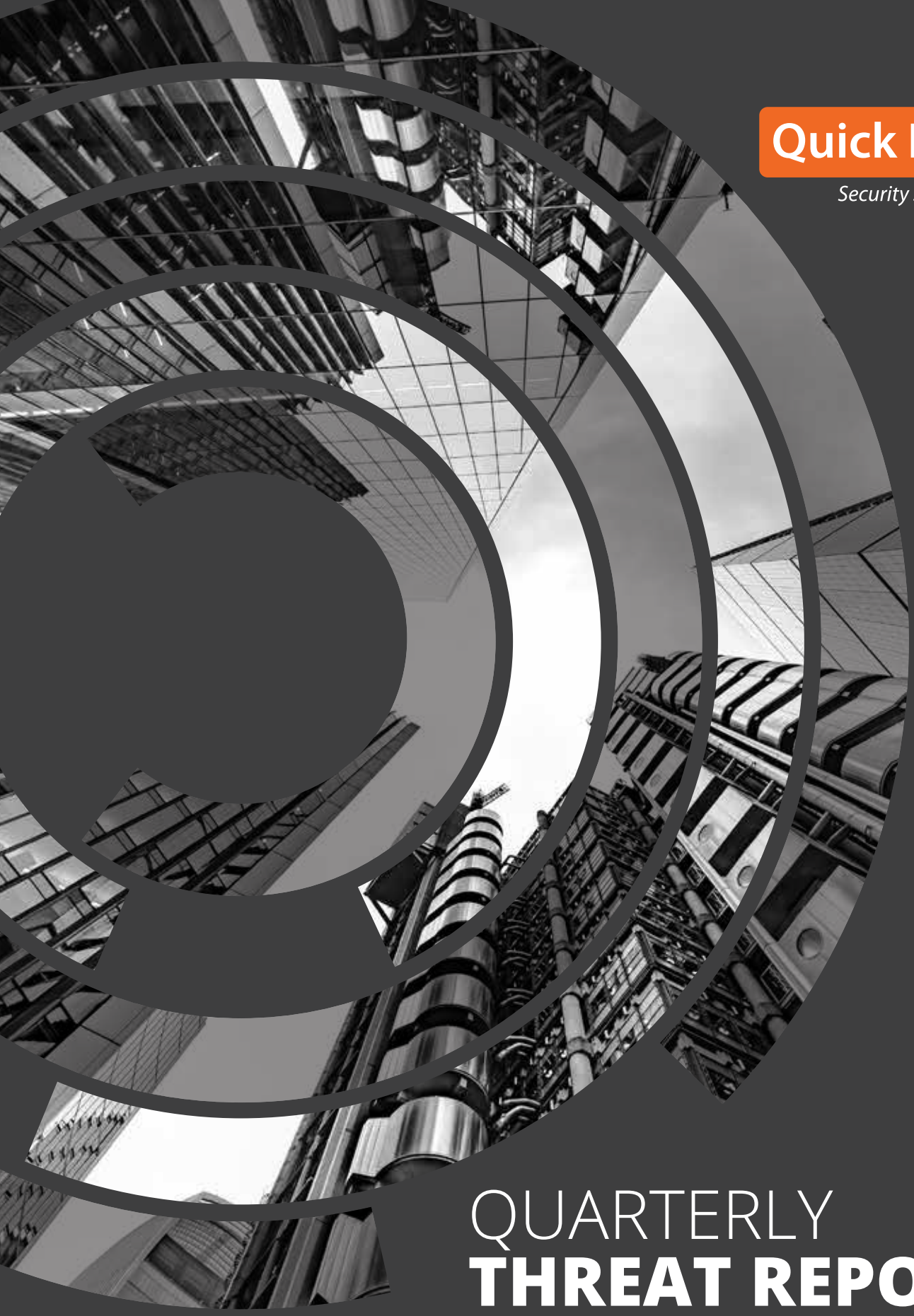


Quick Heal

Security Simplified

QUARTERLY **THREAT REPORT** Q1 - 2021

www.quickheal.com

Contributors

Quick Heal Security Labs
Quick Heal Marketing Team

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.

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
Follow us on:

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

Foreword

The year 2020 saw one of the most significant numbers of data breaches, and the numbers seem to be only rising with the second wave of COVID-19. While businesses worldwide are struggling to implement secure work-from-home policies, the healthcare, and pharma sector coming up with new vaccines to fight COVID-19, and with the biggest vaccine registration drive held by the government – cybercriminals are developing and boosting their attacks at an alarming pace.

There is a 5% rise in the malware numbers as against Q4-2020! Indian pharma firms and healthcare companies face a new wave of ransomware attacks which is likely to rise in 2021. With Bitcoin hitting a new price high in January 2021, there was an uptick in ransomware and cryptojacking attacks.

The Quick Heal Q1 – 2021 Threat Report covers the topic areas into which Quick Heal Security Labs has gained insight from work over the past three months on various cybersecurity events, malware, and spam analysis. It compiles data collected on the malicious campaigns occurring from January to March, Q1, of 2021. By publishing this information, we hope to minimize the damage of future cyber-attacks and strengthen the security posture.

WINDOWS

166 **Million** Windows Malware detected in Q1	**57** **Million** Windows Malware detected in Jan '21	**1.8** **Million** Malware detected daily in Q1

Windows Detection Statistics Q1 2021

Worm:
16 Million
Per Day: 186,838
Per Hour: 7,785
Per Minute: 130

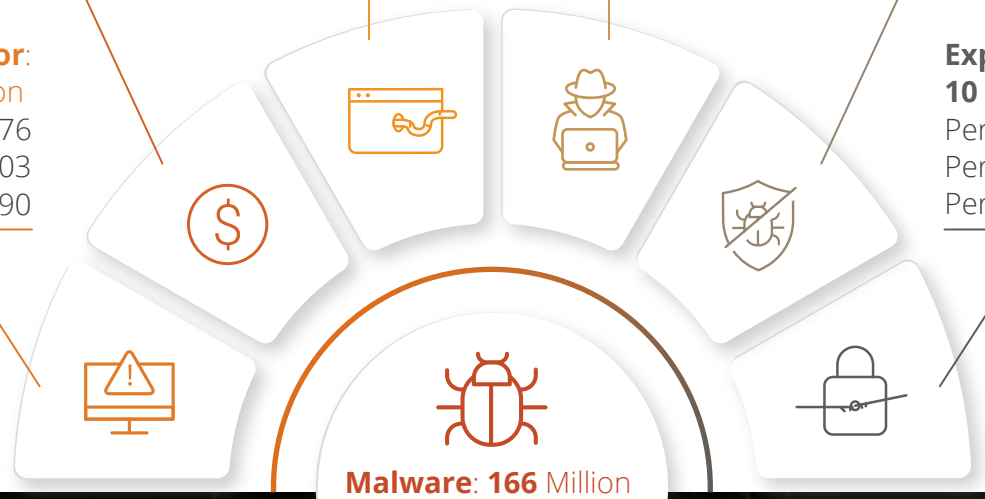
Ransomware:
0.35 Million
Per Day: 3,898
Per Hour: 162
Per Minute: 3

Cryptojacking:
1.5 Million
Per Day: 17,330
Per Hour: 722
Per Minute: 12

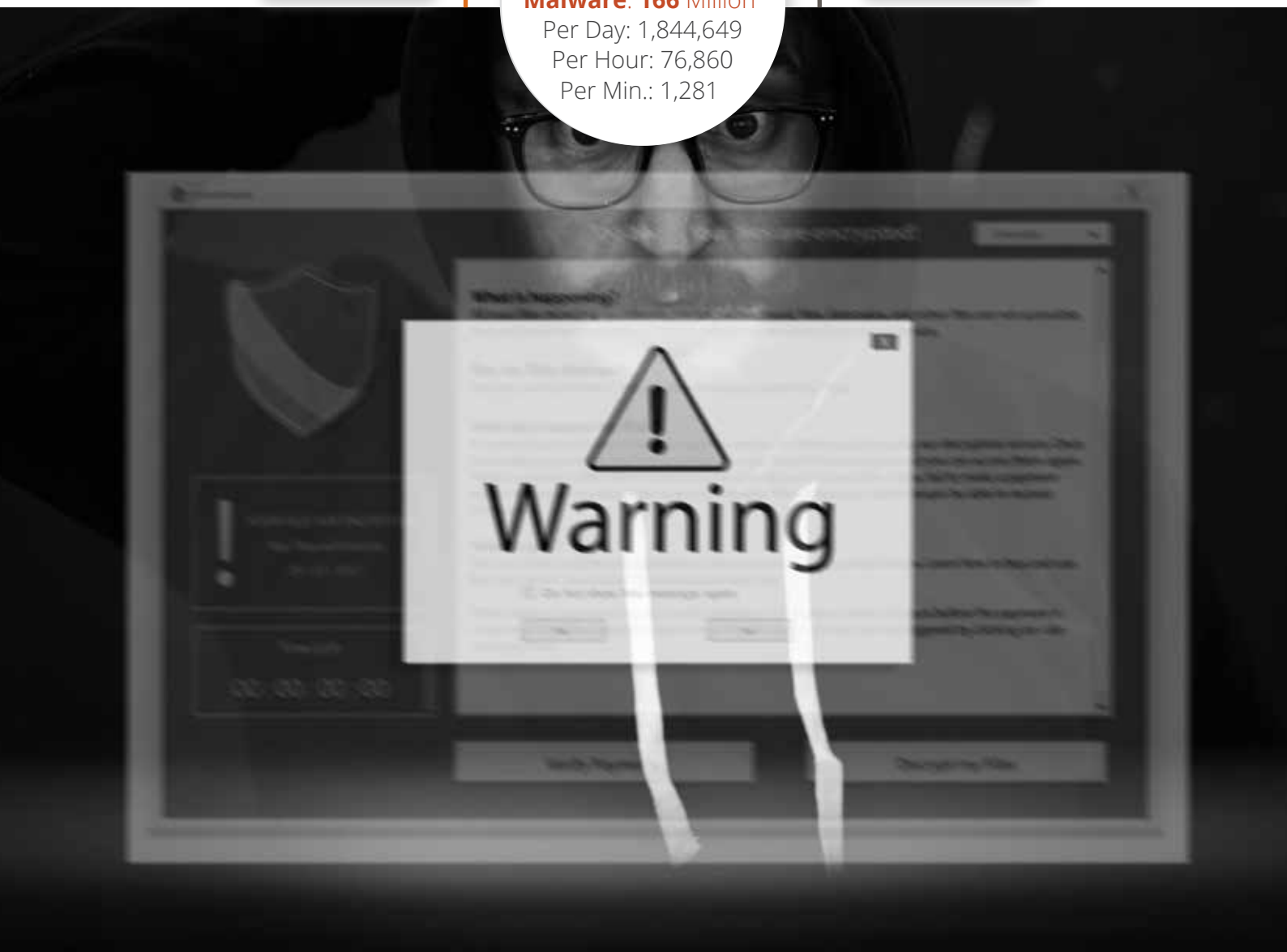
PUA & Adware:
15 Million
Per Day: 171,750
Per Hour: 7,156
Per Minute: 119

Infector:
37 Million
Per Day: 417,676
Per Hour: 17,403
Per Minute: 290

Exploit:
10 Million
Per Day: 120,427
Per Hour: 5018
Per Minute: 84

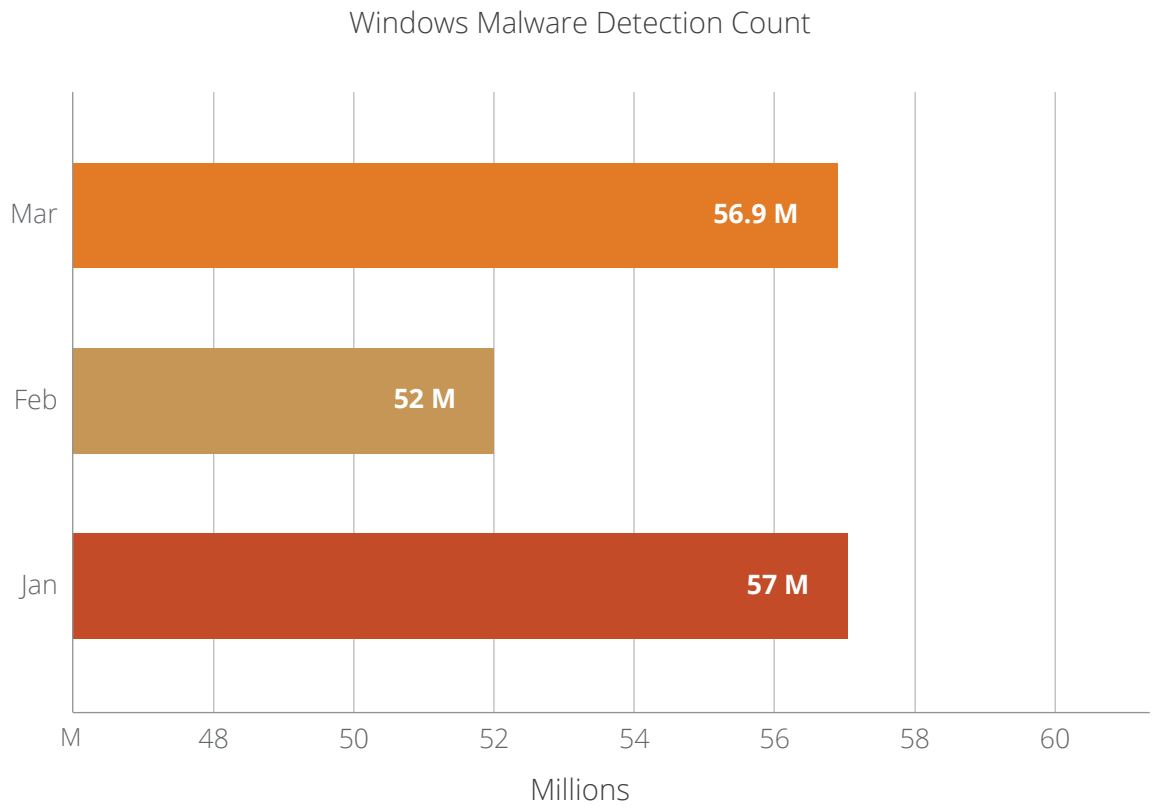


Malware: **166** Million
Per Day: 1,844,649
Per Hour: 76,860
Per Min.: 1,281



Detection Statistics – Month Wise Q1 2021

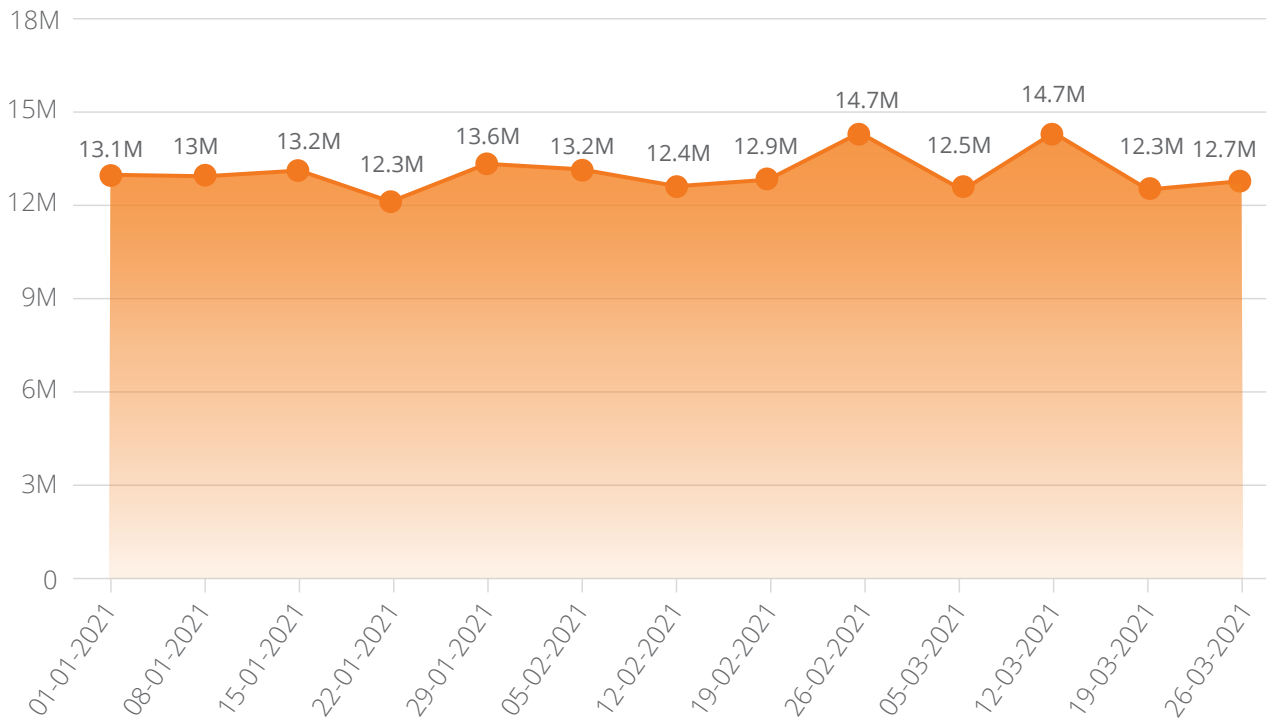
The below graph represents the statistics of the total count of Malware detected by Quick Heal from January to March 2021.



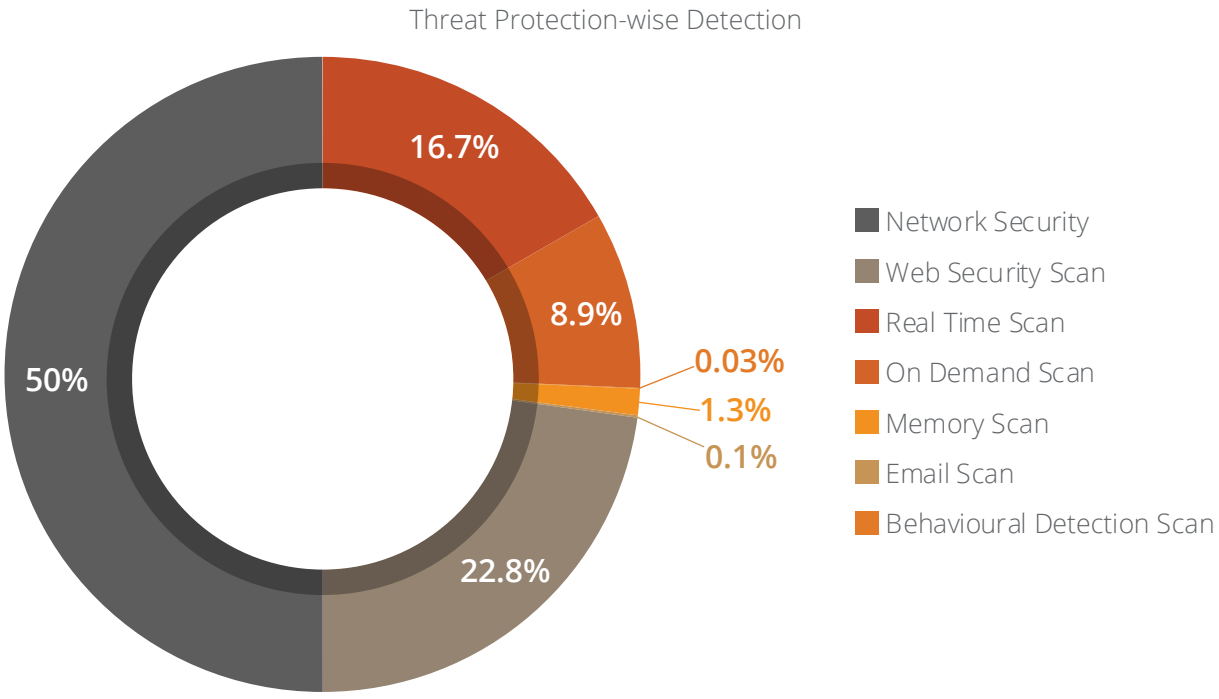
Observations

- Quick Heal detected over 166 Million Windows malware in Q1 2021. There is a 5% rise in the malware numbers as against Q4 2020.
- January clocked the highest detection. The sudden spike in the numbers could be because of the spike in the Bitcoin prices giving rise to cryptojacking attacks, and the pharma firms finalizing on the vaccines to fight against COVID-19.

Detection Statistics – Week-Over-Week



Detection Statistics – Protection Wise



Observations

- Maximum malware detections were made through Network Security Scan, which analyses network traffic to identify known cyber-attacks & stops the packet being delivered to the system.

Here is a brief description of how various detection methods function -

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.

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

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

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

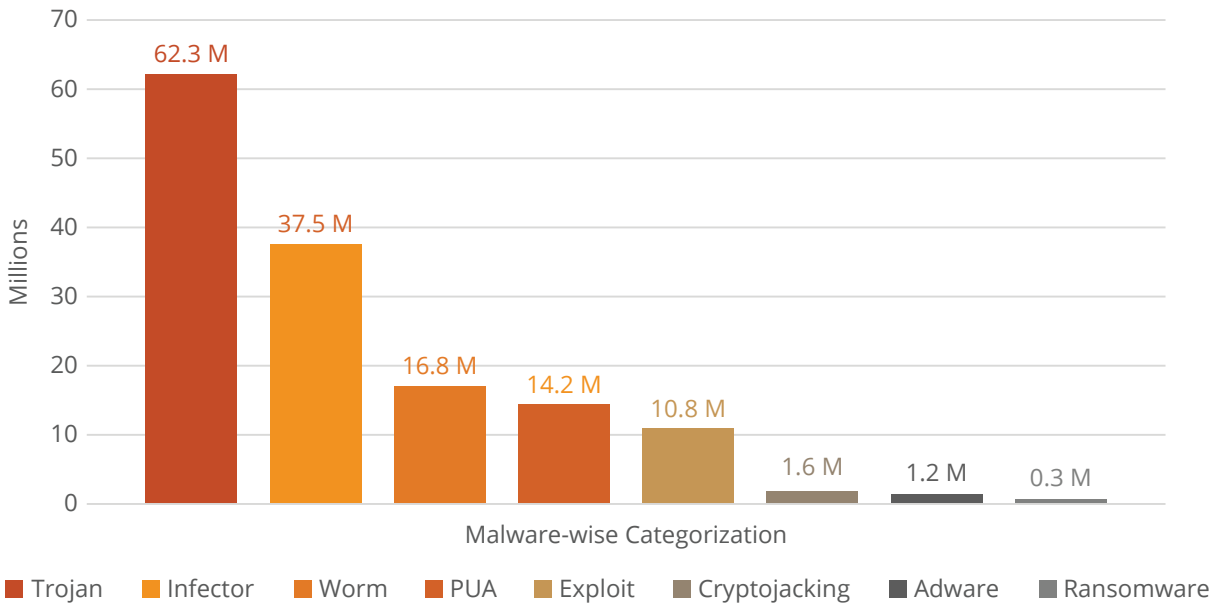
Web Security Scan
Automatically detects unsafe and potentially dangerous websites and prevents you from visiting them.

Network Scan
Network scan (IDS/IPS) analyzes network traffic to identify known cyberattacks & stops the packet being delivered to the system.

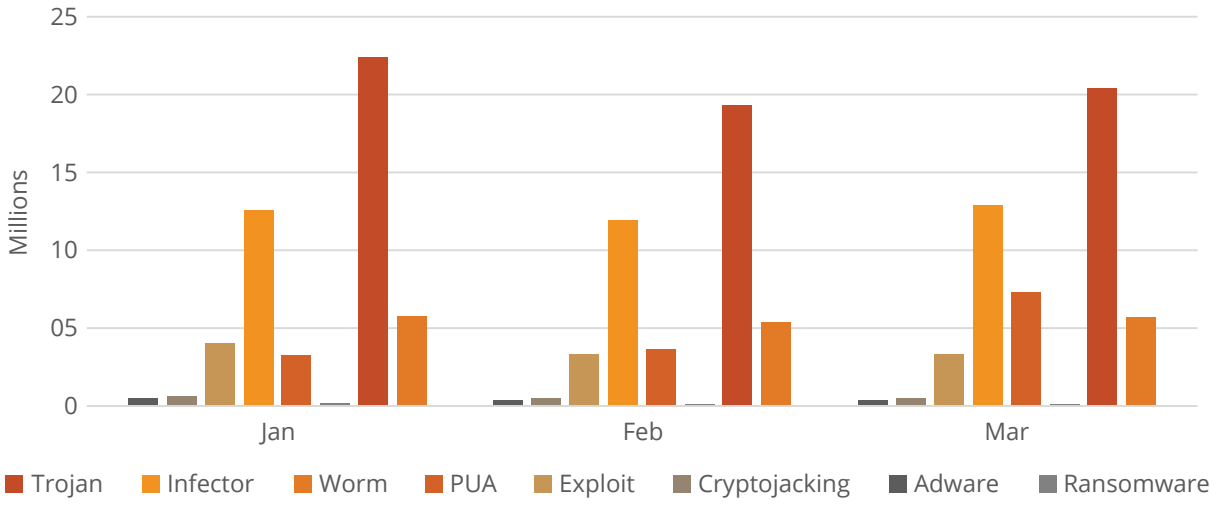
Detection Statistics - Category Wise

Categorization based on various Windows malware detected by Quick Heal in Q1 2021

A) Malware-wise Categorization



B) Month-wise Categorization



What Trojan Malware?

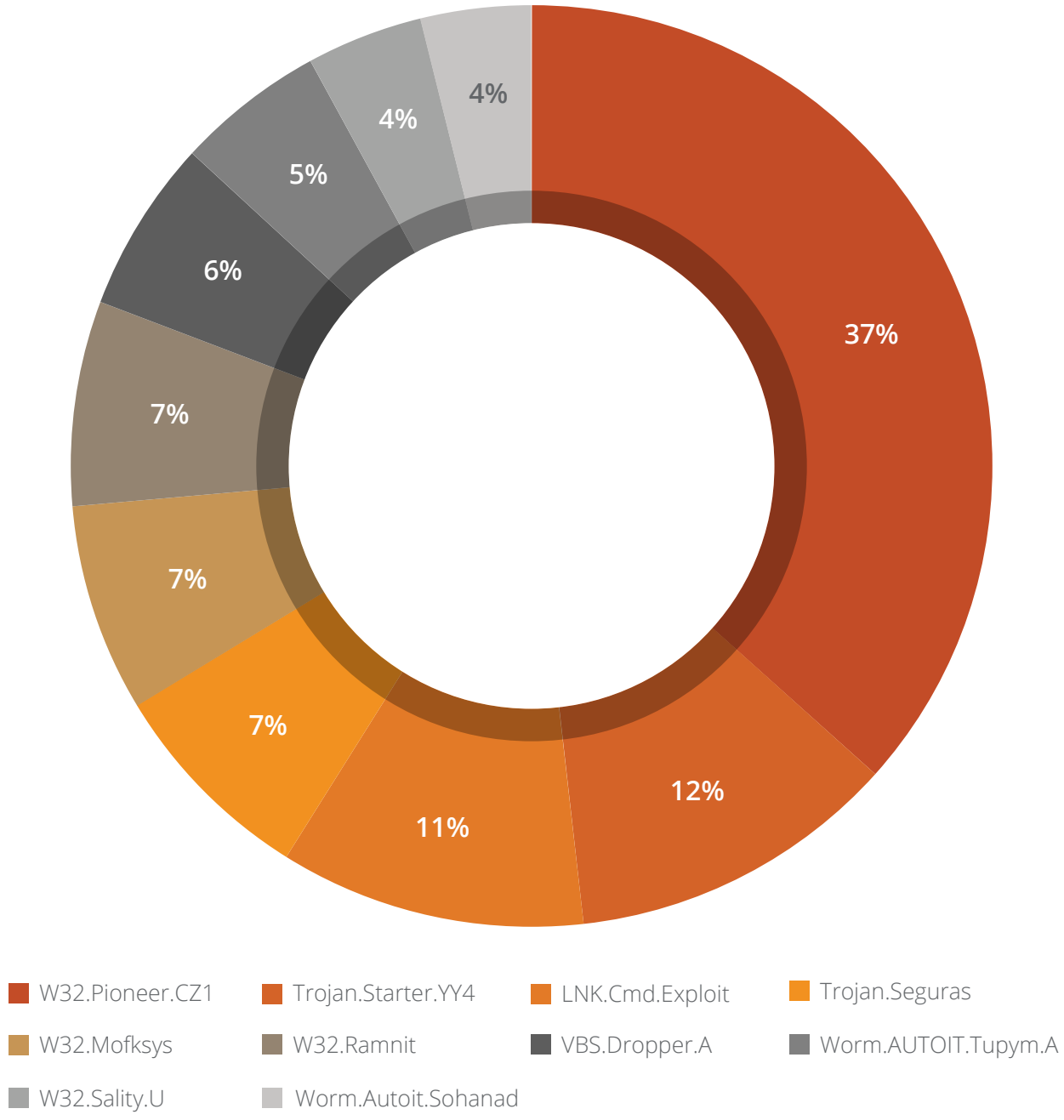
A Trojan horse or simply a Trojan is a malware that misleads users about its true intent. It disguises itself as legitimate software and fools the user to take an action.

Observation

- Trojan malware was found to clock the maximum detection with 62.3 Million in Q1.

Top 10 Windows Malware

The below figure represents the Top 10 Windows malware of Q1 2021. These malware have made it to this list based upon their rate of detection from January to March.



Top 10 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 which may cause a system crash.
- Downloads other malwares like key loggers.
- Slows down the booting and while shutting down the 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 a 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

Trojan.Seguras
Threat Level: Low
Category: Trojan
Method of Propagation: Bundled Applications

Behaviour:

- It often shows fake scan results luring users to purchase its full version.
- May download other malware that can infect the system.
- Degrades performance of the machine

05

W32.Mofksys

Threat Level: High

Category: Worm

Method of Propagation: Removable or network drives

Behaviour:

- It copies itself to following paths:
  - <System>\explorer.exe
  - <Windows>\svchost.exe
  - <Windows>\spoolsv.exe
- It adds these paths to RunOnce registry.
- It can capture the activity like keyboard/mouse inputs, including screen capturing and pass it to the remote intruder.
- Drops a copy of itself on other machines in network through writable shared drives and further uses sc.exe to remotely execute as a service.

06

VBS.Dropper.A

Threat Level: Medium

Category: Dropper

Method of Propagation: Web page

Behaviour:

- This malware spreads via malicious web pages. A web page contains embedded PE file.
- It drops that PE file to specific folder & launches that to perform malicious activity.

07

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.

08 **W32.Ramnit**

Threat Level: Medium

Category: File Infector

Method of Propagation: USB Drives, other malware, Exploit Kits, Spoofing the URL, and Bundled applications

Behaviour:

- This malware has several components embedded within it. After installer is dropped or downloaded, it drops its various components in memory or disk. Each component has specified task. This will also speed up the process of infection.
- It infects all running processes.
- It also infects HTML files by appending script in it while in the case of PE file infection it appends itself in the file.
- It modifies registry entries to ensure

09 **W32.Sality.U**

Threat Level: Medium

Category: File Infector

Method of Propagation: Removable or network drives

Behaviour:

- Injects its code into all running system processes. It then spreads further by infecting the executable files on local, removable, and remote shared drives.
- Tries to terminate security applications and deletes all files related to any security software installed on the system.
- Steals confidential information from the infected system.

10 **Worm.Autoit.Sohanad**

Threat Level: Medium

Category: Worm

Method of Propagation: Spreads through mails, IM apps, infected USB & network drives

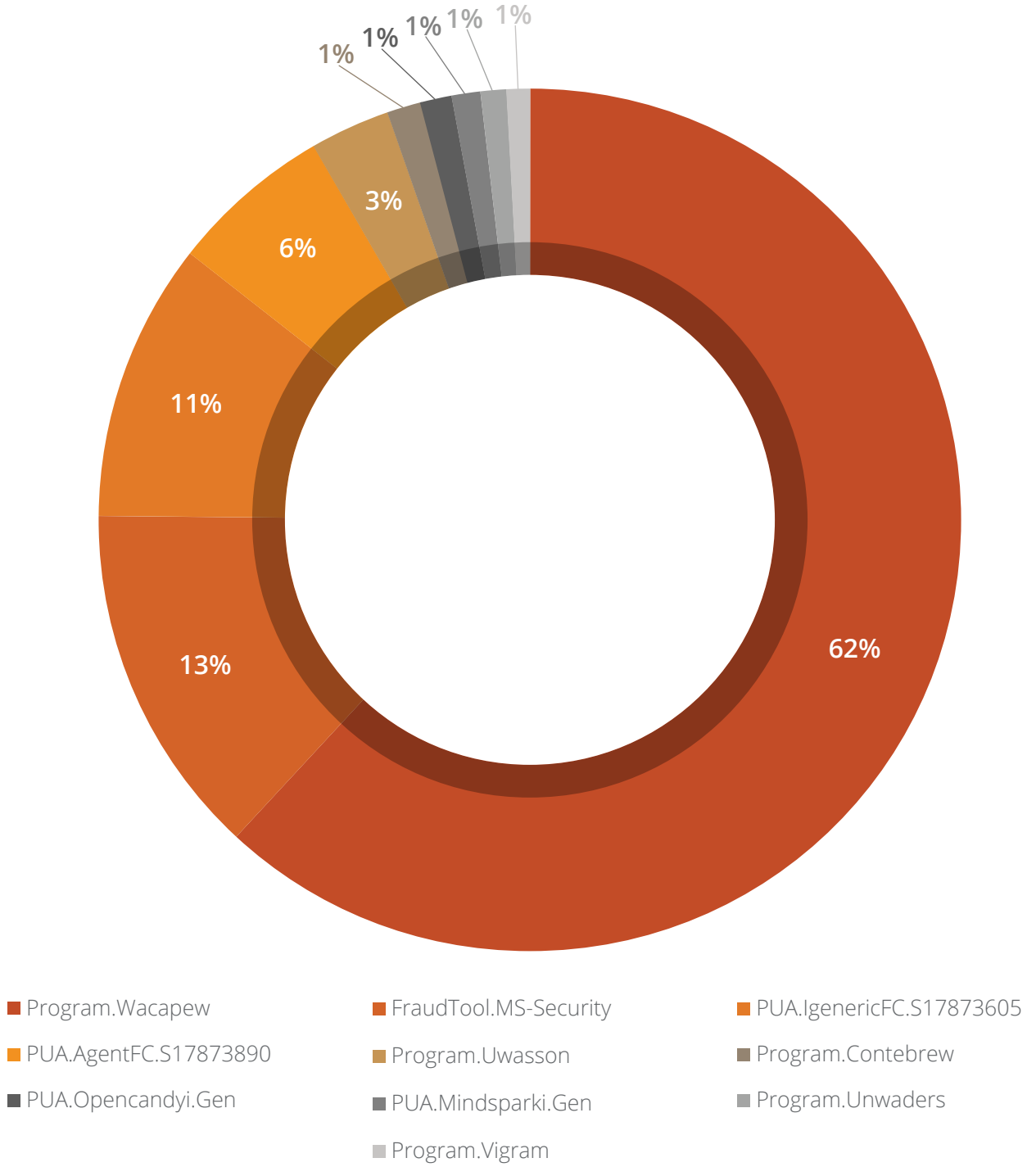
Behaviour:

- It arrives to your computer through Messaging apps, infected USB or network.
- It has ability to spread quickly.
- After arrival it creates copy of itself as exe with typical windows folder icon.
- User mistakenly executes this exe assuming it as a folder and then it spreads over network.
- It infects every connected USB drive too.

Top 10 Potentially Unwanted Applications (PUA) and Adware

Top 10 Potentially Unwanted Applications (PUA) and Adware programs that 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 10 PUAs and Adware detected by Quick Heal in Q1 2021.

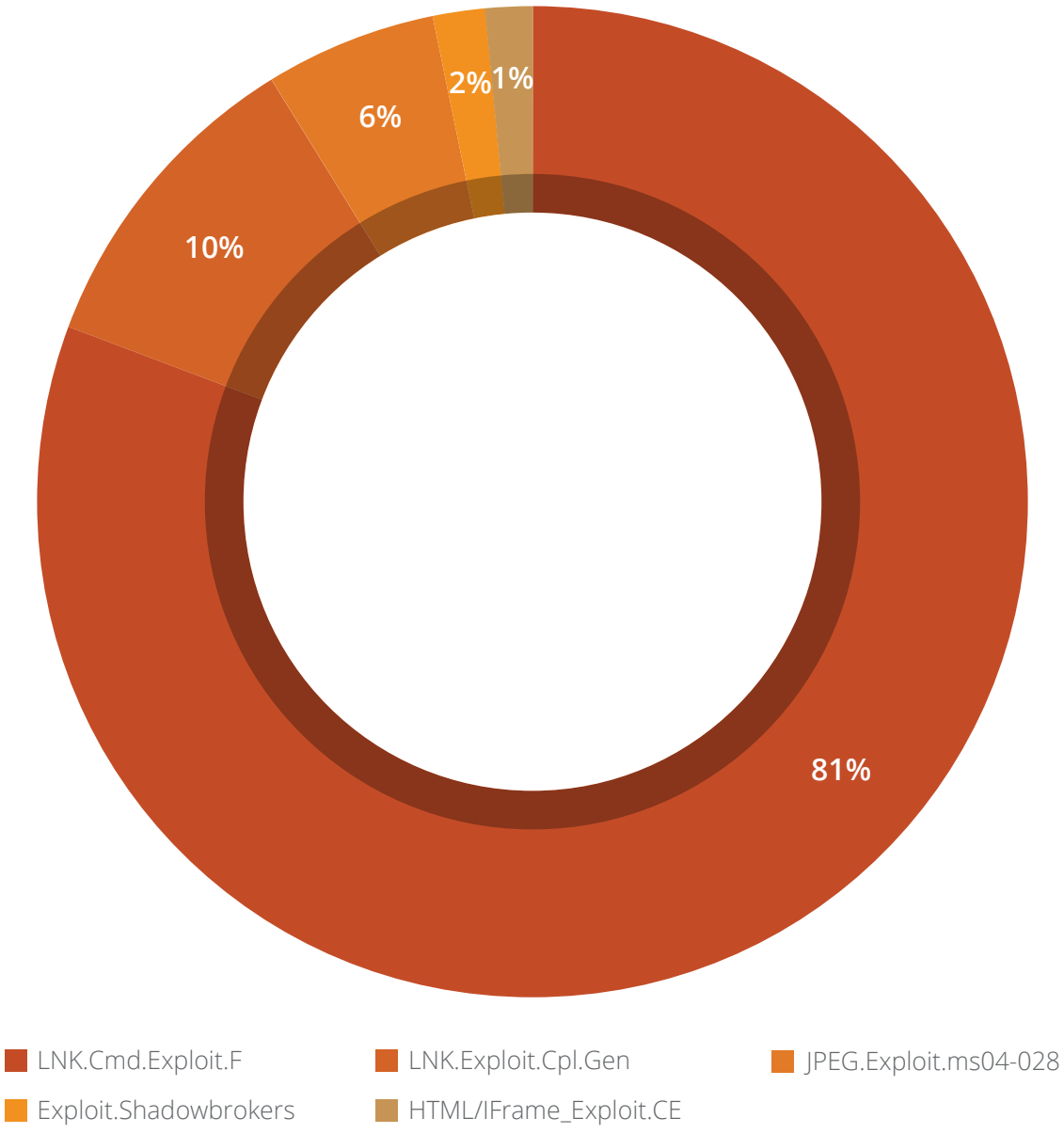


Observations

- Program.Wacapew was detected to be the top PUA, with 5.9 Million detections made in Q1 2021.

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?

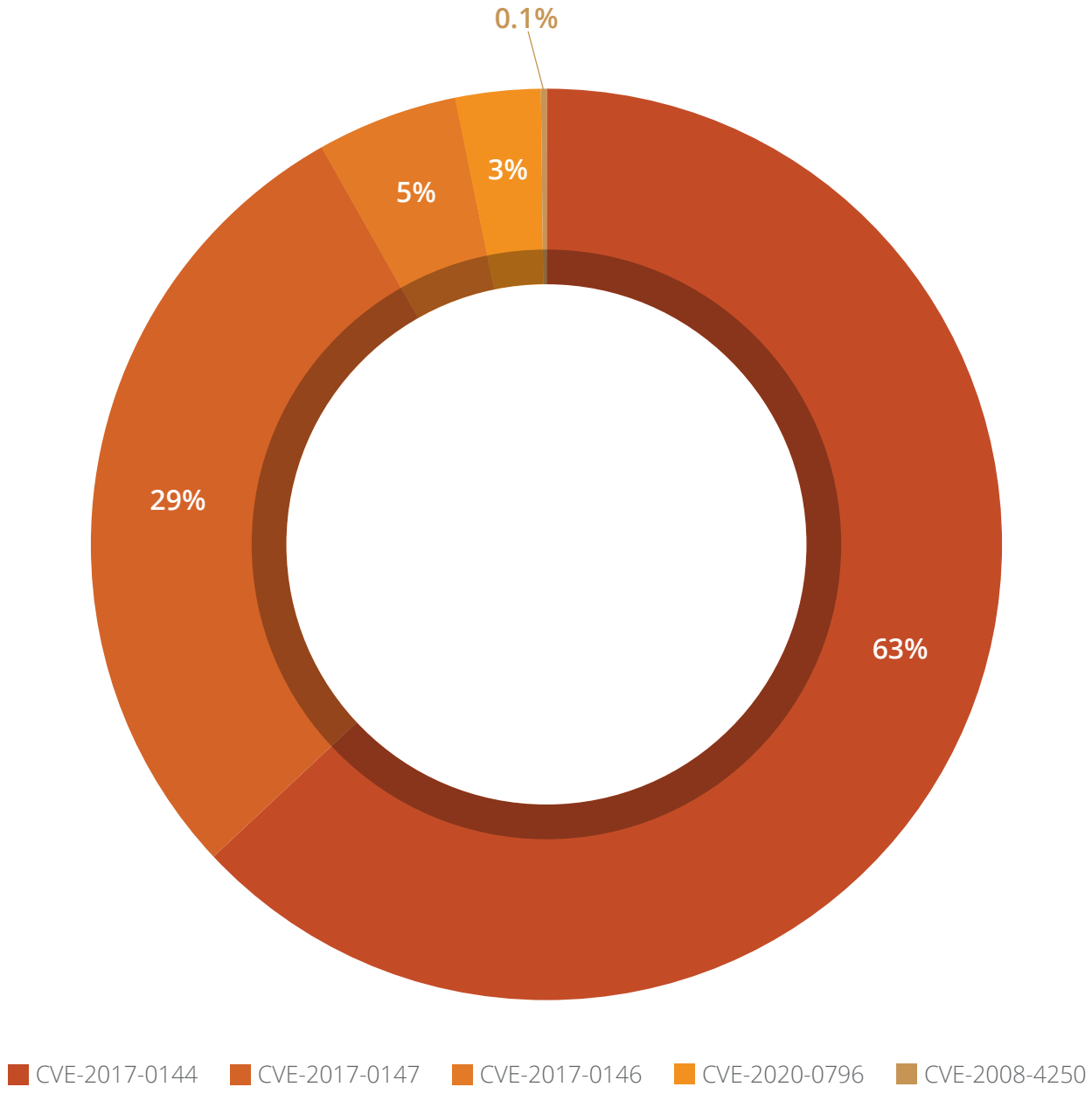
Host-based exploits are those that target security vulnerabilities found in host-based applications (host is a computer or other device connected to a computer network). These exploits are detected by endpoint detection modules such as Virus Protection, Email Protection, and Scanner.

Observations

- LNK.Cmd.Exploit.F was detected to be the top host-based exploit, with 6.1 Million detections made in Q1 2021

Top 5 Network-Based Exploits

Below figure represents the top 5 Network-Based Windows exploits of Q1 2021



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).

Observation

- CVE-2017-0144 was detected to be the top host-based exploit, with around 64 Million detections made in Q1 2021.

Trends in Windows Security Threats

01 First Dlang-based ransomware: Vovalex

Recently, Quick Heal Labs came across new a ransomware called Vovalex which is being distributed through pirated software disguised as popular Window utilities, such as WinRAR, CCleaner, and uTorrent installers. The ransomware encrypts the device files and then drops a ransom note demanding payment in some form. Vovalex might be the primary ransomware written in D language, and it uses a single symmetric key to decrypt files. It is expected that ransomware will evolve and advance its encryption mechanisms.

02 Attack on Indian vaccine makers & Power Grid

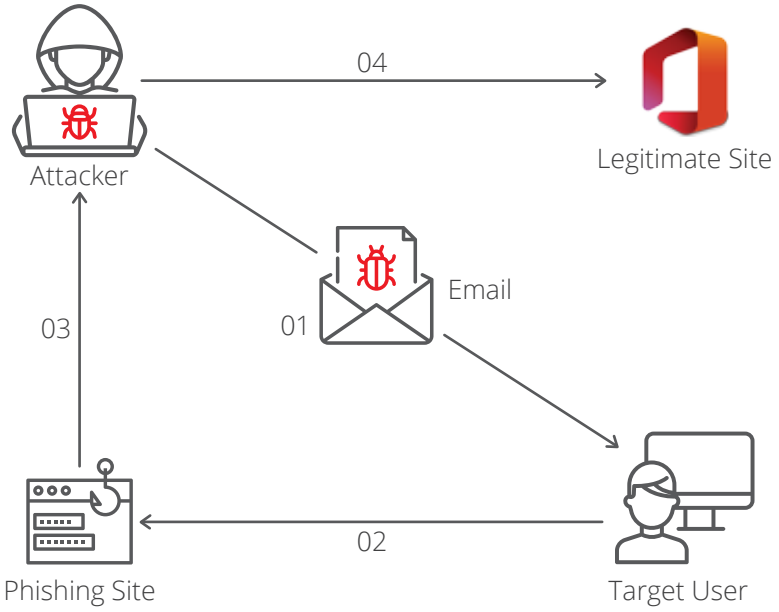
A Chinese state-backed hacking group APT10 has been targeting the systems of Indian vaccine manufacturers, Bharat Biotech and Serum Institute (SII). Hackers have identified certain gaps in the IT infrastructure and supply chain software of these companies. The real motive was exfiltrating intellectual property and getting a competitive edge over Indian pharmaceutical companies. This is not the first time that Chinese hackers have targeted India. Last year, they had an alleged role in attacking India's power grid which caused a blackout in Mumbai.

03 Discord becoming famous among malware authors

Cybercriminals step up efforts to target gamers on Discord – a popular app used to interact over voice calls, videos calls, or text messaging. It also allows users to set up servers or join pre-existing ones easily. Over 100 unique malicious malware are being served through Discord in zscaler cloud over the last two months alone. The attack usually starts with spam emails in which prospective marks are lured with legitimate-looking templates into downloading next-stage payloads. Another feature called Webhooks permits websites and external applications to send a message to the discord channel.

04 Spear Phishing targets Microsoft O365 users to gather credentials

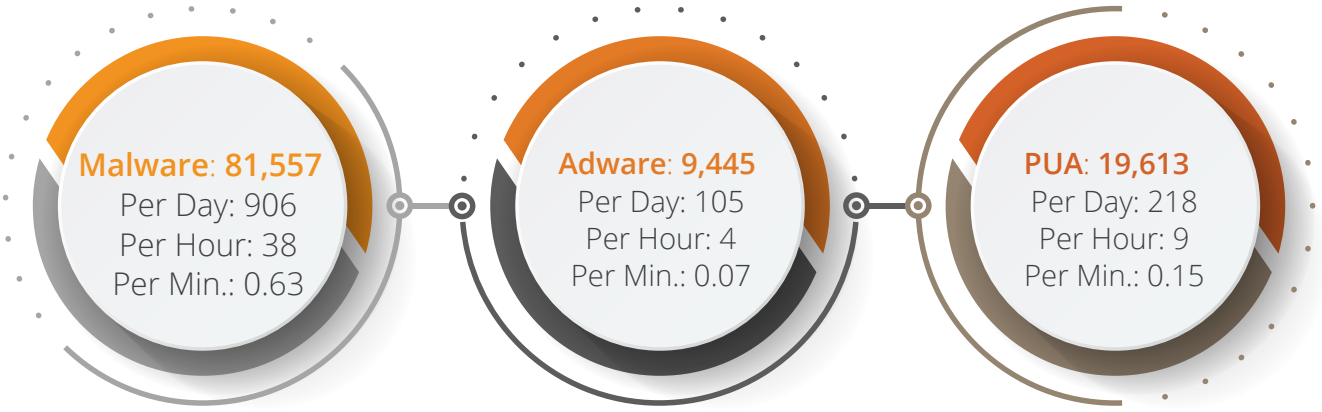
There was a considerable amount of rise in Phishing Attacks during the COVID-19 pandemic. One such Spear Phishing Campaign targets high-profile individuals for credential harvesting. The analysed email links to a fake login page that resembles the victim's organization's Office 365 login. The fake phishing page looks exactly similar to the Microsoft Office login page. The redirected URL can target a substring in your organization to make users believe in the legitimacy of the website. The end goal of the attackers is to spoof the targeted victims to damage the organization's data and reputations, lead to scams, and steal critical information.



74%
of total Android Threats detected in Q1 '21 were Malware

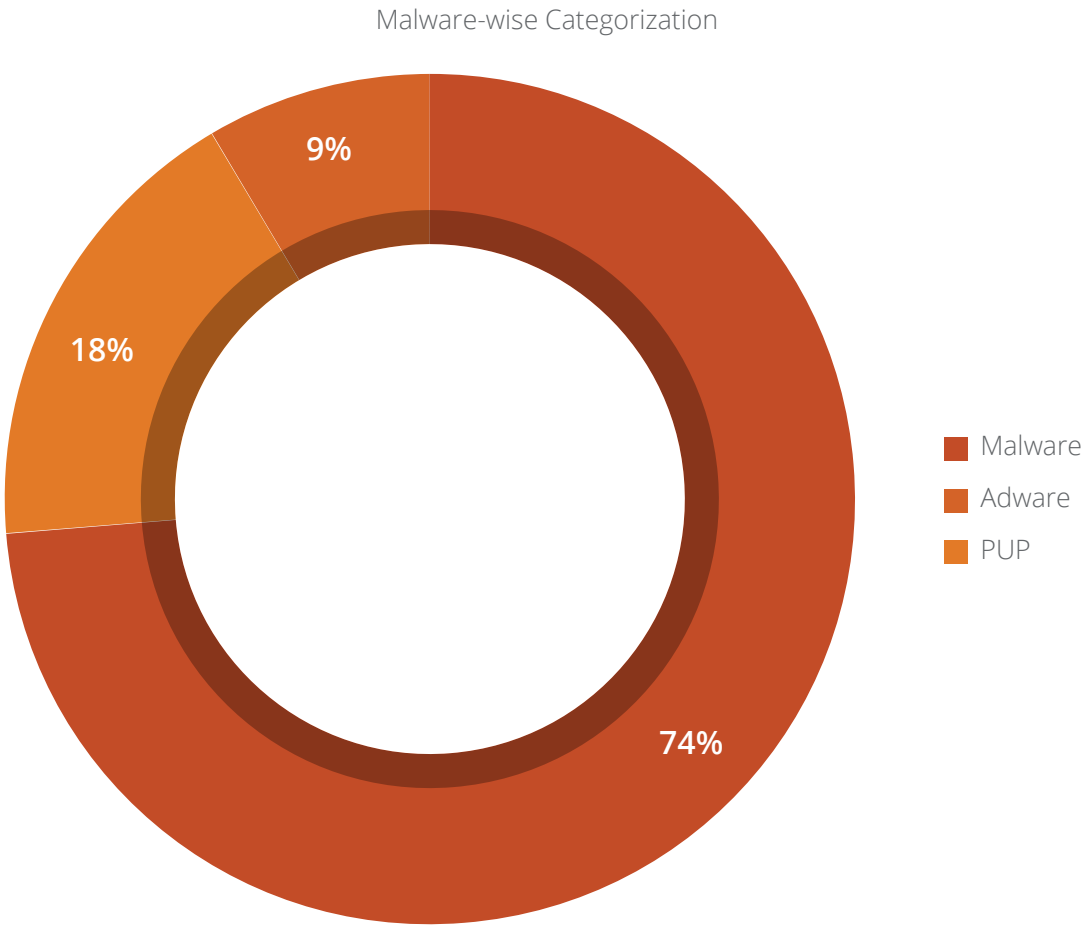
ANDROID

Android Malware Detections for Q1 2021



Detection Statistics: Category Wise

Below figure represents the various categories of Android malware detected by Quick Heal in Q1 2021.

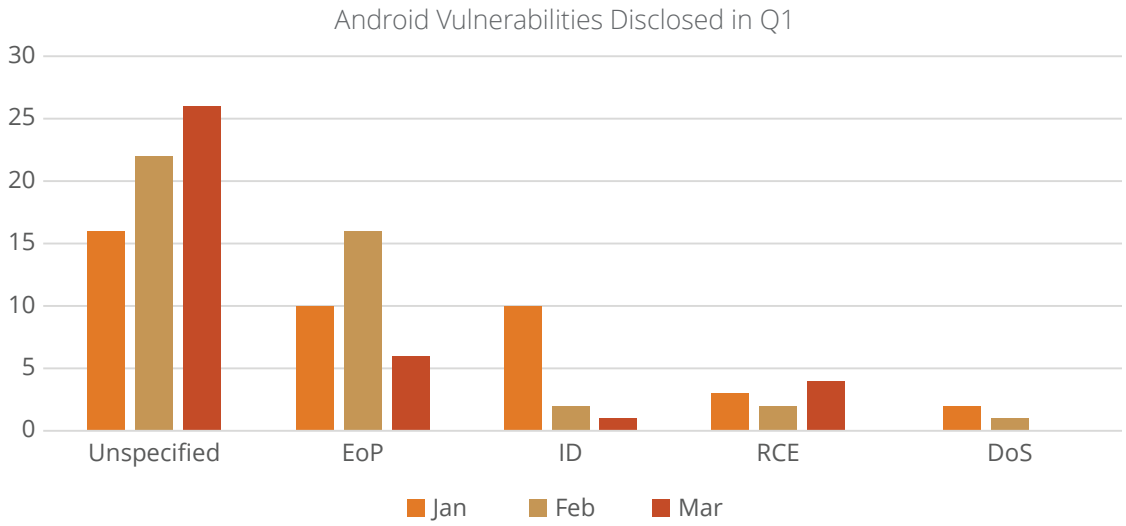


Observations

- Malware clocked 74% of the total Android detections in Q1 2021.

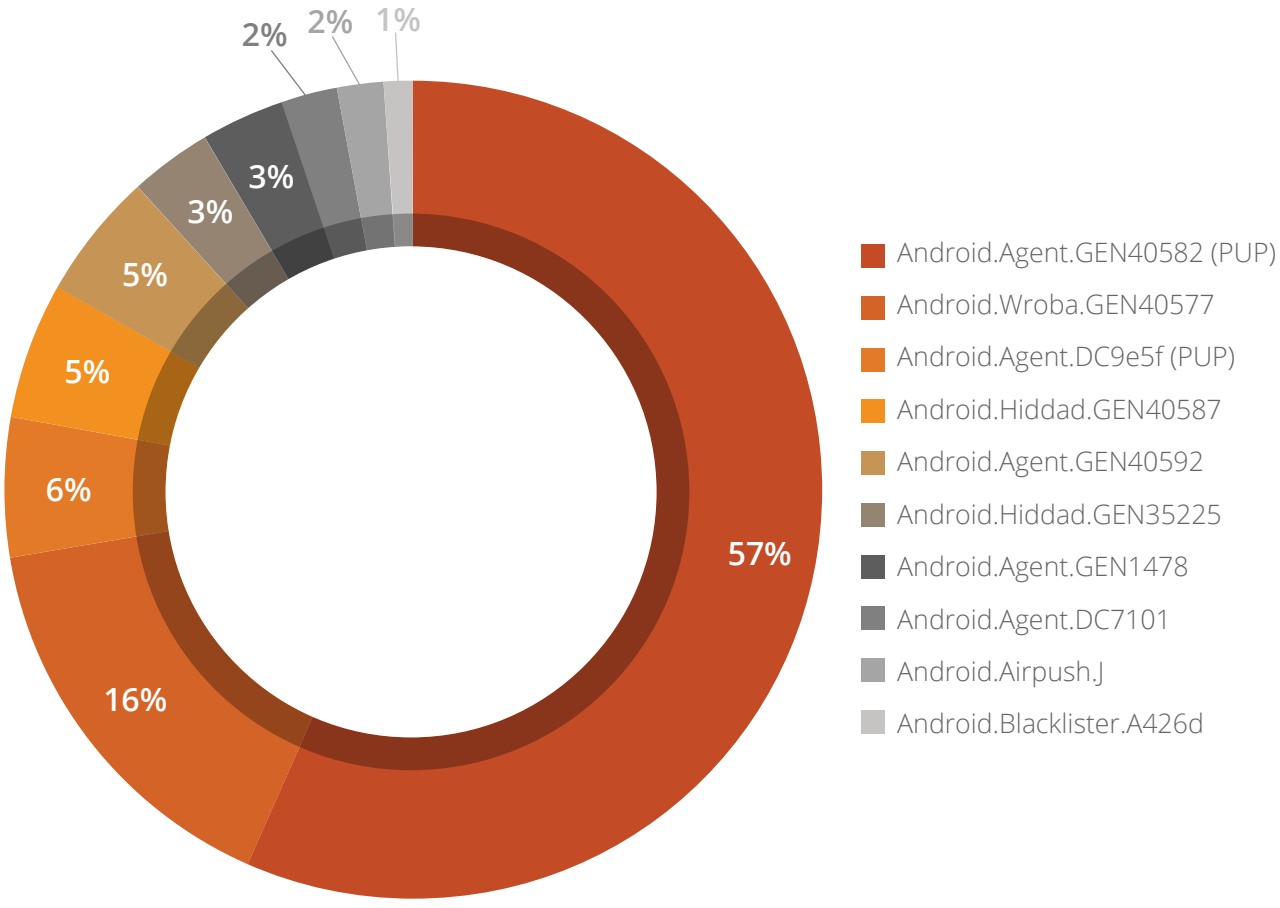
Security Vulnerabilities Discovered

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 January to March 2021.



Top 10 Android Malware for Q1 2021

Below figure represents top 10 Android Malware of Q1 2021. These malware have made it to this list based upon their rate of detection across the year.



Top 10 Threat Details

01

Android.Agent.GEN40582 (PUP)
Threat Level: Medium
Category: Potentially Unwanted Application (PUA)
Method of Propagation: Third-party app stores

Behaviour:

- These are Chinese wallpaper-related apps.
- It runs one service in background and connects to advertisement URLs.
- It collects the infected device's information and sends to the server.

02

Android.Wroba.GEN40577
Threat Level: High
Category: Malware
Method of Propagation: Third-party app stores

Behaviour:

- This malware sends SMS to predefined numbers.
- It can abort some SMS and hide the notification from the user.
- It checks for few applications like task manager and if that application is running, it kills it.
- It sends device information to URL.

03

Android.Agent.DC9e5f (PUP)
Threat Level: High
Category: Potentially Unwanted Application (PUA)
Method of Propagation: Third-party app stores

Behaviour:

- These applications are chat and video calling applications.
- These applications access location details and send it to server.
- It takes contact details, messages data and send it to the server.
- All data shared to the server without encryption

04

Android.Hiddad.GEN40587
Threat Level: High
Category: Malware
Method of Propagation: Third-party app stores

Behaviour:

- It disguises as battery saver application and sends device data to URL which is in encrypted form.
- It uses one counter to maintain ads count.
- It shows hidden ads after checking location and network connectivity.

05

Android.Agent.GEN40592
Threat Level: High
Category: Malware
Method of Propagation: Third-party app stores

Behaviour:

- Upon execution, it retrieves the affected users' IMSI and sends it to a certain URL.
- It also sends text messages to subscribe to certain services
- Which eventually leads to unwanted charges for the affected user.

06

Android.Hiddad.GEN35225
Threat Level: High
Category: Malware
Method of Propagation: Third-party app stores

Behaviour:

- All these apps use a standard SDK (Software Development Kit) for advertising.
- Capabilities of this malware family include showing ads, opening URLs in browser & receiving commands from C&C (Command & Control) server to perform activities.
- It can also hide its icon in the app launcher, making it difficult to notice its existence but runs in the background even after device restarts.
- Intention of these apps seems to generate as much ad revenue as possible.

07

Android.Agent.GEN1478
Threat Level: High
Category: Malware
Method of Propagation: Third-party app stores

Behaviour:

- After it's launched, it hides its icon and runs in the background.
- In the background, it downloads malicious apps from its C&C server.
- The downloaded malicious apps perform further malicious activities and may steal user information.

08

Android.Agent.DC7101
Threat Level: High
Category: Malware
Method of Propagation: Third-party app stores

Behaviour:

- This is from Trojan-Dropper family. It looks like a legitimate application like RAM cleaner.
- It carries encrypted malicious payload with it.
- It uses encrypted Chinese string to decrypt payload for further malicious activity.

09

Android.Airpush.J

Threat Level: Low

Category: Adware

Method of Propagation: Third-party app stores and repacked apps

Behaviour:

- Displays multiple ads while it is running.
- When the user clicks on one of these ads, they get redirected to a third-party server where they are prompted to download and install other apps.
- Shares information about the user's device location with a third-party server.

10

Android.Blacklister.A426d (PUP)

Threat Level: Medium

Category: Adware

Method of Propagation: Google Play Store

Behaviour:

- These apps mimic the functionalities of an Anti-virus or security app but do not have any such functionality
- It only shows fake virus detection alert to users
- It contains pre-defined Blacklist/Whitelist of Apps and permissions to show as a scan result
- The main purpose of these apps is to show advertisements and increase the download count
- It only gives a false impression of being protected, which might harm users' mobiles as they don't have such capabilities to detect real malware.

Trends in Android Security Threats

01

Joker malware dupes its way back to the Google Play Store

A new variant of the Joker spyware hits Google Play yet again with 17 other variants. Quick Heal Security Labs found two malicious apps named “Easy QR Scanner” and “Free Translator” on Google Play Store, which had more than 10k installations. These apps were laced with a new Joker malware variant. We reported these apps to Google’s Android Security team and got these apps removed from the Play Store. Quick Heal detects these applications with names - **Android.Jocker.A**.

Though the malicious apps have been removed, the spyware could still threaten 200,000 other installs. If the harmful apps are still present on your smartphone, it needs to be removed for they can steal your money, contact or device info, and text messages. It silently interacts with advertisement websites and subscribes the victim to premium services without their knowledge.

02

You might get hacked before getting vaccinated

Our blog highlights how malware authors impersonated the official app with malicious code and created a new app with the same name for people to mistake it with the official app and download. Many fake Aarogya Setu apps were found by Quick Heal that were using Spyware - Spynote RAT. We also found a duplicate vaccine registration app - CoWin named “CoWIN App”. Quick Heal detects these apps with the name - **Android.Fakeint.A**

03

ROGUE: The New android RAT malware

Recently, a new type of Android malware called Rouge RAT was discovered, combining two older types of malware, Cosmos and Hawkshaw. The threat could be data exfiltration, including photos, messages, locations, and contacts from the infected device. It also can erase the OS or download additional malicious payloads and mobile ransomware. The malware comes up with a notification sniffer and uses firebase services for the exchange of commands. Quick Heal detects these kinds of malware by the threat name **Android.Hawkshaw.GEN**

04

Android devices are targeted by LodaRAT Windows Malware

Known for targeting Windows devices, the LodaRAT malware is now targeting Android devices. The newly discovered malware variant has been found spying on the devices and recording the user's location, audio calls, environment audio, and photos and screenshots. The SMS, call log, and contact accessing functionalities are also present. Loda4Android is not capable of intercepting SMS messages or phone calls, unlike other banking trojans.
Quick Heal detects these kinds of malware by threat name **Android.Agent.GEN**

05

Domestic Kitten: An Iranian surveillance program

Domestic Kitten is from an advanced persistent threat (APT) group known for spreading via fake or malicious Android apps and lifting a range of sensitive information from victims’ devices. The APT uses mobile malware dubbed FurBall and attack information like text messages, call logs, media files, installed applications, and device location. Such kinds of apps are detected by Quick Heal with names **Android.Campys.GEN** and **Android.Agent.DC**

06 FluBot: SMS malware with malninstall targeting Android devices

FluBot is an Android-targeting malware that impersonates other apps on a victim's phone to steal their banking credentials and other private information. It has infected more than 60,000 users by copying apps like FedEx, DHL, Correos, and Chrome. The malware eavesdrop on the victim's notifications, read and write SMS's, make calls, and transfer the contact list to its C&C. It tricks users into granting accessibility permissions and hides, hence avoiding uninstallation. Such kinds of apps are detected by Quick Heal with the name **Android.Alien.A** & **Android.Dropper.A**

Inference

The second wave of COVID-19 will significantly impact global systems, and cybersecurity will be no exception to its influence. As businesses struggle to survive the disrupting effects of the second wave of the coronavirus, threat actors are moving quickly to capitalize on the resulting chaos.

In January 2021 alone, there were 57 million malware attacks! Hackers are at the top of their game, making individual users or remote workers using new devices or untested infrastructure wonder if their data is safe at all.

With coronavirus-themed attacks, remote work-related threats, ransom and phishing attacks, hackers will continue to evolve, giving companies a hard time. As malware operators innovate their attack strategies further, we might get to see more new revelations in the coming months of 2021. The biggest key takeaway from this report is to be aware and mindful of attacks and be prepared with proper security tools to tackle the unforeseen odds.

Quick Heal

Security Simplified

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

Phone: +91 20 66813232 | Email: info@quickheal.com | Website: www.quickheal.com