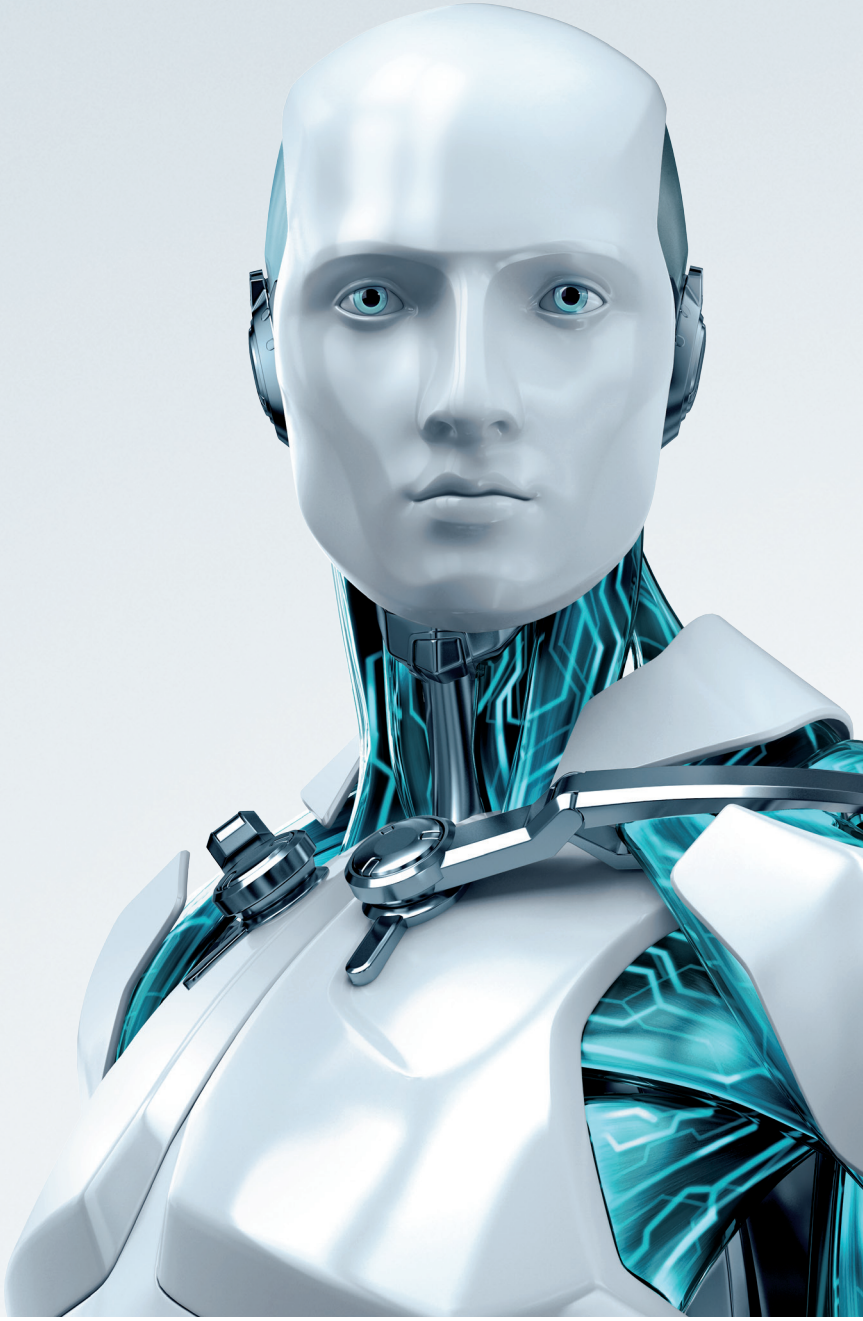
Trends for 2013

Astounding growth of mobile malware

ESET Latin America's Lab



Introduction

At the end of each year, ESET Latin America's Lab prepares a document about trends in malware, cybercrime and other types of malicious computer attacks, based on what has been observed and analyzed throughout the current year. It is important to point out that by a trend we mean a projection performed by the company according to the present state of computer threats and cybercriminal behavior.

This is the background to the investigation we carry out in order to predict the way IT security is most likely to evolve during the coming year. Even while this report was being written, the trends have continued to change. For example, the main trend for 2010 was ***"Crimeware Maturity"***, for 2011 ***"Botnets and Dynamic Malware"***, and for 2012, ***"Malware Goes Mobile"***. Even though all these issues are related to each other, and although behind each one of them there is always the pursuit of financial revenue by cybercriminals, it is quite noteworthy when a single trend experiences such high growth in such a short period as has happened with the mobile malware phenomenon.

During 2012 it was possible to observe how malicious programs designed for Android consolidated their position as a fundamental objective for cybercriminals, who, facing a market that grows by leaps and bounds, have started to generate malware that targets these devices much more quickly.

During the First Quarter of 2012, according to IDC, the Google operating system has recorded a year-over-year rise of 145% in market share and in sales[1] . Furthermore, Juniper Research estimates that in 2013, the number of users accessing banking services from their smartphones will rise to 530 million people[2]. According to the same study, in 2011 there were only 300 million individuals who accessed banks from their phones. In this context of growing sales and different patterns of use, and considering the rapid evolution both of this technology and of malicious programs for mobiles during 2012, we see as the **main trend for 2013 an exponential growth of mobile malware**. We also see them becoming more complex, **thus expanding the range of malicious actions they perform on an infected device.**

In 2013 we also expect to see the consolidation of a paradigm shift that has been developing in recent years: that is, in the ways in which cybercriminals propagate malicious code. Malware propagation by means of removable storage devices is decreasing in favor of the use of an intermediary in order to attract new victims. The intermediary is a web server that has been compromised by a third party in order to host computer threats. Having compromised the server, cybercriminals send out hyperlinks leading the user to the malware in question. At the same time all the stolen information has to be stored on these compromised servers to so as to avoid involving personal computers which may be better protected and where detection and cleaning of malware may result in the criminals losing their stolen data.

1 According to IDC, Android- and iOS-powered smartphones expanded their market share in the First Quarter of 2012. Available at http://www.idc.com/getdoc.jsp?containerId=prUS23503312.

2 Juniper Research. Whitepaper: Banking Anytime Anywhere. Available at http://www.juniperresearch.com/whitepapers/anytime_anywhere.

Taking all this into account, what trends will we see next year? The purpose of this report is to provide clarification and answers to this question so that both corporate and home users can adopt the measures necessary if they are to be properly protected against the latest computer threats.

Major increase in mobile malware

From 2010 onwards, the market and technology for malware for mobiles started to undergo great changes that would shape the subsequent evolution of this kind of threats. First of all, Android began to position itself as the most popular mobile operating system in the market. That same year, FakePlayer would become the first malware to target the Google platform. Then, in 2011, the ESET Latin America's Lab predicted that this operating system for mobiles would become the platform most targeted by malware within a year... which indeed proved to be the case.

A year further on, not only had the rate at which malicious code and variants for Android were created grown considerably, but so had their complexity, and furthermore, so had the time and resources devoted by cybercriminals to the development of malware for mobiles. It is only logical that a mobile operating system with a market share rate of 64.1% is seen as so desirable by cybercriminals, since – all things being equal – they have a greater chance of making illicit profits than they do with an OS attracting a smaller number of users.

The chart below shows the market share rate of the main operating systems for mobiles at present:

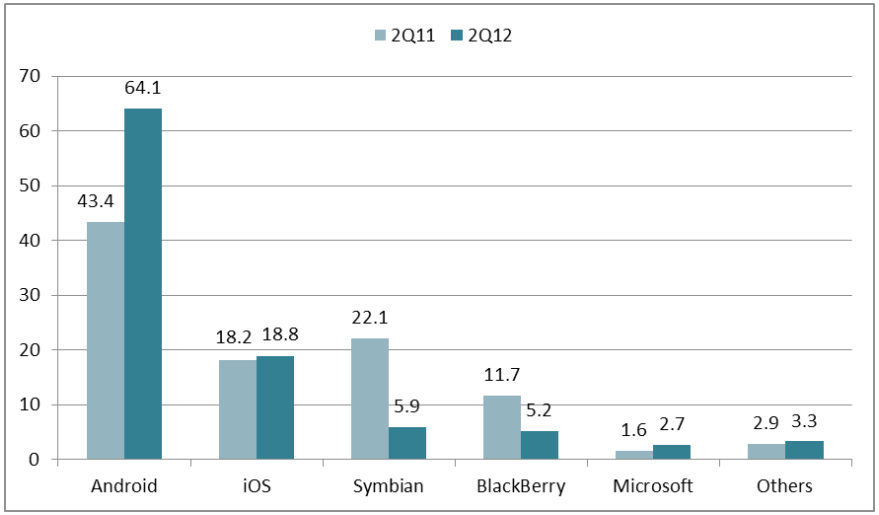


Figure 1: Smartphone sales to end users by operating system in the Second Quarter of 2012, Gartner. Available at http://www.gartner.com/it/page.jsp?id=2120015.

As happened in the same period last year (2011 Q2), it can be observed that Android experienced a growth of 20.7%, iOS (Apple) of 0.6% and Microsoft of 1.1%. Other operating systems showed a decrease in sales compared to 2011. Symbian suffered the biggest drop (16.2%) and BlackBerry was next with 6.5%.

As Android's market share rises and people use it more and more to store personal and corporate information, or for online banking or related services, cybercriminals will develop more malware to steal information, thus gaining illicit revenue. In view of this

expectation, and as happens with malware targeting computers, the cybercriminal's main motive and interest in creating this kind of threat is still financial gain. This has indeed been reaffirmed by the discovery of the case of **"*Dancing Penguins*"**, a trading scheme where cybercriminals use the illegal Pay Per Install (PPI) model to charge between 2 and 5 dollars for installing some kind of malware onto Android devices.

According to a survey carried out by ESET Latin America on the ***uses made of mobile devices***, we were able to determine that, although storage of private information and passwords is not the primary use made of mobile devices at the moment, it does constitute quite a notable percentage of common tasks. The graphic below shows the relevant statistics:

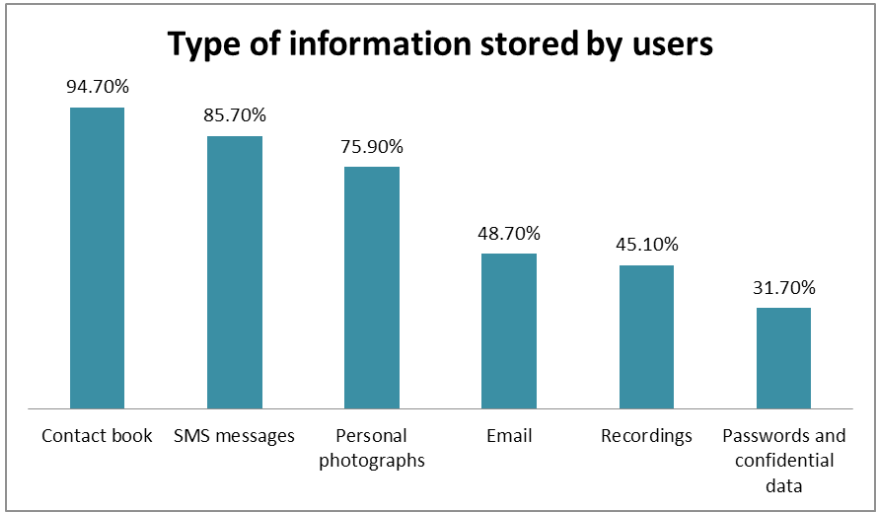


Figure 2: Type of information stored by users in mobile devices

As can be seen from this chart, the most widely used information stored in these devices is the contact/address book. So it's not surprising that there is malicious code for Android designed to steal this kind of data. This is a useful way for cybercriminals to find new victims. **Passwords and private information represent 31.7%** of the data stored, a proportion that will keep on rising as smartphone technology continues to evolve, and services adapt to this trend by developing applications and websites specifically optimized for smartphones.

Increase in the detection of Android malware

The first statistic demonstrating this dizzying rise of mobile malware – one that also allows a determination that the **trend for 2013 is one of exponential growth of malicious code for Android** – is that in 2012 the amount of unique detections grew **17 times globally** compared to 2011. Of the countries that experienced the highest growth rate in detections of Android malware, expressed in number of times, the ones that stand out are Ukraine with 78 times more, Russia with 65 and Iran with 48. On the other hand, if we consider the number of detections during 2012 irrespective of what happened the previous year, China, Russia and Iran are the first three with more detections on a worldwide basis. Mexico is sixth on the list, making it the Latin American country where the most malware detections for the Google mobile platform were seen. With this background, it can be asserted that **the malware growth for Android will rise much more rapidly in 2013**.

In relation to the number of malware families for Android – that is, malicious codes that are different enough to have a unique

classification – this time last year (November) there were 52 families compared to the 56 currently reported. Although this figure did not rise dramatically during 2012, later on in this document it is shown that **the number of signatures and variants did indeed rise significantly**; therefore, we expect that **the number of threats for Android will continue to grow regardless the total number of families,** in much the same way as we see with Windows. It is important to bear in mind that it is much easier for cybercriminals to modify a previously known malicious code (a variant) than write a new one from scratch. Furthermore, detections do not necessarily correlate to strict family classifications: some detections are based on aspects of the malcode that may be common to two or more families. In Figure 1, the families are grouped according to the year and month of discovery.

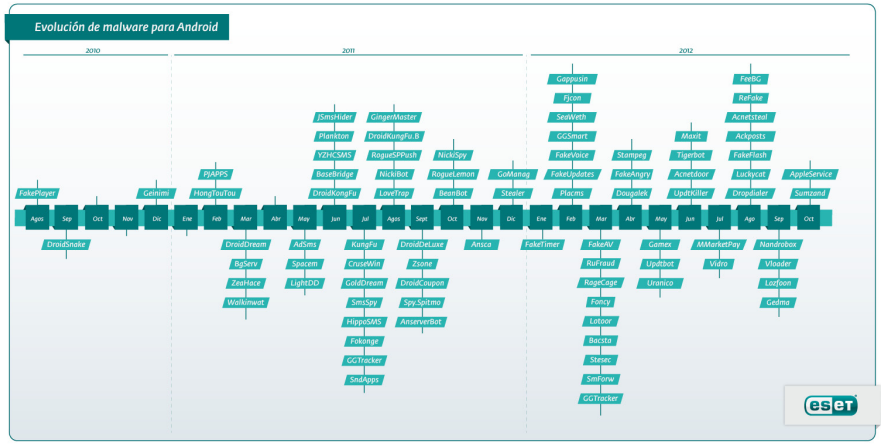


Figure 3: Emergence of malware families for Android

Taking into account the families mentioned above and the malicious actions (payload) carried out by malware on Android-based devices, it is possible to classify such behaviors as follows: information theft (spyware), SMS message distribution to premium-rate numbers, and the transformation of machines into zombies (botnet recruitment). Accordingly, we get the following chart:

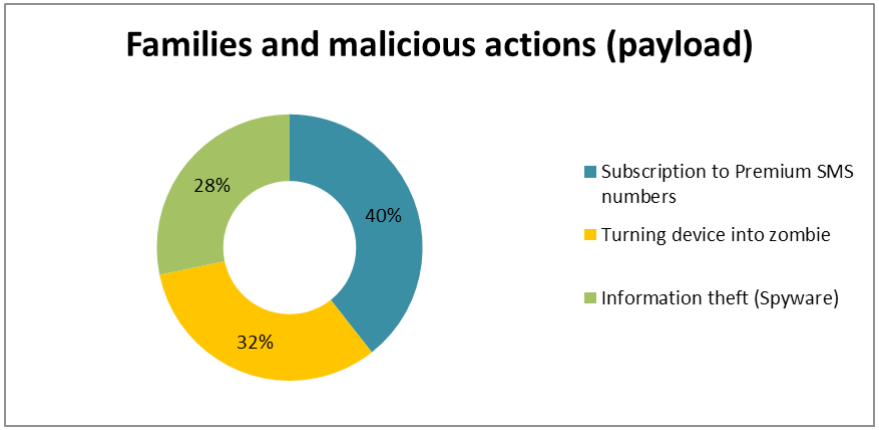


Figure 4: Families of 2010, 2011 and 2012 and their malicious actions

The majority of these families are intended to subscribe the victim to premium-rate messaging numbers. On the other hand, there are threats that transform these devices into zombies. That is, access to the devices falls into the hands of cybercriminals, who can carry out actions remotely such as installing other malicious code, stealing particularly desirable data, and modifying configuration parameters, among other actions. Thirdly, there are the malicious programs that steal information like the phone contact list, text messages or other

data useful to identify the device, such as the IMEI number. Unlike malware that transforms the smartphone into a zombie, other malware steals information without handing over total control of the machine to the cybercriminal. Finally, there are particular cases like *Android/Stampeg*, whose function is to insert an extra image among the JPG files stored in the smartphone, which can lead to the failure of the memory card. Meanwhile, *Android/MMarketPay* is capable of acquiring paid applications from a Chinese market without the user's consent, while *Android/FakeFlas*h, pretends to be a Flash plugin but in fact redirects the user to a particular website.

Significant rise of variants

The number of malware variants for Android has also increased in 2012. A variant is a modified version of a specific and known malicious program. Cybercriminals modify the structure and the code of an existing threat to create a new one with the aim of adding new malicious functions and evading detection by antivirus programs. The graphic below shows four malware families for Android and the number of variants that appeared in 2011 and 2012. It is important to note that for each new major variant that emerges, the ESET Labs add an alphabetically ordered suffix that changes as the quantity increases. For instance, the first version of a hypothetical malicious program will be named as *Threat.A* and the second major variant will be named *Threat.B*. If the number of variants exceeds 26 (or a multiple thereof), the number of letters in the English alphabet, the sequence is augmented with additional letters following the same schema: .AA, .AB, ...AAA, .AAB and so on. NB: despite ***CARO's best efforts*** to regularize malware naming, this simplified model may not altogether apply in a particular case, due to differences in lab procedure and disruptive factors such the sheer volume and complexity of malware families. Furthermore, one vendor's sub-variant naming is nowadays unlikely to be a reliable guide to the name used by another vendor, even where both names apply to the same sample.

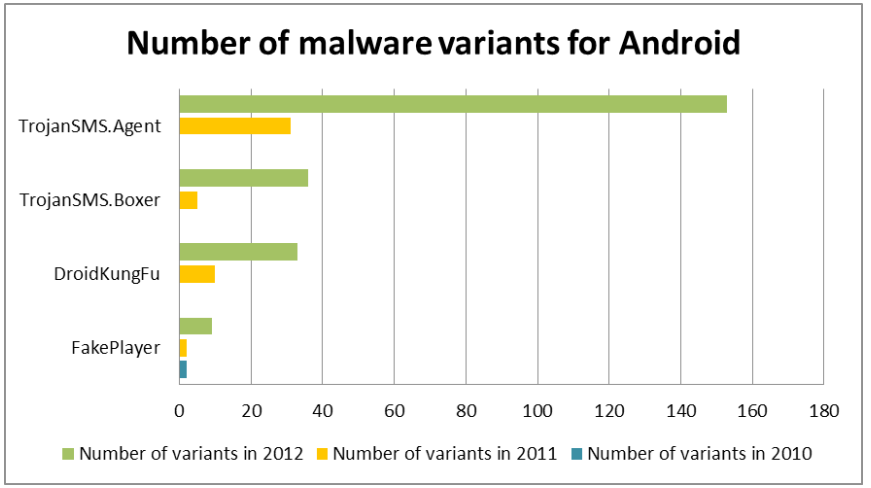


Figure 5: Number of malware variants for Android

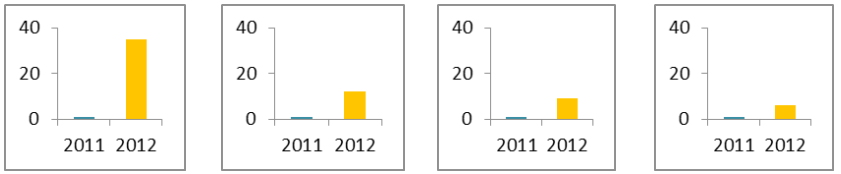
As noted in the chart, the Trojan with the highest growth in 2012 compared to 2011 is *TrojanSMS.Agent*. It corresponds to a prolific malware family whose members differ from each other but which have this objective in common: subscribing the victim to premium messaging services. In 2011 there were only 31 new variants, compared to 2012 when the number rose to 153. Second comes another SMS Trojan known as Boxer. This malware and some of its peculiar characteristics will be explained later in this document; however, it is important to notice that in 2011 this family comprised 5 variants. Up to the present, the number of variants has increased to 36. Similar growth has been seen with *DroidKungFu*: 10 variants in 2011 and 33 in 2012. Finally, there is *FakePlayer*, the first malware targeting Android. In 2010 two variants emerged, as was also the case in 2011; but 2012 brought about 9 new variants.

Higher number of signatures to detect malware for mobiles

The quantity of signatures developed by ESET to detect malicious codes designed for Android has also risen considerably in 2012. This is due to the dramatic growth in malware variants, as shown above. Table 1 shows four families and the corresponding charts. For each of them, yellow represents the growth in 2012 and blue the growth in 2011. It is important to point out that a signature is a segment of code aimed at detecting one or more threats; therefore, if the number of signatures rises, it is due to the need to detect properly all the new malicious code that emerges on a daily basis. Note, however, that because one signature may detect many minor variants, the number of signatures is not directly proportionate to the number of variants, let alone the number of unique binaries.

Growth of families according to the number of signatures added in 2012, compared to 2011

Growth of families according to the number of signatures added in 2012, compared to 2011



Plankton	JSmsHider	DroidDream	DroidKungFu
The number of signatures rose 35 times in 2012	The number of signatures rose 12 times in 2012	The number of signatures rose 9 times in 2012	The number of signatures rose 6 times in 2012

Yellow: 2012
Blue: 2011

Table 1: Growth of families according to the number of signatures added in 2012, versus 2011

According to the table above, the Trojan family with the highest rate of growth in 2012 and the largest amount of signatures required to detect all its modifications was Plankton. This threat grew 35 times compared to 2011. Next, there is *JSmsHider* with 12, *DroidDream* with 9 and

DroidKungFu with 6 times respectively. On the other hand, though to a lesser extent, *BaseBridge* grew 3 times, *LightDD 2*, and *GoldDream* and *Geinimi* once compared to 2011 and the quantity of added signatures.

SMS Trojans: the most common threats for smartphones

SMS Trojans are the most common malware types for Android devices and the highest increases in the number of variants were represented by just two threats of this kind. During 2012, out of the reports of all unique detections of malware designed for the Google operating system, the *Android/TrojanSMS.Boxer.AQ* Trojan tops the list. It is followed by *Android/Plankton.H* and *Android/TrojanSMS.Agent.BY.Gen*. On the next page, there is an infographic explaining how this type of malware for mobiles generally operates:

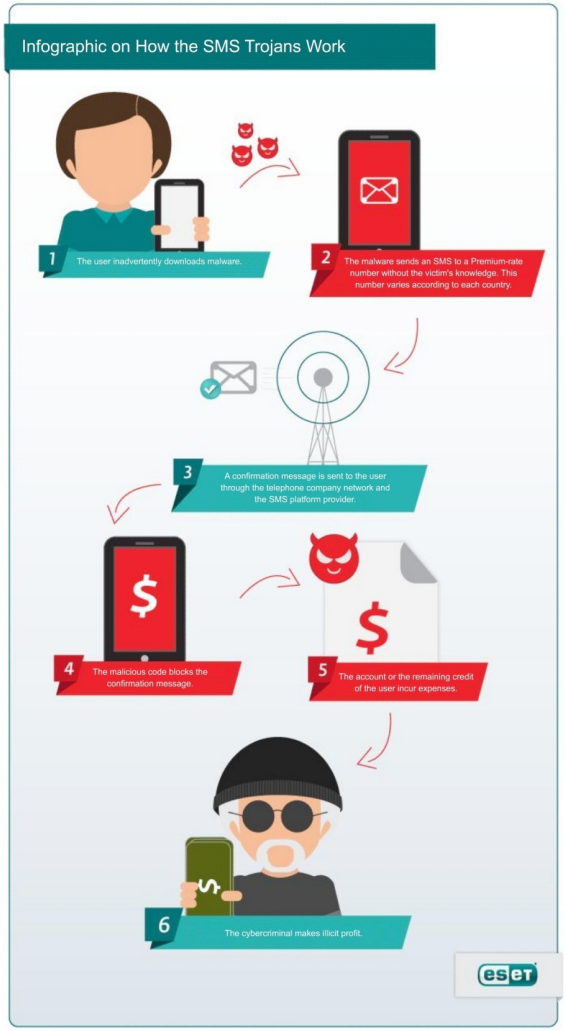


Figure 6: Operation of SMS Trojans

As long as this type of fraudulent business stays profitable and easy to implement for cybercriminals, it is likely that SMS Trojans will continue to be the most common mobile threat category during 2013.

What about Latin America?

Although China, Russia and Iran are the three countries with the highest ratings in the world in the detection of this kind of malware, Latin American countries like Mexico, Argentina, Peru and Chile have also been affected by the phenomenon. The following table shows the growth in detections expressed as the number of times it rose in 2012, compared to the same period in 2011:

Country	Number of times the amount of detections rose in 2012
Peru	28
Mexico	16
Brazil	12
Chile	10
Argentina	7

Table 2: Latin American countries and number of times SMS Trojan detections rose in 2012 vs. 2011

Among the Latin American countries, Peru was the most affected by this trend of progressive growth, increasing 28 times compared to 2011. It is followed by Mexico (16) and Brazil (12). Despite the fact that Chile and Argentina did not exhibit such a dramatic increase as the other nations (10 and 7 times respectively), they are nevertheless the countries in the region with the highest malware detection rates for Android.

Boxer: SMS Trojan affects Latin America

Another landmark in mobile malware development in 2012 was the discovery of a Boxer variant. Boxer is an SMS Trojan whose objective is to subscribe the victim covertly to various premium messaging services in order to generate illicit revenue for cybercriminals. This threat has two characteristics that distinguish it from other similar malicious programs: it is capable of affecting 63 countries around the world, nine of which belong to Latin America (**Argentina, Brazil, Chile, Peru, Panama, Nicaragua, Honduras, Guatemala and Mexico**). Moreover, Boxer was found in 22 Google Play applications. If the user is not cautious and his device is infected with this threat, the malware proceeds to detect the country and the mobile company to which the device belongs. Then, it sends three SMSs to premium numbers in the country in question. The chart below shows the nine Latin American countries affected by Boxer:

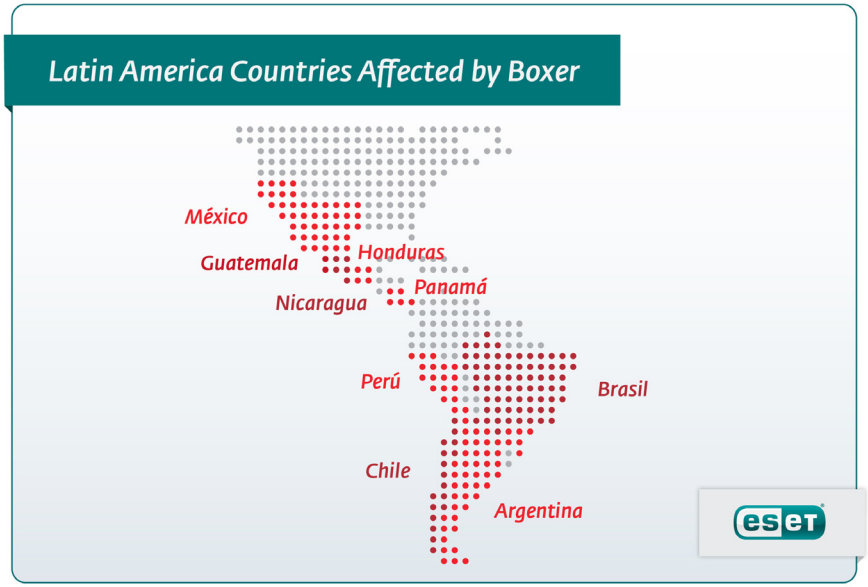


Figure 7: Nine Latin American countries affected by Boxer

While it is common to find SMS Trojans affecting specific countries or even a specific region like Eastern Europe, *Boxer* is capable of affecting Europe, Asia and America; consequently, it is one of the malicious programs for smartphones with the greatest potential for global propagation that has been found to date.

To learn more about this malware, read and download the ***Boxer SMS Trojan*** report.

As noted previously, the malware phenomenon for Android-based smartphones is expected to experience a considerable boom both globally and in Latin America. However, it is not the only growth trend that we'll see in 2013. The year 2012 has been marked, among other things, by cases of industrial espionage such as the ones that took place around the globe using the *Flamer* and *Gauss* malware, as described in the ***Blog of ESET Latin America's Lab***. Nevertheless, the first of a spate of reports of malware-borne stargeted attack was *Stuxnet*, a worm that affected mostly Iranian uranium enrichment plants. Although those attacks have mainly concentrated in the Middle East, there were reports on another that affected a Latin American country, as explained later on in this document.

Malware propagation through websites

The introduction of the first commercial version of Windows XP in 2001 and the massive uptake of removable storage devices (pendrives etc) marked the beginning of the era of worms that spread through these media by exploiting a Windows XP design vulnerability (*Autorun*). Given that this ***problem was solved in 2009*** and that users have migrated towards new versions of Microsoft Windows, the number of malicious programs still using this technique has diminished in the past few years. (Though there is no shortage of malware that includes it on the off chance of finding an unpatched system.)

In fact, throughout 2012, all detections related to exploitation of this design flaw (*INF/Autorun* and others) have been steadily decreasing.

On the other hand, generic detections such as *HTML/ScrInject.B*, *HTML/Iframe.B*, *JS/Iframe* and *JS/TrojanDownloader.Iframe.NKE* started to occupy the second place and other positions respectively, according to the ***Monthly threat propagation ranking*** prepared by ESET Latin America. The purpose of all these signatures is to detect various websites that have been compromised and modified by an attacker so as to propagate malware. In most cases, they are legitimate pages that belong to companies in various lines of business and that – due to a vulnerability, insufficient protection or inadequate configuration – have been modified by a cybercriminal who managed to access the server where they are hosted. Cybercriminals then proceed to inject malicious scripts or iFrames into the legitimate site: these redirect the user to another site where he is at risk of downloading a threat. In some cases the stolen information is also uploaded to this compromised server so as to avoid using personal computers and thus making identification of these individuals much more difficult.

The following table shows the percentage growth rates during 2011 and 2012 for some generic signatures used to detect malicious code propagated through compromised websites and removable storage devices.

Signature	Percentage growth in 2011	Percentage growth in 2012	Trend for 2013
INF/Autorun	5.8%	5.3%	↓
HTML/ScrInject.B	1.7%	4.3%	↑
JS/TrojanDownloader.Iframe.NKE	0.9%	1.2%	↑
JS/Iframe	0.6%	1.7%	↑
HTML/Iframe.B	1.5%	3.0%	↑

Table 3: Percentage growth rates of Autorun and signatures to detect compromised websites 2011 vs. 2012

In the table above, it is possible to see that Autorun decreased in 2012 while all the other signatures related to compromised sites rose. It is important to note that the figures above correspond to the percentage growth of monthly detections for each year and, in some cases, there are detections that were not present throughout all months of the year.

The following chart shows the whole of the year 2011 and January to September 2012, illustrating the percentage of detections associated with Autorun worms and threats spread through a compromised web server. To simplify interpretation of the information, signatures related to compromised websites have been classified as "JS" (JavaScript) and "HTML", and the "INF" prefix has been omitted from the Autorun signature.

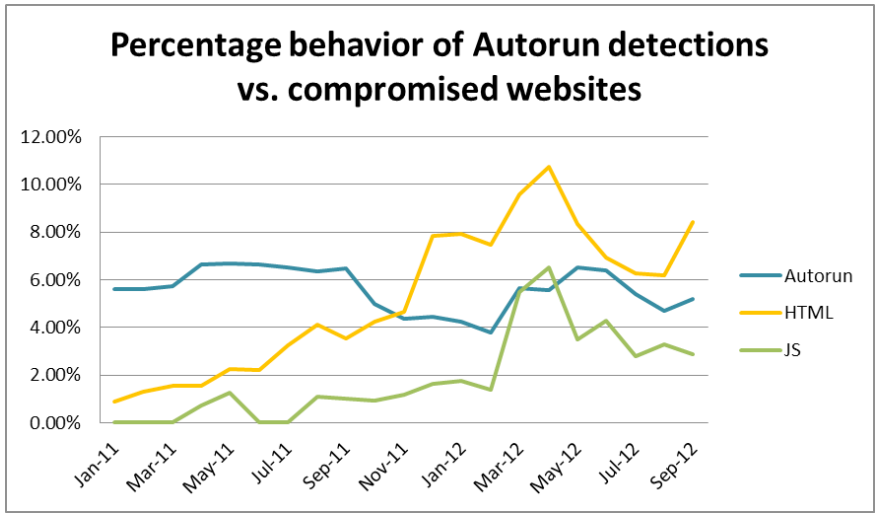


Figure 8: Percentage of Autorun detections versus compromised websites (2011-September 2012)

As can be seen, at the beginning of 2011 the signatures related to compromised websites were practically nonexistent. As the year progressed, the Autorun detection started to decrease, until in September 2011 it was overtaken by HTML detections. Moreover, both HTML and JS have experienced a considerable growth over time. This allows us to state that the **second trend for 2013 is a sustained rise in the use of this technique to infect potential victims**; therefore, the use of worms that exploit removable storage devices for infective purposes will decrease.

Before this trend shift in malware propagation methods, cybercriminals spread malicious code directly through some means (email, social networks, corporate resources, removable storage devices, among others) to the victim's computer, as shown in the following diagram:

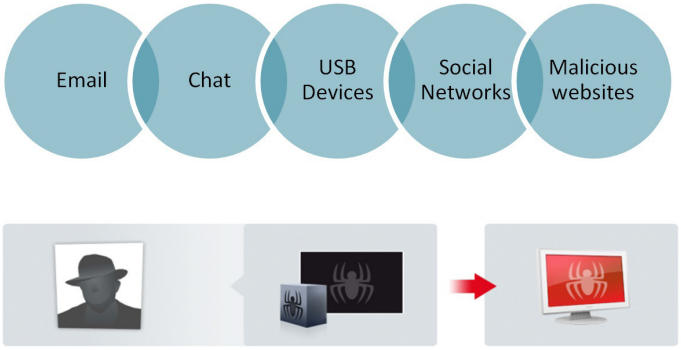


Figure 9: Traditional method of malware propagation

With this new malware distribution paradigm using compromised websites, cybercriminals turn to an intermediary (compromised server) to infect the victims, as can be seen below:

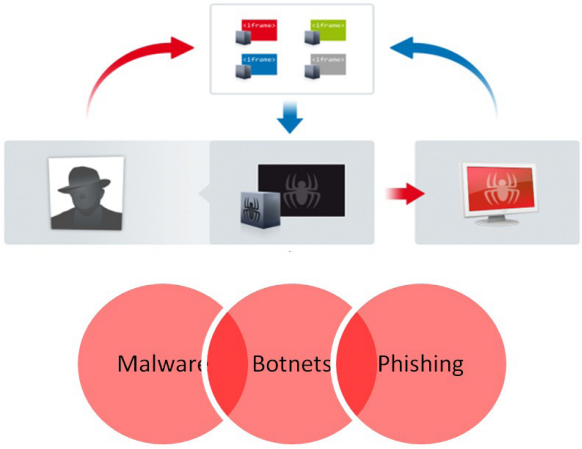


Figure 10: Propagation by means of an intermediary

In order to achieve this kind of propagation through websites, cybercriminal activity goes through the following stages:

1. The cybercriminal exploits an existing vulnerability in a web server. There, he modifies the original site to inject malicious code.
2. He starts to propagate the link that leads users towards the threat hosted on the compromised server. The hyperlink is sent to a list of users through email, social networks or any other means that will achieve its purpose.
3. The user visits this site and downloads the malware. In some cases, the information stolen from the victim is also stored on this intermediary.

Before this trend established itself, cybercriminals skipped the whole of this process and propagated the malware directly to the potential victims. Moreover, the stolen information was sent to and stored on their own computers.

On the other hand, apart from this new propagation technique, there is also the ***Black Hat SEO*** tactic toconsider. With this technique, cybercriminals use illicit techniques so that malicious websites will found near or at the top of the first page of results when a victim carries out a keyword search in a search engine. They generally use keywords related to tragedies (some actually in the news, some simply fabricated) or other issues of massive popular interest to make the potential victims curious enough to visit those malicious pages. Finally, it is important to notice that phishing attacks are usually deployed through an intermediary and also through command and control centers (C&C) belonging to (and running) a botnet.

Medre Operation: Industrial Espionage in Latin America

Since February 2012, ESET Latin America has noticed a significant rise in the detection rate of a quite distinctive malicious program: *ACAD/Medre*. Another novel characteristic in this case was that the vast majority of these infections came from a specific Latin American country: Peru. According to the information gathered by ESET Live Grid, our Early Warning System, 96% of the detections came from that nation. A subsequent investigation allowed us to determine that

this worm had been designed to steal blueprints and projects made with AutoCAD; it managed to steal approximately 10,000 files from Peruvian companies. For that reason, the **Medre Operation became the first known case of industrial espionage to affect the Latin American region.**

Figure 11: Detection map of ACAD/Medre

It is possible that in 2013 more industrial espionage cases will be found in Latin America; nevertheless, they will not necessarily be new attacks. This is due to the fact that in some cases, since these are usually malicious codes specifically designed to attack particular companies or countries, their discovery, detection and remedy may take a long time to materialize. Such situations might be reduced if a joint effort was made with organizations and the IT security industry. For more information, see the presentation ***Medre Operation: Industrial Espionage in Latin America?***

Botnets on the rise

Since 2010, malware designed to steal information and to generate revenue for cybercriminals has greatly consolidated its position. During 2011, there was a marked increase in these threats and this year they have kept on steadily rising, both globally and in Latin America. There is no doubt that the ***Dorkbot*** worm is one of the most prolific threats in the region, capable of turning the victim's computer into a zombie. An example of the reach this threat had is that the members of the ESET Latin America's Analysis and Research Lab found a botnet that comprised more than 80,000 zombie computers belonging mainly to Chile (44%), Peru (15%) and Argentina (11%). *Dorkbot* has spread by using a variety of topics that attracted victims by social engineering, such as fake videos about accidents suffered by Jennifer López, Hugo Chávez, Lionel Messi and Alexis Sánchez. Moreover, they have resorted to fake contests and prizes in order to find new victims. From a technical point of view, some variants of this threat spread through removable storage devices, social networks, Windows Live Messenger and other channels. Furthermore, this threat steals sensitive information like email account names and passwords, among other data. For instance, in this case it was determined that 88% of the email accounts stolen by cybercriminals using *Dorkbot* belong to companies. The remaining 12% are from services like Gmail, Hotmail or Yahoo!. The graphic on the following page shows a chart with the number of zombie computers (bot-infected systems) and types of user classified according to the operating system.

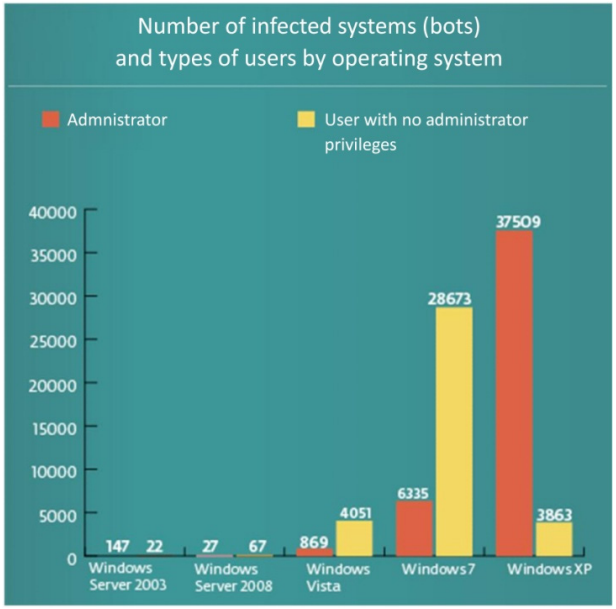


Figure 12: Number of infected systems and user types classified by operating system

According to the chart, it can be seen that most infected users still have a version of Windows XP and use an account with administrator privileges. Although this threat is capable of operating under any kind of account, it is important that people limit themselves to accounts with restricted privileges for everyday use; if they do this, some malicious code is unable to run or, if it does, its functionality is limited. Due to the complexity of *Dorkbot*, cleaning the infected system involves some additional steps the user must follow. For more information, we recommend checking out our ESET Lab's Blog: ***How can I remove Win32/Dorkbot from my computer? (In Spanish.)***

Another malware with botnet characteristics reported in 2012 was ***Flashback***. Unlike other malware of this kind, which has usually been designed to operate under Windows, this Trojan affects computers running with Apple's Mac OS X operating system. According to the information gathered by ESET, Flashback managed to infect around 750,000 Mac users, out of which **40,000 computers are located in Latin America**. Among the countries in the region that were affected the most by this threat, we find Mexico (45%), Brazil (17%) and Chile (13%). This situation once more demonstrates that the user must adopt 'safe hex' behavior patterns regardless of which operating system he uses. At the same time, the number of botnets generally is expected to rise in 2013 due to the flexibility they give to cybercriminals wishing to make money by sending remote instructions to zombie systems.

The cloud and cases of information leakage

Storage in the cloud is another trend that has been growing during 2012. ***According to Gartner*** [3], the increasing use of camera-equipped devices, such as tablets and smartphones, have a direct influence on the increased need of consumers to store more data in the cloud. It's likely that other events, such as floods that hit hard-disk drives factories in Thailand in the first half of 2012 ***have also influenced*** the growth of this technology. According to Gartner's report, it's

3 Source: Smartphone sales to end users by operating system in the Second Quarter of 2012, Gartner. Available at http://www.gartner.com/it/page.jsp?id=2120015.

estimated that in 2011 only 7% of the files belonging to end-users were stored in the cloud, but they predict a growth of 36% by 2016. Although this technology makes it easier for people to access information from practically any device with Internet access, it also makes such devices susceptible to being targeted by computer attacks, which can compromise the security of data and cause information leaks. This was proven when attackers accessed some ***Dropbox*** accounts, having stolen login credentials for this service from elsewhere. While this was not a failure of the Dropbox service itself, the incident prodded the site into improving its security. However - and just like other computer systems - the cloud is not free of dangers. It is probable that the more the use of technology grows, the greater the interest of cybercriminals in exploiting these services in order to generate some kind of profit.

Other portals that were also affected by information leakage incidents during 2012 were LinkedIn, Yahoo! and Formspring. On the other hand, mainstream credit cards companies like Visa and MasterCard had to issue a warning when a payment processing system suffered information leakage. This incident affected a total of 56,455 accounts from both companies, out of which 876 were used to commit some kind of fraud.

Hacktivism

Lately is has been possible to observe a rise in protests and demonstrations by citizens in several countries like Greece, Spain, Chile, Argentina, among other nations, due to some kind of social discontent. Given that technology and the computer world are part of daily life for many people, this activism making use of computer media has also grown (hacktivism). At the beginning of 2012, members of the Anonymous group attacked several sites enraged at the closure of the Megaupload portal. Consequently, the FBI site was knocked offline and sensitive information on Robert Müller, director of this organization in the USA, was also made public. Sony Music Entertainment was also the target of hacktivist attacks when the same group decided to protest against the explicit support given by the company for copyright legislation initiatives. In this case, Anonymous got access to multimedia material of artists and movies contracted to this company, and this material was later made available on the Internet.

Throughout 2012, different hacktivist groups have also protested against other issues, attacking sites belonging to Argentinean, Chilean, Venezuelan and Bolivian government entities, with many other countries also being targeted. In most cases, the websites under attack ceased to be publicly available, making it impossible for Internet users to access them. On other occasions, they used defacement: that is, they modified the original content of a website as a means of protest and even mockery. There have also been reports about cases where these attacks had an even greater impact: for example the AntiSec group claiming to have obtained 12 million iOS UDIDs; the development of a Linux-based operating system (Anonymous OS Live) personalized with tools to initiate Distributed Denial of Service (DDoS) attacks; the use of a personal botnet against GoDaddy; or the leak of information from 200,000 Peruvian domains

by Lulz Security Perú, among many others.
From the point of view of information security, hacktivism has proved organizations still have a lot to do regarding the protection of their systems at the technological, administrative and educational levels. There has been a growing trend, when there is a problem of a social nature, for people to act not only through traditional protests where they are physically present, but also express their discontent using a variety of electronic media. In 2013 we will be very likely to see attacks of this nature when some form of cyber-demonstration is more convenient.

Vulnerabilities

Vulnerabilities are usually exploited by cybercriminals so as to make malware propagation easier. By means of exploiting certain security flaws, it is possible to run malicious code without the need for any intervention by the user. For example, by simply visiting a website with this type ofexploit , it is possible for a user to get infected without attempting to download and run any program, let alone a threat. As proof, we can reference some of the vulnerabilities found during 2012. Using a zero-day exploit that affected Java, a Trojan detected by ESET NOD32 Antivirus as Win32/Poison was propagated. Where a site hosted a malicious applet, the user became infected simply by visiting it.. The problem with Java and security breaches is that the technology operates across multiple platforms; therefore, a security issue could result in the spreading of threats designed for several operating systems. Other software affected by a critical vulnerability was Internet Explorer. This weakness allowed cybercriminals to spread another variant of the Poison worm. Both issues were addressed subsequently by the respective companies. As a way of optimizing these attacks, cybercriminals develop security kits for vulnerabilities that include several security problems and ways to exploit them. Although this trend is not new, the last version (version 2.0) of *Blackhole* –a well known exploit kit– proves that attackers actively incorporate new exploits and functionalities with the purpose of making malware propagation easier. As new security vulnerabilities are found, the methods used to take advantage of them will be optimized to spread malware.

Another vulnerability that stood out in 2012 (and one that is somewhat related to the rise of Android malware phenomenon), is the discovery of a security failure in some computers with the Google operating system, which allows an attacker to restore the factory settings and thereby erase information. If a user visits a malicious site that exploits this flaw, the attacker can reach his objective by executing USSD numbers. As a way to protect the users, it is possible to install ***ESET USSD Control*** for free. This tool is available at the Google Play official repository site. Although Android vulnerabilities are not exploited as actively as Windows vulnerabilities, it is possible that cybercriminals will devote more time to looking for security vulnerabilities affecting these devices with the purpose of getting some kind of financial gain.

Malware for new technologies

As technology moves forward, inventions that used to be simpler, such as television sets, automobiles, routers, and smart cards – among others – have been expanded so as to offer the user new possibilities for using communications technology. For example, some televisions have the ability to connect to the Internet to show personalized content, and there are some cars that implement a GPS system to aid in the search for routes or places, and so on. Although all these innovations, when used correctly, may simplify and/or enhance people's lives, they also make it easier for cybercriminals to develop malware exploiting those technologies. When a device evolves with computerization, both its functions and its complexity increase; therefore, the existence of some vulnerability or failure that allows the creation of a computer threat becomes more feasible. At present, ESET Latin America has been detecting malware specifically designed to attack smart TVs from a well-known Korean manufacturer. The trojan, detected as *Perl/Agent.B*, looks for a network connection. If it finds any, it shows a message to the user indicating that he must install a so-called upgrade. If he accepts, the television turns off. Although this malware does not cause any permanent damage or steal information, it proves that it is possible to develop threats for devices other than computers, tablets or smartphones.

A similar case is the one reported in March 2012, a threat detected as *Linux/Hydra.B*. This is malicious code that attempts to create a network of zombie devices. Unlike other types of malware developed to create a botnet, Hydra affects non-traditional, embedded operating systems such as those found in IP surveillance cameras, home routers, VoIP (Voice over IP) systems, smartphones and tablets. When it was discovered, there were 11,000 bots reporting to the Command and Control Center (C&C), which shows that this malicious code managed to reach its objective of recruiting non-traditional zombie devices. Along the same line, researcher Paul Rascagneres discussed an attack based on malicious code whose purpose was to allow remote access to smart cards. This goal is achieved by harvesting the PIN and exporting the USB device to a C&C. Finally, other research presented at the Blackhat 2011 security conference discussed the possibility of affecting the security systems of next-generation cars. In one particular case, it was possible to illegally access a car system using wireless technology to automatically unlock the doors and start the engine. Although this was merely a proof of concept test and the vendor was informed about the problem, it shows that it is possible to attack the computer systems using this kind of technology.

Smartphones have evolved from a simple cell phone that made phone calls and sent SMS messages, into real pocket computers; and as other traditional devices experience a similar evolutionary processes, it will be possible to see malware designed to attack these targets. This problem increases if we take into consideration that the Java platform is able to function across various operating systems, apart from the fact that it is a popular target for cybercriminals in its own right.

Conclusion: mobile malware goes hand in hand with technology

The phenomenon of malware for mobile devices and the exponential growth that both the devices and accompanying malware will experience in 2013 has an explanation that transcends information security. Since the launch of devices like BlackBerry and iPhone (2007), the smartphone and tablet market has rapidly evolved in several areas: technology (better hardware and more optimized software), market (sales, amount of users, number of applications), and connectivity and infrastructure (3G and 4G LTE). This sector has experienced considerable growth as opposed to "traditional" computer markets, whose sales have seen significant reductions as a result of the growth of mobile devices. An example of this is the predicted growth of a mere 0.9% [4] in 2012 for the personal computer market segment, while smartphones and tablets are in a very different situation: according to the same consulting company, the tablet market segment has experienced a year-over-year growth rate of up to 66.2%[5] in the Second Quarter of 2012. These numbers are an incentive for cybercriminals to focus more time and resources in developing threats for these devices.

Together with the rise in smartphones sales, the number of mobile applications downloaded from Google Play and Apple Store have also drastically increased over the course of time. In July 2011, 15 billion downloads from Apple Store were registered globally, while in March 2012, this number almost doubled (25 billion) with a total of 550,000 available applications for iPhone, iPod, iPad, etc.[6] In the case of Google Play, the figures indicate a similar trajectory: in September 2012, the service reached 25 billion downloads around the world and a total of 675,000 applications and games[7]. At the same time, 1.3 million Android devices are activated every day[8]. The number of activations has also considerably risen as compared to 2011, when it only reached 550 thousand devices per day[9].

Mobile devices (tablets and smartphones) have rapidly evolved in terms of both hardware and software. The market now offers smartphones with quad-core processors, 2 GB RAM, more advanced GPUs (graphic processors) such as the Nvidia Tegra line, and other features that allow more complex tasks than was ever possible before. At the same time, new versions of operating systems like iOS, Android and Windows Phone have improved in areas like usability, functionality, performance and some security aspects. Faced with such technological turmoil, society has increasingly adopted this mobile equipment with the intention of staying connected to family, friends, and work; consuming gaming or informative content; streamlining banking operations, and so on. When we look at this

4 Gen are signatures designed to detect minor modifications of a variant generically, i.e., without the need of having specific signatures for each threat.

5 Gartner predicts that consumers will store more than a third of their digital contents in the cloud. Available at http://www.gartner.com/it/page.jsp?id=2060215.

6 IDC foresees a decline in PCs sales in the Second Quarter of 2012. Available at http://www.idc.com/getdoc.jsp?containerId=prUS23660312.

7 IDC: Apple sales drive tablet market growth. Available at http://www.idc.com/getdoc.jsp?containerId=prUS23632512.

8 Apple's app store downloads top 25 billion. Available at http://www.apple.com/pr/library/2012/03/05Apples-App-Store-Downloads-Top-25-Billion.html.

9 Google Play hits 25 billion apps downloads. Available at http://techcrunch.com/2012/09/26/google-play-store-25-billion-app-downloads/.

situation as a whole, taking into consideration the likelihood that all these statistics will keep on rising in years to come, we can assert that the volume of malware designed for mobile devices is a direct response to the speed at which the technology is being adopted. In other words, if the market grows and technology is enhanced, then as long as users who use these devices to store an increasing amount of sensitive information do not adopt the necessary measures, it is logical to expect cybercriminals to create computer threats to profit from this situation. There is a direct parallel here to what has happened with personal computers, but at a much slower pace over a much longer period.

Another factor reinforcing this dramatic growth trend of mobile malware is BYOD (*Bring Your Own Device*). This phenomenon is getting popular in many regions around the world and is directly related to the development of more and more advanced mobile devices. BYOD implies that a company's employees can carry and use personal devices such as laptops, smartphones and tablets within the corporate environment (including access to Wi-Fi wireless networks, VPNs, shared files and printers, among others). Consequently, until the necessary security measures are taken, ***BYOD could become a grave security problem*** for companies that don't think the strategy through. For example, an employee could have access to all his employer's corporate resources through a smartphone that is infected with a malicious program, and that program could steal the organization's confidential information. Another problem that may arise as a result of this trend is the theft or loss of a mobile device; therefore, if it is not properly protected, a third party could access the sensitive data stored on or accessible via the device.

According to a study carried out by Gartner[10], the devices that usually make up this trend are distributed among smartphones (32%), tablets (37%) and laptops (44%). At the same time, the companies that provide technical support to the personnel's machines vary depending on the region. The graphic shown in the following page compares the results obtained from those companies that do provide help and take this trend into consideration. The shown percentages correspond to countries belonging to the BRICS[11] (Brazil, Russia, India, China and South Africa) as compared to the rest of the world.

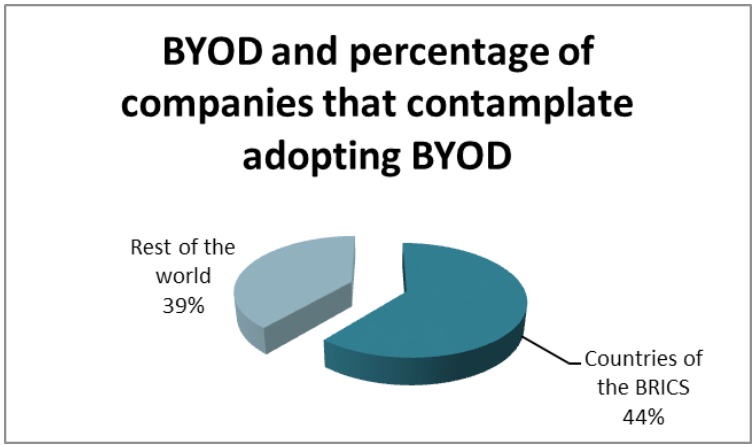


Figure 13: Companies that contemplate BYOD

10 "There have been 500 million Android activations to date. 1,3 million are activated per day". Andy Rubin, Senior Vice President of Mobile and Digital Content at Google. Available at https://en.twitter.com/Arubin/status/245663570812100608.

11 Android reaches 130 million devices. 500,000 new devices are activated each day. Available at http://www.theverge.com/2011/07/14/android-reaches-130-million-devices-growing-550000-day/.

It is possible to state that the larger and more multi-functional these devices become in 2013, the greater the number of companies and employees who will follow this trend. Although some organizations have chosen to ban their use, there are security best practices available, like the use of Wi-Fi networks separate from the core networks, the use of locking passwords for smartphones, the installation of a mobile security solution and the implementation of a corporate security policy that addresses the risks, all of which can minimize the risks that may arise if BYOD is not adopted with due care. The speed of this technical evolution has influenced the development of threats for mobile devices. *FakePlayer*, the first Android-based malware, was reported in 2010. Only two years later, the amount of malware for Android has grown at a dizzying pace. For instance, the number of malware variants for Android, such as TrojanSMS.Agent or TrojanSMS.Boxer, have risen more than 700% compared to 2011. It is also important to highlight that the percentage of signatures needed to detect each variant of a given family has also dramatically increased during 2012. For example, in 2012, the volume of signatures aimed at detecting different variants of the *Plankton* malicious code was 35 times that of the previous year. Malware targeting Android will not only keep on rising at a considerable rate, but also will continue to evolve until they are very similar in capability to their peers in the world of more traditional computers. A case in point is the *Zeus* variant for mobiles (*Zitmo*, *Zeus In The Mobile*), a well-known Trojan capable of turning computers and mobile devices into zombies. In recent years, the new variants of Zitmo that have appeared are capable of being controlled through SMS messages and evade banking systems using two-factor authentication[12]. Given all of the above, it is possible to state that mobile malware will evolve and grow in numbers proportionate to and in parallel with technology; in other words, if the technology has become popularized, commoditized and now constitutes a part of everyday life, computer threats for such devices will follow close behind.

Although Android-based malicious code is the main trend for computer threats in 2013, malware propagation that takes advantage of compromised sites is also a big threat and rapidly increasing; therefore, it has become one of the most popular propagation methods among cybercriminals. Therefore, it is important to take into account that, although the traditional computer market does not evolve at the same pace as sales of smartphones, cybercriminals will continue to develop a huge amount of malware for PCs. They will also find new kinds of attack technique as shown by the increasing visibility of propagation through the web.

As long as users continue making so much use of computers, they will continue to be targets for computer threats. In this sense, any infection vector that can make unauthorized access to a system easier for an attacker, such as security vulnerabilities, will make it likely that industrial espionage cases and botnets will carry on growing in 2013. The challenge for users and the community in general will remain the same: not only to adopt security solutions on their mobiles and PCs, but also to become aware of information security issues affecting this type of technology. Even as they simplify people's lives, these devices can also constitute a serious problem for information security when they are not used with due care.

12 Source: Gartner survey shows BYOD is top concern for enterprise mobile security. Available at http://www.gartner.com/it/page.jsp?id=2048617.