Red Piranha
unified threat management

THREAT INTELLIGENCE REPORT

Mar 05 - 11, 2024

Report Summary:

- **New Threat Detection Added** – 3 (Evasive Panda APT, DFKRAT Malware and JetBrains TeamCity Auth Bypass (CVE-2024-27198 & CVE-2024-27198))
- **New Threat Protections - 102**
- **New Ransomware Victims Last Week - 59**

Newly Detected Threats Added

1. Evasive Panda APT

Evasive Panda, also called BRONZE HIGHLAND and Dagger Fly, is a cyber spying group from China, active since 2012. They've been spying on people in China, Hong Kong, Macao, and Nigeria. Targets include government groups in Southeast and East Asia, like China, Macao, Myanmar, The Philippines, Taiwan, and Vietnam. They've hit other organisations in China and Hong Kong too. Evasive Panda uses their sneaky software, MgBot, to spy on victims. They've upgraded their tricks since 2020, now even using tricky moves like hacking into real software updates to sneak in their spying tools. They've been causing trouble in Hong Kong, India, and Malaysia too.

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	T1189	Drive-by Compromise
Execution	T1129	Shared Modules
Persistence	T1543.003	Create or Modify System Process: Windows Service
Defence Evasion	T1140	Deobfuscate/Decode Files or Information
	T1620	Reflective Code Loading
Discovery	T1083	File and Directory Discovery
	T1057	Process Discovery
	T1012	Query Registry
Command-and-Control	T1095	Non-Application Layer Protocol
	T1571	Non-Standard Port
	T1572	Protocol Tunnelling

2. DFKRAT Malware

In late 2023, we stumbled upon the DFKRAT spy implant in a customer's system. This malware, part of the NGC2180 cluster, has been evolving since 2021. Early on, it spread through targeted phishing emails with downloaders, but the latest versions have a mysterious infection method. The malicious actions involve payloads delivered by downloaders or droppers using DLL side-loading. DFKRAT's main job is stealing files, supporting interactive shells, and potentially fetching more malware from its control server. The compromised servers of Greece's National Center for Scientific Research and an Indonesian company acted as command centres for the latest implant version. We located and examined a piece of the control server.

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	T1129	Shared Modules
Defence Evasion	T1027	Obfuscated Files or Information
	T1027.005	Indicator Removal from Tools
	T1140	Deobfuscate/Decode Files or Information
	T1222	File and Directory Permissions Modification
	T1497.001	System Checks
	T1564.003	Hidden Window
Discovery	T1012	Query Registry
	T1033	System Owner/User Discovery
	T1057	Process Discovery
	T1082	System Information Discovery
	T1083	File and Directory Discovery
	T1087	Account Discovery

3. JetBrains TeamCity Auth Bypass (CVE-2024-27198 & CVE-2024-27198)

JetBrains TeamCity contains an authentication bypass vulnerability that allows an attacker to perform actions with administrator privileges.

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: Attempted-admin

Kill Chain:

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

Known exploited vulnerabilities (Week 2 March 2024):

Vulnerability	CVSS	Description
CVE-2024-21338	7.8 (High)	Microsoft Windows Kernel Exposed IOCTL with Insufficient Access Control Vulnerability
CVE-2023-21237	5.5 (Medium)	Android Pixel Information Disclosure Vulnerability
CVE-2021-36380	9.8 (Critical)	Sunhillo SureLine OS Command Injection Vulnerability
CVE-2024-23225	7.8 (High)	Apple Multiple Products Memory Corruption Vulnerability
CVE-2024-23296	7.8 (High)	Apple Multiple Products Memory Corruption Vulnerability
CVE-2024-27198	9.8 (Critical)	JetBrains TeamCity Authentication Bypass Vulnerability

Updated Malware Signatures (Week 2 March 2024)

Threat	Description
Glupteba	A malware dropper that is designed to download additional malware on an infected machine.
CoinMiner	This malicious software installs and runs cryptocurrency mining applications.
Kuluoz	A backdoor for a botnet. It executes commands from a remote malicious user
Ramnit	A banking trojan used to steal online banking credentials
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.

New Ransomware Victims Last Week: 59

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 a total of 59 new ransomware victims or updates on previous victims across 17 different industries spanning 17 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 (13) distributed across multiple countries. In comparison, Medusa and Play ransomware groups updated 8 victims each, 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
8base	6.78%
Akira	5.08%
Alphv	5.08%
Bianlian	5.08%
Clop	1.69%
Donex	6.78%
Dragonforce	1.69%
Lockbit3	22.03%
Medusa	13.56%
Meow	3.39%
Mogilevich	1.69%
Play	13.56%
Qilin	3.39%
Qqilin	1.69%
Ransomhub	3.39%
Snatch	5.08%

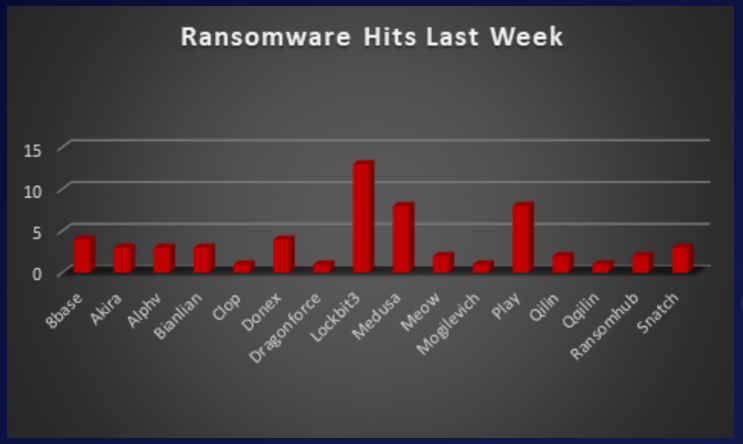

Figure 1: Ransomware Group Hits Last Week

In a comprehensive analysis of ransomware victims across 17 countries, the United States emerges as the most heavily impacted nation, reporting a staggering 32 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
Argentina	1.69%
Australia	3.39%
Austria	1.69%
Belgium	1.69%
Brazil	1.69%
Canada	8.47%
China	3.39%
France	1.69%
Germany	6.78%
India	1.69%
Malaysia	1.69%
Mexico	1.69%
Netherlands	3.39%
Norway	1.69%
Spain	1.69%
Sweden	3.39%
USA	54.24%

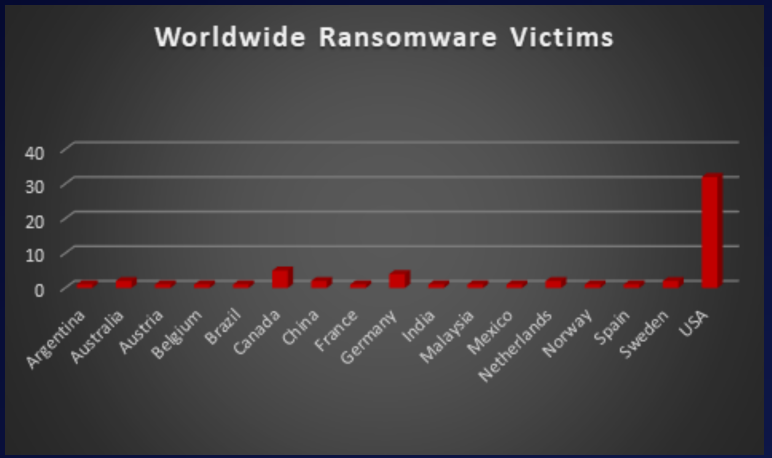

Figure 2: Ransomware Victims Worldwide

Upon further investigation, it has been identified that ransomware has left its mark on 17 different industries worldwide. Notably, the Manufacturing and Business Services sectors bore the brunt of the attacks in the past week, accounting for 13 and 6 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	10.17%
Construction	8.47 %
Consumer Services	1.69%
Education	1.69%
Energy, Utilities & Waste	3.39%
Finance	6.78%
Government	1.69%
Healthcare	5.08%
Hospitality	3.39%
IT	3.39%
Legal Services	5.08%
Manufacturing	22.03%
Organisations	3.39%
Real Estate	3.39 %
Retail	10.17%
Telecom	1.69%
Transportation	8.47%

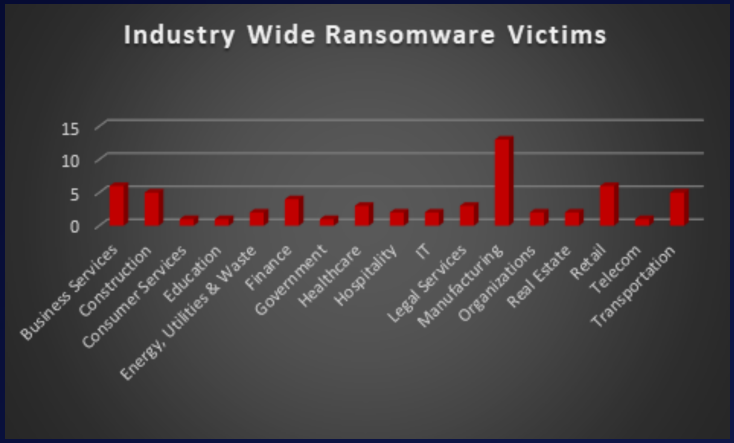

Figure 3: Industry-wide Ransomware Victims