
Red Piranha
unified threat management
THREAT INTELLIGENCE REPORT
July 25 - 31, 2023

Report Summary:

- **New Threat Detection Added** – 3 (NanoCore RAT TraderTraitor APT, and Kimsuky APT)
- **New Threat Protections**
- **New Ransomware Victims Last Week - 130**

Newly Detected Threats Added

1. NanoCore RAT

The NanoCore RAT was discovered in 2013 and sold in underground forums. It is a versatile malware with functions like keylogging, password stealing, tampering with webcams, screen locking, file theft, and more. The current NanoCore RAT is spread through malspam campaigns using social engineering, containing fake bank receipts and requests for quotation. Malicious attachments with .img or .iso extensions are included. Another version is distributed via phishing campaigns with specially-crafted ZIP files to bypass secure email gateways. Stolen data is sent to the attacker's C&C servers.

RAT Capabilities:

- Information Theft
- Backdoor Commands
- Exploits
- Disabling usage capability

Threat Protected: 04
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: Initial Access T1193 - Execution T1204 - Collection T1056 - Exfiltration T1041

2. TraderTraitor APT

GitHub has issued a warning about a sophisticated social engineering campaign aimed at developers working in blockchain, cryptocurrency, online gambling, and cybersecurity industries. The primary objective of this campaign is to compromise their devices with malicious software. The campaign has been attributed to the North Korean state-sponsored hacking group, Lazarus, which is also known by aliases like Jade Sleet (according to Microsoft Threat Intelligence) and TraderTraitor (as per CISA). The US government published a detailed report in 2022, outlining the tactics employed by these threat actors. Notably, Lazarus has a well-documented history of targeting cryptocurrency companies and cybersecurity researchers for cyberespionage and cryptocurrency theft. The group's activities have raised serious concerns within the affected sectors.

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 T1204 - Defence Evasion T1562 - Discovery T1082 - Impact T1486 – Command-and-Control T1071

3. Kimsuky APT

Kimsuky APT, a North Korean threat group known to conduct government cyber espionage operations, has been recently discovered targeting military base maintenance providers. A common tactic for Kimsuky is to lure their targets with phishing emails resembling a notice from the government ministry department. This will include a malicious document that appears as a sign-up form; once executed, it will immediately contact its command-and-control server for further instructions.

Red Piranha has deployed new rules that will detect and prevent the initial domain requests for recently discovered Kimsuky-related sites.

Threat Protected: 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: Initial Access T1566 - Execution T1059 - Persistence T1547 - Command-and-Control T1071

Known exploited vulnerabilities (Week 4 July 2023):

Vulnerability	Description
CVE-2023-35078	Ivanti Endpoint Manager Mobile Authentication Bypass Vulnerability
CVE-2023-38606	Apple Multiple Products Kernel Unspecified Vulnerability
CVE-2023-37580	Zimbra Collaboration (ZCS) Cross-Site Scripting (XSS) Vulnerability

Updated Malware Signatures (Week 4 July 2023)

Threat	Description
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.
Parite	Also known as the W32/Parite Virus which infects Windows computers and is classified as a polymorphic virus
Ramnit	A banking trojan used to steal online banking credentials
Glupteba	A malware dropper that is designed to download additional malware on an infected machine.

New Ransomware Victims Last Week: 130

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 130 new ransomware victims from 20 distinct industries across 21 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 new victims (69) spread across various countries. 8Base and Akira groups follow closely with each hitting 11 and 7 new 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	8.46%
Akira	5.38%
AlphV	3.85%
Black Suit	0.77%
BlackBasta	1.54 %
Clop	53.08 %
Cyclops	2.31%
Donutleaks	0.77%
Everest	0.77%
Karakurt	1.54%
LockBit3.0	4.62%
Mallox	1.54 %
Medusa	2.31%
Monti	1.54%
Noescape	2.31%
Play	3.85%
Ransomware Blog	0.77%
Rhysida	3.85%
Stormous	0.77%

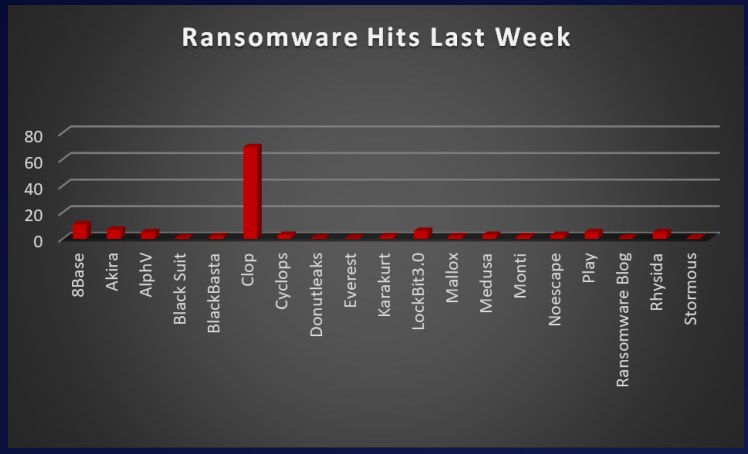

Figure 1: Ransomware Group Hits Last Week

When we examine the victims by country out of 31 countries around the world, we can conclude that the USA was once again the most ransomware-affected country, with a total of 65 new 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	0.77%
Australia	1.54%
Brazil	0.77%
Canada	5.38%
Catalonia	0.77%
China	0.77%
Egypt	0.77%
France	0.77%
Germany	3.85%
Hungary	0.77%
India	0.77%
Iran	0.77%
Ireland	1.54%
Italy	3.85 %
Japan	0.77%
Madagascar	0.77%
Mexico	0.77%
Netherlands	3.08%
New Zealand	0.77%
Nigeria	0.77%
Oman	0.77%
Philippines	0.77%
South Africa	0.77%
Spain	1.54%
Sweden	2.31%
Switzerland	2.31%
Turkey	0.77%
UAE	0.77%
UK	9.23%
USA	50.00%
Vietnam	0.77%

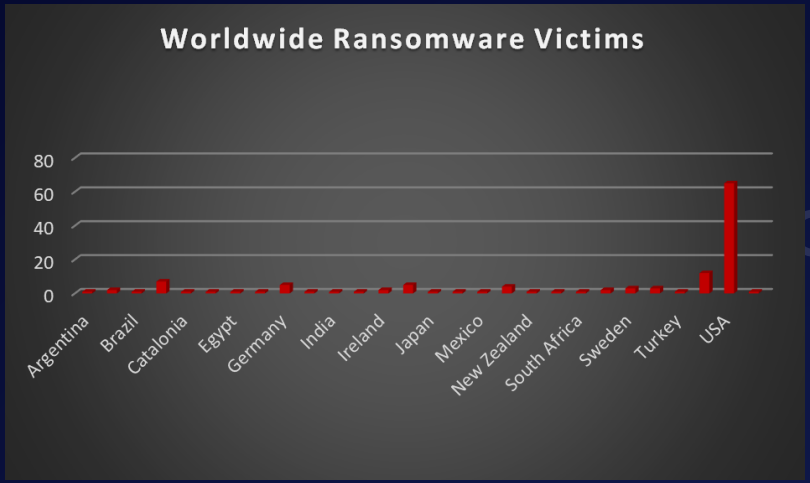

Figure 2: Ransomware Victims Worldwide

After conducting additional research, we found that ransomware has impacted 20 industries globally. Last week, the Manufacturing and Business Services sectors were hit particularly hard, with 19% and 16% 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	16.15%
Construction	6.15%
Consumer Services	2.31%
Education	6.92%
Energy, Utilities & Waste Treatment	2.31%
Finance	7.69%
Government	2.31%
Healthcare	3.85%
Health & Fitness	0.77%
Hospitality	4.62%
Insurance	3.85%
IT	7.69%
Legal Services	3.08%
Manufacturing	19.23%
Media & Internet	1.54%
Real Estate	0.77%
Retail	6.92%
Telecommunication	2.31%
Transportation	0.77%

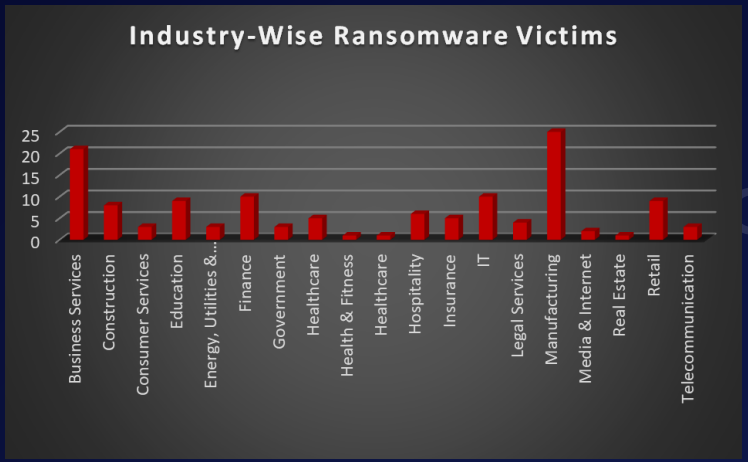

Figure 3: Industry-wise Ransomware Victims