Quick Heal

Security Simplified

Quarterly Threat Report

for Windows & Android - Q1, 2014

Q1

Threat Report:

1st Quarter, 2014

Table of Contents

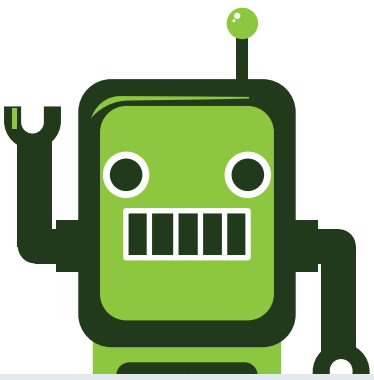
Introduction

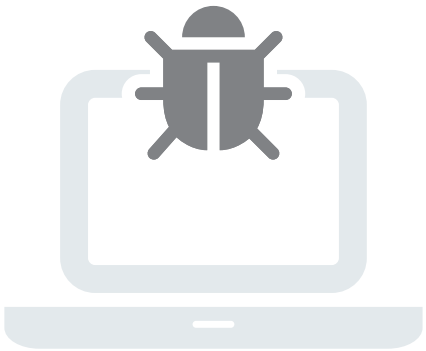
The first quarter of 2014 has been quite an eventful one in the IT Security World. The Quick Heal Threat and Research Center detected the top 10 Windows malware, XP was pulled out of support leaving millions of XP users wide open to attacks, and of course the Heartbleed mayhem. This security threat report gives you a brief on the top Windows malware, their detections, upcoming malware trends, and an insight into Heartbleed.

With close to 80% of smartphone owners adopting Android as the mobile platform of their choice, malware developers are having a field day developing social engineering tricks and software to target Android users. The massive rise in Android phone and tablet users and the unregulated nature of Android app markets, has led to an exponential growth in the numbers of malware as well.

Smartphones are slowly replacing PCs at homes and offices now, so the avenues for malware infection are consequently growing as well. These devices have become treasure troves of personal data and information, and this has been attested by the prominence of Android adware, ransomware and botnets. Social engineering tricks and fake antivirus apps have also now come to the forefront.

The Quick Heal Threat Research & Response Team has received hundreds of thousands of samples of Android malware and a common trend that we have noticed is that Android adware is the most common form of malicious program for this platform. Adware usually accompanies legitimate seeming apps and then siphons off private data from the device to remote servers. Sometimes, it also opens a backdoor for other programs and malware to enter the device.





Top 10 Windows malware
for Q1 2014

- AdWare.Agent.eng - **25.19%**
- VBS/Agent.HGQ - **23.8%**
- VBS/Autorun.LKI - **12.95%**
- VBS/Serverons.A - **8.20%**
- VBS/Dunihi.V - **6.80%**
- Backdoor.Vercuser.A3 - **5.99%**
- VBS/Dunihi.OL - **5.77%**
- VBS/Crypter.A - **4.22%**
- AdWare.ShadyOffer.d - **3.64%**
- Trojan.Sirefef - **3.32%**

AdWare.Agent.eng

AdWare.Agent.eng is a complex adware which is spread over the Internet to carry out detrimental damage.

- It is identified as a browser hijacker. It is designed to take over Internet browsers to advertise products for the malware author.
- Once this malware infects a system, it serves the user with objectionable advertisements for financial gains.
- The malware opens up random websites without user consent.
- The malwares main purpose is to make money from unsuspecting users by redirecting search results to various commercial websites which might also contain malicious codes.
- It is also known to affect computer performance and mess up its registry entries.

VBS/Agent.HGQ

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

- If this worm detects any removable drive in a computer, it copies itself into every folder on that drive. It also creates a shortcut link file pointing to its copy in the removable drive.
- Once inside the targeted computer, the worm steals data such as:
  - Name of the computer
  - User name of the person currently logged on
  - Version of the operating system
  - Hardware identification numbers
- The worm can also allow a hacker to get a backdoor access to the victim's computer.

VBS/Autorun.LKI

VBS/Autorun.LKI works in the same fashion as VBS/Agent.HGQ. However, the way it affects the victim's computer is different.

- The worm can allow hackers to access and control the victim's computer to:
  - Run files
  - Steal online user names, passwords and URLs
  - Update files
- It steals the following information from the victim's PC and sends it to the hacker:
  - IP addresses visited
  - USB drives
  - Active windows
  - Users logged on the machine
  - Operating system

VBS/Serverons.A

Worm:VBS/Serverons.A is a worm crafted to steal information from the victim's machine and send it across to the hacker.

- This worm spreads via infected removable drives (such as USB keys or portable hard disks).
- The worm hides all existing shortcut files (.lnk) on the infected removable drive, and then creates its own shortcut file (help.lnk). This is to lure an unsuspecting user into opening the file thinking it to be a legitimate help file.
- Once installed on the victim's machine, the worm collects the following information:
  - User name
  - The computer's name
  - The version or edition of Windows present on computer

VBS/Dunihi.V

This malware belongs to the worm family. Itusually infects computers via files downloaded online or torrents. Once inside the targeted system, it performs the following actions:

1. Gives a hacker access and control over the compromised PC.
2. It steals user information and sends it to a remote server.

Backdoor.Vercuser.A3

Backdoor.Vercuser.A3 is a destructive and notorious backdoor Trojan that terribly corrupts targeted systems.

- It is designed to steal users' sensitive information for illegal benefits.
- The malware carries out several malicious activities in the background silently.
- It can not only change the victim's system settings and eliminate important files, but can also keep redirecting users to unknown websites without their consent.
- The malware throws commercial ads and bogus notifications whenever the victim is online. This causes many executable programs to malfunction and the system to crash.

VBS/Dunihi.V

VBS.Dunihi is a worm that spreads through removable media and may open a back door on the compromised machine. It keeps working in the background stealing user information, and downloading additional threats.

VBS/Crypter.A

VBS/Crypter.A is detection for malicious Visual Basic script (VBS) files encrypted with a malware encryptor that uses base64 encoding to hide malicious files. The Trojan does not have a distinct functionality, rather it is used as a carrier of other malware.

AdWare.ShadyOffer.d

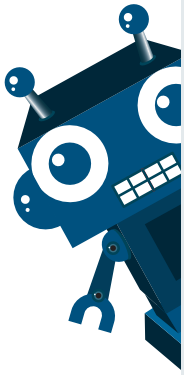
When AdWare.ShadyOffer.d infects a system, it adds a new value to the registry, which enables it to launch itself automatically. Once executed, the adware performs the following actions:

- In the background, this adware installs a browser add-on in order to steal personal information and send it to third parties.
- It can hijack browsers, download more malware on infected systems.
- It generates unwanted pop-up messages.
- The adware can update Windows, Java, Flash Player, browser, etc., without the user's knowledge.
- Executes malicious code to run malicious tasks.
- Spreads to removable drives and other PCs quickly.

Trojan.Sirefef

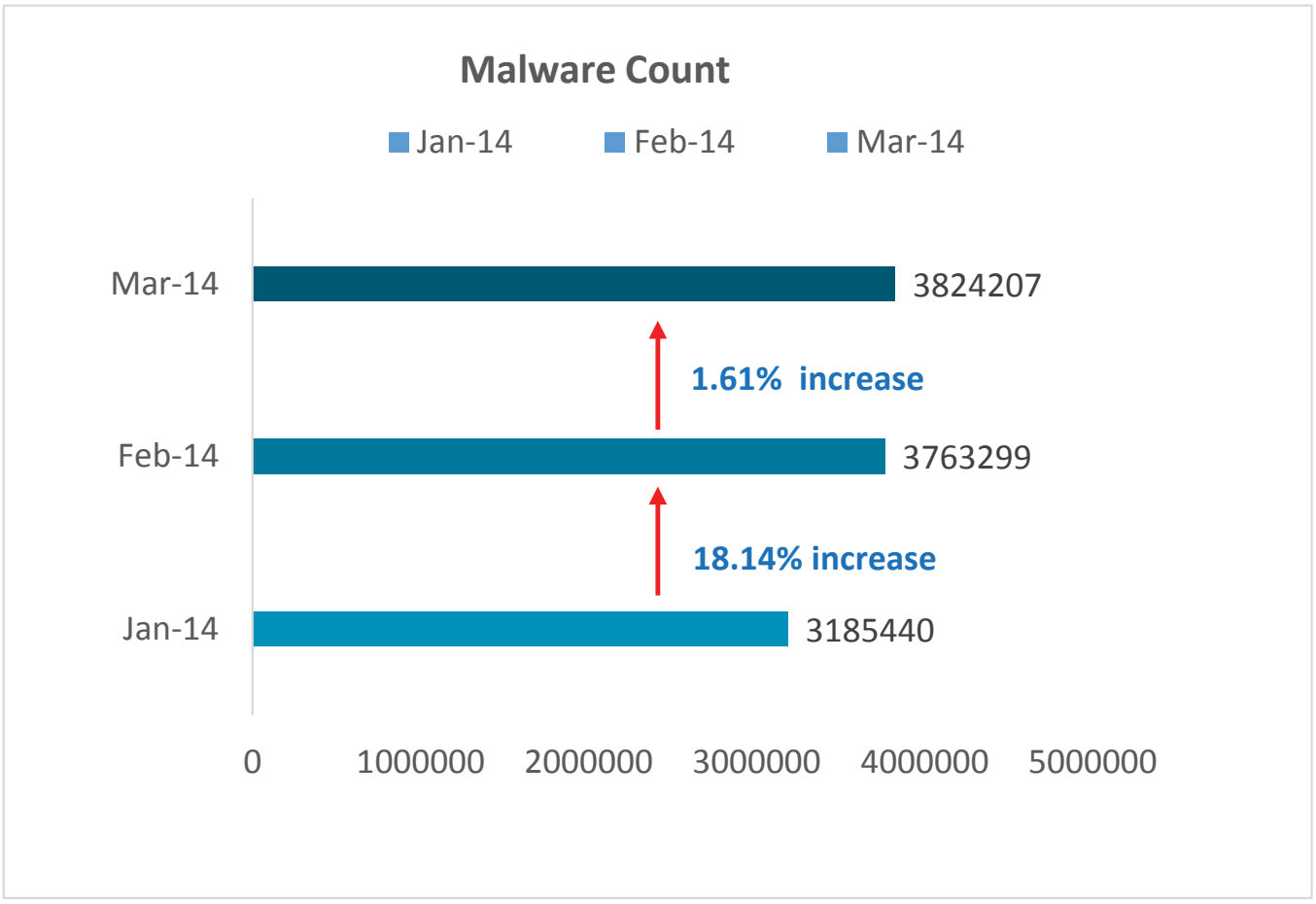
This Trojan malware belongs to the Sirefef family which uses stealth to hide its presence on infected PCs. Trojans in this family can:

- Download and run other files
- Contact remote hosts
- Disable security features
- Change search results to generate money for hackers
- Stop and delete security-related services
- Turn off Windows Firewall
- Infect files/Uses stealth
- Intercept and hijack network traffic
- Create folders to store other malware



Windows Malware detection by Quick Heal

Month	Jan-14	Feb-14	Mar-14	Total
Count	3185440	3763299	3824207	**10772946**



Upcoming trends
for Windows malware

1

Windows XP becomes a lawless land

April 8, 2014 was a monumental day in the history of Microsoft Windows as one of the most loved and used operating systems, aka Windows XP, was finally pulled off life support. Microsoft will no more release security patches or updates for XP and will not offer technical support either. However, a large percentage of people around the globe still use Windows XP due to several reasons. Malware authors now know that they can target Windows XP and millions of potential victims, without the corrective and security measures of Microsoft to stop them. This is going to render XP as a playground for malware and lead to a state of perpetual zero-day threats. Our advice; stay away from Windows XP.

2

Ransomware authors realize the economic viability of encrypting and locking down victims' machines

As the name suggests, ransomware is a highly malicious program that locks down a machine and does not provide access to the user until some money, or ransom, is paid. Taking PCs hostage is nothing new. However, in the coming months ransomware is expected to become even more advanced and malicious. After all, all they need to do is encrypt the data that is already present on a machine. Organized cybercrime bodies have now realized that there is tremendous potential here and it can actually become a feasible model, so they are scaling up the attacks so that they can make more profits. Moreover, they have also started impersonating legal law agencies so that people believe they are actually paying a legal fine, and not a ransom.

3

Botnets to become more stealthy and social

Botnets are large worldwide networks of zombiefied machines that spread malware further, without even knowing that they are infected. These machines send out spam emails or initiate DDoS attacks unwillingly, and it is widely expected that such networks will become more advanced and stealthy in the coming months. Targeted attacks over social media networks that use social engineering tricks are also expected to show up in increased numbers. After all, it just takes one simple click to from an unsuspecting victim to activate that PC as a part of a botnet. So, stay away from suspicious links and pages.

4

64-bit malware agents spotted in the wild

Malware authors mandatorily need to react to changes that occur in the computing world so that they can transform their malware to reach more people and cause greater mayhem. As a result, as more people have now started switching to 64-bit operating systems, malware authors have also started creating 64-bit malware agents. This is a trend that is expected to continue for the foreseeable future as well. In a sense, this move will future-proof the malware variants that adopt this functionality as more users around the world will eventually shift to 64-bit operating systems and web browsers as well.

5

Cloud-based computing will face enhanced data security threats

Cloud computing is the answer to ever-changing industry needs and provides increased flexibility and accessibility. Home users and enterprise users alike make use of this feature and make full use of the associated benefits as well. However, data breaches and data loss are risks that are even more pronounced over cloud platforms. Account hijacking is a threat that can lead to severe leakages and financial hits. Weak and insufficient passwords also contribute to this and this is a trend that we do not believe will go away anytime soon. Cloud storage and accessibility makes life simpler for several tasks, but also makes things harder in case of security breaches.

An Excerpt on Heartbleed

Heartbleed: Exposing millions of passwords online

Data leaks have been around for years, but when a bug on the scale of Heartbleed comes around, the entire computing world sits up and takes notice. OpenSSL technology is used by hundreds of web services around the world, and Heartbleed is a security bug that pointed out a serious flaw in the way this open source technology was adopted by everyone. As a result, any service that made use of OpenSSL had their user passwords exposed for more than 2 years.

This flaw extended to hugely popular services like Google, Facebook, Pinterest, Dropbox and more and showed the whole world that sometimes, even the best laid plans (and passwords) can be rendered completely vulnerable due to the negligence of others. Our comprehensive list of web services whose passwords need to be changed can be viewed here.

Unfortunately, since Heartbleed is a bug that affects the servers of these popular services, there is not much that users can do to combat this apart from changing their passwords. The hope is that web services have moved quickly to minimize the damage posed by Heartbleed and that all user passwords have now been secured. These 3 important things that one should know about Heartbleed will also prove useful.

Quick Heal would also like to warn its users to be wary of fake password reset emails and hoaxes that are doing the rounds after the outbreak of Heartbleed. The widespread panic that has been caused by this bug is something that malware authors are taking undue advantage of and users should be aware of these security risks.

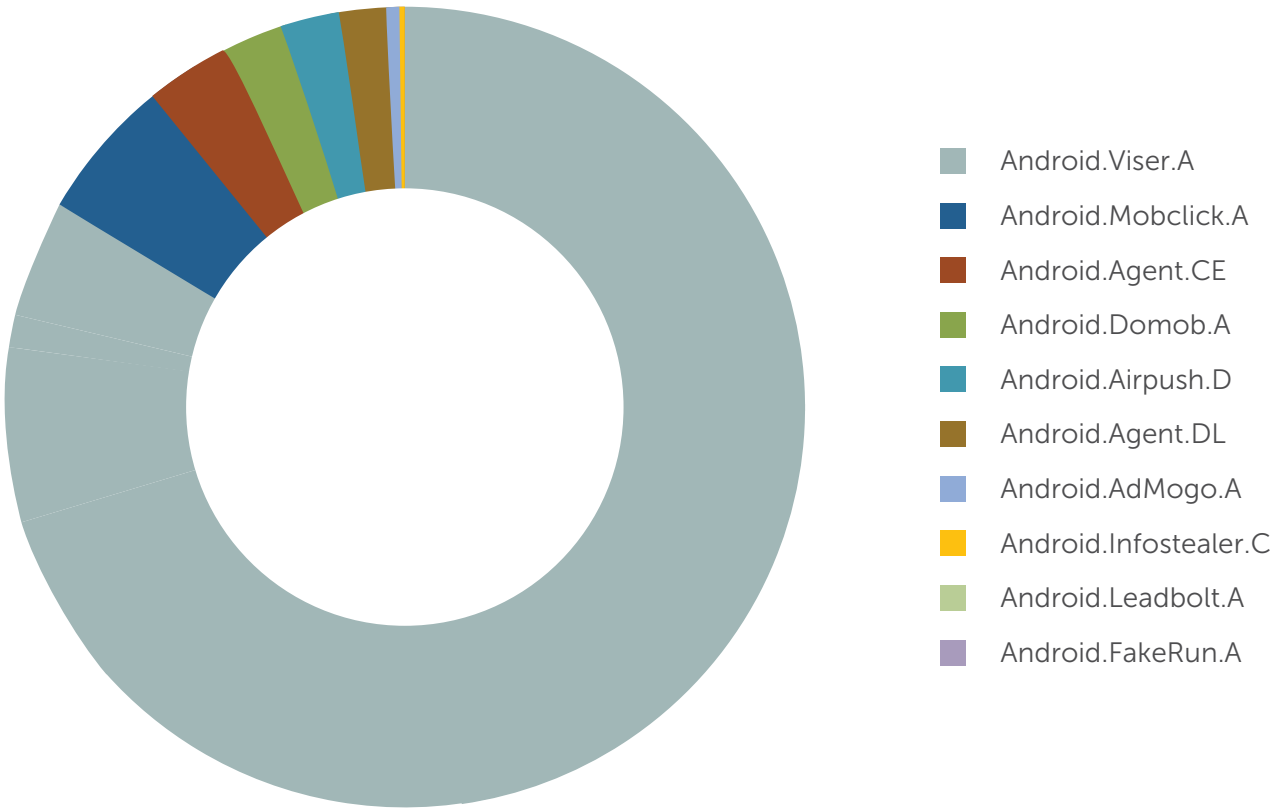
Malware authors have moved on to social engineering tricks and fake antivirus for the popular Android platform.

The Quick Heal Threat Research & Response Team has received hundreds of thousands of samples of Android malware. Android adware is the most common form of malicious program for this platform. Keeping that in mind, here are the most common Android malware that was detected by us from the months of January 2014 to March 2014.

Android Threat Report:

1st Quarter, 2014

Top 10 Android malware **for Q1 2014**



Android.Viser.A

Adware on Android was the single biggest threat to the platform over the last quarter, and the most prominent variation that we found was Android.Viser.A. A highly intrusive and invasive program, this adware gained access through several downloadable applications. Like all forms of malicious adware, it shows unwanted and unnecessary ads. Moreover, removal of the adware requires the removal of the infected application, or the installation of another application that can spot and detect this particular strain of 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

Unsurprisingly, the next biggest threat to the Android platform was also a variant of mobile adware. Android.Mobclick.A is your typical adware that performs all the malicious activities we have come to expect. It accompanies seemingly innocent looking apps and infiltrates Android devices. Once installed, it displays unwanted advertisements and popups and also sends out 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.CE

Coming in next in line is a form of Android malware that can best be described as a Trojan. At its worst however, Android.Agent.CE can be described as an extremely dangerous threat that can suck all the data out of any given Android device and leave it as a shell of its past self. Such forms of malware interrupt the normal operations of a device and simultaneously gain access to the private information that is stored within. Some examples of what this malware is capable of doing are as follows:

- Sends text messages to premium-rate numbers
- Tracks GPS locations and history
- Logs keystrokes and passwords
- Steals contact details and images

Android.Domob.A

Yet another form of adware that aggressively pushes ads and notifications forward is Android.Domob.A; a heavy duty advertisement library. It comes bundled with certain Android applications and performs many malicious activities over the course of time. Needless to say, this adware is highly privacy invasive and siphons off 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.Airpush.D

Certain forms of malware push notifications within applications and other interfaces, but a distinguishing characteristic of Android.Airpush.D is that it pushes intrusive ads into the notification bar of an Android device. Moreover, this adware also reads existing bookmarks that are saved in the device and then modifies them. Altered bookmarks

can inadvertently lead an Android user to fake websites, phishing links or malicious apps that carry 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.Agent.DL

Once within an Android device, this Trojan actively pulls other malware and attempts to grant access to them. With a URL address included within the malware, other files are downloaded from that URL. Android.Agent.DL is part of a 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.AdMogo.A

One of the most commonly seen Android threats in the wild over the last quarter has been Android.AdMogo.A. Like all other forms of Android adware, this variant also severely compromises the user device and personal information. By misusing several user permissions once it enters an Android device, this adware contributes to the loss of the following data:

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

Android.Infostealer.C

Like all other Trojans, this variant of Android malware enters a device through programs that seem safe and harmless. However, once within a device, Android.Infostealer.C systematically leaks all kinds of sensitive and confidential data to remote servers. Once installed, this malware needs the accompanying app to be removed completely, or it needs the installation of another app in order to remove its traces from the device. Along with sending text messages to premium-rate numbers, Android.Infostealer.C also does the following:

- Leaks device location through GPS
- Leaks SIM card information
- Leaks device data like IMEI & IMSI
- Leaks subscriber ID
- Reads phone state
- Leaks Line Number

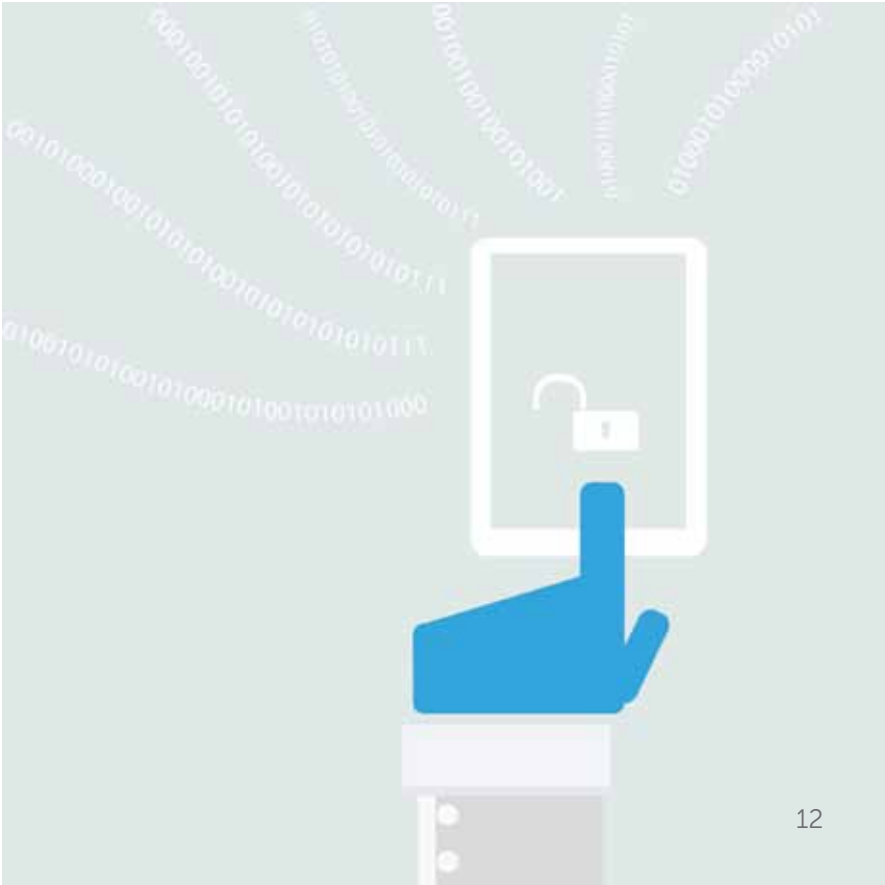
Android.Leadbolt.A

Out of all the other forms of adware that was found in Android devices over the last quarter, Android.Leadbolt.A was unique because it regularly pushed pornographic ads rather than regular ones. Moreover, this variant also created shortcut icons on the homescreen of Android devices. Along with serving up obscene and distasteful content, this adware also served the following data to remote servers:

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

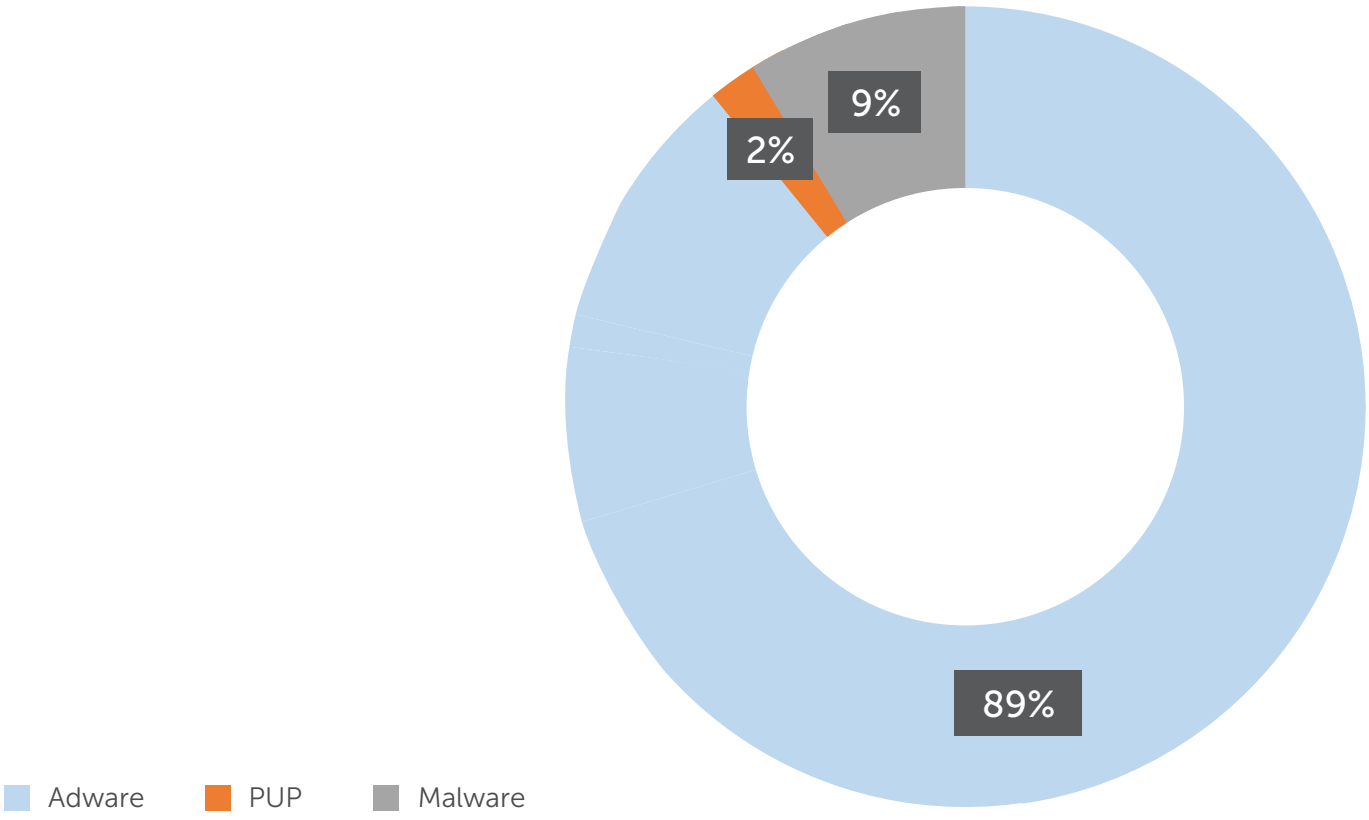
Android.FakeRun.A

Mainly found in the US, this variant of Android mobile malware pushes ads forward and urges Android users to give it a 5-star rating. Doing so enables Android.FakeRun.A to reach a wider audience and garner more eyeballs and downloads. While the Trojan claims to stop ad-modules from functioning, it actually carries 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.



Android Malware detection **by Quick Heal**

Month	Files Received
Jan-14	129,780
Feb-14	169,766
Mar-14	155,702
Total Samples	**455,248**



Upcoming trends **for Android malware**

Thanks to the open-source nature of Android and the widespread usage of the platform, malware developers regularly target this OS. Security is an ongoing concern and here we outline some of the potential threats and trends that could disrupt usage and draw malware towards Android.

1

Preying on victim's social needs

Social network usage and choice has never been higher, so there are bound to be many fake apps that attempt to lure people into giving out their personal details. Illegitimate versions and fake news stories can drive interest to viral levels and this is an Android mobile security threat to be wary of.

2

Fake apps doing the rounds

Unauthorized third-party sources are known to be the playgrounds for nefarious and fake apps. However, fake paid apps that are designed to steal user's money are now showing up on Google Play as well. The store has a system to verify and certify authentic developers. But malicious developers always find a way to get through for a short period of time. As users, always check the authenticity and the credibility of a developer before installing any application.

3

Continued dominance of adware

85% of malicious programs on Android were adware over the last quarter. This presence of adware shows no signs of abating. Vast ad libraries will continue to be present over innocent seeming apps and they will aggressively push forward unwanted advertisements and notifications. Moreover, they will create unwanted icons on homescreens, change saved bookmarks and also leak private user information.

4

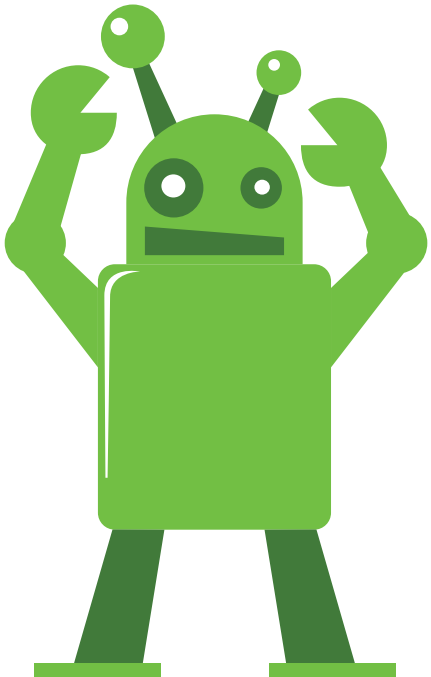
Rise of sinister rogueware and ransomware

Rogueware and ransomware have existed over the Windows platform and infiltrated PCs for many years now. Their presence is guaranteed to increase over the Android platform as well. Programs that lock a device and demand the payment of money to unlock the device will be found more frequently over the coming quarter.

5

Keeping the backdoor open

Once a malicious app enters an Android device it can perform several risky activities. However, the most dangerous thing it can do is open the door for its friends to come in as well. With advanced Command & Control servers on the rise, malicious apps will be remotely able to let in other malware and also leak out sensitive and confidential information.



Some quick facts **about Android malware**

- Roughly, 97% of all mobile malware around the world is designed to target Android.
- A majority of this malware comes from Middle-Eastern and Asian third-party sources.
- One in three apps in unofficial marketplaces are loaded with malware.
- 'Virus Shield' was a fake app on Google Play that was downloaded close to 30,000 times. It cost $3.99. Apparently, Google is now refunding the people who purchases this bogus antivirus app.
- Approximately 18% of Android users are still on old versions like Froyo (2.2) & Gingerbread (2.3). That equates to around 180 million devices globally.
- Permission pileup refers to the process where installed programs ask for more app permissions whenever they are updated. This is a common attack source.
- Cisco says that mobile malware constitutes about 1.2% of the total malware that they have observe over all their deployed networks.

Ways to keep your Android device secure

With such rapid installation and activation of Android devices across the world, knowing how to secure these devices has become imperative. There are many tips that users can easily put into practice that will ensure the security of their smartphones. Such tips can be adopted by enterprise users who adhere to BYOD policies and to home users as well.

Stay aware about mobile risks

The best way to ensure safety is to be aware of the various tricks that Android malware uses to infiltrate devices. Apps and programs are the single biggest source of malware, so users should always study the permissions that an app is asking for upon installation. Moreover, it is highly advisable to refrain from downloading apps from unofficial third-party sources. Always install apps from Google Play only.

Be wary of unsecured Wi-Fi networks

Free Wi-Fi available in public places is a great way to access the web on the move, but there are several ways in which such networks can prove vulnerable. Snoopers can easily intercept and steal data over unsecured Wi-Fi networks, so these should be avoided, especially while dealing with sensitive information. Our blog on the dangers of unsecured Wi-Fi networks can be referred for more information.

Be cautious while carrying out online purchases

With e-commerce portals making their presence felt over Android and coming out with snazzy apps and user interfaces, more and more people are purchasing products through these apps. Online shopping is fun, but not at the cost of security. Without the right safety measures and precautions, financial details can be easily lost or stolen. Here are some online shopping tips over smartphones that nobody really tells you about.

Comply with foolproof BYOD security policies

Organizations that encourage BYOD policies often face the repercussions that come with employee negligence and uncontrolled app downloads. In a situation like this, setting up clear, simple and transparent security policies becomes absolutely necessary. When all devices are connected to the enterprise network, it is a major risk when one employee downloads a malicious copy of Flappy Birds. Proper security policies need to be defined and adhered to in order to avoid widespread mayhem.

Embrace an effective and feasible security suite

Where there are risks, there are also solutions. Security suites for Android devices have now become more than just a luxury, they are a necessity. Without proper security in place, the world of Android devices will become a lawless and dangerous place, so everyone who owns an Android should acquire a security solution to go with it. Just as PCs without an antivirus will always be susceptible to all kinds of threats, an Android without a security suite will always remain vulnerable.

Conclusion

The end of windows XP support might result in a plethora of attacks aimed at exploiting vulnerabilities known and unknown. The risk of ransomeware has not disappeared rather malware authors have now realized the economic viability of it and are honing up their skills to present even craftier malware. Cloud-based computing is another avenue that cyber crooks might just dive into.

Smartphone access and purchases have nowhere to go but upwards, especially as advanced technology is now getting cheaper with every passing month. Malware developers target platforms by the numbers and simply put, Android is the platform where a majority of the people around the globe operate. More online transactions and banking operations are also being carried out over smartphones, so the need for security layers in Android has never been more pronounced.

Cybercriminals will continue to devise new ways to monetize Android malware and it is up to users to ensure that their accounts, social networks, private data and contacts are secure. Google has taken several steps to regulate these devices but there is only so much they can do. As Android malware evolves and gets smarter, so should we.