Quick Heal

Security Simplified

QUICK HEAL
THREAT REPORT
Q3-2020

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

As we look back at the third quarter of 2020, we witness that cyberattacks are on a continuous rise. Compared to the Q2 2020 threat report, we have detected approximately 70 million more malware in Windows. This speaks a lot of the current state of affairs in the cybersecurity landscape.

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

The report has the details of top malware in both Windows and Android and extensively discusses the top trends in cyberattacks.

WINDOWS

213
Million
Windows Malware detected in the Q3

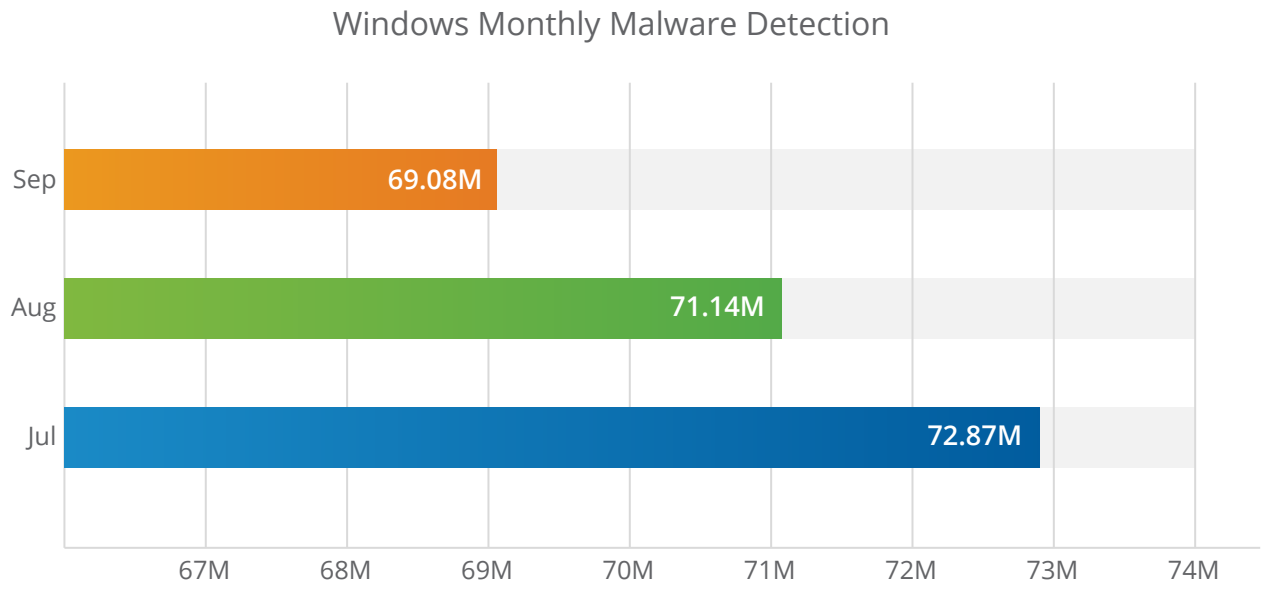
72.8
Million
Windows Malware detected in July '20

2.3
Million
Malware detected daily in Q3

Windows Detection Statistics Q3 2020

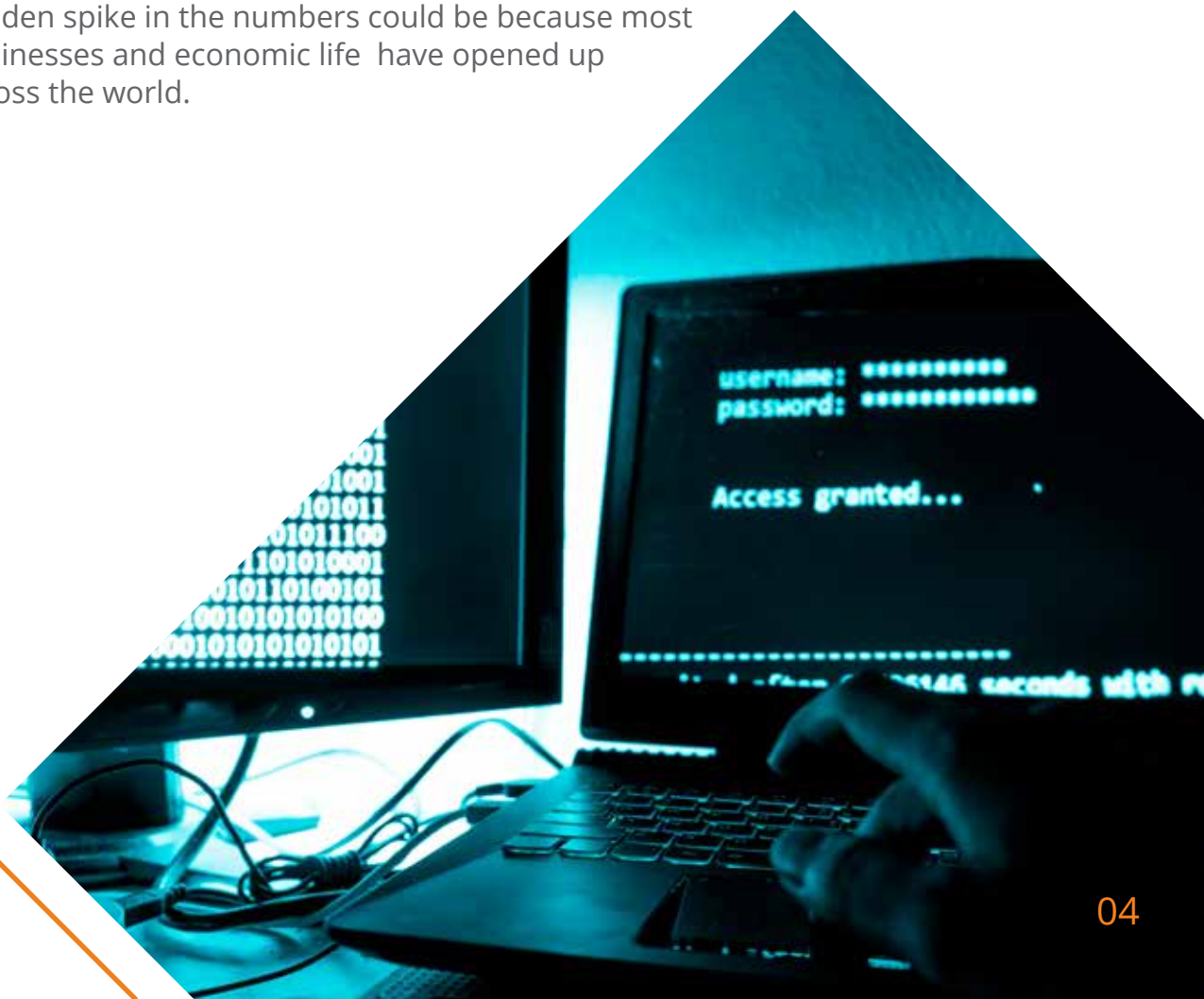
Detection Statistics – Month Wise Q3 2020

The below graph represents the statistics of the total count of Malware detected by Quick Heal from July to September 2020.

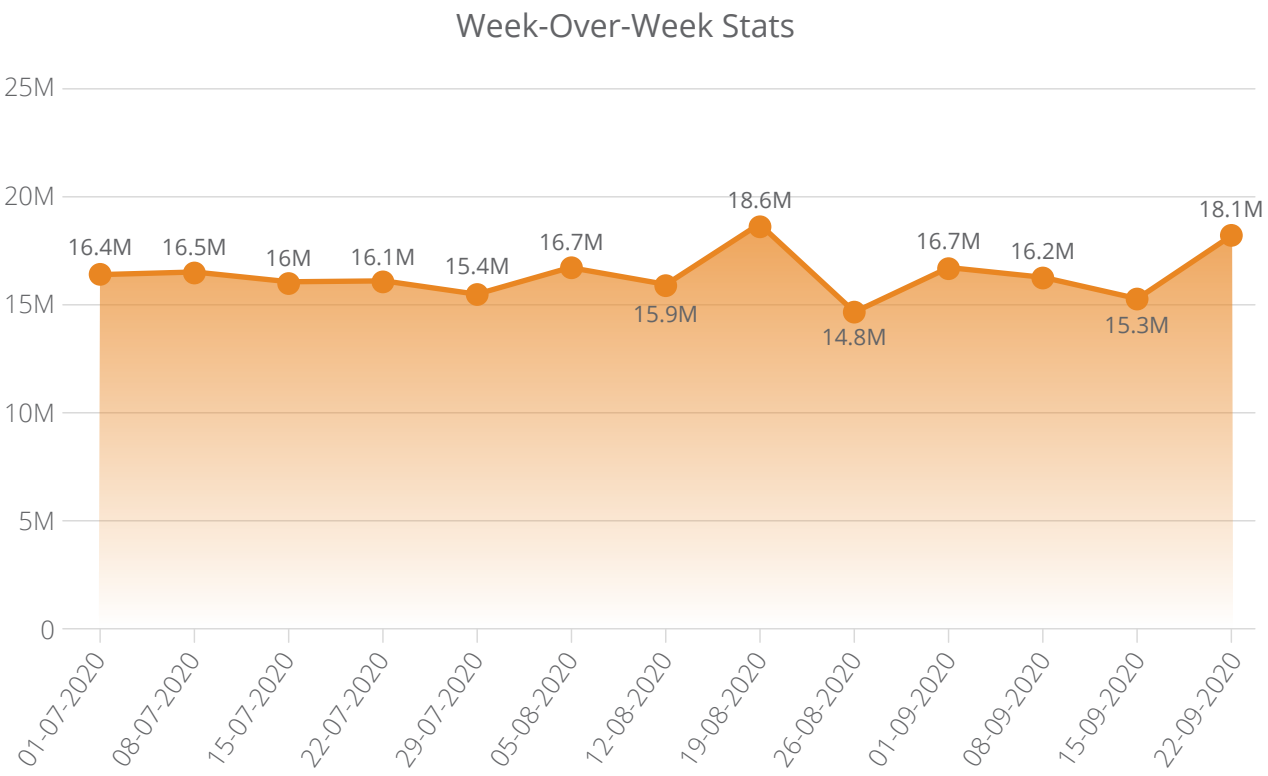


Observations

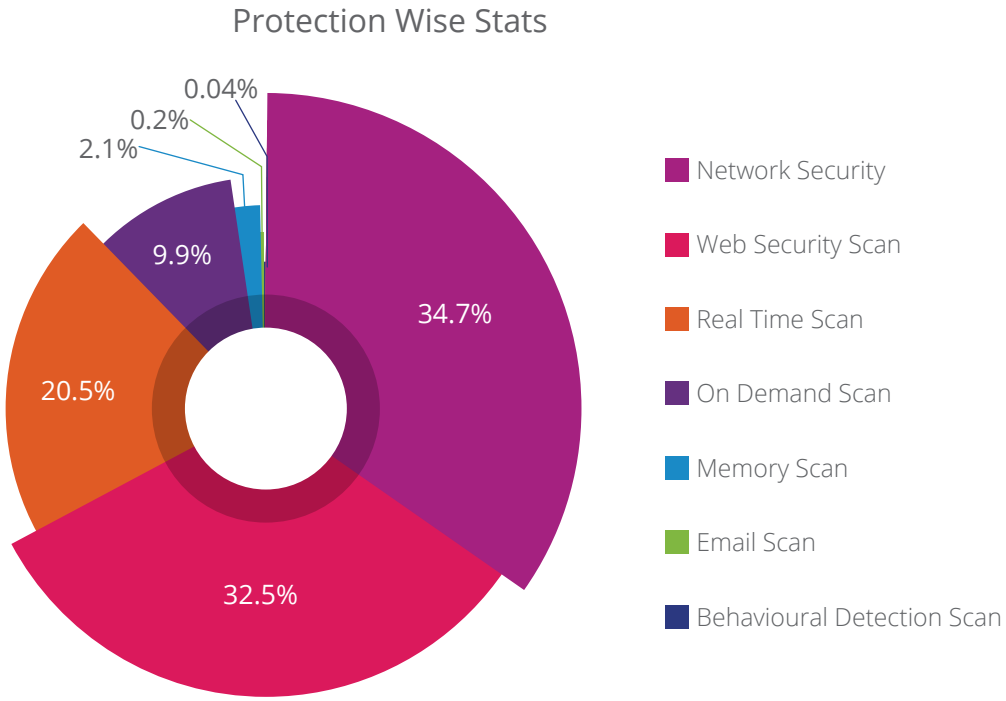
- Quick Heal detected over 213 Million Windows malware in Q3 2020.
- July clocked the highest detection of Windows malware. The reason for the sudden spike in the numbers could be because most businesses and economic life have opened up across the world.



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.

Here is a brief about the different kind so protection scans and what each one of them does:

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.

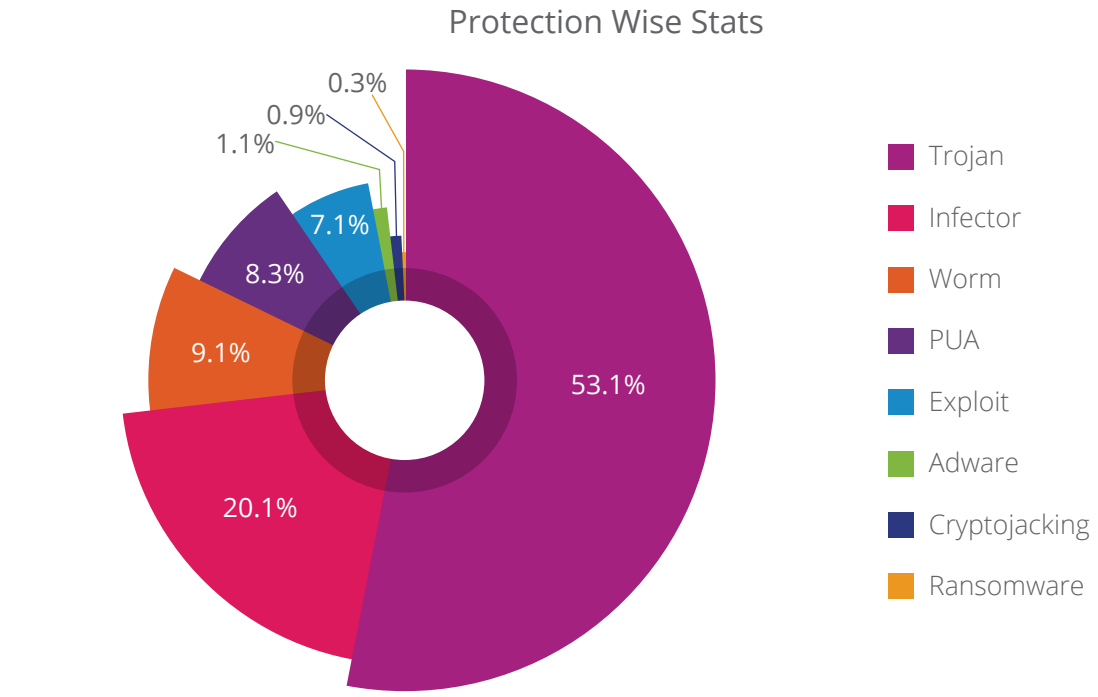
Email Scan
Blocks emails that carry infected attachments or links to compromised or fake and phishing websites.

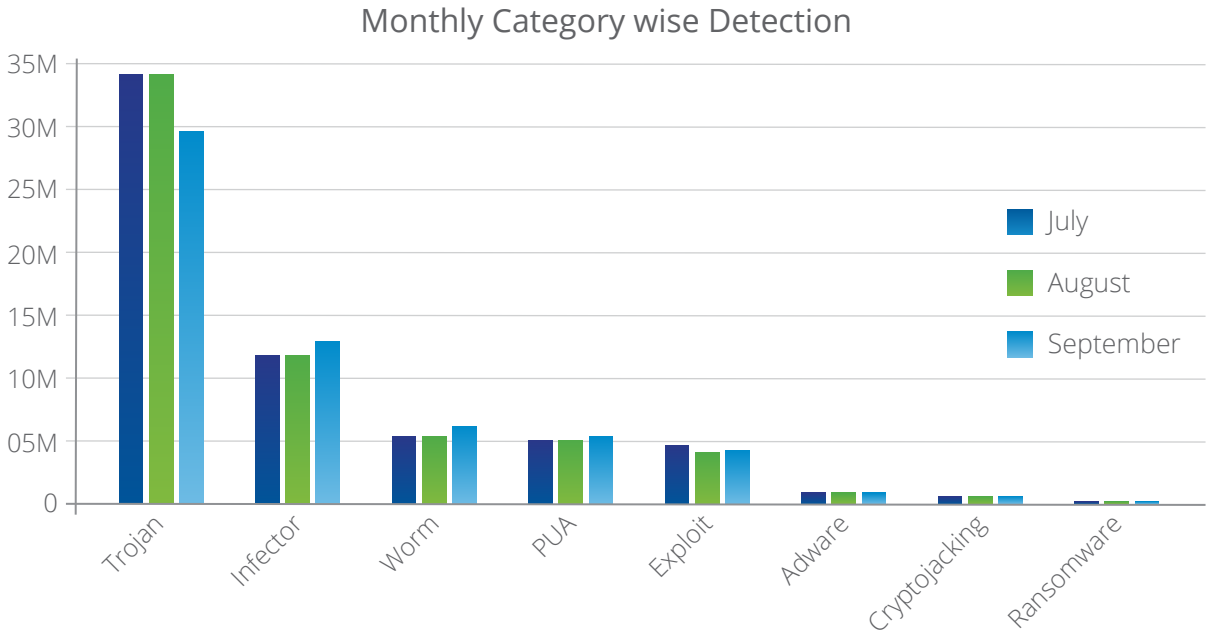
Web Security Scan
Automatically detects unsafe and potentially dangerous websites and prevents you from visiting them.

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 Q3 2020





What is a Trojan?

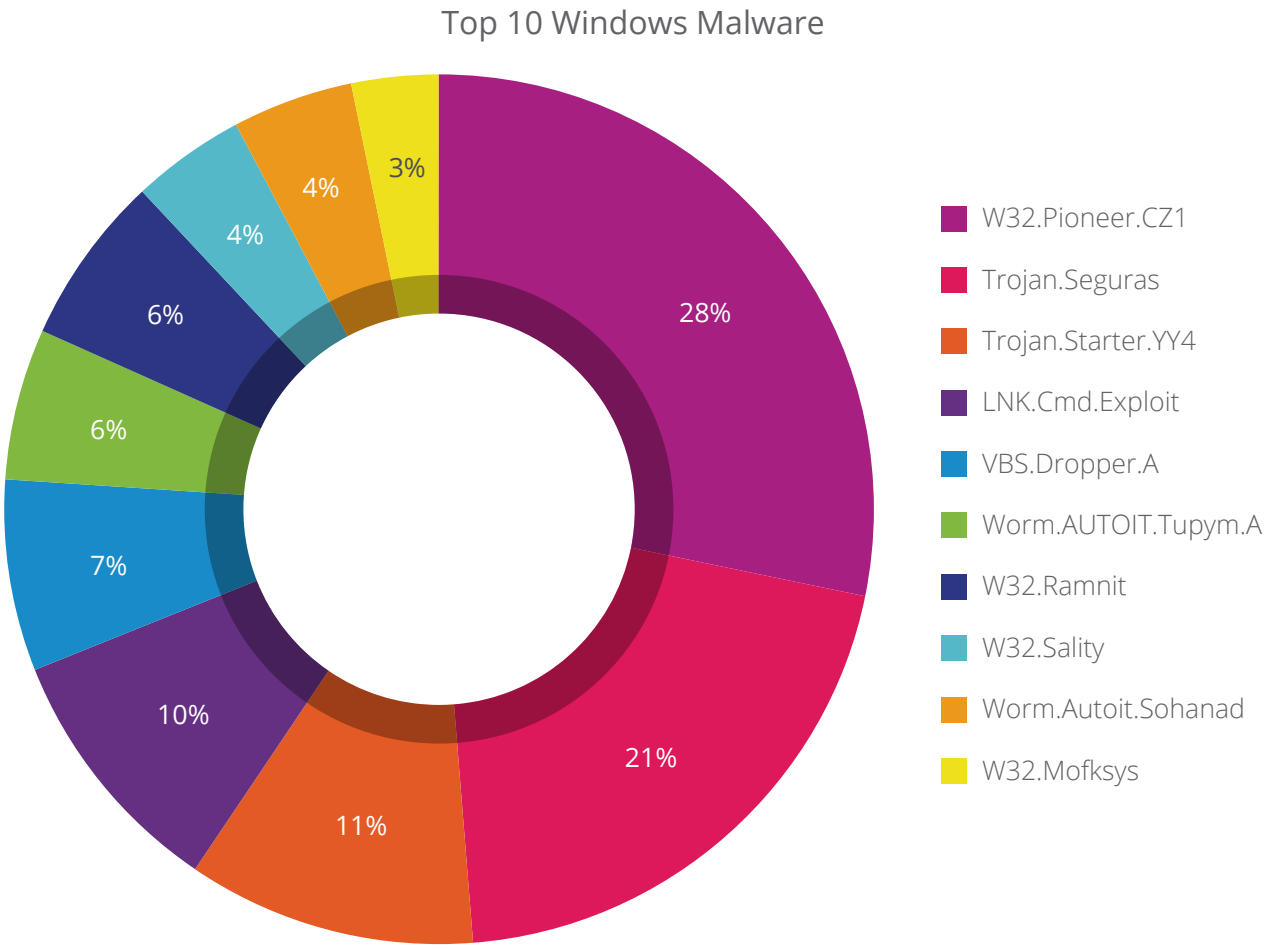
A Trojan horse or simply a Trojan is a malware that misleads users about its true intent. It disguises itself as legitimate software and fools the user to take an action.

Observation

- Trojan malware was found to clock the maximum detection at 52% in Q3 2020.

Top 10 Windows Malware

The below figure represents the Top 10 Windows malware of Q3 2020. These malware have made it to this list based upon their rate of detection from July to September.



Windows Top 10 Threat 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 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.Seguras

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

Behaviour:

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

03

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

04

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.

05

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.

06

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

07

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.

08

W32.Sality

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

09

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.

10

W32.Mofksys
Threat Level: High
Category: Worm
Method of Propagation: Removable or network drives

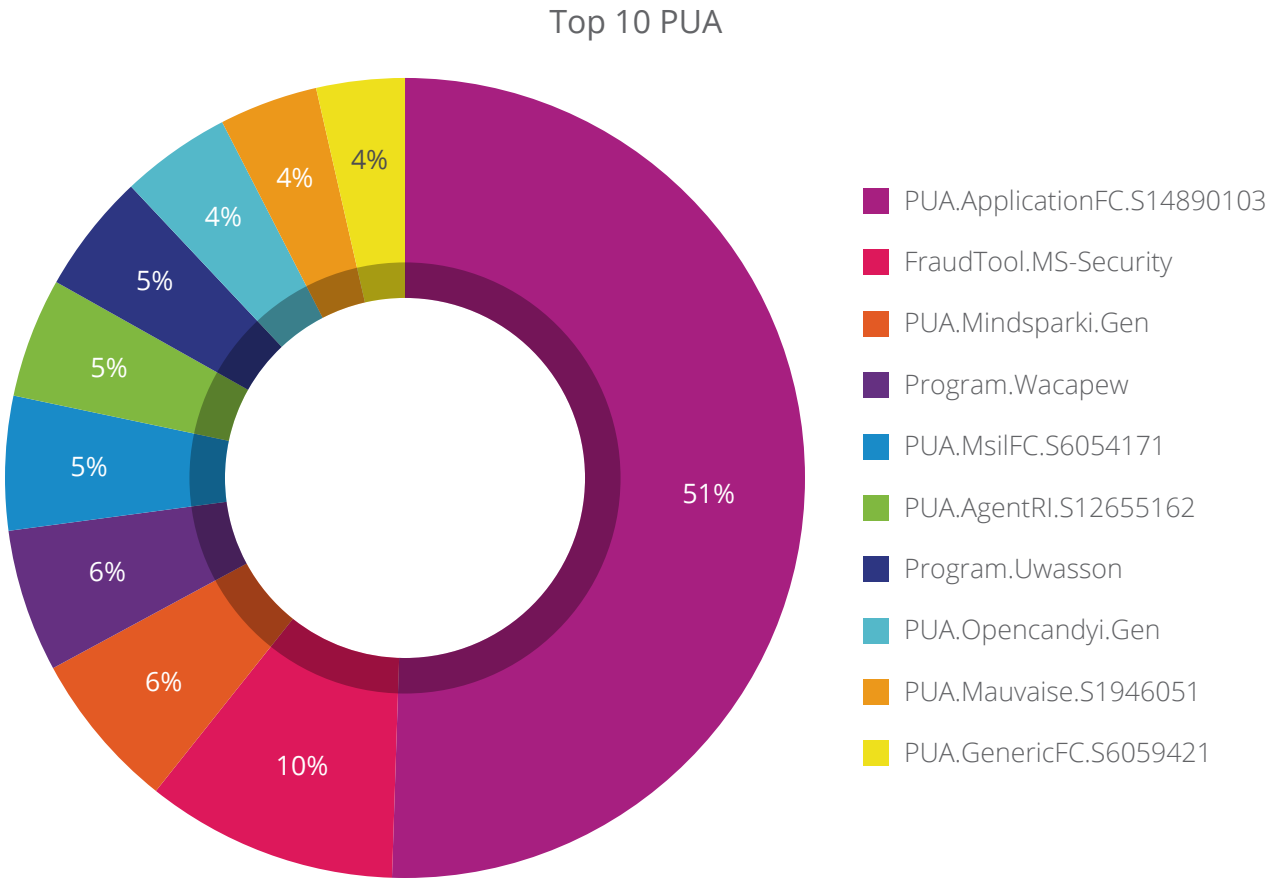
Behaviour:

- 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.

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 Q3 2020.

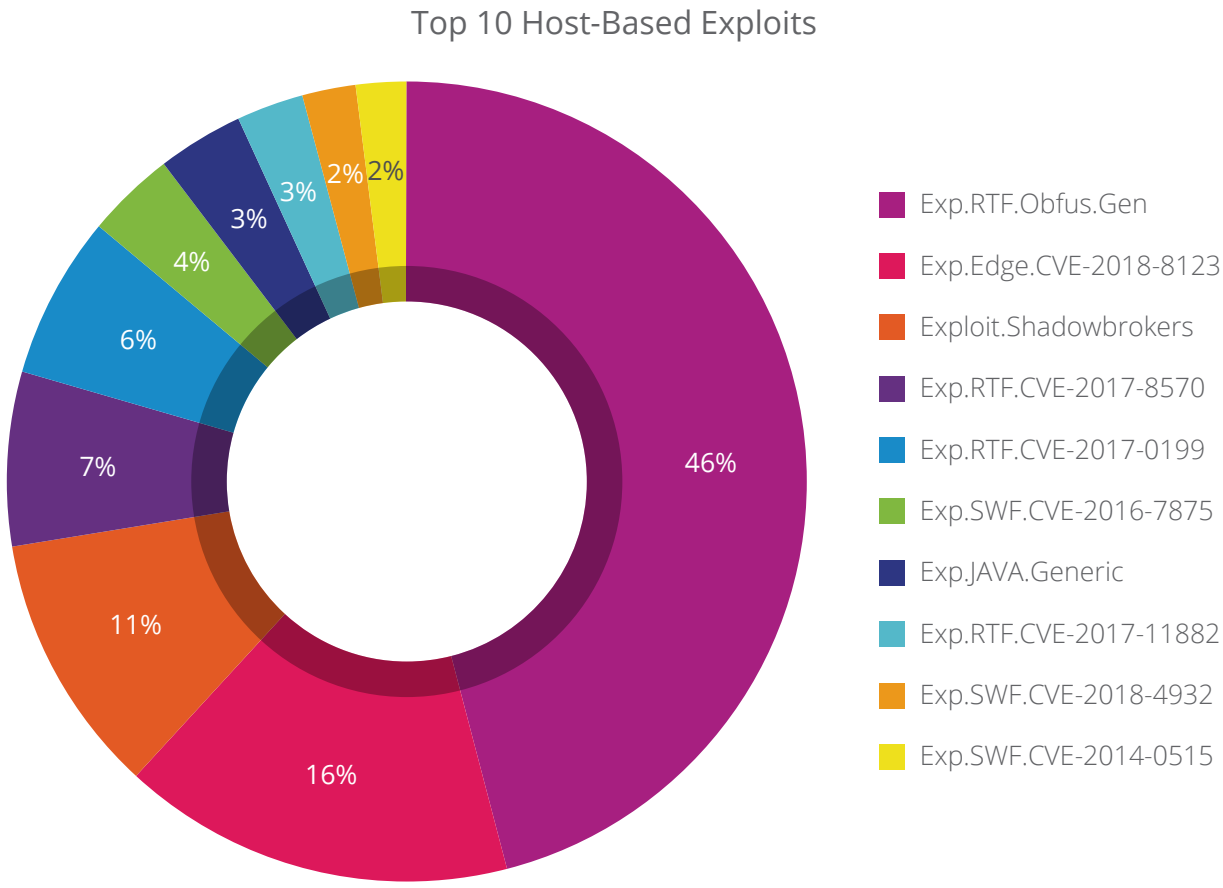


Observation

- PUA.ApplicationFC.S14890103 was detected to be the top PUA, with around 01.7 Million detections made in Q3 2020.

Top 10 Host-Based Exploits

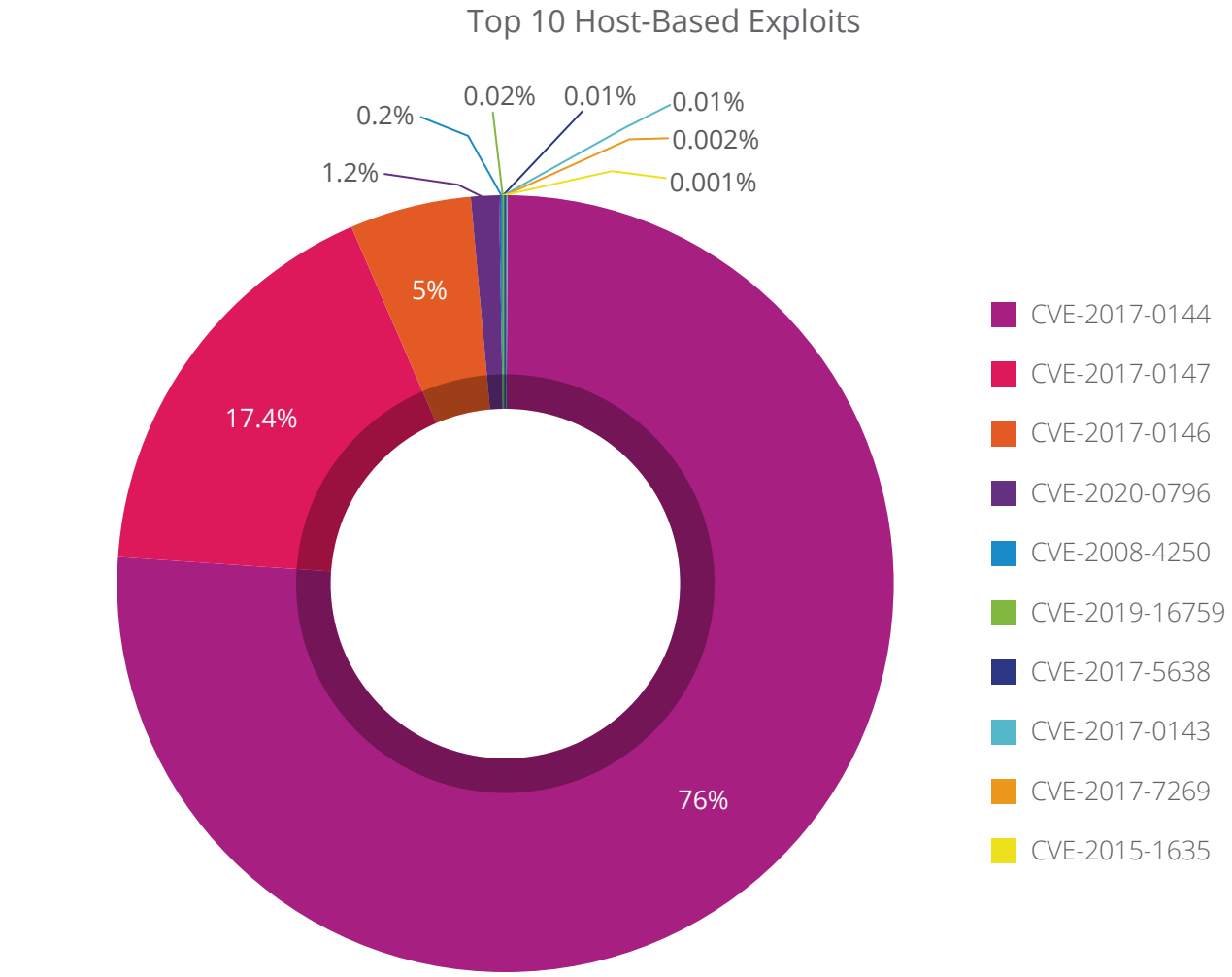
An exploit is a piece of code or crafted data that takes advantage of a bug or vulnerability in the targeted system or an application running on it.



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.

Top 10 Network-Based Exploits

Below figure represents the top 10 Network-Based Windows exploits of Q3 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 host-based exploit, with around 104 million detections made in Q3 2020.

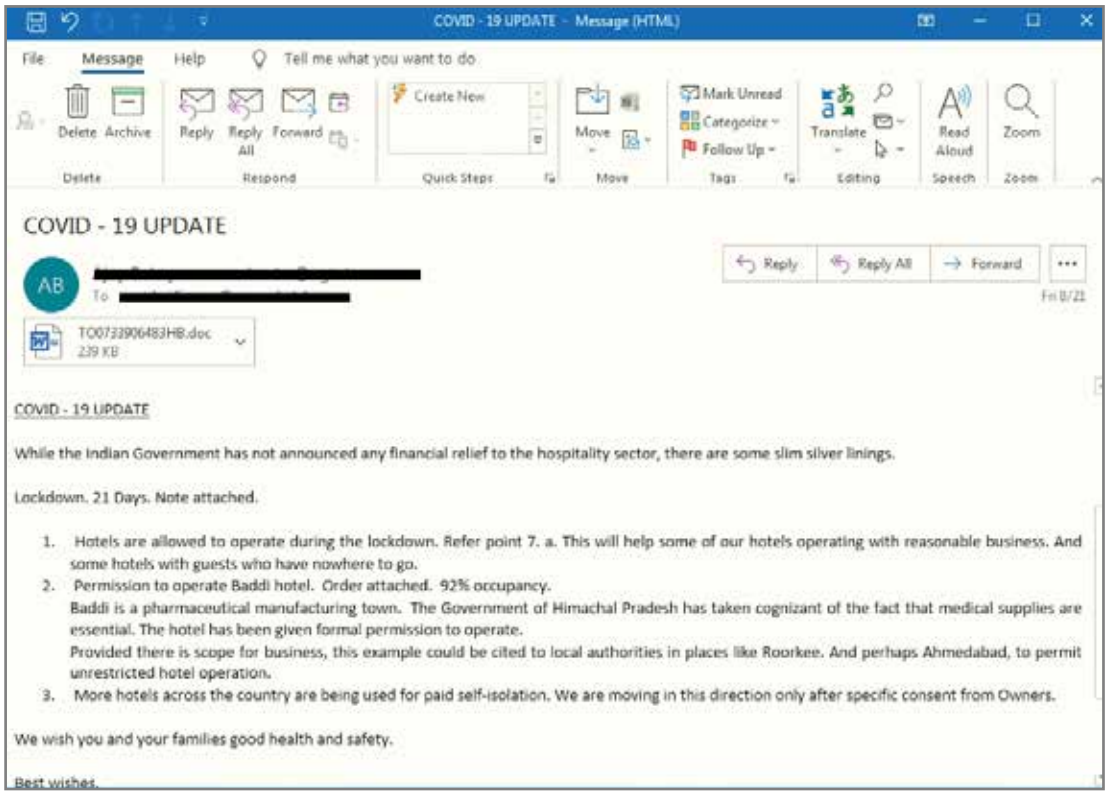
Trends in Windows Security Threats

01 RIPlace in the field with Thanos Ransomware

The new RIPlace tactic has shown its appearance in Thanos Ransomware. It has the potential to maliciously hamper the files without getting identified by the anti-ransomware techniques.

02 Emotet is Back After Unlock!

Emotet Trojan has been a persistent threat actor since long time and is considered highly successful in delivering malware through email. We encountered few Emotet campaigns with our detections triggered on customers from different sectors. Emotet campaign's infection chain starts by sending crafted emails with subject names having keywords like Vaccine for Covid-19, Health Insurance, Payment, Invoice, Job Update/Opening, Cyberattack, Shipping and many more. Here is an example of an Emotet email.



Quick Heal customers are protected from Emotet and COVID-19-themed emails. We are continuously monitoring and tracking such campaigns to protect our customers from persistent threats.

03 Critical Vulnerabilities in Windows Server OS

In last quarter, Microsoft patched two vulnerabilities - **CVE-2020-1350 [SIGRed]** and **CVE-2020-1472 [ZeroLogon]** with CVSS score 10 for Windows Server OS, making it mandatory for server administrators to install the latest updates. Updating the servers in an urgent basis is a tough task since it can cause downtime for organizations. It has been found that there are more than 50,000 Windows Server OS exposed to internet. If not patched, these can turn out to be easy target for attackers.

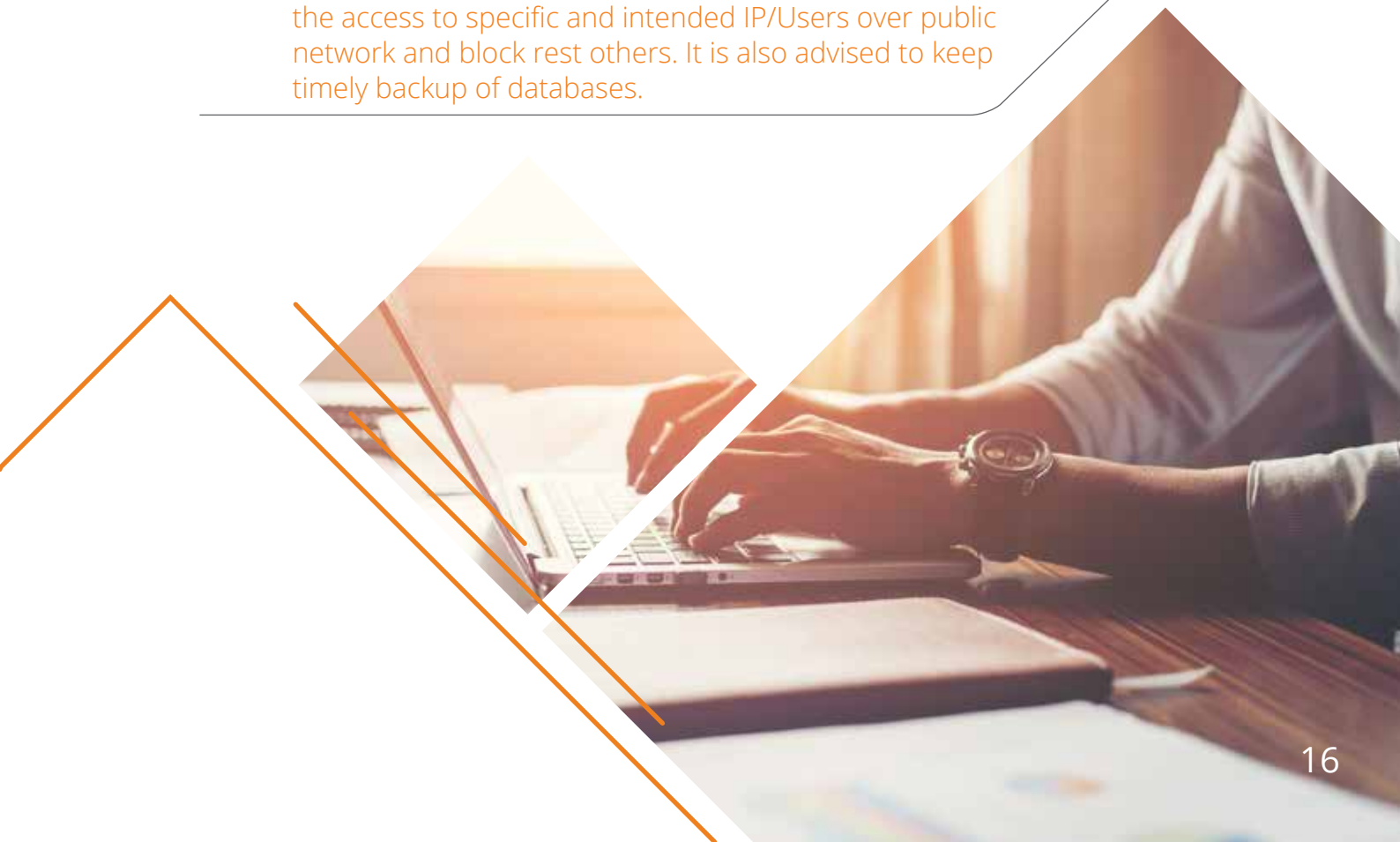
04 MassLogger: An Emerging Spyware and Keylogger

We have observed a new spyware in last quarter, named MassLogger. This advanced keylogger and spyware is distributed via MalSpam attachments and has more features than other present keylogger tools. It has been observed that this campaign is using several different file types as malicious attachments as an initial infection vector.

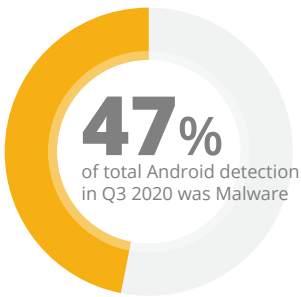
05 MSSQL Bruteforce Attack in the wild for profit

We have observed that attackers are using yet another way to breakthrough in system & make money, this time using MSSQL. Threat actors actively search for publicly open MSSQL servers and then attack them using brute force login attempts. Servers having weak password become easy target for the attacker. Once the attacker gains the system access, they install a cryptocurrency miner that eats up server resources to generate revenue for them.

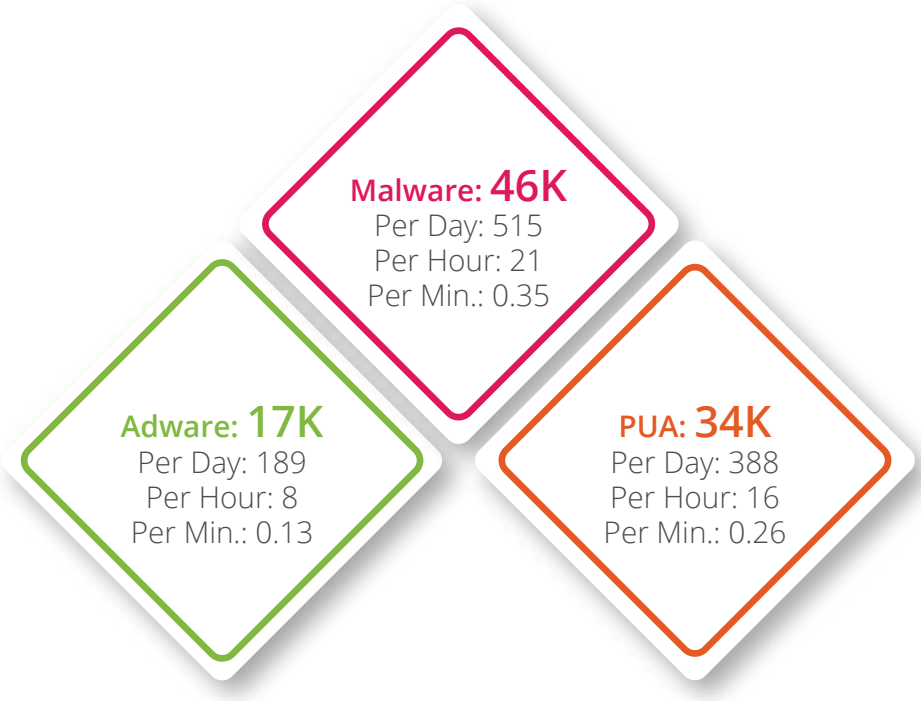
Quick Heal Security Labs recommends to secure SA account with a unique and complex password. It is also suggested to restrict the access to specific and intended IP/Users over public network and block rest others. It is also advised to keep timely backup of databases.



ANDROID

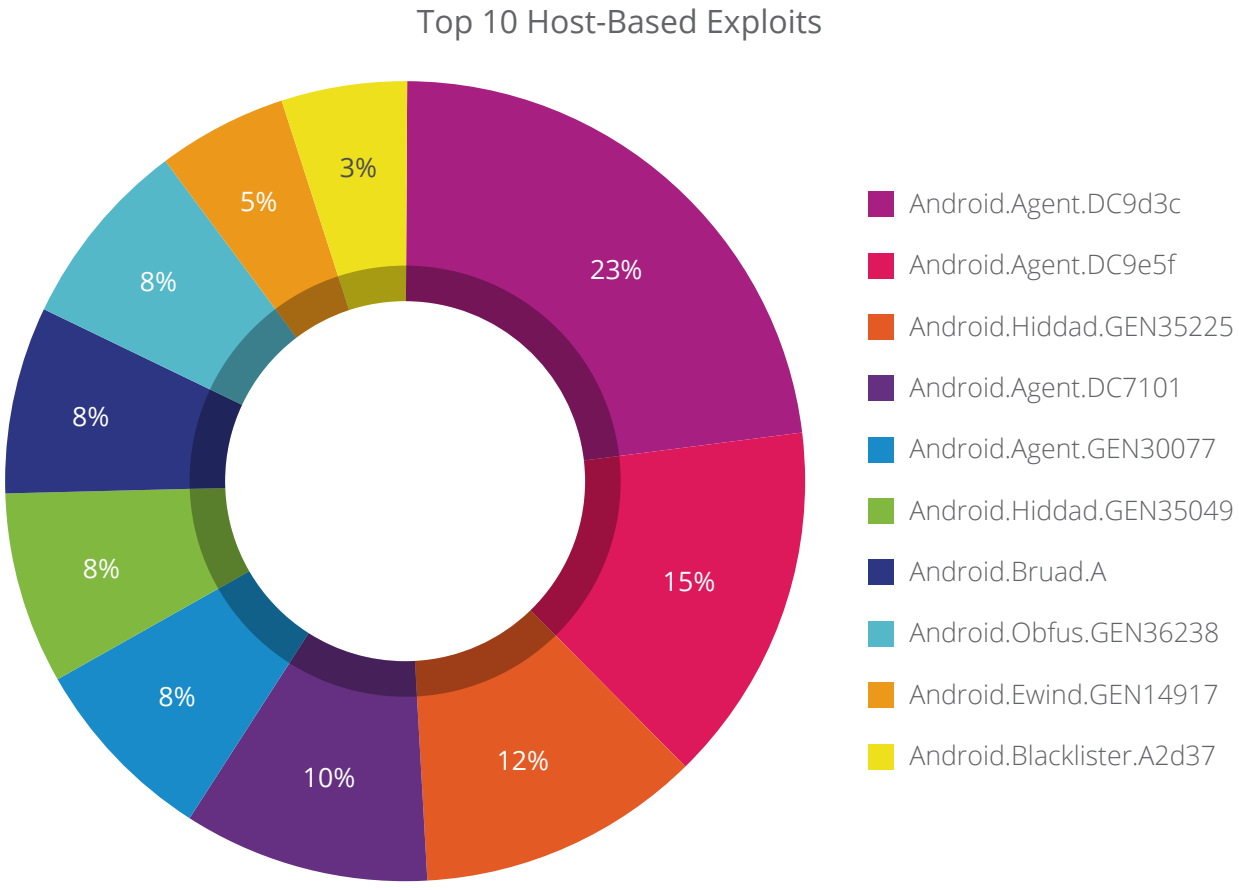


Quick Heal Detection on Android for Q3 2020



Top 10 Android Malware for Q3 2020

Below figure represents the top 10 Android Malware of Q3 2020. These malware have made it to this list based upon their rate of detection across the year.



Android Top 10 Threat Details

01

Android.Agent.DC9d3c
Threat Level: Medium
Category: Malware
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.

02

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.

03

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

Behaviour:

- It disguises as a genuine app. After launching, it hides its icon and runs in the background.
- This Trojan's activity is to visit the web pages in a hidden way and display advertisement that it receives from its C&C server.

04

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.

05

Android.Agent.GEN30077
Threat Level: High
Category: Malware
Method of Propagation: Google Play app store

Behaviour:

- This malware has a self-reinstall mechanism making it difficult to remove from the device.
- It can hide itself from users and download additional malicious apps and display advertisements,
- The malicious payload connects to the attacker's C&C server and waits for commands.
- To prevent this communication from being intercepted, SSL certificate pinning is used for all communication between the victim's device and the C&C server.
- Upon successful connection to the C&C server, additional payloads such as droppers, clickers, and rootkits, may be downloaded to the compromised device.

06

Android.Hiddad.GEN35049
Threat Level: High
Category: Malware
Method of Propagation: Third-party app stores

Behaviour:

- It successfully enters the user's phone by deceiving as a useful app.
- After first launch, it hides its icon and perform its malicious activity in the background.
- After hiding icon, it displays advertisement on user's device.

07

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

08

Android.Obfus.GEN36238
Threat Level: High
Category: Malware
Method of Propagation: Third-party app stores

Behaviour:

- This is from Trojan family.
- It uses obfuscation technique to make reverse engineering difficult.
- It decrypts the code at runtime to execute its malicious activities

09

Android.Ewind.GEN14917 (Adware)
Threat Level: Low
Category: Adware
Method of Propagation: Third-party app stores and repacked apps

Behaviour:

- It displays unwanted ads on the infected device.
- It decrypts the malicious file from the asset file.
- It collects device data like SDK version, brand, model, IMEI, screen height, time zone, etc.

10

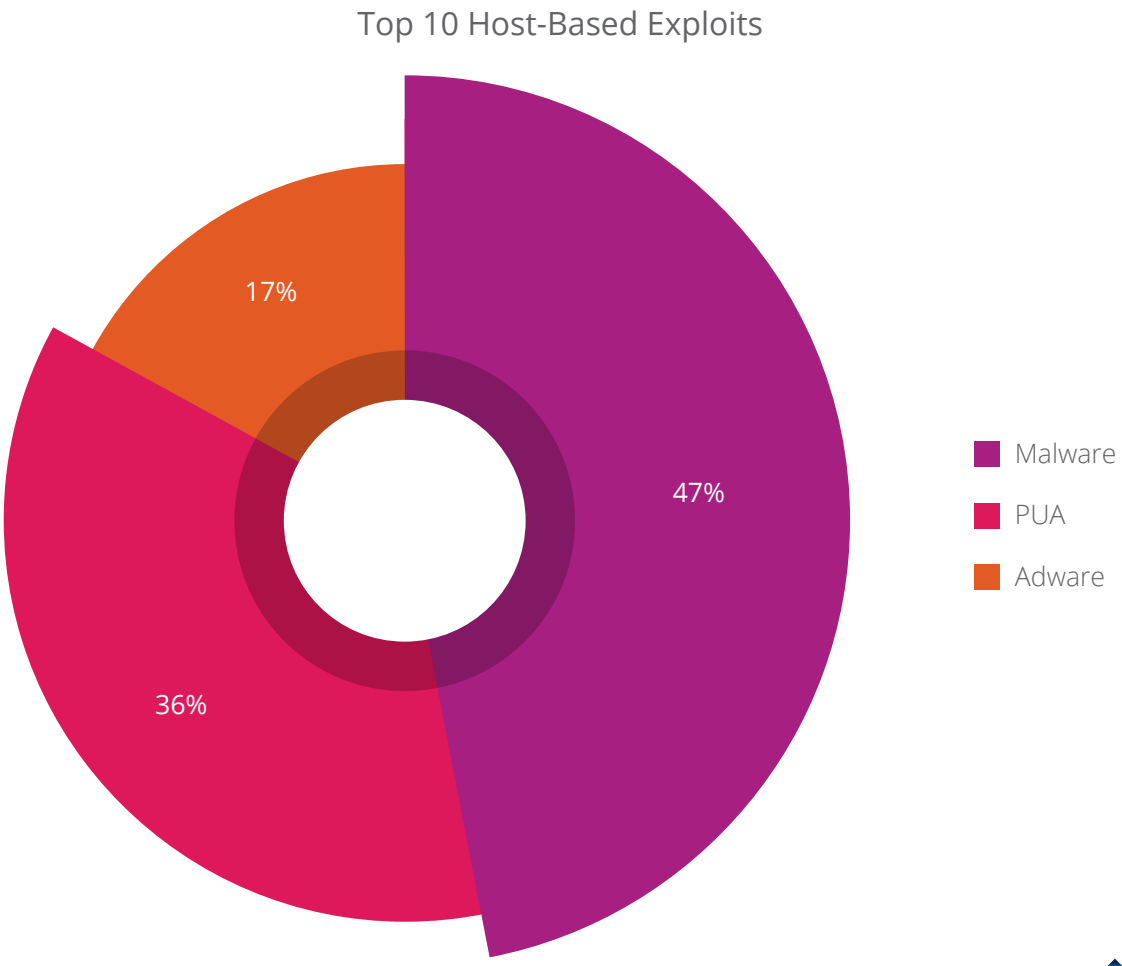
Android.Blacklister.A2d37
Threat Level: Medium
Category: Adware
Method of Propagation: Google Play app store

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

Android Detection Statistics: Category Wise

Below figure represents the various categories of Android malware detected by Quick Heal in Q3 2020.

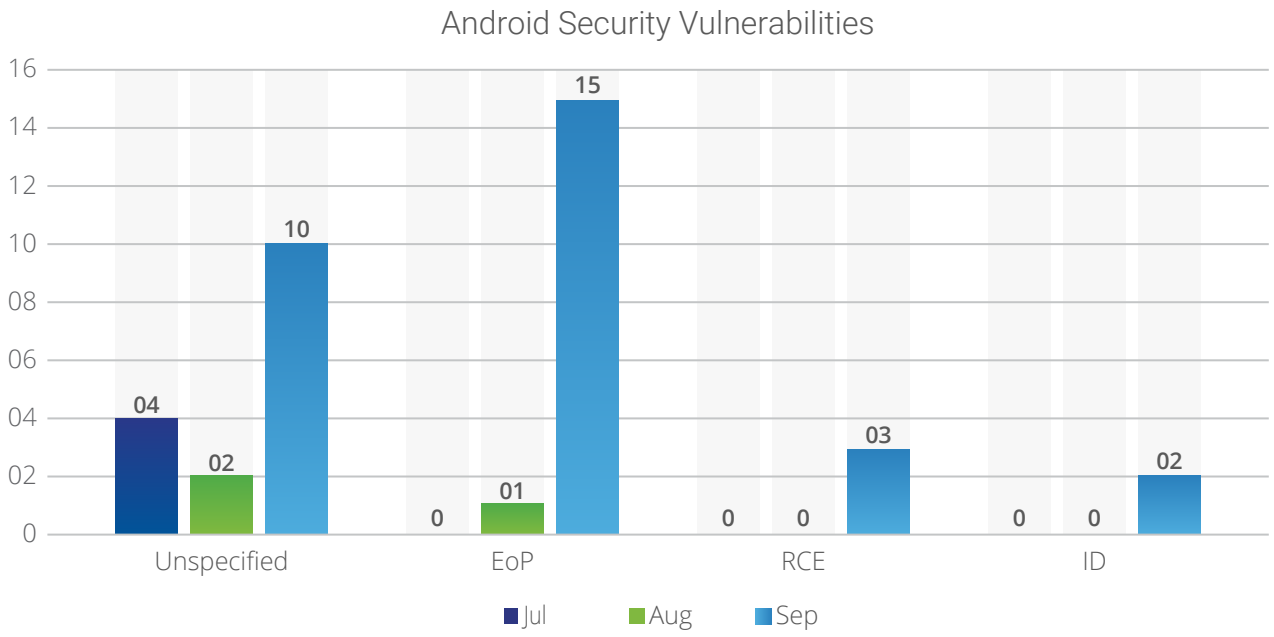


Observation

- Malware clocked 47% of the total Android detections in Q3 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 July to September of 2020.



Trends in Android Security Threats

01 RWhatsApp auto-responder hiding in free Netflix application

WhatsApp Business can help one connect with the customers easily by using tools to automate, sort and quickly respond to messages. But the very same functionality can be used by malware authors for spreading of malware. We came across an app offering free Netflix Streaming which has this functionality implemented in it. Once installed on an Android Phone, this app keeps checking WhatsApp notifications. If a new message notification comes, it creates its own crafted text message and sends it as a reply to the sender. This crafted message also contains a link to download this fake application. This is a way for it's self-promotion.

Quick Heal Mobile AV detects this as Android.Myflix.A6fea.

Users should exercise caution while installing apps from unknown sources and monitor any misuse of the legitimate apps which they have installed on their phones.

02 Joker again found on Google play with new form

A new variant of the infamous Joker Spyware and Dropper is found on the Google Play again in this quarter. This new variant of JOKER hides its malicious payload in manifest file as well as inside the application in encrypted format. It decrypts and load the payload with reflections. It communicates with a remote C&C Server for further loading malicious payloads.

03 Blackrock - Android banking malware

This is a banking trojan. After installation, it hides icon and asks for accessibility permissions to prevent its removal as well as to take full control. After getting permissions, the malware connects to its C&C Server and works as per commands received from it. This malware has features like overlay attacks, send, spam and steal SMS messages, screen-locking, etc. Another important feature of Blackrock is it's capabilities to detect Antivirus application installed on phone. Whenever the user opens the Antivirus application, it redirects the user to home screen.

Quick Heal Mobile AV detects Blackrock malware as variants of Android.Mbot.A

04 Fake clones of the banned Chinese Apps - A new way of spreading malware

Malware authors are generally way too quick in riding the wave of popular sentiments and luring unsuspecting victims. After the recent ban of the popular video-sharing, social networking App -TikTok in India, we observed few spam messages with a link to download a fake TikTok App. This fake App is nothing but a SMS worm. After launch, it asks the user to enter username and password, here user may be tempted to enter his original TikTok credentials.

Quick Heal Mobile AV detects this with Android.GoodNews.GEN36260 name.

Inference

As observed there cyber attackers are on their toes and are swiftly targetting consumers when they are at their most vulnerable. Also, they are at the top of their game and have launched targetted attacks based on recent happenings in the country. For eg after the ban of TiKTok in India we have seen a barrage of attacks disguising as the TikTok app. There have been attacks through fake apps, online games, banking and shopping apps, OTT subscription platforms among others. There's no respite.

5K+ **Ransomware threats detected 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 a good amount of 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.

46K **Malware detected in Android**, which forms **47%** of the total Android detections in Q3 2020. This implies that you need to take mobile security seriously as your Android phone is exposed to many threats.

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