Quick Heal
Security Simplified

Quarterly Threat Report

Q1, 2015

How adware has become device agnostic over Windows &Android

www.quickheal.com

Threat Report:

1st Quarter, 2015

Contents

Summary

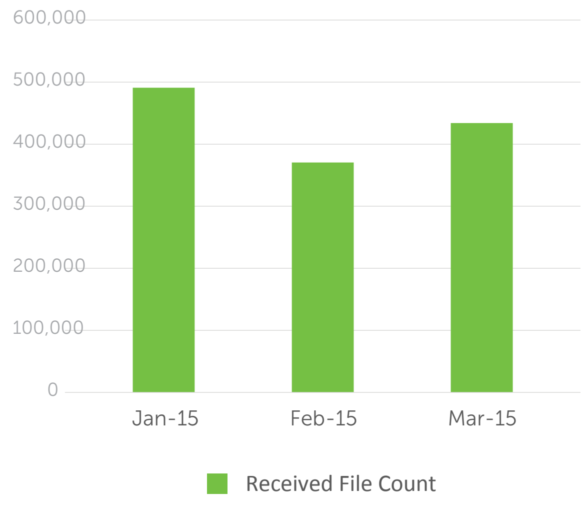
The first quarter of 2015 has been very eventful for security researchers, analysts, and the IT security industry as a whole. The Windows malware charts were again dominated by the Adware family, whose propagation has increased tremendously with increased usage of free software downloads over the Internet. The growing number of Adware has also resulted in swelling up the attack rates of "Malvertising" (malicious ads for spreading infections). Ransomware is another family of malware which has not shown any sign of recess. It has, in fact, shown signs of becoming more sophisticated and deadlier with time. Android is also vulnerable to Adware, while other threats such as ransomware and fake apps have also now come to the fore. This was followed by breaking news of the malicious 'Superfish' Adware that came preinstalled in several Lenovo laptops. The Q1 threat report will shed light on these malware trends and other notable information about malware on the Windows and Android platforms.

Android Malware Collection by Quick Heal

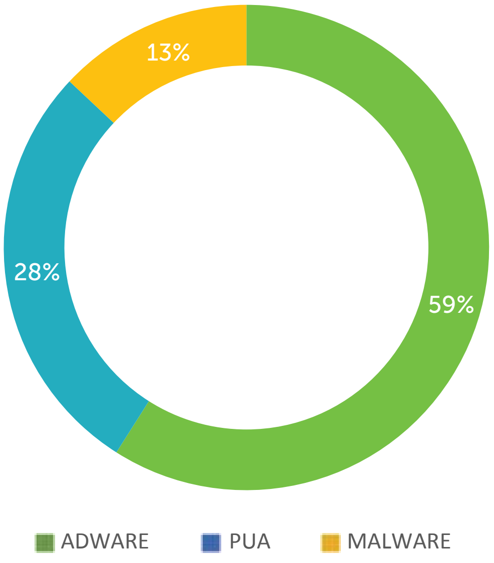
The exponential growth of Android malware that has been witnessed in the recent past has continued in the first quarter of 2015 as well. This comes as no surprise to the IT security world as these are trends that we have predicted and been prepared for since a while. While there have been several new strains and attack vectors that have been discovered recently, the overall methods of Android malware and the tricks they use have remained the same.

In the first quarter of 2015, the Quick Heal Threat Research Labs have found 158 new families of Android malware and these include several strains of Potentially Unwanted Applications (PUAs) and Adware as well. The labs have also discovered a further 212 new variants of existing Android malware families.

Android Samples Received – Q1, 2015



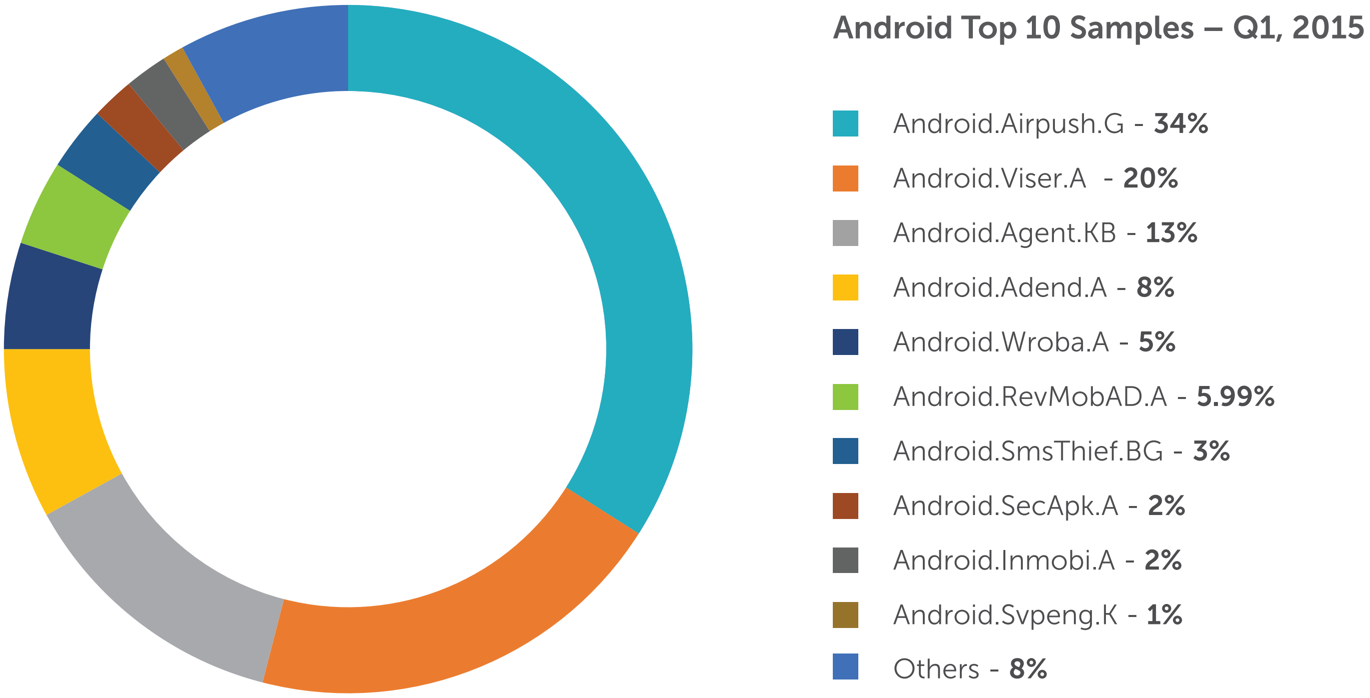
Android Category Detection – Q1, 2015



Top 10

Android Malware

Android Top 10 Samples – Q1, 2015



Android.Airpush.G

This Adware enters systems with bundled software and aggressively pushes ads to the notification bar of infected devices. It can also add desktop shortcuts of these ads. It also has the capability to modify browser bookmarks and change the homepage appearance. It also steals the following information:

- IMEI number and details
- Device location
- Name, device type and device OS version

Android.Viser.A

This is a dominant Adware that has been around for many years and the first quarter of 2015 has been no different. It has the ability to create unwanted icons on the homepage of devices. It also displays unwanted ads and changes the bookmarks of browsers. The Adware also collects the following information:

- Device location
- IMEI number

Android.Agent.KB

This Trojan has the capability to abort all incoming messages to a device. After installation, it can also collect private information of the device and send it to certain numbers via text messages. It collects and sends the following information:

- Device ID
- Subscriber ID
- SIM card serial number
- Device location

Android.Adend.A

This Potentially Unwanted Application (PUA) comes up as a theme launcher in many third-party stores. It also shows up as a widget on the homepage and clicking on that widget may prompt the user to download other malicious applications. Once downloaded, it can change the theme and settings of the device. It also changes the local language of the device to Urdu. It also collects the following information:

- IMEI details
- IMSI details

Android.Wroba.A

This malware family has been known to target banking apps of Korean users by displaying itself as 'Google Services'. It then requests for admin privileges. Once this has been done, it can intercept incoming SMS messages on the device. It can also steal the following information and forward the information to a remote server:

- Device ID
- Contacts list
- Incoming SMS's
- Installed app information
- Login credentials for bank accounts and banking information

Android.RevMobAD.A

This Adware comes affiliated with an ad plug-in. It displays several unwanted ads to an infected device and can also send out personal information to several servers. It collects the below mentioned information from devices:

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

Android.SmsThief.BG

This is a highly potent malware that hides its icon from the menu once it has been launched for the first time. It requests for device administrator privileges and it reports status (enable/disable) to the malware author via SMS. It silently forwards all incoming messages to the malware author.

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 app developers to prevent the tampering or decompiling of their apps. This technique makes reverse engineering very difficult and malware authors use this to stay undetected. Hence, Quick Heal detects apps that use this protector under the Potentially Unwanted Application category as a precautionary measure.

Android.Inmobi.A

This detection comes under the Adware category and displays unwanted ads. It contains several ad libraries and also collects the following user information:

- IMEI details
- Display advertisements

Android.Svpeng.K

This malware commonly targets banking applications and steals login credentials of online banking accounts. It can also search for specific mobile banking apps on infected devices and then lock the device and demand payment for unlocking the device (similar to ransomware). This app has been seen to mainly target Russian users. It can also break into devices through social engineering campaigns using text messages.

Popular Strains of Android Malware in Q1

1

Hijacking the device makes the user believe the phone is switched off

Android.Hijoff.A

This Android malware hijacks the shutdown process of an infected smartphone. It displays a fake shutdown dialog box when the power button is pressed and also shows a fake shutdown animation. Once the user of the device believes that the phone is off, the malware silently works in the background to make calls and send text messages. The malware also has the capability to ask for rooting permission and can inject its malicious code into the operating system's server. This is a rather innovative attack technique.

2

Claims to give Amazon rewards and vouchers to trick users

Android.Gazon.A

This unique Android malware poses as a valid application that grants Amazon rewards and other discounts and vouchers for Amazon purchases. It redirects victims to specific URLs which are malicious in nature and also downloads risky apps from fake domains. It also tricks users into visiting URLs on the pretext of offering Android games for download. Furthermore, it collects contact details from phonebooks and spreads itself via text messages or social networks.

3

Fake Google Play app that pushes ads which resemble system notifications

Android.MobiDash.A

This particular strain comes under the Adware category and it displays pop-up messages that resemble system notifications on Android devices. This app was active on Google Play for some time and it was downloaded by many users. As of now, this app has been removed from the Google Play store. The Adware also pushes ads when the device is unlocked or the app is restarted. In order to remain unnoticed, the Adware uses a timer to show its activity.

Upcoming Trends
for Android Malware

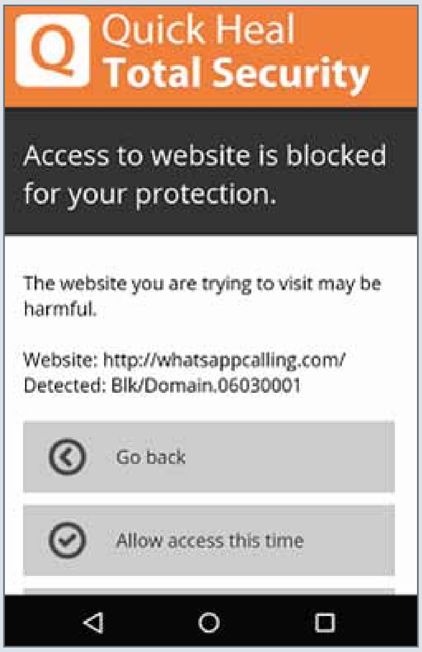
Targeted attacks on banking credentials and data

We are expecting further attacks on banking credentials in the coming months. Our threat research team has discovered 6 new variants of such attacks in the first quarter of 2015 and we expect this trend to continue. These attacks can be achieved through the auto login feature of mobile apps and banking websites which are designed to help users gain faster access. In order to intercept this critical information, attackers will increasingly target mobile devices for broader credential stealing or authentication attacks in the future.

Malware attacks on social networking and chatting apps

Social engineering is a broad term that implies tricks and techniques used by hackers to convince victims to voluntarily give up critical information. These tricks can range from fake phone calls, emails or texts, to phishing pages that fool users into filling up their personal details and sharing them voluntarily. Private information of users is expected to be at serious risk from such social engineering tricks in the upcoming quarter of 2015.

WhatsApp calling feature is used by spammers to spread phishing attacks.



Quick Heal Total Security

Access to website is blocked for your protection.

The website you are trying to visit may be harmful.

Website: http://whatsappcalling.com/
Detected: Blk/Domain.06030001

Ransomware and crypto-ransomware continues to propagate

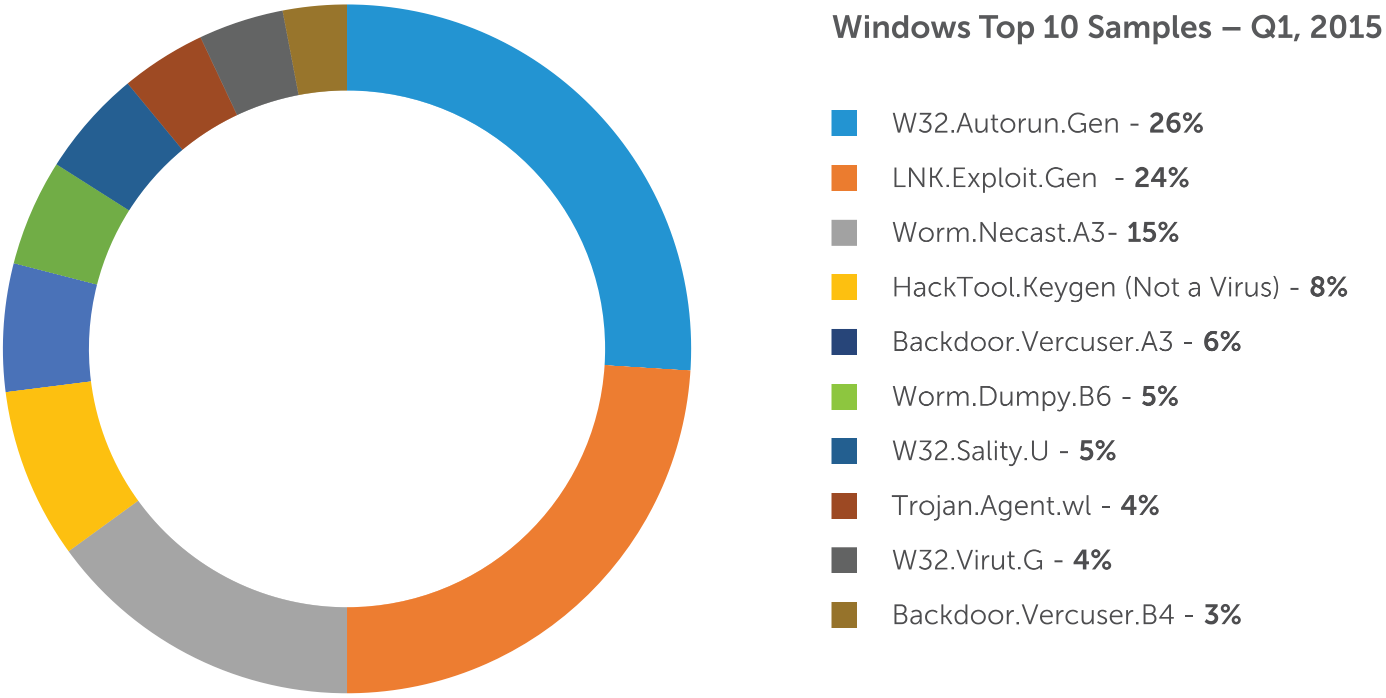
Ransomware and crypto-ransomware are serious threats that are not going to go away anytime soon. We expect several new variants of ransomware to arise in 2015. Most of these samples will utilize tricks that have been commonly used by Windows malware. In the first quarter of 2015, our threat research team has discovered 4 new variants of the popular ransomware "Android.Simplocker".

Continued dominance of Adware on Android devices

Adware has been a leading source of malware on Android devices for the last few years and this pattern will continue in 2015. Adware variants are not going anywhere and they are expected to evolve further and persistently play a leading role in the Android ecosystem. In the first quarter of 2015, we discovered 17 new Adware families and this indicates the upward curve of Android Adware in the future.

Top 10

Windows Malware



Windows Top 10 Samples – Q1, 2015

W32.Autorun.Gen

Family: Autorun Worm

Propagation: The worm can spread to other PCs by infecting removable drives such as USB drives or portable hard disks or network.

How it works: The worm copies itself to the root of the drive, then creates or modifies the autorun.inf file (a text file that can be used by the AutoRun and AutoPlay components of Microsoft Windows operating systems), instructing it to run the dropped worm each time the drive is accessed. When the targeted system is infected with this worm, it then looks for similar drives and propagates its infection. W32.Autorun.Gen is the detection of infected .inf files which are used by worms for spreading to local, network, or removable drives.

LNK.Exploit.Gen

Family: Adware

Propagation: Spreads via malicious websites.

How it works: LNK.Exploit is a windows vulnerability that allows malicious shortcuts to run automatically whenever the shortcut’s folder is viewed in Windows Explorer. It is an adware that displays unwanted pop-up ads, advertisement banners and sponsored links within browsers. The exploit is used by worms, rootkits, and Trojan horses. This malware can:

- Compromise your PC and may result in additional infections triggered by rogue software
- Redirect you to unsafe websites or display fake advertisements
- Slow down your PC
- Delete or rename files and folders on your computer

Worm.Necast.A3

Family: Worm

Propagation: Spreads via malicious websites, free software, and spam emails.

How it works: The malware runs as a self-contained program or as a set of malign procedure. It takes advantage of network connections to form its copies and spread parts of itself into other computers. Due to its sophisticated build and dynamic characteristics, it manages to evade detection and auto-removal by security software. The worm is also designed to exploit system vulnerabilities so that it can drop and install additional threats such as Trojan, keyloggers, fake antivirus programs, and even ransomware on the compromised system.

HackTool.Keygen

Family: Malicious Window platform tool

Propagation: Spreads via untrusted websites.

How it works: This is categorized as a malicious Windows platform tool that generates keys for illegally/illegitimately-obtained software. Although not a virus in itself, this tool can make a system vulnerable to remote attack by hackers. The tool is also known for downloading harmful files and affecting the performance of the system it is installed in.

Backdoor.Vercuser.A3

Family: Backdoor

Propagation: Spreads via free software and online gaming websites.

How it works: The malware is designed to conduct distributed denial of services (DDoS). It changes the infected system's security settings, disables firewall to open a backdoor for other infections. Once installed, the malware configures itself to start automatically when the Operating System is loaded. It also tries to intimidate the user by displaying false infection threats in the form of multiple pop-ups and fake system notifications.

Worm.Dumpy.B6

Family: Worm

Propagation: Spreads via removable drives, software exploits, or network vulnerabilities.

How it works: The worm attempts to connect to preconfigured webservers using a set of usernames and passwords that are embedded in it. When a user starts a web browser and visits specific websites, this worm constantly redirects them to other random websites, causing nuisance while browsing the Internet.

W32.Sality.U

Family: Polymorphic virus

Propagation: Spreads via spam email attachments, freeware, online file sharing, and infected external storage devices.

How it works: The virus infects executable files having .exe and .scr extension on local, removable and remote shared drives. The virus also creates a peer-to-peer (P2P) botnet and receives URLs of additional files to download. It is also designed to disable security software installed on the infected system.

Trojan.Agent.wl

Family: Trojan

Propagation: Spreads via malicious websites, pop-up ads, and infected email.

How it works: An infection by this Trojan results in poor system performance, system errors and frequent crashes. This could result in loss of important data. The Trojan can also download other malware and third party software on the infected machine. It also makes changes in the registry to hide its presence. Trojan.Agent.wl is also designed to steal confidential information such as stored email and ftp login details, passwords, credit card details, bank account information etc.

W32.Virut.G

Family: Virus

Propagation: Fixed, removable and network drives.

How it works: The virus infects .exe, .ASP, .HTML, and .PHP files. It opens a backdoor that allows a remote attacker to perform illicit operations on the compromised computer. The backdoor operates with the help of Internet Relay Chat (IRC) with communication encrypted both ways. It also allows the remote attacker to address compromised computers individually or as a group.

Backdoor.Vercuser.B4

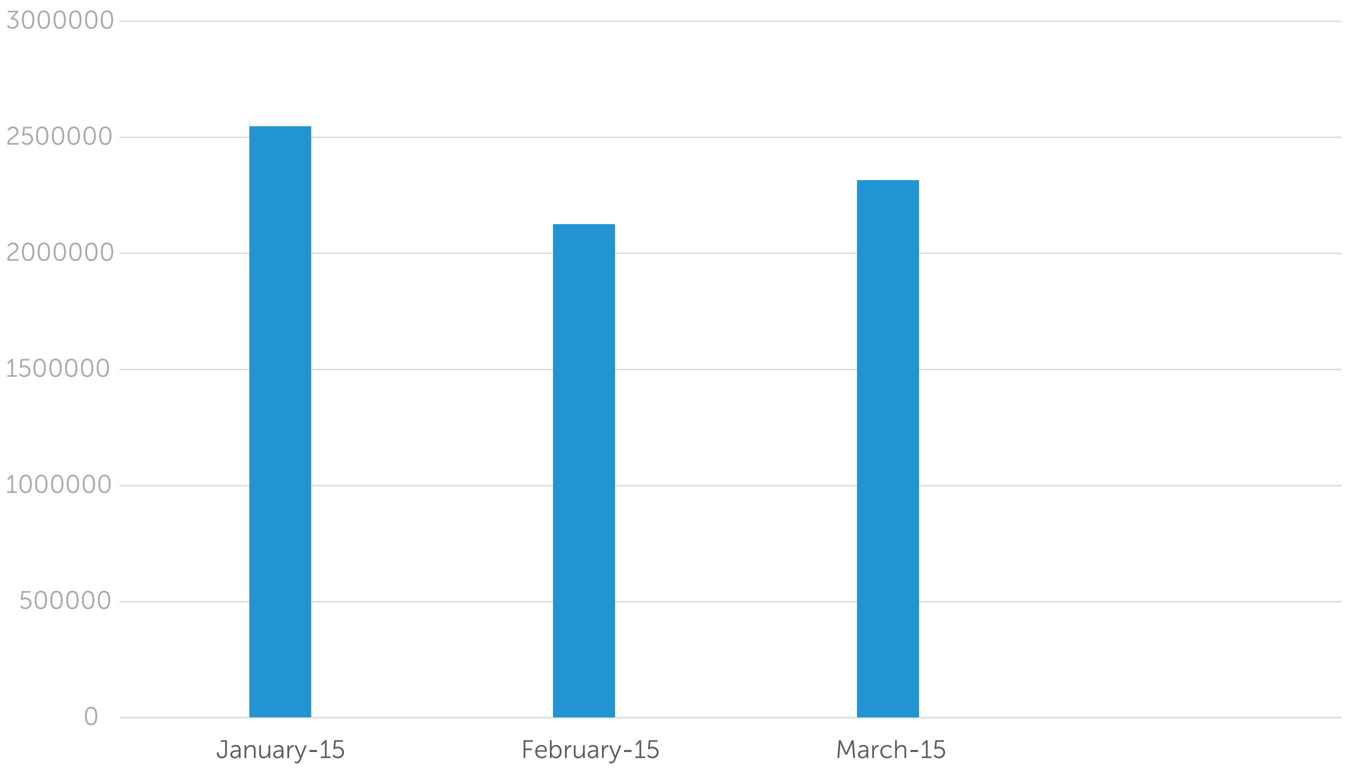
Family: Backdoor

Propagation: Spreads via free software and online gaming websites.

How it works: The malware is a variant of Backdoor.Vercuser.A3 and shares the same characteristic features.

Windows Malware Collection
by Quick Heal

Month	Jan-15	Feb-15	Mar-15	Total
Count	25,33,621	21,03,421	23,97,656	**70,34,698**



Major Windows Malware

Adware - The Unwanted Promotion Specialist

- In the first quarter of 2015, the Adware family continued its dominance. Adware is a software that displays advertising banners and re-directs users to websites. It is often bundled within a legitimate software. Software developers, at times, include advertising functionality (adware) in their software to recover development cost.

- An adware can track details of the user's Internet usage and send this data back to the author. This information is used to deliver specific advertisement based on the user profile.

- Malvertising is another threat that has grown alongside Adware. It is defined as the practice of use of online ads to deliver malware to targeted users.

The Top 5 Adware

- Morstar
- DriverUpd
- SoftPulse
- MultiPlug
- Updater

Ransomware - The Menacing Malware

Ransomware continues to be an extremely aggressive and destructive malware for Q1 2015. 'Cryptowall' and 'CTB Locker' are two previously reported and majorly distributed ransomware that came back with new variants. Their primary medium of propagation remains spam emails.

Below is the list of file encrypting ransomware seen in Q1 2015:

- Cryptowall 3.0
- CTB-Locker
- Ransom.Gulcrypt
- CryptoFortress
- TeslaCrypt
- BandarChor
- CryptoTorLocker2015

Sophisticated Propagation Techniques

Cybercriminals are coming up with more sophisticated ways of propagation and evasion techniques for ransomware attacks.

The recent wave of ransomware has been noticed to have used different tactics to spread via emails and evade heuristic detection by antivirus software. The CTB-Locker, also known as 'Critoni', is one such ransomware. Previously, CTB-Locker came in spam emails as attachment in .ZIP or .RAR format. Now, it comes in .CAB file containing a downloader with .SCR file. Even though these CAB files are not self-extracted archive, users extract the .CAB files manually and execute the malware mistaking it to be a legitimate application, which then downloads the ransomware on the system. Another variant of CTB-Locker has been noticed to use Social Engineering tactic in the form of a malicious email campaign called "Google Chrome update Spam". The fake email message states, "Your version of Google Chrome is potentially vulnerable and out of date. Download new version". For this, the email instructs the user to download a file called "ChromeSetup.exe", which is actually the carrier of the CTB-Locker ransomware.

Ransomware that Encrypts Saved Game Files

Till now, ransomware were targeting important data such as word docs, excel files, PDF, videos, images, PowerPoint files, etc. TeslaCrypt is a new breed of ransomware that targets more than 30 game applications. It searches for saved game files of popular video games (such as Call of Duty, Diablo, Fallout, Minecraft, Warcraft, F.E.A.R, Assassin's Creed, Resident Evil, World of Warcraft, League of Legends, and World of Tanks) and encrypts them (converts the files into a cod). The ransomware then demands a ransom to release a private key which can decrypt these files.

TeslaCrypt is known to spread from websites built using WordPress. Such sites redirect visitors to a malicious page hosting Angler Exploit Kit. This drops the ransomware by exploiting any vulnerability present in older versions of Internet Explorer or Flash Player.

Old Ransomware with New Techniques

A new version of the CryptoWall ransomware, detected recently, uses phishing emails containing a malicious .CHM (Compiled HTML) attachment as an infection vector. Most email filters allow such attachments to pass, which makes this particular ransomware an aggressive malware that can easily infect its target's system. This kind of attack, however, has not been seen to affect a huge number of people. But, this only proves that hackers are trying new methods to evade detection.

Necurs - The Rootkit

Necurs rootkit was first spotted in early 2011 and made the headlines for its stealth functionality. A new variant of this rootkit has been spotted in this quarter. It has been introduced with modifications that makes it more resistant to removal.

Necurs installs itself as an auto-starting Windows service to run automatically after the system restarts.

In its previous version, this rootkit created an unique object named 'Ntsecuresys' which is used as an infection marker to identify its presence in the system.

Case Study -
Lenovo Superfish Vulnerability

What is Superfish Vulnerability?

A software known as Superfish Visual Discovery was pre-installed on Lenovo laptops shipped between September 2014 and February 2015.

The Superfish software was designed to push ads in Google search results and websites to help users find and discover products visually. However, it was discovered that the Superfish software was installing its own self-signed Root Certificate Authority.

The Superfish software had the ability to intercept supposedly-secure communications "HTTPS" via a man-in-the-middle (MITM) attack. In other words, the software had HTTPS-breaking technology that gave it malware-like capabilities. This in turn, exposed users to a hijacking technique by intercepting and decrypting HTTPS connections, tampering with pages and injecting advertisements.

Hackers on the same network such as open Wi-Fi hotspots can easily exploit the Superfish software to steal information such as banking login details or to read the victim's emails.

How does Superfish Work?

This software was designed to intercept users' web traffic to serve them with targeted advertisements. In order to intercept encrypted connections (using HTTPS), the software installs a trusted root CA certificate. Security certificates tell your computer which websites and software can be trusted. They are important for your online security, and for establishing secure connections with secure websites. Trusted websites with secure communication display a padlock in the browser address bar.

All browser-based encrypted traffic to the Internet can be intercepted, decrypted and re-encrypted by the Superfish software, which is a classic man-in-the-middle (MITM) attack. Private key (part of Public Key-Private key combination of Asymmetric Encryption algorithm) used for encrypting communication with actual server could be easily recovered from the installed Superfish software, which creates a bigger security loophole. The attacker can generate a certificate for any website that will be trusted by a system with the Superfish software installed in it. Hence, even secure banking websites, and email sites can be spoofed without showing any type of warning from the web browser.

Conclusion: Systems having the Superfish Visual Discovery software installed is vulnerable to SSL spoofing attacks. Superfish uses a vulnerable SSL decryption library by Komodia; other applications that use the library are also similarly affected.
The good news is, Lenovo has discontinued the practice of pre-installing Superfish Visual Discovery. The company has also provided a list of the affected laptop model versions.

Upcoming Trends for Windows Malware

Adware - More focus on data leakage

We have seen how adware pre-installed on systems could cause serious privacy and security issues, as seen in the previously discussed Superfish case. As advertising software have huge demands in the online world, malvertising is certainly a growing threat. And this is expected to result in more financial frauds and leakage of personally identifiable information which will in turn, result in higher security risks.

Ransomware - Challenge for Security Software

Ransomware are getting more sophisticated and nefarious in their techniques to propagate in the wild, file encryption methodology, and hide from antivirus software. This malware family is also expected to take more advantage of social engineering tactics.

It is highly probable that ransomware will also try to steal login credentials for online backup services and will encrypt the data which is backed up in cloud storage. This would add much more value to the hackers as such attacks will result in higher monetary returns.

Advanced Persistent Threats (APT) also known as Targeted Attacks

Targeted attacks are increasing and showing no signs of recess. APT attacks on government bodies, businesses, educational institutions, banking and financial services, defense sectors, and healthcare institutions will continue to rise. Cybercriminals will continue to attack (PoS) point of sales, as seen in the infamous Target breach. Cyber espionage will increase to steal sensitive information and data privacy will be in the red zone.

Conclusion

While malware over Windows and Android has constantly been evolving and growing in numbers, there are several trends now which have become the norm. One of these is the dominance of Adware over both platforms. The other is the prominence of ransomware and social engineering tricks. A lot of security threats are now showing up over both platforms simultaneously since the lines of device usage have almost disappeared. This makes it harder for IT security solutions to combat device agnostic threats and malware.

It is essential to evolve tools and techniques to combat such security risks and to stay one step ahead of malware authors at all times. For that purpose, the Quick Heal Labs and R&D team is constantly at work to detect new security risks and to devise preventive technologies