
Red Piranha
unified threat management
THREAT INTELLIGENCE REPORT
Apr 18 - 24, 2023

Report Summary:

- **New Threat Detection Added** – 5 (CrossLock Ransomware DAAM Android Botnet, Sliver, CVE-2021-20090, and ScarCruft APT)
- **New Threat Protections**
- **Overall Weekly Observables Count**
- **Daily submissions by Observable Type**
- **New Ransomware Victims Last Week**

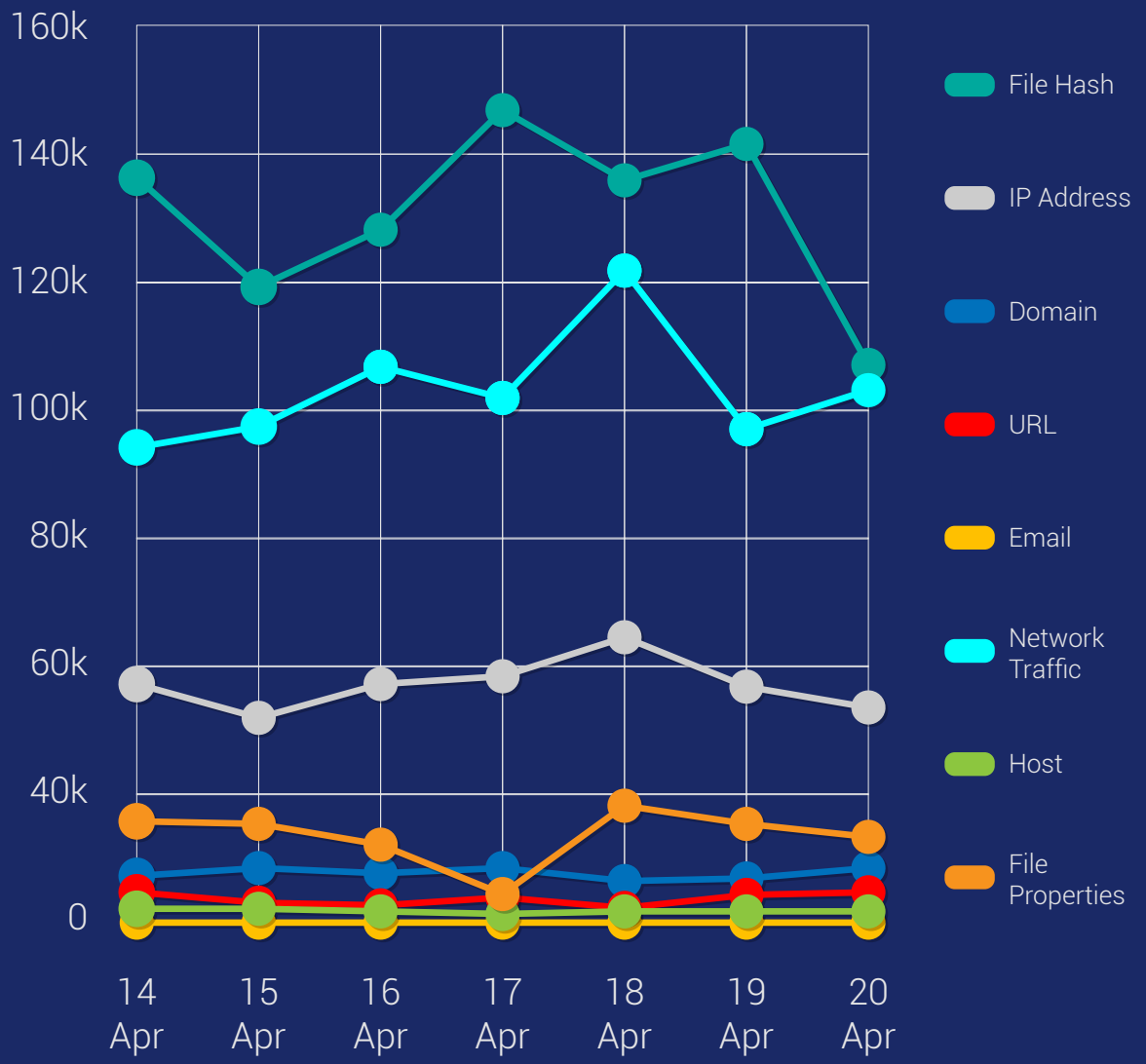
New Threat Protections (Week Ending 24/04/2023):

9

Overall Weekly Observables Count:

2,409,148

Daily Submissions by Observable Type:



Newly Detected Threats Added

1. CrossLock Ransomware

CrossLock is a newly emerged ransomware group that targets businesses, demanding a significant ransom in return. Along with encrypting the victim's files, the attackers also adopt double-extortion tactics by stealing sensitive data and threatening to release it on their onion leak site unless the ransom is paid. The threat actors behind the CrossLock ransomware have coded it using the Go programming language, which offers numerous advantages. One such benefit is the ability to compile a single codebase that can function across various operating systems. However, the use of Event Trace (ETW) bypass techniques by this ransomware is particularly concerning. This feature allows the malware to avoid detection by security systems that rely on event logs. Moreover, CrossLock Ransomware employs several measures to lower the chances of data recovery and increase the attack's effectiveness.

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/T1204/T1047 - Defence Evasion T1564/T1027/T1497/T1070 - Discovery T1082/T1135/T1083/T1057 - Impact T1486/T1490

2. DAAM Android Botnet

A new Android botnet called DAAM has been discovered which is being distributed through trojanised applications. This botnet is capable of executing a variety of malicious actions, including data theft, DDoS attacks, and spamming. It uses a Command-and-Control infrastructure to communicate with its operators and receive instructions. Technical details about the botnet's functionality and the trojanised applications being used to distribute it have been provided by the researchers. To prevent falling prey to such botnets, downloading apps from trustworthy sources is critical. As the DAAM botnet is a significant threat to Android users, it is necessary to stay vigilant and take necessary precautions to avoid being infected.

Threat Protected: 02
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 T1476/T1444 - Collection T1433/T1432/T1429/T1512/T1414 - Discovery T1418 - Persistence T1402 - Impact T1471

3. Sliver

Sliver is an adversarial attack simulation tool designed to elude security products developed by researchers at BishopFox cybersecurity company. Sliver was utilised as a beachhead for the initial infection toolchain. It is utilised in the ransomware delivery framework for attacks observed in the wild. Sliver deployed via active opportunistic scanning and possible exploitation of Log4j/VMware Horizon vulnerabilities. It is utilised in targeting organisations within the Government, Research, Telecom, and University sectors, in addition to sporadic victims of opportunity.

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 - Command-and-Control TA0011

4. CVE-2021-20090

A path traversal vulnerability in the web interfaces of networking devices manufactured by Arcadyan, including Buffalo WSR-2533DHPL2 firmware version <= 1.02 and WSR-2533DHP3 firmware version <= 1.24, could allow unauthenticated remote attackers to bypass authentication. The vulnerability exists due to a list of folders which fall under a "bypass list" for authentication. For most of the devices listed, that means that the vulnerability can be triggered by multiple paths. To have the pages load properly, one will need to use proxy match/replace settings to ensure any resources loaded which require authentication also leverage the path traversal.

Threat Protected: 01
Rule Set Type:

Class Type: Trojan-Activity
Kill Chain: Initial Access T1566 - Execution T1059 - Command-and-Control T1102/T1071

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

5. ScarCruft APT

ScarCruft is an APT group that has been observed to target the healthcare, telecommunications, and technology sectors. They are known to use a variety of TTPs including spear-phishing and watering hole attacks. They are attributed to the Operation Daybreak campaign where an Adobe 0-day was used. Such campaigns happened in early 2016 which also indicates that the APT group is constantly evolving.

Threat Protected: 04
Rule Set Type:

Class Type: Trojan-Activity
Kill Chain: Initial Access T1566 - Execution T1059 - Command-and-Control T1102/T1071

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

Known exploited vulnerabilities (Week 3 April 2023):

For more information, refer to the Forum – Security Advisory

Vulnerability	Description
CVE-2023-2033	Google Chromium V8 Engine Type Confusion Vulnerability
CVE-2019-8526	Apple macOS Use-After-Free Vulnerability
CVE-2017-6742	Cisco IOS and IOS XE Software SNMP Remote Code Execution Vulnerability

Updated Malware Signatures (Week 3 April 2023)

Threat	Description
TeslaCrypt	A ransomware that started in the year 2015. It is usually distributed through spam email campaigns, malicious attachments, and exploit kits.
Zeus	Also known as Zbot and is primarily designed to steal banking credentials
DarkKomet	A remote access trojan that can take full control over an infected machine.
Bunitu	A malware that turns infected machines into a Proxy server for threat actors – also belongs to a family of botnets

New Ransomware Victims Last Week: 83

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 83 new ransomware victims from 19 distinct industries across 28 countries worldwide. This highlights the global reach and indiscriminate nature of ransomware attacks, which can affect organisations of all sizes and sectors.

LockBit 3.0, a specific ransomware, has affected the largest number of new victims (24) spread across various countries. Ransomware blog and Royal groups follow closely with each hitting 21 and 06 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
Abyss-data	1.20%
Alphv	4.82%
Blackbyte	3.61%
Crosslock	1.20%
Cryptnet	2.41%
Dunghill	2.41%
Everest	1.20%
Karakurt	2.41%
Lockbit3	28.92%
Medusa	2.41%
Play	6.02%
Ransomware blog	25.30%
Royal	7.23%
Trigona	7.23%
Unsafe	1.20%
Vicesociety	2.41%

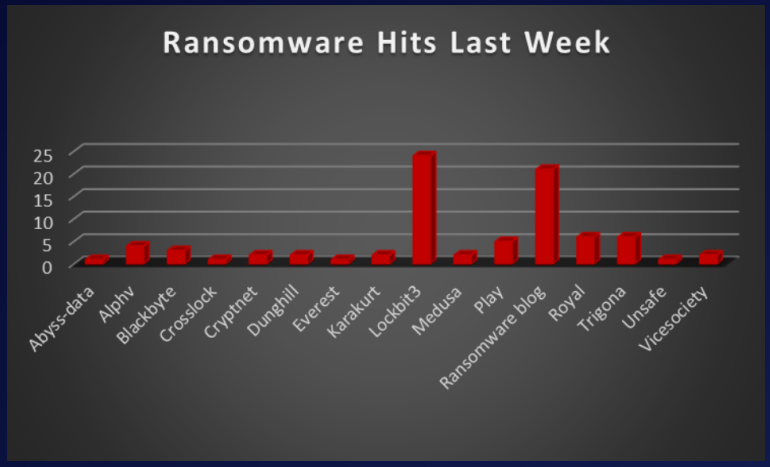


Figure 1: Ransomware Group Hits Last Week

When we examine the victims by country out of 28 countries around the world, we can conclude that the USA was once again the most ransomware-affected country, with a total of 37 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
Angola	1.20%
Australia	1.20%
Brazil	3.61%
Canada	4.81%
France	6.02%
Germany	3.61%
Hong Kong	1.20%
Ireland	2.41%
Israel	2.41%
Italy	2.41%
Japan	2.41%
Mexico	1.20%
Netherlands	2.41%
New Zealand	1.20%
Nigeria	1.20%
Philippines	1.20%
Portugal	1.20%
Romania	1.20%
Slovakia	1.20%
Spain	1.20%
Sweden	1.20%
UAE	2.41%
UK	6.02%
USA	44.58%
Venezuela	1.20%
Vietnam	1.20%

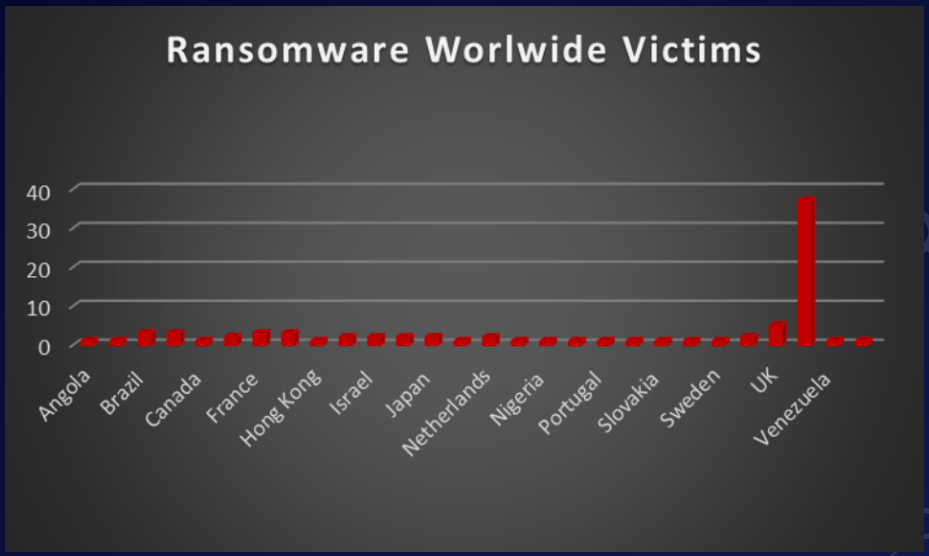


Figure 2: Ransomware Victims Worldwide

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 the loss of 17 and 06 businesses in each sector respectively. The table below presents the most recent ransomware victims sorted by industry.

Industry	Victims Count (%)
Healthcare	4.82%
Agriculture	1.20%
Business Services	9.64%
Construction	7.23%
Consumer Services	6.02%
Education	6.02%
Electricity, Oil & Gas	1.20%
Energy	2.41%
Finance	7.23%
Government	4.82%
Healthcare	2.41%
Hospitality	4.82%
Insurance	3.61%
IT	4.82%
Legal Services	3.61%
Manufacturing	20.48%
Media & Internet	1.20%
Retail	6.02%
Telecommunications	2.41%

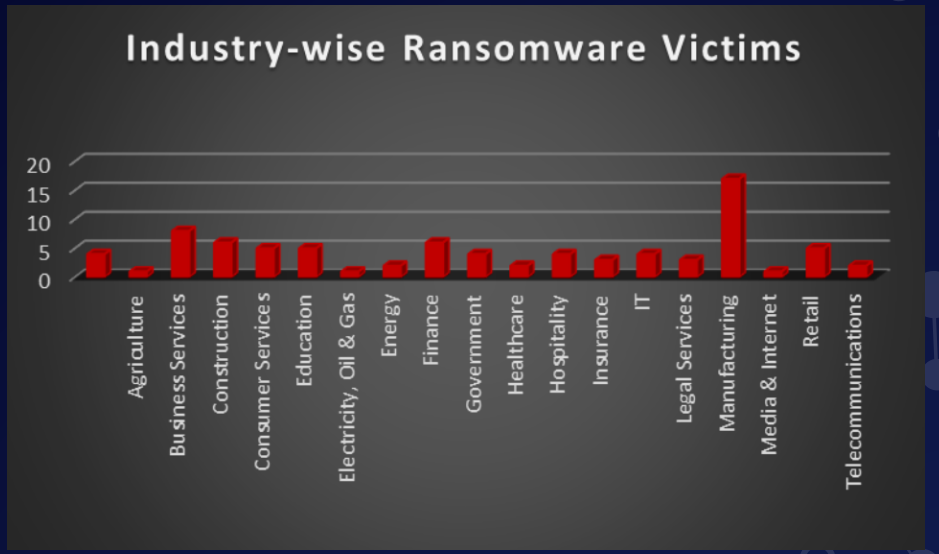


Figure 3: Industry-wise Ransomware Victims