Quick Heal
Security Simplified

QUARTERLY THREAT REPORT Q3-2019

www.quickheal.com

Table of Contents

Contributors

- Quick Heal Security Labs
- Quick Heal Marketing Team

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

Introduction

The third quarter of 2019 witnessed around 257 million Windows malware, which is comparatively lesser than the detection of 242 million made in Q2 of 2019. However, in spite of this, the quarter saw some significant malware detections in both Windows and Android, which reminds us that the threats continue to be alive and active!

The beginning of the third quarter started on a high note with around 92 million detections made in the month of July. The detections ramped up in the consecutive month, with August clocking 97 million malware detections. On a daily basis, Quick Heal detected around 2 Million malware, including 10K Ransomware, 0.2 Million Exploits, 0.1 Million PUA and Adware and 27K Cryptojacking malware.

The number of targeted cyber-attacks continued to outsmart mass attacks in Q3 of 2019. In August'19 Quick Heal Security Labs observed botnet attacks by two cryptomining botnets, on unsecured Android devices via port 5555 – ADB port, 23 telnet and 22 – SSH port. The attacks where a clear indication of the increasing risk that android-based IoT device owners face.

In yet another significant detection, Quick Heal Security Labs spotted 27 malicious apps of dropper category on official "Google Play Store". These apps were removed from Play Store after Quick Heal Security Labs reported it to Google. These apps continuously showed installation prompt for fake "Google Play Store" in an attempt to infect the device with Adware. The trend continued into the month of September, when 29 more malicious apps with 10 million+ downloads were detected on Google Play Store and immediately removed by Google after reports by Quick Heal.

This major detection was followed by yet another significant detection in the beginning of September when our Security Labs spotted multiple Fake Antivirus Apps on Google Play Store. Interestingly, one of these fake AV Apps had been downloaded 100000+ times.

The Trojan horse category continued to dominate the list of most prominent malware in the third quarter of 2019. Trojan.Starter.YY4 was detected to be the topmost Windows Malware, with around 8 Million detections made in Q3 of 2019 while FraudTool.MS-Security topped the list of PUA and Adware, with around 0.4 Million detections.

The third quarter of the year also witnessed Quick Heal Security Labs detecting over 0.1 Million malware, PUA and Adware on Android OS. Android.Necro.A was detected to be the topmost Android malware of Q3.

The quarter began with Android Ransomware making a comeback, this time in the form of SMS carrying malicious link. The Ransomware identified as Android.Filecode.A attempted to draw ransom through Bitcoin address. Yet another Ransomware that strongly made its presence felt in Q3 was Agent Smith, a malware that comes through third-party App stores. These apps look like genuine apps but in the background they infect pre-installed clean applications.

Few other Android Malware were detected like Joker, Funckybot, CamScanner and others that were intended to make targeted attacks.

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

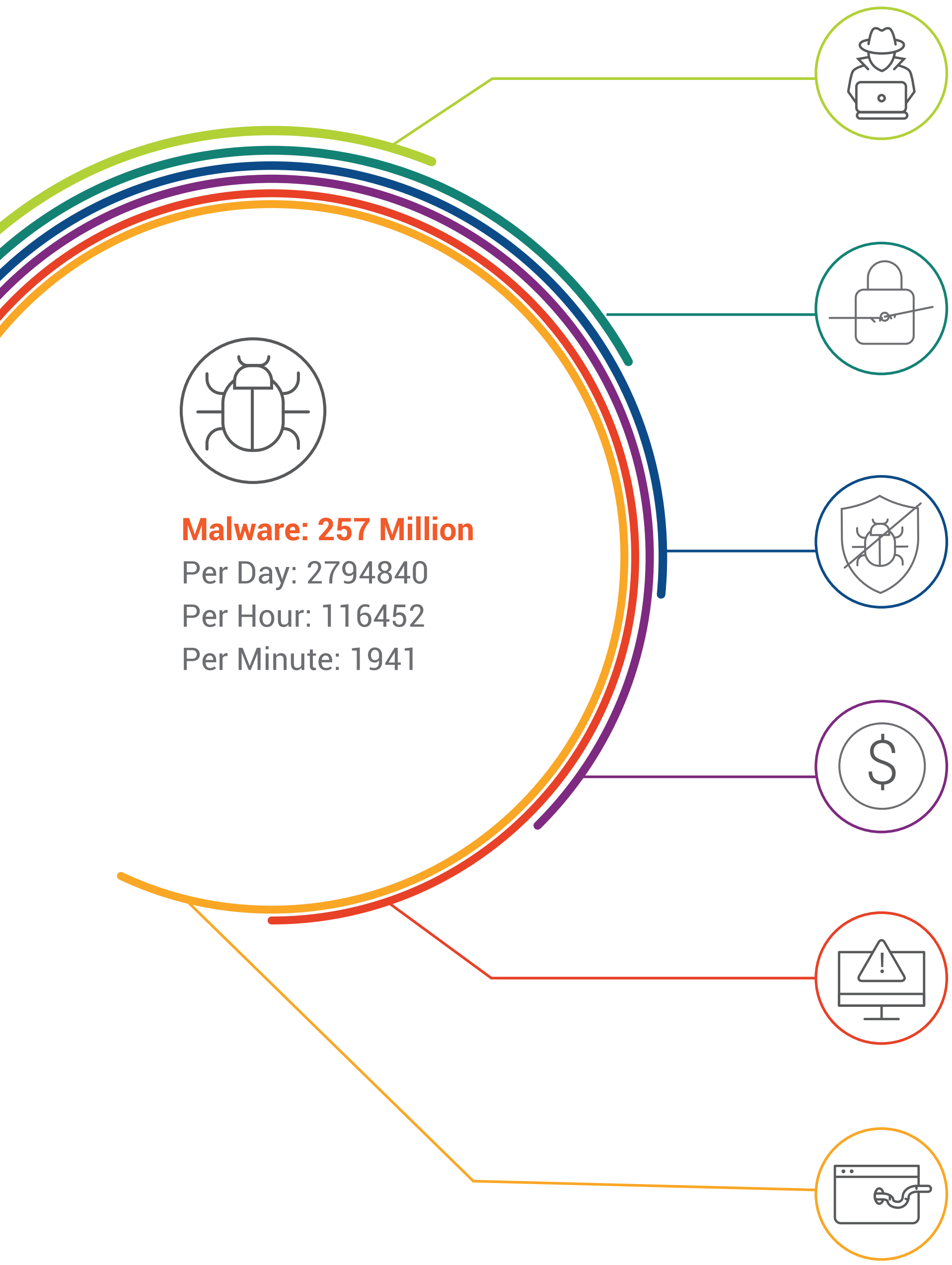
A leading source of threat research, threat intelligence and cybersecurity, Quick Heal Security Labs analyses data fetched from millions of Quick Heal products across the globe to deliver timely and improved protection to its users.

www.quickheal.com

Follow us on:

WINDOWS

Detections Highlights - Q2 2019



Malware: 257 Million
Per Day: 2794840
Per Hour: 116452
Per Minute: 1941

Ransomware: 1 Million
Per Day: 10952
Per Hour: 456
Per Minute: 8

Exploit: 24 Million
Per Day: 259914
Per Hour: 10830
Per Minute: 180

PUA & Adware: 15 Million
Per Day: 168237
Per Hour: 7010
Per Minute: 117

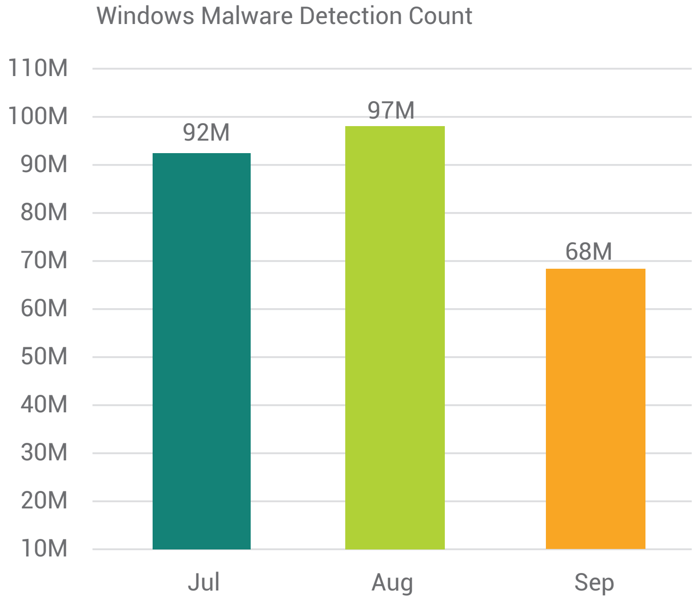
Cryptojacking: 2.5 Million
Per Day: 27761
Per Hour: 1157
Per Minute: 19

Infector: 38 Million
Per Day: 422408
Per Hour: 17600
Per Minute: 293

Worm: 23 Million
Per Day: 257052
Per Hour: 10711
Per Minute: 179

Detection Statistics – Month Wise

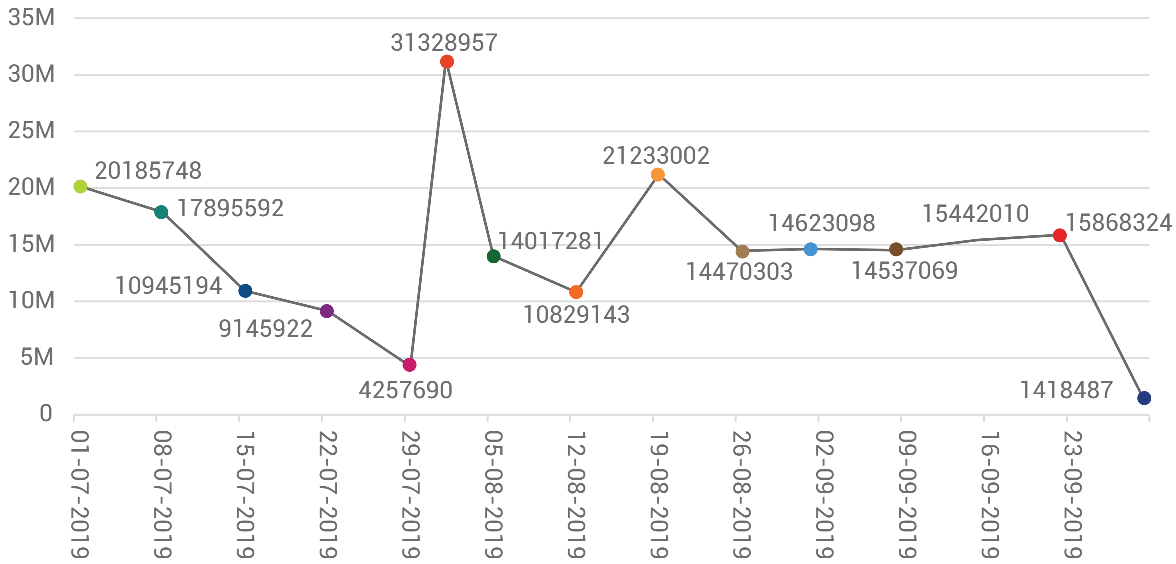
The below graph represents the statistics of the total count of malware detected by Quick Heal during the period of Jul to Sep in 2019.



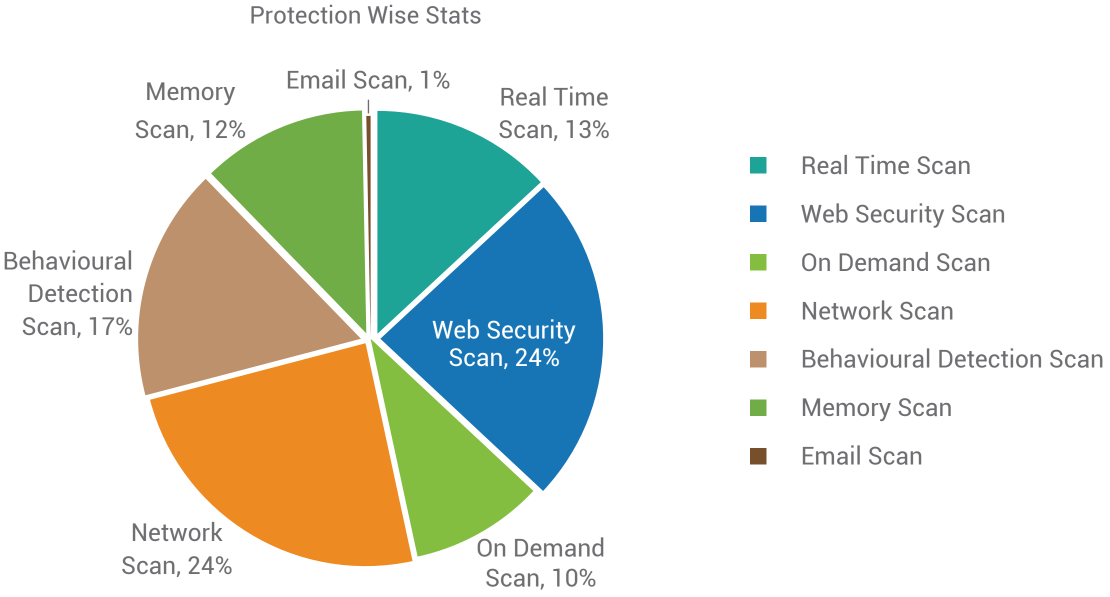
Observations

- Quick Heal detected over 257 million Windows malware in Q3 2019.
- Aug clocked the highest detection of Windows malware.

Detection Statistics – Week-Over-Week



Detection Statistics – Protection Wise



Observations

- Maximum malware detections were made through Web Security Scan and 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 program running & cleans it.

Email Scan

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

Web Security Scan

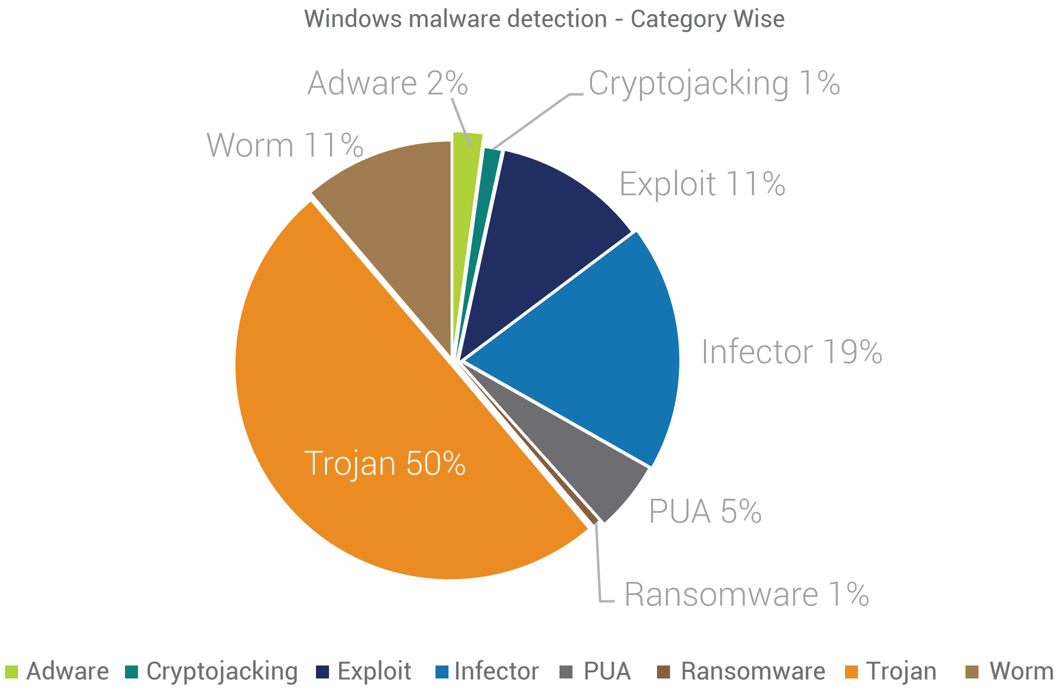
Automatically detects unsafe and potentially dangerous websites and prevents you from visiting them.

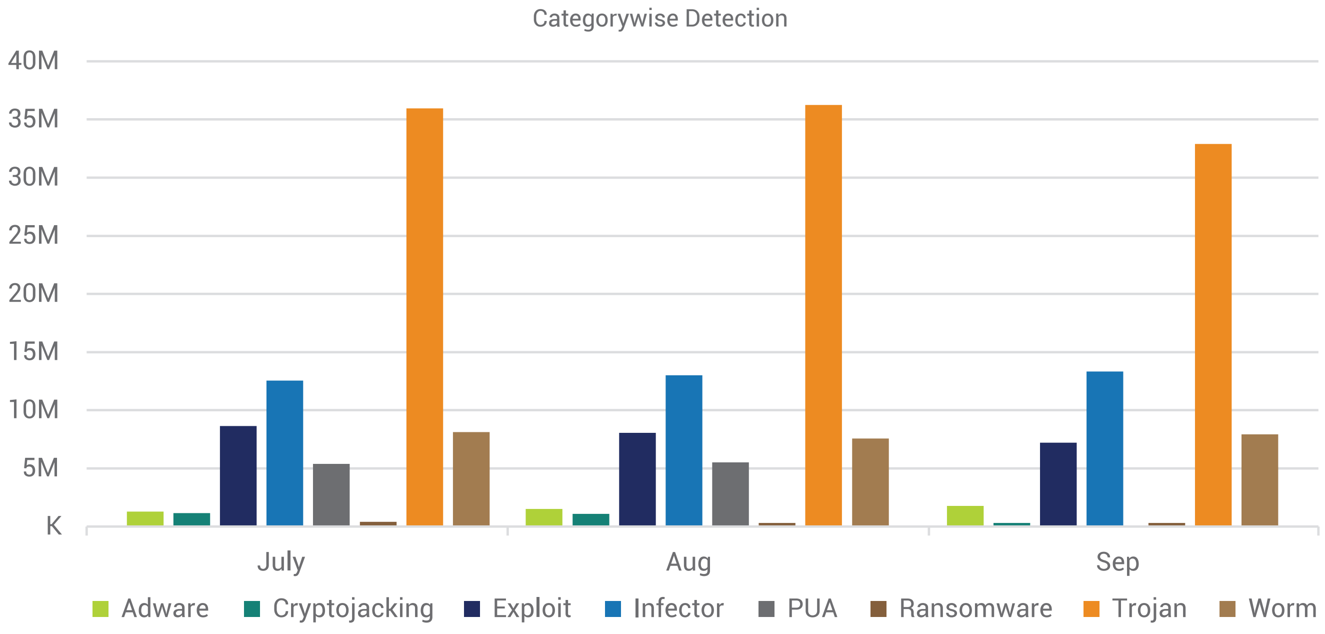
Network Scan

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

Detection Statistics – Category Wise

Below figure represents the various categories of Windows malware detected by Quick Heal in Q3 2019.



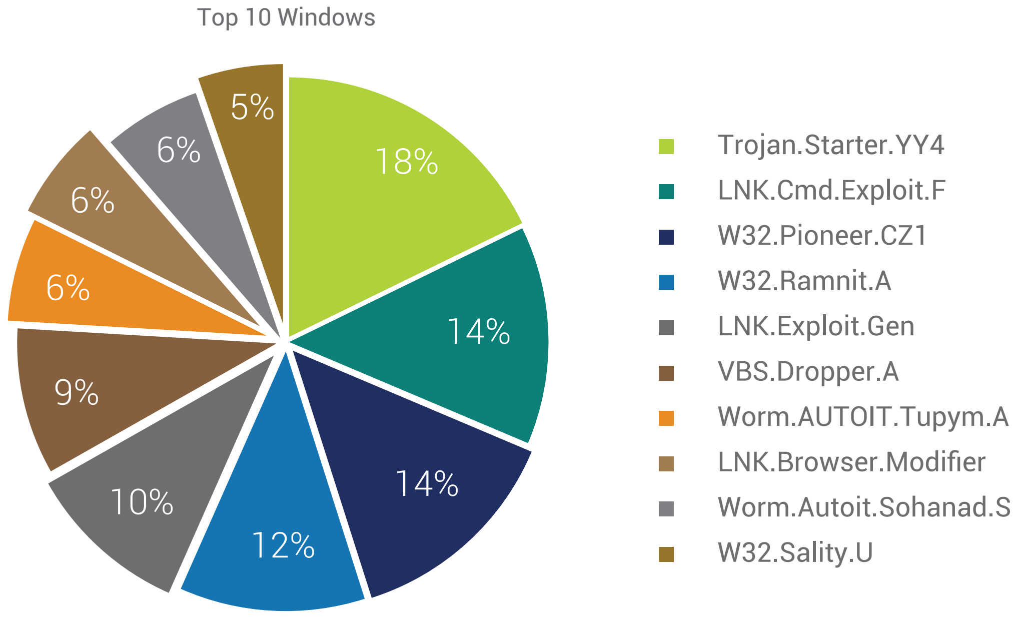


Observations

- Trojan malware was found to clock the maximum detection of 50% in every month of Q3 2019.

Top 10 Malware

The below figure represents the Top 10 Windows malware of Q3 2019. These malware have made it to this list based upon their rate of detection from Jul to Sep.



Observations

- In 2019, Trojan.Starter.YY4 was detected to be the top Windows Malware, with around 8 Million detections made in Q3 of 2019.

1. Trojan.Starter.YY4

Threat Level: High

Category: Trojan

Method of Propagation: Email attachments and malicious websites

Behavior:

- 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

2. LNK.Cmd.Exploit.F

Threat Level: High

Category: Trojan

Method of Propagation: Email attachments and malicious websites

Behavior:

- 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.

3. W32.Pioneer.CZ1

Threat Level: Medium

Category: File Infector

Method of Propagation: Removable or network drives

Behavior:

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

4. W32.Ramnit.A

Threat Level: Medium

Category: Virus

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

Behavior:

- 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 its automatic execution at every system start up.

5. LNK.Exploit.Gen

Threat Level: High

Category: Trojan

Method of Propagation: Bundled software and freeware

Behavior:

- 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.

6. VBS.Dropper.A

Threat Level: Medium

Category: Dropper

Method of Propagation: Web page

Behavior:

- 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.

7. Worm.AUTOIT.Tupym.A

Threat Level: Medium

Category: Worm

Method of Propagation: Malicious links in instant messenger

Behavior:

- 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.

8. LNK.Browser.Modifier

Threat Level: High

Category: Trojan

Method of Propagation: Bundled software and freeware

Behavior:

- 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.

9. Worm.AutoIt.Sohanad.S

Threat Level: Medium

Category: Worm

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

Behavior:

- 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.Sality.U

Threat Level: Medium

Category: File Infector

Method of Propagation: Removable or network drives

Behavior:

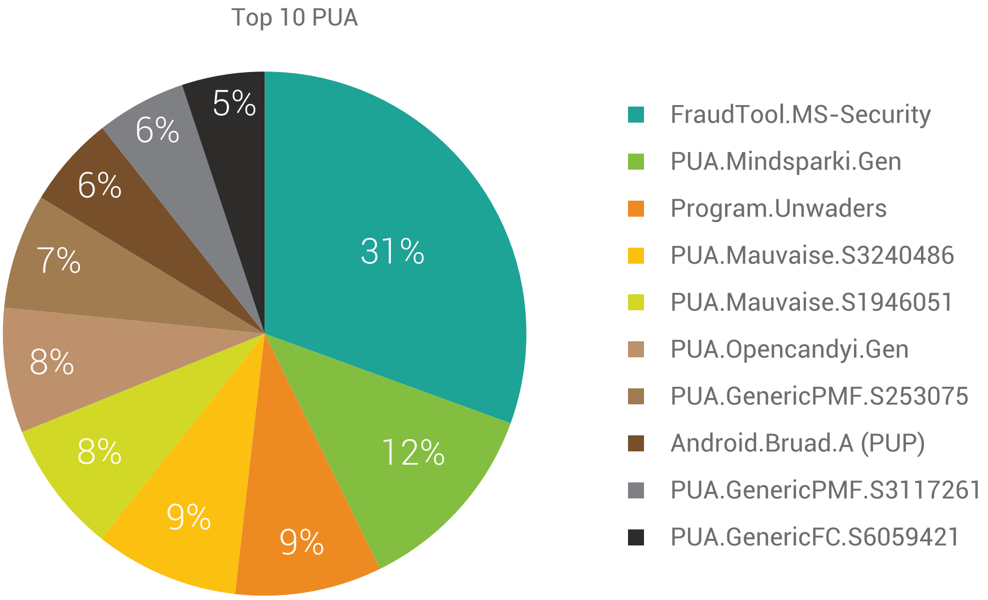
- Injects its code into all running system processes. It then spreads further by infecting the executable files on local, removable, and remote shared drives.
- Tries to terminate security applications and deletes all files related to any security software installed on the system.
- Steals confidential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

Top 10 Potentially Unwanted Applications (PUA) and Adware

Potentially Unwanted Applications (PUAs) 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 Q3 2019.

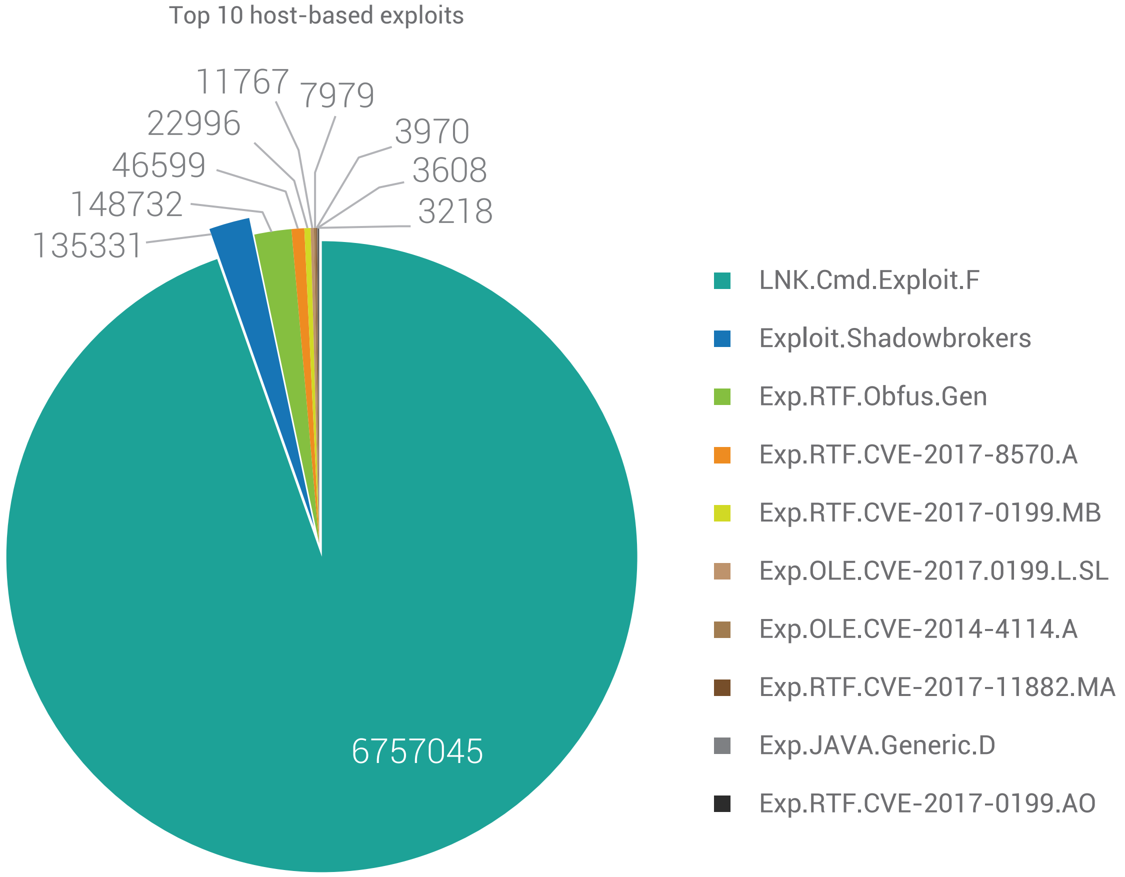


Observations

- FraudTool.MS-Security was detected to be the top PUA, with around 0.4 Million detections made in Q3 2019.

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.

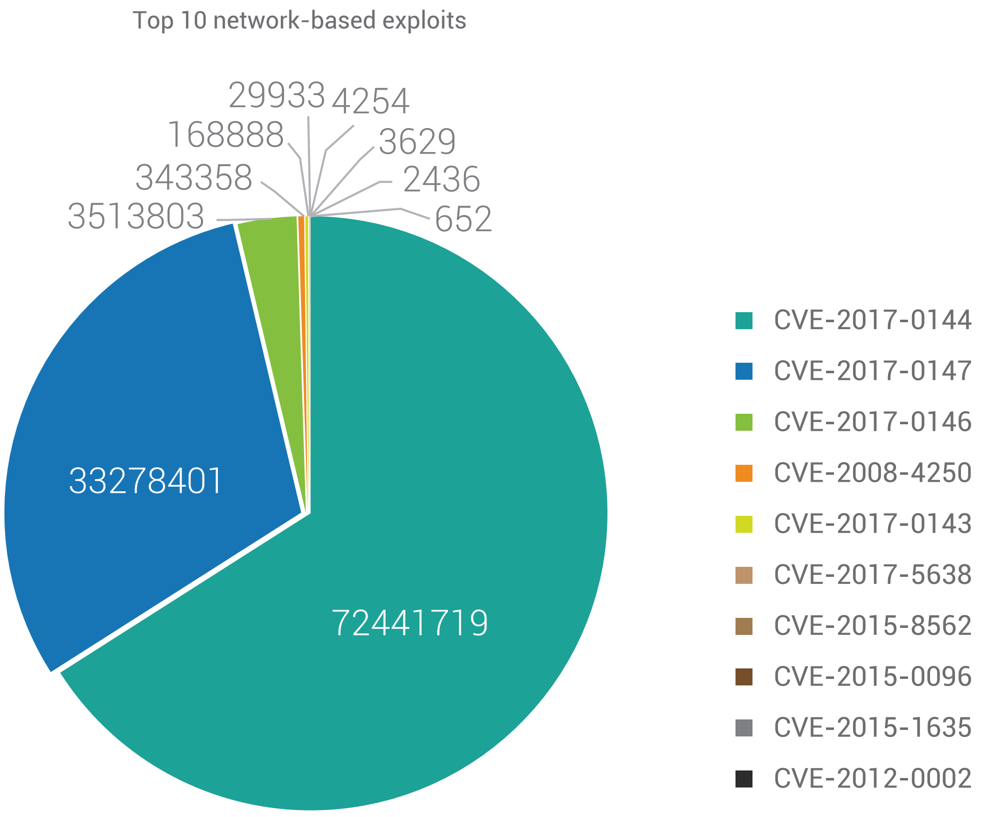


What are host-based exploits?

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 2019.



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).

Trends in Windows Security Threats

1. Exploit kits in upswing

Several exploit kits were seen in this quarter, most of which were delivered through malvertising campaigns. Once a user visits a compromised site, he is redirected to the Exploit Kit landing page. Earlier, Rig exploit kit used the flash exploit CVE-2018-4878 to distribute Azorult, Amadey, Danabot and DarkRAT malware.

The recent Lord exploit kit's landing page first collects the information about browser's version and then delivers CVE-2018-15982 (Flash Player) or CVE-2018-8174 (IE VBScript Engine) accordingly. Multiple end payloads such as njRAT, ERIS ransomware are delivered by the Exploit Kit. The newly seen Spelevo exploit kit takes advantage of exploits like CVE-2018-15982 and CVE-2018-8174 to deliver IcedID and Dridex payloads.

2. MegaCortex Returns

MegaCortex, a new ransomware family continued in 2019 by changing its way of attacking the targeted corporate world. In order to simplify its execution and increase the scale of operation, it uses command prompt and PowerShell in targeted campaigns.

This version of MegaCortex ransomware is a digitally signed sample, which encrypts files using SALSA20 encryption algorithm. To encrypt, it first scans directories and then starts the encryption process by launching another instance of itself. Upon execution, it disables or terminates services related to security software, backup servers, database servers, etc. The ransomware adds the "MEGA-G8=" marker in each file after execution, to save the time and efforts. It maintains a blacklist of around 30 file extensions. To prevent backup and recovery of user files, the shadow files are also deleted and the ransom message is dropped in the C directory.

Through the ransom note, it was observed that the attacker had an aggressive outlook towards the victim and were not ready to negotiate with the victims. The end of ransom note concludes with: "Man is the master of everything and decides everything."

Ref: https://blogs.quickheal.com/megacortex-returns/

3. Tflower Ransomware

A new ransomware named "TFlower" was discovered in July 2019 which is targeting corporate and government agencies. The road to main attack leads through hacking insecure or exposed remote desktop services. The attack proceeds with infecting the local machine and traversing through network using PowerShell, PSExec, etc.

It takes help of a known malicious file named "chilli.exe" which when run shows the infection activity which is being carried out by ransomware. It also tries to modify the windows automatic backup and repair functionality and looks to stop the repair mechanism.

The ransomware adds *tflower marker in each file. After the encryption gets over, it drops a TXT file on various locations mentioning the amount to be paid by victim, if they want their encrypted files back. In order to convince users into believing that whatever the authors are saying in the TXT file is true, they suggest users to try their decrypting mechanism once, for a single file and then decide to pay the whole amount in order to have all the files back.

Quick Heal successfully detects this threat via its multilayered detection.

4. Importance of choosing the right Operating System and Upgrading it on time!

Operating System is a really important factor for any Computer/Host. As choosing an Operating System which is user-friendly and easy to use is important, it's equally important to choose one, where the vendor regularly provides you with updates/patches for the core functionalities and security issues in it. Windows 7 is one of the most loved client-side Operating System worldwide. However, it's reaching End of Support in next couple of months.

Here is Microsoft's official statement on this:

"The specific end of support day for Windows 7 will be January 14, 2020. After that, technical assistance and software updates from Windows Update that help protect your PC will no longer be available for the product. Microsoft strongly recommends that you move to Windows 10 sometime before January 2020, to avoid a situation where you need service or support that is no longer available."

Ref. https://support.microsoft.com/en-in/help/4057281/windows-7-support-will-end-on-january-14-2020

Microsoft has already ended official support for few other old, popular client-side Operating Systems like Windows XP, Windows Vista, etc. in past. But, as per our observations, many users continue to use these Operating Systems on their computers, unaware of the security risk it creates. These Operating Systems which had reached End of Support, were found vulnerable to some devastating attacks like WannaCry and BlueKeep. Microsoft went out of the way and provided security patches for these old Operating Systems. But this might not happen always. Attack surface for these Operating Systems will continue increasing over the time and hence it's wise for the customers to upgrade to the latest Operating System as soon as possible.

Here is the percent wise distribution of attacks that Quick Heal has blocked.

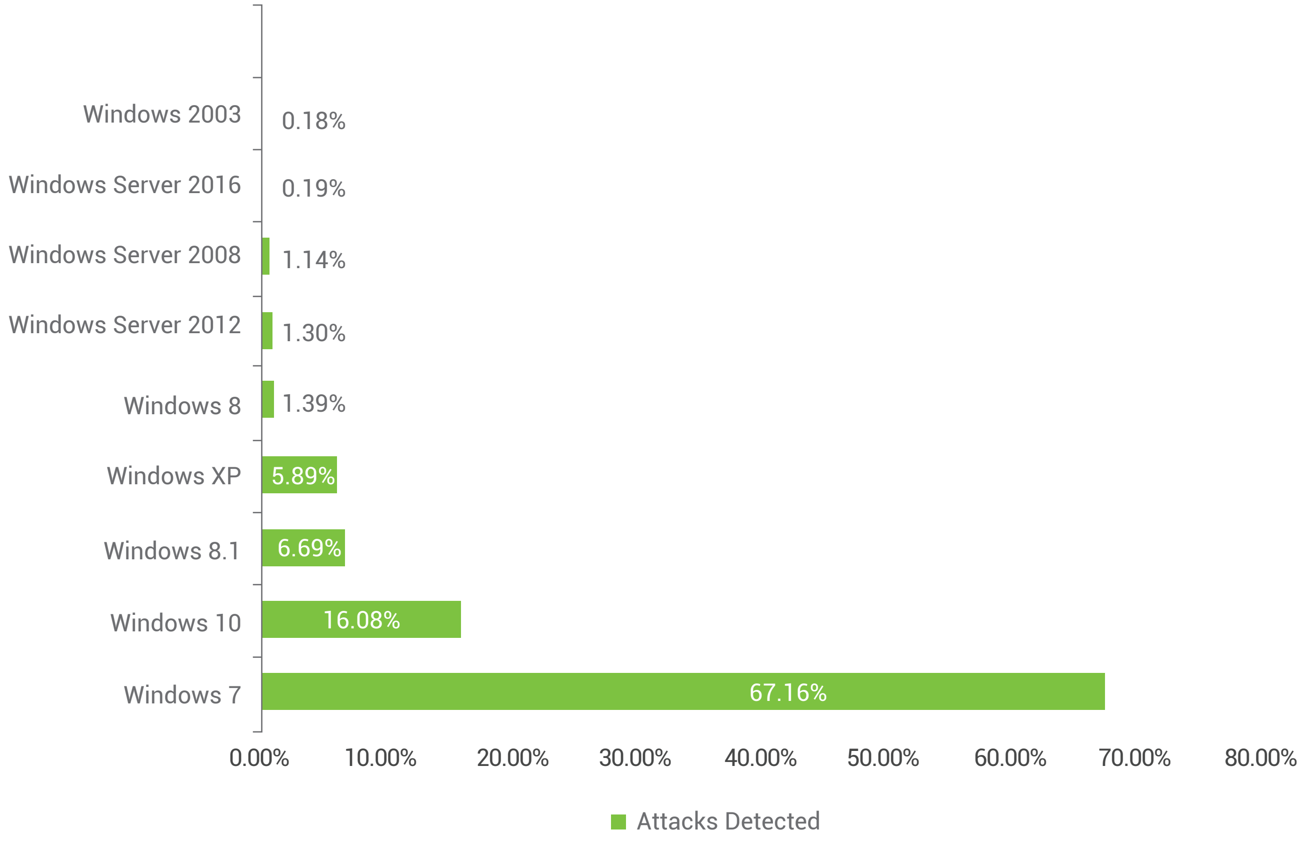


Fig. 1 – Operating System wise distribution of Attacks Detected in Q3 -2019

The above chart shows that Windows XP is still being used by customers almost 5 years after Microsoft ended its extended support. We suspect the same trend will continue in case of Windows 7 as well. QH has detected 67.16% of attacks on Hosts running Windows 7 in just one quarter (Jul-Sep 2019). As Windows 7 is nearing its End of Support very soon, we urge all our customers to upgrade their hosts running Windows 7 to latest supported Operating System well in time.

5. Emotet: A new mask on the dark face

Emotet is now a familiar name in cyber security world. It was the most severe threat last year. It never deviated from its nature of coming frequently in intervals with different techniques and variants, to deliver malware on a victim machine. After a prolonged break, a new variant has been observed with a new wrapper blending and some complex obfuscation techniques. But the interesting thing we noticed is that the main payload inside the file remains the same. So again, it is emphasizing that the choice of advanced layer of protection is critical over conventional signature-based approach, to stop such complex malware campaigns. Emotet is continuing its faith on malspams for spreading.

We have seen journey of Emotet from a banking trojan to a complex threat distributor. Emotet malware campaign has existed since 2014. Initially, Emotet campaign used to spread through malspams with PDF and JS file attachments. Later on, it started exploiting MS Office Word documents with a heavily obfuscated macro inside it. It mostly targeted the websites based on PHP using vulnerabilities like Arbitrary File Upload, Direct access to XMLRPC.php for brute-force attacks, remote privilege escalation, Cross site scripting and Information disclosure vulnerabilities to get root access of a server.

Security measures to follow:

- Don't open any link in the mail body sent by an unknown source.
- Don't download attachments received by an untrusted source.
- Always turn on email protection of your antivirus software.
- Don't enable 'macros' or 'editing mode' upon execution of the document.

6. Stop: Rampant appending of extensions!

With 150+ extensions in the wild, STOP (.djvu) can be considered today's most widespread Ransomware with its share around 35%. Although it's been more than a year, we have seen upgraded versions with more infections in the recent quarter.

The infection vector for this particular ransomware is cracked software from internet. The main advantage is, the user usually tends to allow these cracked software, even when antivirus does not allow it. Over the period, STOP has been observed to use a complete framework to mitigate current detection techniques, whether it may be a newer extension, newer obfuscation techniques or even anti-emulation techniques. According to our observations, crack files or activators for different software like Tally, Mincraft, Nero 7, Autocad, Adobe Photoshop, Internet Download Manager, Cyberlink Media Suite, Microsoft Office, VMware Workstation, DreamWeaver, Corel Draw Graphic Suite, Quick Heal Total Security, Ant Download Manager, IBEESOFT Data Recovery, Any Video Converter Ultimate were seen spreading this ransomware.

The encryption is carried out with the salsa20 algorithm. There are 2 types of encryption: 1. Online Key Encryption 2. Offline Key Encryption. In first case, the encryption key is calculated at the server's end and then used to encrypt files on the victim's system. Here, it's mandatory for the system to have an internet connection. On the other hand, in the second case if the system is not connected to the internet, it uses the predefined encryption key. So, it says that in second case decryption is possible where the key is predefined. The encryption is carried out with the Salsa20 algorithm.

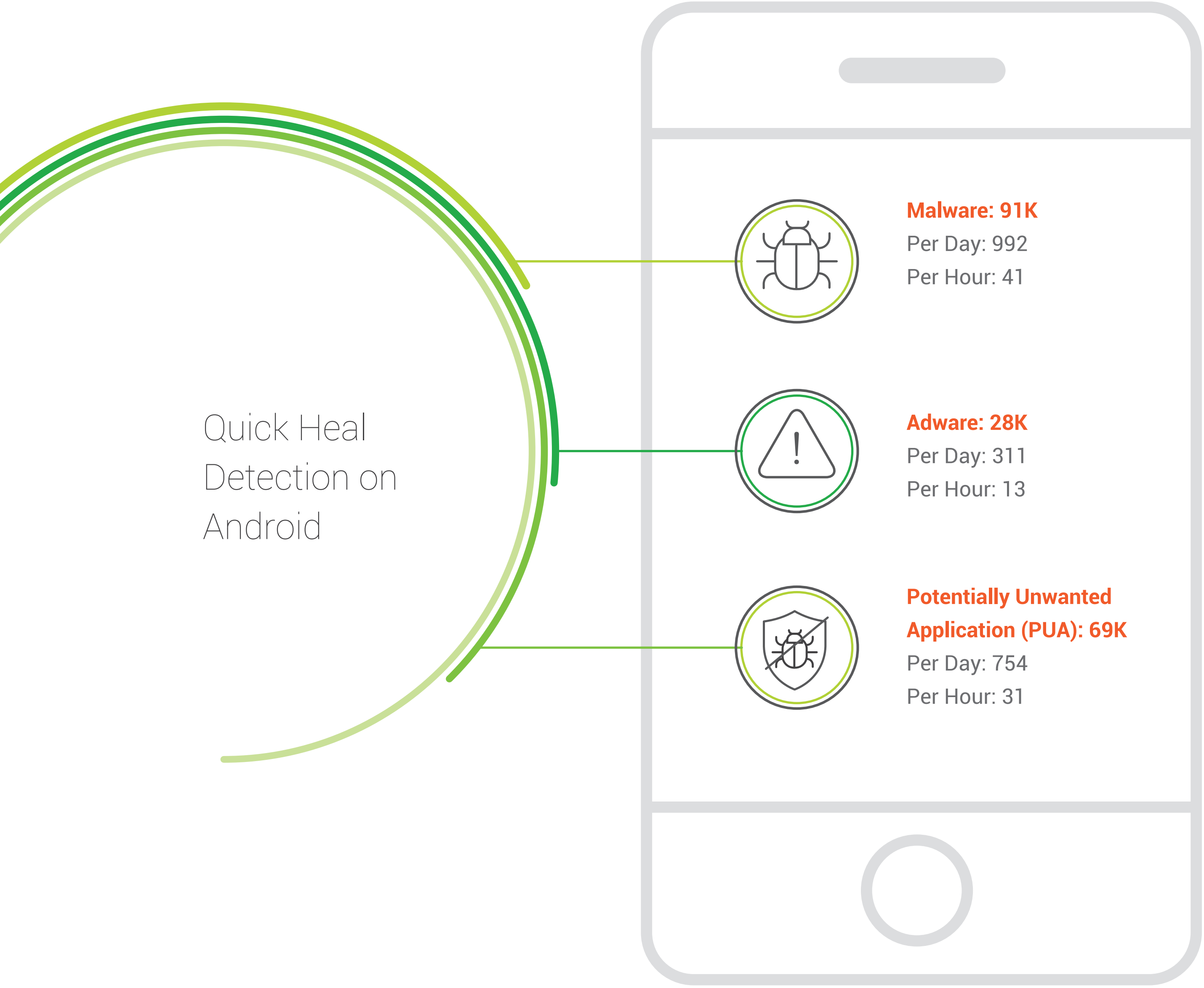
With the continuous introduction of newer extensions, STOP authors keep on adding different software cracks to their infection list. For every new extension, their online CnC servers stay active for a limited period only. After that, it switches to another extension. The usual ransom amount is $980 for which they offer concession of 50% if paid within 48 hrs of encryption.

Here are few tips to help our users stay protected:

1. Do not use/ download crack applications.
2. Do not install software from untrusted sources.
3. Always update your antivirus.
4. Do not allow suspicious/ malicious applications to run.
5. Backup your data.

ANDROID

Quick Heal Detection on Android



Quick Heal Detection on Android

Malware: 91K

Per Day: 992

Per Hour: 41

Adware: 28K

Per Day: 311

Per Hour: 13

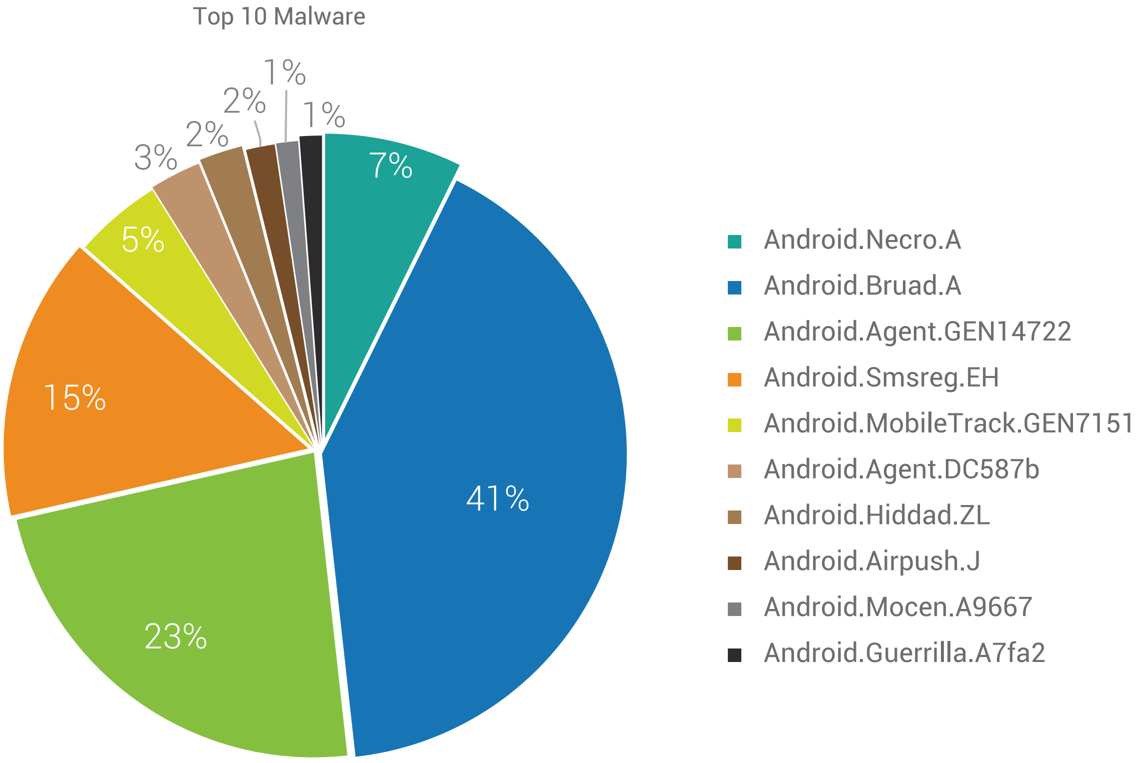
Potentially Unwanted Application (PUA): 69K

Per Day: 754

Per Hour: 31

Top 10 Malware

Below figure represents the top 10 Android malware of Q3 2019. These malwares have made it to this list based upon their rate of detection during the period of Jul to Sep in 2019.



1. Android.Necro.A

Threat Level: High

Category: Malware

Method of Propagation: Google play

Behavior:

- This dropper malware found in CamScanner, the famous legitimate app for PDF creator having 100 million+ downloads.
- It carries encrypted malicious module in its asset directory and it decrypt that module at run-time in background.
- In the background it Connect to C&C server and starts malicious activity.
- These malicious modules may show ads and sign up for paid subscriptions.

2. Android.Bruad.A

Threat Level: Medium

Category: Potentially Unwanted Application (PUA)

Method of Propagation: Third-party app stores

Behavior:

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

3. Android.Agent.GEN14722

Threat Level: High

Category: Malware

Method of Propagation: Third-party app stores

Behavior:

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

4. Android.Smsreg.EH

Threat Level: Medium

Category: Potentially Unwanted Application (PUA)

Method of Propagation: Third-party app stores

Behavior:

- It sends device IMEI and IMSI to premium rate numbers via SMS.
- It collects device information like SDK type, SDK version, phone company, phone number etc.
- It sends the collected data to a remote server

5. Android.MobileTrack.GEN7151

Threat Level: Low

Category: Potentially Unwanted Application (PUA)

Method of Propagation: Third-party app stores

Behavior:

- It's a mobile tracker application.
- Sends the user's device location via SMS to an external server.
- Checks if the device's SIM is changed or not by identifying the IMSI number.
- Sends an SMS after SIM change or phone reboot with specific keywords in body.
- Collects device information such as IMEI and IMSI numbers

6. Android.Agent.DC587b

Threat Level: High

Category: Malware

Method of Propagation: Third-party app stores

Behavior:

- Application has no icon, so not visible to user and working in background.
- In installed applications it shows default android icon, so disguise as system app and remain unnoticeable
- It decrypts payload at run-time and further loads it dynamically.
- It registers many receivers and services to perform malicious activity.

7. Android.Hiddad.ZL

Threat Level: Medium

Category: Adware

Method of Propagation: Google Play

Behavior:

- All of these apps use a common SDK (Software Development Kit) for advertising.
- This malware family shows Ads, opening URLs in browser & receiving commands from C&C server to perform activities.
- It is also able to hide its icon in app launcher making it difficult to notice its existence but runs in the background
- Intention of these apps seems to generate as much ad revenue as possible.

8. Android.Airpush.J

Threat Level: Low

Category: Adware

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

Behavior:

- Displays multiple ads while it is running.
- Shares information about the user's device location with a third-party server.
- 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.

9. Android.Mocen.A9667

Threat Level: Low

Category: Adware

Method of Propagation: Google Play

Behavior:

- These apps disguise as photography or gaming applications.
- If the app has been installed for more than 30 minutes, the app will hide its icon and create a shortcut on home screen. This trick is used to remain uninstalled by dragging and dropping its icon to the uninstall section of the screen.
- It shows full screen ads and users are forced to view the whole duration of the ad before being able to close it.

10. Android.Guerrilla.A7fa2

Threat Level: Medium

Category: Potentially Unwanted Application (PUA)

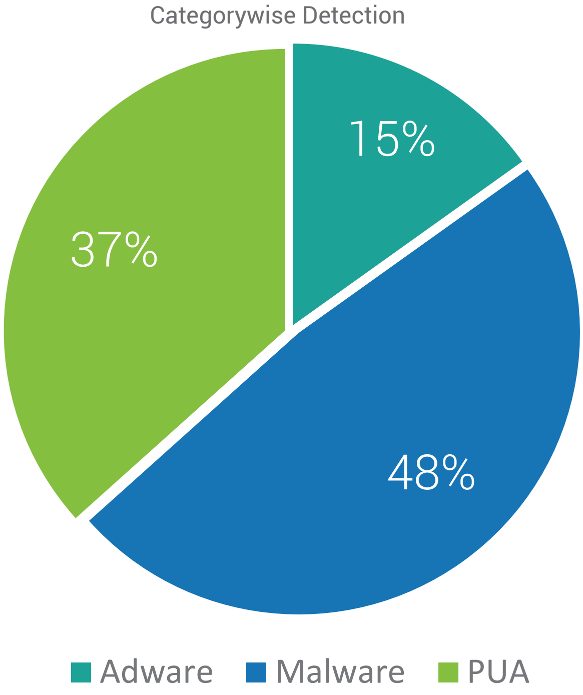
Method of Propagation: Third-party app stores and repacked apps

Behavior:

- It does not have icon and in installed package list it shows app name as xhelper.
- It carries payload with it in encrypted form and drops that file with .jar extension on the affected devices.
- Further load that file to perform malicious activity on device to collect data like brand, screen size, MAC address etc.
- It may push notification and after clicking on it redirects to other websites

Android Detection Statistics: Category Wise

Below figure represents the various categories of Android malware detected by Quick Heal in Q3 2019.

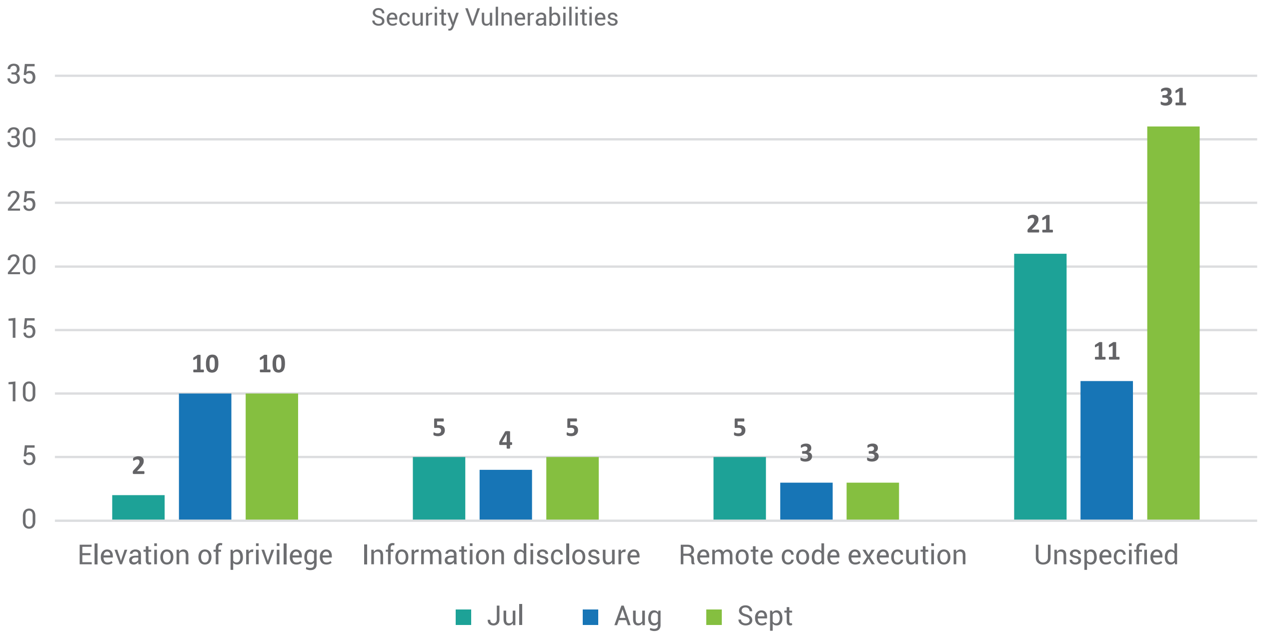


Observations

- Malware clocked 48% of the total Android detections in Q3 2019.

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 Jul to Sep of 2019.



Source: https://source.android.com/security/bulletin/2019

Trends in Android Security Threats

1. Some Android apps bypass permissions to access user data

Over the years, app permissions have become a powerful privacy tool, allowing users to decide which data an app can or cannot access on their smartphone. However, a new study by International Computer Science Institute (ICSI) claims that thousands of Android apps can access restricted data even when users deny them permission. The study was presented at the Federal Trade Commission's PrivacyCon in Washington DC on 27 June.

The study examined more than 88,000 apps on Play Store, and how they accessed user data on the smartphone, to find 1,325 of them were flouting Android app permissions and using covert channels to access user data. Covert channel is when an app, which has been denied permission by users, starts communication with another app that has been granted the permission to access the same data. For this, apps use common SDK (software development kit) libraries embedded within the app.

Researchers note that Android OS protects users by sandboxing the user space in apps, so that they cannot interact arbitrarily with other apps. However, developers integrate third-party libraries in their software for things like crash reporting, analytics services, social-network integration and advertising. So, if an app can access the user's location, then all third-party services embedded in that app can access it, too.

REF- https://www.livemint.com/technology/apps/some-android-apps-bypass-permissions-to-access-user-data-1562866717031.html

2. Android Ransomware is back and is spreading via SMS

Android ransomware is back this quarter but, this time it is spreading via SMS, with a malicious link. After receiving an SMS, if the user clicks on that link, then installation prompt is shown and if user grants the required permissions, then it starts its malicious activity. It sends same SMS to all contacts present in user's contact list and starts file encryption by '.seven' extension. It then shows the ransom note with ransom amount, User ID, BTC address. In ransom note, it mentions that "*if anyone removes the app, the ransomware will not be able to decrypt the files. To draw ransom through Bitcoin address, it communicates with its C&C server*"

Quick Heal detects it as ***Android.Filecode.A***

3. Agent Smith

This malware mostly comes through third-party App stores. These Apps look like genuine apps but in the background they infect pre-installed clean applications. Some of them are WhatsApp, MXplayer, ShareIt, Opera, etc. For infecting clean apps, they drop an encrypted module or payload into the respective clean app's directory.

The payload contains up to six modules namely Loader, Core, Boot, Patch, AdSDK and Updater. Further, it decrypts the payload and shows a pop-up of the update. Due to the vulnerability named as Janus and Man-in-the-Disk, Agent Smith can make it possible. After up-gradation of clean apps, they show full-screen ads.

In last quarterly report, we already discussed these malware which use Janus vulnerability. The same malware is back and named as Agent Smith.

Quick Heal AV detects such malicious apps as ***Android.Infdas.A.***

4. Malicious applications found on Google Play and removed after QH reported it to Google

a. 27 Dropper Apps Found On Google Play

27 dropper applications were uploaded by a malware author on Play Store through some anonymous developer account. These dropper applications continuously show installation prompt for fake "Google Play Store".

If any user falls prey to this trap and installs the Fake "Google Play Store" app through these prompts, this newly installed fake "Google Play Store" hides its icon after launch. Further, it shows aggressive advertisements in random intervals and makes an illusion that it is from the Official "Google Play Store".

Theses apps are now removed from the official Google Play Store, after Quick Heal Security Labs reported the same to Google.

Quick Heal AV detects such malicious apps as **Android.HiddenAd.A**

REF - https://blogs.quickheal.com/alert-27-apps-found-google-play-store-prompt-install-fake-google-play-store/

b. 11 Free Mobile Anti-virus apps you are using can actually be Fake!

11 Apps with genuine looking names like Virus Cleaner and Antivirus security, which appear to be genuine anti-virus (AV) or virus-removal apps, have been spotted on Google Play Store and have seen over a lakh of downloads already. These apps are removed by Google after being reported by Quick Heal. These AV apps mimic the functionalities of a real AV App and have functions like "scan device for viruses". The main purpose of these apps is to show advertisements and increase the download count. These apps don't have any AV engines or scan capabilities except a predefined list of Apps marked as malicious or clean. This list appears to be static and we haven't seen it getting updated during our analysis. The fake AV app contains predefined package lists, like whiteList.json with few whitelist package names, blackListPackages.json with few blacklist package names and blackListActivities.json with a list of blacklisted activities.

Quick-Heal security lab detects it by **Android.FakeAV.E (PUP).**

REF - https://blogs.quickheal.com/free-mobile-anti-virus-using-can-fake/

c. 29 Aggressive adware found on Google Play with high download count

Quick Heal Security Labs reported 29 malicious apps found on Google Play Store, which were removed afterwards. It has a collective download count of more than 10 Million.

One of the Apps from this set, named "Multiapp multiple accounts simultaneously" has crossed 5 million installs already.

Out of these 29 malicious Apps, 24 are from HiddAd category. The HiddAd Apps hide their icon after first launch and create shortcut on Home Screen. Clear purpose of this action is that users should not be able to uninstall it by just dragging the icon.

When users launch the App through the shortcut, these apps show full screen ads on device screen. Few of these Apps can show adds even when the device is in idle state and the App is not in active use. Most of these Apps are of Photography category and are similar to previous HiddAds found on Google Play Store.

The remaining 5 Apps from above list are of Adware category and would generally enter user's Android phones through advertisements. We found out that two such apps have crossed 1 million+ downloads, which proves that many users have already been tricked into downloading this App and they end up with annoying advertisements

Quick-Heal security lab detects it by **Android.Magnify.A (Adware)**

REF - https://blogs.quickheal.com/quick-heal-reports-29-malicious-apps-10-million-downloads-google-play-store/

5. Spyware Back in attack

Recently we came across some spyware applications, which right after the launch, ask for language selection like English or Farsi and also ask for a fake user registration. The apps ask user for permission to access storage and contacts. Since the app looks like a genuine app, user generally accepts the request and grants the requested permissions. The app then shows some genuine activities to make the user think that it is a genuine app. But, in the background, it gathers all SMSs, contacts, files and sends it to its C&C server. These apps use some predefined malicious codes from author AhMyth.

Quick Heal detects it as ***Android.Spy.AH***

6. Analysis of Joker — A Spy & Premium Subscription Bot on GooglePlay

Some of the malicious apps, popular by the name "the Joker" (which was borrowed from one of the C&C domain names) were found on the Google play store, which contain the capability to steal all of victim's data and device information. This spyware communicates with its C&C server in specific time intervals to fetch and execute the commands. In 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 of the authorization codes for premium service subscriptions. Further it encrypts the contact list and sends it over the C&C server.

Quick-Heal security lab detects it by ***Android.AgentJoker.A.***

7. Funckybot

This malware campaign targets Japanese users. It intercepts SMS messages sent to and from infected devices. It uses an open source library that can be found on Github to keep the service alive on the device. It also allows the malware to mute sounds from the device.

Funcky bot harvests the victim's list of contacts for propagation purposes. It generates an SMS message that will be sent to everyone on the list. The malware is also able to set itself as the default SMS handler application, and uses this to upload all the received messages to the CNC server. This functionality can be very dangerous, considering that most banks currently use two-factor authentication through SMS.

8. CamScanner the Dropper

CamScanner, the famous legitimate app for PDF creation having 100 million+ downloads, was recently found to be malicious. CamScanner Version 5.11.7 was found as a dropper as it carried an encrypted malicious module in its asset directory. For performing malicious activity, it decrypts that module and communicates with C&C server. It can perform unauthorized ad clicks and show aggressive ads to the app user. In the latest version, CamScanner has removed the malicious modules and third-party ad library. Quick-Heal detects the CamScanner versions that had a malicious module as Android.Necro.A.

Conclusion

The third quarter of 2019 was full of action, with several previously discovered malware and Ransomware making a strong comeback in the form of new variants like MegaCortex, TFlower and others. Interestingly, these malware have not only evolved in terms of variants but also their mode of attack. This attributes for the rise in malware from 242 million in Q2 to a staggering 257 Million in Q3 of 2019.

One particular Ransomware that continued to rock the cyber world with frequently appearing and evolving variants is Emotet. This time along, the Ransomware has been observed with a new wrapper blending and some complex obfuscation techniques.

However, the Ransomware identified to have most widespread share of 35% was "STOP Ransomware" with around 150+ extensions in the wild. As per observations by Quick Heal Security Labs, crack files or activators for different software like Tally, Mincraft, Nero 7, Autocad, Adobe Photoshop, etc. have been found to spread this ransomware.

While Ransomware continues to create havoc and be the topmost threat for consumers, Crypto Mining attacks are fast picking up pace. This is evident from the recent attacks on Android based IoT devices wherein, cryptocurrency-mining botnets named Trinity and Fbot tried to take control over tens of thousands of unsecured Android devices via open ADP port.

While these cryptomining botnets are here to stay and will only continue to evolve with time, it is clear that android-based IoT device owners need to keep their eyes open for this malware trend and take every necessary measure to ensure the security of their device, when exposed to the internet.

Most Android based devices and phones today come inbuilt with security features. However, none of these can ensure you with the kind and level of security that a robust Antivirus designed with advanced security features can provide.

Every single day there is a new cyber scam or cyber-crime affecting the lives of common internet users. The only way to protect yourself from such attacks, is to be precautious of things that we share or do while being connected to the internet, as it costs nothing to be safe than sorry!

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