Quick Heal

Security Simplified

QUARTERLY THREAT REPORT

Q1 - 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

Quick Heal Security Labs detected 203 million Windows Malware in the first quarter of 2020. Windows Malware detection was visibly lesser than Q2 & Q3, 2019 by 39 million and 54 million attacks respectively. However, this is not an indication that malware has or will be reducing in the future. The entire globe saw the Coronavirus pandemic spread rapidly that may have directly impacted the modus operandi of adversaries.

This theory is further validated in the month-wise detection statistics wherein attacks in January and February remained consistent at 70 million each with a drop in March at 57 million - Coronavirus was at its peak in March.

We detected around 2 Million malware every day that included 6K Ransomware, 0.18 million exploits, 0.17 million Adware & Potentially Unwanted Applications (PUA), 45K Cryptojacking malware, 0.25 million Infector and 0.24 million Worm in Q1 2020.

Coronavirus outbreak forced 20 million people to work from home due to strict government directives in India alone. Cyberattackers launched a barrage of attacks targeting individual users, a lot of them working from their devices, out of secured corporate networks.

Computers and laptops using the Windows Operating System saw a swarm of Coronavirus-themed attacks through emails and web-browsing tricking users in hordes. Web applications providing the information of Coronavirus patients in the vicinity, news on the virus, Government initiatives, health measures and many more digital channels all became attack vectors leaving a bad taste with users.

Ransomware and info-stealers were also seen at large with a new form of attacks seen by Quick Heal's Security Labs that were attaching malware files for disk imaging. One of the most-worrisome attacks though was a vulnerability found in Microsoft's operating system itself which could or did penetrate the systems of millions of users.

Android devices also saw a large number of attacks in Q1 2020, the majority of them happening through malware, PUPs and adware. Android too, was exposed to similar attacks happening to Windows users through Coronavirus themes via Apps, the internet and emails. Our labs continued to see the trend of malicious and Fake Apps through Google's Play Store.

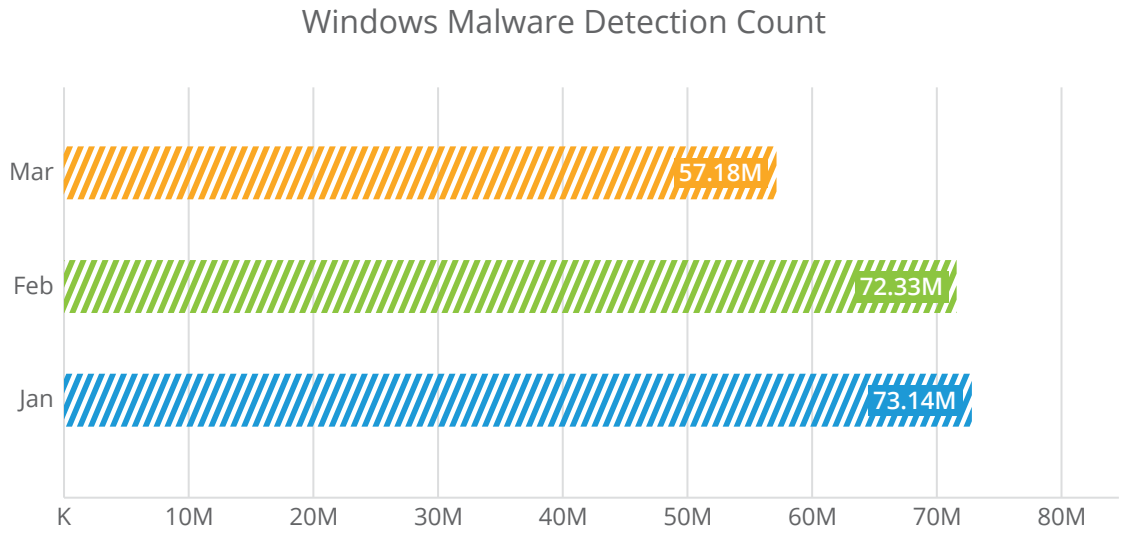
Windows

Windows Detection Statistics Q1 2020*

*Top six malware categories featured in the chart

Detection Statistics – Month Wise Q1 2020

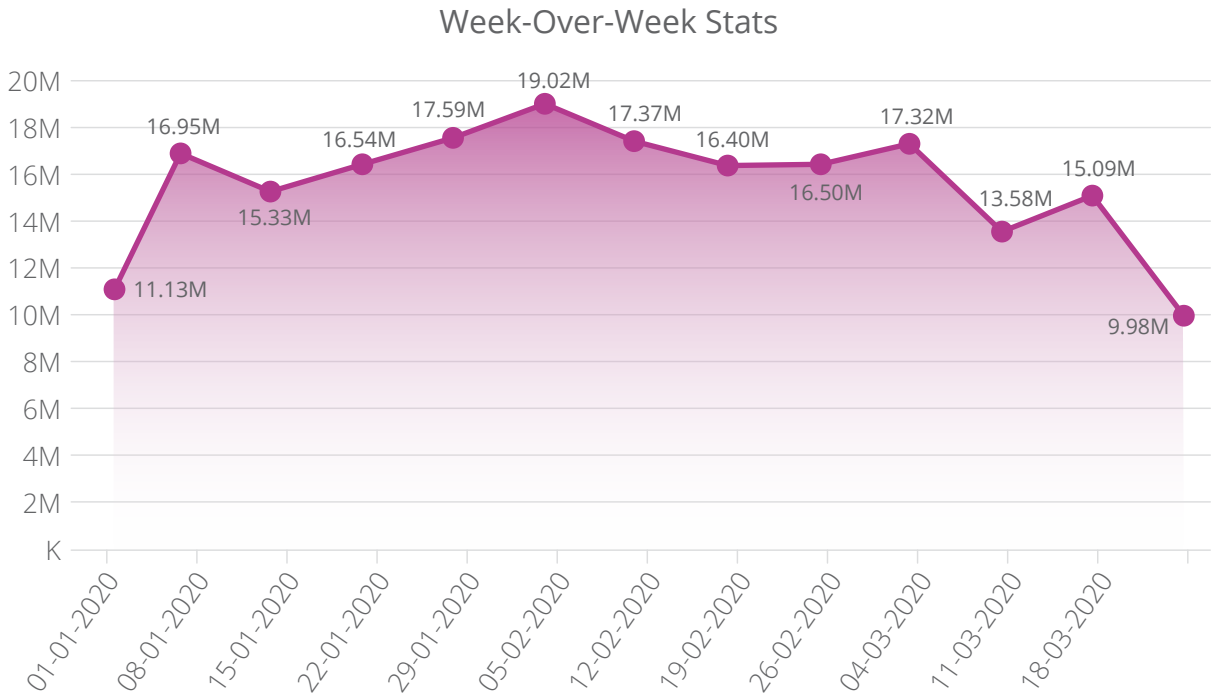
The below graph represents the statistics of the total count of malware detected by Quick Heal from January to March in 2020.



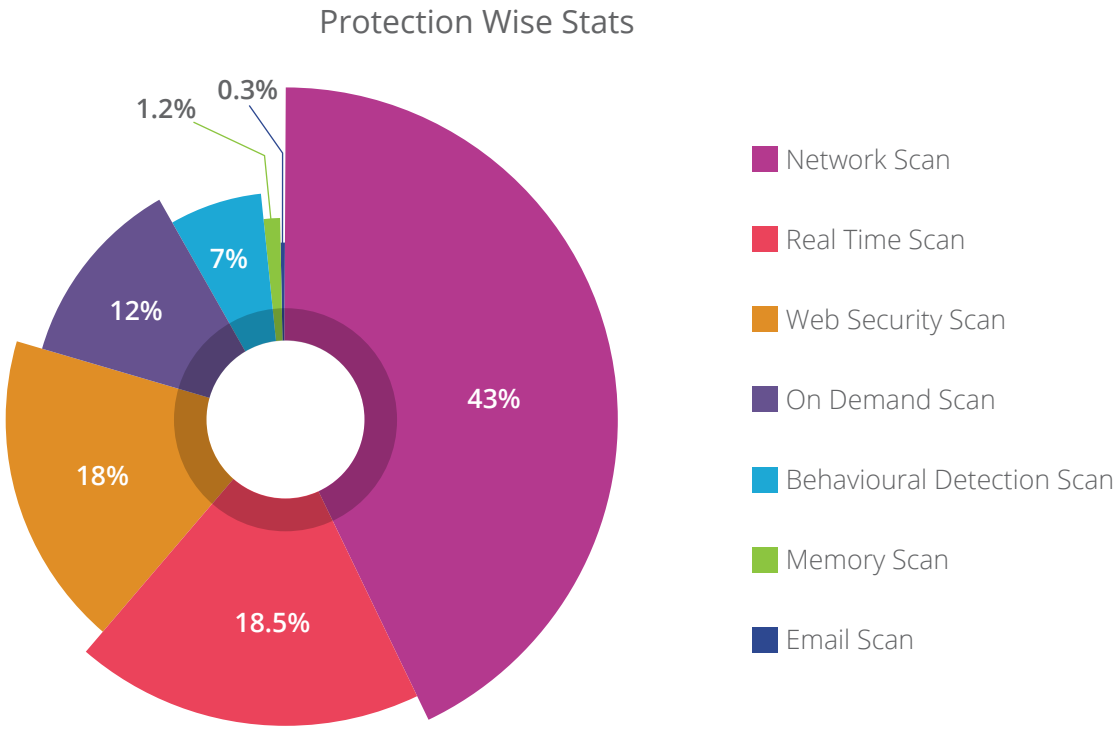
Observations

- Quick Heal detected over 203 million Windows malware in Q1 2020
- Jan clocked the highest detection of Windows malware

Detection Statistics – Week-Over-Week



Detection Statistics – Protection Wise



Observations

• Maximum malware detections were made through Network Scan

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

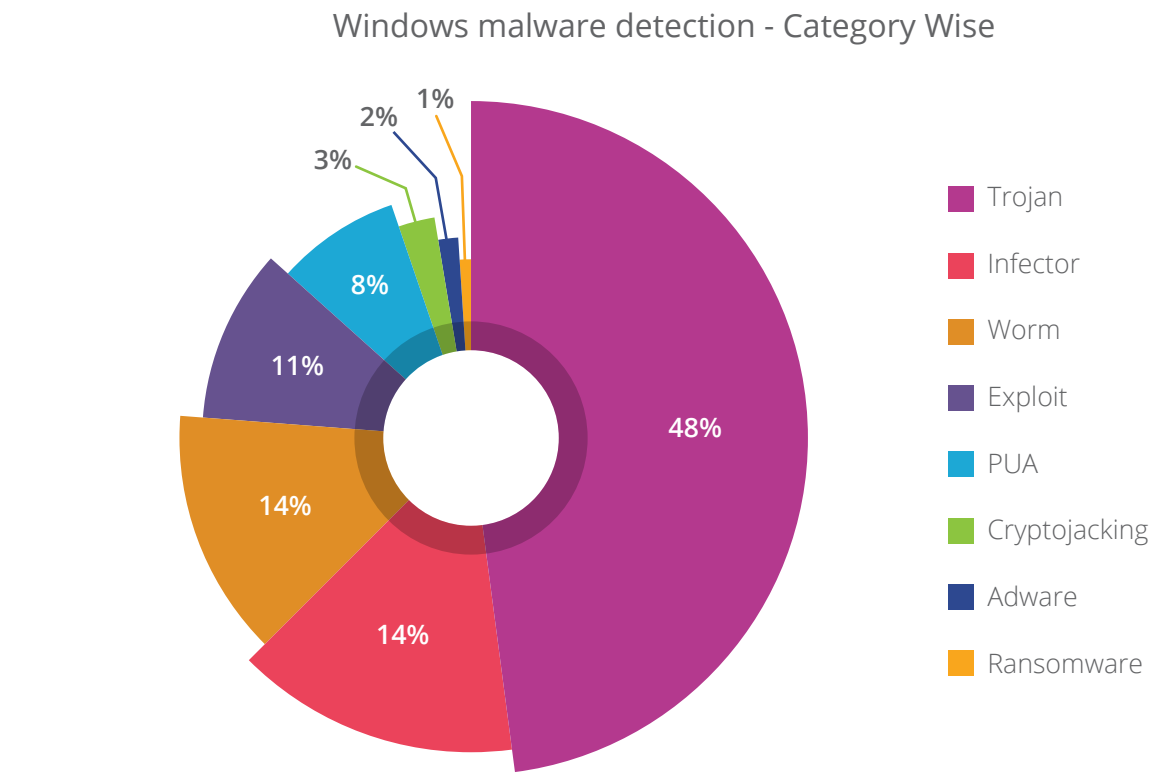
Automatically detects unsafe and potentially dangerous websites and prevents you from visiting them.

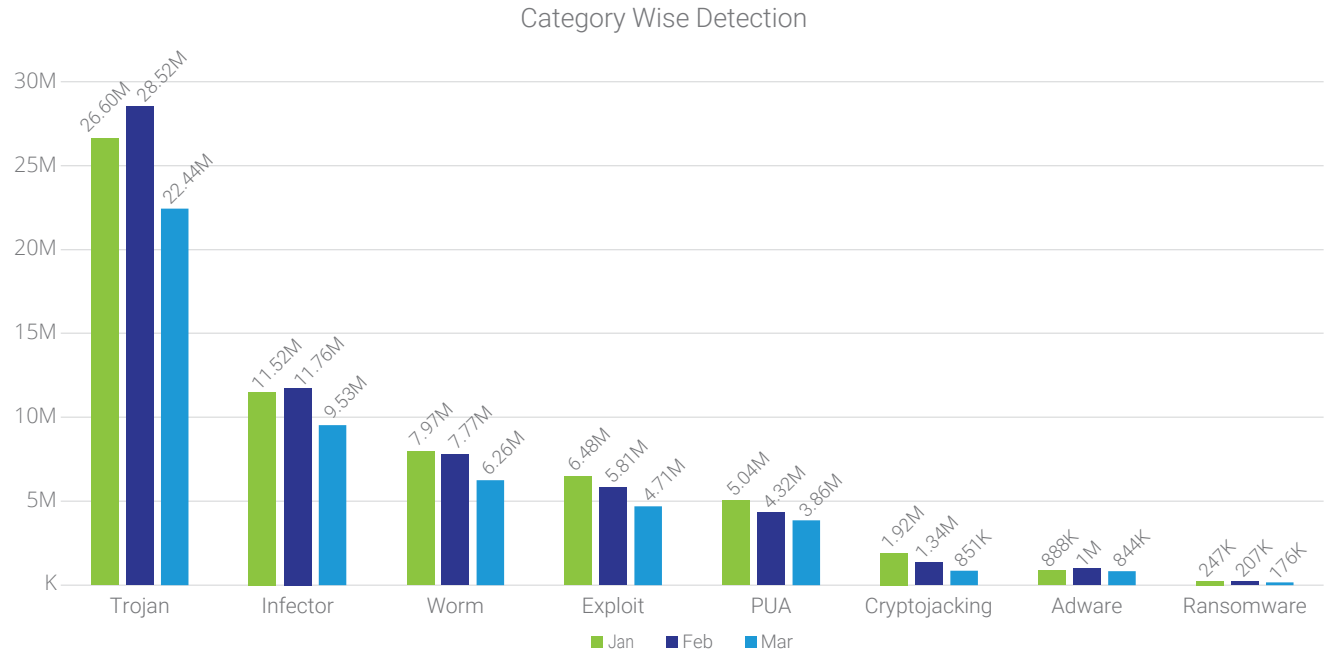
Network Scan

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 Q1 2020



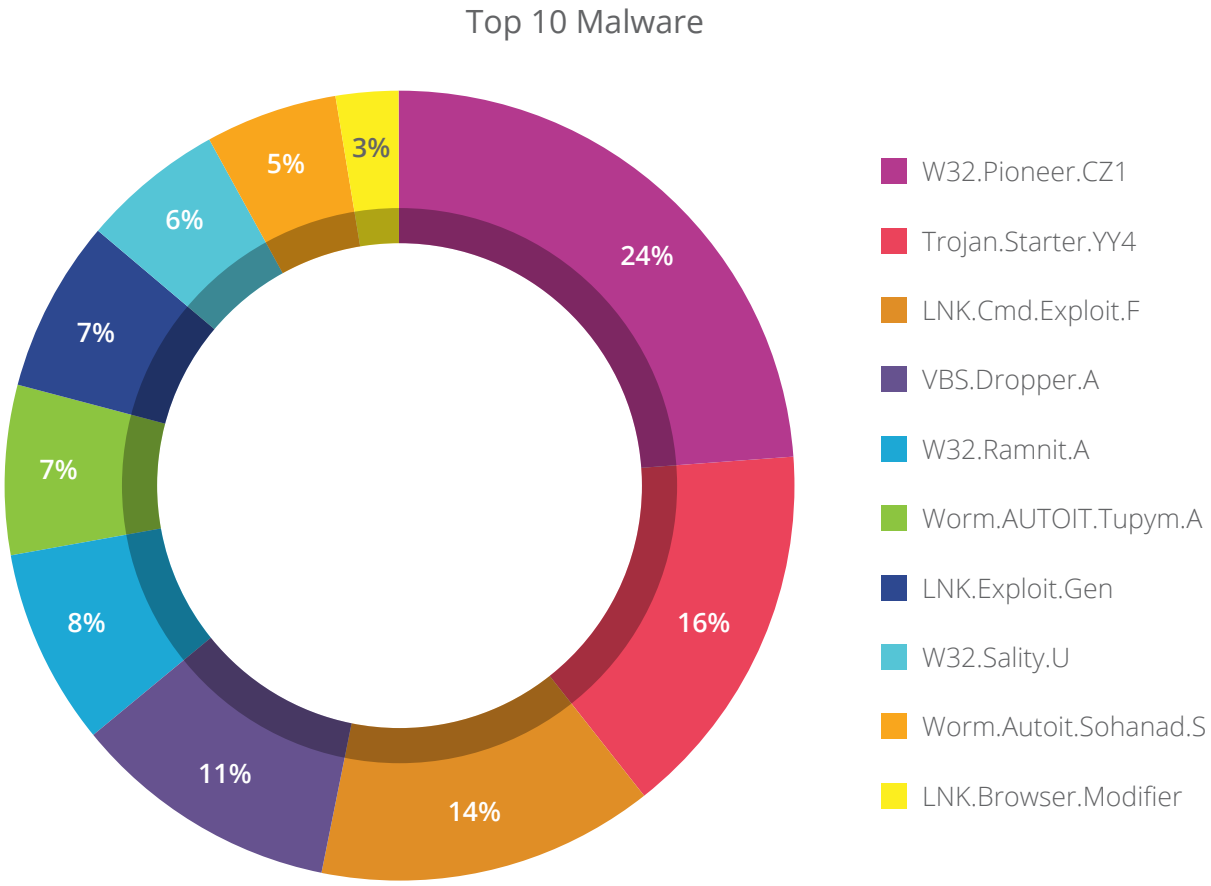


Observations

• Trojan malware was found to clock the maximum detection at 48% in Q1 2020

Top 10 Malware

The below figure represents the Top 10 Windows malware of Q1 2020. These malware have made it to this list based upon their rate of detection from Jan to March.



Observation

- In Q1 2020, W32.Pioneer.CZ1 was detected to be the top Windows Malware, with 16 Million+ detections

1. 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 the 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

2. 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 malware 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

3. 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

4. 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

5. 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 the installer is dropped or downloaded, it drops its various components in memory or disk. Each component has a 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

6. 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 execute it from the dropped location
- It connects to a malicious website, also modifies start page of browser to another site through registry entry and creates Run entry for same dropped file for persistence

7. 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. To redirect the user to dubious websites, the virus modifies system hosts file and hijacks the IP address

8. 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

9. Worm.Autoit.Sohanad.S

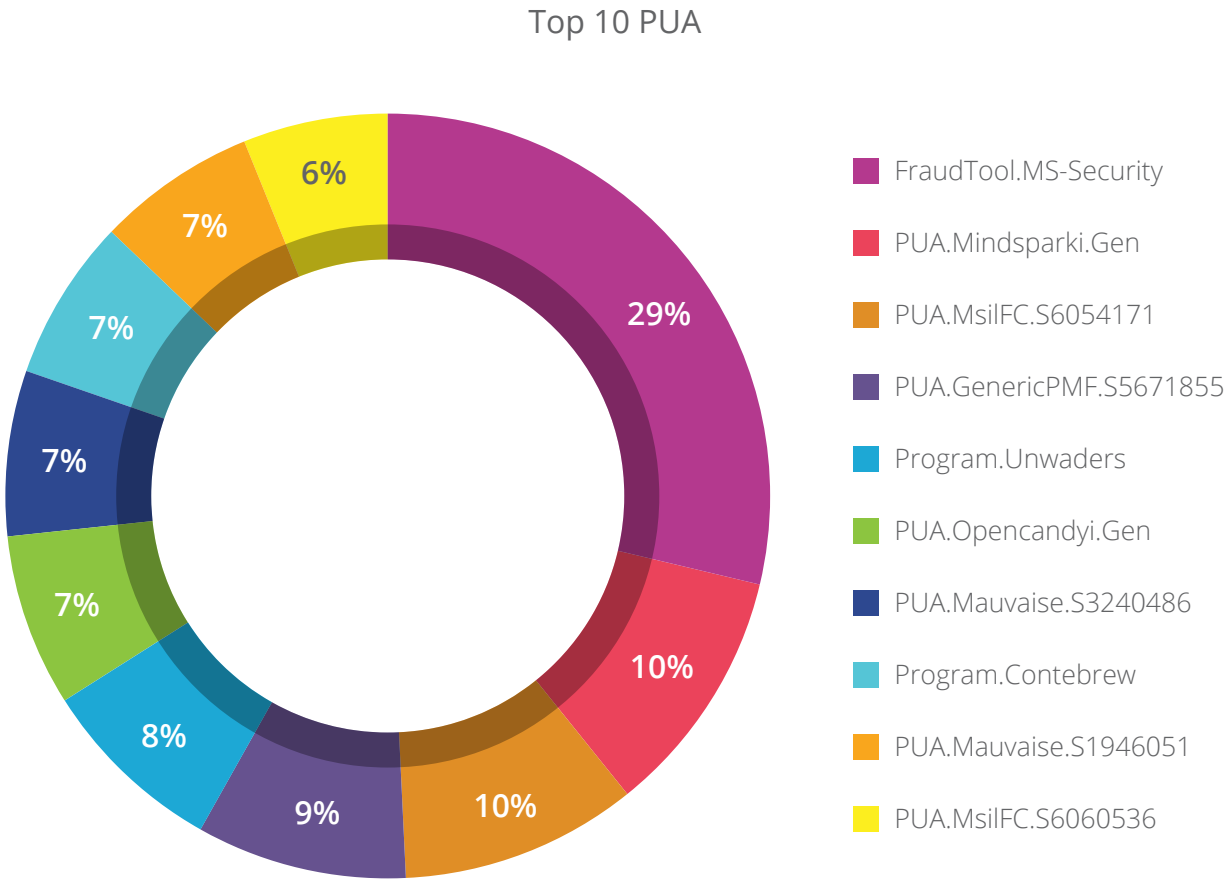
Threat Level: Medium
Category: Worm
Method of Propagation: Spreads through mails, IM apps, infected USB & network drives
Behaviour:
• It arrives at your computer through Messaging apps, infected USB or network
• It can spread quickly
• After arrival, it creates a copy of itself as an exe with a typical Windows folder icon
• A user mistakenly executes this exe assuming it as a folder after which it spreads over the network
• It infects every connected USB drive too

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

Potentially Unwanted Applications (PUA) and Adware 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 Q1 2020.



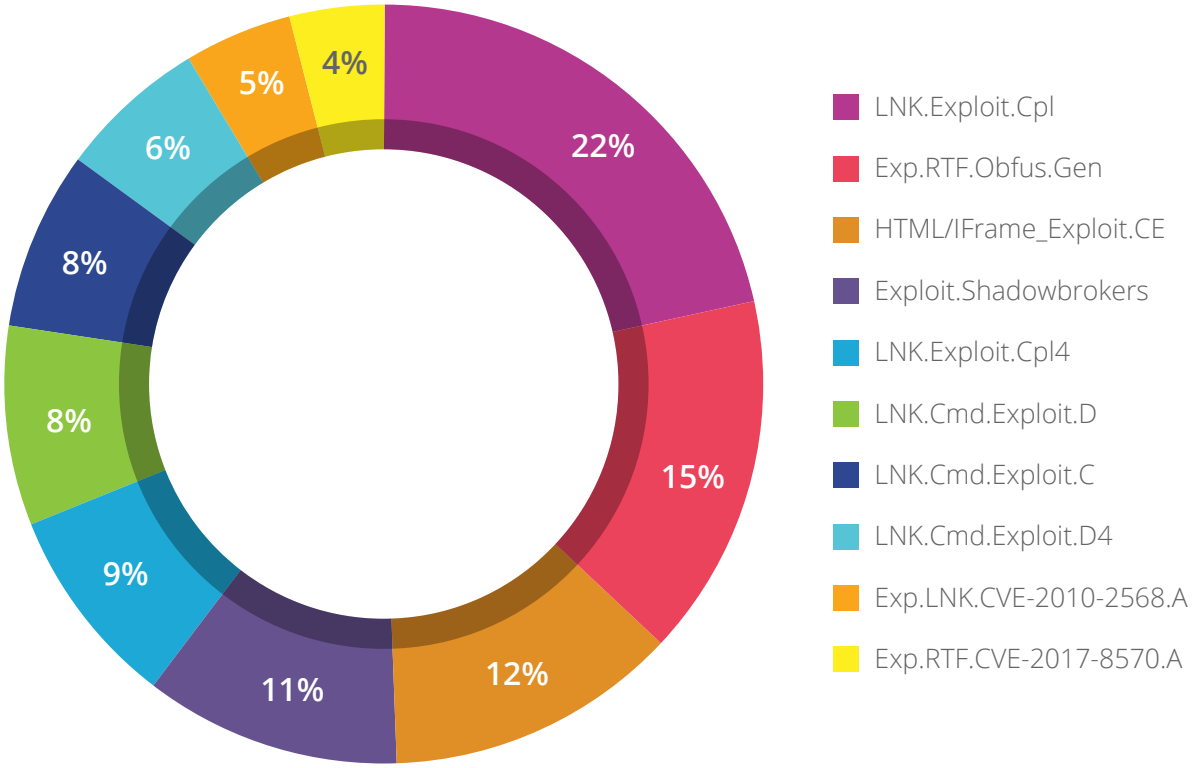
Observation

- FraudTool.MS-Security was detected to be the top PUA, with around 0.7 Million detections made in Q1 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.

Top 10 Host-based Exploits



What are host-based exploits?

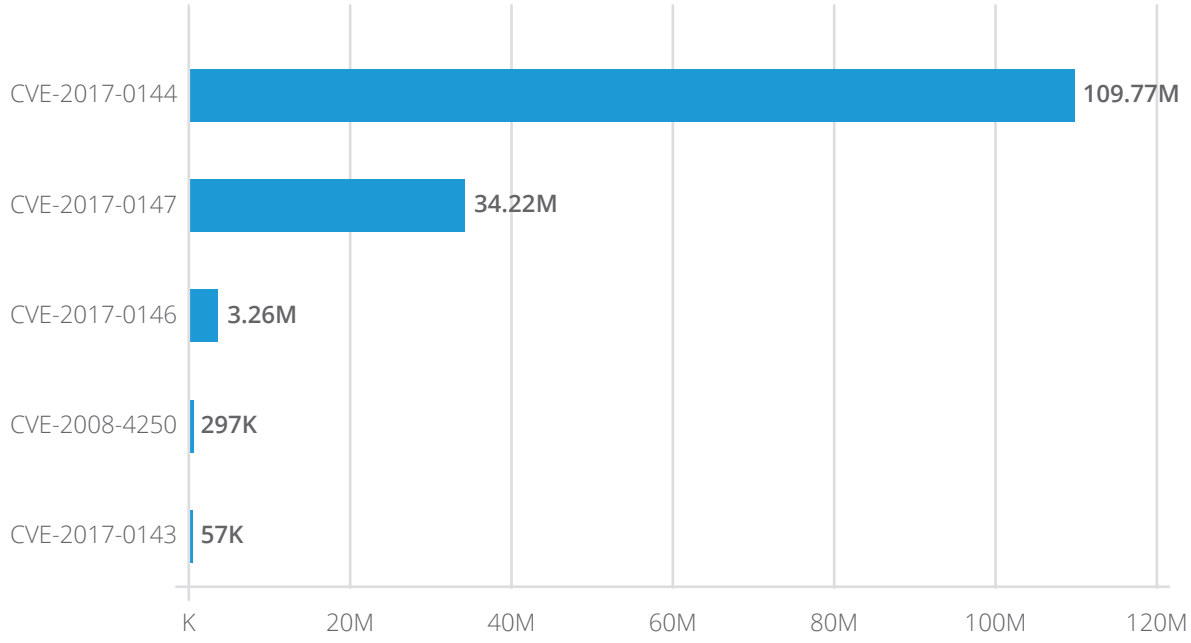
Host-based exploits are those that target security vulnerabilities found in host-based applications (host is a computer or other device connected to a computer network). These exploits are detected by endpoint detection modules such as Virus Protection, Email Protection, and Scanner.

Observation

- LNK.Exploit.Cpl was detected to be the top host-based exploit, with around 0.09 Million detections made in Q1 2020

Top 5 Network-Based Exploits

Below figure represents the top 5 Network-Based Windows exploits of Q1 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 109 Million detections made in Q1 2020

Trends in Windows Security Threats

1. Coronavirus-themed Threats

Q1 2020 saw the Coronavirus spreading, with people anxious to know more about the lethal disease through news and social media to stay updated. To make good use of available opportunities, mal-actors took full advantage of this global issue for delivering different RATs, ransomware and info stealers. New malware sites and domains with the substring 'corona' and 'COVID' were being registered in huge amounts to deceiving users into believing that they are accessing a site showing useful information about the dreadful disease. Some of these domains were using fully functional and real working maps of Coronavirus infected areas and other data from WHO, along with a payload.

Decoy documents and executable files were used having names like "AWARENESS NOTICE ON CORONAVIRUS COVID-19 DOCUMENT_pdf", "COVID-19 Supplier Notice", "UNICEF COVID-19 APP", "WHO-COVID-19 Letter", "Corona", "LetterCovid-19Mesures" and "Solution_to_coronavirus" to trick users into opening it.

Such attacks are still active and very much in use!

Many of such files have a spoofed file extension like pdf, doc or rtf, however, their original extensions are exe, scr or lnk. Malspam campaigns use attachments containing compressed .zip, .rar or .arj files which carry malicious exe, lnk or vbs files.

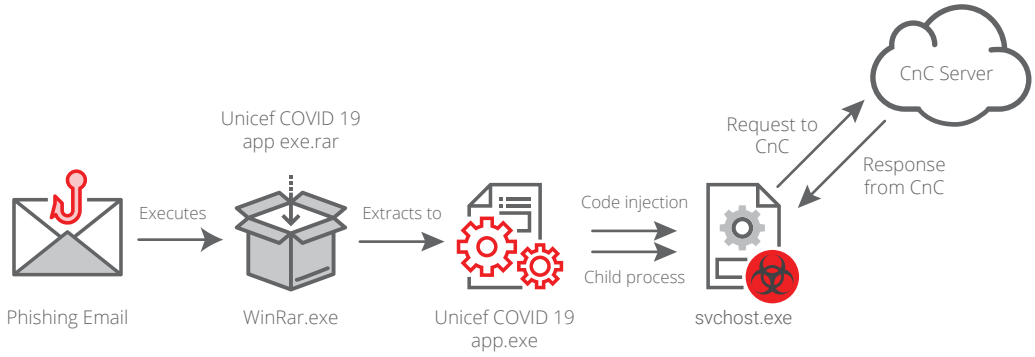


Fig1. Attack Chain

Loki-Bot, Agent Tesla and Netwire RAT are some of the popular threats which use the above-mentioned techniques to infect users. In the current pandemic situation, the healthcare industry needs to stay more careful against cyber threats since thousands of Coronavirus infected patients' health relies on their medical facilities. DoppelPaymer and Maze ransomware operators have posted a 'Press Release' stating that they will stop all activity against all kinds of medical organizations until the end of the pandemic. However, only the test of time would prove if they adhere to their own words (or not).

Quick-Heal detects these malware and malicious domains, however, to be on the safer side following preventive measures can be followed.

- Turn on the email protection of your antivirus product
- Do not open any link in the email body sent by an unknown source
- Do not download and open any attachments from an unknown source

2. Ransomware exploring new technique for process code injection!

Process code injection is a very popular technique among malware authors to evade from security products. Process hollowing is an injection technique where the legitimate process is created in suspended mode, its memory is overwritten with malicious code and process is resumed. It seems like all the malicious activities are performed by a legitimate process, so it is untouched by security products. The new ransomware Mailto or Netwalker is using this old trick in a new way. Instead of creating a process in suspended mode, 'Debug Mode' is used. It gets the process and thread details using debug API WaitForDebugEvent. Then a section is created with a size that of the sample and whole file data is copied. It then manually resolves the relocation.

The sample contains an encrypted JSON file in resource section having required information like a key for generating ID i.e. extension to be added to encrypted files, base64 encoded ransom note, whitelisted paths and email-ids which are part of the extension. The ID is generated using the key kept under the tag 'mpk' in decrypted JSON, the retrieved computer name and the hardware profile information about the machine being infected. SHA-256 of these components is calculated and the first five characters of the output are used as the ID i.e. extension of the files. The name of the ransom note file is also kept the same as ID generated. Changing the extension on each device makes cybersecurity difficult to detect ransomware based on the software's pre-defined extensions.

Ref.: https://blogs.quickheal.com/mailto-ransomware-hiding-under-explorer-exe/

3. Info-stealer hidden in the phishing emails!

Cybercriminals pry on the data precious to you! This data consists of your system details, name, software installed, your browsing history along with cookies stored on the disk and saved passwords too. We have observed multiple phishing emails in this quarter with contents which entice the end-user to download a malware encapsulated as a fake software or a fake update. These software names have strings like demo, free, cracked or plugin etc. Most of the times, these malware payloads are either placed on compromised websites or popular file-sharing service platforms.

Once the malware is executed, it starts getting computer details using Windows APIs and stores it in a file. Sometimes, malware downloads a few supporting files which might be useful for retrieving data — we saw a recent case wherein 5-6 supporting DLLs were downloaded for Mozilla's Firefox browser. For each kind of data, a separate file is maintained with almost all data stored in an SQLite format. All the stolen data is compressed in a single file and sent to the attacker. We have found some variations in the way of sending data. Some malware contained pre-existing CnC details and in some cases, there were few mail IDs seen where this data was being sent using Microsoft's CDO library over port 465. To remove the traces, malware finally deletes all the stolen data and downloaded DLLs from the victim's system.

Ref.: https://blogs.quickheal.com/sloppy-click-can-exfiltrate-important-data/

4. A new wave of mal-spam campaign attaching Disk Imaging Files.

Threat actors keep experimenting with the development of payload in various dimensions. Since Q4 2019, we have been seeing a sudden rise in the use of disk imaging file formats in massive mal-spam campaigns to distribute various RATs attached in emails. The subject of these emails is made to appear as genuine as possible — 'case filed against your company' or 'AWB DHL SHIPMENT NOTICE AGAIN', etc. are few legitimate-sounding emails discovered. The attached files contain compressed malware (RAT's) which have many different names like 'Court Order.img', 'Product Order.img', etc.

The below image displays one such spam email.

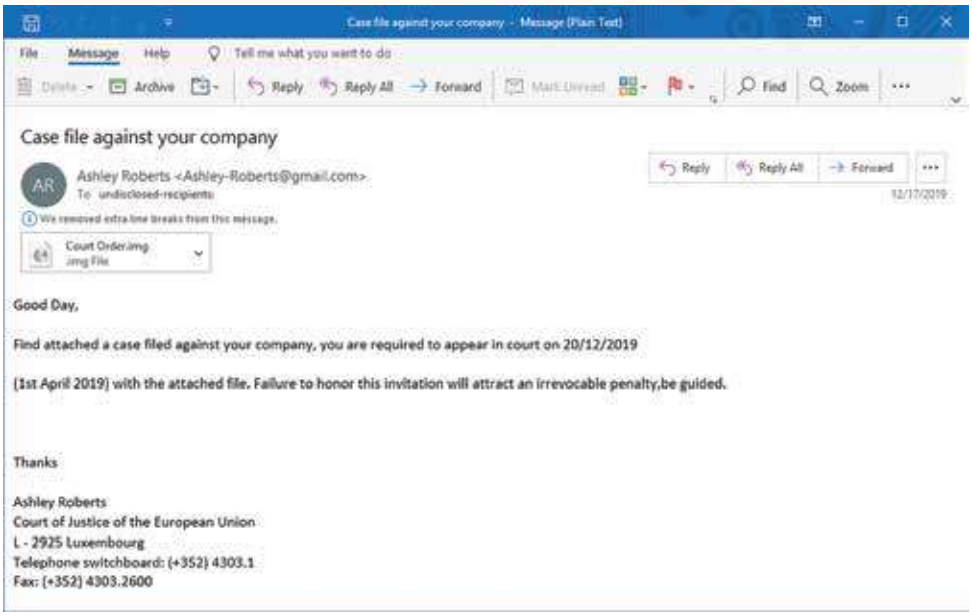


Figure 1: Spam email with a malicious attachment of type IMG

Two of the most bashed disk imaging file formats are IMG and ISO as these files can be directly opened in explorer, automatically mounting them upon a user's system. The count of IMG and ISO files used in such campaigns was at a peak in January and has been declining since then but malware authors may use these file types in future to deliver other malware.

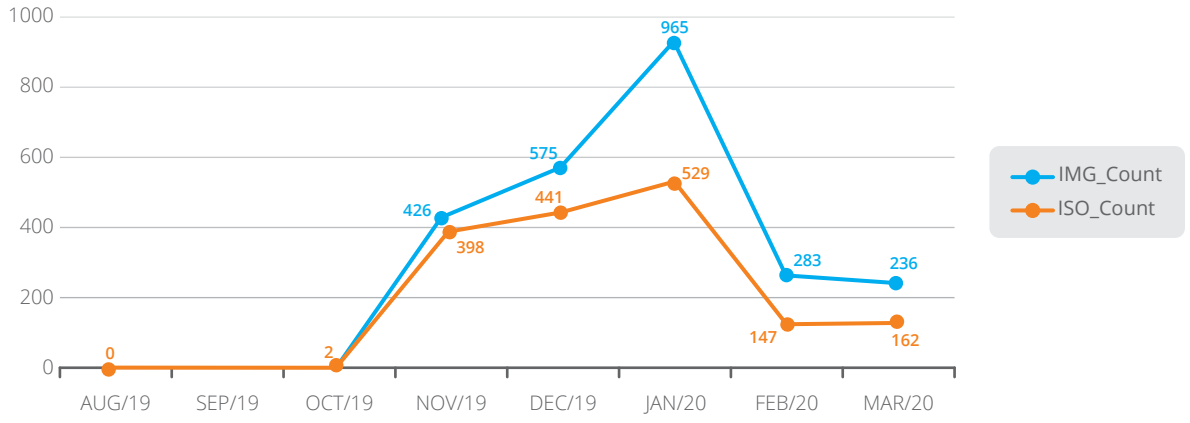


Figure 2: Spam mail with a malicious attachment of type IMG

The most used RATs in this mal-spam campaign are shown in the below figure.

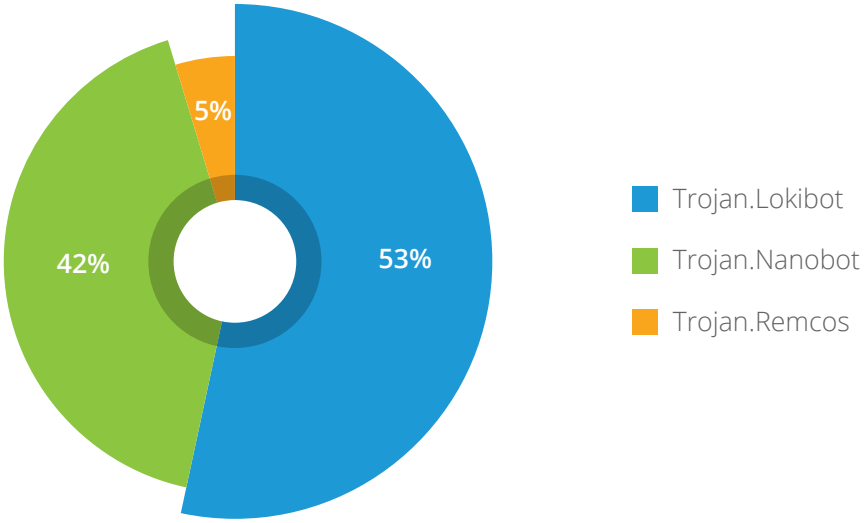


Figure 3: Count comparison of most active RATs in mal-spam

5. CVE-2020-0796 – A 'wormable' Remote Code Execution vulnerability in SMBv3

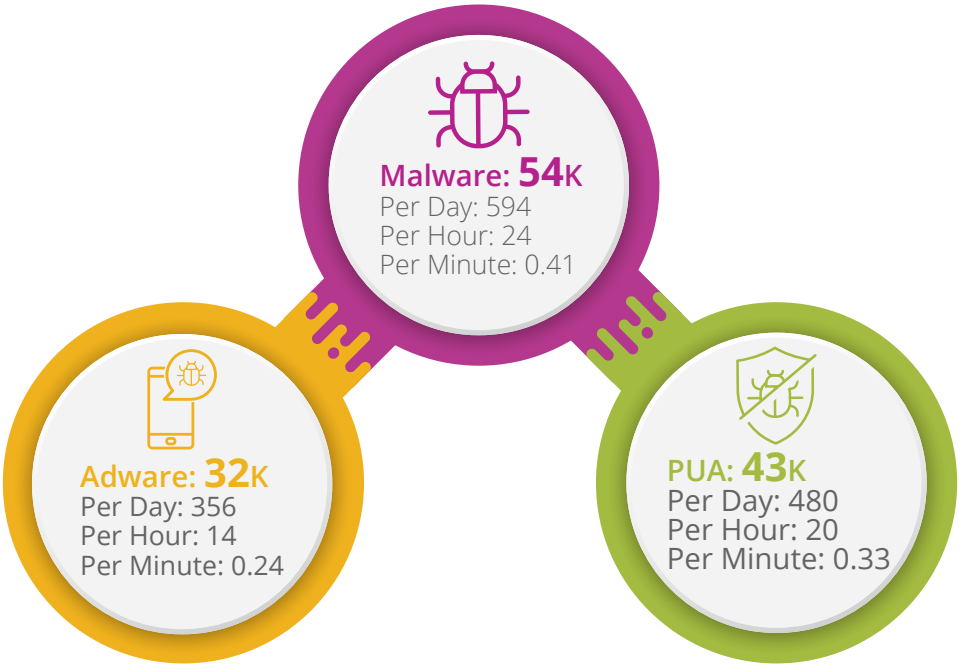
This quarter was very special (and worrisome) for Microsoft and all the users of Windows Operating system. January started with an unpatched IE Zero-day getting actively exploited with February seeing a critical vulnerability in the Crypto API used in Windows for validating ECC Certificates. March witnessed another wormable Remote Code Execution vulnerability -CVE-2020-0796, also known as SMBGhost. It is a vulnerability in the way Microsoft Server Message Block 3.1.1 (SMBv3) protocol handles certain compression requests.

An attacker who successfully exploits the vulnerability could gain the ability to execute code on the target server or client. To exploit the vulnerability against a server, **an unauthenticated attacker could send a specially crafted SMB2 'Compression Transform Header' packet to a targeted SMBv3 server service supporting data compression**.

We advise customers to disable SMB access to their Windows hosts from unknown/public IP addresses unless it's necessary. The fact that remote code execution is possible, and authentication is not required makes this vulnerability very critical. We can expect malware authors adding this exploit in their arsenal for lateral movement, in a similar way as 'Eternal Exploits' were used in the past.

Android

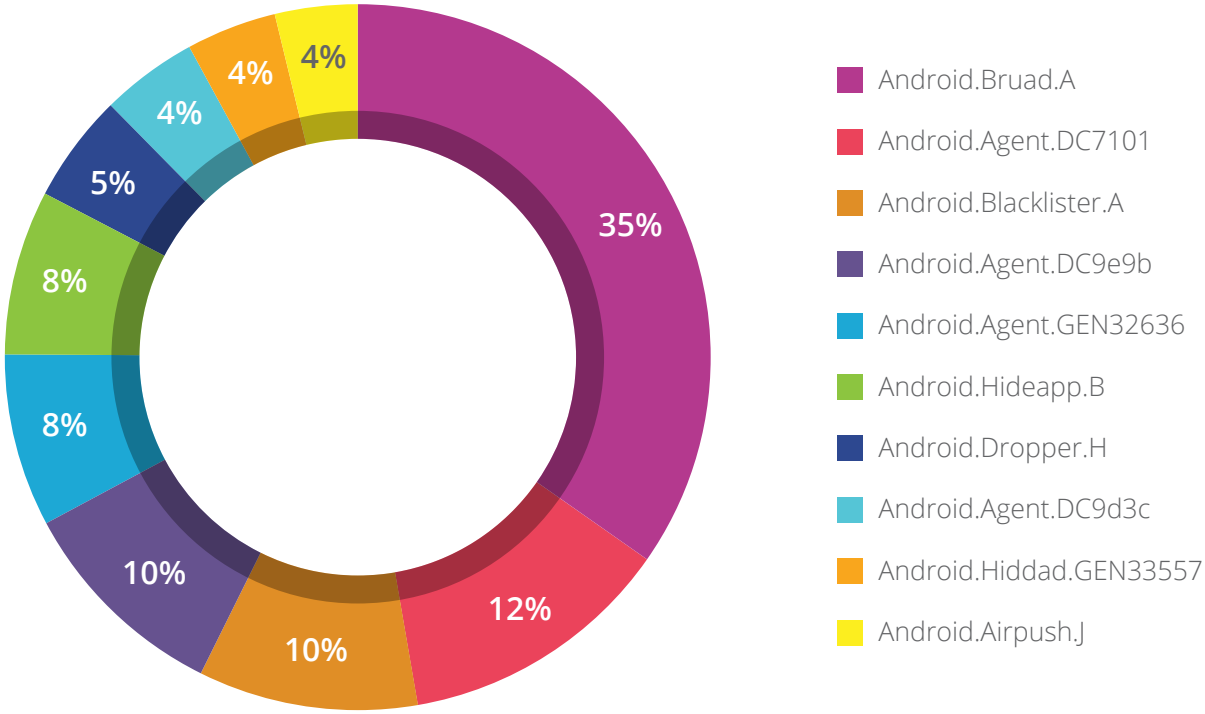
Quick Heal Detection on Android



Top 10 Android Malware for Q1 2020

Below figure represents the top 10 Android malware of Q1 2020. These malware have made it to this list based upon their rate of detection across the year.

Android Top 10 Detection



1. 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

2. Android.Agent.DC7101
Threat Level: High
Category: Malware
Method of Propagation: Third-party app stores
Behaviour:
- This malware is from the dropper category
- It drops malicious hidden Ad application on users' phone
- The dropped file hides its icon and shows pop up ads after installation
- It uses Chinese language strings with decryption code to get malicious code at runtime

3. Android.Blacklister.A (PUP)
Threat Level: Medium
Category: Potentially Unwanted Application (PUA)
Method of Propagation: Google play app 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

4. Android.Agent.DC9e9b
Threat Level: High
Category: Malware
Method of Propagation: Third-party app stores and repacked apps
Behaviour:
- It connects with C&C server
- It collects device data like IMEI, manufacturer, model, device number, contacts from device and sends it over to a C&C server
- It can draw the overlay window on other applications

5. Android.Agent.GEN32636

Threat Level: High
Category: Malware
Method of Propagation: Third-party app storesBehaviour:
• After installation, it doesn't show any icon
• After execution, it decrypts files from asset and drops another Android executable on the device
• Dropped file is nothing but Android.Bruad.A adware which shows Ads and collects device information to send it to its C&C server

6. 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

7. 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
• On its first launch, it hides its presence and loads encrypted payload from its resources Folder
• Encrypted payload has advertised SDK which shows Fullscreen advertisements

8. 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

9. Android.Hiddad.GEN33557

Threat Level: Medium
Category: Malware
Method of Propagation: Third-party app stores
Behaviour:

- It uses string obfuscation to evade from Anti-virus engines and to make analysis difficult
- Hides its icon after installation and displays advertisement
- Connects to advertisement URLs and sends the infected device's information to a remote server

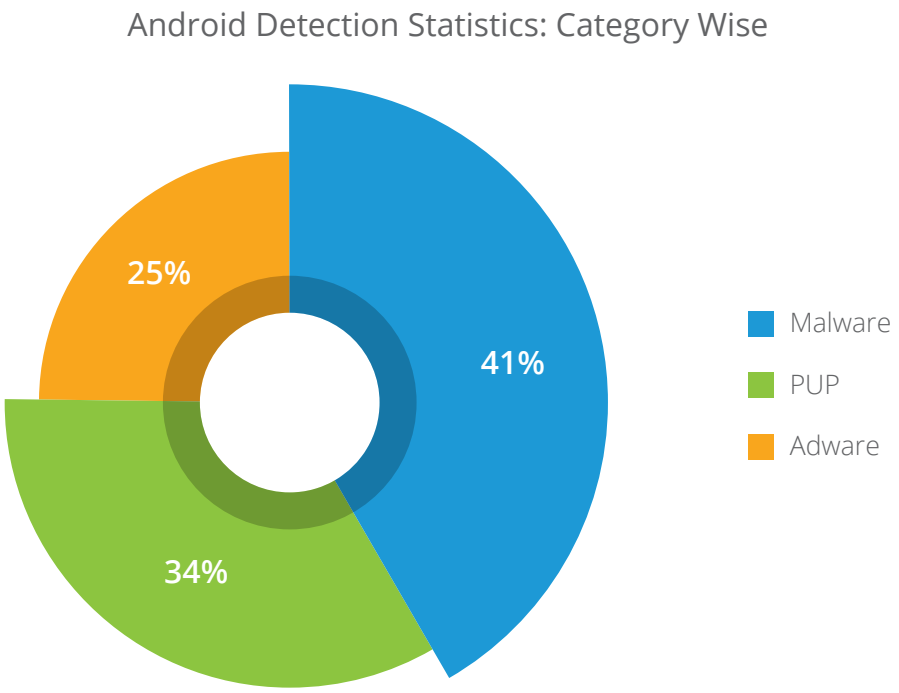
10. Android.Airpush.J

Threat Level: Low
Category: Adware
Method of Propagation: Third-party app stores and repacked apps
Behaviour:

- Displays multiple ads while it is running
- When 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

Android Detection Statistics: Category Wise

Below figure represents the various categories of Android malware detected by Quick Heal in Q1 2020.

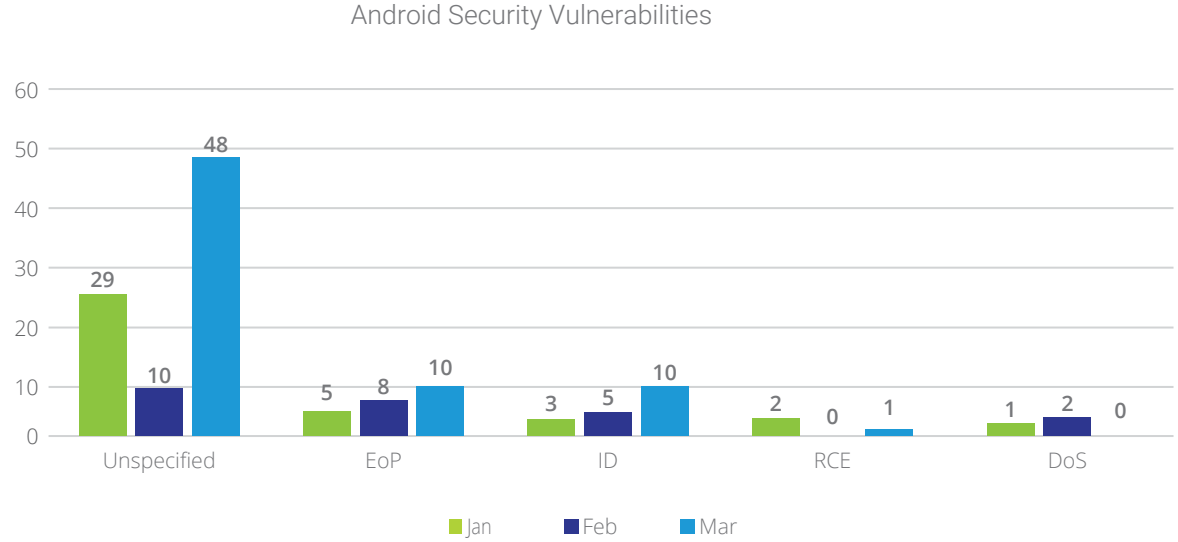


Observation

• Malware clocked 41% of the total Android detections in Q1 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 January to March of 2020.



Trends in Android Security Threats

1. Malicious Android apps carrying Windows malware found on Google Play

Quick Heal Security Labs found a few Android applications on Google Play Store that were infected by Windows malware. We suspect the App developer's host might have been infected with Windows malware that further infected files from APK during the application development cycle.

Typically, Windows malware may not harm the Android Platform but it contains malicious files that are harmful to other platforms. Hence, Google differentiates such applications as Non-Android threats.

One such popular application that we analyzed and reported to Google was the G Buddy - Smart 'LIFE'. This application had a few HTML files which were infected by Windows malware. The HTML files were appended with malicious VBScript code — the VBScript had an encrypted code to drop malicious Windows executable when the script was executed after opening the HTML file. Quick Heal Security Labs reported this app to Google Security on 20th February 2020 and Google removed the infected app from the Google Play Store. Now an updated version of the application is available on the Play Store which doesn't have infected HTML files. Quick Heal Mobile Security Products detect all such malicious apps proactively before they infect your Android Phones or your hosts where you connect the phones for data transfer, etc.

2. Malware abusing the pandemic situation of the Novel Coronavirus

As the Coronavirus spreads across countries creating fear across the globe, everybody wants to stay on top of any information related to it wanting to remain safe and away from infected people. Malware authors are also taking advantage of this situation. A few days ago, there were many applications present on the Android Play Store which claimed that they can provide Coronavirus tracking information. However, Google has set up some rules for these types of applications and have considered these under the 'Sensitive Events' category. According to the policies under this rule, Google proactively removed many applications from Play Store to stop malware authors to take advantage of this situation.

So now we see that malware authors are using their websites to publish malicious apps. We came across one such website named 'coronavirusapp[.]site' where an Android application is hosted. This application claims to get real-time info about Coronavirus patients. The application claims to give notification to the user if a Coronavirus patient is present in the vicinity. But as you can guess, it is nothing more but a ransomware application which locks your screen to demand ransom money for an unlock code. Details: https://blogs.quickheal.com/fake-coronavirus-tracking-app/

In another reported case, an app with the name coronavirus was found to be a banking trojan, dubbed as Cereberus. This trojan family came in light in June 2019 —Cereberus trojan uses rented service from group Cereberus. It uses accelerometer sensor inputs to

prevent analysis i.e. if a device is moved, only then will it start its malicious activity. Malware uses RAT (remote access trojan) functionality i.e. It gives access to a user's device to a C&C server and starts its malicious activity according to commands received from C&C. It has all the features of banking trojans like overlaying, SMS harvesting etc. In new Cerberus variants, it has additional functionalities including stealing device screen-lock credentials and 2FA tokens from the Google Authenticator application.

Quick Heal Security Labs is monitoring all malware activities around the ongoing Coronavirus pandemic closely and will continue protecting our customers against any such attacks.

3. Android malware auto-subscribes users to premium services without their knowledge

Recently, there has been news of a new wave of Android malware which subscribes users to premium services in the background, without their knowledge. Here are a few variants in this category.

I. Subscription by invisible browser

There is a category of malware dubbed as 'MobOK' which subscribes to premium-rate services without user's knowledge. It collects device information like operator and device screen size, then sends it to a remote C&C server. Malware launches an invisible browser where it browses the URLs it has received and executes JavaScript commands to subscribe the user to premium-rate mobile services. It takes permissions to read notifications and then can retrieve the content of SMS messages.

In its latest generations, 'MobOk' uses different evolution stages like 'carrying encryption files within it and decrypting it at runtime & the use of packers to escape from detection.

II. Subscription by Clicker malware

The Haken malware takes data from a user's device and signs them up for expensive premium subscriptions unknowingly. After download, Haken communicates with a C&C server and asks for permissions that the downloaded app doesn't require. Haken clicker uses native code and injection to Facebook (Facebook Ad Center) and AdMob (specifically Google AdMob) libraries. This malware has the potential to access any (specifically Google AdMob) library and any sensitive information on the mobile screen.

Reference link:
https://threatpost.com/haken-malware-family-infests-google-play-store/153091/

III. Subscription by Joker - A Spyware & Premium Subscription Bot

The popular Spyware named as 'Joker' (which was borrowed from one of the C&C domain names) were found on the Google play store with more obfuscation techniques for hiding its APIs and malicious code. Also, some of the samples tried to hide some malicious code in its native libraries. It can steal all the victim's data and device information. In the first stage, it finds the targeted country, by checking the country code. Depending on the

country code, it delivers a second-stage component, which silently simulates the interaction with advertisement websites, steals the victim's SMS messages, the contact list, and device info. The automated interaction with the advertisement websites includes simulation of clicks and entering the authorization codes for premium service subscriptions.

IV. Xiny – An old adware which becomes a malware in this generation

Xiny malware makes files as read-only and by doing this renders it difficult to remove them from infected devices. After the installation of the malware on a mobile device, it remotely downloads many unwanted applications on the device. — it is like the Xhelper and reinstall itself after the removal and its entire activity is controlled by C&C servers. Protection from removal is the main feature of the new variants of this malware that comes at the start of 2020.

It acquires root permissions and replaces the system files by appending "_server" to filenames. Also, it removes some preinstalled applications and root privileges applications. By doing so, it makes it very difficult to gain root access and remove the trojan components from system directories.

In the past years it came up with adware activity and Quick Heal Labs detected its previous variants as adware but now its activity has become more aggressive and we detect it as malware with detection name **AndroidELF.Lotoor.A3b9d**

Reference link: https://news.drweb.com/show/?i=13627&lng=en

V. Quick Heal's protection against harmful apps found on Google Play Store

In this quarter, Quick Heal Security Labs found 32+ Fake Anti-Virus applications, 2 of them have 5 million+ downloads and 15+ Hidden Ads applications, 2 of them having 1 million+ downloads.

Inference

As the world crumbles under the pandemic, attackers are relentless in their pursuit of attack channels that are in tandem with the current world happenings. Attacks are predicted to get increasingly personal since the emergence of a multitude of new subjects that users are interested in now consisting of statistics, employment, finances, health, etc. Other than keeping themselves safe users are also additionally expected to take preventative measures such as -

1. Being extremely careful in their digital interactions with elements related to the Coronavirus.
2. Keeping their device software and cybersecurity solution up-to-date
3. Practising 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 are putting in war-time efforts to provide maximum detection during the testing times of the Novel Coronavirus. All our teams are alert round-the-clock adding new detections in our products and providing support to our customers. We urge our customers to not panic and stay vigilant to safeguard their assets.

Ransomware attacks were seen in this quarter as well with 6,921 attacks per day. Users should be pro-active and initiate data back-ups for their sensitive data. Maximum malware detections (43%) were made through Quick Heal's Network Scanning capabilities in Q1 2020. Trojan malware was found to clock the maximum detection at 48% while W32.Pioneer.CZ1 was detected to be the top Windows Malware, with 16 Million+ detections.

Android devices saw 54K malware attacks in Q1 2020 with malware clocking the highest detection in these attacks (42%) followed by PUPs (34%). Android users saw the most attacks from Android.Bruad.A, a Potentially Unwanted Program (PUP).

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 these dark times in the world.

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