Red Piranha
unified threat management

THREAT INTELLIGENCE REPORT

Mar 19 - 25, 2024

Report Summary:

- **New Threat Detection Added** – 4 (Remcos RAT, CloudAtlas APT, Fenix Botnet and Viessmann Vitogate 300 Command Injection (CVE-2023-5702))
- **New Threat Protections - 98**

Newly Detected Threats Added

1. Remcos RAT

Researchers found that in South Korea, some malicious software is being disguised as adult games and shared through webhards, which are websites for storing and sharing files. These websites, along with torrents, are often used to spread harmful software in Korea. The malware is hidden within several games, all prompting users to run a file named Game.exe. After extracting the files, users will find what appears to be a game launcher, but the actual program used to run the game is different. Inside, there are harmful scripts that run alongside the game, potentially causing harm to the user's device. Users should be cautious when downloading from file-sharing sites and stick to trusted sources.

Rules Created: 01
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:

Tactic	Technique ID	Technique Name
Execution	T1129	Shared Modules
Persistence	T1055	Process Injection
Defence Evasion	T1027 T1036 T1055 T1564.003	Obfuscated Files or Information Masquerading Process Injection Hidden Window
Credential Access	T1056 T1056.001	Input Capture Key
Discovery	T1018 T1057	Remote System Discovery Process Discovery
Command-and-Control	T1071	Application Layer Protocol

2. CloudAtlas APT

CloudAtlas, aka Inception or RedOctober, is a group of cyber attackers known for their advanced tactics. They have been active since around 2014 and focus on government, military, and diplomatic organisations in Eastern Europe and Central Asia. Their methods include techniques like spear-phishing, planting traps on popular websites, and sending harmful files disguised as legitimate documents. They use their special software, like PowerShower and FlowCloud, along with the infamous RedOctober program. CloudAtlas is skilled at changing its methods to avoid getting caught and to keep getting into its target's computer networks.

Rules Created: 06
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:

Tactic	Technique ID	Technique Name
Execution	T1064 T1203	Scripting Exploitation for Client Execution
Persistence	T1574	DLL Side-Loading
Privilege Escalation	T1574.002	DLL Side-Loading
Defence Evasion	T1036 T1036	Masquerading Scripting
Discovery	T1018	Remote System Discovery
Command-and-Control	T1071 T1573	Application Layer Protocol Encrypted Channel

3. Fenix Botnet

In a recent attack targeting people in Latin America, the Fenix Botnet was used as a separate kind of malware. The attackers tricked people by disguising the harmful software as real tools inside .zip files. When someone opens these files, the harmful software gets installed on their computer. This software can steal information, like passwords and banking details, by recording what people type or extracting data from their devices. The attackers specifically go after data related to big banks in Latin American countries, trying to get valuable information. It's important to be careful when opening files from unknown sources to avoid falling victim to such attacks.

Rules Created: 30
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:

Tactic	Technique ID	Technique Name
Execution	T1059 T1059.001 T1064	Command and Scripting Interpreter PowerShell Scripting
Privilege Escalation	T1055	Process Injection
Defence Evasion	T1027.002 T1036 T1055	Software Packing Masquerading Process Injection
Discovery	T1010 T1018	Application Window Discovery Remote System Discovery
Command-and-Control	T1071 T1573	Application Layer Protocol Encrypted Channel

4. Viessmann Vitogate 300 Command Injection (CVE-2023-5702)

The Vitogate 300, the gateway used to connect the Viessmann LON to BACnet or Modbus, was deployed with a vulnerability that allowed an attacker to access sensitive content such as configuration files without logging in.

Rules Created: 01
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: Attempted-admin

Kill Chain:

Tactic	Technique ID	Technique Name
Initial Access	T1190	Exploit Public-Facing Application

Known exploited vulnerabilities (Week 4 March 2024):

Vulnerability	CVSS	Description
CVE-2024-23334	7.5 (High)	aiohttp Directory Traversal Vulnerability

Updated Malware Signatures (Week 4 March 2024)

Threat	Description
Cerber	Another type of ransomware but instead of the usual ransom text files, it plays audio on the victim's infected machine.
Remcos	Remcos functions as a remote access trojan (RAT), granting unauthorised individuals the ability to issue commands on the compromised host, record keystrokes, engage with the host's webcam, and take snapshots. Typically, this malicious software is distributed through Microsoft Office documents containing macros, which are often attached to malicious emails.
Gh0stRAT	Gh0stRAT is a widely recognised group of remote access trojans strategically crafted to grant an assailant full authority over a compromised system. Its functionalities encompass monitoring keystrokes, capturing video via the webcam, and deploying subsequent malware. The source code of Gh0stRAT has been openly accessible on the internet for an extended period, substantially reducing the hurdle for malicious actors to adapt and employ the code in fresh attack endeavours.
MacStealer	A remote access trojan enables its operator to take control of a victim machine and steal data. It is usually distributed through spam and phishing emails.

Ransomware Report

The Red Piranha Team actively collects information on organisations globally affected by ransomware attacks from various sources, including the Dark Web. In the past week alone, our team uncovered new ransomware victims or updates on previous victims across 16 different industries spanning 19 countries. This underscores the widespread and indiscriminate impact of ransomware attacks, emphasising their potential to affect organisations of varying sizes and sectors worldwide.

Lockbit3.0 ransomware group stands out as the most prolific, having updated a significant number of victims (25%) distributed across multiple countries. In comparison, Hunter and Bianlian ransomware groups have updated 10% and 7% victims, respectively, in the past week. The following list provides the victim counts in percentages for these ransomware groups and a selection of others.

As you read above, LockBit3.0 has emerged as one of the most dangerous ransomware strains, affecting the highest number of victims globally. Take a moment to delve into the dark history and the profound impact that the LockBit3.0 ransomware group has had:

LockBit3.0, also known as LockBit Black, stands out as a highly dangerous ransomware that has inflicted widespread damage on a global scale. Its history unfolds with the emergence of the original LockBit in 2016, initially a basic but effective ransomware. By 2019, LockBit 2.0 arrived, featuring enhanced encryption and a focus on larger organisations.

A significant shift occurred in 2020 when LockBit transformed into a Ransomware-as-a-Service (RaaS) model, allowing anyone to launch ransomware attacks through its platform. This evolution marked a turning point, granting widespread access to LockBit and amplifying its threat level. In 2022, LockBit3.0, or LockBit Black, made its debut, introducing increased modularity, evasion tactics, and customisation, making detection and prevention more challenging.

LockBit3.0 has left a trail of disruption across critical sectors, impacting hospitals, schools, and government agencies. In 2021, it notably crippled the Colonial Pipeline, leading to significant fuel disruptions in the US. Even manufacturing giants like CISA and Samsung have fallen victim to LockBit's powerful encryption.

Efforts are underway globally to dismantle LockBit and its operators, with companies investing heavily in defence measures. Despite these endeavours, LockBit3.0 remains a persistent threat. Its RaaS model ensures constant evolution, posing an ongoing challenge for the cybersecurity community. Staying vigilant and implementing robust security practices are crucial to confront this ever-growing and evolving cyber threat. Read more.

Name of Ransomware Group	Percentage of new Victims last week
8Base	6.25%
Bianlian	7.81%
Black Suit	1.56%
Blackbasta	7.81%
Cactus	4.69%
Dragonforce	1.56%
Hunters	10.94%
Inc Ransom	1.56%
Killsec	6.25%
Lockbit3	25.00 %
Medusa	7.81%
Play	1.56%
Qilin	3.13%
Ransomhub	3.13%
Rhysida	3.13%
Trigona	7.81%

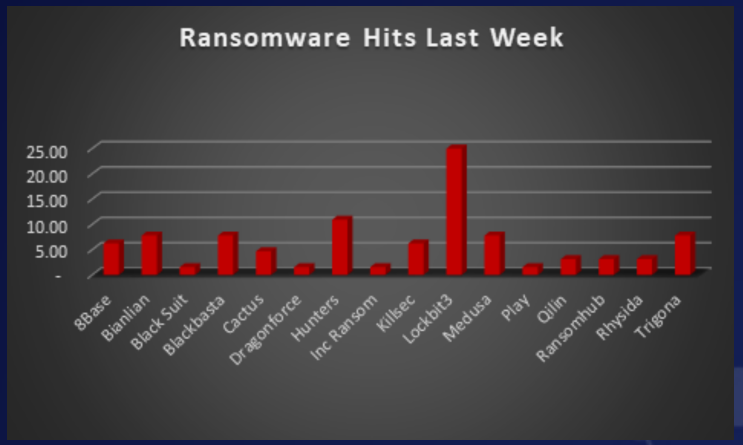

Figure 1: Ransomware Group Hits Last Week

In a comprehensive analysis of ransomware victims across 19 countries, the United States emerges as the most heavily impacted nation, reporting a staggering 45% victim updates in the past week. The following list provides a breakdown of the number and percentage of new ransomware victims per country, underscoring the persistent and concerning prevalence of ransomware attacks, with the USA particularly susceptible to these cybersecurity threats.

Name of the affected Country	Number of Victims
Brazil	1.56%
Canada	9.38%
China	3.13%
Egypt	1.56%
Germany	6.25%
Honduras	1.56%
India	3.13%
Indonesia	3.13%
Namibia	1.56%
New Zealand	1.56%
Poland	1.56%
Portugal	1.56%
Spain	3.13%
Sweden	1.56%
Switzerland	4.69%
Tunisia	1.56%
Turkey	1.56%
UK	6.25%
USA	45.31%

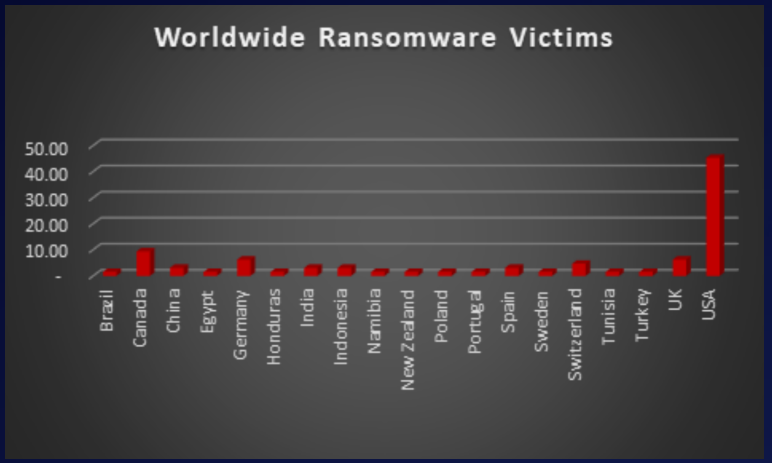

Figure 2: Ransomware Victims Worldwide

Upon further investigation, it has been identified that ransomware has left its mark on 16 different industries worldwide. Notably, the Manufacturing and Business Services bore the brunt of the attacks in the past week, accounting for 15 and 12 victims respectively. The table below delineates the most recent ransomware victims, organised by industry, shedding light on the sectors grappling with the significant impact of these cyber threats.

Industry	Victims Count (%)
Business Services	12.50%
Construction	6.25%
Consumer Services	1.56%
Education	4.69%
Energy, Utilities & Waste Treatment	3.13%
Finance	6.25%
Government	3.13%
Healthcare	9.38%
Hospitality	9.38%
Insurance	4.69%
IT	3.13%
Legal Services	3.13%
Manufacturing	15.63%
Real Estate	1.56%
Retail	12.50%
Transportation	3.13%

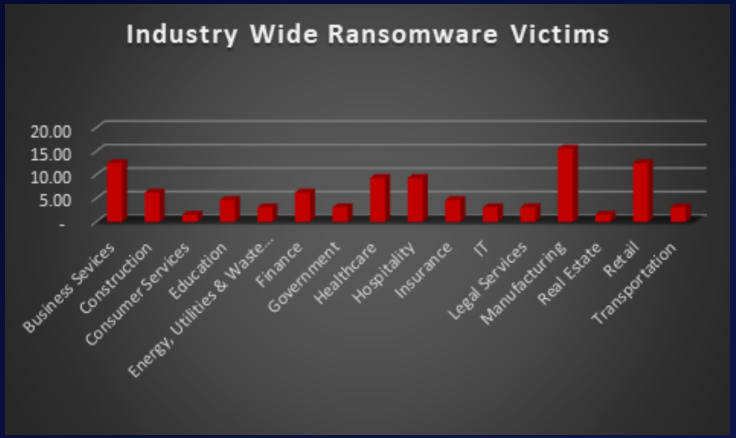

Figure 3: Industry-wide Ransomware Victims