Reject	Reject
Security	Reject	Drop
WAF	Disabled	Disabled
Connectivity	Alert	Alert
OT	Disabled	Disabled

Class Type: Attempted Admin
Kill Chain: Privilege Escalation TA0004 - Defence Evasion TA0005

2. DarkCloud Stealer

DarkCloud Stealer, a highly sophisticated infostealer, is being distributed through various spam campaigns. It starts with a phishing email containing a malicious link/attachment and copies itself into the system directory, creating a task scheduler entry for persistence. It loads the final payload written in Visual Basic (VB) into the memory of a running process and gathers sensitive data from multiple applications on the targeted system. The malware is capable of collecting system information, capturing screenshots, monitoring clipboard activities, and retrieving data from cryptocurrency applications. It also offers a crypto-swapping feature for popular cryptocurrencies like Bitcoin and Ethereum. The malware exfiltrates stolen data to the command and control (C2) server via different methods such as SMTP, Telegram, Web Panel, and FTP. The attackers behind DarkCloud Stealer target applications like web browsers, FileZilla, CoreFTP, and Pidgin.

Threat Protected: 01
Rule Set Type:

Ruleset	IDS: Action	IPS: Action
Balanced	Alert	Alert
Security	Reject	Drop
WAF	Disabled	Disabled
Connectivity	Alert	Alert
OT	Disabled	Disabled

Class Type: Trojan- Activity
Kill Chain: Initial Access T1566.001 - Execution T1204/T1053- Persistence T1053 - Defence Evasion T1140 - Credential Access T1555/T1539 - Discovery T1087/T1518 - Command-and-Control T1071

3. ShellBot

Shellbot malware enables the attackers to communicate with the C&C server to run commands within the victim machine. The C&C server, also called the IRC server in this scenario, can directly send some messages to its victims' machines to keep the communication channel alive and to specify what commands they must run. Its peculiarity is that the victim machine downloads and launches multiple binaries after the first execution. Many of them have the same purpose but are conceived for different OS (32/64 bits) and CPUs (arm, mips).

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: Malware
Kill Chain: Execution TA0002 - Privilege Escalation TA0004 - Defence Evasion TA0005 - Discovery TA0007

4. Tsunami Malware

The Tsunami malware can still give remote control access to malicious users. Thus, potential attackers can take full control of the infected systems and leverage them to exploit their computational resources or to propagate attacks elsewhere. Two files are downloaded on the infected machine sshexec and sshpass. The former is a bash script that sets some variables and arguments that later will be used as sshpass parameters.

The latter is an executable binary that seems like a mass executor for non-interactively performing password authentication with SSH. It can be used against a list of hosts previously received or set by the sshexec bash script.

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: Malware
Kill Chain: Defence Evasion T1027 - Credential Access T1003 - Discovery T1518.001 -Command-and-Control T1573

5. RokRAT

RokRAT is a remote access trojan used to steal sensitive information from victim machines. It was first discovered in 2017 targeting government sectors in South Korea as well as journalists, activists, and North Korean defectors. The infection scheme starts with lures using phishing emails or social engineering attacks. It sends seemingly interesting documents to its targets which contain LNK files that run malicious PowerShell scripts. One of many samples of RokRAT was observed to have utilised Twitter as its Command-and-Control server and others have used Yandex or Mediafire. The latest RokRAT samples analysed today rely on cloud storage for their Command-and-Control communications.

Threat Protected: 08
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 T1566 - Execution T1059 - Persistence T1547 - Command-and-Control T1071

Known exploited vulnerabilities (Week 4 April 2023):

Vulnerability	Description
CVE-2023-1389	TP-Link Archer AX-21 Command Injection Vulnerability
CVE-2021-45046	Apache Log4j2 Deserialization of Untrusted Data Vulnerability
CVE-2023-21839	Oracle WebLogic Server Unspecified Vulnerability

Updated Malware Signatures (Week 4 April 2023)

Threat	Description
Bifrost	A remote access trojan enables its operator to take control of a victim machine and steal data. It is usually distributed through spam and phishing emails.
Cerber	Another type of ransomware but instead of the usual ransom text files, it plays audio on the victim's infected machine.
Kuluoz	A backdoor for a botnet. It executes commands from a remote malicious user.
XtremeRAT	A remote access trojan interacts with the infected machine via a remote shell, uploads/downloads files, and records from a webcam/microphone.
Ramnit	A banking trojan used to steal online banking credentials.
njRAT	A remote access trojan typically spreads using phishing emails or social engineering tactics. It allows a threat actor to steal sensitive information, install additional malware, and control the victim's machine remotely.
Tofsee	A malware that is used to send spam emails, and conduct click frauds as well as crypto mining.

New Ransomware Victims Last Week: 109

Red Piranha proactively gathers information about organizations impacted by ransomware attacks through various channels, including the Dark Web. In the past week, our team identified a total of 109 new ransomware victims from 22 distinct industries across 22 countries worldwide. This highlights the global reach and indiscriminate nature of ransomware attacks, which can affect organizations of all sizes and sectors.

Blackbasta, a specific ransomware, has affected the largest number of new victims (23) spread across various countries. Akira and Alphv groups follow closely with each hitting 15 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
Akira	13.76%
Alphv	10.09%
Avoslocker	5.50%
Blackbasta	21.10%
Backbyte	0.92%
Clop	1.83%
Cuba	3.67%
Lockbit3	9.17%
Medusa	2.75%
Monti	1.83%
Play	8.26%
Qilin	7.34%
Rancoz	1.83%
Ransomhouse	2.75%
Royal	5.50%
Snatch	0.92%
Trigona	0.92%
Vicesociety	1.83%

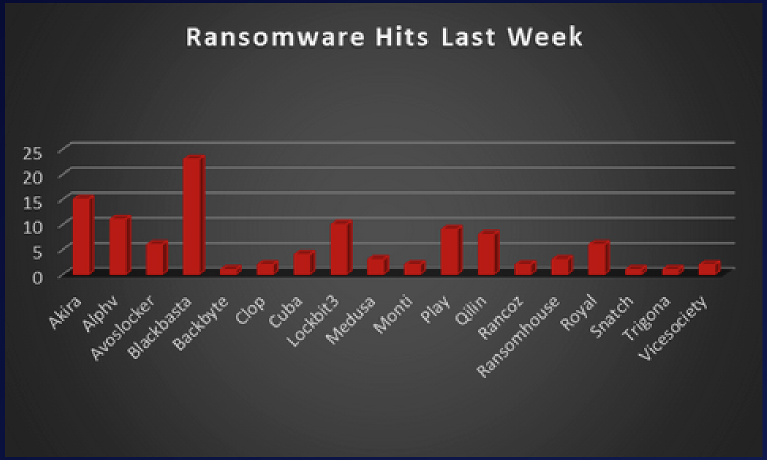


Figure 1: Ransomware Group Hits Last Week

When we examine the victims by country out of 22 countries around the world, we can conclude that the USA was once again the most ransomware-affected country, with a total of 71 new victims reported last week. The list below displays the number (%) of new ransomware victims per country.

Name of the affected Country	Number of Victims
Australia	1.83%
Austria	1.83%
Canada	10.09%
Colombia	0.92%
France	0.92%
Germany	1.83%
India	0.92%
Italy	1.83%
Japan	0.92%
Lebanon	0.92%
Mexico	0.92%
Netherlands	1.83%
Philippines	0.92%
Poland	0.92%
Serbia	0.92%
Singapore	1.83%
South Africa	0.92%
Spain	0.92%
Switzerland	0.92%
Turkey	0.92%
UK	1.83%
USA	65.14%

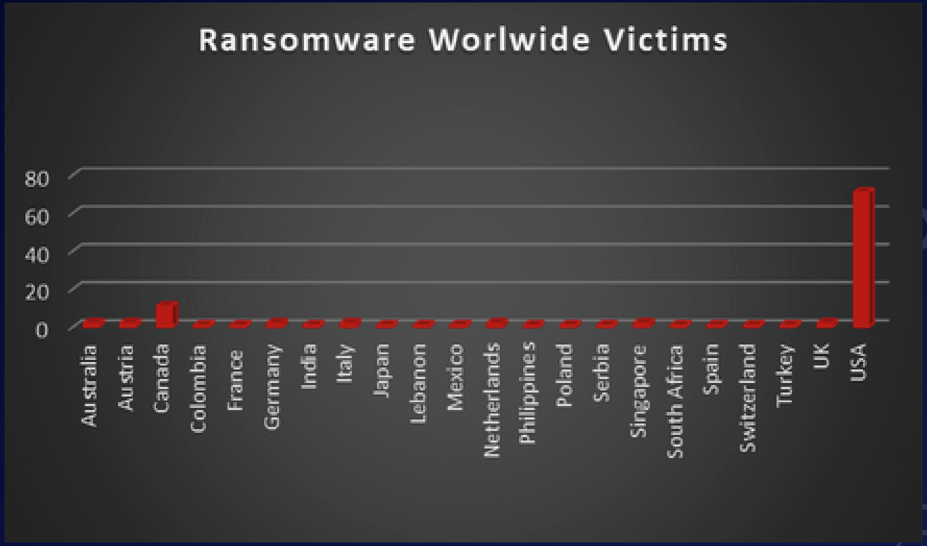


Figure 2: Ransomware Victims Worldwide

After conducting additional research, we found that ransomware has impacted 22 industries globally. Last week, the Manufacturing and Education sectors were hit particularly hard, with the loss of 19 and 12 businesses in each sector respectively. The table below presents the most recent ransomware victims sorted by industry.

Industry	Victims Count (%)
Agriculture	1.83%
Business Services	2.75%
Construction	6.42%
Consumer Services	0.92%
Education	11.01%
Energy	1.83%
Finance	3.67%
Government	1.83%
Healthcare	7.34%
Hospitality	1.83%
Insurance	1.83%
IT	3.67%
Legal Services	4.59%
Manufacturing	17.43%
Media	0.92%
Media & Internet	0.92%
Metal & Mining	0.92%
Organizations	1.83%
Real Estate	7.34%
Retail	9.17%
Telecommunications	2.75%

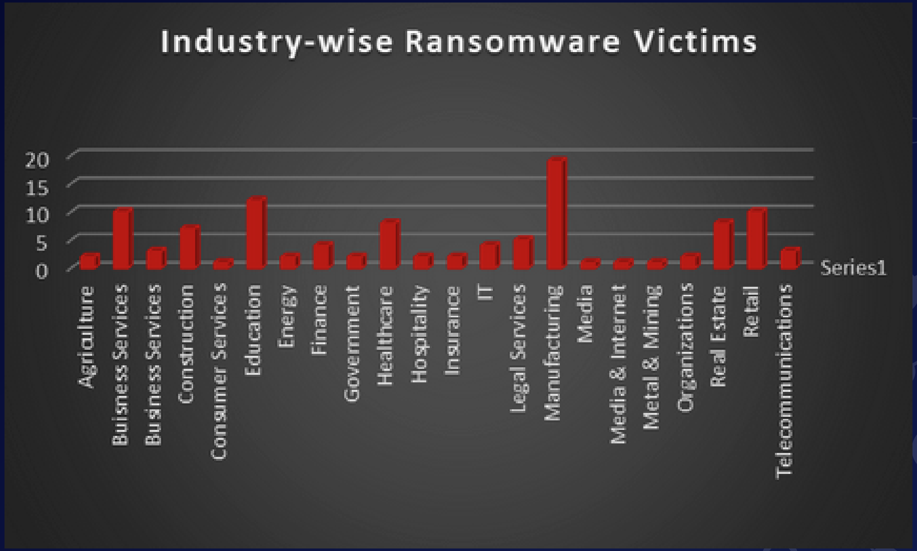


Figure 3: Industry-wise Ransomware Victims