Quick Heal

Security Simplified

Quick Heal
ANNUAL THREAT REPORT
2020

www.quickheal.com

CONTRIBUTORS

Security Labs
Content Marketing

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

EXECUTIVE SUMMARY

The Quick Heal Annual Threat Report 2020 collates and publicizes threat intelligence gathered by Quick Heal Security Labs from millions of product installations and active license user base. The report provides deep insight on threats and attacks that unfolded in the realm of cybersecurity in the year 2019 – divided into two sections viz. Windows and Android.

Our comprehensive report begins with significant threat predictions that we had made for the year 2019 and that turned out to be true as the year progressed. This can be attributed by the comparative YoY graphical representation of malware detections made in 2019 as against 2018, which goes on to explain that 2019 indeed was a year that witnessed significant rise in malware attacks.

While cybersecurity experts made it a point to give a hard time to cyber criminals, there were several previously discovered malware variants that continued to work in the wild and reappeared as new variants in 2019. Our report cites some of the top cyber-attack stories that created havoc in 2019, bringing the focus back on existing and new cyber-attack vectors.

An interesting and significant section of this annual report are the Heat Maps that narrow down the malware detections to the State and City level. These maps provide a fair understanding of the regional threat landscape and the fact that it's not just the metro and bigger cities that are under risk of attack, but even the security of smaller cities are at stake.

Furtheron, the report throws light upon Windows malware detection highlights of 2019 – a breakup of detections made per day, per hour, per minute followed by a graph showing the quarter that clocked the highest detections in 2019, top 10 Windows malware, top 10 exploits, top 10 PUAs and Adware. This section is sealed with some interesting trends that have been observed in Windows Security threats in 2019.

Yet another significant section of the annual threat report is the Android malware detection highlights of 2019, which again provides a deep dive into per day, per hour, per minute detections, followed by the top 10 Android malware of 2019. The section concludes with some comprehensive insights on the trends observed in Android Security threats in 2019.
The best part of this annual threat report however comes towards the end, with Quick Heal Security Labs making significant Cybersecurity Predictions for 2020.

WORD OF CAUTION FROM OUR CTO

> “No matter from which device the user is connected to the internet, the risk of your data or privacy getting hacked continues. So, look for security solutions that can protect you at all vulnerable endpoints.”

ABOUT QUICK HEAL

Quick Heal Technologies Limited is one of the leading providers of IT Security and Data Protection Solutions with a strong footprint in India and an evolving global presence. Incorporated in the year 1995, it is an all-round player in cybersecurity with presence in B2B, B2G and B2C segments across multiple product categories – endpoints, network, data and mobility.

ABOUT QUICK HEAL SECURITY LABS

With its state-of-the-art R&D centre and deep intelligence on the threat landscape, Quick Heal helps in simplifying security by delivering the best in class protection against advanced cyber-threats. Its portfolio includes solutions under the widely recognized brand names 'Quick Heal' and 'Seqrite' across various operating systems and devices.

www.quickheal.com
Follow us on:

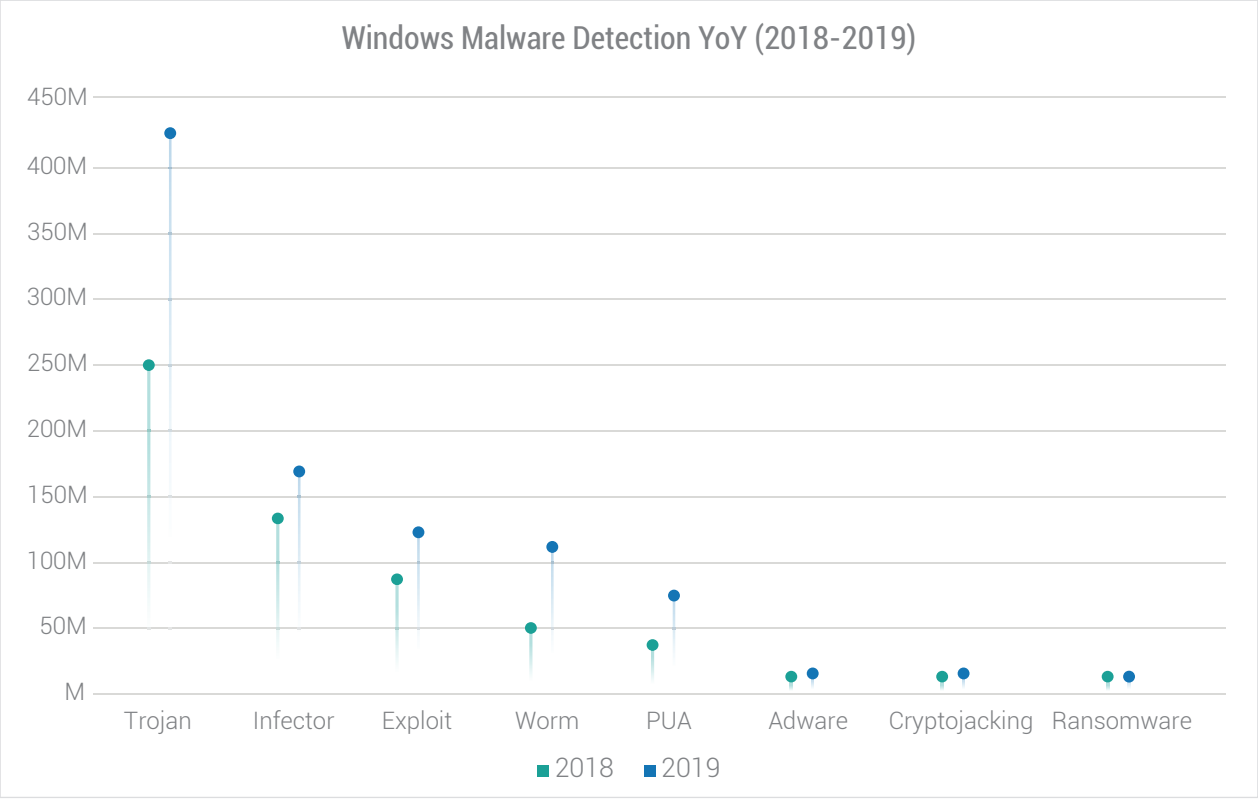
2019 PREDICTIONS THAT TURNED OUT RIGHT

Our 2019 Predictions that proved right:

- Increase in Web Skimming attack
- Projected rise in Ransomware attacks targeting utility infrastructure
- An increase in targeted IoT-based attacks http://bit.ly/2KlxCac
- Mobile landscape expected to become more threat-prone in 2019
- Rise in targeted attacks to exploit supply chain vulnerabilities
- Data protection to become essential due to data-centric attacks
- Cryptomining and cloud-based attacks to rise

WINDOWS DETECTION STATISTICS 2019

The below graph represents the statistics of the total Windows malware detected by Quick Heal Security Labs, along with a YoY comparative view of detections made in 2019 as compared to 2018.



TOP CYBER-ATTACK STORIES OF 2019

1 BlueKeep Attacks seen in the wild!

RDP is Remote Desktop Protocol, typically used for taking remote control of a Windows machine. For most of the home users, RDP functionality is not required. It's typically used in offices for accessing remote hosts.

CVE-2019-0708, popularly known as BlueKeep, is an RDP pre-authentication vulnerability which allows attacker to compromise a vulnerable system without user's interaction. This exploit is also wormable, meaning that it can spread to other vulnerable systems in a similar way as the WannaCry malware spread across the globe in 2017. Interestingly, healthcare products like radiography, X-ray and other imaging software of various healthcare vendors running on Windows OS are also affected by the BlueKeep exploit. Since the time this vulnerability was patched by Microsoft, multiple PoCs exploiting it have emerged in public. In September, exploit code for this vulnerability was added in the popular exploitation framework, Metasploit for triggering DoS. Chances are that, script kiddies would jump on this Metasploit module to carry out large scale attacks on vulnerable hosts with RDP port open to Internet. Recently, attackers exploited this vulnerability for dropping cryptocurrency miner on the unpatched vulnerable machines.

2 Widespread Javascript Skimmer – Magecart

Every day we hear about new attacks and new vulnerabilities getting surfaced in threat landscape, prominent ones in this are web skimming attacks like Magecart. Web skimming is a form of internet fraud, where attackers compromise an ecommerce website to inject malicious scripts in its payment page, to collect user's sensitive data like customer name, credit card number, expiry date, CVV number, etc. This collected information is then sent to remote attacker-controlled server, which is ultimately sold on darkweb.

Magecart mainly targets Magento based e-commerce websites like ticketing, touring, flight booking services, shopping, cosmetics, healthcare etc. There are multiple ways through which Magecart gets entry into the payment pages. One way is by directly compromising a website and injecting heavily obfuscated javascript code into the payment page itself. Other way is to employ supply-chain attack strategy and compromise third-party or externally hosted libraries, to deliver the malicious scripts. We have seen a surge in such attacks this year.

3 Android based IoT devices with open ADB port - A low hanging fruit for Crypto-miners

IoT devices like smart TV, phones, IP Cameras, etc. are powered by processors that run either Android or stripped-down versions of Linux operating system. These devices use ADB Port (Android Debug Bridge), which is part of the Android SDK, to manage communication between other nearby devices. The IoT devices with certified version of Android come with the ADB port disabled by default. However, there are several smart TV manufacturers that sell these TV's with uncertified versions of Android, having the ADB port open. In addition, many a times, users manually enable debugging, for side loading of apps like Netflix and Hotstar on their smart TV's. This again causes the ADB port to be left open and vulnerable. Attackers can use this ADP port to install malicious apps, drop malware like miners and steal any data from these devices.

Since, the ADB port does not require any authentication, it becomes easy for cyber criminals to exploit the port and make changes in the target device. Using this port, attacker can take complete access of the device including its app installation, webcam, etc. Once installed, the botnet spreads to other connected devices making them susceptible to attack.

In recent times, there have been cases of botnet attacks named Trinity and Fbot, fighting to take control over tens of thousands of unsecured Android devices via ADB port 5555 and run crypto-miners on the infected devices.

4 Fake Sextortion: Ransom for your Cyber Habits

"I do Know xxxxxx is one of your passwords. Let's get straight to the purpose."
Ever received this kind of message in an email? That's how a common fake sextortion mail starts! Attacker initially retrieves one of your account's credentials somehow, and then sends mail to you claiming that they have got full access to your computer. They claim to have gained access to the victim's system by exploiting RDP or using RATs (Remote Access Tools).

"Last year, electronic extortion complaints rose 242% to 51,146 reported crimes, with total losses of $83 million." says CNBC (https://www.cnbc.com/2019/06/17/email-sextortion-scams-on-the-rise-says-fbi.html). Mostly, this is just a game of human psychology. The attackers usually do not have anything against the victim, but by using few techniques, they just manage to retrieve victim's password from internet and claim to have access to victim's computer or webcam. These scammers do not have any proof like photos or videos against the victim, but by pretending they hacked the account, they ask for considerable amount of money.
Here is an example of the fake sextortion mail:

This account is hacked! Change the pswd this time!
You might not know me me and you obviously are most likely interested why you are reading this particular letter, is it right?
I'mhacker who exploitedyour email boxand digital devicestwo months ago.
Don't try cut to communicate with me or seek for me, it's not possible, since I sent you this message using YOUR hacked account.
I have set up spyware to the adult videos (porn) website and suppose that you enjoyed this site to enjoy it (think you understand what I really mean).
Whilst you were keeping an eye on videos, your internet browser started out functioning as a RDP (Remote Control) having a keylogger which granted me permission to access your display and webcam.
Afterward, my software programstoleall data.
You put passwords on the web services you visited, I sniffed all of them.
Surely, you are able change them, or have already modified them.
But it does not matter, my app renews information every 5 minutes.
And what I have done?
I got a reserve copy of the system. Of all files and each contact.
I have managed to create dual-screen videofile. The 1 section presents the film that you were observing (you've a good preferences, wow...), the second screen presents the video from your own web camera.
What should you do?
Great, in my opinion, 1000 USD will be a inexpensive price for our little riddle. You'll make the deposit by bitcoins (if you do not know this, go searching "how to buy bitcoin" in any search engine).
My bitcoin wallet address:

13Epn22pqjdTkpyUCHiWTYs1ysqm5PsVrz

(It is cAsE sensitive, so just copy and paste it).
Important:
You will have 2 days to make the payment. (I put an exclusive pixel in this email, and at this moment I know that you have read this email).
To tracethe reading of a letterand the activityin it, I installeda Facebook pixel. Thanks to them.
(The stuff thatcan be usedfor the authorities should helpus.)
If I fail to get bitcoins, I shall certainly send your video to each of your contacts, including relatives, colleagues, and many more?

Why do people panic?

1. Mostly attackers use generic statements that can be personalized to everyone (like: 'At the moment, I have harvested a solid dirt...on you...I saved all your emails and chats from your messengers. I also saved the entire history of sites you visit'). So, victim thinks the person behind the mail knows him/her.

2. Attackers mention the hacked password in the mail so the victim thinks that he has got access to everything. Sometimes, these passwords are not even the correct email passwords. Hence, there is less risk involved here for the user. But in such cases, immediate password strengthening is required.

3. Attacker claims to have gained access to user's contacts and they threaten to leak data publicly or specifically to these contacts.

4. Users who watch porn would panic when someone claims that they know about the adult content they have been watching online. Attackers sell fear by mentioning that they have recorded the video of victim watching adult contents.

In some of the cases, instead of bitcoin wallet numbers, victims are provided links for online payment. When this link is accessed, ransomware or RAT gets downloaded which when executed, demands payment from victims. In such cases, it becomes difficult for the victim to get the data back.

What to do if you receive one:

- Keep calm and do not reply to such mails as these are just spams.
- Change your password immediately.
- Do not trust their claims (these are mostly lies!).
- Do not click on any of the provided links in such emails.
- Do not pay the attacker.

5 Insecure Remote Desktop & SMB

Quick Heal Security Lab observed continuous attack using RDP and SMB brute force. Criminals look for unsecured RDP, SMB services to exploit and access enterprise networks. Ransomware like Dharma, CrySis distributed through hacked RDP or SMB share by brute forcing. Remote Desktop Protocol (RDP) is widely used for remotely connecting to Windows systems, whereas, Server Message Block (SMB) Protocol is a client-server communication protocol used for sharing access to files, printers, serial ports and other resources on a network.

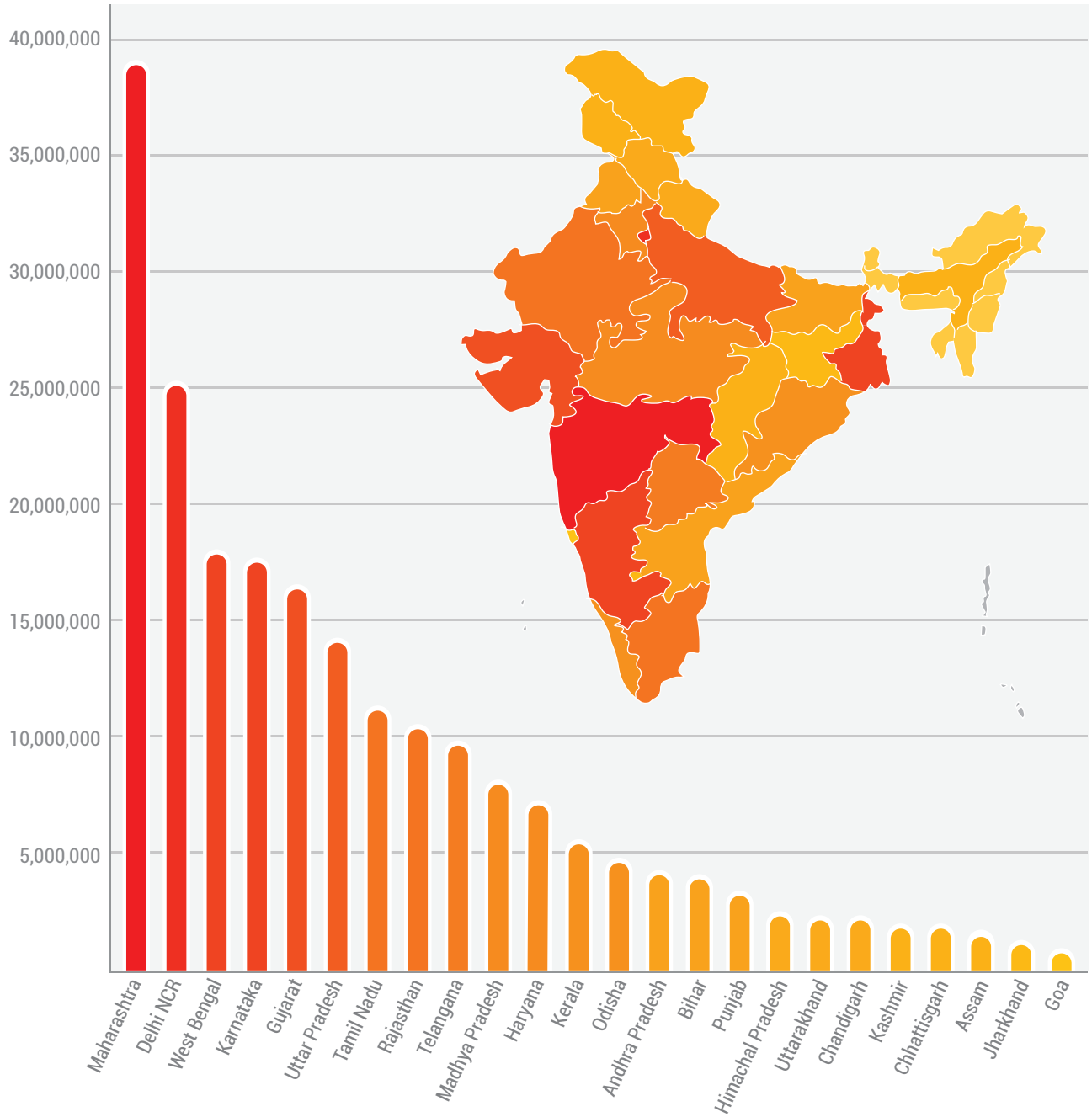
Brute Force Attack: A brute force attack is a trial-and-error method used to retrieve critical information such as usernames and passwords. A brute force attack is generally carried out through automated scripts.

RDP Brute Force Attack: The Remote Desktop Protocol (RDP) running on default port 3389. By brute forcing the user credentials to access the RDP on a victim's machine, attackers can uncover usernames and passwords. Once credentials are obtained, attacker gets the ability to carry out any type of attack.

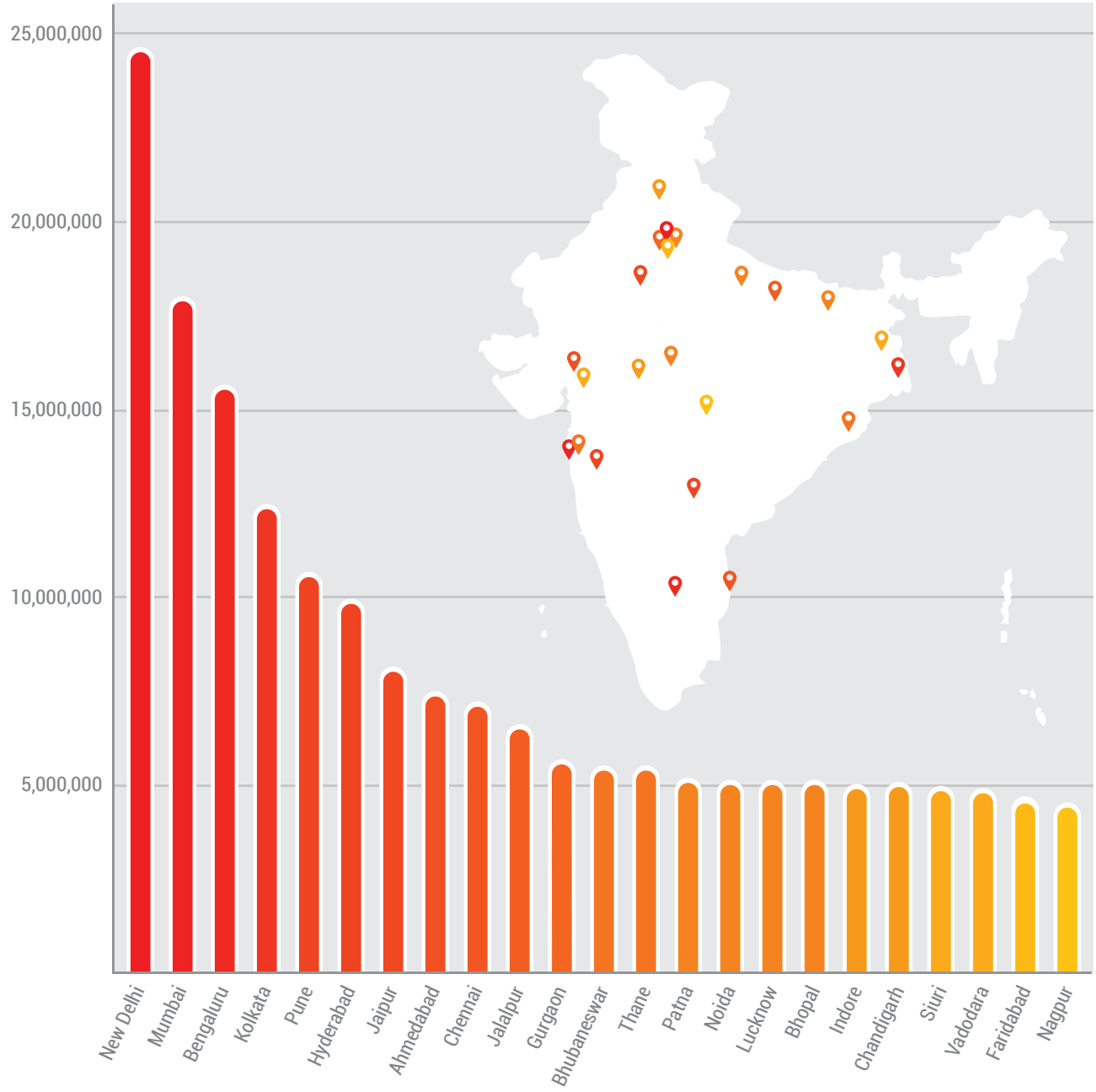
SMB Brute Force Attack: The Server Message Block (SMB) Protocol running on port 445, is targeted with a typical brute force attack using Metasploit. As a result of the brute force, the attacker gets reverse Meterpreter shell. Then attacker can create new user with administrative rights on victim's machine. Once attacker creates user, he gets the ability to carry out any type of attack.

Many organizations fail to secure RDP services against unauthorized access. It is strongly advised to protect it by setting up appropriate configuration (For Eg. Firewall, Do not keep RDP over Public Network). Keep Operating System up to date. Along with setting up complex password; password expiration & account lockout policies should also be implemented. Most important – Keep backup of important data.

INDIAN STATES MOST AT RISK

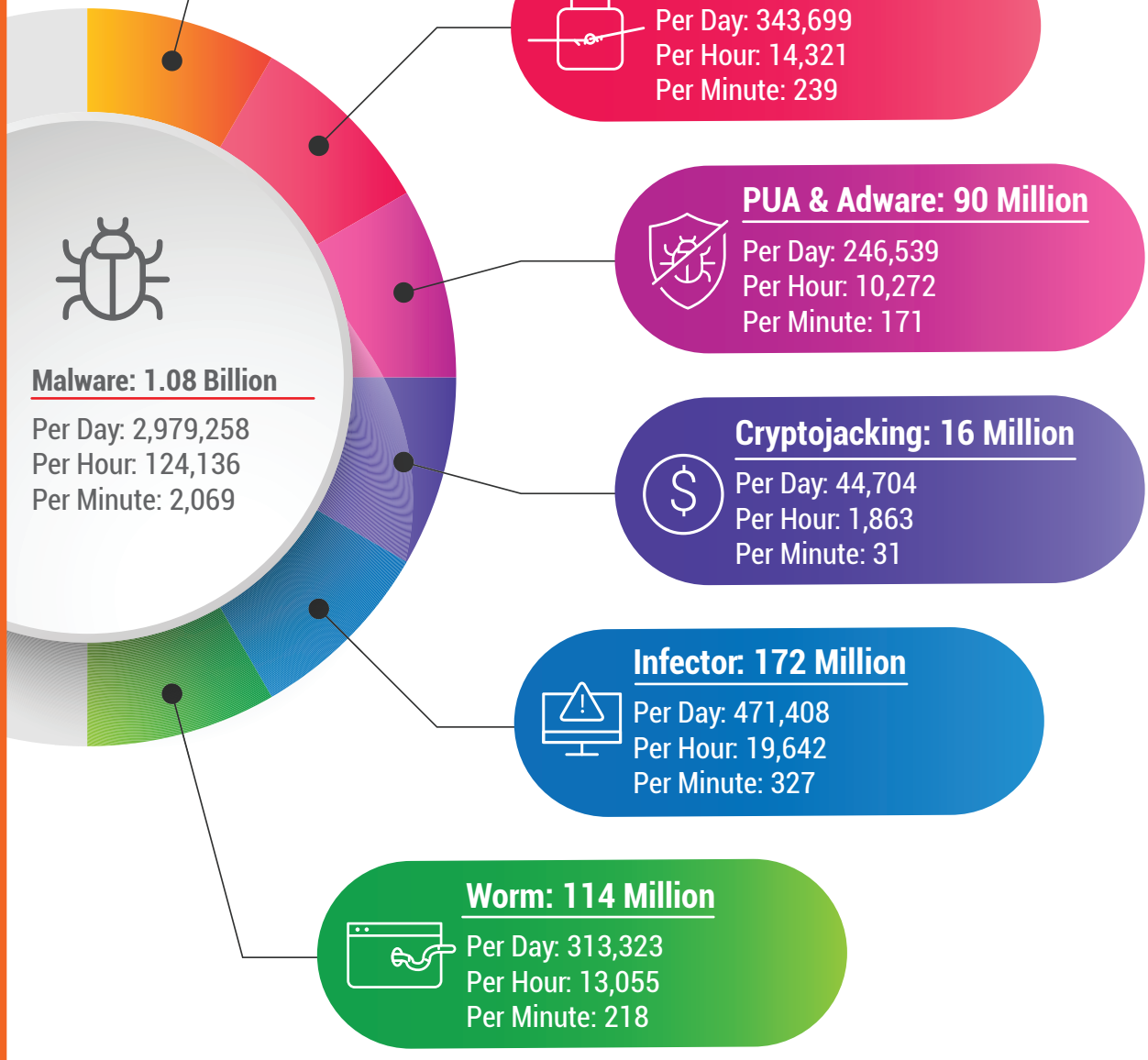


INDIAN CITIES MOST AT RISK

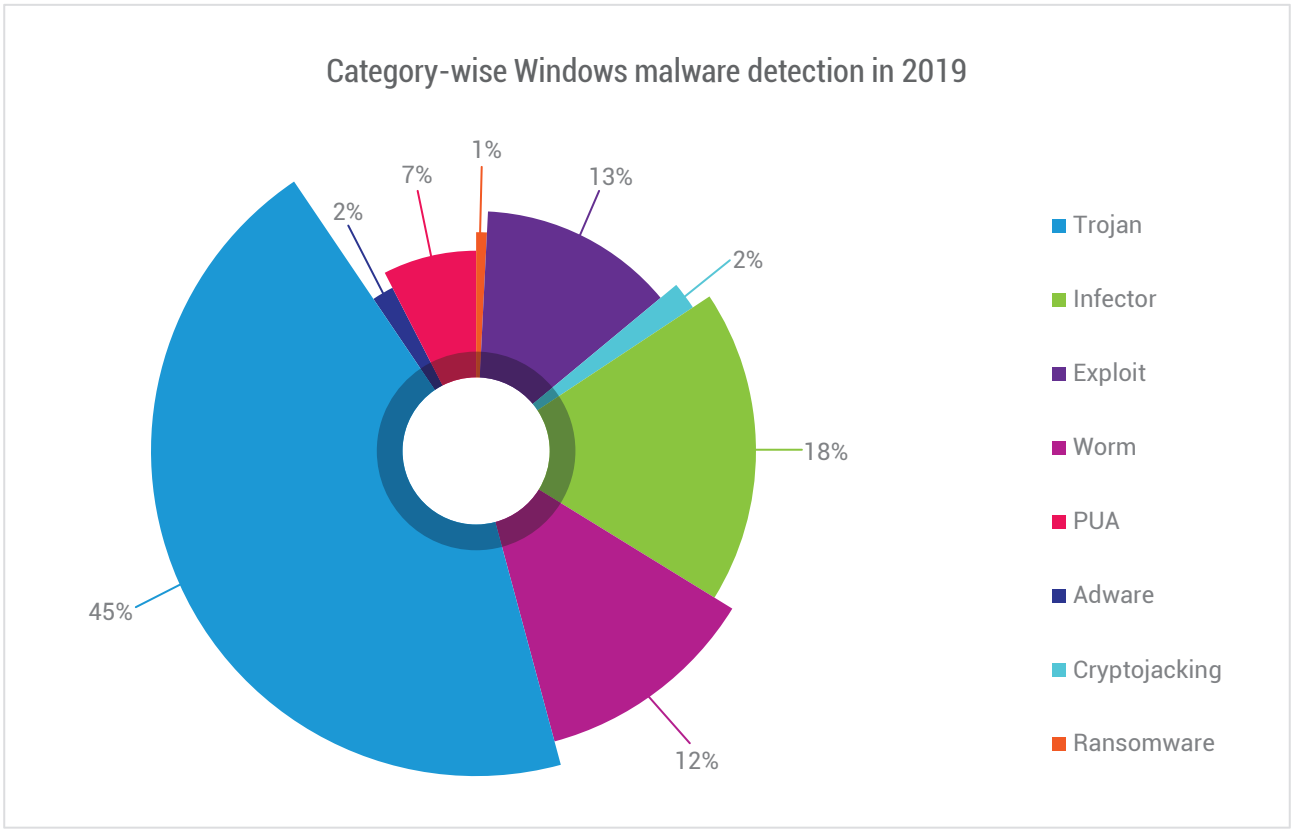


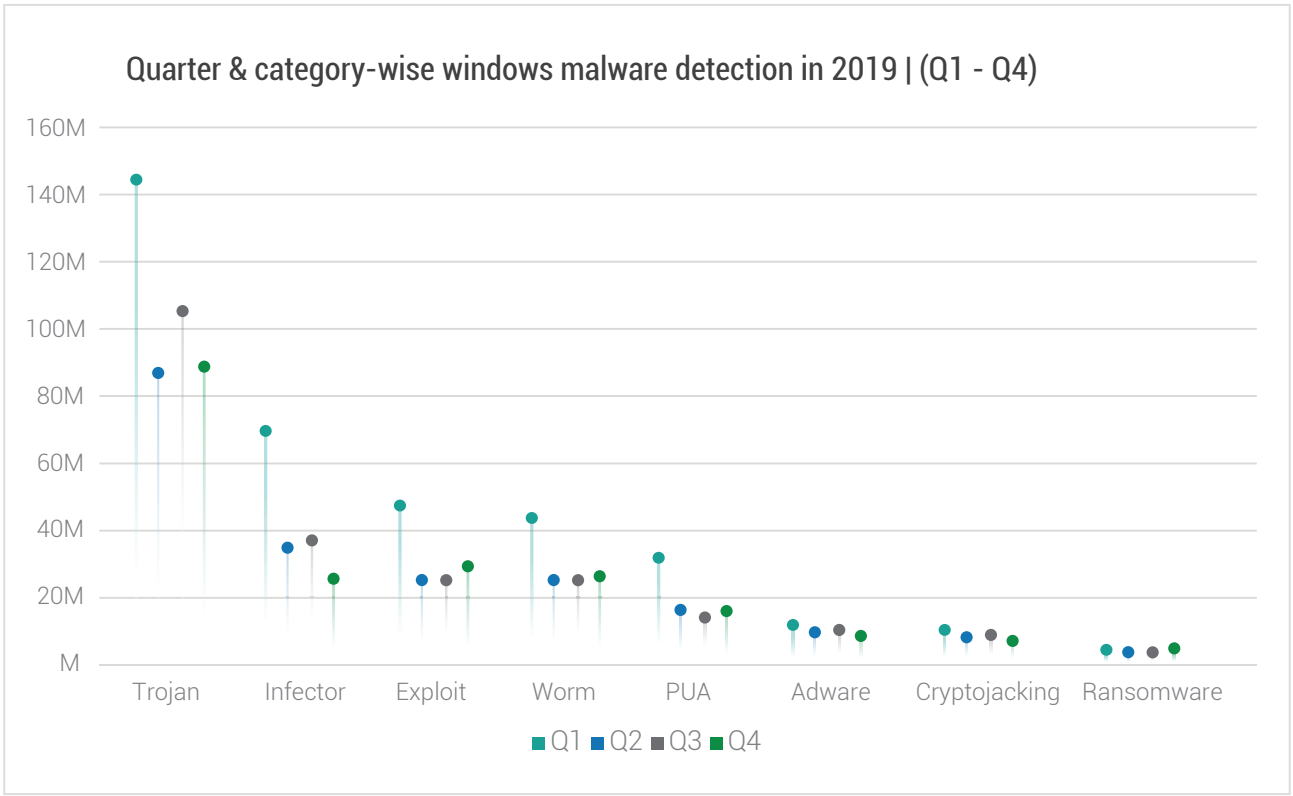
WINDOWS

DETECTION HIGHLIGHTS – 2019

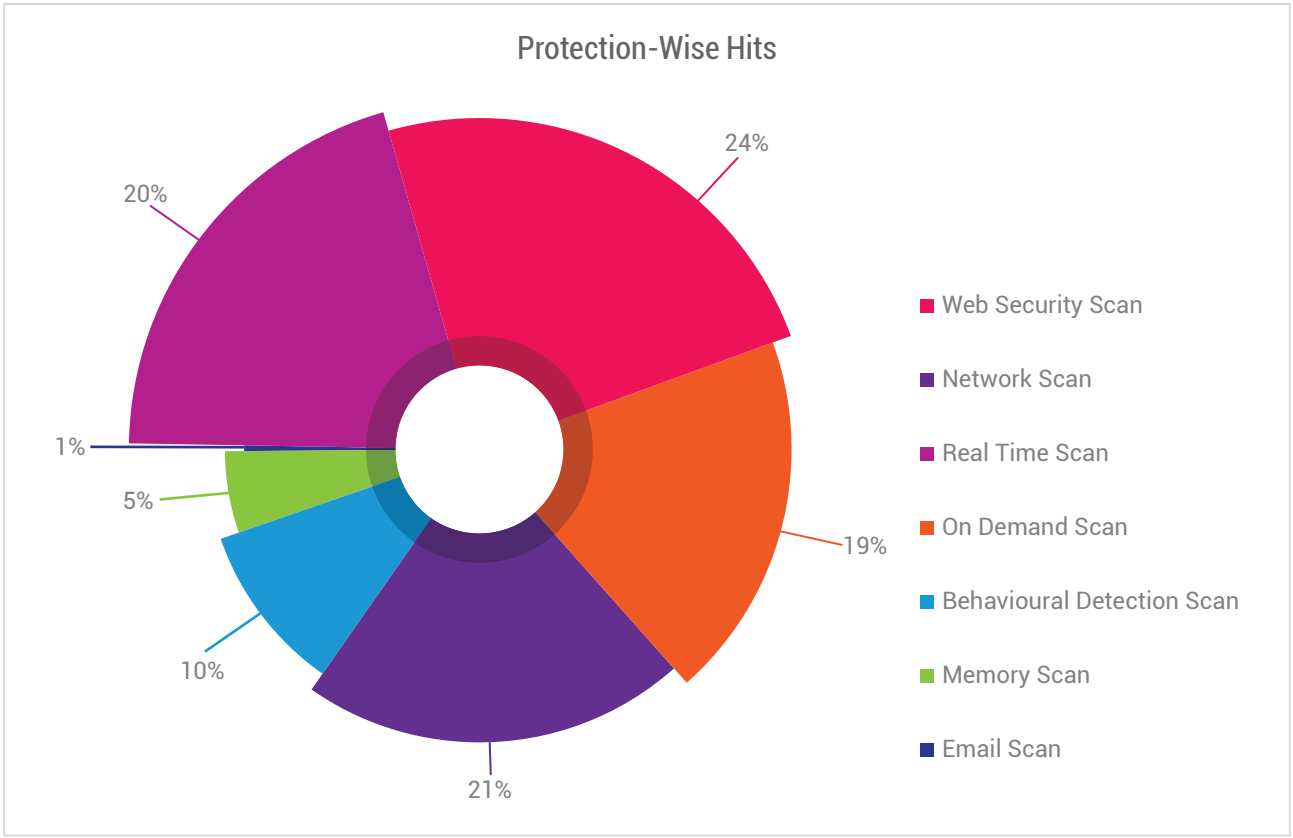


WINDOWS DETECTION STATISTICS 2019





DETECTION STATISTICS – PROTECTION WISE



Observation

- 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.

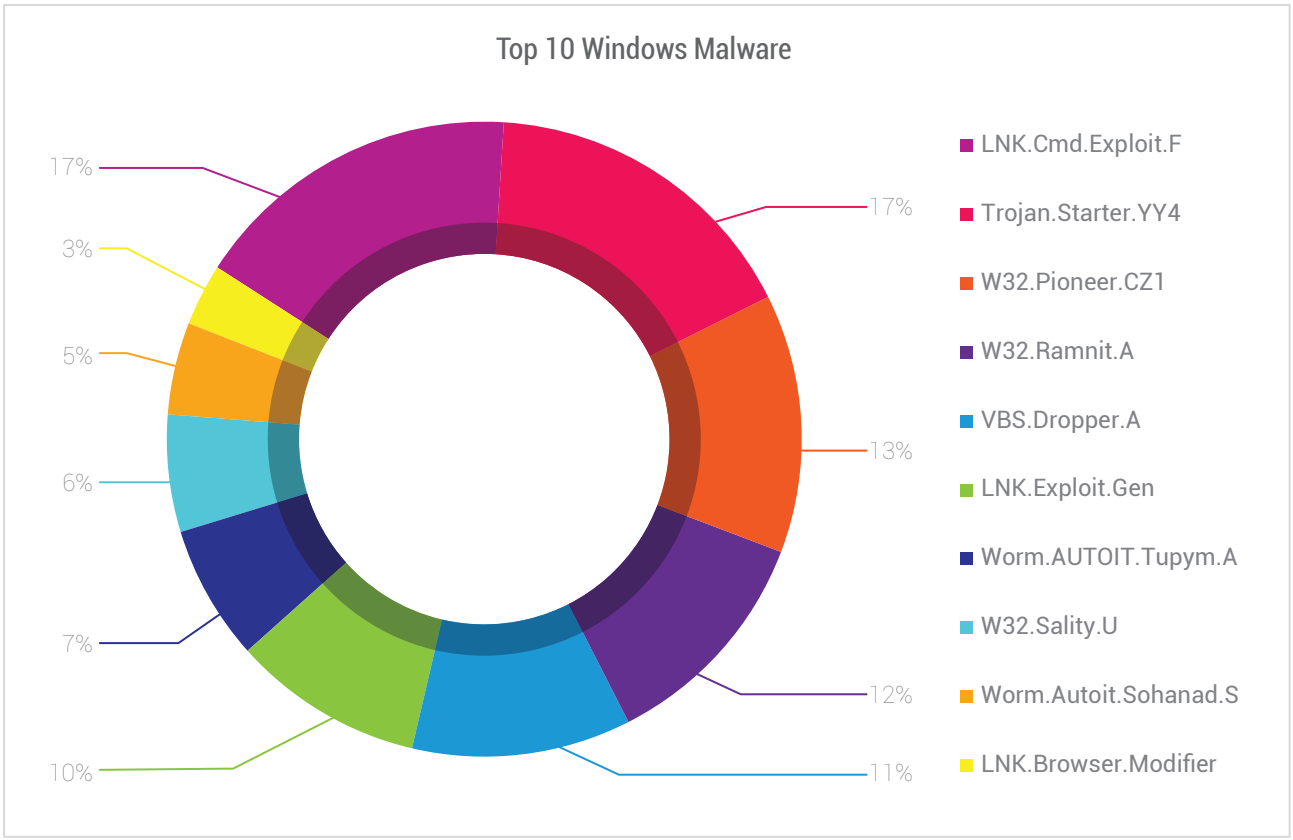
Email Scan
Blocks emails that carry infected attachments or links to compromised or fake and phishing websites.

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.

TOP 10 WINDOWS MALWARE OF 2019

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



Observation

- In 2019, LNK.Cmd.Exploit.F was detected to be the topmost Windows Malware, with around 56 Million detections made.

1. 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.

2. 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.

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. 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.

6. 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.

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. 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.

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. LNK.Browser.Modifier

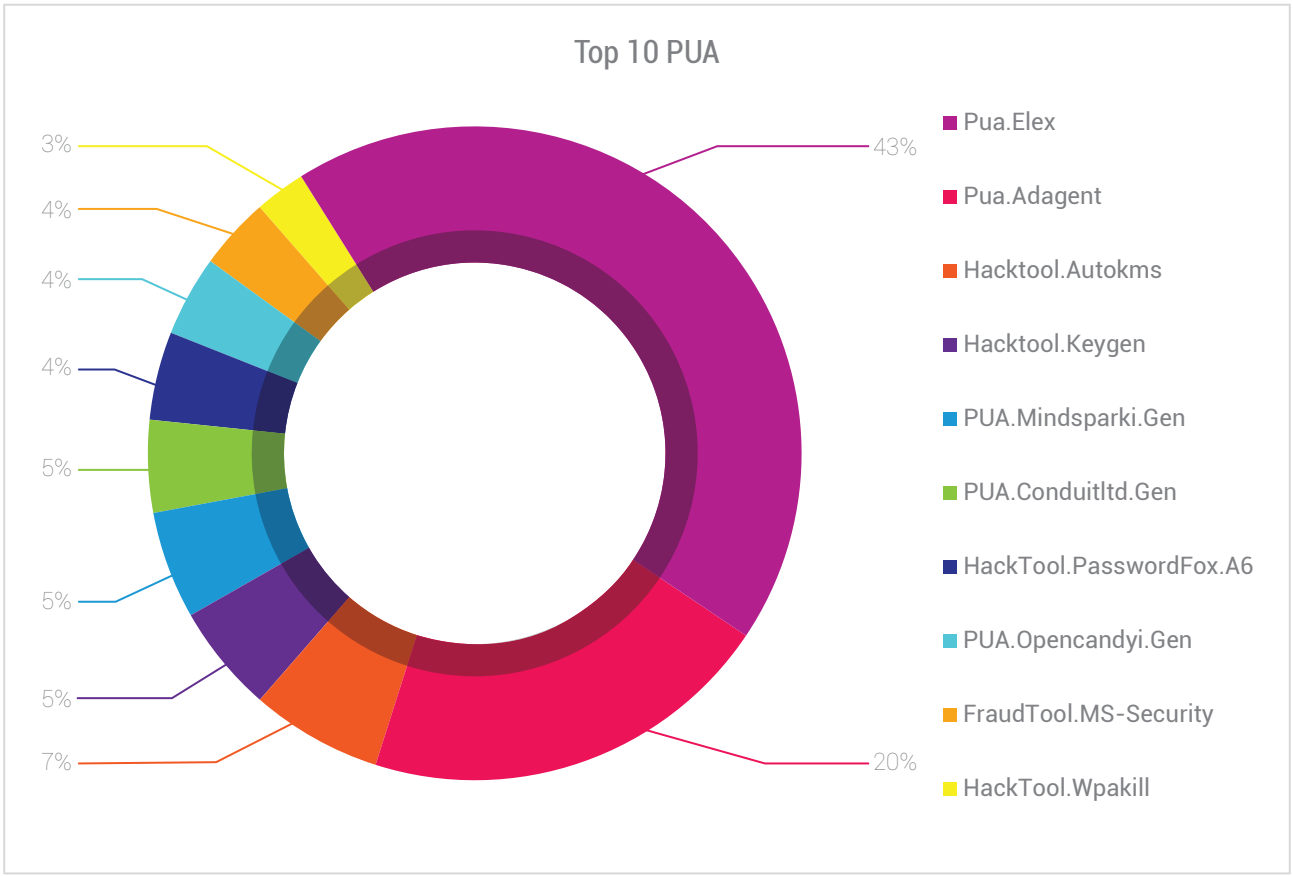
Threat Level: High
Category: Trojan
Method of Propagation: Bundled software and freeware
Behavior:

- 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.

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 Security Labs in 2019.

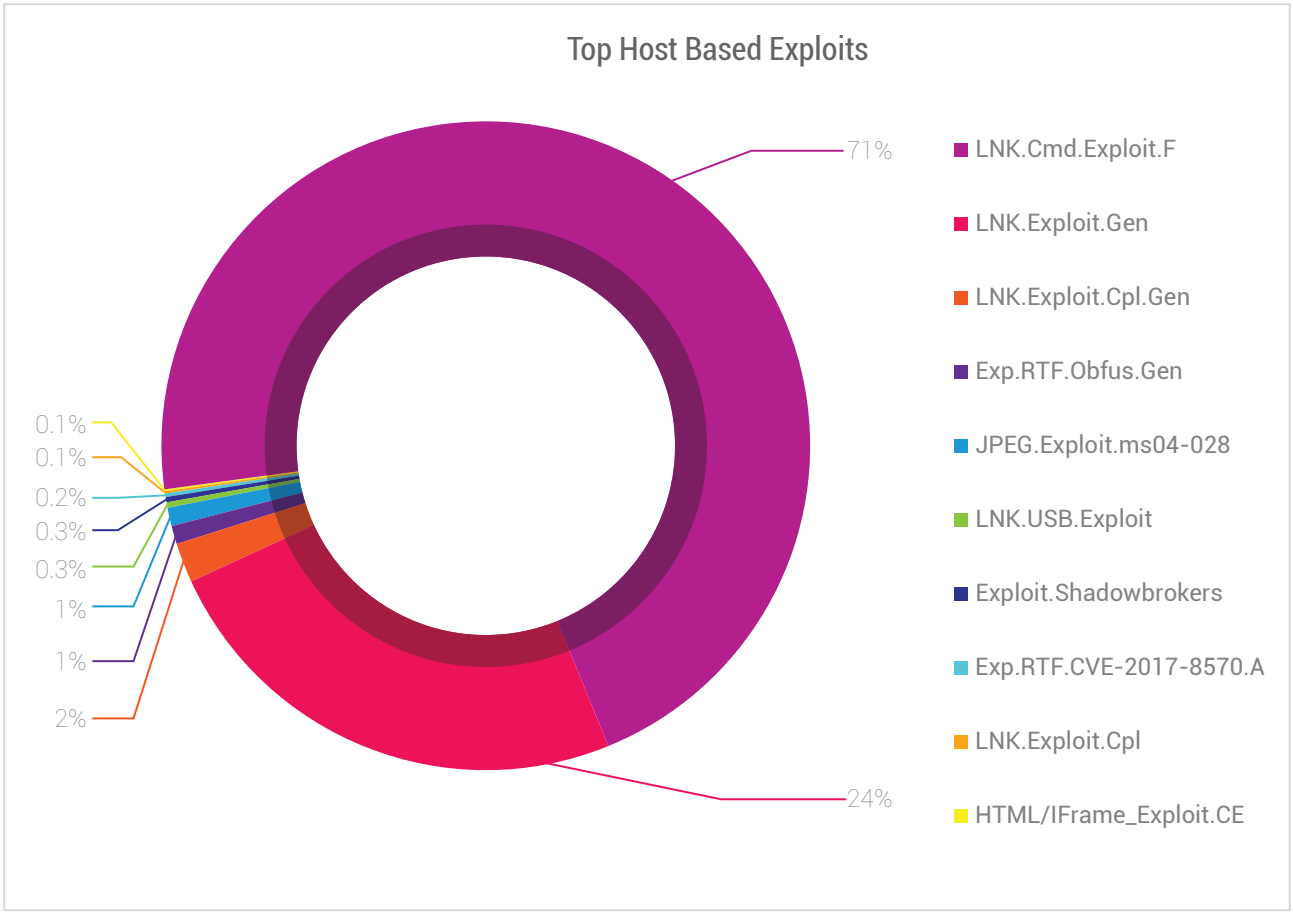


Observation

- Pua.Elex was detected to be the topmost PUA, with around 8 Million detections made in 2019.

TOP 10 HOST-BASED EXPLOITS

A computer exploit is an attack designed by a hacker to take advantage of a particular security vulnerability the targeted system has. Below figure represents the top 10 Host-Based Windows exploits of 2019.

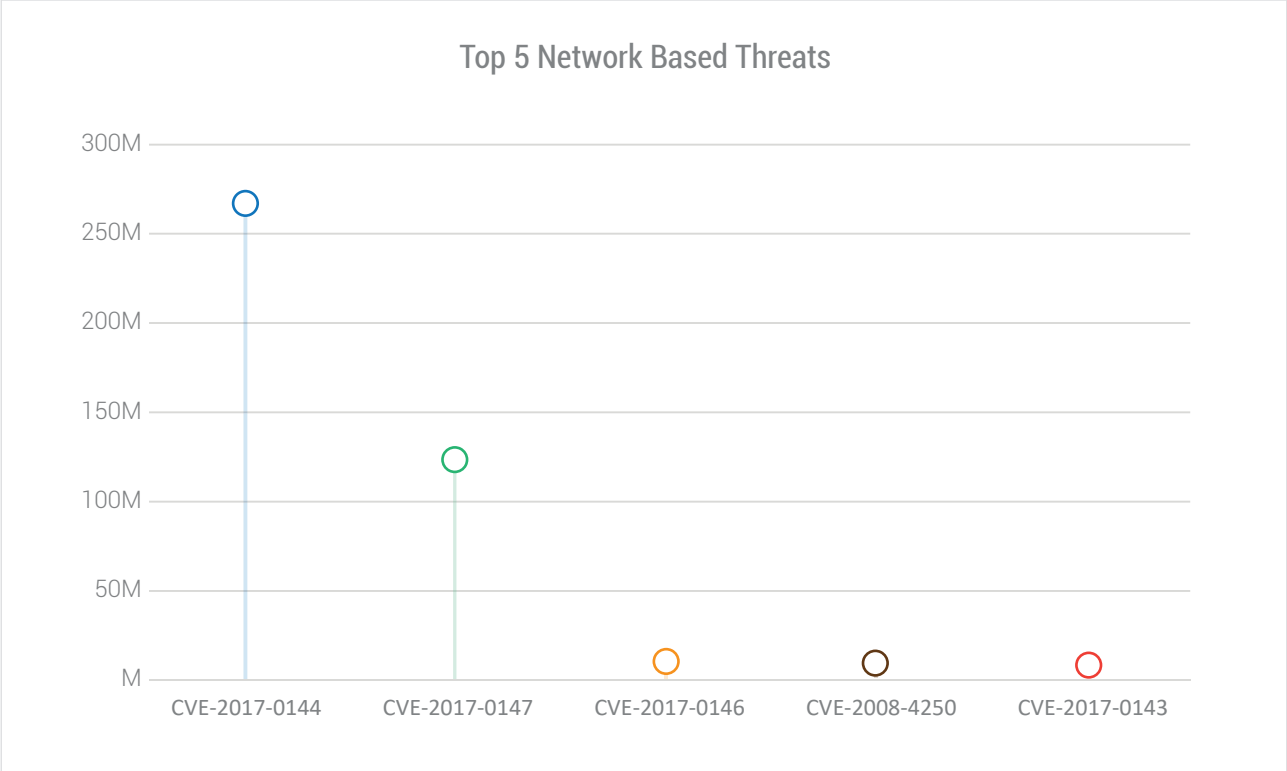


What are host-based exploits?

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 5 NETWORK-BASED EXPLOITS

Below figure represents the top 5 Network-Based Windows exploits of 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. Stop Assaulting Your System with Cracks!

With 180+ extensions in the wild, STOP (.djvu) can be considered as the most widespread ransomware of this year. The infection vector for this ransomware is particularly cracked software downloaded from internet. In cases of cracked software, user tends to ignore the antivirus detection and execute it by taking risk, which is the main reason behind its success. Over the period Stop ransomware has been observed to use a complete framework to mitigate current detection techniques, whether it be a newer extension, newer obfuscation techniques or even anti-emulation techniques. According to our observations, cracked files or activators for different software like Tally, Minecraft, 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. Whereas in the second case, if the system is not connected to the internet, it uses the predefined encryption key. This predefined encryption key varies from sample to sample. Hence, in the second case, decryption is possible where the key is predefined.

With the continuous introduction of newer extensions, STOP author keeps on adding different software cracks to their infection list. For every new extension, their online CnC servers stay active for a certain 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 hours of encryption.

To stay protected we will advise our users:

1. Do not use or download cracked software.
2. Do not install software from untrusted sources.
3. Always keep your Anti-virus definitions up-to-date.
4. Do not allow suspicious or malicious applications to run.
5. Backup your data.

2. Emotet: Continues aggressive spreading over the globe

Emotet is now a familiar name in cybersecurity world. It is the most severe threat since last couple of years. 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 in mid-2019, a new variant of Emotet has been observed with a new wrapper blending and some complex obfuscation techniques. Additionally, interesting thing we noticed is that change in its communication pattern i.e. previously it was sending all data in cookie header of GET requests, now it is sending all data as a part of POST requests. 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 propagation. Interestingly, it uses geographically targeted emails according to local-language lures and brands. Also, it chooses current events for crafting of spams like at the end of 2019, Halloween themed spamming emails were observed. From the start, Emotet has been seen delivering its payloads in America, Europe and South Asia regions. In the late 2019, it was spreading in Australia and Japan as well.

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, it started exploiting MS Office Word documents with a heavily obfuscated macro embedded in 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:

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

3. Use of MySQL for attacks on enterprises

Database servers like MySQL, MongoDB, MSSQL are used for storing this precious data. But unfortunately, not everyone is conscious about its security. In fact, approximately 90% of these applications have credentials like root:root, scott:tiger. In some cases, we observed people even don't use credential for database server's root account. MySQL server is one of the most successful open source products. MySQL has been a regular target for malicious users or hackers wanting to exploit and steal data. This type of exploit can be serious; it can include putting malicious software on your web server and using the website to host malware.

MySQL server runs as a service, so it runs with system privilege. If attacker enters the network using MySQL, it then executes with system privileges, so it can access everything on infected host without any vulnerability. Now once attacker gets access to MySQL database, it can do anything. It can manipulate your data, delete it or steal it. But MySQL doesn't understand windows API function like CreateProcess or UrlToDownloadFile. Attackers can play with the database like they can drop existing table and create new table for malicious purpose or use MySQL as an entry into Linux or Windows system and then drop a backdoor.

In some cases, we observed that attackers insert DLL in hex format in a table with one column of blob type in database named "mysql". This dll contains definition for user-defined functions; now attacker can use their own user-defined functions in MySQL. These functions are used for downloading new malicious files from internet and execute them on the infected server. Any application executed by mysqld.exe will run with system privileges and can be used to launch file-less malware attacks. Till now, we have seen these MySQL attacks being used for dropping ransomware and Virus infector which ultimately drops another backdoor with IoT capabilities.

4. Living-Off-the-Land tactics used by Attackers

In the recent years, there has been an increase in use of Living-off-the-Land (LoLBins) tactics. Attackers are actively using windows native/system tools to carry out their attacks. Using LoLBins, attackers can easily bypass traditional security solutions, bypass application whitelisting, execute files-less attacks and download another payload. Below are widely used LoLBins attacks observed by our lab:

A) Powershell.exe

PowerShell is a command-line interface utility which can be used by an attacker to perform several actions such as code execution, discovery of network, information, etc. PowerShell can also be used to download and execute a file from the internet. It also has the capability to load an executable in system's memory. Using PowerShell, it is possible to connect with remote systems and execute a command on these systems.

B) Certutil.exe

Certutil is a command-line utility in windows that is used to obtain certificate information and configure Certificate Services. Actors used this tool to download encoded payload. Certutil can be used to decode malware payload hidden inside certificate files as Base64 information. Generally, it is whitelisted by admins and security solutions and thus allows bad guys to download payload.

C) Mshta.exe

Mshta.exe is a utility responsible for executing .HTA (Microsoft HTML Application) files. Attackers execute malicious HTA files like JavaScript or VBScipt files through legitimate applications. Mshta.exe can be used to bypass application whitelisting solutions. For e.g., by exploiting Office application, mshta.exe gets executed which further downloads and executes next stage malware.

D) Regsvr32.exe

Regsvr32.exe is a Windows command-line utility used to register and unregister object linking and embedding of controls including dynamic link libraries (DLLs). Attackers use this utility to bypass process whitelisting functionality to load COM scriptlets for executing malicious DLLs. This utility is also responsible to download external components from the internet.

E) Bitsadmin.exe

Bitsadmin.exe is component for Windows Background Intelligent Transfer Service. Attackers use this tool to download, upload and execute payload.

ANDROID

QUICK HEAL DETECTION ON ANDROID

Adware: 125K

Per Day: 344
Per Hour: 14
Per Minute: 0.24

Malware: 639K

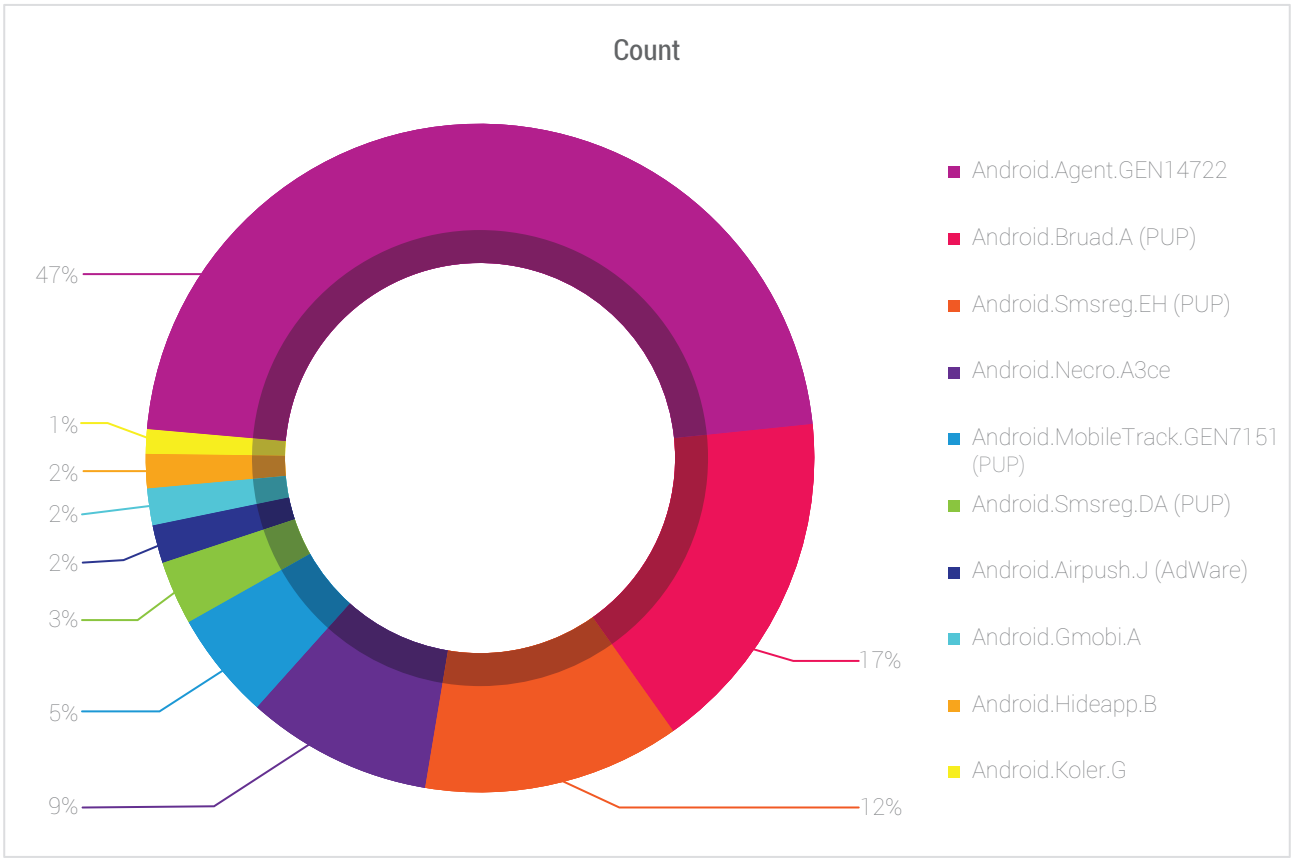
Per Day: 1752
Per Hour: 73
Per Minute: 1.22

Potentially Unwanted Application (PUA): 360K

Per Day: 987
Per Hour: 41
Per Minute: 0.69

TOP 10 ANDROID MALWARE OF 2019

Below figure represents the top 10 Android malware of 2019. These malware have made it to this list based upon their rate of detection across the year.



1. 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.

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

3. 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 data like SDK type, SDK version, phone company, phone number, etc.
- It sends the collected data to a remote server.

4. Android.Necro.A3ce

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.

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 the body.
- Collects device information such as IMEI and IMSI numbers

6. Android.Smsreg.DA

Threat Level: Medium
Category: Potentially Unwanted Application (PUA)
Method of Propagation: Third-party app stores
Behavior:

- Asks targeted Android users to make payments through premium rate SMSs in order to complete their registration.
- Collects personal information such as phone numbers, incoming SMS details, device ID, contacts list, etc., and sends it to a remote server.

7. Android.Airpush.J (AdWare)

Threat Level: Low
Category: Adware
Method of Propagation: Third-party app stores
Behavior:

- 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.

8. Android.Gmobi.A

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

- 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.Hideapp.B

Threat Level: High
Category: Malware
Method of Propagation: Third-party app stores
Behavior:

- It hides its ICON on first launch.
- Shows message like "Application is unavailable in your country".
- Run services in background and shows Full screen advertisements.
- It collects device information like Country code, IMEI, phone number etc.
- It then send collected information in encrypted form to remote server.

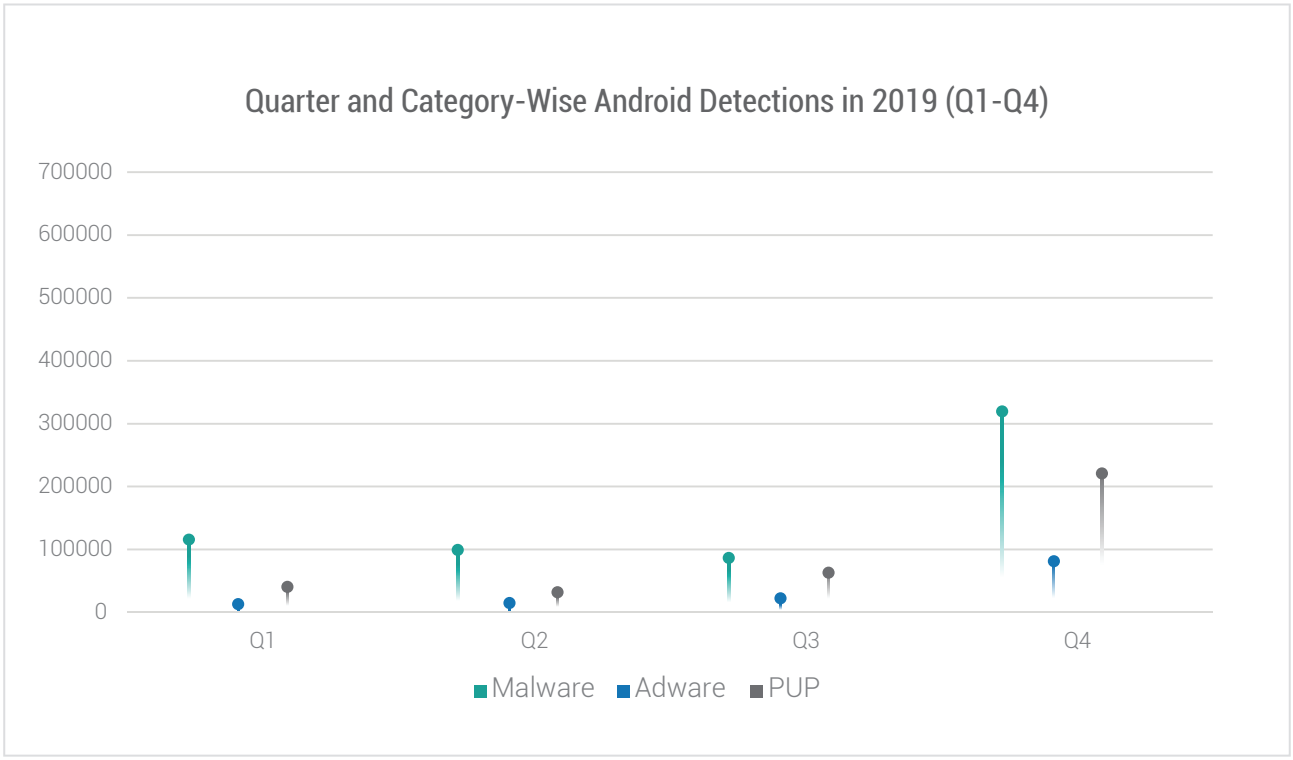
10. Android.Koler.G

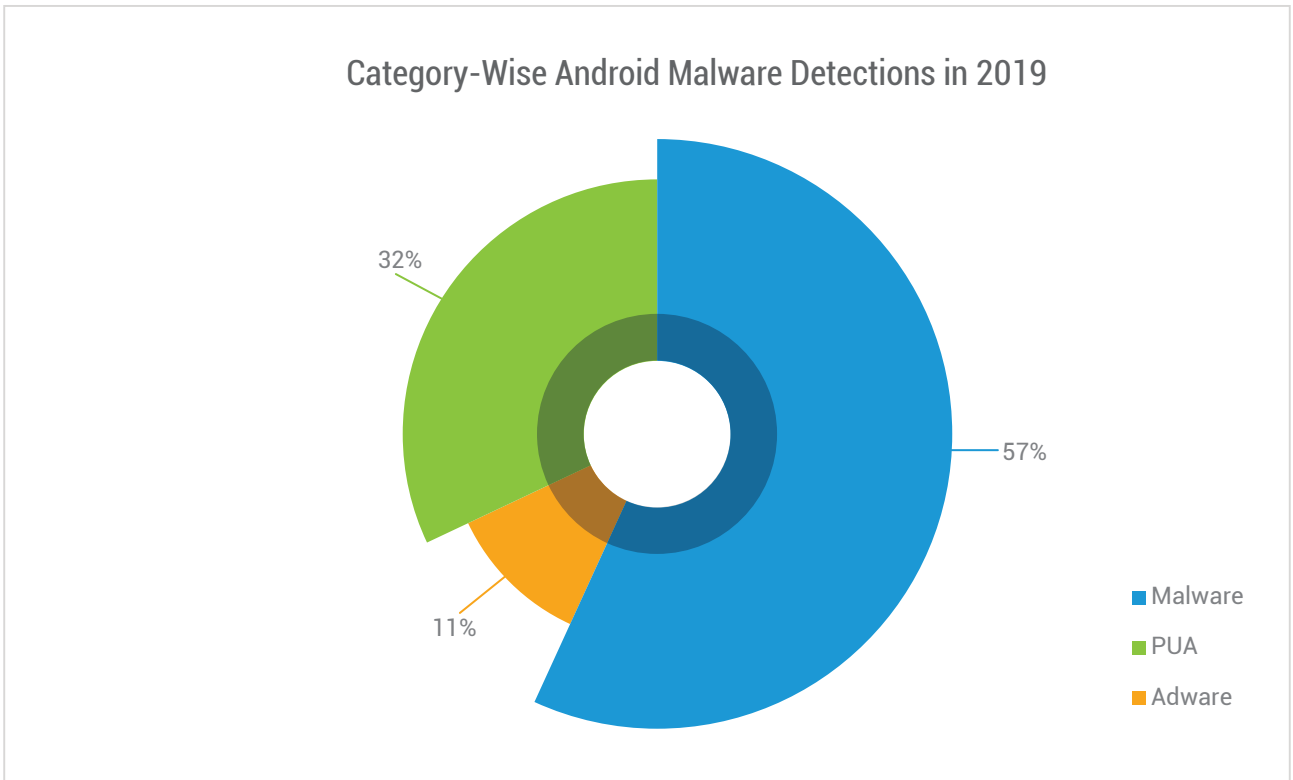
Threat Level: High
Category: Malware
Method of Propagation: Third-party app stores and repacked apps
Behavior:

- This malware sends IMEI and device country to remote server.
- It then block access to the device and shows ransom message in specific language according to country.
- It receives commands from C&C server and disable the back button.
- The APK code is obfuscated to make analysis difficult.

ANDROID DETECTION STATISTICS: CATEGORY WISE

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





TRENDS IN ANDROID SECURITY THREATS

- **GINP**

  The code snippets used by this Banking Trojan is very similar to the Anubis trojan. It performs overlay attack, which makes it different from other malware, because overlay screens are almost identical to the legitimate banking apps. It asks for accessibility permission and checks which services are running in foreground. If name of any service matches one from the target list, then it displays its overlay. This screen helps to steal critical banking data like user's login credentials and credit card details. The accessibility permission allows attacker to gain full control of user's device and perform malicious activities like SMS reading, contacts collection, SMS and call forwarding, installed application listing etc. It hides the icon from user, preventing it from getting un-installed.

- **VULNERABILITIES IN WHATSAPP: Allows to trigger RCE and DoS**

  Recently, a stack-based buffer overflow vulnerability CVE-2019-11931, was found in WhatsApp. By exploiting this vulnerability, the attacker can achieve arbitrary code execution by just sending a specially crafted MP4 file to targeted WhatsApp user. The root cause of this vulnerability was the component of the MP4 file handler. Parsing of the specially crafted MP4 file leads to memory corruption, which allowed the attacker to place an arbitrary code in a memory address which can run with high privileges.

  Another WhatsApp vulnerability, CVE-2019-11932, which was a double-free vulnerability allowed the attacker to take RCE and DOS. The bug was present in a library called libpl_droidsonroids_gif.so, which is part of the android-gif-drawable package. Even though this flaw has been patched, still there are lots of apps which are still using the older version of the android-gif-drawable package that remains at risk.

- **Android flaw: With NFC beaming hackers can infect your device**

  Hackers could plant malware with the help of NFC (Near Field Communication) beaming vulnerability CVE-2019-2114. NFC Beaming is mainly used for sharing data between two paired devices and for doing contact-less payments. If any malicious app is sent via NFC beaming it will be stored on the disk and a prompt "Install Apps from Unknown Sources" is displayed, if the system wide setting is set so. Versions prior to Android 8 allowed to install apps from any sources. From Android 8 onwards, Google redesigned the System-wide setting mechanism into an app-based setting, which allows the device owners to enable or disable the permission for each app separately. The bug was that Android Beam was by default whitelisted for allowing app installation from unknown source. These privileges to System Apps allow attacker to bypass the check of “Install unknown app" and go directly to the install prompt.

  To avoid these scenarios, remove the permission "Install unknown apps" for NFC service. This October, Android released patches and removed the Android Beam service from the OS whitelist of trusted sources.

- **Bad Binder vulnerability**

  Bad Binder (CVE-2019-2215) is a use-after-free vulnerability in binder driver of the Android kernel, which can be used to allow local privilege escalation. If chained with a browser renderer exploit, this bug could fully compromise a device through a malicious website. Binder is Android-specific inter-process communication mechanism. One Android process can call a routine in another Android process, by using binder to identify the target method to invoke.

  Exploitation of this vulnerability would require either the installation of a malicious local application or a separate vulnerability in a network facing application. This android kernal vulnerability was used by NSO group to install malicious Pegasus spyware on target devices.

  According to Android October Security Bulletin, security patch level 10/6/2019 addresses this issue and it got fixed.

- **JOKER - Android Malware name influenced by DC character?**

  Joker which is a popular DC comics character, is also the name of an Android spyware. Joker only infects users of a specific country, which it finds by checking the country code. If the user's country code doesn't match in the list it maintains, then it won't download the next payload. As spyware, it can steal all victim's data and device info as well. It communicates with its C&C server from time to time, to take and execute the commands. It does the spying activities like reading the notifications, interacting with advertisement sites and can also sign premium subscriptions without any user interaction. It takes all SMS messages, contact list and stores it into a JSON format. Further, it encrypts and sends it over to the C&C server.

  There are multiple variants of Joker available. One of the variants use encrypted sites from which it downloads the payload, while another version has encrypted package which is present in its resources.

- **Dropper apps found on Google Play**

  Trojan Droppers are usually implemented as scripts or small applications. They don't carry any malicious activities by themselves, but instead open a way for attack by downloading/decompressing and installing the core malicious modules. To avoid detection, a dropper may also create noise around the malicious module by downloading/decompressing some harmless files. They copy themselves to some random, hidden file and run after the system is restarted, attempting to download the malicious modules again. In such cases, to get rid of the downloader, it is necessary to find and remove the created keys and the hidden file.

  Malicious URL is embedded in the code of the dropper app, but it's obfuscated to prevent the URL string from being flagged by any human analysis or app store security checks. The server responds with an obfuscated JSON message that contains configuration data for the dropper app and additional URLs, which point to the location of the adware APK. Once the malicious payload is downloaded from the hosting service, the dropper apps initiate an install process. Once installed by the dropper, the adware APKs wait approximately 10 minutes before initiating malicious functionality. Then they display fullscreen video ads, outside of the app, without any user interaction. In previous quarters also we observed similar behavior adware on Google play. https://blogs.quickheal.com/quick-heal-reports-29-malicious-apps-10-million-downloads-google-play-store/

- **FunkyBot**

  This malware uses social media to obtain its C&C server. For this, it downloads the webpage of a photo-less Instagram account. It then extracts the biography field of this account and decodes it using base64. After having sent all of the device's contacts to C&C server, it waits for a response which contains a telephone number and a message body. It constructs an SMS using the received data and sends it to all the numbers from contact list. It is interesting to note that the malware identifies the SIM card provider and checks if it is a specific Japanese telecommunication provider. FunkyBot alters the device settings to make itself the default SMS handler application. This functionality can be very dangerous, considering that most banks currently use two-factor authentication through SMS.

- **Pegasus**

  WhatsApp recently confirmed that it had informed several Indian users that their android phones had been targeted by a spyware named Pegasus. The victims mainly include several journalists, activists, lawyers and senior government officials and are believed to have been put on surveillance for couple of weeks in April/May, 2019. Pegasus is a spyware for mobile operating systems like Android, iOS and others. Pegasus is developed by the Israeli firm, NSO Group. Pegasus infected the phones of some users after it was delivered through the WhatsApp messaging platform.

  It used to enter Mobile phones through a malicious link and had capabilities to read text messages, track calls, collect passwords, gather data from other apps and collect geo-location of the phone. Pegasus came in news several times after that, with new functionalities and abilities to infect Android as well as other Mobile Operating Systems. In May 2019, Facebook patched CVE-2019-3568, a critical remote buffer overflow vulnerability in WhatsApp. It's a vulnerability in WhatsApp's VOIP stack that could allow remote code execution via specially crafted series of RTCP packets sent to a target phone number. It has been reported that, attackers exploited this vulnerability in WhatsApp to infect victim's Mobile Phones with the infamous spyware Pegasus. This bug in the Audio/Video call feature of vulnerable WhatsApp versions allowed the attacker to install Pegasus spyware on the victim's device, irrespective of whether the call was answered or not. Facebook was quick enough to patch this vulnerability and alert users to update their apps to latest version.

  Possibly, there can be different ways through which Pegasus can infect your mobile phones and it's not just limited to a malicious link or a malicious call to the users running vulnerable versions of WhatsApp app. User's should be always alert while clicking on links received through messages, emails or any Social Media platforms and should refrain from installing apps from Third-party App Stores.

- **Xhelper**

  This malware having ability to a self-reinstall mechanism that it made difficult to remove. It can hide itself from users, download additional malicious apps, display advertisements and it can also remain hidden from the system's launcher as well. Xhelper can't be launched manually since there is no app icon visible on the launcher. Instead, the malicious app is launched by external events, such as when the compromised device is connected to or disconnected from a power supply, the device is rebooted, or an app is installed or uninstalled. 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.

PREDICTIONS FOR 2020

Increase in Web Skimming attack

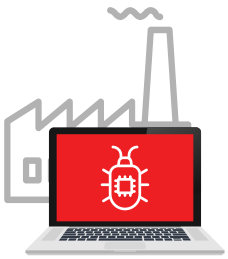
Magecart proved to be a prominent web skimming attack in 2019 as well, with thousands of websites compromised to deliver skimming code. Similar to Magecart, Pipka is another web skimmer which has recently emerged and it comes with self-deleting code. We suspect that skimming attacks are set to increase in 2020, as we see huge number of hits for these attacks at this point of time.

Lookout for more Bluekeep-like wormable exploits

Until now, publicly available exploit codes for Bluekeep can only achieve DoS on the victim machine, but it's only a matter of time before attackers will figure out ways to exploit the vulnerability to its full potential and perform more severe attacks like delivering Trojans and Ransomware. Ransomware authors are constantly in lookout for such wormable exploits, as it makes it makes lateral movement easier.

Deepfakes to cyber-frauds

Deepfakes are fake/manipulated video or audio clips of a person, created using deep learning technology. This can be used to create fake news and even carry out cyber frauds in cases like a deepfake video of boss asking his colleagues or employees to transfer funds to an unknown bank account.



APT attacks on critical infrastructures

The recent APT attack on Kudankulam Nuclear Power Plant has emphasized on the significance of security of the critical infrastructures. We may witness rise in such APT attacks on the critical public infrastructures like transportation networks, power plants, telecommunication systems, etc. Such attacks can cease the major functionalities of a nation and may take several days to bring back to life.

Increase in threat landscape because of 5G

With 5G network, everything from your car to refrigerator will now have access to high-speed connectivity. This will in turn create more exposure to attacks and more potential entry points for attackers. Threat actors, organizations & institutions will have larger landscape to monitor and the growth of the confidentiality and privacy threats will be unprecedented. Also, main functions of 5G depend on software rather than hardware which leaves it vulnerable to malicious attacks.

Attacks against Windows 7 to increase

Since Microsoft is ending its support for Widows 7 from January 14, 2020, technical support and software updates from Windows Update will no longer be available to users. In last quarter we saw 67% of attacks on Windows 7 itself, which will increase even more in 2020 because security updates will not be available for Windows 7.

Increased use of LOLBins

Cyber criminals will increase the use of "Living Off the Land" techniques to bypass traditional security tools and application whitelisting. They may adopt new "Living Off the Land" techniques to bypass behavioral based detections.

Increase in Office macro-based attacks over office exploits

As Microsoft has taken many steps to block MS Office exploits in newer version of Windows, so it is hard to execute exploit code on Windows. Moreover, exploits are specific to application versions, but macros will execute in all versions of MS Office. There are many open source obfuscator and macro generation tools freely available to create a macro-based payload. Many security vendors are also blocking a macro execution but Excel macro 4.0 is also available to bypass these techniques.

CONCLUSION

In wake of the significant rise in cyber-attacks observed in the year 2019 as compared to 2018 as rightly cited in our annual threat report, it comes as no surprise that the threat landscape is only expected to become more complex and challenging hereon.

The threats are expected to rise not just in terms of new entry points and types of variants but also on the geographic front. With cyber criminals increasingly targeting smaller cities where people have come to depend on smart devices & smartphones without much regards to their security factor, it has become indispensable for individuals to become aware of best security practices to avoid becoming a victim.

The predictions made by Quick Heal Security Labs for the year 2020, provide a kick-off for areas that are in serious need of robust security, to prevent critical attacks on infrastructure, business data and privacy. These predictions also provide important leads for best security practices to follow, while browsing through the internet, storing & sharing important data, accessing free network, making digital transactions and so on.

The most important step however for ensuring a safe and carefree 2020, would be to make sure that all your software are up-to-date at all times and the protection levels on your security software are always ON, so that you don't leave any vulnerabilities that can be easily exploited.

Few other essential precautionary measures that can save you from devastating cyber-attacks include:

- Keep backup of all important data.
- Keep strong and separate passwords for all your accounts.
- Install a robust antivirus as the first strong level of protection.
- Enable Two-Factor Authentication
- Regularly patch your systems with latest software & security updates.
- Be careful while clicking or responding to emails received from unknown senders, to stay safe from phishing emails.
- Be cautious while clicking/downloading anything over internet.
- Try not to access confidential accounts on public devices or networks.
- Respond to Antivirus notification sensibly.