
Red Piranha
unified threat management
THREAT INTELLIGENCE REPORT
Apr 11 - 17, 2023

# Report Summary:

- **New Threat Detection Added** – 4 (Chameleon: Android Banking Trojan, Cylance Ransomware, Havoc demon backdoor, and CaddyWiper)
- **New Threat Protections**
- **Overall Weekly Observables Count**
- **Daily submissions by Observable Type**
- **New Ransomware Victims Last Week**

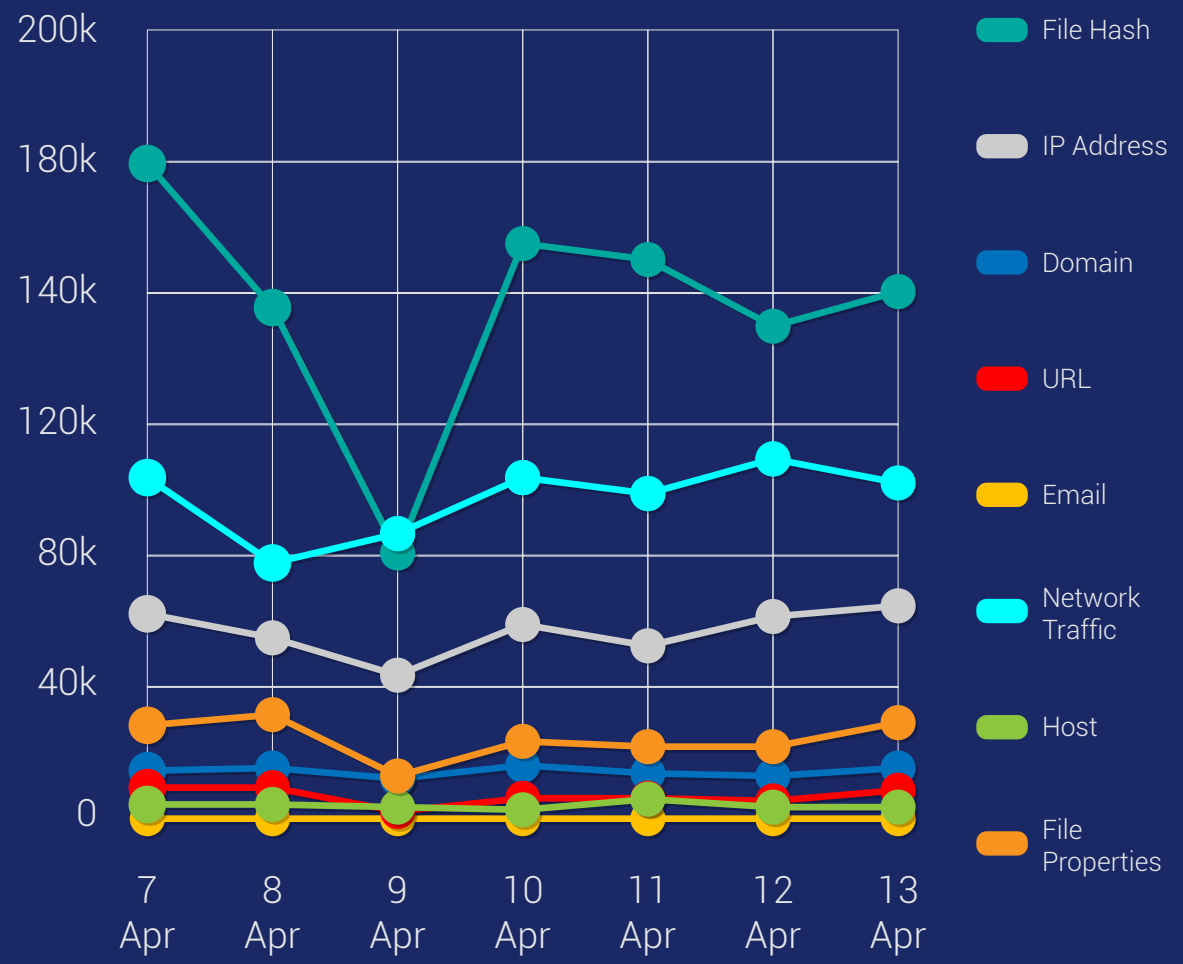
## New Threat Protections (Week Ending 17/04/2023):

**6**

## Overall Weekly Observables Count:

**2,358,910**

## Daily Submissions by Observable Type:



# Newly Detected Threats Added

## 1. Chameleon: Android Banking Trojan

A novel Android Banking Trojan has recently been identified by researchers and is dubbed "Chameleon". This new strain appears to be unrelated to any known Trojan families and has been active since January 2023, with users in Australia and Poland being specifically targeted. The Chameleon Trojan uses the Accessibility Service to perform malicious activities similar to other Banking Trojans and masquerades as legitimate apps like CoinSpot, a cryptocurrency app, and government agencies in Australia and Poland, such as IKO Bank. The Trojan was observed using different software icons to infect Android users, including ChatGPT, Chrome, and Bitcoin.

Distribution of the Chameleon Trojan is through various means, including compromised websites, Discord attachments, and Bitbucket hosting services. The Trojan is capable of several malicious activities, such as keylogging, overlay attacks, SMS harvesting, preventing uninstallation, cookie stealing, lock grabbing, and employing anti-emulation techniques. Additionally, the Trojan can disable Google Play Protect, and to auto-uninstall.

At present, the Chameleon Banking Trojan is still in its early stages of development and has limited capabilities, with injection and keylogging techniques being its primary methods for stealing users' credentials. However, the malware may have new features added in the future. The Trojan communicates with a Command-and-Control (C&C) server and users are advised to be cautious while downloading applications from unknown sources.

**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:** Initial Access T1476/T1444 - Collection T1517/T1412/T1409 - Discovery T1418 - Persistence T1402 - Impact T1510 - Defence Evasion T1523/T1406/T1508/T1576

## 2. Cylance Ransomware

A new ransomware that can target both Linux and Windows operating systems has been identified by researchers. The ransomware has the ability to accept different command line parameters and can flexibly adjust to customized encryption tactics. Upon execution, the ransomware enables various Windows privileges for the current process, which allows access to restricted actions typically only permitted for processes with higher privileges. These actions include debugging other processes, modifying system security settings, and restoring files and directories. The ransomware then creates a scheduled task entry for persistence, enabling it to run automatically every time the victim logs into their computer.

The ransomware gathers details about disk volumes and their associated file systems. As organizations implement measures to protect themselves against ransomware attacks, there is a corresponding increase in the number of new ransomware groups emerging. These groups continuously evolve their tactics and expand their operations to maximize their financial gains.

**Threat Protected:** 01
**Rule Set Type:**

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

**Class Type:** Trojan- Activity
**Kill Chain:** Initial Access - T1133/T1566/T1091 - Execution T1059/T1204/T1047 - Persistence T1053 - Privilege Escalation T1134 - Defence Evasion T1564/T1027 - Discovery T1082/T1135/T1083 - Impact T1486

## 3. Havoc Demon Backdoor

A new threat campaign leveraging the open-source Havoc C2 framework targeting Government organisations has been observed. The backdoor consists of three components –

- ShellCode Loader
- KaynLdr Shellcode
- Demon DLL

The shellcode loader Disables the Event Tracing for Windows (ETW) to evade detection mechanisms and Decrypts and executes the shellcode via CreateThreadpoolWait(). The KaynLdr Reflectively loads the Havoc's Demon DLL without the DOS and NT headers to evade detection and Performs an API hashing routine to resolve virtual addresses of various NTAPIs by using a modified DJB2 hashing algorithm. The Demon DLL's tasks are Parsing configuration files, Usage of Sleep Obfuscation Techniques, Communication with the CnC Server - CheckIn Request and Command Execution, Performs In-Direct Syscalls and Return Address Stack Spoofing and more.

**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:** Backdoor
**Kill Chain:** Execution TA0002 - Defence Evasion TA0005 - Discovery TA0007 - Command-and-Control TA0011

## 4. CaddyWiper

A destructive wiper termed CaddyWiper has been found targeting government organisations. The wiper is deployed by group policy to the infected system. Once run, as administrator, the system will crash. Once the computer is rebooted it crashes and will not start anymore and prompt that it cannot locate the operating system. If the sample is opened in a disassembler, in this case, Ghidra, it can be seen that it uses a lot of stack strings for obfuscation. Upon start, the wiper uses the API call DsRoleGetPrimaryDomainInformation to check if the computer is the primary domain controller by comparing it to the hard-coded value 0x5, which comes from the struct DSROLE_MACHINE_ROLE. If it is the primary domain controller it will exit. This is probably done because the threat actor is using the domain controller as the source of distribution of the wiper and not to ruin its foothold.

**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:** Malware
**Kill Chain:** Execution TA0002 - Persistence TA0003 - Defence Evasion TA0005 - Credential Access TA0006 - Discovery TA0007 - Command-and-Control TA0011

## Known exploited vulnerabilities (Week 2 April 2023):

For more information, refer to the Forum – Security Advisory

| Vulnerability | Description |
|---|---|
| CVE-2023-20963 | Android Framework Privilege Escalation Vulnerability |
| CVE-2023-29492 | Novi Survey Insecure Deserialization Vulnerability |
| CVE-2023-28252 | Microsoft Windows Common Log File System (CLFS) Driver Privilege Escalation Vulnerability |
| CVE-2023-28205 | Apple Multiple Products WebKit Use-After-Free Vulnerability |
| CVE-2023-28206 | Apple iOS, iPadOS, and macOS IOSurfaceAccelerator Out-of-Bounds Write Vulnerability |

Updated Malware Signatures (Week 2 April 2023)

| 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. |
| QuasarRat | A remote access trojan that was made available to the public as an open-source project. Once installed on a victim's machine, it is capable of keylogging, data and screen capturing among other things. It is also known to be highly customizable depending on the threat actor's intended need. |
| TeslaCrypt | A ransomware that started in the year 2015. It is usually distributed through spam email campaigns, malicious attachments, and exploit kits. |
| LokiBot | An information-stealer malware used to gather data from victims' machines such as stored account credentials, banking information and other personal data. |
| Cerber | Another type of ransomware but instead of the usual ransom text files, it plays audio on the victim's infected machine. |
| Glupteba | A malware dropper that is designed to download additional malware on an infected machine. |
| Upatre | Upatre is also a malware dropper that downloads additional malware on an infected machine. It is usually observed to drop banking trojan after the initial infection. |

## New Ransomware Victims Last Week: 82

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 82 new ransomware victims from 20 distinct industries across 29 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 (32) spread across various countries. Bianlian and Money message groups follow closely with each hitting 11 and 08 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 | 7.32% |
| Avoslocker | 3.66% |
| Bianlian | 13.41% |
| Blackbyte | 4.88% |
| Dunghill | 1.22% |
| Karakurt | 2.44% |
| Lockbit3 | 39.02% |
| Medusa | 1.22% |
| Money message | 9.76% |
| Play | 8.54% |
| Royal | 7.32% |
| Unsafe | 1.22% |

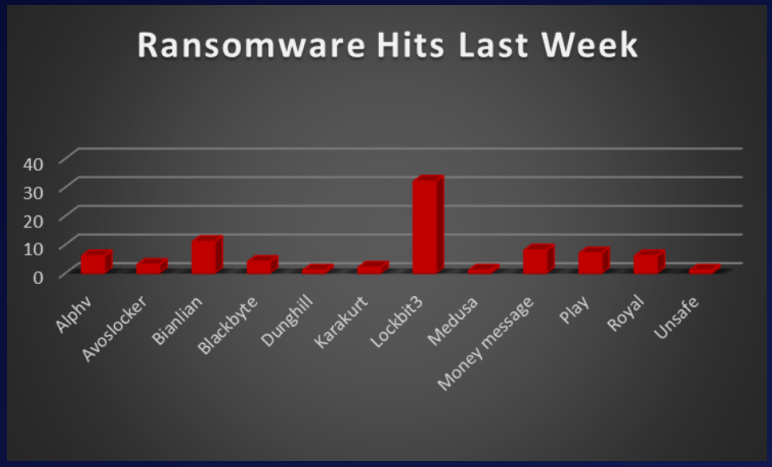



*Figure 1: Ransomware Group Hits Last Week*

When we examine the victims by country out of 29 countries around the world, we can conclude that the USA was once again the most ransomware-affected country, with a total of 39 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 |
|---|---|
| Australia | 1.22% |
| Belgium | 1.22% |
| Canada | 7.32% |
| Chile | 1.22% |
| Cyprus | 1.22% |
| Czech Republic | 1.22% |
| Egypt | 1.22% |
| Europe | 1.22% |
| France | 1.22% |
| Germany | 2.44% |
| Greece | 1.22% |
| Italy | 1.22% |
| Malaysia | 2.44% |
| Mexico | 2.44% |
| Netherlands | 1.22% |
| Peru | 1.22% |
| Philippines | 3.66% |
| Poland | 2.44% |
| Romania | 1.22% |
| Spain | 3.66% |
| Switzerland | 1.22% |
| Taiwan | 1.22% |
| Thailand | 1.22% |
| UK | 3.66% |
| USA | 47.56% |

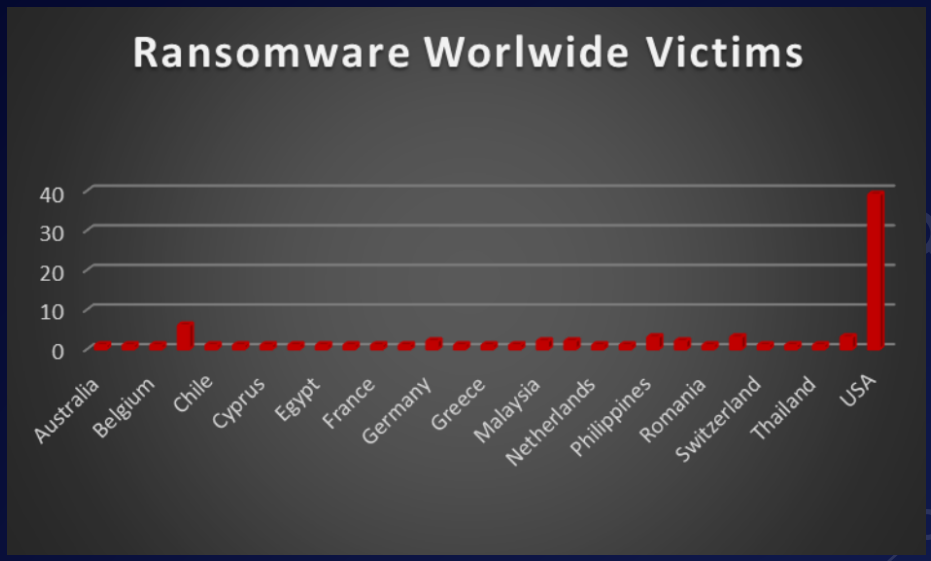



*Figure 2: Ransomware Victims Worldwide*

After conducting additional research, we found that ransomware has impacted 19 industries globally. Last week, the manufacturing and Business Services sectors were hit particularly hard, with the loss of 20 and 07 businesses in each sector respectively. The table below presents the most recent ransomware victims sorted by industry.

| Industry | Victims Count (%) |
|---|---|
| Agriculture | 1.22% |
| Business Services | 8.54% |
| Construction | 8.54% |
| Consumer Services | 2.44% |
| Education | 3.66% |
| Energy | 3.66% |
| Finance | 6.10% |
| Government | 3.66% |
| Healthcare | 7.32% |
| Hospitality | 3.66% |
| Insurance | 2.44% |
| IT | 7.32% |
| Legal | 2.44% |
| Manufacturing | 24.39% |
| Media | 2.44% |
| Real Estate | 1.22% |
| Retail | 4.88% |
| Telecommunications | 1.22% |
| Transportation | 4.88% |

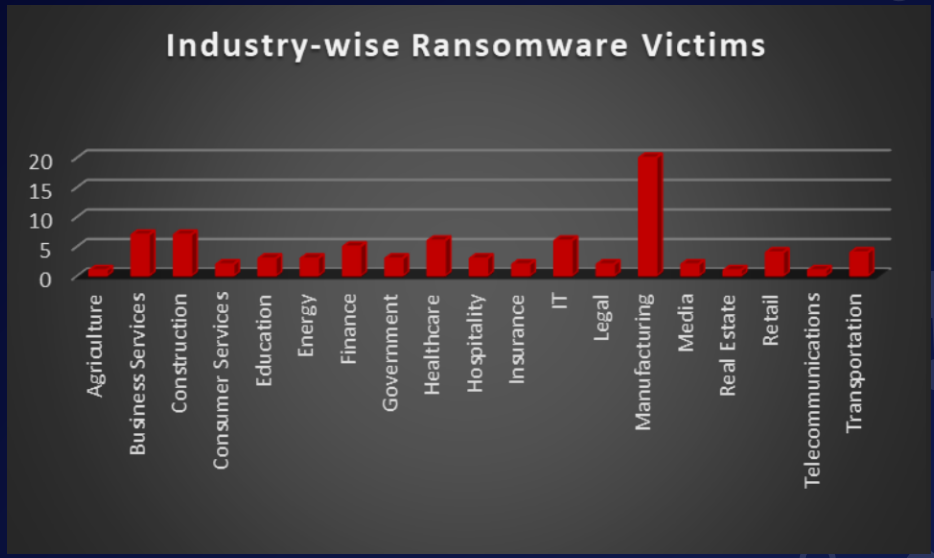



*Figure 3: Industry-wise Ransomware Victims*