PROJECT, DESIGN AND MANAGEMENT

ISSN: 2683-1597

PROJECT DESIGN & MANAGEMENT

Cómo citar este artículo:

Cassinda Qussanga, F. (2019). Caracterização de sistemas operacionais móveis celulares: Android, Symbian, iphone e Windows phone. *Project, Design and Management, 1*(2), -. doi: 10.35992/pdm.v1i2.200

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

Fernando Cassinda Quissanga
Escola Superior Aberta do Brasil (Brasil), Universidad Europea del Atlántico (España)
fernandoquissanga@hotmail.com · https://orcid.org/0000-0003-4468-7206

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 baseada pelo referencial bibliográfico, os dados coletados em livros, manuais técnicos, informações de fabricantes e em sites da internet; à análise dos dados é documental, feita em tabelas. Entretanto, conclui-se que nem todo tipo de vírus informáticos infectam os telefones celulares, depende do núcleo (kernel) do sistema operacional. 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++ proveniente da 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 são colocados inúmeros aplicativos. A tecnologia *bluetooth* representa maior forma de transmissão de vírus informáticos.

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

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

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.

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, istemas operacionales.

Introdução

Entende-se um considerável número de telefones móveis celulares, entretanto, estes dispositivos atualmente, permitem a comunicação, o envio de mensagem em multimídia, transferências bancárias, consulta de serviços meteorológicos, serviços de localização geográfica, sistema de posicionamento global ou geográfico (GPS), impressão de documentos, outros serviços de convergência tecnológica, calculadora, agenda de contatos, galerias, partilha de dados, de internet (*hotspot* portatil) podendo transmitir o sinal de internet para 10 ou mais dispositivos transferência de informação por *bluetooth*. Possuem memórias, processadores e um sistema operacional embutido, que permite maior fluxo, manuseamento e troca de informações entre os usuários, sendo que, possibilita insegurança, sobre tudo, a perda e o roubo das informações tem sido a maior preocupação. Notavelmente o crime virtual aumentou, no entanto, o celular tornou-se muito vulnerável a ataques de vírus informáticos.

Segundo Gimenez (2011) afirma que "a primeira coisa que se precisa saber é que, uma solução de segurança para celular é completamente diferente de uma para desktop ou *notebook***.** Por exemplo, de acordo com a Symantec, há mais de 286 milhões de *malwares* para computador, há cerca de 1000 para celulares […]". Diante desta citação, podemos perceber que os sistemas operacionais móveis são diferentes uns aos outros, quanto a sua robustez e vulnerabilidade, no entanto, os vírus de um sistema operacional android não atacam o da iOS vice-versa, devido o seu núcleo (*kernel*), ou seja, depende do código fonte e a sua linguagem de programação.

Objetivo Geral: caracterizar qual dos sistemas operacionais móveis celulares, é o mais seguro e o mais susceptível aos vírus informáticos.

A pesquisa é qualitativa baseada pelo referencial bibliográfico, que permitiu avaliar o material de interesse de estudo do tema referido, como sustento do artigo científico. As técnicas e instrumentos de pesquisa foi aplicado um (1) questionário, oito (8) entrevistas. No entanto podemos analisar a definição de Chaer, Diniz, e Ribeiro. (2011, p. 260 apud Gil, 1999, p.128): "como a técnica de investigação composta por um número mais ou menos elevado de questões apresentadas por escrito às pessoas, tendo por objetivo o conhecimento de opiniões, crenças, sentimentos, interesses, expectativas, situações vivenciadas etc."Através das entrevistas foi possível identificar diferença entre os referidos sistemas operacionais de telefonia móvel celular.

Concernente, os dados coletados, é possível notar, um número limitado de publicações em obras sobre vírus informáticos em telefonia móvel celular. Entretanto, foi feita a pesquisa em livros, manuais técnicos, artigos científicos, informações de fabricante e em sites da internet. "A análise documental, como processo intrínseco à Organização da Informação no domínio da Ciência da Informação, estabelece parâmetros teórico-metodológicos, de natureza descritiva, que explicitam os procedimentos do fazer analítico que levam à identificação de conceitos do documento." (Nascimento, 2009).

Vírus Informáticos em telefonia móvel celular

Falar de vírus hoje nesta sociedade, vem em mente os vírus biológicos que são traduzidos como veneno, toxina ou agentes infecciosos, mas neste capítulo, vamos mencionar sobre os vírus informáticos em telefonia móvel celular, que podemos definir como um *software* malicioso feito por linguagem de programação que infecta o sistema operacional e se hospeda no programa e replica-se para outros locais do sistema, corrompe e impede o funcionamento normal do *software* ou programa do seu arranque.

> Os *Crackers* (criminosos virtuais), são muito agis em linguagem de programação, possuem conhecimentos de redes de computadores, telecomunicações e engenharia de *software*, algumas vezes sem nível de escolaridade, criam os vírus com intuito de tirar dividendo, monitoram todas vias possíveis, quebram senhas e detetam falhas de segurança em várias áreas, empresas, bancos entre outros (Quissanga, 2015, p. 10).

Existem relatos que afirmam que alguns vírus não foram realizados de maneira intencional, todavia com o intuito de testar o sistema de segurança, como meio de conhecer melhor o comportamento dos vírus, outros para estudo em laboratórios permitindo maior interação dos estudantes, outra vertente podemos afirmar que alguns vírus, foram feitos por programadores amadores e *hacker* por diversão, sem saber os riscos e medir consequências. Esses vírus não são tão conhecidos, mas têm causados enumeras dificuldades, para além de danificarem os sistemas operacionais também

existem vírus específicos para o roubo de informações, visto que nos telefones móveis servem para efetuar muitas operações, quer bancárias, transferências de aplicativos o envio de emails, mensagens, ele é específico para telefonar, com internet permite interagir nas redes sociais, gravações, ou seja, tudo que chamamos de convergência tecnológica. No entanto essa característica de convergência tecnológica sobre tudo ao se conectar a internet possibilita a transmissão de vírus informáticos aos dispositivos móveis celulares, por esse motivo devemos proteger o sistema operacional utilizando antivírus, *antimalware* e *antispyware*. De acordo com Trif & Vişoiu (2011, p.119) afirmam que: "As novas conquistas nas tecnologias de dispositivos móveis abriram o caminho para novas aplicações projetadas para rodar em dispositivos móveis. No início, os dispositivos móveis ofereciam uma funcionalidade muito limitada devido à pouca memória, poder de computação e interação difícil."

No entanto, os roubos informáticos por telefonia móvel celular tem sido de forma silenciosa, o usuário não tem noção que o seu dispositivo está vulnerável a crime virtual, está ser alvo de espionagem, as suas credenciais são captadas por criminosos virtuais, seus emails são monitorados, seus dados bancários estão em perigo. São enumeras motivações que os prevaricadores informáticos têm para poder criar os vírus e efetuar qualquer crime virtual.

No entanto, é oportuno mencionar o comportamento ou motivação que leva os programadores informáticos criarem os vírus, embora que a real motivação é feita para destruir os sistemas operacionais.

Entretanto, os vírus contemplam duas vertentes:

- O programador criar o vírus para destruir ou corromper os aplicativos do telefone móvel celular;
- O envio de mensagens para furtar dados dos usuários.

> Muitas vezes, o usuário permite que os meios de propagação aumentem substancialmente, por falta de precaução e pouco conhecimento de causa sobre as formas de transmissão dos vírus, portanto, todo e qualquer fabricante, desenvolvedor ou empresas de direito, devem promover a realização de palestras, debates, fóruns e seminários sobre as causas, formas de propagação, danos e prevenção dos vírus informáticos […] (Quissanga, 2015, p. 10).

Os vírus em telefones móveis celulares, têm a sua origem em 2004, que podemos considerar ser muito recente comparando com os vírus de computadores nos finais dos anos 80. Entretanto, podemos observar a Empresa F-Secure sobre o relato da descoberta do primeiro vírus em telefonia móvel celular.

Segundo Martinelli, (2008, p. 94):

> No ano de 2004, o primeiro vírus para celulares foi descoberto pela empresa de segurança F-Secure foi denominado Cabir.A. Cabir.A na verdade é um *worm* que se propaga apenas pelos celulares utilizando a tecnologia de transmissão sem-fio *Bluetooth*, afetando dispositivos baseados no sistema operacional Symbian - mais conhecido como plataforma Series 60.

Mas a praga não se estende a todos dispositivos, pelo que, vemos algumas restrições por ter vírus específico para cada sistema operacional. A tecnologia *bluetooth* é uma das tecnologias de transmissão rede sem-fio que permite a troca de informação entre os dispositivos, ela possui uma característica muito peculiar de efetuar o baixo

consumo de energia. O vírus Cabir.A originou desta tecnologia pelo envio de mensagem infectada ao dispositivo móvel celular. No entanto, é considerado como a primeira via de disseminar o vírus em telefonia móvel celular. Geralmente essa tecnologia permite de forma muito simples a transferência de informação de forma ponto a ponto. Na maior parte os dispositivos móveis têm sido desprovidos de qualquer antivírus que impeça que vírus informáticos infectam o sistema operacional e por sua vez danifica-lo ou o roubo de informações, razão pela qual que os telemóveis têm que possuir proteção porque a maior via de transmissão do vírus nos telefones móvel celular tem sido o *bluetooth* e a internet.

Descrever os possíveis tipos de vírus informáticos em telefonia móvel celular.

Depois de abordamos a origem dos vírus é oportuno mencionar os tipos vírus em telefonia móvel celular.

No entanto, os vírus de computadores são mais abrangentes quanto a forma de se propagar e actuar na sua presa, para alem de possuir muitos desenvolvedores, desta forma existem muitos tipos de vírus, o que não acontece com os vírus dos dispositivos móveis celulares, sendo a sua descoberta muito recente, que limitou a pesquisa e o desenevoamento assim como a inserção de vírus no mercado e o acesso aos seus dispositivos muito recente que de alguma forma desenvolvimento dos mesmos.

Atualmente são frequentes os vírus silenciosos, os *crackers* utilizam para espionar e tirar dividendo qualquer vulnerabilidade do dispositivo móvel celular como imagens, vídeos, informações comprometedoras ou confidenciais, códigos bancários para efetuar diversas transferências. Devemos ter cuidado com as informações que colocamos nos nossos dispositivos móveis celular quando não possuímos um antivírus, *antimalware* e *antispyware.*

Os vírus de celular não são tão populares como os de computadores, percebe-se também pela evolução das diversas gerações de telefonias móveis, no entanto, os telefones móveis de marca Nokia e o Siemens que utilizavam o sistema operacional Symbian, quanto a classificação dos sistema operacional eram monotarefa e monousuários, apresentavam uma tecnologia ainda rudimentar comparando com os atuais dispositivos móveis multitarefa e multiusuários. Entretanto, não permitiam, grandes volumes de dados ou informações, vídeos, imagens, contatos, e SMS, MMS, E-mails, ou seja, uma convergência tecnológica, uma interface gráfica como apresenta os atuais dispositivos de telefonia móvel celular.

Tabela 1. *Vírus informáticos em telefonia móvel celular*

Nº	Nome do vírus/*Worm*/*Ano (Actualizado)*	Sistema Operacional
1.	Cabir A (Junho de 2004)	Symbian
2.	Cavalo de Tróia (Março de 2017)	Symbian, *Windows*, Android e Mac OS X
3.	CommWarrior (Outubro de 2018)	Symbian e Android
4.	Crossover (Março de 2011)	*Windows Mobile*
5.	Doomboot (Julho de 2019)	Symbian
6.	Liberty (Setembro de 2007)	*Palm* OS
7.	RedBrowser (Setembro de 2017)	J2ME
8.	FlexiSpy (Junho de 2019)	Symbian e Android
9.	Skuller (Junho de 2004)	Symbian
10.	Gingermaster (Abril de 2011)	Android
11.	Ikee (Novembro de 2009)	*iPhone* OS (IOS)
12.	DroidKungFu (Junho de 2011)	Android
13.	Zitmo (Abril de 2018)	Symbian, Android, *Windows Mobile* e *Blackbarry*
14.	YiSpecter (Abril de 2018)	*iPhone* OS (IOS)

Nota: Fonte: Elaboração própria (2018).

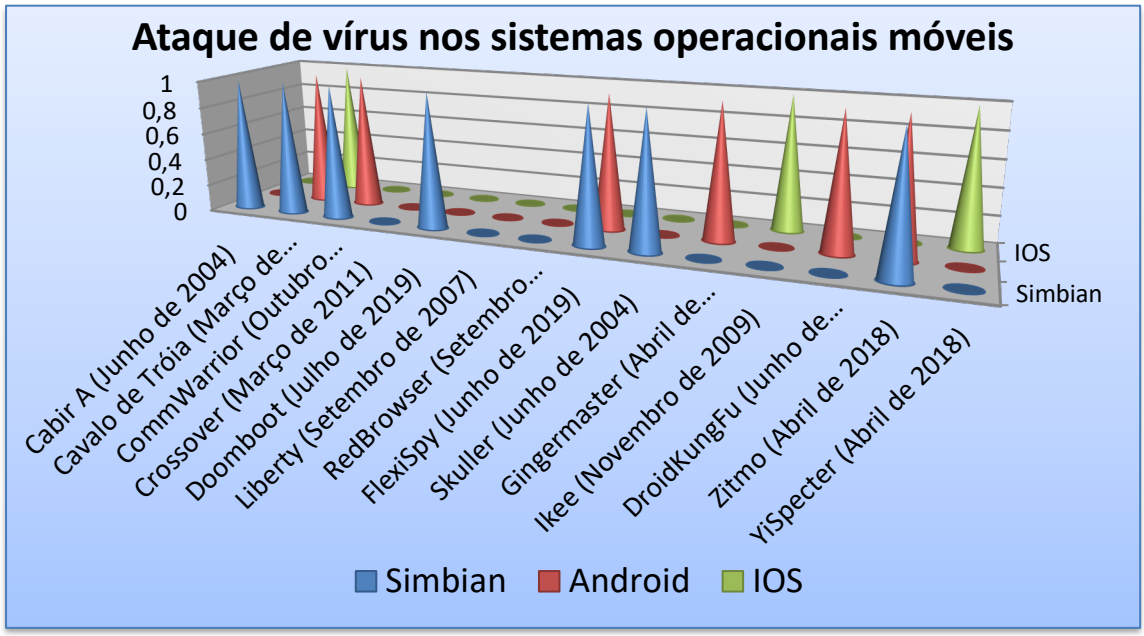

Figura 1. Ataque de vírus nos sistemas operacionais móveis celular

Nota: Fonte: Elaboração própria (2019).

Segundo o Figura 1., é possível observar que, o sistema operacional Symbian representa 50% dos 14 vírus, por apresentar 7 tipos de vírus que infectam o sistema operacional. Em segundo lugar podemos observar o sistema operacional Android com uma representação de 6 vírus e por último o IOS com 3 variedades de vírus.

O sistema operacional Mac OS X é infectado pelo cavalo de tróia, no entanto, o Mac não é imbatível, notamos que uma das características do cavalo de tróia, a sua capacidade de transmissão que pode ser cliente e servidor, algumas vezes pode-se apresentar oculto em um arquivo e a medida que é executado pelo cliente o sistema envia instruções para o servidor.

O cavalo de tróia dos vírus que infectam os telefones móveis celulares, como se pode observar na tabela 1., é o tipo de vírus que ataca maior número de sistemas operacionais, como o seu nome indica, e conhecemos melhor o comportamento do cavalo, possui uma característica muito veloz de transmissão, possui uma capacidade oculta no sistema, ataca de forma silenciosa sem que a presa se apercebe, nos *downloads* são os seus preferidos, no entanto ao baixar um determinado programa ele matem-se oculto, ao instalar o *software* fidedigno instala-se também o vírus e aos poucos vai destruindo o sistema de arranque do sistema operacional. Esses vírus apresentam duas formas de propagação: uma instala-se ocultamente na sua presa e outra precisa de auxílio de um criminoso virtual para contaminar a presa.

Mas o investimento que se faz para conter esses vírus ainda não é satisfatório, precisa-se investir muito mais na segurança da informação. Não existe uniformização na legislação penal para os crimes cibernéticos ou para o cibertorrorismo, que a cada dia aumenta substancialmente, deveríamos possuir uma lei universal para punir os prevaricadores ou leis próximas porque o crime pode ser transversal estando com um computador remoto na Rússia e cometer o crime em Angola, e não é fácil a sua descoberta, tem que haver uma política universal para poder levar criminalmente os criminosos virtuais. Os crimes destes géneros implicam muita tecnologia para descobrir o criminoso.

No entanto é oportuno abordar os diferentes sistemas operacionais, apresentar a sua robustez e sua fragilidade e qual deles é o mais susceptível a pragas virtuais e qual apresenta maior segurança a essas pregas virtuais.

Sistemas operacionais móveis celulares

Windows Phone 7

O *Windows phone* é um sistema operacional móvel evoluído do *Windows mobile*, o *MS-Windows Mobile* é distribuído em telefones celulares das principais empresas do mundo, a única exceção é a Nokia que utiliza o Symbian em seus telefones. Segundo Tumejormovil (2019): "Os sistemas operacionais *Windows Phone* , atualmente *Windows 10 Mobile* , pertencem à *Microsoft* e foram fabricados para oferecer o melhor desempenho possível para *smartphones* e *tablets*. Ele fechou o código e seu núcleo é o *Windows NT*."

Entretanto, os *Windows phone* é um dos últimos sistemas operacionais móveis elaborado pela Microsoft, foi desenhado por um projeto de grande magnitude do ponto de vista da segurança da informação, os celulares deste sistema possuí muitas limitações de transferências no *Marketplace*, que não permite que o mesmo seja vulnerável a diversas pragas virtuais.

Observamos no artigo de Sandeep, Chollie e Bandi (2012, p. 1575) afirmam que:

> O aplicativo de telefone do *Windows* é projetado desde o início com segurança como alta prioridade. *Windows* incluiu recursos de segurança e

> facilitou a criação de segurança adicional para os aplicativos do *Windows Phone*. O modelo de segurança do *Windows Phone* é a base para proteger a confidencialidade, integridade e disponibilidade de dados e comunicações.

No entanto o sistema operacional *Windows Phone* possui uma gráfica muito simples mas que a sua linguagem de programação não é muito conhecida, esse motivo impede os *hackers* desenvolverem *softwares* maliciosos para os dispositivos móveis celulares.

Figura 2. Telefone móvel de Sistema Operacional Windows Phone 8.1

Nota: Fonte: Buld (2014).

Segundo a tabela 1., declara sobre a praga virtual que geralmente ataca o *Windows Mobile* é o *Crossover*, o tipo de vírus conceito. O vírus apaga o diretório "Meus Documentos" e se replica sempre que o celular é reiniciado.

É possível notar que o *Windows Mobile* é vulnerável por ser infectado facilmente pelo vírus *Crossover* muito destrutivo. No entanto, com a plataforma do *Windows phone* apresenta-se maior resistência ao vírus, Segundo Altermann (2013):

> Os aparelhos que utilizam o sistema *Windows Phone* se mostram um dos mais seguros até o momento. Pelo fato de não executarem nenhum arquivo que não esteja vinculado ao *Marketplace*, ainda não foi descoberto nenhum vírus desenvolvido pela plataforma.
>
> O fato de ser um sistema com pouca representatividade em relação a número de vendas também colabora para que não haja muitas pessoas preocupadas em criar vírus para tal plataforma. Mas isso não significa que você não deva manter os mesmos cuidados que teria com qualquer outra plataforma.

Entretanto o *Windows phone* podemos afirma que apresenta mais robustez que outros sistemas operacionais, como podemos observar a citação de Sandeep, Cholli e Bandi (2012, p. 1575) afirmam que: "O *Windows Phone* 7 é um sistema operacional que encadeia número grande de métodos de criptografia que contam *AES, SHA1 e SHAA256*. O *Windows phone 7* possui o modelo de segurança, base para proteger o sigilo, integridade, acessibilidade de dados, e interações".

A criptografia é também chamada de escrita codificada, permite escrever mensagens em código e decifrar ou cifrar determinada informação. São as melhores formas de autenticação, da chave primária, pública, banco de dados, dados bancários, têm sucesso graças as técnicas fundamentais da criptografia. É sabido nos dias de hoje, para que haja uma segurança eficiente, recorre-se ao uso da criptografia, por permitir maior segurança, pela variação dos diversos códigos de acesso, não permitindo que os criminosos virtuais descubram a senha. Por exemplo os nossos, cartões de créditos, senhas para proteger a redes de roteadores, para que haja proteção utiliza-se a técnica de criptografia. Segundo Quissanga (2015, p.14) "A *Microsoft* investiu bastante na segurança do *Windows phone 7*. Pelo que, restringiu o acesso ao *app store* para impedir que o usuário baixe programas fora do mercado, visto que, a cada dia são colocados inúmeros aplicativos." Diante desta temática é que torna o *windows phone* muito seguro a ataques informáticos. Assim como representa inferior o número de programadores de vírus informáticos de telefonia móvel celular para esse sistema operacional, a exemplo da *Microsoft* outras companhia deveriam optar por esse sistema de segurança.

Android 4.3.2

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, tornando muito vulnerável a ataques informáticos. Segundo Munhoz (2017) afirma o seguinte "Um novo vírus para Android surgiu agora e pode ser a perdição para muita gente, pois o *software* malicioso realiza *downloads* automaticamente, incluindo de *apps* e jogos pagos".
Entretanto, pode-se observar na tabela 1., o sistema é infectado por 6 tipos de vírus. Segundo Tumejormovil (2019): "De fato, de acordo com estudos de 2017, 67,1% dos celulares em todo o mundo têm Android e, especificamente na Espanha, 90%, portanto, é demonstrado que é um bom sistema operacional e que poderia ser silenciosamente o melhor do mercado." O sistema operacional Android também é vulnerável ao ataque de pragas virtuais, na estatística é possível observar o maior número de representações telefônicas no mercado, pelo que, ficam susceptíveis aos *crackers* e *hackeres* efetuarem o furto por apresentar fragilidades. A possibilidade do usuário usar *softwares* fora da loja permite que *softwares* maliciosos infectam o dispositivo móvel celular, a facilidade de transferência de programas e aplicativos, a conexão do sistema na internet sem proteção permite a contaminação ao dispositivo móvel celular.

É possível observar segundo Lima (2013):

> Dentre os cincos principais sistemas operacionais disponíveis no mercado (Android, iOS, *Windows Phone*, *Blackberry* OS, Symbian), o *Windows Phone* 8 pode ser considerado como sendo um dos mais seguros entre eles. Enquanto no Android 1 em cada 10 *apps* contém algum conteúdo malicioso, vírus para o *Windows Phone* surgem apenas em rumores."

No entanto, Lima afirma que os vírus informáticos, para o *Windows Phone* ainda é rumores, tudo isso porque o sistema de segurança não é vulnerável, já para o Android é susceptível para ataques cibernéticos, o seu *apps store* contém muitos *softwares* suspeitos, que permitem a contaminação dos dispositivos móveis, na tecnologia dos dispositivos Android existe nas definições, aplicações e posteriormente encontramos a opção origens desconhecidas sendo ativada permite instalação de softwares ou aplicações fora do mercado.

iPhone 3.1.2

O *iPhone* é um dispositivo móvel da *Apple*, lançada em 29 de Junho de 2007, foi um dos grandes eventos da história da telefonia móvel celular. Milhares de pessoas foram para serem os primeiros a comprar nas lojas da *Apple* antes de seu lançamento. Provavelmente três e meio milhão de *iPhones* foram vendidos nos Estados Unidos da América (EUA) nos primeiros seis meses de seu lançamento. De acordo com Tumejormovil (2019): "O IOS , anteriormente chamado de iPhone OS, é o segundo sistema operacional com mais *smartphones* do mundo. Ao contrário do Android, seu código é diretamente fechado e é fabricado pelo *kernel* do sistema operacional da *Apple*, o MAC OS,[…]."

Podemos também fazer referência sobre a segurança do sistema operacional Mac OS X é infectado pelo cavalo de tróia, hoje já não é realidade de que o Mac não é infectado por pragas virtuais, notamos que uma das características do cavalo de tróia é a sua capacidade veloz de transmissão que pode-se apresentar como cliente e ao mesmo tempo servidor, maior parte das vezes oculta-se em um arquivo e a medida que é executado pelo cliente o sistema envia instruções para o servidor. Segundo Power (2018): "Primeiro *Worm* escrito em C por ikee para *iPhone*. Esse *worm* explora o fato de que a maioria dos usuários de *iPhone / iPod touch* com *jailbreak* instala o SSH e também se esquece de alterar a senha do *root / mobile* (que é "alpino" por padrão)."

Entretanto, ele permite autenticar-se ao usuário sem que o mesmo dê conta, o usuário algumas vezes introduz as suas credenciais ou senha sem saber que as instruções não são autênticas, essa característica do vírus torna-lhe tão perigoso e eficiente.

O sistema operacional da *Apple* não é invencível ele também é susceptível a vírus, a Rede Social *Reddit* segundo Souza (2014) "[…] descobriu um novo *malware* Batizado de *Unflod Baby* Panda, o vírus afecta todo e qualquer aparelho que sofreu *jailbreak* e está programado para roubar *Apple* IDs dos dispositivos infectados, enviando essas credenciais para seus criadores". É notável que os vírus que afecta o *iphone* não são muito conhecidos, assim como algumas literaturas afirmam que ele é menos propenso a ataques em relação a tecnologia do sistema operacional Android, por apresentar menor representatividade no mercado. Quanto a segurança temos a clara evidência de que a internet é uma das mais velozes vias de transmissão de vírus informáticos. Existe algumas medidas paliativas para impedir que vírus não infectam certos dispositivos móveis celulares, mas afirmar que um determinado sistema operacional está imune a ataques informáticos, estaríamos errados, a cada dia surgem novos vírus informáticos da mesma maneira que a tecnologia desenvolve-se é da mesma que o cibercrime evolui. A politica foi da seguinte maneira: restringir o seu *app store*, para impedir que outras fontes não autorizadas tenham acesso, evitando a possível transmissão de qualquer *malware*.

Segundo Lima (2013) afirma o seguinte:

> Também sabemos que essa relação de quantidade de vírus para o Sistema Operacional é diretamente proporcional a sua popularidade e ao número de usuários ativos. Sendo assim, quanto mais popular o *Windows Phone* for ficando, maiores serão as chances de surgirem mais vírus e *malwares*, contudo, não necessariamente aumentarão também as suas vulnerabilidades.

Entretanto, é impossível dizer que estamos totalmente seguros, quando estamos ligados a internet, ou seja, quanto mais pensamos que estamos seguros, somos surpreendidos com uma tecnologia que pode alterar 90º ou 100º o nosso sistema de segurança.

Entretanto, ainda abordando sobre a vulnerabilidade do sistema operacional do *iPhone* como se pode observar Segundo Pandya e Stamp (2010, p. 84):

> É claro que o *iPhone* é um dispositivo vulnerável com várias falhas de segurança. A filosofia de segurança do *iPhone* em si tem uma falha significativa. A abordagem da *Apple* para tornar o *iPhone* um dispositivo seguro era reduzir "a intensidade do ataque do dispositivo ”ou“ a exposição do dispositivo a vulnerabilidades ” Para isso, a *Apple* permitiu o acesso de gravação apenas a uma área de *sandbox* no sistema de arquivos e instalação não permitida de aplicativos de terceiros.

As empresas de telefonia móvel têm que investir bastante na segurança da informação, para dar mais credibilidade aos utentes dos seus dispositivos, porque o telefone atualmente tornou-se bastante pertinente no nosso quotidiano, depositamos muita informação, que deve ser protegida.

> Apenas no caso de a *Apple* estar se sentindo excluída, em 2015 surgiu o primeiro *malware iOS* para dispositivos não *jailbroken*. O YiSpecter basicamente criou um *backdoor* em dispositivos comprometidos que permitiam aos invasores instalar e desinstalar aplicativos, baixar arquivos e exibir anúncios, entre outras coisas. (Power, 2018).

A *Apple* possui uma filosofia nos seus dispositivos móveis que impede a transferência de informação por via *bluetooth*, que podemos dizer que esta medida de certa forma impedi a transmissão de vírus informáticos para outros dispositivos, a transmissão via *bluetooth* é a maior de todas outras formas estudadas.

Entretanto, quando começamos a projetar ou desenvolver um protótipo, um dispositivo móvel, pensamos sempre como este será do ponto de segurança, e nunca imaginamos que essa tecnologia, ou sistema será capaz de resistir aos diversos ataques cibernéticos, a exemplo da *Apple*, surpreendentemente os *hackers* já estavam preparados para denegrir o sistema de segurança e trazer insegurança para os consumidores.

Symbian^3

As empresas que utilizam este sistema são: Nokia, Sony Ericsson, Panasonic, Siemens e Samsung. O Symbian é muito susceptível ao ataque de um vírus, considerado o mais popular e destrutivo da história, o famoso cavalo de tróia, assim como *worm* originou a praga virtual cabir.A, o primeiro vírus móvel. Segundo Martinelli (2008, p. 88) afirma que: “Cabir foi escrito na linguagem C++, originalmente para infectar sistemas móveis baseados no Symbian série 60. O vírus utilizava exclusivamente a tecnologia *Bluetooth* para se propagar entre os celulares”. Percebe-se que a linguagem de programação C é a mais popular, nos afirma o Olhar Digital (2013), “A linguagem C contínua sendo a mais utilizada no mundo segundo novo relatório da empresa Tiobe *Software*. Ao conquistar 18,15% dos programadores, o C ampliou sua vantagem em relação ao Java, opção de 16,5% dos profissionais”. A linguagem C++ integra maior parte dela, pelo que permite maior número de desenvolvedores na criação de vírus informáticos com o objetivo de infectarem o sistema operacional Symbian. Entretanto, se existe maior número de desenvolvedores, também é possível haver maior número de amadores criadores da linguagem, de outra forma, por existir grande representação de telefones no mercado, traduzindo também maior número de presas virtuais. Na atualidade esse sistema operacional encontra-se em pouca expressão, visto que mercado internacional é mais procurados os dois grande gigantes da tecnologia móvel que é a

Apple e a Samsung representado os sistemas operacionais iOS e o Android. Sendo entre eles o mais seguro.

Resultados e Discussão

Os sistemas operacionais possuem a sua própria gráfica, a sua estrutura é elaborada consoante o seu desenvolvedor sem descorar algum padrão universal, cada sistema possui o seu protótipo, e essas características pode - lhes tornar fortes ou débeis aos ataques informáticos, por exemplo o sistema operacional Symbin apresenta uma característica similar segundo a análise encontrada podemos observar que os sistemas são criados com linguagem de programação muito conhecida e com maior facilidade de desenvolveres, estes sistemas permitiu maior número de programação de vírus informáticos no mercado. A facilidade de instalações de *softwares* ou aplicativos fora da loja dos dispositivos celulares, que maior parte transporta os vírus informáticos ocasionam uma vulnerabilidade e danificando os sistemas de arranque do dispositivo.

No entanto ao contrário o sistema operacional do *Windows Phone,* possui uma realidade diferente, são sistemas com uma estrutura robusta, possui uma proteção que não permite instalações fora da loja, para instalação de *software* maliciosos, no entanto essa característica lhe torna muito seguro porque não permite a transmissão de vírus de forma fácil, de outra forma não permite os desenvolvedores programarem os vírus devido os desconhecimento da sua linguagem de programação visto que a contaminação só acontece quando for o mesmo código fonte ou seu núcleo (*kernel*). O sistema operacional *Windows Phone 7* utiliza muito o sistema de métodos criptográficos de proteção. Essa característica impede inúmeros ataques informáticos no sistema operacional.

Os vírus do sistema operacional não são tão conhecidos mas, não podemos afirmar que não são atacados, mas também são vulneráveis ao vírus Ikee. O *iphone* não é tão vulnerável como os sistemas operacionais Symbian e o Android. No entanto fazer menção sobre o sistema operacional *iPhone* da *Apple*, possui uma característica que impede que programas ou alguns dispositivos afectam o sistema, porque é sabido que em telefonia móvel celular a tecnologia *bluetooth* é a forma mais veloz de transmissão de vírus informáticos e a *Apple* restringiu a transferência de aplicativos por essa tecnologia para outros dispositivos. A sua linguagem de programação não possui muitos desenvolvedores. Essas características lhe tornam menos susceptíveis a pragas informáticas.

Conclusão

Ao conhecer melhor os sistemas operacionais móveis celulares pode-se concluir que: as infecções por vírus informáticos em telefones móveis celulares, tem a ver com o sistema operacional, o seu núcleo (kernel), a tecnologia do telefone, e a linguagem de programação como afirma Martinelli (2008, p. 32) “Todo sistema operacional possui um núcleo chamado de *kernel* o qual delimita suas funções. Ele é um dos motivos que faz um vírus de celular não se espalhar facilmente a outros dispositivos, devido as diferentes versões e estrutura interna dos variados sistemas operacionais mobiles”.

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++ proveniente da 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.

Os sistemas operacionais em telefonia móvel celular, como o Android, *iPhone*, Symbian e *Windows Phone*, finalmente concluímos que, o sistema operacional *Windows Phone* 7 é o mais seguro do ponto de vista de segurança a ataques virtuais, porque é sabido que 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 são colocados inúmeros aplicativos maliciosos e não só.

Referências

Altermann, D. (2013). Como remover vírus do celular: Como remover vírus do Windows Phone? *Tech tudo.* Retrieved from http://www.techtudo.com.br/dicas-e-tutoriais/noticia/2012/08/como-remover-virus-do-celular.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, v. 7, n. 7, p. 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-seguranca-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-seguranca-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-linguagem-de-programacao-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. Retrieved from https://campusonline.esab.edu.br/campusonline/modulos/campus/index.cfm.

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-descoberto-por-usuario-do-reddit.htm.

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

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

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

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.

Fecha de envío:18/03/2019
Fecha de revisión:18/11/2019
Fecha de aceptación: 02/12/2019