PROJECT, DESIGN AND MANAGEMENT

ISSN: 2683-1597

PROJECT DESIGN & MANAGEMENT

How to cite this article:

Cassinda Qussanga, F. (2019). Characterization of Cellular Mobile Operating Systems: Android, Symbian, Iphone and Windows Phone. *Project, Design and Management, 1*(2), 75-88. doi: 10.29314/pdm.v1i2.200

CHARACTERIZATION OF CELLULAR MOBILE OPERATING SYSTEMS: ANDROID, SYMBIAN, IPHONE AND WINDOWS PHONE

Fernando Cassinda Quissanga
Open University of Brazil (Brazil), European University of the Atlantic (Spain)
fernandoquissanga@hotmail.com · https://orcid.org/0000-0003-4468-7206

Abstract: The present theme refers to the characterization of cellular mobile operating systems: Android, Symbian, iPhone, Windows Phone. To present which of the cellular mobile operating systems, is the most secure and the most susceptible to computer viruses, the qualitative methodology based on the bibliographic reference, data collected in books, technical manuals, manufacturer information and on internet sites; to the analysis of the documentary data, done in tables. However, it is concluded that not all types of computer viruses infect cell phones, it depends on the kernel of the operating system. It was possible to know that Symbian is the operating system most prone to contamination of computer viruses, this operating system is made of a C ++ programming language coming from the C language one of the most popular and has many developers. Android is a mobile operating system, not so secure, based on the kernel of Linux, being free software allows more number of developers of the technology. Windows phone is the least susceptible to virtual pests. And Microsoft has invested heavily in their security system, restricted access to the app store to prevent the user from downloading programs out of the market, since every day are placed numerous applications. Bluetooth technology represents a major form of virus transmission.

Keywords: Cellular Phone, computer viruses, operational systems.

CARACTERIZAÇÃO DE SISTEMAS OPERACIONAIS MÓVEIS CELULARES: ANDROID, SYMBIAN, IPHONE E WINDOWS PHONE

Resumo: O presente tema refere-se à caracterização dos sistemas operacionais móveis celulares: Android, Symbian, iPhone, Windows Phone. Apresentar qual dos sistemas operacionais móveis celulares, é mais seguro e o mais susceptível aos vírus informáticos, a metodologia de forma qualitativa baseadapelo referencial bibliográfico, os dados coletados em livros, manuais técnicos, informações de fabricantese em sites da internet; à análise dos dados é documental, feita em tabelas. Entretanto, conclui-se que nemtodo tipo de vírus informáticos infectam os telefones celulares, depende do núcleo (kernel) do

sistemaoperacional. Foi possível saber que o Symbian é o sistema operacional mais propenso a contaminação de vírus informáticos, este sistema operacional é feito de uma linguagem de programação C++ provenienteda linguagem C uma das mais populares e possui muitos desenvolvedores. O Android é um sistema operacional para dispositivos móveis, não tão seguro, baseado no núcleo (kernel) do Linux, sendo um software livre permite maior número de desenvolvedores da tecnologia. O Windows phone é o menos susceptível a pragas virtuais. E a Microsoft investiu bastante no seu sistema de segurança, restringiu o acesso ao app store para impedir que o usuário baixe programas fora do mercado, visto que a cada dia sãocolocados inúmeros aplicativos. A tecnologia bluetooth representa maior forma de transmissão de vírusinformáticos.

Palavras-chave: Telefone Móvel Celular, vírus informáticos, sistemas Operacionais.

CARACTERIZACIÓN DE SISTEMAS OPERACIONALES MÓVILES CELULAR: ANDROID, SYMBIAN, IPHONE Y WINDOWS PHONE

Resumen: El presente tema se refiere a la caracterización de los sistemas operativos móviles móviles: Android, Symbian, iPhone, Windows Phone. En el caso de los sistemas operativos móviles, es más seguro y más susceptible a los virus informáticos, la metodología de forma cualitativa basada en el referencial bibliográfico, los datos recogidos en libros, manuales técnicos, informaciones de fabricante y en sitios de Internet; al análisis de los datos documentales, hecha en tablas. Sin embargo, se concluye que no todo tipo de virus informáticos infectan los teléfonos celulares, depende del núcleo (núcleo) del sistema operativo. Es posible saber que Symbian es el sistema operativo más propenso a la contaminación de los virus informáticos, este sistema operativo está hecho de un lenguaje de programación C ++ proveniente del lenguaje C una de las más populares y posee muchos desarrolladores. Android es un sistema operativo para dispositivos móviles, no tan seguro, basado en el núcleo (Linux) de Linux, siendo un software libre permite mayor número de desarrolladores de la tecnología. Windows Phone es el menos susceptible a las plagas virtuales. Y Microsoft ha invertido bastante en su sistema de seguridad, ha restringido el acceso al app store para impedir que el usuario descargue programas fuera del mercado, ya que cada día se plantean numerosas aplicaciones. La tecnología bluetooth representa una mayor forma de transmisión de virus.

Palabras clave: Teléfono móvil. Virus informáticos. Sistemas operacionales.

Introduction

Nowadays, there is a considerable amount of cell phones, however, these devices currently allow communication, multimedia messages, bank transfers, weather consulting services, geographic location services, global positioning system (GPS), printing of documents, other technological convergence services, calculator, address book, galleries, data exchange, and internet (portable hotspot). They can also transmit the internet signal to 10 or more Bluetooth information transfer devices. They have memories, processors and a built-in operating system, which allows a greater flow, handling and exchange of information between users. However, they spread insecurity, especially related to the loss and theft of information. It should be noted that cybercrime has increased, however, cell phones have become very vulnerable to attacks from computer viruses.

According to Giménez (2011): “The first thing to know is that a mobile security solution is completely different from a desktop or a notebook security solution. For example, according to Symantec, there are more than 286 million computer malwares, there are about 1000 for mobile devices [...]”. Considering this quote, we can see that mobile operating systems are different from each other in terms of their reliability and

vulnerability, however, viruses in an Android operating system do not attack the iOS inversely due to its kernel, i.e. it depends on the source code and its programming language.

General objective: to identify which of the mobile operating systems is the safest and most susceptible to computer viruses.

The research is qualitative and is based on the bibliographic reference, which allowed to evaluate the material of interest for the study of the subject referred to as support of the scientific article. One (1) questionnaire and eight (8) interviews were used as research techniques and instruments. However, we can analyze the definition of Chaer, Diniz and Ribeiro. (1987, p. 15). 260 apud Gil, 1999, p.128): "as the research technique composed of a more or less high number of questions presented in writing to people, with the objective of knowing opinions, beliefs, feelings, interests, expectations, situations, experiences, etc." Through the interviews it was possible to identify differences between the mobile operating systems mentioned.

Regarding the data collected, it is possible to observe a limited number of publications on computer viruses in mobile telephony. However, the research was conducted in books, technical manuals, scientific articles, manufacturer information and on websites. "Documentary analysis, as a process intrinsic to the organization of information in the field of information science, establishes theoretical-methodological descriptive parameters that explain the analytical elaboration procedures that lead to the identification of the concepts found in the document". (Nascimento, 2009)

Computer Viruses on Cell Phones

When talking about viruses in today's society we think of biological viruses (poison, toxins or infectious agents) However, in this chapter we will discuss computer viruses in cell phones, which can be defined as malicious software made by programming language. Programming that infects both the operating system and the hosts in the program and spreads to other locations on the system, corrupts and prevents the software or program from working properly.

> Crackers (computer criminals) are very skilled in the programming language, and have knowledge of computer networks, telecommunications and software engineering, sometimes without having received any education in these fields. They create viruses to take dividends, monitor all possible routes, break down passwords and detect security breaches in different areas, companies, banks and others (Quissanga, 2015, p. 10).

There are stories claiming that some viruses were not made intentionally, but to test the security system in order to learn more about the behavior of viruses. Another reason was to be able to study in labs that allowed greater student interaction. It is also claimed that some were created by amateur programmers and hackers for fun, without actually knowing the risks and thinking about the possible consequences. These viruses are not as well known, but besides damaging the operating systems, they have caused many other problems. There are also specific viruses for information theft, as cell phones are used for many purposes, be it banking operations, transfers, sending emails, messages... It is an example of technological convergence since at first it was only used for calling, but thanks to the internet it now has many other uses such as interacting in social networks, recording, etc. However, this feature of technological convergence, especially when connected to the Internet, allows the transmission of computer viruses to cell phones. That is why we must protect the operating system with antivirus, anti-

malware and anti-spyware. According to Trif and Vişoiu (2011, p.119): “New achievements in mobile technologies have paved the way for new applications designed for mobile devices. Initially, mobile devices offered few features due to low memory, computing power and difficult interaction”.

But cell phone theft is done silently, as the user has no idea that their device is vulnerable to cybercrime, and that they are being spied on. These criminals steal users' identities, hack into their emails, and compromise their bank details. Hackers have many reasons for creating viruses and carrying out any cybercrime.

Even though the real motivation for computer programmers to create viruses is to destroy operating systems, they have two other possible purposes.

The programmer creates viruses to:

- Destroy or corrupt cell phone applications;
- Steal users’ data through messages.

> The user often facilitates the spread of these viruses due to lack of caution and little knowledge of the ways in which they are transmitted, that is why any manufacturer, developer or law firm should promote conferences, debates, forums and seminars on the causes, forms of propagation, damage and prevention of computer viruses [...] (Quissanga, 2015, p. 10).

Viruses on cell phones originated in 2004, which can be considered very recent compared to the origin of computer viruses in the late 1980s. It was F-Secure Company who discovered the first virus in cell phones.

According to Martinelli, (2008, p. 94):

> The first cell phone virus was discovered in 2004 by the F-Secure Company (a security company) and was called Cabir.A. Cabir.A is actually a worm that spreads only in cell phones that use Bluetooth wireless transmission technology, which affects devices based on the Symbian operating system, better known as the Series 60 platform.

But the plague does not spread to all devices, which means that there are some restrictions for each virus depending on the operating system. Bluetooth technology is one of the wireless network transmission technologies that allows the exchange of information between devices while having a low power consumption. The Cabir.A virus originated from this technology by sending infected messages to the mobile device. It is considered to be the first form of propagation of mobile phone viruses. This technology usually allows a very simple transfer of information from one point to another. Most mobile devices to date are lacking any antivirus to prevent computer viruses from infecting the operating system and, in turn, damaging it or stealing information. Cell phones must be protected because the main transmission route of the virus on these devices has been Bluetooth and the Internet.

Describir los posibles tipos de virus informáticos en la telefonía móvil celular.

After addressing the origin of viruses, it is advisable to mention the types of viruses in cell phones.

However, computer viruses are more focused on how to spread and act on their targets and they have many developers, hence there are many types of viruses, which is not the case with cell phone viruses. Their very recent discovery has limited research and

development, as well as the introduction of viruses to the market and very recent access to the devices that somehow developed them.

Silent viruses are quite common these days. Crackers use them to spy on users and remove any vulnerabilities from the mobile device, such as images, videos, compromising or confidential information, bank codes for multiple transfers. We must be careful with the information we put on our mobile devices when we have no antivirus, antimalware or antispyware.

Cell phone viruses are not as popular as those of computers, which may also be due to the evolution of several generations of cell phones. For example, Nokia and Siemens cell phones used the Symbian operating system. This system classification was single task and single user technology, but rudimentary compared to today's multitasking and multiuser mobile devices. They did not allow large volumes of data or information, videos, images, contacts, SMS, MMS, and emails, therefore the graphical interface was very different from today's mobile devices.

Tabla 1. Computer viruses on cell phones

N°.	**Virus/Worm Name/Year (Updated)**	**Operating System**
1.	Cabir A (June 2004)	Symbian
2.	Caballo de Troya (March 2017)	Symbian, *Windows*, Android and Mac OS X
3.	CommWarrior (October 2018)	Symbian and Android
4.	Crossover (March 2011)	*Windows Mobile*
5.	Doomboot (July 2019)	Symbian
6.	Liberty (September 2007)	*Palm* OS
7.	RedBrowser (September 2017)	J2ME
8.	FlexiSpy (June 2019)	Symbian and Android
9.	Skuller (June 2004)	Symbian
10.	Gingermaster (April 2011)	Android
11.	Ikee (November 2009)	*iPhone* OS (IOS)
12.	DroidKungFu (June 2011)	Android
13.	Zitmo (April 2018)	Symbian, Android, *Windows Mobile* and *Blackberry*
14.	YiSpecter (April 2018)	*iPhone* OS (IOS)

Note: Source: Author's own creation (2018).

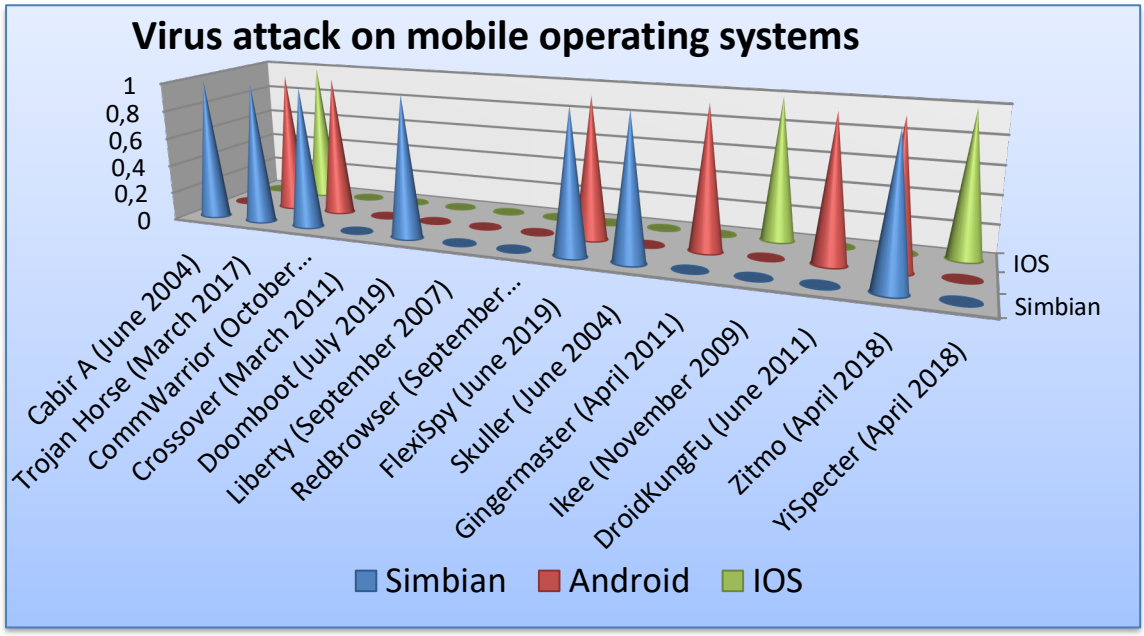

Figure 1. Virus attack on mobile operating system

Note: Source: Author's own creation (2019).

According to Figure 1., it can be seen that the Symbian operating system represents 50% of the 14 viruses, as it has 7 types of viruses that infect the operating system. Secondly, we can see the Android operating system with a total of 6 viruses and finally the IOS with 3 varieties of viruses.

Mac OS X operating system is not impenetrable as it is infected by the Trojan horse. Trojans must spread through user interaction such as opening an email attachment or downloading and running a file from the Internet and when they do so, the system sends instructions to the server.

The Trojan horse virus that infects mobile phones, as shown in Table 1, is the type of virus that attacks the most operating systems. This virus was named this way because of its high-speed transmission characteristic. It also has the ability to hide in the system and attack silently without the user even noticing. Downloads are its favorite hiding place. If a certain program is downloaded, it also installs the virus and slowly destroys the operating system. These viruses have two ways of spreading: one of them is hiding from the user and the other one requires the help of a cybercriminal in order to infect the target.

But the investment made to control these viruses is still not sufficient. Much more investment is needed in information security. There is no consensus in criminal law for cybercrime or cyberterrorism, which increases substantially every day. There should be a universal law to punish criminals or similar laws in each country because this kind of crimes can be transversal, for example, something can be done from a computer in Russia and commit crime in Angola, as it is not easy to detect. Crimes of this kind involve a lot of technology to uncover the criminal.

For all this, it is important to address the different operating systems, to present their strengths and weaknesses and find out which one is the most susceptible to virtual plagues and which one presents greater security against these viruses.

Mobile Operating Systems

Windows Phone 7

Windows Phone is a mobile operating system and the replacement successor to Windows Mobile. MS-Windows Mobile is distributed in cell phones of the main companies in the world; the only exception is Nokia, which uses Symbian in its phones. According to Tumejormovil (2019): "The Windows Phone operating systems, currently Windows 10 Mobile, are owned by Microsoft and are designed to provide the best possible performance for smartphones and tablets. It is closed-source and its kernel are Windows NT".

However, Windows Phone is one of the latest mobile operating systems designed by Microsoft. Built as a large-scale project from the point of view of information security, phones of this operating system have many download limitations in the Marketplace, which reduces the risk of having viruses.

In Sandeep, Chollie and Bandi's article (2012, p. 1575), it is stated that:

> The Windows phone application was designed from scratch and its main priority is security. Windows has added security features for Windows Phone applications. The Windows Phone security model was designed to protect the confidentiality, integrity and availability of information and communications.

The Windows Phone operating system has very simple graphics, but its programming language is not very well known, which prevents hackers from developing malicious software for mobile devices.

Figure 2. Cell phone with Windows Phone 8.1 Mobile Operating System

Note: Source: Buld (2014).

According to Table 1, the virtual plague that generally attacks Windows Mobile is claimed to be Crossover, a type of conceptual virus. This virus removes the "My Documents" directory and self-replicates each time the phone is rebooted.

Windows Mobile is considered to be very vulnerable to this destructive virus. However, the Windows Phone platform is more resistant to the virus, according to Altermann (2013):

> Windows Phone devices are among the safest so far. Since they do not run any files that are not linked to the Marketplace, no viruses developed by the platform have yet been discovered.
>
> The fact that it is a low-selling system also contributes to the fact that not many people are concerned about creating viruses for this platform. But that does not mean they should not pay the same attention as with any other platform.

Nevertheless, it is fair to say that Windows Phone is more resistant than other operating systems, as Sandeep, Cholli and Bandi (2012, p. 1575) state: "Windows Phone 7 is an operating system that brings together a large number of encryption methods including AES, SHA1 and SHAA256. Windows Phone 7 has the security model, which is key to protect the confidentiality, integrity, availability of information and interactions.

Cryptography is also called coded writing, which allows you to write coded messages and decode or encode certain information. Private key, public key, database, and bank data are successful thanks to the fundamental techniques of cryptography and are considered the best forms of authentication. Nowadays it is known that, to ensure efficient security, cryptography is used, as it allows greater security by modifying the different access codes, preventing cybercriminals from discovering the password. For example, both our credit cards and Wi-Fi passwords are encrypted to ensure protection. According to Quissanga (2015, p.14) “Microsoft has invested a lot in safety in Windows Phone 7. For example, restricting access to the application store to prevent users from downloading programs from the market, since many applications are downloaded every day.” For this reason, Windows Phone is very safe from computer attacks. Because of this company's low virus rate, others should take a cue from Microsoft and opt for this security system.

Android 4.3.2

Android is a not so safe mobile operating system based on the Linux kernel and its open source allows more vulnerable to computer attacks. According to Munhoz (2017) "A new virus for Android has emerged now and may be the bane of many people, as malware is downloaded automatically, including paid applications and games".

However, as shown in Table 1, the system is infected by 6 types of viruses. According to Tumejormovil (2019): “In fact, according to studies from 2017, 67.1% of mobile phones worldwide have Android and, specifically in Spain, 90%, which shows that it is a good operating system and could be the best on the market.” The Android operating system is also vulnerable to virtual plague attacks. In the statistics we can see that it is the most prevalent phone on the market, but it has weaknesses in terms of theft by hackers and crackers. The user's ability to use software outside the store allows malware to infect the device. The ease of transferring programs and applications in

addition to the system's unprotected Internet connection leads to contamination of the device.

According to Lima (2003), we can see:

> "Among the five main operating systems available on the market (Android, iOS, Windows Phone, Blackberry OS, Symbian), Windows Phone 8 is considered one of the safest. While 1 in 10 Android applications has malicious content, viruses are very rare in Windows."

However, Lima says the reason for this is that Windows Phone's security system is not vulnerable, while Android is susceptible to cyber-attacks, since its application store contains many suspicious programs that allow contamination of mobile devices. For example, there is an option to enable unknown sources which allows the installation of off-market software or applications.

iPhone 3.1.2

iPhone is a mobile device from Apple, launched on June 29th, 2007. It was one of the main events in the history of mobile telephony. Thousands of people lined up at Apple stores before its launch. About three and a half million iPhones were sold in the United States in the first six months since its launch. According to Tumejormovil (2019): "The IOS, formerly called the iPhone OS, is the second operating system with most smartphones in the world. Unlike Android, it is closed source and is made by Apple's operating kernel, MAC OS, [...]".

As far as operating system security is concerned, Mac OS X is infected with a Trojan virus. One of the main characteristics of this virus is its fast capacity, and that they must spread through user interaction. It often hides in files and when the user runs them, the system sends instructions to the server. According to Power (2018): "First Worm written in C by ikee for iPhone This worm exploits the fact that most jailbroken iPhone/iPod touch users install SSH and also neglect to change the password for root / mobile (which is "alpine" by default)."

The user logs in without even realizing it, sometimes entering his or her credentials or password without knowing that the instructions are not authentic, a feature that makes the virus so dangerous as well as efficient.

The Apple operating system is not perfect, it is also vulnerable to viruses. The social network Reddit, according to Souza (2014) "[...] discovered a new malware called Unflod Baby Panda, the virus affects all devices with jailbreak and is programmed to steal Apple IDs from infected devices by sending these credentials to their creators". It should be noted that the viruses affecting the iPhone are not well known, just as some publications claim that it is less prone to attacks on Android operating system technology because it is less in demand. As far as security is concerned, there is clear evidence on how the Internet is one of the fastest ways of spreading computer viruses. There are some palliative measures to prevent viruses from infecting certain mobile devices but saying that a certain operating system is immune to computer attacks would not be entirely correct as new computer viruses emerge every day. Technology develops as cybercrime evolves. The policy was: restrict your application store to prevent other unauthorized sources from accessing it, preventing any possible transmission of malware.

According to Lima (2013):

> We also know that this virus/operating system relationship is directly proportional to its popularity and the number of active users. Therefore, the

> more popular Windows Phone is, the more likely it is that more viruses and malware will emerge, but that does not mean that their vulnerabilities will necessarily increase.

However, it is impossible to say that we are totally safe when we are connected to the Internet, that is to say, no matter how safe we think we are, we can suddenly be surprised by a technology that can alter our security system by 90° or 100°.

The vulnerability of the iPhone operating system is still addressed as seen by Pandya and Stamp (2010, p. 84):

> Of course, iPhone is a vulnerable device with multiple security holes. The security philosophy of the iPhone itself has a significant flaw. Apple's approach to making the iPhone a secure device was to reduce the "intensity of the device's attack" or the "exposure of the device to vulnerabilities". Apple only allowed write access to one sandbox area in the file system and the unauthorized installation of third-party applications.

Mobile companies have to invest a lot in information security to make their devices more reliable, because nowadays the phone has become quite relevant in our daily life, we store a lot of information that must be protected.

> In case Apple was feeling left out, the first iOS malware for devices without jailbroken arrived in 2015. YiSpecter basically created a backdoor on compromised devices that allowed intruders to install and uninstall applications, download files and display ads, among other things. (Power, 2018).

Apple has a philosophy in its mobile devices that prevents the transfer of information via Bluetooth and it is safe to say that this measure prevented some transmission of computer viruses to other devices. Transmission via Bluetooth is the most common of all forms.

However, when a mobile device prototype is designed or developed, we always think about how it will look from a security point of view, and we never thought that this technology or system could resist several cyber-attacks, like Apple, surprisingly hackers were ready to break into the security system and spread insecurity to the consumers.

Symbian^3

The companies using this system are: Nokia, Sony Ericsson, Panasonic, Siemens and Samsung. Symbian is very vulnerable to virus attacks and is considered the most popular and destructive virus in history. The famous Trojan horse, just like the worm, originated the virtual plague cabir.A, the first mobile virus. According to Martinelli (2008, p. 88): "Cabir was written in the C++ language, originally to infect mobile systems based on the Symbian 60 series. This virus used exclusively Bluetooth technology to spread among cell phones". The C programming language is the most popular, says Olhar Digital (2013), "The C language continues to be the most used language in the world according to a new report from Tiobe Software. By conquering 18.15% of programmers, C expanded its lead over Java, an option for 16.5% of professionals". The C++ language integrates most of it, allowing more developers to create computer viruses to infect the Symbian operating system. However, if there are more developers, it is also possible to have more amateur language creators, just as if there is a large representation of cell phones in the market, this translates into a greater number of possible virus targets. Nowadays, this operating system is in decline, as the international market is conquered

by the two major mobile technology companies, Apple and Samsung, which have the iOS and Android operating systems respectively. Both are the most reliable operating systems on the market.

Results and Discussion

Operating systems have their own graphics, their structure is designed according to their developer but including all universal standards, and each system has its own prototype. These features can make them strong or weak to computer attacks. An example is the Symbin operating system. Symbin has a similar feature according to the analysis. We can see that the systems are created with a well-known and easy to develop programming language, and they allowed a greater programming of computer viruses in the market. The ease of installing software or applications outside the mobile device store, which primarily carry computer viruses, is considered a vulnerability as it damages the device's boot system.

However, unlike the Windows Phone operating system, Symbin has systems with a strong structure, which does not allow downloads outside the store, thus preventing malicious software from being installed. This feature makes it very safe because it does not allow the transmission of viruses easily and does not allow developers to program viruses since they do not know their programming language, because contamination only occurs when it is the same source code or kernel. The Windows Phone 7 operating system uses the system's cryptographic protection methods. This feature prevents many computer attacks on the operating system.

Operating system viruses are not as well known, but we cannot assert that they are not at risk, they are also vulnerable to the Ikee virus. iPhone is not as vulnerable as the Symbian and Android operating systems. However, it is worth mentioning that Apple's iPhone operating system has a feature that prevents programs or some devices from affecting the system. Bluetooth is known to be the fastest way for mobile phones to transmit computer viruses and Apple has restricted the transfer of applications to other devices via Bluetooth. Its programming language does not have many developers. These characteristics make it less vulnerable to computer viruses.

Conclusion

As we learn more about mobile operating systems, we can conclude that: computer virus infections in cell phones have to do with the operating system, its kernel, the technology of the phone and the programming language. Martinelli (2008, p. 32) states "Every operating system has a kernel that delimits its functions. This is one of the reasons why a cell phone virus does not spread easily to other devices, due to the different versions and internal structure of the various mobile operating systems.

It is known that Symbian is the operating system most likely to be contaminated by computer viruses, since it is made of a C++ programming language that comes from the C language, one of the most popular languages, which also has many developers.

Android is a less reliable mobile operating system based on the Linux kernel, and its open source feature allows for a larger number of developers of the technology. Finally, we

conclude that among mobile phone operating systems such as Android, iPhone, Symbian and Windows Phone, the latter is the safest from the virtual attack security point of view, because it is known that Microsoft has invested heavily in its security system, restricting access to the app store to prevent the users from downloading programs off the market, since every day several malicious applications are added in there.

References

Altermann, D. (2013). Como remover vírus do celular: Como remover vírus do Windows Phone? *Tech tudo*. Retrieved from http://www.techtudo.com.br/ticas-e-tutorials/noticia/2012/08/how-remove-virus-do-cellular.html.

Buld (2014). *Microsoft Officially Intros Windows Phone 8.1, Details Cortana*. Retrieved from https://news.softpedia.com/news/BUILD-2014-Microsoft-Intros-Windows-Phone-8-1-Details-Cortana-435504.shtml.

Chaer, G. Diniz, R. R. P. Ribeiro, E. A. (2011). A técnica do questionário na pesquisa educacional: O questionário em questões de cunho empírico. *Evidência, Araxá*, *7*(7), 251-266, Retrieved from. http://www.educadores.diaadia.pr.gov.br/arquivos/File/maio2013/sociologia_artigos/pesqusia_social.pdf.

Gimenez, R. (2011). *5 Antivírus para celular e por que você precisa deles*. Retrieved from https://danresa.wordpress.com/page/14/?app-download=nokia.

Lima, A. (2013). *A segurança da informação no seu Windows Phone 8, Windows Phone Brasil*. Retrieved from http://windowsphonebrasil.com.br/a-security-da-informacao-no-seu-windows-phone-8/.

Lima, A. (2013). *A segurança da informação no seu Windows Phone 8, Windows Phone Brasil*. Retrieved from http://windowsphonebrasil.com.br/a-security-da-informacao-no-seu-windows-phone-8/.

Martinelli, H. (2008). *Vírus de celular: Estudo e classificação para um protótipo de defesa: Telefonia celular e vírus*. Porto Alegre: Uniritter. Retrieved from http://www.uniritter.edu.br/graduacao/informatica/sistemas/downloads/tcc2k8/TCC%202%20final(Horst).pdf.

Martinelli, H. (2008). *Vírus de celular: Estudo e classificação para um protótipo de defesa: ANEXO B: Código do vírus Cabir*. Porto Alegre: Uniritter. Retrieved from http://www.uniritter.edu.br/graduacao/informatica/sistemas/downloads/tcc2k8/TCC%202%20final(Horst).pdf.

Munhoz, V. (2017) *Skyfin: o malware de Android capaz downloads e compras ilegalmente*. Tecmundo. Retrieved from https://www.tecmundo.com.br/malware/113680-skyfin-malware-android-capaz-fazer-downloads-compras-ilegalmente.htm.

Nascimento, L. M. B. do. (2009) Análise documental e análise diplomática: perspectivas de interlocução de procedimentos. Resumo. Retrieved from http://marilia.unesp.br/Home/PosGraduacao/CienciadaInformacao/Dissertacoes/nascimento_lmb_do_mar.pdf.

Olhar Digital. (2013). *C se mantém como a linguagem de programação mais popular*. Retrieved from https://olhardigital.com.br/pro/noticia/c-se-mantem-como-a-programcao-mais-popular/38882.

Pandya, V. R. & Mark, S. (2010). *iPhone Security Analysis: Security Analysis. Journal of Information Security*. Retrieved from https://file.scirp.org/pdf/JIS20100200003_25782595.pdf.

Power. J. P. (2018). Maliciosamente móvel: uma breve história do malware móvel: Ikee. Retrieved from https://medium.com/threat-intel/mobile-malware-infosec-history-70f3fcaa61c8.

Power. J. P. (2018). Maliciosamente móvel: uma breve história do malware móvel: YiSpecter. Retrieved from https://medium.com/threat-intel/mobile-malware-infosec-history-70f3fcaa61c8.

Quissanga, F. C. (2015). Caracterização de vírus informáticos em telefonia móvel celular: Os Crackers .(Trabalho de conclusão do curso) Escola Superior Aberta do Brasil -ESAB - Vitoria: Espírito Santo-Brasil.

Quissanga, F. C. (2015). Caracterização de vírus informáticos em telefonia móvel celular: Propagação e infeção. (Trabalho de conclusão do curso) Escola Superior Aberta do Brasil -ESAB - Vitoria - Espírito Santo. Retrieved from https://campusonline.esab.edu.br/campusonline/modulos/campus/index.cfm.

Quissanga, F, C. (2015). Caracterização de vírus informáticos em telefonia móvel celular: Windows Phone 7. Escola Superior Aberta do Brasil - Vitoria - Espírito Santo. Retrieved from https://campusonline.esab.edu.br/campusonline/modulos/campus/index.cfm.

Sandeep, B. V, Cholli, N. G, & Bandi, S. (2012). Securing Applications in Windows Phone: Introduction. International *Journal of Electronics and Computer Science Engineering-IJECSE, 1*(3), 1574. doi=10.1.1.259.7340&rep=rep1&type=pdf.

Sandeep, B. V; Cholli, N. G; & Bandi, S. (2012). Securing Applications in Windows Phone: Windows Phone security. *International Journal of Electronics and Computer Science Engineering-IJECSE*, 1(3) 1575. doi=10.1.1.259.7340&rep=rep1&type=pdf.

Souza, R. de. (2014) *Novo malware para iOS é descoberto por usuário do Reddit: Batizado como UnflodBaby Panda, vírus é de origem chinesa e afeta qualquer dispositivo que tenha sofrido processo de jailbreak*. Tecmundo. Retrieved from http://www.tecmundo.com.br/ios/53792-novo-malware-para-ios-e-discovered-by-userio-do-reddit.htm.

Tumejormovil (2019). Comparação Dos Sistemas Operacionais Móveis Mais Utilizados (Android, IOS, Windows Phone): Sistema operacional Android. Retrieved from https://tumejormovil.com/operative-systems/.

Tumejormovil (2019). Comparação Dos Sistemas Operacionais Móveis Mais Utilizados (Android, IOS, Windows Phone): Sistema operacional IOS. Retrieved from https://tumejormovil.com/operative-systems/.

Tumejormovil (2019). Comparação Dos Sistemas Operacionais Móveis Mais Utilizados (Android, IOS, Windows Phone): Sistema operacional Windows Phone. Retrieved from https://tumejormovil.com/operative-systems/.

Trif, S., & Vişoiu, A. (2011). Business Intelligence Mobile applications. Informatica Economică, 15(2), 119. Retrieved from http://revistaie.ase.ro/content/58/11%20-%20Trif,%20Visoiu.pdf.

Date received: 18/03/2019
Date reviewed: 18/11/2019
Date accepted: 02/12/2019