Red Piranha
unified threat management

THREAT INTELLIGENCE REPORT

Aug 01 - 07, 2023

Report Summary:

- **New Threat Detection Added** – 4 (Fruity Malware, IcedID Malware, Ivanti CVE-2023-35082, and Chamilo CMS CVE-2023-34960)
- **New Threat Protections**
- **New Ransomware Victims Last Week - 77**

Newly Detected Threats Added

1. Fruity Malware

Fruity serves as a tool for cybercriminals to spread the Remcos RAT, a remote-control tool enabling remote computer access for malicious purposes. This gives them access to sensitive data like passwords, credit cards, and real-time screen monitoring. Moreover, it facilitates file downloads and execution, opening the door to more malware. Beyond Remcos RAT, Fruity can distribute various other malware types, including banking trojans, ransomware, and remote access tools. Banking trojans steal financial data, ransomware encrypts files for a ransom, and remote access tools compromise systems. Fruity victims face substantial harm, with unauthorised access to personal data, leading to identity theft, financial losses, and privacy breaches. Its capacity to introduce more malware triggers additional infections, causing operational disruptions, data loss, and potential ransomware extortion.

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 T1059/T1129 - Persistence T1574 - Privilege Escalation T1055/T1548.002 - Defence Evasion T1027/T1055/T1112 - Discovery T1012/T1057/T1083

2. IcedID Malware

IcedID, also known as BokBot, emerged in 2017. Initially tied to the banking trojan payload, the term "IcedID" now encompasses the entire infection process. After a few years under the radar, it resurfaced in 2019 using steganography to conceal its payload.

As time passed, IcedID loaders advanced, adopting various steganography techniques such as "Photoloader" and more recently "Gziploader." The core functionalities of the banking trojan have seen limited changes. IcedID operates in three stages, employing two DLL loaders via rundll32.exe. While the final stage is a banking trojan, IcedID can serve as a conduit for other threats like Ransomware or as an entry point for lateral spreading. By employing both VMware EDR and NDR solutions, comprehensive visibility, detection, and prevention against threats like IcedID are achieved across all attack stages.

Threat Protected: 03
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 T1064/T1203 - Persistence T1574.002 - Privilege Escalation T1055/T1574.002 - Defence Evasion T1027/T1036/T1055 - Discovery T1012/T1018/T1018 - Collection T1114 — Command-and-Control T1071/T1105

3. Ivanti CVE-2023-35082

CVE-2023-35082 enables an external unauthorised attacker to gain access to the API endpoints of a publicly accessible management server. Exploiting these API endpoints provides the attacker with a range of functionalities as outlined in the official API documentation. These functionalities encompass the potential to reveal personally identifiable information (PII) and make alterations to the platform. Moreover, if an additional vulnerability is present in the API, the attacker can combine these vulnerabilities. For instance, the attacker could leverage CVE-2023-35081 in conjunction with CVE-2023-35082 to create a chain of exploits, thereby allowing the attacker to upload malicious webshell files to the appliance, potentially leading to their execution.

Threat Protected: 02
Rule Set Type:

Class Type: Trojan-activity
Kill Chain: Initial Access T1190

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

4. Chamilo CMS CVE-2023-34960

An inherent flaw in the wsConvertPpt module within Chamilo versions ranging from v1.11.* to v1.11.18 introduces a command injection vulnerability. This vulnerability empowers attackers to execute arbitrary commands by manipulating a SOAP API call, utilising a specially crafted PowerPoint filename.

Threat Protected: 01
Rule Set Type:

Class Type: Trojan-activity
Kill Chain: Initial Access T1190

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

Known exploited vulnerabilities (Week 1 August 2023):

Vulnerability	Description
CVE-2023-35081	Ivanti Endpoint Manager Mobile (EPMM) Path Traversal Vulnerability

Updated Malware Signatures (Week 1 August 2023)

Threat	Description
njRAT	A remote access trojan typically spreads using phishing emails or social engineering tactics. It allows a threat actor to steal sensitive information, install additional malware, and control the victim's machine remotely.
Parite	Also known as the W32/Parite Virus which infects Windows computers and is classified as a polymorphic virus.
Tofsee	A malware that is used to send spam emails, and conduct click frauds as well as cryptomining.
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.
Ramnit	A banking trojan used to steal online banking credentials.

New Ransomware Victims Last Week: 77

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 77 new ransomware victims from 18 distinct industries across 20 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 (14) spread across various countries. RA Group and Play group follow closely with each hitting 10 and 8 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	5.19%
Akira	6.49%
Alphv	7.79%
Bianlian	3.90%
Blackbasta	1.30%
Clop	1.30%
Cuba	2.60%
Karakurt	1.30%
LokBit3.0	18.18%
Mallox	2.60%
Medusa	2.60%
Monti	3.90%
Noescape	5.19%
Nokoyawa	10.39%
Play	10.39%
Ra Group	12.99%
Ransomware Blog	1.30%
Rhysida	1.30%
Snatch	1.30%

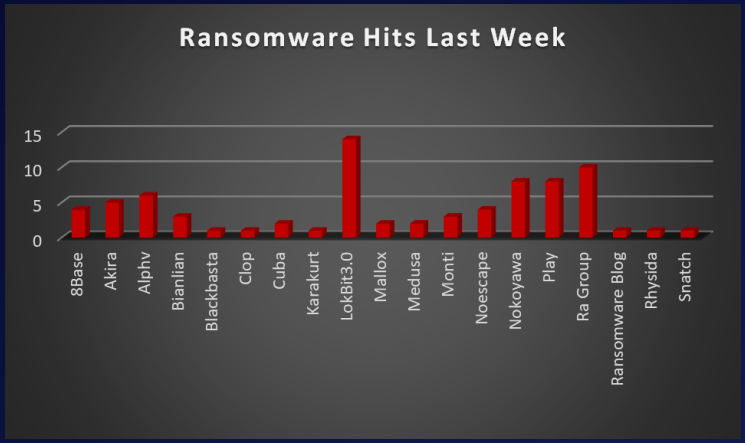

Figure 1: Ransomware Group Hits Last Week

When we examine the victims by country out of 20 countries around the world, we can conclude that the USA was once again the most ransomware-affected country, with a total of 42 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	1.30%
Austria	1.30%
Cameroon	1.30%
Canada	5.19%
France	5.19%
Germany	3.90%
Hungary	1.30%
India	3.90%
Indonesia	1.30%
Italy	1.30%
Japan	1.30%
Korea	2.60%
Portugal	1.30%
Qatar	1.30%
South Africa	1.30%
Spain	3.90%
Taiwan	1.30%
Thailand	1.30%
UK	5.19%
USA	54.55%

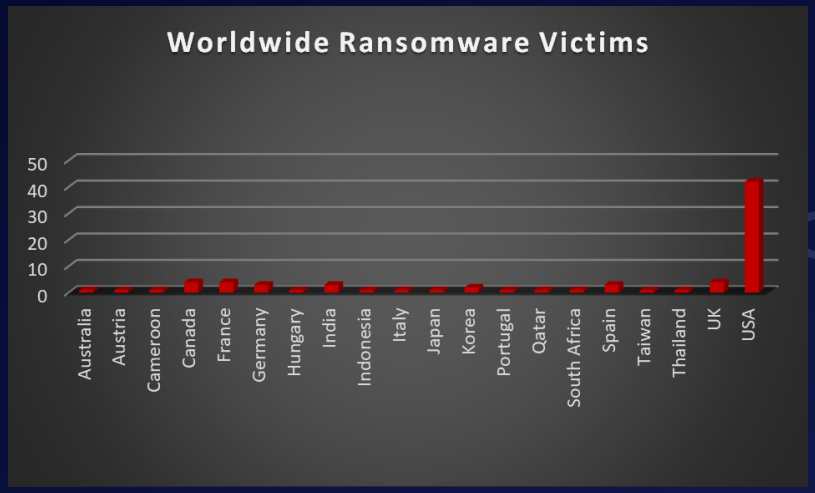

Figure 2: Ransomware Victims Worldwide

After conducting additional research, we found that ransomware has impacted 20 industries globally. Last week, the Manufacturing and Business Services sectors were hit particularly hard, with 19% and 16% 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 (%)
Agriculture	1.30%
Business Service	7.79%
Construction	7.79%
Consumer Services	3.90%
Education	6.49%
Energy, Utilities & Waste Treatment	1.30%
Finance	3.90%
Healthcare	3.90%
Hospitality	7.79%
Insurance	3.90%
IT	7.79%
Legal Services	5.19%
Manufacturing	15.58%
Organisations	7.79%
Real Estate	1.30%
Retail	7.79%
Telecom	2.60%
Transportation	3.90%

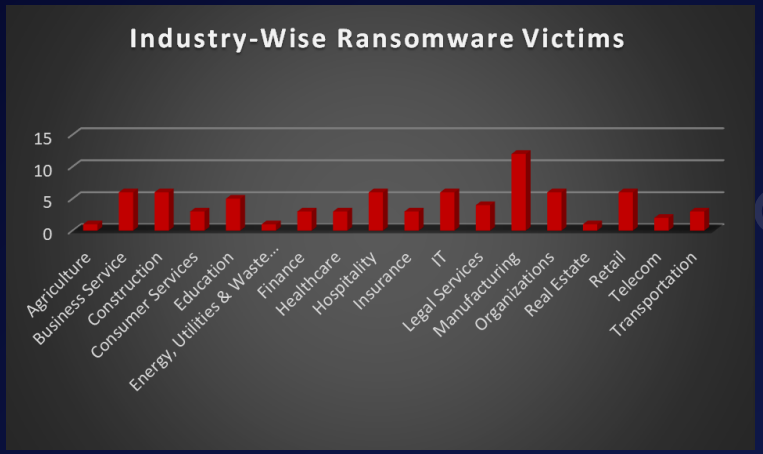

Figure 3: Industry-wise Ransomware Victims