Red Piranha
unified threat management

THREAT INTELLIGENCE REPORT

Feb 27 - Mar 04, 2024

Report Summary:

- **New Threat Detection Added** – 2 (Lumma Stealer and WINELOADER Malware)
- **New Threat Protections - 367**
- **New Ransomware Victims Last Week - 84**

Newly Detected Threats Added

1. Lumma Stealer

Lumma is a piece of malicious software categorised as a stealer. Malware within this category is designed to steal sensitive data. These programs are capable of exfiltrating data from infected systems and the applications installed onto them. Lumma's behaviour is like that of the Mars, Arkei, and Vidar stealers. Stealer-type malware can exfiltrate both device/system and personal data. The latter entails downloading various files (e.g., databases, images, documents, videos, etc.) from the compromised system. Typically, these malicious programs can extract information from browsers, which could include browsing and search engine data, autofills, usernames/passwords, personally identifiable details, credit card numbers, and so forth. Stealers often target various accounts like emails, social media, social networking, messengers, gaming-related software, online banking, e-commerce, cryptocurrency wallets, FTPs, password managers, authentication software, VPNs, and many others.

Rules Created: 10
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 T1140 T1222	Obfuscated Files or Information Deobfuscate/Decode Files or Information File and Directory Permissions Modification
Discovery	T1057 T1083	Process Discovery File and Directory Discovery
Impact	T1496	Resource Hijacking

2. WINELOADER Malware

Researchers found a suspicious PDF from Latvia. It pretends to be an invitation from the Indian Ambassador to a wine-tasting event in February 2024. The PDF links to a fake survey leading to a harmful ZIP file on a compromised site, starting the infection. More digging uncovered another similar PDF also from Latvia. We found a new backdoor called 'WINELOADER'. This likely involves a nation-state aiming to exploit India's ties with European diplomats. The attack targets European diplomats but is low-profile. WINELOADER is sophisticated, hiding data and evading detection. We're watching closely for updates on this threat.

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	T1129	Shared Modules
Persistence	T1547.001	Registry Run Keys / Startup Folder
Defence Evasion	T1027	Obfuscated Files or Information
Discovery	T1082	System Information Discovery

Known exploited vulnerabilities (Week 1 March 2024):

Vulnerability	CVSS	Description
CVE-2023-29360	8.4 (High)	Microsoft Streaming Service Untrusted Pointer Dereference Vulnerability

Updated Malware Signatures (Week 1 March 2024)

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.
CoinMiner	This malicious software installs and runs cryptocurrency mining applications.
Nanocore	The Nanocore trojan, built on the .NET framework, has been the subject of multiple source code leaks, resulting in its widespread accessibility. Similar to other remote access trojans (RATs), Nanocore empowers malicious actors with complete system control, enabling activities such as video and audio recording, password theft, file downloads, and keystroke logging.
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: 84

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 84 new ransomware victims or updates on previous victims across 18 different industries spanning 22 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 stands out as the most prolific, having updated a significant number of victims (15) distributed across multiple countries. In comparison, Alphv and Medus ransomware updated 9 and 6 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	4.76%
Abyss-Data	1.19%
Akira	2.38%
Alphv	10.71%
Bianlian	3.57%
Black Suit	1.19%
Blackbasta	5.95%
Blackout	1.19%
Cactus	3.57%
Ciphbit	1.19%
Clop	2.38%
Dragonforce	3.57%
Dunghill	1.19%
Hunters	1.19%
Inc Ransom	3.57%
Lockbit3	17.86%
Medusa	7.14%
Mogilevich	3.57%
Monti	2.38%
Play	2.38%
Qilin	3.57%
Ransomhouse	5.95%
Ransomhub	4.76%
Rhysida	2.38%
Trigona	2.38%

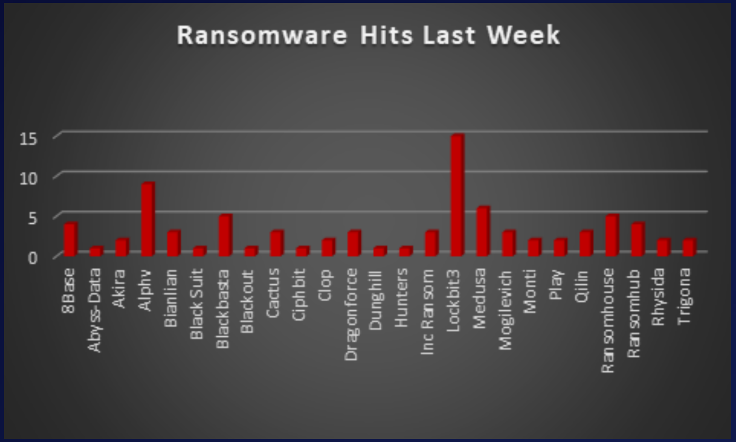

Figure 1: Ransomware Group Hits Last Week

In a comprehensive analysis of ransomware victims across 22 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	2.38%
Bangladesh	1.19%
Canada	4.76%
Costa Rica	1.19%
France	1.19%
Germany	2.38%
India	1.19%
Italy	3.57%
Macedonia	1.19%
Malaysia	1.19%
Netherlands	4.76%
Philippines	1.19%
Saudi Arabia	1.19%
Singapore	1.19%
South Africa	1.19%
Spain	1.19%
Sweden	1.19%
Switzerland	2.38%
Thailand	1.19%
UK	1.19%
USA	60.71 %
Vietnam	2.38%

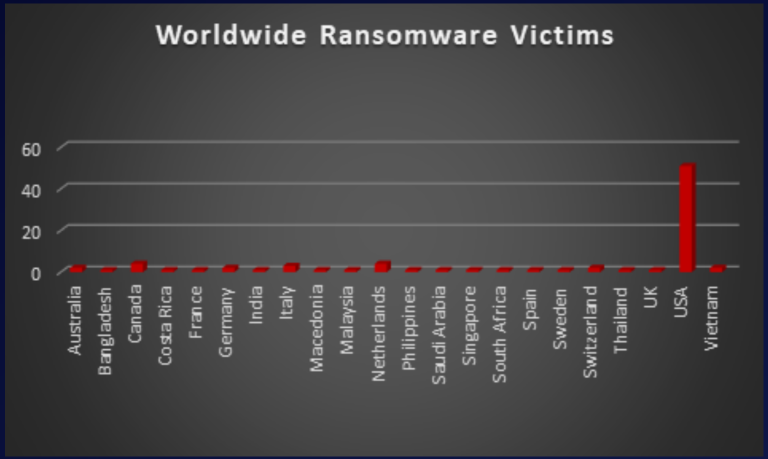

Figure 2: Ransomware Victims Worldwide

Upon further investigation, it has been identified that ransomware has left its mark on 18 different industries worldwide. Notably, the Manufacturing and Healthcare sectors bore the brunt of the attacks in the past week, accounting for 23 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	1.19%
Business Services	2.38%
Construction	9.52%
Consumer Services	1.19%
Education	4.76%
Energy, Utilities & Waste Treatment	1.19%
Finance	2.38%
Government	2.38%
Healthcare	13.10%
Hospitality	4.76%
Insurance	1.19%
IT	7.14%
Legal Services	5.95%
Manufacturing	27.38%
Media & Internet	2.38%
Real Estate	2.38%
Retail	7.14%
Transportation	3.57%

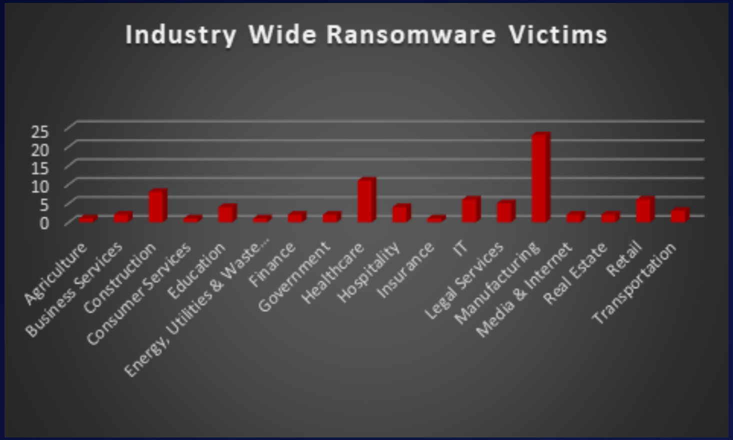

Figure 3: Industry-wide Ransomware Victims