Trends for 2014

The Challenge of Internet Privacy

ENJOY SAFER TECHNOLOGY™

Trends for 2014: The Challenge of Internet Privacy

Author:
ESET Latin America's Research Team

Introduction

As usual for the end of the year, ESET Latin America's Research Laboratory has written ESET's annual threat trends report, which addresses several subjects in Information Security. the aim of this report is to make the community aware of the present computer threat landscape and, accordingly, attempt to predict its possible evolution in the coming years. On this basis, in 2011, a growing trend for botnets and malware for profit was noticeable[1]. In 2012, the main trend was directly related to threats designed for mobile platforms[2]. One year later, our main topic was vertiginous growth of malicious codes for mobile devices[3] and at present, although these threats keep growing and evolving, the main topic focuses on the growing concern expressed by users regarding Internet privacy.

In this sense, cases such as the revelations by Edward Snowden concerning the National Security Agency (NSA) of the United States had influence on the growing concern about Internet security. Nevertheless, this trend has not meant a decrease in cases of people affected by any malicious code or other kind of computer threat. It can be asserted that concern about privacy is a good starting point on the user side; however, it is essential for people to be aware of all aspects of Information Security. Otherwise, it is not possible to mitigate the impact of computer threats. This situation is equivalent to a person being worried about the safety of his home, but not actually installing an alarm system, so that he is still just as likely to become the victim of some incident.

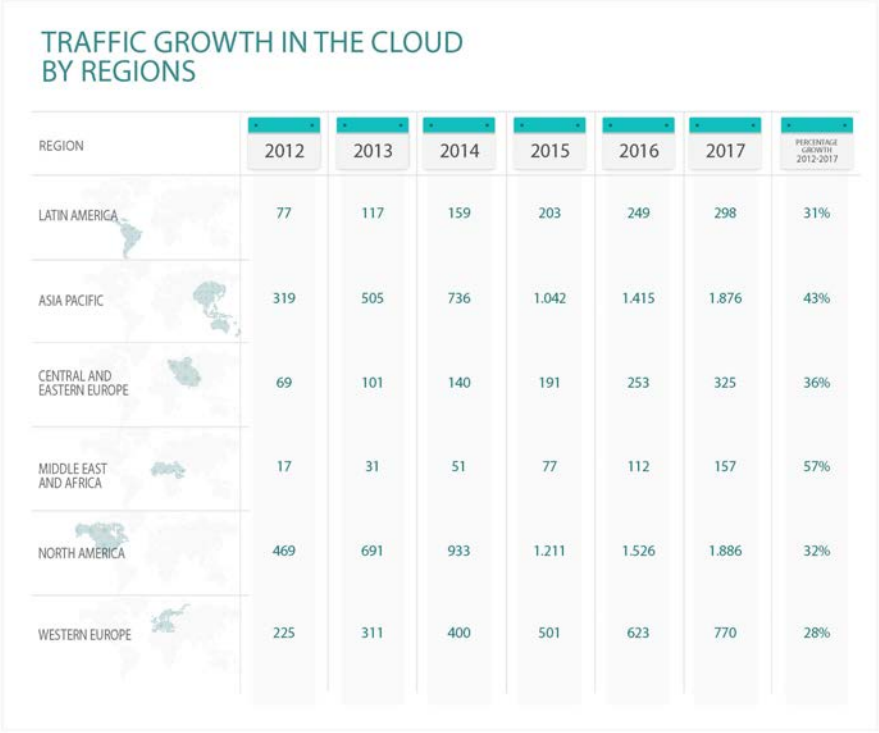
Another trend noted during 2013 and which we expect to trend upwards in the coming years is related to the increasing number and complexity of malicious code designed for the Android operating system. Cybercriminals are applying classic attack methodologies of attacks to newer, mobile platforms. On this basis, the discovery of critical vulnerabilities and their later exploitation through malicious code represent an evolution of cybercrime affecting mobile technology. On the other hand, an increase in complexity of botnets, 64-bit threats and malicious codes which try to obtain profits by stealing electronic coins, are all topics that have lately gained prominence. Finally, a variety of non-traditional devices such as smart cars, game consoles, smart TVs and others, introduce the possibility that in a future, threats for this kind of technology may be seen.

Taking into account the abovementioned topics, will privacy on the Internet be possible?

Loss of Privacy and Mechanisms to Protect Information on the Internet

Over the last few years, cloud storage technology has grown considerably in terms of the number of individual users and companies using it. Previously, it was normal to share information through diskettes, optical media (CD/DVD), USB removable storage devices and so on; it is currently possible to note a clear trend towards a massive use of the cloud to the detriment of other "traditional" means. the advantages that the cloud offers are considerable: for example, it provides easier to access information since files are available from almost any place and device connected to the Internet. Thus, in case of backups, it isn't necessary to choose a physically safe place to save the backup media. All these advantages have

caused the cloud to become more popular among all kinds of users. In this respect, Gartner stated that in 2011 only 7% of final user's information was stored in the cloud. However, it is expected that by 2016 this percentage will increase to 36%[4]. On the other hand, publication of the "*Global Cloud Index*" from Cisco, estimates that in 2017 Latin American users will have stored a quantity of 298 exabytes of information in the cloud (1 billion gigabytes)[5]. the following chart shows the projected cloud growth in several regions of the world and the quantity of stored data (expressed in exabytes):



REGION	2012	2013	2014	2015	2016	2017	PERCENTAGE GROWTH 2012-2017
LATIN AMERICA	77	117	159	203	249	298	31%
ASIA PACIFIC	319	505	736	1.042	1.415	1.876	43%
CENTRAL AND EASTERN EUROPE	69	101	140	191	253	325	36%
MIDDLE EAST AND AFRICA	17	31	51	77	112	157	57%
NORTH AMERICA	469	691	933	1.211	1.526	1.886	32%
WESTERN EUROPE	225	311	400	501	623	770	28%

Chart 1 Traffic growth in the cloud by region (expressed in exabytes)

The chart above indicates a growth in cloud storage in every region, i.e., the use of this technology by the users is growing over time. In the case of Latin America, the percentage growth expected for 2017 is 31%, compared to previous years. Despite this growth and its advantages for users, it is important to consider that this technology is not exempt from the risks associated with information security.

This trend of "going to the cloud" has many information security implications, but there is another subject which has suffered some changes due to the use and misuse of technology; that subject is **privacy**. In this sense, it is necessary to understand that humans are social beings who use different means to communicate with others such as speech or sign language, among others. the aim of communication is to share emotions, opinions and other points of life in society. If this case is applied to the technology environment, it is possible to relate it to social networks, services which make personal interaction easier through an online platform. However, despite this social and / or public human activity, there is another dimension with the same importance related to privacy. At this, the Internet is not an exception. In the same way that you would keep a professional or personal secret, in the virtual world there also exists confidential information which should not be available to unauthorized third parties. If a person needs to protect legal documents or any valuable object, he is more likely to think about a safe or any other secured place.

Although Internet users face the same scenario, mechanisms to adequately protect data are not always known or even when they are, used correctly. Although this subject arose decades ago with

the growing availability of information technology, cases such as that involving the National Security Agency (NSA) in the United States have caused, in a way, increased user interest in protecting the information stored in the cloud.

The NSA and the Privacy Debate

As an aspect of Internet and some value-added services such as search engines, social networks, and webmail, among others, privacy of information started to gain more significance for the community in general as opposed to security-conscious companies and experts in computer security. In 2004, it was noticeable at the time of the launch of Gmail, Google's web-based email service, some users were worried about their privacy[6]. the reason for this is that the company analyzes the contents of email and shows users advertisements based on that

On the assumption that actions performed on the Internet may have tangible consequences (whether positive or negative), several countries have applied regulations to address activities the results of which may cause damage related to aspects of social interest such as hacking, electronic fraud (malicious codes, phishing, etc.), pedophilia, and national security, among others. This last item was precisely the main subject of the incident and media debate created from public disclosures by *Edward Snowden*. Snowden was born in United States, he worked as an *NSA* technician through a contractor company until June 2013 when he leaked massive quantities of intelligence information related to the control exercised by US government over data privacy of citizens of the world in general[7]. This caused a global debate between countries which do not support this kind of control and the United States, which considers this as an action justified by the need to prevent terrorist attacks.

Beyond ideological, legal and moral debates created around this subject, there also exist incompatibilities dealing directly with Security of Information. From this point of view, it is important to understand that the security measures a user should take do reduce the impact and occurrence of several computer attacks such as hacking, malicious codes, information theft, etc. but they are not so efficient at the moment at preserving the privacy of the individual in scenarios of determined intrusion, such as those popularly associated with the NSA. In this sense, if a technological provider company establishes in its privacy policy any clauses that mention possible uses for the stored information, "traditional" protection mechanisms set up by users do not prevent such information from being used with some purpose established in the agreement. For example, some providers still keep users files even if the service is cancelled; thus, even former customers' data could be jeopardized in the event that the company is victim of any computer incident.

Regarding "traditional" protection mechanisms, a security solution protects the user from different malicious codes, a firewall defends against hacking, two-factor authentication defends against password-stealing attacks, and so on. However, in the case of user data that is stored in a system whose use depends on the acceptance of the privacy policy, it is the company rendering the service itself which may make use of such information; thus, other measures are required to strengthen security. In this context, it is crucial to read thoroughly the Terms and Conditions of Service agreement and

the software they use. It is important to take into account that when a person accepts this kind of agreement, he is explicitly accepting all items it contains whether he actually read them or not.

Greater Concern of Users about Privacy in the Cloud

As was previously mentioned, problems related to security and privacy of data stored in the cloud existed from the moment this technology started to take off. However, what has happened with NSA has caused more users to concern themselves with Information Security. the first statistical study to confirm this increase is related to web traffic from the search engine *DuckDuckGo*[8]. This site is known for offering users a higher level of privacy by offering the chance to search the Internet without registering internet user information. In this way, anyone using DuckDuckGo will obtain the same results regardless of their individual interests, location, and other personalization factors. In this sense, the amount of traffic registered by the site underwent a considerable increase after information regarding NSA surveillance leaked. Here is a chart illustrating this information:

Graph 1: DuckDuckGo Monthly Average Search Per Day

As can be seen in the graph, was registered an increased number of searches from May. It is important to mention that, at that time, there had been no massive leakage of information regarding NSA surveillance disclosures. Increase of searches was proved as from June, when Snowden gave details of how NSA works. From that moment, monthly visits to DuckDuckGo experienced a sustained increase of more than 200%, from 1,755,121 searches in May to a total of 3,890,084 in September. Although these numbers are considerable lower than those from Google, they suggest an increase in the number of users worried about Internet privacy since Edward Snowden´s leaking of information.

Another research showing popular concerns about Internet privacy is the survey performed by ComRes, a research consultancy from the United Kingdom. This research showed that out of 10,354 people interviewed living in nine different countries (Brazil, United Kingdom, Germany, France, Spain, India, Japan, South Korea and Australia), 79% expressed their worries about their privacy on the Internet[9].

Likewise, countries which were shown to be more worried about this subject are: India (94%), Brazil (90%) and Spain (90%). Next, a chart summarizing the main findings of that research is shown. Information is categorized on the basis of the nine countries considered in the research[10]:

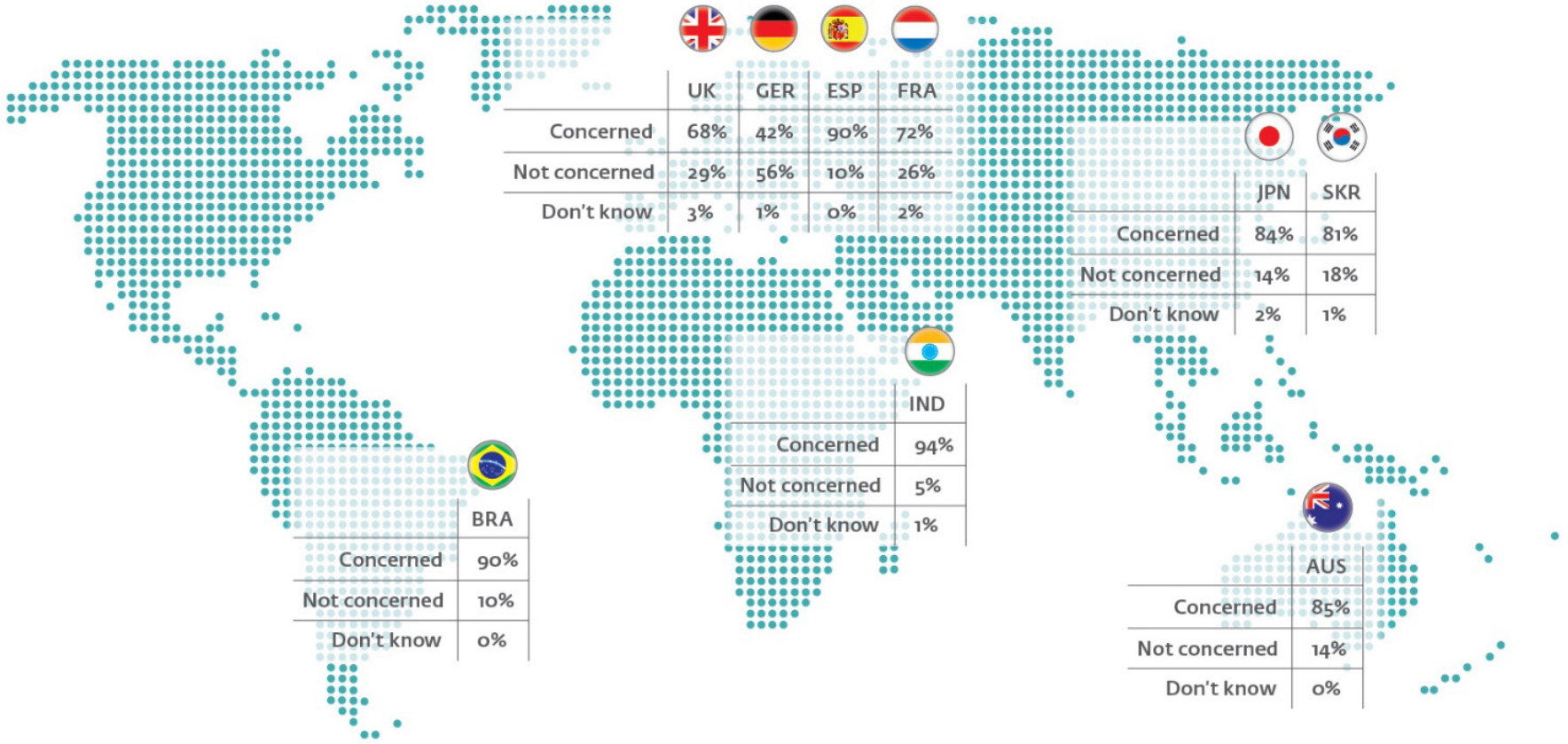


Chart 2: Summary of the survey by countries

The second column shown in the chart reflects the degree to which people in each of the countries are worried about privacy on the Internet. the next column is related to how companies obtain personal information, that is, which users' personal information is stored by organizations and how it's internal internally. the third item is about research started by the European Union measuring attitudes to a change in privacy policy applied by Google in 2012 and allows the company to unify data from different services that users use[11]. Finally, the fourth column confirmed the degree of agreement regarding the need for more severe regulation of Internet users' privacy protection.

According to the information gathered in countries taken into account in the research, Germany is the least worried about privacy in the Internet. the other nations share a more consensual view of the importance of how people's privacy should be protected on the net.

Beyond these specific cases, the current global trend is towards a higher concern regarding the ways in which companies and governments store, control and use private information of Internet users. It is possible that what happened with the NSA and Edward Snowden[12] had contributed to this concern, in that so many people around the world have become aware of the situation and, thus, have become more interested in preserving their own online privacy. Notwithstanding this concern, which was to all intents and purposes extended to the world and beyond social and media debate caused by initial concerns about the NSA, the protective measures taken by users to maintain their own privacy and security in the computer environments they use (computers, smart phones, tablets, and so on) are not enough in some cases. Likewise, as a consequence of this lack of security awareness, people often act in ways that are risk-laden, from the point of view of Information Security. For example, a survey applied by ESET Latin America showed that *67% of users who received a "Skype worm" were eventually infected with the threat in question*. the aforementioned malicious code was spread using suggestive messages, shortened links and Skype; a combination of social engineering techniques which proved to be effective enough to spread it in impressive numbers.

This affected percentage contradicts the trend which indicates that people are becoming more worried about their privacy in Internet. This is because malicious codes are threats which are generally developed to steal information, thus "invading" the privacy of those who become affected. Although at first sight this is an inconsistency per se, it can be explained by the fact that many users, even while using security technologies such as antivirus, firewalls and other tools, do not pay enough attention to security awareness. In fact, education is fundamental to the adequate protection of a computer environment and, in that way, it improves user privacy on the Internet. This opinion is borne out by analysis of the results of the ESET Latin America's *Security Report 2013*[13]. In that document, it is possible to observe that companies adopting awareness plans regarding Information Security are less prone to be victim of computer attacks, compared to those which do not carry out that kind of practices or do so inconsistently. It is important to mention that security consciousness, whether corporate or personal, must be persistent and sustained over time since security is a field which

evolves quickly. the following diagram aims to show that, although installation of a security solution grants an additional protection layer, consciousness is fundamental to obtain an adequate protection level:

Diagram 1: Greater concern is not synonymous with more privacy

As it may be seen in the diagram, there is more concern to keep privacy in Internet, however, lack of consciousness is still one of the main obstacles at the moment hampering adequately protection of information and privacy. Another survey which confirms the trend is the one carried out by ESET Latin America in July 2013. In that instance the subject was social networks. Regarding the question of how safely users think their information is kept on social networks servers, *52.2% think that they are slightly unsafe*, i.e. more than half of the respondents consider it is possible that such information may be obtained by a third party.

Before explaining the factors which may affect a person's privacy, it is essential to understand the role the user plays in this whole process. In the first instance, it is the user who decides which piece of information he wants to publish and which he does not, a decision which may increase or decrease his level of privacy in the Internet. At first sight, this process may seem simple, however, it is necessary to be careful and to understand properly the real scope and distribution an Internet publication may have.

In a first attempt to reduce this problem, some social networks such as Facebook have applied simpler methods to limiting the information a person publishes, such as buttons to set up visibility of something transmitted. In this setting, the user can choose to make the content public or just for the user's friends or exclusively for a single individual. On the other side, Facebook also applied *a new menu which allows the Facebook user to manage user privacy easily*. To relieve problems at this first stage, it is important for the user to know that this kind of control exists and also to think about the implications this situation may have. One example might be the chance that a spiteful third person may obtain personal information if potential victims make public any data such as domicile, telephone numbers, workplace, and so forth.

The Cloud and Information Storage in Other Countries

As was previously mentioned, the cloud is not a new online storage technology: however, its flexibility has caused, with the passage of time, a massive increase in use in homes and by companies. According to Gartner research projecting several aspects of the state of the cloud between 2011 and 2016, Latin America is not the region which has economically invested the most in this technology (that would be the United States with 59% of investments); however, some individual countries in Latin America, such as *Argentina, Mexico and Brazil are nations with higher rates of growth of services in the cloud*[14].

Despite this increase, and the flexibility given by a service of this kind, the cloud is still creating controversies and uncertainties regarding the security and privacy of the stored data. In this respect, some users express their concern because this technology does not allow

direct control over data as does a local server or the user's own system. To clarify this subject, it is necessary to understand some aspects of the technology in question. First, it must be considered that the information or the platform in which it will be stored in the cloud may have been compromised before, during or after data transmission. the following diagram shows the three previously mentioned stages:

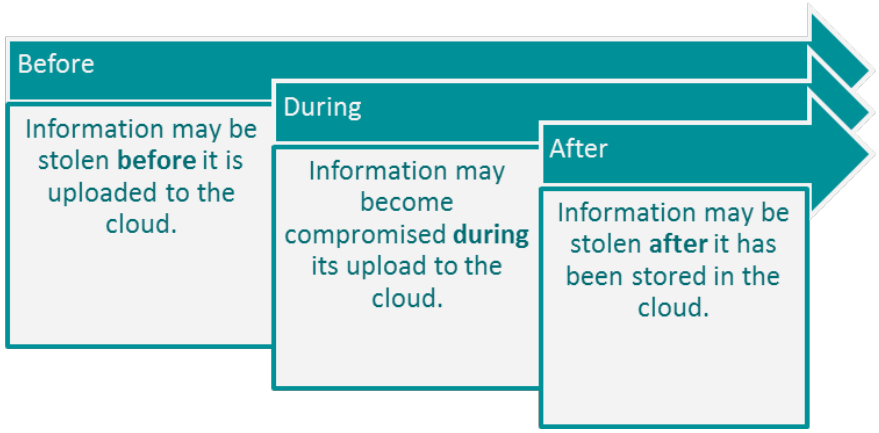


Diagram 2: Stages in which information theft may happen in the cloud

According to the diagram above, the first stage at which information may be compromised is before it is stored in the cloud. For example, a company whose systems are infected with *malicious code* is vulnerable to having information stolen before it is ever uploaded to the cloud. On the other hand, information may also be at risk if organization sends information through an unsafe connection. In this case, hacking would happen during transmission of data due to attacks such sniffing or packet theft. At the third stage, security adopted by the service provider in the cloud such as data encryption, policies governing use and security, and so on, also determines the probability that information to be stored in the cloud may be damaged as the result of an attack against the services provider.

Likewise, the country where the server that stores information resides may also have a critical influence on information security and privacy. Each country has a different set of rules regarding data protection in computer environments. Thus, more restrictive legislation may be of benefit at the data protection level. However, a less severe legal system or absence of specific regulation may affect information privacy.

Greater Legal Regulation and Clearer Privacy Policies

Legislation is one of the means employed by countries to regulate Internet use, penalizing acts such as information theft, fraud, pedophilia-related crime, and hacking, among others. Accordingly, in 2013 Peru tried to penalize specific activities that may attempt, whether direct or indirectly, to work against users' privacy in Internet. In this case, the Peruvian congress passed its *Computer Crime Law*. This law tries to punish pedophilia-related traffic and electronic fraud. For example, in case of privacy breaches, the law establishes a six-year prison punishment.

On the other hand, in the wake of NSA case, the president of Brazil, Dilma Rousseff, was worried about the privacy of citizens using Internet. For that reason, she raised the possibility that companies would be obliged to store all data from Brazilians on local servers[15], that is, computer systems that are physically established in that

country so that Brazilian data protection legislation may be applied. More precisely, about the location of a computer system and regulations applicable within the said countries is one of the problems specific to the cloud and it is explained in detail in the following pages. As it may be seen, cybercrime as well as government surveillance issues have caused users' Internet privacy to be a priority for society as a whole.

Companies have played their own part in this situation. There is a growing trend towards making known and simplifying the privacy policy of services such as Facebook, *LinkedIn* and *Pinterest*. In the case of Facebook, the company inserted changes into its *Data Use Policy* and *Bill of Rights and Responsibilities* for users of that service. Updates try to explain some aspects of these documents and also give advice focused on privacy such *removing Facebook applications no longer used*. In the case of LinkedIn, the aim was to make privacy policy easier to understand. For its own part, Pinterest carried out a system which offers personalized content and which can change set-up parameters related to the privacy of the account[16].

With all these changes, it seems that there is a trend towards publicizing privacy policy and making people more aware of the topic. Similarly, some countries in the region have gradually shown more interest in regulating the Internet and users privacy.

How to Protect Information on the Internet

Starting from the premise that the Computer Security of individuals can be observed and quantified, it is necessary to understand the different factors which may compromise the individual's privacy. In the same way, it is essential to know which technologies may mitigate the impact of this problem. the next chart exposes the different factors that may compromise user privacy. Technologies and protection measures are also summarized that may be adopted to reduce such impact (see Chart 3).

In the above chart, some concrete measures are mentioned that the user may apply in order to increase security and privacy on the Internet. Some actions in particular, such as encryption of data and two-factor authentication, are explained in detail in the following pages.

FACTORS WHICH MAY COMPROMISE USER PRIVACY

FACTORS	Description	Protection measures and tecnologies
COMPUTER THREATS 1	Threats such as malicious codes, phishing, scam, infringement of servers and passwords, among others, usually steal confidential imformation from the victim.	> Implementing security technologies (antivirus, firewall, two-factor authentication, etc.) > Having a safe and precautious behaviour. > Being aware of the latest trends regarding compùter attacks.
NON-CLEAR OR ABUSIVE PRIVACY POLICIES 2	Some programs or services include not so clear or abusive privacy policies which may affect users.	> Before installing a software or a particular service, read the privacy policy carefully. It is important to consider that, when using any of these products, you accept the privacy clauses.
UNAUTHORIZED ACCESS BY THIRD PARTIES 3	Taking into account that no computer system is exempt from suffering attacks, it is possible that user's information is accessed by third persons if the provider company does not take the necessary measures.	> Data encryption (cypher) is a technique which consists in making a piece of information illegible in case the correct decryption password is not entered. Open code applications are recommended and those with 1024-bit or 1048-bit passwords.

Chart 3: Factors which may compromise user privacy

Data Encryption (Cryptography)

Another effective security measure in this context is data encryption (crypto). Simply expressed, this is a method of making information unreadable in such a way that it is necessary to use a key (password, passphrase, PIN, token) to decipher data and make it readable again. In this event, information may still be obtained by a third person: however, if adequately encrypted, it isn't readable without the necessary password. However, as with every computer protection measure, it is not infallible. the degree of security given by encryption depends on the robustness of the encryption algorithm, that is, the way in which information is encoded to make it unreadable. Although it seems paradoxical, it's important to read one more time the user agreement in case the software or the encryption service includes among its policies the right or necessity to share the key or decryption algorithm, in which case user information may be further exposed.

Next, we show a diagram summarizing the data encryption operation:

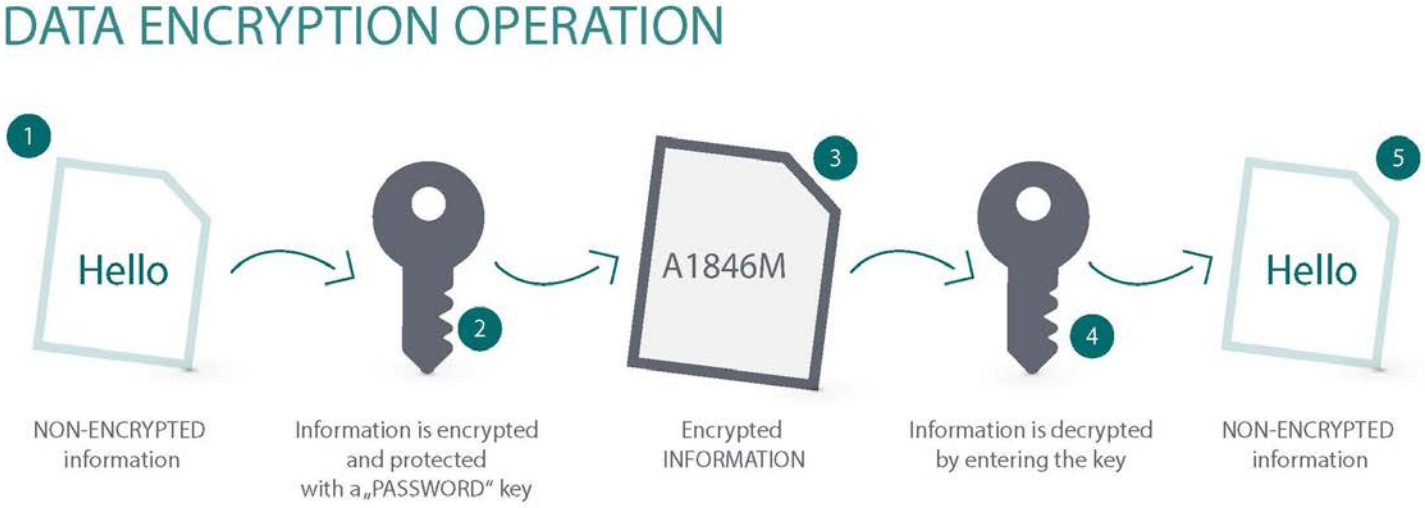


Diagram 3: Data encryption operation

As may be seen in the diagram, the original information is in plain text, i.e., not encrypted (1). At the second stage, information is encrypted and protected by a key (2). Next, any user who tries to access encrypted data and does not have the right key will not be able to access or at any rate read the information (3).Finally, those persons who actually have the key are able to decrypt the data (4) and view the original message as it was before encryption (5).

On this basis, it is always convenient to encrypt information before uploading it to the cloud. In this way, data is not vulnerable to being decrypted and accessed by unauthorized third persons. Similarly, technologies such as *Microsoft BitLocker* allow stored files to be encrypted in the local system (i.e. on the user's own device). Thus, to encrypt information locally as well as in the cloud considerably reduces the possibility that an attacker might access and misuse data.

Information Theft and Mitigating Attacks with Two-Factor Authentication

As was already explained in the document *Trends for 2013: Astounding growth of malware for mobiles*, cases of information leaks due to attacks by third persons have been taking place since 2013. Cases such as the *Burger King breach*, where the attacker compromised the fast food franchise's Twitter password and used its Twitter account to publish advertisements for one of its competitors, as well as the different computer threats which tried to steal passwords (malicious codes, brute force attacks, attacks to servers and phishing), have proved that simple authentication through the knowledge factor (single-factor authentication by password, i.e., something the authorized user knows) is not enough to reduce the impact of attacks.

Two-factor authentication is a methodology which implements a second authentication stage, so that it reduces the risk of successful attacks. For example, when a user accesses his account (mail, social network, bank, etc.), as well as entering access credentials (simple authentication by password) he has to enter a second corroboration code such as a software token which might be sent to a smartphone by SMS or provided by an application. In this way, if an attacker can obtain the name of the user and password, he still cannot compromise user privacy because he does not know the second authentication factor.

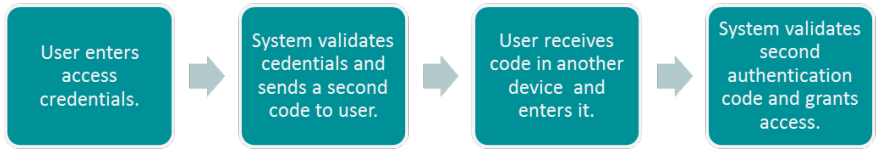


Diagram 4 How two-factor authentication operates

The next diagram simplifies and clarifies the way this system works:

A trend which became evident during 2013 is the increase in the number of companies which have used two-factor authentication systems as a way of reducing some computer attacks. Except for financial entities which have a longer history of working with this technology, this protection system has been adopted by organizations such as *Facebook*, *Apple*, *Twitter*, *LinkedIn, Evernote, Google, and Microsoft*,

among others. Generally, in order to improve usage of this system, they just request the second authentication factor in the event that the person uses a new or unknown device (one which has not been previously added as a safe device). This prevents the user from entering the second authentication code every time he wants to use the service. Likewise, at present several services enable the use of this kind of protection using *Google Authenticator*, an application, available for mobile platforms, which creates a random code that may be entered as a second authentication factor for accounts with (for example) Microsoft, Google, Facebook, Amazon Web Services, and Evernote. Accordingly, ESET put on the market *ESET Secure Authentication*, a solution created to implement a two-factor authentication system for VPN networks and corporate email servers.

While more companies are offering this kind of protection, lack of user awareness of this technology makes it difficult to make much impact on the total number of computer attacks. Even worse, two-factor authentication often comes deactivated by default; thus user activation and manual set up becomes necessary. In order to measure how aware users are with respect to two-factor authentication, ESET Latin America carried out a survey on this topic. According to the information obtained, *more than 64% of users in Latin America do not know what two-factor authentication is*. There is evidently a serious lack of user awareness of this mechanism, certainly, at the moment as regards taking advantage of a two-factor authentication system.

Taking into account the fact that concern about enhancing Internet privacy is a topic of social interest, it is possible that in future we will see users moving towards this kind of double protection; and programs raising awareness of this subject. To this end, ESET Latin America published the document *Is it the end of passwords? Simple authentication more and more threatened*. In the cited text, there is more information about the operation of this authentication method and how to activate it in the context of a number of services.

Cybercrime

As was already explained in the previous pages, user awareness of Internet information privacy issues has increased; however, certain computer threats, such as malicious code, are still one of the main causes of information theft and loss of privacy. Although the lack of user awareness plays the main part in the "success" of these attacks, the cybercrime world constantly improves and updates its methods in order to improve its profit margins.

As was already explained in the document *Trends for 2013: Astounding growth of malware for mobiles*[17], the increase of computer threats for Android devices – as well as for the mobile market in general – has evolved quickly. To this effect, and as happened in 2013, the number of detections, families, versions, variants and of signatures to detect malicious codes for Android will continue to accelerate.

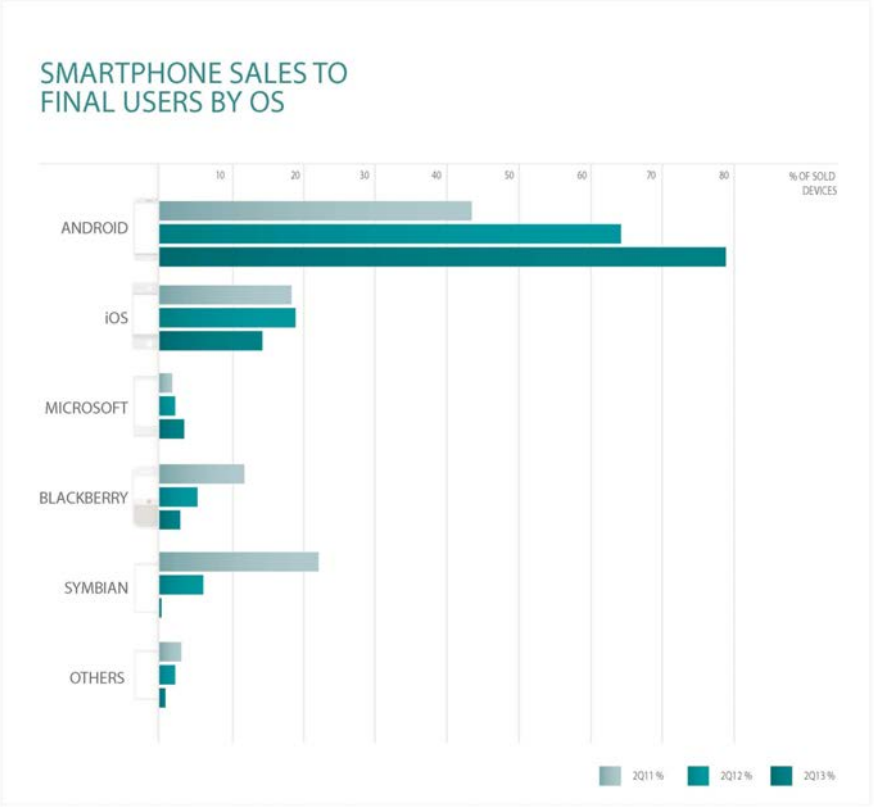
Beyond the trends stated in the previous paragraphs, we have also noticed the technical evolution of certain kinds of malicious code. the first category relates to threats designed for botnets, that is, networks of compromised computers (zombies) which are operated by an attacker for malicious purposes. In the second place, malware designed for 64-bit platforms, which has become increasingly complex and sophisticated lately. Finally, it is important to point out that

blackmail using malware (*ransomware*) as a method of making illicit profit has become more common in Latin America, being no longer a technique executed exclusively in countries such as Russia and the United States.

Android: Market Leader and Most Attacked

In the document 'Trends for 2013', it became evident that the Android operating system from Google has consolidated its position as the most widely used mobile platform. In this sense, the leading trend regarding the market segment occupied by Android is an accelerating take-up rate; this might explain the increase and consolidation of different computer threats affecting this platform, as we shall explain later. Going back to the mobile market, it can be noticed that Apple iOS is still the second most popular operating system. the following graphic shows the evolution experienced by different existing mobile platforms. For that purpose, two Gartner[18] research documents were used, which consider the market statistics for the second quarter of 2011, 2012 and 2013 (see the chart on the right).

According to the results published by Gartner, in the second quarter of 2011 Android had 43.4% of the market. One year later, that percentage increased to 64.3% and at present, it has reached 79%. This growth goes hand in hand with a directly proportional increase of the quantity of malicious codes developed for Android. Likewise, evolution of some threats for this operating system and the discovery of certain vulnerabilities show the increasing interest that cybercriminals have in attacking this segment.



Sources: Smartphones sales to final users 2Q11 and 2Q12-13, Gartner

Regarding other operating systems, iOS keeps its position in spite of some ups and downs as the second most popular platform on the market. Windows Phone experienced a slight increase while BlackBerry and Symbian suffered a decrease.

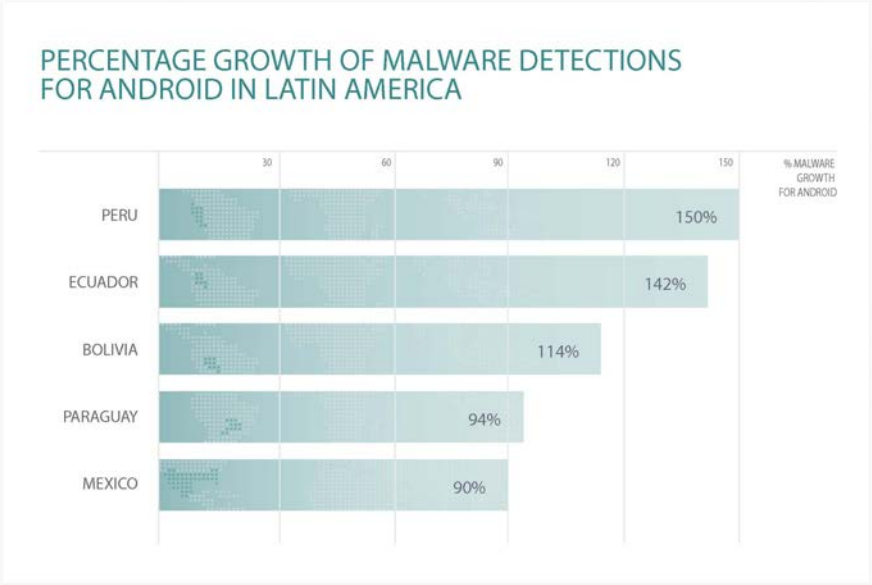
The following pages explain the growth experienced by some threats for mobile platforms regarding the number of detections, their complexity and other factors. Then, in the third section, the trend for "non-traditional" devices will be explained – i.e., devices which host Android and other operating systems – and the risk for security and privacy this may entail for users.

Computer Threats for Android Keep Increasing

As was forecast in the document Trends for 2013, malicious codes for Android are rapidly increasing. the first number to corroborate this item is related to the quantity of unique detections. Comparing detections that occurred in 2012 and 2013, it is possible to establish that they have increased by 63%. It is important to mention that we are contemplating the whole of 2012 and only part of 2013 (from January 1st to October 22nd). This is therefore a significant increase.

Countries with greater growth of the number of detections of malware for Android are Iran, China and Russia. On the other hand, there are five Latin American countries, which also showed a larger percentage rate of detections in 2013 compared to 2012: Peru (150%), Ecuador (142%), Bolivia (114%), Paraguay (94%) and Mexico (90%). the following graphic shows the aforementioned percentages more visually (see the chart on the right)

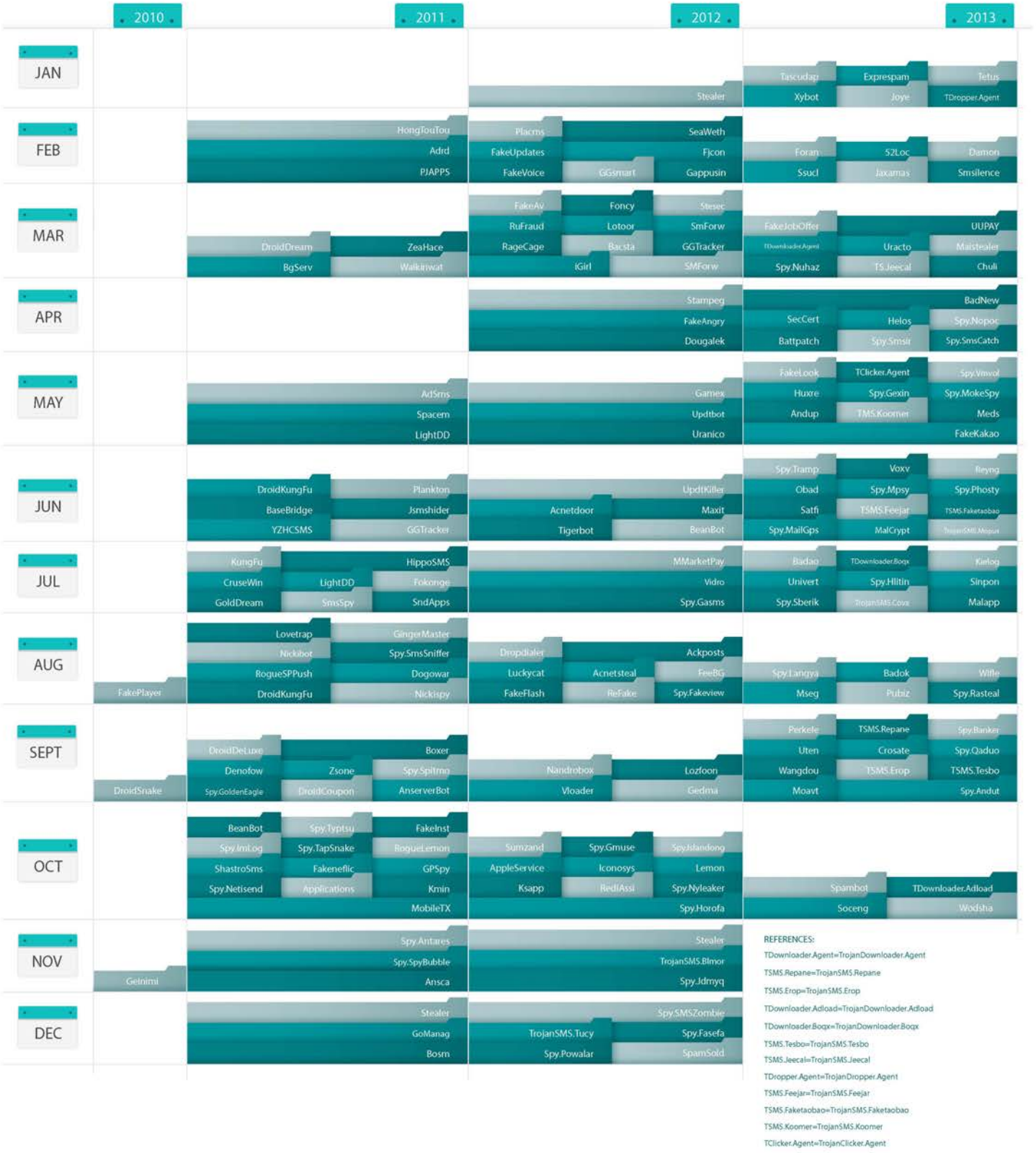
Comparing numbers of this year and those expressed in Trends for 2013, Peru and Ecuador are still leading this ranking. Below them are Colombia (63%), Chile (17%) and Argentina (20%) making way for Bolivia, Paraguay and Mexico.



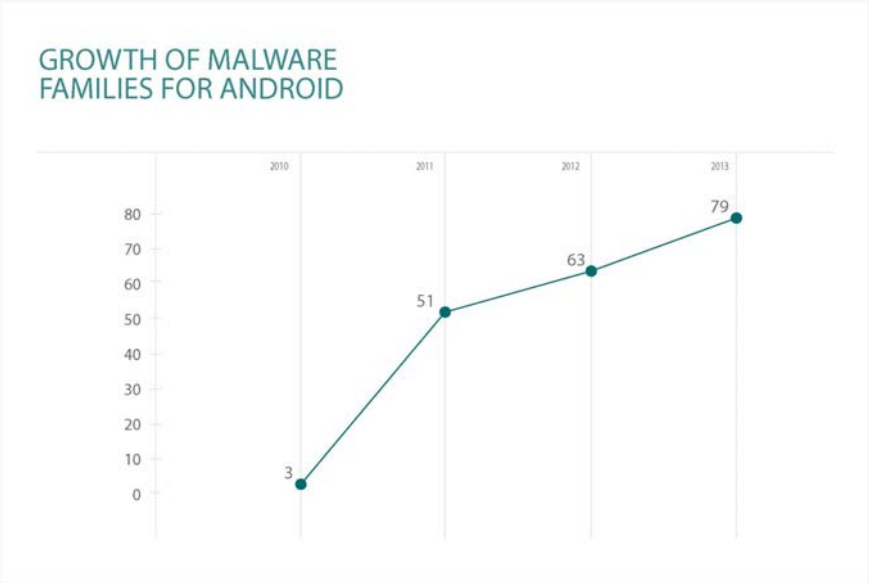
New Families and Types of Malware for Android

Concurrently with the percentage growth of detections of malicious programs for Android, an increase can also be noticed in the number of malware families for this operating system. It is important to point out that a family is a group of malicious codes which share some characteristics. Next, there is a diagram reviewing families which appeared in the last four years (2010-2013):

EVOLUTION OF MALWARE FOR ANDROID



The graphic shows that in 2010 there were only three families. As the years passed, the aforesaid number increased so that in 2011, 51 families were reported; 63 families were reported in 2012; and 79 were reported in 2013 (up to October). the following graphic shows the trend:



It is important to point out that the greatest number of malware families for Android was reported in 2013, even though we are considering only the first ten months of the year. If we compare the same period of time (from January to October) in 2012, 55 families appeared and 79 in 2013. This represents a growth of 43.6% during 2013. Another interesting aspect to our analysis regarding malware families is the discovery of new categories of Trojans for Android. Until one year ago, it was usual to find spyware Trojans, SMS Trojans, and botnet malware that tries to turn the device into a zombie. However, in 2013, four sub-categories of Trojans were reported that were only related to Windows and other "conventional" platforms:

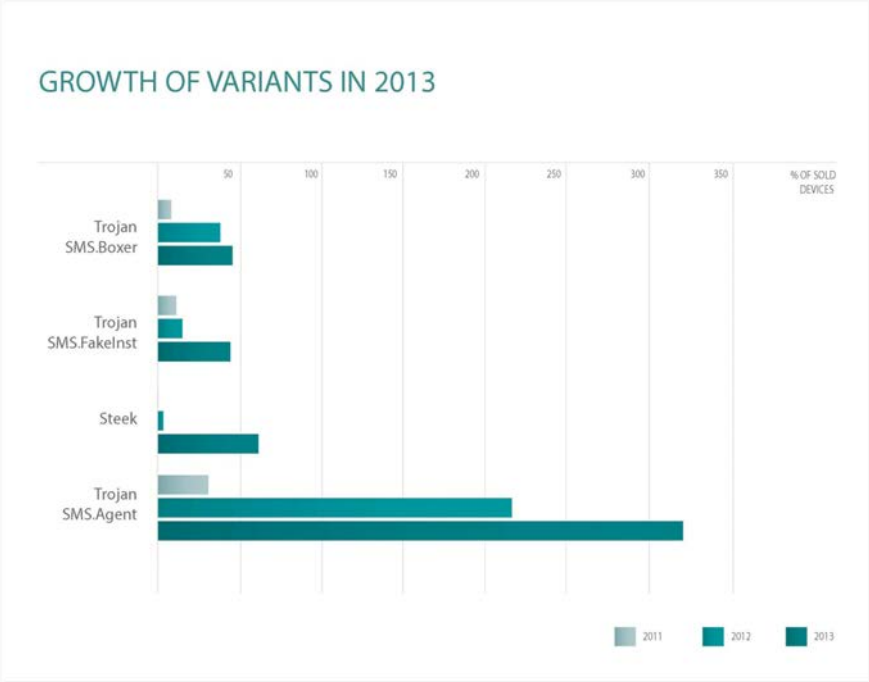
1. Downloader Trojan: tries to find other threats from Internet to subsequently install them in the device.
2. Dropper Trojan: installs other threats that the Trojan itself includes in its code.
3. Clicker Trojan: intended to create traffic in a site or advertisement with the aim of artificially increasing the number of "clicks". This allows the attacker to create a greater yield.
4. Bank Trojan: specifically tries to steal information related to financial entities and Banks.

The prevailing trend is not only related to the growth of threats for the Google mobile platform but also to appearance of subtypes of Trojans which previously affected only "traditional" operating systems. It is probable that, in the future, the number of families composing each of these sub-categories will increase.

Malware Versions also increasing

Another figure which has increased again is the number of versions comprising each family; i.e., relatively minor changes to known malicious code. Attackers usually develop new versions with the aim of detecting security solutions and to add new malicious functionalities. It is important to point out that for every new version that appears, the ESET laboratories assign a new letter as a suffix to the threat name which increments according to alphabetical order.

For example, two versions of a new malicious code would be classified as Threat.A and Threat.B. In the event of exceeding the available letters, the alphabet is repeated:.AA,.AB, etc. the following graphic takes into account four families of malicious codes for Android. For each one, the number of versions which appeared in 2011, 2012 and 2013 is included, as appropriate:



Once again, the family which experienced the highest growth in versions is *TrojanSMS.Agent*. the first version of this malware dates from 2011 and, in that year, it comprised 31 versions. In 2012, 214 versions were discovered and one year later, 324. the next highest growth is shown by the Steek Trojan, whose first version was discovered in 2012. Nowadays, the aforesaid malicious code is comprises 61 versions compared to the three detected in 2012. Boxer and FakeInst also increased in 2013 with 45 and 48 new versions respectively.

Vulnerabilities in Mobile Platforms

Vulnerabilities are programming mistakes that, under certain circumstances, may be used by attackers to compromise a system and (for instance) steal information. Mobile technology is not immune to this problem, since mobile devices also use software and hardware, which may contain errors and bugs. Nevertheless, at present more cases are seen of vulnerability exploitations affecting "traditional" systems than affecting mobile platforms. However, in 2013 it has been very clear to us that cybercriminals are focusing on exploiting security gaps in operating systems for mobiles like Android.

A piece of evidence confirming this assertion is the discovery of the *Obad Trojan*. This malicious code can be manipulated by a third person through SMS and it can download other threats and steal sensitive information, such as the victims' contacts. Although such Trojan characteristics do not amount to innovation, the exploitation of vulnerabilities unknown till the discovery of the Trojan (0-day) does. the first one resides in the program *dex2jar*, software used by the security industry to analyze malicious codes designed for Android statistically. the second vulnerability exploited by Obad resides specifically in the Android operating system.

Before clarifying this aspect, it is necessary to explain that Android has a list, visible to the user, enumerating those applications installed that request administrator authorization to function. This list can be accessed in some devices from Settings → Securities → Device Administrators. Based on this, a security vulnerability allowed this malicious code privileged execution within the list of programs requesting legitimate authorization. In this way, it was impossible for the victim to see Obad as an application that required administrator authorization. Although this situation, where malicious codes exploit 0-day threats (unknown until that moment), is not new in platforms such as Windows, it is novel for Android. Obad's discovery shows that cybercriminals are looking for new vulnerabilities in operating systems, such as Android, with the aim of carrying out computer attacks easily.

On the other hand, *Bluebox Labs* researchers found an enormous vulnerability affecting almost all Android systems (from 1.6 to 4.2). Its discoverers named it "Master Key": this fault makes it easier for attackers to develop malicious codes which steal information and turn devices into zombies and camouflage them as genuine applications. Exploitation of this vulnerability affects the way in which Android corroborates an application's cryptographic signature[19]. In other words, every legitimate application has a *unique key* which allows its authenticity to be confirmed. In this way, if a third person arbitrarily modifies a program, Android prevents installation of software because the cryptographic signature is broken. However, by means of this vulnerability, a cybercriminal could alter an application yet leave the cryptographic key intact. Thus, the malicious program would be executed without any warning by the operating system.

NFC Technology

Near Field Communication (*NFC*) technology allows interchange of information by putting together two devices. Although it can be used for file transfers, some countries such as Chile are using this communication protocol to pay services more easily, such as restaurants and malls, amongst others[20]. Its aim is to make everyday life easier so that people do not have to carry credit cards or other means of payment with them. However, it is important to consider that any technology used for bank transfers is a potential target of computer attacks. In this sense, it is possible that as this means of payment becomes more popularly used, it will be easier to find malicious codes trying to steal information relating to such payment transactions.

In the case of NFC technology, information theft could happen at the moment in which user makes the payment. Thus, it is essential that payment data stored in the equipment as well as the process of information transmission at the moment of payment are strongly encrypted.

Other Trends in Cybercrime

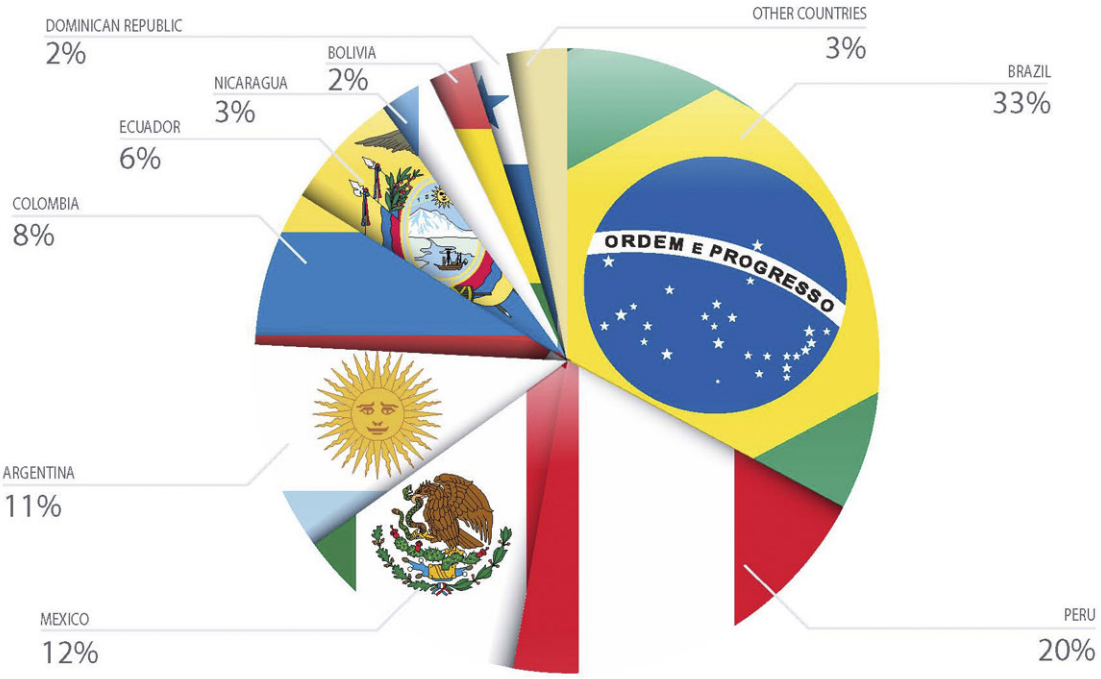
Vulnerabilities – Java and Latin American Sites

In the article Trends for 2013, one of the main trends analyzed was the spread of malicious codes using an intermediary such as a web service which has been breached by attackers for that purpose At that time, it was clear that detection statistics related to that method of spreading showed a sustained increase. Nowadays, this trend is still growing in Latin America, *blogs* being *one of the most widely breached types of service in the region*. They represent 47% of total amount of affected sites according to a list of compromised pages.

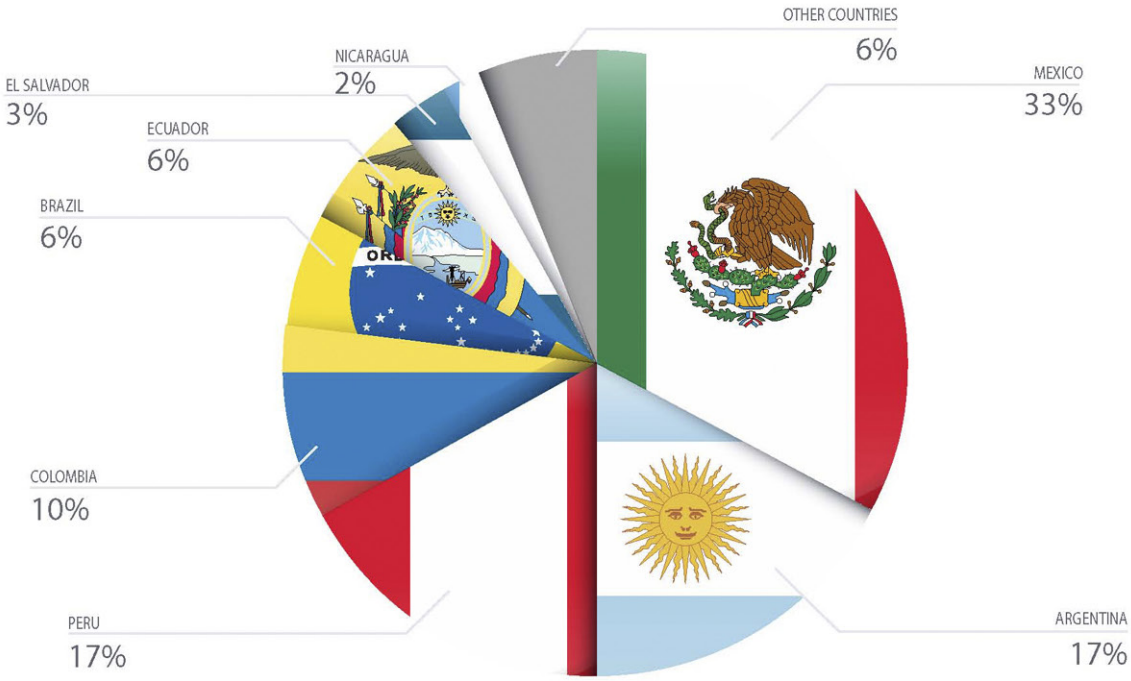
On the other hand, ESET Latin America Research Laboratory was able to determine that *Brazil, Mexico and Peru* have the greatest proportion of official and education sites which have been compromised by third persons in order to spread malicious codes. From 4500 compromised sites which were studied, 33% belonged to Brazilian government pages, followed by Peru with 20% and Mexico with 12%.

Of the *malicious codes hosted in those sites*, 90% belong to Trojan families and the remaining 10% was divided between worms and backdoors. As regards compromised pages belonging to educational entities, Mexico is leading with 33%, followed by Peru and Argentina with 17%, as can be seen in the following graph.

PERCENTAGE OF AFFECTED GOVERNMENT DOMAINS BY COUNTRY



PERCENTAGE OF AFFECTED EDUCATION DOMAINS BY COUNTRY



On the basis of the information summarized in the previous paragraphs, it is notable that the trend towards the use of an intermediary has kept on rising in the region; however, these problems have also increased in technical complexity. This is due to the increase of exploitation of different Java vulnerabilities and the development of new malicious codes designed to automate the exploitation of vulnerabilities in Linux web servers and the spread of computer threats.

The first aspect of this technical evolution is related to exploitation of *vulnerabilities in Java*. It is important to consider that Java is a multiplatform technology (working on several operating systems) which has the capacity to add new functionalities to websites. Thus, it combines two characteristics which are useful for cybercriminals. On the one hand, the fact that it works in different operating systems makes it easier for attackers to compromise different environments; and on the other hand, as it is a popular technology, cybercriminals make sure they affect the greatest number of users.

The efficacy of attacks exploiting vulnerabilities in java was empirically proven when companies such as *Facebook* and *Apple* were infected. Later investigations showed that the cause to be a malicious program which could enter systems belong to both companies through exploitation of vulnerabilities in this software. To achieve that aim, the attackers breached a website that Apple and Facebook employees used to visit. Cybercriminals installed a malicious applet (Java application) which exploited a security hole on that page. Finally, and after a victim visited the compromised site, infection could be accomplished with little or no participation on his part. Next, the stages which made both attacks possible are shown:

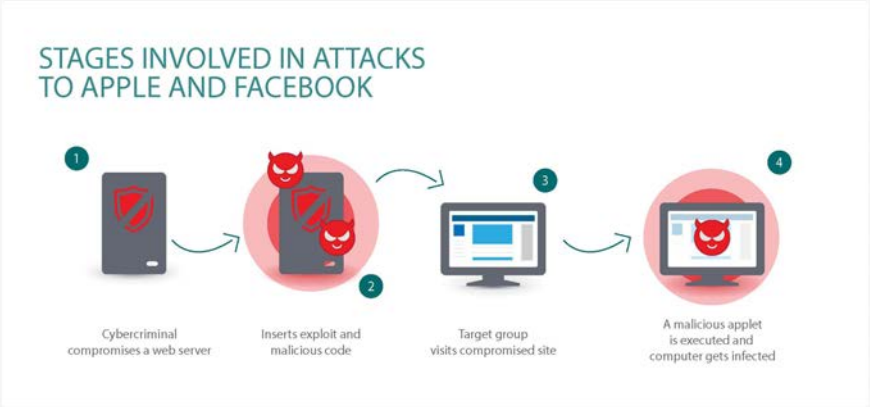


Diagram 5: Stages involved in attacks to Apple and Facebook

The second aspect of this technical evolution has to do with the development of new malicious codes designed to breach Linux-hosted web servers. Where cybercriminals used to breach a server through the exploitation of a vulnerability in order to use it to host malware, nowadays, that "manual" operation is being replaced by the use of malicious programs intended for that purpose, such as *Cdorked*, *Chapro* and *Snakso*. In these three cases, malware is specifically designed to compromise Linux web servers. Later, these threats fulfill the aim of changing sites and spread other malicious codes designed for Windows, eventually successfully automating the whole attack process.

Botnets

As was mentioned in the publication *Trends for 2010: Crimeware Maturity*, the authors of computer threats started to develop malicious codes whose main aim is profit. This trend has been constant over time and has been combined with malware which tries to establish botnets. These are computer networks that once infected (zombified – see *Net of the Living Dead: Bots, Botnets and Zombies*), are at the mercy of a group of cybercriminals (botmasters) who use them to steal information, attack other systems, and store illegal content without the victims' consent, among other malicious actions.

If we consider that the main aim is to obtain increase illegal profits, it is understandable that cybercriminals use their resources for the creation of botnets. In this way, the larger the number of infected computers, the greater the chances of making money. Apart from the malicious programs having this functionality that have been observed, we also see techniques which try to increase the complexity of this kind of threat to avoid disruption of the botnet by the authorities or other organizations. the first case observed in 2013 has to do with a malicious code detected as *Win32/Rootkit.Avatar*. This threat uses Yahoo! Groups as a means of controlling zombie computers. Likewise, this malicious code has techniques used to avoid *expert analysis*, That is, to obstruct those researches performed with the aim of determining aspects of infection needed for forensic purposes.

Another trend in botnets is the *use of TOR as a way to hide the performance of cybercriminals*. Although this is not a new technique per se, in the last months we have noticed an increase in the use of this methodology for the following reasons. Sometimes analysis of data transmitted to and from a botnet allows us to determine what information is being stolen; likewise, it makes botnet disruption easier, and, potentially, tracing of the persons responsible. However, when using TOR, attackers make all the previously mentioned aims much more difficult to achieve, since this network was specifically created to encrypt all transmitted data, making traffic capture more difficult. Throughout 2013, it has also been established that besides using several versions of malware families already known, cybercriminals also develop new families such as *Napolar*, a piece of malware which has affected countries such as Peru, Ecuador and Colombia. This threat was spread through Facebook and has the ability to create a botnet, make denial of service (DoS) attacks (massive bulk sending of requests to a server until it knocks websites offline), and steal information from the victim, among other actions.

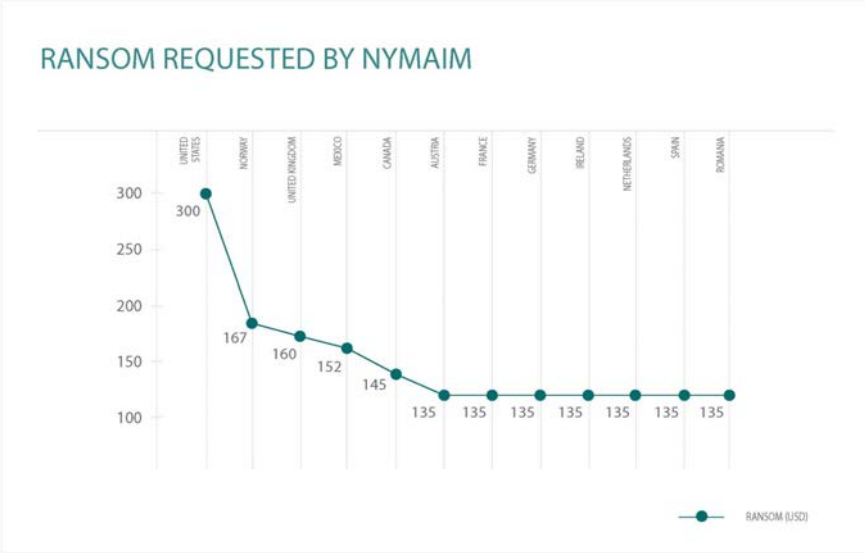
On the other hand, proof of concept phenomena such as the *creation of a botnet net integrated by 1,000,000 surfers*, as presented at the BlackHat 2013 conference, reaffirm the possibility that in the future cybercriminals will use other techniques to use zombie computer networks to make illegitimate profits. As was already mentioned, the use of these methodologies not only adds complexity and the consequent difficulty in the study of these threats but also increases by way of countering the effectiveness of security solutions. In this sense, as proactive detection methods such as heuristics and generic signatures evolve, so do threats. It is probable that in the future new cases of malicious codes and families destined to be part of these kind of network will be detected and, at the same time, cybercriminals will establish techniques to make such threats more effective.

Ransomware in Latin America

Until fairly recently, malicious codes of the ransomware kind – i.e., the ones which demand money for the recovery of systems and information they delete or encrypt – mainly affected countries such as Russia. However, this attack methodology is becoming established in Latin America and there are already several users who have been affected. In the case of the malicious programs referred to in the previous sections, the profit resides in the direct theft of information. However, in the case of *ransomware*, the profit comes from the extortion of money from the victim.

When a user executes malicious code with these characteristics, it may happen that access to the system is locked. an example of this behavior is presented by the *LockScreen* (Multi Locker) malware family, more commonly called the "*Police Virus*". In this case, a person cannot have access to the equipment until the system threat is removed. In other cases, information is encrypted in the same way that the *Filecoder* malware family operates. In both cases, cybercriminals demand money from the victim in return for the control of the computer or for access to "kidnapped" information.

Regarding the increase of ransomware threats in Latin America, *Mexico stands out as the country most affected by Multi Locker*. LockScreen detection in this nation has increased almost three times compared to 2012. Likewise, in 2012, Mexico occupied the 37th world level position of LockScreen detection; currently, it occupies the 11th position. Likewise, *Nymaim is another malicious code affecting that country* which requests an amount of money (150 dollars approximately) for the recovery of the system. It is important to mention that the price of the rescue varies according to the country. the next graphic shows the amount requested in various nations:



As regards Filecoder statistics in the region, Peru is shown to be the country with the highest rate of detections in Latin America during 2013, Russia being the world´s most affected nation. In relation to the technical complexity of this malware family, it is important to mention that in some cases, it's possible to recover encrypted files because the encryption algorithm used is so lightweight, or because the decryption password is found within the threat code itself. However, as these malicious programs evolve, the implementation of more and more complex algorithms is precisely one of the 'improvements' being added, and such algorithms make it difficult

or impossible to recover the files. There is more information about encryption methods in *Filecoder: money for kidnapped information*.

This kind of methodology arises from the premise that users store valuable information and do not make necessary backups; thus, when confronted with a desperate situation the victim may decide to pay for the "rescue" as even a *Massachusetts police force did*. This action encourages and stimulates illegal business activity, so *not paying and adopting the necessary countermeasures* contributes to preventing and combating this kind of malicious code.

Malware Evolution for 64-Bit Systems

64-bit platforms are not new. In fact, in 2005 Microsoft already offered a version of Windows XP designed to work on processors that use the *x86-64* instruction set. Despite this, at that time this technology was not widely used, so it was not targeted by cybercriminals. This situation has been changing and computers with 64-bit architecture are now more frequently found. According to statistics published by Microsoft, in June 2010 46% of Windows 7 installations globally were 64 bit versions[21]. Likewise, according to information published by Digital Trends, Gartner predicts that for 2014, 75% of corporate computers will be using some version of 64-bit Windows[22].

The increase in the use of 64-bit systems is logical if we consider that this technology allowed the use of more than 4 GB of RAM; something that usually 32-bit versions of Microsoft's desktop operating systems cannot natively handle (unless features like Physical Address Extension, PAE are used). Besides, some complex applications are benefited in terms of profitability if they are developed for 64-bit systems. In this context, cybercriminals are developing more threats specifically designed for this technology and over time, they have evolved technologically. *Expiro, for instance* is an example of this kind of virus, which can infect 32-bit as well as 64-bit files; this makes it a highly versatile and infectious threat. Expiro's aim is to steal data entered by the victim on various websites.

In consequence, detection rates for malicious codes designed for 64-bit platforms have also increased in Latin America. Countries such as *Mexico, Peru and Argentina have experienced the most important growth in the region according to this trend*. Next, a graphic showing the percentage for each country is shown:

Mexico (23.9%) and Peru (23.7%) are the countries in the region most affected by malicious codes designed for 64-bit Windows platforms. Meanwhile, Argentina (9.2%) is quite a long way behind and other

countries such as Chile and Brazil are even further behind with 5.9% and 5.4% respectively. Among the most detected 64-bit malicious programs in Mexico and Peru, the *Win64/Sirefef* and *Win64/Conedex* families stand out.

This trend will probably increase even more in the future. Likewise, launching of smartphones using 64-bit operating systems such as iPhone 5s suggests the likelihood that, in time, we will detect the first computer threats designed for 64-bit mobile platforms.

Bitcoins

Bitcoins represent a relatively new electronic currency not controlled by any central authority. They also allow the purchase of "real" assets and not necessarily just virtual ones. These characteristics make this currency an attractive target for cybercriminals. Consequently, more and more threats can take advantage of CPU and GPU calculation power of the user´s computer to obtain Bitcoins. In this sense, and taking into account the fact that Bitcoins are electronic coins, system resources can be used to 'mine' for such currency. However, the computation necessary to obtain a Bitcoin is *so complex* that it requires substantial resources and processing time, so that cybercriminals use botnets to achieve this goal more easily. the advantage of the use of several computers in parallel is summarized in the following diagram:

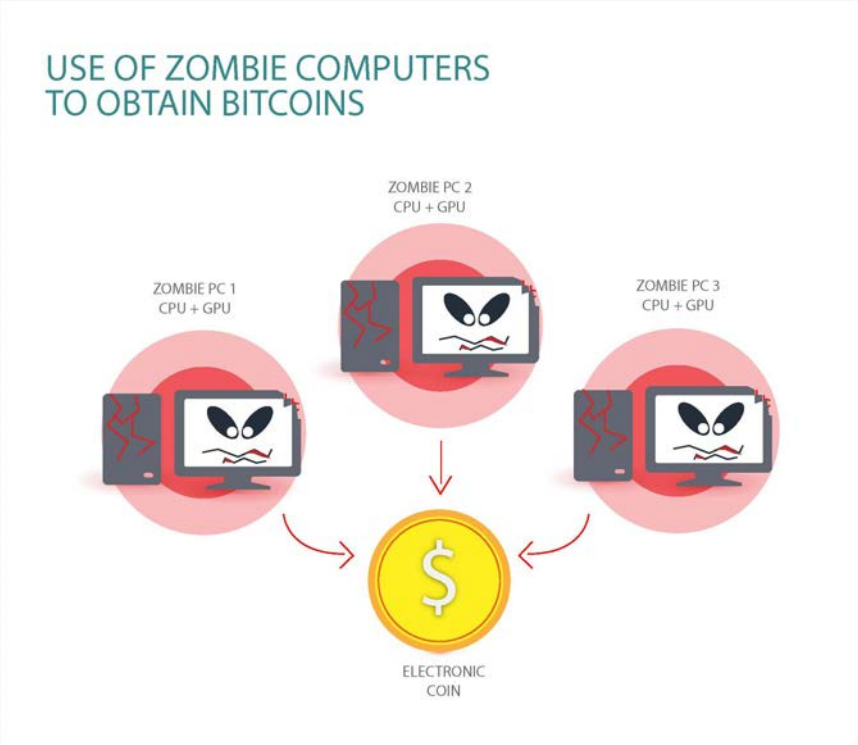


Diagram 6: Use of zombie computers to obtain bitcoins

The most widely used method profiting from these currencies is by calculation of an algorithm used by digital coins. Among examples of malicious codes used for this kind of processing are *Win32/Delf.QCZ* and the even larger *CoinMiner* malware family. Although Bitcoin is the most widely used electronic currency these days, there are alternatives which have similar characteristics and which have also become targeted of attackers. an example is *MSIL/PSW.LiteCoin.A*.

There is a second method by which attackers can obtain illegal earnings from users of these currencies. Generally, they use electronic wallets to store this kind of tool for electronic transactions: hence the development of malicious code designed to steal exactly the file where this information is located. This methodology is not new, but the increasing popularity of electronic coins leads us to expect that these threats will increase in number and complexity. For more information about this subject, we recommend reading "*Bitcoins, Litecoins, Namecoins and how electronic money is stolen in the Internet*".

Malware Diversification: Computerization of all Kinds of Electronic Devices which Allow Internet Connection and Data Sharing

Ten years ago, few would have thought that a cell phone could be infected with malicious code. At that time, these devices had only basic functions such as telephone calls and SMS. Thus, it was technically difficult or even impossible to discover computer threats targeting these types of equipment. However, at present, the situation is radically different. the evolution experienced by this technology has been such that smartphones can perform actions similar to those performed by a computer such as photo editing, high speed Internet connection, bank proceedings, games, etc. This technological advance has been enabled by software (applications and more complex operating systems) as well as hardware (four core processors, larger RAM memory, 64-bit architecture, etc.).

Together with this technological evolution, there is a trend not only of growth of this market and of computer threats for mobile phones but also diversification into other "non-traditional" devices using Android as operating system. In consequence, products such as games consoles (*NVIDIA Shield*), smart glasses (*Google Glass*), refrigerators (*some Samsung models*), washing machines (*Samsung Touch Screen washing machines*), among others, are already available in some countries. Although this kind of technology has not been massively adopted in Latin America and other regions, it is probable that this will happen. This suggests that in the future there will be computer threats designed for smart appliances and other equipment which are not strictly mobile devices. This likelihood increases if we consider that the operating system of these devices is Android, which makes it easier to develop malicious codes and other threats that target them.

On the other hand, it must be considered that Android is not the only operating system being used in smart devices. Other companies have chosen to develop proprietary platforms, that is, systems designed specifically for a group of smart appliances and not based on open source code. In this case, it's harder for computer threats to be developed. However, there is no case where the creation of malicious code is inconceivable or impossible. Finally – and bearing in mind what happened in the mobile market and the growth of threats targeting this equipment – it is possible to deduce that latest-generation appliances and other "non-traditional" devices could be turned into targets for attackers, based on three factors. the first one is related to technological evolution; then, the use of these devices; and finally, the ways in which that use could be monetized by cybercriminals.

Next, some "non-traditional" devices which have evolved in computer terms are considered. Likewise, the state of computer security for these devices is explained:

Automobiles

Nowadays, some automobiles have more and more complex computer systems which allow manipulation of some parameters through a smartphone and software. This includes measurement and monitoring of fuel and oil levels, of mileage or kilometers covered, on-board entertainment systems, geolocation technologies (GPS), and so on. As these are complex devices, there is an increasing likelihood of the existence of vulnerabilities that may be discovered and exploited by attackers.

Consequently, recent investigations show that computer systems in some latest-generation automobiles are vulnerable to computer attacks. As a result, it has been proved, through proof of concept, that it is possible to remotely manipulate a car and start the engine, open the doors and even deactivate the braking system[23]. It is important to mention that these proof-of-concept tests have been made possible by means of a physical link through a wire, nevertheless, Internet connection capacity included in some automobiles could make such an attack easier.

Smart TV

In technological terms, televisions have evolved and some of them already include the ability to connect to the Internet to download content. Furthermore, there is already a proof-of-concept test capable of turning off the TV. Likewise, inclusion of a frontal camera, which can film what happens in the residence where the TV is kept, increases the chance that, in the future, these devices will become target of cybercriminals. a research presented at BlackHat 2013 also demonstrates it: "Smart TVs have almost the same vectors of attacks as smartphones"[24].

In fact, we have seen this year how one *Smart TV manufacturer* had issues with data collection from its users. It is possible that in the future, more threats designed for this equipment will be observed; however, it is also possible that the emphasis will be on invading the privacy of the victim rather than in the procurement of direct profit.

Smart Homes

The field that makes possible the design and implementation of smart homes is called home automation. In other words, it is a group of systems which provide a house or a closed area with efficient energy management, comfort, and security, and so on. It could also be understood as technology integration within a house, building or another kind of engineering construction. Taking into account the previous definition, there are several conventional devices which have evolved and nowadays are part of a smart home, for example toilets, refrigerators, lighting systems, and IP (Internet Protocol) cameras, among others.

In the following paragraphs, we mention some of these devices and how a cybercriminal could make an attack against these technological devices:

Smart Toilets

Smart toilets are also vulnerable to security attacks. Some of them include cleaning, deodorization systems and even monitoring of pressure and glucose levels in blood, which are important for some health conditions, such as diabetes. Despite these characteristics, Trustwave investigators were able to alter the normal behavior of a smart toilet by making it spray water on the person using it and make the seat open and close[25]. Although this may seem an action which does not bring important consequences, these kinds of toilet are usually components of other smart systems: thus, if this element of the house is compromised, it may mean that other components are exposed to computer threats as well.

Smart Lighting Systems

Due to technological advances, lighting systems have also evolved to the extent that they can be controlled using an application installed in a smartphone connected to Internet. There is already in the market a product with such functionality and which also allows the user to change the intensity and color of lights according to preference. Despite the comfort and enjoyment granted by such a system, a researcher showed that through an exploit he can steal victims' credentials to manipulate their smart lighting system without their consent[26]. Such a situation can not only be troublesome but a danger to the physical security of the place where the system is installed.

Refrigerators

Some refrigerators have Internet connection. This gives the user the chance to check the state and quantity of foods and find recipes on line, among other actions. Likewise, *companies such as LG have launched onto the market refrigerators which use Android* to offer user intelligent "characteristics" of added value. Such features give a third party the chance to develop malicious codes to compromise the accurate functioning of this kind of technology. an attacker could, for example, open the door of the refrigerator in the night, change the readings for the state and quantity of food and so on.

IP Cameras

Other "unconventional" devices which may become targeted by cybercriminals are IP cameras. This kind of technology allows the system owner to monitor a site in real time through the Internet and see what is going on there. Researchers from Core Security discovered several vulnerabilities in a range of IP cameras allowing an attacker to obtain recordings without the consent of the victim, and to execute arbitrary commands in the web interface of these devices[27]. Vulnerabilities in this technology may have a serious impact if it is considered that a third person could access private recordings which show access points at a location, times when people are not at home, and so on.

Digital Lock

It is also possible to find digital locks in the market. These may include a register of people who go into the property, and make access easier due to the use of electronic cards, among other authorization mechanisms. the increased complexity of these devices makes possible attacks such as access card cloning, lock opening, etc. On this basis, research presented at Black Hat 2013 showed the feasibility

of an attack where a third party may capture transmitted packets through Bluetooth when some wireless lock systems are used[28].

Google Glass and Other Intelligent Accessories

One of the devices that certainly changed the market during 2013 was Google Glass. These are glasses which offer the experience of expanded reality and the possibility to connect to Internet through voice commands. Regarding the security of these devices, a researcher discovered a vulnerability which makes possible the theft of information through a Wi-Fi connection especially manipulated for that purpose[29]. If the user employs Google Glass and sends unencrypted information, this could be obtained by an eavesdropping third party.

Likewise, another security gap (subsequently closed) allowed a specifically manipulated malicious QR code to connect user device automatically to a malicious Wi-Fi[30].

In the event that this device starts to enjoy massive user-adoption and is used to access banks, pay services, and so on, it is highly probable that it will be targeted by malicious code designed to steal information. This aspect is even more worrying considering that, at the moment, Google Glass uses Android 4.0.4 as operating system and not a more recent version of that platform.

Android in Other Devices (NVIDIA Shield Portable Games Console, Clocks, Home Appliances, Among Others)

As was previously mentioned, many non-traditional devices use Android as their operating system. This means that companies don't need to develop proprietary software, thus reducing the development and production costs of such devices. Likewise, when using a known operating system, more applications are available than is the case with a platform whose development is focused on a particular company. What is positive in terms of lower costs, accessibility and standardization may also have a *negative* impact when it comes to user security. This is because the use of the same operating systems in a wide range of different devices makes it possible that the attacker develops malicious codes with the capacity to work across the whole range of those devices.

Nowadays, the market offers clocks, refrigerators, automobiles, photographic devices, fixed line telephones, games consoles and even mirrors which allow the user to check content on line. All these devices share one characteristic: they use Android as their operating system[31].

Conclusion: Is Internet Privacy Possible?

Throughout this document, we have proven how user concern about security on the Internet has increased. Similarly, we have discussed the evolution of computer threats regarding the quantity, complexity and diversification of attacks. To this extent, it is probable that the reader experiences a sensation of distrust regarding computer technologies, and indeed, we always advise that people shouldn't

get too complacent about their online security. However, our main objective is not to stop people using the Internet under any circumstances, but to help them use the Internet and other tools in a more secure way. So is privacy possible on the Internet?

To an extent, it is, since there are measures people can take leading to enhanced security and privacy of information; however, no computer system is immune to attack. Something similar happens with automobiles: it is possible to have the latest safety technology and take care regarding cautious and safe driving, but the possibility of a car accident still exists.

In the same way, security is also a challenge when employing protection technologies and awareness-raising strategies to increase privacy levels and the security of the Internet. For this reason, we should adopt a strict protection methodology that asks the user for confirmation when confronted with any action which could risk information integrity, as can happen with the execution of programs, surfing the Internet, and so on. a system of this nature could be highly effective if the user reads every message in detail and answers in the appropriate way (yes or no, depending on the action). However, due to the lack of usability and practicality of a system like this, it would probably be deactivated by most users.

Something similar happened with the UAC (User Account Control) implemented by Microsoft in Windows Vista. That security system was designed so that all programs executed by the user did so with restricted privilege levels. Faced with applications which need administrator privilege, people are obliged to explicitly allow or deny the execution of software. It cannot be disputed that a system like this gives a greater level of security. However, it was such a bothersome experience for users that Microsoft found itself obliged to modify UAC in Windows 7 to make it less "intrusive"[32]. If the previous example is taken as a precedent, it will be necessary to create measures which can effectively protect users but, at the same time, are not perceived as obstructive or invasive.

Taking these points into account, the first effective measure to maintain privacy of information is data encryption. In this case, and as was discussed in depth in the "Privacy" section, there are programs which encrypt user files. Significant protection may be achieved by the installation of such programs: however, the security value of this defensive mechanism varies according to the robustness of the encryption algorithm.

Another measure to improve privacy on the Internet is the use of Tor, an application designed to enable anonymous surfing. As it says on the program's own site: "Tor is free software and an open network that helps you defend against traffic analysis, a form of network surveillance that threatens personal freedom and privacy, confidential business activities and relationships, and state security."[33]. Simply expressed, Tor´s functionality consists of an updated version of Mozilla Firefox browser with certain parameters and extensions intended to give a higher level of anonymity while surfing the Internet. Other functions included in the program allow the user the ability to surf through the Deep Web[34] (Deep Internet or Deepnet).

Simply expressed, the *Deep Web* is all Internet content which is not part of the Surface Web: that is, sites and content not indexed by mainstream search engines such as Google. Part of the Deep Web is composed of pseudo domains like.onion which are used with the aim of making anonymous access to web pages easier. These pages include different topics such as abusive content, sales of narcotics, cybercriminals' forums and other generally illegal topics or those beyond conventional ethics and even legality. Even though Tor gives a higher level of anonymity and privacy than a "standard" browser, it is not an infallible system either. Some documents revealed by Edward Snowden affirm that NSA have tried to exploit vulnerabilities found in the Tor client (as opposed to in the net), allowing in that way disclosure of the identity of certain users of this tool[35]. In addition, Tor developers have warned the community that some old versions of the software are vulnerable due to a security flaw found in versions of Mozilla Firefox prior to 17.0.7[36].

In this case, the solution to the aforementioned vulnerabilities is the Tor update. However, it is possible that other security flaws will be found in the future; thus, the use of this tool, as with any other security measure, must be considered as a way to increase security but not as a complete solution to invasion of privacy. Taking into account all the information in this document, Internet privacy is possible but only with some reservations: that is, to assume that it can be made 100% secure would be a mistake which would actually *undermine* user security.

References

1. ESET Latin America. *Trends for 2011: Botnets and Dynamic Malware*
2. ESET Latin America. *Trends for 2012: Malware Goes Mobile*
3. ESET Latin America. *Trends for 2013: Astounding Growth of Malware for Mobiles*
4. Gartner Says That Consumers Will Store More Than a Third of Their Digital Content in the Cloud by 2016. Available at http://www.gartner.com/newsroom/id/2060215.
5. Cisco: Global Cloud Index (GCI). Available at http://www.cisco.com/en/US/netsol/ns1175/networking_solutions_solution_category.html#~Overview.
6. Electronic Privacy Information Center – Gmail Privacy FAQ. Available at http://epic.org/privacy/gmail/faq.html#1.
7. Wikipedia – 2013 mass surveillance disclosures. Available at http://en.wikipedia.org/wiki/2013_mass_surveillance_disclosures.
8. Detail of DuckDuckGo traffic. Available at https://duckduckgo.com/traffic.html.
9. New Research: Global Attitudes to Privacy Online. Available at http://www.bigbrotherwatch.org.uk/home/2013/06/new-research-global-attitudes-to-privacy-online.html.
10. Big Brother Watch – Online Privacy Survey. Available at http://www.slideshare.net/fullscreen/bbw1984/global-privacy-research/3.
11. Diario El País, European Union and USA agree to research Google. Available at http://tecnologia.elpais.com/tecnologia/2012/10/16/actualidad/1350370910_859384.html.
12. Further information available at *Wikipedia – Edward Snowden*.
13. ESET Latin America's Security Report 2013. Available at http://www.eset-la.com/pdf/prensa/informe/eset-report-security-latinoamerica-2013.pdf.
14. Gartner Says Worldwide Public Cloud Services Market to Total $131 Billion. Available at http://www.gartner.com/newsroom/id/2352816.
15. El Financiero México - Google and Facebook, in the object of attention of Dilma Rousseff. Available at http://www.elfinanciero.com.mx/secciones/internacional/32329.html.
16. Pinterest Español.Net – New privacy policy and more personal PINs. Available at http://pinterestespanol.net/nueva-politica-de-pivacidad-y-pins-mas-personales/.
17. Trends for 2013: Astounding growth of malware for mobiles. Available at http://www.eset-la.com/centro-amenazas/articulo/Tendencias-2013-Vertiginoso-crecimiento-malware--moviles/2863.
18. http://www.gartner.com/newsroom/id/1764714 y http://www.gartner.com/newsroom/id/2573415.
19. Vulnerability information CVE-2013-4787. Available at http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2013-4787.
20. EMOL: They introduce pilot scheme of cell phone payment using NFC technology in Chile. Available at http://www.emol.com/noticias/tecnologia/2013/08/08/613576/presentan-programa-piloto-de-pago-con-celulares-usando-tecnologia-nfc-en-chile.html.
21. Microsoft: 64-Bit Momentum Surges with Windows 7. Available at http://blogs.windows.com/windows/b/bloggingwindows/archive/2010/07/08/64-bit-momentum-surges-with-windows-7.aspx.
22. Digital Trends: Most Corporate PCs to Run 64-bit Windows by 2014, Says Gartner. Available at http://www.digitaltrends.com/computing/most-corporate-pcs-to-run-64-bit-windows-by-2014-says-gartner/.
23. DEFCON: Hacking cars and unmanned vehicles. Available at http://blogs.eset-la.com/laboratorio/2013/08/03/defcon-hackeando-autos-y-vehiculos-no-tripulados/.
24. BlackHat: Is it time for SmartTV? Available at http://blogs.eset-la.com/laboratorio/2013/08/02/blackhat-es-la-hora-de-los-smarttv/.
25. Here's What It Looks Like When A 'Smart Toilet' Gets Hacked [Video]. Available at http://www.forbes.com/sites/kashmirhill/2013/08/15/heres-what-it-looks-like-when-a-smart-toilet-gets-hacked-video/.
26. Vulnerability discovered in Philips Hue,system. Is it sure Internet of things? Available at http://alt1040.com/2013/08/vulnerabilidad-philips-hue.
27. CORE-2013-0303 - D-Link IP Cameras Multiple Vulnerabilities. Available at http://seclists.org/fulldisclosure/2013/Apr/253.
28. BLUETOOTH SMART: THE GOOD, THE BAD, THE UGLY, AND THE FIX! Available at http://www.blackhat.com/us-13/archives.html#Ryan.
29. Google Glass still vulnerable to Wi-Fi attack. Available at http://www.computerworld.com/s/article/9240909/Google_Glass_still_vulnerable_to_Wi_Fi_attack
30. Google Glass susceptible to poison-pill QR code. Available at http://www.networkworld.com/news/2013/071813-google-glass-271960.html.
31. Android Everywhere: 10 Types of Devices That Android Is Making Better. Available at http://www.androidauthority.com/android-everywhere-10-types-of-devices-that-android-is-making-better-57012/.
32. Aol Tech: User Account Control to be less annoying in Windows 7. Available at http://downloadsquad.switched.com/2008/10/09/user-account-control-to-be-less-annoying-in-windows-7/.
33. Tor. Available at https://www.torproject.org/.
34. Wikipedia: Deep Web. Available at http://es.wikipedia.org/wiki/Internet_profunda.
35. The Guardian: NSA and GCHQ target Tor network that protects anonymity of web users. Available at http://www.theguardian.com/world/2013/oct/04/nsa-gchq-attack-tor-network-encryption.
36. Tor security advisory: Old Tor Browser Bundles vulnerable. Available at https://blog.torproject.org/blog/tor-security-advisory-old-tor-browser-bundles-vulnerable.