Quick Heal

*Security Simplified*

# Quarterly Threat Report

## for Windows & Android - Q2, 2014

Q2

# Threat Report:

2nd Quarter, 2014

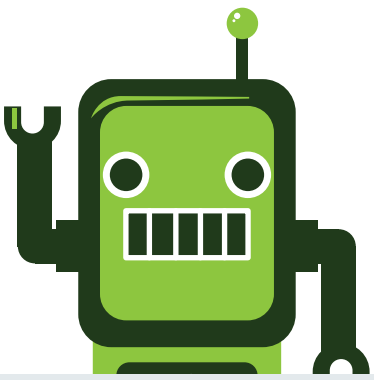
## Table of Contents

# Summary - Android

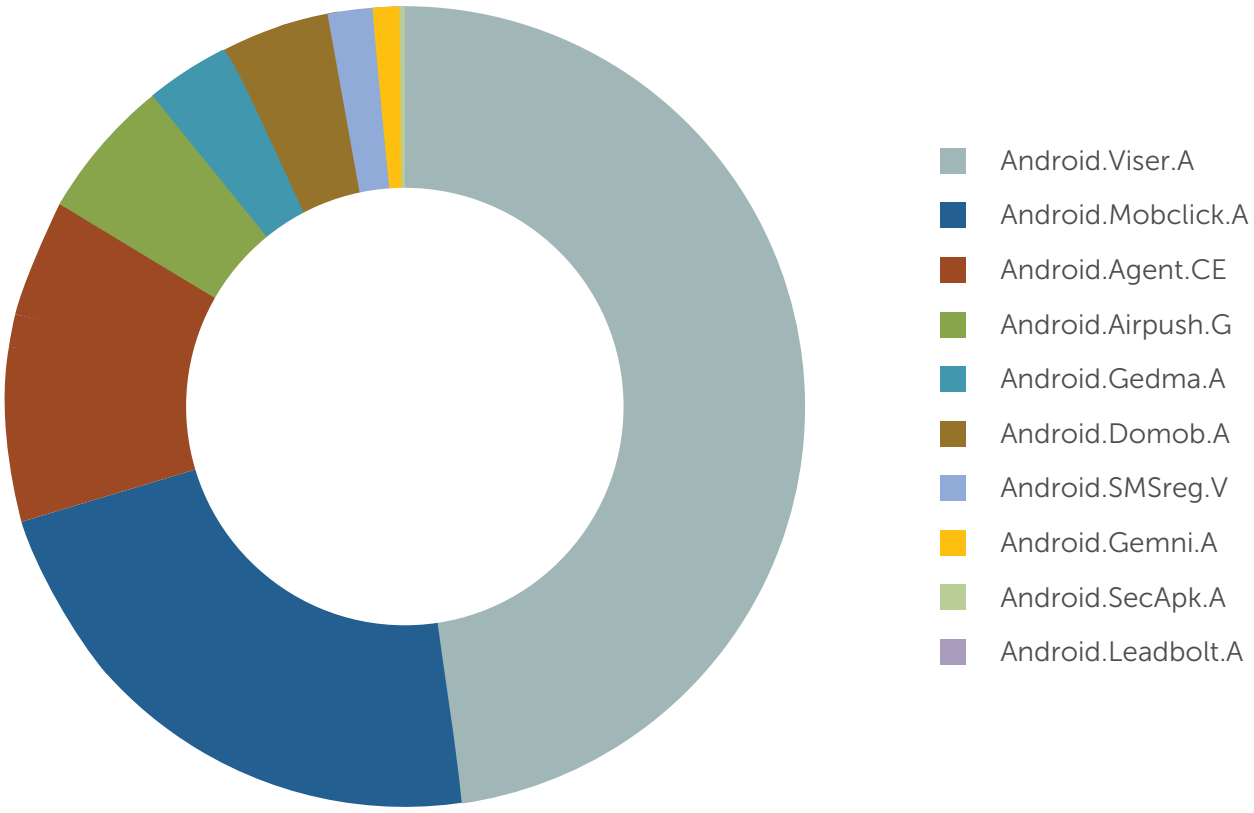
Android malware saw a massive surge in the second quarter of 2014. We witnessed a rise of more than 100% in the samples that we collected from various sources and this can simply be attributed to the large number of Android smartphones and tablets that are currently being used by people all across the world.

New attack techniques and an alarming lack of security awareness amongst Android users has led to malware authors targeting Android owners, as they are aware that these users are prone to be more susceptible than other platforms that are inherently more secure. Just like Windows became a hotbed for PC malware and viruses, Android has become the platform of choice for these attackers.

With advanced forms of malware (some strains of ransomware) now reaching Android devices as well, these attacks are becoming stronger and more resilient. Increased security risks need to be neutralized with the help of advanced mobile security solutions, and this is what the Quick Heal Threat Research Labs and the R&D team is constantly striving to do. With that in mind, here's a look at some of the most common forms of Android malware and their functions from Q2, 2014.



# Top 10 Android malware
## for Q2 2014



## Android.Viser.A

Again, Mobile Adware on Android was the biggest threat to the platform over the last quarter, and the most prominent strain that we came across was Android.Viser.A. A very risky and invasive program, this version gains access through several downloadable applications over Google Play and third-party sources. Once installed, it displays unwanted and unnecessary ads. Moreover, removal of this adware requires the removal of the bundled application that is infected, or the installation of another security application that can spot and detect this adware. Some other malicious activities that Android.Viser.A performs are:

- Transmitting device location through GPS
- Transmitting device IMEI & IMSI
- Transmitting text messages to premium-rate numbers.

## Android.Mobclick.A

The next biggest threat to the Android platform in Q2, 2014 was also a strain of mobile adware. Android.Mobclick.A performs like a typical adware that carries out all the activities we have come to expect. It accompanies innocent and safe looking apps and compromises Android devices. Once installed, it showcases unwanted advertisements and popups and also transmits sensitive device information and personal data to remote servers. Data that is stolen and sent out includes, but is not restricted to:

- Device geographical location
- Device ID
- Device system state

## Android.Agent.DL

This is a variant of the Trojan family and once it enters within an Android device, it actively pulls other malware to the device and attempts to grant entry access to them. With a URL address included within the malware, other malicious files are downloaded from that URL. Android.Agent.DL is part of a much larger family of Android Trojans that carry out the following malicious activities:

- Stealing contacts and their details
- Collating device location history
- Leaking subscriber ID and device ID
- Forwarding messages to premium-rate numbers

## Android.Airpush.G

Certain variations and types of malware push notifications within installed applications and other screens, but a distinguishing characteristic of Android.Airpush.G is that it actively pushes intrusive ads into the notification bar of an Android device. Moreover, this adware also scans and logs the bookmarks that are saved in the device and then modifies them as well. Altered bookmarks inadvertently lead an Android user to fake phishing websites, phishing links or malicious apps that hold further security risks. Additionally, this adware also performs the following activities:

- Sending text messages to premium-rate numbers
- Creating shortcut icons on the homescreen of the device
- Sending out device information like IMEI & IMSI

## Android.Gedma.A

This is a form of Android malware that falls into the Trojan category and it can be very dangerous indeed. Android.Gedma. A gains unlawful entry into an Android device through trickery, and once inside, it gains control over the victim's private information. Amongst other things, this Trojan performs the following activities:

- Steals contact information from the device
- Steals contact lists from infiltrated devices
- Transmits the device's location and GPS signal
- Sends SMS's to premium-rate numbers without user consent or knowledge

## Android.Domob.A

Yet another variant of adware, Android.Domob.A aggressively pushes ads and notifications forward. It comes bundled along with many official and unofficial Android applications and performs several activities. Like other adware strains, this version is highly privacy invasive and steals a lot of confidential data of unsuspecting Android users. Amongst other things, the most common functions of this particular adware are as follows:

- Texting premium-rate numbers
- Modifying saved bookmarks on the device
- Downloading and installing other malicious apps
- Transmitting network operator information

## Android.SMSreg.V

Going by the name of "Battery Improve" on several third-party sources for Android apps, Android.SMSreg.V has infiltrated many unsuspecting devices over the past few months. Deemed as a potentially unwanted program, this security risk is capable of stealing the following data:

- Device model
- IMEI number
- Other device information
- Device location

## Android.Gemni.A

Yet another strain of Potentially Unwanted Programs (PUP), Android.Gemni.A comes bundled with repackaged versions of legitimate applications or games. This is especially true of applications that have payload activities embedded. This PUP then establishes contact with an external and remote command & control server, and connects to this server using HTTP access. Beyond that, it performs the following activities:

- Transmits geographical location of the device with the help of the GPS signal
- Copies contacts and text messaging data and uploads this data to the remote server
- Downloads and install other apps and potentially unwanted programs

## Android.SecApk.A

This strain of malware, or Potentially Unwanted Program (PUP), has previously been found in the Google Play store and over other third-party application repositories as well. Android.SecApk.A infections and detections have ironically started as a result of an online service called App Shield that encrypts apps and prevents virus infections. Once installed on an Android device, it performs the following activities:

- Gains and misuses admin rights over the infected device.
- Harvests and steals private information from the device.
- Consumes disk space and RAM on the device, thus slowing it down considerably.

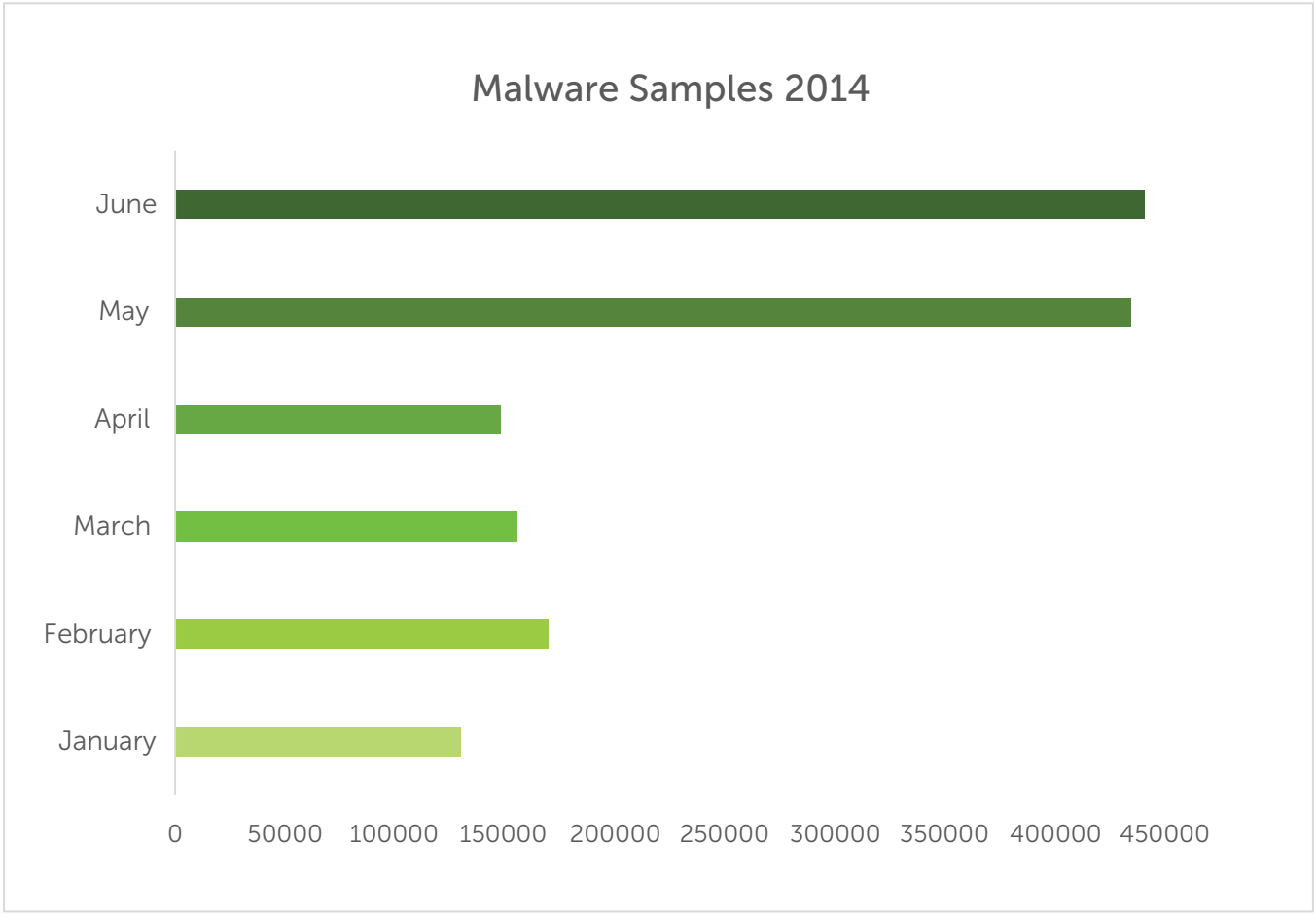
## Android.Leadbolt.A

Amongst all the strains of adware that were found in Android devices in Q2, 2014, Android.Leadbolt.A was unique as it regularly pushed through pornographic ads rather than regular advertisements. Moreover, this strain also created shortcut icons on the homescreen of Android devices without any intimation, warning or command. Along with serving up obscene and distasteful content in the form of ads, this adware also served the following data to remote servers:

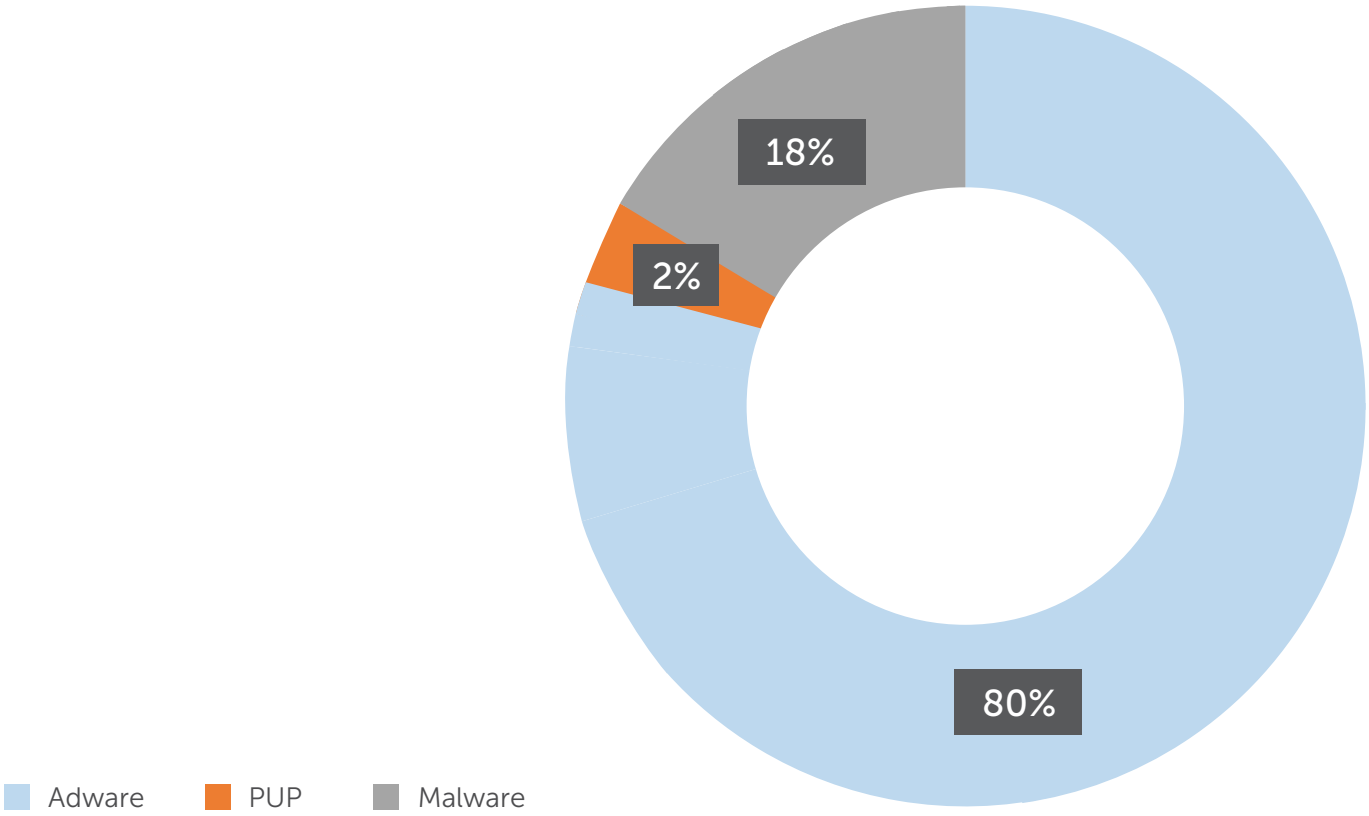
- Operator name and phone number
- Device ID and information
- Device location
- Device state

# Android Malware Collection by Quick Heal

| Month | Files Received |
|---|---|
| April 2014 | 147,894 |
| May 2014 | 434,742 |
| June 2014 | 440,705 |
| **Total Samples** | **1,023,341** |



# Android Category Detection



# Upcoming trends **for Android malware**

1

## Mobile Madware is not going anywhere soon

Madware is a popular term that is commonly used to refer to aggressive mobile ad libraries that bundle several apps within them and show up when those apps are run. Android users may be familiar with these ads as they often appear in the notification tray of the device and sometimes appear in the entire screen when an app is closed or the Home button is tapped. There are around 100 known ad libraries worldwide today, and a majority of them can be categorized as 'aggressive'. The phenomenon of Madware is not going to slow down any time soon, so Android users should be prepared to deal with such ads when they do show up.

2

## Fake apps on Google Play on the rise

Earlier, fake apps would only be available on third-party sources and only people who had 'sideloading' (a setting where third-party apps can be downloaded) enabled could install them. But now, even official apps on Google Play are not completely trustworthy as fake apps have begun to infiltrate this platform as well. For example, 'Virus Shield' was a fake app on Google Play that was downloaded close to 30,000 times. This app cost $3.99, so this amounted to a cool profit of $120,000 for the developer. Similarly, there are many more fake apps that users need to look out for. It is crucial to study the app developer and the app reviews before installing an application from Google Play.

3

## Remote access tools will be more widely implemented

Android malware is designed in different ways and is intended to perform several different functions. One attack vector that has been noticed recently is that concerning remote access tools. Via such tools like iDroidBot, Dendroid and more, an attacker can completely control an infected device with the help of a user-friendly control panel. This method is especially risky as far as banking information is concerned, and this is the data that attackers also go after. Banking credentials, credit card numbers and mobile wallets are especially vulnerable.

4

## Keyloggers a major threat on the rise

Just as on desktops and laptops, keyloggers are malicious programs that can capture and store the keys that are tapped on a device. So if a program knows that a user has visited a banking website or portal, it can record the keystrokes and then use this highly confidential data for financial gains. With the proliferation and spread of online shopping apps, this is an issue that gains even more importance. An effective security solution goes a long way in protecting against keyloggers and other similar functioning Android malware.

5

## Innovative routes into Android devices

Android malware is heavily dependent upon users installing a malicious program into their device. One method of entering devices that has not been used much, but is now coming to the fore, is the desktop. Hybrid threats that enter a PC and infect it, and then enter and infect an Android phone when it is connected have been spotted recently. In order to avoid such threats, users should ensure that they do not plug their data into unknown computers and they should also ensure that they have security software installed on the PC as well as the smartphone for hybrid protection. As the 'Internet of Things' begins to spread, more devices will become Internet enabled and a potential source of Android malware, so Android users need to be extremely cautious at all times.

6

## Android ransomware will continue to proliferate and evolve

Ransomware has existed over the Windows platform for many years now, and it is expected to evolve further with regards to the Android platform as well. With wide usage and increasing financial transactions over smartphones, this is an inevitable development and we do not expect it to slow down any time soon. Programs that lock a device and demand the payment of money to unlock the device will be found more frequently over the coming quarter. We expect increased attacks of ransomware over the Android platform to persist in the 3rd quarter of 2014 as well.

# Popular Android Blogs

The Quick Heal blog is a great source to learn about prevalent and predicted Android threats, and here is a gist of some of the Android malware related posts that you can read about.

1. **What is the best age for a child to get a smartphone?**
   This post explores the pros and cons about giving children smartphones at a very young age, and invites our users to share their insights and points of view.

2. **5 tips for online smartphone shopping nobody tells you about.**
   In this post we discuss the rise of online shopping, especially in India, and we offer you 5 safety tips that retailers don't want to talk about. If you are a fan of online shopping, this is a must read.

3. **Simple privacy tips for WhatsApp users.**
   WhatsApp has more than half a billion users across the world today and the brand itself is worth more than $19 billion. Here are some simple tips to keep yourself secure on WhatsApp.

4. **The rise of WhatsApp Plus and should you install it.**
   WhatsApp Plus is a clone of WhatsApp and functions in exactly the same way. However, it has several more features and cosmetic enhancements, but it may not exactly be legal. So should you install it?

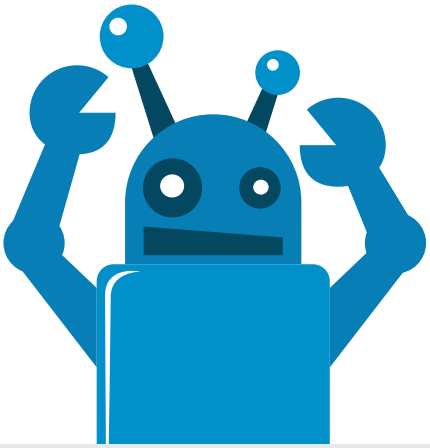
5. **Mobile ad libraries pose new security threats.**
   Aggressive ad libraries are dangerous to regular Android users, but far more dangerous to enterprise users due to the amount of crucial data that is involved. With BYOD now the norm, the number of app permissions and security risks that an employee carries is staggering.

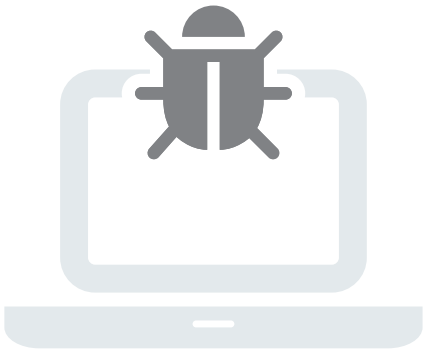
# Summary - Windows

With the rapid insurgence and widespread usage of smartphones and tablets, we expected malware strains afflicting Windows platforms to face a slow drop. However, this has not been the case recently, especially in the case of the second quarter of 2014. Quick Heal's Threat Research Labs have witnessed a rise as high as 90% in the samples of malware (from all collection sources) that we came across over the last 3 months, vis-à-vis the first quarter of 2014.

Reasons for this are manifold, and one possible explanation for this can be the continued usage of Windows XP on several machines, months after Microsoft has removed all technical support for the operating system. Several people still continue to work on this OS which has now become a landmine for zero-day vulnerabilities.

Another potential reason for this can be the rise of Advanced Persistent Threats, or APTs. These are threats that are aimed at specific individuals or entities and remain dormant over a period of several years. They remain undetected and record data over long periods of time, thus adopting the mantra of "Go low and go slow". Over time though, their impact can be highly dangerous. Another reason for this surge in high malware samples can be the various phishing scams and fake links associated with the recently concluded FIFA World Cup; or even the lack of adequate number of machines being protected with updated versions of effective antivirus an integrated security solutions. Either way, here are the top 10 malware samples received by the Quick Heal Labs over the last 3 months of April, May and June 2014.





# Top 10 Windows malware
## for Q2 2014

- AdWare.Agent.eng - **20%**
- TrojanDownloader.Filcout.r5 - **19%**
- VBS/Agent.HGQ - **17%**
- WebToolbar.SearchSuite.r5 - **8%**
- VBS/Dunihi.V - **7%**
- VBS/Autorun.LKI - **7%**
- Trojan.Sefnit.r5 - **7%**
- Trojan.Agent.g5 - **6%**
- W32.Autorun.Inf.Gen - **5%**
- AdWare.BHO.r6 - **4%**

## AdWare.Agent.eng

Adware.Agent.eng is a highly advanced and widespread form of adware that also comes under the category of 'Browser Hijacker'. In effect, it takes over an Internet browser to advertise several products that are generated by the malware author in conjunction with illicit ad libraries. As all forms of adware, this strain is also designed to provide financial gains for the author.

Unsuspecting users are taken to commercial sites as per the directives of the adware and several times, malicious codes are also present within these websites. So the risk here is twofold. Additionally, it also greatly affects the performance of an infected machine and its registry files.

## TrojanDownloader.Filcout.r5

While it may not be harmful by itself, TrojanDownloader.Filcout.r5 is risky because it downloads and installs other strains of malware or potentially unwanted programs (PUPs) that are far more severe in nature. This malware can be dubbed as a facilitator for other malware as it can target particular files on websites that contain exploit codes.

In turn, these codes allow websites to drop and run malicious applications on vulnerable systems. Moreover, it also permits cybercrooks to gain unauthorized remote access over infected machines. This malware is also known to download variants of the Sefnit malware family and it usually enters vulnerable systems through spam emails, infected USB/external drives, software downloads or compromised webpages.

## VBS/Agent.HGQ

VBS/Agent.HGQ is a worm that features high on this list and is unique due to the fact that it spreads itself via removale USB drives. Interestingly, if this worm is present in a machine and detects that a removable drive has been inserted into the machine, it quickly copies itself and spreads to every single folder within that removable drive. Furthermore, once it has infiltrated the removable drive it creates a shortcut link that points to its various copies on the drive.

It also conspires to steal crucial data and information such as the name of the PC, the user name of the account which is currently logged in, details about the operating system of the machine and various hardware identification numbers of the machine. This worm also opens a backdoor into the infected machine for remote hackers

## WebToolbar.SearchSuite.r5

Though not technically a virus, WebToolbar.SearchSuite.r5 shows plenty of malicious signs that suggest it needs to be considered on par with several viruses. This PUP showcases rootkit capabilities that hook down deep into operating systems on infected machines. It also carries out Browser Hijacking and other malicious activities that interfere with user experience.

It usually comes bundled with several custom installers of software products, and sneaks into machines stealthily. Once there, it modifies the default or custom settings of the browser and changes the home page, search settings and even other settings like Internet Explorer's load time threshold. Moreover, this PUP is also an ad-supported browser plugin and is capable of full functionality on Internet Explorer, Firefox and Chrome.

## WebToolbar.SearchSuite.r5

Though not technically a virus, WebToolbar.SearchSuite.r5 shows plenty of malicious signs that suggest it needs to be considered on par with several viruses. This PUP

showcases rootkit capabilities that hook down deep into operating systems on infected machines. It also carries out Browser Hijacking and other malicious activities that interfere with user experience.

It usually comes bundled with several custom installers of software products, and sneaks into machines stealthily. Once there, it modifies the default or custom settings of the browser and changes the home page, search settings and even other settings like Internet Explorer's load time threshold. Moreover, this PUP is also an ad-supported browser plugin and is capable of full functionality on Internet Explorer, Firefox and Chrome.

## VBS/Autorun.LKI

Similar to the worm VBS/Agent.HGQ, this worm also enters machines and spreads further via removable drives. However, VBS/Autorun.LKI has more severe and long lasting effects on the machines that it infects. This is what serves as the distinguishing factor here.

The details that are stolen and shared by this worm range from IP addresses of websites that are visited, a full history of all removable drives that have ever been inserted into the machine, all active windows and tabs in the web browser, the number and details of all users that have logged into the machine, details about the operating system and many more. It also grants remote control to hackers who can then run files and update files on the machine. Lastly, online usernames, passwords and URLs are also at risk.

## Trojan.Sefnit.r5

Trojans are highly capable and dangerous infections to deal with, as they are capable of carrying out several malicious activities once they enter a machine. Trojan.Sefnit.r5 is a prime example of this and is capable of stealing personal and confidential information, downloading more strains of malware and granting remote access of the machine to hackers and malicious parties.

Some of the most common attack vectors and methods of entry of this Trojan are spam emails, infected USB drives, bundled software and hacked websites. As the name suggests, a Trojan finds a way to enter a machine without raising any alarms and once inside, it has the ability to cause complete chaos.

## Trojan.Agent.g5

Another dangerous member of the Trojan family, Trojan.Agent.g5 is a harmful piece of software that looks completely legitimate. Once activated, it can accomplish minor irritations like pop-ups right to major security breaches such as complete system shutdown.

Amongst other things, this Trojan can hijack active browser sessions, slow down the performance of a PC, modify Windows registry, delete several saved files and programs, alter system settings and browser settings, alter desktop appearance and functionality, steal personal data and information, block system restore capabilities and most importantly, disable any antivirus program that is installed on the machine.

## W32.Autorun.Inf.Gen

Autorun functionality is not malicious by default and it is commonly used by removable drives and CDs/DVDs. However, malware authors commonly make use of this functionality to spread infections further. When this functionality is misused over the Windows platform, it falls under the category of Autorun.Inf.

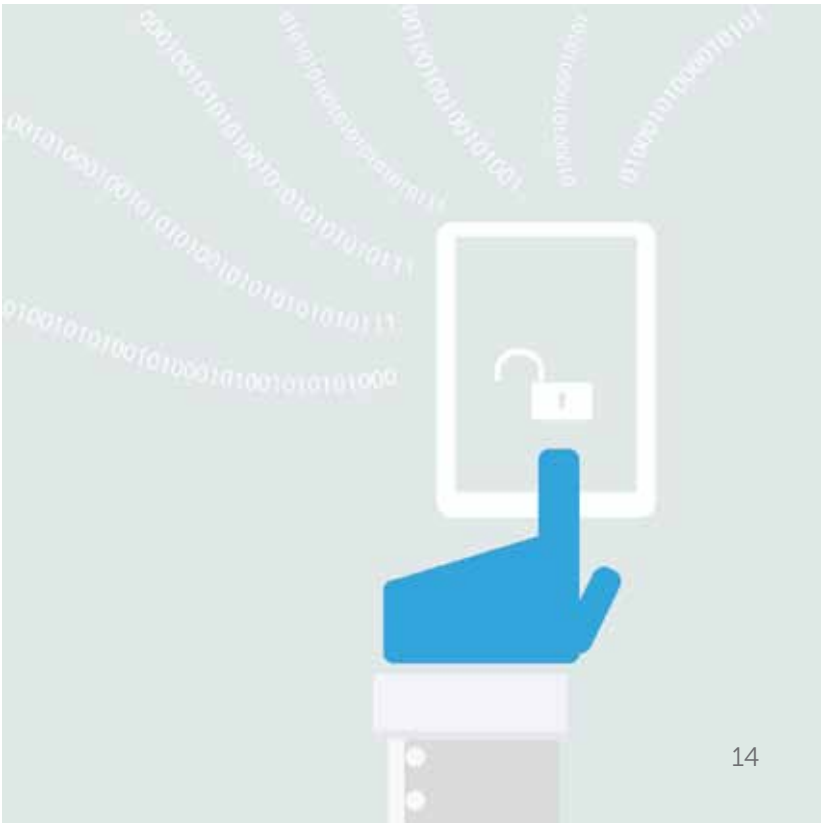
W32.Autorun.Inf.Gen is one such Autorun infection that has been noticed on Windows machines over the last quarter. When this file is opened, it instructs the operating system about what actions it should take with regards to certain files; so it is a

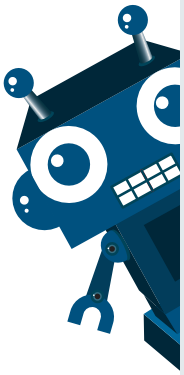
highly potent and dangerous infection to deal with. Since it gets embedded into the root of a targeted drive it also proves to be very difficult to detect and remove from a system.

## AdWare.BHO.r6

BHO stands for Browser Helper Object and this is a module that works as a plugin for Internet Explorer, so as to add more functionality. Adware.BHO.r6 is a variant of adware that takes advantage of this functionality in order to meet the malware authors' malicious intent. In order to enter into and infect a machine, this adware needs to be manually installed or dropped by another malware that is already installed on the machine.

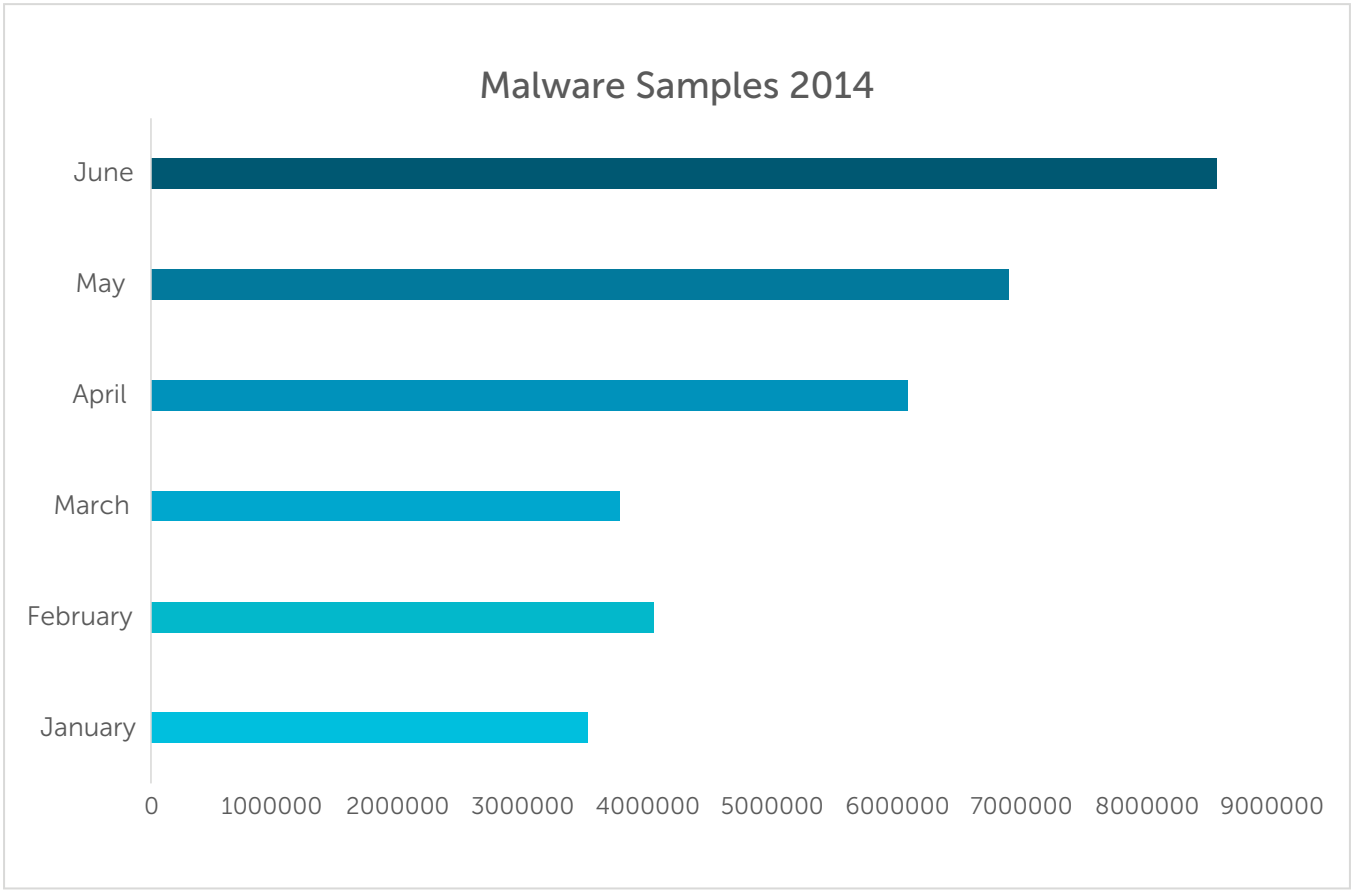
Once within a PC, it disguises itself as an Internet Explorer plugin and modifies the home page of the browser with several ad-fuelled extensions. This allows the adware to point an unsuspecting user to a website which contains malware. In effect, this program converts a machine into a source of income through unknown visits/clicks to several ad libraries without the user's knowledge. This process is commonly known as 'Click Fraud'.





# Windows Malware Collection by Quick Heal

| Month | Apr-14 | May-14 | Jun-14 | Total |
|---|---|---|---|---|
| Count | 6,059,901 | 6,868,846 | 8,535,416 | **21,464,163** |



# Analysis of CryptoDefense Ransomware

By definition, ransomware is a highly advanced software that locks down a machine and takes control over it. Once it has locked a PC down, it demands the payment of some money, or a 'ransom'. The malicious program also claims that it would unlock the machine only upon the payment of said ransom and also threatens the victim by claiming to be from some higher authority. This induces a sense of panic within the victim which then pushes him/her to actually make the payment to free their 'kidnapped' machine.

CryptoDefense is an advanced strain of malware that the Quick Heal Labs came across this past quarter. This malware uses Microsoft's inbuilt infrastructure and Windows API in order to generate encryption and decryption keys that carry out the end goal of the program. CryptoDefense targets the following operating systems:

- Windows XP
- Windows Vista
- Windows 7
- Windows 8

Once a target is honed down upon and the malware is injected within it, CryptoDefense performs the following activities:

- It deletes shadow volume copies.
- It scans the entire system and encrypts data such as text files, images, videos and Office documents.
- It takes a screenshot of active windows and sends it to the command and control server.
- CryptoDefense then generates keys at the user's end and sends it to the remote server.
- Every folder is then encrypted.
- Details about the required payment method and payment site are then stored in each folder.

The ransomware then proceeds to use scare tactics on a user by claiming that they have 4 days to pay the ransom of $500 (in Bitcoins) or else the amount will be doubled. And if no payment is received within a month, then the files are permanently encrypted and seemingly lost forever. The payment site that is referred to is located on a TOR network so is pretty much untraceable. Additionally, the files are encrypted using RSA-2048 encryption, rendering them useless to brute force decryption methods.

# Upcoming Trends **for Windows Malware**

1

## Worldwide localization of ransomware scare tactics

As observed in the individual case study of CryptoDefense as stated above, ransomware is increasingly becoming more advanced in nature. Attackers are finding new ways to deploy ransomware, new ways to encrypt private information and even more innovative scare tactics. Localized ransomware authors are now creating templates and impersonating well known law enforcement agencies of specific regions.

In the midst of our analysis, we came across several templates localized to the native languages of Switzerland, Germany, Austria, France, Netherlands and many more. This is a trend that we expect will continue and increase over the coming months. The reason for this is that potential victims will fear their national law agencies (whose names they are familiar with) more than a far-fetched international law agency, hence making this a highly effective scare tactic.

2

## Botnets and APTs make a hacker's dream team

Botnets are some of the most dangerous existing security threats around, and Advanced Persistent Threats (APTs) are high-risk threats that are on the rise. State-sponsored attacks and malware that target individual business or Government entities pose massive security threats, and when these two mammoth risks combine, it is a recipe for disaster. As a result, hackers are increasingly using botnets to steal information and launch large-scale malicious networks during targeted attacks.

Once targets are chosen, hackers carry out long-term and 'persistent' attacks using various methods. Moreover, many compromised machines unconsciously participate in such attacks. The malicious software that is used by botnets is often customized based on weaknesses in the targeted systems as well. Increasingly hard to detect in their latent or infected phase, these malicious programs mutate at a rapid pace, thus making it hard for signature-based detection techniques to catch them.

3

## Rise of Bitcoin mining programs

Bitcoin mining has been gathering speed in the past few months, and this is a phenomenon that is expected to continue in the near future as well. Bitcoins are one of several new-age digital currency formats, and it has become rather popular. So much so that many people treat it on par, or even as more valuable, than real money. Naturally, malware authors and hackers have followed suit and have devised ways to steal this currency from its rightful owners.

Bitcoin mining applications are relatively easy to develop, and they are silently pushed to networks without the knowledge of unsuspecting users. Such applications usually come bundled with software downloads, especially pirated and illicit downloads. The exact process of Bitcoin mining depends on the system resources of an infected machine such as hardware configuration, bandwidth usage and more. This is a trend that will not buckle down anytime soon; Bitcoin owners have been warned.

4

## Emergence of PoS malware

Another upcoming security threat to look out for is PoS (Point of Sale) malware attacks. A PoS simply refers to the place at which a retail transaction is completed, usually with a debit/credit card. Increasingly, botnets are being devised which infiltrate the machines that these cards are swiped on, and these machines are infiltrated with 'Brute Force' attacks. Interestingly, these attacks are termed as "BrutPoS".

A brute force attack is a dangerous method that breaks down a password by entering all possible combinations of characters. The initial phase makes use of default and commonly used usernames and passwords, and then it becomes more advanced. The infected system begins to connect to Port 3389, and if it finds the port open, it adds the IP address to a list of servers that can later be targeted by BrutPoS attacks. So, card users need to be aware of this threat which is spreading at a rapid rate.

# Conclusion



The second quarter of 2014 has witnessed an abnormal surge in malware samples across all platforms and this can be attributed to several different causes. The Quick Heal Lab is constantly on the lookout for such samples so that up-to-date signature detection and removal can be carried out seamlessly.

The Android platform has turned out to be massive hunting ground for malware authors and adware strains; in spite of this a large majority of Android smartphone and tablet users have resisted the installation of effective security solutions for their devices, and this plays right into the hands of the bad guys.

Cybercriminals and malicious software authors are constantly devising methods to penetrate home and enterprise networks. In this war of attrition, the biggest weapon users can possess is that of information on the latest threats, attack methods and the precautions they can take.