Quick Heal
Security Simplified

QUICK HEAL

THREAT REPORT

QUARTER 2 - 2022

Join Us

THREAT REPORT
Q2-2022

About Quick Heal

Quick Heal Technologies Ltd. is one of the leading IT security solutions company. Each Quick Heal product is designed to simplify IT security management for home users, small businesses, Government establishments, and corporate houses.

Contributors

Quick Heal **Security Labs** | Quick Heal **Marketing Team**

About Quick Heal Security Labs

A leading source of threat research, threat intelligence and cybersecurity, Quick Heal Security Labs analyses data fetched from millions of Quick Heal products across the globe to deliver timely and improved protection to its users.

www.quickheal.com

For an overview of the latest security threats and trends for enterprises, please refer to the threat report by Seqrite, enterprise security brand of Quick Heal Technologies Ltd. Visit **www.seqrite.com**

Contents

1. FOREWORD 01
2. WINDOWS 02
- Windows Detection Statistics Q2 2022 03
- Detection Statistics – Month Wise 04
- Detection Statistics – Week-Over-Week 04
- Ransomware – Week-Over-Week 05
- Detection Statistics – Protection Wise 05
- Detection Statistics – Category Wise 07
- Coin Miner Detection Statistics 08
- Phishing Attack Statistics 09
- Top 5 Windows Malware 10
- Top 5 Potentially Unwanted Applications (PUA) and Adware 13
- Top 5 Host-Based Exploits 14
- Top 5 Network-Based Exploits 15
- Top 5 Affected Cities 17
- Top 5 Affected States 17
- Trends in Windows Security Threats 18

3. ANDROID 20
- Quick Heal Android Malware Detection for Q2 2022 21
- Detection Statistics: Category Wise 22
- Security Vulnerabilities Discovered 22
- Top 5 Android Malware for Q2 2022 23
- Trends in Android Security Threats 26

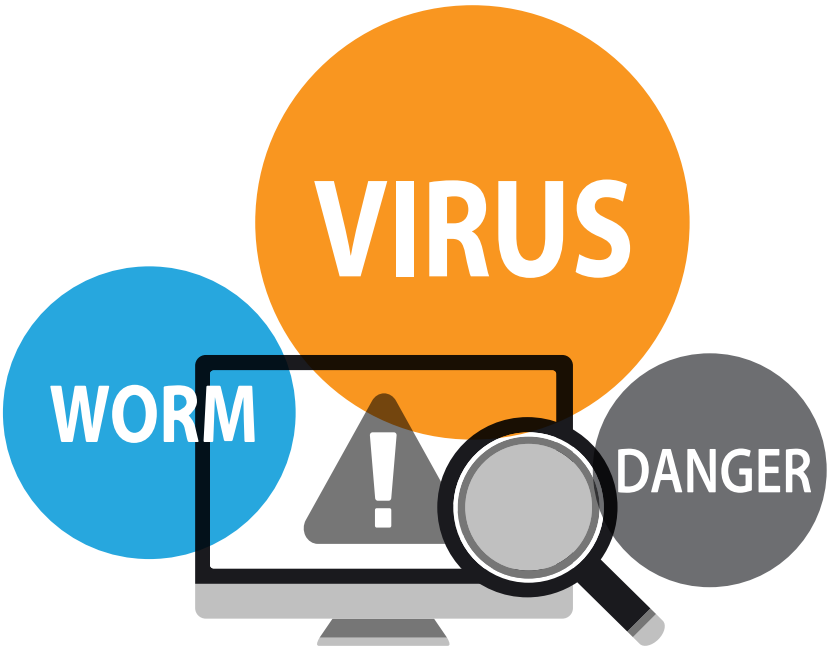
4. Inference 28

Foreword

The internet has changed the way we browse our computers. From online shopping to business execution, the internet is evolving people socially. However, when accessing the internet, many of us forget the basics of using the internet, which is – maintaining our online privacy, which the hackers can use for their advantage leading to various cyber-attacks.

Threat actors are nowadays busy rebuilding older malware and spend the saved time discovering new exploits. They are becoming more sophisticated and personal in attempts to steal information by handpicking their targets according to priorities.

This Quick Heal Threat Report covers the insights from the past three months on various Malware, Trojan, and Exploits. Read the report to get more insights into the threat landscape and multiple tips to save yourself from the latest vulnerabilities.



WINDOWS

103 Million Windows Malware detected in Q2 2022

34 Million Windows Malware detected in June'22

1.13 Million Malware daily average detected in Q2 2022

Windows Detection

Statistics Q2 2022

Malware:
103 Million
Per Day: 1,131,051
Per Hour: 47,127
Per Minute: 785

Ransomware:
0.22 Million
Per Day: 2,436
Per Hour: 102
Per Minute: 2

Exploit:
5.20 Million
Per Day: 57, 190
Per Hour: 2,383
Per Minute: 40

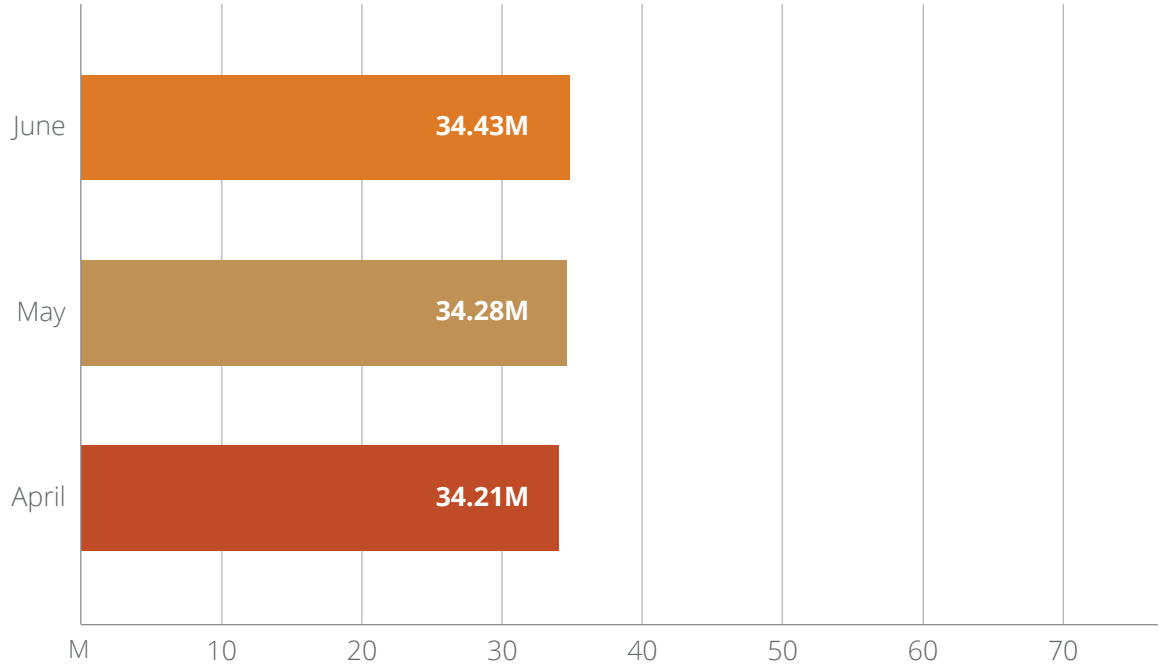
PUA & Adware:
6.03 Million
Per Day: 66,218
Per Hour: 2,759
Per Minute: 46

Cryptojacking:
3.58 Million
Per Day: 39,318
Per Hour: 1,638
Per Minute: 27

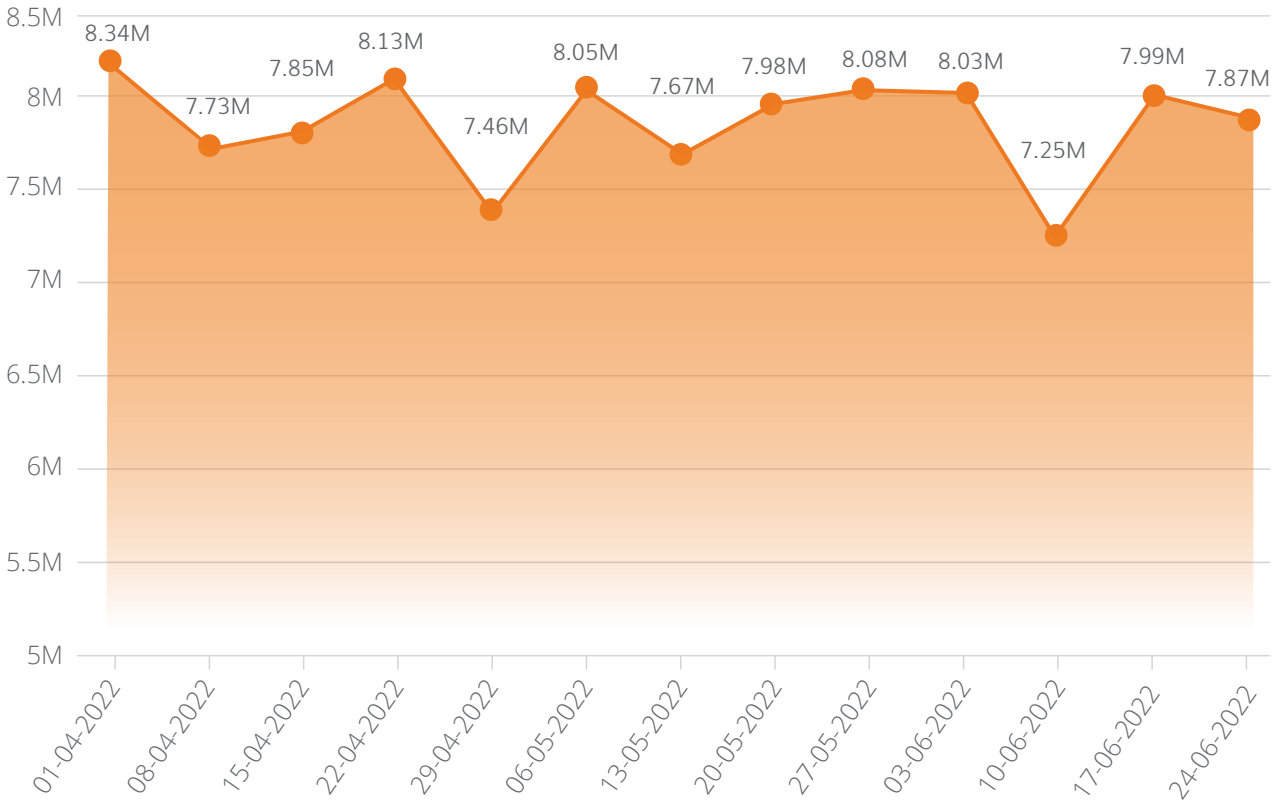
Infector:
25.02 Million
Per Day: 274,903
Per Hour: 11,454
Per Minute: 191

Worm:
9.81 Million
Per Day: 107,799
Per Hour: 4,492
Per Minute: 75

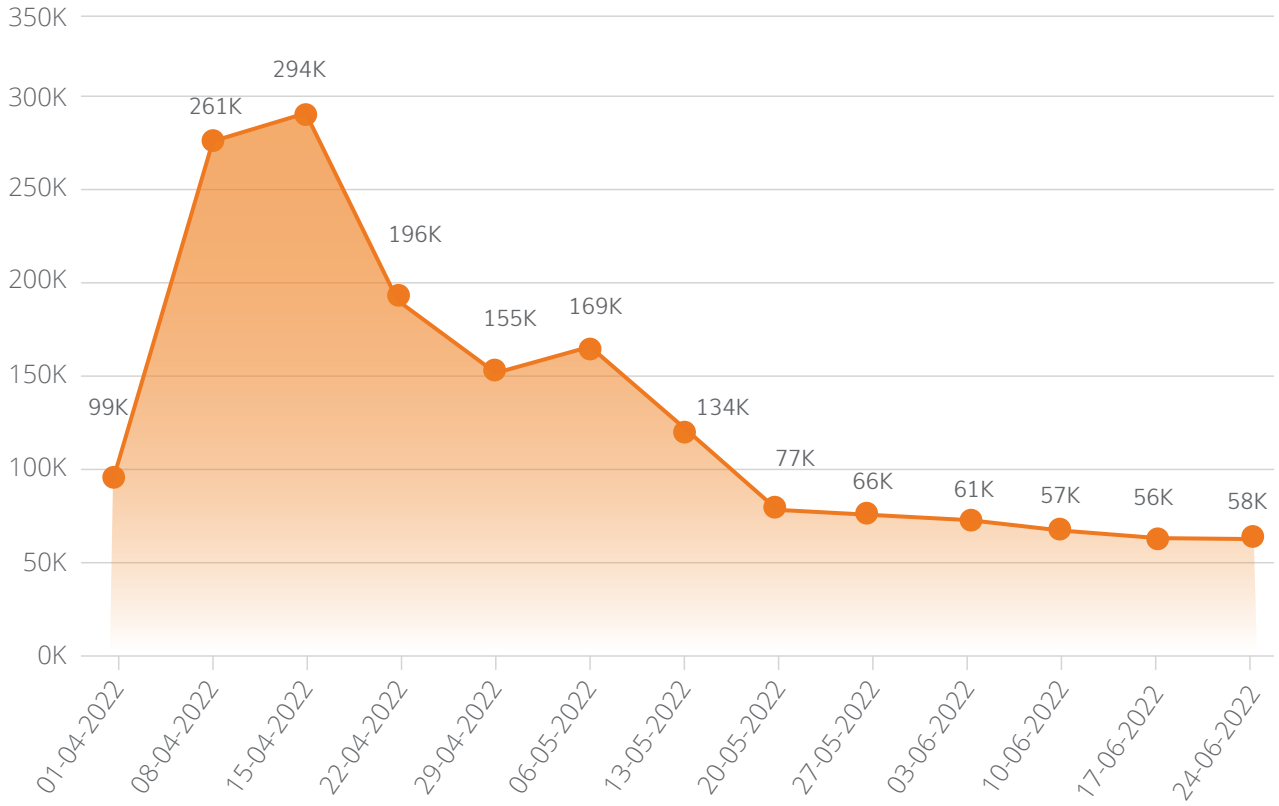
Detection Statistics – Month Wise Q2 2022



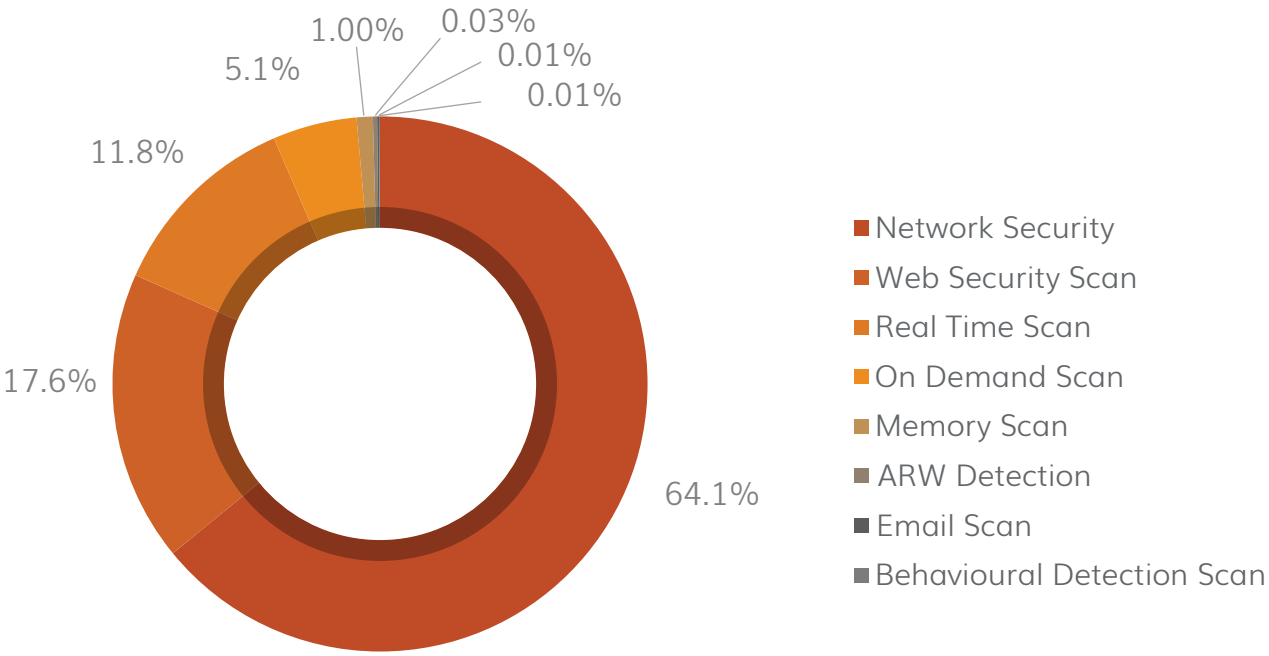
Detection Statistics – Week-Over-Week



Ransomware – Week-Over-Week



Detection Statistics – Protection Wise



Brief description about
various threat protection mechanisms

Network Scan
Network scan (IDS/IPS) analyses network traffic to identify known cyber-attacks & stops the packet from being delivered to the system.

Web Security Scan
Automatically detects unsafe and potentially dangerous websites and prevents you from visiting them.

Real-Time Scan
Real-time scanning checks files for viruses or malware each time it is received, opened, downloaded, copied, or modified.

On-Demand Scan
It scans data at rest, or files that are not being actively used.

Memory Scan
Scans memory for malicious programs running & cleans it.

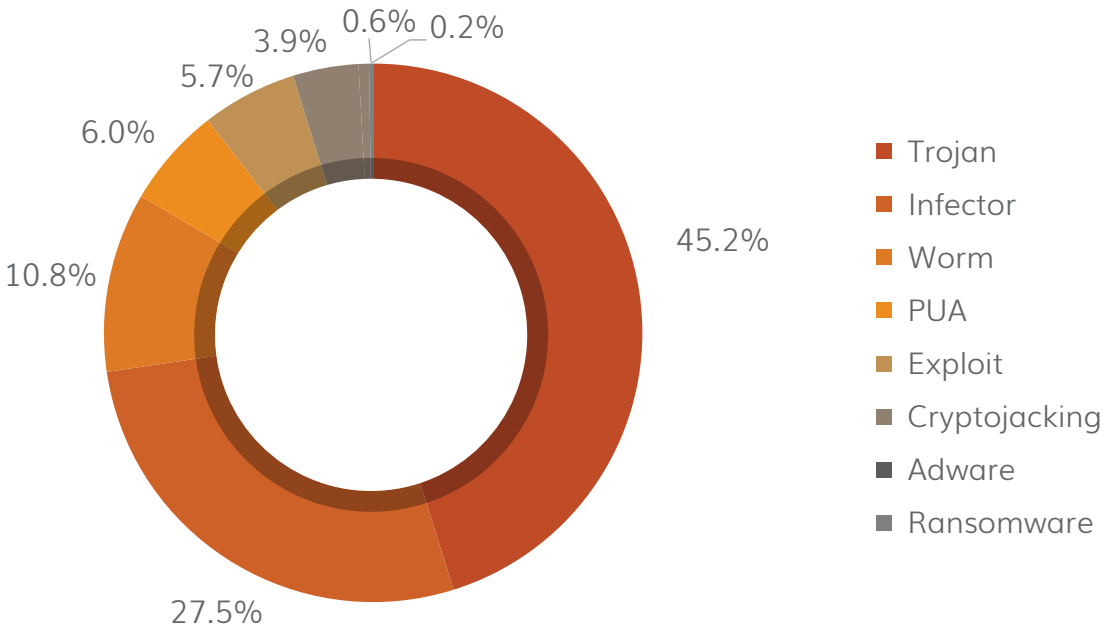
ARW Detection
Behavioural based Ransomware Protection solution to automatically protect against most sophisticated ransomware from encrypting the files

Email Scan
Blocks emails that carry infected attachments or links to compromised or fake and phishing websites.

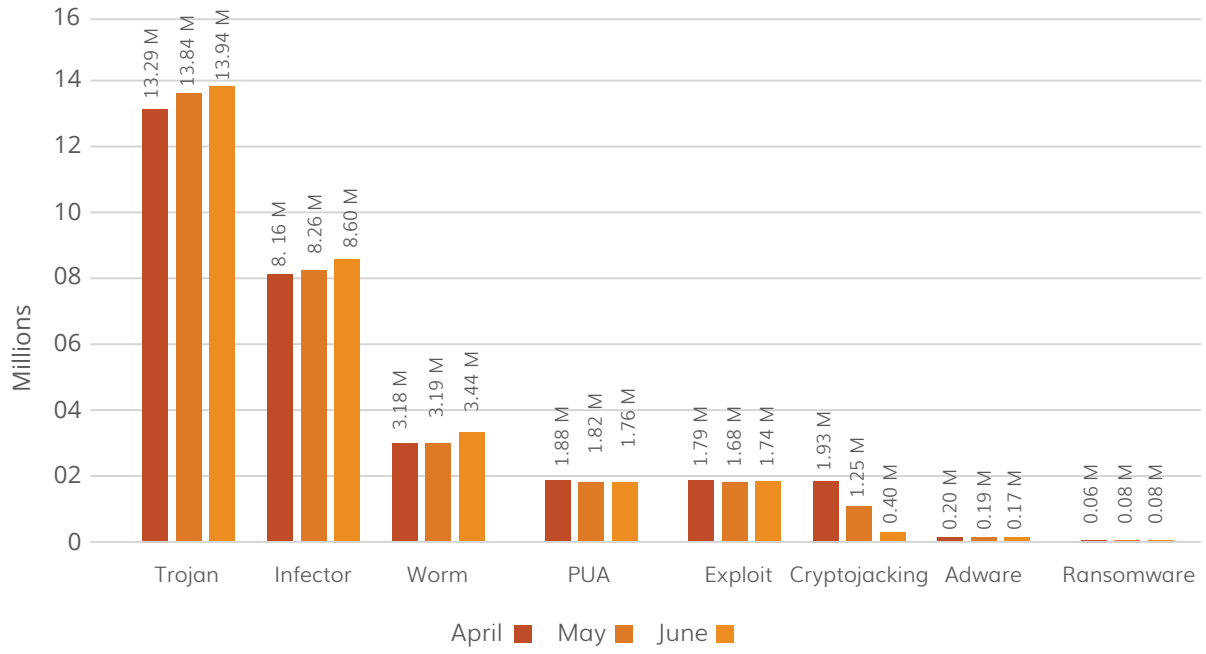
Behavioural Detection Scan
It detects and eliminates new and unknown malicious threats based on their behaviour.

Detection Statistics - Category Wise

A) Malware-wise Categorization



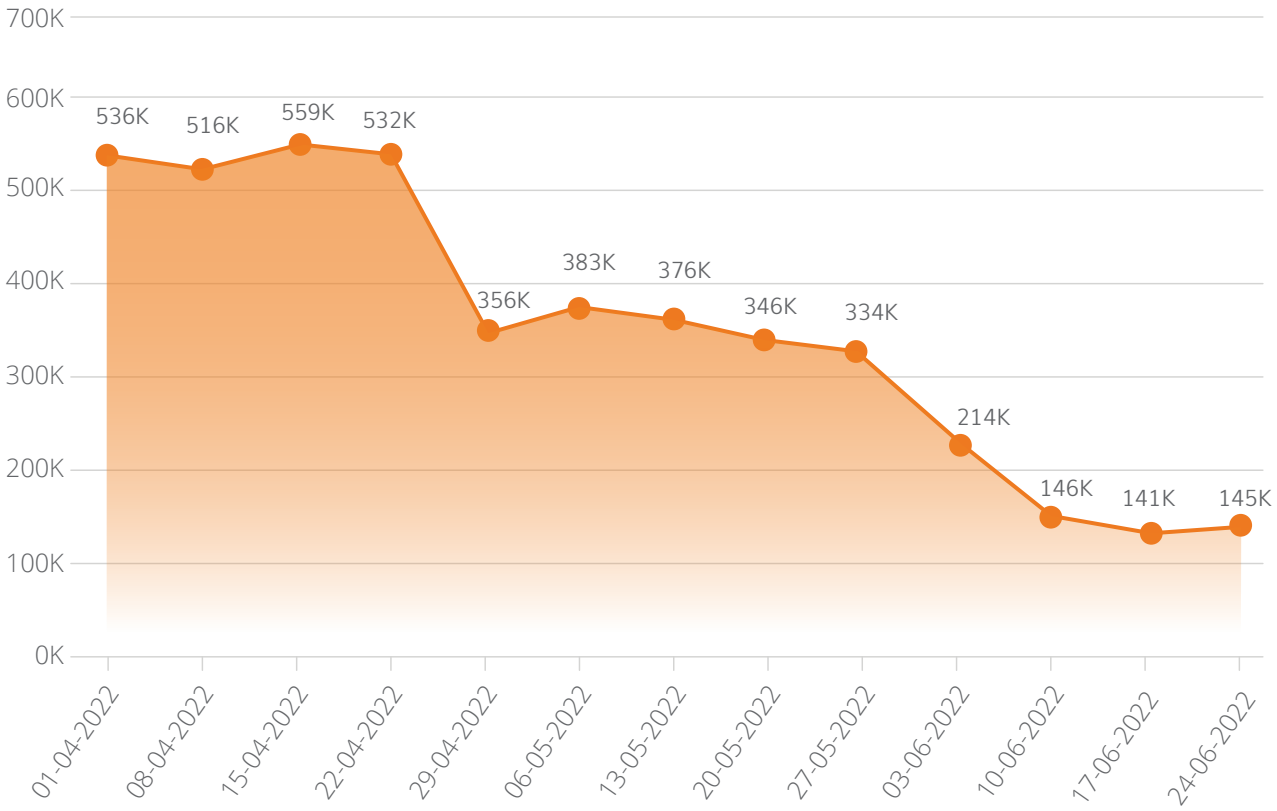
B) Month-wise Categorization



What is Trojan Malware?

A Trojan is a type of malicious program that is designed to inflict harmful actions on your computer by damaging, stealing or taking control. They usually disguises itself as legitimate software.

Coin Miner Detection Statistics

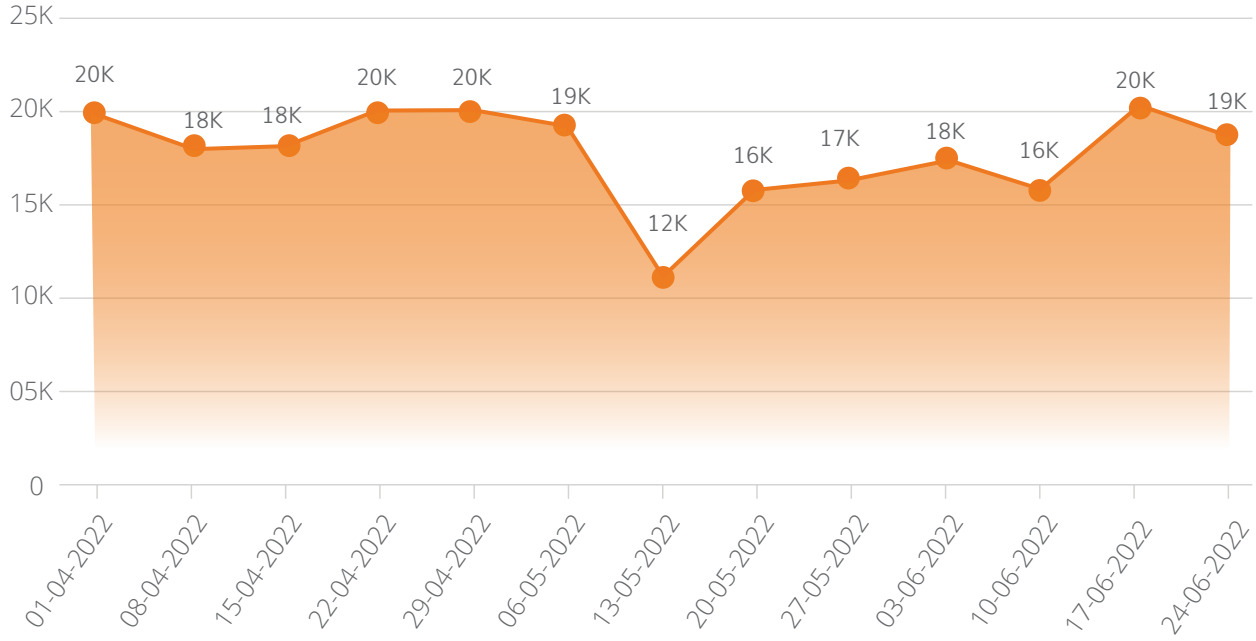


What is Coin Miner Malware?

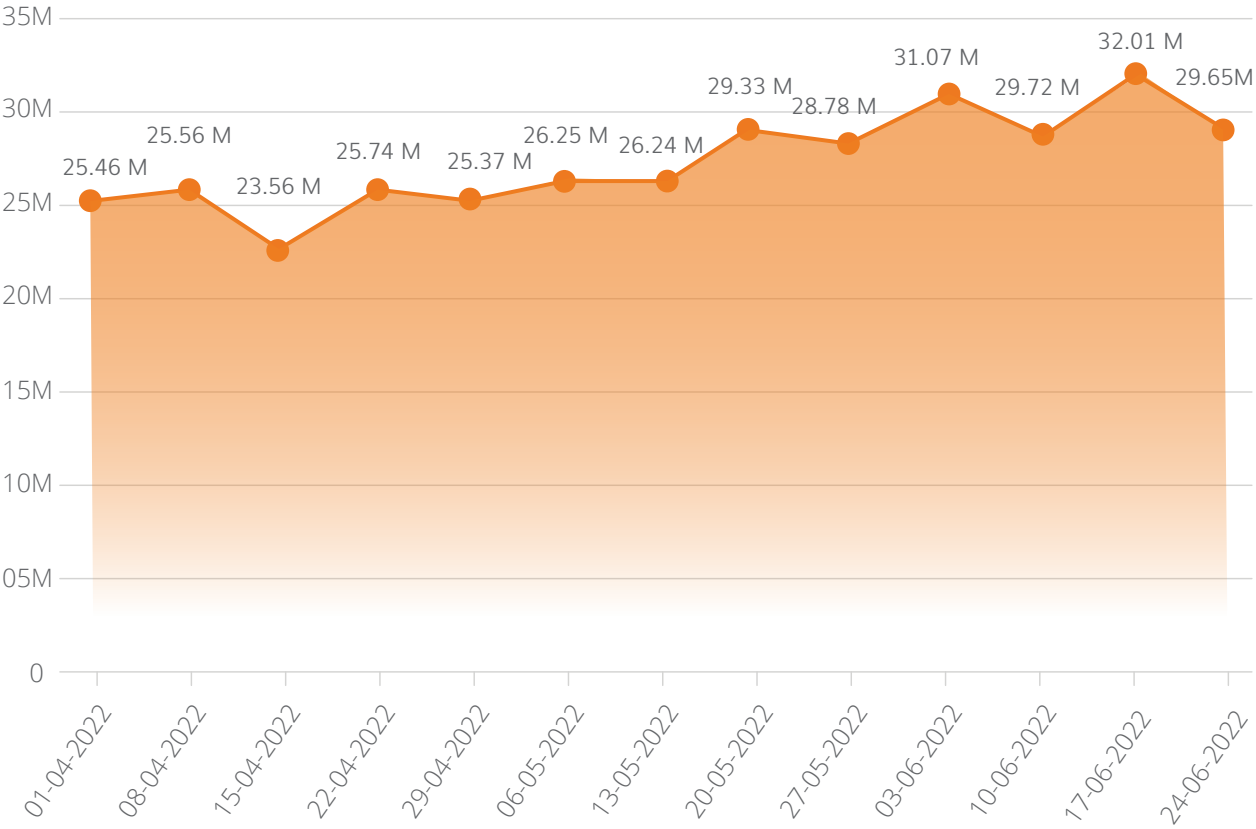
Coin Miners (also called cryptocurrency miners) are programs that generate Bitcoin, Monero, Ethereum, or other cryptocurrencies that are surging in popularity. When intentionally run for one's own benefit, they may prove a valuable source of income.
Cyber criminals have created threats and viruses which use commonly available mining software to take advantage of someone else's computing resources (CPU, GPU, RAM, network bandwidth, and power), without their knowledge or consent (i.e. crypto jacking).

Phishing Attack Statistics

A) Phishing Email Attacks

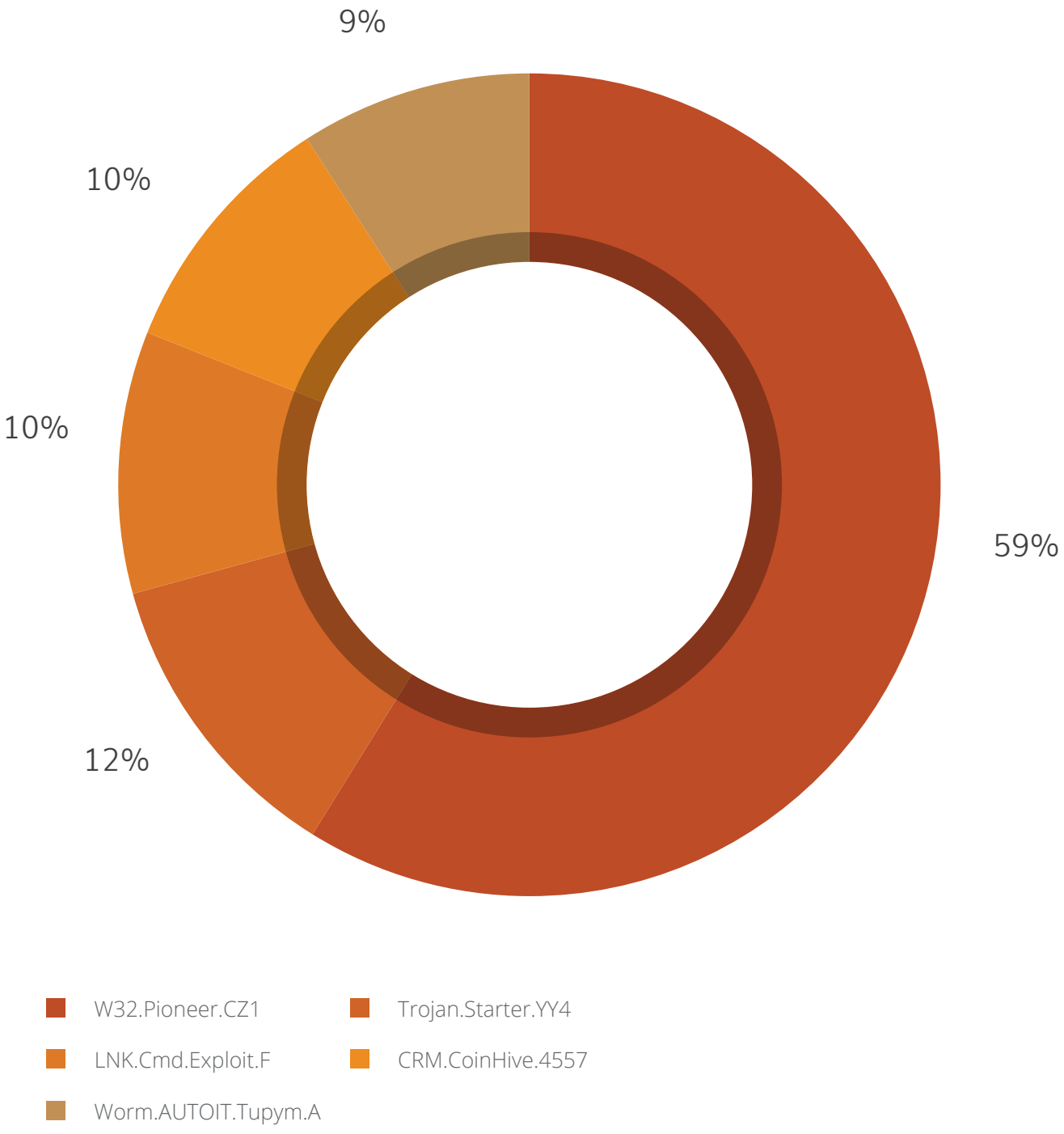


B) Phishing URL Attacks



Top 5 Windows Malware

The below figure represents the Top 5 Windows malware of Q2 2022.
These malwares have made it to this list based upon their rate of detection from January to March of current calendar year.



Top 5 Windows Malware Details

01

W32.Pioneer.CZ1
Threat Level: Medium
Category: File Infector
Method of Propagation: Removable or network drives

Behaviour:

- The malware injects its code to the files present on disk and shared network.
- It decrypts malicious DLL present in the file & drops it.
- This DLL performs malicious activities and collects system information & sends it to a CNC server.

02

Trojan.Starter.YY4
Threat Level: High
Category: Trojan
Method of Propagation: Email attachments and malicious websites

Behaviour:

- Creates a process to run the dropped executable file.
- Modifies computer registry settings that may cause a system crash.
- Downloads other malware like keylogger.
- Slows down the booting and shutting down process of the infected computer.
- Allows hackers to steal confidential data like credit card details and personal information from the infected system.

03

LNK.Cmd.Exploit
Threat Level: High
Category: Trojan
Method of Propagation: Email attachments and malicious websites

Behaviour:

- Uses cmd.exe with "/c" command line option to execute other malicious files.
- Executes simultaneously malicious .vbs file with name "help.vbs" along with a malicious exe file. The malicious vbs file uses Stratum mining protocol for Monero mining.

04

CRM.CoinHive.4557
Threat Level: High
Category: Coin Miner
Method of Propagation: Malicious websites and software bundle

Behaviour:

- They are suspicious chrome extensions that contain mining URLs that perform crypto mining whenever the browser gets loaded.

05

Worm.AUTOIT.Tupym.A

Threat Level: Medium

Category: Worm

Method of Propagation: Malicious links in instant messenger

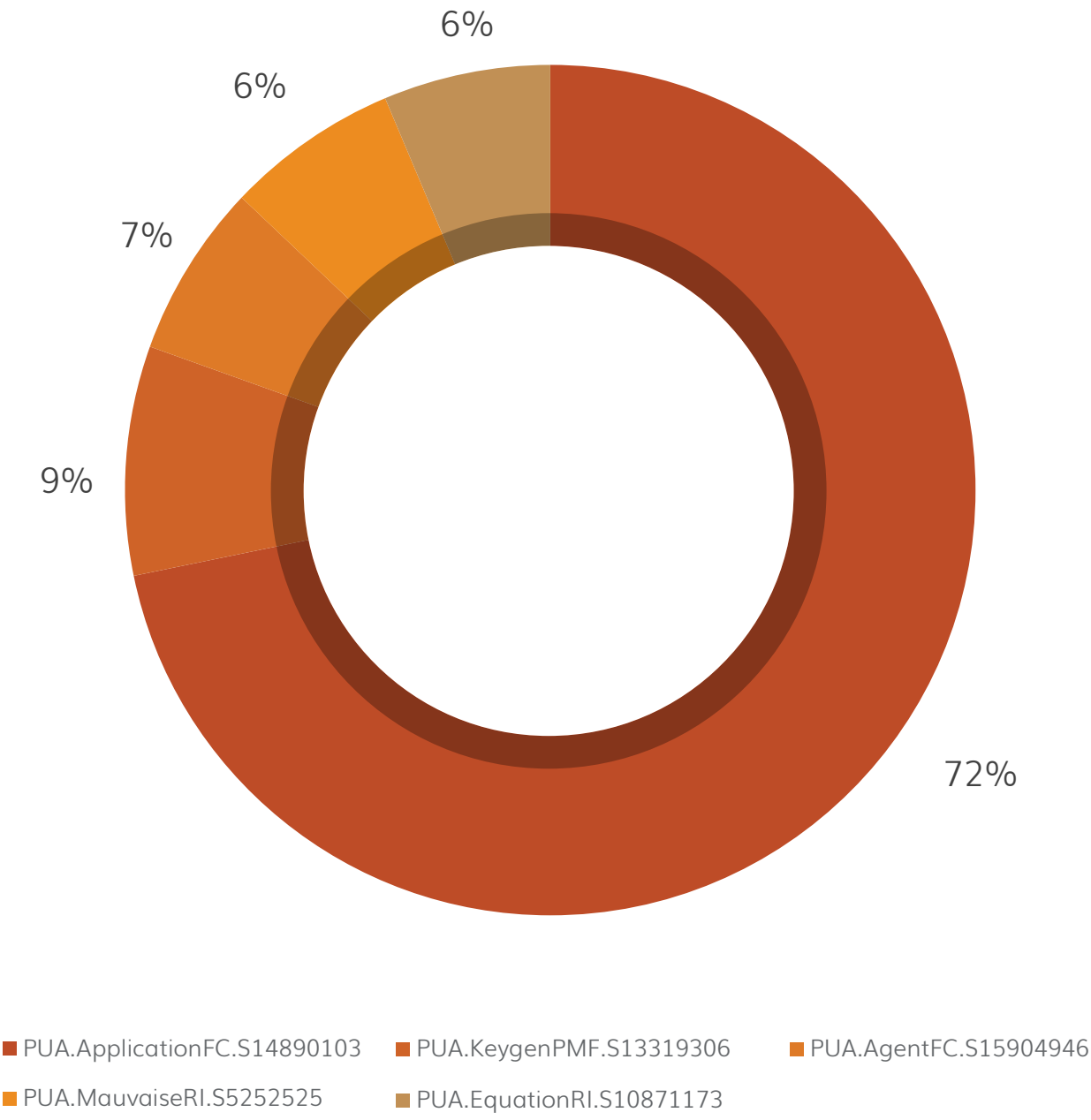
Behaviour:

- Malware drops file in system32 folder and executes it from dropped location.
- It connects to malicious website, also modifies start page of browser to another site through registry entry. Also Creates Run entry for same dropped file for persistence.

Top 5 PUA (Potentially Unwanted Applications and Adware)

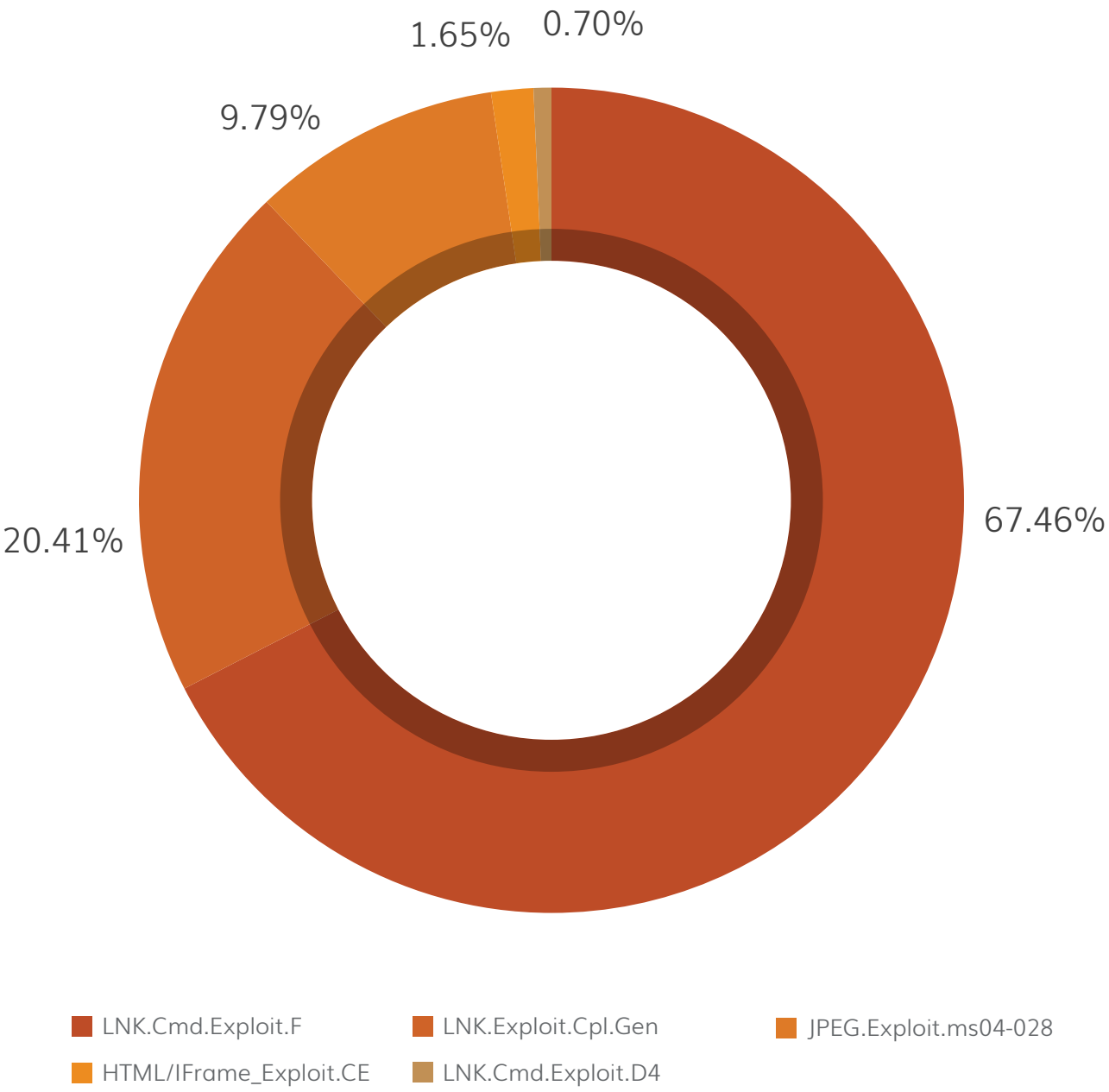
Potentially Unwanted Applications (PUA) and Adware programs are not necessarily harmful but using them might lead to security risks. Adware are software used to display ads to users; some are legitimate while some are used to drop spyware that steals user information.

Below figure represents the top 5 PUAs and Adware detected by Quick Heal in Q2 2022.



Top 5 Host-Based Exploits

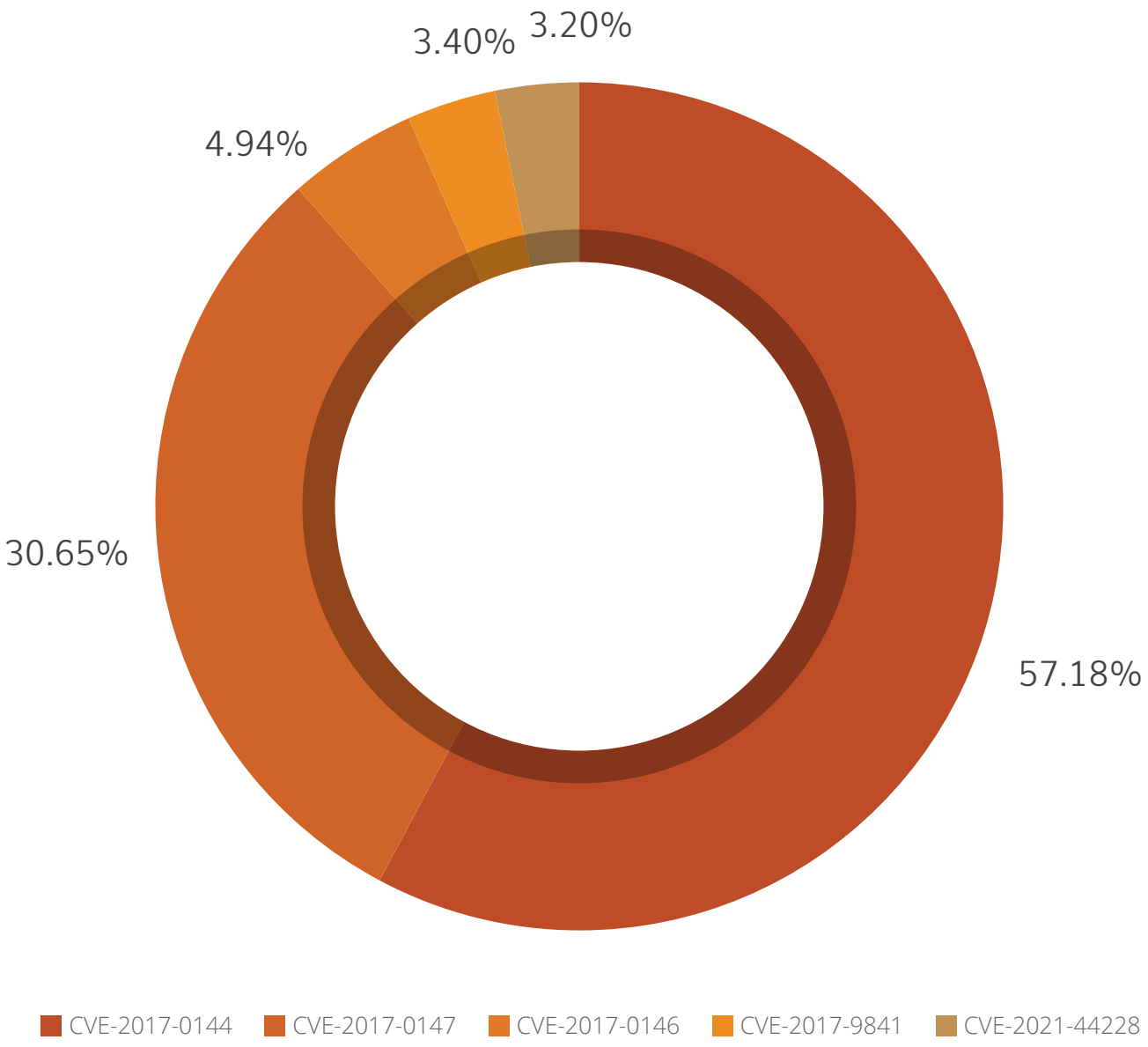
An exploit is a piece of code or crafted data that takes advantage of a bug or vulnerability in the targeted system or an application running on it.



What are host-based exploits?
Host-based exploits are those that target security vulnerabilities found in host-based applications (host is a computer or other device connected to a computer network). These exploits are detected by endpoint detection modules such as Virus Protection, Email Protection, and Scanner.

Top 5 Network-Based Exploits

Below figure represents the top 10 Network-Based Windows exploits of Q2 2022



What are network-based exploits?
Network-based exploits are those that target security vulnerabilities found in network-based applications. Such exploits are detected by IDS/IPS (Intrusion Detection and Prevention System).

CVE descriptions

1. CVE-2017-0144

Microsoft Windows SMB Remote Code Execution Vulnerability
This vulnerability enables the attacker who successfully exploited the vulnerability could gain the ability to execute code on the target server

2. CVE-2017-0147

Microsoft Windows SMB Information Disclosure Vulnerability
An attacker who successfully exploited this vulnerability could craft a particular packet, leading to information disclosure from the server.

3. CVE-2017-0146

Windows SMB (SMBv1) Remote Code Execution Vulnerability
A remote code execution vulnerability exists in how the Microsoft Server Message Block 1.0 (SMBv1) server handles specific requests. An attacker who successfully exploited the vulnerability could gain the ability to execute code on the target server.

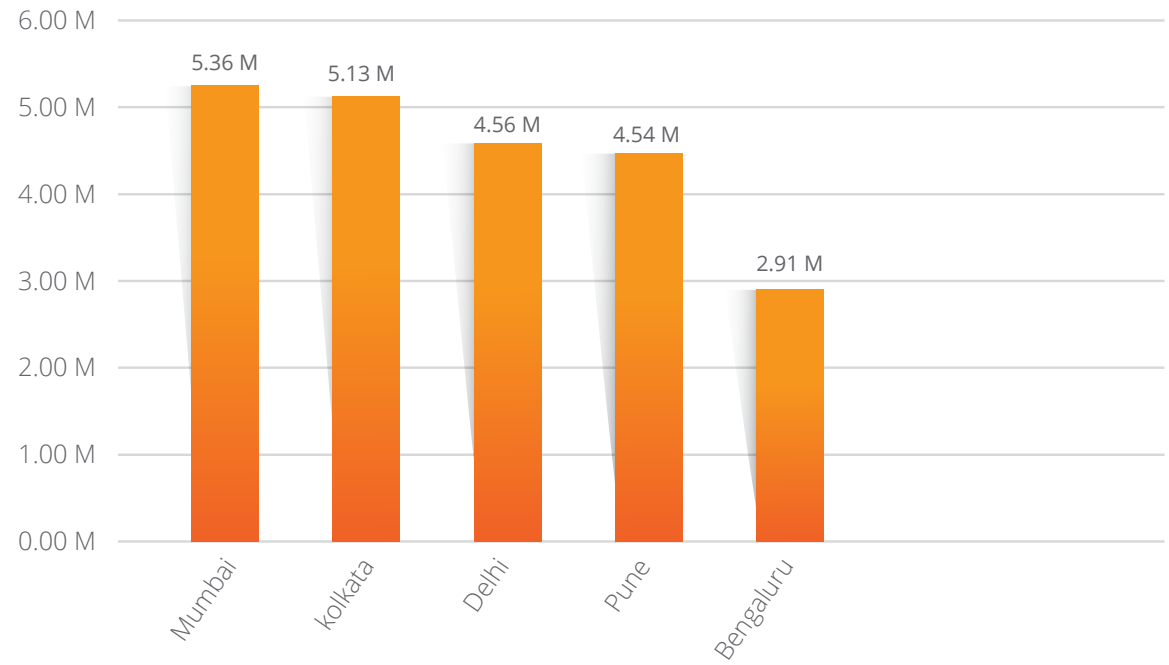
4. CVE-2017-9841

Code injection vulnerability in PHP Unit
This vulnerability allows remote attackers to execute arbitrary PHP code via HTTP POST data beginning with a "<?PHP " substring

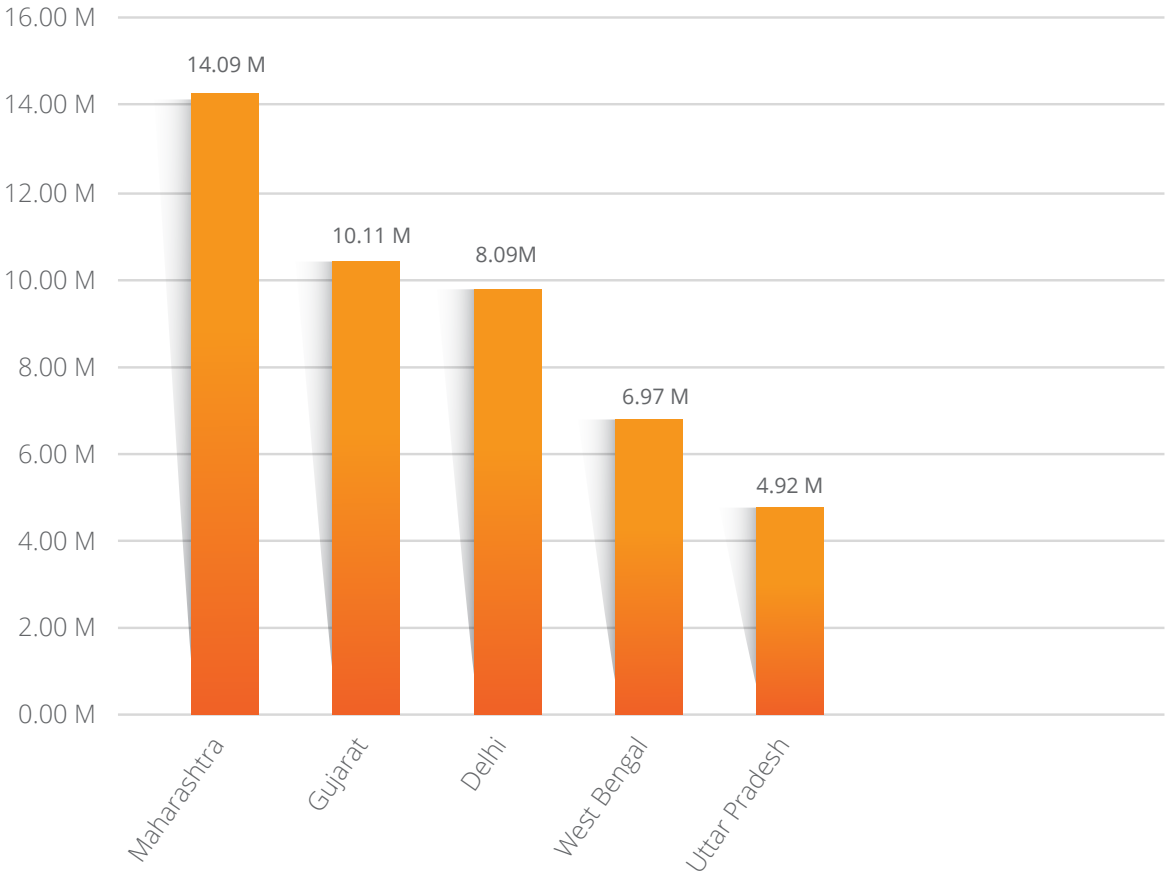
5. CVE-2021-44228

Apache log4j-core vulnerability
An attacker who can control log messages or parameters can execute arbitrary code loaded from LDAP servers and other JNDI-related endpoints when message lookup substitution is enabled.

Top 5 Affected Cities



Top 5 Affected States



Trends in Windows Security Threats

1. Robin Hood Ransomware 'Goodwill' Forces Victims For Charity

Goodwill Ransomware is known to promote social justice on the internet. It encrypts documents, databases, videos, or photos after it infects the whole system. The files become inaccessible for the victims, and Robinhood 'Goodwill' asks the victim to donate for socially driven activities to retrieve their files and data. For example: 'Goodwill Ransomware forces victims to donate new clothes to the homeless, provide financial assistance to the poor, and many more. Subsequently, it then asks victims to post the "proof" of their donations online as a mandatory step before decrypting the infected files. This ransomware seems related to an open-source red team tool named Jasmin on GitHub. The strings present in the file, such as "Error h bhaiyya," seems that the roots of this ransomware originated in India.

2. Emotet updates itself and re-emerges with new techniques

After a long break from its operations, we have seen Emotet malware active again in the previous quarter. Emotet uses an office document file (.doc/.xls) as the initial infection vector, and then malicious macros execute base64 encoded PowerShell commands to download DLL from various URLs. This year we observed some new methods implemented in official documents, such as the use of hex encoded IP and the use of Excel 4 macros. The payload executable has switched from 32-bit to 64-bit. The CFF (Control Flow Flattening) technique has been used along with API hashing to make reverse engineering difficult. It changed its encryption mechanism from RSA to ECC. It has also used Crypt APIs from bcrypt.dll while previously it was using ADVAPI.DLL.

3.Expiro is Back

The Expiro virus has been around for more than a decade. It infects exe files in all drives and collects user credentials from an infected computer allowing backdoor access to control the infected computer. Expiro is unique because it infiltrates executable files on 32-bit and 64-bit Windows operating systems by appending its viral code to the executable. Recently we have seen a new variant of Expiro with a significant change in its infection routine. The previous version patched some code at the entry point only, and that code jumps to the last section. In the newer versions, it fixes calls in the text section, which jumps to the previous section. Also, the code for calculating the address of the call which is patched is obfuscated, making it difficult to track.

4.Phishing campaign impersonating SBI evades by mixing reverse tunnels and URL shortening services

An uptick in the use of reverse tunnel services along with URL shorteners for large-scale phishing campaigns has been observed, making it more challenging to prevent. One phishing campaign abusing these services was impersonating the YONO digital banking platform by the State Bank of India. URL defined by the attacker hidden behind "cutt[.]ly/UdbpGhs" led to "ultimate-boy-bacterial-generates[.]trycloudflare[.]com/sbi" that used Cloudflare's Argo tunneling service. This phishing page requested bank account credentials, PAN card numbers, Aadhar numbers, and mobile phone numbers. Distribution of simplified URLs is done via email, text messages, WhatsApp, Telegram,

fake social media pages, etc. Reverse tunnels can host phishing pages locally and route connections through external services. This shields phishing sites by handling all connections to the local server so that any incoming connection is resolved by the tunnel service and forwarded to the local machine. URL shortening services can generate new links as often as they want to bypass detection.

- The most widely abused reverse tunnel services are Ngrok, LocalhostRun, and Cloudflare's Argo.
- Bit[.]ly, is[.]gd, and cutt[.]ly URL shortening services are also getting more prevalent.
- Even if a URL is reported or blocked, threat actors can easily host an alternate one using the same template.

Sensitive information collected can be sold on the dark web, used to empty bank accounts, launch ransomware attacks, or business email compromise (BEC) frauds.

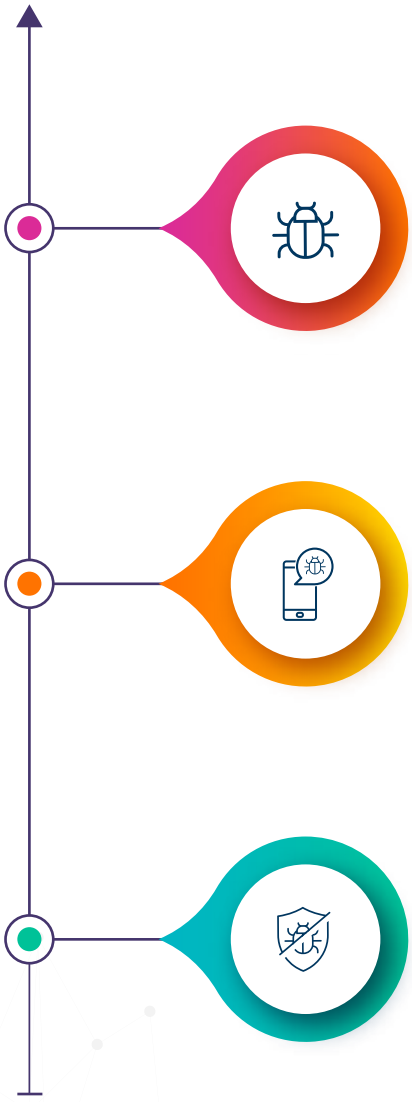
ANDROID

70.62%

of total Android detections
in Q2 2022 were Malware.

ANDROID MALWARE DETECTIONS

FOR Q2 2022



22,536

Malware

Per Day: 248
Per Hour: 10
Per Minute: 0

4,234

Adware

Per Day: 47
Per Hour: 2
Per Minute: 0

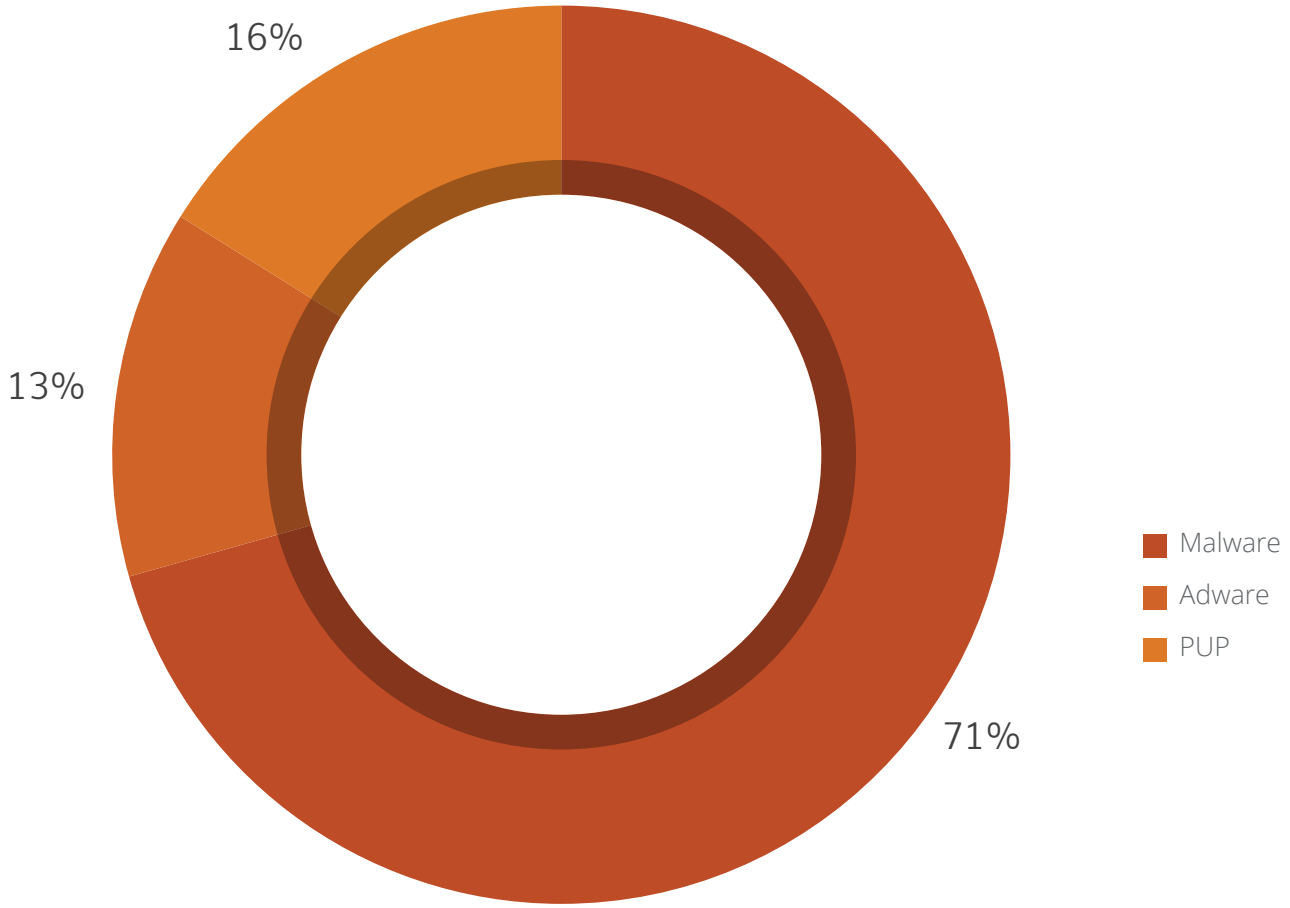
5,138

Potentially Unwanted Application (PUA)

Per Day: 56
Per Hour: 2
Per Minute: 0

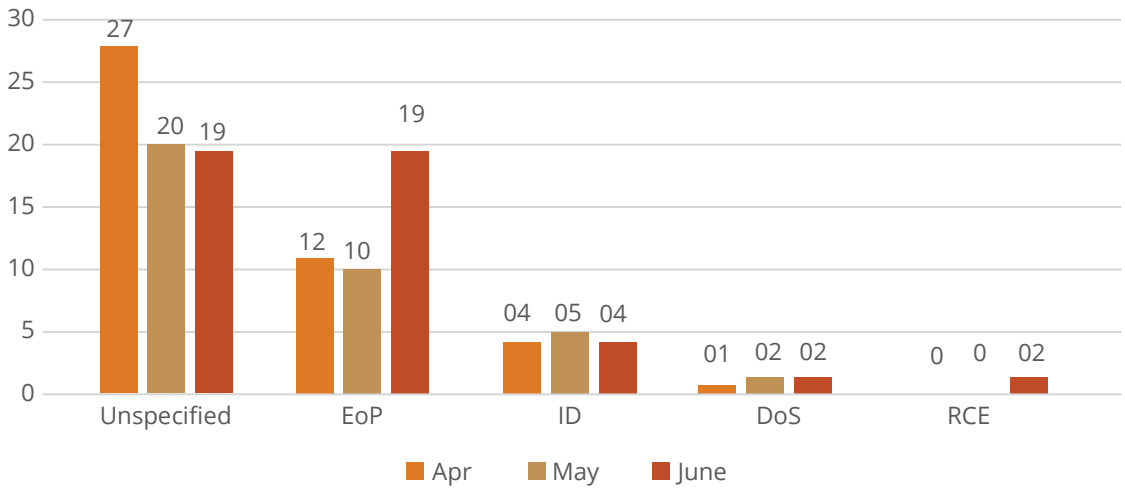
Detection Statistics: Category Wise

Below figure represents the various categories of Android malware detected by Quick Heal in Q2 2022.

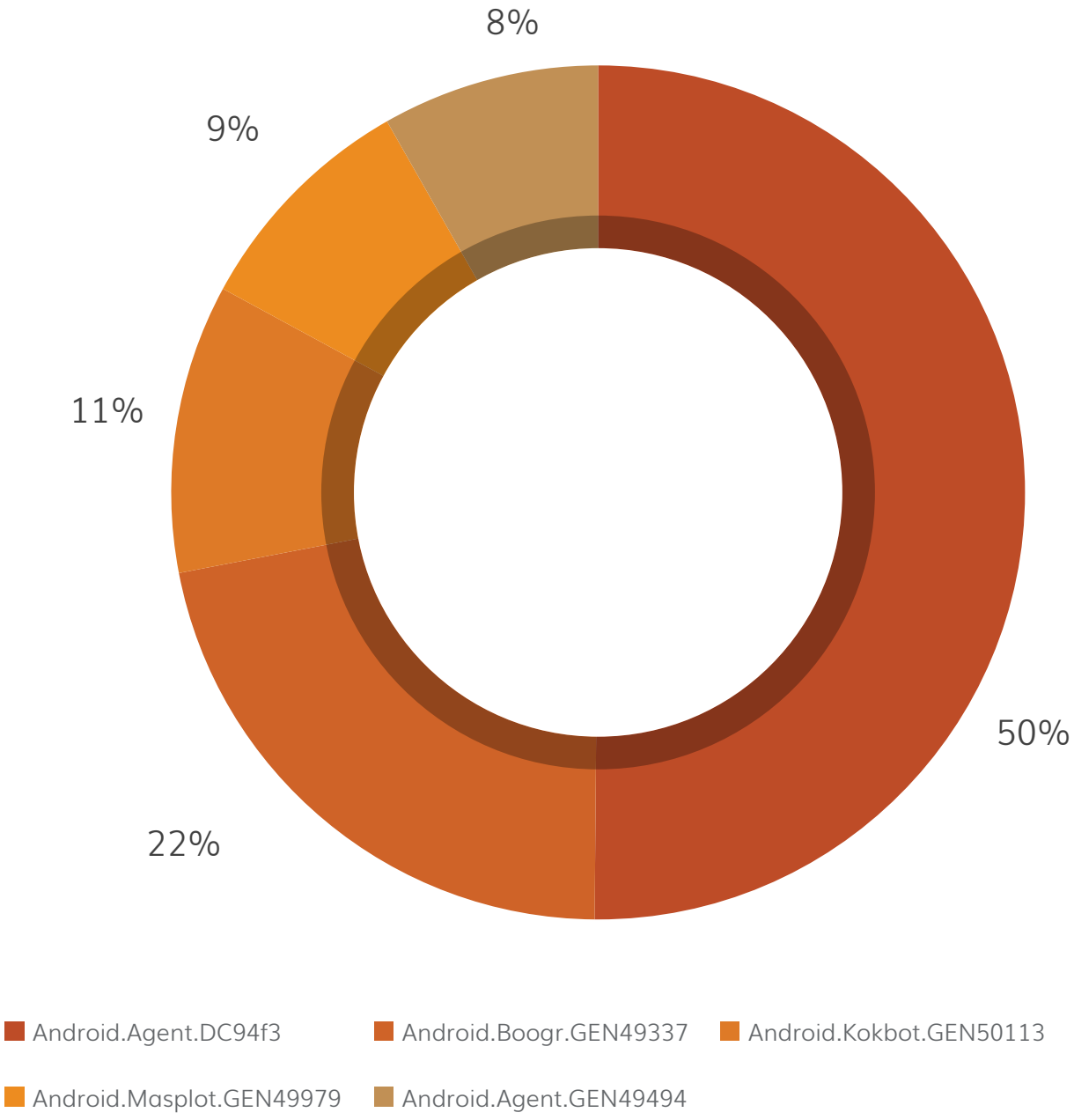


Security Vulnerabilities Discovered

A security vulnerability (also known as a security hole) is a security flaw detected in a product that may leave it open to hackers and malware. Below figure shows the type of Android security vulnerabilities and their growth from April to June 2022.



Top 5 Android Malware for Q2 2022



Top 5 Android Malware Details

01

Android.Agent.DC94f3
Threat Level: High
Category: Malware
Method of Propagation: Third-party app stores

Behaviour:

It is a Trojan-Dropper malware, it drops malicious Android file in background.
- It looks like a legitimate application such as settings or messaging.
- On its first launch, it hides its presence and loads encrypted payload from Resources.
- Encrypted payload has advertised SDK which shows full screen advertisements.

02

Android.Boogr.GEN49337
Threat Level: High
Category: Malware
Method of Propagation: Third-party app stores

Behaviour:

- Uses similar icon of legitimate apps.
- It is performing malicious activity like stealing SMS data, call logs, contacts and send it to C&C server.
- Downloading other malicious files on device and installing it on device.

03

Android.Kokbot.GEN50113
Threat Level: High
Category: Malware
Method of Propagation: Third-party app stores

Behaviour:

- This malware is performing spying activity.
- It accesses sensitive information like phone number, contacts, SMSs data, call logs, installed applications, clipboard data etc.
- Further it send this data to C&C server.

04

Android.Masplot.GEN49979
Threat Level: High
Category: Malware
Method of Propagation: Third-party app stores

Behaviour:

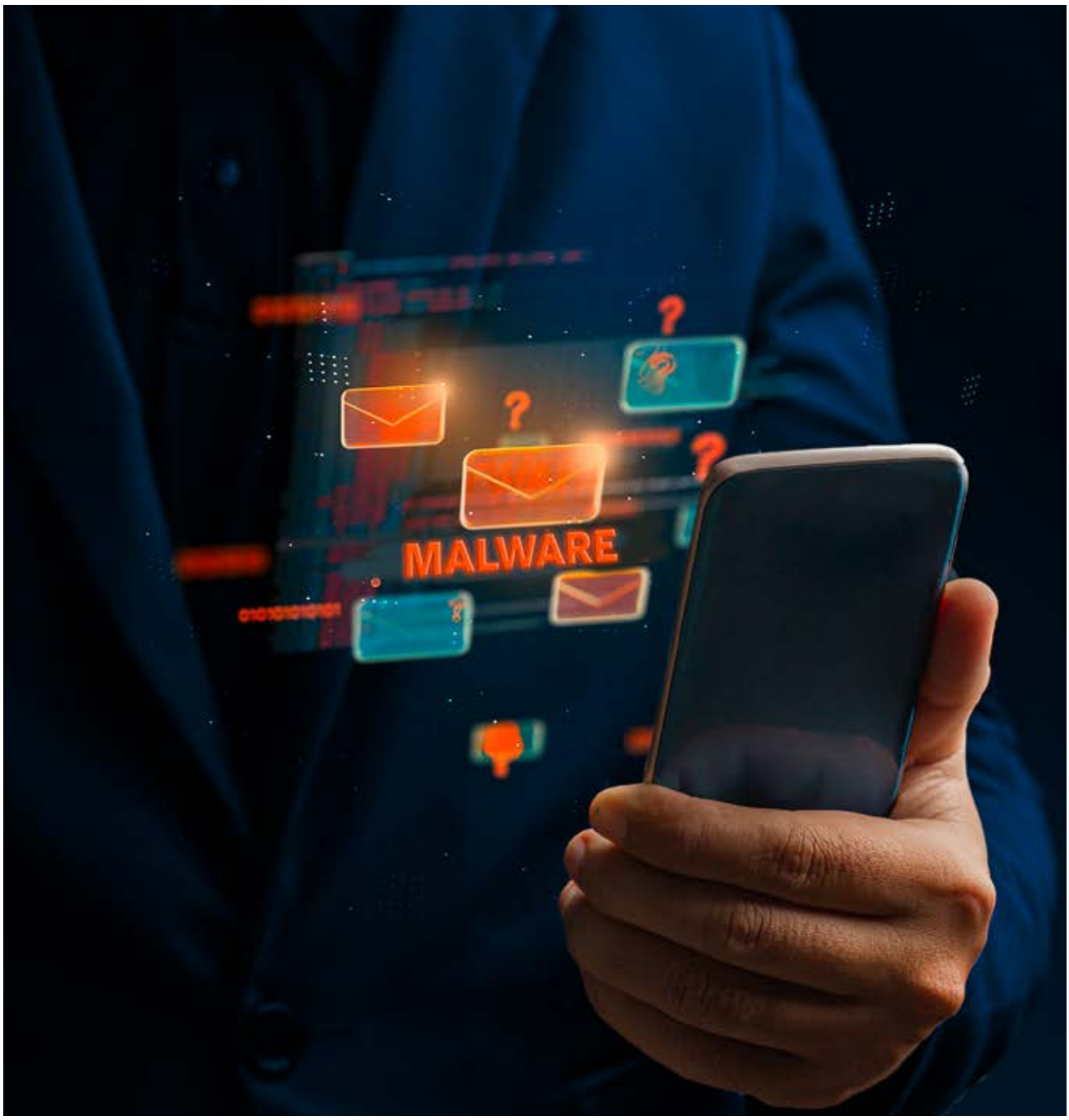
This malwares uses Metasploit framework which is designed for penetration testing but malware authors use it in malicious way.
- By using this attackers takes complete access of the victim's device and perform malicious activity.

05

Android.Agent.GEN49494
Threat Level: High
Category: Malware
Method of Propagation: Third-party app stores

Behaviour:

- Uses icons of famous apps for spreading
- Places a shortcut of a game icon on the screen.
- In the background, it visits multiple URLs without user knowledge



Trends in Android Security Threats

Android banking malwares hit the ground running-

In this quarter we have found below trojan bankers -

** Escobar:*

We found a new Aberebot malware variant named "Escobar." This malware came with some new features and a new avatar. It uses VNC Viewer to control the screen remotely. The malware tries to steal Google authenticator codes, having the capacity to kill itself. We have also seen some applications pretending to be banking reward applications and using legitimate Indian application icons. The malware can steal credit/debit card information, net-banking passwords, and SMS to read/submit one-time generated passwords on the victim's behalf and sends the information to the C2 server after encryption.

Quick Heal detects these malicious apps with variants of "Android.Agent" & "Android.Banker"*

** Teabot:*

Teabot downloads from a GitHub repository and continuously asks for Accessibility Service. After getting permissions, the malicious app decrypts the malicious payload. The trojan then attempts to intercept SMS messages, aborts the new SMSReceived broadcast to the victim, and acts as a keylogger. This malware also terminates a predefined list of apps, including some anti-malware apps, to lower its detection rate.

Quick Heal detects these malicious apps with variants of "Android.Agent" & "Android.Boogr"

** Trojan banker Targeting Malaysian banks:*

Attackers targeted eight Malaysian banks using fake websites that posed as legitimate services. These applications are fake apps used to steal banking credentials. To look legitimate, a fake application copies the product catalog as well as the design of the original application. Moreover, they use the payment gateway page in which they provided the eight Malaysian banks. As the victim fills out the credentials and submits for payment, the credential will be sent to the CNC server. And the user receives a prompt with the message user ID or password they provided was invalid. Its main goal is to steal banking credentials and forward 2FA SMS messages from the infected device to threat actors.

Quick Heal detects these malicious apps with variants of "Android.Smsthief.A"& "Android.Piom.A".

** Octo Banking Trojan:*

This malware is an advanced version of ExobotCompact or cooper banking trojan. Both ExobotCompact and Octo have remote access capability which allows the trojan to

** Octo Banking Trojan:*

This malware is an advanced version of ExobotCompact or cooper banking trojan. Both ExobotCompact and Octo have remote access capability which allows the trojan to perform on-device fraud. This capability is called VNC(Virtual Network Computing). It uses MediaProjection for screen streaming and AccessibilityService to perform actions remotely. The malware uses a native library to decrypt and load the malicious payload, which makes it hard to analyze and detect. It has keylogging capability. Trojan has commands that malware author can use to enable or disables keylogger, Stops running Trojan, opens specified URL, Sends a text message with specified text from the infected device to the specified phone number, etc.

Quick Heal detects these malicious applications with "Android.Octa.A" detection name.

SharkBotdropper applications on Google Play store

SharkBot is an Android banking malware found at the end of October 2021. It initiates money transfers via Automatic Transfer Systems (ATS) - this technique is an advanced attack technique. It enables adversaries to auto-fill fields in legitimate mobile banking apps and initiate money transfers.

This malware steals credentials and banking information. The malware implements geofencing features and evasion techniques. It also makes use of Domain Generation Algorithm. Recently, we observed some SharkBot delivering applications on Google Play store.These malicious droppers are published in the Google Play Store as a fake Antivirus and cleaner applications.

Quick Heal detects these applications with "Android.Sharkbotdropper.A"

SMSFACTORY steal money:

Researchers have found malicious applications that steal money from victims by sending premium SMS and making calls to premium-rate phone numbers. These numbers appear to be part of a conversion scheme, where the SMS includes an account number, identifying who should receive the money for the messages sent.

It affects the users of Russia, Brazil, Argentina, Turkey, Ukraine, US, France and Spain. The malware is spreading through malvertising, push notifications, and alerts displayed on sites offering game hacks, adult content, or free video streaming.

Quick Heal detects these malicious apps with variants of "Android.Agent"& "Android.Fakeapp"

WhatsApp Mother day scam:

Getting text messages from random numbers is disturbing. But spam messages aren't just annoying; they can also be a dangerous vehicle for malware. And these days, pretty much every medium we use to communicate is vulnerable to spam messages, emails, social media messaging apps, and yes, even WhatsApp. Recently, a new WhatsApp scam on "Amazon 2022 Mother's Day Contest" is doing the rounds promising rewards to the users if they click on the given link.

The objective of such a campaign is: –

To promote their Apps & increasing the download counts

Potentially drop malicious Android application (APK) files in future

Generate advertising revenue

Quick Heal's advanced features keep users safe by blocking these malicious websites.

Inference

While the threat tactics continuously change as the threat actors evolve and respond to detection the enforcement techniques, users must ensure to take steps to limit their exposure to the upcoming risks. From the Threat report, we can easily witness the surge in Windows Malware detection in Q2 2022 of about 103 Million, of which 34 Million were alone detected in June 22, and 1.13 Million Malware were detected on a daily average.

Quick Heal Security Labs have spent hours in identifying and detecting various Malwares or cyberattacks, which have been put to use in compiling this Threat Report. This report not only offers a snapshot of the critical analysis of all the prevalent cyber-attack numbers crunched in but also offers an insight into the latest threat stories. We aim to raise awareness of the prevalence of cyber threats, thus helping make the digital world safer

Quick Heal

Security Simplified

Quick Heal Technologies Limited
Marvel Edge, Office No.7010 C & D, 7th Floor, Viman Nagar,
Pune 411014, Maharashtra, India.

+91 20 66813232
www.quickheal.com
info@quickheal.com