Red Piranha
unified threat management

THREAT INTELLIGENCE REPORT

Jan 30 - Feb 05, 2024

Report Summary:

- **New Threat Detection Added** – 4 (AllaKore RAT, WhiteSnake Stealer, BlueNoroff APT and Jenkins Unauth RCE CVE-2024-23897)
- **New Threat Protections - 180**
- **New Ransomware Victims Last Week - 74**

Newly Detected Threats Added

1. AllaKore RAT

A group driven by financial motives is attacking Mexican banks and cryptocurrency traders using custom installers to distribute a modified version of AllaKore RAT, a remote access tool. The attackers use deceptive tactics, employing naming conventions from the Mexican Social Security Institute (IMSS) and links to seemingly harmless documents. The modified AllaKore RAT enables them to steal banking credentials and authentication details, which are then sent to a command-and-control server for financial fraud. The targets are varied, with a focus on large companies, particularly those with revenues exceeding USD 100 million. The campaign, using numerous Mexico Starlink IPs and Spanish-language instructions, suggests the threat actors are based in Latin America.

Threat Protected: 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	T1059.001	PowerShell
	T1106	Native API
Defence Evasion	T1036	Masquerading
	T1070.006	Timestamp
	T1112	Modify Registry
	T1140	Deobfuscate/Decode Files or Information
	T1222	File and Directory Permissions Modification
	T1497	Virtualisation/Sandbox Evasion
Credential Access	T1056	Input Capture
Discovery	T1016	System Network Configuration Discovery
	T1018	Remote System Discovery
	T1082	System Information Discovery
	T1083	File and Directory Discovery
	T1497	Virtualisation/Sandbox Evasion
Collection	T1056	Input Capture
Command-and-Control	T1071	Application Layer Protocol
	T1095	Non-Application Layer Protocol
	T1105	Ingress Tool Transfer

2. WhiteSnake Stealer

WhiteSnake, also known as Gurcu, is a harmful malware designed to steal sensitive information from computers. Those behind it sell the malware on a hacker forum, offering different access durations at prices ranging from $120 to $1500. This malware works on both Windows and Linux systems, extracting data like passwords, credit card numbers, and screenshots. It targets popular browsers and crypto wallets, extracting information from Brave, Chrome, Edge, Firefox, and wallets like Atomic and Electrum. Additionally, it can access messaging apps like Discord, retrieve files from email clients, and more. The stolen data can be misused for identity theft, fraud, or sold on the dark web, making WhiteSnake a potent tool for cybercriminals.

Threat Protected: 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	T1047	Windows Management Instrumentation
	T1053.005	Scheduled Task
	T1129	Shared Modules
Persistence	T1053.005	Scheduled Task
Privilege Escalation	T1053.005	Scheduled Task
Defence Evasion	T1006	Direct Volume Access
	T1027	Obfuscated Files or Information
	T1036	Masquerading
	T1070	Indicator Removal
	T1140	Deobfuscate/Decode Files or Information
	T1497	Virtualisation/Sandbox Evasion
Credential Access	T1003	OS Credential Dumping
	T1056	Input Capture
Discovery	T1010	Application Window Discovery
	T1012	Query Registry
	T1016	System Network Configuration Discovery
Collection	T1005	Data from Local System
	T1056	Input Capture
	T1119	Automated Collection
	T1123	Audio Capture
Command-and-Control	T1071	Application Layer Protocol
	T1095	Non-Applican Layer Protoco
	T1105	Ingress Tool Transfer

3. BlueNoroff APT

A new type of malware linked to the BlueNoroff APT group has been discovered. This group is known for financially motivated attacks on cryptocurrency exchanges, banks, and venture capital firms. In routine threat hunting, a Mach-O universal binary was found communicating with a known malicious domain. This executable, not detected on VirusTotal during analysis, raised concerns. The malware, written in Objective-C, operates as a simple remote shell, executing commands from the attacker's server. While the initial access method remains unclear, it appears this malware serves as a later-stage tool for manual command execution after a system compromise. Despite its simplicity, the malware is functional, aligning with BlueNoroff's focus on providing remote shell capabilities. Jamf Threat Labs labels it as ObjCShellz within the RustBucket campaign.

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:

Tactic	Technique ID	Technique Name
Execution	T1064	Scripting
Defence Evasion	T1036.001 T1064 T1553.002	Invalid Code Signature Scripting Code Signing
Discovery	T1082 T1518.001	System Information Discovery Security Software Discovery
Command-and-Control	T1071 T1095 T1573	Application Layer Protocol Non-Application Layer Protocol Encrypted Channel

4. Jenkins Unauth RCE CVE-2024-23897

Jenkins versions 2.441 and earlier, as well as LTS 2.426.2 and earlier, do not deactivate a feature in their CLI command parser. This feature substitutes the content of a file for an argument containing an '@' character followed by a file path. This vulnerability enables unauthenticated attackers to read arbitrary files on the Jenkins controller file system.

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 1 February 2024):

Vulnerability	CVSS	Description
CVE-2024-21893	8.2 (High)	Ivanti Connect Secure, Policy Secure, and Neurons Server-Side Request Forgery (SSRF) Vulnerability

Updated Malware Signatures (Week 1 February 2024)

Threat	Description
Valyria	A Microsoft Word-based malware which is used as a dropper for second-stage malware.
LokiBot	An information-stealer malware used to gather data from victims' machines such as stored account credentials, banking information and other personal data.
DarkKomet	A remote access trojan that can take full control over an infected machine.
Qakbot	A malware designed to acquire valuable data such as banking credentials and is also capable of stealing FTP credentials and spreading across a network by utilising SMB.

New Ransomware Victims Last Week: 74

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 74 new ransomware victims or updates on previous victims across 19 different industries spanning 14 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 (16) distributed across multiple countries. In comparison, 8Base and Akira ransomware groups updated 8 and 7 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	1.35%
8Base	10.81%
Abyss-Data	1.35%
Akira	9.46%
Alphv	8.11%
Bianlian	6.76%
Black Suit	1.35%
Blackbasta	1.35%
Cactus	6.76%
Cuba	1.35%
Everest	1.35%
Inc Ransom	6.76%
Knight	4.05%
Lockbit3	21.62%
Medusa	2.70%
Meow	1.35%
Mydata	1.35%
Play	1.35%
Qilin	1.35%
Rhysida	1.35%
Trigona	6.76%
Werewolves	1.35%

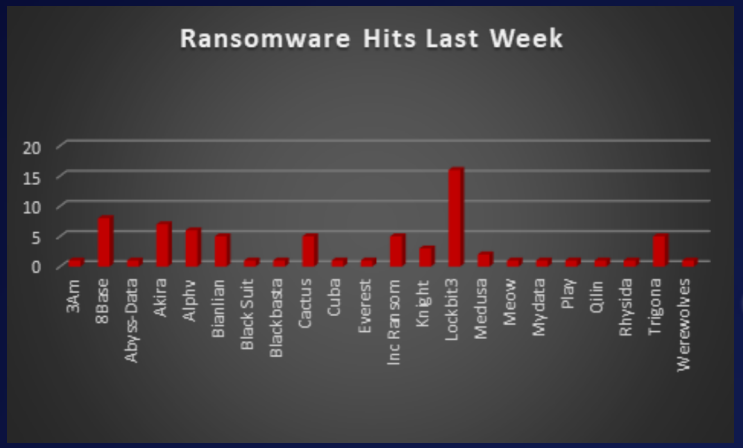

Figure 1: Ransomware Group Hits Last Week

In a comprehensive analysis of ransomware victims across 14 countries, the United States emerges as the most heavily impacted nation, reporting a staggering 51 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	4.05%
Brazil	2.70%
Canada	2.70%
Denmark	1.35%
France	4.05%
Germany	1.35%
Mexico	2.70%
Norway	1.35%
Peru	2.70%
Spain	1.35%
Sweden	1.35%
Texas	1.35%
UK	4.05%
USA	68.92%

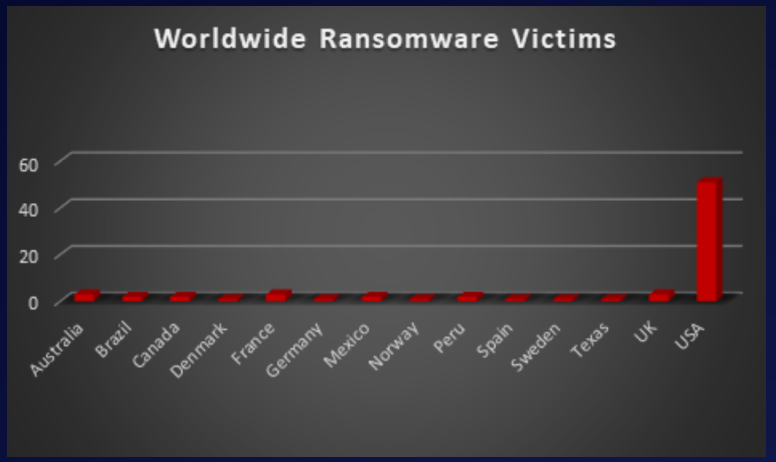

Figure 2: Ransomware Victims Worldwide

Upon further investigation, it has been identified that ransomware has left its mark on 19 different industries worldwide. Notably, the Manufacturing and Business Services sectors bore the brunt of the attacks in the past week, accounting for 12% of the total ransomware victims, each. 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	12.16%
Cities, Towns & Municipalities	2.70%
Construction	9.46%
Consumer Services	4.05%
Education	6.76%
Energy, Utilities & Waste Treatment	5.41%
Government	1.35%
Healthcare	6.76%
Hospitality	2.70%
Insurance	1.35%
IT	5.41%
Legal Services	9.46%
Manufacturing	12.16%
Media & Internet	1.35%
Metals & Mining	2.70%
Organisations	1.35%
Real Estate	2.70%
Retail	5.41%
Transportation	6.76%

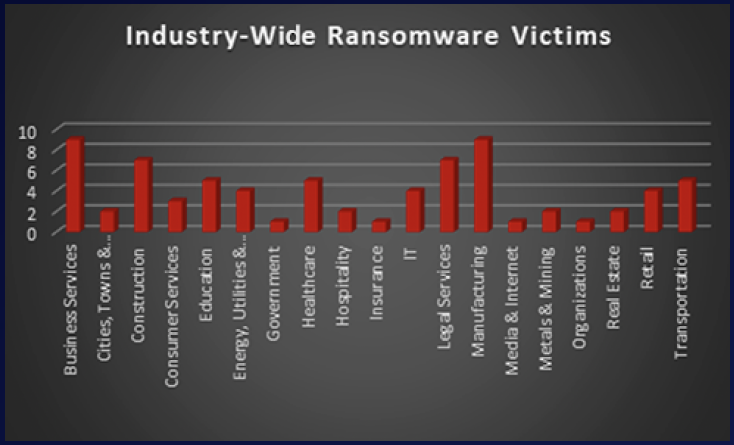

Figure 3: Industry-wide Ransomware Victims