Quick Heal
Security Simplified

Quarterly Threat Report

Q2, 2015

Advanced Point of Sale (PoS) malware threatens sensitive card data

www.quickheal.com

Threat Report:

2nd Quarter, 2015

Contents

Summary

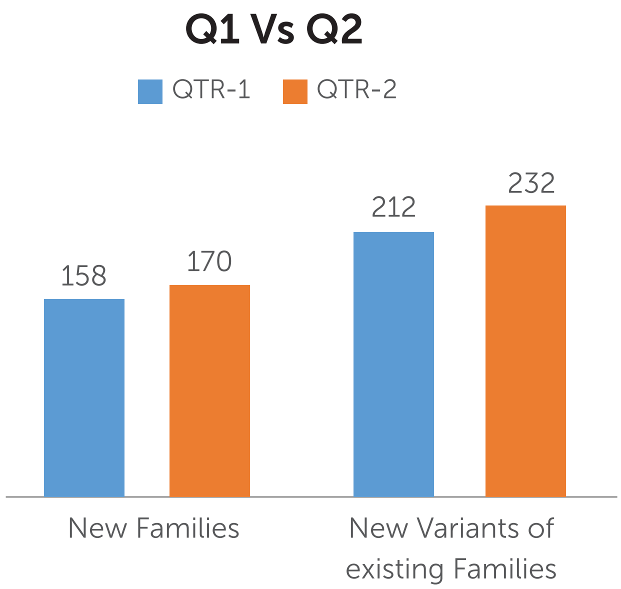
The second quarter of 2015 has seen a rapid growth in the malware collection and detection figures by the Quick Heal Threat Research Labs. This growth has been especially higher for the Windows section. Additionally, this in-depth report offers a detailed look into the top malware samples that afflicted the popular computing platforms – namely, Android and Windows. The report also sheds light on the upcoming security trends and predictions for these platforms. With 17 million customers in more than 112 countries worldwide, Quick Heal receives real-time global virus signature updates for desktops and mobile devices over multiple platforms and operating systems and this data will be explored further here.

Android Malware Collection by Quick Heal

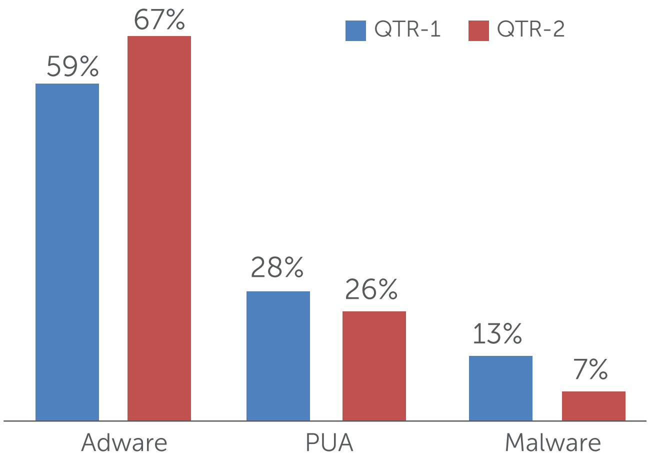
In the second quarter of 2015, Android malware families and variants of existing families have seen a comparatively lesser rise in their numbers. The Quick Heal Threat Research Labs have carefully studied these samples and noted that this trend indicates that people are adopting more security measures to protect their Android smartphones and tablets.

For the months of April, May and June 2015 we have detected 170 new families of Android malware and these samples include several strains of Potentially Unwanted Applications (PUAs) and Adware samples as well. Furthermore, 232 new variants of existing Android malware families have also been detected.

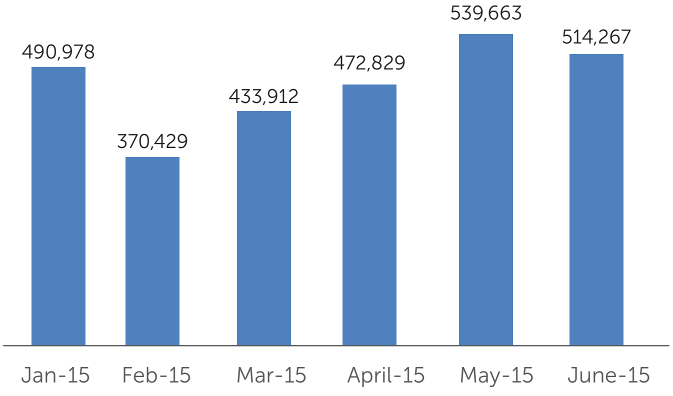
Comparison of malware families between Q1 and Q2 2015:



Comparison of Android category detection between Q1 and Q2 2015:

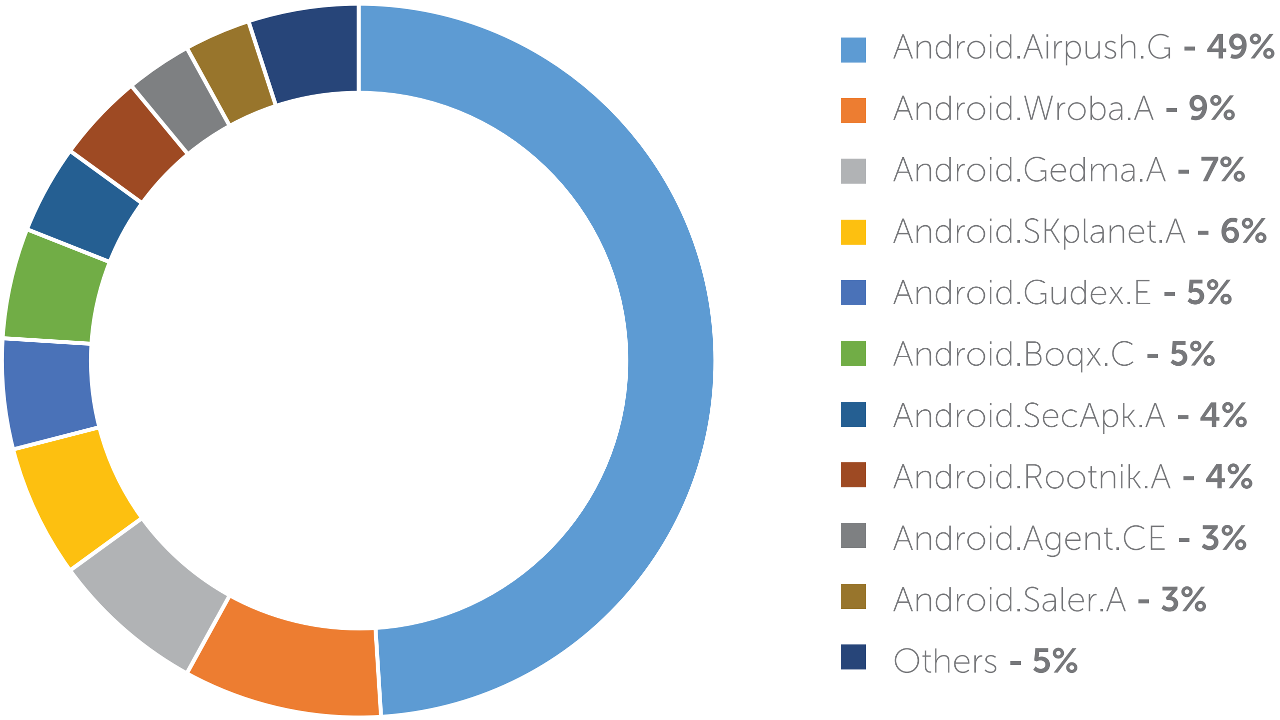


Samples received by Quick Heal Threat Research Lab:



Top 10

Android Malware



Android.Airpush.G

This Adware aggressively pushes ads to the notification bar of all infected devices. It also has the capability of adding desktop shortcuts of these ads. In most cases, this Adware enters Android devices through bundled software and gets installed as a part of it. It is also capable of modifying browser bookmarks in the device and changing the appearance of the homepage. It also steals the following information:

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

Android.Wroba.A

This family of Android malware mostly targets Korean online banking applications and their users. After installation, this application appears as a fake “Google Play Store app” or as “Google Services”. It immediately requests administrator privileges as well. It also performs the following tasks on devices by replacing legitimate banking apps with fake ones:

- Siphons device ID and contacts list information
- Steals user data like phone numbers, incoming messages and more
- Monitors installed applications

- Tries to gain login credentials for bank accounts and other banking information

Android.Gedma.A

This malware variant commonly targets users residing in China. After installation, this application compromises user devices and steals private information from them. The following stolen information is then transmitted via SMS to malware authors:

- IMEI details
- IMSI details
- Device name and type

Android.SKplanet.A

This Adware category application is a high-risk ad plugin that can compromise devices. It can also steal the following user details and perform the following activities:

- SIM serial number
- SIM card status
- Phone number
- Map geo-location data

Android.Gudex.E

This malware usually poses as a pornographic application before a user installs it on a device. It also makes use of complex protection techniques that make reverse engineering and analysis very difficult. The malware also has the potential to perform the following tasks:

- Send SMS to premium-rate numbers without user consent
- Read contacts
- Read all call logs and history
- Send all personal details and device details to the malware author

Android.Boqx.C

This application falls under the malware category of Android variants. In addition to the malicious activities that it is capable of performing on infected devices, it downloads and installs other malicious Android applications on compromised devices.

Android.SecApk.A

This is a Potentially Unwanted Application (PUA) that uses the “Bangcle” Android application protector to afflict Android devices. This protector is commonly used by Android application developers to prevent the tampering or decompiling of their apps. With the help of this technique, reverse engineering of apps is very difficult and this enables malware authors to remain undetected. As a result, Quick Heal detects Android apps that use this protector under the PUA category as a precautionary measure.

Android.Rootnik.A

This malware comes bundled with genuine apps over third-party sources and it has the ability to root infected Android devices. It can also perform the following activities:

- It mounts system partition
- It loads native libraries
- It takes admin privileges after rooting and thus voids device warranty
- Sends device information to a remote server
- Steals IMEI and IMSI numbers
- Accesses the camera application
- Gathers device location data

Android.Agent.CE

This application falls under the Trojan category and it can intercept and abort all incoming messages to an infected device. After installation, it also steals the following private information from the device:

- Device ID
- Subscriber ID

- SIM serial number
- GSM cell location
- It also sends SMS messages to certain numbers

Android.Saler.A

This is another Android malware variant that falls under the Trojan category. It installs a fake app on the device that is known as “SaleRecord”. After installation, it hides itself from the home screen of the infected device. The malware gets executed every time the device is booted or restarted. It can also send premium-rate messages at regular time intervals. Additionally, it also collects and sends the following information:

- IMEI and IMSI numbers
- SIM serial numbers (ICCID number)
- Device ID details

Upcoming Trends for Android Malware

1

BYOD policies to be targeted in the next quarter

Bring Your Own Device (BYOD) policies have now allowed enterprises to manage the ever increasing usage of employee smartphones and tablets. Malware authors are also now well aware of this trend and are doing all they can to leverage the inherent weakness of this policy. By intercepting insecure personal devices, malware authors are stealing corporate data and intellectual property. Such types of trends are expected in the upcoming quarters.

2

More mobile devices with pre-installed spyware

The Quick Heal Threat Research Labs have analyzed several pre-installed apps on new devices and have found that these devices were equipped with spyware apps from the factory itself. This raises concerns about the in-built and pre-installed apps that come loaded on new devices in the market. We expect more such cases to come to the forefront in the near future.

3

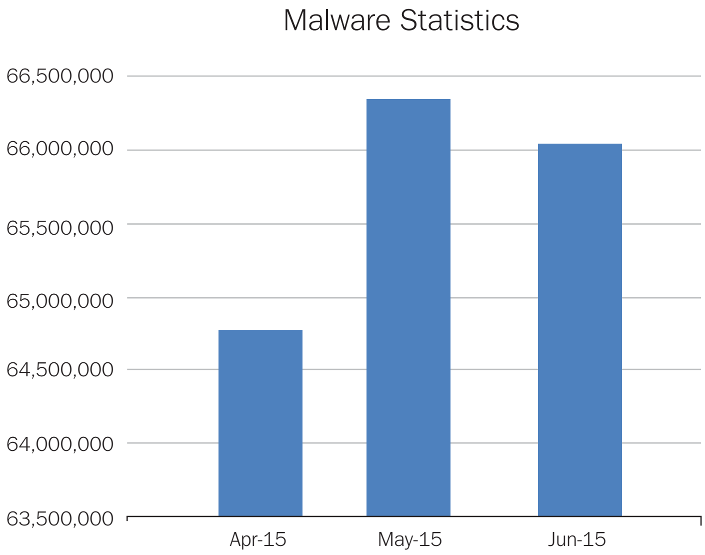
3.Continued dominance of Adware on Android devices

Adware has been a leading source of malware and security concerns on Android devices over the last few years and this is a pattern that is expected to continue in 2015 as well. Adware variants are not going anywhere and they are expected to evolve further and persistently play a leading role in detected Android malware samples. In the second quarter of 2015, we discovered 17 new variants of Adware families and this indicates the upward trajectory of this malware family.

Windows

Malware Collection

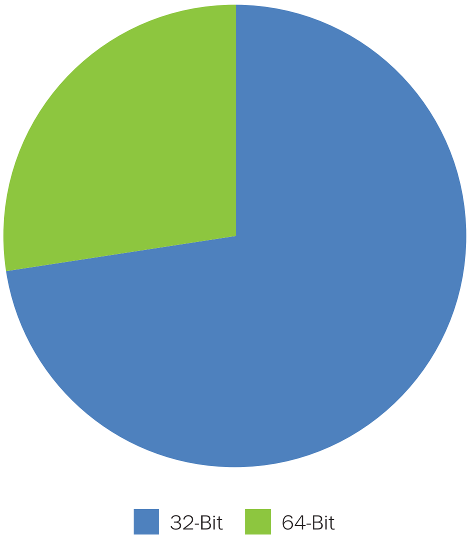
Given below are the detailed statistics for the malware samples detected over the Windows platform over the last 3 months – April, May and June 2015.



Month	Total
Apr-15	6,47,80,906
May-15	6,63,62,542
Jun-15	6,55,88,416

Platform Wise Malware Detections

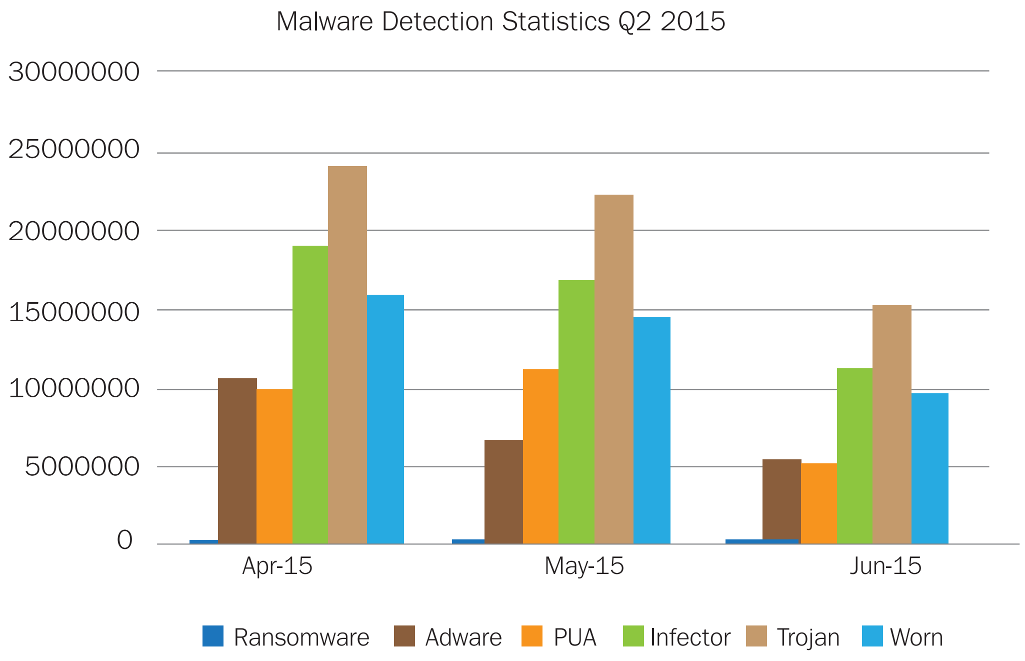
Shown below are the malware detections according to the operating system platform and architecture. Most of the infected systems are run on 32-bit platforms and are afflicted by in-the-wild malware variants. These variants do not run on 64-bit platforms so it is highly recommended that people who are buying new systems should purchase a 64-bit platform.



Major Windows Malware Categories

Given below are the detailed statistics for the malware categories and samples detected over the Windows platform over the last 3 months – April, May and June 2015.

Month	Ransomware	Adware	PUA	Infector	Trojan	Worm
Apr-15	330824	10580351	10003851	19117481	23860057	15828521
May-15	357769	6626459	10972044	16814000	22261819	14421857
Jun-15	321233	5426289	5178531	11290058	15046172	9633217



1. Adware

Adware retains its dominance as a major malware category in the second quarter of 2015 as well. Adware is software that supports advertisement banners and plugins that are displayed on them. Adware enters systems bundled with freely or cheaply available software programs. It can also be delivered while accessing malicious websites. Adware can also behave as spyware on systems as it can track user activity and can steal data which may be later sent to a remote server. This leaves the victims of Adware at great data leakage related risks.

As online shopping has become a part of day to day lives, 'Malvertising' has also become a new trend surfacing in the online market. Malvertising is a technique of inserting a malicious advertisement into a genuine advertisement and webpages. It is used for delivering other malicious content to the systems of victims. The following are the major Adware families observed in the wild:

- MultiPlug
- BrowseFox
- Coupon
- Klingontec
- OutBrowse
- Mystart

2. Ransomware

The second quarter of 2015 was not an exception for the tradition of file encryptor ransomware samples. Cybercriminals seem to be more focused on releasing new versions of ransomware and then changing their behavior rather than developing and releasing new ransomware variants each time. “TeslaCrypt flavors” and “Crypt0L0cker” are two such ransomware variants found. TeslaCrypt remains as a successor to AlphaCrypt, TeslaCrypt (Cryptolocker-v3) and New TeslaCrypt. The Crypt0L0cker encryptor inherited itself from the previously found TorrentLocker ransmoware. Some other ransomware samples seen in Q2 2015 are:

- CryptoWall 3.0
- New BitCryptor
- CRYPVAULT
- Crypt0L0cker
- Troldesh_Ransomware
- Threat Finder Ransomware
- Trojan.Win32.Reconyc as a file Encryptor
- Breaking Bad themed ransomware

3. PoS (Point of Sale) Malware

The Point of Sale (PoS) mechanism is a payment system where a customer makes payments to the merchant at shopping centers using his credit/debit card. PoS malware is designed to target these PoS systems by stealing credit card or debit card information.

Shopping centers, hotels and restaurants are the most vulnerable sectors to PoS malware. PoS malware samples are also getting more sophisticated and are using more advanced techniques to read the information that is stored on the magnetic stripe at the back of payment cards. PoS malware uses memory scrapping, keylogging and other similar techniques to read the payment card information. Some of the interesting and prominent PoS malware samples include PoSeidon, NitlovePoS and more. Another variant of PoS malware uses SSL encrypted connections for sending collected data to avoid being intercepted by network security products.

NewThingsPoS, Punkey, PoSeidon, Nitlove are some of the new PoS malware families seen in Q2 2015 and many more may hit at PoS terminals soon as well. Use of unpatched and outdated operating systems like Windows XP with vulnerable software on PoS terminals definitely makes the swiping of payment cards at merchant outlets riskier.

4. Exploit Kits

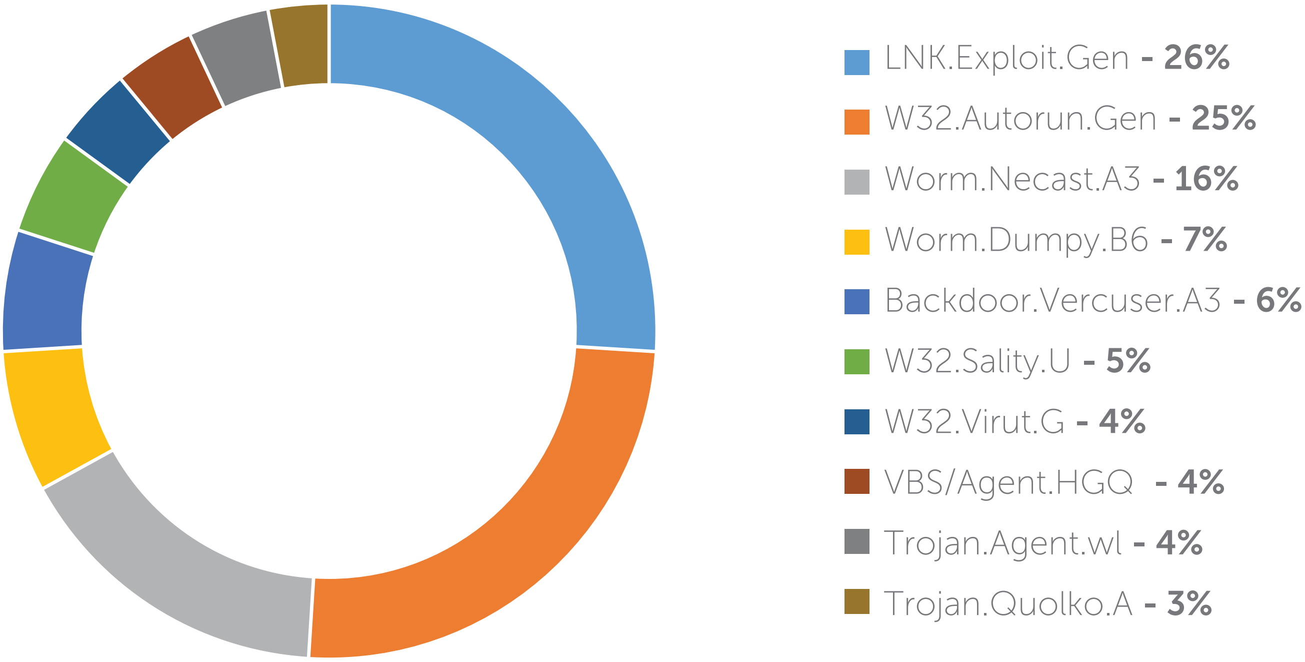
Exploit kits are commonly used by attackers to deliver malicious payloads to the systems of victims against vulnerabilities of installed software such as web browsers, Java Runtime Environment, Adobe Flash Player, Microsoft Office etc. Exploit kits constantly change and improve in order to remain undetected from security software. Various Java versions and Adobe Flash Players have been found to be the current choice of attackers for exploitation.

Angler and Nuclear are two major exploit kits active in the second quarter of 2015. Angler exploit kit exploits Adobe Flash Player vulnerabilities using SWF flash files which allow attackers to install ‘Bedep’ banking malware and a distribution botnet that can load multiple payloads on compromised systems. Nuclear is another exploit kit that also uses vulnerabilities in Adobe Flash Player. Rather than delivering malware that steals data or downloads other malware, Nuclear delivers the Crypto-Ransomware malware to the infected system.

Exploits for CVE-2012-2539 and CVE-2012-0158, which are used in APTs that target specific organizations, are now found in spam campaigns. CVE-2014-1761 is another security hole in Microsoft Office and is also gaining popularity with exploited documents as email attachments that contain malicious codes. Once a document is opened, it injects malicious code into a system process that runs with administrative privileges while bypassing user access control.

Top 10

Windows Malware



LNK.Exploit.Gen

Damage Level: Moderate

Summary: LNK.Exploit.Gen is an illegitimate application that grants an attacker unauthorized remote access to infected computers. The attacker can use a backdoor to spy on a user, manage files, install additional software or dangerous threats, control the entire plant including the present applications or hardware devices, shutdown or reboot a computer or attack other hosts.

Method: An exploit is a piece of software, a chunk of data, or a sequence of commands that take advantage of a bug, glitch, or vulnerability in order to cause unintended or unanticipated behavior to occur on a computer.

LNK.Exploit.Gen is a Windows vulnerability that allows malicious shortcuts to run themselves whenever the shortcuts folder is viewed in Windows Explorer. The potential harmful effects of LNK.Exploit.Gen are:

- It can compromise your system and introduce additional infections like rogue software
- It may redirect you to unsafe websites and untrusted advertisements
- It can slow down your PC by reducing its speed

- It can delete or rename files and folders on the computer
- It can display several unwanted and unsafe pop-up messages

W32.Autorun.Gen

Damage Level: High

Summary: This worm can spread to PCs by infecting removable external drives (such as USB drives or portable hard disks) or network shares. If the infected removable drive is then inserted into another PC, the worm then enters and infects that PC as well.

Method: The Autorun feature is provided by Microsoft Windows OS to help applications automatically launch a program which can guide a user through an installation process. This method is widely used with installation media such as CDs and DVDs. The Autoplay feature examines newly discovered removable media and devices and based on content such as pictures, music or video files, launches an appropriate application to play or display the associated content.

The simplest Autorun.inf files have just two settings: one specifying an icon that represents the CD in Windows Explorer (or 'My Computer') and the other specifying application to run. An Autorun worm copies itself to the root of the drive, then creates or modifies the Autorun.inf file, instructing it to run the dropped worm each time the drive is accessed. When the system is infected with such a worm, it looks for similar drives and repeats the process on any other drives that are discovered.

W32.Autorun.Gen is the detection of infected .inf files which are used by worms for spreading to local, network or removable drives.

Worm.Necast.A3

Damage Level: Moderate

Summary: Worm.Necast.A3 is a type of computer malware which runs as a self-contained program or a set of malign procedures. It gets onto computers when malicious websites are visited, and it is also bundled with freeware as a part of spam emails.

Method: Worm.Necast.A3 is not required to attach itself to the host program in order to perform its operation. It simply takes advantage of network connections so as to reproduce copies of itself and propagate parts of itself onto other machines. Its delivery mechanism is primarily through the Internet and spam emails. It also uses the latest programming language and technology and is endowed with changeable characteristics to evade detection and removal from antivirus software. It also utilizes advanced Java, Active X and VBScript techniques to propagate its components onto HTML pages.

The Worm.Necast.A3 malware may also exploit system vulnerabilities so that it can then drop and install additional threats such as Trojans, keyloggers, fake antivirus programs and even ransomware. Also, remote hackers can utilize the infected system loopholes to access the compromised machine without user consent or knowledge.

Worm.Dumpy.B6

Damage Level: High

Summary: Worm.Dumpy.B6 connects to a remote server in order to install corrupt files onto a compromised computer. The worm is also able to open up a backdoor entry to the computer and perform other malicious executions.

Method: A computer worm is a standalone malware program that replicates itself in order to spread to other vulnerable or connected PCs. It uses a computer network to spread itself, relying on security loopholes of target computers to access them. It also attempts to connect to computers by making use of preconfigured user names and passwords in the background. When you visit specific websites over the Internet, worms can constantly redirect users to other randomly chosen or unsafe locations.

Backdoor.Vercuser.A3

Damage Level: High

Summary: It comes through free Internet downloads or from infected online gaming websites. Once executed within a vulnerable machine, it exposes the infected system to additional security threats and exploits.

Method: This malware is designed to conduct a Distributed Denial of Service (DDoS) attack. It changes the security settings of machines and also tries to disable installed firewalls. It opens a backdoor entry for other infections to gain control over compromised systems. It also configures itself to start automatically when Windows boots up. It also tries to intimidate the user by flooding the screen with pop-ups and fake system notifications, which present the user with fake infection messages.

W32.Sality.U

Damage Level: Medium

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

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

W32.Virut.G

Damage Level: Medium

Summary: After execution, this virus injects its code within running system processes and starts infecting the executable files present on local drives and removable drives. It also performs some backdoor functionality on infected machines.

Method: This virus creates a botnet that is used for DDoS attacks, spam frauds, data theft, and pay-per-install activities. It also opens a backdoor entry that allows a remote attacker to perform malicious operations on the infected computer. The backdoor functionality allows additional files to be downloaded and executed. It also spreads by infecting the executable files on local, removable and remote shared drives.

VBS/Agent.HGQ

Damage Level: Medium

Summary: VBS/Agent.HGQ is a worm that spreads via removable drives.

Method: If this worm detects any removable drive in a computer, it copies itself onto every folder in that drive. It also creates a shortcut link file pointing to its copy in the removable drive. The worm can also allow a hacker to get backdoor access to the victim's computer. Once inside the targeted computer, the worm steals data such as:

- Name of the computer
- User name of the person currently logged in
- Version of the running operating system
- Hardware identification numbers

Trojan.Agent.wl

Damage Level: Medium

Summary: This Trojan is a non-replicating type of malware program that contains malicious code.

Method: This Trojan is written with malicious intent and is designed to find its way onto vulnerable computers. It achieves this by tricking users into downloading it, either by disguising itself as a useful file or program or by attaching itself to or hiding within a helpful file or program. After execution, it can cause:

- Data corruption
- Formatting of internal disks
- Use of the machine as part of a botnet
- Infections on other machines and connected devices within the network
- Data theft
- Downloading or uploading of files for various purposes
- Downloading and installing of other malware
- Keylogging and recording of key strokes

Trojan.Quolko.A

Damage Level: Medium

Summary: This malware performs backdoor functionality on infected machines and gives access to hackers.

Method: Trojan.Quolko.A acts as a backdoor by contacting a remote controller who can then gain unauthorized access to affected computers. Infected machines may also appear to run slower due to heavy processor and network usage.

Case Study:
Another Evaluation in Upatre

What is Upatre?

Upatre is a Trojan downloader variant of malware and it downloads other pieces of potentially malicious files on compromised systems. Earlier, Upatre has been seen delivering critical malware samples such as Zeus and Zbot, and ransomware samples such as Crilock file encryptor, ROVNIX and others to infected systems. While Upatre is not a new malware, it is however one that is continuously being developed and improved to evade detection using server side obfuscation and encryption.

Propagation Mechanism

Recently encountered variants of Upatre are delivered to victims as compressed (.rar or .zip) attachments within spam mails that contain executable files with PDF icons. Once executed, Upatre downloads and opens a PDF file to lure the user. However, in the background it actually downloads another malware strain onto the machine. This downloaded malware is responsible for delivering the famous 'Dyre' banking Trojan to the victim's machine with .rtf, .pdf or .png file extensions. Usually, these are executable files in completely encrypted formats.

Encrypted Delivery and Data Stealing (SSL communication over the network)

First discovered in August 2013, the Upatre downloader has been under constant development since then. Migration from normal GET HTTP to SSL component for communication with server has added immense value to Upatre as the communication cannot be traced easily.

Before delivering the malicious payload, Upatre collects system information like IP address, region, date and time, host name and OS details of the compromised system. Earlier variants used 'HTTP GET' requests to 'checkip.dyndns.org' to identify this information. Newer Upatre variant have employed SSL components for all communications in order to send the stolen information. It also has the added advantage of keeping all communication between the client and server well-hidden on the network.

After setting up the SSL connection and information check, the malware makes an encrypted delivery of the 'Dyre' banking malware onto the victims system. Furthermore, 'Dyre' is used to steal sensitive information and credentials from compromised systems in encrypted formats. Also, the same malware can be used to download other malicious files from the C&C server.

Users' confidential data is at high risk from such malware samples. Delivering payloads in encrypted formats makes it very difficult for security products to trace and detect the samples.

Upcoming Trends for Windows Malware

1. Adware: Unwanted Caretaker

Online advertisements are getting more personal. Internet browsing patterns of individuals are under continuous monitoring so as to deliver advertisements as per online browsing habits. The current trend of 'Malvertising' techniques continues to deliver unwanted and malicious content to systems, without the consent or knowledge of users. With the help of browser hijacking techniques, Adware may collect personal and confidential data of victims along with their browsing information as well.

2. Ransomware: More variants, more encryption, more profits

Encrypting files and demanding a ransom to unlock them has become a great business model for cybercriminals. Old ransomware families are expected to make a comeback with new features. The recent wave of crypto-ransomware samples showcased advanced evasion and encryption techniques with the goal of collecting as much money as possible. The ability to attack cloud storage services is also the most disturbing advancement in detected ransomware variants. Targeting specific industry sectors like banking, healthcare and education could be another possible source of income for ransomware writers.

3. Spamming remains an effective infection vector

Most of the ransomware variants encountered in Q2 2015 spread and propagated via spam emails and had improved security evasion and bypass techniques. CryptoWall 3.0 and CRYPVAULT crypto-ransomware are two such ransomware samples that employed noticeable techniques. Both of them used a malicious JavaScript file as an attachment for hitting victims' systems. They also made use of .js files which are helpful for evading detection from security software by using complex obfuscation techniques. Once bypassed, delivered and executed, this .js file connects to Command & Control servers that download additional payloads. These payloads also exist in tricky formats either with lured or encrypted extensions so as to remain undetected.

4. More specific banking Trojans

Threat authors have now moved their attention and efforts to the banking sector, as this is a home for money. "Dyre" and "Vawtrak" have already proven themselves as proficient money stealing malware variants. Another technique has been spotted through which macros are used for delivering the 'Dridex' banking malware into vulnerable systems. So, malware families with more advanced techniques are expected to hit machines soon. Spear phishing emails and social engineering tactics can also be used as carriers for delivering banking malware to organizations. The use of RAT (Remote Access Control) tools for remotely controlling ATM machines is also expected to lead to the exposure of sensitive card data.

CONCLUSION

The Quick Heal Quarterly Threat Report for Q2, 2015 highlights the constantly rising malware threats over the leading computing platforms – Windows and Android. While Adware has become commonplace over both these platforms, other threats such as Ransomware, Malvertising and Exploit Kits are beginning to show up more often on Android mobile devices as well. This has led to a greater risk for Internet users, irrespective of the device they actually use. With the Internet of Things also almost upon us, this does not bode well for the future of IT security, especially when adequate and effective security measures are not adopted.

The Quick Heal Threat Research Labs are compiling and analyzing malware variants round the clock and this information is shared with the R&D Labs so as to create the most efficient, proactive and advanced security products and services. With the best security mechanisms in place, malware authors will find it harder to penetrate connected devices with traditional and recently seen techniques. However, the need for awareness and effective security measures is now higher than ever and cannot be looked over.