Red Piranha
unified threat management

THREAT INTELLIGENCE REPORT

July 11 - 17, 2023

Report Summary:

- **New Threat Detection Added** – 4 (Playful Taurus (APT) Cinoshi Stealer, and RomCom (APT))
- **New Threat Protections**
- **New Ransomware Victims Last Week - 137**

Newly Detected Threats Added

1. Playful Taurus (APT)

Playful Taurus, also known as APT15, is an advanced persistent threat group from China involved in cyber espionage. Since 2010, they have targeted government and diplomatic entities across multiple regions, including North and South America, Africa, and the Middle East. In June 2021, ESET reported that Playful Taurus upgraded their toolkit with a new backdoor called Turian. This backdoor, which is still being developed, is exclusively used by the Playful Taurus actors. We have recently observed new variants of this backdoor and identified new command-and-control infrastructure. Our analysis indicates that several Iranian government networks may have been compromised by Playful Taurus. Playful Taurus consistently evolves their tactics and tools. The recent upgrades to their Turian backdoor and the deployment of new command-and-control infrastructure indicate their continued success in cyber espionage campaigns. While Iranian government networks are likely compromised, it is important to note that Playful Taurus also targets other government and diplomatic entities across North and South America, Africa, and the Middle East using similar techniques and tactics.

Threat Protected: 02
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: Defence Evasion TA0005/T1027/T1497 - Credential AccessTA0006/T1056 - Discovery TA0007/T1018/T1018/T1622 - Collection T1622/T1056 - Command-and-Control TA0011/T1071

2. Cinoshi Stealer

Cinoshi Stealer is a freely available tool accompanied by an integration-supporting panel. Attackers can use the Developers Panel to build the binary without the need for hosting a separate server. The stealer possesses various functionalities such as gathering data (passwords, cookies, cards) from Gecko, Chromium, and Edge-based browsers, collecting data from crypto wallets and browser extensions, stealing sessions from platforms like Steam, Telegram, and Discord, extracting information about the victim's computer like capturing screenshots and webcam photos from the victim's device. The stealer build can be customised using the web panel. It allows attackers to configure features such as preventing the exfiltration of logs with limited data and blocking the execution of the malware build in countries. Additionally, the panel enables TAs to set up Telegram notifications for build-related activities.

Threat Protected: 02
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 - Defence Evasion T1027 - Credential Access T1555/T1539 - Collection T1113 - Discovery T1087/T1518 - Command-and-Control T1071 - Exfiltration T1041 - Impact T1489

3. RomCom (APT)

Two malicious documents originating from Hungary were recently discovered being used to target supporters of Ukraine. Due to the NATO Summit, the threat actors are impersonating the Ukrainian World Congress organisation to distribute these malicious documents to participating supporters of Ukraine. The MS Word documents contain an OLE object which instructs the victim machine to connect to its C&C server to download a second-stage malware. The initial malware utilises the Follina vulnerability. If successful, it allows an attacker to execute code on the victim's machine.

Threat Protected: 08
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: Initial Access T1566 - Execution T1204/T1059 - Command-and-Control T1071/T1102

Known exploited vulnerabilities (Week 2 July 2023):

Vulnerability	Description
CVE-2022-31199	SolarView Compact Command Injection Vulnerability
CVE-2023-37450	Apple Multiple Products WebKit Code Execution Vulnerability
CVE-2023-32046	Microsoft Windows MSHTML Platform Privilege Escalation Vulnerability
CVE-2023-32049	Microsoft Windows Defender SmartScreen Security Feature Bypass Vulnerability
CVE-2023-35311	Microsoft Outlook Security Feature Bypass Vulnerability
CVE-2023-36874	Microsoft Windows Error Reporting Service Privilege Escalation Vulnerability
CVE-2022-31199	Netwrix Auditor Insecure Object Deserialisation Vulnerability

Updated Malware Signatures (Week 2 July 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's machine remotely.
Zusy	Zusy, alternatively referred to as TinyBanker or Tinba, is a trojan specifically designed to engage in man-in-the-middle attacks to pilfer banking data. Upon execution, it inserts itself into legitimate Windows processes like "explorer.exe" and "winver.exe." As the user visits a banking site, Zusy deceitfully presents a fraudulent form, aiming to deceive the user into providing personal information.
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.
Redline	A .NET-based information stealer malware.

New Ransomware Victims Last Week: 137

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 137 new ransomware victims from 23 distinct industries across 33 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 (56) spread across various countries. 8Base and Tormous groups follow closely with each hitting 19 and 15 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	13.87%
Akira	3.65%
Alphv	4.38%
Arvinclub	0.73%
Bianlian	4.38%
Clop	40.88%
Cuba	0.73%
Dnutleaks	6.57%
Lockbit3	4.38%
Mallox	0.73%
Medusa	0.73%
Noescape	1.46%
Play	0.73%
Qilin	1.46%
Ragnarlocker	0.73%
Rancoz	0.73%
Ransomhouse	0.73%
Rhysida	1.46%
Snatch	0.73%
Tormous	10.95%

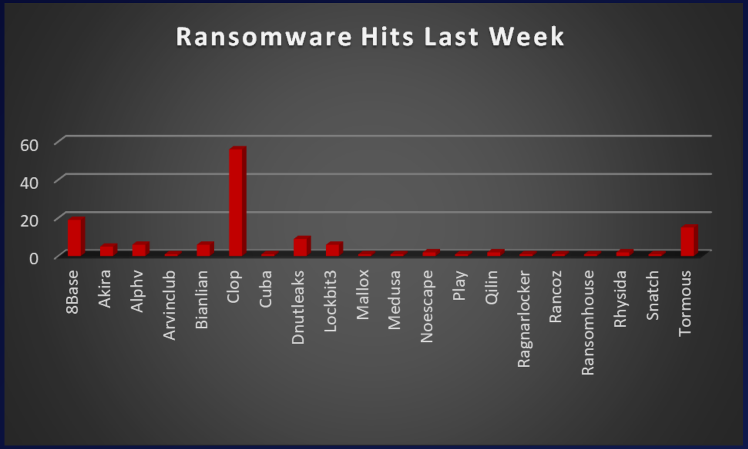

Figure 1: Ransomware Group Hits Last Week

When we examine the victims by country out of 33 countries around the world, we can conclude that the USA was once again the most ransomware-affected country, with a total of 81 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	1.46%
Australia	1.46%
Bangkok	0.73%
Belgium	0.73%
Belize	0.73%
Canada	2.92%
China	1.46%
Colombia	0.73%
France	0.73%
Germany	3.65%
Guatemala	0.73%
India	2.19%
Indonesia	0.73%
Iran	0.73%
Israel	0.73%
Italy	2.19%
Japan	0.73%
Malaysia	0.73%
Mauritius	0.73%
Mexico	0.73%
Namibia	0.73%
Netherlands	2.19%
Ohio	0.73%
Peru	1.46%
Philippines	0.73%
Qatar	0.73%
Spain	1.46%
Switzerland	0.73%
Turkey	0.73%
UAE	0.73%
UK	5.11%
USA	59.12%

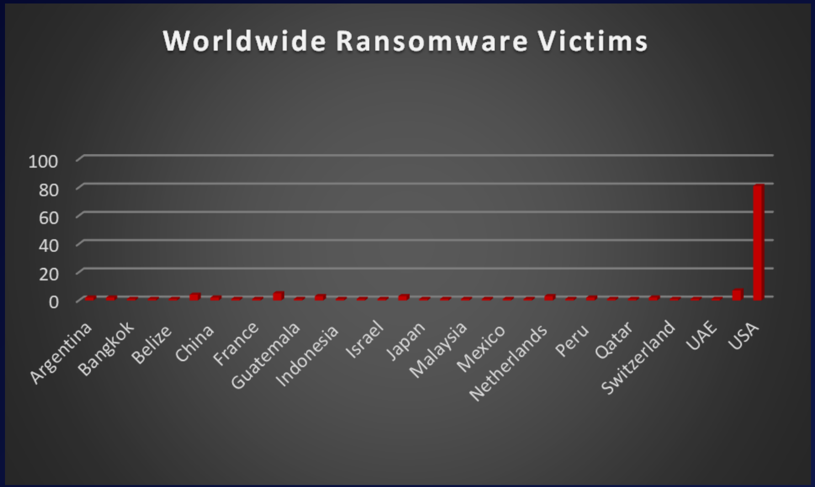

Figure 2: Ransomware Victims Worldwide

After conducting additional research, we found that ransomware has impacted 23 industries globally. Last week, the Manufacturing and Business Services sectors were hit particularly hard, with 18% 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	0.73%
Business Services	16.06%
Construction	2.19%
Consumer Services	2.92%
Education	4.38%
Energy	2.19%
Finance	5.84%
Healthcare	7.30%
Hospitality	10.22%
Insurance	2.19%
IT	7.30%
Legal Services	2.92%
Manufacturing	18.25%
Media	0.73%
Media& Internet	1.46%
Metals & Mining	1.46%
Mining	0.73%
Oil & Gas	0.73%
Organisations	2.19%
Real Estate	2.19%
Retail	5.84%
Telecom	1.46%
Transportation	0.73%

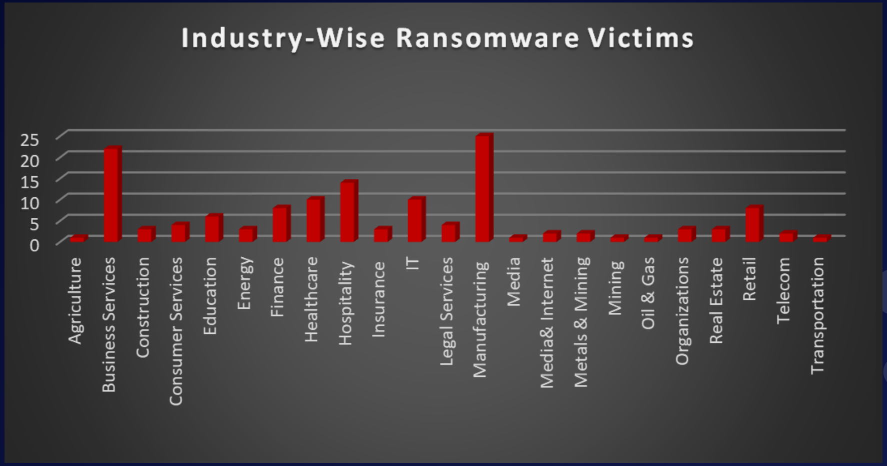

Figure 3: Industry-wise Ransomware Victims