Red Piranha
unified threat management

THREAT INTELLIGENCE REPORT

Apr 25 - May 01, 2023

Report Summary:

- **New Threat Detection Added** – 5 (LeftHook Stealer Malware LimeRAT Malware, CVE-2022-47966, Sch Linux Malware and Atomic MacOS Stealer)
- **New Threat Protections**
- **Overall Weekly Observables Count**
- **Daily submissions by Observable Type**
- **New Ransomware Victims Last Week**

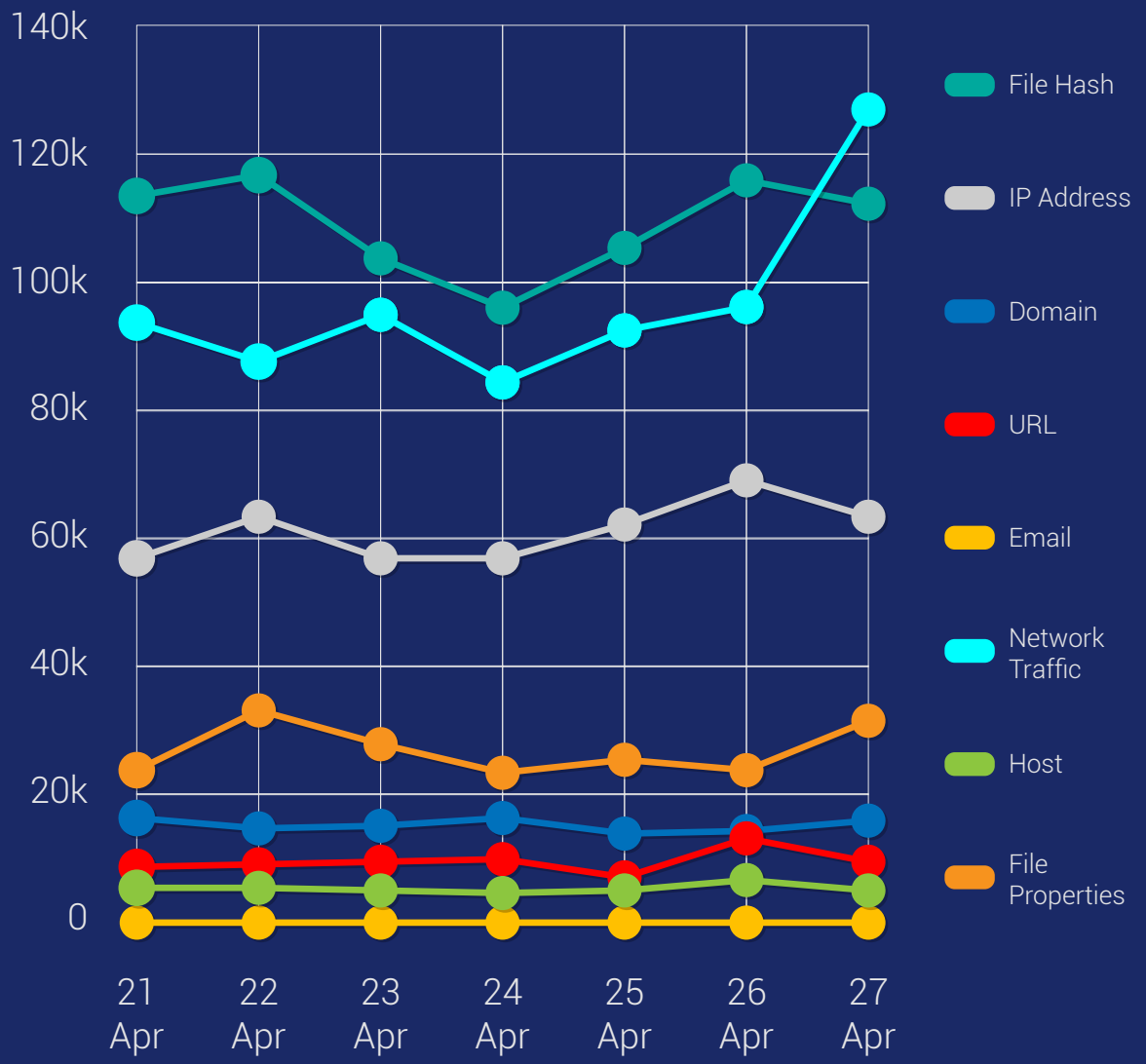
New Threat Protections (Week Ending 01/05/2023):

7

Overall Weekly Observables Count:

2,225,194

Daily Submissions by Observable Type:



Newly Detected Threats Added

1. LeftHook Stealer Malware

LeftHook Stealer malware is a dangerous computer virus that specialises in stealing sensitive information from infected systems. This type of malware can enter a computer system through phishing emails or malicious links on compromised websites. Once installed, the malware runs undetected in the background and silently collects valuable data such as login credentials, banking details, and personal information. LeftHook Stealer is known for its advanced techniques, including its ability to evade detection by antivirus software and the use of encryption to protect stolen data. It is essential to keep software and security systems up-to-date and to use strong and unique passwords to prevent the infiltration of LeftHook Stealer and other similar malware.

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: Execution T1053/T1059/T1129 - Persistence T1053 - Privilege Escalation T1053/T1134 - Defence Evasion T1027/T1036 - Credential Access T1003 - Command-and-Control T1071/T1095 -Impact T1529

2. LimeRAT Malware

The LimeRAT malware is a sophisticated and dangerous threat to computer security, with the ability to capture sensitive information and execute unauthorised commands on infected systems. A detailed analysis of the malware conducted by cybersecurity experts reveals its complex structure and the various techniques it employs to evade detection and compromise target systems. LimeRAT uses a multi-stage infection process, making it difficult to detect and remove. Its command-and-control infrastructure is also highly resilient and difficult to take down. Organisations and individuals are advised to take proactive measures to protect themselves against this and other emerging malware threats.

Threat Protected: 01
Rule Set Type:

Class Type: Trojan- Activity
Kill Chain: Defence Evasion T1027/T1112 - Discovery T1012/T1033/T1057/T1082/T1083

Ruleset	IDS: Action	IPS: Action
Balanced	Alert	Alert
Security	Reject	Drop
WAF	Disabled	Disabled
Connectivity	Alert	Alert
OT	Disabled	Disabled

3. ManageEngine RCE (CVE-2022-47966)

CVE-2022-47966 is a critical vulnerability that affects Zoho ManageEngine versions before 14.3 build 14330. The vulnerability in Zoho ManageEngine's SAML authentication feature occurs due to improper validation of XML signatures in SAML assertions. Specifically, the vulnerability is due to using an insecure XSLT (Extensible Stylesheet Language Transformations) processor in the signature validation process. An attacker can exploit this vulnerability by crafting a malicious SAML assertion that includes a specially crafted XSLT stylesheet that triggers the vulnerable XSLT processor, allowing the attacker to execute arbitrary code on the affected system.

Threat Protected: 02
Rule Set Type:

Class Type: Malware
Kill Chain: Initial Access T1190 - Execution T1059

Ruleset	IDS: Action	IPS: Action
Balanced	Reject	Drop
Security	Reject	Drop
WAF	Disabled	Disabled
Connectivity	Alert	Alert
OT	Disabled	Disabled

4. Sch Linux Malware

It has been observed that a Linux malware developed with Shc has been installing a CoinMiner. Shc is an abbreviation for Shell Script Compiler and is responsible for converting Bash shell scripts into an ELF (Executable and Linkable Format). The Shc data section contains the original Bash shell script encoded with the Alleged RC4 algorithm. When it is executed afterwards, the same ARC4 algorithm is used to decode the original script, and the decoded script commands are executed.

Threat Protected: 01
Rule Set Type:

Ruleset	IDS: Action	IPS: Action
Balanced	Alert	Drop
Security	Reject	Drop
WAF	Disabled	Disabled
Connectivity	Alert	Alert
OT	Disabled	Disabled

Class Type: Malware
Kill Chain: Execution TA0002 - Persistence TA0003 - Privilege Escalation TA0004 - Defence Evasion TA0005 - Discovery TA0007 - Exfiltration TA0010 - Command-and-Control TA0011

5. Atomic MacOS Stealer

Atomic MacOS Stealer (AMOS) is a new information-stealer that has been discovered being advertised in Telegram channels. It is designed to steal sensitive information from MacOS machines. It is capable of collecting Keychain passwords, system information, files and documents, as well as, crypto wallets. The threat actor also provides additional services for AMOS such as a web panel for managing the infected machines among others for a monthly subscription.

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 T1204 - Credential Access T1110/T1555 - Command-and-Control T1132 - Exfiltration T1041

Known exploited vulnerabilities (Week 4 April 2023):

Vulnerability	Description
CVE-2023-2136	Google Chrome Skia Integer Overflow Vulnerability
CVE-2023-27350	PaperCut MF/NG Improper Access Control Vulnerability
CVE-2023-28432	MinIO Information Disclosure Vulnerability

Updated Malware Signatures (Week 4 April 2023)

Threat	Description
MacStealer	A remote access trojan enables its operator to take control of a victim machine and steal data. It is usually distributed through spam and phishing emails.
Zeus	Also known as Zbot and is primarily designed to steal banking credentials.
LokiBot	An information-stealer malware is used to gather data from victims' machines such as stored account credentials, banking information and other personal data.
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.

New Ransomware Victims Last Week: 94

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 94 new ransomware victims from 18 distinct industries across 34 countries worldwide. This highlights the global reach and indiscriminate nature of ransomware attacks, which can affect organisations of all sizes and sectors.

LockBit 3.0, a specific ransomware, has affected the largest number of new victims (35) spread across various countries. Alphv and Royal groups follow closely with each hitting 28 and 05 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
Alphv	30.11%
Bianlian	5.38%
Blackbyte	2.15%
Clop	2.15%
Everest	1.08%
Karakurt	5.38%
Lockbit3	37.63%
Medusa	4.30%
Play	2.15%
Ragnarlocker	1.08%
Ransomhouse	2.15%
Royal	5.38%
Vicesociety	1.08%

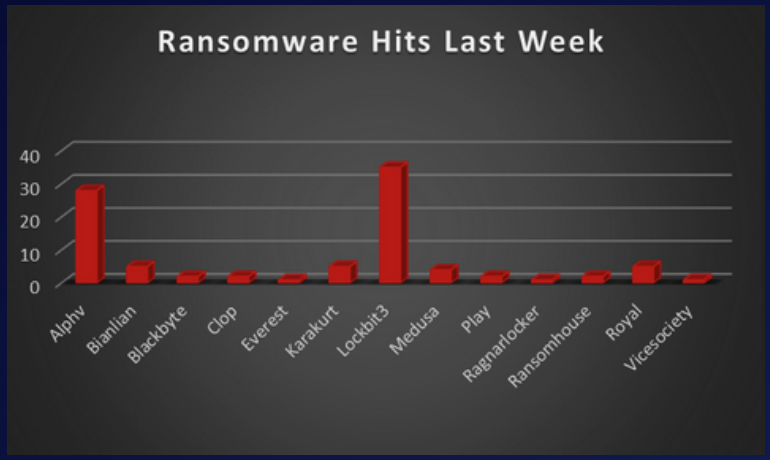


Figure 1: Ransomware Group Hits Last Week

When we examine the victims by country out of 34 countries around the world, we can conclude that the USA was once again the most ransomware-affected country, with a total of 36 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
Africa	2.15%
Angola	1.08%
Argentina	1.08%
Australia	1.08%
Austria	1.08%
Brazil	2.15%
Cameroon	1.08%
Canada	3.23%
Chile	1.08%
China	2.15%
Colombia	1.08%
Croatia	1.08%
France	7.53%
Germany	6.45%
Greece	1.08%
Guatemala	2.15%
Hong Kong	1.08%
India	2.15%
Italy	2.15%
Japan	2.15%
Kenya	1.08%
Kuwait	1.08%
Malaysia	2.15%
Morocco	1.08%
Netherlands	1.08%
Norway	1.08%
Spain	1.08%
Sweden	1.08%
Switzerland	2.15%
Thailand	1.08%
UAE	1.08%
UK	3.23%
USA	38.71%
Venezuela	1.08%

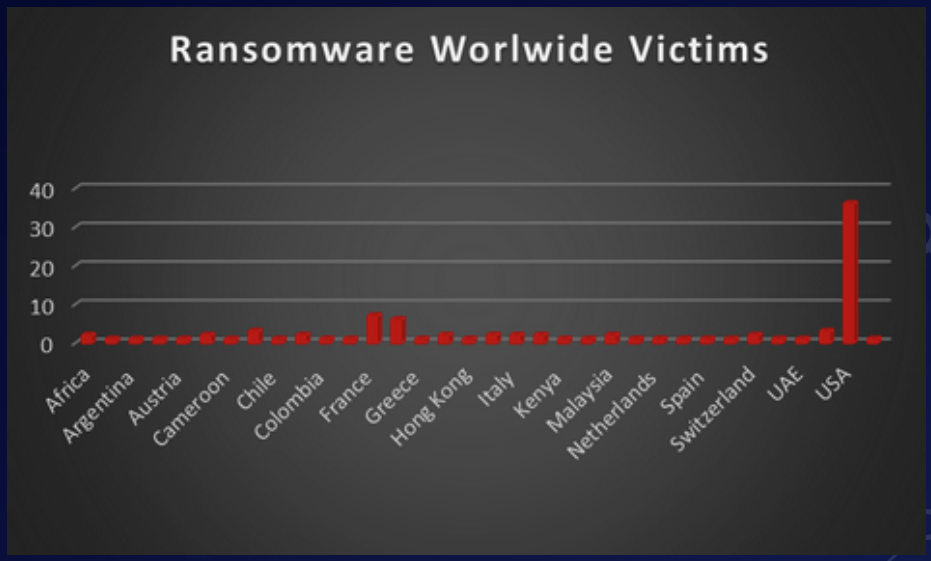


Figure 2: Ransomware Victims Worldwide

After conducting additional research, we found that ransomware has impacted 18 industries globally. Last week, the Manufacturing and Retail sectors were hit particularly hard, with the loss of 21 and 13 businesses in each sector respectively. The table below presents the most recent ransomware victims sorted by industry.

Industry	Victims Count (%)
Business Services	11.83%
Agriculture	2.15%
Construction	4.30%
Education	5.38%
Energy	3.23%
Finance	3.23%
Government	1.08%
Healthcare	11.83%
Hospitality	4.30%
Insurance	1.08%
IT	3.23%
Legal Services	2.15%
Manufacturing	22.58%
Organisations	1.08%
Real Estate	2.15%
Retail	13.98%
Telecommunication	1.08%
Transportation	5.38%

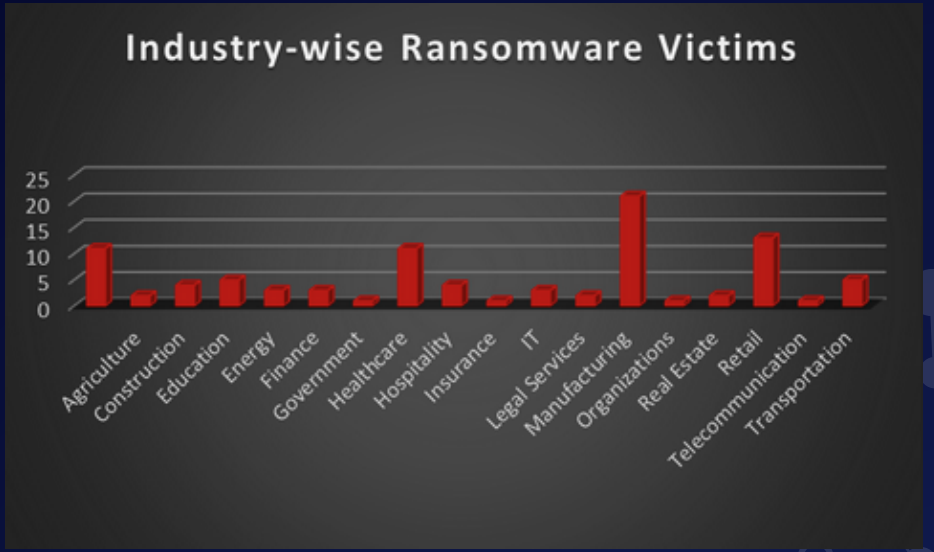


Figure 3: Industry-wise Ransomware Victims