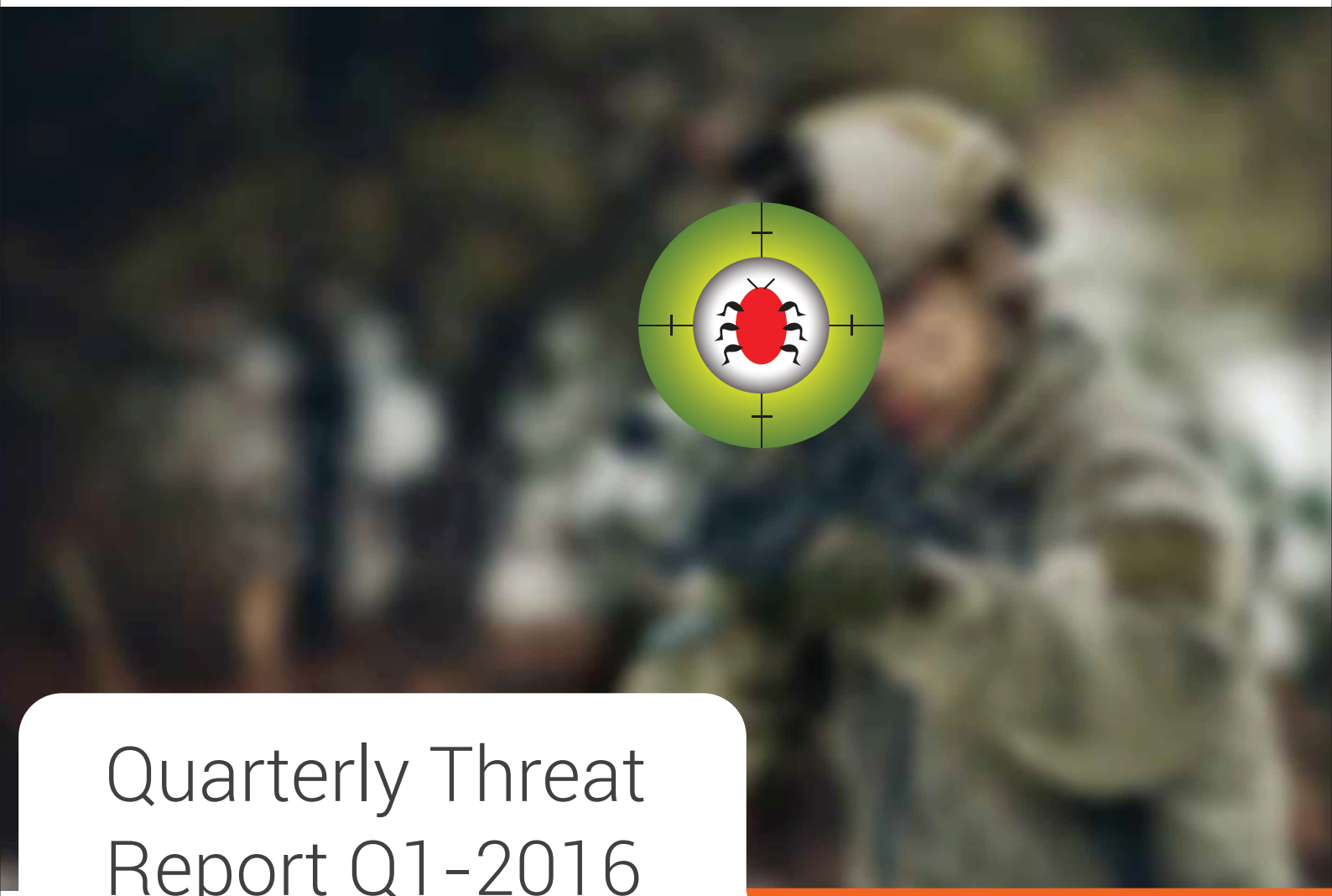
Quick Heal
Security Simplified

SEQRITE
Enterprise Security Solutions From Quick Heal



Quarterly Threat Report Q1-2016

www.quickheal.com

TABLE OF CONTENTS

INTRODUCTION

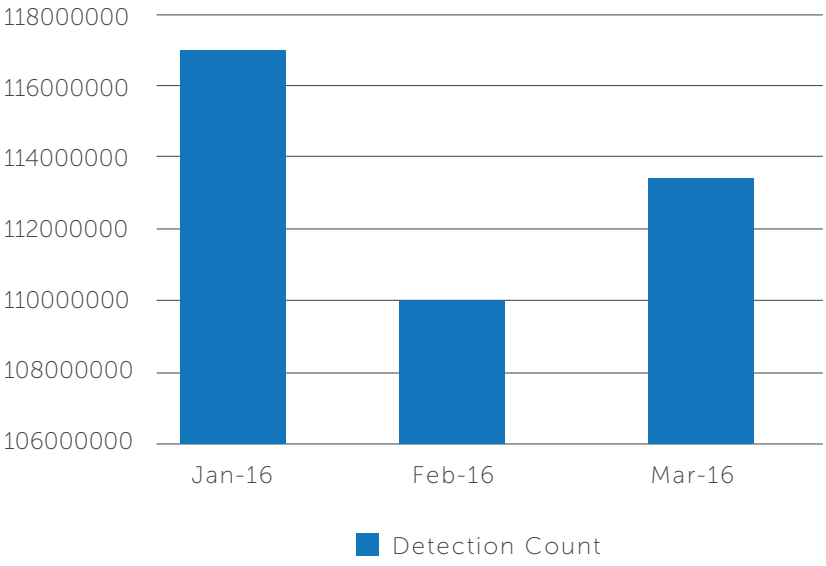
In the first quarter of 2016 (January, February and March) the Quick Heal Threat Research Lab received malware samples running into hundreds of thousands for the Android and Windows platforms combined. Malware propagation techniques and levels have increased exponentially over the years. With the number of connected smartphones and computers surpassing the global population levels worldwide, the large number of infected machines and malware samples detected is an expected outcome.

In this quarterly threat report we list out the malware samples detected in this quarter and pinpoint the notable trends and observations about these attacks. Moreover, we also look to the future and speculate about the kinds of threats that are expected in the upcoming months of 2016. The Quick Heal Threat Report is a reference guide to get insightful data about global malware threats and trends, and what they mean to the Internet users from all around the globe.

WINDOWS MALWARE DETECTION STATISTICS

The Quick Heal Threat Research and Response Labs detected malware samples running into millions over the first quarter of 2016. These numbers surpassed the malware detection from the same period in 2015 by a massive amount. Given below are the detection statistics of malware samples over the Windows platform from the first quarter of 2016.

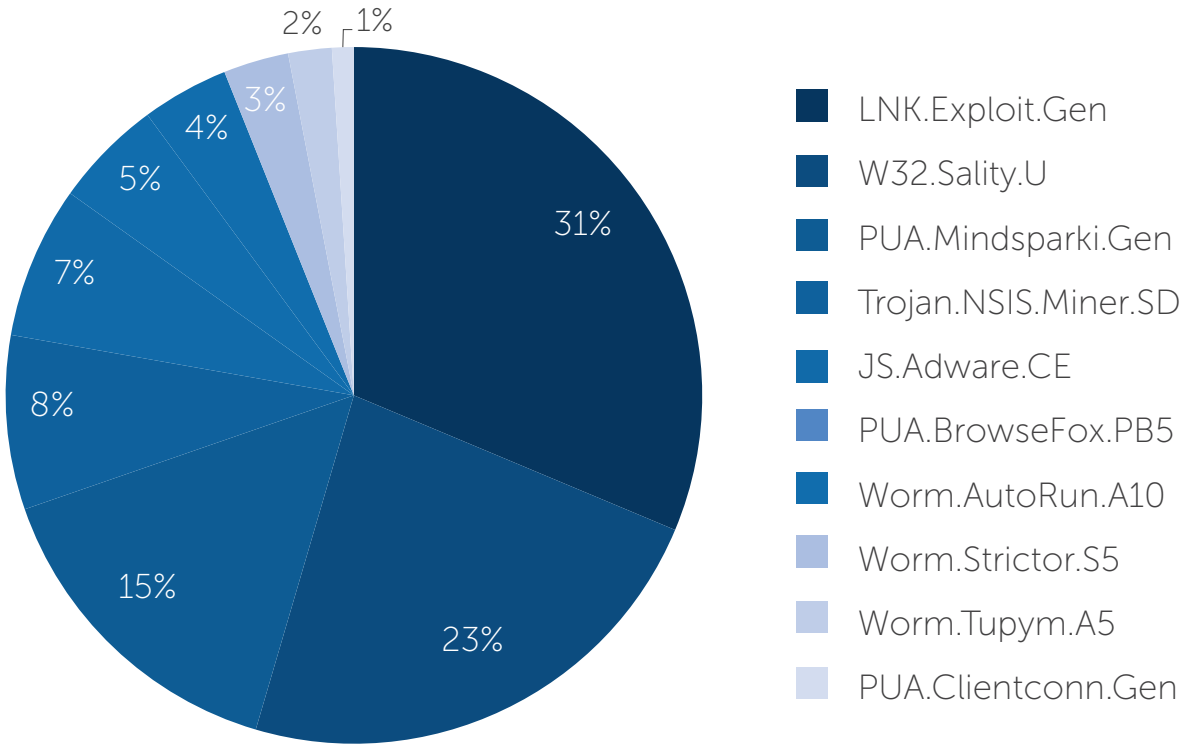
Windows Malware Detection Statistics



MONTH	DETECTION COUNT
January 2016	116,834,042
February 2016	109,943,093
March 2016	113,388,567
TOTAL	**340,165,702**

TOP 10
WINDOWS MALWARE

During the last 3 months of 2016, here are the top 10 malware samples that were detected by Quick Heal.



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 an infected computer. An attacker can use a backdoor to spy on the targeted user, manage files install more software or threats, shut down or reboot a computer or even attack other connected machines within the network.

Behavior: An exploit is a piece of software or a sequence of commands that take advantage of a bug or vulnerability in the system to cause unintended or unanticipated behavior on a computer. LNK.Exploit.Gen targets Windows vulnerabilities that allow malicious shortcuts to run themselves when the shortcut folder is viewed in Windows Explorer. It can easily compromise a system and install another rogue software on it. It can also redirect users to unsafe websites and suspicious advertisements which further slow the infected system down.

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 the executable files present on local drives, removable drives and remote shared drives.

Behavior: 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 deletes all files related to security software installed on the system. The malware also has the additional ability of stealing sensitive information from infected systems.

TOP 10 WINDOWS MALWARE

PUA.Mindsparki.Gen

Damage Level: MEDIUM

Method of Propagation: Bundled software and malicious websites

Summary: This PUA comes from third-party bundled installer applications and software downloaders. It falls into the Potentially Unwanted Applications (PUAs) category and changes the browser's homepage and default search engine to "ask.com" or "yahoo.com".

Behavior: It also installs a toolbar powered by "ask.com" in the system. It further recommends software that is mentioned on the toolbar to the user as well. The PUA attracts the user's attention so that he knowingly or unknowingly installs it on his machine. At times this malicious behavior gets mentioned in the EULA (End User License Agreement) displayed during the installation of these applications. If a user does not read the EULA carefully nor check what is mentioned in the custom installation, he ends up installing unwanted bundled applications on his system.

Trojan.NSIS.Miner.SD

Damage Level: HIGH

Method of Propagation: Bundled software and freeware

Summary: Trojan.NSIS.Miner.SD comes bundled with freeware and shareware programs. After installation of this Trojan, users get redirected to other malicious websites.

Behavior: Trojan.NSIS.Miner.SD enters into a system through hacked websites or unverified links. The Trojan then downloads and installs some free software on the system from malicious websites. These tasks are performed in the system background without the user's consent. The Trojan automatically starts when the system is booted up and it also modifies important system files and Windows registry settings. The Trojan makes excessive use of system resources and this further degrades system performance. It also opens a backdoor for other infections to enter into the vulnerable system.

JS.Adware.CE

Damage Level: LOW

Method of Propagation: Bundled installers

Summary: This Adware comes bundled with installers and are dropped into vulnerable systems during the installation process.

Behavior: JS.Adware.CE displays continuous pop-ups showing advertisements which consume excessive system resources and thus results in overall system performance degradation. The Adware also steals the user's financial information such as credit/debit card information and banking login credentials. It adversely affects system performance and browsing experience as well.

PUA.BrowseFox.PB5

Damage Level: LOW

Method of Propagation: Bundled software and malicious websites

Summary: PUA.BrowseFox.PB5 comes bundled with free software that is malicious in nature. It hijacks web browser and after installation, it also downloads additional malicious software on the infected system.

Behavior: This malware displays randomly placed pop-up ads and messages including discount coupons, deals, sales and offers whenever the targeted user visits online shopping portals or similar websites. If the user selects and downloads a free bundled application, he also receives unwanted extra toolbars, browser plug-ins and add-ons with the installation package. These extra tools may be marked as optional software during installation, but if the user does not deselect a checkbox, the software may cause unwanted system changes. It also tracks the user's browsing activity and uses the collected information for targeted marketing.

Worm.AutoRun.A10

Damage Level: HIGH

Method of Propagation: Spam emails and bundled software

Summary: This worm steals personal and confidential information from infected systems.

Behavior: Once within a system, it downloads other hazardous threats on the infected system. The worm also uses system resources in a manner that degrades system performance. It steals personal and confidential information such as credit/debit card details, banking information, email passwords, account passwords, private photos and more from affected user machines. It can also download additional malicious programs without user consent. It searches for vulnerabilities in installed programs on infected systems and even leads to cases of system crashes.

Worm.Strictor.S5

Damage Level: LOW

Method of Propagation: Spam emails and malicious websites

Summary: This worm actively spreads through spam emails that contain malicious links or attachments. It modifies an infected system's registry settings for the auto start. It also drops other Adware and Spyware samples into the infected system.

Behavior: Worm.Strictor.S5 actively changes the homepage settings and substitutes existing websites with potentially malicious ones. It also redirects user web searches to other harmful domains which may contain other additional threats, and it also prompts users to download some free software, videos, games etc.

Worm.Tupym.A5

Damage Level: LOW

Method of Propagation: Removable drives and network drives

Summary: This worm has the capability to change various browser settings such as the homepage and the default search engine. This threat also utilizes system resources in a manner that degrades overall system performance.

Behavior: Worm.Tupym.A5 has the ability to steal personal user information such as credit/debit card details, banking login credentials and more. It actively searches for removable drives and network drives in order to replicate itself and spread to other systems in the network via these drives.

PUA.Clientconn.Gen

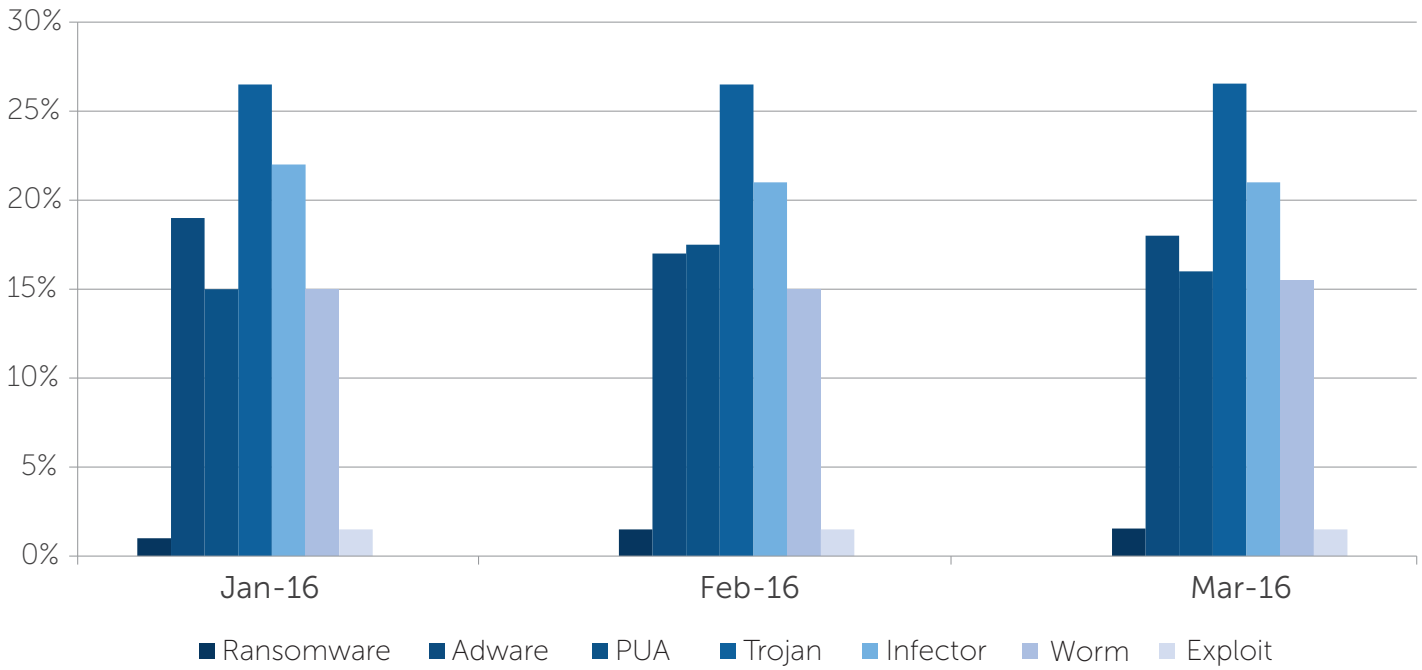
Damage Level: MEDIUM

Method of Propagation: Bundled software and malicious websites

Summary: This PUA alters the default search engine settings for the web browser to services such as default-search.net, search.ask.com and Trovi search.

Behavior: SearchProtect, SafetyNut Inc., Aztec Media Inc. are all Adware program publishers whose programs are promoted by and downloaded thanks to bundled software. They have the capabilities to change the default browser configuration settings and add entries of the aforementioned search engines. They also display an excessive number of ads when a user is browsing the web.

MALWARE CATEGORY WISE DETECTION STATISTICS

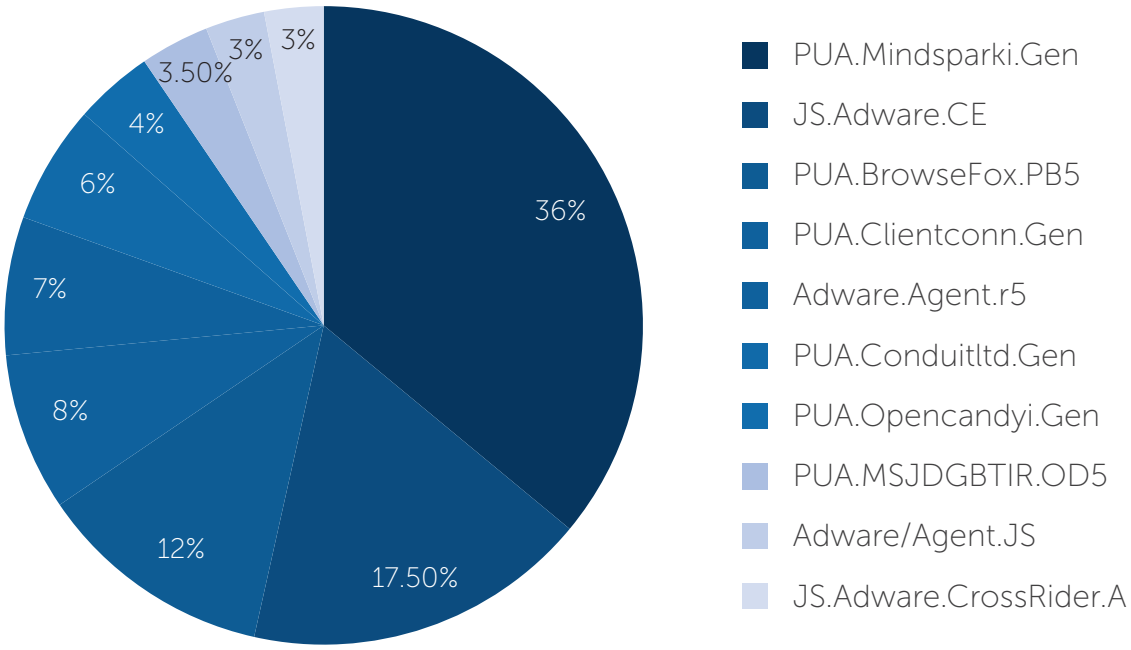


Observations:

1. Trojans (~26%), Infectors (~21%), Worms (~15%) and Exploits (~1.5%) all have near constant detection rates for every month within this quarter.
2. The contribution of Adware and PUAs combined is also constant around the 34% mark for malware detection.
3. Ransomware detection has grown by 50% in February 2016. While its share in total detection was 1% in January, in February and March this figure has grown to 1.5%, highlighting a big jump in the number of ransomware samples that have been detected.

TOP 10
PUAs AND ADWARE

During the last 3 months of 2016, here are the top 10 PUA and Adware samples detected by Quick Heal.

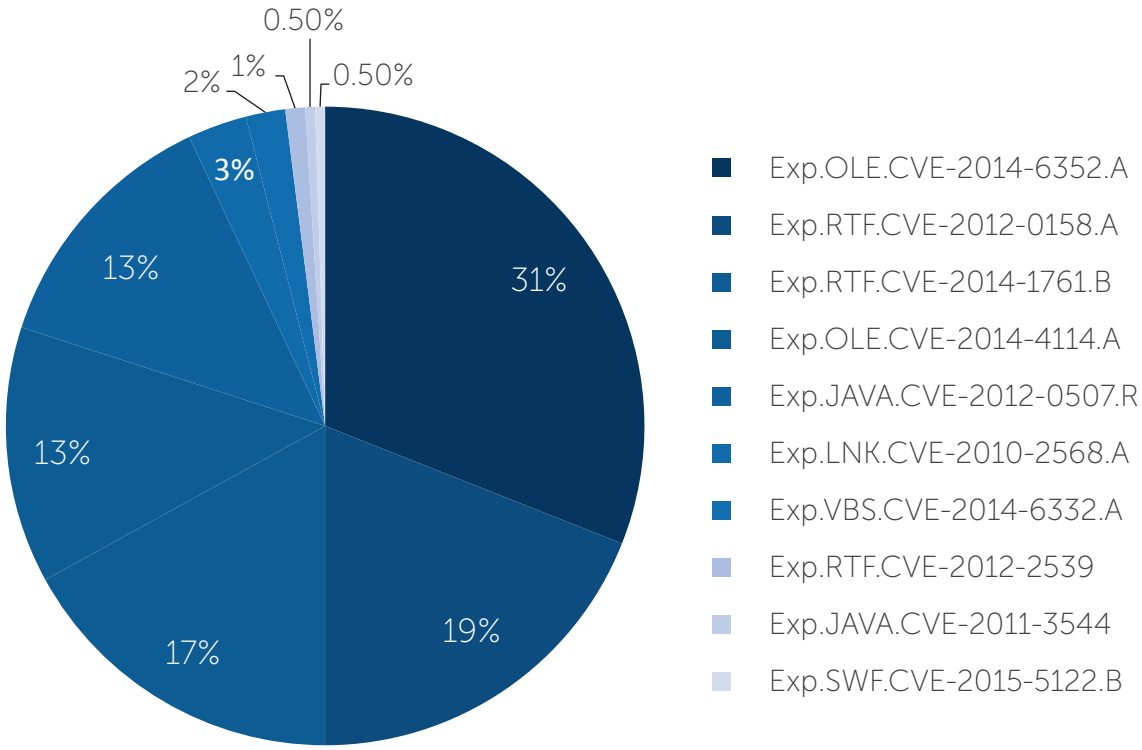


Similar to previous quarters, Q1 of 2016 was also witness to major PUA contributions from Mindsparki, BrowseFox and Clientconnect. These samples have been found to feature very prominently on a majority of client computers. Most of these PUAs are bundled with free software that is available on sites such as CNET, Softonic, Brothersoft and more. These PUAs have also been found to be a part of advertisement supported programs. PUAs are generally classified as low-risk malware. However, some PUAs can be more dangerous since they can open potential backdoors for other forms of malware. After installation, these PUAs generally display pop-up ads and coupon ads while the user is browsing the web.

Another trend that has been observed is that these PUAs make use of the video player and download manager programs on infected machines. Although they are not outright malicious in nature, their stealthy behavior and ability to install themselves on web browsers without user consent can enable them to support the download of other malicious applications.

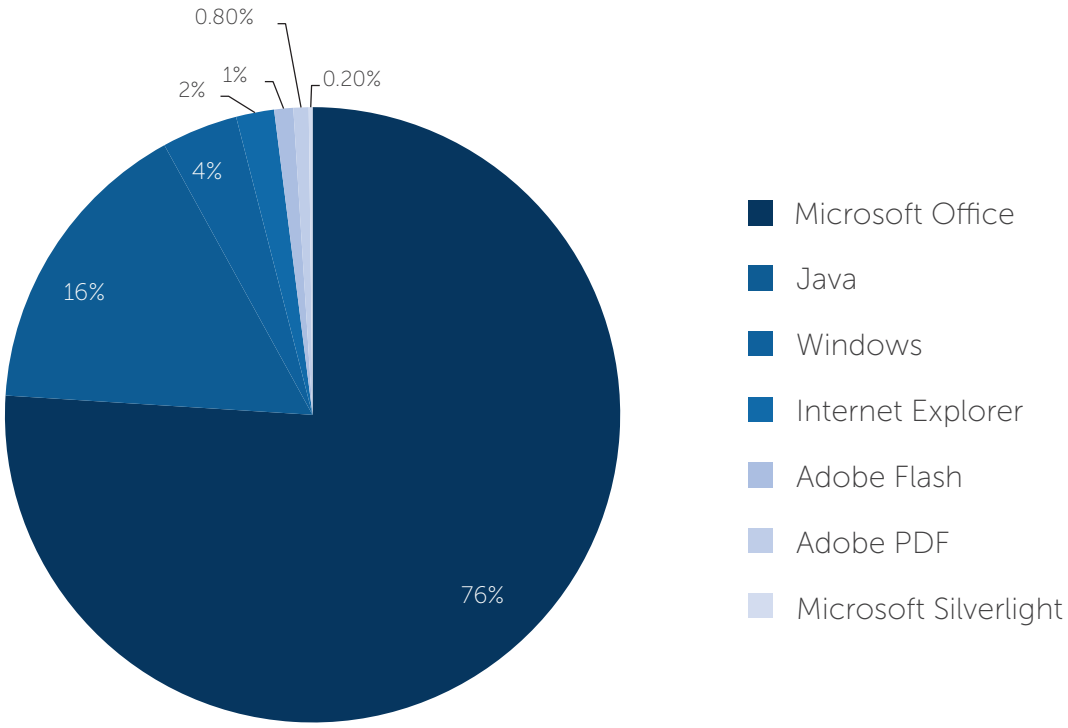
TOP 10
EXPLOITS

During the last 3 months of 2016, here are the top 10 exploits that were detected by Quick Heal.



A notable observation here is that OLE (Object Linking and Embedding) and RTF (Rich Text File) format related vulnerabilities contributed to 80% of detection, whereas JAVA vulnerabilities contributed only 13.5%.

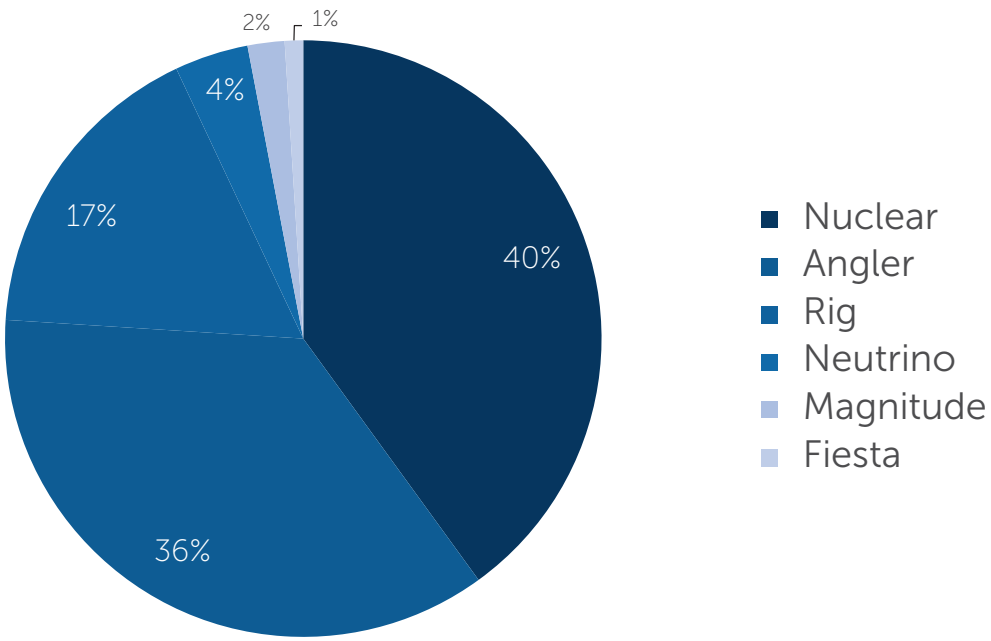
Application-Wise Distribution of Exploits



Microsoft Office and JAVA vulnerabilities together contributed 92% of the most used exploits.

Distribution of Exploit Kits

Nuclear (40%) and Angler (36%) are the dominant exploit kits from Q1 2016, followed closely by Rig at 17%.



MAJOR WINDOWS MALWARE DETECTED

PUAs and Adware

PUAs and Adware have continued to be major contributors to detected malware samples in Q1 2016. Adware is a program that displays pop-ups on user machines and can be commonly used by attackers to carry out other malicious activities as well. Many online publishers provide custom toolbars, free applications, software bundles or downloaders on various websites other than the sites of the publishers. PUAs make use of such services to reach the systems of vulnerable users by bundling unwanted and harmful software within them.

Recently, Adware samples have been found to focus more on attacking network resources such as DNS settings, hijacking proxies, disabling the auto update feature on web browsers and more. Given below are some of the common samples that we came across.

Dotdo FastInternet Adware acts as a proxy hijacker. After installation, it changes Google Chrome's browser shortcut target to – "-proxy-server=http=127.0.0.1:8877" argument. Dotdo FastInternet maintains a list of security-related related domains and if a victim tries to connect through the proxy, all the listed domains remain inaccessible.

Dynamic Pricer Adware installs an old version of Google Chrome and then disables automatic updates for the browser and for Mozilla Firefox as well.

Instant Support is another Adware that has been observed and it changes the DNS server address to 208.XX.XXX.16 and disables Google Chrome and Mozilla Firefox. Additionally, it automatically launches itself when the victim logs in on Windows and then it constantly displays an icon of "Instant Support" on the title bar of the active window or the taskbar.

Some of the top Adware samples from Q1 2016 were:

- Mindsparki
- BrowseFox
- Conduitltd
- Opencandyi

Ransomware

Ransomware remains a major and rapidly growing threat in 2016. This is due to the many variations of ransomware that are easily available and can be easily spread. Cyber criminals are increasingly using ransomware to force their victims to fall for their tactics and pay the ransom to recover their important documents that have been encrypted.

TeslaCrypt is a major new ransomware that emerged a year ago and has now evolved into many different versions. This year it has been found with several new infection and propagation techniques. The 3.0 version of TeslaCrypt used '.MP3' extensions for encrypted files with new ransom note filenames. The latest 4.0 version also subsequently released with new filenames and explanations on how to pay the ransom in order to recover encrypted files, and it also does not append any file extensions to the encrypted files. Propagation vectors of this ransomware are still the Angler Exploit Kit and various spam emails.

'Locky' is a new ransomware variant that is propagated via spam emails with malicious MS Office documents. Recently, this ransomware has also started using obfuscated JavaScript files as attachments. When such JavaScript files are executed, they download and install the Locky ransomware on victims' machines. The ransomware encrypts most of the documents available on the system and then demands a ransom payment from the user.

Some of the ransomware samples from Q1 2016 were:

- Ransom32
- Cerber
- CryptoJocker
- CRYPTEAR
- CTB-Locker
- HYDRACRYPT
- 7ev3n Ransomware

Targeted Attacks

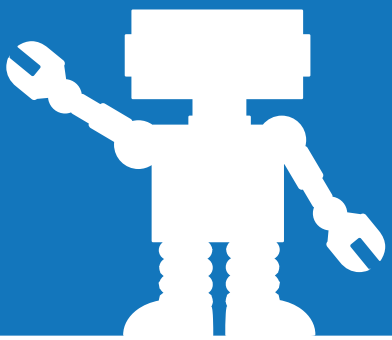
In the first quarter of 2016, politically motivated and profit making targeted attacks have been observed in large numbers. Malware authors are successfully using the old and unpatched system and application vulnerabilities for exploitation. Social engineering tactics still also remain advantageous for attackers.

One such attack was observed against the Indian Ambassador to Afghanistan. Attackers exploited the old CVE-2010-3333 vulnerability that then downloaded the 'Rover' malware with plugins and got installed on the system. This malware then performed spying activities and sent confidential information to its remote C&C servers.

Another targeted attack was observed against employees of a Russian bank. This attack tricked victims with fake job-related emails and made use of 'Trojan.Ratopak'. The credentials of targeted employees were obtained with the possible intention of financial gain. A similar attack was also observed in Ukraine, where the victim was targeted by the 'BlackEnergy' APT campaign. Macro-containing documents were sent to the victims via spam emails and when they were opened, the 'Phdet' backdoor entered into the system. This backdoor then gave complete remote access and control to the attacker. By increasingly targeting the healthcare and banking sectors, attackers seem to be altering their strategies from long-term attacks to shorter and more intense ones.

Hollywood Presbyterian Medical Center in Los Angeles was attacked by ransomware that encrypted emails, patient records, CT scans, lab work and more. The ransomware then demanded a huge sum to hand over control to the hospital authority and to get its records back. All affected systems were offline for a week and daily work at the hospital was heavily affected and brought to a complete standstill.

Bangladesh Central Bank was another noteworthy targeted attack. Attackers installed malware on a Bangladesh Bank computer and then stole critical information which was used to carry out fraudulent transactions and electronic theft. After receiving the attackers fake requests, the Federal Reserve Bank of New York transferred over $80 million from Bangladesh Bank to fake accounts based in the Philippines and Sri Lanka.



UPCOMING TRENDS FOR WINDOWS MALWARE

1 Ransomware

While this quarter has seen a drastic rise in the number of ransomware samples detected by Quick Heal, these detection are expected to rise even further in the upcoming months. The 'CryptoWall' ransomware was relatively low in its prevalence in Q1, but we firmly expect it to show itself in massive numbers and advanced variance again. 'TeslaCrypt' is another ransomware that is constantly evolving and we expect it to surface with new variants and advanced propagation techniques soon.

The 'Locky' ransomware is another family that will pose an active challenge for security products and computer users with its constantly changing infection techniques. This ransomware is not just limited to macros in MS Word documents or obfuscated JavaScripts. 'Locky' can also be embedded in videos, PDFs and other formats, thus making it a high-risk ransomware in the upcoming months.

2 PUAs and Adware

The growth of PUAs and Adware is a current trend in the security threats scenario and these forms of malware are expected to grow further in 2016 as well. As the internet is opening up and becoming easily available to many more people around the world, Adware attacks are reaching more users. Adware serves attackers by delivering information stealers is destructive malware strains into machines. Malvertising campaigns are also expected to continue taking advantage of old system vulnerabilities.

In the near future, Adware may find new ways to inject ads and pop-ups. Some of these ways may include patching genuine library files on systems, proxy hijacking, blocking security domains, changing DNS settings and more. Adware samples can also make use of advanced anti-detection techniques and disable any anti-malware software that is installed on infected machines.

3 Targeted Attacks

We have already witnessed several high-profile targeted attacks in the first quarter of 2016, and the healthcare and banking sector are expected to be the latest lucrative targets of such attacks. Additionally, other sectors such as Government organizations, educational institutions, and defense institutions are also expected to be affected by cyber attackers in the coming months.

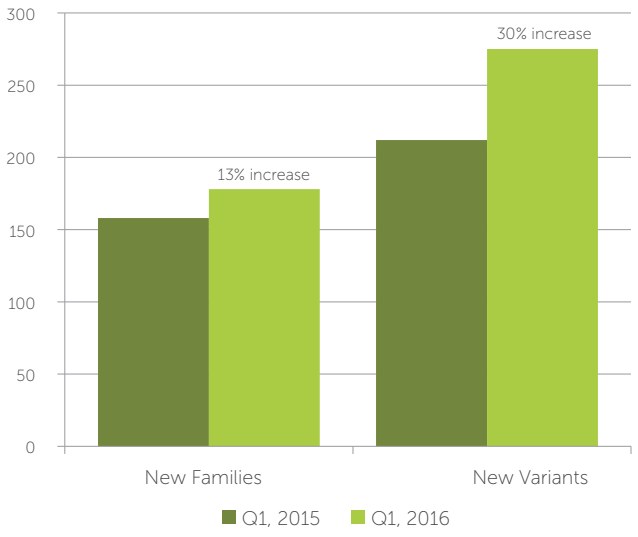
Such attacks persistently remain hidden and steal critical information from systems, but recently, destructive malware samples have also started being used in such attacks. Such methodologies can enable attackers to make big money very quickly. Other attack sectors such as attacks related to ATM machines, Point of Sale (PoS) terminals and Internet of Things (IoT) will also be soft targets that can be compromised by attackers soon.

ANDROID MALWARE DETECTION STATISTICS

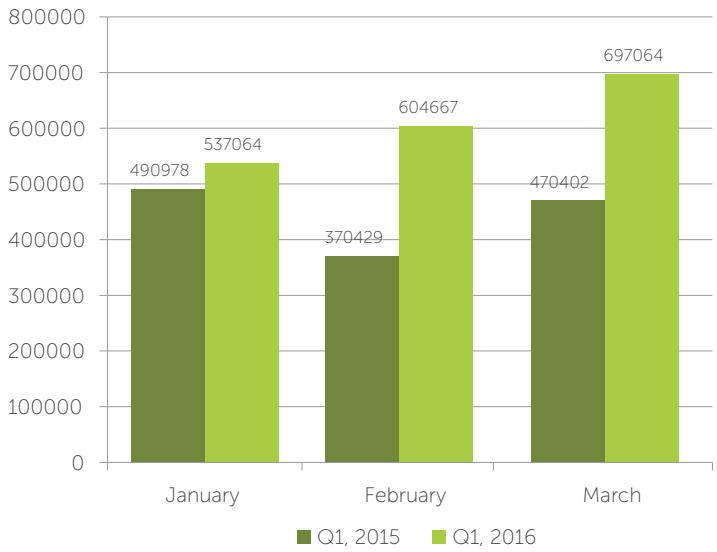
ANDROID MALWARE DETECTION STATISTICS

The Quick Heal Threat Research and Response Lab detected 178 new malware families and 275 new variants affecting the Android platform in Q1 2016. When compared with similar figures from Q1 2015, this represents a 13% increase in the number of new malware families and an increase of 30% in the number of new variants detected. Given below are the detection statistics of malware samples over the Android platform from the first quarter of 2016.

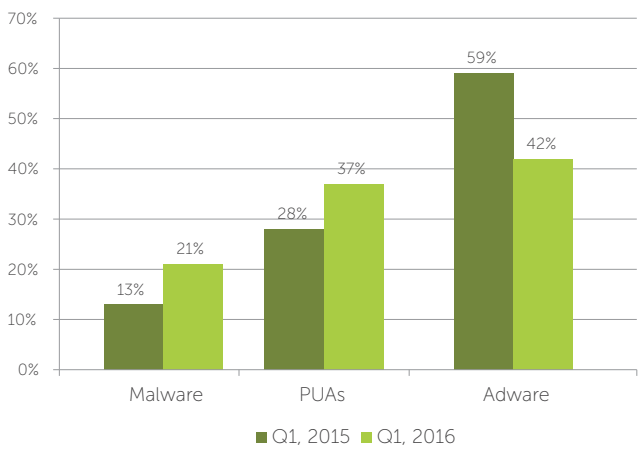
New Malware Families and Variants



Samples Received by Quick Heal



Detection Category Flow Q1, 2016

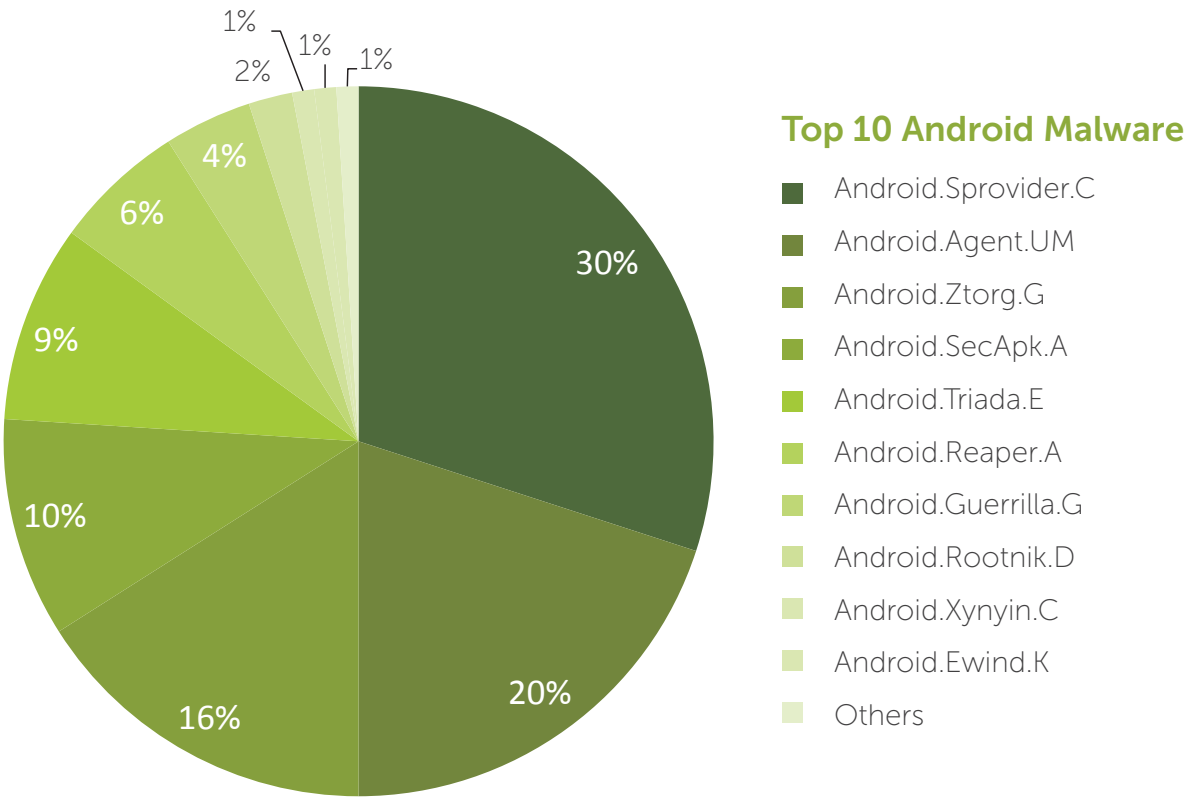


Observations:

- On average, around 20,000 malware samples were detected on a daily basis in Q1, 2016.
- This represents a 38% increase from the same period in 2015.
- Adware samples saw a drop in detection from 59% to 42%.
- Malware and PUAs have become more common and constitute larger proportions in the detected malware sample.
- Detected malware samples grew from 13% to 21% and detected PUA samples grew from 28% to 37%.

TOP 10
ANDROID MALWARE

During the last 3 months of 2016, here are the top 10 malware samples that were detected by the Quick Heal Lab.



Android.Sprovider.C

Damage Level: LOW

Method of Propagation: Third-party app stores

Behavior:

- Pushes ads in the notification bar.
- Pushes full-screen ads and the back button or home button does not work leading to the ad getting clicked.
- Once the ad is clicked, an installation prompt appears and an app download begins.
- Uses obfuscation, encryption and dynamic loading to make analysis difficult.
- Downloads additional modules and then runs them.
- Few samples hide their launcher after the first run.
- Frequent downloading also leads to usage of data bandwidth and negative impact on other apps.

Android.Agent.UM

Damage Level: HIGH

Method of Propagation: Third-party app stores

Behavior:

- Downloads other apps on the infected device without the user's consent.
- After first time execution, it asks for device admin permission and checks if the device is rooted or not rooted.
- It downloads other malicious apps from third-party stores or malicious servers.
- It silently installs these downloaded apps without informing the user.
- It hides and starts its service in the background.
- If the user attempts to remove device admin privileges, it shows a pop-up in a continuous loop.

Android.Ztorg.G

Damage Level: HIGH

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

Behavior:

- It displays unwanted ads and downloads other malicious apps in the background. Even if it is removed, the app will appear on the device after a restart.
- It uses Java reflection to load other classes.
- It contains advertisement frameworks which are used to download and display ads.
- It 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 his code in the system folder and also get root privileges.
- It downloads files in /system/xbin/ which is UPX packed ARM binaries.
- It then accesses the root terminal and executes commands on the device.
- It then downloads other malicious apps on the device without user consent.

Android.SecApk.A

Damage Level: MEDIUM

Method of Propagation: Protector plug-in

Behavior:

- This is a Potentially Unwanted Application (PUA) that uses the 'Bangcle' Android app protector to infect Android devices.
- The protector is commonly used by app developers to prevent their apps from being tampered with or decompiled.
- This technique makes reverse engineering of apps extremely difficult.
- This fact enables the authors of this malware to remain undetected.
- It is also wrapped with a particular wrapper code which makes it difficult for static analysis as all activities are performed during execution.

Android.Triada.E

Damage Level: HIGH

Method of Propagation: Fake apps in third-party app stores

Behavior:

- Since the app uses a system icon, or even has no icon in some cases, its malicious activity begins as soon as it gets installed and a specific service is triggered, or when the user clicks on its icon.
- It collects all device info such as IMEI, IMSI, model name, version details, network information and details related to installed apps.
- The C&C server gives an encrypted configuration file and is stored as /system/app/com.sms.server.socialgraphop.db.
- This database contains the field 'mModuleUpdate' which tells whether or not to download a new dex file and load it in the memory. This newly loaded file is used to send SMSs.

Android.Reaper.A

Damage Level: MEDIUM

Method of Propagation: Third-party app stores

Behavior:

- After installing this app, a pop up that says "User Experience Improvement Plan" is shown and the app gets hid.
- It sends OS related information such as boot events, battery events, Bluetooth enabled events, external storage events, headset plug events, ringer mode change events and more.
- It also sends other information and details such as IMEI, IMSI, MAC address, operator name, country, OS version, display screen details and more.

Android.Guerrilla.G

Damage Level: HIGH

Method of Propagation: Third-party app stores

Behavior:

- Downloads and installs other malicious apps without the user's permission.
- After execution, it asks for the device admin permission.
- After rooting, it starts two services – Time Service and Monkey Test.
- This Trojan carries out aggressive advertising campaigns for other apps.
- It displays ads in the notification bar and in other third-party apps.

- It downloads and installs other unwanted apps in the system folder.

Android.Rootnik.D

Damage Level: HIGH

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

Behavior:

- This app is hard to get rid of, and 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.
- Further rooting activity is also performed by the Ztorg malware.

Android.Xynyin.C

Damage Level: HIGH

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

Behavior:

- In addition to installing other malicious apps without the user's consent and also showing unwanted ads in the infected device, this app also reappears on a device restart even after it has been uninstalled.
- The Trojan sends details such as IMEI, IMSI, MAC address, OS details, language, name of network operator, country, SD card availability, package name of the malicious app and its version number, name of all apps installed and the name of all apps running in the background.
- It shows unwanted ads and can trigger the download of other malicious apps.
- It uses a unique technique of 'steganography'.
- It can download an image from its C&C server. This image looks like an ordinary file but it hides encrypted data on it.
- The decrypted file is nothing but a dex file that has the ability to install/uninstall other apps.
- Attackers use this technique because they only need to change the code from the image located at the server side without changing the code of the application itself.

Android.Ewind.K

Damage Level: LOW

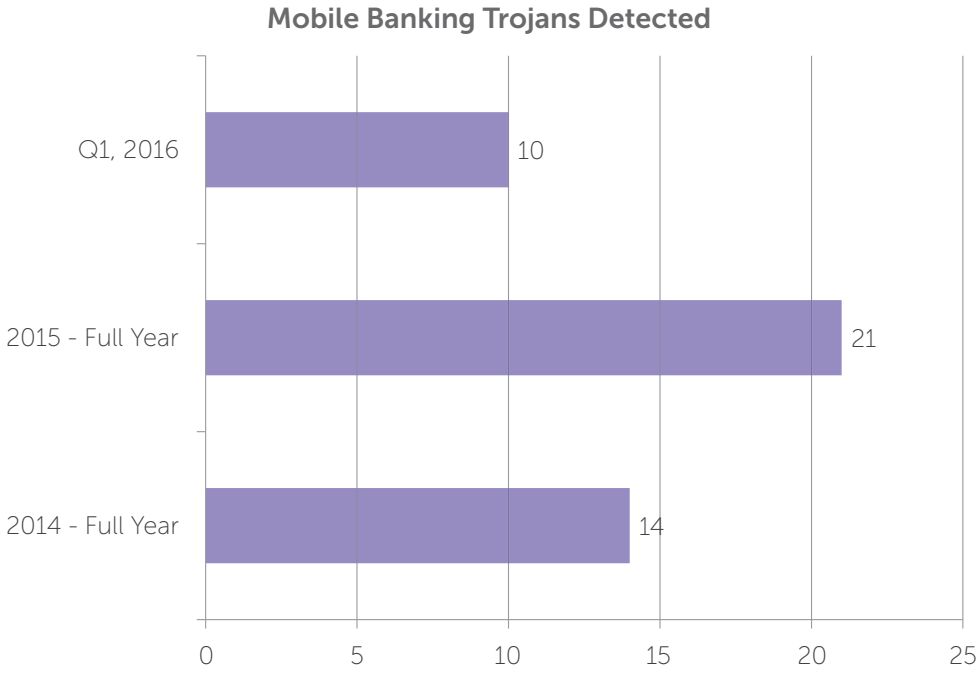
Method of Propagation: Third-party app stores

Behavior:

- It displays unwanted ads on the infected device.
- All malicious apps from this family are obfuscated in nature.
- After execution, it decrypts the malicious file from the asset file. This is the previous version of this Adware and it then shows a prompt for installing the same

MOBILE RANSOMWARE AND BANKING TROJANS

In the first quarter of 2016, mobile ransomware and banking Trojans have increasingly come under the spotlight. Many new variants of these malware types were detected by Quick Heal and the growth of these types has increased since the corresponding period last year. Quick Heal detected 4 new ransomware variants that target Android devices, including old and new families.
Additionally, 10 families of mobile banking Trojans were also detected. These included completely new variants and new variants of existing families as well.



Observations:

1. These mobile banking Trojans steal financial information, account details and login credentials from infected devices.
2. Once this information has been obtained by hackers, it is used to conduct illegal financial transactions and online theft.
3. Newer variants of mobile banking Trojans are using obfuscation techniques to bypass and avoid security detection.

MALWARE USING UNIQUE TECHNIQUES

MazarBOT: A new Android malware sample that steals SMSs and wipes phones

This dangerous new malware sample, MazarBOT, has been discovered in-the-wild and found to have the capability to hijack an unsuspecting user's smartphone. The malware gets into a device with a simple SMS and then downloads an APK onto the device. The SMS contains words that trick the user into clicking on the link within, and this then causes the APK to immediately start downloading on the compromised device.

The malicious activities performed by MazarBOT are as follows:

- All incoming SMSs are forwarded to the C&C server.
- MazarBOT can wipe all device data when it receives the 'hard reset' command from the C&C server.
- It sends an SMS to premium-rate numbers and this leads to high mobile bills.
- It can monitor which app is currently being used.
- It can inject itself into Google Chrome and then modify the HTML content on open web pages.
- It can make calls to any number, reject incoming calls or enable call forwarding to specific numbers.
- It can also lock the phone when it receives a 'lock' command.

Quick Heal detects this malware on Android smartphones as **Android.Mazarbot.A.**

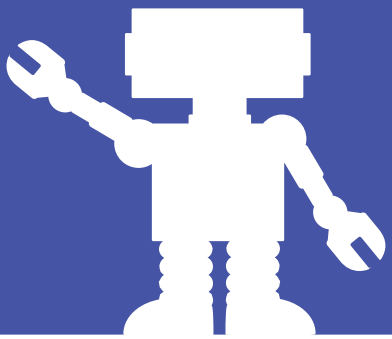
MALWARE ON iOS

In addition to propagating mobile malware threats over Android, malware authors are now increasingly targeting iOS also. As the percentage of iOS users worldwide is growing, so are the security threats that concern them. Over Q1 2016 iOS has become a common target of mobile malware authors, and jailbroken devices, in particular have, featured atop the list of common targets. The most popular malware afflicting iOS users was 'AceDeceiver'.

AceDeceiver

Three different iOS apps from the AceDeceiver family were uploaded to the official Apple App Store and these apps pretended to be wallpaper apps. These fraudulent apps successfully bypassed Apple's security code review at least 7 times by performing malicious activity only when the device was in China. The location can also be easily modified by the malware author. Subsequently, Apple removed these fake apps from the store, but they can still be installed on devices.

AceDeceiver also encourages users to enter their Apple IDs and passwords for additional features. If shared, these details are then sent to AceDeceiver's remote C&C server. These malicious apps further create a connection with third-party app stores that are controlled by the malware author, in order to download other apps and games on iOS devices.



UPCOMING TRENDS for MOBILE MALWARE

1

Ransomware and crypto-ransomware continue to reign

So far in 2016, Quick Heal has detected 4 new families of ransomware. These are continually seen as threats to the mobile user base around the world and we expect many new variants of existing ransomware families to arise soon. Initially, mobile ransomware samples simply copied the tricks and techniques of Windows samples, but these samples are getting more advanced now and we expect them to surpass the techniques used by Windows samples.

2

Mobile payment mechanisms under threat

The popularity of banking transactions conducted from mobiles is at its highest and this has opened up this avenue to increased threats from malicious parties. This is indicated by the growing number of sophisticated malware families that have been found to attack the official apps of banks and other merchant sites from different countries.

"Android.Acecard.A" and "Android.Tiny.D" are some of the most popular malware families that target banking apps and pose a risk to mobile payment portals. It is strongly expected that hackers and malicious authors will continue to target such apps and portals in the near future.

CONCLUSION

The first quarter of 2016 has seen a steady rise in the detection of Android and Windows-based malware samples. While malware authors constantly devise new techniques to infiltrate systems and trick unsuspecting users, IT solutions providers have to work harder to counter these attack vectors with unbreakable security mechanisms in place. In this time period, the month of January witnessed a large number of detection over the Windows platform. Whereas, the Android platform also witnessed a steady increase in new variants detected and new versions of old variants when compared with the similar time period from 2015.

With ransomware coming to the fore and becoming a major threat agent over all platforms, the need of the hour is vigilant monitoring of all systems and proactive removal of malicious software from all machines. It is essential to keep all applications, programs and operating systems updated to avoid security vulnerabilities. Users should also keep basic security precautions in mind and stay away from phishing pages, malicious emails and more. Complete security is possible when all potential attack vectors have been blocked.