Quick Heal
Security Simplified

SEQRITE
Enterprise Security Solutions by Quick Heal

# ANNUAL THREAT REPORT 2017

# Executive Summary

The Annual Threat Report 2017 presents a detailed insight into the state of digital security for Windows and Android users. The report begins with the Windows malware detection figures of 2016, followed by the top 10 Windows malware and their characteristic features. The report further delves into the detection statistics of various malware categories, top 10 PUAs (potentially unwanted applications), adware and exploits. Information about the most concerning Windows malware of 2016 also forms a part of this report. The Android section of the report elaborates on the Quick Heal's detection stats of mobile malware, top 10 Android malware, mobile ransomware, and mobile banking Trojans. Quick Heal's Threat Research Labs observed a few malware to be using unique techniques and these have also been discussed in this report, followed by a brief on security vulnerabilities affecting the Android platform. Towards the conclusion, some important security trends and predictions have been discussed to present an overview of what users can expect in the near future.

# TABLE OF CONTENTS

# INTRODUCTION

Quick Heal Labs detected over 1.2 billion malware affecting the Windows platform in 2016, with Q1 clocking the highest detection rate. Trojan leads the pack of the malware family, followed by infector, worm, and adware. Ransomware detections on Windows have gone up 92% from the year before. Several targeted attacks were observed in 2016; one of these attacks was launched against an Indian government organization. Technical Support scams were rampant this year, and so was the use of audio ads by the adware family. 14 new Windows ransomware families were discovered in 2016, cementing the fact that ransomware attacks are only increasing. In terms of the Android platform, Quick Heal detected a 50% increase in the detection count. Mobile ransomware has clocked a 450% increase from Q1 to Q4 in 2016 while mobile banking Trojan has shown a 110% rise. In 2016, we observed an increase of 1364% in the use of security vulnerabilities to gain privileges on infected mobile devices, when compared with 2015. Important trends and predictions discussed include threats arising from the lack of security standards in Internet of Things (IoT) devices, adware deploying advanced techniques, file-encrypting ransomware that can steal user data, and increasing attacks on e-wallet and other online payment systems.

# WINDOWS MALWARE DETECTION STATISTICS

Given below is the statistics of Windows malware detected by Quick Heal Labs in 2016.

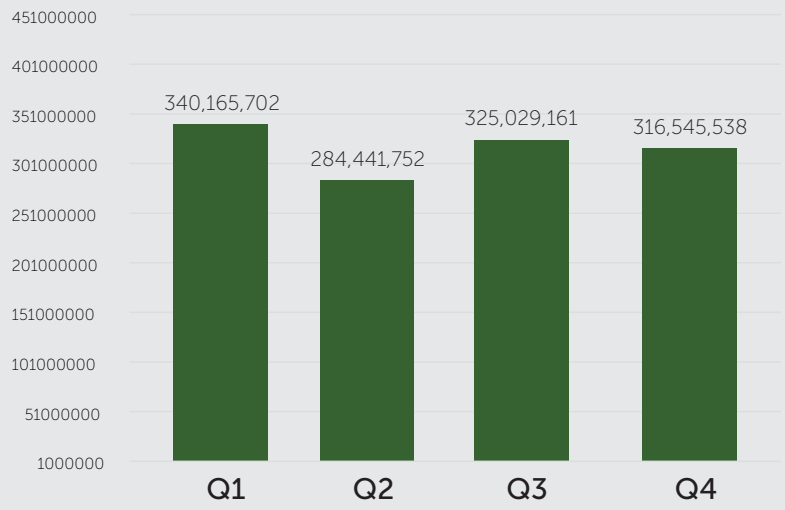



Fig 1

| 2016 | DETECTION COUNT |
|---|---|
| Q1 | 340,165,702 |
| Q2 | 284,441,752 |
| Q3 | 325,029,161 |
| Q4 | 316,545,538 |
| **TOTAL** | **1,266,182,153** |

# TOP 10 WINDOWS MALWARE

These are the top 10 Windows malware detected by Quick Heal in 2016.

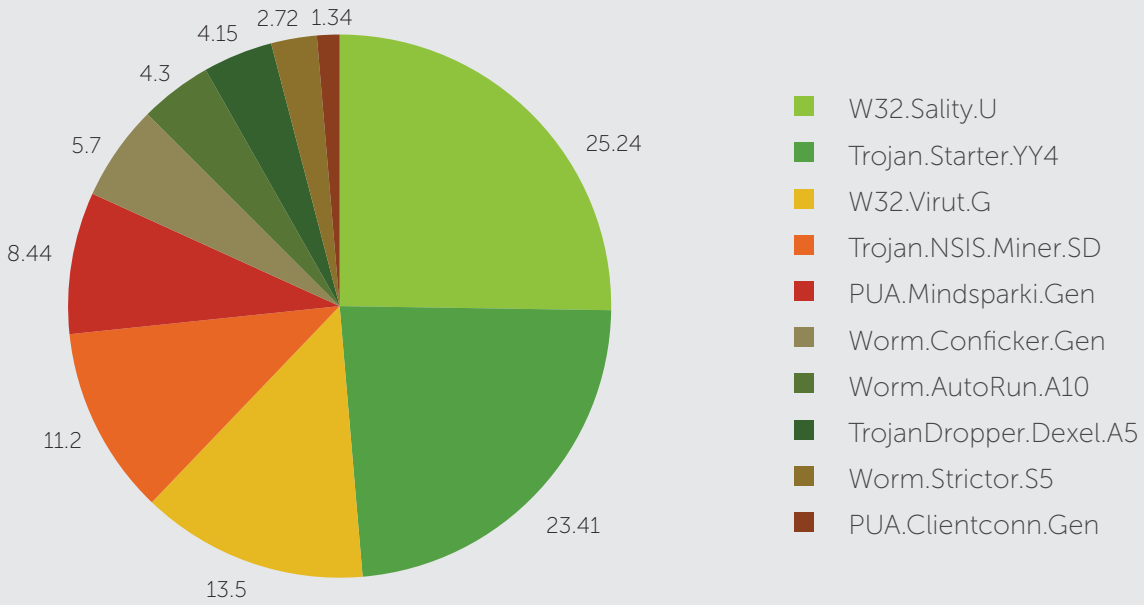



Fig 2

### 1. W32.Sality.U

**Damage Level**: MEDIUM

**Method of Propagation**: Bundled software and freeware

**Summary**: W32.Sality.U is a polymorphic file infector. After execution, it starts computing and infecting all the executable files present on local drives, removable drives, and remote shared drives.

**Behavior Post Infection**:

- 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.

### 2. Trojan.Starter.YY4

**Damage Level**: HIGH

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

**Summary**: Trojan.Starter.YY4 is a Trojan that works by connecting to a remote server and installing other malware on the computer that it infects. In other words, it is used as an entry point by other malware. This malware is linked to various banking Trojans and worms designed to spread over networks.

**Behavior Post Infection**:

- 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.

# TOP 10 WINDOWS MALWARE

### 3. W32.Virut.G

**Damage Level**: MEDIUM

**Method of Propagation**: Bundled software and freeware

**Summary**: W32.Virut.G is a family of viruses associated with various botnets. It injects its code within running system processes and starts infecting the executable files present on local drives and removable drives. It also lets other malware enter the infected system.

**Behavior Post Infection**:

- Creates a botnet that is used for Distributed Denial of Service (DDoS) attacks, spam frauds, data theft, and pay-per-install activities.
- Opens a backdoor entry that allows a remote attacker to perform malicious operations on the infected computer. The backdoor functionality allows additional files to be downloaded and executed on the affected system.

### 4. Trojan.NSIS.Miner.SD

**Damage Level**: HIGH

**Method of Propagation**: Bundled software and freeware

**Summary**: Trojan.NSIS.Miner.SD is a Trojan that comes with freeware and shareware programs. Once installed on the infected computer, it redirects the victim to malicious websites.

**Behavior Post Infection**:

- Downloads or installs free software from malicious websites.
- Automatically executes when the system starts.
- Modifies important system files and Windows registry settings.
- Makes excessive use of system resources for bitcoin mining which further degrades the infected system's performance.
- Opens a backdoor for other malware to enter the infected system.

### 5. PUA.Mindsparki.Gen

**Damage Level**: MEDIUM

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

**Summary**: PUA.Mindsparki.Gen is a Potentially Unwanted Application (PUA) that comes with third-party bundled installer applications and software downloaders.

**Behavior Post Infection**:

- Changes the infected system's Internet browser homepage and default search engine to ask.com or yahoo.com.
- Installs a toolbar powered by ask.com.
- Asks the user to download software mentioned on the toolbar.

### 6. Worm.Conflicker.Gen

**Damage Level**: HIGH

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

**Summary**: Worm.Conficker.Gen is a worm that can automatically spread from one system to the other in a network, without any human interaction.

**Behavior Post Infection**:

- Allows remote code execution when file-sharing is enabled on the infected system.
- Disables several important system services including security software.
- Downloads and executes other malware on the infected system.
- Stops victims from visiting websites related to security software and services that can assist in its removal.

### 7. Worm.AutoRun.A10

**Damage Level**: HIGH

**Method of Propagation**: Spam emails and bundled software

**Summary**: Worm.AutoRun.A10 is a worm designed to steal personal and confidential information from the infected system.

**Behavior Post Infection**:

- Utilizes system resources resulting in degradation of system performance.
- Steals user's personal and confidential information such as credit card details, banking information, email passwords, other account passwords, private photos, etc.

- Downloads other malicious programs on the infected computer without user's consent.
- Searches for vulnerabilities in installed programs on the infected system for destructive purposes and this may cause a system crash.

### 8. TrojanDropper.Dexel.A5

**Damage Level**: HIGH

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

**Summary**: TrojanDropper.Dexel.A5 is a Trojan that can break the infected system's security.

**Behavior Post Infection**:

- 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.

### 9. Worm.Strictor.S5

**Damage Level**: LOW

**Method of Propagation**: Spam emails and malicious websites

**Summary**: Worm.Strictor.S5 is a worm that spreads through spam emails that contain malicious links or malicious attachments. It modifies the infected system's registry settings for auto start. It also drops other malware such as adware and spyware on the infected system.

**Behavior Post Infection**:

- Worm.Strictor.S5 changes the homepage settings and substitutes the existing website with a malicious one.
- Redirects user's web searches to harmful domains.
- Asks the user to download free software, videos, games, etc.

### 10. PUA.Clientconn.Gen

**Damage Level**: MEDIUM

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

**Summary**: PUA.Clientconn.Gen is a PUA that protects its search engine settings for browsers like default-search.net, search.ask.com, and Trovi search.

**Behavior Post Infection**:

- SearchProtect, SafetyNut Inc., and Aztec Media Inc., are adware program publishers which are promoted and downloaded by bundled software.
- Changes browser's configuration settings and adds entries of the above-mentioned search engines.
- Displays excessive advertisements when the user is browsing.

# MALWARE CATEGORIES

The below graph presents the statistics of every category of Windows malware detected by Quick Heal in 2016.

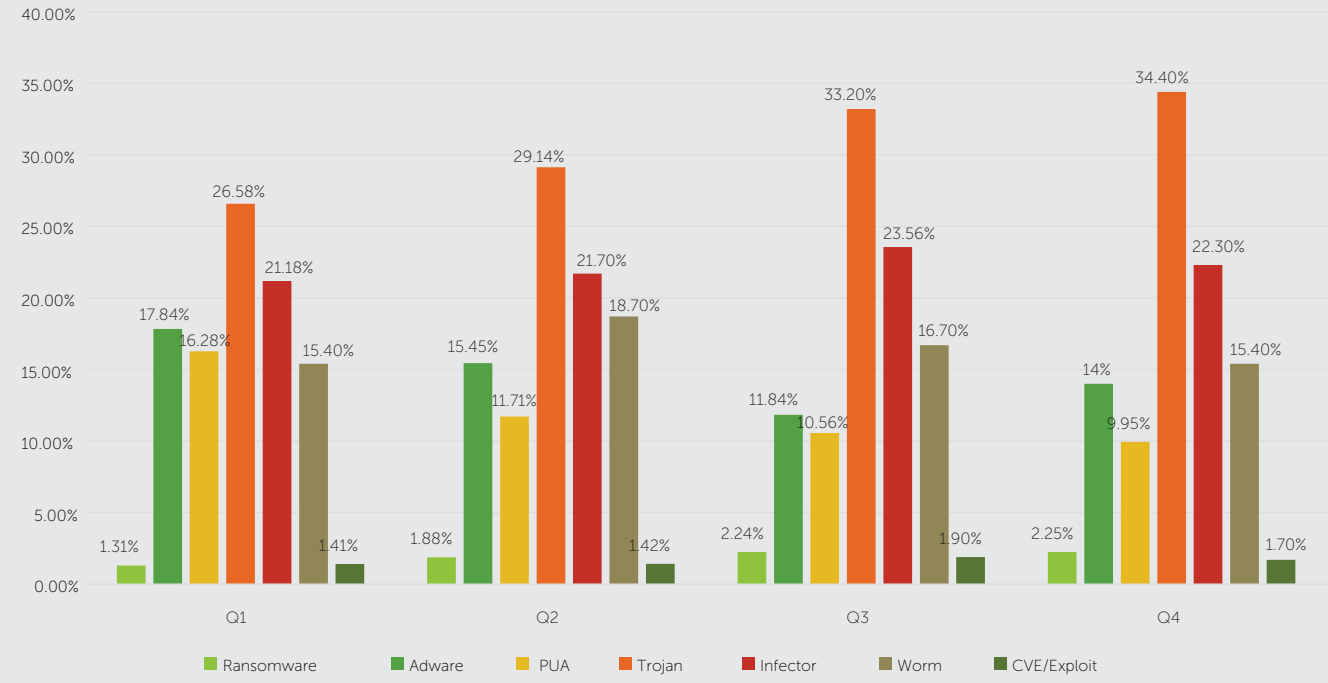



Fig 3

## Observations

**1**

**Trojan** leads the pack with **(≈30.83%)** (fig 3)

**Infector** follows with a detection of **(≈22.18%)** (fig 3)

**Worm** accounts for **(≈16.55%)** of the detection count (fig 3)

**2**

**RANSOMWARE GROWTH**

**1%** (2015)

↑ **92%**

**1.92%** (2016)

**3**

**Adware** detection contributed **(≈14.78%)** (fig 3)

# TOP 10 PUAs AND ADWARE

Potentially Unwanted Applications (PUAs) are classified as a low-risk malware category. However, some of them may lead to the download of other malware and threats. After installation, PUAs may display unwanted pop-up ads or coupon ads based on the browsing habits of the user. Here are the top 10 PUAs and adware samples detected by Quick Heal in 2016.

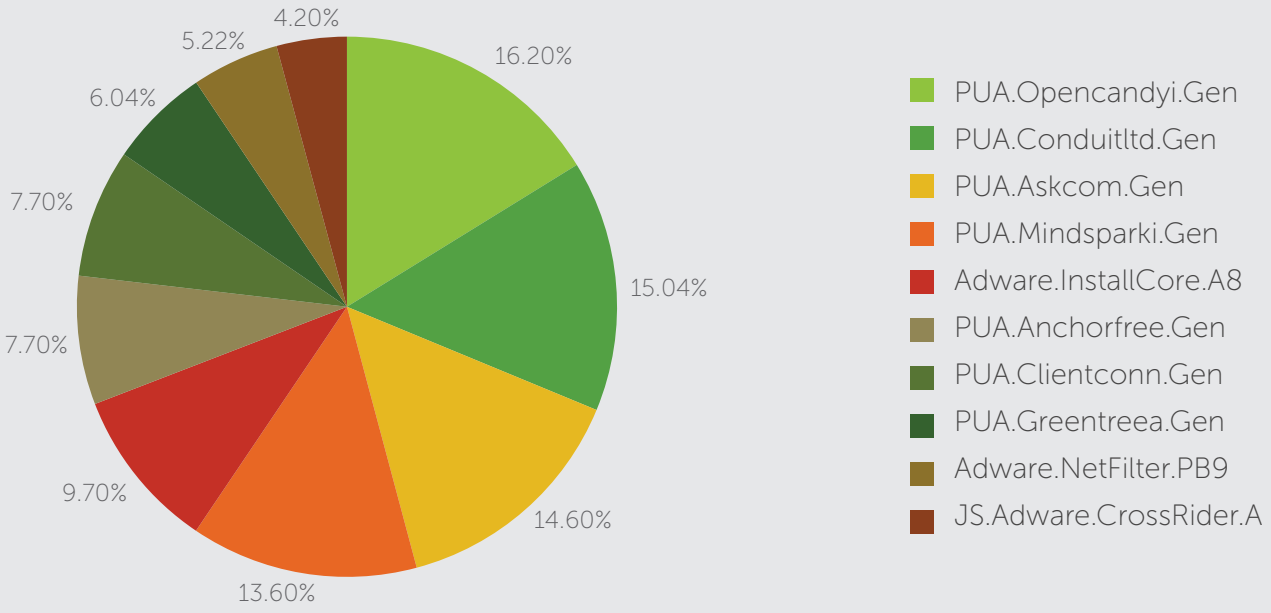



Fig 4

## Observations

- Some of these PUAs and adware come with free software. As observed, video players and download manager programs are the common PUAs that are being distributed in the market. Although these are not malicious, their stealthy behavior such as installing toolbar or plugins for web browsers without user consent could label them as Potentially Unwanted Applications that support downloading of other related (mostly unwanted) applications.
- Opencandyi, Conduitltd, Mindsparki, and Askcom are the top PUAs of 2016.
- Anchorfree is a browser hijacker and often comes bundled with free software. It changes browser settings such as homepage and search engine, and also adds unwanted toolbars.
- Adware Crossrider may install BHO/Plugins/extensions and change some of the browser settings without user consent. It also displays pop-up ads on web pages while the user is surfing the Internet. The adware can also inject advertising banners into web pages.

# TOP 10 WINDOWS EXPLOITS

A computer exploit is defined as an attack designed by a hacker to take advantage of a particular security vulnerability the targeted system has.

Here are the top 10 Windows exploits of 2016.

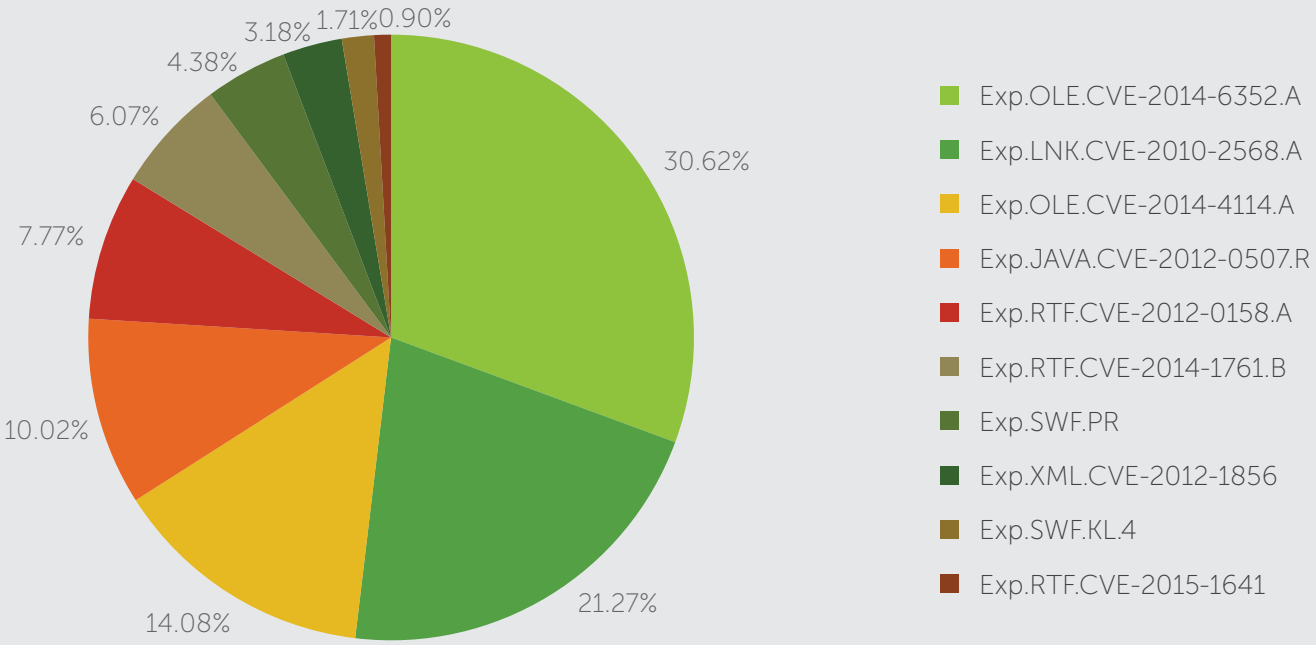



Fig 5

# MAJOR WINDOWS MALWARE

## Targeted Attack

2016 is another year that has witnessed the discovery of many targeted attacks. Various activity groups have been found to be active since long and running silently; stealing information for financial gains remains the main objective of such attacks.

- This year, Quick Heal detected a targeted attack on an Indian government organization. The group behind this attack goes by the name 'Quarian' and has been active since 2011. This group carries a reputation of having attacked government agencies and embassies of various countries in the past. In 2016, this group targeted an Indian government organization (name undisclosed) using spear phishing e-mails loaded with malicious Microsoft Office documents designed to exploit an old 'CVE-2010-3333' vulnerability. Although this vulnerability was patched by Microsoft long time back, it is still being used in many targeted attacks. When the victim opens this malicious document, it drops the main payload which is an executable file. The decoy document indicates that it is specially developed to target Indian government organizations. Once installed successfully, it collects system information, provides remote shell access to the attacker, monitors file activities, and has an ability to update itself.
- SWIFT (Society for Worldwide Interbank Financial Telecommunication) banking system was compromised by attackers in May 2016. SWIFT is an institution that interconnects banking system worldwide. Just after the SWIFT attack, Bangladesh's Central Bank was also compromised, resulting in a fraudulent monetary transaction.
- Attackers were found to be making use of available source codes on various code sharing platforms. The 'Bolek banking Trojan' was inherited from the leaked source code of Carberp and Zeus banking Trojan. It was then used to steal confidential information of the customers of a bank in Russia.
- In September 2016, the TrickBot bot family was observed. It is suspected to have been possibly developed by the authors of the famous Dyre banking malware. Launched early in its development phase, TrickBot improved itself and became fully operational from the first week of November 2016. The updated Trickbot malware is known to have employed some of the most revolutionary techniques, server-side injections, and redirection attacks. This bot has already targeted a few Australian and Canadian banks with its advanced techniques.
- In 2016, Quick Heal lab had also come across a targeted attack aimed at a private online marketing firm that caters to small businesses in the U.S. To make the attack look more legit, the attackers first gathered various details about the company from social networking sites and the company's website. This information was then used to craft content in macro-laced malicious Microsoft Office documents. These documents were then sent as an attachment in spear phishing emails to the employees of the company. When these documents were opened, the attackers were able to compromise the company's system and steal confidential business data.

## PUA and Adware

- In 2016, adware performed activities that were not limited to displaying pop-up ads on the user's computer. We had observed adware changing the DNS settings or acting as a proxy hijacker on compromised systems. Adware were also found to be making changes in the shortcut links of installed browsers and adding the argument of a proxy server. Furthermore, these software were designed to modify the host file or dropped text file at a particular location, containing a list of security domains. This list is maintained by an adware to block the user's access to any security software website.
- We have observed a behavior where an adware automatically installs an old version of web browsers and then disables their automatic updates.
- In 2016, some adware were found to steal information related to CPU, hard drives, network adapters, and other data about the victim's computer. This information was then uploaded to the developer server. By doing so, attackers can trigger ads on the victim's computer according to the system configuration and benefit from it.
- We observed that many freeware bundles such as Hohosearch and YesSearches come with browser hijacker inside them. When installed, they change browser settings and set their homepage. Additionally, they can redirect the victim to targeted advertisement pages and show pop-up ads on the browser.
- Adware were also observed to be using a different approach with pop-ups having audio advertisements, which when clicked perform browser hijacking. This technique is known as Browser Hijacking using 'File-in-the-Middle'.

### Tech Support Scams

Technical support scams are popular with fake error or fraud troubleshooting messages which ask a user to call on their fake toll-free numbers to fix the problem. In some cases, it has also been observed that the victim receives fraud calls from attackers pretending to be calling from Microsoft Corporation. The scammers trick the victim with fake error reports and charge them for fixing the problem.

In 2016, we had observed Microsoft tech support scams which use fake 'blue screen of death' and fake 'Windows Activation' scams, asking users to call on a toll-free number for help. By following these instructions, victims had to pay for non-existing problems.

### Ransomware

Ransomware remains a major and rapidly growing threat even in 2016. This year, many ransomware variants came up with new infection and propagation techniques. Many new ransomware families were discovered with improved encryption and anti-detection techniques.

**New ransomware observed in 2016:**

- Locky
- Cerber
- Cryptxxx
- Petya
- GoldenEye
- Hydracrypt
- LeChiffre
- CryptoHost
- JigsawLocker
- TrueCrypter
- Hades
- AlphaLocker
- CryptoMix
- CrypMIC

**Ransomware detected in 2015 and were active until May 2016:**

- Teslacrypt
- Troldesh

## The Troldesh (XTBL/Crysis) Ransomware

In 2016, we observed criminals spreading and executing the Troldesh/CrySiS ransomware by directly gaining access to the victim's computer through Remote Desktop. The decryption of files encrypted by this ransomware has been made possible thanks to the recent release of its master decryption keys. The Quick Heal Threat Research Labs developed a 'XTBL/CrySiS decryption tool' with the published keys. This tool comes for free and can be downloaded from our official blog here > http://bit.ly/2hmEgOW

But it wasn't long before two new variants of the CrySiS ransomware were spotted again towards the end of 2016. Like their predecessor, these variants were spreading through the same technique of Remote Desktop Protocol (RDP) brute forcing wherein, once the access is gained, criminals simply deactivate the system's defenses and run the payload. The new variant encrypts files and appends the '.Dharma' and '.Wallet' extension to the encrypted file. Decryption of these new variants is not possible as decryption keys are not available.

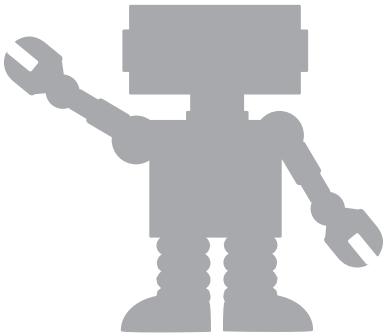
### The evolution of Locky ransomware

Locky Ransomware was first discovered in mid-February 2016. Spreading through compromised sites and spam campaigns, Locky used integration of symmetric and asymmetric ciphers to make it uncrackable till date. Since its emergence, Locky has kept updating itself with enhanced features with every new variant. These variants are as follows:

- **Locky Variant** completely disarranged the victim's filename to a 32 hexadecimal string followed by '.locky' extension. The encrypted files looked like '140E87B9982828DA30CF54705AB380B3.locky'. It changed the victim's desktop image showing recovery instructions and personal ID. It also added ransom notes showing the same on desktop and encrypted folder as '_Locky_recover_instructions.txt'.
- **Zepto Variant** appeared in August 2016 with a new '.zepto' extension replacing .locky in the renaming pattern. Similar to the earlier version, it scrambled file names to a hexadecimal string but with five blocks separated by hyphen and changing their extension to .zepto like '7CE1B2C7-F4E9-FEE1-4317-9A6FC4E6CBE3.zepto'.

- **Odin Variant** appeared in September 2016; it encrypted files to '.odin' extension. Recovery instructions were added with '_HOWDO_text.html' and '_WHAT_is.bmp'.
- **Shit Variant** that stayed for a short span was discovered towards the end of October 2016. Without many external modifications, this variant used '.shit' extensions for encrypted files. The ransom note was changed to '_WHAT_is.html' and '_WHAT_is.bmp'
- **Thor Variant** emerged just within 24 hours of the release of its older version (Shit). The word 'shit' had changed to the Norse mythological God's name 'THOR'. The only visible change made was the reformation of its extension from '.shit' to '.thor'.
- **Aesir Variant** used another mythological name 'Aesir' following its predecessor for encrypted files. The file names were now morphed to hexadecimal entities using pattern '[8_chars]-[4_chars]-[4_chars]-[4_chars]-[12_chars].aesir'. This variant added recovery information with following files '[random_No.]-INSTRUCTION.html', '[random_No.]-INSTRUCTION.html', and '[random_No.]-INSTRUCTION.bmp'.
- **ZZZZZ Variant** discovered in November 2016 had only one observable change in the extension added by it after encryption. Extension of encrypted files were changed to '.zzzzz'.
- **Osiris Variant** is an ongoing version of Locky with the Norse mythological God's theme. Encrypting files to a .osiris extension, this variant also changed file renaming pattern as a random, scrambled entry with hexadecimal characters separated by two hyphens, e.g., '[8_chars]--[4_chars]--[4_chars]--4_chars]--[12_chars].osiris'. Another visible change was observed in the ransom notes added to the folders of the encrypted files - 'OSIRIS-[4_chars].htm' and the 'OSIRIS.bmp' that get set to desktop image.

# TRENDS AND PREDICTIONS



1

### Targeted Attacks

Lack of security standards in Internet of Things (IoT) devices was brutally misused by the Mirai botnet. Linux Mirai botnet used these devices to carry out some of the largest DDoS attacks in 2016 resulting in some popular websites temporarily going out of service. More of such attacks are likely to occur where 'smart' IoT devices will be involved due to their lack of security.

Attachments in spam e-mails still remain a favorite infection vector to deliver malware to victims. Attackers will use new file types for their attachments to avoid detections by security software. Spam e-mails will appear more legitimate to trick unsuspecting users into opening malicious attachments. Use of Instant Messaging (IM) services to deliver malware is highly suspected to rise in the coming years.

2

### Adware

Advertisements using audio messages is a new technique observed in 2016 that attackers are using to target users. It is expected that this trend will continue in 2017 also. Adware with data stealing and destructive capabilities could be seen in the future.

3

### Ransomware

New ransomware families and their variants were discovered with improved encryption and anti-detection techniques in 2016. Ransomware will remain a major and rapidly growing threat even in 2017.

Cerber Ransomware variants will continue to update themselves with new encryption and anti-detection techniques. Due to its vast email campaigns and lack of decryption techniques, Locky was considered to be one of the most dangerous ransomware in 2016. We expect that the variants of this ransomware will keep rising in the coming year as well. File-encrypting ransomware that have data stealing capability are expected to occur in the future. Ransomware can also be embedded in video files, PDFs, and other formats, making it a prevailing threat.

Ransomware-as-a-service (RaaS) attacks may increase due to its user friendliness and its availability.

Use of e-wallets and online payment systems are increasing rapidly due to their ease of use and the Government promoting a cashless economy. Thus, financial gain and data theft will continue to be the motive behind most cyberattacks.

# ANDROID SAMPLES AND THEIR DETECTION STATISTICS

Several incidents of cyberattacks on popular mobile apps occurred in 2016 and mobile ransomware and banking Trojans have grown tremendously. Quick Heal Labs also observed growth in malware that are designed to root Android devices; some of these malware are known to persist in an infected device even after a factory reset.

Fig 1 represents the statistics of Android samples received by Quick Heal in 2016.

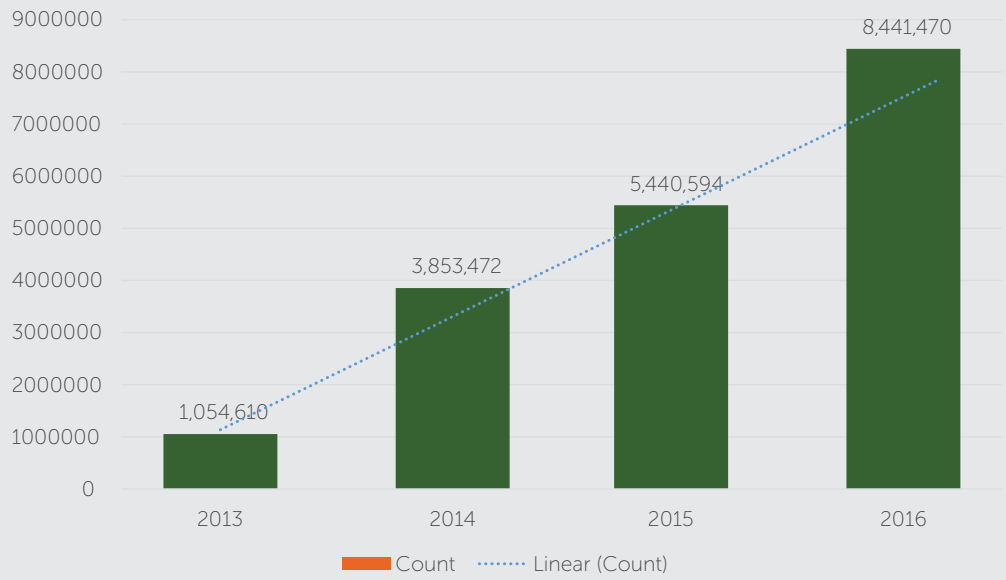
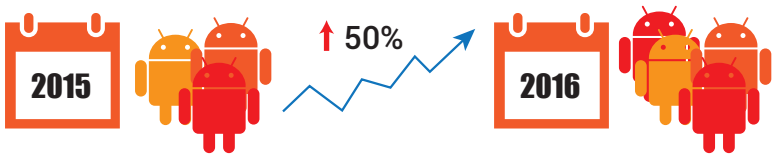


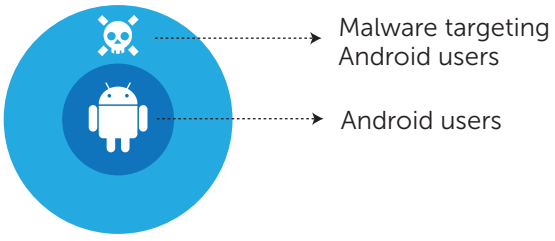

Fig 1

## Observations

- **50%** increase in Android samples detection count.




- With increased usage of Android devices, malware targeting them have also grown at an enormous rate.



## Android samples received by Quick Heal Threat Research Labs

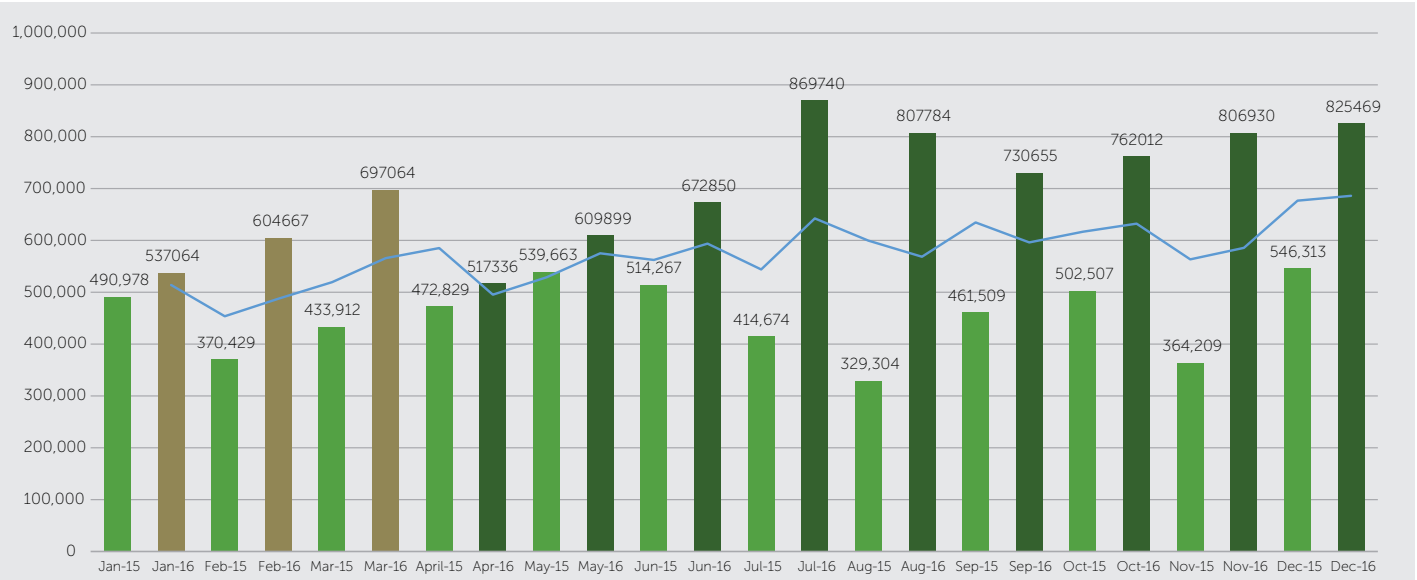
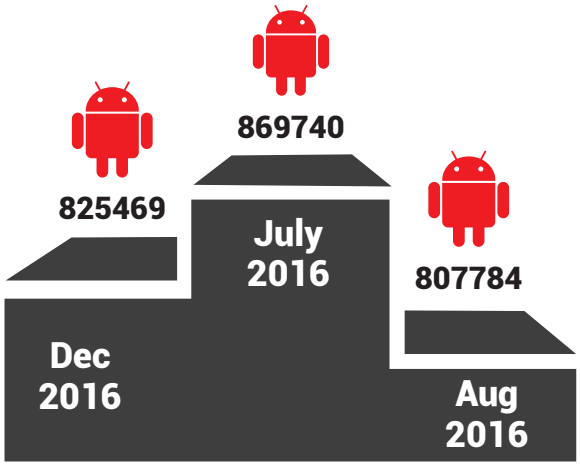



Fig 2

### Observations

- July 2016 recorded the highest detection count, followed by Dec 2016 and Aug 2016.



## Android category flow in 2016

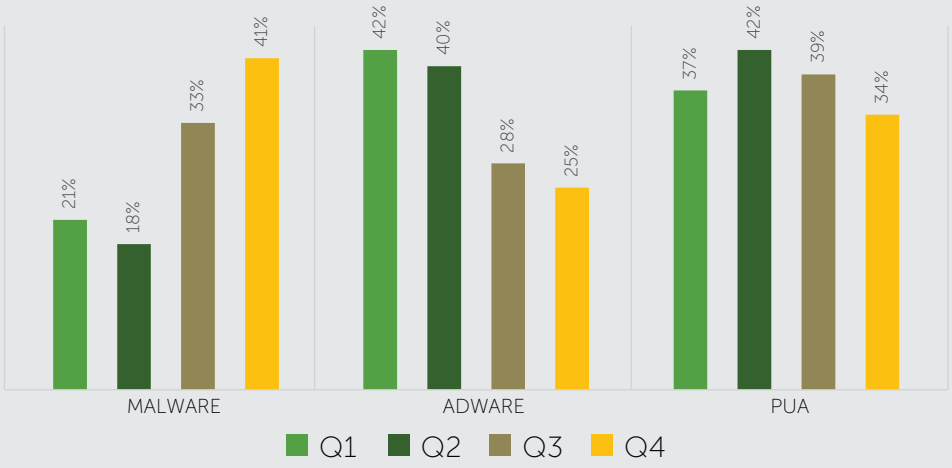



Fig 3 (a)

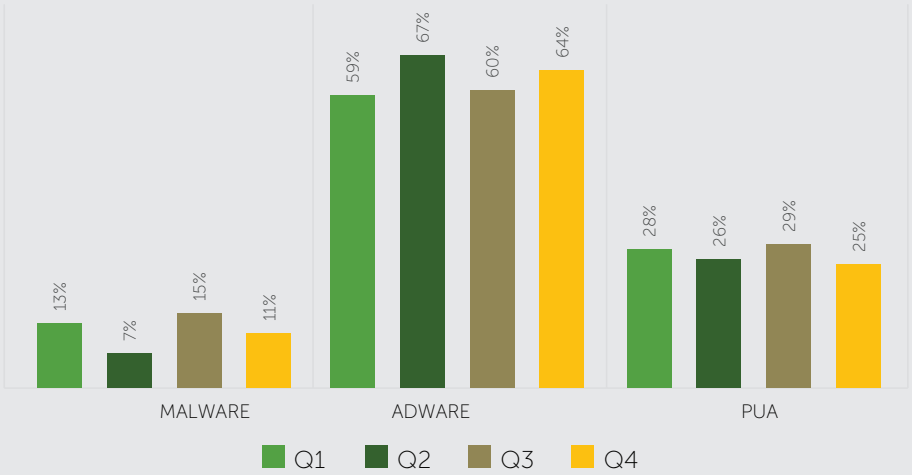
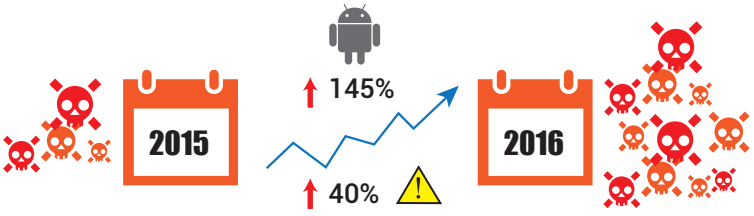



Fig 3 (b)

### Observations

- **145**% increase in malware detection count.
- **40**% increase in PUA detection count.



# TOP 10 ANDROID MALWARE

The top 10 Android malware detected by Quick Heal in 2016.

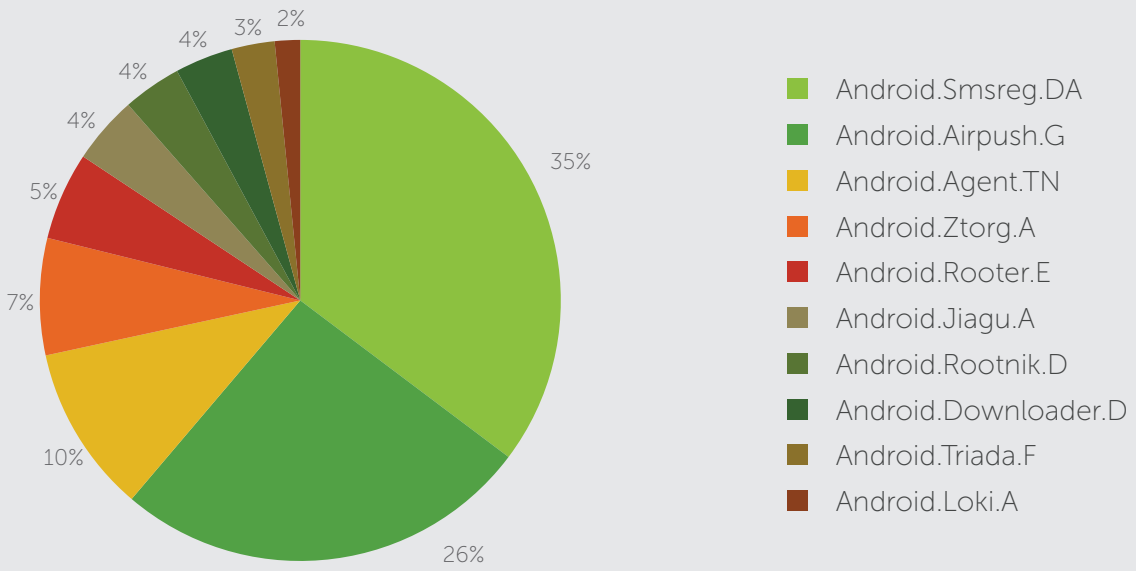



Fig 4

### 1. Android.Smsreg.DA

**Damage Level**: MEDIUM

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

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

**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, contact list, etc., and sends it to a remote server.

### 2. Android.Airpush.G

**Damage Level**: LOW

**Category**: Adware

**Method of Propagation**: Ad plugin

**Behavior**:

Upon gaining entry, it aggressively pushes ads to the notification bar of the infected device. It can also add a shortcut of these ads to the home screen. The adware can modify browser bookmarks in the compromised device and change the appearance of the home screen. It can also steal the following types of data:

- IMEI number
- Device location
- Device name, type, and OS version details

### 3. Android.Agent.TN

**Damage Level**: MEDIUM

**Category**: Malware

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

**Behavior**:

- Displays itself as an adult app and performs malicious activities in the background.
- Attempts to gain the infected device's admin rights.
- Sends device information to an external server.
- Requests for action from the adware component of another ad.
- On receiving certain information about how the user is interacting with the app (such as 'user present' and 'connectivity change'), the app stops itself.

### 4. Android.Ztorg.G

**Damage Level**: HIGH

**Category**: Malware

**Method of Propagation**: Repacked apps in third-party app stores

**Behavior**:

- Displays unwanted ads and downloads other malicious apps in the background. Even if it is removed, the app still appears on the device after a restart.
- Uses Java reflection to load other classes.
- Contains advertisement frameworks which are used to download and display ads.
- Downloads other files and installs them on the 'system/app' folder and remounts the whole system folder in write mode. The attacker can then write their code in the system folder and also gain root privileges.
- Downloads files in '/system/xbin/' which is UPX packed ARM binaries. It then accesses the root terminal and executes commands on the device.
- Downloads other malicious apps on the infected device without user consent.

### 5. Android.Rooter.E

**Damage Level**: HIGH

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

**Method of Propagation**: Google Play Store, Kingroot.net, and forum.xda-developers.com

**Behavior**:

- Displays unwanted ads.
- Checks whether superuser privileges are activated on the device. If not, it prompts the user for granting these privileges.
- Roots the infected phone with one click.
- Gathers device information such as IMEI, IMSI, etc.

### 6. Android.Jiagu.A

**Damage Level**: MEDIUM

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

**Method of Propagation**: Third-party app stores and protector plug-ins

**Behavior**:

- Such applications use the 'Jiagu' Android app protector. This protector is commonly used by developers to prevent their apps from being tampered or decompiled.
- This technique makes it difficult to run reverse engineering on the malicious app because it encrypts the dex file and saves it in native files.
- It releases the data into memory and decrypts it while runtime.
- Decrypted DEX file may be a malicious or a clean file.

### 7. Android.Rootnik.D

**Damage Level**: HIGH

**Category**: Malware

**Method of Propagation**: Repacked apps in third-party app stores

**Behavior**:

- This app is hard to get rid of; even after uninstalling it, it appears when the device is restarted.
- It installs other malicious apps without the user's permission.
- It contains encrypted malicious files.
- It decrypts the first 56 or 128 bytes of the file that are present in the asset.
- It carries the 'Ztorg' malware with it to perform further rooting activities.

### 8. Android.Downloader.D

**Damage Level**: MEDIUM

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

**Method of Propagation**: Google Play Store and third-party app stores

**Behavior**:

- Masks itself as a gaming app.
- Sends information about the infected device to a remote server.
- Automatically or on-click downloads other PUAs or adware.
- Installs additional malicious apps.

### 9. Android.Triada.F

**Damage Level**: HIGH

**Category**: Trojan

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

**Behavior**:

- Hides its icon and runs silently in the background.
- On execution, it asks the user to grant device admin permissions.
- Starts displaying a pop-up that prompts the user to download other apps. The prompt cannot be dismissed and it keeps showing up continuously on the mobile screen.
- In the background, it downloads and installs several other malicious apps.
- Records device information and sends it to a remote server.

### 10. Android.Loki.A

**Damage Level**: HIGH

**Category**: Trojan spyware

**Method of Propagation**: Forum.xda-developers.com and third-party app stores

**Behavior**:

- Uses the native library for carrying out its malicious activities.
- Incorporates itself into system processes and gains system privileges for carrying out malicious activities by taking root privileges.
- Can be used for creating and flashing a custom kernel.
- Can manage the lifecycle of any application (i.e., it can install, update, kill or uninstall apps) and can use any app based on the command received by the attacker.
- Can display ads.
- Also acts as a spyware; it steals information like IMEI, IMSI, etc., and sends it to the attacker.

# MOBILE RANSOMWARE AND BANKING TROJANS

Below are the detection statistics of mobile ransomware and mobile banking Trojan in 2016 (fig 5, 6, 7, 8).

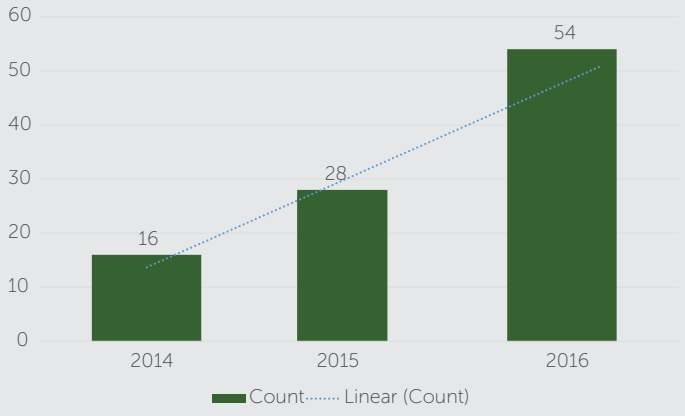



Fig 5

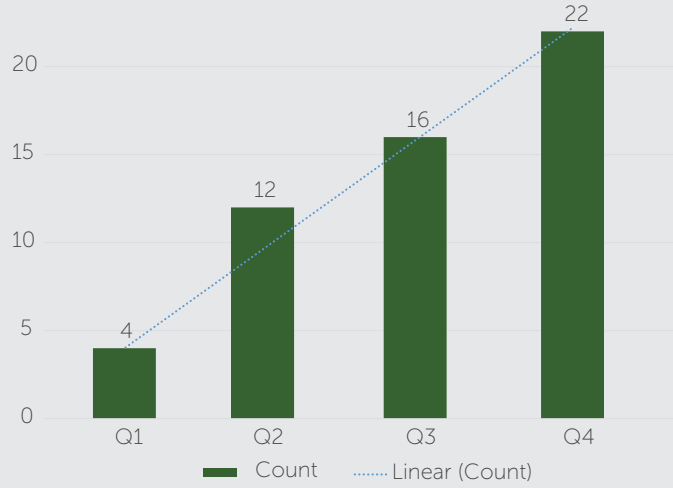



Fig 6

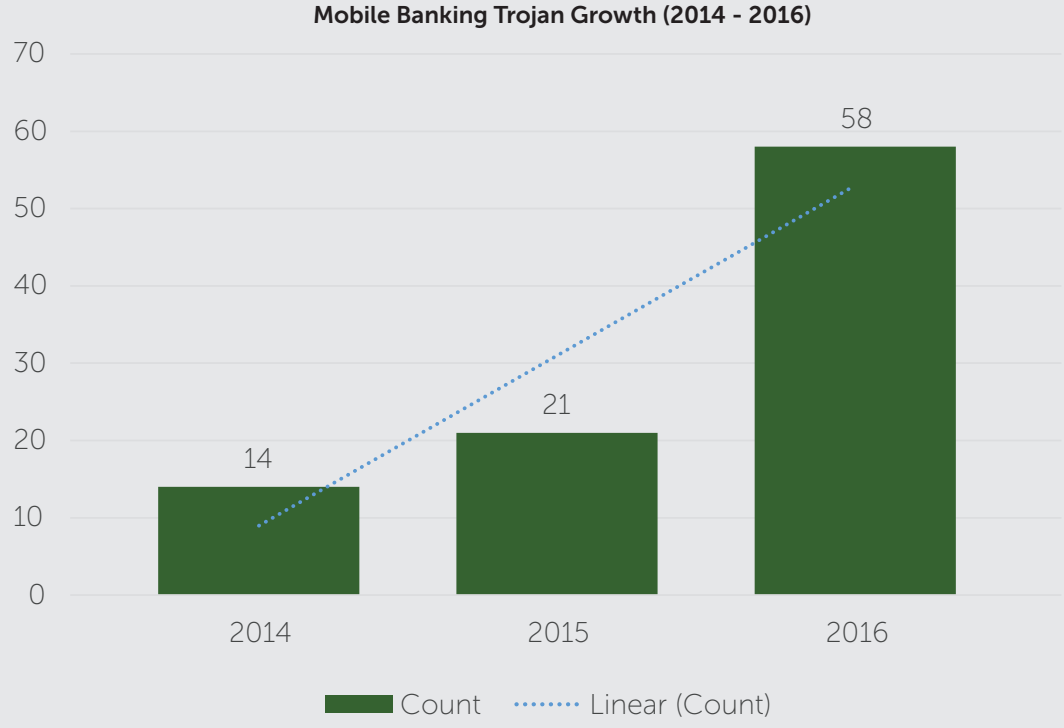



Fig 7

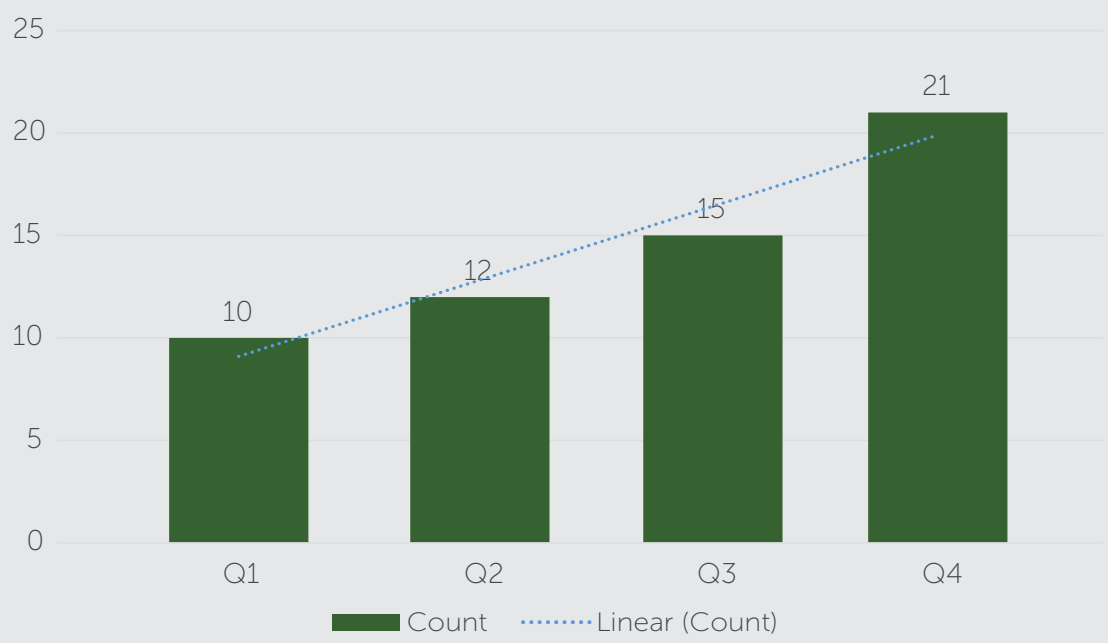
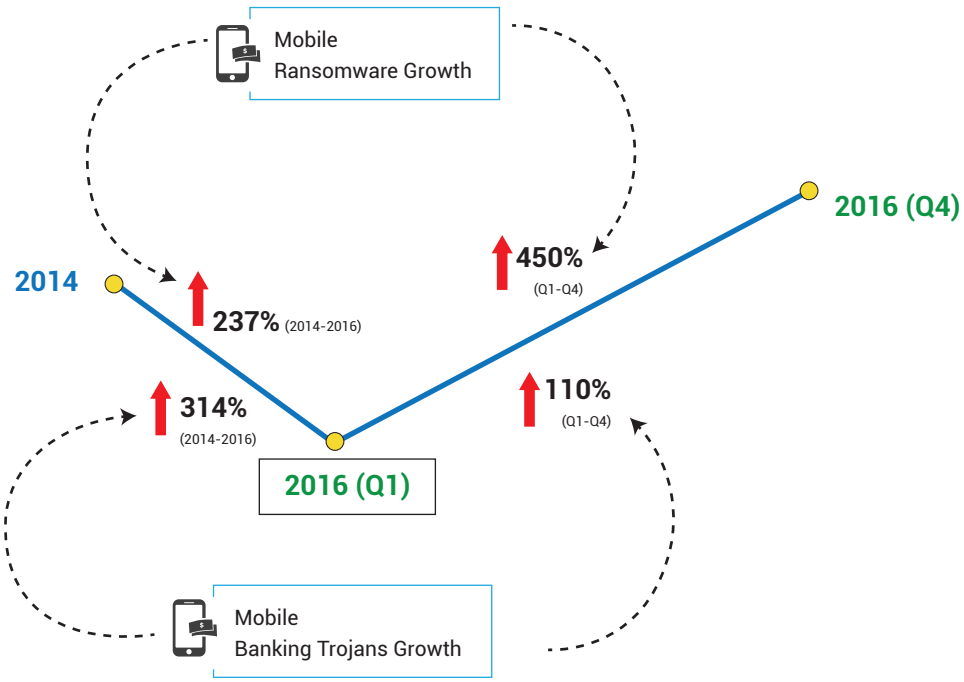



Fig 8

## Observations



# MALWARE USING UNIQUE TECHNIQUES

### 1. Android.Puxis.A

**Damage Level**: MEDIUM

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

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

**How is this malware unique?**

- This malware is built for auto rooting, language detection, and gaining remote access via TeamViewer. This helps the attacker read the TeamViewer ID which is displayed to the user on the device. The accessibility service reads this ID which allows the attacker to control the device remotely.
- Asks the user of the infected device to activate accessibility services for the malicious app.
- Tries to download and run a third-party rooting tool.
- Many banks in Austria, Hungary, Romania, and Switzerland have been targeted by this malware.

### 2. Android.Rittew.A

**Damage Level**: HIGH

**Category**: Trojan

**Method of Propagation**: Third-party app stores or download links in SMSs

**How is this malware unique?**

- It is a Twitter-controlled Android botnet.
- Once launched, it hides its icon and starts running in the background as a service.
- It contacts a particular Twitter account after regular intervals to get commands.
- Based on the commands received, it can download different malicious apps.
- To prevent detection at the network level, it uses encrypted messaging communication.
- It can also change the Twitter account dynamically so that it starts receiving commands from the new account.

### 3. Android.SilverPush.GEN9039

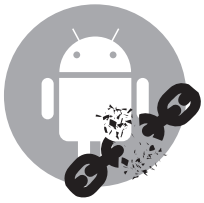
**Damage Level**: MEDIUM

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

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

**How is this malware unique?**

- SilverPush is a piece of software that can be included in third-party apps.
- It is designed to catch near-ultrasonic sounds from ads displayed on TVs, web browsers, or radios. These messages are picked up by the built-in microphone of smart devices.
- The malware also collects certain personal information like IMEI, OS version, location, and identity of the user.



# VULNERABILITIES AND ANDROID OS

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. Fig 9 shows how security vulnerabilities in the Android platform have grown from 2015 to 2016.

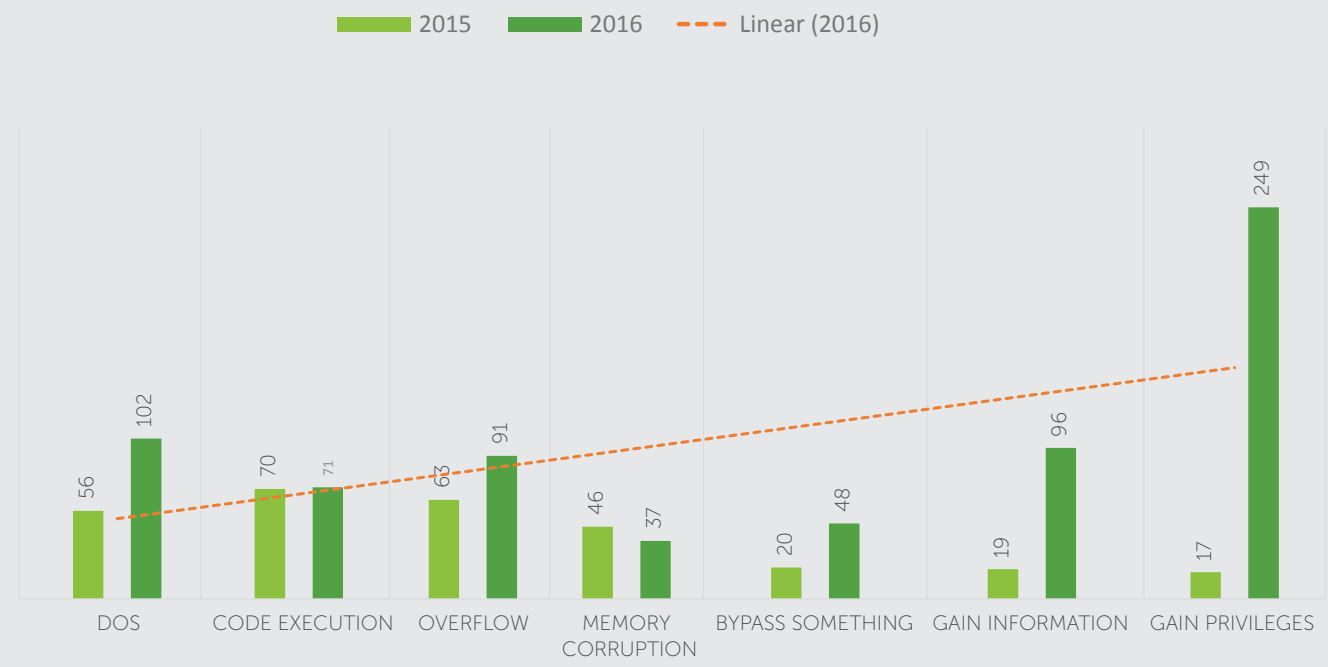


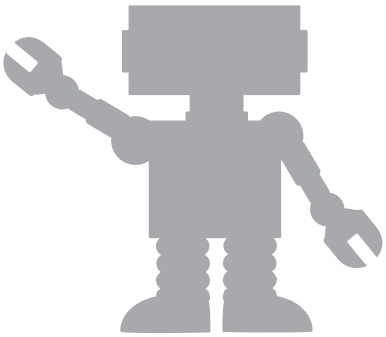

Fig 9

Source: http://www.cvedetails.com

## Observations

1. Security vulnerabilities misused by attackers to gain privileges on infected devices have the highest detection. Compared with 2015, it has shown a giant (≈1364%) increase.
2. Detections of almost all the vulnerability types have been higher in 2016 when compared with those in 2015.

# TRENDS AND PREDICTIONS



1

### Payment system and banking malware

Owing to increasing banking transactions over mobile devices, mobile payment mechanisms are under a constant threat. This is indicated by the growing number of sophisticated malware families that have been found to attack official apps of banks and other merchant sites from different countries. Banking malware threats in 2016 are up by 176.1% when compared with 2015. This is going to be a major concern for security experts and more for users of mobile Internet banking, in the near future.

### Mobile Ransomware

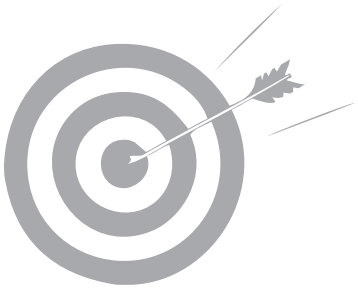
Ransomware has yet again retained its crown for being the most dangerous threat in 2016. And we have all reasons to believe that it will continue to do so in 2017. We expect new variants of mobile ransomware to crop up, most of which are likely to execute tricks that are commonly used by malware that target the Windows platform.

2

3

### Internet of Things (IoT) security is a concern

The data that is floating around the world through billions of IP network-connected IoT devices is converting into a digital environment of corporate enterprise networks and home consumers - a bigger, more lucrative and weaker target for attackers, thanks to their weak security. A far bigger problem lies with enterprises that lack skills, complex architectures, weak security features, and operational immaturity. All these just paint a scary picture where attackers will leave no opportunity in targeting every type of IoT device.



# CONCLUSION

The difference between our real life and our digital selves gets blurred with every passing day. We are gradually getting enveloped by a digital ecosystem - where devices connected to the Internet exchange our personal data to bring us the comfort of services such as online shopping and banking, entertainment, learning, and even air conditioning. The Internet is exploding into several digital fragments and we are getting attached to these fragments while ignoring the fact that we are being watched! Cybercriminals have increased their attack perimeter to trap every kind of user who is connected to the Internet. Ransomware - the most dangerous malware of the present time, began its journey by locking computer screens. But now, it has germinated into a full-blown business where it abducts data and demands ransom in exchange. What's worse, ransomware is being sold as a service creating a whole new monster to deal with. Data still remains the most precious prize for cybercriminals - steal it, sell it, and make money out of it. In a time where technology and the Internet are becoming one, we must embrace ourselves for the best and worst that this union will bring to us. We can guess the best, but can we guess the worst? The more we educate ourselves about digital security hygiene, the different digital threats we are surrounded by, the steps we must take and defense we must fortify ourselves with, the more prepared we will stand against the brewing storm called the battle of cybersecurity.