Red Piranha
unified threat management

THREAT INTELLIGENCE REPORT

Aug 08 - 14, 2023

Report Summary:

- **New Threat Detection Added** – 3 (Agniane Stealer, TOAD Attacks, and Formbook Malware)
- **New Threat Protections**
- **New Ransomware Victims Last Week - 48**

Newly Detected Threats Added

1. Agniane Stealer

Agniane Stealer is a potent information theft tool equipped with various capabilities. Notably, it excels at extracting passwords and cookies from popular web browsers like Chrome, Firefox, and Edge, amassing valuable user credentials. It extends its reach to messaging platforms such as Telegram and Discord, intercepting ongoing sessions and accessing private conversations, which can have serious consequences for users' privacy. Additionally, Agniane Stealer displays a keen interest in cryptocurrency, targeting crypto wallets to seize digital assets discreetly. The malware captures screenshots to provide cybercriminals with a visual overview of victims' activities. Disseminated through phishing emails, it tricks recipients into opening attachments, facilitating the theft of user data, crypto wallets, browser specifics, VPN credentials, and more. This enables attackers to also access victim details like geolocation and IP address.

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: Execution TA0002/T1047/T1106 - Defence Evasion TA0005/T1027/T1036 -Credential Access TA0006/T1003/T1539 - Discovery TA0007/T1010/T1018 - Collection TA0009/T1005 - Command-and-Control TA0011/T1071/T1573

2. TOAD Attacks

Researchers have noticed a rise in TOAD (Telephone-oriented attack delivery) phishing campaigns. TOAD involves luring victims to engage with deceptive call centres run by malicious actors. These campaigns aim to steal credentials or implant malware. The messages in these attacks impersonate companies like Norton, PayPal, or McAfee, citing service bills or transaction fees. Recipients are prompted to view an attached PDF invoice and call a provided number for cancellations or refunds. These messages falsely suggest accidental service sign-ups. They lead to fake customer service helplines that seek credentials and encourage downloading malicious software. While potential victims should be cautious, signs like unofficial email accounts, vague details, and basic formatting can help identify these schemes. We identified some TOAD domains and created some rules to prevent attacks against our users.

Threat Protected: 10
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: Command-and-Control T1071/T1105

3. Formbook Malware

FormBook is a type of malware that is designed to steal sensitive information from infected computers. It is primarily used for cybercriminal activities, such as stealing login credentials, financial data, and other personal information. FormBook is typically distributed through malicious email attachments, phishing websites, and other deceptive methods. Once a system is infected, FormBook can capture keystrokes, take screenshots, and record user interactions, effectively capturing sensitive data entered by the victim. This stolen information is then sent to remote servers controlled by the attackers. FormBook has been used in various cyberattacks and has evolved over time with new features and capabilities to evade detection and improve its effectiveness. It has been a significant concern for cybersecurity professionals and organizations due to its potential to cause financial and data breaches.

Threat Protected: 01
Rule Set Type:

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

Class Type: Trojan-activity
Kill Chain: Initial Access T1566 - Execution T1059 - Collection T1119/T1005/T1185 - Command-and-Control T1132 - Exfiltration T1041

Known exploited vulnerabilities (Week 2 August 2023):

Vulnerability	Description
CVE-2017-18368	Zyxel P660HN-T1A Routers Command Injection Vulnerability
CVE-2023-38180	Microsoft .NET Core and Visual Studio Denial of Service Vulnerability

Updated Malware Signatures (Week 2 August 2023)

Threat	Description
njRAT	A remote access trojan typically spread using phishing emails or social engineering tactics. It allows a threat actor to steal sensitive information, install additional malware, and control the victim machine remotely.
TeslaCrypt	A ransomware that started in the year 2015. It is usually distributed through spam email campaigns, malicious attachments, and exploit kits.
Upatre	Upatre is also a malware dropper that downloads additional malware on an infected machine. It is usually observed to drop banking trojan after the initial infection.
Vidar	A stealer designed to collect sensitive data from infected machines. It usually targets Windows-based machines and is spread through email attachments or downloads from compromised websites.
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.
Zeus	Also known as Zbot and is primarily designed to steal banking credentials.

New Ransomware Victims Last Week: 48

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 48 new ransomware victims from 16 distinct industries across 15 countries worldwide. This highlights the global reach and indiscriminate nature of ransomware attacks, which can affect organisations of all sizes and sectors.

LockBit3.0, a specific ransomware, has affected the largest number of new victims (19) spread across various countries. Akira and AlphV hit 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
8Base	10.42%
Abyss-Data	2.08%
Akira	12.50%
AlphV	12.50 %
Everest	4.17%
LockBit3.0	39.58%
MeduSA	2.08%
Noescape	6.25%
Play	6.25%
Rhysida	4.17%

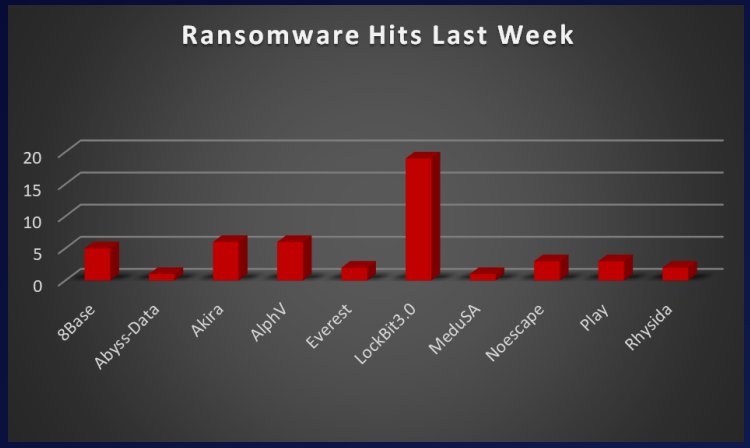

Figure 1: Ransomware Group Hits Last Week

When we examine the victims by country out of 15 countries around the world, we can conclude that the USA was once again the most ransomware-affected country, with a total of 28 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	2.08%
Australia	4.17%
Canada	2.08%
Egypt	2.08%
Germany	2.08%
Kuwait	2.08%
Mauritius	2.08%
South Africa	4.17%
Spain	2.08%
Sweden	2.08%
Switzerland	4.17%
Thailand	2.08%
Turkey	2.08%
UK	8.33%
USA	58.33%

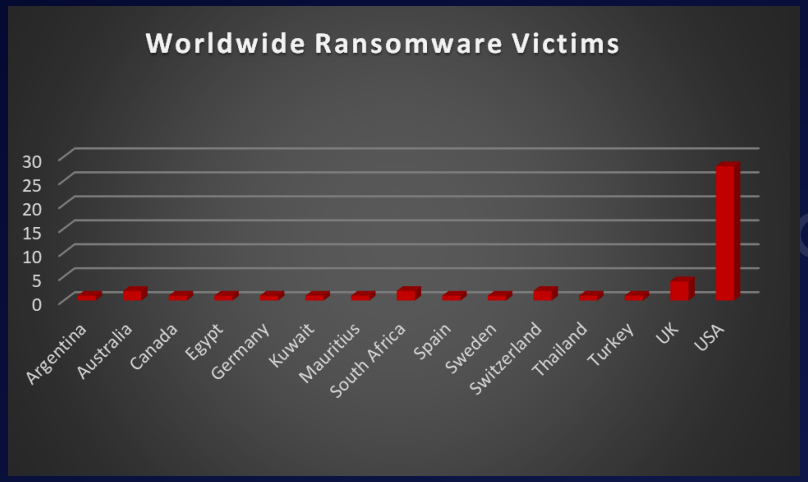

Figure 2: Ransomware Victims Worldwide

After conducting additional research, we found that ransomware has impacted 16 industries globally. Last week, the Manufacturing and Education sectors were hit particularly hard, with 14% and 12% of the total ransomware victims belonging to each of those sectors respectively. The table below presents the most recent ransomware victims sorted by industry.

Industry	Victims Count (%)
Business Services	12.50%
Construction	6.25%
Consumer Services	6.25%
Cultural	2.08%
Education	12.50%
Finance	4.17%
Government	4.17%
Healthcare	6.25%
IT	8.33%
Legal Services	4.17%
Manufacturing	14.58%
Media & Internet	2.08%
Metals & Mining	2.08%
Organisation	2.08%
Retail	6.25%
Telecom	6.25%

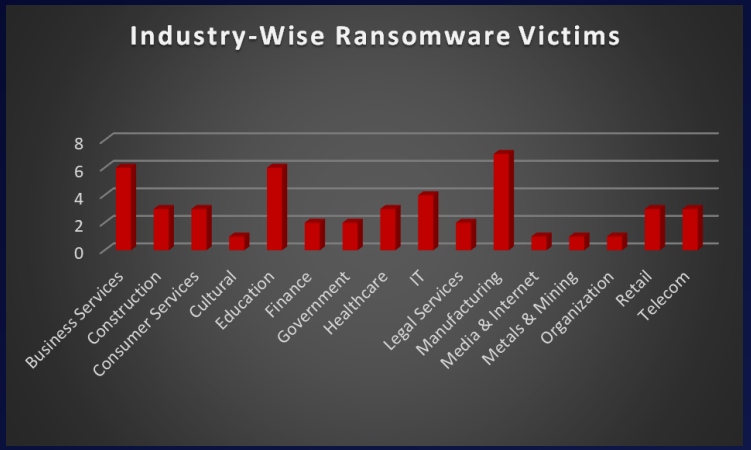

Figure 3: Industry-wise Ransomware Victims