Red Piranha
unified threat management

THREAT INTELLIGENCE REPORT

Mar 12 - 18, 2024

Report Summary:

- **New Threat Detection Added** – 3 (Xeno RAT, Stately Taurus APT and RustDoor Malware)
- **New Threat Protections - 125**
- **New Ransomware Victims Last Week - 81**

Newly Detected Threats Added

1. Xeno RAT

In today's fast-evolving cyber world, understanding and tackling complex malware like Xeno RAT is crucial. Xeno RAT, coded in C#, is a powerful malware with advanced features. Xeno RAT, available on GitHub, was customised and spread via Discord CDN, disguised as a WhatsApp screenshot. It employs various techniques like process injection, DLL manipulation, and obfuscation to infiltrate systems, monitor activities, and communicate with its Command-and-Control server covertly.

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	T1059.003	Windows Command Shell
	T1053.005	Scheduled Task
	T1204.001	Malicious Link
	T1024.002	Malicious File
Persistence	T1053.005	Scheduled Task
Defence Evasion	T1622	Debugger Evasion
	T1497	Virtualization/Sandbox Evasion
	T1055	Process Injection
Discovery	T1622	Debugger Evasion
	T1497	Virtualization/Sandbox Evasion
Command-and-Control	T1071.001	Web Protocols

2. Stately Taurus APT

The State Actor Taurus threat group, linked to Chinese interests, is using various versions of the PUBLOAD malware. Some versions employ Cobalt Strike instead of PlugX and include infostealers. Despite variations, evidence suggests these campaigns are connected. A key clue is the use of specific titles, like one mentioning rebel attacks in Myanmar. Additionally, shared infrastructure indicators such as certificate Common Names, IP addresses, and code similarities tie these campaigns together. This indicates a coordinated effort by the threat group, potentially serving China's geopolitical goals.

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	T1064	Scripting
Persistence	T1543.002	Systemd Service
Privilege Escalation	T1543.002	Systemd Service
Defence Evasion	T1064 T1070 T1564.001	Scripting Indicator Removal Hidden Files and Directories
Discovery	T1082 T1083	System Information Discovery File and Directory Discovery
Command-and-Control	T1071 T1095	Application Layer Protocol Non-Application Layer Protocol

3. RustDoor Malware

RustDoor is a malicious program for Macs, coded in Rust. It acts as a backdoor, sneaking into devices to create access for further infections. Currently, three versions of RustDoor are known, suggesting ongoing development. Though there's weak evidence linking it to certain ransomware groups, shared infrastructure doesn't necessarily imply collaboration. Once inside a device, RustDoor connects to a Command-and-Control server, allowing attackers to issue commands, manipulate files, and even display fake dialogs to trick users. It targets various file types, collecting and sending them to cybercriminals. RustDoor can also download additional malware and steal sensitive data. Future versions may have different or enhanced capabilities.

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: Attempted-admin

Kill Chain:

Tactic	Technique ID	Technique Name
Persistence	T1547.011	Plist Modification
Privilege Escalation	T1547.011	Plist Modification
Defence Evasion	T1564.001	Hidden Files and Directories
Discovery	T1057 T1082	Process Discovery System Information Discovery
Command-and-Control	T1071 T1095 T1105	Application Layer Protocol Non-Application Layer Protocol Ingress Tool Transfer

Known exploited vulnerabilities (Week 3 March 2024):

Vulnerability	CVSS	Description
N/A	N/A	No known exploited vulnerabilities

Updated Malware Signatures (Week 3 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: 81

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 81 new ransomware victims or updates on previous victims across 20 different industries spanning 20 countries. This underscores the widespread and indiscriminate impact of ransomware attacks, emphasising their potential to affect organisations of varying sizes and sectors worldwide.

Play ransomware group stands out as the most prolific, having updated a significant percentage of victims noted (16.05%) distributed across multiple countries.

The Play ransomware group has emerged as a significant threat, having executed over 300 successful attacks since June 2022, according to cybersecurity authorities in the United States and Australia.

This group, known for its devastating tactics, has targeted major American cities such as Oakland and Lowell, Massachusetts, along with Dallas County, causing extensive disruptions and data breaches that took days to rectify. Additionally, they've struck Switzerland, prompting government alerts due to data theft from an IT provider.

Operating discreetly, Play ransomware perpetrators prefer direct email contact for negotiations, omitting ransom demands from their initial communications. Their "double-extortion" approach involves encrypting systems after stealing data, utilising stolen credentials and exploiting vulnerabilities in popular software like FortiOS and Microsoft tools.

To add pressure, they threaten to publish exfiltrated data on the Tor network if victims refuse ransom payments, typically made in cryptocurrency. The Play group's tactics include adding a ".play" extension to filenames and using a variety of tools to disable anti-virus software and exfiltrate data to their control.

Initially targeting Latin American government entities, Play has expanded its reach globally, garnering attention for high-profile attacks on cities like Oakland and organisations like Stanley Steemer and central Virginia's transit system. These attacks have resulted in the exposure of sensitive data, including government records and personal information of citizens and officials, totalling hundreds of gigabytes released on their leak site.

In comparison, Blackbasta and Lockbit3 ransomware groups updated 12 and 11 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
8base	4.94%
Abyss-data	3.70%
Akira	1.23%
Bianlian	2.47%
Black suit	6.17%
Blackbasta	14.81%
Blackbyte	1.23%
Cactus	8.64%
Donutleaks	3.70%
Hunters	6.17%
Lockbit3	13.58%
Medusa	7.41%
Play	16.05%
Qilin	1.23%
Ransomhub	7.41%
Rhysida	1.23%

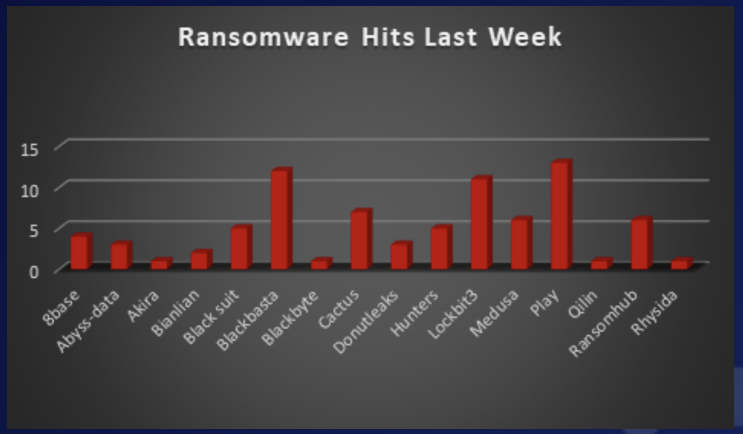

Figure 1: Ransomware Group Hits Last Week

In a comprehensive analysis of ransomware victims across 20 countries, the United States emerges as the most heavily impacted nation, reporting a staggering 41 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
Austria	1.23%
Belgium	1.23%
Canada	7.41%
China	2.47%
Dublin	1.23%
France	2.47%
Germany	4.94%
India	2.47%
Italy	1.23%
Japan	1.23%
Malaysia	1.23%
Mexico	1.23%
Netherlands	3.70%
New Zealand	1.23 %
South Africa	1.23%
Spain	1.23%
Sweden	1.23%
Turkey	1.23%
UK	11.11%
USA	50.62%

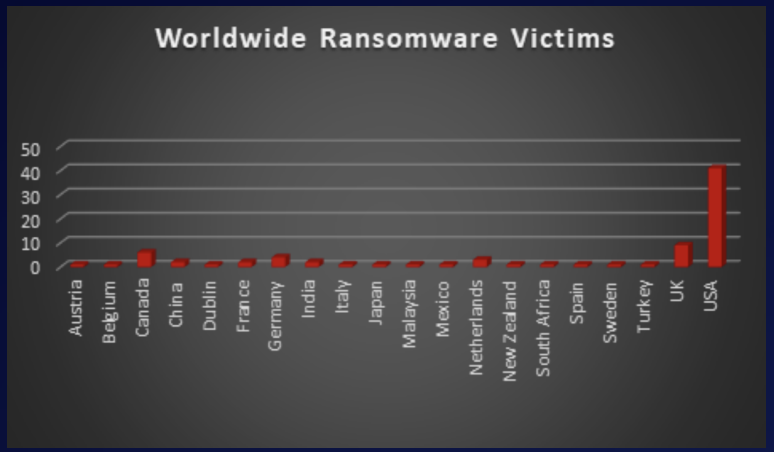

Figure 2: Ransomware Victims Worldwide

Upon further investigation, it has been identified that ransomware has left its mark on 20 different industries worldwide. Notably, the Manufacturing and Construction bore the brunt of the attacks in the past week, accounting for 13 and 11 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 (%)
Agriculture	1.23%
Banking	2.47%
Business Services	12.35%
Construction	13.58%
Consumer Services	3.70%
Education	3.70%
Electronics	1.23%
Energy, Utilities & Waste Treatment	2.47%
Finance	2.47%
Government	1.23%
Healthcare	4.94%
Hospitality	1.23%
Insurance	4.94%
IT	3.70%
Manufacturing	16.05%
Media & Internet	1.23%
Real Estate	2.47%
Retail	11.11%
Telecom	1.23%
Transportation	6.17%

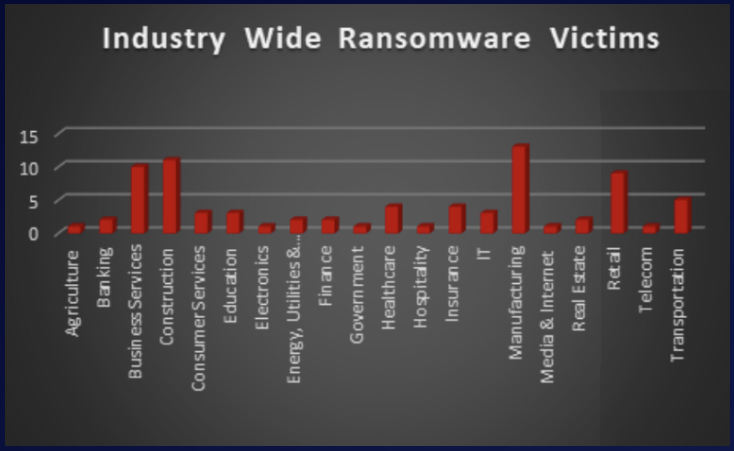

Figure 3: Industry-wide Ransomware Victims