Red Piranha
unified threat management

THREAT INTELLIGENCE REPORT

Sept 12 - 18, 2023

Report Summary:

- **New Threat Detection Added** – 3 (MMRat Malware, DarkGate Malware, and Session Manager IIS Backdoor)
- **New Threat Protections - 14**
- **New Ransomware Victims Last Week - 59**

Newly Detected Threats Added

1. MMRat Malware

In a recent development, cybersecurity researchers have unearthed a formidable new Android banking trojan known as MMRat (AndroidOS_MMRat.HRX). Since its emergence in late June 2023, this insidious malware has set its sights on mobile users in Southeast Asia. MMRat derives its name from its distinct package label, com.mm.user, but its capabilities go far beyond a mere identifier.

This sophisticated threat possesses the ability to clandestinely capture user input and screen content, rendering it a potent tool in the hands of cybercriminals. What makes MMRat particularly concerning is its capacity to exert remote control over compromised devices through a variety of techniques, thereby providing malevolent operators with the means to perpetrate bank fraud directly on the victim's device.

Adding a layer of complexity to its operation, MMRat employs a specialised custom command-and-control (C&C) protocol that relies on protocol buffers, also known as Protobuf. This data serialisation format, commonly used in open-source environments, is an unusual feature in the realm of Android banking trojans. Its incorporation enhances MMRat's efficiency when transmitting substantial volumes of data, further underscoring the sophistication of this emerging cyber threat.

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: Command-and-Control T1071/T1095 - Defence Evasion T1418/T1447 - Credentials Access T1414 - Discovery T1418/T1421/T1430 - Impact T1447/T1448 - Collection T1414/T1429/T1430/T1507 - Network Effects T1449

2. DarkGate Malware

The latest version of DarkGate employs a multifaceted distribution strategy, utilising malvertising, search engine poisoning, and spam campaigns to infiltrate systems. DarkGate is fortified with robust anti-detection and anti-analysis mechanisms, featuring obfuscation, anti-virtual machine detection, and Microsoft Defender Antivirus evasion. It conceals itself within Windows Task Manager and remains invisible upon startup, even against advanced tools.

DarkGate possesses the capability to escalate privileges, granting it admin permissions and remote desktop functionality. It can manipulate files, including moving, copying, viewing, creating, and deleting. Moreover, DarkGate poses a serious threat as it can facilitate chain infections, potentially leading to trojans, ransomware, or cryptocurrency miners.

This malicious program excels in data theft, targeting browsers to extract browsing histories, cookies, and login credentials. Additionally, it can capture tokens from the Discord platform and boasts keylogging abilities, recording keyboard input. Vigilance against this versatile and invasive malware is crucial.

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 T1129 - Privilege Escalation T1055 - Defence Evasion T1027/ T1497 - Discovery 1082 - Command and Control T1095/T1573

3. Session Manager IIS Backdoor

SessionManager is a malicious IIS module coded in C++. It is designed to infiltrate IIS applications and handle legitimate HTTP requests continuously sent to the server. These modules await crafted HTTP requests from operators, executing hidden instructions and then forwarding the requests to the server for normal processing. This approach makes it challenging to detect through standard monitoring, as they do not exhibit typical signs of suspicious behaviour like initiating communication with external servers or using specialised servers to receive commands. The execution is often hidden within overlooked file locations alongside genuine files, further concealing their presence.

This access was utilised for activities such as email collection, malicious access updates, or discreet management of compromised servers that could serve as malicious infrastructure. The SessionManager backdoor has been employed against various types of organisations across different regions, including government entities, military, and industrial organisations in Africa, South America, Asia, Europe, Russia, and the Middle East. it is suspected that the GELSEMIUM threat group may be behind the deployment of this malicious IIS module as part of their espionage operations.

Threat Protected: 10
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: Initial Access T1190 - Execution T1059 - Collection T1005/T1114 - Command-and-Control T1071

Known exploited vulnerabilities (Week 3 September 2023):

Vulnerability	Description
CVE-2023-41061	Apple iOS, iPadOS, and watchOS Wallet Code Execution Vulnerability
CVE-2023-41064	Apple iOS, iPadOS, and macOS ImageIO Buffer Overflow Vulnerability
CVE-2023-36802	Microsoft Streaming Service Proxy Privilege Escalation Vulnerability
CVE-2023-36761	Microsoft Word Information Disclosure Vulnerability
CVE-2023-4863	Google Chromium WebP Heap-Based Buffer Overflow Vulnerability
CVE-2023-20269	Cisco Adaptive Security Appliance and Firepower Threat Defense Unauthorised Access Vulnerability
CVE-2023-35674	Android Framework Privilege Escalation Vulnerability
CVE-2023-26369	Adobe Acrobat and Reader Out-of-Bounds Write Vulnerability

Updated Malware Signatures (Week 3 September 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: 59

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 59 new ransomware victims or updates in a few past victims from 17 distinct industries across 20 countries worldwide. This highlights the global reach and indiscriminate nature of ransomware attacks, which can affect organisations of all sizes and sectors.

LockBit3.0, a specific ransomware, has affected the largest number of victims (08) updates spread across various countries. Cactus and Noscape updated 05 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	1.69%
Abyss-Data	3.39%
Akira	3.39%
Alphv	6.78%
Bianlian	1.69%
Black Suit	1.69%
Blackbyte	3.39%
Cactus	8.47%
Everest	1.69%
Inc Ransom	1.69%
Knight	6.78%
Lockbit3	13.56%
Lorenz	3.39%
Medusa	3.39%
Monti	3.39%
Noescape	8.47%
Play	5.08%
Qilin	1.69%
Ra Group	1.69%
Ransomed	6.78%
Ransomhouse	3.39%
Rhysida	5.08%
Stormous	1.69%
Trigona	1.69%

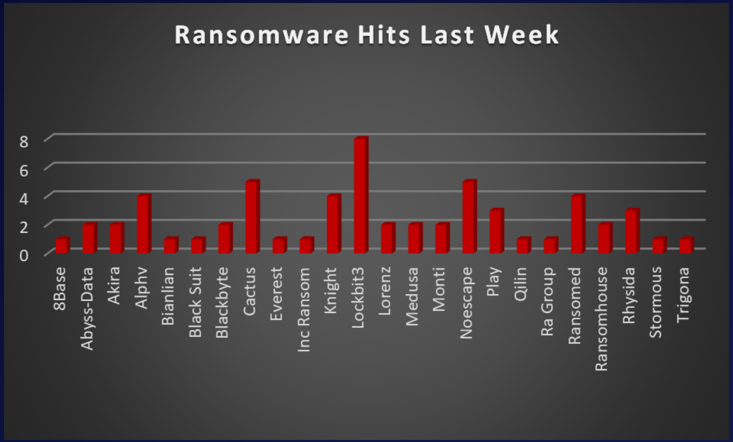

Figure 1: Ransomware Group Hits Last Week

When we examine the victims by country out of 20 countries around the world, we can conclude that the USA was once again the most ransomware-affected country, with a total of 30 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	3.39%
Belarus	1.69%
Bulgaria	5.08%
Canada	8.47%
Catalunya	1.69%
Denmark	1.69%
France	3.39%
Germany	3.39%
Italy	1.69%
Jamaica	1.69%
Japan	1.69%
Mauritius	1.69%
Mexico	3.39%
Singapore	1.69%
Slovakia	1.69%
Spain	1.69%
Thailand	1.69%
UK	3.39%
USA	50.85%

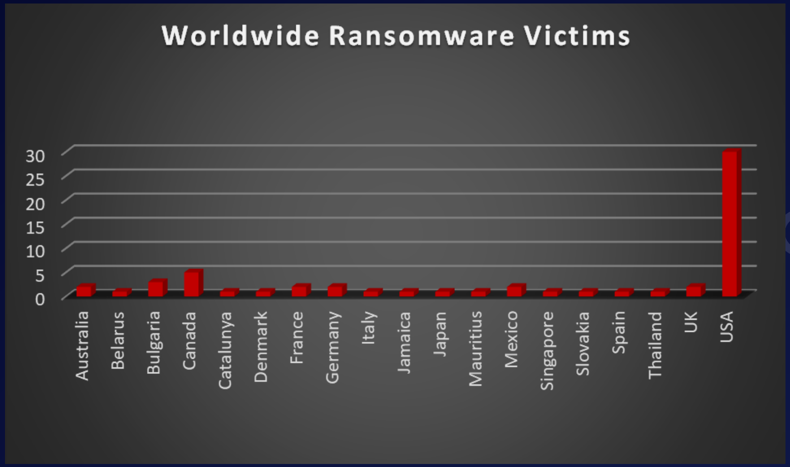

Figure 2: Ransomware Victims Worldwide

After conducting additional research, we found that ransomware has impacted 17 industries globally. Last week, the Retail and Manufacturing sectors were hit particularly hard, with 16% and 15% 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	8.47%
Construction	1.69%
Consumer Services	1.69%
Education	3.39%
Finance	6.78%
Government	6.78%
Healthcare	6.78%
Hospitality	3.39%
Insurance	5.08%
Legal Services	3.39%
Manufacturing	15.25%
Organisation	6.78%
Real Estate	5.08%
Retail	16.9%5
Retails	1.69%
Telecom	3.39%
Transportation	3.39%

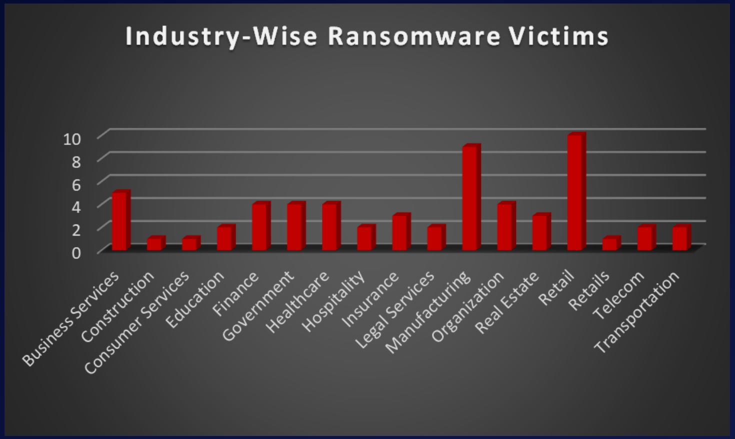

Figure 3: Industry-wise Ransomware Victims