Quick Heal

Security Simplified

Annual
Threat Report 2016

www.quickheal.com

EXECUTIVE SUMMARY

The Annual Threat Report 2016 highlights the extremely critical aspects related to the security of Windows and Android devices. The Report gives an insight into the top 10 Windows malware of 2015, detection statistics of various malware categories, top adware and exploits, major Windows malware and important trends that concern them. The Report also elaborates Quick Heal's detection stats of Android malware, top 10 Android malware, mobile ransomware and important trends and predictions affecting the Android OS in 2015. Besides addressing the security aspects of Windows and Android devices, the report comprehensively looks into the growing threat of mobile banking Trojan, most popular mobile malware of 2015 and malware affecting the iOS platform amongst others.

TABLE OF CONTENTS

INTRODUCTION

In the world of cyber security, every year happens to be more eventful than its predecessor; a fact that is excellently vouched by 2015. The past year stands witness to so many cyberattacks, that it simply cements the saying "No one is immune to hacking". From the infamous Ashley Madison Data Breach, the Sony Pictures Hack and the LastPass hack, to the hack of the Harvard University, 2015 has seen it all. And these incidents happen to be just the tip of an iceberg, and paint a scary picture of the growing number of malware, hackers, and cyber espionage campaigns.

In 2015, Quick Heal detected about 1.4 billion malware samples affecting the Windows platform. In case of Android, the detection amounted to 803 new malware families and 757 new variants of existing families. The various methods of propagation for Windows malware seem to be email attachments, infected websites, removable drives, and bundled software. Trojan dominated the year as the most detected malware, followed by Infector and Worms including other malware families. For Android, adware remains the most potent threat. The common vectors of Android malware include ad plug-ins, third party stores, in-app purchases, Trojanized apps, fake apps, and protector plug-ins.

Windows malware detection statistics

Figure (1) represents the statistics of the total malware samples detected by Quick Heal on the Windows platform over the last 4 Quarters of 2015, at its customers' end.

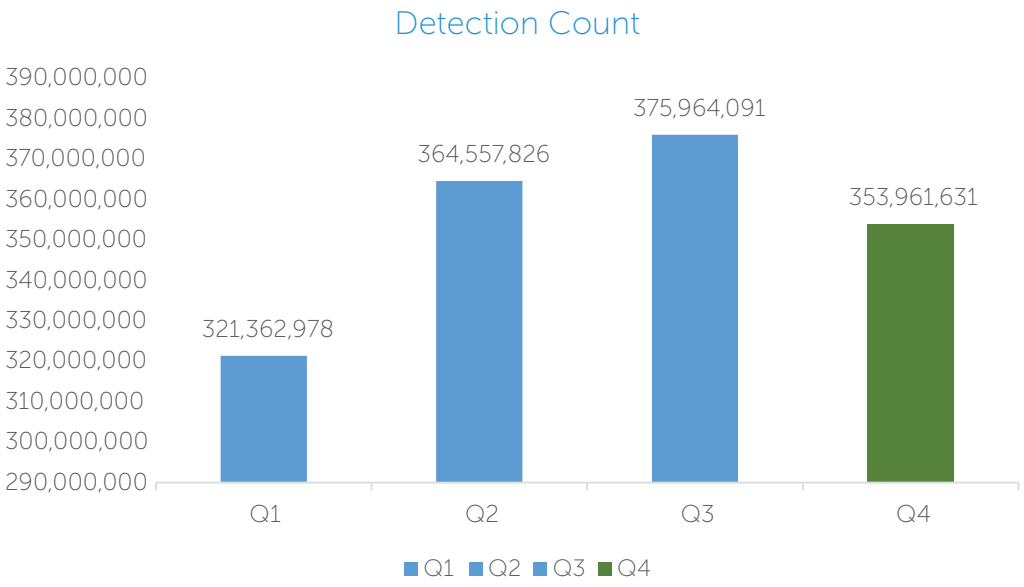

Figure (1)

Top 10 Windows malware

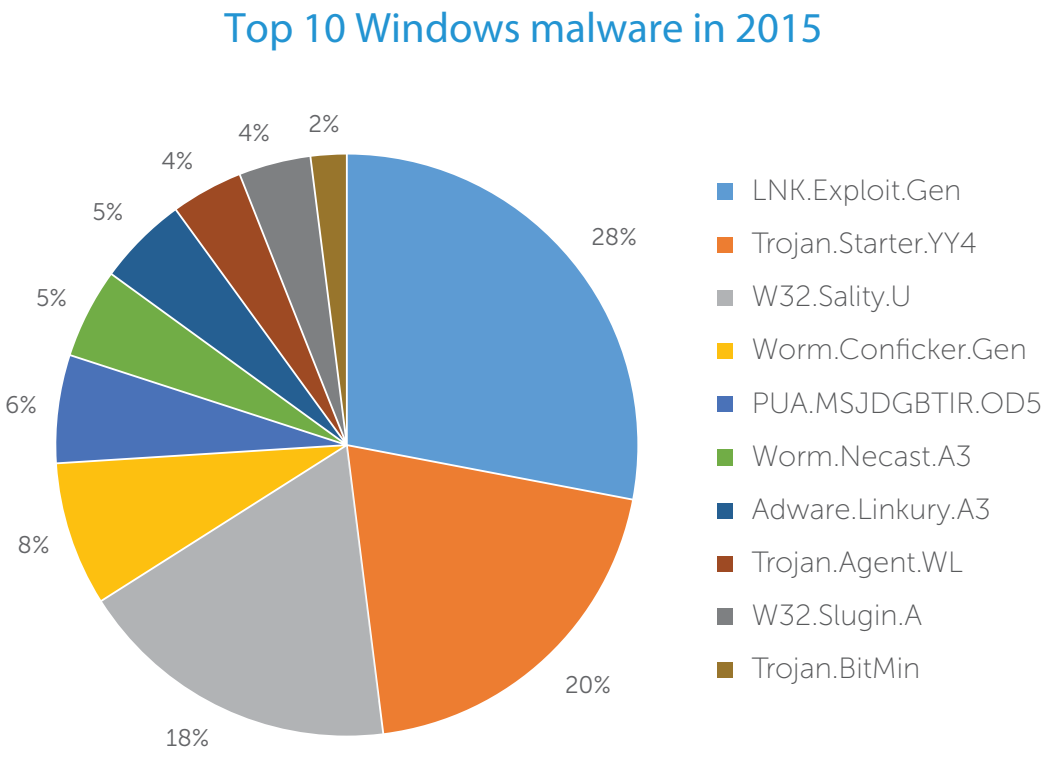

Figure (2)

Top 10 Windows malware

LNK.Exploit.Gen

Damage Level: Medium

Method of Propagation: Removable or network drives

Summary: LNK.Exploit.Gen enables an attacker to gain unauthorized remote access to the infected computer. The attacker can use a backdoor to spy on the targeted user, manage files, install additional software or threats, shutdown or reboot a computer, or attack other machines in the network.

Behavior Post Infection: An exploit is a piece of software or a sequence of commands that take advantage of a bug or vulnerability in a software or system in order to cause unintended or unanticipated behavior to a computer. LNK.Exploit.Gen targets Windows vulnerability that allows malicious shortcuts to run themselves whenever the shortcut folder is viewed in Windows Explorer. It can compromise your system and introduce additional infections such as rogue software. It may redirect you to unsafe websites and untrusted advertisements which will further slowdown the infected system.

Trojan.Starter.YY4

Damage Level: High

Method of Propagation: Email attachments and malicious websites

Summary: Trojan.Starter.YY4 is designed to connect to a remote server and install other malware on the victim's computer. This malware is used as an entry point module by other malware. It is linked to various banking Trojans and worms designed to spread over networks.

Behavior Post Infection: Trojan.Starter.YY4 creates a process to run the dropped executable file. It will modify computer registry settings which may result in system crash. It may download other malware like keyloggers. A system infected with Trojan.Starter.YY4 may take longer time to boot and shut down. Hackers may steal confidential data like credit card details and personal information from the infected system.

W32.Sality.U

Damage Level: Medium

Method of Propagation: Removable or network drives

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

Top 10 Windows malware

Behavior Post Infection: The malware injects its code into all running system processes. It then spreads further by infecting the executable files on local, removable, and remote shared drives. It also tries to terminate security applications and delete files related to security software. The malware has an additional capability of stealing sensitive information from infected systems.

Worm.Conficker.Gen

Damage Level: High

Method of Propagation: Removable or network drives

Summary: Worm.Conficker.Gen replicates itself to the Windows system folder. It may spread through removable drives and file sharing.

Behavior Post Infection: Without any human interaction, the worm can infect systems and can spread to other systems in the network automatically. It allows remote code execution when file sharing is enabled on your system. Conficker has the ability to disable several important system services and security software. It can also download and execute different malware on the targeted system. Victims may face issues while visiting websites related to security vendors and services that assist in the removal of this worm.

PUA.BrowseFox.PB5

Damage Level: Low

Method of Propagation: Bundled software and malicious websites

Summary: PUA.BrowseFox.PB5 comes bundled with free software. It hijacks web browsers, and after installation it downloads additional malware on the infected system.

Behavior Post Infection: The malware shows random pop-up ads and messages including discount coupons, deals, sales and offers when the targeted user is visiting online shopping portals and other similar websites. When the user selects to download & install a free application, it may carry extra toolbars, browser plug-ins and add-ons in the installation package. These extra tools may be marked as optional software, however if the user does not deselect a check box, it may do undesired system changes. It tracks the user's browsing activity and the collected information is used for targeted marketing.

Top 10 Windows malware

Worm.Necast.A3

Damage Level: Medium

Method of Propagation: Spam emails and malicious websites

Summary: Worm.Necast.A3 is a type of malware that runs as a self-contained program. It breaches the system via spam emails or when a user visits websites loaded with exploits. It also comes bundled with freeware.

Behavior Post Infection: Worm.Necast.A3 does not require to attach itself to the host program in order to perform its operation. It simply takes advantage of network connections in order to reproduce copies of itself and propagate parts of itself onto other systems. Its delivery mechanism is primarily the Internet and spam emails. It also uses the latest programming language and technology, and is endowed with changeable characteristics to evade detection and removal by antivirus software. The worm utilizes advanced Java, Active X and VB Script techniques to propagate its components onto HTML pages. It is also known to exploit system vulnerabilities so that it can then drop and install additional threats such as Trojans, keyloggers, fake antivirus programs and even ransomware. Remote hackers can utilize the infected system's loopholes to access the compromised machine without the user's knowledge and consent.

Adware.Linkury.A3

Damage Level: Medium

Method of Propagation: Bundled software

Summary: Adware.Linkury.A3 is an adware program that comes in the form of a browser add-on; for instance, as part of a CD Burning software installer.

Behavior Post Infection: The adware gains access to the user's search details, visited websites and cookies. It shows advertisements that the user finds attractive and also redirects them to malicious websites. Continuous pop-up ads utilize more system resources which degrades overall system performance.

Trojan.Agent.wl

Damage Level: High

Method of Propagation: Spam emails, removable or network drives

Summary: Trojan.Agent.wl propagates via spam emails, removal

Top 10 Windows malware

drives, and unprotected files sharing networks.

Behavior Post Infection: The Trojan can download other malware and third party software on the infected machine. It makes changes to the registry to hide its presence. Trojan.Agent.wl is designed to steal confidential information such as stored email and ftp login details, passwords, credit card details, bank account information, etc.

W32.Slugin.A

Damage Level: High

Method of Propagation: Spam emails, removable or network drives

Summary: W32.Slugin.A is a file infector that spreads through networks, removable drives and also via infected email attachments.

Behavior Post Infection: W32.Slugin.A loads during startup and spreads through emails and infected files. The virus searches for files having the '.exe' extension, on fixed and removal drives attached to the system. It also contains a backdoor component that can be remotely controlled by the attacker. It performs malicious actions such as changing system settings and redirecting the browser to malicious websites. It may remain unnoticed to the infected user for a long time.

Trojan.BitMin

Damage Level: High

Method of Propagation: Malicious websites and removable drives

Summary: Trojan.BitMin is distributed through infected webpages, social networking sites and removable drives. It is a potentially unwanted application that uses the victim's computer resources to generate bitcoin blocks. Attackers are using systems with powerful GPUs to mine bitcoins for making money.

Method: Bitcoins is a virtual currency. Users with high-end graphics card and Internet access can generate bitcoins and then sell the coins in exchange for hard currency. Visiting unsafe websites and downloading programs from them may result in the Trojan.BitMin infection. Sometimes, it freezes the system as the CPU gets tied up to the bitcoin mining process.t

Windows malware categories

Figure (3) represents the statistics for malware categories and detection percentage on the Windows platform in 2015.

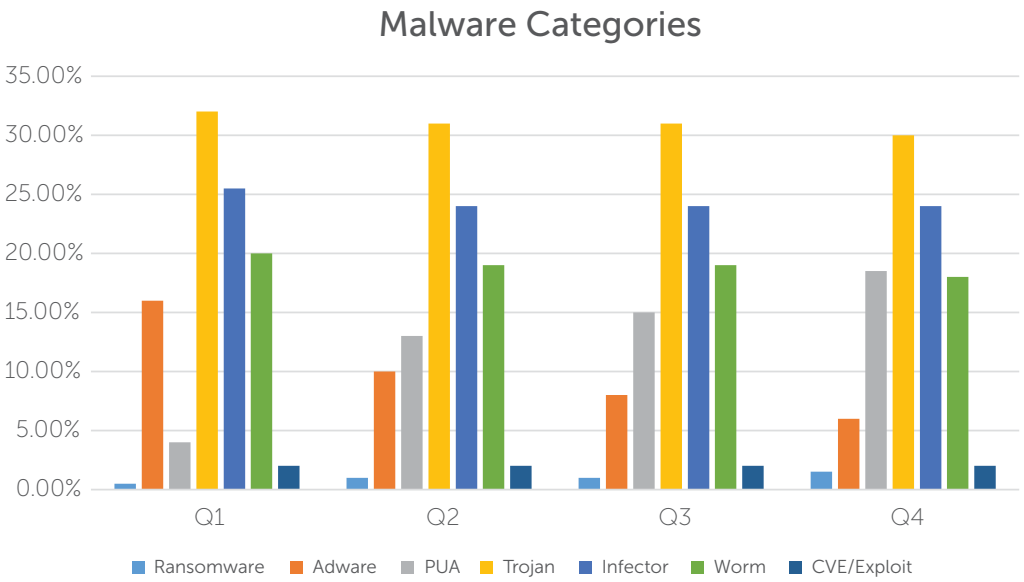

Figure (3)

Analysis:

It is interesting to see that the Trojan (31%), Worm (19%), Infector (24%) and Exploits (2%) categories have constant contributions to the detection stats. More importantly, Ransomware has shown a staggering 300% growth from 0.5 % to 1.5 % over the last year. Although, adware detection has dropped from 16% to 6%, the gap has been compensated by PUAs, whose growth has risen from 4% to 18.5%. PUAs are becoming more troublesome for customers and has been a prominent malware category over the last year.

Top 10 PUA and Adware

Figure (4) represents the statistics for the Potential Unwanted Programs (PUA) and Adware detected on the Windows platform in 2015.

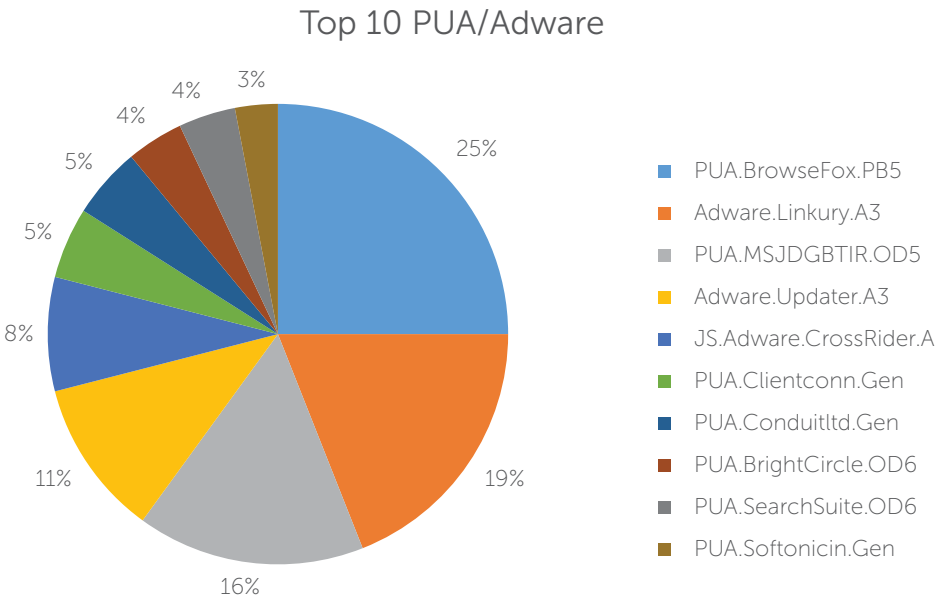

Figure (4)

Top 10 exploits

Figure (5) represents the statistics of Exploits detected on the Windows platform in 2015. Most of the prominent exploits date back to CVE discovered in 2012 or 2014. It shows a gap of users not applying patches to their Operating System, Internet browsers, Microsoft Office, Adobe, and Java.

It is observed that 43% of Quick Heal users are still using Windows XP, followed by Windows 7 - contributing 45%. Such a slow transition to the latest and more secured Operating System and laid-back application of security patches keep users vulnerable to attacks.

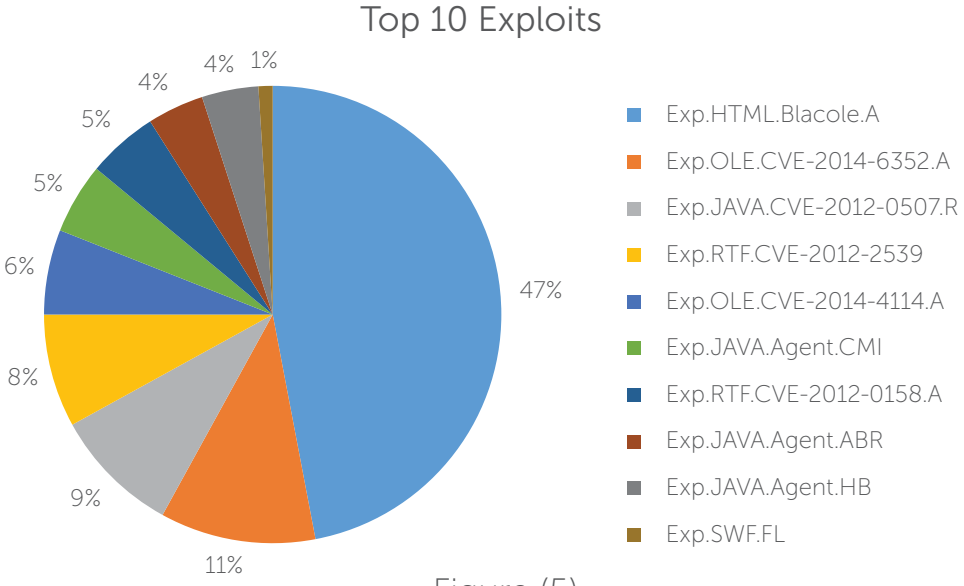

Figure (5)

Major Windows malware

Ransomware - evaluating encryption and ransom demanding tactics

Ransomware continued its dominance as the most destructing malware in 2015 as well. Ransomware is a category of malware that hijacks a user's system or encrypts its important files and demands a ransom to unlock the system or release the encrypted files. Many new ransomware families have been discovered to be armed with improved encryption and anti-detection techniques. In mid-2015, the discovery of "Ransomware as a Service" or RaaS shows another evolution. This has commoditized the creation of ransomware and allowed attackers to develop customized ransomware and distribute them.

Chimera brings ransomware and data extortion techniques

Attackers are continuously looking for new tricks to frighten victims into paying up the ransom. Chimera is one of such crypto-ransomware malware that was discovered at the end of 2015. Chimera is armed with three disturbing capabilities - Encrypting files, Data breaching, and Demanding extortion. After encrypting files, if the ransom is not paid, attackers claim to make those files public over the Internet. And this trick, in most cases, subdues the victim into paying up the ransom 'despite having a data backup.' A chimera attack is usually carried out by sending job-related fake emails to the employees of the targeted organization. These emails contain a link to a DropBox file, claiming that the file contains more information about the job. Once the victim downloads and executes the file from Dropbox, the malware springs into action and starts encrypting the data present on the local system.

CryptoWall and TeslaCrypt, the consistent performers

CryptoWall remained as a profit-maker to attackers by continuously delivering its new variants. CryptoWall 3.0 attacks users via spam emails containing JavaScript attachments. It is also to known to have used Google Drive in one of its campaigns for delivering malware and encrypting user's files. This malware focuses mainly on making its detection difficult to trace by security software.

CryptoWall 4.0 was released with the capability of encrypting a filename along with its data. The Angler Exploit Kit was used to

deliver this malware.

TeslaCrypt is another ransomware that came with different variants like AlphaCrypt, TeslaCrypt 2.0, and TeslaCrypt 2.1. After encryption, it appends different extensions like .ecc, .ezz, .exx, .zzz, .abc, .ccc, .vvv.

Some prominent and new ransomware observed in 2015:

- Troldesh
- Breaking_bad
- TrojanRansom.Xorist
- Ransom.Criakl
- Ransom.Denisca
- CryptoFortress
- Pacman
- Encryptor Raas
- ORX Locker
- CryptInfinite or DecryptorMax

Some of the ransomware families that continued to wreak havoc in 2015:

- Reveton
- Ransom.Terrac
- CTB-Locker

PUA and adware acting in system without your permission

PUA and adware remain the rising malware categories in 2015 as well. These are malicious or unwanted software which show unwanted advertisements. There are many publishers who provide custom toolbars, free applications, software bundlers or downloaders from websites other than the product publisher's website. Attackers make use of these services to reach the users' system by bundling unwanted or harmful software. During installation, some software have such bundled applications selected by default. Installing software packages with default options allows the installer to download other unwanted programs. This puts the user's system at more risk.

BrowseFox is one of such PUAs that tops the list in last year's detections. It breaches the system bundled with other free software. It can hijack web browsers or download additional malware into the system. It tracks the user's browsing activity and the collected information is used for targeted marketing.

The SearchProtect adware changes the user's default search engine to Bing.com and browser's home page to Trovisearch.com. It shows ads about software saying that they are highly recommended, and downloads from the site cdn.downloaddabs.com, which is blacklisted.

Adware that we came across in 2015:

- BrowseFox
- Linkury
- Updater
- CrossRider
- Clientconn

Exploit: Adobe Flash Player most targeted for discovering vulnerabilities

Exploit kit is a tool for exploiting security holes or vulnerabilities in particular applications. Successful exploitation can cause attackers to download malicious content on the victim's system and execute them. Internet browsers, Java, Adobe Flash Player, Adobe Acrobat Reader, etc., are known to be some of the favorite applications attackers exploit. In 2015, attackers were found to be more focused on targeting Adobe Flash Player vulnerabilities. Hacking Team Leak exploiting Adobe Flash Player was one of the serious threats that occurred this year. CVE-2015-5119, CVE-2015-5122, and CVE-2015-7645 are some of the major vulnerabilities identified in Adobe Flash Player for Windows, Mac and Linux. These exploit kits allow attackers to take control of the infected systems.

Attackers made use of the CVE-2015-7645 vulnerability in 'Operation Pawn Storm' which was spread via malicious emails containing URLs leading to the exploit. The recently occurred Malvertising campaigns in 'DailyMotion Pictures' and 'The Independence News' were also found to be exploiting the same vulnerability. Exploitation in the 'DailyMotion Malveretising Campaign' delivered Bedep and other info-stealing malware. Whereas, exploitation in 'The Independence Malveretising Campaign' was found to be delivering TeslaCrypt 2.2.0, the crypto-ransomware malware.

Major Windows malware

Banking malware trying everything to remain undetected

In 2015, banking malware families were found to be one of the major concerns for both users as well as security vendors. Attacks were carried out using sophisticated anti-detection, and long-term persistence. Two of the famous banking malware - Dyre and Dridex were found to be largely contributing to the banking malware family. Upatre downloader has been used as a carrier to deliver the Dyre malware into the infected systems. The payload was found hosted on compromised routers to avoid takedown of C2 servers. Later, the Upatre downloader employed secure SSL connections to deliver Dyre into the system and the same secure connection was used by the downloaded Dyre malware to send stolen credential data to its servers. Another Upatre variant has been discovered in the wild possessing a polymorphic nature. One of the variants of Dyre has been found affecting Windows 10, targeting the Edge web browser.

Dridex was spotted spreading in the wild with the help of a Digital Certificate campaign. Dridex infection is carried out via malicious spam emails containing macro-based Microsoft Word Documents. Once opened, the document instructs the user to enable the macro setting, and doing so drops Dridex into the victim's system.

PJSC BIZNES AVTOMATYKA, Private Person Parobii Yuri Romanovich, AVTOZVIT Scientific Production Private Company, etc., are some of the Digital Certificates used in the campaign to evade detection by security software.

Bartalex, Rovnix, and Vawtrack are some of the other banking Trojans that use macros in Microsoft Office documents for their propagation.

APTs focus more on tactics than techniques

As predicted, Advanced Persistent Threats or APTs maintained their dominance in the year 2015. APT campaigns are seen to be highly focused on bypassing various security checks and remaining persistent in the infected system for a longer duration of time. Their main objective is to steal data instead of causing damage to the network or the attacked organization.

Major Windows malware

The 'Dark Hotel APT' campaign is one of such attacks wherein attackers used '.hta files' as an infection vector. '.hta file' is used by developers to take the features of HTML together with the advantages of scripting languages like JScript or VBScript. Attackers used this file for hiding malicious JS code.

The 'TVSPY APT' campaign made use of a vulnerability in the TeamViewer application. The first incidence of using such attacks was last seen in 2012 and it continued in 2015 with its new variants.

Another interesting campaign was carried out by the Gaza Cyber-gang. In this campaign, malware files were sent to IT and IR (Incident Response) staffs with a motive to gain access to higher level of information. Files were dropped to the staff's mailbox via spear-phishing emails, with job-related fake subject lines.

Sophistication in using Anti-Sandbox, Anti-VM techniques is on the rise in APT families which makes it difficult for security software to detect them.

The Advanced Persistent Threat Annual Report 2015 published by Quick Heal highlights some of the major APT samples detected by the Quick Heal Threat Research and Response team in 2015. These attacks were analyzed based on their threat level, propagation, behavior post infection, detection statistics, common tactics used by attackers, and C&C (command and control) servers-related information. The analysis revealed that a majority of the targeted companies are from Government, Finance, Infrastructure, and Defense organizations. It is also indicated that the most common entry for these attacks are emails and malicious attachments, propagated using spear phishing and social engineering techniques. The same concludes that zero-day threats and security vulnerabilities in the most popular software programs such as Microsoft Office, Adobe Flash, Java and others are the primary entry points for APTs. Further, browser-based exploits are also becoming more prevalent and common for deploying APTs into networks.

Upcoming trends for Windows malware

Ransomware

Ransomware will continue to be a challenge in 2016 for security experts. Attackers are continuously evolving their mechanism to make money. Rise in the use of Ransomware as a Service (RaaS) can easily swell the malware's growth. Hence, more customized ransomware can be expected to be seen in the coming year. Attackers have shown this approach by targeting staff in organization with malware. Targeted ransomware attacks could be a new phenomenon expected in the coming years. Financial sectors like Banking, Stock Market, etc., can be the most vulnerable and lucrative targets. There may be a rise in file-encrypting ransomware with data-theft capability. There can be a rise in ransom-extortion cases in which victims will be warned by attackers to pay the ransom or risk their files go public. More ransomware for iOS platforms and IoT devices could be expected as these are becoming more popular among users. CryptoWall and TeslaCrypt variants will continue to sophisticate themselves with new encryption and anti-detection techniques.

Exploits

Adobe Flash-based exploits have been one of the favorite tools for attackers this year. However, security updates released by Adobe on 8th December 2015, covering a staggering 79 vulnerabilities, including an entire range of user-after-free, security bypass, stack based, memory and heap corruption vulnerabilities are expected to mark down the exploitations.

Unpatched systems with vulnerable Java, PDF, and MS-Office-related exploit attacks will remain as they are in 2016 with new critical vulnerabilities in the high-risk zone. It's interesting to see how attackers approach Microsoft's Edge Browser, as its descendant, Internet Explorer, was one of their favorite targets. Edge's new features like Garbage Collector can be a difficult but viable target for attackers.

Exploits related to the Internet of Things (IoT) will be another trend, mainly due to the sheer lack of attention paid to the security features in these devices.

Upcoming trends for Windows malware

PUA and Adware

2015 depicted that PUA and adware growth is still a current trend in the threat landscape and it is expected to remain so in 2016. Use of the Internet is constantly increasing and this is opening more avenues for cyber crooks to hit their targets with more sophistication. PUA and adware can be used by attackers to silently deliver other malware, get remote administration and introduce hacking tools into the user's system without their knowledge.

Websites built using WordPress are continuously under attack for malvertising. DailyMotion and The Independence attacks demonstrated just how malvertising campaigns are effective. In 2016, more of such campaigns are expected to come through.

Attacks on E-Cash Wallets

Users are getting used to online transactions because of its simplicity and time-saving characteristic. One only needs to have sufficient e-cash in their payment cards like Credit Card or E-Cash Wallets. E-Cash Wallet is a growing trend in the market in which a third party stores financial information like card type, card number, expiry date, etc., to perform transactions conveniently. When a user initiates a payment next time, the payment system asks only for the user's 3 digit CVV number, and all other data is processed automatically. With such third party payment systems on the rise, attacks on its servers could be a dangerous financial threat in the coming days. As credentials have a significant role to play in online payment system, 'Steal and Sell Attacks' against them can also be seen in the future.

Internet of Things

Advancement in technology is spawning multiple intelligent and smart devices. However, sometimes security is not considered as a priority during the creation of these devices. This leaves many features vulnerable to attackers. Internet of Things (IoT) is a mass collection of physical devices connected over the Internet to exchange data, ranging from automobile vehicles to wireless wearable products.

Upcoming trends for Windows malware

Recent incidents like car hacks, baby monitor vulnerabilities, DNS changer malware attack on network router, etc., are some glaring indications of the emerging IoT threats. With routers, it is observed that most of these devices have a known admin password by default or vulnerabilities that are used to achieve remote access to compromise the system for malicious purposes. The Upatre malware family was found to be using compromised routers as C2 servers to host payload components.

In the future, smart devices including TV, refrigerators, cars, drones, smart cameras and wearables like smart watches, etc., are being seen as common targets for hackers and malware.

Android malware collection stats

Quick Heal Threat Research Labs detected 803 new malware families and 757 new variants affecting the Android platform, in 2015. This accounts to a rise of 49.8% (new malware families) and 22.8% (new variants) when compared to 2014.

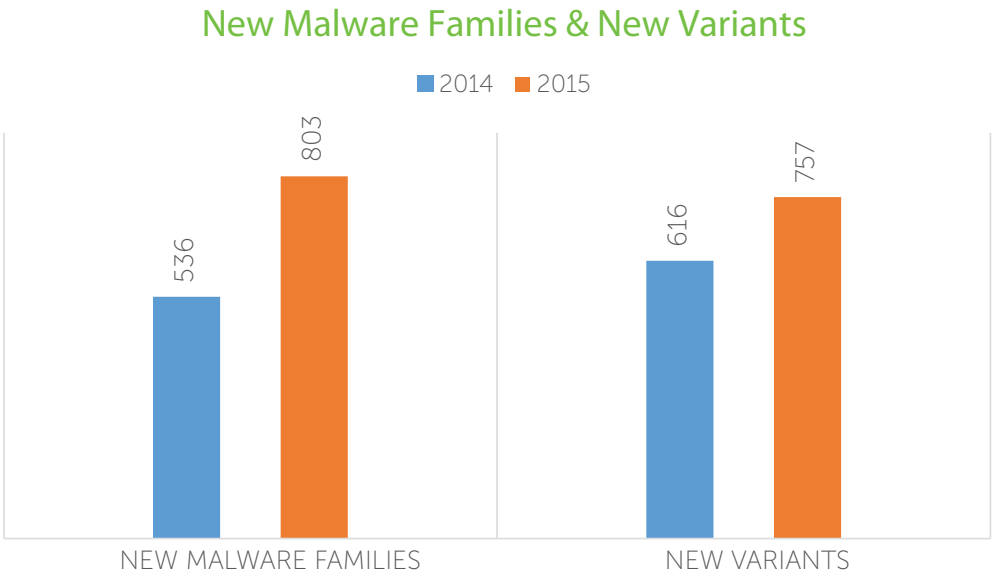

Figure (6)

As exhibited by the following figure (7), both new variants of existing malware families and new families have shown a significant rise in their growth. This is followed by figure (8) highlighting the malware samples received by Quick Heal in 2015. Even here, there has been a staggering rise accounting to more than 5.4 lakh samples. Figure (9) presents a breakdown of Adware, Potentially Unwanted Applications (PUAs) and other malware. Maintaining its undisputed position as the top detected malware, Adware still remains the most dominating threat to mobile devices in 2015.

Malware variants flow

Malware Variants Flow | 2015

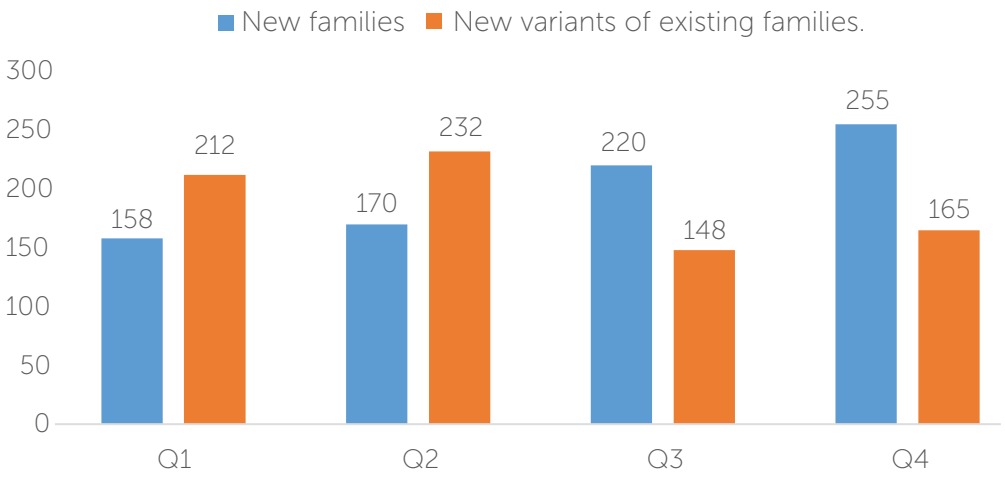

Figure (7)

Samples Received by Quick Heal | 2015

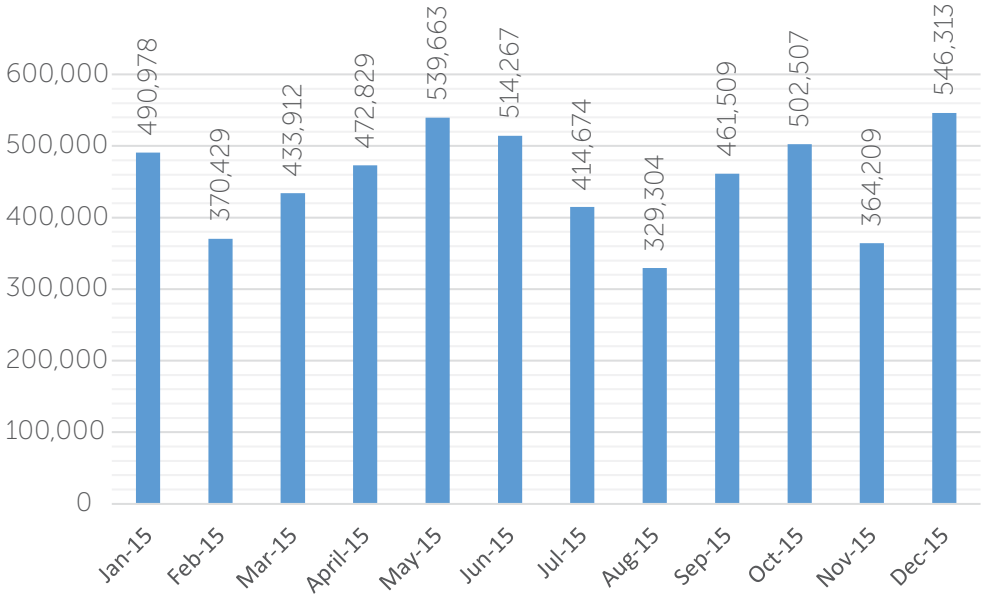

Figure (8)

Malware variants flow

Detection Category Flow

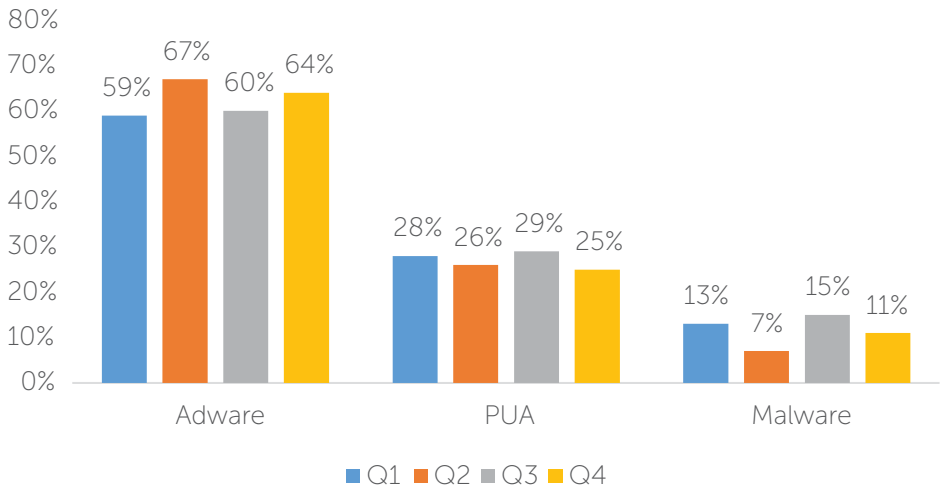

Figure (9)

Malware Growth Observed from 2013 - 2015

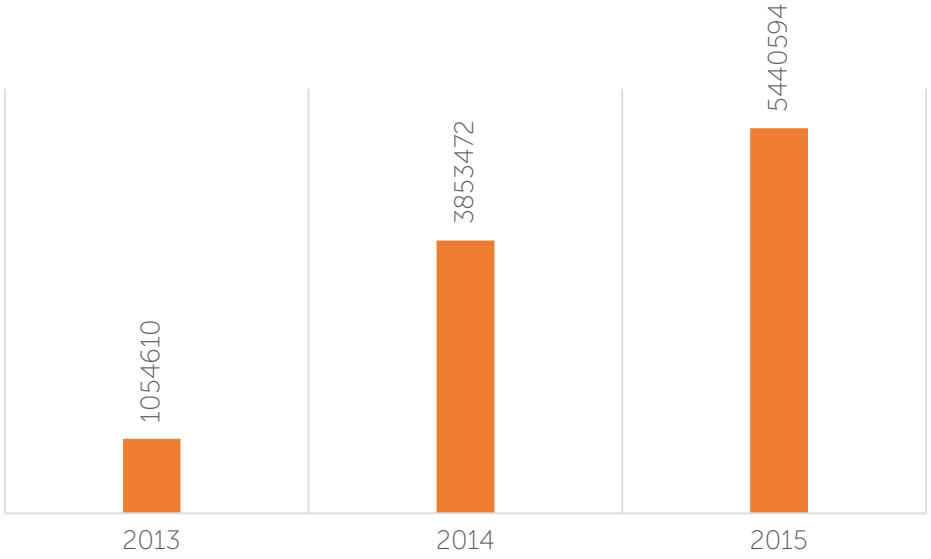

Figure (10)

TOP 10 Android malware

TOP 10 Android Malware in 2015

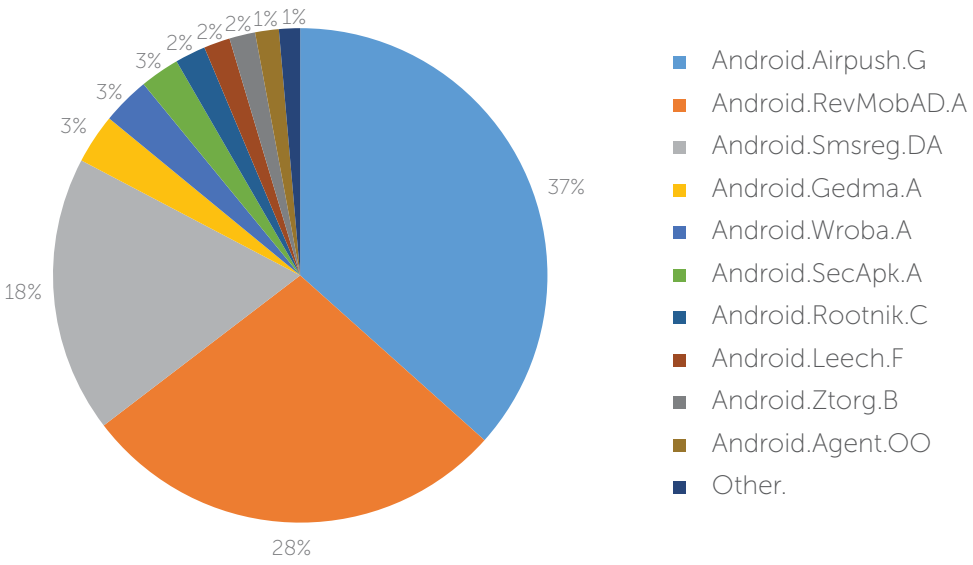

Figure (11)

Android.Airpush.G

Damage Level: Low

Method of Propagation: Ad plug-in

Behavior Post Infection: 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 is capable of modifying browser bookmarks in the compromised device and altering the appearance of the home screen. It can steal the following types of data:

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

Android.RevMobAD.A

Damage Level: Low

Method of Propagation: Ad plug-in

Behavior Post Infection: The malware displays several unwanted ads on the infected device and relays user information to several external servers. It collects the following data from the infected device:

- IMEI details
- Device provider
- Device ID
- GPS location
- Contacts list

TOP 10 Android malware

Android.Smsreg.DA

Damage Level: Medium

Method of Propagation: In-app purchases; mostly found in gaming apps

Behavior Post Infection: This a malicious Android app that comes under the category of Potentially Unwanted Applications (PUA). It asks Android users to make payments through premium-rate SMSs in order to complete their registration. The app collects the following types of information:

- User's phone number
- Incoming SMS details
- Device ID and contacts list

Android.Gedma.A

Damage Level: Medium

Method of Propagation: Trojanized apps in third party markets

Behavior Post Infection: The malware commonly targets users residing in China. After infecting the user's device, it steals the following information before relaying it to the attacker.

- IMEI details
- IMSI details
- Device name and type

Android.Wroba.A

Damage Level: High

Method of Propagation: Fake apps

Behavior Post Infection: This malware family has been known to target banking apps of users in Korea. The app appears as a fake 'Google Play Store app' or as 'Google Services'. Post installation, it immediately requests for administrator privileges. If the user is fooled into providing the same, the app intercepts incoming SMSs on the infected device. It also steals the following information and forwards it to a remote server:

- Device ID
- Contacts list
- Incoming SMSs
- Information of other apps installed on the device
- Login credentials of bank accounts and other banking information

TOP 10 Android malware

Android.SecApk.A

Damage Level: Medium

Method of Propagation: Protector plug-in

Behavior Post Infection: This is a Potentially Unwanted Application (PUA) that uses the 'Bangcle' Android application protector to infect Android devices. This protector is commonly used by Android application developers to prevent their apps from being tampered or decompiled. The use of this technique makes reverse engineering of apps extremely difficult, and this is what helps the malware authors of this malware remain undetected. The application may be a malware, adware, PUP or might even be clean.

It is wrapped with a particular wrapper code which makes it difficult for static analysis as all the activities are performed during execution.

Android.Rootnik.C

Damage Level: High

Method of Propagation: Third party stores

Behavior Post Infection: Roots Android devices, and performs the following malicious activities:

- Mounts system partitions
- Loads native libraries
- Takes admin privileges after rooting
- Voids device warranty
- Sends device information to a remote server
- Steals IMEI and IMSI numbers
- Accesses camera
- Gathers device location data
- Installs other applications without user's knowledge
- Shows advertisement over other applications
- Installs applications in ROM as system applications; making it difficult to uninstall the same

Android.Leech.F

Damage Level: High

Method of Propagation: Trojanized apps

Behavior Post Infection: The malware carries out the following malicious activities:

TOP 10 Android malware

- Connects to a malicious server to download infected files
- Reads destination files and inserts file names on SD cards
- Hides some apps, acquires a wake lock and then releases it after carrying out the malicious activity
- Exploits Android OS vulnerabilities one after another to gain super user privileges
- Installs other malicious apps in the system application folder (/system/app)

Android.Ztorg.B

Damage Level: High

Method of Propagation: Compromised websites and infected memory cards

Behavior Post Infection: It drops downloaded packages, extracts binaries from them and tries to execute them with root privileges on the infected device. It also performs the following malicious activities:

- Downloads malicious files
- Lowers security settings
- Steals personal information

Android.Agent.OO

Damage Level: Medium

Method of Propagation: Trojanized apps

Behavior Post Infection: The malware receives different commands from the attacker. Depending on the received command, it can carry out the following tasks:

- Intercept received SMSs
- Receive certain keywords to abort broadcast

Mobile ransomware in 2015

In 2015, malware authors were able to create many new variants of ransomware. The Quick Heal Threat Research Labs discovered about 28 such variants that are targeted at Android devices.

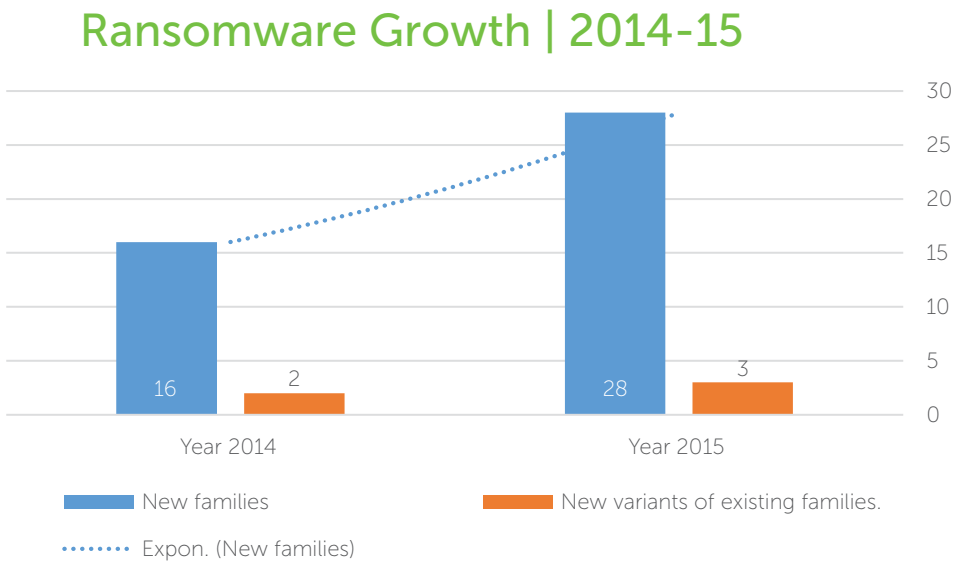

Figure (12)

The Lockerpin is known as the most popular Android ransomware in 2015. The malware modifies the infected device's PIN after infection. Quick Heal Mobile Security software detects and blocks this malware as '**Android.Simplocker.R**'.

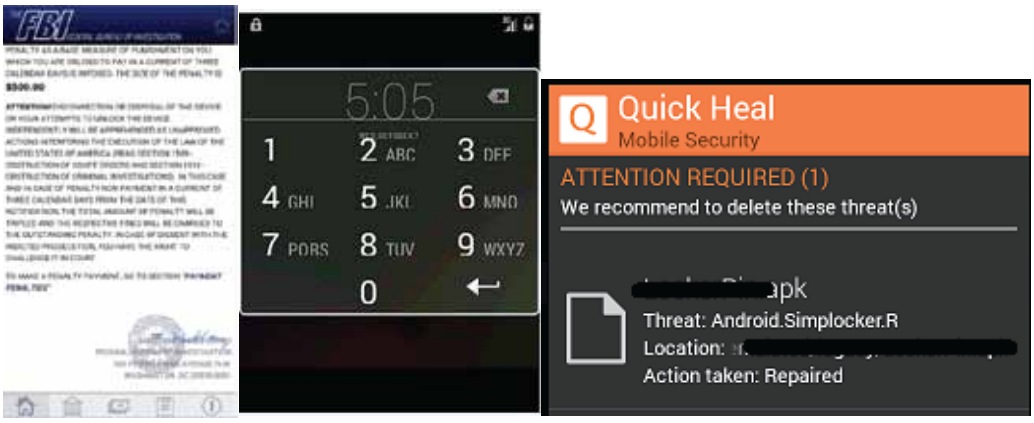

Figure (13)

Mobile banking Trojan - a new threat on the rise

The Quick Heal Threat Research Labs exposed about 21 families of mobile banking Trojans in 2015. These include completely new variants & new variants of existing families.

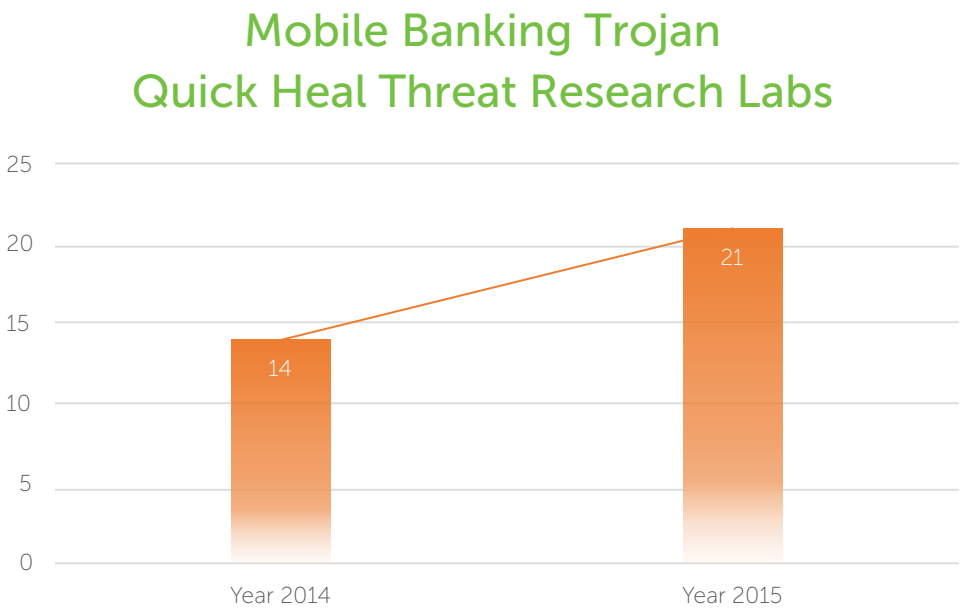

Figure (14)

Quick Facts about Banking Trojans

- They steal financial information, account details and login credentials from infected devices.
- Hackers use the stolen information to conduct illegal financial transactions.
- Newer variants of banking Trojans are using obfuscation techniques to bypass security detection.

The most popular banking malware analysed by Quick Heal Threat Research Labs - Android.Jisut.B

- The malware masquerades itself as a popular app like Adobe Flash Player, Viber, WhatsApp, etc.
- It carries a malicious payload embedded inside an image file (.PNG). The file is encrypted with Base 64. It decodes the image file, creates an apk on the device's SD card and then installs it on the device.
- After installation, it asks the user to grant 'Administrator Privilege' rights.
- If the user tries to deny this request, the app keeps asking their permission repeatedly.

- Once installed successfully, the malware launches an innocuous looking pop-up window as soon as the user opens their mobile banking application or the Google Play Store app.
- An unsuspecting user can be easily tricked into providing their login ID and passwords to the pop-up window. These and other sensitive details can be then passed on to the hacker.

Most popular malware using unique techniques, discovered in 2015

Android.MobiDash.A

- The malware comes under the Adware category. It displays pop-up messages that look like system notifications.
- The app hosting the malware was downloaded by millions of users from Google Play Store. As of now, the app is no more available in Google Play.
- Some of the apps loaded with this adware wait for a few days before beginning their malicious activities.
- It is difficult to spot the time during which the app launches the pop-up ads on the infected device.
- The malware serves ads continuously, whenever the user unlocks their device or restarts the application.

Quick Heal detects and blocks this malware as **Android.MobiDash.A**

Android.Mkero.A

- The malware was found in Google Play Store in the 3rd quarter of 2015.
- It has been designed to bypasses CAPTCHA. Using this technique, the malware subscribes the user to premium-rate services without their knowledge or consent.
- It redirects CAPTCHA online image-to-text recognition service.
- The malware has inbuilt advanced concealment capabilities, which help it to operate stealthily and bypass detection.
- It carries out the following activities in the compromised device:
  - Store details such as the list of installed applications
  - Read incoming SMSs
  - Send and delete SMSs

Quick Heal detects this malware as **Android.Mkero.A**

Most popular malware using unique techniques, discovered in 2015

Android.Hijoff.A

- The malware hijacks the shutdown process of the infected Android device. In this state, the malware can make calls and take photos.
- After successful installation, it asks for root permissions. If granted, the malware injects its code in the OS code to show fake animation and a fake dialog box.
- The malware can send SMSs and make calls to premium-rate numbers using the infected device.

Quick Heal detects this malware as '**Android.Hijoff.A**'.

Malware affecting the iOS platform

After Android, the iOS platform has been the favourite prey of mobile malware in 2015. Jailbroken devices have been particularly vulnerable and on top of the target list of hackers. iOS devices were mostly affected by the following malware family in 2015:

- YiSpecter
- XcoedGhost
- TinyV

Mobile malware trends and predictions

1

Ransomware and crypto-ransomware continue to reign

In 2015, Quick Heal Threat Research Labs discovered 28 new families of ransomware. These are seen as serious threats for 2016. We expect more new variants of ransomware to crop up. Most of them are likely to execute tricks that are commonly used by malware targeting the Windows platform.

2

Continued dominance of adware on Android devices

Adware has been the leading source of malware on Android devices for a long time now and this pattern will continue to prevail in 2016. The growth in adware is not showing any signs of recession; it will only swell as the years pass by. Existing adware variants are expected to evolve and be a major contributor to Android malware samples.

3

Cloud data

Cloud data hosting is gaining popularity by the masses and businesses all over the world. As data is the golden trophy these services hold, they could easily become one of the most targeted preys of hackers and perpetrators of cyber espionage campaigns.

CONCLUSION

As we embrace and adapt to new technologies, we unknowingly get closer to the dangers that feed on it. With apps, free software, connected devices, and online services swelling out of proportion, we will have a hard time in filtering the right from the wrong and this will work to the benefit of cyber criminals. In the New Year, we must prepare ourselves for newer technologies, their benefits and the security concerns to security that they might involve.

Internet of Things (IoT) could be the next best thing to look out for. Connected devices and exchanging data through these devices has made lives simpler but at the same time, has raised concerns over the security of data that is exchanged through various platforms. IoT devices are sold with unpatched and often outdated operating systems and software which make them susceptible to getting hacked. So, while researchers and experts work to make this platform safer for us, we must ensure that we are secured with the devices that we currently use, by following the basic and most recommended security principles, measures, and policies and by using the right security tools.