Red Piranha
unified threat management

THREAT INTELLIGENCE REPORT

Mar 26 - Apr 01, 2024

Report Summary:

- **New Threat Detection Added** – 4 (PureLogs Stealer, TheMoon Malware, NimPlant C2 and FortiOS Remote Code Execution CVE-2024-21762)
- **New IDPS Rules Created - 70**

Newly Detected Threats Added

1. PureLogs Stealer

PureLogs, created by a threat actor named PureCoder, is a software designed to steal information. PureCoder sells various malicious programs, including miners, information stealers, VNC, and crypters, on their website. They promote their tools in cybercrime forums to attract customers. PureLogs and PureCrypt, their most impactful creations, are used by multiple threat actors in their campaigns. PureLogs, priced at $99 for a year, is a harmful .NET program. It targets browser data, crypto wallets, and applications like FTP clients, email clients, and VPNs installed on a computer, aiming to steal valuable information from users.

Rules Created: 03
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	T1204	User Execution
Defence Evasion	T1140 T1562	Deobfuscate/Decode Files or Information Impair Defences
Discovery	T1082 T1083	System Information Discovery File and Directory Discovery
Collection	T1119 T1005	Automated Collection Data from the Local System
Command-and-Control	T1071	Application Layer Protocol
Exfiltration	T1020	Automated Exfiltration

2. TheMoon Malware

Since 2014, TheMoon has quietly grown, now hosting over 40,000 bots from 88 countries by early 2024. Most of these bots serve as the backbone for Faceless, a notorious cybercriminal proxy service. TheMoon facilitates Faceless' expansion, adding around 7,000 new users weekly. Researchers have mapped Faceless' structure, revealing a recent campaign targeting 6,000 ASUS routers in under 72 hours. Faceless offers cybercriminals anonymity, attracting operators of botnets like SolarMarker and IcedID. This discovery underscores the escalating threat of cybercrime and the importance of tracking and understanding such networks for cybersecurity.

Rules Created: 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:

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

3. NimPlant C2

NimPlant is a lightweight, first-stage C2 implant made in Nim and Python. It is easy to configure and offers a sleek web GUI for smooth operations. All traffic is encrypted and compressed by default, with static strings obfuscated in implant artefacts. It supports various implant types like native binaries, shellcode, or self-deleting executables. NimPlant includes commands for early-stage operations such as local enumeration, file and registry management, and web interactions. More advanced functionalities or payloads can be deployed easily via inline-execute, shinject, or in-thread execute-assembly. It operates on any platform, though currently targeting x64 Windows.

Rules Created: 08
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
Command-and-Control	T1071 T1573	Application Layer Protocol Encrypted Channel

4. FortiOS Remote Code Execution CVE-2024-21762

A vulnerability in SSLVPNd has been discovered, potentially enabling remote unauthenticated attackers to execute arbitrary code or commands on Fortinet SSL VPNs through carefully crafted HTTP requests.

Rules Created: 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:

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

Known exploited vulnerabilities (Week 5 March 2024):

Vulnerability	CVSS	Description
CVE-2019-7256	10.0 (Critical)	Nice Linear eMerge E3-Series OS Command Injection Vulnerability
CVE-2021-44529	9.8 (Critical)	Ivanti Endpoint Manager Cloud Service Appliance (EPM CSA) Code Injection Vulnerability
CVE-2023-48788	9.8 (Critical)	Fortinet FortiClient EMS SQL Injection Vulnerability
CVE-2023-24955	7.2 (High)	Microsoft SharePoint Server Code Injection Vulnerability

Updated Malware Signatures (Week 5 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 19 different industries spanning 25 countries. This underscores the widespread and indiscriminate impact of ransomware attacks, emphasising their potential to affect organisations of varying sizes and sectors worldwide.

RaGroup ransomware group stands out as the most prolific, having updated a significant number of victims (16%) distributed across multiple countries. In comparison, Blackbasta and Play ransomware group updated 10% and 9% victims, respectively, in the past week. The following list provides the victim counts in percentages for these ransomware groups and a selection of others.

Name of Ransomware Group	Percentage of new Victims last week
3Am	0.75%
8Base	2.26%
Abyss-Data	1.50%
Akira	6.02%
Bianlian	3.01%
Blackbasta	10.53%
Cactus	2.26%
Cloak	3.76%
Clop	1.50%
Dragonforce	2.26%
Everest	1.50%
Hunters	0.75%
Inc Ransom	6.77%
Lockbit3	7.52%
Medusa	5.26%
Play	9.02%
Qilin	2.26%
Ra Group	16.54%
Ransomexx	3.01%
Ransomhub	1.50%
Red Ransomware	9.02%
Rhysida	0.75%
Snatch	2.26%

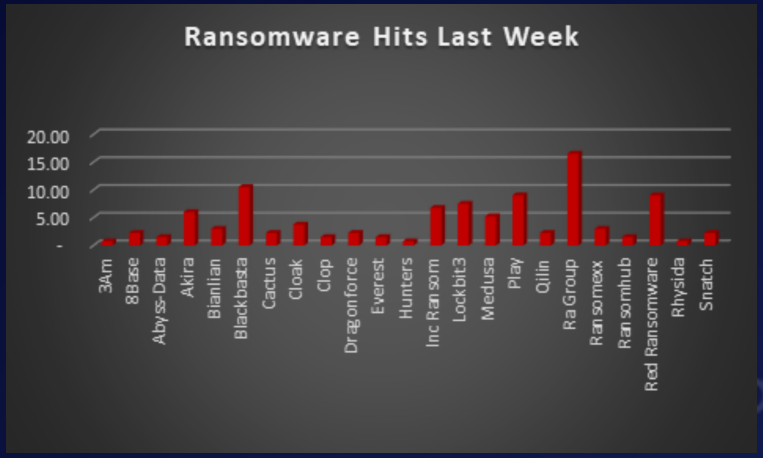

Figure 1: Ransomware Group Hits Last Week

RA Group Ransomware

The RA Group is a relatively new ransomware operation that emerged in April 2023. Utilising a custom ransomware variant built upon the leaked source code of Babuk ransomware, RA Group presents a significant threat to organisations. While the specific attack vectors employed by RA Group are not definitively established, potential methods include phishing emails, exploit kits, or compromised software updates.

One distinguishing characteristic of RA Group's tactics is its use of intermittent encryption, which encrypts portions of files rather than the entirety. While this may allow for partial data recovery, it still poses a substantial risk to businesses. Additionally, RA Group engages in double extortion tactics, stealing data before encryption and threatening to leak it if the ransom is not paid.

The group primarily targets organisations in the United States and South Korea, with a focus on industries such as pharmaceuticals, insurance, wealth management, and manufacturing. RA Group's personalised ransom notes and encryption of executables with the victim's name suggest a level of customisation in their attacks.

The financial impact of RA Group's attacks can be substantial, encompassing ransom demands, data recovery costs, and reputational damage. As such, a proactive approach to cybersecurity is imperative.

In a comprehensive analysis of ransomware victims across 25 countries, the United States emerges as the most heavily impacted nation, reporting a staggering 60% 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
Australia	1.50%
Bermuda	0.75%
Brazil	1.50%
Canada	4.51%
China	0.75%
Denmark	0.75%
France	0.75%
Germany	6.77%
India	1.50%
Indonesia	0.75%
Italy	1.50%
Japan	0.75%
Mexico	1.50%
Netherlands	0.75%
Norway	0.75%
Peru	0.75%
Poland	2.26%
South Korea	0.75%
Switzerland	0.75%
Taiwan	0.75%
Thailand	0.75%
Tobago	0.75%
UK	7.52%
USA	60.15%
Venezuela	0.75%

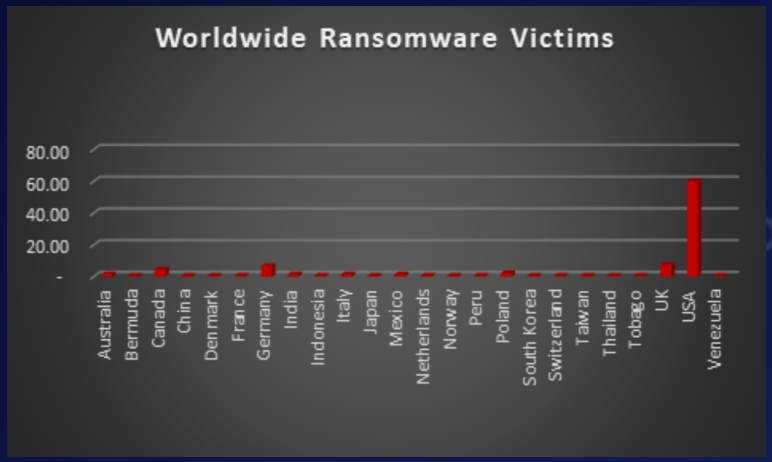

Figure 2: Ransomware Victims Worldwide

Upon further investigation, it has been identified that ransomware has left its mark on 19 different industries worldwide. Notably, the Manufacturing and Business Services bore the brunt of the attacks in the past week, accounting for 28% and 9% of 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	9.02%
Construction	8.27%
Consumer Services	6.77%
Education	5.26%
Energy, Utilities & Waste Treatment	1.50%
Finance	3.01%
Government	3.76%
Healthcare	8.27%
Hospitality	3.01%
Insurance	3.01%
IT	0.75%
Legal Services	3.01%
Manufacturing	28.57%
Media & Internet	0.75%
Metals & Mining	1.50%
Organisations	1.50%
Real Estate	2.26%
Retail	6.77%
Transportation	3.01%

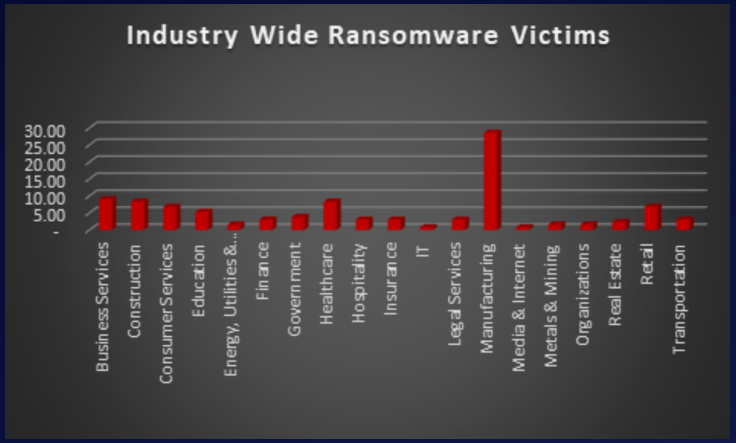

Figure 3: Industry-wide Ransomware Victims