COMPUTER PROGRAMS THAT DAMAGE MOBILE PHONES

Tarsila Jorge Raibida, Diolete Marcante Lati Cerutti, Lauro Cesar Araujo Manfredini
Universidade Estadual de Ponta Grossa (UEPG)
tj.raibida@gmail.com, diolete@uepg.br, lcamanfredini@uepg.br

Abstract: This article glimpsed need as much as threats of computer programs can disrupt cell phones and how you can prevent and even cure to the problem and show in general how these harmful computer programs, and its goals. In this work, research is described in several studies done around the world on issues of malicious programs for mobile telephone and studies of best operational program or right for a person who does not want to have problems like malicious programs for mobile phones.

Abstract: Mobile Phones; Computer Programs; Malicious Programs; Mobile Phone Viruses.

1. INTRODUCTION

The man already was experimenting with wireless communication long before the invention of satellites, cell phones and radios, using relay systems with different types of signals to increase the reach of messages - essential to overcome great obstacles [3].

Africa, New Guinea and pre-Columbian America, "talking drums" as Africans Waganda the illustration above, were used to send messages to 160 kilometers per hour, covering great distances. Signs of fire and smoke were also well employed in pre-modern societies, and are still used in traditional ceremonies such as the choice of a new pope in the Vatican.

Forerunner of the electric telegraph, the signaling traffic lights represented the first telecommunications system of the industrial age. Holders of traffic lights, a sort of flag, sent relied on visual signs of towers and a variety of signaling devices such as swivel shutters and flags, as the military network depicted in this illustration of the American Civil War.

The towers were lined up along a track, all in preparation for the next season, which generally were 10 kilometers away (or more, if there were a waterway on the way). Although the construction and costly maintenance, the system was faster and more efficient than other methods of communication at the time. Over time, the semáforas towers fell out of favor with the popularization of the electric telegraph.

Alexander Graham Bell grew fascinated by the sound. Her mother was deaf, taking it early to refletirsobre sound characteristics. As taught to deaf children in Boston, he became obsessed with the idea of transmitting the voice electrically, which led him to invent the telephone in 1876. When Bell accidentally spilled acid during one of the first telephone tests, I would have said, "Lord Watson Come here. I need you".

The message to Thomas Watson, his assistant, is considered the first phone call the world. Graham Bell presented his creation in the Centennial Exposition in Philadelphia in 1876, which made him famous in the international scientific community.

Guglielmo Marconi, considered the father of long distance radio transmission, shared the Nobel Prize in Physics 1909 with Karl Ferdinand Braun for his contributions to the development of wireless telegraphy. However, initially his ideas were not so well received.

At 20, Marconi began working in electrical communication experiments with the help of his butler. With the support of parents, he began to conduct tests with transmitters and receivers, sending signals kilometers away. In search of more resources, Marconi wrote to the Italian government, but an employee dismissed the idea, saying it was better to present it in an insane asylum.

He then traveled to London, where the idea was well received. From there, he sent the first wireless signal in the main telegraph office in town. On May 13, 1897, Marconi made the first wireless transmission in open sea when its signal crossed the Bristol Channel, between Wales and Devon. The message: "Are you ready?"

During World War II, an idea which prevented the detection of torpedo control signals of Marine came from the most unlikely person: Hedy Lamarr, a goddess of the Hollywood pantheon. Although it was famous for the beauty, the Austrian-American actress was also seen as a mechanical genius with an incredible skill in applied mathematics. With the help of journalist and composer George Antheil, Lamarr created a solution that involved the constant replacement of frequencies while sending a message, preventing it to be intercepted by the enemy radio.

At the time, his idea was rejected by the US Navy, but twenty years later, the technique of frequency hopping was used in the North American warships during the crisis of the Cuban Missile - in secret, of course, and without due credit to Lamarr.

The brilliant idea of Hedy Lammar is the basis of current technology, which guarantees reliable and private conversations between mobile phones. Moreover, his invention today integrates modern military communication systems, GPS, wireless modems and satellite communications.

Marty Cooper, director of research and development at Motorola made the first call from a portable cell phone on the streets of New York in 1973. Three months before, AT & T rival began to monopolize the nascent market of wireless communications. To cope with the competition, Cooper suspended all other Motorola designs and challenged his team to create a functional handset within 90 days.

Cooper - this photo of 2003 with an original cell 1973 DynaTAC - used his new invention to call Joel Engel, head of development at AT & T. After a brief greeting, Cooper said, "I'm calling you from a cell phone, but a real mobile, portable." The only response from the other end was silence.

On December 3, 1992, Neil Papworth, an engineer at Vodafone, sent the first text message to his colleague Richard Jarvis: "MERRY CHRISTMAS". Papworth sent the message to a computer keyboard, as the mobile phones had not yet alphabetic keyboards. It would take years until the business phones incorporate this functionality. In 2011, it is estimated that more than 2.3 trillion text messages were sent worldwide.

The Nokia Communicator 9110 (pictured) was released in 1998 and became one of the first devices to transmit text messages and data. The invention of the first camera for mobile was inspired by love. When his wife came m labor on June 11, 1997, Philippe Kahn, a successful entrepreneur from California, decided to call a cell phone to a digital camera, with the help of components purchased at an electronics store.

Minutes after the birth of her daughter, Sophie, Kahn took the picture we see here. The camera was connected to your computer, allowing you to quickly postasse the Internet. Then he used the phone to send it to the two thousand of its agenda, with the following message: "" Philippe Kahn sent a picture for you." That memorable day of 1997 was marked by two births: the Kahn's daughter and the cell phone camera.

Five years after Philippe Kahn and his cell phone camera improvised, the first commercial models finally hit the market. The Sanyo CSP-5300 was launched in the fall of 2002 and ran exclusively on the Sprint network. It was the first phone to integrate a digital camera capable of recording images at a resolution of 640x480 pixels. At the time, it was sold at $ 400.

The model Sanyo CSP-5300 photo was distributed as special gift, along with a Fendi handbag, for Oscar nominees 2002. When a tsunami struck Southeast Asia in 2004 were not reporters who reported the news to the world, but citizen journalists armed with camera phones. This dramatic image of a wall of water forming was recorded by Eric Skitzi, a British tourist who was on vacation at a resort in the seaside town of Panang, Malaysia.

Tourists sent reports and first-hand images, which were widely reported on blogs and social networks like Facebook. The camera phones and citizen journalism laid the foundations for the explosive growth of user-generated content.

Smartphones existed before Steve Jobs introduce the world to the iPhone in 2007, but most of these devices was aimed at businesses, not to consumers. The iPhone would come to shape the future smartphones with its innovative technology and design, including touch-screen keypad, motion sensor and a graphical browser.

A short time later, Google would launch its own mobile phone operating system, Android, offering an alternative open source to Apple's closed system. Together, the operating systems IOS and Android move more than 640 million mobile devices worldwide.

The Arab Spring gained momentum, in part, by disclosure in social media, with images recorded by ordinary citizens phones. In the photo, a woman covered by a veil takes pictures with his cell phone during clashes with Egyptian police near Tahrir Square in Cairo in November 2011.

Mobile devices and social media have become powerful tools, helping protesters to organize and communicate. The revolution started in Tunisia and spread to Egypt, Yemen, Libya, Bahrain, Syria and other countries to help - in some of them - to create new governments where old autocracies ruled long ago. Indeed, some political and social observers concluded that the new tools at least made it difficult to cover up the oppression and crimes committed by the state.

Was the prototype of this model, on April 3, 1973, Martin Copper, then engineer at Motorola, made the first public call with a cell phone. The historical connection was made the corner of 56th and Lexington Avenue in Manhattan, New York. The DynaTAC 8000X went on sale just ten years later, in 1983. The media device 33 centimeters and weighed more than half a kilo. The battery needed to be recharged after eight hours of standby time or an hour of conversation. The price, US $ 3,995 at the time, about $ 10,000 in today's values [2, 3].

The MicroTAC® 9800X, as the name says, was a "micro" version of DynaTAC. At the time, it was released as a "pocket phone." The design was innovative, with the front flip, very common in machines of the 1990s and 2000s. Simon is the first device to bring together features of a palmtop with a cell phone, making it the precursor of smartphones. He was so ahead of its time it had operating system and even touchscreen. Developed by IBM in partnership with Mitsubishi, it sold about 50,000 units and was discontinued a few months after launch. The third generation of Motorola phones revolutionized the market. The previous models, the StarTAC only saves the last three letters in the name. For the first time, the design has become as important as the functionality (remember the phone with her purse). Lightweight and stylish, the device was elected as the 6th best gadget of the story by a magazine specializing in technology. The first BlackBerry device, launched in 1999, was a kind of pager, which sent e-mails and messages. In 2002, the gadget turned mobile. But not an ordinary mobile: the BlackBerry 5810 had a QWERTY keyboard. The news hit the tastes of consumers and, before long, other manufacturers followed suit. Simple, with flashlight and cheap, very cheap. That's how the Nokia 1100 was a hit and became the best-selling phone in history. Were 250 million handsets sold, mostly in emerging markets in Africa and Asia.

Before the revolution the iPhone, Nokia has launched the N70 sophisticated, accepting applications and came with two cameras, with a 2MP (two mega pixels). It was one of the devices that crystallized the habit of recording everything with his cell phone. By also bring an audio player and an FM radio tuner, the N70 was important to sell the idea that the cell could one day replace the iPod. In technology, it can be said that there is a world before the iPhone and another after the iPhone. By 2007, Apple was a company revered by macmaníacos and iPod fans, period. The following year, the iPhone 3G was the best selling phone in the world, since it was occupied by some Nokia device since 1998. Today, the company founded by Steve Jobs is the most valuable in the world, leaving behind giants of old, such as Microsoft and Google. Since launching in 2007, the iPhone reigned supreme in the smartphone market. The lull lasted five years until Samsung has a weight of competitor: the Galaxy SIII. Despite not having the charm of the Apple brand carries the instrument is considered by many the best available in the market, at least until its successor, the Galaxy S IV, hit the shelves.

2. MATERIALS AND METHODS

The virus, which already took the sleep of personal computer users for some time, are coming in increasing numbers to cell phones.

A recent survey of a security specialist company "online", Kaspersky showed the reality of the current virus scenario. Infection of personal computers is in the background, with mobile devices being the main targets. Viruses are not the same, but the problems they can cause are also great [1, 2].

Recently, for example, a virus was identified "practically impossible to be eliminated to a certain operating system mobile phones." And this particular operating program is precisely the main target of "cybercriminals" who develop malicious files. According to a report on the evolution of viruses on mobile devices made by the same company, 99% of today's threats are aimed at this operating system in question, which also is a record in sales, at least in Brazil.

After all, which of the existing operating systems for mobile phones, the less sold to sellers, it is the safest? In 2004, the first virus for mobile phones has been discovered by security company F-Secure and was named Cabir.A [F-Secure 2004]. Actually, Cabir.A is a worm that spreads only by mobile phones using Bluetooth wireless transmission technology, affecting devices based on the Symbian operating system - better known as platform Series 60. Unlike a virus, worm had only function self-propagating, not identified any information about processes that originassem potential ways destruction or damage.

After the incident in 2004, it realized the fragility that mobile devices could suffer a not too distant future. Phones, for having limitations in processing power and memory, do not have a comparable safety of a computer virus. This opportunity studies generated by large security companies in this market segment, called mobility.

Mobile viruses can spread primarily in three ways:

• Internet: It consists of the data transmission to the mobile via the browser that uses a network with access to other computers.

• SMS and MMS messages: consists of sending short text messages or multimedia (MMS).

• Bluetooth Wireless Transmissions: Similar to the way the Internet, but more limited only to other phones that have Bluetooth and are within reach near the device. Usually up to ten meters barrier-free.

• Regarding the most common damage they can cause are:

• Damage to the battery: Technically running any device function that download more quickly. Examples: Play the music or video player zero volume, play a game or application without the user's permission, activate Bluetooth. Delete contacts or calendar files: The virus deletes all contacts found in the device calendar or specific file extension. Sending SMS or MMS: Similarly it can be contaminated by messages type MMS or SMS when infected could end up sending messages to other contacts phonebook. Thus depleting the credits with the operator or generating costs to the user.

Viruses can infect by downloading files from the Internet to mobile later causing some types of damage to the unit commented. Of course, the SMS structure was designed as a fast and efficient delivery service for messages, but virus writers have proved they can exploit flaws in this type of system and generate chaos if steps are not taken.

According to research results of the PNAD (National Survey of Household Sampling) released by the IBGE [UOL News in 2008], each year a growing number of Brazilian fans to mobile phones. Many of the new phones already in the new 3G wireless Internet technology with great speed and coverage, making it possible to believe that a great potential for mobile phones to infections will be observed in the coming years in the country.

There are proprietary solutions in the market of security companies in the industry, highlighting the McAfee solutions, F-Secure and Kaspersky Labs. Some of these solutions enable the control of data flow almost total input and cellular data output. However, so there is no alternative open solutions like antivirus for desktop computers.

Considering the huge amount of applications and the popularity of all operating systems for mobile phones, including the least vendindos the most sold, the less vendindos seem to be the main security option, especially in terms of corporate organization to have been produced with a view for purposes that are more professional and not for entertainment. Protections against access to the users of these operational programs information are top-notch and this makes the safest cell phone. However, the user has to have protection precautions to ensure safe system even if the system is already being held by its factory design.

The big question on the safety of mobile phones is precisely the same as the personal computers: every computer can be safe or vulnerable, depending on user behavior. In the cell, this also happens. Most important of all, regardless of system is always protected and avoid acting risky way.

Thus, manufacturers of the best selling systems want the right combination of security against viruses and their systems more popularly desired, something that is being worked tirelessly for developers to avoid losing sales to competitors with more secure operating systems, but more secure systems and less desired that have been produced for more professional audience that already runs the option of the general public who actually makes a profit for the manufacturers of the best selling systems. Today thousands of pests circulating on the internet and spread due to common causes such as security holes in operating systems, ignorance and curiosity of users run unknown programs, file sharing, reliability [3].

Recently, for example, a virus was identified "practically impossible to be eliminated to a certain operating system mobile phones." And this particular operating program is precisely the main target of "ciber criminals" who develop malicious files. According to a report on the evolution of viruses on mobile devices made by the same company, 99% of today's threats are aimed at this operating system in question, which also is a record in sales, at least in Brazil. After all, which of the existing operating systems for mobile phones, the less sold to sellers, it is the safest? [1, 2].

Theoretical survey about computer viruses, defining: ratings, how they act, activation criteria and propagation, serving the same way as the foundation and introduction to the new trend with targets in the cell. This also threatens the emerging market in terms of security for mobile devices. Will be discussed important issues related to the two arms (computers and mobile phones).

Obviously, all operating systems, manufacturers that have devices sold more popularly, has serious flaws that can be exploited by students of the computer science area, as operating systems less protected the most protected plant [1, 2].

Computer scientists are able to create applications such as antivirus for mobile phones. With it becomes important to an investigation of the most secure operating system, appointed by professional research, upon purchase. Know which device is the safest, if your system has protection against malicious files. The specific objective of this study and guide the user to the best operating systems for mobile phones, as well as the prevention of virus.

3. RESULTS AND DISCUSSION

Over the past quarters, we realize that a certain operating system for mobile phones is the most popular target of "mobile virus", it is the best selling and the weakest of policy restrictions on the transfer of certain applications that can be downloaded to the mobile phone. This quarter was no different. Virtually all new viruses developed for mobile phones are targeted is the "platform" in question, which is the most sold and one of the most successfully attacked by the virus. This "package" of viruses includes malicious text messages, as well as threats to the security of important data from the mobile phone such as passwords, files like photos, videos and personal phone contacts. The issue is the fact that the best-selling operating system for mobile phones, contributes to the fact that the system is considered one of the most "dangerous"?

From the point of view that the best selling is the most "ill-organized security policies", (more open to have weak policy regarding the purchase applications), the answer is yes. However, a study of an IT research firm, the Sourcefire, another operating system, third-party, which is the second most sold, not getting almost nothing behind the first, has accumulated a large number of vulnerabilities than all its competitors together in recent years. But the use of security application for viruses of this operating system and the rules of the manufacturer, this system for applications (computer programs) in your virtual store end up causing it to be more protected and not have so many cases of the virus [1, 2].

Considering the huge amount of applications and the popularity of all operating systems for mobile phones, including the least sold the most sold less sold seem to be the main security option, especially in terms of corporate organization to have been produced with a view for more professional purposes and not for entertainment. Protections against access to the users of these operational programs information are top-notch and this makes the safest cell phone. However, the user has to have protection precautions to ensure safe system even if the system is already being held by its factory design.

The big question on the safety of mobile phones is precisely the same as the personal computers: every computer can be safe or vulnerable, depending on user behavior. In the cell, this also happens. Most important of all, regardless of system is always protected and avoid acting risky way.

Thus, manufacturers of the best selling systems want the right combination of security against viruses and their systems more popularly desired, something that is being worked tirelessly for developers to avoid losing sales to competitors with more secure operating systems, but more secure systems and less desired that have been produced for more professional audience that already runs the option of the general public who actually makes a profit for the manufacturers of the best selling systems.

A smartphone is a mobile tele with advanced features that can be extended through programs run by your operating system. The operating systems of smartphones allow developers to create thousands of additional programs with several utilities, aggregated on sites such as Google Play. Generally, a smartphone has minimum requirements of hardware and software, the main data networks with connection capacity for internet access, synchronization capacity of organizer data with a PC and an address book that you can use all available memory cell is not limited to a fixed number of contacts. A smartphone can be considered a mobile phone with the functionality of a PDA. In the second quarter of 2013, smartphones surpassed sales for the first time in history the traditional mobile phones, also known as dumbphones. Smartphones accounted for 51.8% of sales of mobile phones, with 225 million units, according to Gartner. The first concept of combining telephony with computing came in 1973, but the first product to combine the two features was the IBM Simon and only came to be released in 1993, the smartphone term was first used in 1997 pelaEricsson. In 1996 Nokia launched the Nokia 9000. The popularization came in the late 1990s with the PDAs, which mainly used the Palm OS systems, BlackBerry OS and Windows CE / PC Porkcet for several years, BlackBerry has dominated the smartphone market to the launch of Apple's iPhone in 2007, which was the first multitouch and without physical keyboard smartphone. In 2008, Google launched Android, free operating system that is currently the most used in smartphones.

The Palm OS is a pioneer in the segment and brings advantages and disadvantages for it. Initially it was known for its ease of use and its speed. Then, with market developments, their versions, especially prior to 5.0, began to hinder the implementation of more complex applications. The market corporative these disadvantages weighed heavily and so their success with the general public does not compare with the business. Today the Palm OS is no longer an option. Very few cell should still run on the system, especially with the giant competitors that we will see soon.

Symbian is the operating system that, worldwide, prevails among Nokia mobile phones to date. However, research shows that leadership can no longer belongs to him in 2011. Symbian is owned by Nokia and had its open source so that anyone can develop his or her own applications. Among the advantageous features of the system are its ability to be multi-task and handle real-time applications, its high stability, memory protection capability, efficiency and good integration that it establishes between phone and computer. In addition, it performs well on modest equipment, a niche that accounts for the vast majority of handsets sold.

Windows Mobile, Microsoft, has a clear objective: to translate all features of the desktop version for mobile phones. Due to some problems in Windows CE version, the OS has been redesigned to be lighter and have support for different types of hardware. Today, in version 7, Windows Mobile can not be classified as multi-task, but it simulates this feature alternating use of computer solutions with applications running. This latest version has an interesting twist: a feature that allows it to communicate with other Microsoft devices such as the Zune and Xbox 360. In short, this system is a simplified version of software for desktops, which usually facilitates much to the user's life, that already have much familiarity with the platform. The iOS is the operating system developed by Apple from Mac OS X. The version is simpler, supercustomizada, has quick and easy access to the devices and was popularized when equipped the iPhone. Divided into three areas: the machine level software - used to meet the working needs of all users; the system level software - used to meet the critical system functions; user level software - illegal for meeting the needs of a particular user. The multitasking features were acquired only in version 4 before Apple did not believed to be necessary to provide the feature. The user interface is the big reason why this operating system became so well known. The intuitive interface enables a user with little knowledge make use of the operating system.

Android is an operating system that runs on the Linux core. It was developed at first by Google, which remains responsible for product management and engineering processes, and later by the Open Handset Alliance. Android supports a wide variety of connectivity technologies, including Bluetooth, EDGE, 3G, and Wi-Fi, the browser available in the system is based on the open source framework. The platform advantage is that it can be adapted both larger devices and VGA as the traditional smart phone. The BlackBerry OS is a mobile operating system owner, developed by Research In Motion (RIM) for their BlackBerry smartphone line. The platform is well known by support for corporate e-mail, through MIDP 1.0 and, more recently, a subset of MIDP 2.0, which allows activation without complete and sync cord with Microsoft Exchange, Lotus Domino or Novell GroupWise -mail, calendar, tasks, notes and contacts, when used in conjunction with BlackBerry Enterprise Server. The operating system also supports WAP 1.2 [1].

Those who use computers already know viruses and other malware. However, the threats, previously restricted to desktops and laptops, now have a new target: your smartphone. In increasing numbers, these applications hamper the performance of gadgets and try to steal users' personal data. However, does the mobile phone viruses act like the computer?

In computers, the programs are running on different security levels within activities of layers. The most important run in safer and less accessible operating system environments, since the less essential are in a more exposed site and subject to change.

It is precisely the most vulnerable that much of the malware begin to run and can send copies and extend their actions to other applications, also located on this level of security. Already the most aggressive programs can circumvent system security levels and take root in important layers may compromise your computer's performance and jeopardize its functioning.

Meanwhile, the process of infection is quite different in the smartphone. Android and iOS systems have architecture with only two layers: a narrower, with the main executions and the native apps of the system, and another where the information, files, and user-downloaded programs.

When malware infects a smartphone, your actions will be restricted to the exposed level, limited to users of the data and rarely having access to vital system functions. However, unlocked handsets via jailbreak or root increase the risk of malware that even harmless compromise the essential functions of the system.

Currently, to infect your smartphone with these "digital pests" just be connected to the internet or receive malicious files for transmission via Bluetooth, SMS and MMS.

Any method that takes data from another device is a gateway to these harmful programs. The safest way to use your mobile phone is still in the "Offline Mode".

Much of the malware for cell phones are in their own official stores of applications such as Google Play. However, a recent report has shown that these threats began circulating via spam. Some of these programs, once downloaded, steal your data and alter system settings, with the ability to send copies of itself or other malware for different data transmission media.

One of the first symptoms of malware, both on smartphones as computers, is compromising the system performance. Due to the operations of these harmful applications, the data processing system is replaced by a greater expenditure of memory, which ultimately leave the system slower, prone to errors and freezes.

Another indication of "contagion" is the significant increase in the network data transmission, besides sending SMS, MMS, e-mails and other messages over the Internet without the knowledge of users.

These two features are malware behavior patterns. They were designed to steal and transmit data, whether images, contacts, browsing the web and reports to banking information, such software end up compromising the operation of your smartphone.

Most harmful malware, however, can disrupt your phone's performance, interrupt or prevent connections, and can also infect other devices. These malicious apps are also able to transmit messages, run applications, destroy the operating system, increasing the drain on the battery of your device and even damage the hardware. The first thing to do to keep mobile phones safe from rogue applications is be aware of the data sent and received by your phone. Try to always ensure that the download has a secure provenance, noting comments on suspicious behavior and complaints [1, 2].

Malware can also be disguised in videos, music, apps and photos sent by e-mail, SMS, MMS and Bluetooth transmissions. Therefore, confirm the content with the person who sent you the file before opening it.

In addition to these precautions, it is good to have on your smartphone a good antivirus to ensure that your system is safe and prevent future infections. In the online application stores, there is a good amount of different free antivirus, which can be very useful in protecting your device. Stay tuned to the sites you visit, because if your phone does not have an antivirus or firewall, you will be more prone to infection by little malware that can open doors to more dangerous software. Remember to schedule periodic scans with the antivirus installed on your device.

This can prevent the occurrence of small errors and prevent facilities that may camouflage more serious infections. As smartphones are devices designed to transmit and receive intense form of information, these devices have become much more vulnerable to viruses and malware environments than computers. So stay informed about new kinds of infections and on the operation of your smartphone. If your phone is showing some suspicious behavior, install or replace your antivirus and if the problem persists, take it to the service center.

Users are already used to find malware on the computer, but in time to see how to remove cell phone viruses are complicated. And as they become more popular, the major operating systems geared to mobile technologies also become targets of several types of viruses. Know prevention is always the best medicine, but what you should do if you download a malicious file on your Android, iOS, Windows Phone or Symbian? [2].

The virus or malware can manifest itself in various forms, including technical malfunction. It is common in these cases receive unsolicited advertisements (and suspicious), automatic redirection to strange pages, appearance of strange icons, slowness on the part of the device, excess data connection usage, among other strange activities. The damage caused by the virus are varied, from the simplest , trying you to push advertising to steal files from within the machine , steal passwords and even use it as a zombie in a botnet , where the person behind the virus can remotely control your device and perform various tasks with it. One of the dominant platforms today, Android is one of the main targets of these viruses. The fact that a common system, sold on a large scale and open collaborate so that you target these technological virus.

Viruses on the Android manifest themselves in different ways, the most common being the use of unofficial applications. So many times, you will need only remove the infected application. Some viruses and malware can be removed only by scanning your device using a virus from your computer. You can do this by connecting your phone to your computer and sweeping it the same way you would with a pen drive. Handsets with Windows Phone system will show one of the safest to date. Because they do not perform any file that is not linked to the Marketplace, it has not found any virus developed by the platform. The facts to be a system with little representation in relation to number of sales also collaborate so that there are not many people concerned about creating viruses for this platform. But that does not mean you should not keep the same precautions you would with any other platform.

AVG has come to launch an antivirus application to the platform in late 2011, but was later removed. If you happen to find a virus on your device, try to reset the system. Despite the IOS be known as a very safe platform, since there are some attempts of virus production also for Apple devices. Despite not having arisen nothing serious so far, some companies have reported malware that infect the iPhone, but can only act when they are transferred to a Windows computer.

Some developers have already demonstrated to be possible to overcome the iTunes safety barreias, but none of them was very effective and each time, it becomes harder to get into a close between approved applications. An example of virus for iOS took place in July 2012. An application called "Find and Call" was going for simple app contact list, but in fact accessed the user's contacts and sent to a remote server. Once discovered, the application was removed.

Many also claim that the release of iOS, aka jailbreak, you can leave the platform more susceptible to viruses. Despite this, there are not many dangerous virus news that affected who did it and usually occurring are linked to carelessness of users with the security of their devices [1].

Still very strong in some countries, Symbian is a system that is present in most Nokia smartphones that are still active, although the company have stopped to manufacture devices with this platform to devote only to Windows Phone.

Symbian viruses also exist, but like in iOS, are usually not serious and most often can be avoided by following the instructions to prevent the malicious files. If this happens with your device, the most recommended is to do a factory reset, which works similar to that reported with Android.

According to the report of the company "Mobile Malware Evolution", 99% of today's threats are made to the Google platform. The main problems are SMS Trojans and exploits. The research shows that the company has identified more than 43 000 malicious programs for the operating system in 2012.

The most common threats on Android can be divided into three major groups: SMS Trojans that steal money by sending text messages to premium numbers; adware and exploits that are used by criminals in order to get full access to the device and data stored on it. Another attack that caught the company's attention was the botnet called Foncy. Through it, the crackers could control smartphones and tablets [4].

Denis Maslennikov analyst, responsible for research, pointed out that the market growth of mobile devices is not the only reason. According to him, the great popularity of the new systems is crucial, but the lack of care users to download files and the easy spread of malware on mobile environment.

Criminals are driving real mobile devices, because currently they contain more private information than in our PCs. In 2012 we registered thousands of new malicious programs that were created to steal information, money and spy on users. Unfortunately, the Android platform has become a dangerous environment in urgent need of protection.

The most sophisticated Android malware has done is "loose". Identified by the company specializes in computer security Kaspersky, the Trojan "Backdoor.AndroidOS.Obad.a" is virtually impossible to be eliminated threat. The virus is very dangerous both for those who are infected and for friends of this person.

The malware installs not only can the device itself as well as sending malicious files to nearby devices via Bluetooth and remotely perform commands in the console smartphone. Among the applied strokes are sending messages to the so-called premium numbers and download other malicious files [2].

Despite the way this malware, which draws more attention is the difficulty that the user may have to remove the malicious file from the device. The only chance is to delete it in the next moment to infection. If the virus can exploit the vulnerability of Android and assume administrator role, the process is very complicated.

A feature of this Trojan is that the malicious application can not be deleted after gaining administrator privilege, which it does by exploiting a yet unknown vulnerability in Android.

The company says it has informed Google of the vulnerability in question. Fortunately, the virus has not spread much. Only about 0.15% of malware infections in Android were caused by the trojan. The Android has a practical and versatile structure that enables the creation of applications of all kinds. The big problem is that this freedom makes many of the programs available are malicious files, to damage your phone or your personal data. However, this disadvantage can be offset by the large amount of virus available in Google Play. Know the best and most reliable. With a free version for mobile devices and other paid with more features and specific to certain functions, AVG is one of the most reliable antivirus in the Google Play Store and has been downloaded by almost 500,000 users. Designed to detect malicious apps once installed, the application keeps an automatic scanning function from a system that alerts dangers when surfing the web.

The program also has an antitheft system that locks your data if the device is stolen, and has features that protect your private data from being accessed by other applications without your consent. In addition, AVG controls the performance of your device, showing battery status, managing tasks, scheduling scans and providing resources to clear data from the physical memory. With more than 400,000 downloads, the Lookout is a free antivirus that has basic features ranging from the protection of your device against viruses, malware and spyware, to copy and back up all your data.

With a rigid system of checks, this program investigates installed applications, mobile contacts and even e-mail attachments. It also offers a paid version that guarantees a safer internet surfing, checking suspicious URLs and blocked access to private data by other apps. The Lookout Security & Antivirus also has an effective antitheft system that allows the user to track the last location of your phone by Google Maps, blocking data and photos uploaded to anyone tried to unlock your device.

Regarded as one of the most complete antivirus for both computer and smartphone, this app provides an extensive administration of your device by doing a scan so installed, indicating the power level of your battery and displaying a control icon in the notification bar. With a very complete widget to run on Android, the app also shows the intentions of access to their private data by other programs, scans all websites that are loaded, filters SMS and calls messages and also manages the internal memory of your device.

Avast also has an economic system that is triggering when the battery is at the end and an effective firewall to Wi-Fi networks, which also has an interesting antitheft system that works for SMS, and allows complete blocking of the device, triggering the alarm and, in extreme cases, cleaning the data on your device remotely. Despite only being available in English, this app is very objective and extremely easy to use, with a scan that is constantly updated and performed quickly and accurately. Ensuring greater protection of your device's internal memory, the Anti-Virus Dr.Web Light can also shield and check the content present on the SD card loaded in your mobile device. An effective quarantine system for suspicious files, Dr.Web also provides access to a table that displays the data statistics of malware detected since its installation. The Android version of this famous virus is very effective and has several features to your anti-theft system. With a scan performed by the entire contents of your smartphone or tablet, the app also blocks access to sites and dubious text messages. Offering backups and user data restore, the program also tracks and locates lost or stolen devices, data cleansing allowing remotely, including the contents of the SD card is in the device, sending messages and triggering alarms while sending the phone's location GPS.

Aimed specifically for smartphones, this antivirus is entirely in Portuguese and is quite efficient, even having a filter for blocking unwanted contacts in phone calls or SMS messages.

With a very efficient scanning system, Kaspersky Mobile Security Lite scans all applications on your device and still has access to your private data and content of your SIM card.

Counting also with an antitheft system, this app allows you to remotely lock or wipe your private data, saving your contacts in a virtual database.

4. CONCLUSION

As partial conclusions about the current state of the project can be seen some important aspects of the study of viruses for mobile phones. First, the cell phone does not necessarily use Java to send and receive messages while supporting technology. This is a proprietary standard and feature the manufacturer's discretion, just as there is no standardization as the port number defined for this purpose from one model to another. The same can be said about the non- standardization of manufacturers adopt the same operating system. Second, certain viruses for mobile phones only spread on specific conditions such as the need for some form of wireless transfer be active, need of having credits in mobile messaging, or particular kind of mobile operating system (Symbian OS, Windows Mobile, Palm OS). Still, the risk of viruses by sending automatic SMS is great danger.

REFERENCES

[1] Lira, R. L. **Dossier v1ru5 - unravel as Technical paragraph Creating a computer virus - Dossier series** (Book in Portuguese). 1. Ed . São Paulo-SP : Digerati Books, 2003. 318p.

[2] Lecheta, R. R. **Google android -Learn to create applications for mobile devices with android SDK.** (Book in Portuguese) 3. Ed Santa Terezinha -SP : . Novatec , 2013. 824p.

[3] Paladino, E. **The era of the phone.** (Book in Portuguese) 1. Ed Rio de Janeiro -RJ : . Modern Science , 2009. 176p. ”paper in portuguese”

[4] Bonaventure, E. **Research methodology - Monograph, dissertation, thesis**. (Book in Portuguese) 1. ed . Curitiba -PR : Atlas , 2004. 160P.

[5] Simões, D. D.; Pereira, J. C. **Mobile Operating Systems - Android X IOS**. (Article in Portuguese) Unipar, Paranavaí-PR. Unipar , 2014. 6P.