Red Piranha
unified threat management

THREAT INTELLIGENCE REPORT

June 13 - 19, 2023

Report Summary:

- **New Threat Detection Added** – 4 (RisePro Stealer, DoubleFinger Malware, Jockerspy, and GravityRAT)
- **New Threat Protections**
- **Overall Weekly Observables Count**
- **Daily submissions by Observable Type**
- **New Ransomware Victims Last Week - 132**

Newly Detected Threats Added

1. RisePro Stealer

RisePro Stealer, closely resembling Vidar, is an insidious information-stealing malware that operates by collecting sensitive data and exporting it in log format. Developed using C++ programming language, RisePro is commonly distributed through PrivateLoader, a malware downloader. The creators of this malicious software have resorted to selling it on the popular messaging platform Telegram. Primarily, cybercriminals exploit information stealers like RisePro to extract valuable credentials such as usernames, passwords, credit card details, social security numbers, and ID card information. One prevalent technique employed by stealers involves keylogging, which records keyboard inputs. Infections often commence when victims unknowingly download the PrivateLoader malware, typically facilitated through malicious email links or attachments, counterfeit software updates, pirated/cracked software pages, P2P networks, third-party downloaders, or free file hosting sites. Various file formats, including malicious MS Office and PDF documents, ISO files, archives like ZIP or RAR, executables, and JavaScript files, are employed by threat actors to disseminate this malware.

Threat Protected: 04
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: Trojan-activity
Kill Chain: Initial Access T1476/T1444 - Collection T1432/T1412/T1512/T1513 - Discovery T1418

2. DoubleFinger Malware

Researchers have uncovered a sophisticated attack leveraging the DoubleFinger loader, accompanied by the cryptostealer GreetingGhoul and the remote-access Trojan Remcos. This multistage attack, resembling an advanced persistent threat (APT), begins with a malicious PIF file delivered via email. The stages of the attack involve executing shellcodes, downloading encrypted components from Imgur.com, bypassing security software, and replacing legitimate processes. The final payload, GreetingGhoul, steals cryptocurrency wallet data and intercepts user input, allowing cybercriminals to gain control and withdraw funds. Additionally, some variations of DoubleFinger install the remote access Trojan Remcos, granting complete surveillance and control over the compromised system. This attack demonstrates a high level of technical sophistication and poses a significant threat to victims' digital assets and privacy.

Threat Protected: 03
Rule Set Type:

Class Type: Trojan- Activity
Kill Chain: Execution TA0002/T1204 - Persistence T1547 - DefenCe Evasion TA0005/T1070

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

3. Jockerspy

Jockerspy malware is a highly sophisticated and malicious form of spyware that poses significant threats to individuals and organisations alike. By infiltrating computer systems through various delivery mechanisms, such as malicious email attachments or compromised websites, Jockerspy establishes its presence and employs persistence techniques to evade detection. Once active, it establishes communication with its command-and-control infrastructure to receive instructions and transmit stolen data. With its extensive information-gathering capabilities, remote control functionality, and data exfiltration techniques, Jockerspy enables attackers to monitor activities, access files, and exfiltrate sensitive information. Its ability to propagate within networks further amplifies its potential for widespread damage. Understanding the operational intricacies of Jockerspy is crucial for implementing effective cybersecurity measures to protect against this potent threat.

Threat Protected: 01
Rule Set Type:

Class Type: Trojan- Activity
Kill Chain: Persistence TA0003 - Privilege Escalation TA0004 - Defence Evasion TA0005 - Discovery TA0007 - Command-and-Control TA0011

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

4. GravityRAT

GravityRAT is a highly advanced and sophisticated remote access Trojan (RAT) that poses a significant threat in the world of cybersecurity. Known for its stealthy capabilities and targeted attacks, GravityRAT enables remote control and surveillance of infected systems, allowing attackers to gain unauthorised access, steal sensitive information, and execute malicious commands. With its ability to evade detection, propagate within networks, and gather intelligence, GravityRAT poses a serious risk to individuals, organisations, and even governments, highlighting the need for robust cybersecurity measures to combat this formidable malware.

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
Kill Chain: Reconnaissance T1590 - Weaponization T1027- Delivery T1566- Exploitation T1203 - Installation T1059 - Command-and-Control T1102 - Lateral Movement T1570 - Collection T1119 - Exfiltration T1041

Known exploited vulnerabilities (Week 3 June 2023):

Vulnerability	Description
CVE-2023-27997	Fortinet FortiOS and FortiProxy SSL-VPN Heap-Based Buffer Overflow Vulnerability

Updated Malware Signatures (Week 3 June 2023)

Threat	Description
Kuluoz	A backdoor for a botnet. It executes commands from a remote malicious user.
Redline	A .NET-based information stealer malware.
Upatre	A malware dropper that downloads additional malware on an infected machine. It is usually observed to drop banking trojan after the initial infection.
Nanocore	The Nanocore trojan, built on the .NET framework, has been the subject of multiple source code leaks, resulting in its widespread accessibility. Similar to other remote access trojans (RATs), Nanocore empowers malicious actors with complete system control, enabling activities such as video and audio recording, password theft, file downloads, and keystroke logging.
Ap0calypseRAT	A Remote Access Trojan dropped by other malware. It periodically shows up on hacking forums.
Ramnit	A banking trojan used to steal online banking credentials.
Zeus	Also known as Zbot and is primarily designed to steal banking credentials.
Valyria	A Microsoft Word-based malware which is used as a dropper for second-stage malware.
Cerber	Another type of ransomware but instead of the usual ransom text files, it plays audio on the victim's infected machine.

New Ransomware Victims Last Week: 132

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 132 new ransomware victims from 21 distinct industries across 32 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 (35) spread across various countries. 8base and Lockbit3 groups follow closely with each hitting 18 and 17 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
8base	13.64%
Akira	3.03%
Alphv	9.09%
Blackbasta	2.27%
Blackbyte	4.55%
Clop	26.52%
Daixin	0.76%
Darkrace	0.76%
La piovra	0.76%
Lockbit3	12.88%
Medusa	2.27%
Noescape	1.52%
Oilin	2.27%
Rancoz	0.76%
Ransomhouse	2.27%
Ransomware blog	1.52%
Rhysida	6.06%
Royal	1.52%
Snatch	6.06%
Unsafe	0.76%

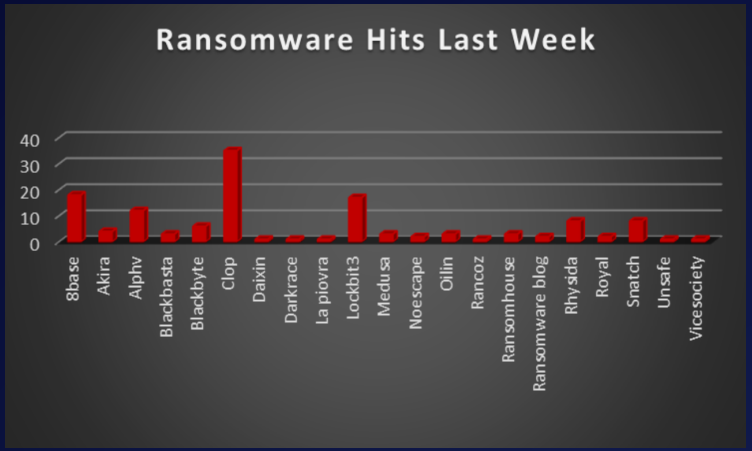

Figure 1: Ransomware Group Hits Last Week

When we examine the victims by country out of 32 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
Argentina	1.52%
Australia	1.52%
Austria	0.76%
Bangladesh	0.76%
Belgium	1.52%
Brazil	3.79%
Canada	1.52%
Chile	0.76%
China	0.76%
Colombia	1.52%
France	1.52%
Germany	3.79%
India	1.52%
Italy	3.03%
Jakarta	0.76%
Japan	0.76%
Lebanon	0.76%
Luxembourg	0.76%
Malaysia	0.76%
Mexico	0.76%
Minneapolis	0.76%
Netherlands	0.76%
Portugal	0.76%
Romania	0.76%
South Africa	0.76%
Spain	1.52%
Sri Lanka	0.76%
Sweden	1.52%
Switzerland	3.03%
UAE	0.76%
UK	6.06%
USA	53.79%

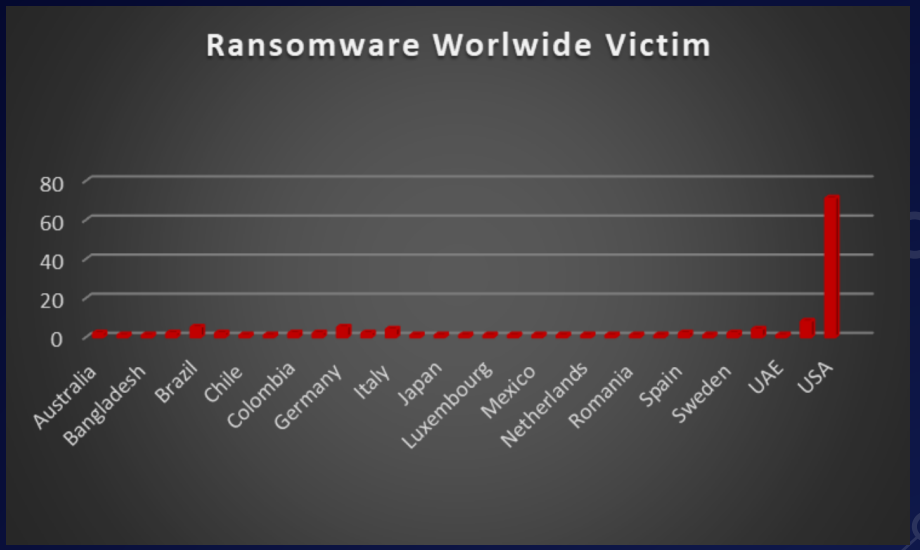

Figure 2: Ransomware Victims Worldwide

After conducting additional research, we found that ransomware has impacted 21 industries globally. Last week, the Finance and Manufacturing sectors were hit particularly hard, with the loss of 16 and 15 businesses in each sector respectively. The table below presents the most recent ransomware victims sorted by industry.

Industry	Victims Count (%)
Business Services	10.61%
Construction	6.06%
Consumer Services	1.52%
Education	1.52%
Education	8.33%
Energy	0.76%
Finance	12.12%
Government	1.52%
Healthcare	6.06%
Hospitality	2.27%
Insurance	6.06%
IT	3.79%
Legal Services	2.27%
Manufacturing	11.36%
Metals	0.76%
Metals & Mining	1.52%
Organisations	3.79%
Real Estate	0.76%
Retail	6.82%
Transportation	6.06%

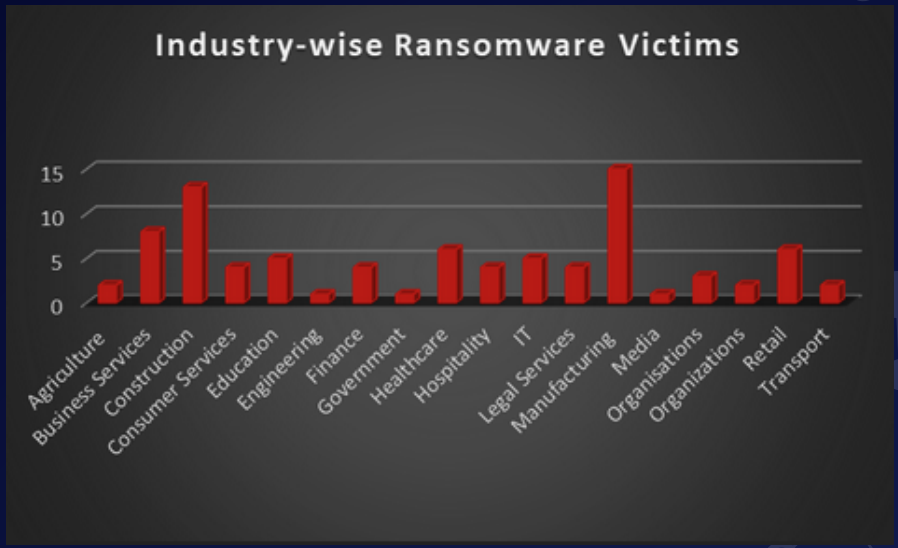

Figure 3: Industry-wise Ransomware Victims