Report

H2 2011 Android E-Threat Landscape

Author
Bogdan BOTEZATU
Senior E-Threat Analyst

Contributors:
Vlad ILIE
Virus Researcher

Bitdefender®

The Cost of Living in a Smarter World

It took smartphones more than a decade to penetrate the business environment and make their way to the regular mobile services consumer. Starting with the release of the first iPhone in 2007, smartphones have been constantly gaining ground and, as of late 2011, more than a quarter of the 4 billion active mobile phones worldwide were smartphones.

Smartphones allow users to interact with their phones in new ways, including accessing the web, performing e-banking transactions and building functionalities on top of the dedicated operating system by installing additional applications.

However, the cost of flexibility rapidly started to show: increased malicious activity, especially on the Android sector, helped by the open architecture of the operating system and widespread availability of development tools.

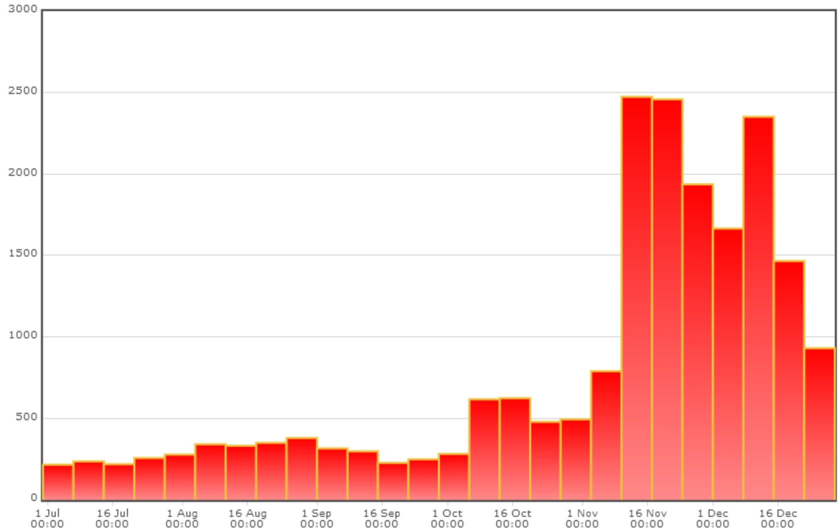


Figure 1: Increased malicious activity on Android during 2011

The security model implemented in the Android operating system has major improvements over other platforms, but still relies on the user to take critical decisions when installing third-party applications. The Android security model relies on isolation and permission-based access control to ensure that a specific application can't access sensitive information on the phone or can access device data within the scope of the permission.

However, despite the rigorous checks, the user is ultimately in control of what happens with the application, as mentioned earlier. The fact that Google's approach to software certification is more relaxed and allows any software developer to publish applications on the Android Market without approval, has led to a significant number of malicious applications for Android that rely on users to grant them access to critical device systems, such as geolocation, SMS, address book or email.

With online banking becoming more and more popular with smartphone and tablet users, organized cyber-criminal gangs have started to develop mobile-specific threats specifically targeting the financial sector. One of these e-threats is the mobile version of the Zeus banker Trojan (dubbed ZitMo or Zeus in the Mobile), a piece of spyware that forwards mTAN[1] codes that attackers use to bypass two-factor authentication.

---

[1] mTAN - http://en.wikipedia.org/wiki/Transaction_authentication_number#Mobile_TAN_.28mTAN.29

Mobile Threats in Review

Statistics provided by Bitdefender Mobile Security show a serious increase in malware families in 2011. While in 2010 we had just 3-4 malware strains, in 2011 we discovered more than 100 malware families - a 4,500% increase which generated close to 10,000 malicious applications. While the most frequent e-threats identified by Bitdefender are related to device rooting via operating system exploits, new breeds of highly advanced malware and even carrier-condoned privacy-invading mechanisms surfaced in late 2011.

The Risks of Device Rooting

Through rooting, the smartphone user can circumvent some limitations imposed by the carrier or by the mobile phone vendor. These limitations usually prevent the user from altering system applications or running code that requires “root” (administrative) permissions. Rooting also allows a user to completely wipe the operating system and replace the vanilla Android with a heavily modified one, for instance.

Rooting is highly controversial because, on one hand, it allows users to control their devices as they see fit, but, at the same time, increases the danger in case of a Trojan attack, which can carry severe implications.

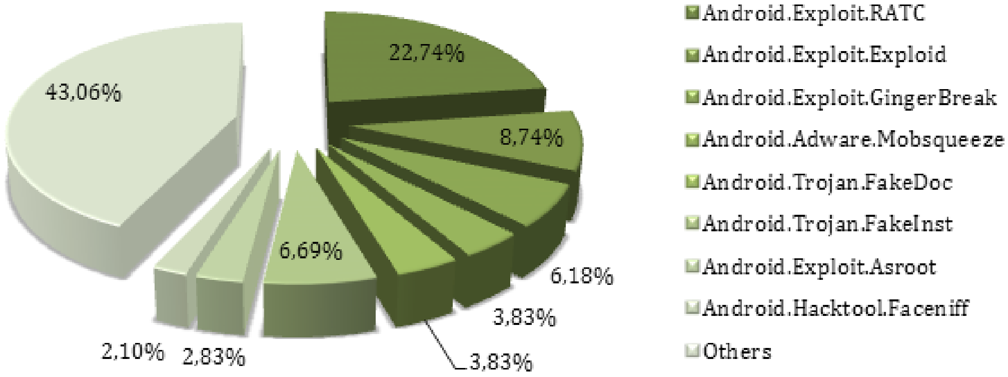


Figure 2: Android malware breakdown

Android.Exploit.RATC – 21.14%

Android.Exploit.RATC, also known as Rage against the Cage, is one of the most popular methods of Android rooting (attaining privileged control over the phone). This particular exploit, RATC – has been identified in a notorious piece of malware known as Android.Trojan.DroidDream.A that appeared on the Android Market in early 2011. DroidDream is particularly important because it can bypass the security container of Android operating system prior to version 2.2.1.). Once infected, it collects critical phone information such as the International Mobile Equipment Identity (IMEI) and International Mobile Subscriber Identity (IMSI) and can install anything it wants on the affected phone without the user even realizing.

Android.Exploit.Exploid – 8.74%

Ranking second in the Android malware top, Android.Exploit.Exploid is also a frequently encountered means of subverting the Android operating system. However, just like Android.Exploit.RATC, this particular exploit has been detected both in the form of a stand-alone tool that can be used willingly by the smartphone owner, as well as bundled with malicious applications, such as the notorious DroidDream, an Android package that attempts to root the operating system so it can circumvent the operating system’s security container.

Android.Exploit.GingerBreak – 8.74%

Android.Exploit.GingerBreak is another popular exploit that makes use of an operating system vulnerability to root smartphones running version 2.3.3 of Android (also known as Gingerbread). In most cases, the smartphone owner is aware of the exploit and triggers it voluntarily. But the exploit code is also integrated in several variants of Android malware, such as the notorious Android.Trojan.GingerMaster.A that is distributed with repackaged legit applications.

Android.Adware.Mobsqueeze.A – 6.18%

This piece of scareware ranks fourth in the Android malware top for H2 2011, with 6.18% of the total number of infections. Android.Adware.Mobsqueeze.A passes as a utility able to recharge the battery, but instead steals information stored on the smartphone. The Trojanized application, named Battery Doctor or Battery Upgrade, connects to the remote server and sends private information about the phone's make and model as well as about its owner.

Android.Trojan.FakeDoc.A

Android.Trojan.FakeDoc.A steals information from the victim's phone and uploads it on a server controlled by the attacker. This is a variant of the Android Battery Doctor application, but, instead of regenerating the battery, it silently accesses the user's Gmail account once every four hours and forwards the received messages to the attacker. More than that, the application displays popup messages.

High-Profile Incidents

In early December, a controversial application appears to have emerged[2] from an unexpected source: the very carrier that sold the phone. Dubbed CarrierIQ, for the name of the software company that built it, this package has been identified in mobile phones sold by an assortment of carriers around the world deeply buried within the Android operating system. CarrierIQ allegedly had access to usage patterns, geolocation data, call history or SMS history and contents - information that was supposed to reach carriers as part of an anonymous feedback program to boost service quality. It is currently unknown if or how the data that could be collected through the package was used, but its presence on devices was showcased as a severe privacy invasion, especially as owners of non-rooted handheld devices were unable to remove it. Bitdefender offered a stand-alone scanning tool that identifies and reports the presence of the CarrierIQ package.

Top Regions in Terms of Infection

Russia, China and the United States are the top three countries in terms of smartphone users affected by malware, either because of increased smartphone penetration, or because of pirated, re-packaged applications bundled with malware and delivered through alternative Android Markets.

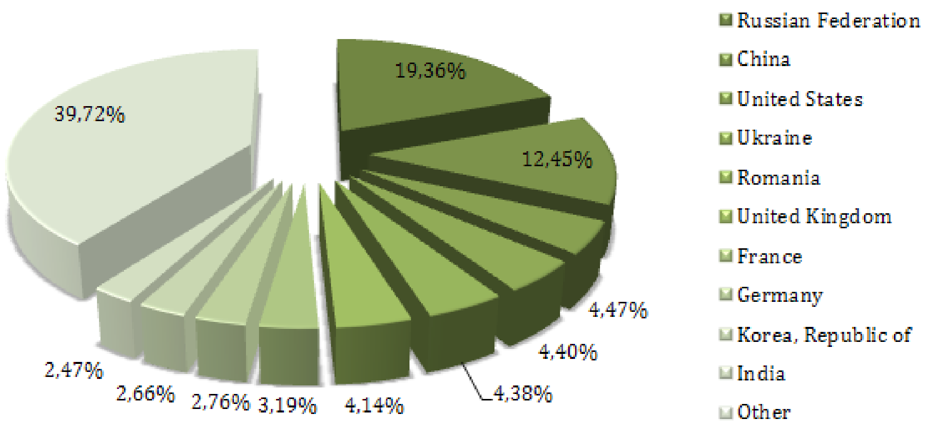


Figure 3: Top infected countries

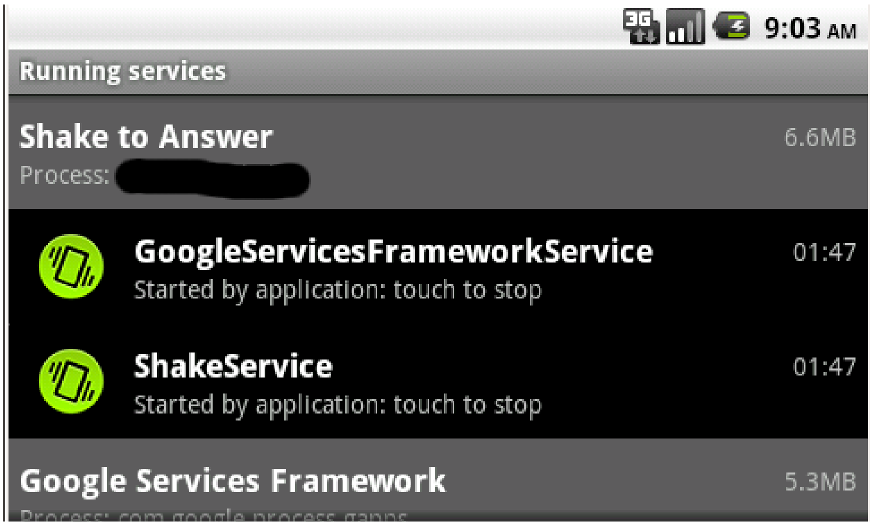
---

[1] Read full info at http://www.malwarecity.com/blog/new-tool-to-detect-carrier-iq-tracking-package-available-for-free-1230.html

Malicious Application Dissemination

Repackaged applications have become endemic especially in countries where access to the official Android Market has been restricted (i.e. China) and smartphone users have to get their applications from alternative sources that take fewer precautions to counter the risk level of a package.

This is the case with a series of repackaged applications featuring an additional malicious service that connects to a C&C server and fetches a list of links to different APKs. Most of these applications were downloaded by cyber-criminals from the genuine Android Market, tampered with and then re-uploaded to regional, unsanctioned Markets. This Trojan, dubbed Android.Trojan.FakeUpdates.A, requires an extensive array of privileges upon installing, in order to make sure it can take full control over the smartphone whenever necessary. From time to time, it displays update notifications in the operating system's notification area, which confuses the user and increases the chance of success.



Running services

Shake to Answer 6.6MB
Process: [redacted]

GoogleServicesFrameworkService 01:47
Started by application: touch to stop

ShakeService 01:47
Started by application: touch to stop

Google Services Framework 5.3MB
Process: com.google.process.gapps

The Trojan can install any of the APKs present in the list on the attacker's server. This makes it particularly dangerous, as it can download and install anything, from trial versions of software in pay-per-install campaigns to spyware and other Trojans.

However, repackaging applications, although it takes the lion's share of malware dissemination, is just one of many ways crooks push badware on the market. Another popular method of having users install shady applications is by describing the malicious payload and hoping no users actually go through it. This kind of provision usually ensures the application persists even on the genuine Android Market, which won't take apps down for functionalities that are part of a contractual relationship. One example is Android.Trojan.SndApps. This is a family of Android malware that steals sensitive information from the victim's phone and uses it to display unsolicited ads in such a way that the victim has no way of linking the ads to the infected application. Several applications infected with SndApps are hosted on Google's Android Market and cannot be taken down because they specifically state in the EULA (End-User Licensing Agreement) that the application collects user information and provides advertisements.

Malicious updates are also an important mechanism of infestation. In this case, the attacker uses a popular clean application to gain as many installs and positive votes as possible. As soon as they reach a decent number of installations, they issue an "updated version" that comes bundled with malware. Since users already trust and like the application, they install the update without hesitation and compromise the security of their device.

Other Threats and Vulnerabilities

Compromised applications may account for the largest number of infections, but they are not for the only threats to smartphone users. Web-based threats have been constantly gaining ground with the introduction of larger data plans and widespread availability of hotspots in urban areas.

Smartphone users are twice as active on social media as non-smartphone users. Given that roughly 200 million Facebook users access the service from their smartphones, they expose their device and account to a wide range of threats. An Android user's chance of stumbling on an unsafe link increases exponentially, and almost doubles from the previous year. According to a Bitdefender study published in January 2011[3], almost 24% of the Facebook and Twitter users exposed to scams are browsing from a mobile device. Constant monitoring reveals that this is an increasing trend and the probability of mobile users clicking a compromising link will reach as much as 40% in 2012.

At the same time, some e-threats, such as spam and phishing, do not discriminate based on medium. More than that, smartphones' limited screen size may sometimes work in favor of the attacker, concealing parts of the accessed link and making it much easier for the user to fall into a trap.

Future Outlook

With mobile Internet usage set to surpass desktop traffic by 2014, cyber-crooks will seek new ways to capitalize on standard smartphone users. Malicious attacks, phishing and e-banking fraud will continue to play a key role in the Android e-threat landscape. Here are some more:

The introduction of new technologies: the widespread deployment of HTML5 to mobile devices will offer the smartphone user new ways of interacting with the web, but, at the same time, will allow the web to interact with the user. As the Android Browser gets more and more support for HTML5 such as Web Notifications, cyber-criminals will have extra tools to create fake popups and warnings, impersonate forms and deliver more convincing scams straight in the browser.

More applications in the Market: More than 400,000 apps were available for the Android operating system as of December 2011 and the number was rising rapidly. The abundance of applications will likely make it more difficult for Google to scan, identify and remove malicious applications from the Market.At the same time, it will give cyber-crooks more rough material for repackaging and re-publication.

Device theft or loss: as more tablets and smartphones are bought and activated, more of them will be stolen or lost. Given that some of these devices are used in the corporate (and will be used in the military) environment, involuntary exposure of classified information is imminent. The installation of a solution that features full-drive encryption, remote locking and remote data wiping will become mandatory.

Wi-Fi traffic sniffing will also become a widespread problem in the next six months. With half of Twitter's subscriber base using the service on smartphones and over 200 million clip views on YouTube every day, the future looks mobile, with hotspots as the favorite type of connectivity. Tools like Android.Hacktool.Faceniff.A, and prank instruments such as Network Spoofer, make it easier to intercept and modify traffic sent through public hotspots such as those in shopping malls, airports, learning institutions or campuses.

Mobile phishing is an increasingly risky trend as more and more users migrate from – or use in parallel – social networking accounts, web-based e-mail and even online banking. However, traditional phishing is not the only form of deception in the mobile world: dedicated applications advertised as e-banking or e-mail clients syphon usernames and passwords to remote attackers. Application-based phishing is much more difficult to detect and mitigate, which ultimately leads to an aggravated, continual form of password disclosure.

Despite the fact that Google has introduced "Bouncer" - the scanning solution that constantly analyzes Android applications posted on the market, the number of malicious APKs will continue to increase. More and more pieces of malware for Android feature advanced polymorphism, VM protection and even fetch malware at runtime to avoid getting detected through conventional methods.

---

[3] Full report:
http://www.bitdefender.com/news/malware-targeting-social-networks-may-be-the-biggest-current-mobile-security-threat-says-bitdefender-1947.html

Bitdefender®