Quick Heal

Annual Threat Report 2015

www.quickheal.com

Table of Contents

Introduction

As far as the IT security industry is concerned, the year 2014 was highly eventful and memorable for several different reasons. Microsoft Windows, still the most dominant OS for computers around the world, was subjected to several high profile attacks and security vulnerabilities. Nonetheless, the platform recovered from all these flaws but not without hundreds of thousands of machines falling prey to these loopholes.

Malware attackers and hackers discovered new targets such as Sony Pictures, nationalized institutions and many more, but the security industry was always at hand to provide protection and security against these newfound threats. 2014 was also the year in which Ransomware matured and reached several new territories and also became localized as a result. Along with ransomware, Adware was also a prominent threat during the year and became highly sophisticated in order to inject banner ads into webpages, to hijack web browsers and search engines and to hinder PC performance.

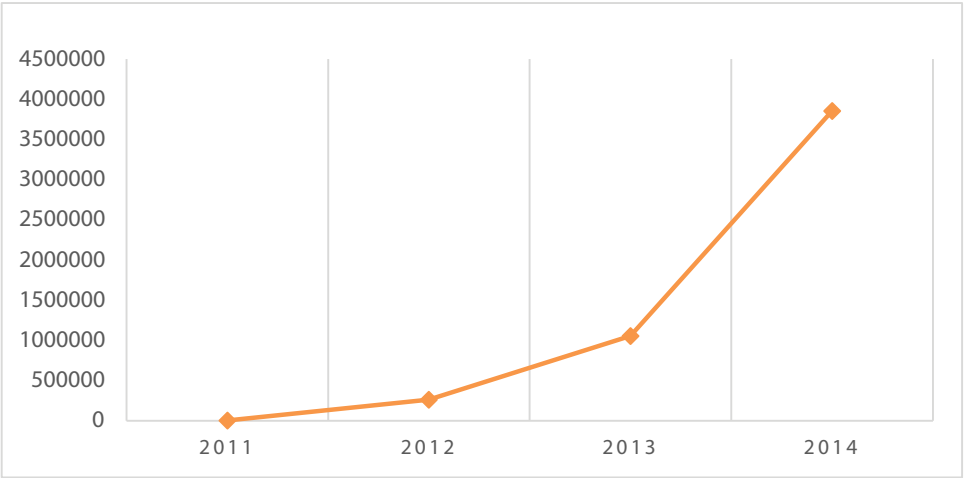
As far as Android is concerned, malware samples saw an exponential growth and Quick Heal detected close to 3 million malware samples throughout the year. Moreover, attackers have devised techniques to pervade the Google Play store and have now started publishing fake apps and games on this official channel in order to trick unsuspecting users as well. Adware and Ransomware have become common over Android as well, and this indicates a growing trend of malware becoming platform and device agnostic. With that in mind, here is a detailed look into the major malware threats and attacks over Windows and Android in the year 2014.

Android Malware
Collection Statistics 2014

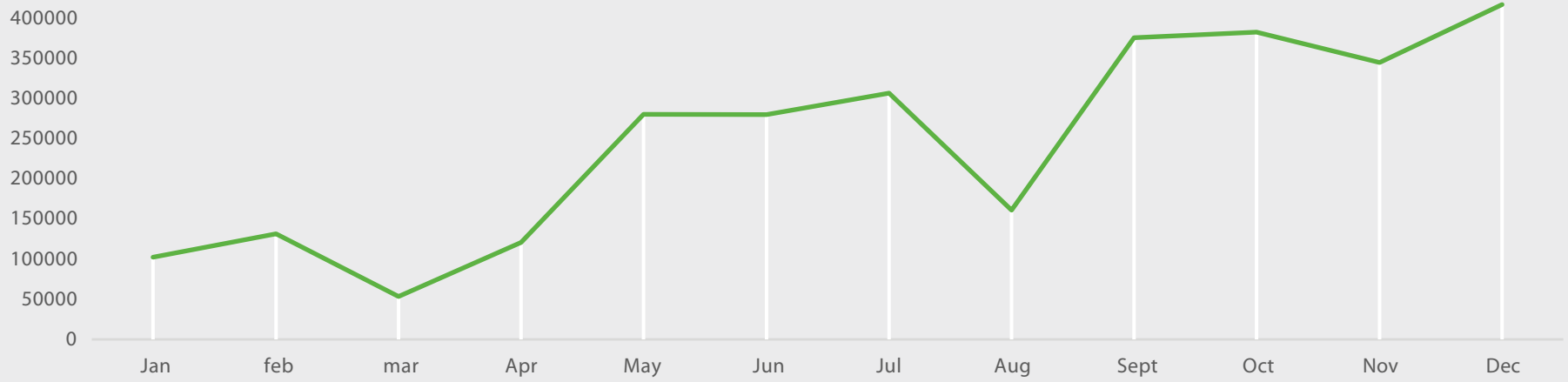
The year 2014 has seen an exponential growth in the figures of Android malware that have been detected and reported. In the three years since 2011, Quick Heal Threat Research Labs has witnessed a 304 times growth in Android malware and this figure is directly attributed to the high rise in Android smartphone sales and usage across the world. These uprising trends also indicate that the dominance of mobile malware attacks will continue in 2015 as well.

The Quick Heal Threat Research Labs have found 536 new families in the category of Android Adware, Malware and PUP (Potentially Unwanted Programs) and a further 616 new variants afflicting the Android platform.

Growth of Android malware from 2011 to 2014



Android Malware Collection Statistics 2014



Top 10 Android Malware Variants 2014

- Android.Viser.A
- Android.Mobclick.A
- Android.Gedma.A
- Android.Coogos.Ad388
- Android.Agent.DL
- Android.Smsreg.W
- Android.Domob.A
- Android.Invis.A
- Android.SeaWeth.D
- Android.SecApk.A
- Other

Android.Viser.A

This is the most prominent Adware category that has been detected. It displays a high amount of unnecessary ads to a user's device and it also has the ability to make alterations to the saved bookmarks on a device. Additionally, it steals critical information such as:

- Device location
- IMEI number of the device
- Sends SMS to premium-rate numbers

Android.Mobclick.A

Mobclick also performs similar functions and aggressively pushes unwanted ads to an Android device. However, this Adware is categorized as an ad-plugin bundle app and it steals the following data without the users consent.

- Network information
- SIM serial number
- Phone number
- Email address

Android.Gedma.A

This application is a malware variant that primarily targets users residing in China. Upon installation, this application compromises user devices and steals the below mentioned private information and then transmits it via SMS.

- IMEI details
- IMSI details
- Device name
- Device type

Android.Coogos.Ad388

This malware falls under the category of PUP and illegally gains access to the following information from an Android device. It also misconfigures the camera application in a device and attempts to steal banking information from the handset.

- Contact information
- Device location
- SIM card information and details
- Subscriber ID
- Device ID

Android.Agent.DL

This malware family is highly dangerous since it enables other malicious applications to be downloaded onto a device through a backdoor entry. The primary application also steals and transmits the following information to its command and control servers.

- Contact list information and details
- Device location details and banking information

Android.Smsreg.W

This malicious app comes under the category of Potentially Unwanted Applications and it asks Android users to make a payment through premium-rate SMS in order to complete registration. The cost of these text messages is determined by the malware author. The premium rate number SMS is not sent until the user selects the option to pay for the mentioned service.

Since the user has already downloaded and installed the app prior to registration, he loses some data usage bandwidth. In many cases, the app also checks for particular network operators and sends SMSs. The app also collects personal user information.

Android.Domob.A

This is a prominent Adware that pushes unwanted ads to the notification bar of the device and persistently checks the network status of the device. It also steals the following private information:

- System logs and entries
- Device location details
- Device ID and information

Android.Invis.A

This is a malicious application that gains in-depth access to the private data that is stored on an Android device. The following data types are siphoned by this application:

- Information from the Contacts list
- Subscriber ID
- Device ID
- It also monitors incoming text messages and calls and downloads other malicious apps

Android.SeaWeth.D

After installation, this application gains access to private information from an Android device. The app displays itself as a clean weather forecasting app so it does not raise any suspicions. It sends the below mentioned private information to premium-rate numbers that it receives from a particular link.

- IMEI data
- IMSI data
- Application name along with the latest version
- Gives the link of the app location via SMS

Android.SecApk.A

This is a Potentially Unwanted Application for Android device owners. It uses the Bangcle Android application protector which is commonly used by Android application developers to prevent the tampering or decompiling of their apps. This technique makes reverse engineering very hard on this malicious app as malware authors use this to stay undetected.

As a result, Quick Heal detects Android apps that use this protector under the Potentially Unwanted Application category as a precautionary measure.

Android Malware and Google Play

When an Android user views a featured application on Google Play, he immediately places a degree of trust and faith in that application and assumes that it has been effectively screened for malware and other security risks by Google. Several techniques and processes are involved before an app is allowed to feature on the Play store. Hence, it is preferable to download and install apps directly from Google Play.

However, malware authors have identified this as a weakness and are increasingly targeting Google Play and attempting to serve fake apps within the store. They have started pushing fake malware developers with familiar app names in order to trick users into installing such apps to cause havoc due to the cascading effect. Naïve users then find it difficult to identify fake apps from real ones.

Sometimes, Google Scanner is unable to remove fake apps from the marketplace before they are installed by unsuspecting victims. Malware authors have become increasingly adept at deriving the benefit from this and obtaining private data from user devices.

1 First fake paid application

Android.VirusShield.A

In the 2nd quarter of 2014, the website 'Android Police' came across a fake sample of Android.VirusShield.A on Google Play. This app featured as a top paid application in the store and was thus installed by a large number of users. The app author claimed it was an antivirus program that protected personal information from dangerous viruses. The app also promised to scan files, media, settings and other installed apps in real-time to prevent malware installation. Instead, the app stole critical device information, personal user data and hampered the battery life and device performance once it was installed.

2 Malware attacks on social networking and chatting apps

Android.Wabek.A

In the 1st quarter of 2014, we came across an application on Google Play that was called "Camara Vision Nocturna". This app was responsible for video recording and other related functionalities. Unknown to the user, the app was stealing user data and uploading it to a remote server in the background. The data included vast amounts of contact info from apps such as WhatsApp, ChatOn and other social networking/chatting apps. The malicious app also sent text messages to premium-rate numbers in the process.

3 First RAT (Remote Access Toolkit) infects Google Play

Android.Dingwe.A

A RAT (Remote Access Toolkit) is a type of malware that can remotely control the access and status of devices when it is installed on the device. While this app was active on Google Play for a while, it has since been removed. Mentioned below are the malicious activities that were performed by this malware:

- Clicks photos from the camera of the device
- Sends SMS from the device
- Captures audio and video clips from the device
- Downloads pictures from the device gallery
- Records active calls
- Downloads details of other accounts (email, social media, VPN) that are stored on the device

4 First sneaking malware

Android.Agent.HD

This malware was discovered in the 2nd quarter of 2014. Posing as a genuine application on Google Play, this malware went by the name "Google Play Stoy". Many unsuspecting users believed that the application was a version or an update of the authentic Google Play and went ahead and installed it on their device. After installation, the app stayed well hidden from the screen and ran in the background in order to collect private data and transmit it to remote servers. It also intercepted incoming text messages and data entered by users to access online banking services.

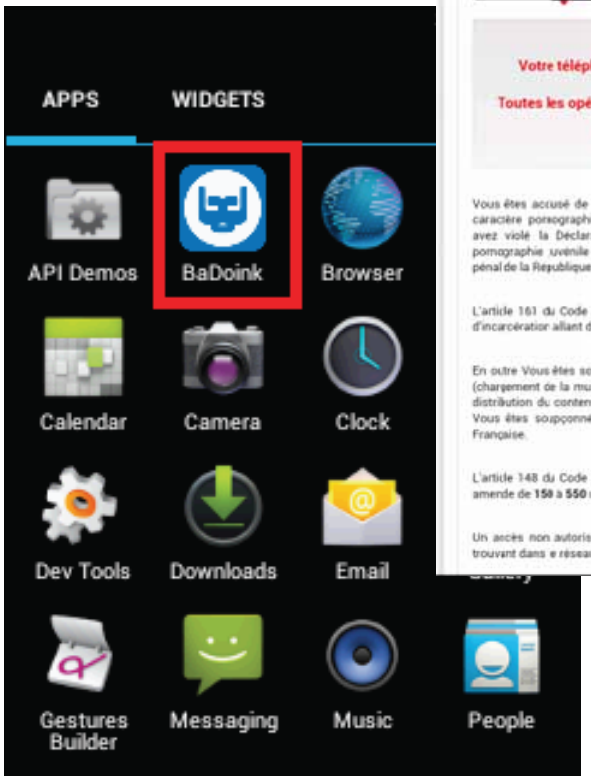
Most Popular Malware as per Technique in 2014

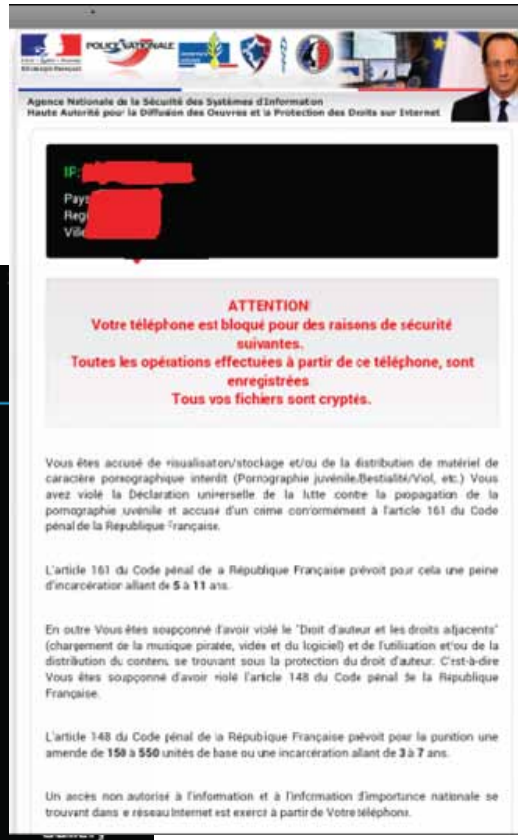
In 2014, we came across several new techniques that were implemented by Android malware developers. While some of these techniques were imitations of Windows based tricks, there were some new and unique methods that were spotted as well. Moreover, all these tricks were relatively new and unique as far as the Android platform is concerned.

Top Ransomware

a) Android.Koler.A

Koler is a new Android ransomware that has been spreading to users as a fake adult themed streaming service known as "BaDoink". Once installed on the device, it takes over the handset via random webpages that are opened. The Home button works for a short period of time and then the device is locked and the user only views a device locked screen after a few seconds. This app then demands a payment from the user and displays symbols of the FBI and other police agencies in order to intimidate users and to look legitimate.



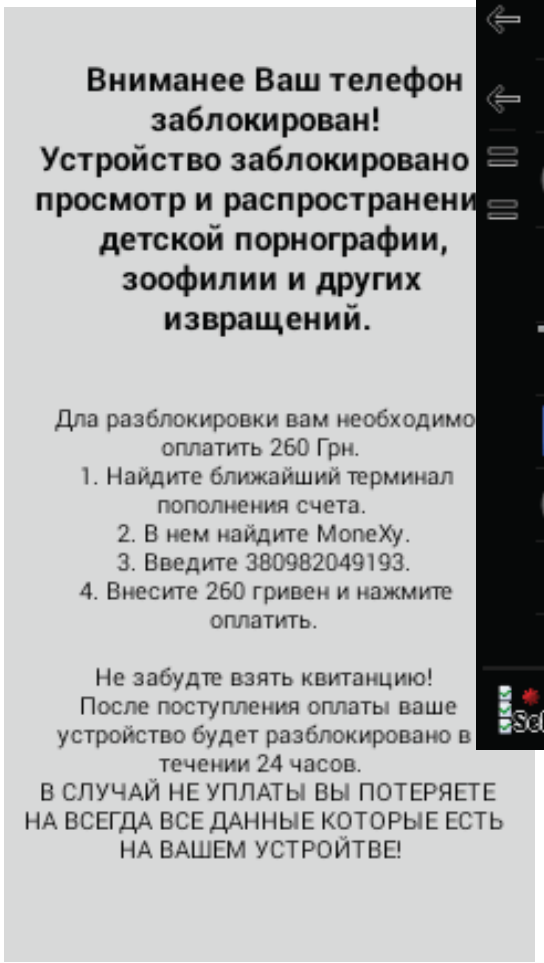


b) Android.Simplocker.A

Simplocker is a notorious Trojan that masquerades as a harmless application for Android devices. Once installed on a device, it displays a message in Russian informing the user that his device has been locked and only the payment of a ransom can unlock it. The app has not been found on Google Play and is only known to exist in third-party sources and app repositories. The ransomware also steals the following data:

- IMEI number
- Device model and information
- Manufacturer of the product/hardware
- Operating System version

Once installed on a device, Simplocker displays an icon named "Sex xonix". The Trojan also possesses the ability to scan the SD card inserted into the device for specific file types (.jpeg; .bmp; .gif; .doc; .docx and more) and encrypt them.



First worm spreads through SMS 2

Android.Selfmite.B

This is a Worm for Android devices that spreads primarily through text messages. It manifests itself as an APK file and then sends SMS to the first 20 contacts in the phone book of the infected device. After installation on a phone, it displays itself on the device under an alternative icon such as Google+, Mobogenie, Mobo Market or others. However, for a device to be infected upon receiving the aforementioned SMS, a user would have to click on the spam link within the SMS and then manually download and install the APK.

First boot-kit on Android 3

Android.Oldboot

In the 1st quarter of 2014, Quick Heal Threat Research Lab came across a type of virus never seen before on Android. This malware was utilizing a new technique to modify the device boot partition within Android devices.

It also modified the boot script to extract malicious applications before the booting process actually began on an infected device. After installation, it gained access to the private information stored on the device and was observed to have following capabilities:

- It had C&C connectivity and downloaded malicious configuration files
- It had the capability to download and install other Android applications
- It had the capability to uninstall system applications from the device

Upcoming Trends for Android Malware in 2015

Exploit & Vulnerability Kits

We strongly expect more Android exploit kits using tactics similar to the Black Hole Exploit Kit (BHEK) which took advantage of security issues caused by Android fragmentation. Greater attacks which take advantage of vulnerabilities will be seen as malware authors will devise more loopholes and exploit kits.

Wi-Fi networks will also become a serious attack vector for mobile devices. Hackers will be able to perform an advanced man-in-the-middle (MITM) attack against compromised networks and devices. This will be achievable by interrupting, redirecting or intercepting mobile traffic packets in the form of voice, SMS etc.

Targeted attacks on banking credentials and data

It is widely expected that banking credentials of individuals and other entities will be under risk in 2015. This can be largely attributed to the auto login feature of mobile apps and banking websites that are commonly used by individuals. In order to intercept this data, attackers will increasingly target mobile devices for broader credential stealing or authentication attacks in the coming year.

3 New payment systems being targeted

Mobile payment platforms offer up a tempting and rewarding target for cyber criminals. A known vulnerability called Android Fake ID allowed attackers to steal Google Wallet credentials of victims for a short duration. WeChat also started a method of allowing users to purchase goods sold by predetermined retailers with the help of so-called "credits". All these initiatives and more cashless payment systems enable cyber criminals to take advantage of virtual wallets and steal money from users through vulnerabilities in apps.

4 Ransomware and crypto-ransomware will continue to rise

This year we have come across many variants of ransomware on Android devices and we expect this trend to continue in the next few months. Ransomware is a type of malware that previously used to afflict Windows machines only, but it has now become prominent on the Android platform and devices as well. Some of the most widespread ransomware variants of 2014 are Android.Simplocker.A, Android.Torec.A and Android.Koler.A.

5 Social engineering attacks

Social engineering is a broad fisted term that implies techniques and tricks used by hackers to convince victims to voluntarily give up critical information. These tricks range from fraudulent phone calls, emails and text messages, to phishing pages that dupe home users or enterprise users to fill up details and share them voluntarily on fake pages or forms. Private information of users is expected to be at serious risk from social engineering tricks in 2015.

Fake apps prevalent on Google Play

In 2014 we came across several fake and malicious apps present on Google Play and we expect this number to rise further. As low cost Android phones make devices available to all market segments, there is bound to be a large number of people that mistakenly install malicious apps from Google Play and lose critical information. Malware authors have also become clever about the names and tricks they use to trick unsuspecting victims, so this is a trend that will not slow down any time soon. Few of the commonly seen malicious apps on Google Play in 2014 were *Android.VirusShield.A, Android.Wabek.A, Android.Dingwe.A and Android.Agent.HD.*

Continued dominance of Adware

Adware has been a leading source of malware on Android devices for the last few years and this is a pattern that will continue into 2015. Adware variants are not going anywhere and they will persistently play a leading role in Android malware samples. In 2014, we discovered several new Adware families and this indicates the upward curve of the malicious apps that serve up unwanted and unnecessary ads to Android devices.

Malware on Other
Mobile Operating Systems

While Android has been the primary target of mobile malware, other operating systems are also increasingly coming under the radar of malware authors. There have been some noteworthy incidents on other platforms as well, and this does not bode well for smartphone users in general.

- After Android, iOS is a hugely popular OS for smartphone users across the world. But this was also the year that WireLurker, one of the most dangerous malware to ever hit Apple devices, was found in-the-wild and affected hundreds of thousands of Apple customers. The malware primarily spread through apps that were downloaded from third-party stores and then stole information from infected devices. It even possessed the ability to reach Apple laptops and desktops when an iPhone was connected via a USB cable. In 2015, Apple's Cloud Drive, Apple Pay and NFC systems also seem to be at risk.
- Malware that targets Symbian OS seems to be on a downward spiral due to the dwindling numbers of Symbian device users. However, a notorious malware called Cabir that spread through unsecured Bluetooth connections completed 10 years in 2014.
- Thanks to the rising numbers and popularity of Windows Phone OS, it is expected that 2015 will see tremendous growth in malware samples and attacks over the platform.

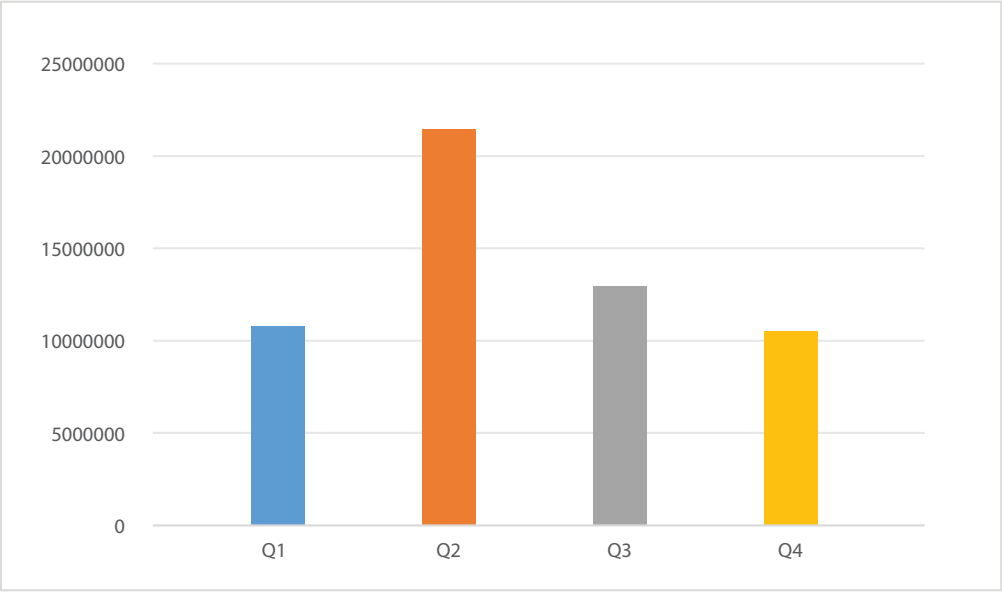
Summary - Windows Malware

Quick Heal's Threat Research Labs have come up with the Annual Threat Report for Windows for the year 2014 and there are several interesting and noteworthy trends here for further study and analysis. Ransomware has shown complete dominance in the year gone by and it has also shown tremendous evolution in its propagation techniques. Encryption techniques of ransomware have also become far more advanced and ransomware has also displayed localized customizations in many instances.

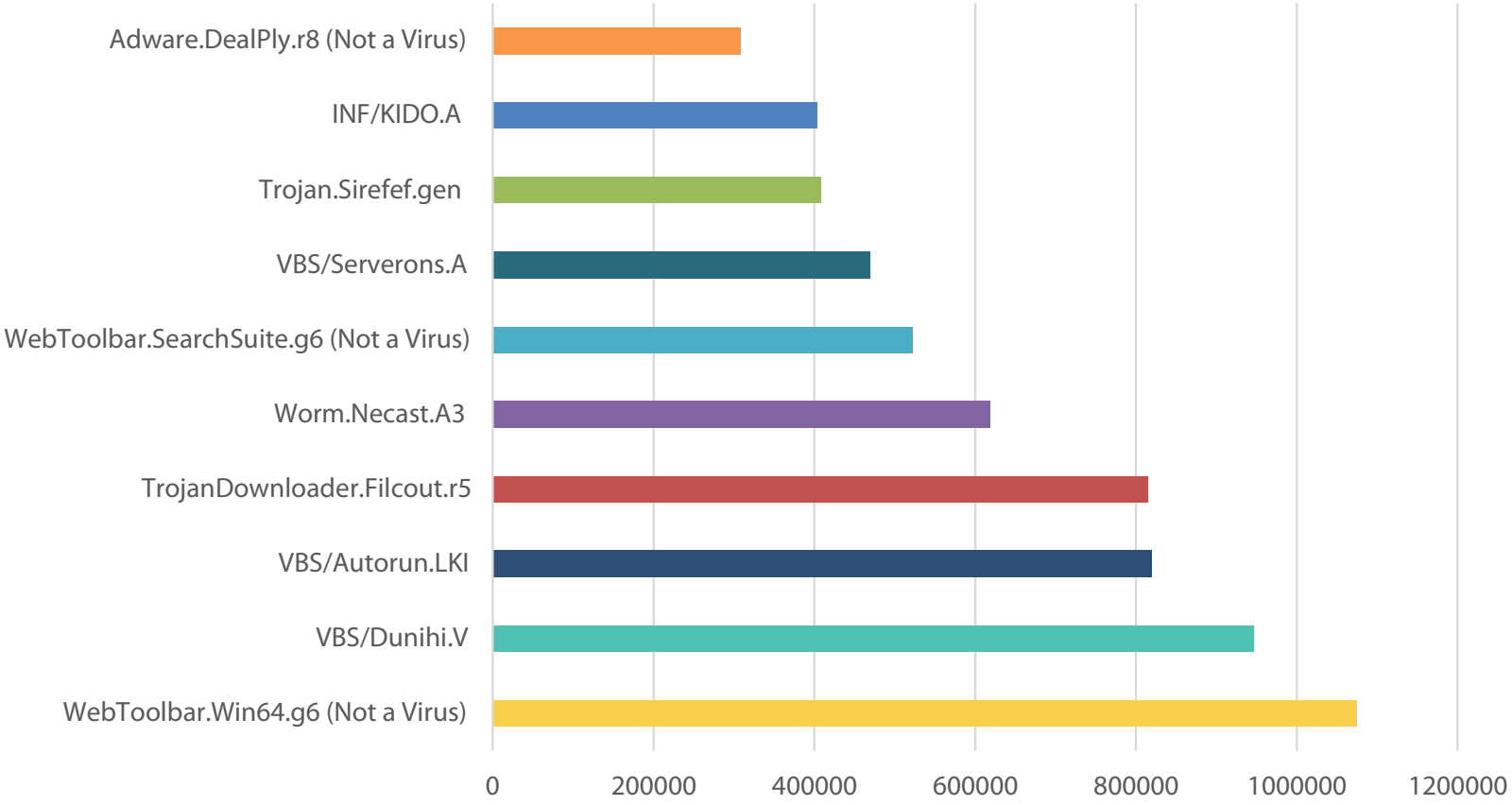
On the other hand, we have detected large numbers of spam emails containing malicious attachments in the archive format, thus leading to widespread distribution of malware such as Trojans, worms, backdoors and exploit kits. It has been detected that these variants frequently receive instructions from remote C&C (command and control) servers from across the globe.

Adware has also been growing at an alarming pace since the 2nd quarter of 2014. Adware techniques have been modified in order to propagate ransomware further and this technique is known as "Malvertising". New techniques have also been seen in malware propagation and infection with the sole purpose of avoiding detection by antivirus software and security protocols. With that in mind, here is an in-depth look into the Annual Threat Report for Windows for the year 2014.

Windows Malware
Collection Statistics 2014



Top 10 Windows Malware Variants 2014



WebToolbar.Win64.g6

This Windows malware performs the following malicious activities:

- Injects banner ads into websites and displays pop-ups that do not originate on these sites
- Makes unauthorized changes to important files and registry entries which ultimately affects system performance
- Hijacks the default home page and search engine to generate unwanted ads
- It enters the system through browsers such as Chrome, Firefox and Internet Explorer through user downloads and freeware programs

VBS/Dunihi.V

This is a worm that spreads through removable drives. If a user attaches a removable drive to an infected system, a .LNK file that runs the VBScript worm is created. This .LNK file is created with the same name as files that are already present on the removable drive.

When executed, this worm creates a copy of itself in folders such as "%TEMP%", "%APPDATA%" or "%USERPROFILE%" with random file names. The worm also copies itself into the <startup folder>. Once installed, it steals information such as PC name, user profile details, OS version details and more.

VBS/Autorun.LKI

- It copies itself in the "%TEMP%" folder and <startup folder>
- It ensures that it runs every time Windows is started up by creating a registry entry in "HKLM\Software\Microsoft\Windows\CurrentVersion\Run"
- It spreads and propagates through removable drives and creates a copy of itself and a .LNK file within every folder of a removable drive upon detecting a connected drive
- Once executed, it steals information such as OS version details, hardware identification numbers and PC details

TrojanDownloader.Filcout.r5

TrojanDownloader.Filcout.r5 registers and installs itself on a PC by modifying registry entries. When executed, it sends a HTTP GET request to the remote server that is controlled by malware authors. This remote center then replies with a command to download a malicious file. Once this file has been downloaded, it installs other malware into the PC.

Worm.Necast.A3

- It spreads through all the accessible drives of an infected computer whether they are fixed, removable or network drives
- It then drops a copy of itself as "NEW.scr"
- It steals sensitive information and then takes unauthorized remote access and control of a PC
- When executed, it drops a copy of itself at the location "%windir%\Temp\svchost.exe"

WebToolbar.SearchSuite.g6

- It has many malicious traits such as rootkit capabilities to hook into the OS, browser hijacking and displaying pop-up ads which disrupt work

- This PUP (Potentially Unwanted Program) is used for advertising, marketing and to promote products or software
- It enters a PC through freeware such as MP3 converters, doc to PDF converters and more
- It is also bundled within custom installers on many download sites such as CNET, Brothersoft or Softonic from which users get free installers or software

Trojan.Sirefef.gen

- This malware gets installed on a PC through other malware such as the Trojan.Necurs.gen family.
- It drops files such as GoogleUpdate.exe in critical paths like "%LOCALAPPDATA%\Google\Desktop\Install\<GUID>\<Unreadable name>\<Unreadable name>\<Unreadable name>\<GUID>\GoogleUpdate.exe"
- The <GUID> is unique and of a specific size containing alphanumeric series for a given system
- Furthermore, this malware also finds other infected systems within the network

VBS/Serverons.A

- This worm copies itself in the "%TEMP%" folder as help.vbs
- It spreads and propagates via removable drives
- It creates .LNK files and leave a copy of the worm in the targeted path
- Once executed, the worm steals information such as PC name, currently logged in user and more
- The worm also ensures that it is executed every time the PC is started by adding a registry entry into "HKLM\Software\Microsoft\Windows\Current Version\Run"

INF/KIDO.A

- This malware copies itself as a <random name>.dll and creates Autorun.inf files
- It creates its own service with a random name
- It also performs malicious activity such as accessing different websites to infect the system and attacking network hosts with Windows vulnerabilities

Adware.DealPly.r8

This is an Adware that may flood the desktop of an infected system's Windows OS with various online ads, discount offers and savings deals. The Adware is also known to offer various coupon deals or offers through e-commerce and shopping websites.

It also changes the browser settings and adds malicious add-ons without user approval. Default home pages and search engines on browsers are also modified and numerous ads about coupons, discount codes and deals keep getting displayed on the browser. This Adware also spreads through freeware program downloads.

Major Windows Malware in 2014

1 Ransomware

The major challenge of 2014 has been dealing with ransomware. This malware variant usually locks the screen of infected systems or encrypts the data present on machines or both. It has been found that encryption related ransomware has primarily afflicted millions residing in the United States, European nations and some Asian countries.

Ransomware arrives on a system through different mediums such as:

- Email attachments (social engineering)
- Botnet (zbot)
- Drive-by downloads
- Exploit kits (advanced technique)
- Malvertising (advanced technique)

When executed, it performs actions such as memory code injection within genuine processes in order to evade antivirus detection. Malware authors commonly use RSA algorithms to encrypt user data and this data cannot be decrypted without the unique private key, thus leaving the victim with no option other than to pay the ransom demanded. It has also been found that the ransom is usually paid in the form of Bitcoins so as to render the transactions untraceable. Some forms of ransomware also have inbuilt self-destruction capabilities after execution to ensure that security providers cannot get their hands on the malware sample.

Common ransomware families of 2014 were as follows:

- Cryptolocker
- CryptoDefence
- CTB Locker
- Cryptowall
- TROJ_POSHCODER.A
- ".OMG!"
- Ransomcrypt File Encryptor
- ".LOCKED" File Encryptor

Encryption Techniques:

Ransomware samples use different techniques to encrypt data in order to demand payment and they cannot be easily decrypted. Common methods of encryption are as follows:

- XOR Algorithm
- Tiny Encryption Algorithm
- Asymmetric Encryption, which requires a public and private key (advanced technique). Observed uses of different bit lengths of keys are 512, 1024 and 2048.

Some ransomware bring the "Public Key" along with them and then communicate with the remote server for the public key. Remote servers are generated using Domain Generation Algorithm, and this generates random domain names which are available for short durations. In the Malware Author prospect, DGA overcomes the detection of remote servers by security providers.

After the encryption of data, ransomware is used to display a message that states the encryption of data with instructions to decrypt it in localized formats such as time zone, language, current city and more.

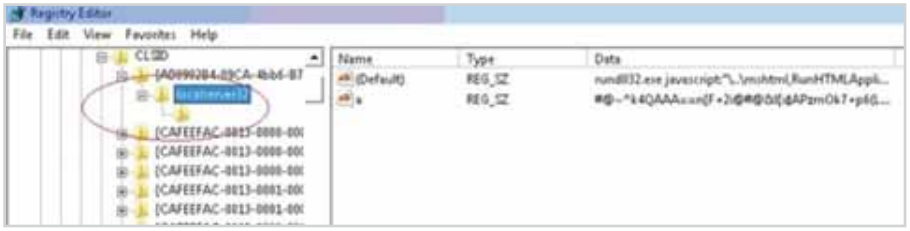
2 Adware(s)

In 2014, Adware has been a major challenge to tackle for security vendors as they routinely plug into web browsers and display context-based ads by overwriting existing visual ads or by inserting new ones on various web pages. Technically speaking, Adware is not a virus but it does actively disrupt user experience once present in a machine. It can hence be classified as an unwanted application/program/file. Adware can hijack the default browser home page and search engine on machines and it can also interfere with systems while browsing the Internet.

Adware usually spreads through malicious URLs over the web and get downloaded and installed on machines without user consent. It also interrupts regular CPU usage and causes the system performance to drop drastically. In many cases, genuine URLs also redirect users to promotional links which leads to a rise in phishing incidents. Moreover, other dangerous malware variants can also use Adware to gain entry into systems or networks.

3 Memory Only Approach – "Poweliks"

The Poweliks malware family uses a 'memory only' approach to attack infected systems. It has been found to enter vulnerable systems through other malware variants or through exploit kits. It functions not by infecting the system with malicious files; rather, it injects seemingly innocent codes into legitimate system processes. This helps Poweliks avoid detection by security software.

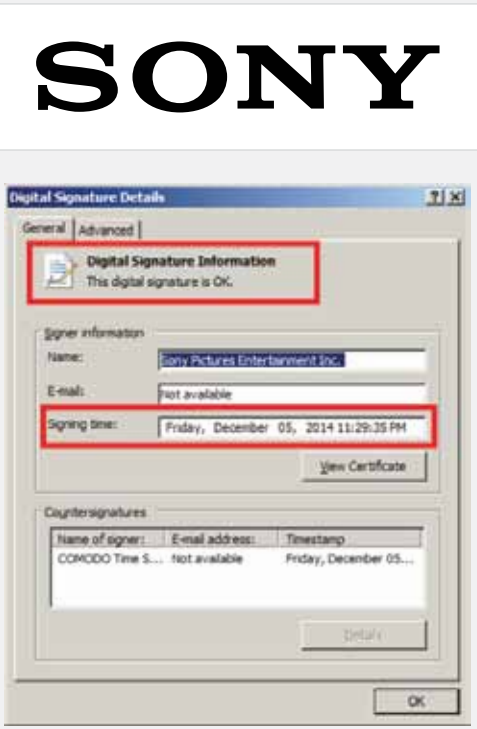


This code is placed into hidden registry keys within infected systems and this ensures that the malware is executed every time Windows is started up. The malware is a JavaScript and PowerShell code. Once installed, steals information about PC details and it also enables the installation of other malware into infected systems.

4 Targeted Attack – "Destover"

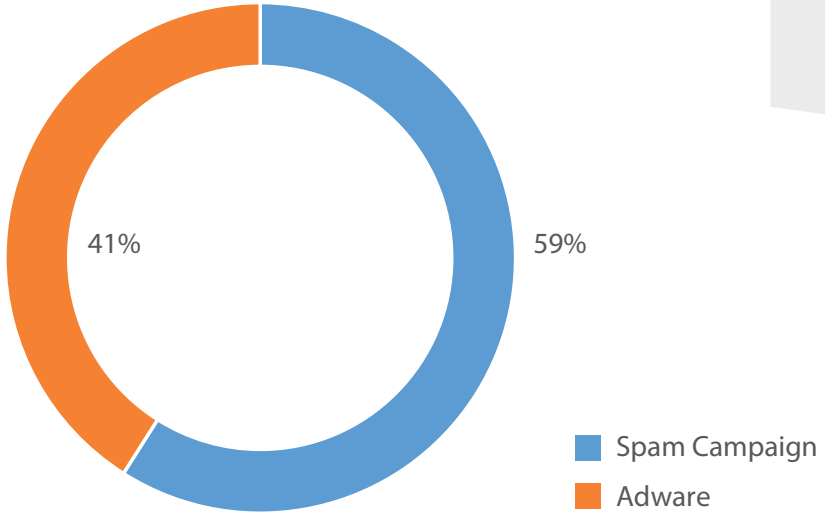
With Sony Pictures Entertainment in the news recently for the severe hack into their systems, this is a good time to speak about Destover. This is a targeted attack that was aimed at Sony Pictures Entertainment and it usually gets installed on a system via a backdoor entry. It then connects to a C&C server through which an attacker gains access into the system. This malware has massive destruction capabilities and can completely wipe out all data from infected machines. It also connects to other systems within the network via port 8080. Additionally, it also performs malicious activities such as deleting all files on the hard drive or shared drive, modifying partition table and connecting to a large number of external IP addresses.

- Destover is a targeted attack on Sony Pictures.
- The Destover family of Trojans has been used in several high profile attacks like this one.
- The new detected sample is unusual in the sense that it is signed by a valid digital certificate from Sony.
- These digital certificates are stolen from Sony Pictures.
- Sony digital certificates ensure the genuineness of files and can help bypass security checks and filters.
- Destover is a particularly damaging form of malware that is capable of completely wiping all data from an infected computer.
- Once installed, it listens in on a particular port (backdoor activity) and once the attacker connects to the infected computer, it may flash different warnings.



When executed, Destover connects to these external IP addresses within range and looks for other systems to infect. This propagates the malware to other systems within the network. Moreover, the malware sample is digitally signed by a stolen Sony certificate to evade suspicion from user's eyes.

Dominant Prevalence of Spam and Adware



Spam Campaign

As per our reports, 2014 has been the most active year for malicious emails containing malware attachments till date. This campaign seems to be going stronger than ever, but the techniques used here are nothing new. Malware authors send emails in huge volumes and these mails contain attachments which appear legitimate but actually contain malicious code such as Trojans, worms or backdoors. Some of the emails also contain malicious URLs which download and install Potentially Unwanted Programs into the system. This inadvertently affects system performance and slows it down as well.

These emails usually contain subject lines like alerts from banks related to credit/debit cards which drive users to open the attachments. This executes the files which in turn affect the entire system and the network. This opens a backdoor into the system for attackers and they can install malware and other dangerous files into the system.

Adware(s)

Adware is a software and bundled program that supports online advertising by displaying continuous pop-ups of visual ads in order to generate revenue for product sellers. The use of this software for business is increasing tremendously and social networking sites such as Facebook and email services such as Gmail are also playing a huge role in this development. However, it is very difficult for users to differentiate whether installed advertising software is legitimate or not. This leads to millions of users getting exposed to attackers.

Though Adware is not the same as a virus, it usually presents unwanted ads and pop-ups on a PCs screen. This worsens the user experience of an individual while browsing the Internet and this software usually gets installed on a machine without the user's consent. They could potentially steal personal and financial information. Or they could also be malvertisers that spread malware rapidly. All in all, online advertisements provide a reliable platform for spreading malware.

Upcoming Trends for Windows Malware in 2015

Ransomware with different propagation techniques

Ransomware is expected to get stronger in 2015 and improvements in encryption techniques will also make recovery harder. It is increasingly likely that ransomware could drop other malware components addition to performing system encryption on infected devices and steal financial information. Ransomware can connect to remote C&C servers and this also enables them to add PowerShell code to infected systems.

Adware continually on the rise

Advertising software is in huge demand in the online world and the demand for this is expected to grow as it generates revenue for products services online. Keeping the primary purpose of advertising in mind, it becomes difficult for users to differentiate between which software is legitimate and which is not. A spyware or malvertiser can easily get downloaded and installed into a machine via legitimate software. Adware is risky as it can drop malicious files, steal sensitive information. We expect malware authors to take maximum advantage of these characteristics in 2015.

3

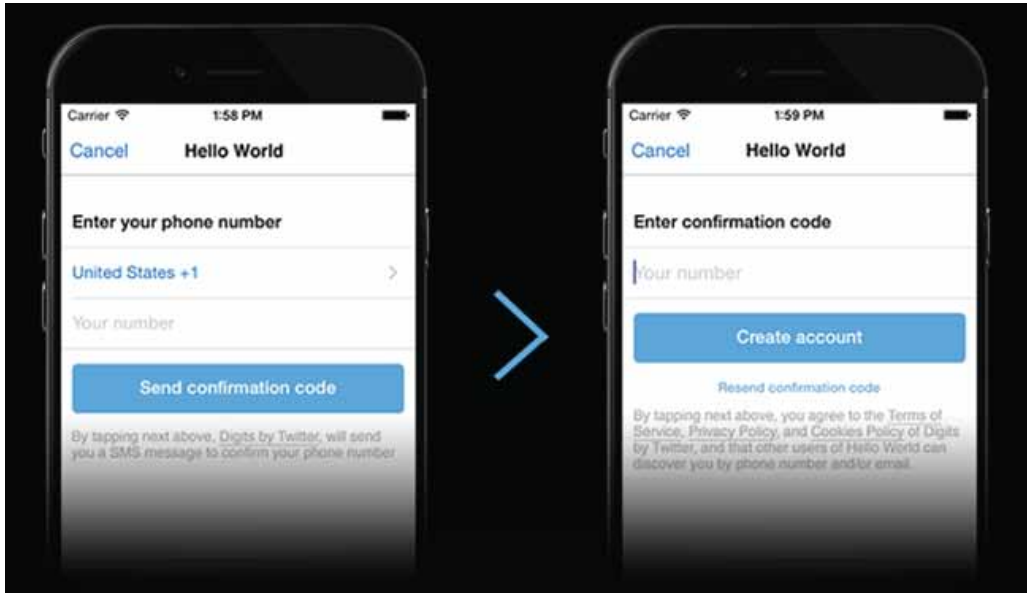
Advanced Persistent Threats (APTs)

APTs have recently surged in popularity and usage and 2015 is expected to be the year that these tools come to the fore. APTs easily attack a network and gain unauthorized control and their primary intention is to steal data silently. In such a scenario, the network is not harmed by this threat, but is continuously monitored so that crucial data can be extracted. The most common targets of APTs are national defense bodies, manufacturing industries and financial institutions. APTs regularly use a social engineering trick known as spear fishing in order to gain access to networks. If the attack is successful, the attacker establishes a backdoor entry and begins gathering data such as user credentials and sensitive data and also starts spreading over the network.

Noteworthy posts from the Quick Heal Blog

Your passwords are on the way out, leave it to Twitter 1

If there is one thing we could change about the Internet today, it would most certainly be the dissolution of the need for passwords to access web-based accounts. An average Internet user today has around 10 passwords that he needs to remember at all times. Moreover, these passwords need to be unique, hard to remember and mutually exclusive.



Empower your users to sign up into your app in two simple steps

However, as most people can vouch for, a majority of users do not follow these rules. Remembering 10 different passwords with a mix of special characters, numbers and the like is a highly demanding ritual. What this leads to is a situation wherein people use the same password, or some variant, for their multiple accounts. This leaves them vulnerable to hack attacks and social engineering tricks. With all the advances that the tech world has seen recently, it is surprising that we still rely on something as archaic as a password to access our personal accounts. It's about time we saw some changes here and thankfully, steps are being taken in order to rectify this outdated conception.

"Digits" is a new development tool offered by Twitter that allows people to sign in to their apps using their mobile numbers, and thankfully this has nothing to do with passwords. With the help of Digits, an API developer can enable an end user to receive a one-time authentication code on his mobile phone every time he wishes to login. Embedded within Twitter Fabrics, Digits is a standalone tool that can be used by developers to make their apps safer, better and more lucrative. Sure this may sound a bit tedious, but the benefits are easy to see. A user will never need to remember his password. Instead, he will simply punch in the authentication code that he receives on his phone.

Heartbleed takes the online world by storm 2

Password leaks and targeted attacks are nothing new and the latest security bug related to a massive loss of passwords across the world is 'Heartbleed'. This bug has received a lot of media coverage over the last few months, so there is a lot of confusion about what it is and what one needs to do to fix the issue.

Heartbleed is a security bug that affects servers that use OpenSSL (Secure Sockets Layer) technology. When you log in to your email account, or make a financial transaction online, the server that hosts this activity is protected by the SSL technology, which is denoted by the symbol of the padlock near the address bar and the unmistakable presence of "HTTPS" as a prefix of the URL itself. Heartbleed is a bug that afflicts this very protective measure and exposes information that SSL attempts to protect. What this means then, is that sensitive information like passwords, credit/debit card details and more are susceptible to this bug and can be stolen. This also means that there is nothing wrong with your PC or your antivirus software. This is an issue that needs to be dealt with by the people who run the websites that make use of SSL. Moreover, if you are surfing the Internet you will not be able to tell if a service you are using is affected by Hearbleed or not.

Beware of the Poodle bug 3

There's a new security bug in town. Technically, it is called CVE2014-3566, and elsewhere, as the Poodle Bug. Three Google engineers have discovered this security vulnerability in SSL version 3. SSL (Secure Sockets Layer) is an encryption service that keeps your Internet communications (such as your connection to your bank's website, online shopping site, etc.) private and from getting into the wrong hands.

SSL 3.0 is an 18-year old technology. Although stronger encryption technologies such as TLS (Transport Layer Security) are now in force, SSL 3.0 is still used in 1% of web traffic, and supported by 95% of web browsers. Coming to POODLE, it stands for 'Padding Oracle On Downgraded Legacy Encryption'. It is a security flaw that exists in SSL version 3. Under the right conditions, the POODLE bug can allow an attacker to access your session cookies. With this information at hand, an attacker can take control of your online accounts including your email, banking and social networking account. Now all this may sound scary, but the POODLE bug is not as threatening as Heartbleed or Shellshock that took the Internet by storm. It is harder to exploit.

Looking ahead to 2015, the diversification of devices, the Internet of Things (IoT) and the device agnostic feature of malware are security threats to look out for. As malware authors and attackers get more sophisticated and extreme in their targets and methods, end users need to be more aware and proactive than ever before. Social engineering and spear phishing are now things of the past, though still hugely prevalent. New-age threats such as ransomware and adware are the security dangers to be forewarned against.

As the future unfolds, home users and enterprises need to be aware about the security risks of unsecured Wi-Fi networks, Advanced Persistent Threats (APTs) and attacks over cashless Point of Sale systems and online banking applications. With the constantly evolving threat landscape constantly hovering over the horizon, it is essential to take adequate steps to ensure consistent and foolproof IT security with the right tools and practices.

Conclusion