Red Piranha
unified threat management

THREAT INTELLIGENCE REPORT

July 18 - 24, 2023

Report Summary:

- **New Threat Detection Added** – 3 (Konni APT, Mallox Ransomware, and ChaosRAT)
- **New Threat Protections**
- **New Ransomware Victims Last Week - 139**

Newly Detected Threats Added

1. Konni APT

The Konni APT is a sophisticated cyber espionage group dating back to at least 2014, suspected to operate from North Korea. Known for targeting government agencies in South Korea and the US, they use phishing messages to distribute the malicious Konni RAT tool. Once victims open weaponised files, the attackers gain access to their systems, extracting sensitive information and deploying a remote interactive shell. Linked to alleged attacks across Russia, East Asia, Europe, and the Middle East, the group shows code similarities with NOKKI malware. Their activities also involve targeting malicious Russian documents, and a spear phishing campaign in January 2022 revealed their continued cyber threat, necessitating heightened vigilance and proactive defence measures.

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 T1027 - Credential Access T1056 - Discovery T1018/ - Collection T1622 - Command-and-Control TA0011

2. Mallox Ransomware

The ransomware dubbed "TargetCompany," which emerged in June 2021, garnered attention for its distinct approach of adding the targeted company's name as a file extension to encrypted files. Initially identified as "Mallox" due to its use of the ".mallox" extension, the ransomware variant has evolved. A recent encounter reveals it now uses the ".malox" extension instead. The malware is distributed through BatLoader, akin to RATs and Stealers. The Mallox ransomware group has integrated BatLoader into their operations to deliver the ransomware payload. This loader exhibits resemblances to previously identified ones utilised in disseminating malware like Quasar RAT, Async RAT, Redline Stealer, and DC RAT. The adoption of new infection techniques underscores the group's dedication to evasiveness and maintaining their malicious 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 - Defence Evasion T1140/T1562/T1222 - Discovery T1082 - Impact T1486 - Command-and-Control T1071

3. ChaosRAT

CHAOS is a free and open-source Remote Administration Tool that allows any user to generate binaries to control remote operating systems. Rules have been created to detect the usage of Chaos as it can be used for nefarious activities.

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: Trojan-activity
Kill Chain: Initial Access T1566 - Execution T1059 - Persistence T1547 - Command-and-Control T1071

Known exploited vulnerabilities (Week 3 July 2023):

Vulnerability	Description
CVE-2023-36884	Microsoft Office and Windows HTML Remote Code Execution Vulnerability
CVE-2023-3519	Citrix NetScaler ADC and NetScaler Gateway Code Injection Vulnerability
CVE-2023-38205	Adobe ColdFusion Improper Access Control Vulnerability
CVE-2023-29298	Adobe ColdFusion Improper Access Control Vulnerability

Updated Malware Signatures (Week 3 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: 139

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 139 new ransomware victims from 22 distinct industries across 28 countries worldwide. This highlights the global reach and indiscriminate nature of ransomware attacks, which can affect organisations of all sizes and sectors.

Nokoyawa, a specific ransomware, has affected the largest number of new victims (25) spread across various countries. Clop and LockBit3.0 groups follow closely with each hitting 24 and 21 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	2.16 %
Abyss Data	2.16 %
Akira	1.44 %
AlpHv	6.47 %
Bianlian	3.60 %
Cactus	12.23 %
Clop	17.27 %
Cyclops	0.72 %
LockBit3.0	15.11 %
Medusa	2.88 %
Money Message	1.44 %
NoEscape	3.60 %
Nokoyawa	17.99 %
Play	4.32 %
Rhysida	3.60 %
Royal	0.72 %
Snatch	2.88 %
Stormous	1.44 %

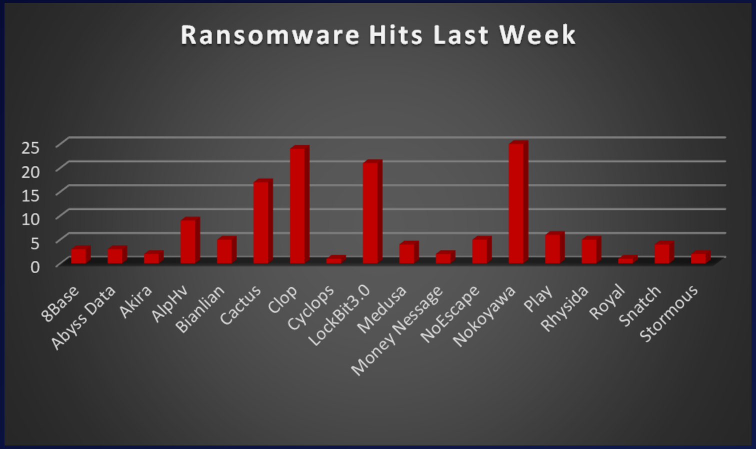

Figure 1: Ransomware Group Hits Last Week

When we examine the victims by country out of 28 countries around the world, we can conclude that the USA was once again the most ransomware-affected country, with a total of 75 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	3.60 %
Belgium	0.72 %
Brazil	0.72 %
Canada	3.60 %
China	1.44 %
Denmark	0.72 %
Fiji	0.72 %
Finland	0.72 %
France	2.16 %
Germany	2.16 %
Ireland	0.72 %
Italy	3.60 %
Japan	0.72 %
Jordan	0.72 %
Lebanon	0.72 %
Malaysia	1.44 %
Morocco	0.72 %
Namibia	0.72 %
Netherlands	0.72 %
Portugal	0.72 %
Romania	0.72 %
Spain	1.44 %
Sweden	0.72 %
Switzerland	2.88 %
Tunisia	0.72 %
Turkey	0.72 %
UK	11.51 %
USA	53.96 %

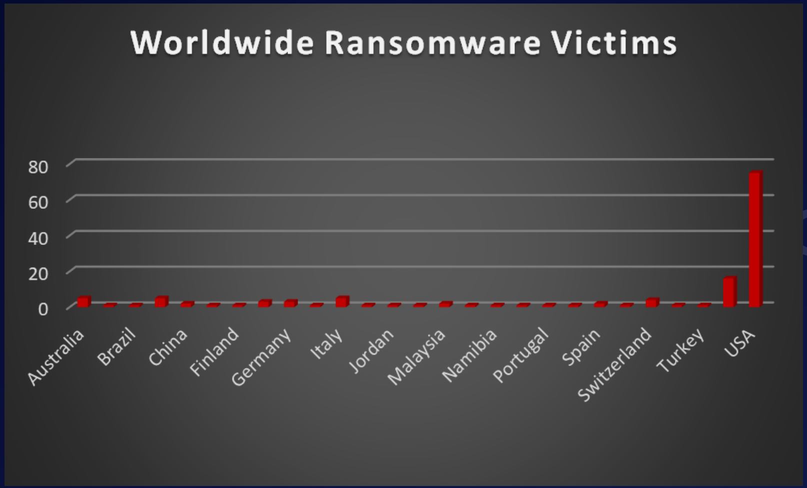

Figure 2: Ransomware Victims Worldwide

After conducting additional research, we found that ransomware has impacted 22 industries globally. Last week, the Manufacturing and Business Services sectors were hit particularly hard, with 17% and 9% 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	9.35%
Cities, Towns & Municipalities	0.72%
Construction	7.92%
Consumer Services	4.32 %
Education	9.35%
Electricity, Oil & Gas	1.44%
Finance	2.16 %
Government	2.16 %
Healthcare	5.04%
Hospitality	1.44%
Insurance	2.16%
IT	8.63%
Legal Services	2.16%
Manufacturing	17.99%
Media & Internet	2.16%
Metals & Mining	0.72 %
Oil & Gas	0.72%
Organisations	2.88%
Real Estate	0.72%
Retail	7.91%
Telecommunication	2.88%
Transportation	7.19%

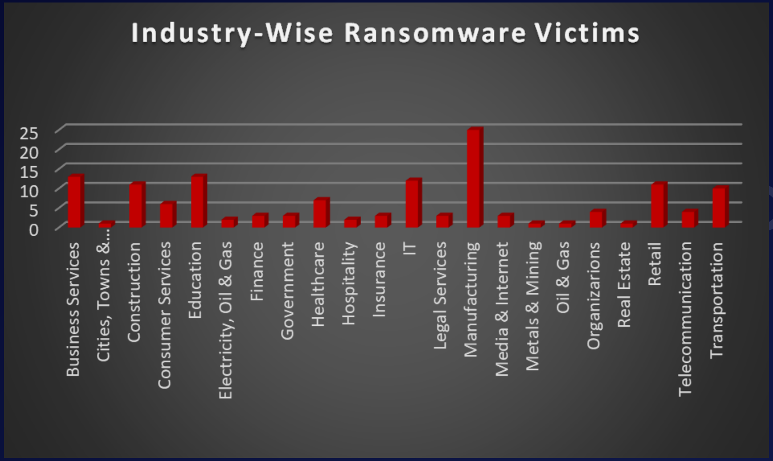

Figure 3: Industry-wise Ransomware Victims