Mobile malware: A network view

Black Hat Mobile Security Summit – London 2015

MOTIVE
BY ALCATEL-LUCENT

Table of contents

INTRODUCTION

This paper is based on a presentation given at the Black Hat Mobile Security Summit held in London in June 2015.

Mobile devices are becoming the target of choice for cybercriminals. This paper will provide an in-depth view of the mobile malware that is currently active on the Internet. It describes the infection rates, what the malware does, how it is monetized and the impact it has on network resources and the user experience.

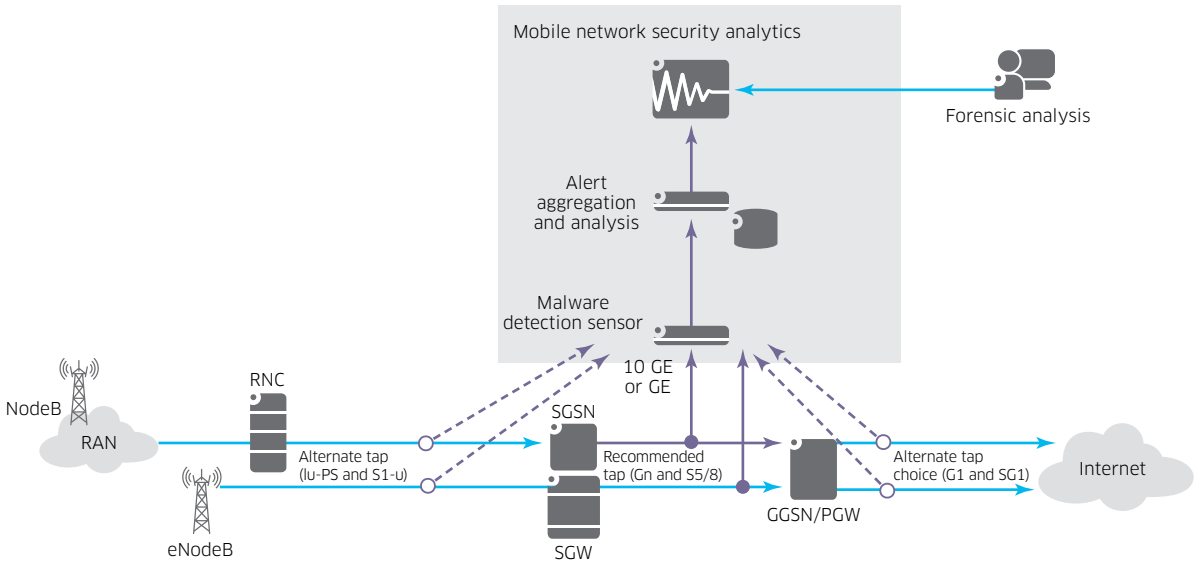
Motive Security Guardian, Alcatel-Lucent's network-based malware detection system, is deployed covering close to 100 million devices in major mobile carriers in the United States, Europe, Asia and the Middle East. It uses deep packet inspection (DPI) technology to detect malware command and control (C&C) traffic to identify the malware infection. Aggregated statistics on the infection rates for malware in these networks has been reported in regular quarterly **malware reports**. This paper leverages the most recent aggregated information from these deployments.

We will start with a brief description of where the data comes from and describe how C&C traffic is used to accurately detect and positively identify the malware. We then review the overall malware infection statistics for mobile devices, including the infection rate, the type of malware involved and the types of devices that are infected. We provide a summary of the top malware infections seen in mobile networks, outlining what the malware does, how the device is infected, the impact on the network and the impact on the user experience.

Monitoring malware in the mobile network

Figure 1 illustrates how the Motive Security Guardian is deployed in the mobile network. The system consist of multiple detection sensors deployed in the mobile network connected to a centralized Alert Aggregation and Analysis system that is usually deployed in the service providers data center.

Figure 1. Deployment diagram



1
Mobile malware: A network view
Alcatel-Lucent

The detection sensors are deployed on taps on the Gn interface (3G) or S5/S8 interface (4G). These monitor the GTP-C and GTP-U traffic between the serving gateways (SGWs) and PDN gateways (PGWs). Alternatively, they can tap the S1-u or Gi interfaces.

The GTP-C traffic contains control sequences to set up the tunnels to carry the mobile Internet traffic. The system monitors this to extract session identification information such as the international mobile subscriber identity (IMSI), international mobile equipment identifier (IMEI) and access point name (APN) and to provide a mapping between the IP addresses used in the tunneled data traffic and the endpoint devices. The IMSI identifies the user and their mobile carrier. The IMEI identifies the mobile device type and manufacturer. This information is used to map malware alerts to specific devices.

The GTP-U provides the tunnels to transport data traffic between the mobile devices and the Internet. The system decapsulates and looks for evidence of malware communications within the data traffic. It uses a snort-based detection engine with customized detection rules to look for:

- Malware C&C traffic
- Exploit attempt
- Evidence of distributed denial of service (DDoS) activity
- Hacking activity

For the most part the detection system uses malware C&C traffic to positively identify malware infection with a high degree of accuracy.

When malware traffic is detected, the detection event is sent to the central analysis system. The event consists of the IP addresses and ports associated with malware communication, a malware identifier, timestamp and other metadata about the alert. The system can optionally capture the trigger packet for the event. The analysis system uses the IP address from the alert to associate it with a specific user/ device and stores the event in a database.

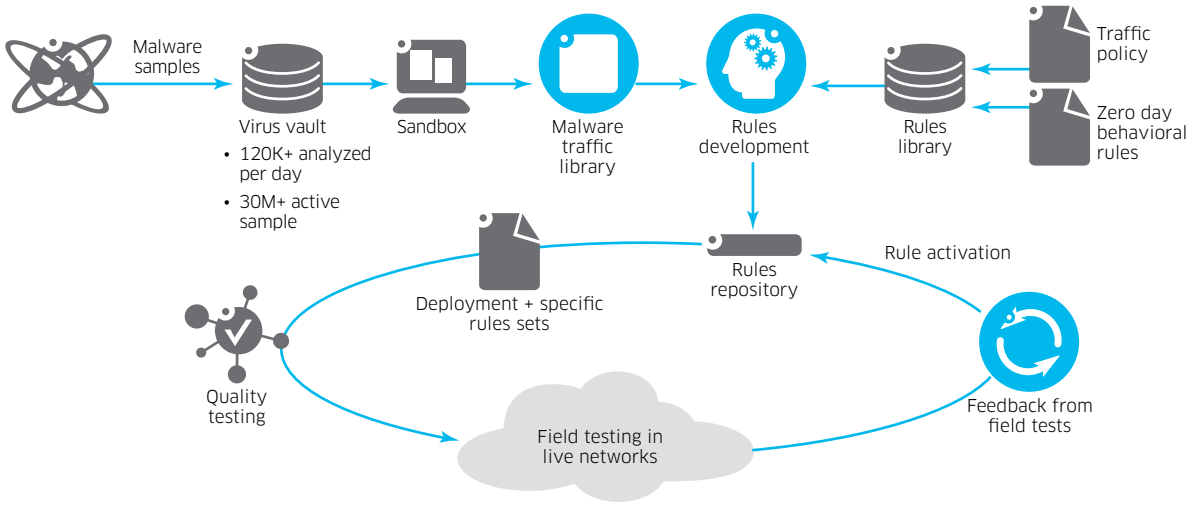
The system provides network security specialists with information on the malware that is active in the network, provides input to policy management systems such as the Policy and Charging Rules Function (PCRF) on infected devices, provides customer care with information on which users are infected and can be used as the basis of a customer-facing malware notification service.

Maintaining the detection rules

The key to doing network-based malware detection is an up-to-date set of detection rules. That is the role of Alcatel-Lucent's Motive Security Labs.

Figure 2 illustrates how the detection rules are kept up to date. Over 120,000 malware samples are received each day. These are classified using standard antivirus techniques and stored. If the sample is not already known, it is run in a sandbox environment and the network traffic is collected. If this does not trigger an existing detection rule, we develop a new rule and push it out to the field for testing. After successful field tests, it is promoted to an active rule and is used in our production system.

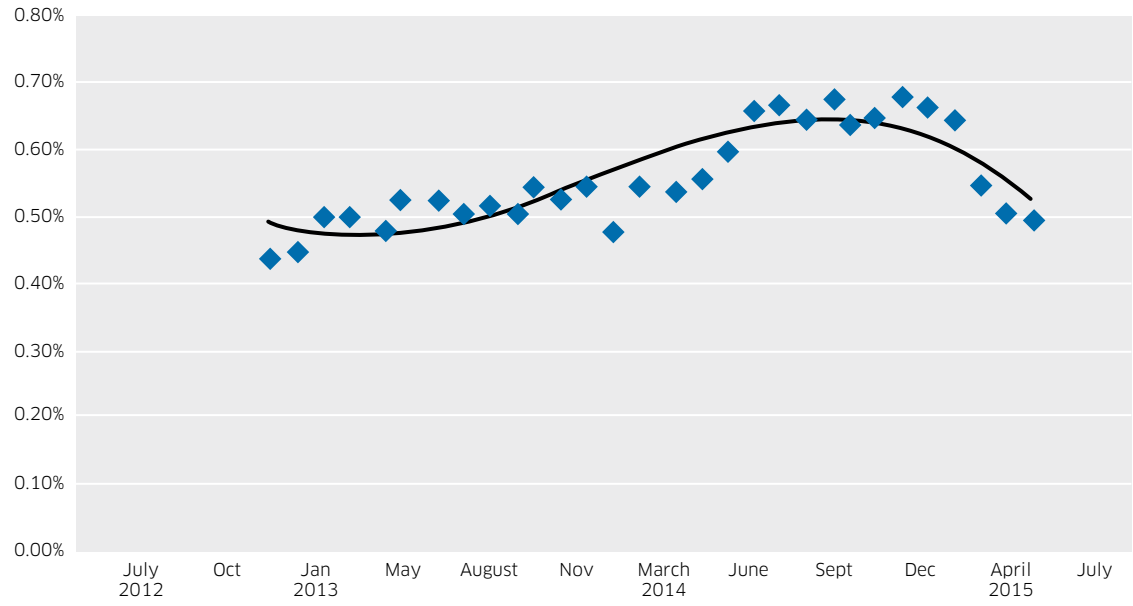
Figure 2. Rules development process



Infection rate

Figure 3 shows the infection rate aggregated across mobile deployments from December 2012 until the end of May 2015.

Figure 3. Infection rates

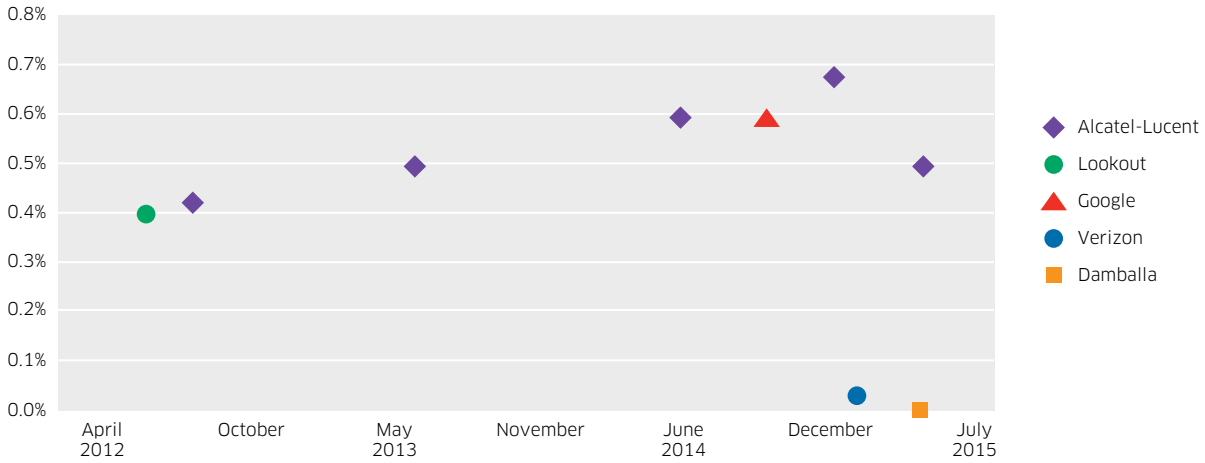


It includes all infected devices, including tethered PCs running Microsoft Windows®. In 2015 the drop in the infection rate is mostly due to a decrease in infections on devices running the Android™ operating system.

Recently there have been two reports that offer a significantly different view. In its "2015 Data Breach Investigation Report," Verizon says that only 0.03% of mobile devices in its network are infected. At the 2015 RSA conference, a researcher from Damballa reported only 0.0064%.

The graph in Figure 4 includes these numbers and data points from Google and Lookout.

Figure 4. Infection rate comparison



The Google data point is from its "Android Security 2014 Year In Review." They have used information from their "Verify apps" component to determine how many devices have installed "Potentially Harmful Applications" (PHAs). The report says…

> *"… US English devices have a PHA installed on about 0.4% of devices, which is about 0.2% below the worldwide average."*

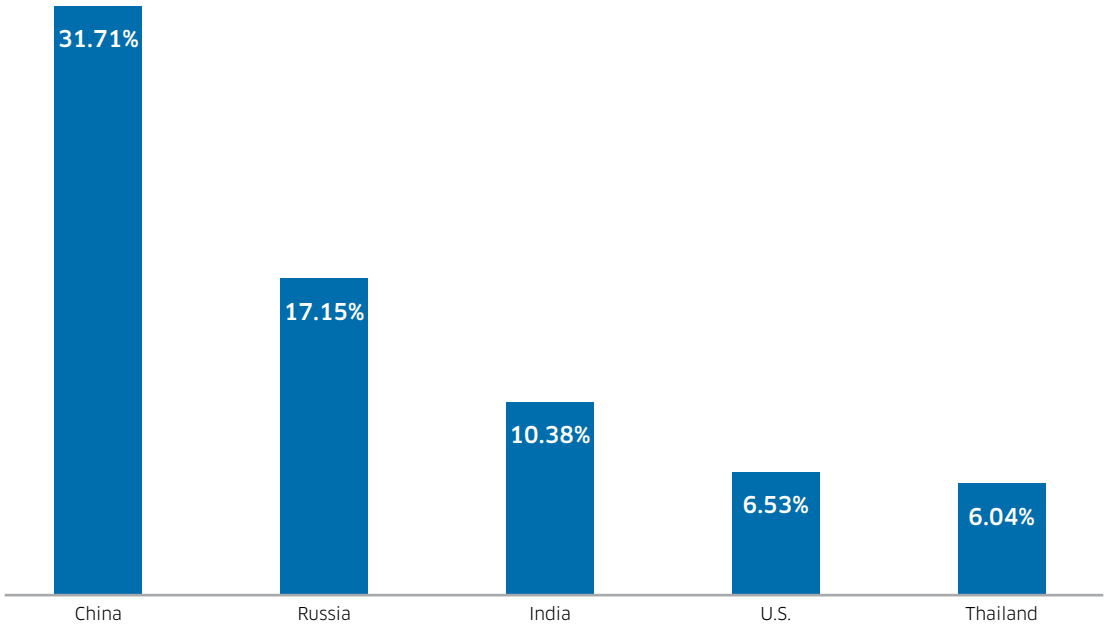
The Lookout data point is from its "State of Mobile Security 2012" where they report infection rates for a number of geographic locations. They show infection rates ranging from 0.2% to over 1.0% depending on the location. The average was about 0.4%.

This difference is predominantly due to different definitions of what exactly constitutes malware. Verizon counts only very high threat level malware that is obviously not yet prevalent in the mobile environment. Damballa is using a mobile blacklist that is based on a small number of common Android malware families. Google, Lookout and Alcatel-Lucent have a less restrictive view that includes moderate threat level malware and some aggressive adware. A common thread among all parties is that regular adware is now so common that it should not generally be counted as malware.

Misquoted in the press

Sometimes legitimate results can be misquoted in the press. Figure 5 shows a chart published by NQ Mobile in their 2013 report.

Figure 5. Chart from NQ Mobile report



Source: NQ Mobile

In the report they very clearly stated that:

> *"31.7% of infected devices are in China"*

Unfortunately this was subsequently reported in the press as:

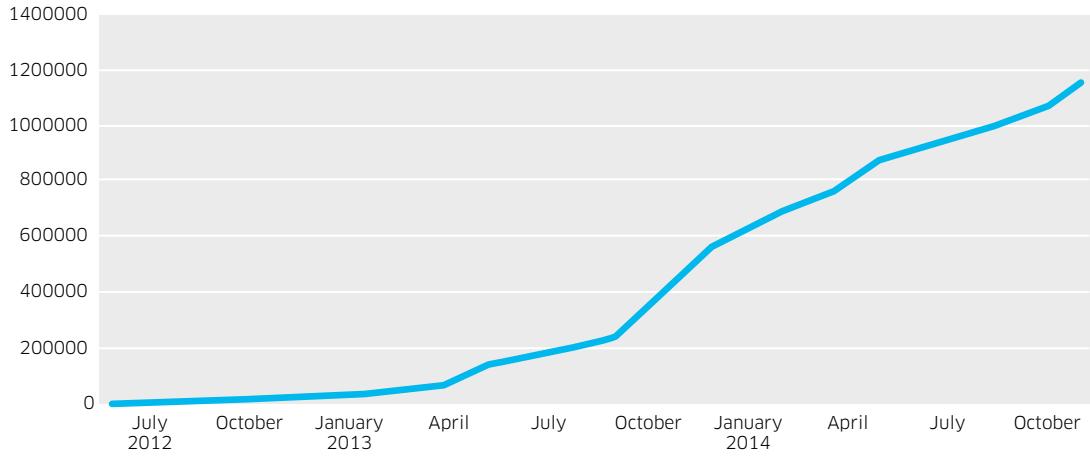
> *"31.7% of devices in China are infected"*

A slight change in word order resulted in a huge change in meaning.

Malware samples

Figure 6 shows the number of mobile malware samples we have in our data base since 2012.

Figure 6. Mobile malware samples

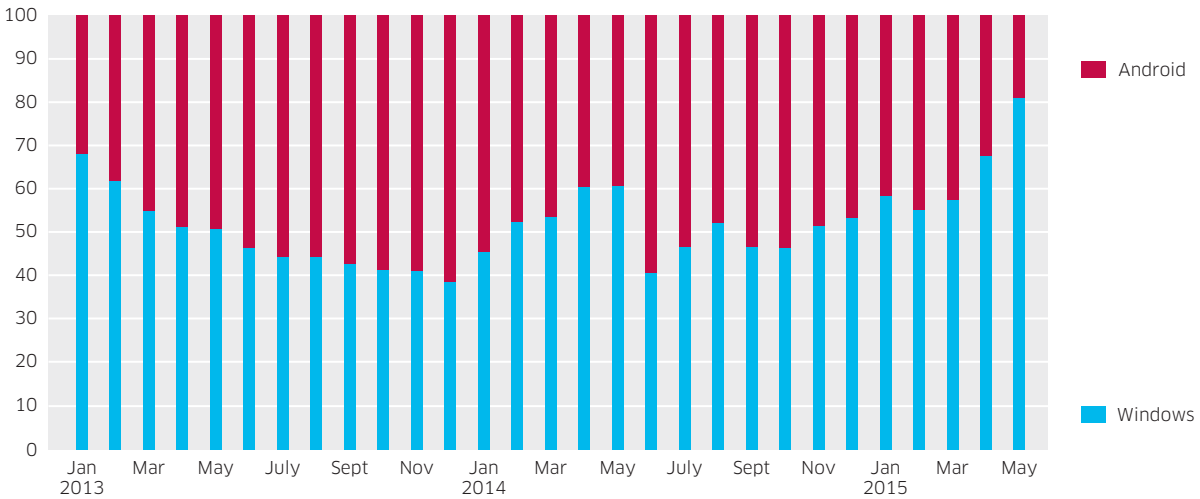


In 2013 the number of samples doubled each quarter. In 2014 the rate has been more linear with an increase of 160%. 95% of the samples are “Trojanized” Android apps.

Breakdown by device type

Figure 7 shows the infection breakdown by device type.

Figure 7. Infection breakdown by device type 2013 - 2015

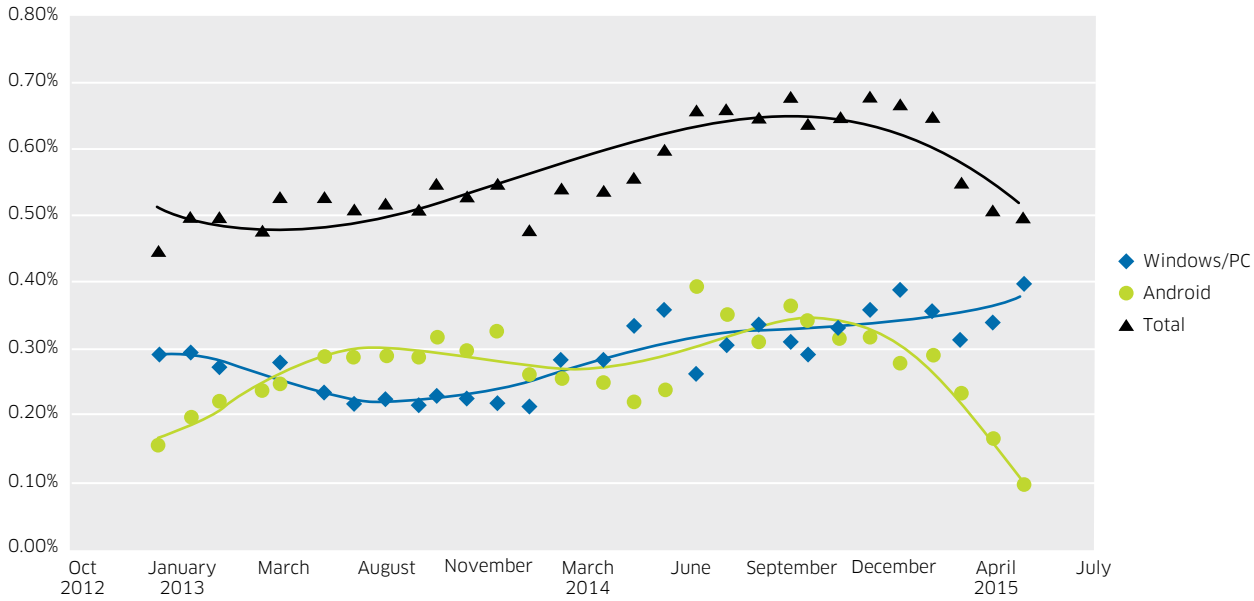


Throughout this period on average:

- ~50% of infected devices run the **Android** operating system
- ~50% of devices are **PCs** running the **Windows** operating system and connected to the mobile network
- <1% are iPhone, Blackberry, Symbian, Windows Mobile devices

However in 2015 we have seen a significant reduction in the proportion of infections on Android devices. This is illustrated in the graph below.

Figure 8. Malware infection rates by device type



The noticeable drop in the infection rate in 2015 is due to a significant decrease in the Android infection rate. This is due to the efforts of Google to reduce the malware on Google Play and their introduction of the "Verify apps" feature.

Malware impact

Windows malware

Professional cybercrime has a considerable investment in the Windows PC platform. The technology for exploiting the Windows platform is mature and effective. The platform is targeted by exploit kits. Rootkit technology is well entrenched and C&C is mature and robust. A cybercriminal economy is built around this platform, with different players creating and packaging the exploits, infecting endpoints, creating and managing botnets, monetizing the bots and finally laundering the financial gains.

In fixed broadband networks we see infection rates close to 15% – 5% if you count only high threat level malware. We see the same infection profile in Windows PCs and on laptops that are active on the mobile network. Despite their relatively small number compared with mobile phones, they make up over 50% of the malware activity that we observe in the mobile network. They are primarily connected via mobile Wi-Fi® devices or USB dongles, but some are tethered through phones.

The types of Windows malware have the same profile as in the fixed broadband case; they include botnets, rootkits, spam, identity theft, banking Trojans, DDoS, ad-click, Bitcoin, fake antivirus (FakeAV), ransomware, hacktivism, spyware…

The impact on the network varies depending on the type of malware. Spam and ad-click bots can have a significant impact on network bandwidth consumption. However with the advent of Long Term Evolution (LTE) networks, this impact is somewhat reduced due to the higher capacity of the underlying network infrastructure. Often the C&C protocol can have a significant impact on the radio resources due to 24/7 air time or high radio signaling activity caused by periodic heartbeat packets.

Examples:

- A laptop running Windows infected with a proxy-bot created 800,000 TCP sessions and consumed 3 gigabytes of bandwidth in a 24-hour period.
- A roaming user infected with the ZeroAccess p2p bot draws traffic from over 4000 peers around the Internet. All this is backhauled from his home network to the network he's roaming in.
- A bot checks in every minute with its C&C server. This ensures that if the device is otherwise idle, the radio connection must be re-established each time.

Impact on the user includes:

- Identity theft due to key loggers and password stealers
- Financial loss due to banking Trojans
- Excessive charges due to bandwidth usage
- Extortion due to ransomware
- Performance degradation due to consumption of computing and network resources
- Embarrassment from spamming and infecting friends

Android malware

Android malware comes mostly in the form of Trojanized apps that are downloaded from third-party app stores or Google Play and installed by the user. The malware is often embedded in free games or ripped off versions of commercial apps that are offered for free on third-party stores.

Sometimes some sort of phishing or social engineering campaign is used to entice the user to install the malware. For example the NotCompatible proxy bot gets its name from the fact that when potential victims visited infected web sites, they were told that their browser was not compatible with the site and that they should download and install the update, which of course contained the malware. The Koler ransomware bot enticed visitors to Internet-based pornographic sites to download and install a "premium access video player."

Generally speaking, when compared with the more mature Windows variety, Android malware is not nearly as sophisticated or threatening. Specifically:

- C&C servers are hard-coded in the source code as URLs, domain names or IP addresses.
- The C&C protocol is not robust and can be disrupted by taking out a single server.
- The malware makes no real attempt to conceal itself or avoid detection by antivirus software.
- The malware makes no attempt at persistence and can be removed by a simple uninstall.

Adware is very common, to the point where we don't actually count it as malware at all. Ad networks will offer software development kits (SDKs) that developers can embed into apps to provide targeted advertising that is used to fund the application. These SDKs will typically use the devices IMSI and IMEI to identify the device to the ad server. Often location and demographic information is also provided. In some cases the adware will send additional information, such as the contact list or list of installed apps. Here the distinction between adware and malware get a bit blurred.

Infostealers send information from the device to the C&C server where it can be used for a variety of purposes. Often the phone's contact list is stolen and used in subsequent spam campaigns. More serious are the password stealers that look for social media credentials.

Spy phone apps are very common. These are apps that are used to spy on the phone's owner. They track the phone's location, monitor ingoing and outgoing calls and text messages, monitor email and track the victim's web browsing. A number of these apps are available commercially. They are often used by parents to monitor their children, but can also be used to track a spouse, employee or business associate. Mobile spyware is definitely on the increase. Six of the mobile malware infections in the 2014 top 20 list are mobile spyware.

SMS Trojans make money by sending text message to premium short message service (SMS) numbers where the user is billed for the message. This is more common in geographies where it is easy for the cybercriminals to launder the proceeds. This is an example of a "green field" opportunity for cybercrime to take advantage of a facility that was not available in the traditional Windows malware ecosystem. The impact in the user's phone bill depends on how aggressive the malware is.

Banking Trojans are now making the move to the mobile space. Originally this was in the form of malware, like Spitmo, that was designed to intercept the one-time access credentials sent to the user via SMS. However as people start banking from their phones, we expect to see a large increase in this area.

Ransomware in the form of encryptors and fake security software are also common on the mobile space. As the phone becomes the network access device of choice, we expect to see more of these.

Why Android

Why is the Android platform most targeted by malware? Modern mobile phone operating systems (Android and iOS) have been designed with security in mind, so the easiest attack path is through Trojanized apps. The Android app ecosystem is the most vulnerable because it allows apps to be installed from third-party app stores, and due to lax app signing practices Android apps are very easy to hijack. A large market share and open source environment also contribute to its popularity.

Sideloading

The main reason Android is so highly targeted is the ability to download and install apps from just about anywhere. This provides the malware developer with an easy way to deliver the malware. iPhone apps are only available from Apple, but anyone can distribute Android apps. Most third-party app stores offer good quality apps that have been checked for malware, but a few have been specifically set up to provide pirated software with a high malware content.

Google Play

The official Google Play store has also been known to harbor malware. In 2014 over a 3-month period we downloaded 130,000 free apps from Google Play and submitted them to VirusTotal.

- **2.3% were identified** by at least three antivirus vendors.
- Of those **94% were adware**
- However that leaves **0.138% that were identified as malware**, about 1 in 700

However, since then Google has made significant progress in reducing the level of malware on Google Play and also introduces a Verify app feature that reduced infection in the field. We have noticed a significant reduction in the Android infection rate since then.

App hijacking

All Android apps must be digitally signed by the developer. The following is from the Android developer's web site.

> *"Android requires that all apps be digitally signed with a certificate before they can be installed. Android uses this certificate to identify the author of an app, and the certificate does not need to be signed by a certificate authority. Android apps often use self-signed certificates."*

Since the certificate is self-signed, the developer can put whatever information into that certificate that they want. For example I could sign an app as developed by the "Queen of England."

iPhone apps, on the other hand, are signed by a developer's certificate that is issued to the developer by Apple. So Apple controls the content of the certificate used in the signing process. This is from Apple:

> *"Before your Mac app or iOS app can be used with store services, installed on an iOS device for development or testing, or submitted to the App Store, it must be signed with a certificate issued by Apple."*

When you combine this lax signing policy with some standard developer tools, it becomes very easy to hijack an existing application, inject some malware and republish the app on a third-party app store.

1. Get the APK file for the target app.
2. Open it using "apktool d".
3. Cut and paste the Trojan "smali" code directories into target app.
4. Edit the onCreate() function in the apps main activity to invoke the Trojan service.
5. Edit manifest to add the Trojan service and any required permissions.
6. Rebuild the app using "apktool b".
7. Use "jarsigner" to sign the app (any key will do).
8. Use "zipalign" to complete the process.

This of course can be scripted for mass production.

Some examples of Android malware

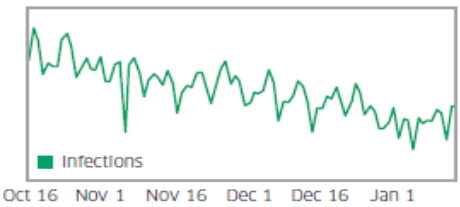
Top 20 2014

Table 1. Top 20 Android malware detected in H2 2014

NAME	THREAT LEVEL	% OF TOTAL	H1 2014
Android.Adware.Uapush.A	Moderate	45.57	New
Android.Trojan.Ackposts.a	High	17.08	6
Android.MobileSpyware.SmsTracker	High	14.67	3
Android.Adware.Counterclank	Moderate	9.56	New*
Android.MobileSpyware.SpyMob.a	High	1.87	12
Android.Bot.Notcompatible	High	1.65	5
Android.Trojan.FakeFlash	Moderate	1.62	New
Android.Trojan.Wapsx	High	1.09	8
Android.MobileSpyware.GinMaster	High	0.85	32
Android.Trojan.Qdplugin	High	0.82	7
Android.Trojan.Sms.Send.B	High	0.76	4
Android.MobileSpyware.SpyBubble	High	0.64	9
Android.ScareWare.Koler.C	High	0.64	New
Android.Backdoor.Advulna	High	0.52	10
Android.MobileSpyware.Phonerec	High	0.45	13
Android.MobileSpyware.Tekswon.A	High	0.33	New
Android.ScareWare.Lockdroid.F	High	0.25	New
Android.Adware.Kuguo.A	Moderate	0.2	15
Android.Trojan.MMarketPay.a	High	0.16	29
Android.Trojan.JSmsHider.D	High	0.16	64

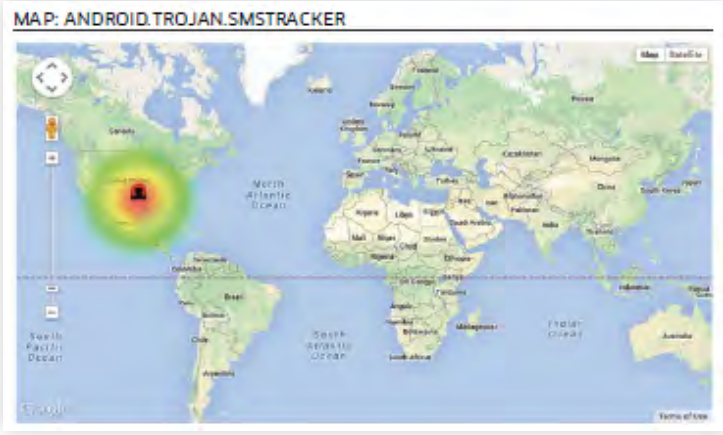
UAPush

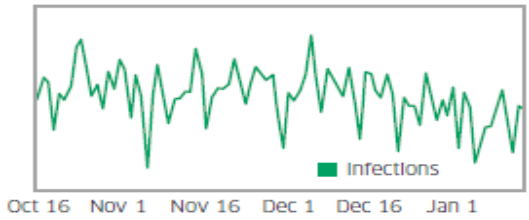
- **Uapush.A** is an Android adware Trojan with a moderate threat level.
- It sends IMSI, IMEI, contact information, bookmarks and call history to a C&C server in China.
- It also may send SMS messages without the user's consent.
- Activity on this decreased steadily since the first half of the year.



SMSTracker

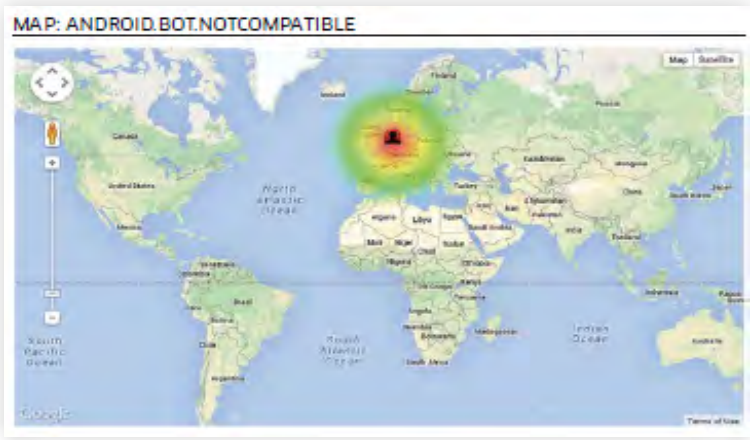
- **SMSTracker** is an Android spy phone app that provides a complete remote phone tracking and monitoring system for Android phones.
- It allows the attacker to remotely track and monitor all SMS, Multimedia Messaging Service (MMS), text messages, voice calls, GPS locations and browser history.
- This is also known as Android.Monitor.Gizmo.A.

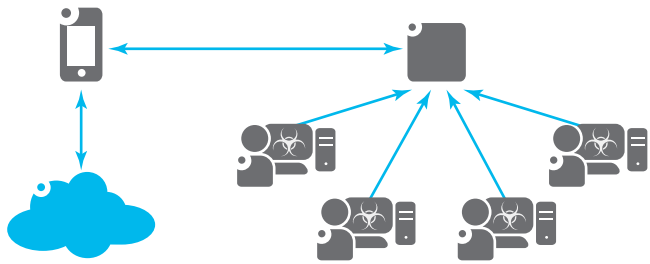




NotCompatible

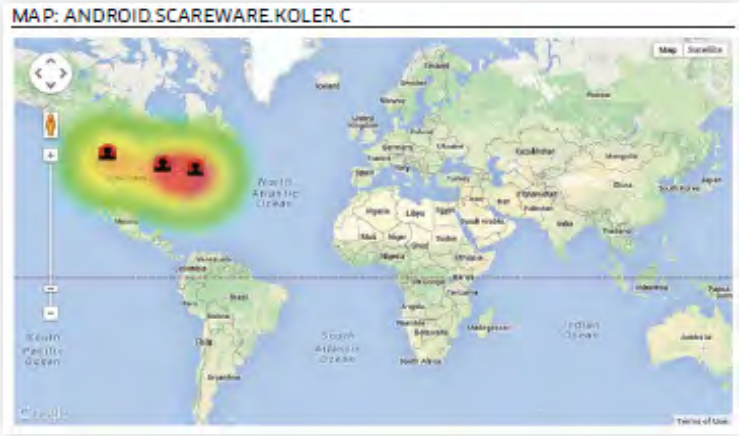
- Web proxy bot ported from Windows to the Android environment
- Uses same C&C as Windows version
- Allows remote miscreants to anonymously browse the web through the victim's phone
- Consumes lots of bandwidth
- 165 megabytes in two hours over 300,000 TCP sessions
- Infection rate is currently only 0.03%
- In a network of 1 million users, that's 600 gigabytes per day





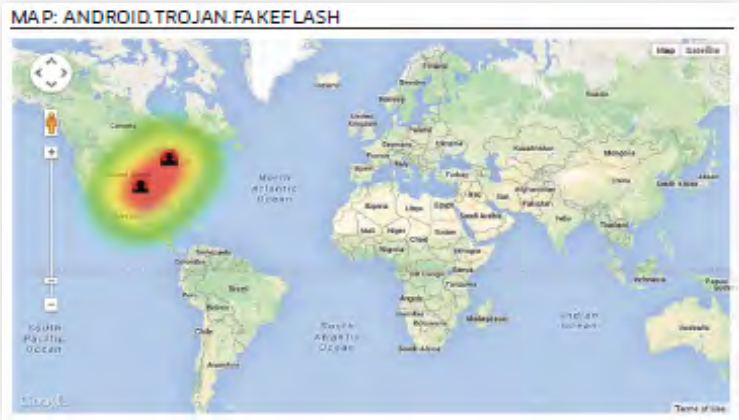
Koler

- **Koler** is an Android scareware Trojan that claims it has encrypted all the data on your phone and demands a ransom to restore the data.
- The victims are usually visitors to Internet-based pornographic sites, who are duped into downloading and installing a “premium access video player.”
- The malware “lock-screen” is customized depending on the location of the phone.



FakeFlash

- **FakeFlash** is a scam application distributed under the name “Install Flash Player 11.”
- It charges money for downloading and installing the Adobe Flash Player.



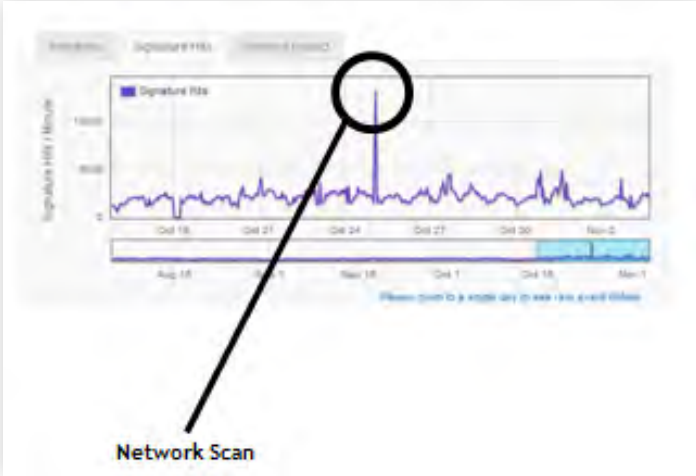
Mobile Spyware

- **Mobile spyware** is definitely on the increase. Six of the mobile malware infections in the 2014 Top 20 list are mobile spyware.
- These are apps that are used to spy on the phone’s owner.
- They track the phone’s location, monitor ingoing and outgoing calls and text messages, monitor email and track the victim’s web browsing.

DDoS

Impact of scanning

- Cybercriminals and security researchers often scan the Internet for vulnerable devices.
- In mobile networks these scans can cause excessive radio paging and signaling as large numbers of idle devices must be reconnected to the network to respond to the scan.
- Not a problem if the mobile subnets are “NATed”



DNS amplification DDoS attack in mobile network

- Mobile Wi-Fi devices have been used in DNS DDoS amplification attacks.
- Device configuration problem caused some devices to provide an Internet-facing recursive DNS service
- This attack is very similar to the Spark DDoS attack on Sept 8-9, 2014 in New-Zealand, where the mobile and fixed data services were down for almost two days due to 138 compromised devices.

CONCLUSION

Malware targeting mobile devices is currently not as sophisticated as the typical malware that infects PCs and laptops running Windows. The malware is typically distributed as a Trojanized application that users must install themselves due to social engineering or phishing. It makes no serious attempt to conceal itself and can be removed by uninstalling the app. The C&C is not very robust, often using hard-coded IP addresses or domain names. The infection rate is significantly less than in fixed broadband networks.

Currently Windows PCs and Laptops account for more than 50% of the malware infections that are seen on the mobile network. The computers running Windows are either tethered to phones or connected via dongles or mobile wireless hotspots. Obviously Windows is still the platform of choice for professional cybercriminals, who have years of experience invested in the platform.

However, as people use their mobile phone as the Internet connectivity device of choice, cybercrime will certainly move onto the mobile platform, the C&C protocols will become more sophisticated and the malware more difficult to detect and remove. Cybercrime has certainly been quick to move in to green field opportunities provided by premium SMS numbers and spyphone capabilities.

Android is currently the most targeted mobile platform. This mostly due to:

- The ability to sideload apps from third-party app stores
- The fact that it is relatively easy to hijack an Android app
- Weak rules governing app signing

Going forward we expect malware to take advantage of unique opportunities presented by the smartphone platform. Specifically:

- Botnets move to mobile devices for SMS and voice spam
- More sophisticated C&C, persistence & stealth
- DDoS against SMS and voice
- Hacktivism goes mobile
- Internet of Things gets hit

For more information contact:
kevin.mcnamee@alcatel-lucent.com

Or visit the Motive Security Guardian web site at:
https://www.alcatel-lucent.com/solutions/security-guardian

MOTIVE
BY ALCATEL-LUCENT