Red Piranha
unified threat management

THREAT INTELLIGENCE REPORT

Aug 29 - Sept 04, 2023

Report Summary:

- **New Threat Detection Added** – 2 (Konni APT, and IcedID Malware)
- **New Threat Protections - 4**
- **New Ransomware Victims Last Week - 214**

Newly Detected Threats Added

1. Konni APT

The Konni Advanced Persistent Threat (APT) group, suspected to originate from North Korea, has been operating since at least 2014. Their primary focus has been infiltrating government agencies and institutions in South Korea and the United States. This North Korean hacking group delivers the Konni Remote Access Trojan (RAT) through deceptive phishing messages or emails. The infection process starts when the target interacts with a rigged file. Once inside a victim's system, Konni RAT enables the attackers to gather data, capture screenshots, pilfer files, and establish a remote interactive connection. KONNI has been associated with multiple cyberattacks, allegedly orchestrated by North Korea, targeting political entities across Russia, East Asia, Europe, and the Middle East. Notably, KONNI shares a substantial code base with the NOKKI malware family. Konni's APT group maintains its focus on attacking documents written in Russian, often related to Russian-North Korean trade and economic investments. In January 2022, this APT group was detected targeting the Russian diplomatic sector, using a spear-phishing scheme centred around New Year's Eve celebrations as bait. When the recipient opens and processes the malicious email attachment, a sequence of events unfolds, ultimately resulting in the installation of a Konni RAT family implant as the final payload.

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: Execution T1064 - Persistence T1547 - Privilege Escalation T1547 - Defence Evasion T106 - Discovery T1082 - Command-and-Control T1071/T1105

2. IcedID Malware

IcedID, a persistent malware, circumvents antivirus defences via process-hollowing. It infiltrates key API functions erasing the hooks to spawn a "svchost.exe" service process, embedding itself in "KERNEL32.DLL" and "SHLWAPI.DLL." Payload placement in "%ProgramData%" or "%AppData%" depends on account privileges. A scheduled task ensures reboot persistence, with three "svchost.exe" subprocesses containing its shellcode. IcedID delays execution until reboot, mimicking legitimate OS functions. It spreads across networks, observing activities, exfiltrating data, and executing man-in-the-browser attacks. These assaults involve web-injection, proxy setup, and redirection. IcedID injects shellcode into web browsers, adjusting memory and altering protection. It intercepts traffic through "Ws2_32:connect," channelling it to a proxy server for data capture. Recent versions include an Automatic Transaction System (ATS) Engine for autonomous data theft and injection, apart from the Command-and-Control (C2) server. The proxy crafts counterfeit banking sites, snaring login details and bypassing multi-factor authentication (MFA). IcedID communicates via HTTPS through its proxy, employing obfuscation and encryption to confound analysis. These tactics enable IcedID to infiltrate systems, exfiltrate sensitive data, and exploit network weaknesses.

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: Defence Evasion T1497 - Discovery T1010/ T1082/ - Command-and-Control T1071/ /T1573

Updated Malware Signatures (Week 5 August 2023)

Threat	Description
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.
Bifrost	A remote access trojan that enables its operator to take control of a victim machine and steal data. It is usually distributed through spam and phishing emails.
LokiBot	An information-stealer malware used to gather data from victims' machines such as stored account credentials, banking information and other personal data.
XtremeRAT	A remote access trojan interacts with the infected machine via a remote shell, uploads/downloads files, and records from a webcam/microphone.

New Ransomware Victims Last Week: 214

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 214 new ransomware victims or updates in few past victims from 24 distinct industries across 36 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 victims (100) updates spread across various countries. LockBit3.0 and Everest updated 50 & 14 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	3.74%
Abyss-Data	0.47%
Akira	3.74%
AlphV	5.14%
BianLian	0.93%
Clop	46.73%
Everest	6.54%
INC Ransom	0.47%
Karakurt	0.47%
LockBit3.0	23.83%
Lorenz	0.47%
Medusa	1.87%
Noescape	2.34%
Play	0.47%
Qilin	0.47%
RA Group	0.47 %
Ransomed	1.40%
Snatch	0.47%

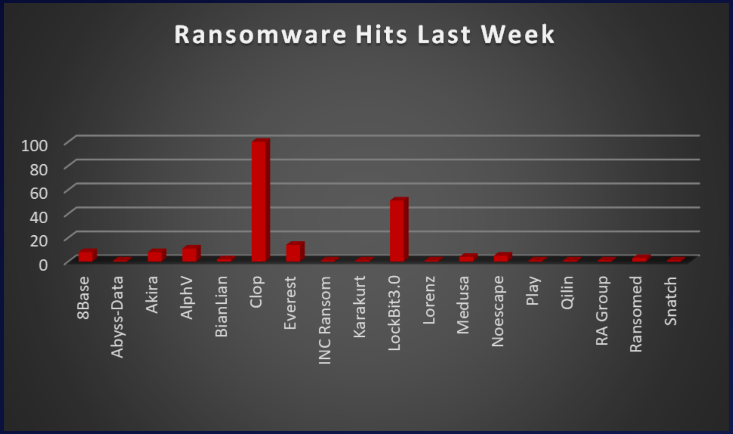

Figure 1: Ransomware Group Hits Last Week

When we examine the victims by country out of 36 countries around the world, we can conclude that the USA was once again the most ransomware-affected country, with a total of 114 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	0.47%
Australia	2.34%
Austria	0.47%
Belgium	0.93%
Canada	5.61%
China	1.40%
Denmark	0.47%
Egypt	0.47%
Finland	0.47%
France	2.34%
Germany	3.27%
Guatemala	0.47%
India	3.74%
Indonesia	0.47%
Irelan	0.47%
Israel	0.47%
Italy	0.93%
Japan	0.93%
Korea	0.47%
Malaysia	0.93%
Netherlands	2.34%
Oman	0.47%
Panama	0.47%
Peru	0.47%
Philippines	0.47%
Portugal	1.40%
Spain	1.40%
Sri Lanka	0.47%
Sweden	0.93%
Switzerland	1.87%
Tunisia	0.47%
Turkey	0.93%
UAE	0.47%
UK	6.54%
Uruguay	0.47%
USA	53.74%

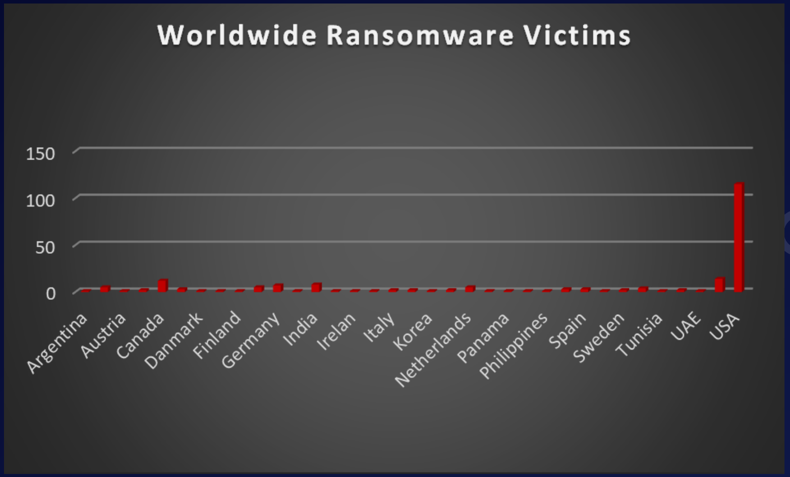

Figure 2: Ransomware Victims Worldwide

After conducting additional research, we found that ransomware has impacted 24 industries globally. Last week, the Manufacturing and Business Services sectors were hit particularly hard, with 21% and 11% 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	0.93%
Banking	3.74%
Business Services	11.68%
Construction	7.01%
Consumer Services	2.80%
Education	5.61%
Electricity, Oil & Gas	1.40%
Energy, Utilities & Waste Treatment	2.34%
Finance	2.34%
Government	0.93%
Healthcare	3.74%
Hospitality	4.21%
Insurance	3.74%
IT	6.07%
Legal Services	6.07%
Manufacturing	21.03%
Media & Internet	1.87%
Metals & Mining	1.40%
Museums & Art Galleries	0.47%
Organisation	0.93%
Real Estate	2.34%
Retail	5.61%
Telecom	1.40%
Transportation	2.34%

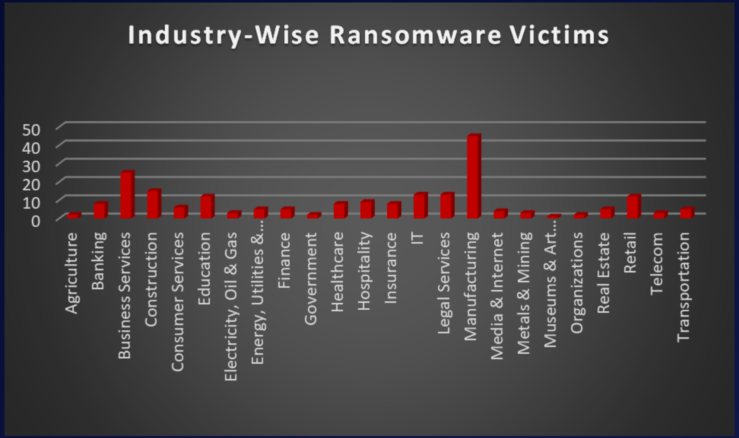

Figure 3: Industry-wise Ransomware Victims