Quick Heal
*Security Simplified*

# QUICK HEAL

## ANNUAL THREAT REPORT

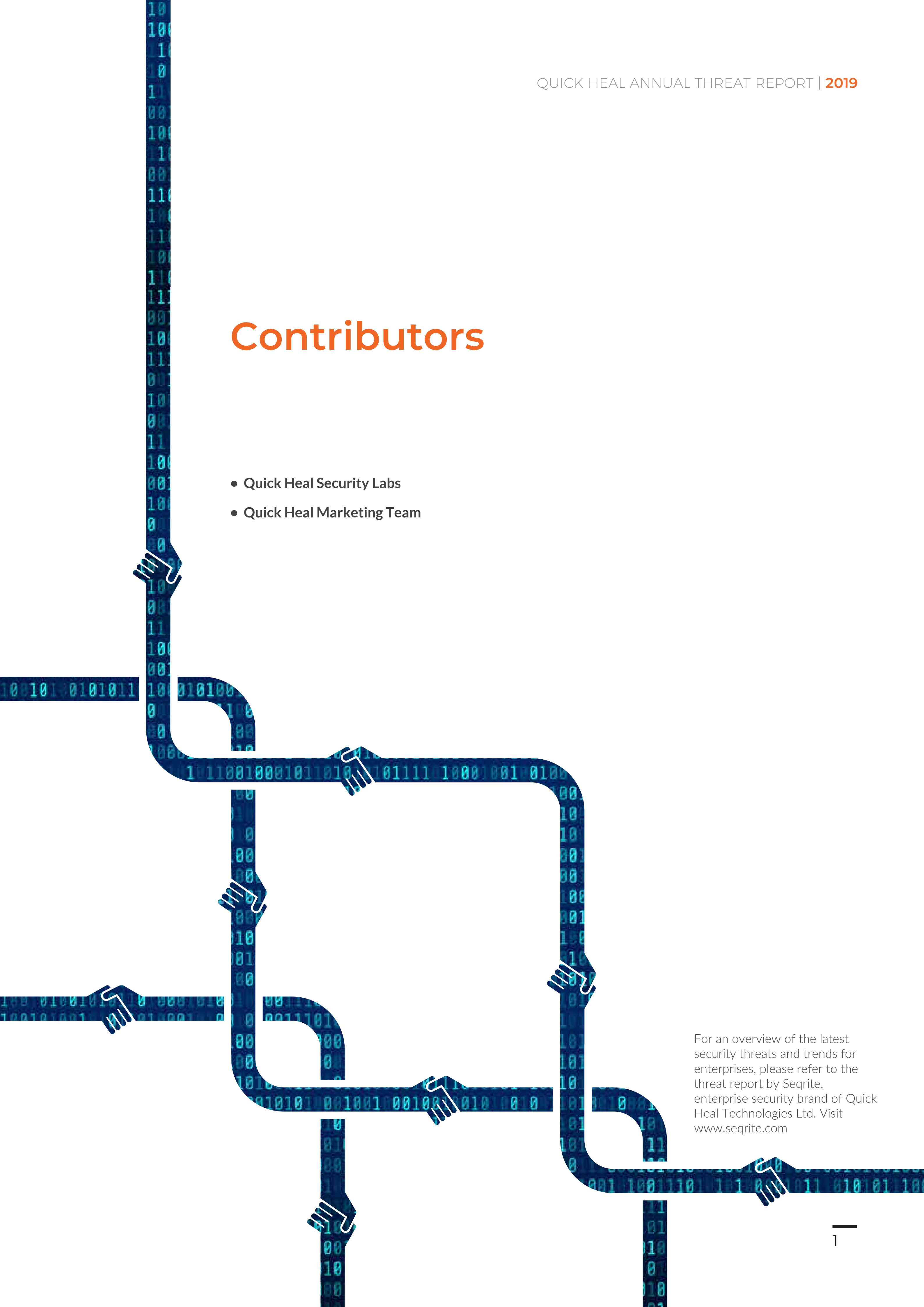
**2019**

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

# Executive Summary

2018 witnessed some devastating cyber-attacks, data breaches and IT outages that made cyber risk a core concern for customers and businesses across the world and pushed cyber security to the very forefront. As cybercriminals started adapting to advanced cyber-attack techniques for targeting various geographical locations, business sectors and end users, it became essential for people to understand the gravity and benefits associated with installing robust anti-virus software in their laptops, PCs and smartphones, to fight against the ever evolving threat landscape.

Quick Heal Annual Threat Report 2019 brings forth insights and intelligence gathered by Quick Heal Security Labs about all that unfolded in the realm of cybersecurity in 2018 – divided into two sections viz. Windows and Android.

The threat report begins with significant cyber-attack predictions made by Quick Heal Security Labs in 2018 that proved to be true, flagging off the possibility for future cyber-attacks. The report also sheds light on detection highlights of 2018 for both Windows and Android, with a breakup of detections made per day, per hour, per minute, and the entire year, along with a list of top 10 Windows and Android malware.

Also included in the report are interesting graphical representation of Indian states and cities to have clocked the highest detections in 2018 that automatically puts them under the radar of high risk zones for cyber-attacks in 2019.

The report also cites stories around some notable cybersecurity incidents that occurred in 2018 and potential sources of cyber-attacks like IoT in the near future, which indicate that its high time we brace up our security measures, to be cyber-attack ready.

This also sends out a trigger for millions of end users, to adapt to robust security measures and install reliable anti-virus software like Quick Heal to prevent their laptops, PCs and mobiles from getting hacked!

This annual report concludes with an outlook on how 2019 will play out for cybersecurity with significant predictions made for the year 2019 along with essential precautionary steps people should follow to keep cyber-attacks at bay.

## WORD OF CAUTION FROM OUR CTO

**User's sensitive information will always be the target, no matter from which device the user is connected to the internet.**

Disclaimer: We have made some improvements in the way we calculate our telemetry data. Hence, an increment in detection counts may be observed in Q3 and Q4, as compared to the previous quarters.

# 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.

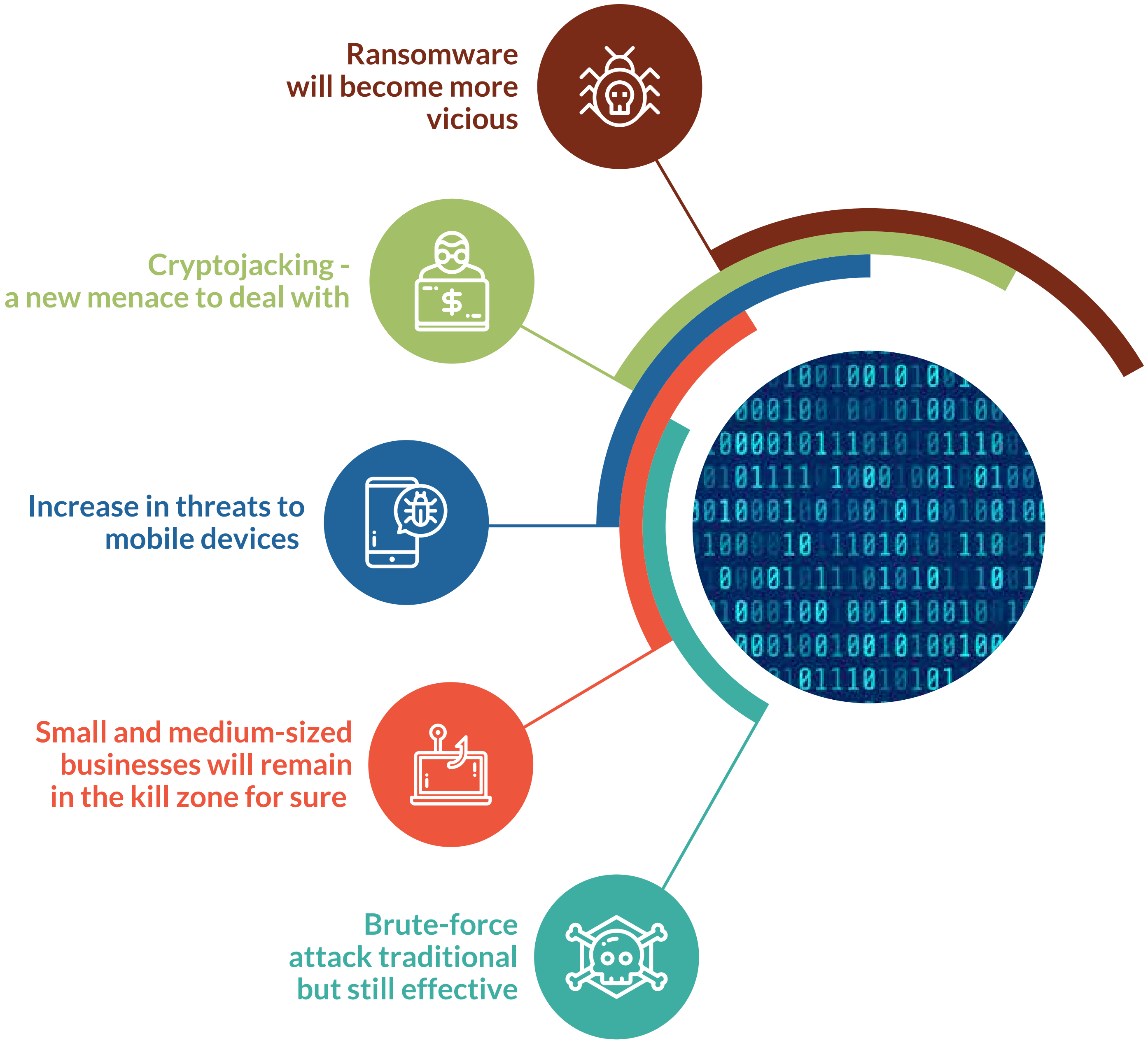
# About Quick Heal Security Labs

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:

# 2018
# Predictions that turned out right



Ransomware will become more vicious

Cryptojacking - a new menace to deal with

Increase in threats to mobile devices

Small and medium-sized businesses will remain in the kill zone for sure

Brute-force attack traditional but still effective

# Top **cyber-attack stories of 2018**

## RANSOMWARE GRABBED ATTENTION IN 2018

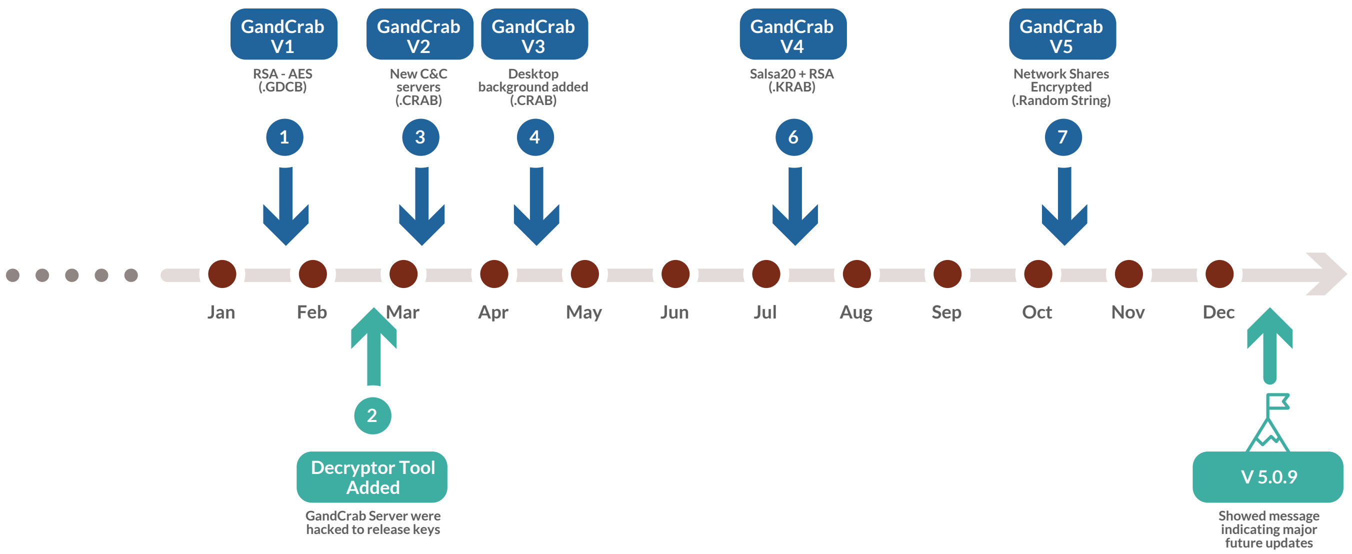
**In 2018, Quick Heal Security Labs observed many new destructive ransomware that immediately grabbed their attention:**

### 01 GANDCRAB: EVOLVING TO SECURE THE SHELL!

**Change is a law of life. But even in information security, Ransomware authors like Gandcrab seem to have taken this seriously. GandCrab was first observed in late January 2018 and within a month they claimed to have infected over 48,000 nodes. This massive infection undoubtedly turned Europol's head and made them coordinate with a security firm to hack GandCrab servers for decryption keys. Malspam emails is being observed as a major attack vector in GandCrab.**

**Since then, Gandcrab has kept evolving.**

## GandCrab Timeline



| Version | Description | Drawback |
|---|---|---|
| 1st Version | This is the first Ransomware which used Dash Currency. Office, database and other important processes like mail applications were stopped and files were encrypted so that no important file which might be in use is left behind without encryption. AES-256 was used for file encryption and AES-256 Key and IV was encrypted with RSA-2048. | Poorly protected C&C servers. Dependent on internet connectivity, i.e. encryption didn't continue until it found a server, meaning if a PC wasn't connected to internet at the time of infection, one could remove the malware and the data was safe!<br>Decryptor for this version was launched in late February. |
| 2nd Version | Started using Namecoin powered .Bit TLD (Top-Level-Domain) as C&C Servers (keys and data moved to a more secure location). Security researchers and police who hacked servers for keys were honoured by using their names for Hostnames. Ransomware used autorun entry in RunOnce registry key. | Dependent on internet connectivity, i.e. encryption didn't continue until it found a server, meaning if PC wasn't connected to internet at the time of infection, one could remove malware and data was safe! |
| 3rd Version | This time, ransomware had added a desktop wallpaper and also continued to use autorun entry in RunOnce registry key. | This version could not execute correctly on Windows 7 PCs. It resulted in users not being able to access their desktop. |
| 4th Version | Continued using Dash crypto currency, instead of AES, it started using SALSA20 algorithm for file encryption. Salsa20 made the encryption process faster. Salsa20 key was encrypted with RSA-2048, thus it made encryption impossible without the private key. Encryption process didn't wait for C&C server response. Distribution was carried out by compromised websites. | Continued to use DASH crypto currency that many users are unaware of. |
| 5th Version | Started encrypting files with random extensions thus AV might not detect by extension. HTML ransom note also included. Network shares are also encrypted. Many variants of version 5 were launched. | |

At the end of year 2018, GandCrab launched multiple variants. One variant was showing message box 'We will become back very soon :)!' This may be an indication of major update launching at the start of the coming year for a celebration of GandCrab's Birthday!

Ref: https://blogs.quickheal.com/gandcrab-says-will-become-back-soon/

## 02 DHARMA

**Variant of Dharma ransomware was observed to be able to disable/remove security software before execution of the ransomware payload. More than 150 extensions were observed in this ransomware campaign. For encryption it used AES 256 algorithm. The AES key was further encrypted with an RSA 1024. This encrypted AES key was kept at the end of the encrypted file. Before execution it executed PowerShell script to download multiple components from C&C which was used to perform determined attack chain. In downloaded contents, it contained Sticky key exploit, WannaCry vulnerability scanner tool and main Dharma payload. What's more dangerous was that after successful encryption, it tried to spread over the network. To deal with payment for decryption, they used email.**

Ref: https://blogs.quickheal.com/analysis-dharma-ransomware-outbreak-quick-heal-security-labs/

## 03 RYUK

**This ransomware campaign affected many users worldwide and seems to be a spear phishing attack or it exploits multiple windows vulnerability. The compelling thing, it encrypts victim files without appending any extension but making files unreadable. This ransomware targets small and medium business. Ryuk uses robust military algorithms such as 'RSA4096' and 'AES-256' to encrypt files. Ryuk demands ransom ranging from 15 BTC to 50 BTC in the form of Bitcoin to decrypt the files. Ryuk ransomware earned around half a million dollars from a single victim. This leads to the possibility of a few larger ransom payments which are not traced till date.**

Ref: https://blogs.quickheal.com/new-ransomware-campaign-wildryuk/

## 04 SOPHISTICATED KATYUSHA RANSOMWARE

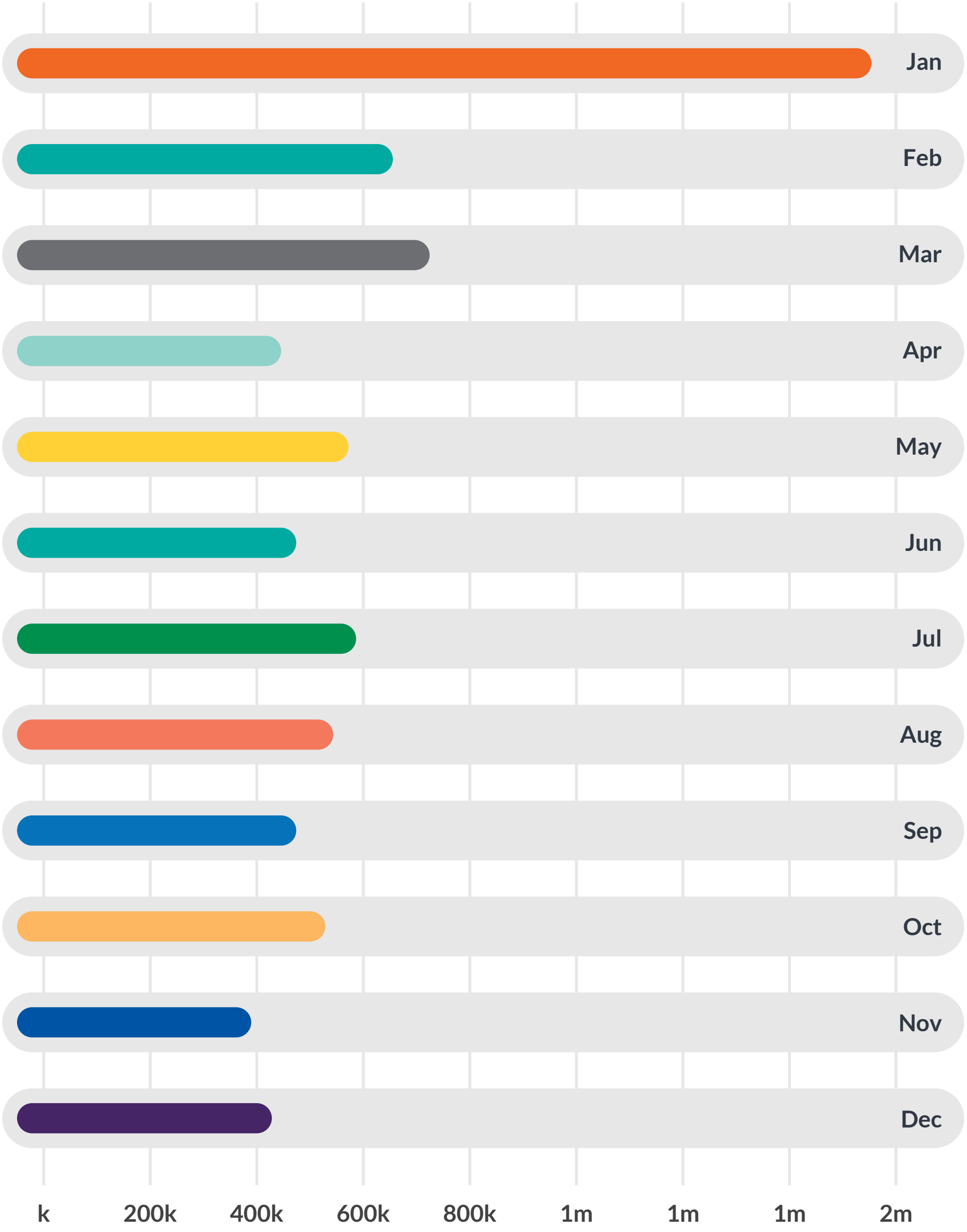
**Katyusha ransomware is more sophisticated ransomware. The ransomware package contains EternalBlue and DoublePulsar for lateral network activity together with the infamous password stealer Mimikatz. Also, uses a unique attack technique called "squiblydoo" to spread over the network, in this technique it injects malicious DLL. At the time of file encryption Katyusha encrypts files with RSA and adds extension ".katyusha" to encrypted files. It contains an exclusion list of files and folders (list contains names of many AV products) if found these directories or files in enumerated file paths then it will exclude that path from encryption. Also, it deletes shadow copies from the system. In ransom note, it demands an amount of 0.5 btc within three days and also threatens to release the data to public download if the ransom is not paid.**

Blog: https://blogs.quickheal.com/sophisticated-ransomware-katyusha/

**In addition to the above mentioned ransomware, few other ransomwares have also shown prevalence in the year 2018:**

- **WannaCry**
- **Foreign**
- **Blocker**
- **Cerber**
- **Jigsaw**
- **Onion**
- **Locky**
- **CTBLocker**

# Ransomware Detection Stats – 2018

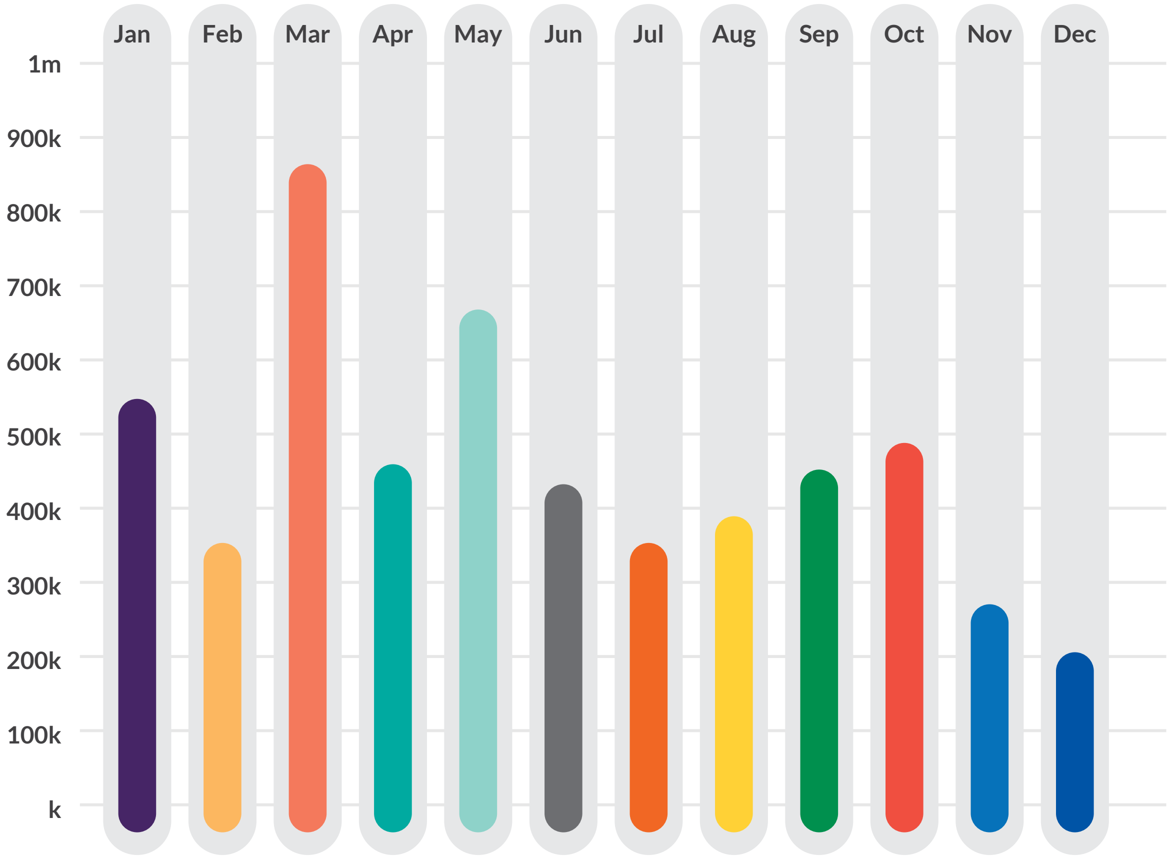


Ransomware Detection Stats - 2018

## CRYPTOJACKING

What attracts more than a magnet? You might have guessed it right – money! And where there is easy money, there is a lot of hustle and bustle. Cryptojacking - which uses someone else's computer to generate digital cash, aka cryptocurrency, for an attacker as long as they want. Due to its ease of deployment and an instant return of investments, cryptojacking has replaced ransomware as the number one threat for consumers and enterprises.

If one's computer is being used for cryptojacking, the only sign they might notice is slower performance or lag in execution. Most crypto mining scripts eat 100% of the targeted computer's CPU power which can significantly lower the lifespan of the hardware itself. In most cryptojacking cases that got reported, neither the owners of the compromised website nor its users were aware that they were the victims.



Cryptojacking Detection Stats - 2018

## EXPLOIT KIT ON RISE: NEW RECRUITS FOR EXPLOIT KITS

The year 2018 saw the emergence of two new exploit kits, Underminer and Fallout. Both exploit kits integrated the most recent exploits embedded in its landing pages to infect users when they access the compromised websites. The landing page served obfuscated code of CVE-2018-8174 which triggers remote code execution vulnerability in IE's VBScript engine (mshtml.dll). If the scripting option is disabled in user's browser then it launches flash's CVE-2018-4878 exploit which leverages a use after free vulnerability on a DRM operation listener object. Both these zero days have remained the trending exploits of 2018 since being weaponized in many APT attacks, exploit kits and malspam campaigns. The peculiar thing about CVE-2018-8174, also dubbed as Double Kill, is that apart from being delivered from malicious websites, it can also be exploited through OLE files wherein a URL moniker can be used to load mshtml.dll and execute the vbscript code. The recently discovered similar flash exploit CVE-2018-15982 is also expected to be incorporated in Exploit kits very soon.

## MAAS MOVING TOWARDS APT AS A SERVICE

Continuing with our last year annual threat report, our prediction about the new pillar of MaaS (Malware as a Service) that is RaaS (Ransomware as a Service), became true.

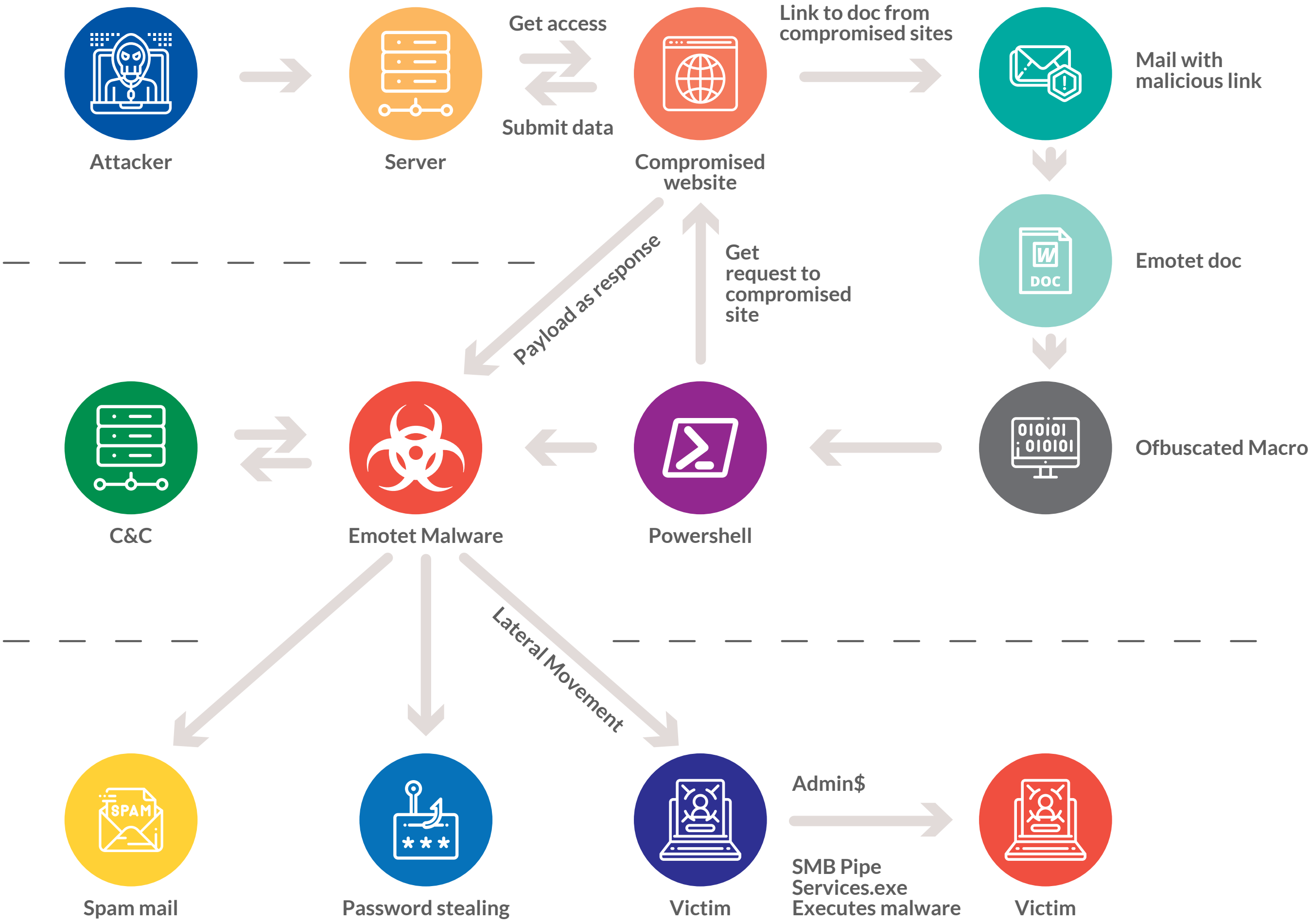
Initially interested only in the development of ransomware payload, RaaS developers started selling entire attack package along with the intrusion mechanism for a lucrative cut in the loot. Newer versions of SATAN Ransomware like DBger were spread in the first half of the year 2018 using RaaS. Satan conceived modular approach by using different templates but similar encryption technique. Here percentage of ransom was given to RaaS developers as a cut for their services. Again, others like FilesLocker ransomware developers are paying affiliate around 70% of their ransom.

This evolution of RaaS is actually pointing towards the future possibility of As-a-Service model for APTs too. We all know that planning and execution of APT (Advanced Persistent Threat) requires lots of skills, resources and time. Hence, in future malware authors may invest their time to find generic loop-holes in particular sectors like health, banking or cloud and then they will sell a well-organized attack vector to the attackers. Also, another possibility of APTs against particular countries, large organizations, government agencies, law enforcement systems, etc. may become a new pillar of 'Malware as a Service philosophy'. As roots of MaaS are spreading fast, we must be prepared with strengthened security shields against this organized cybercrime.

## EMOTET: A BANKING TROJAN KEPT TRENDING DURING 2018

Emotet is also known as a malware distributor. Throughout the year, we have seen many different patterns in Emotet campaign's initial attack vector, which is malicious doc or xls file. Those files contain highly obfuscated VBA macro code which ultimately executes cmd.exe through calls to Shell () and Run () functions. It further executes a second stage obfuscated PowerShell code to download and execute the malware from malicious domains. The PowerShell script holds 2 or more malicious URLs in case some domains are inactive. Emotet's obfuscated macro patterns have evolved over the year and has employed various obfuscation techniques to evade signature-based detection. Initially the macro was seen to be obfuscated with different mathematical functions like Mid, Sin, Tan, Trim and Shapes etc. Then it switched to using split string and string reverse patterns.

## EMOTET COMPLETE LIFE CYCLE

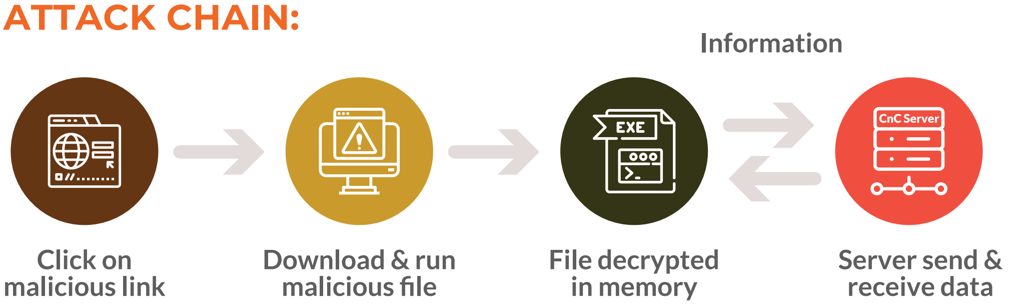


## AZORULT – THE INFORMATION EXFILTRATOR

**While most of the researchers were busy tracking ransomwares in the wild, AZORult was busy harvesting and exfiltrating data from the victim's machine to the C&C server. AZORult mainly used malicious links to download the malware. Infection vector is believed to be phishing emails. The AZORult Payload had multiple encrypted strings and data with high entropy. It tried to disable DEP. The code inside file was mostly obfuscated or encrypted. The conversation with C&C server carried information like installed software names, browser information and user/machine related information in encrypted form. It also collects information about the different cryptomining wallet from Electrum, MultiBit, monero-project etc. Stolen data can be used widely to gain unauthorized access to email accounts, bank accounts, and other online information. This stolen personal information can harm the user mentally as well as financially.**

Blog: https://blogs.quickheal.com/86983-2/

### ATTACK CHAIN:

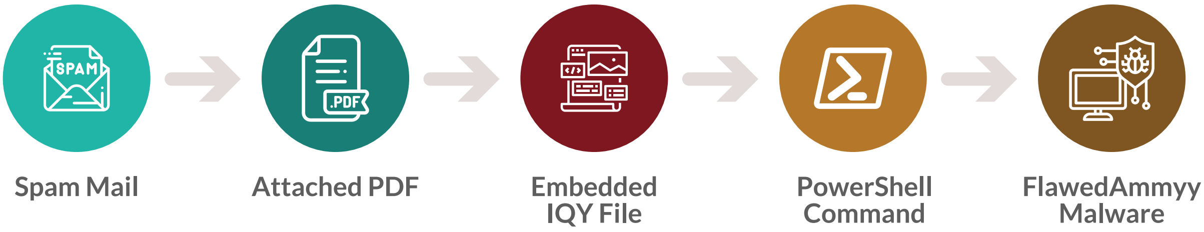


## Emerging trend of spreading malware through IQY files

**Attackers are constantly in search of finding new ways to spread malware; and delivering malware through IQY files is gaining lots of attention lately. IQY file is an Excel Web Query file that is used to download data from the internet. Attackers use Spear Phishing campaigns and spam mails with attached PDF or IQY files. In PDF, the 'importDataObject' function is used to import IQY file, and when the security checks are enabled, .iqy file is downloaded at %temp% location of victim machine and executed. Attackers have used this attack to deliver RATs like FlawedAmmyy RAT (remote access trojan).**

Blog: https://blogs.quickheal.com/emerging-trend-spreading-malware-iqy-files/

### ATTACK CHAIN:



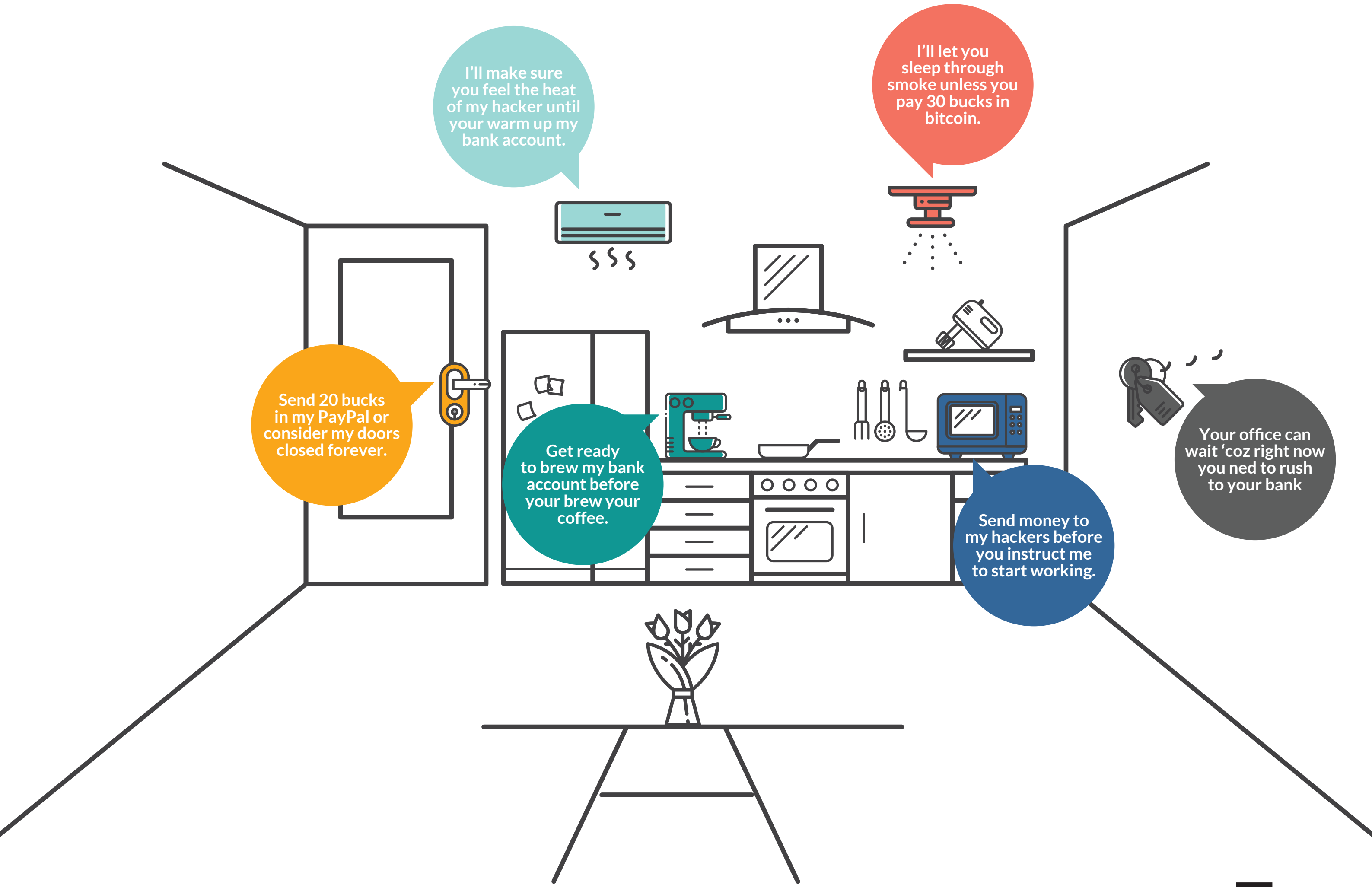
## IoT

While cyber criminals have been using various means for conducting cyber-attacks since long, Internet of Things (IoT) is fast coming up as the latest and rapidly trending means of cyber-attack. This can be attributed to the relative scalability and simplicity of the millions of devices that can easily be turned into potential victims, to cause cyber-attacks of a larger scale and stronger impact.

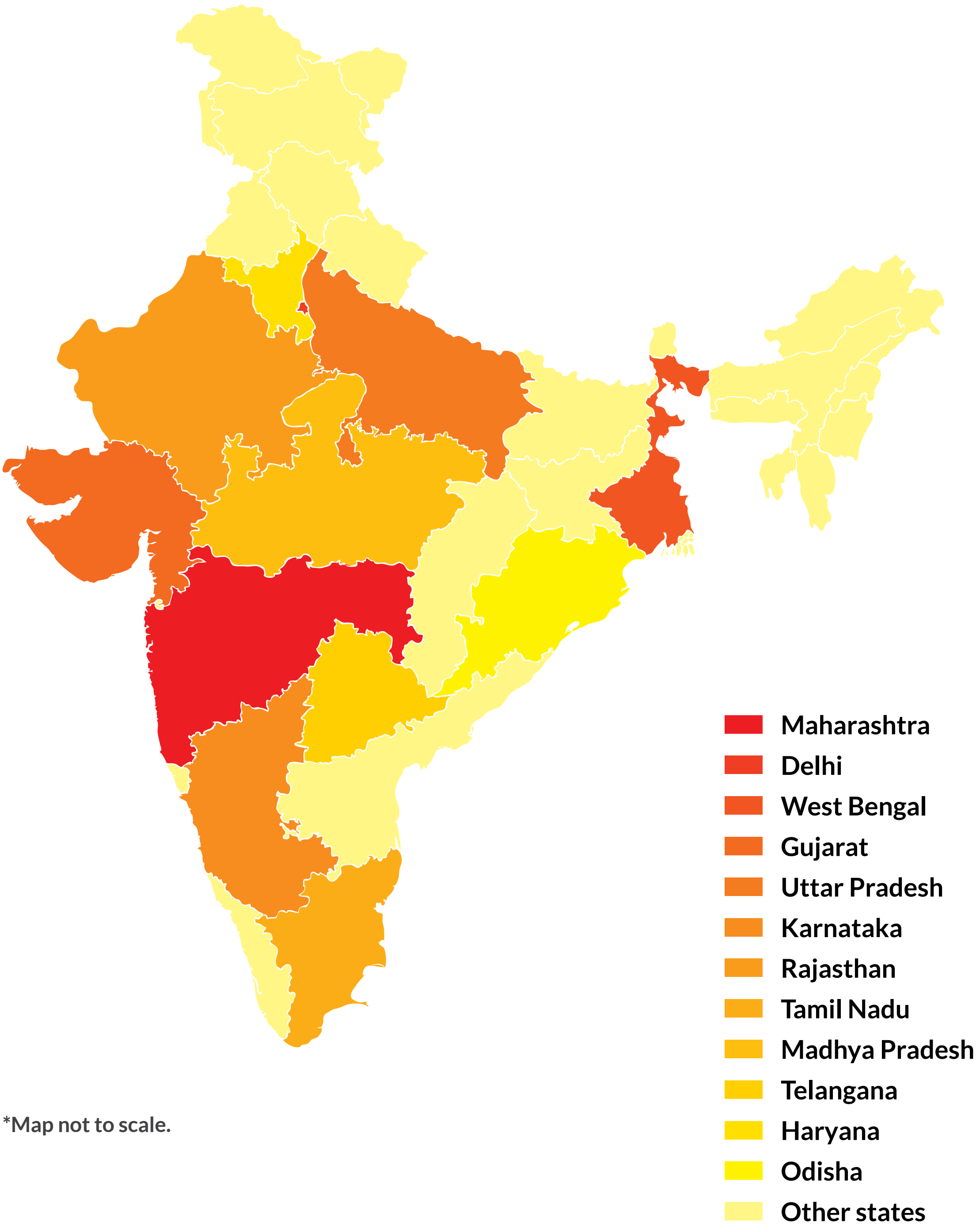
This simply means that it won't be long before your brand new connected coffee machine, refrigerator, microwave or for that matter your connected car, will serve as potential entry points to your network, leading to security risks and privacy intrusion.

While the types of cyber-attacks are usually the same and follow a similar pattern, depending on the device or ecosystem being used for conducting the attack and their protection level, the impact can vary dramatically.

Thus, while Internet of Things is playing a significant role in increasing the convenience level of people, careless safekeeping of devices connected to internet like your mobile, smartwatch, etc. can often put your personal data in the hands of opportunistic hackers and malicious thieves.

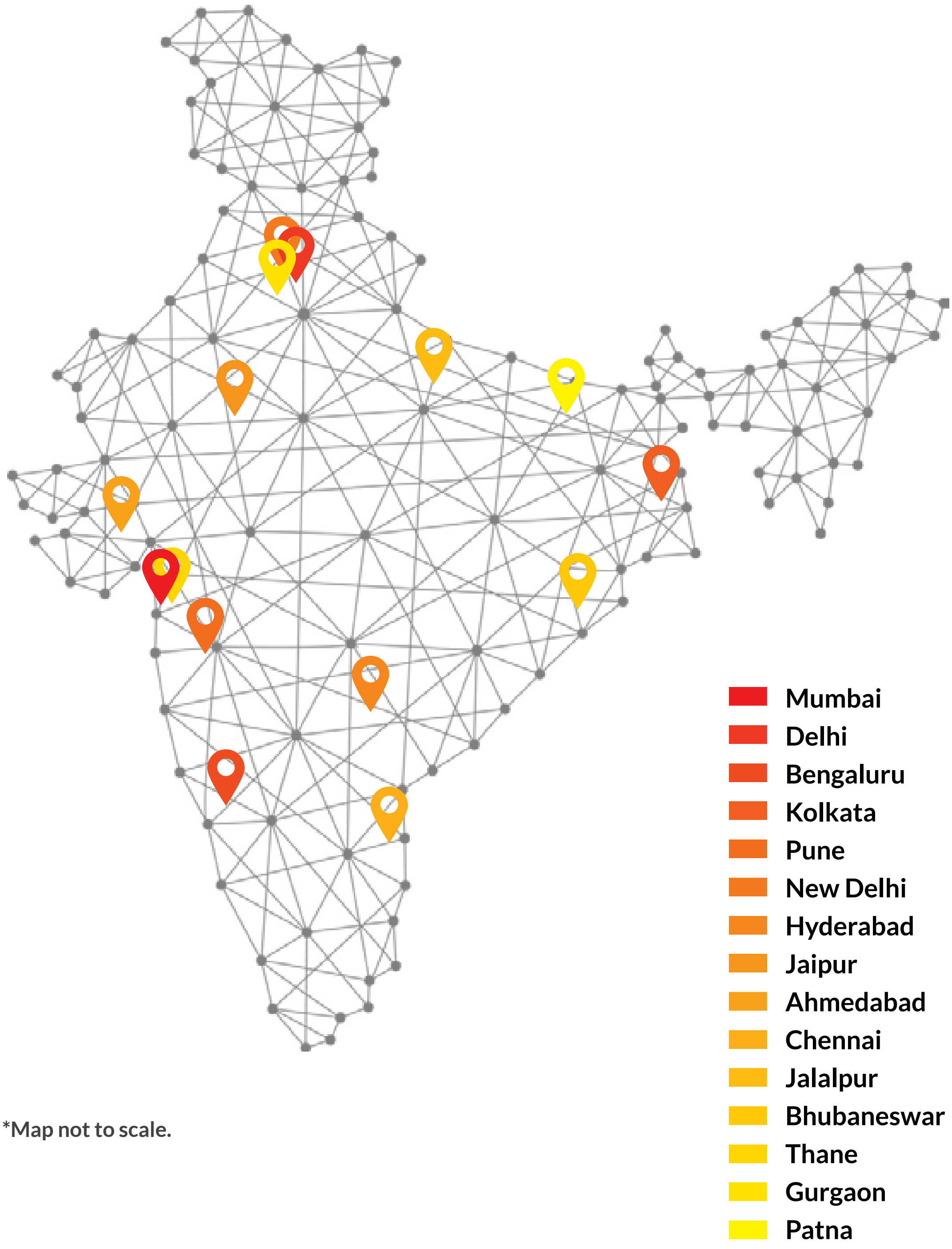

I'll make sure you feel the heat of my hacker until your warm up my bank account.
I'll let you sleep through smoke unless you pay 30 bucks in bitcoin.
Send 20 bucks in my PayPal or consider my doors closed forever.
Get ready to brew my bank account before your brew your coffee.
Your office can wait 'coz right now you ned to rush to your bank
Send money to my hackers before you instruct me to start working.

# Indian states **most at risk**



*Map not to scale.

# Indian cities **most at risk**



*Map not to scale.

# Windows

## Malware 973 Million

| | |
|---|---|
| Per Day: | 2,666,957 |
| Per Hour: | 111,123 |
| Per Minute: | 1,852 |

### Ransomware

| | |
|---|---|
| Per Day: | 19,671 |
| Per Hour: | 820 |
| Per Minute: | 14 |

### Exploit

| | |
|---|---|
| Per Day: | 145,807 |
| Per Hour: | 6,075 |
| Per Minute: | 101 |

### PUA & Adware

| | |
|---|---|
| Per Day: | 88,732 |
| Per Hour: | 3,697 |
| Per Minute: | 62 |

### Cryptojacking

| | |
|---|---|
| Per Day: | 16,296 |
| Per Hour: | 679 |
| Per Minute: | 11 |

### Infector

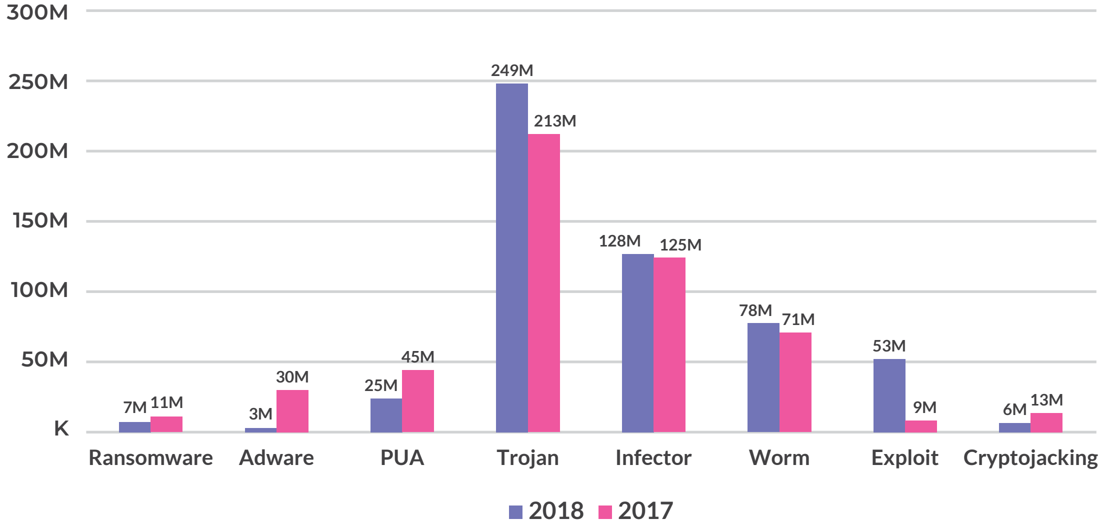
| | |
|---|---|
| Per Day: | 350,091 |
| Per Hour: | 14,587 |
| Per Minute: | 243 |

### Worm

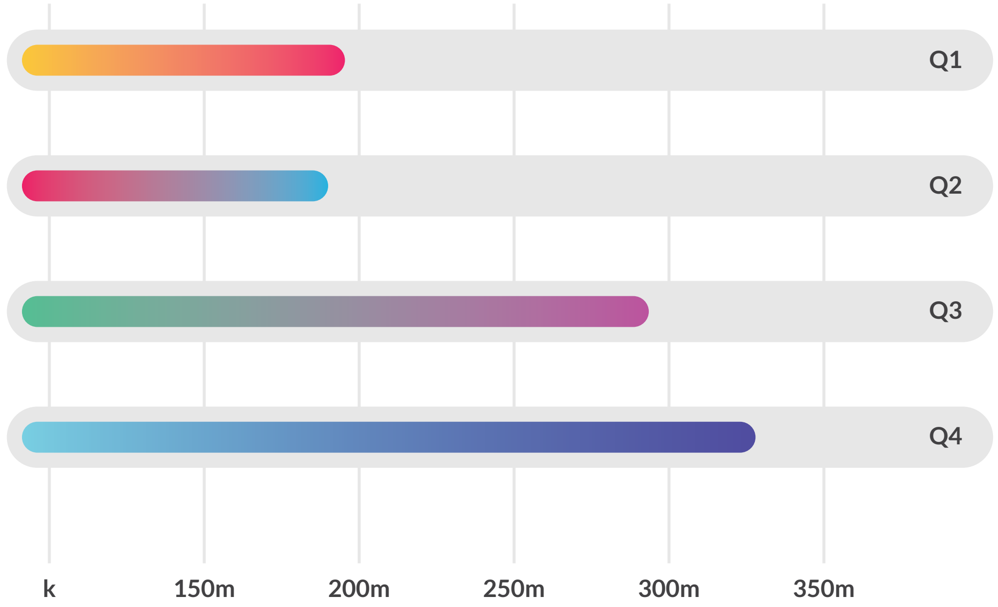
| | |
|---|---|
| Per Day: | 213,240 |
| Per Hour: | 8,885 |
| Per Minute: | 148 |

## WINDOWS DETECTION STATISTICS 2018

**The below graphs represent the statistics of the total Windows malware detected by Quick Heal Labs across the quarters, along with a comparative view of detections made in 2018 as compared to 2017.**

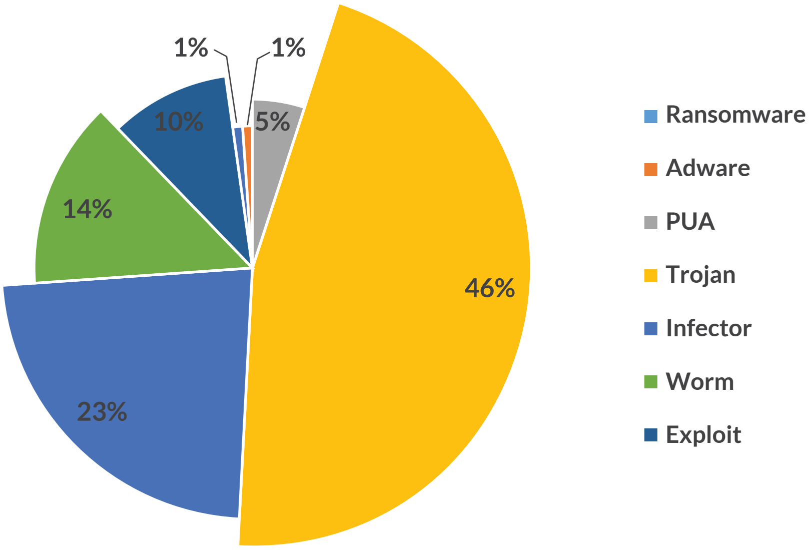


Windows malware detection YoY (2018-2017)

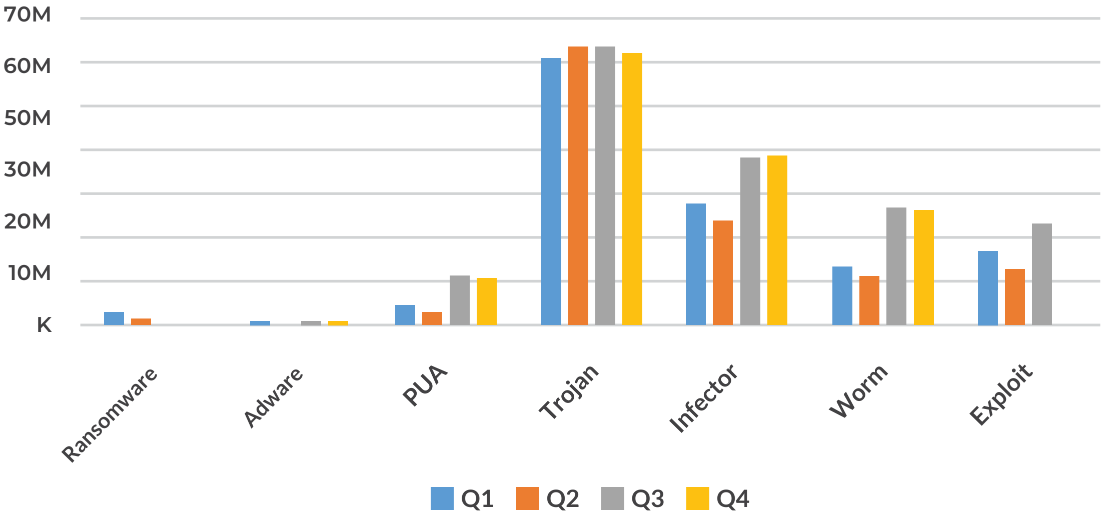


Quarter-wise Windows malware detection count in 2018

# WINDOWS DETECTION STATISTICS 2018



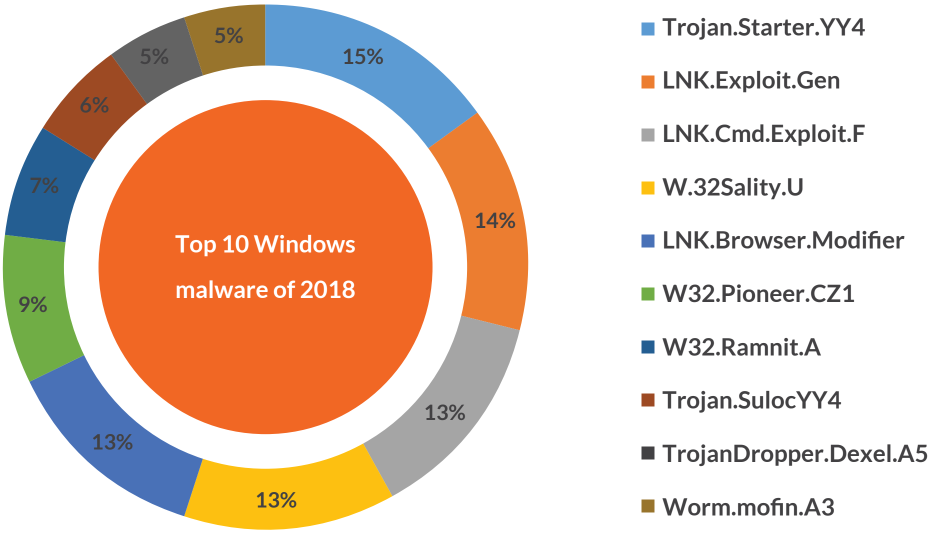
Category-wise windows malware detection in 2018



Quarter & category-wise Windows malware detection in 2018 (Q1 -Q4)

## TOP 10 WINDOWS MALWARE OF 2018

**The below figure represents the top 10 Windows malware of 2018. These malwares have made it to this list based upon their rate of detection across the year.**



Top 10 Windows malware of 2018

## Observations

**In 2018, Trojan.Starter.YY4 was detected to be the top Windows Malware, with around 23 Million detections made in 2018.**

### 01 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 the infected system to crash.
- Downloads other malware like keyloggers and file infectors.
- 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.

## 02 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.

## 03 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.

## 04 W32.Sality.U

**Threat Level:** Medium

**Category:** 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.

## 05 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.

## 06 W32.Pioneer.CZ1

**Threat Level:** Medium

**Category:** Infector

**Method of Propagation:** Removable or network drives

**Behavior:**

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

## 07 W32.Ramnit.A

**Threat Level:** Medium

**Category:** Infector

**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 the installer is dropped or downloaded, it drops its various components in memory or disk. Each component has a specified task. This will also speed up the process of infection.
- It infects all running processes.
- It also infects HTML files by appending script in it, while in the case of PE file infection, it appends itself in the file.
- It modifies registry entries to ensure its automatic execution at every system start up.

## 08 Trojan.Suloc.YY4

**Threat Level:** Medium

**Category:** Trojan

**Method of Propagation:** Bundled software and malicious websites

**Behavior:**

- Copies itself on the targeted drive, and start-up drive.
- Modifies registry entries to execute itself automatically and hides file extensions.
- Nested process continuously queries the information of dropped files and copies itself in download folder.

## 09 TrojanDropper.Dexel.A5

**Threat Level:** High

**Category:** Trojan

**Method of Propagation:** Email attachments and malicious websites

**Behavior:**

- Allows entry of other malware into the infected system. Changes registry and browser settings.
- Automatically redirects the user to malicious websites to drop more Trojan malware on the system.
- Steals confidential data from the infected system and can also destroy the data.
- Slows down system performance by consuming more resources.

## 10 Worm.Mofin.A3

**Threat Level:** Medium

**Category:** Worm

**Method of Propagation:** Removable or network drives

**Behavior:**

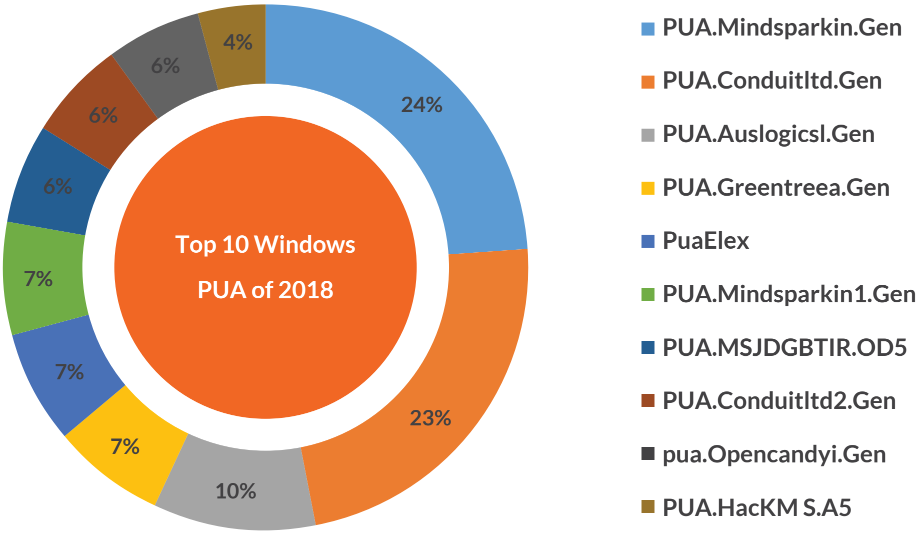
- Uses the Windows Autorun function to spread via removable drives. Creates an autorun.inf file on infected drives.
- This file contains instructions to launch the malware automatically when the removable drive is connected to a system. Searches for documents with extensions such as .doc, .docx, .pdf, .xls, and .xlsx. It copies the files it finds and sends them via SMTP (Simple Mail Transfer Protocol) to the attacker.

## 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 2018.



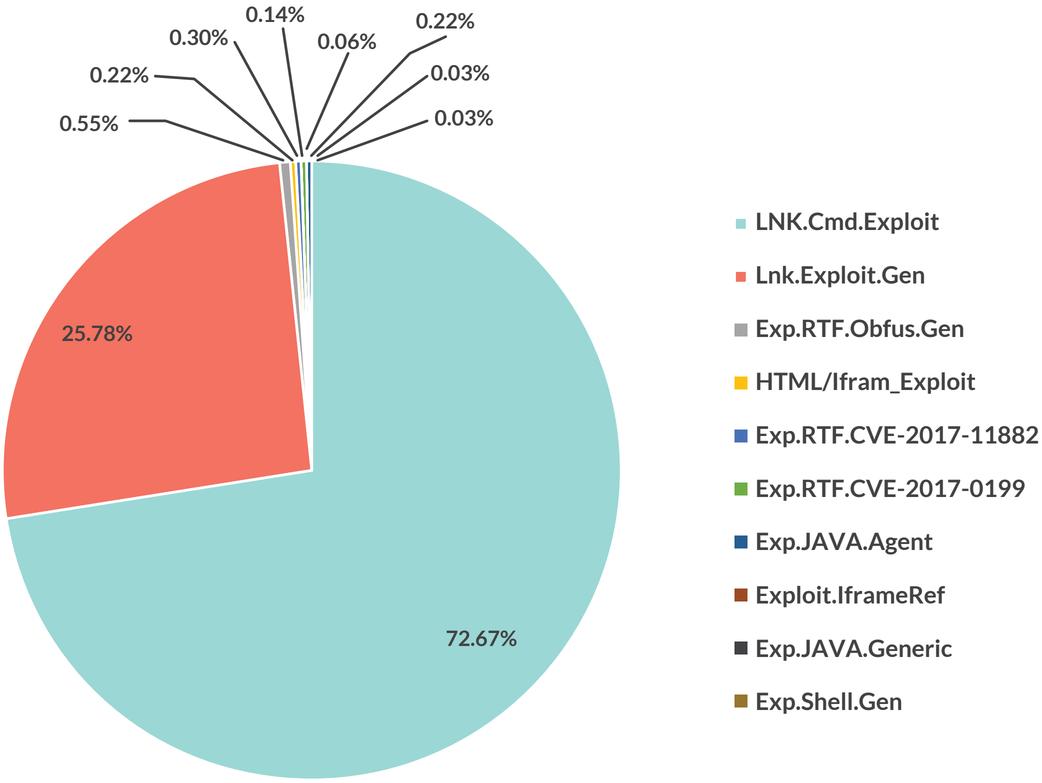
Top 10 Windows malware of 2018

## Observations

In 2018, PUA.Mindsparki.Gen was detected to be the top PUA, with around 1 Million detections made in 2018.

## TOP 10 HOST-BASED EXPLOITS OF 2018

A computer exploit is an attack designed by a hacker to take advantage of a particular security vulnerability the targeted system has. Below figures represent the top 10 Windows host-based exploits of 2018.



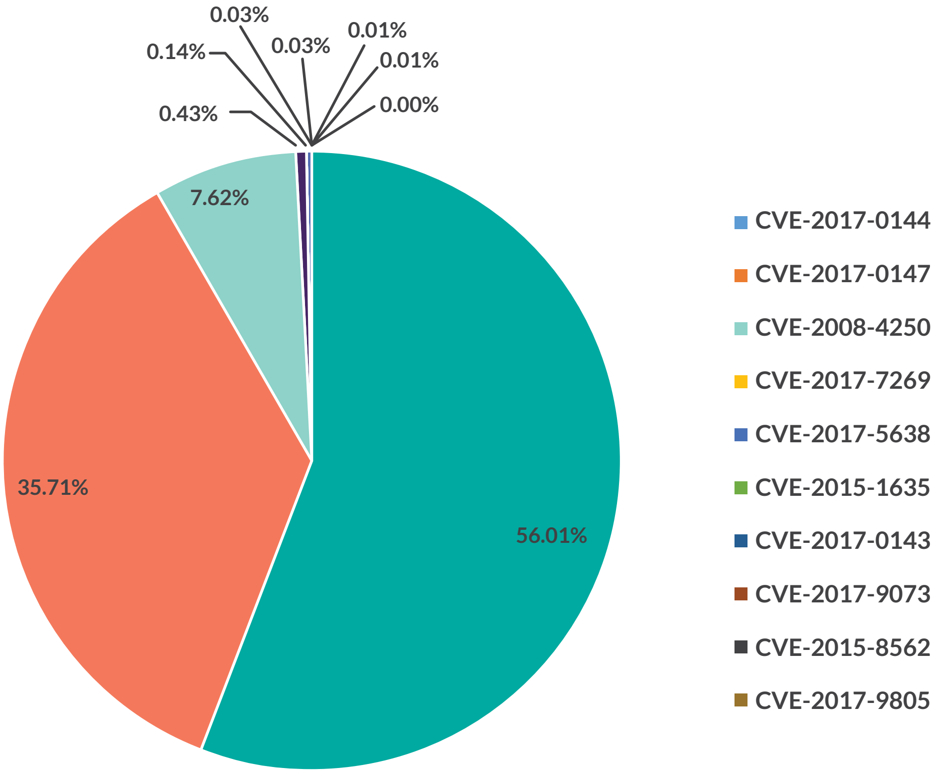
Top 10 host-based exploits of 2018

## 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 OF 2018

A computer exploit is an attack designed by a hacker to take advantage of a particular security vulnerability the targeted system has. Below figures represent the top 10 Windows network-based exploits of 2018.

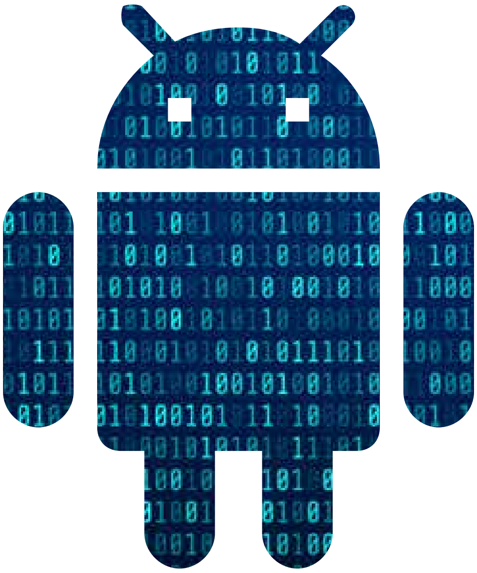


Top 10 network-based exploits of 2018

### 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).

# Android



## Malware

| | |
|---|---|
| Per Day: | 3,059 |
| Per Hour: | 127 |
| Per Minute: | 2 |

## Adware

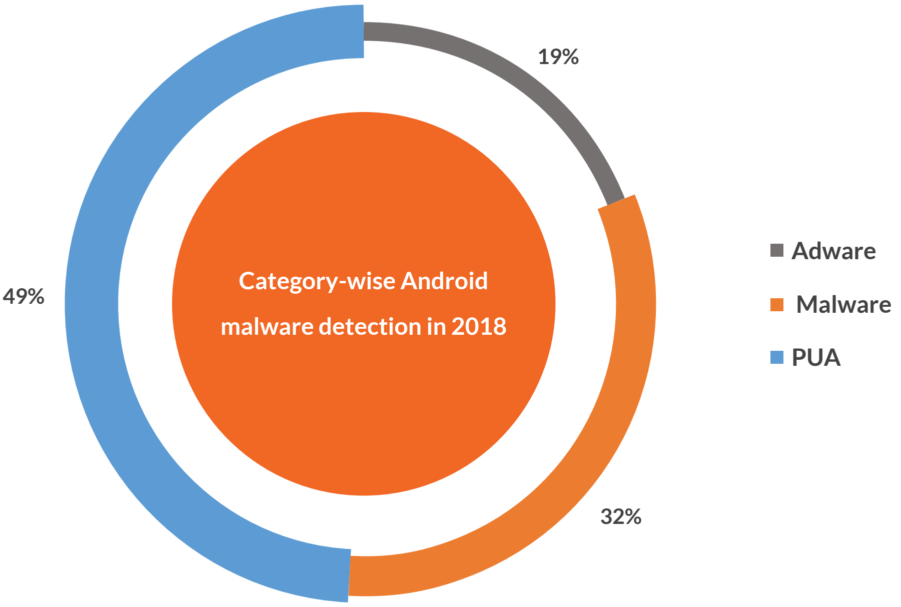
| | |
|---|---|
| Per Day: | 1,786 |
| Per Hour: | 74 |
| Per Minute: | 1 |

## PUA

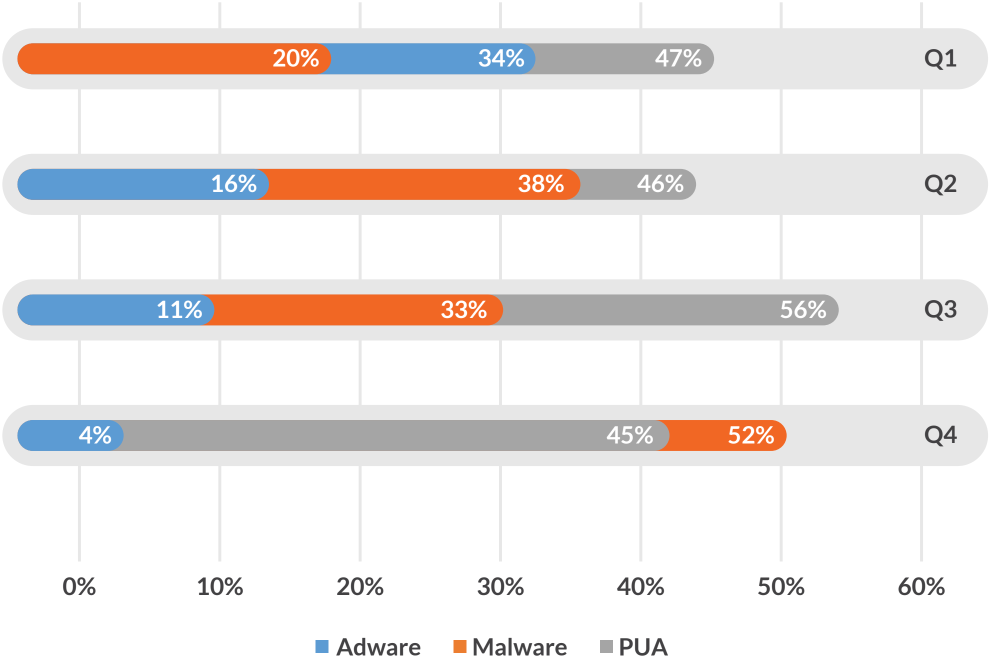
| | |
|---|---|
| Per Day: | 4,670 |
| Per Hour: | 195 |
| Per Minute: | 3 |

# ANDROID DETECTION STATISTICS 2018: CATEGORY WISE

**The below graphs represent the statistics of the total Android malware detected by Quick Heal Labs across the quarters in 2018.**



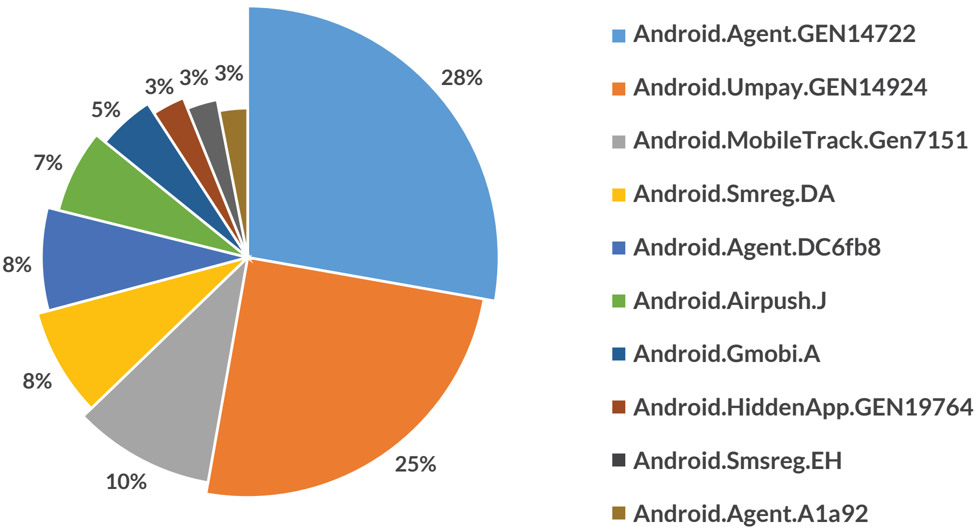
Category-wise Android malware detection in 2018



Quarter & category-wise Android malware detection in 2018 (Q1 -Q4)

## TOP 10 ANDROID MALWARE OF 2018

**Below figure represents the top 10 Android malware of 2018. These malwares have made it to this list based upon their rate of detection across the year.**



Top 10 Android malware of 2018

## Observations

**In 2018, Android.Agent.GEN14722 was detected to be the top Android malware, with around 0.1 Million detections made in 2018.**

### 01 Android.Agent.GEN14722

**Threat Level:** Medium

**Category:** Malware

**Method of Propagation:** Third-party app stores (Other than Google Play Store)

**Behavior:**

- Once launched, it hides its icon and works in the background.
- It can download other applications and prompt to install them.
- The downloaded applications can be malicious and infect the device further.
- Downloaded application may steal user information and send it to a malicious server.

## 02 Android.Agent.DC6fb8

**Threat Level:** Medium

**Category:** Malware

**Method of Propagation:** Third-party app stores (Other than Google Play Store)

**Behavior:**

- It disguises as a 'System Update'.
- It does not have any launcher icon and it works in the background.
- It starts its service after some interval from installation.
- It downloads other applications in background and prompts for installation.
- It collects device information like model, country, OSVersion, location, etc. and sends it to C&C server
- It also shows advertisements.

## 03 Android.Umpay.GEN14924

**Threat Level:** Medium

**Category:** Potentially Unwanted Application (PUA)

**Method of Propagation:** Third-party app stores (Other than Google Play Store)

**Behavior:**

- Umpay is a Chinese mobile payment SDK, which allows developers to request payments through Web, WAP & SMS.
- The SDK has many capabilities to make payment process easier & secure for app developers.
- Capabilities include sending SMS, collecting GPS location, intercept SMS, and checking if a device is rooted or not.
- It has been observed that some apps are misusing this SDK to earn money.
- It is used to send SMSs to premium numbers without user consent and for the collection of user information.

## 02 Android.MobileTrack.GEN7151

**Threat Level:** Low

**Category:** Potentially Unwanted Application (PUA)

**Method of Propagation:** Third-party app stores (Other than Google Play Store)

**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.

## 05 Android.Airpush.J

**Threat Level:** Low

**Category:** Adware

**Method of Propagation:** Third-party app stores (Other than Google Play Store) and repacked apps

**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.

## 06 Android.Agent.A1a92

**Threat Level:** High

**Category:** Malware

**Method of Propagation:** Third-party app stores (Other than Google Play Store)

**Behavior:**

- This malware is highly obfuscated and it carries an encrypted payload with it.
- It decrypts that payload during execution and drops another file, which is nothing but trojan banker.
- This trojan banker shows phishing login overlay on targeted bank application to steal user's credentials.
- This banker malware can steal contacts, messages and bank credentials.

## 07 Android.Smsreg.DA

**Threat Level:** Medium

**Category:** Potentially Unwanted Application (PUA)

**Method of Propagation:** Third-party app stores (Other than Google Play Store)

**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.

## 08 Android.Gmobi.A

**Threat Level:** High

**Category:** Adware

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

**Behavior:**

- Makes use of SDK (Software Development Kit) to easily recompile other genuine apps.
- Downloads other apps on the device causing unnecessary memory usage.
- Shares the infected device's information such as location and email account with a remote server.
- Displays unnecessary ads.

## 09 Android.HiddenApp.GEN19764

**Threat Level:** Medium

**Category:** Potentially Unwanted Application (PUA)

**Method of Propagation:** Third-party app stores (Other than Google Play Store)

**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.

## 10 Android.Smsreg.EH

**Threat Level:** Medium

**Category:** Potentially Unwanted Application (PUA)

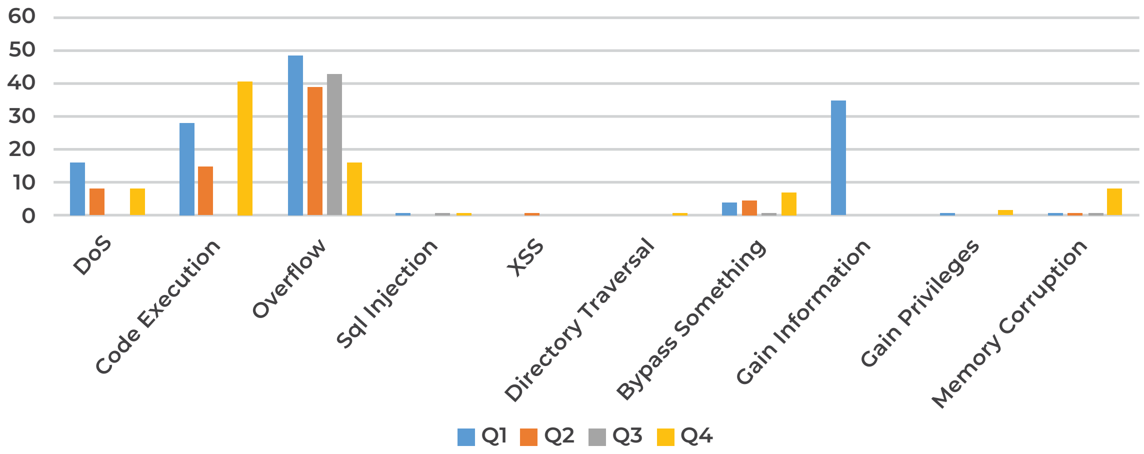
**Method of Propagation:** Third-party app stores

**Behavior:**

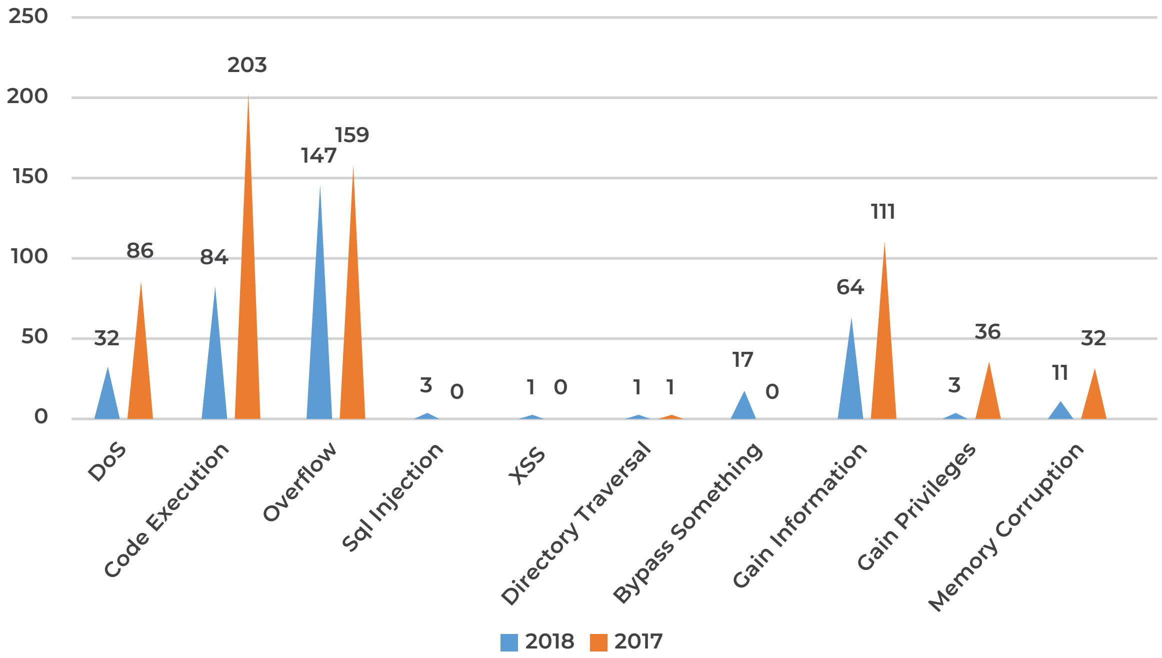
- It sends device IMEI and IMSI to premium rate numbers via SMS.
- It collects device data like SDK type, SDK version, phone company, phone number, etc.
- It sends the collected data to a remote server.

# ANDROID SECURITY VULNERABILITIES DISCOVERED IN 2018

**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 in 2018.**



Android security vulnerabilities in 2018



Android security vulnerabilities | 2018 vs 2017

Source: https://www.cvedetails.com/

# TRENDS IN ANDROID SECURITY THREATS

## Social networking accounts used for malicious purpose

**Day-by-day, malware authors are improving code complexity and use multiple layers to install malicious application. In AUG 2018 Quick Heal observed one malware that has all basic functionalities of the Android banker along with additional features like call forwarding, sound recording, keylogging and ransomware activities. It has ability to launch user's browser with URL received from the C&C server. This malware author uses the Twitter account to get C&C server address. It takes the encrypted server address from the specified Twitter account that starts with <zero> and ends with </zero>. It repeatedly opens the accessibility setting page until the user switches ON the 'AccessibilityService'. The AccessibilityService allowing the Trojan to enable and abuse any required permission without user concern. After launching one of the targeted application, the Trojan displays an overlay phishing login form of confidential information over its window where it asks the user to enter a username, password, and other sensitive data.**

Ref:

https://blogs.quickheal.com/android-malware-combines-banking-trojan-keylogger-ransomware-one-package/

## Hiddad applications found on Google Play

**This year, Quick Heal Security Lab has spotted number of applications on Play Store which hide themselves after installation and display full screen ads after specific time intervals. This trend is used by most of the developers these days to earn revenue through displaying ads by hiding itself. This application does not have other functionality other than displaying ads. There were more than 30 such apps on Play Store and after Quick Heal reported it to Google, they got removed from Play Store. The main purpose of this app is to display unwanted apps at random intervals, while other applications run. Once an app is installed, it displays an error and hides itself. But it still runs in background and shows ad after certain interval. These malicious applications use different names and icons like Play Store, YouTube, Play Services after hiding, which makes it difficult for the user to identify the malacious application to uninstall manually.**

Ref:

https://blogs.quickheal.com/aware-hiddad-malware-present-google-play-store/

## Fakeapp trick to increase download count

**Quick Heal Security Lab has spotted few FakeApps with over 48,000 installs on Google Play Store. These applications seem to be genuine as they use icons of genuine and famous apps but have no functionality other than downloading other apps to improve ratings. It just loads a URL and asks for login and displays the page to install the sponsored application to unlock the functionality of the fake application. They ask users to install the application and rate it 5 star, to access the functionality after 24 hours. The basic intention behind this is to increase the download count and good rating of the sponsored app. The sponsored app also does the same thing in order to use other apps. This is the trick of author to increase the download count to earn revenue in easily.**

Ref:

https://blogs.quickheal.com/fakeapp-discovered-google-play-store-increases-download-count-rating-applications/

## Beware!! PDF attachments launching Android malware

**Recently, at Quick Heal Security Lab, we observed a malicious PDF file sent to users as an attachment via a phishing email. These PDF files look like a regular document but that is not the truth. It looks locked out and blurred to misguide and make the user curious to open it. These kind of malicious documents are designed to lure the user into opening such documents. This is a key entry point for the malware to the device. These types of PDFs try to get attention of the user to click on it by using various ways like “To open this document, update your Adobe Reader” or “To unlock this document press below button”. When the user performs click action on that document, then it downloads malicious APK (Android executable) file from a malicious link present in that PDF. We found that malicious APK is nothing but spyware and spies on almost every activity on the user’s phone.**

Ref:

https://blogs.quickheal.com/beware-pdf-attachments-launching-android-malware/

# Predictions for **2019**

## THREATS TO BECOME MORE SOPHISTICATED AND EQUIPPED WITH ADVANCED AI-LED CAPABILITIES

According to researchers at Quick Heal Security Labs, threat actors are expected to deploy sophisticated and advanced, AI-led attacks, to boost the speed, scalability, accuracy and impact of their campaigns.

## INCREASE IN WEB SKIMMING ATTACKS

With cybercriminals expanding the scalability of their attacks, new variants of web skimming attacks such as Magecart are also expected to gain prominence in 2019. These skimming attacks are meant to skim login credentials and other sensitive information in addition to credit card data.

## INCREASE IN WEB SKIMMING ATTACKS PROJECTED RISE IN RANSOMWARE ATTACKS TARGETING UTILITY INFRASTRUCTURE

A significant rise is expected in Ransomware attacks on utilities such as electricity, mobility, oil etc. Cybercriminals through such attacks will primarily aim to increase the possibility of better pay-outs by holding critical infrastructure to ransom. Targeted Ransomware attacks against organisations is also expected to increase, especially during the fiscal closing period 2018-19.

## AN INCREASE IN TARGETED IOT-BASED ATTACKS

The adoption of internet connected devices (Internet of Things or IoT) in various sectors, will propel cybercriminals to easily turn these devices into potential victims owing to their relative scalability and simplicity.

## INCREASE IN TARGETED CYBERCRIMES ACROSS DESKTOP, MOBILE, AND CLOUD ENVIRONMENTS

Quick Heal Security Labs predict 2019 to witness a significant rise in spamming, phishing, malvertising, social engineering, and fake news during important public events such as, the General Elections, ICC World Cup, FIFA Women's World Cup, IPL etc.

## CRYPTOMINING AND CLOUD-BASED ATTACKS TO RISE

Cryptomining attacks are stealthier and generate instant returns from infecting a system, which will drive their popularity amongst cybercriminals in 2019. Cloud-based environments became the favourite haunt for cryptocurrency mining malware in 2018 and these are only expected to explode in the coming year.

## MOBILE LANDSCAPE EXPECTED TO BECOME MORE THREAT-PRONE IN 2019

**Quick Heal Security Labs predicts a significant rise in the number of mobile-focused malware and banking trojans. Another major mobile-based threat expected to gain prominence is the introduction of malicious code into clean owned applications post update. This is most likely to take place once the download count has hit a significant landmark on the Google Play Store.**

## RISE IN TARGETED ATTACKS TO EXPLOIT SUPPLY CHAIN VULNERABILITIES

**Cybercriminals move from attacking target to exploiting supply chain vulnerabilities; increase in the number of file-less malware designed to evade security products.**

## ATTACKS ON THE FINANCIAL SECTOR TO INCREASE

**Cybercrimes aimed at the BFSI sector are predicted to increase even further, prominently in areas with low cybersecurity awareness and adoption, such as the SAARC region, Southeast Asia, and Central Europe.**

## DATA PROTECTION TO BECOME ESSENTIAL DUE TO DATA-CENTRIC ATTACKS

**Owing to the major policy changes, such as the implementation of the European Union's Data Protection Regulation (GDPR) and the discussion around draft bill for data protection in India, Quick Heal Security Labs expects data protection to become an essential component of security strategy.**

# Conclusion

In wake of the significant rise in targeted cyber-attacks across various platforms, sectors and environments, Quick Heal's Annual Threat Report can help people at large adapt robust security measures across their networks, devices, applications and environments.

With cyber-attack highlights from 2018 and important predictions made for the year 2019, it will become easier for you to inculcate best security practises while browsing the internet, storing and sharing important data, using free network connections, making online transactions or depending on connected devices.

However, the most important step for ensuring a safe and carefree 2019 would be to make sure that all the protection levels on your security software are always ON for the first line of protection.

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

- Keep strong passwords for all your accounts.
- Enable Two-Factor Authentication
- Keep backup of all important data.
- Regularly patch your systems with latest software & security updates.
- Check sender's genuineness & be careful while responding to emails to stay safe from phishing emails.
- Be cautious while clicking/downloading on anything over internet.
- Try not to access confidential accounts on public devices or networks.
- Respond to Antivirus notification sensibly.
- Keep regular audit of reports of system, antivirus, network etc.