Quick Heal

Security Simplified

QUARTERLY THREAT REPORT

Q2 - 2020

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

With Coronavirus pandemic still looming large at us, cyberattacks are on the rise. We are facing new and never heard of cyberthreats as we tread along this difficult time.

Cybercriminals are taking advantage of COVID-19 pandemic for spreading malware and infecting devices to steal victim's data. A modular malware attacked users through fake COVID-19 phishing emails and Black Lives Matter campaigns. In Android too coronavirus themed attacks were prevalent, for example the fake Aarogya Setu App which managed to hack user's information.

This threat report collates cyberthreats detected and subsequently destroyed by our Security Labs team in the second quarter of 2020.

Quick Heal Security Labs detected 143 million Windows Malware in the second quarter of 2020. The report has the details of top malwares in both Windows and Android and extensively discusses the top trends in cyber attacks.

We detected around **1.5 million Malware every day** that included 5K Ransomware, 0.11 million Exploits, 0.13 million Adware & Potentially Unwanted Applications (PUA), 16K Cryptojacking malware, 0.25 million Infector and 0.13 million worm in Q2 2020.

The coronavirus outbreak has kept people on their toes and a majority of the population still works from home even though half of the year is over as we step in July. Schools and colleges are still resorting to online classes, giving cyber attackers even more opportunities to strike.

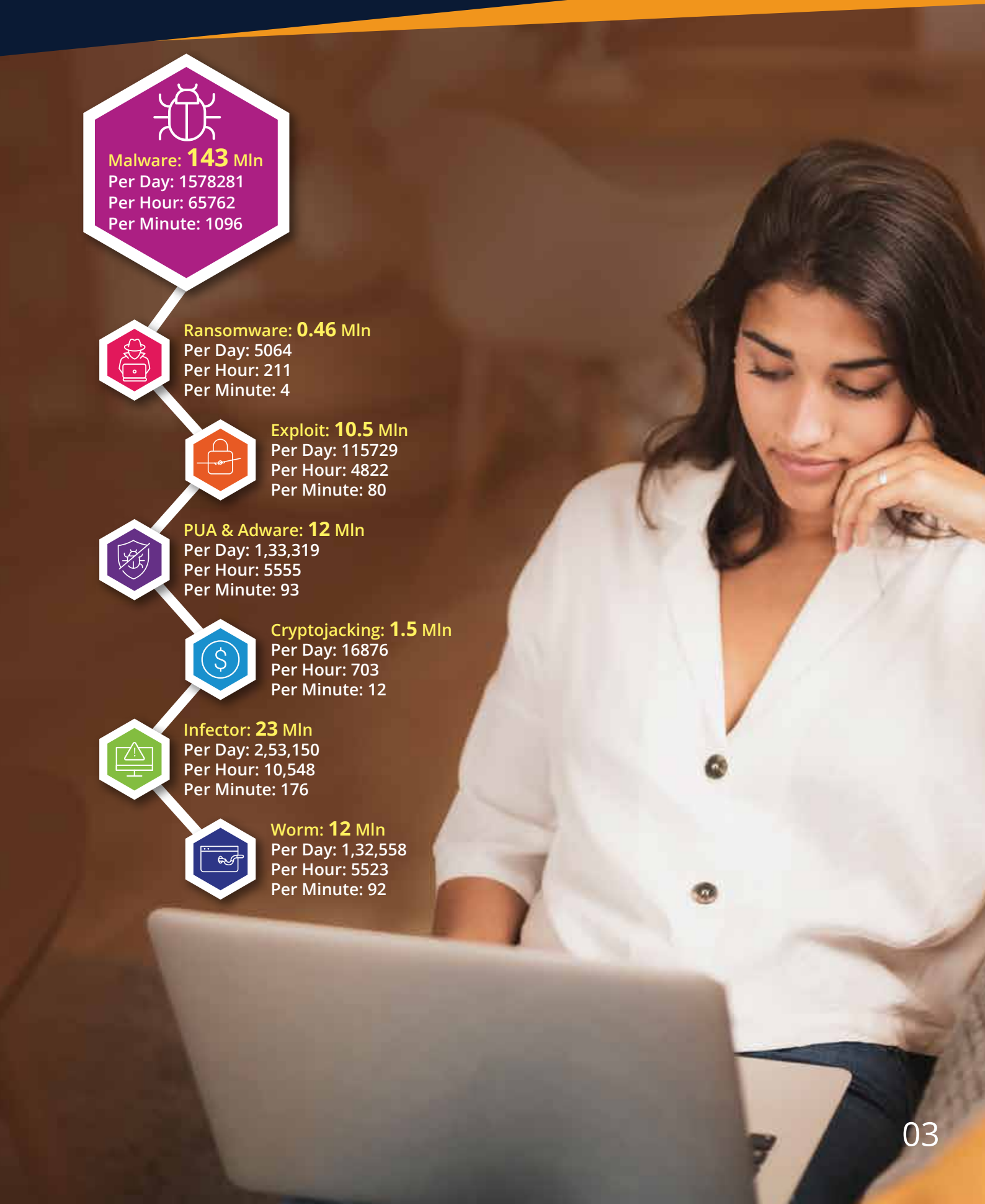
Windows

143
Million
Windows Malware detected in the Q2

64
Million
Windows Malware detected in June ‘20

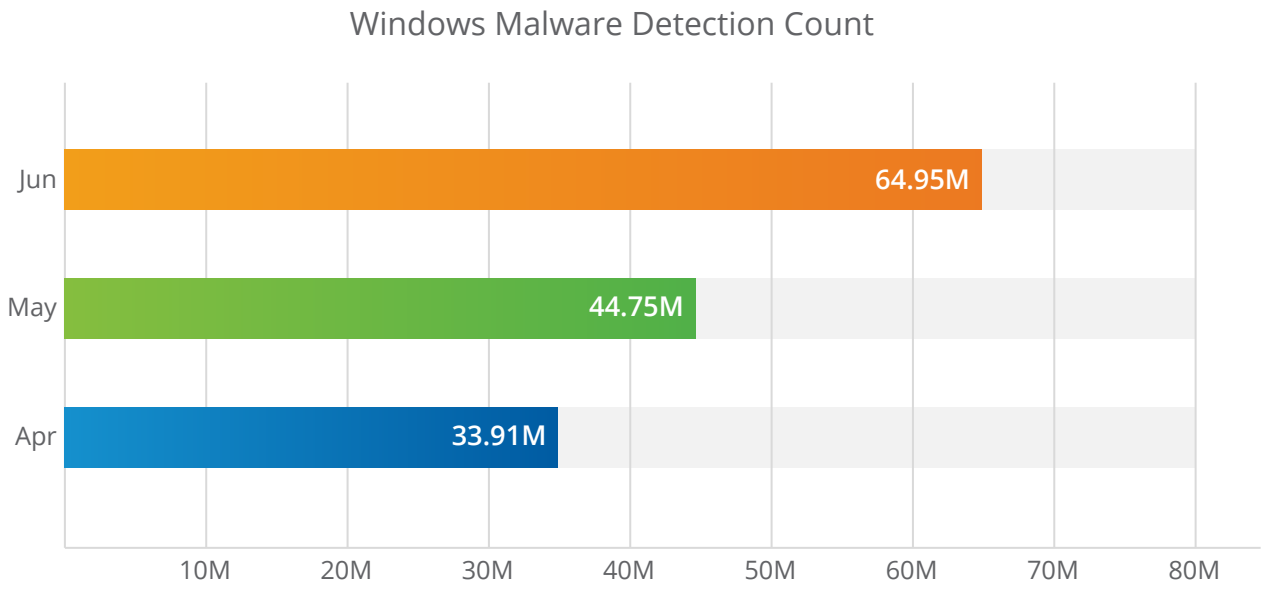
1.5
Million
Malware detected daily in Q2

Windows Detection Statistics Q2 2020



Detection Statistics – Month Wise Q2 2020

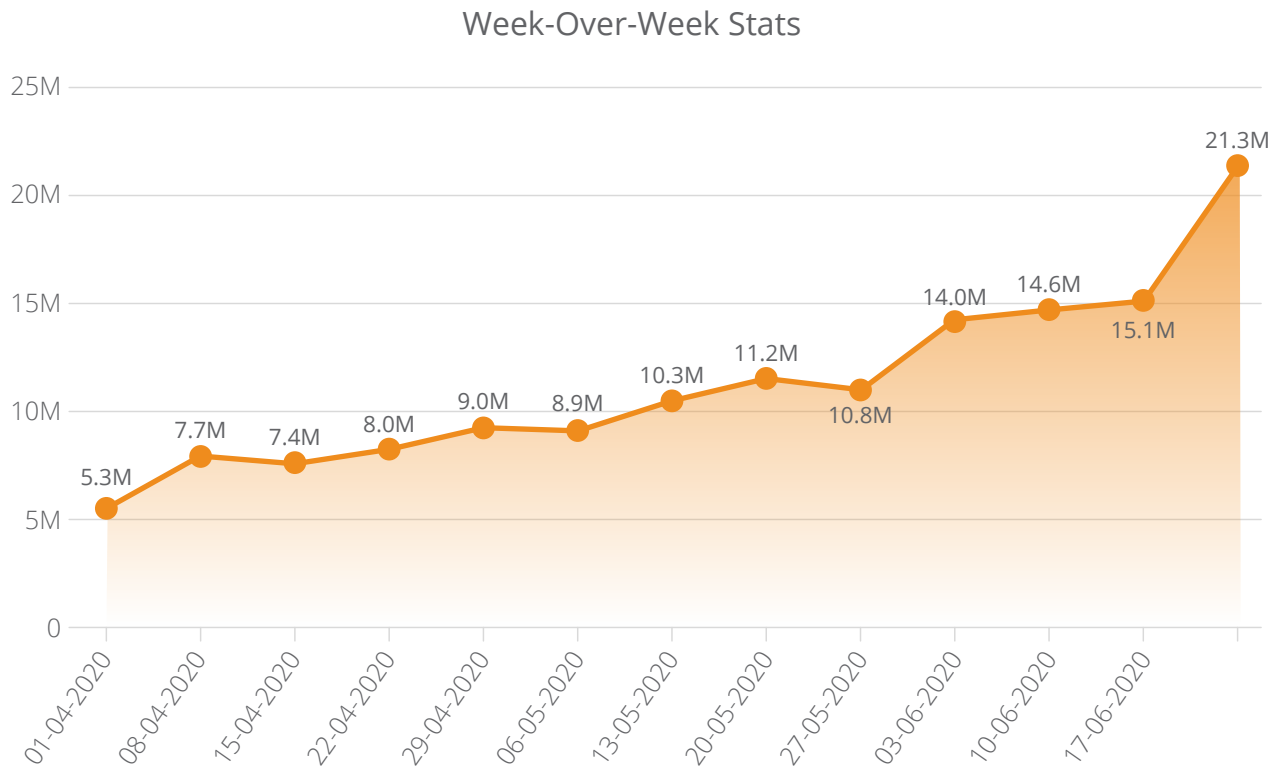
The below graph represents the statistics of the total count of malware detected by Quick Heal from April to June in 2020.



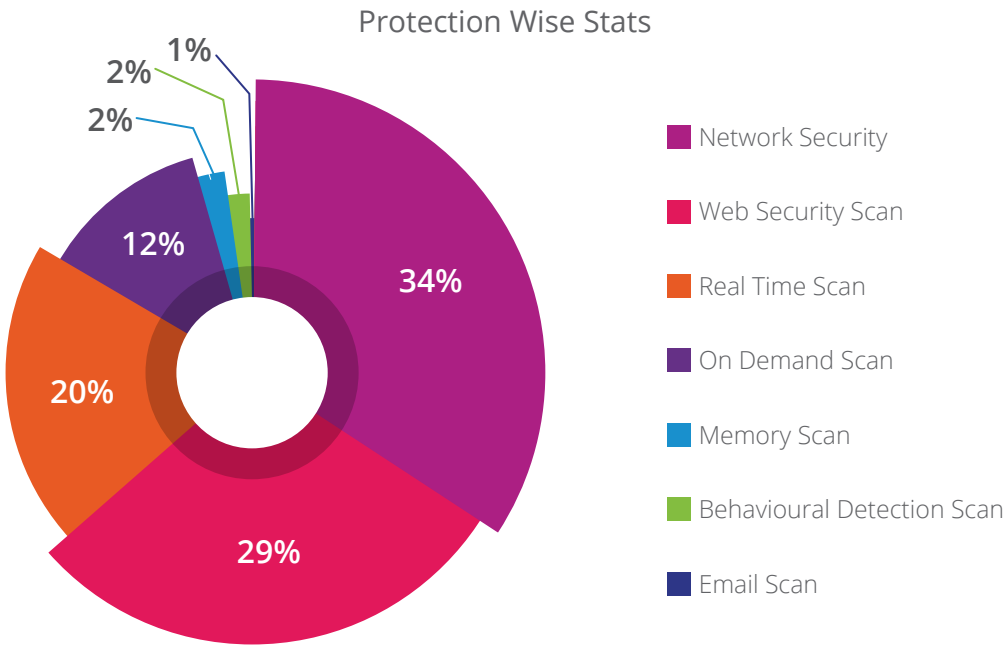
Observations

- Quick Heal detected over 143 million Windows malware in Q2 2020.
- June clocked the highest detection of Windows malware. The reason for the sudden spike in June numbers could be because of businesses opening up in June under the unlock phase.

Detection Statistics – Week-Over-Week



Detection Statistics – Protection Wise



Observation

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

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.

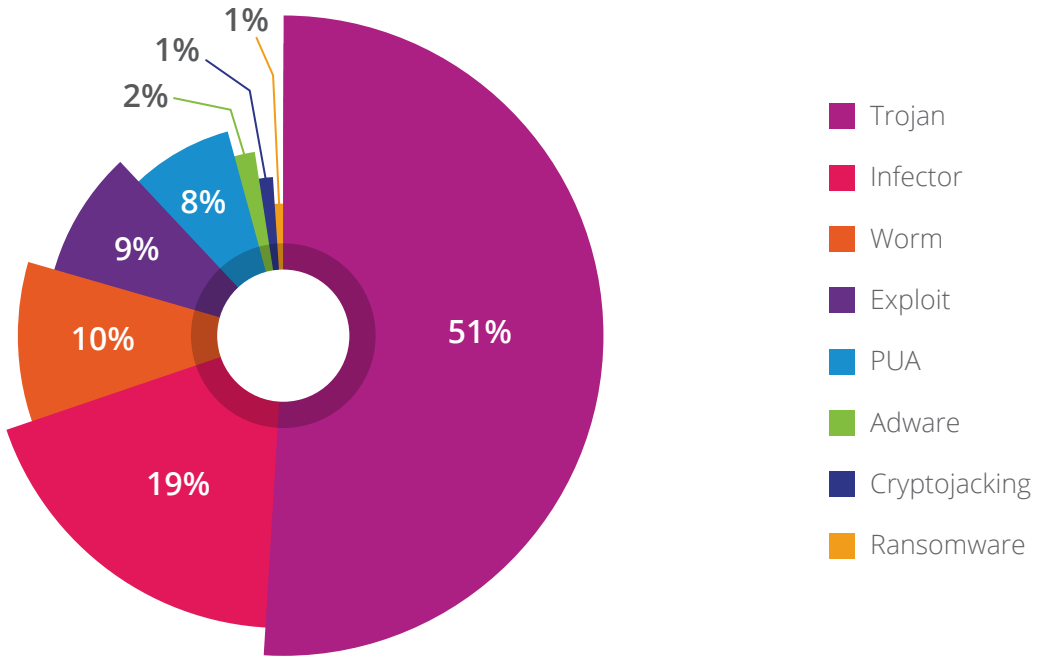
Network Scan

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

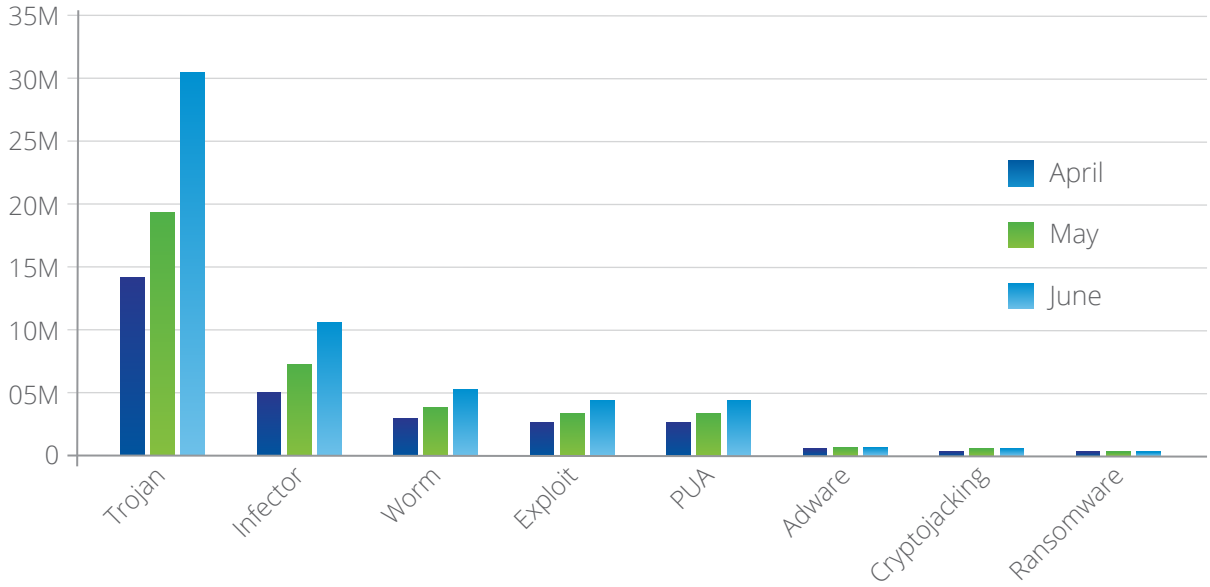
Detection Statistics – Category Wise

Below figures represent the various categories of Windows malware detected by Quick Heal in Q2 2020

Windows malware detection - Category Wise



Monthly Category wise Detection



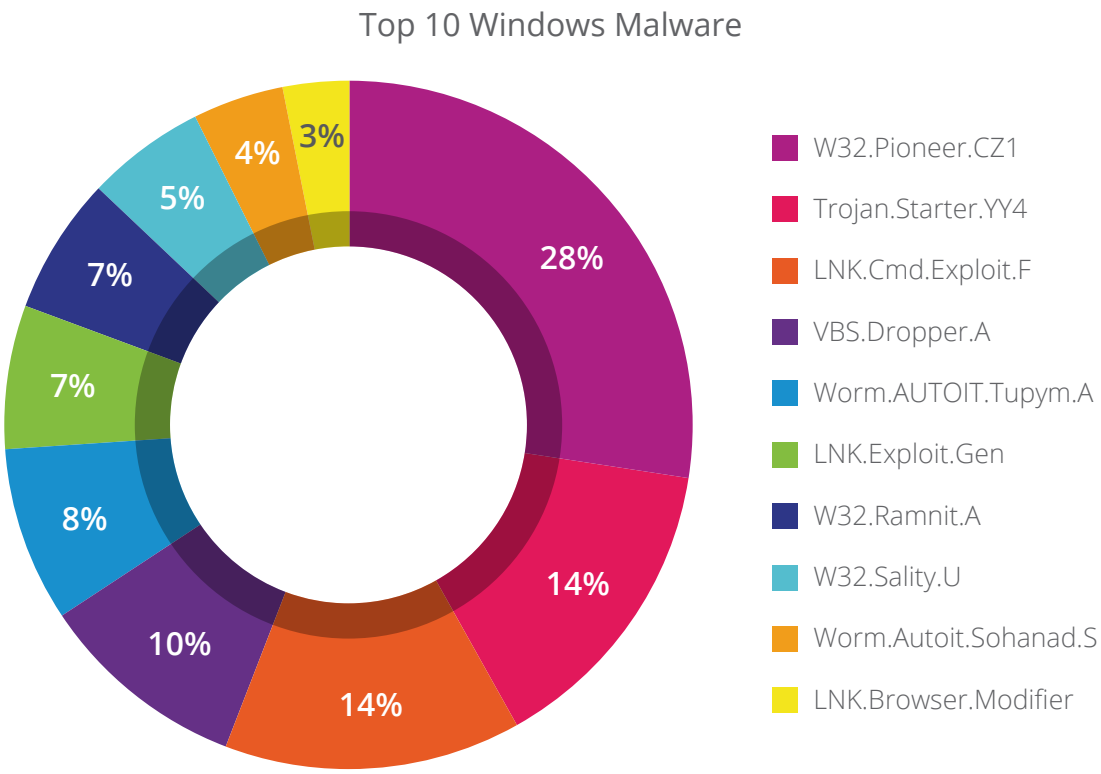
What is a Trojan?
A Trojan horse or simply a Trojan is a malware that misleads users about its true intent. It disguises itself as legitimate software and fools the user to take an action.

Observation

- Trojan malware was found to clock the maximum detection at 51% in Q2 2020.

Top 10 Malware

The below figure represents the Top 10 Windows malware of Q2 2020. These malware have made it to this list based upon their rate of detection from April to June.



Observation

• In Q2 2020, W32.Pioneer.CZ1 was detected to be the top Windows Malware, with 10 Million+ detections.

01

W32.Pioneer.CZ1

Threat Level: Medium

Category: File Infector

Method of Propagation: Removable or network drives

Behaviour:

- The malware injects its code to files present on disk and shared network.
- It decrypt 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 keyloggers.
- 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.F
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

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.

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

06

LNK.Exploit.Gen
Threat Level: High
Category: Trojan
Method of Propagation: Bundled software and freeware

Behaviour:

- It is a destructive Trojan virus that could hide in spam email attachments, malicious websites and suspicious pop-ups.
- This kind of virus can be installed on Windows systems by using illegal browser extensions.
- It changes some of the system files without the user knowing about it. Next time the user launches the Windows system, this virus will run in the system background and spy on their activities. In order to redirect the user to dubious websites, the virus modifies system hosts file and hijacks the IP address.

07

W32.Ramnit.A
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

08

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 nfecting 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

09

Worm.Autoit.Sohanad.S
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.

10

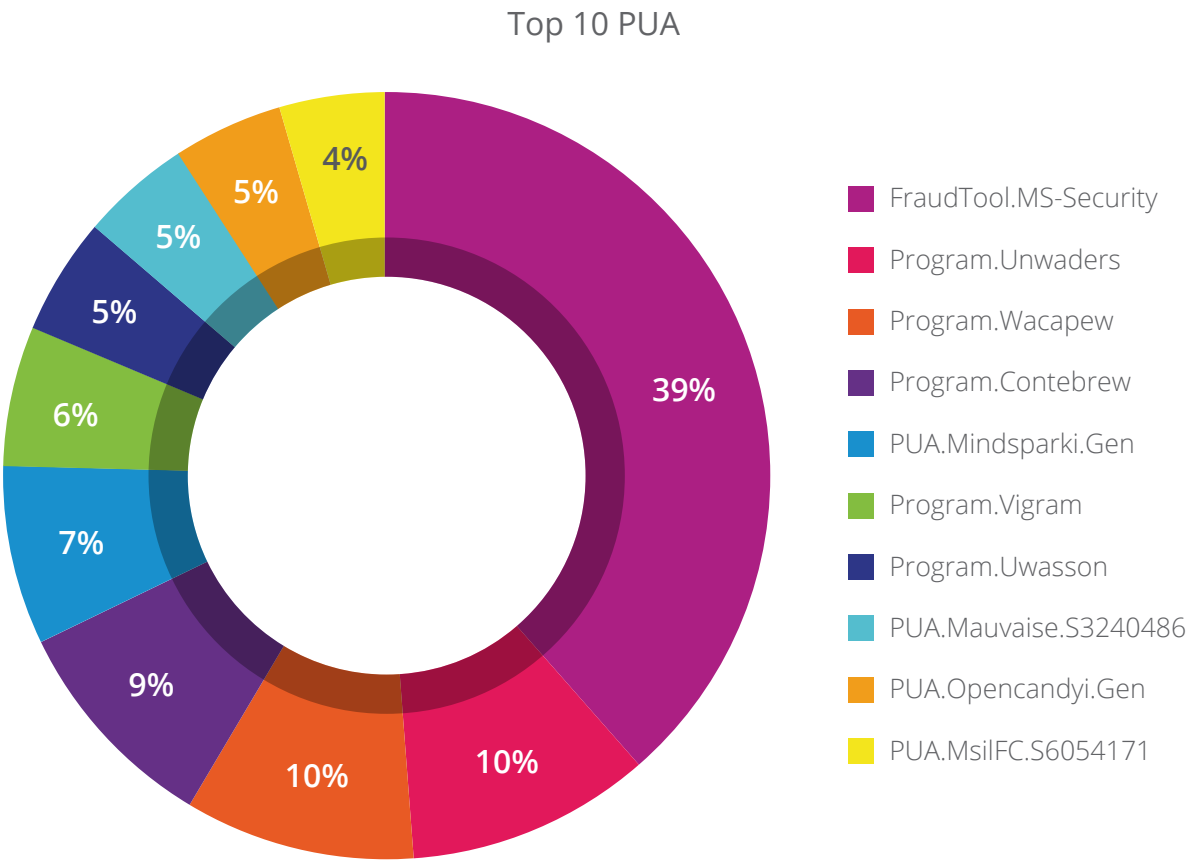
10. LNK.Browser.Modifier
Threat Level: High
Category: Trojan
Method of Propagation: Bundled software and freeware

Behaviour:

- Injects malicious codes into the browser which redirects the user to malicious links.
- Makes changes to the browser's default settings without user knowledge.
- Generates ads to cause the browser to malfunction.
- Steals the user's information while browsing like banking credentials for further misuse.

Top 10 Potentially Unwanted Applications (PUA) and Adware

Top 10 Potentially Unwanted Applications (PUA) are 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 Q2 2020

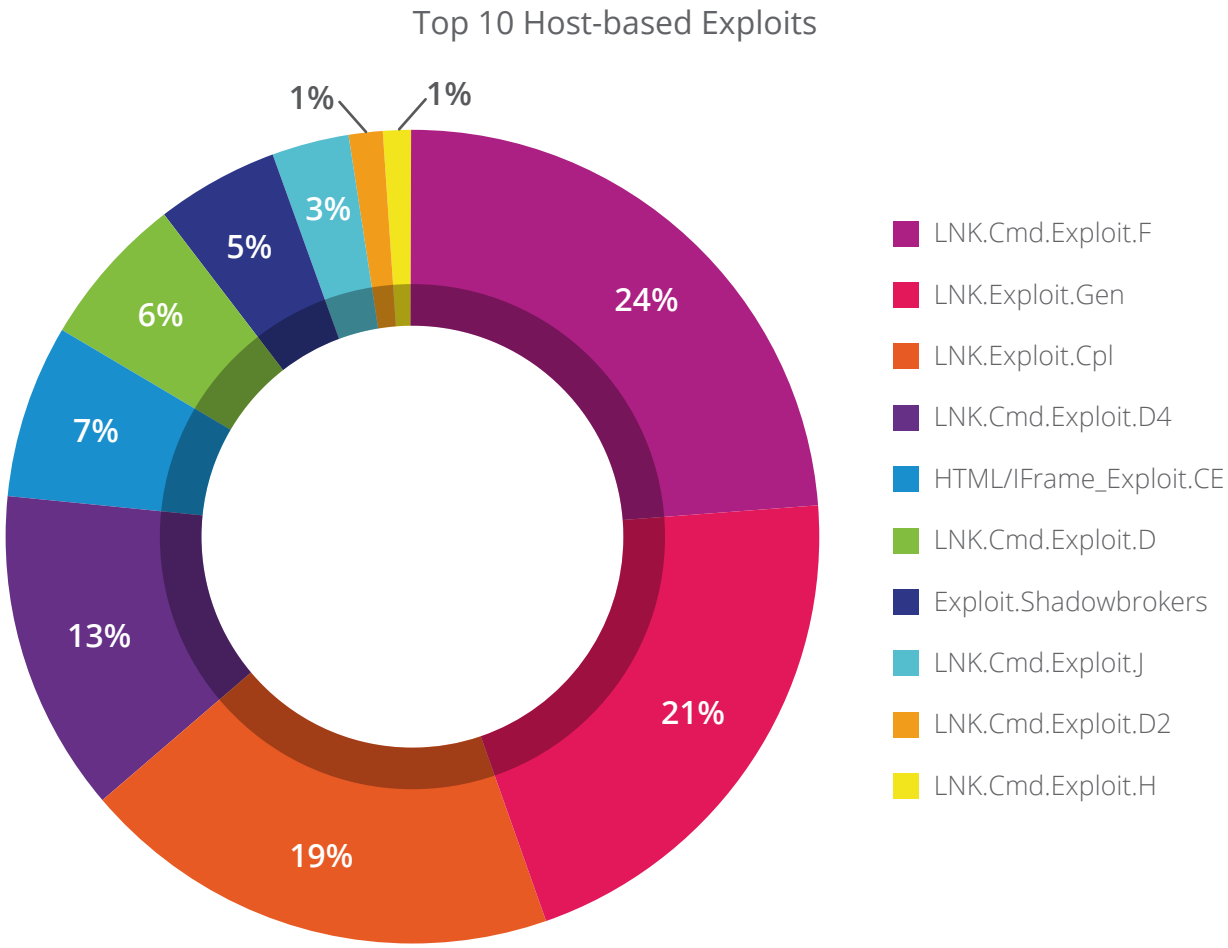


Observation

- FraudTool.MS-Security was detected to be the top PUA, with around 0.9 Million detections made in Q2 2020.

Top 10 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



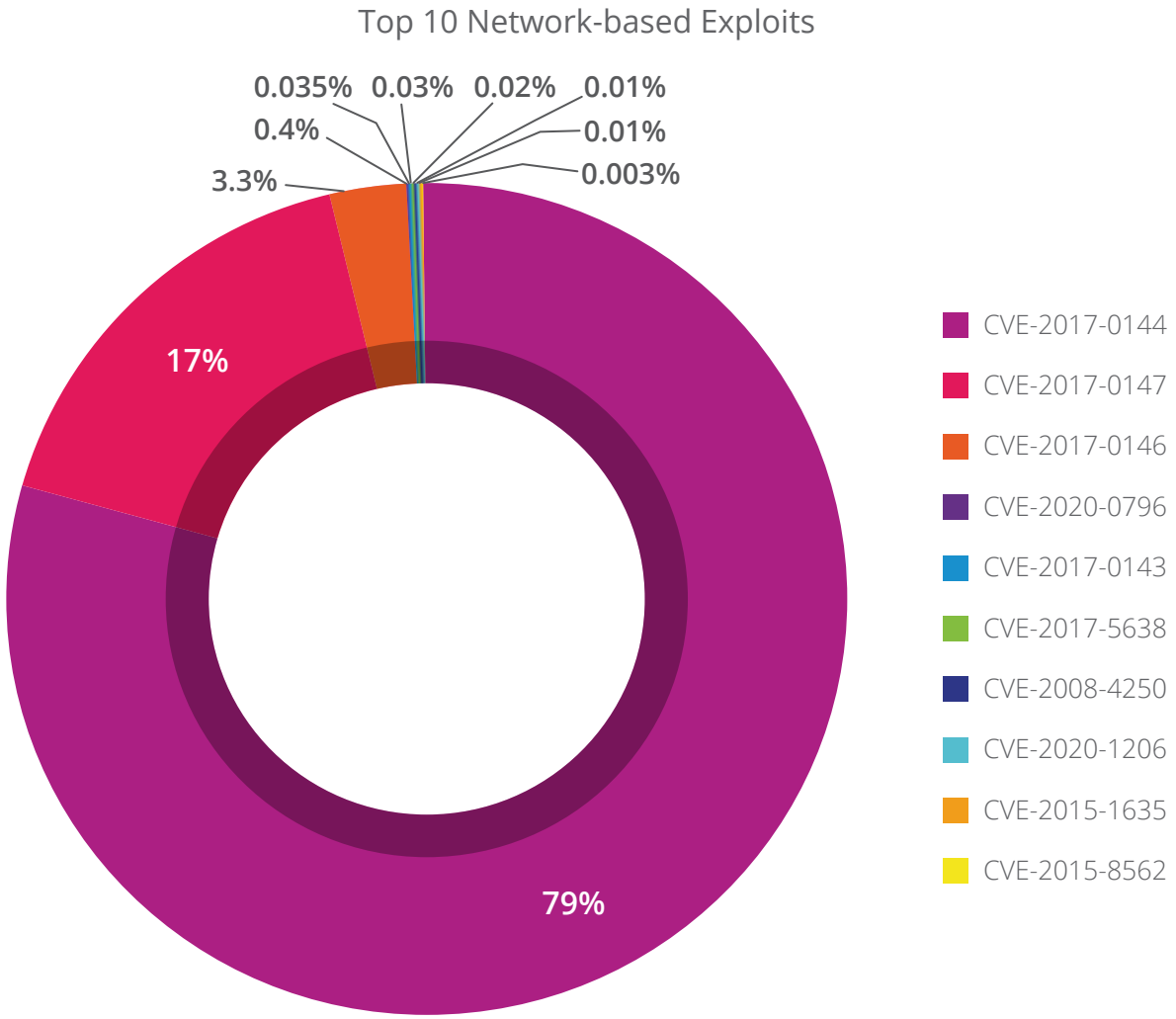
What are host-based exploits?
Host-based exploits are those that target security vulnerabilities found in host-based applications (host is a computer or other device connected to a computer network). These exploits are detected by endpoint detection modules such as Virus Protection, Email Protection,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

Observation

- LNK.Cmd.Exploit.F was detected to be the top host-based exploit, with around 0.09 million detections made in Q2 2020.

Top 10 Network-Based Exploits

Below figure represents the top 10 Network-Based Windows exploits of Q2 2020.



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 network-based exploit, with around 55 million detections made in Q2 2020.

Trends in Windows Security Threats

01

Zloader Riding high on Excel 4.0 Macro Wave

In the last few months, Quick Heal lab has observed that Excel macro 4.0 is widely used by attackers in malspam campaigns to distribute Zloader malware. After successful execution of the macro, Zloader payload is downloaded which performs infostealer activities on the victim's machine.

02

New Update in TrickBot

TrickBot has been present in the threat landscape for a long time and has been very dynamic in nature. It keeps updating new functionalities and manages to evade AV products

The infection vector for TrickBot is mostly a phishing/spam mail, which tricks the user into downloading the initial payload.

Recently, few of these included fake COVID-19 phishing and fake Black Lives Matter campaigns.

Over the years, Trickbot has proved to be an effective distributor for multiple malware including Ryuk ransomware.

03

Corona-Themed Malspam on a rise

Cyber-criminals are taking advantage of COVID-19 pandemic for spreading malware and infecting users to steal victim's data. We have found cases where there are different initial attack vectors and varying payload getting delivered.

Case 1

The attacker sends a document file as an initial attack vector containing exploits like CVE-2017-8570 and CVE-2017-11882. When the user opens this document, a .NET payload is dropped which further injects Agent Tesla in Windows Native process to collect data from victim's machines.

Case 2

Attacker sends a compressed archive as an e-mail attachment. The archive contains a malicious file having a double extension (for ex. COVID19.pdf.exe, COVID-19 Supplier Notice.jpg.exe). When the user clicks on the attachment, it gets downloaded and extracted in some folder.

Case 3

The victim receives a compressed zip file containing a malicious JAR file. When the user executes the Jar file, it self-extracts again and drops another .jar file in %appdata% location.

Case 4

The victim receives a macro enabled PowerPoint presentation which spawns mshta.exe to download malicious HTA script from “pastebin.com”.

The final motive of all campaigns mentioned above is to steal data and get sensitive information from the user or sell the stolen data in Dark Web.

04 Emergence of new SMB exploits

Vulnerabilities in network protocols like SMB and RDP are critical in nature since they can allow an attacker to take remote control of the victim’s machine or crash any system in the network.

Multiple critical SMB protocol vulnerabilities have been patched recently by Microsoft. SMBGhost, SMBleed and SMBLost are some of the named SMB vulnerabilities which have surfaced since March 2020 for which exploits or PoCs are also available in public.

In the past, publicly available SMB exploits like Eternalblue and MS08_067_NETAPI have been used for many years by worms for lateral movement. The new exploits are not of that high severity as compared to Eternal exploits since the vulnerabilities do not apply to all versions of Windows. But it can still cause a high impact on the production systems vulnerable to any of these exploits.

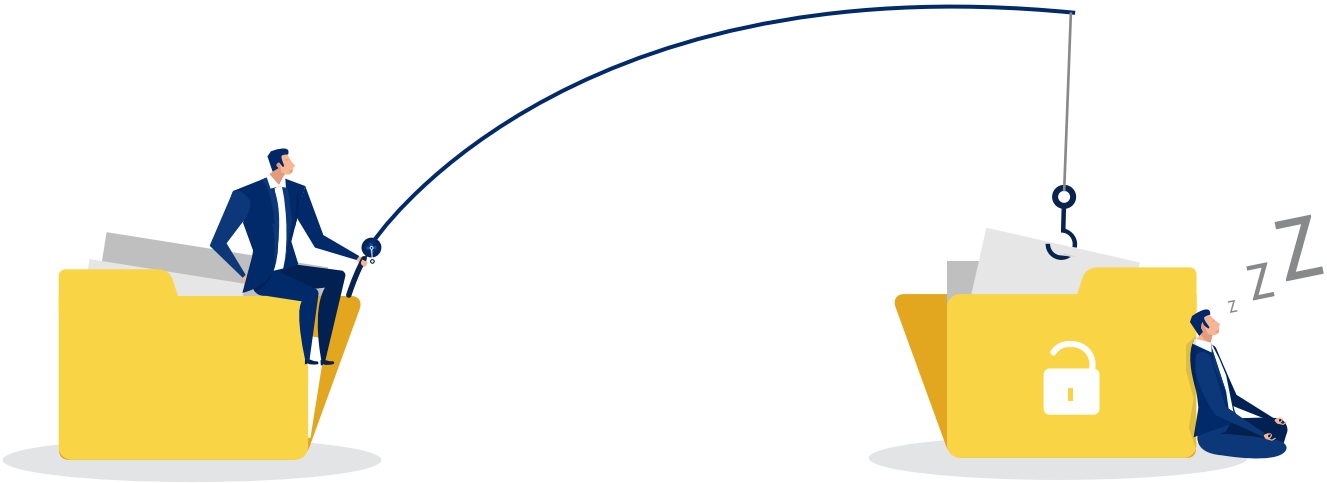
All Quick Heal customers are protected against attacks exploiting these vulnerabilities through our IPS rules. To keep their hosts secure, we urge all our customers to keep your Quick Heal product’s virus definitions up-to-date. Additionally, as per the best practices, apply Microsoft’s official patches as early as possible.

05 Poulight- An info-stealing trojan might be teaching you how to play Minecraft

Poulight is an info-stealer trojan which most probably originated in Russia. It is written in the .NET. It can collect various sensitive information and deliver it to cybercriminals. Ever since it’s the first appearance, it has been growing and taking different forms. The main infection vector remains spear-phishing emails.

- It begins with a doc file named “Minecraft how to play guide.docm”, which is a Microsoft word file.
- This file contains an image of the Minecraft game along with some abusive Russian text. This word file contains macro code, which is executed automatically if macros are enabled.
- The macro acts as a downloader and uses powershell to download exe file, which is the loader for Poulight.

In the future, it has the potential to become a sophisticated and infamous stealer looking at the rate of growth. However, for now, it lacks the obfuscation and any novelty in its code.



Read more here:
https://blogs.quickheal.com/poulight-info-stealer-might-teaching-play-minecraft/

06

A New Era in Ransomware

Ransomware has evolved from being a simple screen locker to an advanced file infector which encrypts user's important files and mapped network drives. Ransomware authors always update their TTPs to attack a large number of systems and gain maximum benefit.

Essentially, they evolve in two directions,

- One uses different encryption techniques and
- Others use different attack vectors to encrypt a large number of systems.

We have listed down few attack techniques which are used in recent malware attacks worldwide.

1 **WoL (Wake on Lan) in Ryuk Ransomware**
Wake on Lan (WoL) is a hardware feature that allows a computer to be turned ON or awakened by a network packet.

2 **Process Hollowing in Mailto aka Netwalker Ransomware**
The Mailto or Netwalker performs process hollowing in explorer.exe — this helps in evading the Anti-Virus software (AVs) to easily perform the encryption.

3 **Exploiting Vulnerabilities in System/Products i.e. CVE-2020-0601 By HorseDeal Ransomware, CVE-2018-19320, Gigabyte by Robinhood Ransomware**

It is a spoofing vulnerability in Windows CryptoAPI (Crypt32.dll) validation mechanism for Elliptic Curve Cryptography (ECC) certificates. HorseDeal leveraged this vulnerability by making use of a spoofed ECC certificate to evade detections.

Refer to:
https://blogs.quickheal.com/horsedeal-riding-curveball/

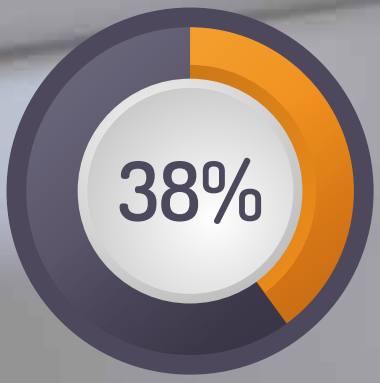
4 **RagnarLocker Ransomware Hides in Virtual Machine**

Threat actors developed a new type of ransomware attack that uses virtual machines. It was observed that this variant was deployed inside a Windows XP virtual machine to hide the malicious code from security products. Since ransomware application runs inside the virtual guest machine, its processes and behaviour can run unhindered, because they are out of the reach of security software on the physical host machine.

5 **PonyFinal and Tycoon Ransomware used JAVA as the language/file format for Encryption**

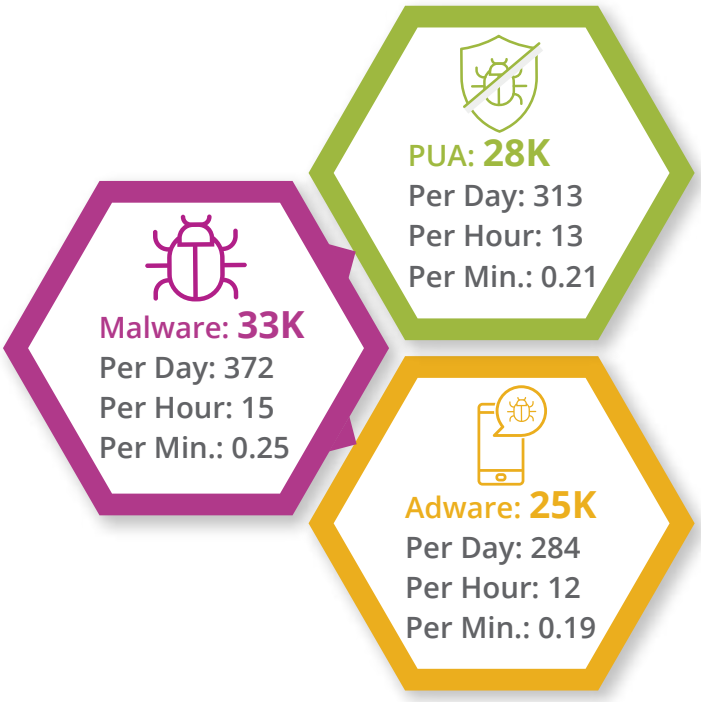
PonyFinal is Java-based ransomware which requires JRE (Java Run-Time Environment) in the system. It specifically targets enterprise organizations as JRE is available in most of the systems.

Android



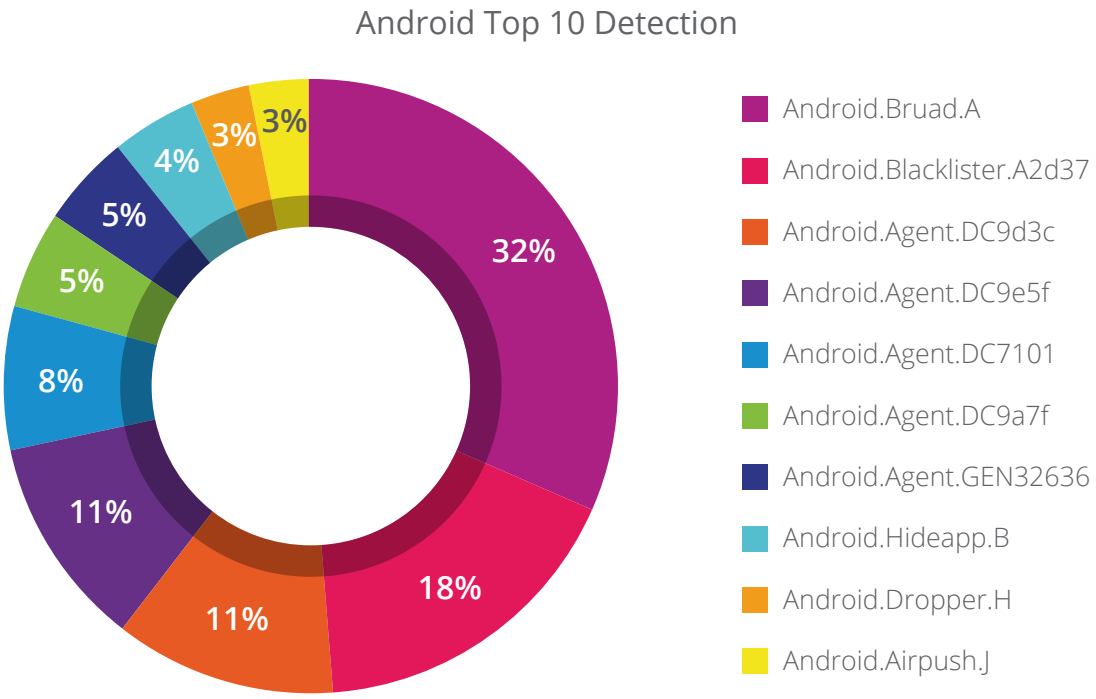
Of total Android detection in Q2 2020 was Malware

Quick Heal Detection on Android for Q2 2020



Top 10 Android Malware for Q2 2020

Below figure represents the top 10 Android malware of Q2 2020. These malware have made it to this list based upon their rate of detection across the year.



01

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

Behaviour:

- Hides its icon after installation
- Connects to advertisement URLs and sends the infected device's information such as IMEI, IMSI, model number and location to a remote server

02

Android.Blacklister.A2d37
Threat Level: Medium
Category: Adware
Method of Propagation: Google Play app store

Behaviour:

- These apps mimic the functionalities of an Antivirus 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

03

Android.Agent.DC9d3c
Threat Level: High
Category: Adware
Method of Propagation: Third-party app stores and repacked apps

Behaviour:

- Makes use of SDK to easily recompile other genuine apps.
- Downloads other apps on the device causing unnecessary memory usage.
- Shares device information such as location and email account with a remote server.
- Displays unnecessary advertisements.

04

Android.Agent.DC9e5f
Threat Level: Medium
Category: Potentially Unwanted Application (PUA)
Method of Propagation: Google Play app store

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 sends to server.
- All data shared to server without encryption.

05

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 string to decrypt payload for further malicious activity.

06

Android.Agent.DC9a7f
Threat Level: High
Category: Malware
Method of Propagation: Third-party app stores

Behaviour:

- It is from Trojan-Downloader family
- It collects device details like country code, model, IMEI, SIM details, phone number, installed packages list, running process info etc.
- It collects contact list, call logs, SMS data and send all collected information to C&C server.
- It downloads malicious application and install it

07

Android.Agent.GEN32636
Threat Level: High
Category: Malware
Method of Propagation: Third-party app stores

Behaviour:

- It mimics legitimate app or system app.
- It hides its icon on the first launch
- Runs services in the background and shows full screen advertisements.
- To evade detections it carries encrypted malicious files in asset directory.
- At runtime it decrypts this file and loads malicious code to perform malicious activity.

08

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

Behaviour:

- It hides its icon on the first launch
- Shows message like 'Application is unavailable in your country'
- Runs services in the background and shows Fullscreen advertisements
- It collects device information like Country code, IMEI, phone number etc
- It then sends collected information in an encrypted format to a remote server

08

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

Behaviour:

- It is a Trojan-Dropper
- It looks like a legitimate application such as settings or messaging
- During its first launch, it hides its presence and loads encrypted payload from its resources folder
- Encrypted payload has advertised SDK which shows fullscreen advertisement

10

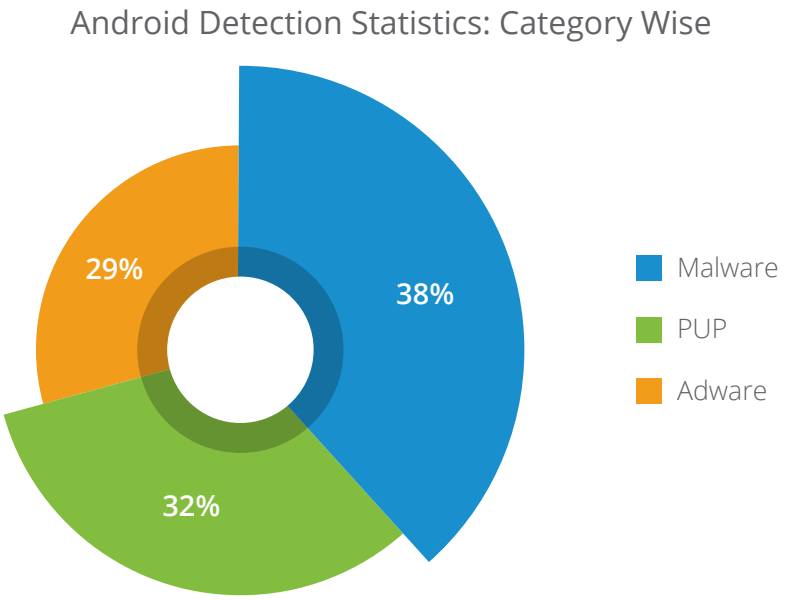
Android.Airpush.J
Threat Level: Low
Category: Adware
Method of Propagation: Third-party app stores and repacked apps

Behaviour:

- Displays multiple ads while it is running
- When 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

Android Detection Statistics: Category Wise

Below figure represents the various categories of Android malware detected by Quick Heal in Q2 2020.

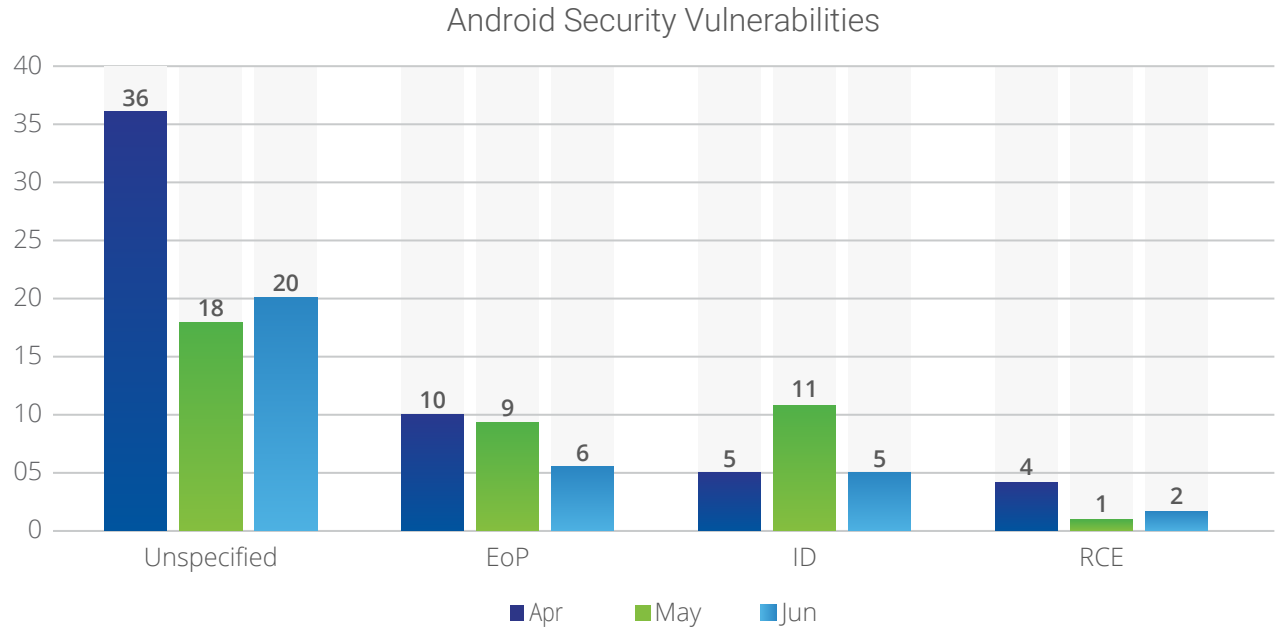


Observation

- Malware clocked 38% of the total Android detections in Q2 2020.

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 of 2020.



Trends in Android Security Threats

01

Fake Aarogya Setu Applications:

Malware authors are misusing the name 'Aarogya Setu' to plant malicious apps into the end users' phone. Quick heal mobile security team collected many applications from various sources that impersonate the original Aarogya Setu App. While analyzing these applications, we found some malicious applications that looked exactly like the official app. All the samples that we have are modified versions of previously found malware with few minor changes done to give a look like the Aarogya Setu App.

Quick heal security lab have published a detailed blog on this - https://blogs.quickheal.com/sure-right-aarogya-setu-app-phone/

02

Eventbot – A new banking trojan:

Eventbot malware is a mobile Trojan that steals private and valuable information from mobile banking and financial apps in Android. It hacks into Android's in-built accessibility features and steals data by reading into SMSs, banking PINs, etc. and bypasses the two-factor authentication criteria that most banking apps have.

Quick heal security lab have published advisory blog on this - https://blogs.quickheal.com/eventbot-malware-need-know-new-mobile-banking-trojan/

03

Scams during this crucial time of CoronaVirus pandemic:

Due to the lockdown, people are spending more time on their mobile phones and laptops. Fraudsters are taking advantage of this situation. You may have seen messages offering free data, free subscriptions with some link mentioned. These types of links can be malware spreading vectors.

Quick heal mobile security team analyzed one of the links. The messages offered free Netflix subscription with domain netflix-usa[.]net. The link opens a page asking to share the same message with Ad pop ups. This message was used to generate traffic for particular site.

Another case Quick heal mobile security team came across is fake UPI ID of PM Care fund. Fraudsters registered Fake UPI ID 'pncare@sbi' which is similar to real PM Care fund UPI ID "pmcares@sbi" to disguise people and earn money.

Quick heal security lab have published detailed blog on these topic - https://blogs.quickheal.com/beware-scams-crucial-time-coronavirus-pandemic/

Inference

Cyber attackers are taking advantage of the vulnerable state of affairs that we all are exposed to during the coronavirus pandemic. It has opened a plethora of avenues for the attackers to plan and deploy attacks targeting individual users given the fact that the dependence on online activities is on an all-time high. There have been attacks through fake apps, online games, banking and shopping apps, OTT subscription platforms among others. There's no respite. It's predicted that these attacks might be on an upward graph as we try to get out of the pandemic.

Other than keeping ourselves safe as users we should also take preventative measures such as -

1. Being extremely careful in their interactions with elements related to the Coronavirus.
2. Keeping our device software and cybersecurity solution up-to-date
3. Practicing caution when downloading new applications from Third-Party App Stores
4. Reporting suspicious activities to the support functions of their cybersecurity vendors
5. Checking emails with an extreme vigil as to not open attachments from unverified sources

We detected more than 5k ransomware threats per day in this quarter too. It is advisable for you as a user to proactively back up all your sensitive and important data in a separate storage device.

We also noticed that maximum malware detections were made through Web Security Scan, which automatically detects unsafe and potentially dangerous websites and prevents you from visiting them. You must be aware of malicious and dangerous websites and never visit them.

Trojan malware was found to clock the maximum detection at 51% in Q2 2020 and W32.Pioneer.CZ1 was detected to be the top Windows Malware, with 10 Million+ detections.

We detected 33k malware in Android, which forms 38% of the total Android detections in Q2 2020.

We are continuing our efforts of finding fake applications on the Play Store and reporting it to Google. We are actively publishing a lot of content on several platforms about all that we are doing to uphold cybersecurity for our customers during dark times in the world.

Trojan malware was found to clock the maximum detection

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