Red Piranha
unified threat management

THREAT INTELLIGENCE REPORT

Mar 28 - Apr 03, 2023

Report Summary:

- **New Threat Detection Added** – 5 (Laplas Malware, Cinoshi Stealer, SideCopy APT, WhiskerSpy Backdoor, and 3CX Supply Chain Attack)
- **New Threat Protections**
- **Overall Weekly Observables Count**
- **Daily submissions by Observable Type**
- **New Ransomware Victims Last Week**

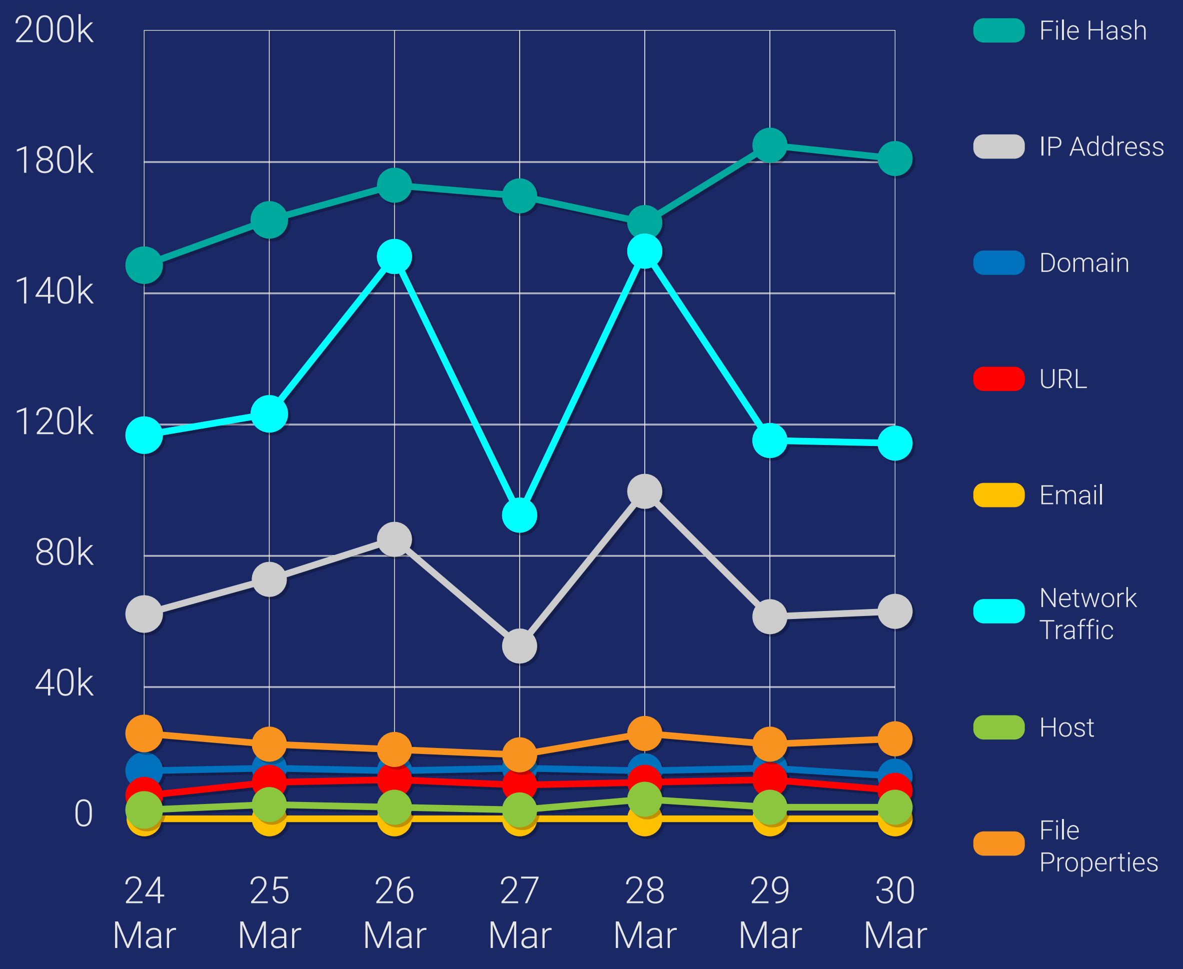
New Threat Protections (Week Ending 03/04/2023):

26

Overall Weekly Observables Count:

2,931,972

Daily Submissions by Observable Type:



Newly Detected Threats Added

1. Laplas Malware

The clipper malware family has been noticed using a new malware in their attacks termed Laplas. This malware hijacks a cryptocurrency transaction by swapping a victim's wallet address with the wallet address owned by TAs. When a user tries to make a payment from their cryptocurrency account, it redirects the transaction to TAs account instead of their original recipient. Clipper malware performs this swap by monitoring the clipboard of the victim's system, where copied data is stored. Whenever the user copies data, the clipper verifies if the clipboard data contains any cryptocurrency wallet addresses. If found, the malware replaces it with the TAs wallet address, resulting in the victim's financial loss.

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: Malware
Kill Chain: Execution T1204 – Persistence T1053 - Privilege Escalation T1055 - Defence Evasion T1027 – Discovery T1057 - Command-and-Control T1071

2. Cinoshi Stealer

The Cinoshi Stealer is a type of Trojan malware that is used to steal sensitive information from a victim's computer system. It uses several anti-tampering techniques, such as heavy obfuscation and modifying its code during runtime, to make it difficult to analyse and hinder its detection. After execution, it fetches a Command-and-Control (C&C) URL and acquires various .NET dependencies files from it. The stealer targets sensitive data from web browsers, crypto wallets, and popular applications such as Discord, Telegram, and Steam. It stores the stolen data in a zip file and exfiltrates it through POST requests to a C&C server. Finally, it deletes the zip archive to remove traces of its activities.

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 T1204 - Persistence T1547/T1053 - Defence Evasion T1027- Credential Access T1555/T1539 - Collection T1113 - Discovery T1087 /T1518 - Command-and-Control T1071 - Exfiltration T1041/T1567 - Impact T1489

3. SideCopy APT

SideCopy is a sophisticated APT group known for emulating the tactics of the Sidewinder APT in order to distribute its own malware. The group's attack strategy often involves using malicious LNK files to initiate a complex chain of infection, which includes multiple HTAs and loader DLLs. These tactics are designed to evade detection and ultimately lead to the deployment of the group's final payloads. Notably, SideCopy has been observed targeting government and military officials in India and Afghanistan. The group's tactics are continuously evolving, with new tools regularly incorporated into its arsenal, making it a formidable adversary for security professionals.

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: Initial Access T1566 - Execution T1204 - Defence Evasion T1036/T1218 - Persistence T1547/T1047 - Discovery T1016/T1057 - Collection T1185 - Command-and-Control T1071/T1105

4. WhiskerSpy Backdoor

A new backdoor termed WhiskerSpy has been observed targeting Korean websites and using them to gain access to user devices. This attack method is known as a watering hole attack where the attacker compromises an infrastructure where the targeted users might frequently visit and use that website to gain access to the user's devices. This attack was targeted only to some users, i.e., if the visitor is not from the targeted IP addressed, the pop-up with a malicious payload will not appear. This made it more difficult to identify the attack. The targeted victim Ip's are mainly from China, Japan, and Brazil.

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: Backdoor
Kill Chain: Privilege Escalation TA0004 - Defence Evasion TA0005 - Credential Access TA0006 - Discovery TA0007 - Collection TA0009

5. 3cx Supply Chain Attack

3CX has recently been a victim of a supply chain attack. The attackers breached the update server of 3CX and replaced the legitimate update files with malicious ones. This allowed them to distribute a backdoor trojan to 3CX users who installed the affected updates. The attack was detected in early March 2023 and 3CX has since released a security update to fix the issue. However, it is unclear how many users may have been affected and what data may have been compromised. It is important for 3CX users to update their software to the latest version and to be vigilant for any signs of suspicious activity.

Red Piranha's Crystal Eye has deployed rules based on verified Indicators-of-Compromise in order to detect and prevent traffic attributed to this supply chain attack

Threat Protected: 21
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 T1195 - Execution T1204 - Command-and-Control T1071

New Ransomware Victims Last Week: 110

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 110 new ransomware victims from 21 distinct industries across 29 countries worldwide. This highlights the global reach and indiscriminate nature of ransomware attacks, which can affect organisations of all sizes and sectors.

Clop, a specific ransomware, has affected the largest number of new victims (22) spread across various countries. LockBit 3.0 and Stormous groups follow closely with each hitting 21 and 20 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	1.82%
Alphv	5.45%
Bianlian	1.82%
Blackbasta	7.27%
Clop	20.00%
Daixin	0.91%
Karakurt	0.91%
Lockbit3	19.09%
Mallox	0.91%
Medusa	0.91%
Play	10.91%
Ransomhouse	3.64%
Royal	5.45%
Snatch	0.91%
Stormous	18.18%
Vicesociety	1.82%

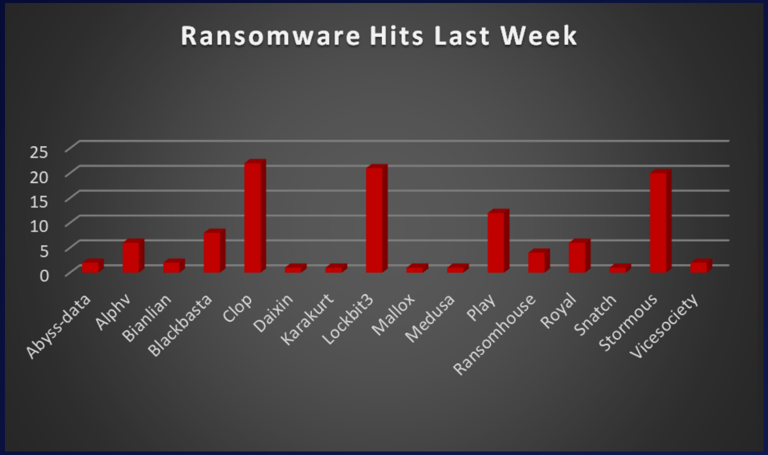


Figure 1: Ransomware Group Hits Last Week

When we examine the victims by country out of 29 countries around the world, we can conclude that the USA was once again the most ransomware-affected country, with a total of 51 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	3.64%
Bahrain	0.91%
Belgium	0.91%
Brazil	1.82%
Cameroon	0.91%
Canada	3.64%
Chile	0.91%
Education	0.91%
Estonia	0.91%
Europe	0.91%
Finland	0.91%
France	5.45%
Germany	2.73%
India	5.45%
Italy	1.82%
Japan	0.91%
Kenya	0.91%
Korea	0.91%
Malaysia	0.91%
Mexico	0.91%
Netherlands	0.91%
Poland	0.91%
Qatar	0.91%
South Africa	0.91%
Spain	3.64%
Turkey	1.82%
UAE	1.82%
UK	6.36%
USA	46.36%

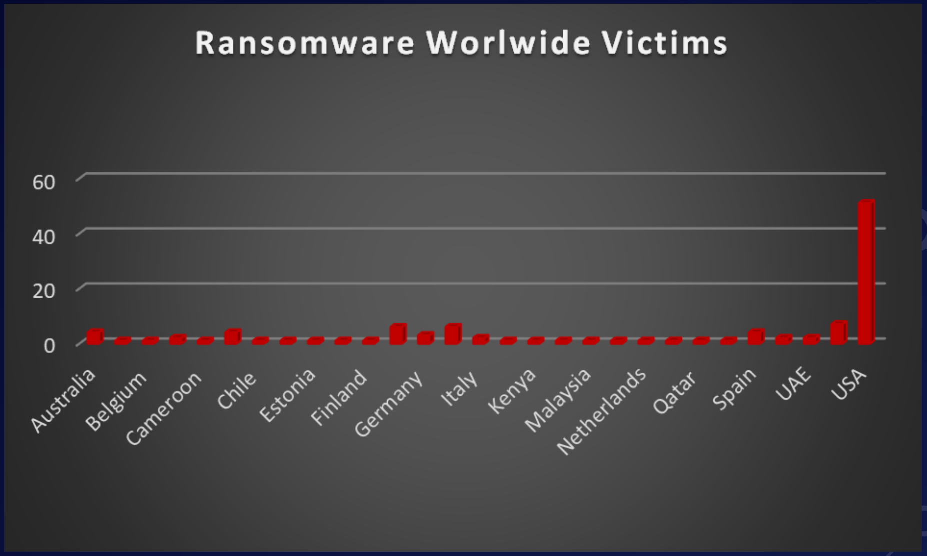


Figure 2: Ransomware Victims Worldwide

After conducting additional research, we found that ransomware has impacted 21 industries globally. Last week, the manufacturing and Business Services sectors were hit particularly hard, with the loss of 22 and 12 businesses in each sector respectively. The table below presents the most recent ransomware victims sorted by industry.

Industry	Victims Count (%)
Legal Services	4.55%
Automobile	0.91%
Business Services	10.91%
Construction	4.55%
Consumer Services	0.91%
Education	8.18%
Energy	3.64%
Finance	4.55%
Government	2.73%
Healthcare	2.73%
Hospitality	5.45%
Insurance	6.36%
IT	3.64%
Manufacturing	20.00%
Media	2.73%
Metals & Mining	1.82%
Organisations	2.73%
Real Estate	2.73%
Retail	6.36%
Telecommunications	0.91%
Transportation	3.64%

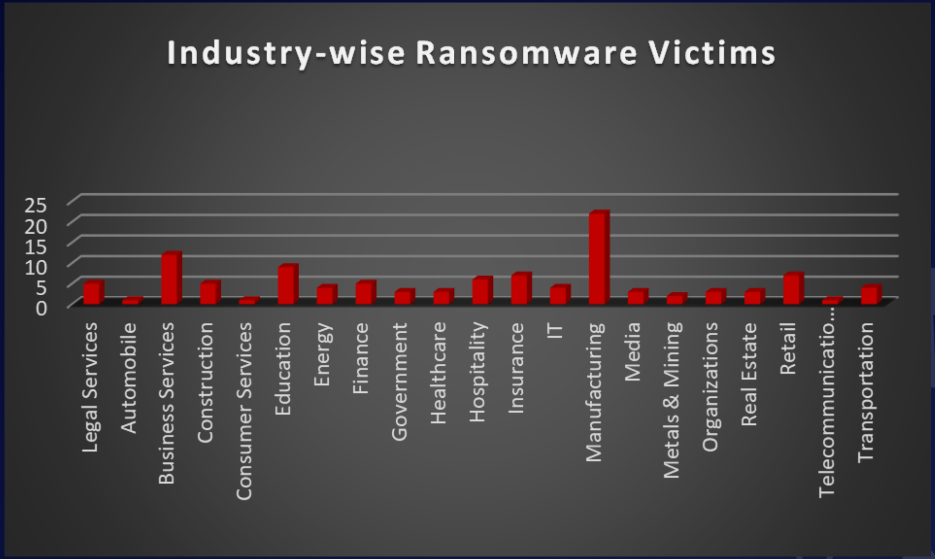


Figure 3: Industry-wise Ransomware Victims