Red Piranha
unified threat management

THREAT INTELLIGENCE REPORT

Jan 16 - 22, 2024

Report Summary:

- **New Threat Detection Added** – 3 (Lumma Stealer, HailBot and Xeno-RAT)
- **New Threat Protections - 26**
- **New Ransomware Victims Last Week - 57**

Newly Detected Threats Added

1. Lumma Stealer

Lumma Stealer, also known as LummaC2 Stealer, is an information-stealing tool built in C language and accessible through a Malware-as-a-Service (MaaS) model on Russian-speaking forums since August 2022. Attributed to the threat actor "Shamel" or "Lumma", it primarily focuses on pilfering from cryptocurrency wallets and two-factor authentication (2FA) browser extensions. The stolen data is then sent to a Command and Control (C2) server through HTTP POST requests with the user agent "TeslaBrowser/5.5". Notably, Lumma Stealer includes a non-resident loader capable of delivering extra payloads in various formats such as EXE, DLL, and PowerShell.

Threat Protected: 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: Execution T1059/T1064/T1129 - Persistence T1547.009 - Privilege Escalation T1055 - Defence Evasion T1027/T1036/T1055/T1064/T1140/T1222 - Credential Access T1056 - Discovery T1018/T1033/T1082/T1497 - Collection T1056 - Command-and-Control T1071/T1095/T1573

2. HailBot

HailBot, derived from Mirai's source code, recently surfaced with attack capabilities supporting four DDoS methods using TCP and UDP protocols. The name stems from the curious output "hail china mainland." Initially active in building its Mirai-based botnet last year, hailBot exhibited exploratory test attacks and increased Command-and-Control (C&C) infrastructure, signalling a large-scale deployment. Investigation into the controller's assets unveiled an IP address connection to distributing bait documents exploiting CVE-2017-11882 vulnerability, aiming for victims in financial institutions. The hailBot controller appears as a systematic, multi-faceted attacker, initially targeting finance and trade, later shifting focus to IoT platforms.

Threat Protected: 14
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: Execution T1064 - Persistence T1543 - Privilege Escalation T1543.002 - Defence Evasion T1064/T1070 - Discovery T1082/T1083 - Command-and-Control T1071/T1095

3. Xeno-RAT

Xeno-RAT stands out as an open-source remote access tool (RAT) crafted in C#. This sophisticated tool offers an extensive array of features for seamless remote system management. From HVNC and live microphone functionality to a reverse proxy and beyond, Xeno-RAT presents a robust toolkit designed to cater to diverse remote access needs.

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: Execution T1047/T1053.005 - Persistence T1053.005/T1547.001 - Privilege Escalation T1053.005/T1547.001 - Defence Evasion T1070.004/T1112/T1620 - Discovery T1012/T1033/T1057/T1082/T1083/T1087 - Collection T1213/T1560.002

Known exploited vulnerabilities (Week 3 January 2024):

Vulnerability	CVSS	Description
CVE-2018-15133	8.1 (High)	Laravel Deserialisation of Untrusted Data Vulnerability
CVE-2023-6549	8.2 (High)	Citrix NetScaler ADC and NetScaler Gateway Buffer Overflow Vulnerability
CVE-2023-6548	5.5 (Medium)	Citrix NetScaler ADC and NetScaler Gateway Code Injection Vulnerability
CVE-2023-35082	9.8 (Critical)	Ivanti Endpoint Manager Mobile (EPMM) and MobileIron Core Authentication Bypass Vulnerability

Updated Malware Signatures (Week 3 January 2024)

Threat	Description
Zeus	Also known as Zbot and is primarily designed to steal banking credentials.
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.
Trojan Miner	This malicious software installs and runs cryptocurrency mining applications.
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: 57

Red Piranha CTI & OSINT Team 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 57 new ransomware victims or updates in the few past victims from 16 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.

We observed that the LockBit3.0 ransomware group has affected the largest number of victims (17) spread across various countries. Akira and 8Base ransomware groups updated 5 victims each last week. Below are the victim counts (%) for these ransomware groups and a few others.

Name of Ransomware Group	Percentage of new Victims last week
3Am	3.51%
8Base	8.77%
Akira	8.77%
Alphv	1.75%
Bianlian	8.77%
Black Suit	1.75%
Cactus	5.26%
Hunters	3.51%
Inc Ransom	1.75%
Insane Ransomware	1.75%
Knight	3.51%
Lockbit3	29.82%
Medusa	1.75%
Qilin	3.51%
Rhysida	1.75%
Slug	1.75%
Snatch	5.26%
Stormous	3.51%
Unsafe	3.51%

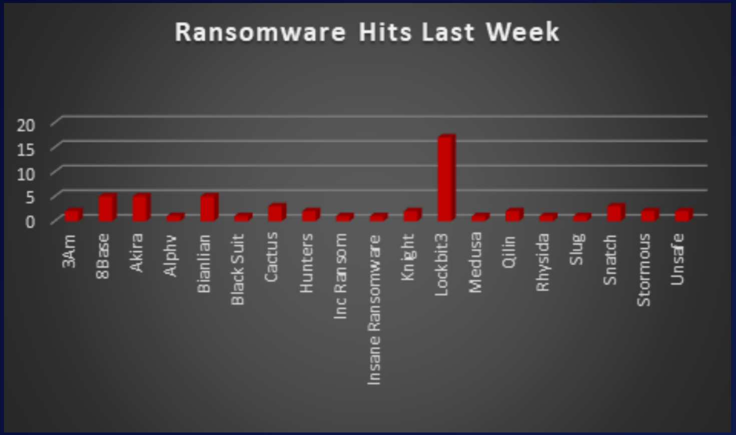

Figure 1: Ransomware Group Hits Last Week

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 25 victims updates last week. The list below displays the number (%) of new ransomware victims per country.

Name of the affected Country	Number of Victims
Australia	1.75%
Brazil	1.75%
Canada	8.77%
Florida	1.75%
France	3.51%
Honduras	1.75%
India	5.26%
Indonesia	1.75%
Ireland	1.75%
Italy	3.51%
Japan	1.75%
Monaco	1.75%
Netherlands	1.75%
Norway	3.51%
Spain	1.75%
Sweden	3.51%
Switzerland	1.75%
Thailand	1.75%
UK	7.02%
USA	43.86%

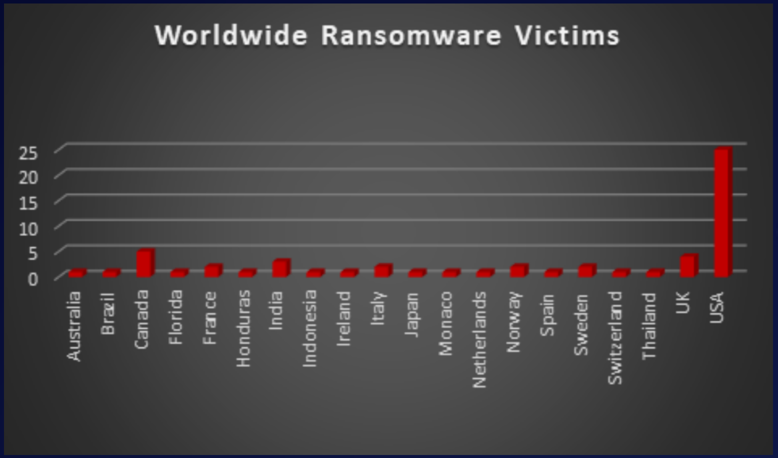

Figure 2: Ransomware Victims Worldwide

After conducting additional research, we found that ransomware has impacted 16 industries globally. Last week, the Manufacturing and Retail sectors were hit particularly hard, with 22% and 12% 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	10.53%
Construction	8.77%
Consumer Services	3.51%
Education	8.77%
Finance	3.51%
Government	1.75%
Healthcare	3.51%
Hospitality	3.51%
IT	1.75%
Legal Services	1.75%
Manufacturing	22.81%
Organisations	3.51%
Real Estate	3.51%
Retail	12.28%
Telecom	5.26%
Transportation	5.26%

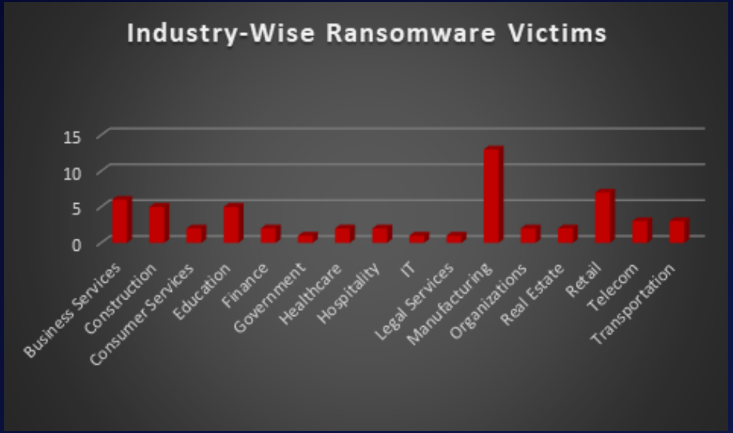

Figure 3: Industry-wise Ransomware Victims