Quick Heal

Security Simplified

Quarterly Threat Report

for Windows & Android - Q3, 2014

Q3

Threat Report:

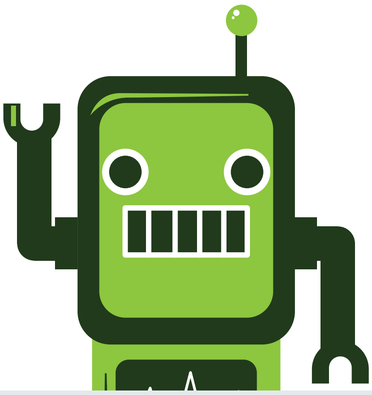
3rd Quarter, 2014

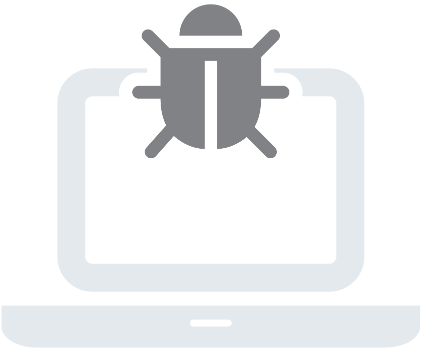
Table of Contents

Summary Windows

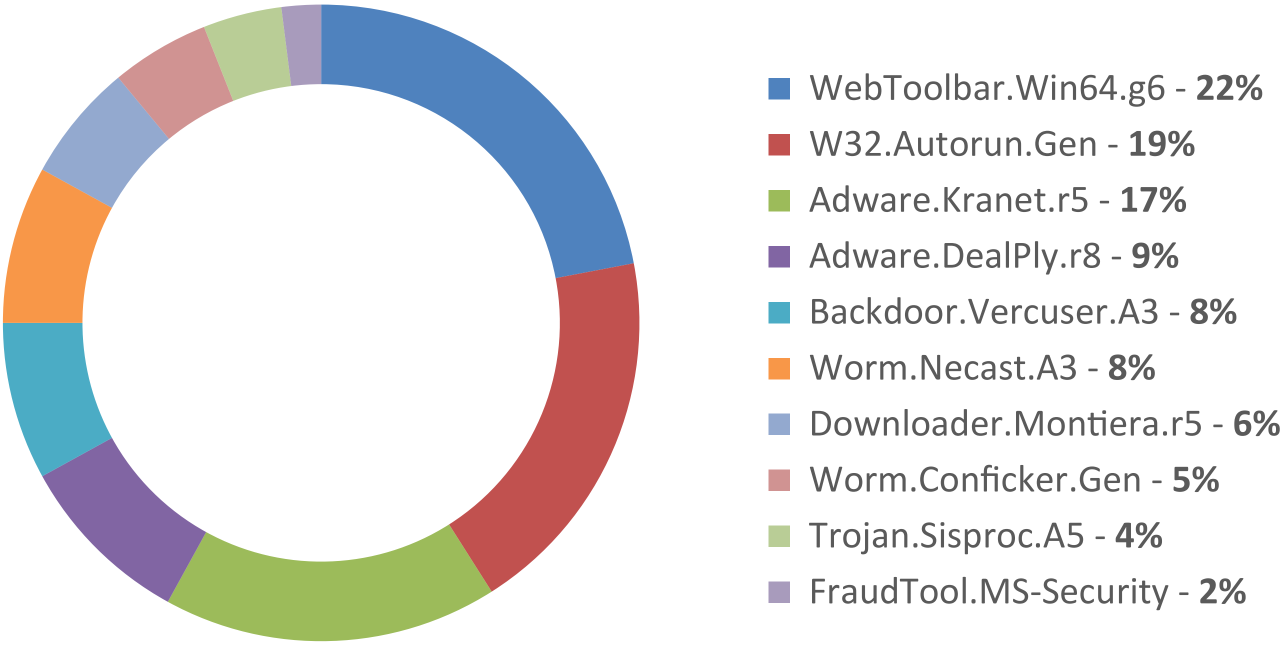
In the third quarter of 2014, Quick Heal Research Labs have seen a huge increase in the numbers of Adware samples that have been reported. These are Potentially Unwanted Programs (PUPs) which are bundled with downloaders and program installers, with or without user knowledge. They display unwanted ads while browsing the net, change the default settings of the browser homepage and search engine and also install various add-ons and plugins. Such adware programs are used by malware authors to gather system information, monitor browsing habits and upload malicious data for nefarious purposes.

It has also been found that 5% of malware samples are of the Kido worm, or "Worm.Conficker.Gen". This is a worm that afflicts unpatched Windows XP running machines, and this is a disturbing trend because Windows XP has no official support from Microsoft anymore. This is a highly vulnerable platform and users are highly advised not to operate on it. The ransomware known as "CryptoWall" has also been highly dominant this quarter. With that in mind, here are the top 10 malware samples for Q3 2014 and the upcoming security trends to lookout for.





Top 10 Windows malware
for Q3 2014



WebToolbar.Win64.g6

Target: All versions of Windows OS released since Windows XP.

Propagation: It is downloaded through web browsers such as Chrome, Firefox, Internet Explorer and others. Usually comes bundled with freeware programs.

Behavior:

- Injects banner advertisements into websites and displays pop-ups that do not originate on these websites.
- Makes unauthorized changes to important files and registry entries. This diminishes system performance.
- Hijacks the homepage and the search engine of a PC.

W32.Autorun.Gen

Target: All versions of Windows operating systems.

Propagation: It spreads by copying itself to a mapped network of removable drives.

Behavior:

- This malware creates a file named ' Autorun.inf' in the root of a targeted drive.
- This malicious file is used and run by the Autorun and AutoPlay components of Windows operating systems.
- The malicious Autorun file also contains execution instructions for the OS which are invoked when the drive is viewed through Windows Explorer.

Adware.Kranet.r5

Target: All versions of Windows operating systems and the web browsers within them.

Propagation: It is often bundled with, or embedded within, freeware programs such as clocks, messengers, alerts, weather reports and others, and it spreads on the system when executed.

Behavior:

- This adware plugs into the web browser and displays context-based ads by overwriting existing ads or by inserting new ones.
- It also gathers information from a user's computer that is related to the web browser usage and other computer habits.
- It is primarily responsible for the countless pop-up ads that are seen while browsing the Internet.

Adware.DealPly.r8

Target: All versions of Windows operating systems and the web browsers within them.

Propagation: It is often bundled with, or embedded within, freeware programs.

Behavior:

- This adware floods the desktop with various online ads, discount offers and savings deals.
- It is also known to offer various coupon deals or savings offers through various shopping sites on the Internet.
- It changes the settings of the web browser and adds malicious add-ons with approval or knowledge. The default homepage and search engine of the PC are also changed.

Backdoor.Vercuser.A3

Target: All versions of Windows operating systems and unprotected email users.

Propagation: It enters systems through spam emails and malicious attachments.

Behavior:

- It causes loss of personal data as it deletes sensitive files from the PC.
- It changes browser settings, homepage settings and default search engine settings.
- It connects to a remote server and downloads other infectious files and malicious attachments.
- It slows down a PC during startup, shut down, while running programs and games and also while surfing the web.
- It misuses Internet bandwidth and leads to a drop in Internet speed.
- It prevents many programs from functioning properly.
- It infects the registry files and uses it to launch pop-up ads.

Worm.Necast.A3

Target: All versions of Windows operating systems and unprotected email users.

Propagation: It enters systems through spam emails and malicious attachments.

Behavior:

- This worm intimidates users by showing constant notifications and pop-ups depicting fake infection.
- It will carry out fake scans of the system and give misleading safety reports.
- It slows down a PC by misusing system resources.
- It causes installed antivirus programs to display constant pop-ups about infection notifications.
- It shuts down the antivirus that is installed and also limits its functionality.
- It infects the registry entries on a machine.
- Many programs and functions will not work properly as their functionality will be affected by this worm.
- It prohibits System Restore functions from clearing out the machine. causes many executable programs to malfunction and the system to crash.

Downloader.Montiera.r5

Target: Web browsers such as Chrome, Firefox, Internet Explorer and more.

Propagation: Installation of the Montiera toolbar.

- This toolbar tracks a user's activity and gathers all the information available.
- It alters system settings and opens a backdoor entry on the system.
- Afflicts all web browsers on a PC and alters the homepage and search engine of these browsers.
- Causes PCs to slow down and crash from time to time.
- Causes various pop-up ads and banner ads to get displayed.
- Causes all the web browsers to perform slowly.

Worm.Conficker.Gen

Target: All versions of Windows operating systems.

Propagation: Vulnerability loop hole within Windows operating systems.

Behavior:

- Infects systems across a network by exploiting vulnerabilities in the Windows Server service (SVCHOST.EXE).

- If the vulnerability is successfully exploited, it allows the execution of remote codes whenever file sharing is enabled.
- It also spreads via removable drives, network shares and weak administrator passwords.
- This multi-component worm also carries various payloads once it is executed on a PC.
- This worm also injects various harmful codes into system files. This conceals the threat from antivirus programs and only legitimate system processes will be visible.

Trojan.Sisproc.A5

Target: All versions of Windows operating systems.

Propagation: Downloads of freeware programs that are initiated through the web browser.

Behavior:

1. This Trojan usually installs itself by copying its executable file to the Windows Systems folder and then modifying its registry files to run on startup.
2. It contacts a remote host at “opencapture.co.kr” using Port 80 for the following purposes:
   - To report a new infection to its author.
   - To receive configuration settings or other data.
   - To download and execute arbitrary files (including updates or additional malware).
   - To receive instructions from a remote attacker.
   - To upload the data that is gathered from infected systems.

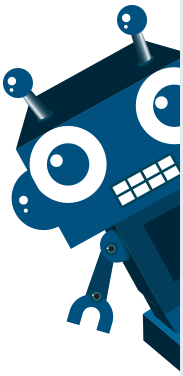
FraudTool.MS-Security

Target: All versions of Windows operating systems.

Propagation: It spreads during the installation of or by clicking on infected programs, processes or links.

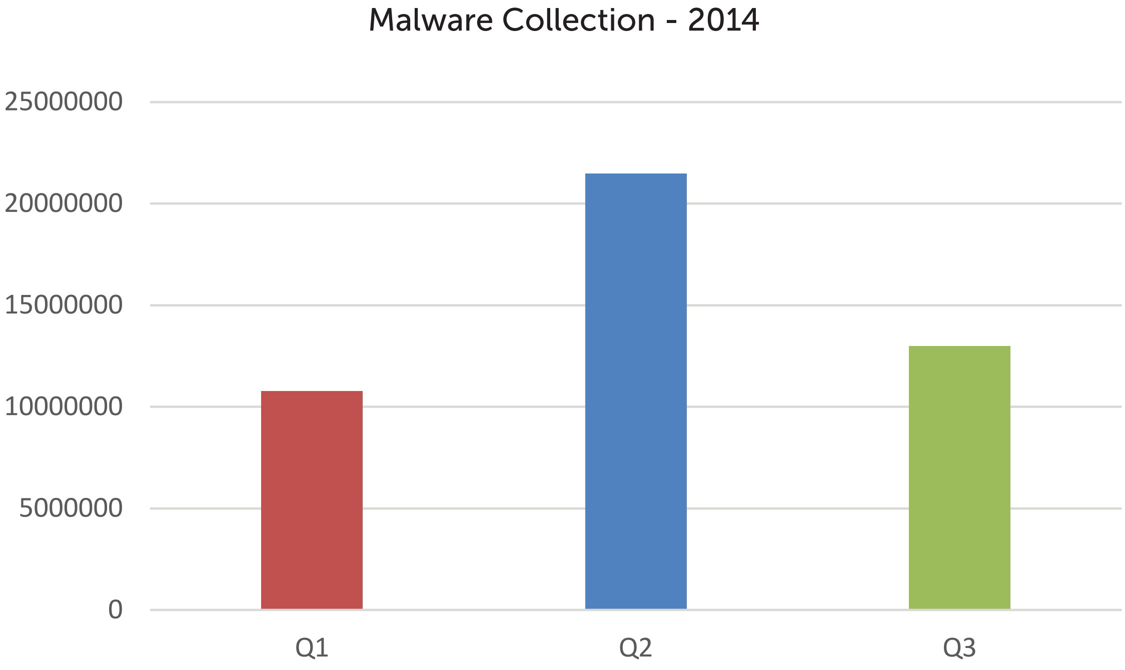
Behavior:

- When this malware is executed, it immediately disables the use of Portable Executable (PE) files.
- It prompts fake security alerts in order to manipulate users into purchasing the trial version of fake antivirus applications called ‘Spyware Protection’.



Windows Malware detection by Quick Heal

Month	Files Received
July 2014	4,138,885
August 2014	4,899,229
September 2014	3,946,776
Total Samples	**12,984,890**



Case Study: Analysis of Bash Bug aka Shellshock Vulnerability

What is Bash?

Bash is the default shell for Linux, UNIX and Mac OS X platforms. It stands for Bourne-Again Shell and it was created in 1989 and it enables users to run other programs within these platforms.

What is the Shellshock vulnerability?

Shellshock is a newly discovered Remote Code Execution (RCE) vulnerability within Bash. Via this vulnerability, an attacker can inject malicious commands into the system and run them. Since Bash runs several programs in the background, all the attacker needs to do is prevent his malicious text from getting detected. In this scenario, harmless looking data is usually accompanied by malicious texts. Malware writers are expected to take advantage of this vulnerability in the near future and devise methods to target other platforms as well.

Who is vulnerable to Shellshock?

Bash, the command shell, is most commonly used in Apple's OS X operating system. Additionally, it is also present in several web servers and home appliances such as routers and other devices which face the Internet. This creates a risky scenario since updates for such devices are not easy to acquire or implement. As a result, these devices will continue to be at risk against the Bash vulnerability and Shellshock could potentially disrupt several services and homes.

Upcoming trends
for Windows malware

1. Malvertising Techniques

In order to target Windows machines, attackers have now come up with a new technique known as “Malvertising”. Via this method, they distribute malware through legitimate advertising networks such as Google Doubleclick. In order for Malvertising to work effectively, ad networks such as YouTube, Yahoo and other top sites are used and their JavaScript is obfuscated. This allows malware authors to deliver malicious codes through Flash ads and banners. In addition to obfuscating the JavaScript, this technique also adds an iFrame to redirect users to malicious URLs that serve the STYX exploit kit, a well-known banking Trojan. Malvertising is expected to reach more people via additional ad networks in the near future.

2. Advanced Persistent Threats

Advanced Persistent Threats (APTs) are techniques that are used to attack a network and gain unauthorized control over the network. The main intention here is to steal data from that particular network, and the victims are carefully picked and infiltrated. In such scenarios, the network is not harmed but silently spied upon, sometimes for many years at a stretch. These threats follow the motto of “Go low and go slow” in order to continuously monitor and extract sensitive data from specific targets. Usually, these targets fall under national defense, manufacturing and finance, amongst others. APTs also involve the use of social engineering techniques known as Spear Phishing in order to gain access to these networks. In case of successful attacks, a backdoor into the network is opened and the gathering of valid user credentials, sensitive data and spreading over the network is then begun. The threat of APTs is expected to rise further in the coming months.

3. Ransomware and CryptoWall to Evolve Further

ryptoWall is a file-encrypting ransomware which was found to be active in April 2014. It specifically targeted Windows operating systems and is still functional and expanding its reach. When this malware enters a system, it scans the PC for data files such as doc, xls and others and then encrypts these files using RSA encryption. For the files to be decrypted, the ransomware asks the user to pay $500 if they pay within 5 days, $750 if they pay after 5 days and greater amounts that go up exponentially if any delays occur. This ransom is demanded in the form of Bitcoins, and the address on which this sum is to be transferred is dynamic and changes for every victim. The primary source of distribution of this malware is via emails that contain ZIP attachments which contain executables disguised as PDF files. These files are usually named as invoices, bills, purchase orders etc. in order to manipulate a user into clicking on them so as to spread the infection further. CryptoWall has infected more than 100,000 computers and we expect this number to rise further.

4. BadUSB Vulnerability to Manifest in Multiple Devices

USB drives have been a boon for computer users as they enable simple and fast data transfer from one point of control to another. While USB drives are one of the easiest ways for data transfer, they are not very high on the safety factor. There is plenty of open source code that is available which can be used to convert a USB drive into a silent malware installer. This vulnerability already exists and it is termed as “BadUSB”. This vulnerability hides in the firmware that is meant to control the ways in which USB devices connect to a computer, and this is how it spreads. Through this vulnerability, an attacker can insert malicious code into the USB firmware. Users who use USB drives and keyboards and other USB enabled devices are increasingly at risk here, as USB sticks can be reprogrammed to spoof other device types in order to take control of a computer, extract data or spy on a user.

So far we have not detected any malware related to the Shellshock vulnerability and the BadUSB vulnerability, but these are both highly critical and severe vulnerabilities and there is a strong possibility that they will be exploited by malware authors in the near future.

Summary Android

After the massive surge in Android based malware that we saw in the previous quarter, Q3 has also seen a large number of malware strains discovered on Android devices. The Quick Heal Threat Research Labs have come across several new and never been seen before strains in these last 3 months, and this just goes to highlight how Android malware is constantly evolving.

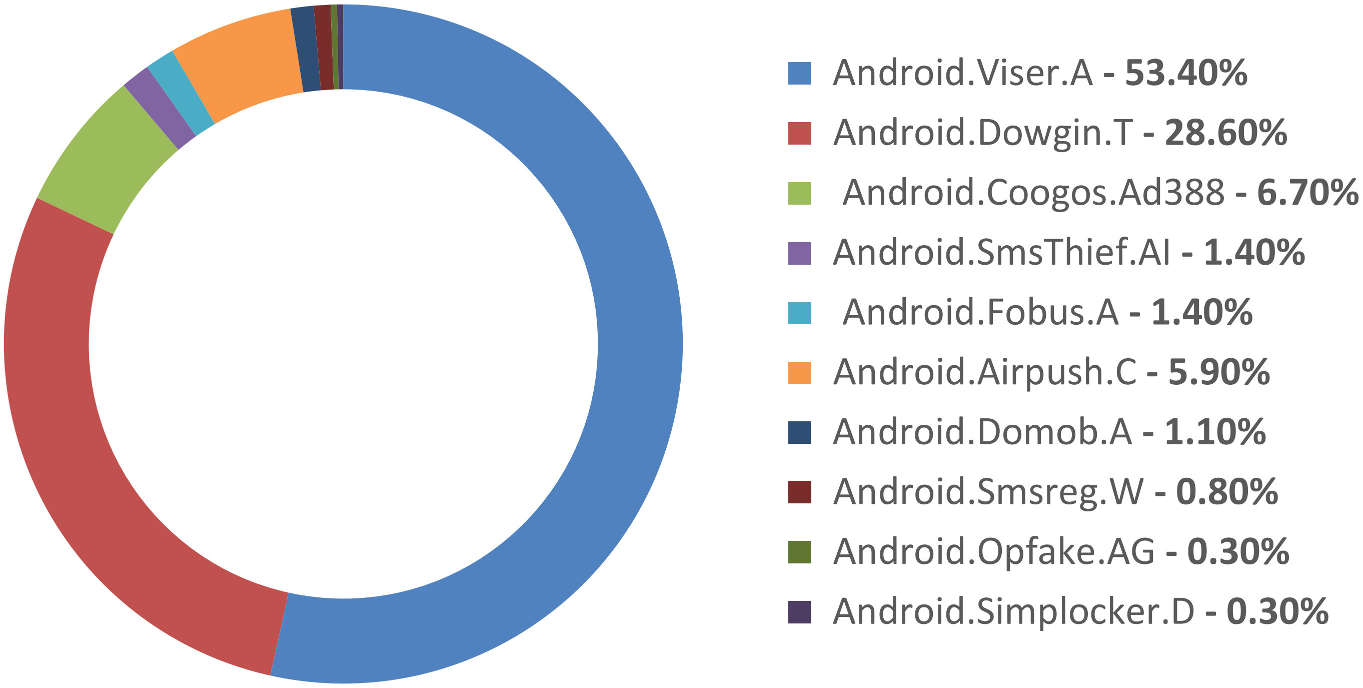
In the last quarter alone, we have detected several new Android malware families and new variants of previously detected malware as well. We discovered a staggering 47 new Android malware families and 218 new variants of previously seen malware as well. Android malware now has the scope to reach far more devices than ever before, and these new samples are testament to that.

As before, Android adware is at the top of the pile by infiltrating the most devices. Such programs create havoc within systems and also collect user sensitive data which can be used for multiple purposes. With that in mind, here are the common malware samples and trends found by the Quick Heal Research Labs from the months of July – September 2014.

Android Threat Report:

3rd Quarter, 2014

Top 10 Android malware for Q3 2014



Android.Viser.A

Just like the last two quarters of 2014, this quarter also sees Android.Viser.A topping the list of Android samples detected. A prominent form of mobile adware, this strain enters devices through applications on Google Play and third-party sources. Removing this adware requires the removal of the installed application altogether. The following are the functions that this adware performs:

- Displays unnecessary ads on the device
- Alters the saved bookmarks of the device
- Steals and broadcasts device location, IMEI number of devices
- Sends text messages to premium-rate numbers

Android.Dowgin.T

A new strain of malware that has been discovered recently, Android.Dowgin.T performs malicious functions that have been seen many times before. It goes one step further and displays unwanted ads on the notification bar of the device. While continually monitoring device state, it steals the following functions:

- Reads system log and details
- Locates the device's geolocation
- Transmits the subscriber ID
- Broadcasts the device ID and other sensitive information

Android.Coogos.Ad388

Android.Coogos.Ad388 is a new form of potentially unwanted program that gains access into private user and device information such as:

- Contact information
- Device location history
- SIM card details and device ID
- Photos and videos and camera related functionss

Android.SmsThief.AI

Continuing with the trend of newly discovered malware strains this quarter, several new discoveries have been made. Android.SmsThief.AI is one such malware sample that has not been found before. As suggested by the name, this sample deals with the text messages on a device. It performs the following malicious activities:

- Sends SMSs from the devices to a malware author
- Sends call records to a malware author
- This is achieved through an active Internet connection
- This can also be achieved by forwarding details in the traditional manner

Android.Fobus.A

This is a very complex malware family that is immensely hard to detect by a security program or an analyst. Android.Fobus.A has a very strong and effective hiding mechanism and this enables it to stay hidden and undetected for a long period of time. While its service keeps constantly running in the background, it performs the following activities:

- Sends SMSs to premium-rate numbers for financial gains
- Sends text messages and sensitive device information to remote Command & Control servers

Android.Airpush.C

Mobile adware has been one of the most common forms of Android threats we have found over the years. Free apps and games are the perfect many ad-modules like Leadbolt and Airpush, other variants of Android adware that have been mentioned above. The ideal method to avoid this variant is to disable app installations from unauthorized and third-party sources.

- Modifies the bookmarks that are saved on the device
- Drops malicious shortcut icons on the home screen of a device
- Sends SMSs to premium-rate numbers in remote areas

Android.Domob.A

Similar to Android.Airpush.C, this also displays ads on the notification bar of an infected device. Android.Domob.A constantly checks the network status on the device and misuses the data bandwidth available there. It also steals the following private information:

- System logs and other private information on the device
- Device location and geolocation history
- Device ID and other details like IMEI & IMSI numbers
- It also sends out messages to premium-rate numbers

Android.Smsreg.W

Malicious applications which come under this category and family can be classified as potentially unwanted applications. Android.Smsreg.W asks a user to make payments through premium messages for registration.

- The cost of such messages can be prompted by the malware author
- Most times, registration doesn't occur even after the payment has been made
- The registration depends on geographical locations and network providers

Android.Opfake.AG

Unlike other forms of Android malware, this is a Trojan horse that affects devices via SMS. Once inside a device, Android.Opfake.AG can perform a lot of malicious activities.

- This Trojan usually comes bundled with the Opera mobile browser
- It successfully steals all the contact information from a device
- It forwards text messages containing its own link to all contacts from the device
- It also steals banking credentials and sends usernames and passwords to remote servers

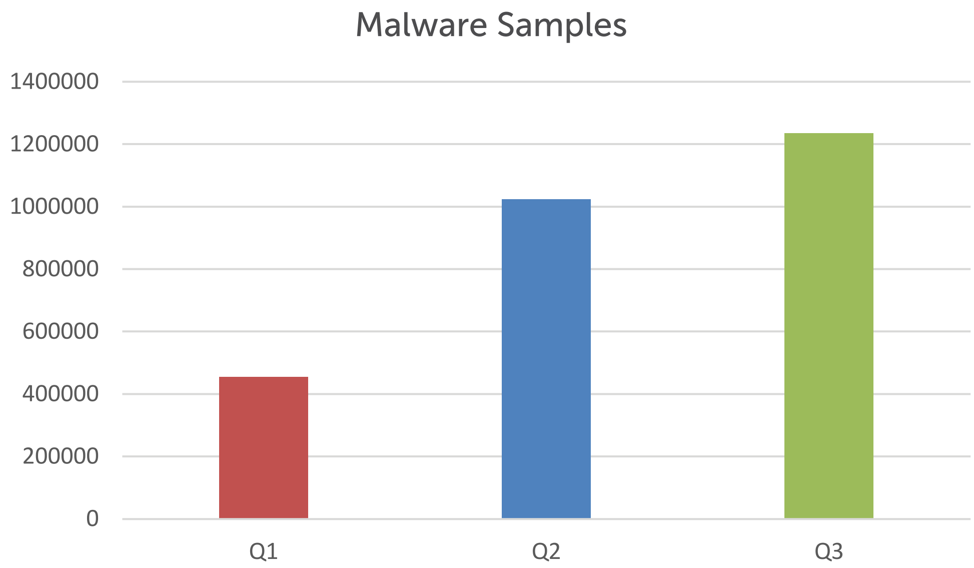
Android.Simplocker.D

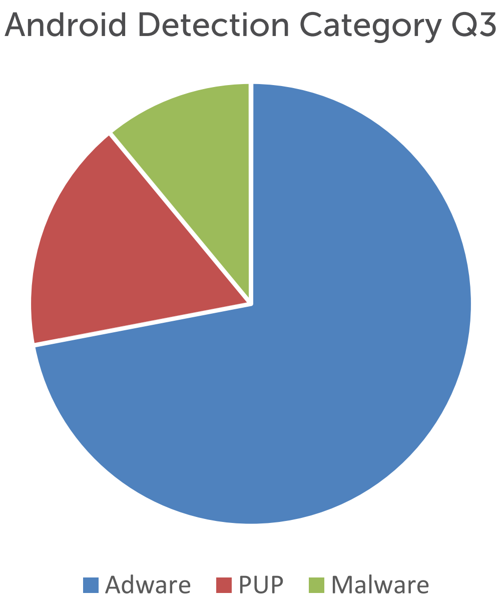
A notorious form of ransomware, Android.Simplocker.D resembles a genuine application in appearance and text. However, as soon as it is installed, it takes the device user to a lock screen and displays a fake message from the FBI. At other times, it displays nothing on the screen but simply encrypts all the files present in the SD card, in the background. It also makes the following accusations and asks for a ransom to unlock the device:

- Violation of copyrights and other related laws
- You have been viewing and distributing prohibited pornographic content

Android Malware Collection by Quick Heal

Month	Files Received
July 2014	454677
August 2014	344325
September 2014	435970
Total	**1234972**





Upcoming trends for Android malware

1. Banking credentials and information the next great target

With the festive season around the corner and so many online shopping deals and sales going on all around, online shopping and banking has become the next big thing. What this means for attackers is that they have a lot more victims to target now in their attempts to gain banking information and credentials. With more people using their smartphones and shopping apps for banking and shopping now, this is highly crucial information that is sure to be targeted by attackers in the near future.

2. Further evolution of social engineering techniques

With the large number of apps and games and social networks available to people, there is no dearth of social engineering tricks that attackers make use of in order to trick people into giving away their personal details and confidential information. These methods and tricks are only going to increase in number and become more devious and manipulative in the foreseeable future. Android users need to be wary and careful about the pages they visit, the links they click and the information that they share.

3. Continuous presence of adware in the upcoming quarter

Adware has always been a major problem on the Android platform. Since there are so many apps that are easy to develop and publish, bundling ads with them has become very easy. Such ads usually enter devices without user knowledge, and once there, they perform several malicious activities. Android adware has the ability to kill running apps and also to display ads from malicious servers. Furthermore, adware also has the ability to download other malicious apps into a device and infect it further. This is a trend that we do not see slowing down anytime soon.

4. Ransomware and Crypto-ransomware will continue to rise

Following the trend on Windows platforms, Android ransomware has also become more dangerous and wide reaching. Along with the ransomware families that have been circulating in the past, we also expect new samples and strains to turn up. “Crypto-ransomware” is also finding its way to devices with malware such as “Simplocker”. Once installed, this kind of application steals private information and takes full control of a device. It also forwards a download link to users on the contacts list. Social networking sites and URL shortening services are also being taken advantage of by attackers and malware authors.

Tips for safe online shopping on smartphones

With massive sales on major e-commerce shopping portals this festive season, there are many people who will be making their purchases via their smartphones. Most of the portals have their own dedicated apps for buyers now, but there are several people who will still follow unknown URLs and make purchases via their web browsers. Entering financial details on smartphones is a risky affair though, and here are some safety tips for online shoppers to keep in mind.

1. Always shop through official apps

While shopping online, credit/debit cards are your biggest assets. To safeguard them, it is imperative to shop through the officially released apps of shopping portals only. Granted, these apps do not offer foolproof security measures, but this is the safest way to make an online purchase.

2. Never shop through email links and URLs

If you receive an email with festive season sales and offers, you must never follow through on the links mentioned in the email when you make the purchase. Instead, it is advisable to visit the website separately and search for the product or the offer there itself. Fake emails and links are common tools to lure people into giving away their information, and smartphone users should avoid such links.

3. Always look for HTTPS verification

Mobile browsers can be tricky, especially for shoppers. The tricks that help detect phishing websites on desktop browsers do not apply here. Mobile browsers appear and function separately, so noticing the HTTPS certification is harder. The address bar is usually not visible so shoppers must ensure that they check the address bar properly and spot the HTTPS certification before making a purchase from a web link.

4.Use a card that is solely dedicated to shopping

The one golden rule that no one tells you is about the card that you use to actually make a purchase. Online purchases are never completely foolproof and can always go awry. So never use a debit card of an account where you have all your savings piled up. Instead, open a new account with limited money in it and use that debit card for purchases. That way, even if you lose the details for that account, the hit you take will be minimized.

5. Use a secure and password protected Wi-Fi connection

Free Wi-Fi in coffee shops and airports and malls are great for people who are constantly on the move. However, making an online purchase through these connections should be strictly avoided. Wi-Fi snoopers and interceptors can steal private data over unsecured Wi-Fi networks, so stick to secured and private networks at your home or office for making purchases.