Red Piranha
unified threat management

THREAT INTELLIGENCE REPORT

Apr 04 - 10, 2023

Report Summary:

- **New Threat Detection Added** – 6 (Snake Keylogger, Typhon Reborn V2, Tampered NetSupport Manager, Gamaredon APT, RapperBot, and Adwind RAT)
- **New Threat Protections**
- **Overall Weekly Observables Count**
- **Daily submissions by Observable Type**
- **New Ransomware Victims Last Week**

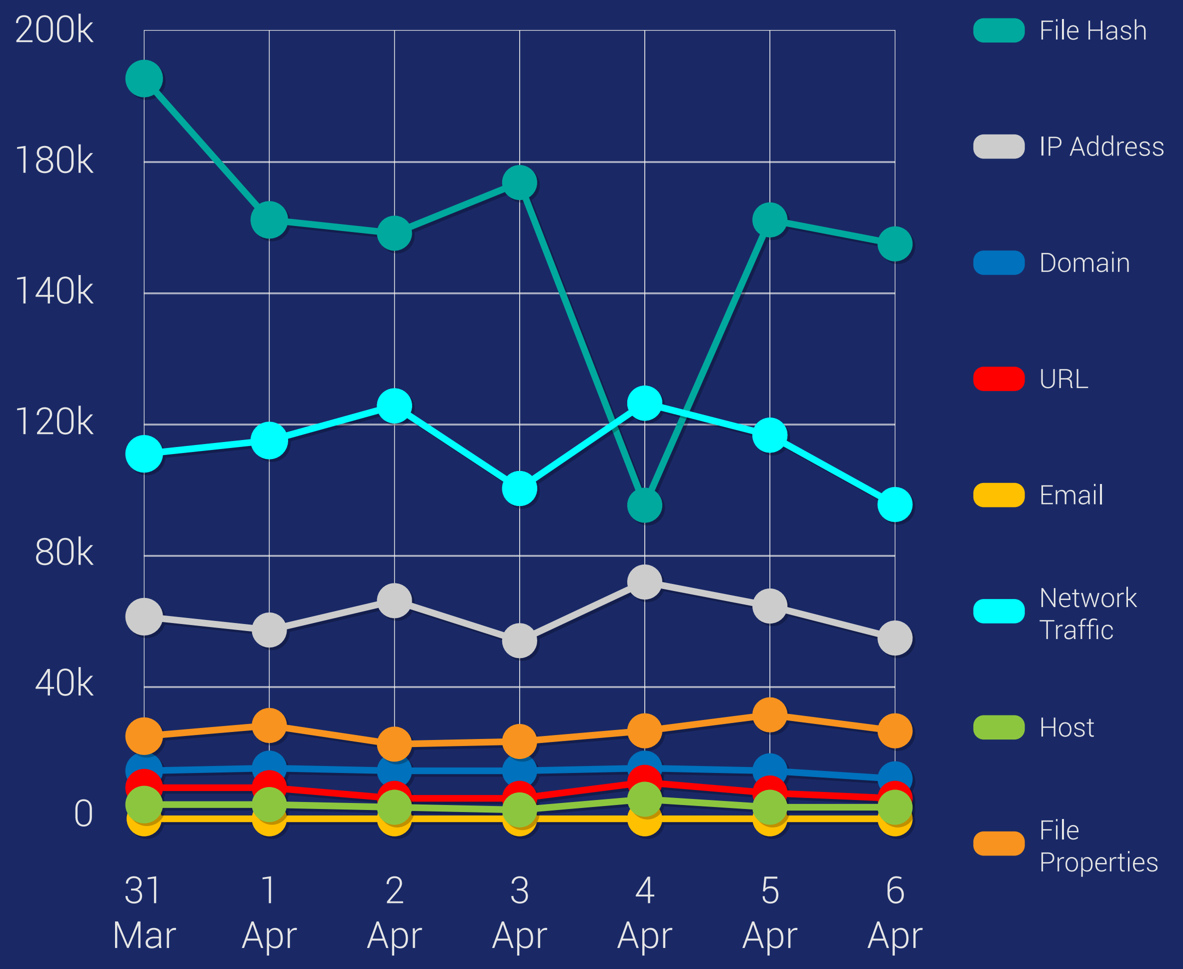
New Threat Protections (Week Ending 10/04/2023):

27

Overall Weekly Observables Count:

2,751,307

Daily Submissions by Observable Type:



Newly Detected Threats Added

1. Snake Keylogger

Researchers have discovered a new variant of the Snake Keylogger malware, which is designed to steal sensitive information from Microsoft Windows users, including saved credentials, keystrokes, screenshots, and clipboard data. This variant was found in a Microsoft Excel sample used to spread the malware. The Snake Keylogger family has been increasing in popularity and is now one of the top 10 malware families. The blog post provides details on how this variant is downloaded, executed, and protected from the analysis. The impact of this malware is considered critical due to the sensitive information it collects from its victims.

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: Privilege Escalation T1055 - Defence Evasion T1036/T1055/T1497 - Discovery T1012/T1018/T1082 - Command-and-Control T1071/T1095/T1573

2. Typhon Reborn V2

Typhon is an information stealer that was first reported in mid-2022 and is designed to steal sensitive information, including cryptocurrency wallet data, from various applications. It has undergone continuous development, with the latest version, Typhon Reborn V2, being released in January 2023, which includes improved anti-analysis and anti-virtual machine capabilities to evade detection. The malware is being sold on underground forums for $59 per month or $540 for a lifetime subscription, which is relatively cheap compared to other info stealers. Typhon Reborn 2 has been observed in the wild, and it is expected to be used in future attacks to harvest and exfiltrate sensitive information via the Telegram API.

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: Execution T1047/T1053/T1064/T1106 - Persistence T1053 - Privilege Escalation T1053 - Defence Evasion T1027/T1036/T1064/T1112 - Credential Access T1003/T1056 -Discovery T1010/T1016/T1018 - Collection T1005/T1056 - Command-and-Control T1071 -Impact T1496

3. Tampered NetSupport Manager

NetSupport Manager is a legitimate software used by helpdesk or service desk professionals to remotely access computers. However, it has been discovered recently that some malware includes a tampered version of NetSupport Manager to gain unauthorized access to computers. It is usually distributed via a phishing email and when the malware is executed, it allows its operator to gain access to the victim's machine and steal sensitive data.

Threat Protected: 04
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 - Command-and-Control T1102

4. Gamaredon APT

Gamaredon is an APT group that is known to conduct cyber espionage campaigns against military and government organisations. They have been linked or attributed to various attacks against the Ukraine government. It was recently observed to be targeting the energy sector of different regions worldwide.

Newly discovered domains attributed to Gamaredon have been identified and were added as rules to the Crystal Eye for detection and prevention.

Threat Protected: 16
Rule Set Type:

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

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

5. RapperBot

RapperBot exclusively scans and attempts to brute force SSH servers configured to accept password authentication. The bulk of the malware code contains an implementation of an SSH 2.0 client that can connect and brute force any SSH server that supports Diffie-Hellmann key exchange with 768-bit or 2048-bit keys and data encryption using AES128-CTR. Once RapperBot successfully brute forces an SSH server, the valid credentials are reported to the C2 server on a separate port (currently 48109) without executing further commands on the remote victim.

Threat Protected: 02
Rule Set Type:

Class Type: Malware
Kill Chain: Defence Evasion TA0005 - Discovery TA0007 - Command-and-Control TA0011

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

6. Adwind RAT

Adwind RAT is a cross-platform, multifunctional remote access program which is distributed through a single malware-as-a-service platform. It checks the system to see if it is running in a Virtual Environment. Adwind RAT infects the victim's machine by initial infection vectors of spam campaigns with attachment (EML), and a suspicious URL to download the malware. The attachment is an MS Word document (.DOCX). The threat actor can trick the user to click on the blurred image to view the document's content. Once the user opens the .img content, use the embedded doc to drop the .JAR file in the %temp% folder to start infecting and perform the threat actor's action on the objective.

Threat Protected: 02
Rule Set Type:

Class Type: Trojan-activity
Kill Chain: Defence Evasion TA0005 - Discovery TA0007

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

Threat	Description
Parite	Also known as the W32/Parite Virus which infects Windows computers and is classified as a polymorphic virus
Ramnit	A banking trojan used to steal online banking credentials
QQhelper	A trojan downloader in the guise of a browser toolbar
KATES	A malware designed to steal FTP credentials
DarkKomet	A remote access trojan that can take full control over an infected machine.
Zeus	Also known as Zbot and is primarily designed to steal banking credentials
HawkEye	A trojan and keylogger used to steal various account credentials
Expiro	A malware that installs browser extensions, modifies security settings and steals information from infected machines
Kuluoz	A backdoor for a botnet. It executes commands from a remote malicious user
Nymeria	A remote access trojan is written in AutoIT language designed for automation. This trojan is designed to steal information and upload the contents to its command-and-control server.
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: 63

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 63 new ransomware victims from 17 distinct industries across 12 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 (17) spread across various countries. Alphv and Royal groups follow closely with each hitting 13 and 10 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
Alphv	20.63%
Bianlian	3.17%
Clop	1.59%
Karakurt	3.17%
Lockbit3	26.98%
Lorenz	7.94%
Medusa	6.35%
Ransomhouse	1.59%
Royal	15.87%
Snatch	3.17%
Stormous	9.52%

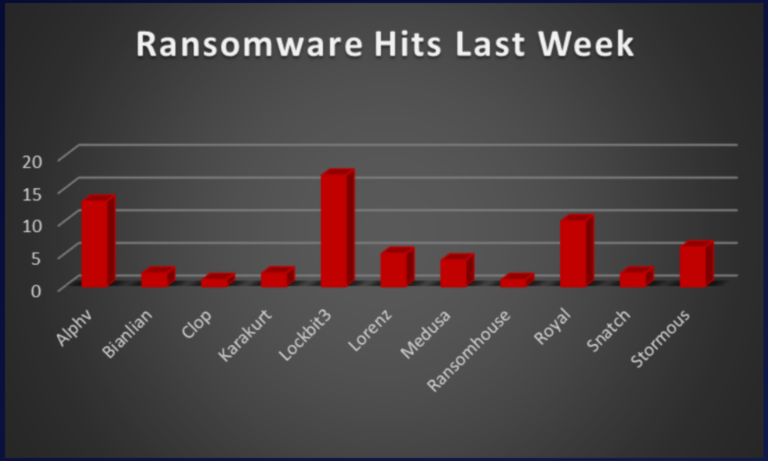


Figure 1: Ransomware Group Hits Last Week

When we examine the victims by country out of 12 countries around the world, we can conclude that the USA was once again the most ransomware-affected country, with a total of 44 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	1.59%
Belgium	1.59%
Cyprus	1.59%
Denmark	1.59%
Egypt	1.59%
France	1.59%
Italy	7.94%
Malaysia	1.59%
Spain	3.17%
Switzerland	1.59%
UK	6.35%
USA	69.84%

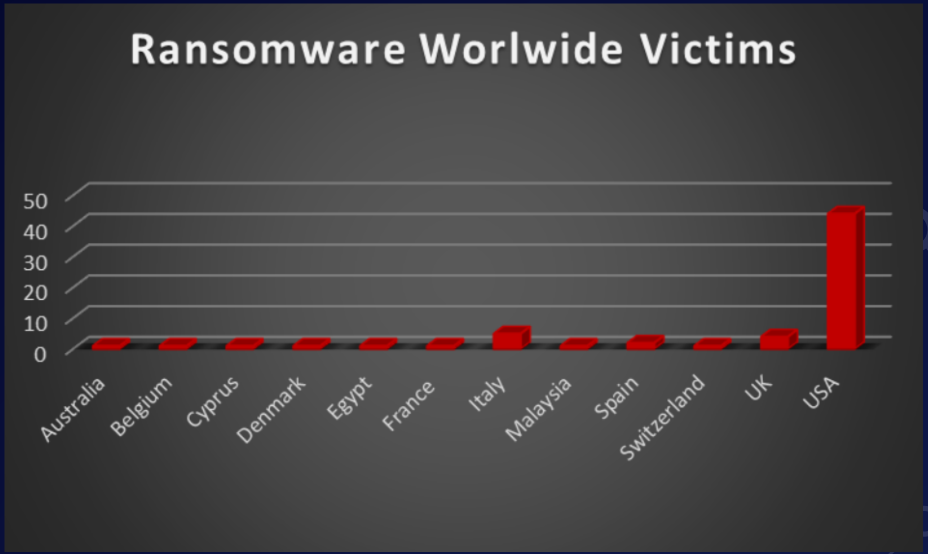


Figure 2: Ransomware Victims Worldwide

After conducting additional research, we found that ransomware has impacted 17 industries globally. Last week, the manufacturing and Business Services sectors were hit particularly hard, with the loss of 14 and 07 businesses in each sector respectively. The table below presents the most recent ransomware victims sorted by industry.

Industry	Victims Count (%)
Business Services	11.11%
Construction	11.11%
Consumer Services	1.59%
Education	6.35%
Finance	1.59%
Healthcare	3.17%
Hospitality	1.59%
Insurance	3.17%
IT	6.35%
Legal Services	3.17%
Manufacturing	22.22%
Media & Internet	1.59%
Organisations	1.59%
Real Estate	6.35%
Retail	9.52%
Telecommunications	6.35%
Transportation	3.17%

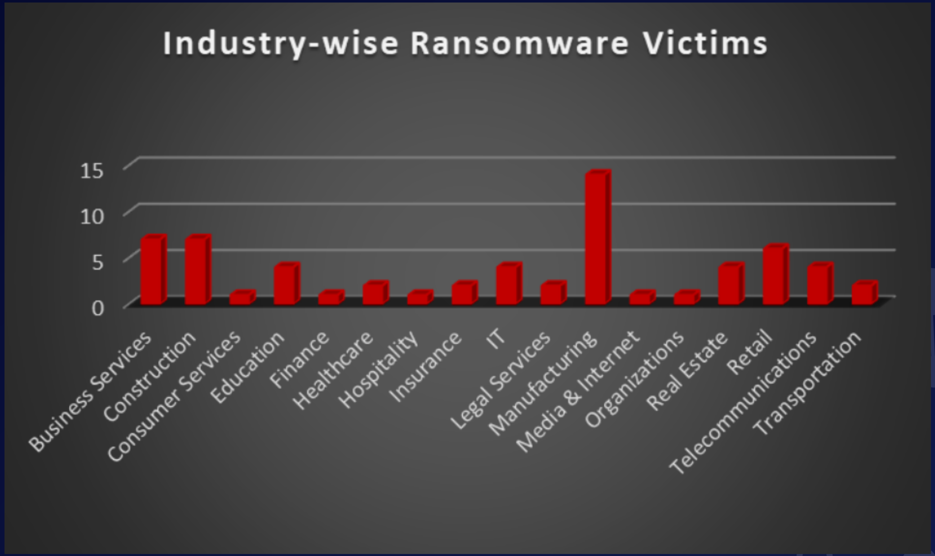


Figure 3: Industry-wise Ransomware Victims