UNIVERSIDADE FEDERAL DE ALAGOAS
INSTITUTO DE COMPUTAÇÃO
CURSO DE BACHARELADO EM SISTEMAS DE INFORMAÇÃO

JOSÉ FRANCISCO DA SILVA JUNIOR

CONFECÇÃO E AVALIAÇÃO DE UMA CARTILHA SOBRE A PREVENÇÃO E MITIGAÇÃO DE ATAQUES DE RANSOMWARES

MACEIÓ

2019

JOSÉ FRANCISCO DA SILVA JUNIOR

CONFECÇÃO E AVALIAÇÃO DE UMA CARTILHA SOBRE A PREVENÇÃO E MITIGAÇÃO DE ATAQUES DE RANSOMWARES

Trabalho de Conclusão de Curso submetido ao Curso de Sistemas de Informação do Instituto de Computação da Universidade Federal de Alagoas como requisito parcial para a obtenção do Grau de Bacharel em Sistemas de Informação.

Orientador: Prof. Lucas Benevides Viana de Amorim

Maceió

2019

JOSÉ FRANCISCO DA SILVA JUNIOR

CONFECÇÃO E AVALIAÇÃO DE UMA CARTILHA SOBRE A PREVENÇÃO E MITIGAÇÃO DE ATAQUES DE RANSOMWARES

Este Trabalho de Conclusão de Curso (TCC) foi julgado adequado para obtenção do Título de Bacharel em Sistemas de Informação e aprovado em sua forma final pelo Instituto de Computação da Universidade Federal de Alagoas.
Maceió, ____ de _____ de 2019.

_____

Prof. NOME COMPLETO DO COORDENADOR, Dr.
Coordenador do Curso de Sistemas de Informação

Banca Examinadora:

_____

Prof. NOME COMPLETO DO ORIENTADOR, Dr.
Orientador

_____

Prof. NOME COMPLETO DO MEMBRO DA BANCA, titulação.
Instituição

_____

Prof. NOME COMPLETO DO MEMBRO DA BANCA, titulação.
Instituição

AGRADECIMENTOS

A Deus por ter me dado saúde e força para superar os desânimos e às dificuldades que surgiram.

Ao professor Lucas, pelas orientações, paciência e compreensão durante a elaboração desse trabalho.

A todos que direta ou indiretamente fizeram parte da minha formação.

LISTA DE QUADROS

LISTA DE GRÁFICOS

LISTA DE ABREVIATURAS E SIGLAS

APP	Aplicativo
API	*Application Programming Interface*
EJA	Educação de Jovens e Adultos
PDF	*Portable Document Format*
SMB	*Server Message Block*
RSA	Rivest-Shamir-Adleman
RS	Redes Sociais
WPP	*Whatsapp*
URL	*Uniform Resource Locator*

RESUMO

Nos últimos anos, o Malware Ransomware, também conhecido como sequestrador digital, está se espalhando e fazendo mais vítimas pelo mundo. Muitas vezes, pela falta de conhecimento, as pessoas têm seus computadores ou dispositivos móveis invadidos e seus dados sequestrados, sem garantias de que serão devolvidos mesmo depois do pagamento de um resgate exigido. Então, o presente trabalho tem como objetivo desenvolver e testar uma cartilha com informações sobre Ransomware e como preveni-lo. Para tanto, foi desenvolvido uma pesquisa bibliográfica sobre a história dos Ransomwares, como ocorrem os ataques e como se previne. A partir disso, foi confeccionada uma cartilha usando quadrinhos onde são apresentadas conversações entre personagens sobre o Malware, observações, algumas manchetes de noticiários, bem como os links, que o leitor poderá usar para se aprofundar e conselhos. E, para fins de teste de eficiência do material, foi aplicado um questionário a dois grupos de pessoas, um dos quais, leu a referida cartilha. Além disso, foi feito um teste de hipóteses para melhor respaldar a conclusão do trabalho.

Palavras-chaves: prevenção, ransomware, sequestro digital, cartilha

ABSTRACT

In recent years, the Ransomware malware, also known as a digital hijacker, is spreading and making more victims around the world. Often, because of a lack of knowledge, people have their computers or mobile devices invaded and their data hijacked, with no guarantee that they will be returned even after payment of a required redemption. So, the present work aims to develop and test a booklet with information about Ransomware and how to prevent it. For this, a bibliographic research was developed on the history of Ransomwares, how the attacks occur and how it is prevented. From there, a booklet was created using in a comic book style where characters have a conversation about the malware, observations, news headlines and links are presented, which the reader can use to get more depth and advice. And, for purposes of testing the efficiency of the material, a questionnaire was applied to two groups of people, one of whom read the booklet. In addition, a hypothesis test was done to better support the completion of the work.

Keywords: prevention, ransomware, digital sequestration, primer

SUMÁRIO

1 INTRODUÇÃO

A internet, nos dias atuais, é um serviço acessado por muitas pessoas e se tornou essencial em suas vidas. A internet é usada para fazer compras, operações bancárias, contatos profissionais e pessoais, pesquisas, entre outras utilidades. Apesar de muitos precisarem da internet, nem todos estão capacitados para navegar de forma segura, o que é algo oportuno para os cibercriminosos.

1.1 MOTIVAÇÃO

Como a informação é algo que tem muita importância, deve-se ter muito cuidado para não ocorrer a perda de acesso a elas e nem sua interceptação para usos indevidos. O impacto advindo da perda de acesso às informações pode ser tão grande a ponto de causar prejuízos pessoais e profissionais.

Entre outras formas de acessar os dados alheios, os cibercriminosos utilizam os chamados códigos maliciosos, também conhecidos como Malwares. Dentre esses Malwares, será foco do presente trabalho o Ransomware, ou seja, o “sequestrador de dados”.

Os malwares do tipo Ransomware, invadem os dispositivos de usuários que navegam pela internet sem as devidas precauções, acessando sites afetados por esse código malicioso ou baixando arquivos ou softwares contaminados, inclusive anexos de e-mails não confiáveis. Além disso, a contaminação ocorre com o uso de dispositivos de armazenamento removíveis, como pendrives ou CDs. Após a contaminação, a ação desses softwares mal intencionados é bloquear o sistema operacional ou criptografar os arquivos. O que chama a atenção nesse tipo de ataque e ainda caracteriza esse malware como sequestrador de dados, é a exibição de uma interface ou pop up, com mensagem exigindo pagamento para a liberação do sistema ou dos arquivos. Para pressionar a vítima, alguns Ransomwares são programados com um temporizador e, a cada período de tempo, vão deletando arquivos até que o “resgate” seja pago. A depender do tipo de informação sequestrada, o usuário entra em desespero e, em muitos casos, contrata técnicos para recuperar os dados e muitos tentam sem sucesso. Essas tentativas frustradas

se devem à alta complexidade da criptografia usada no sequestro dos dados, o que a torna difícil de ser contornada, restando ao usuário pagar o “resgate”, mesmo sem ter a certeza de que seus dados serão liberados, ou perder seus dados.

Dado este contexto, propõe-se o presente trabalho como uma maneira de prover a conscientização dos usuários que lidam com computadores e dispositivos móveis, no que se refere a prevenção de ataques de Malwares do tipo Ransomware.

1.2 PROBLEMA

Devido à existência de pouco material didático e informativo sobre o Ransomwares para leigos, propõe-se um trabalho que tem como resultado uma cartilha informativa sobre o referido tipo de Malware. A cartilha deverá responder adequadamente:

- O que são Ransomwares e quais são os danos que podem causar a aparelhos informáticos?
- Quais procedimentos que um leigo pode adotar para evitar contaminação de seu(s) aparelho(s) informático(s) por Ransomwares?

1.3 HIPÓTESES

Diante do exposto, iremos testar a referida cartilha com um de dois grupos de pessoas voluntárias. Para fins de testes de hipóteses na fase de análise dos resultados, formalizamos as seguintes hipóteses nula e alternativa:

Hipótese Nula (H_0): Uma pessoa que consulta a cartilha, em média, não responderá melhor a um questionário com situações usadas por cibercriminosos para a contaminação de computadores e dispositivos móveis por Ransomwares.

Hipótese Alternativa (H_A): Uma pessoa que consulta a cartilha, em média, responderá melhor a um questionário com situações usadas por cibercriminosos para a contaminação de computadores e dispositivos móveis por Ransomwares.

1.4 OBJETIVO

O trabalho apresentará a avaliação da citada cartilha como método de conscientização e prevenção dos ataques de Malwares do tipo Ransomware. Assim, formalizamos o objetivo geral e os objetivos específicos.

1.4.1 Objetivo Geral

Propor e mostrar a eficácia de uma cartilha como instrumento de conscientização e prevenção dos ataques de Malwares do tipo Ransomware.

1.4.2 Objetivos Específicos

1. Estudar uma maneira eficaz de conscientização dos usuários quanto a ameaças, principalmente dos Ransomwares, por meio de um abordagem educativa, fornecendo informações sobre esses malwares, suas principais formas de ataques e como se faz a prevenção de maior parte deles;
2. Confeccionar uma cartilha para usuários de computadores e dispositivos móveis, que deverá servir para transmitir aos mesmos, de forma didática, informações necessárias para o uso mais seguro dos referidos aparelhos informáticos;
3. Testar a cartilha com dois grupos de pessoas diversas, onde um dos grupos consulta a cartilha e o outro não;
4. Discutir os resultados do questionário aplicado durante o teste da cartilha;
5. Concluir se a cartilha poderá ser usada como instrumento de conscientização e prevenção para usuários de computadores e dispositivos móveis, navegando ou não pela internet.

1.5 METODOLOGIA

O trabalho terá um caráter experimental, uma vez que a cartilha supracitada será testada com um grupo de 22 das 45 pessoas que participarão do experimento. O primeiro grupo terá contato com as informações da Cartilha, enquanto o segundo não. Ambos os grupos serão formados por pessoas com e sem facilidades no manuseio de tecnologias, mas que usam, no mínimo, smartphones. As pessoas têm graus de instrução variados, desde ensino fundamental incompleto a ensino superior completo.

Os dois grupos responderão a um questionário de situações sobre ataques de Malwares, principalmente do tipo Ransomwares.

A princípio, serão entregues cópias da cartilha para um dos grupos, que terá 05 dias para realizar a leitura e análise. Enquanto o outro grupo não terá nenhuma informação sobre o experimento até o dia do mesmo.

No dia do experimento, os participantes responderão ao questionário com situações típicas de engenharia social, de usos de dispositivos de armazenamento removíveis, navegação na internet em diversos sites, confiança no antivírus de seu aparelho, uso de e-mails e uso de softwares piratas e etc. O questionário contará com questões objetivas em que serão descritas situações relacionadas à segurança na rede onde cada uma culminará numa pergunta a respeito do que o usuário faria, ou seja, qual a alternativa o usuário acha mais adequada marcar diante da situação exposta na questão. Os participantes serão instruídos a marcar uma alternativa por questão.

Depois de respondidos, os questionários serão analisados a fim de se constatar se o grupo que consultou a cartilha responde melhor às situações do que o grupo que não consultou. Isso será exposto através de análise de gráficos com o desempenho dos grupos e teste de hipóteses, o que permitirá concluir sobre a validade ou não da hipótese alternativa, o que permitirá analisar a eficácia da cartilha.

1.6 ESTRUTURA

Adiante, o trabalho será dividido da seguinte forma: No Capítulo 2 abordaremos a definição de Ransomware, sua história, seus tipos e técnicas de prevenção. No Capítulo 3, abordaremos a contextualização do problema, ou seja, a falta de informação e de conscientização de muitos usuários de computadores e dispositivos móveis relativo aos Malwares, além da proposta e avaliação da cartilha. No Capítulo 4, será discutido o resultado da avaliação da cartilha para que, com o Capítulo 5, conclua-se o trabalho.

2 FUNDAMENTAÇÃO TEÓRICA

A internet, nos dias atuais, é uma rede acessada por muitas pessoas e se tornou essencial em suas vidas. Ela é usada para fazer compras, operações bancárias, contatos profissionais e pessoais, pesquisas, entre outras utilidades. Com isso, a sociedade se torna, com o passar do tempo, mais dependente dos computadores e das redes, devido aos benefícios oferecidos pela alta tecnologia que cresce a cada dia [2]. À medida que as vidas das pessoas se tornam cada vez mais digitais, elas armazenam dados importantes em seus aparelhos informáticos [16]. Apesar de muitos precisarem da internet, deve-se pensar que as pessoas não estão preparadas para usá-la, uma vez que muitas acham que não correm riscos, pois supõe que ninguém tem interesse em utilizar o seu computador ou smartphone que, entre os diversos aparelhos informáticos conectados à Internet, o seu dificilmente será localizado. É justamente este tipo de pensamento que é explorado pelos atacantes, pois, ao se sentir seguro, o usuário pode achar que não precisa se prevenir [22].

A rede mundial de computadores é algo relativamente novo para a maior parte dos usuários. Muitos desses usuários acessam a internet graças a popularização dos dispositivos móveis, cada vez mais acessíveis, ao barateamento de microcomputadores, as instituições de ensino, entre outros. Mas, a navegação na internet tem ficado cada vez mais perigosa, principalmente por causa engenhosidade dos chamados cibercriminosos.

Na maioria das vezes, os usuários são vítimas de Malwares por falta de preparo para navegar na internet. Ou seja, a falta de preparo, por exemplo, os leva a clicar em *links* ou abrir anexos de e-mail descuidadamente, o que pode ocasionar em acesso a sites falsos e contaminado com malwares [11].

Segundo dados do estudo Fraud Beat 2017, que elencou os principais malwares do ano, os ataques de phishing aumentaram 65% em 2016. Com base no estudo feito pela Easy Solutions, 97% das pessoas não sabem reconhecer um e-mail com conteúdo fraudulento e 30% deles acabam sendo abertos [20].

Muitos usuários navegam despreocupados pela internet, não atualizam os softwares, fazem uso de softwares piratas, não verificam arquivos com antivírus,

utilizam pendrives descuidadamente, são descuidados ao ver e-mails, são vítimas de golpes para roubo de dados pessoais (phishing), entre outros descuidos [12].

2.1 RANSOMWARES

O Ransomware é uma forma de código mal-intencionado ou malware que infecta um computador e se espalha rapidamente para criptografar os dados ou para bloquear aparelhos informáticos. Este malware torna os dados inacessíveis para os usuários e os atacantes exigem pagamento (resgate) desse usuário para que os dados sejam desencriptados [13]. Em outras palavras, o Ransomware foi projetado para gerar receita diretamente [16]. Além disso, em alguns casos, ocorrem ameaças de exposição de informações confidenciais do usuário para o público se o pagamento não for feito. Então, há três opções básicas a escolher: 1) tentar restaurar os dados a partir de um backup; 2) pagar o resgate; ou 3) perder os dados [14].

Muitas vezes, a primeira indicação de que ocorreu um ataque de Ransomware é uma janela de mensagem que se abre e o usuário não pode fechar, contendo instruções sobre como pagar o resgate [14].

Os usuários de computadores e dispositivos móveis podem se deparar com Ransomwares de várias maneiras: através de acesso, intencional ou não, a sites maliciosos ou comprometidos; abertura de anexos de e-mails, suspeitos ou não; executar programas obtidos de fontes desconhecidas ou instalados por outros tipos de malware já inseridos no computador ou dispositivo móvel; por meio de brechas de segurança decorrentes de sistema operacional ou programas desatualizados. Tais brechas são chamadas de vulnerabilidades.

Os cibercriminosos por trás dos Ransomwares estão constantemente inovando. Com mais dispositivos conectados a internet no mundo, outros Ransomwares aparecem em diversos tipos de dispositivos onde nunca foram vistos antes [16].

2.2 HISTÓRIA DOS RANSOMWARES

A origem do Ransomware ocorreu no final da década de 80 e, desse período até os dias de hoje, foi fortemente influenciado pelo desenvolvimento tecnológico, econômico e cultural [16]. A seguir, veremos uma breve cronologia da evolução dos Ransomwares, começando pela década de 80 até os dias atuais.

2.2.1 Década de 80

O primeiro malware com características de Ransomware de que se tem notícia foi o Trojan AIDS, também conhecido como PC Cyborg, em 1989. Foi criado pelo biólogo Joseph L Popp, participante de uma conferência da OMS sobre AIDS que ocorreu na época. Popp criou 20000 disquetes rotulados “AIDS Information – Introductory Diskettes”. Os disquetes foram distribuídos a instituições de investigação médica, principalmente sobre AIDS, que os recebiam em embalagens da PC Cyborg Corp., uma empresa falsa criada pelo referido biólogo. Ao acessar os disquetes, os computadores eram infectados e, após 90 inicializações, o Trojan AIDS iniciava sua ação, criptografando os arquivos e ocultando os diretórios e uma mensagem era exibida, informando a vítima de que o seu sistema voltaria ao normal depois que fosse enviado $189 para uma caixa postal no Panamá. O ataque consistia numa combinação de chave simétrica e um vetor de inicialização para criptografar os arquivos presentes nas máquinas infectadas. Algumas dessas instituições perderam até 10 anos de pesquisas [13] [23].

O Trojan AIDS, foi bem parecido com o Ransomware atual no que se refere criptografia dos arquivos do disco rígido e a extorsão baseado na exigência de pagamento para descriptografia [15].

2.2.2 De 2005 a 2009

O próximo Ransomware da história foi detectado em meados de 2005, foi o Ransomware GPCoder. Nesse ano, a Internet já era bastante usada pelo mundo, o

que ajudou na disseminação desse Ransomware. Os programadores melhoraram o método de encriptação, variando até uma Criptografia RSA mais complexa [1]. O GPCoder infectava computadores com Windows, copiava os arquivos e os criptografava, deletando os originais. Esse Ransomware usava criptografia forte RSA-1024, o que garantia insucesso na maior parte das tentativas de desbloqueio dos arquivos. Após o processo de criptografia, era exibida uma mensagem na tela inicial dos usuários, direcionando-os para um arquivo .txt salvo na área de trabalho, que continha instruções de como pagar o resgate, para o desbloqueio dos arquivos [5]. No mesmo ano, os antivírus começaram a detectar o GPCoder e removê-lo, indicando que os lucros foram relativamente baixos com esse ataque.

Em 2006, mais duas famílias de Ransomwares começaram a se espalhar, a Cryzip e a Archiveus. O ataque do Cryzip procurava arquivos com extensões específicas, entre as quais: .pdf, .xml, .txt, .tar, .rar e .jpg. Em seguida, colocava os arquivos, criptografados, em uma pasta compactada com senha [13]. O Archievus simplesmente criptografava tudo que encontrava na pasta Meus Documentos da vítima. A vítima ainda poderia usar o computador e qualquer arquivo armazenado em outras pastas, mas como a maior parte das pessoas colocava muitos de seus arquivos importantes na pasta Meus Documentos, ocorreram prejuízos na época [5].

Um outro Ransomware usado entre 2008 e 2009 foi o Fake AV, que consistia em falso programa antivírus. Ele aparentemente tinha a funcionalidade e aparência de software de segurança e realizava varreduras simuladas, encontrando grandes números de ameaças e problemas de segurança falsos no computador da vítima. O usuário, através de mensagens, era avisado o tempo todo sobre os problemas e que, para corrigí-los, teria de pagar uma taxa entre US$ 40 e US$ 100. No entanto, algumas vítimas do Fake AV optaram por remover o software, resultando em um menor retorno sobre investimentos para cibercriminosos [16].

O Fake AV foi considerado Ransomware por causa da tentativa de extorsão nas mensagens insistentes de problemas falsos, convidando o usuário a pagar pela correção dos mesmos ou remoção dos falsos vírus detectados. Pela definição, ele não se encaixa como sequestrador de dados ou de computadores.

2.2.3 De 2010 aos dias atuais

Em 2011, surgiu o WinLock Trojan cuja ação era a de impossibilitar o login no dispositivo. A funcionalidade desse Ransomware consistia em copiar o sistema de ativação do Windows e bloquear o acesso dos usuários, até eles comprarem uma chave de ativação. Para isso, era exibida uma mensagem na tela de ativação falsa que comunicava as vítimas que a conta delas do Windows precisava ser reativada por causa de fraude [5].

A maior parte dos WinLocks foram escritas em C++ e algumas em Visual Basic. A mensagem de pedido de resgate era exibida na tela num documento em HTML incorporado nos recursos do Trojan. Uma vez lançado, o Trojan.Winlock.3260, por exemplo, bloqueava o teclado, o que não permitia o uso de combinações como Ctrl + Alt + Del ou Ctrl + F4 [10].

Em 2012, outros Ransomwares como Reveton e o ACCDFISA começaram a se espalhar na internet. Eles exibiam o aviso de pagamento de multas por autoridades policiais [13]. O Reveton, ao infectar o computador, impedia que o usuário o acessasse e tipicamente exibia uma página de notificação supostamente enviada por órgão de segurança local, informando a vítimas que elas foram pegas fazendo uma atividade ilegal online e devem pagar uma multa. Para saber qual órgão de segurança tem jurisdição o usuário, o Reveton rastreava a localização geográfica da vítima. Assim, o usuário cujo computador foi infectado nos EUA recebia uma notificação do FBI, enquanto aquele cujo computador foi infectado na França recebia notificação da *Gendarmerie* Nationale (força policial militar subordinada ao Ministério da Defesa francês). Uma vez que um sistema está infectado com variantes Reveton, os usuários são solicitados a pagar através *UKash*, *PaySafeCard*, ou *MoneyPak*, que são métodos internacionais de pagamento em dinheiro, que perpetuam o anonimato e adequado para quem deseja comprar, pagar e jogar na Internet [25].

Em 2013, surgiu o Cryptolocker que, ao contrário de outros Ransomwares, ele não bloqueou o computador, apenas arquivos pessoais, como fotos e documentos. Esse Ransomware espalhou-se pela internet, principalmente através de e-mails falsos. Ele usava criptografia de RSA 2048 bits e exibia na tela dos computadores

das vítimas uma mensagem indicando que seus dados serão destruídos se você não pagar um resgate para obter a senha de liberação. O resgate era algo em torno de US $300 [6].

Descoberto em junho de 2014, o Ransom.Cryptowall criptografava arquivos no computador, fazendo uso da criptografia RSA de 2048 bits, e depois era exibida uma mensagem informando à vítima que seus arquivos tinham sido criptografados. A mensagem também continha instruções de como obter a senha para desbloquear os arquivos. Esse Ransomware foi distribuído principalmente através de spans, sites infectados, anúncios maliciosos ou outros tipos de malwares [31].

Os primeiros exemplos de Ransomwares para dispositivos Android apareceram em 2014 e copiaram o formato tipo “polícia”. O Sypeng, que infectou dispositivos através de uma falsa mensagem de atualização do Adobe Flash, bloqueava a tela e exibia uma mensagem falsa do FBI que exigia o pagamento de multa de U$ 200, em MoneyPacks, o mesmo que fazia o Reveton. O Koler era um Ransomware semelhante, conhecido por ser um dos primeiros exemplos de worm Ransomware. Ele enviava automaticamente uma mensagem para todos os contatos da lista de um dispositivo móvel infectado, com um link de download para o referido Malware. Além disso, exibia mensagens falsas de órgãos de segurança, para enganar a vítima, mencionando que a mesma deveria pagar uma multa por atividade ilegal online, para o dispositivo ser liberado [5].

No final de fevereiro de 2015 foi descoberto o Teslacrypt ransomware, que chamou atenção por atacar, além de arquivos comuns, como documentos, imagens e vídeos, arquivos relacionados a jogos. Ou seja, depois que o computador era infectado, o referido Malware verificava todas as unidades, criptografava arquivos e exibia uma mensagem de resgate informando a vítima para instalar o navegador Tor e efetuar o pagamento através de um site no domínio do referido navegador [32].

Em fevereiro de 2016 surgiu o Locky Ransomware, que infectou vários computadores e criptografou, entre outros arquivos, vídeos, imagens e arquivos do Microsoft Office. Esse Ransomware criptografava os arquivos e colocava a extensão .locky. Após a criptografia, aparece a mensagem instruindo sobre o pagamento do resgate para a liberação dos arquivos. Nessa época, os clientes da empresa de energia espanhola Endesa foram vítimas depois de terem sido infectados com um

ataque de phishing que tinha a identidade da empresa [6].

Em março de 2016, surgiu o KeRanger, primeiro Ransomware para Mac OS X, que foi baixado por mais de 6.000 usuários via BitTorrent . Esse Malware tinha um certificado válido de desenvolvedor Apple e conseguia passar pelo GateKeeper. Ele tem comportamento semelhante àqueles destinados ao Microsoft Windows [34] [35].

Para fazer pressão psicológica, algumas telas de bloqueio de Ransomwares até exibiam um contador e informava que, se o pagamento não for feito até tal hora, todos os arquivos serão deletados. Um ransomware chamado *Jigsaw* (inspirado nos filmes *Jogos Mortais*), identificado também nesse ano de 2016, agia assim: a vítima tinha 72 horas para efetuar o pagamento; a cada hora, uma parte dos arquivos era deletada para aumentar o senso de urgência [36]. Uma vez instalado, o Ransomware Jigsaw examinava o sistema a procura de certas extensões para encriptar os arquivos. Normalmente ele atingia arquivos com as seguintes extensões:

gif, .png, .bmp, .pdb, .sql, .php, .asp, .swf, .xml, .ppsm, .asx, .mpg, .wmv, .vob, .m4u, .xlsb, .raw, .png, .java, .jar, .class, .doc, .docx, .ppt, .xpm, .zip, e outros. Depois alterava os nomes dos seus ficheiros e adiciona-lhes uma extensão .fin para que se tornem .gif.fun, .png.fun, etc [37].

Em maio de 2017, surgiu o Ransomware WannaCryptor (WannaCry), responsável por um dos maiores ciberataques da história, infectando computadores em diversos países. Esse Malware, que possui a característica de auto replicação, usou a ferramenta (exploit) EternalBlue para explorar o protocolo de compartilhamento SMB do Microsoft Windows para se disseminar nas redes de computadores. A empresa Microsoft alegou, na época do ataque, que já havia, desde março de 2017, uma atualização para o Windows, a MS17-010, que corrigia a referida vulnerabilidade, protegendo os computadores de ataques que pudessem se aproveitar dessa falha. Entretanto, muitos usuários ainda não haviam instalado a atualização ou usavam versões antigas do Windows, que não recebiam mais atualizações. O Wannacry criptografou arquivos de documentos como: imagens, vídeos, textos, etc e, para tê-los de volta, a vítima teria de pagar, no mínimo, US$ 300 [8] [27].

O Petya Ransomware, cujas primeiras versões surgiram em 2016, funcionava criptografando alguns setores-chaves do disco rígido, especialmente a tabela de Arquivos Mestre impedindo que o sistema Windows iniciasse e que qualquer software acessasse a lista de arquivos no disco. As versões mais atuais desse Ransomware exibem a mensagem com pedido de resgate logo que o computador é ligado [9]. Esse Malware se aproveitou da mesma vulnerabilidade do Windows usada pelo WannaCry [5].

Em setembro de 2017, surgiu o Bad Rabbit Ransomware que infectou computadores de várias partes do mundo, principalmente Rússia e Ucrânia. A infecção ocorreu através de uma mensagem de atualização do software Adobe Flash Player, onde os usuários que clicaram no botão “instalar” tiveram o seu computador infectado pelo referido Ransomware, que se espalhou rapidamente por redes internas e externas através do serviço SMB, como o WannaCry e o Petya. Após a infecção, esse Malware criptografava os arquivos do computador e adicionava a extensão .encrypted. Então, uma mensagem pop-up surgia, com um contador regressivo para pressionar a vítima a pagar pelo resgate mais rápido. O resgate exigido era de 0,05 Bitcoins, cerca de US$ 280 na época [41].

2.3 TIPOS DE RANSOMWARES

Existem dois tipos de Ransomwares: o Crypto e o Locker. Eles são criados para impedir o acesso a algo importante para o usuário em seu equipamento informático, liberando apenas após o pagamento de um resgate. Apesar dos objetivos serem semelhantes, cada tipo de Ransomware tem abordagens bastante diferentes.

Os Ransomwares do tipo Crypto ou Crypto-Ransomware, são aqueles criptografam arquivos. Depois da infecção, um típico Crypto-Ransomware procura discretamente e criptografa arquivos. O objetivo é ficar oculto até que ele encontre e criptografe todos dos arquivos importantes da vítima. Quando, então, a vítima é apresentada a uma mensagem do malware que informa que seus arquivos foram criptografados, oferecendo-os de volta após o pagamento de resgates bastante caros [16]. Em meados de 2006 a família GPcoder começou a evoluir e isso indica

claramente a era do crypto Ransomware [13].

Em 2011, emergiu uma nova forma de Ransomware. O WinLock Trojan é considerado o primeiro exemplo do que se tornou conhecido como “Locker” Ransomware. Em vez de criptografar arquivos no dispositivo da vítima, simplesmente impossibilitava o login no dispositivo [5].

Esse tipo de Ransomware muitas vezes se disfarça como autoridade policial e alega emitir multas aos usuários por supostos delitos ou atividades criminosas para pressionar a vítima a pagar o resgate. O Ransomware Locker pode ser particularmente eficaz em dispositivos com opções limitadas para os usuários interagirem, como é o caso de alguns dispositivos portáteis e outros na área da Internet das coisas (IoT), onde milhões de dispositivos conectados poderiam potencialmente estar em risco com este tipo de Ransomware. Como esse malware podia ser potencialmente removido para restaurar um computador para algo perto do seu estado original, isto faz o Ransomware do tipo Locker menos eficaz na extorção em comparação com o seu parente mais destrutivo, o Crypto-Ransomware [16].

2.4 PRÁTICAS DE PREVENÇÃO

O Ransomware, como já visto, é uma ameaça que causa inacessibilidade aos arquivos ou computadores e dispositivos móveis. Para evitar ser vítima de um ataque desses, faz-se necessário certificar-se da confiabilidade dos sites onde se baixa arquivos e manter-se atento ao navegar na internet.

Muitos usuários não estão conscientes da necessidade de criar *Backups* para proteção contra falhas no disco rígido ou a perda ou roubo do computador, muito menos um possível ataque Crypto-Ransomware. Isso pode ser porque os usuários não têm o know-how ou não percebem o valor dos dados até que eles sejam perdidos. Configurar um processo de backup efetivo requer algum trabalho e disciplina, por isso não é uma proposta atraente para o usuário médio [16].

Contra Ransomwares, é melhor prevenir do que remediar, então, vejamos com detalhes a seguir, algumas medidas a serem adotadas para evitar a infecção inicial por Ransomwares.

2.4.1. Boas Práticas de Navegação

Nem todos os usuários se preocupam quando se trata de navegação na rede mundial de computadores. O caminho mais fácil e barato para obter uma informação ou documento na internet nem sempre é seguro. Então, é necessário tomar cuidado ao acessar sites ou e-mails desconhecidos, sempre tendo em mente que Ransomware é algo real, e qualquer um pode ser vítima [7]. Além disso, o usuário deve ser cuidadoso ao clicar em links pela internet [4]. Então, caso haja suspeita ou desconhecimento de sites, links ou e-mails, se informar antes de acessar ou não acessar. Uma maneira de se informar a respeito de sites e links é submetê-lo ao serviço da web chamado VirusTotal, que analisa gratuitamente arquivos e URLS, verificando se há vírus, worms, cavalos de tróia, entre outros [29]. Ou seja, basta colocar o endereço que se quer acessar e o referido serviço fará a análise para a detecção de Malwares. Caso haja a detecção de Malwares, é só não acessar.

2.4.2. Ter Antivírus e Programas Atualizados

Com novas ameaças surgindo constantemente, além de instalar um bom antivírus nos computadores e dispositivos móveis utilizados, é importantíssimo manter os programas atualizados.

Os antivírus atuais, protegem automaticamente a navegação na internet, avisando sobre sites maliciosos ou suspeitos, avisam quando um download de aplicativos ou arquivos é suspeito, fazem varreduras periódicas no computador para detectar malwares e, em alguns casos, vulnerabilidades, entre outros recursos.

2.4.3. Instalar um Firewall

Um Firewall tem, entre suas principais vantagens, a característica de proteger as informações. Muitos antivírus já vem com firewall, que impedem maioria dos acessos maliciosos a computadores e dispositivos móveis mas, em especial para empresas, é necessário a montagem de um firewall corporativo, para proteger, por

exemplo, informações relacionadas aos empregados e aos clientes de acessos não autorizados. Com esse tipo de ferramenta instalada numa rede, fica muito mais difícil atacantes entrarem num computador ou dispositivo móvel e sequestrar os dados.

2.4.4. Fazer Backup na nuvem ou Hds Externos

De modo geral as informações são valiosas demais para ficarem exclusivamente em unidades físicas, principalmente as de uma empresa. É por isso que uma boa gestão das informações e principalmente os *Backups* são essenciais atualmente. Então, uma das soluções é o armazenamento na nuvem. Ou seja, as informações podem ser armazenadas em repositórios como o Google Drive ou OneDrive, por exemplo. Com isso, as informações são mantidas seguras em datas centers e acessadas pelo usuário em qualquer computador ou dispositivo móvel conectado a internet.

Outra solução para o armazenamento seguro das informações é o disco rígido (HD) externo, onde o usuário poderá colocar as informações, atualizadas constantemente, e guardar em local seguro.

Em caso de ataque de Ransomware, o usuário poderá formatar o computador e restaurar os arquivos a partir dos HDs externos ou da nuvem.

2.4.5. Usuário Bem Informado

De nada adianta as informações de prevenção anteriores se o usuário for desinformado sobre as ferramentas informáticas que utiliza associadas a navegação na internet. Ou seja, o conhecimento é a melhor forma de prevenção contra qualquer malware, principalmente o Ransomware. Recomenda-se não menosprezar tal risco e não esperar se tornar vítima de cibercriminosos para adotar medidas de segurança para as informações.

É importante controlar quem acessa os aparelhos informáticos [24]. O controle pode se dar ministrando informações de segurança para quem for usar seja uma rede doméstica ou corporativa, principalmente quando se tratar de crianças, adolescentes ou pessoas leigas em relação a navegação na internet.

3 CARTILHA DE PREVENÇÃO E MITIGAÇÃO DE RANSOMWARES PARA LEIGOS

Este capítulo discorre a respeito da construção e avaliação da Cartilha de Prevenção e Mitigação de Ransomwares para Leigos. A proposta da cartilha surgiu devido a pouco material didático e informativo existente sobre o assunto para leigos. Nesse contexto, a proposta da construção da cartilha se faz útil no que tange a ser mais uma ferramenta a auxiliar na prevenção de Ransomwares, principalmente para as pessoas leigas, que fazem uso de computadores e dispositivos móveis para diversos fins.

De forma geral, usar um computador ou dispositivo móvel atualmente não é uma atividade simples e, ao mesmo tempo, todos são obrigados a entender um pouco de tecnologia, seja em empresas ou ao conversar com os filhos em casa. Então, a cartilha foi escolhida como produto desse trabalho porque fornece informações em linguagem adequada para a compreensão, esclarecendo aspectos técnicos dos procedimentos a serem adotados, podendo auxiliar na minimização das infecções, de computadores e dispositivos móveis, por Ransomware bem como outros Malwares.

Essa iniciativa poderá auxiliar, também, o desenvolvimento de uma cultura de uso seguro da tecnologia, visto que não há como o usuário doméstico controlar as ameaças às suas informações, mas sim as vulnerabilidades de seus dispositivos. Para isso, é necessário adotar medidas de segurança práticas, procedimentos e mecanismos para a proteção dos referidos dispositivos e, por consequência, suas informações.

3.1 ELABORAÇÃO DA CARTILHA

Frente a problemática dos Ransomwares, e a poucos materiais didáticos que visem auxiliar sua compreensão e orientação para o público leigo, e tendo em vista a importância desse entendimento, buscou-se reunir informações necessárias para a compreensão de processos de infecções de computadores e dispositivos móveis por Ransomwares, bem como as consequências de sequestros de informações

pessoais e/ou profissionais por parte do referido Malware para, a partir daí, confeccionar a Cartilha de Prevenção e Mitigação de Ransomwares para Leigos (Apêndice A). O referido material é composto por ilustrações, em forma de estórias em quadrinhos, com diálogos entre as personagens sobre Ransomwares e prevenção, bem como pequenos textos explicativos, formulados de modo a ser compreendido por pessoas não técnicas em informática ou com pouco conhecimento nessa área.

Para o desenvolvimento da cartilha, utilizou-se como base teórica os materiais técnicos usados na confecção do presente trabalho, bem como as informações de blogs e vídeos sobre o assunto.

3.2 AVALIAÇÃO DA CARTILHA

A avaliação da cartilha foi feita mediante a aplicação de um questionário (Apêndice A) de 26 questões. O questionário foi aplicado para dois grupos de pessoas. O primeiro grupo, que denominaremos de G1, de 22 pessoas, leu as informações da Cartilha, enquanto o segundo, que chamaremos de G2, de 23 pessoas, não leu a cartilha. Ambos os grupos foram formados por pessoas diversas, com e sem facilidades para manuseio de tecnologias, mas que, no mínimo, possuem computador e/ou smartphone. Essa forma de testar a cartilha serviu para verificar se ela cumpriu com seu propósito de ferramenta informativa, o que significou testar as hipóteses colocadas na introdução do presente trabalho. Então, detalhando o propósito das questões do questionário, temos: com as questões de 1 a 5 a pretensão foi caracterizar o usuário no que se refere a grau de instrução, se possui cursos de informática e se possui computadores ou dispositivos móveis; com as questões de 6 a 12, a pretensão é analisar as alternativas respondidas frente a situações de administração de contas de e-mail e redes sociais, no que se refere a abertura e compartilhamento de arquivos e ao cadastro de suas senhas nesses serviços; da 13 a 21 a pretensão é analisar as alternativas respondidas frente a situações alguns hábitos de navegação do usuário, inclusive cadastros em sites, que serve para testar a conscientização dos respondentes frente as situações apresentadas; e, por fim, de 22 a 26 a pretensão é analisar as alternativas

respondidas frente a situações de aquisição programas e aplicativos de fontes confiáveis ou não confiáveis, de manter ou adquirir aplicativos desatualizados e manter ou não arquivos pessoais seguros. Nessas últimas questões, pretende-se verificar, diante da análise, se as respostas dos usuários culminam em deixar o computador ou dispositivo móvel vulnerável a ataques de Ransomwares, e os arquivos pessoais sem cópias de segurança.

Os grupos G1 e G2 tinham jovens e adultos, com idades que variam entre 15 e 70 anos, entre os quais se destacam professores, estudantes, domésticas, pedreiros etc, o que caracteriza que os respondentes foram pessoas comuns e não técnicas, ou seja, pessoas para os quais é destinada a cartilha.

Será apresentado, no próximo capítulo, os gráficos e análises das respostas dos questionários.

4 RESULTADOS E DISCUSSÕES

Para a análise e discussão do questionário, foram usados gráficos de estilo barras verticais e pizza, com informações numéricas percentuais. O primeiro estilo de gráfico nos permitiu abordar várias questões de mesma categoria e o segundo tipo, foi adequado para fazer comparativo das alternativas de duas das questões.

Vamos considerar G1, como o grupo de pessoas que leram a cartilha, e G2, o grupo de pessoas que não leram.

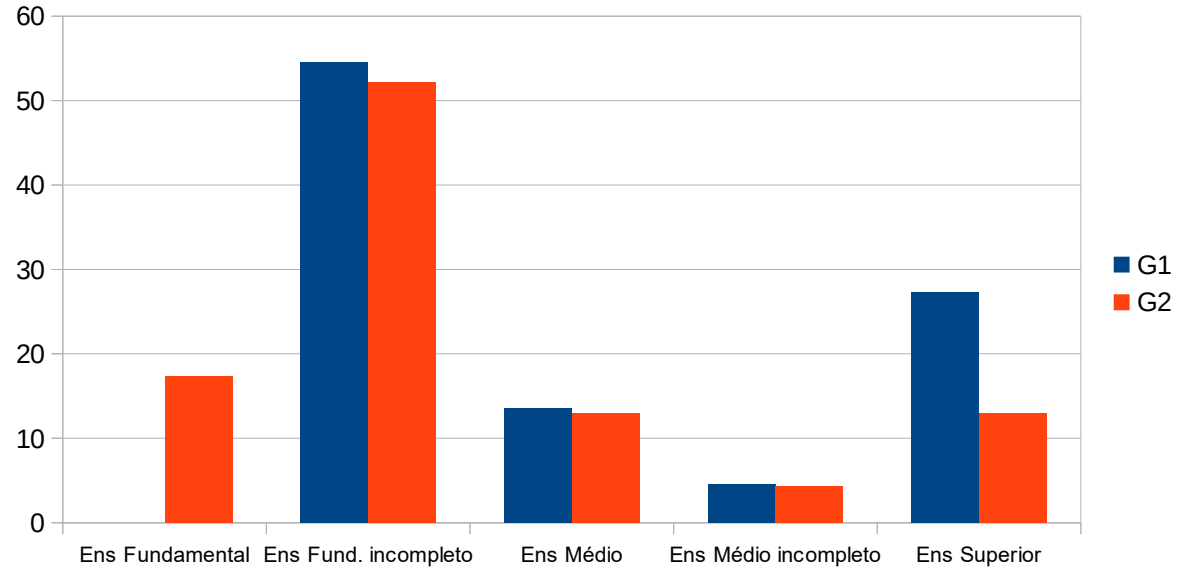
A análise foi dividida em:

- níveis de escolaridade dos respondentes;
- aparelhos informáticos que possuem;
- caracterização dos respondentes no que se refere cursos de informática, como adotam senhas para os serviços de internet e se atualmente clicam em links de propagandas quando navegam na internet;
- ações adequadas relativos a recepção de mensagens de e-mails de desconhecidos ou bancários;
- ações adequadas relativas a acessos a páginas da internet, a acesso e compartilhamento de links no *Whatsapp* ou redes sociais;
- ações adequadas relativas a adotar a mesma senha para redes sociais, e-mails e cadastros na internet;
- ações adequadas quanto a cadastros em sites;
- ação adequada quanto a aquisição de aplicativos;
- ação adequada quanto a *Backups* dos arquivos pessoais ;
- ações adequadas relativos posse de aplicativos obsoletos e, por fim,
- uma análise comparativa e qualitativa das respostas dos respondentes de G1 e G2 em relação ao grau de escolaridade.

Por fim, foi feito o teste das hipóteses propostas no início desse trabalho, onde foi aplicado o Teste de Wilcoxon, por se tratarem de dados Qualitativos Ordinais.

Nos primeiros gráficos temos os níveis de escolaridade dos respondentes do questionário.

Gráfico 1 – Níveis de escolaridade dos respondentes

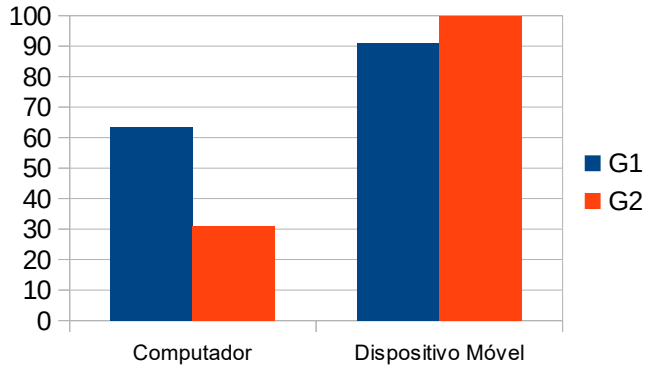


Fonte: Próprio autor

Percebe-se no gráfico 1 que a maioria dos respondentes tinha nível de escolaridade fundamental incompleto. Mais especificamente, a maior parte dos respondentes cursa o 2º segmento do ensino fundamental de EJA (Educação de Jovens e Adultos), de uma Escola da Prefeitura de Maceió.

Em seguida, temos o gráfico 2, de caracterização de ambos os grupos quanto aos equipamentos informáticos que possuem.

Gráfico 2 – Dispositivos informáticos que os respondentes possuem

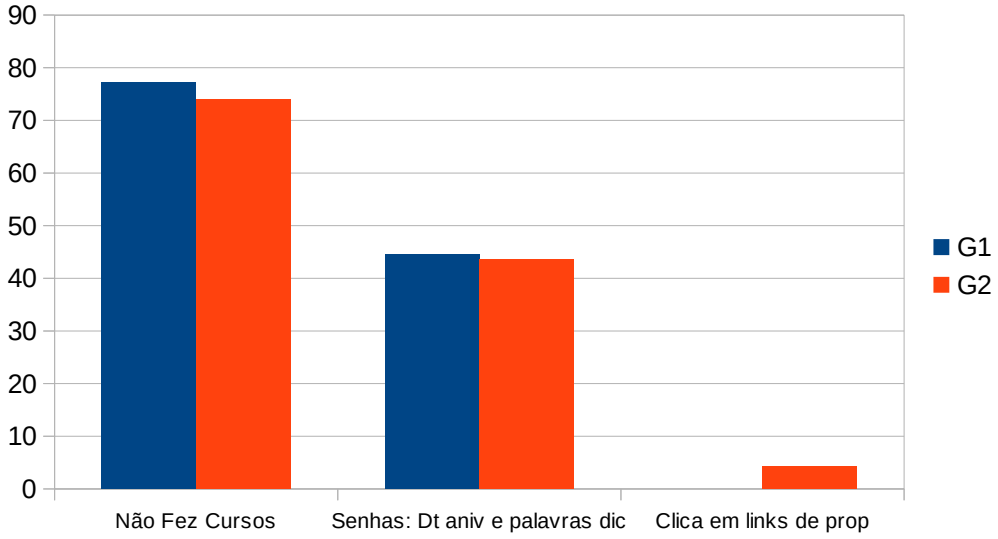


Fonte: Próprio autor

Nesse gráfico, temos que a maioria dos respondentes possui dispositivos móveis e alguns, computador, indicando que têm experiência no uso principalmente

dos primeiros aparelhos citados.

Gráfico 3 – Conhecimentos formais e alguns hábitos

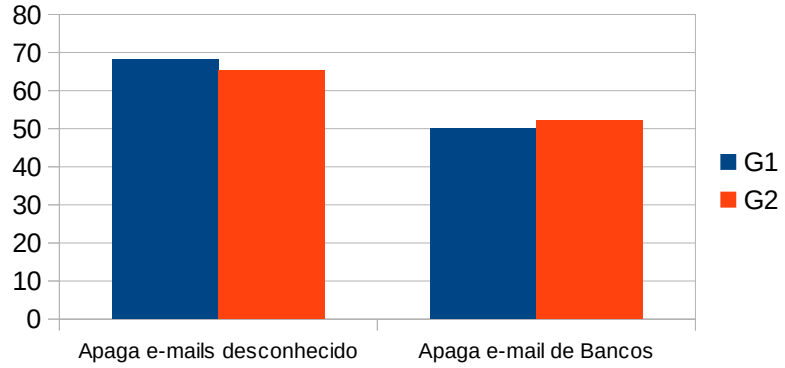


Fonte: Próprio autor

No gráfico 3, observa-se que em ambos os grupos, pouquíssimas pessoas fizeram cursos de informática, caracterizando, assim, que a maioria obteve conhecimentos de manuseio dos aparelhos através de terceiros e/ou intuitivamente. Alguns hábitos como os de usar nomes comuns ou datas de aniversário nas senhas é presente em quase 50% dos respondentes em ambos os grupos, indicando que já existe uma certa consciência da maioria na adoção de senhas. Além disso, temos um número expressivo de respondentes que não clicam em links de propagandas pela internet.

No gráfico 4, estão representados as crenças de G1 e G2, quanto às situações descritas. Nesse caso, percebe-se que maioria acredita que apagar e-mails de desconhecidos ou de Bancos é a melhor ação, indicando que a cartilha não impactou significativamente devido aos respondentes já possuírem hábitos defensivos.

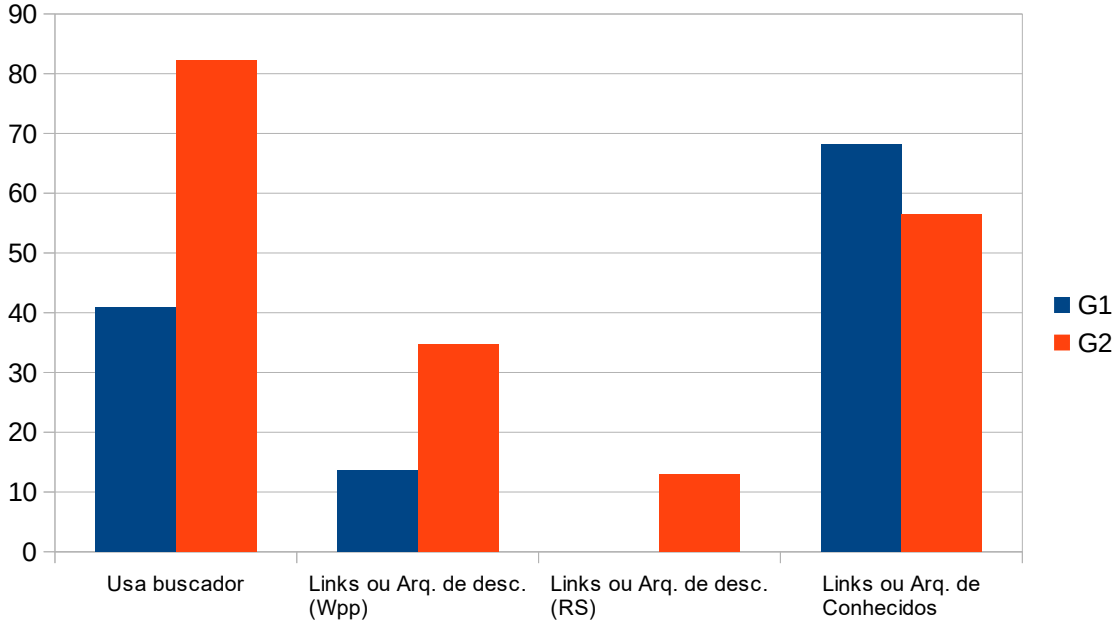
Gráfico 4 – Ações adequadas sobre e-mails desconhecidos ou de Bancos



Fonte: Próprio autor

O gráfico 5, nos permite analisar ações adequadas no que diz respeito a uso ou não de ferramentas de busca para acessar sites e compartilhamento de arquivos de conhecidos ou desconhecidos por *Whatsapp*(Wpp) ou Redes Sociais(RS).

Gráfico 5 – Uso de buscadores e Compartilhamento de arquivos



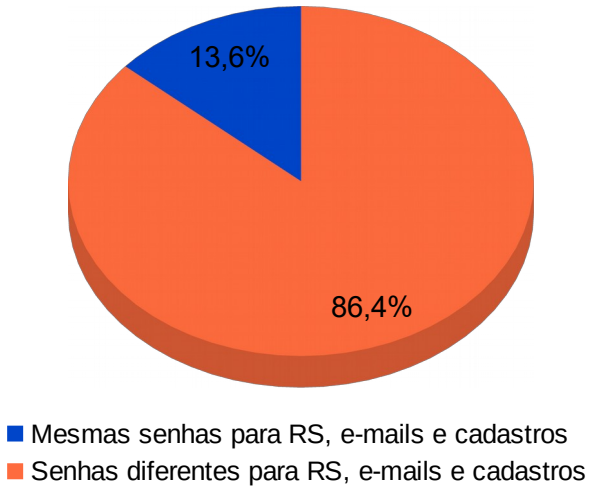
Fonte: Próprio autor

A respeito de acesso a sites, houve uma porcentagem maior de respondentes de G2 em relação a G1 que acreditam ser melhor acessar sites por buscadores e não digitando o endereço na barra de endereços do navegador. Sabe-se que pelos buscadores tem-se a possibilidade de o resultado das pesquisas aparecerem links para sites falsos ou contaminados por malwares. Para essa questão, as informações

da cartilha impactaram positivamente nas respostas de G1.

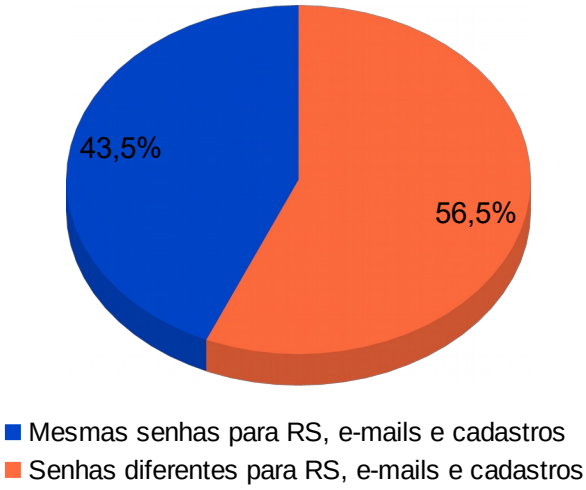
Sobre abertura e compartilhamento de links e arquivos de desconhecidos em *Whatsapp* ou Redes Sociais, acredita-se que as informações da cartilha influenciaram levemente as respostas, uma vez que tivemos uma porcentagem bem menor de G1, em relação a G2. Mesmo assim, quando se trata de links e arquivos de pessoas conhecidas, maioria dos dois grupos abrem e compartilham. Isso significa que há uma confiança das pessoas no que vem de origem conhecida. Mas isso ainda é perigoso, pois um conhecido desinformado pode compartilhar vídeos ou imagens contaminadas por Malwares ou links que levem a sites falsos, devido a alguma propaganda falsa ou, até mesmo a conta de RS pode ter sido hackeada e estar disseminando arquivos contaminados por Malwares. Nesse último caso, a cartilha não conscientizou o suficiente o grupo que a leu.

Gráfico 6 – Adoção de senhas (G1)



Fonte: Próprio autor

Gráfico 7 - Adoção de senhas (G2)



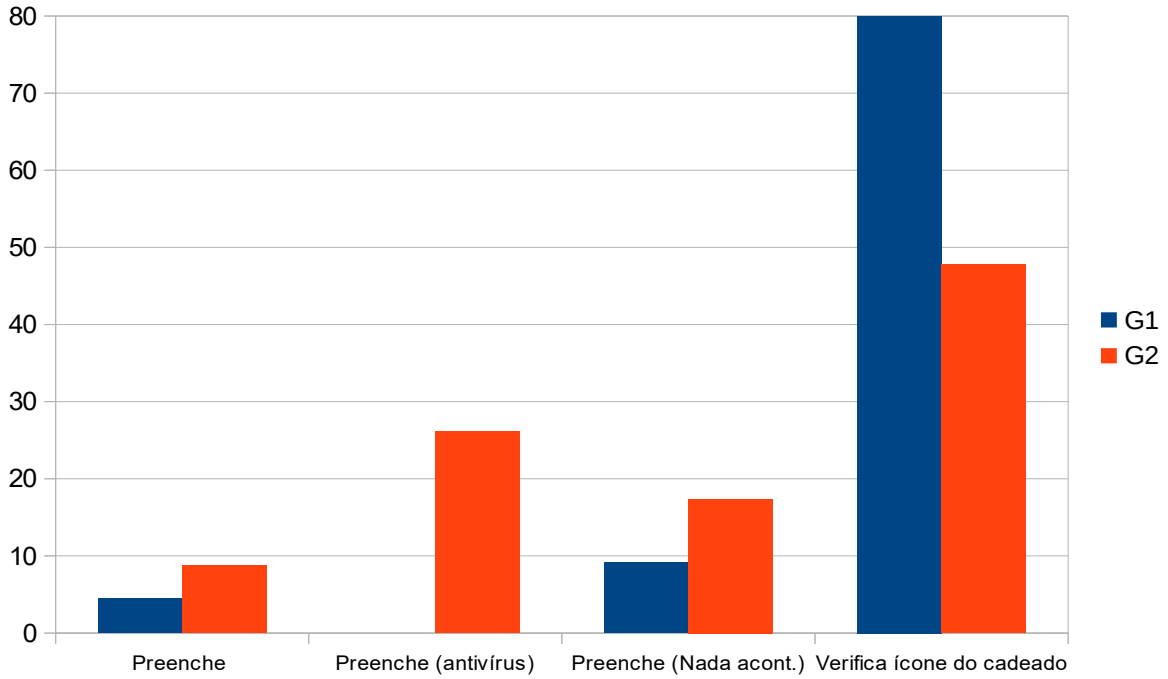
Fonte: Próprio autor

Referente a adoção de senhas para RS, cadastros em sites e e-mails, conforme o gráfico 6 e gráfico 7, uma porcentagem razoavelmente maior de G2 em relação a G1, acha que deve adotar as mesmas senhas, para facilitar e não ter de guardar tantas senhas ou não acharem que isso tem um impacto na segurança de seus dados. Para esse questionamento, temos que ainda há um descaso relacionado a senhas de cadastros, o que pode facilitar a quebra dessas senhas e invasão de contas, com consequente apropriação indevida de dados e até uso indevido de contas de e-mail para proliferação de Malwares. Para esse questionamento, houve um impacto razoável das informações da cartilha na opinião de G1.

Quando questionados a respeito de cadastros em sites, onde tem que colocar dados como número de CPF, de identidade e endereço, a maioria dos respondentes de G1, acreditam que devem verificar se a página do cadastro possui o ícone do cadeado na barra de endereços, caso contrário, procuram outro site. Já os respondentes de G2, pouco menos da metade verifica, ou tem conhecimento ou desconsidera o ícone do cadeado, além de uma parte acreditar ser adequado finalizar o cadastro, confiando que seu equipamento tem antivírus e nunca ocorreu nada em outros cadastros que tenham feito. Então, uma maioria significativa dos respondentes que leram a cartilha ficaram cientes que o ícone do cadeado traz informações de segurança e autenticidade de um site, indicando uma contribuição a

mais para a segurança dos dados desses usuários. Essa situação é analise do gráfico 8.

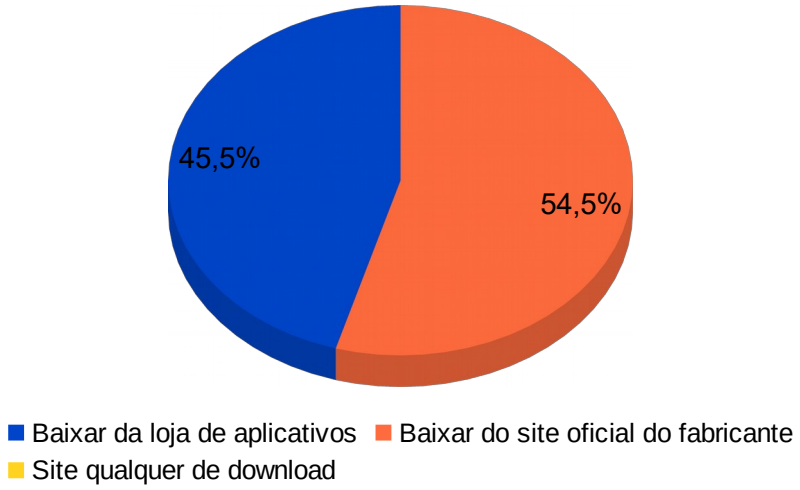
Gráfico 8 – Preenchimento de cadastro em sites



Fonte: Próprio autor

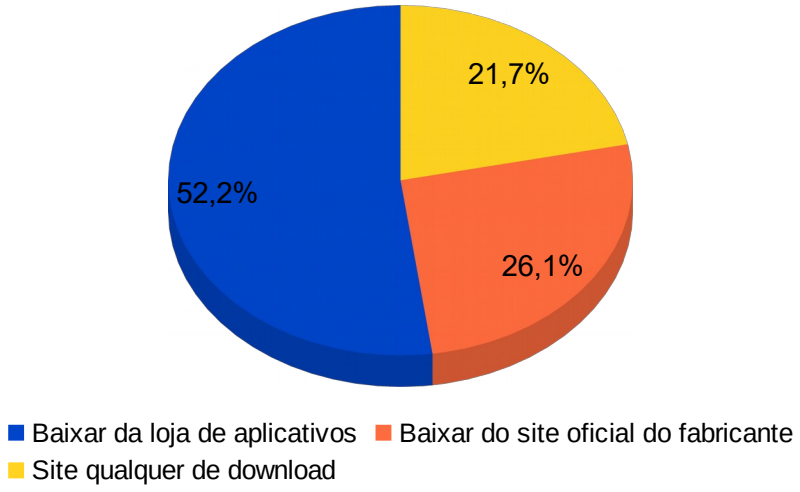
Quanto a adquirir aplicativos para seus dispositivos informáticos, pode-se concluir que, devido aos percentuais próximos dos respondentes de G1 e G2, já há a crença de que baixar de sites oficiais ou da loja de aplicativos é mais seguro. Entretanto, no gráfico relativo a G2, destaca-se um percentual de pessoas que acreditam ser adequado baixar aplicativos de sites quaisquer, o que pode acarretar em downloads de aplicativos contaminados por Malwares. Tal análise refere-se aos gráficos 9 e 10:

Gráfico 9 – Baixar aplicativo para computador ou dispositivo móvel (G1)



Fonte: Próprio autor

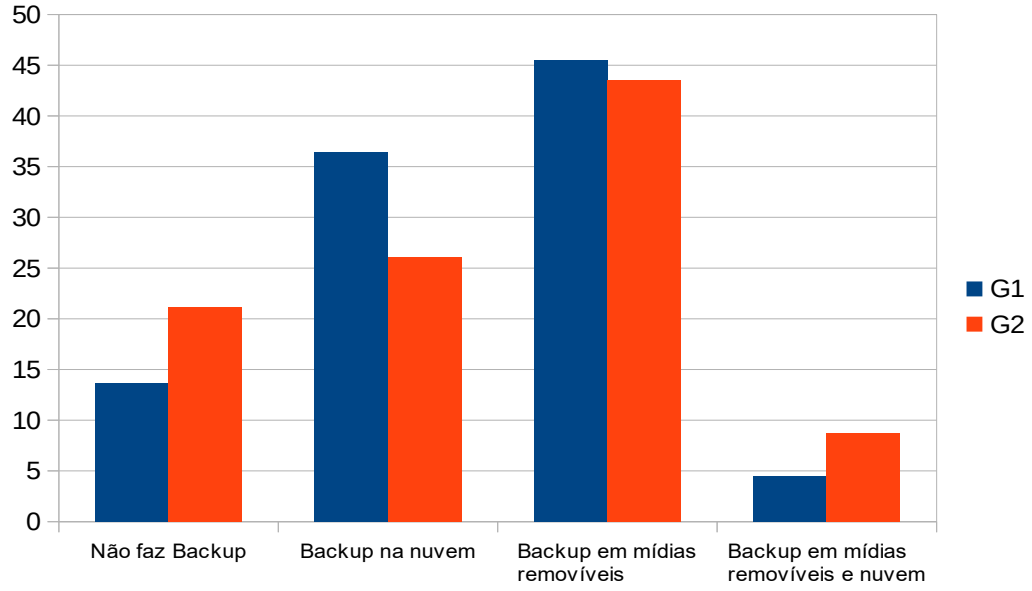
Gráfico 10 - Baixar aplicativo para computador ou dispositivo móvel (G2)



Fonte: Próprio autor

Quanto aos arquivos importantes armazenados em computador ou dispositivo móvel, tais como: fotos e vídeos de melhores momentos, músicas, etc, maioria dos respondentes dos dois acredita que deve fazer cópias de segurança em repositórios na internet ou pendrives e Hds externos. Em ambos os grupos, grande parte dos respondentes confiam em mídias removíveis. Nesse caso, os respondentes de G1, responderam com a consciência de acreditar que efetuando *Backups* estarão protegendo seus arquivos de ataques de Ransomwares, evitando perda dos arquivos ou prejuízos para reavê-los. Esses dados são análise do gráfico 11:

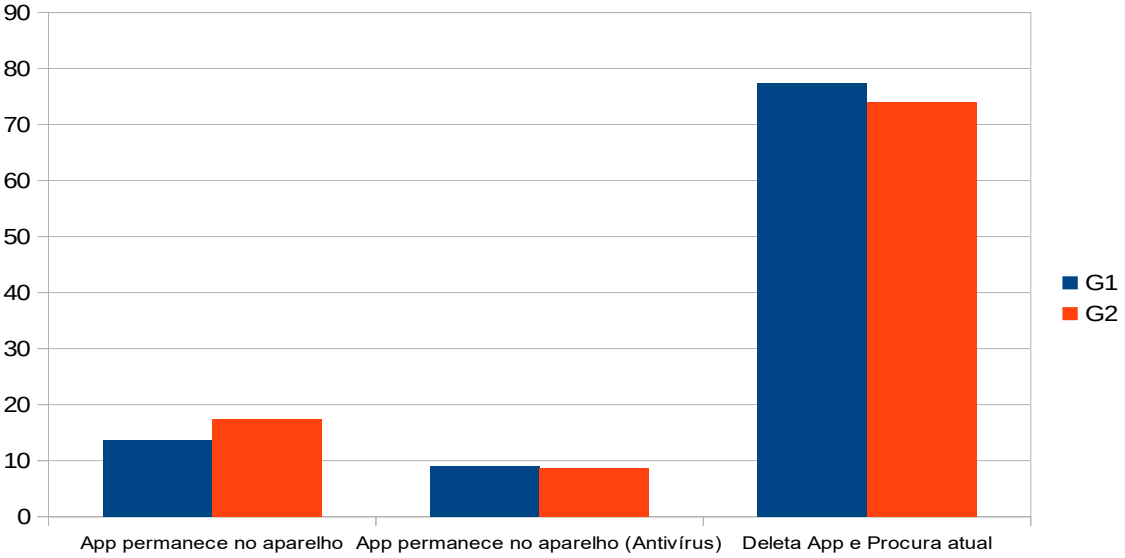
Gráfico 11 – Cópias de segurança de arquivos pessoais



Fonte: Próprio autor

O gráfico 12, mostra que houve percentuais próximos para G1 e G2, indicando que já há uma crença de que é adequado descartar aplicativos obsoletos dos dispositivos informáticos. Com isso, há menos possibilidade de serem atacados por Malwares que exploram vulnerabilidades de programas obsoletos.

Gráfico 12 – Aplicativos obsoletos no computador ou dispositivo móvel

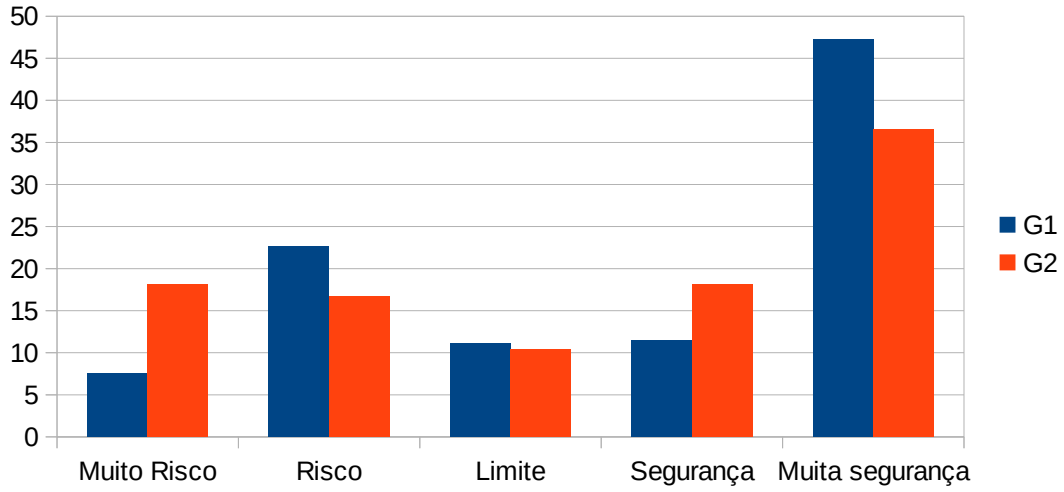


Fonte: Próprio autor

E, por fim, será feita uma análise comparativa sobre os respondentes de G1 e G2 em relação ao grau de escolaridade e classificação das respostas. Essa classificação das alternativas do questionário, a saber: Maior Risco, Risco, Limite, Segurança e Maior Segurança, está presente no questionário do Apêndice C.

Então, no gráfico 13, podemos notar que os respondentes com ensino fundamental completo ou não do G1 conseguiram um percentual maior de respostas dos itens classificados com Maior Segurança, em relação aos de G2.

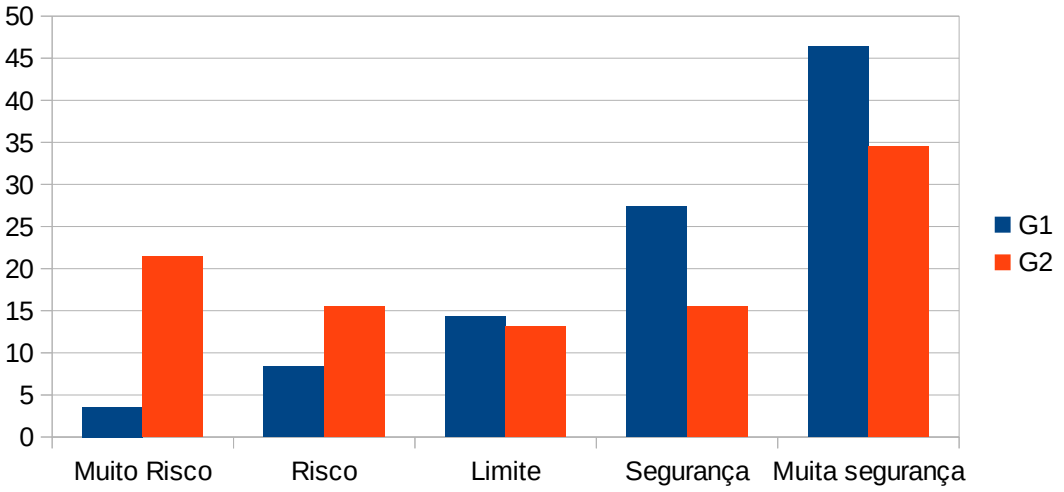
Gráfico 13 – Qualificação das respostas dos respondentes de ens. fundamental completo ou não.



Fonte: Próprio autor

Em relação aos respondentes com ensino médio completo ou não, observa-se uma acentuação de respondentes de G2 com respostas classificadas em Risco e Maior Risco, indicando que nesse grupo houve uma certa quantidade de respostas que indicam descuido em relação às situações abordadas no questionário. E os respondentes de G1 superaram nas respostas classificadas como Limite, Segurança e Muita Segurança, significando, assim, que eles foram um pouco mais atentos a leitura da cartilha e das situações propostas, em relação aos do nível de escolaridade analisado no gráfico 12. Isso é retratado no gráfico 14:

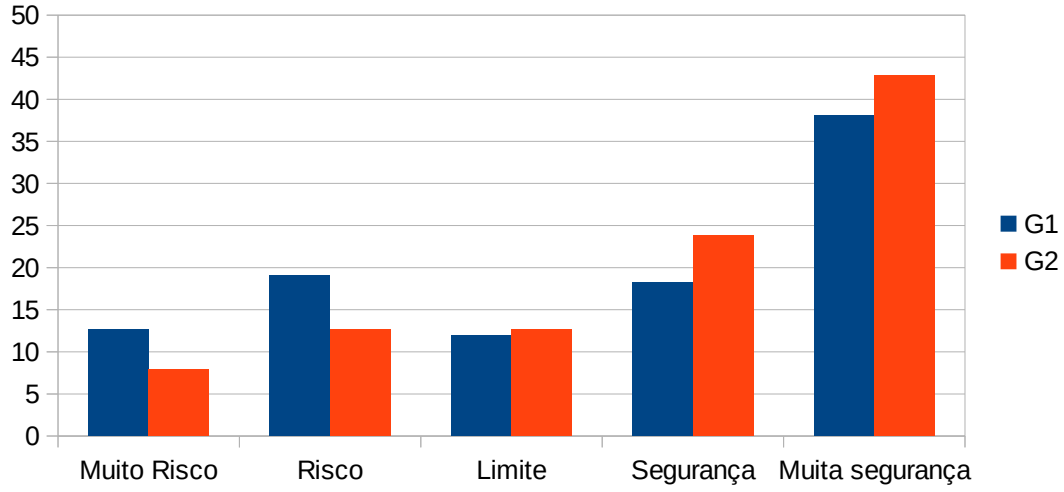
Gráfico 14 - Qualificação das respostas dos respondentes de ens. médio completo ou não.



Fonte: Próprio autor

Fazendo a mesma análise para os respondentes de ensino superior, temos que há alguns respondentes de G2 que responderam melhor ao questionário. Isso indica que os respondentes de G2 já possuem alguns conhecimentos defensivos no que se refere a situações que levam a contaminação de dispositivos informáticos por Malwares. Os respondentes de G1, mesmo lendo a cartilha, não foram sensibilizados o suficiente pelas informações ou não atentaram para elas. Como podemos observar no gráfico 15:

Gráfico 15 – Qualificação das respostas dos respondentes de ens.superior completo.



Fonte: Próprio autor

Finalizando, observou-se que os respondentes de ensino fundamental completo ou não, e ensino médio completo ou não de G1 responderam melhor ao questionário em relação aos de ensino superior que, pela análise, mesmo lendo a cartilha, fariam escolhas descuidadas frente as situações do questionário.

4.1 TESTE DE HIPÓTESES

Como a proposta do presente trabalho é mostrar a eficácia da cartilha como instrumento de conscientização e prevenção dos ataques de Malwares do tipo Ransomware, foram propostas as hipóteses:

- Hipótese Nula (H_0): Uma pessoa que consulta a cartilha, em média, não responderá melhor a um questionário com situações usadas por cibercriminosos para a contaminação de computadores e dispositivos móveis por Ransomwares.
- Hipótese Alternativa (H_A): Uma pessoa que consulta a cartilha, em média, responderá melhor a um questionário com situações usadas por cibercriminosos para a contaminação de computadores e dispositivos móveis por Ransomwares.

Para o teste das hipóteses, foi aplicado um questionário para 45 pessoas, que foram separadas em dois grupos, um grupo denominado G1 de 22 pessoas, que leu a cartilha e outro, chamado G2 de 23 pessoas, que não leu. Os dois grupos responderam ao questionário com situações típicas de usos de dispositivos de armazenamento removíveis, navegação na internet em diversos sites, cadastros em sites, compartilhamento de arquivos e links em redes sociais ou *Whatsapp*, confiança no antivírus, uso de e-mails e uso de softwares piratas, softwares obsoletos e cópias de segurança de arquivos pessoais.

Às alternativas, a partir da 6ª questão do questionário, foram atribuídas classificações as alternativas: Maior Risco, Risco, Limite, Segurança e Maior Segurança. Essas classificações, estão presentes no questionário do Apêndice B.

Para esse teste de hipóteses, foram analisadas as respostas das questões de acordo com as classificações acima mencionadas, nos dois grupos. Isso leva a caracterizar as amostras analisadas como independentes, por se tratarem de grupos

diferentes, e os dados analisados serem qualitativos ordinais, por se tratarem de dados não numéricos e poderem ser colocados em ordem de classificação. Levando em conta essas características é que foi escolhido e aplicado de Teste de Wilcoxon.

Para a realização do teste de Wilcoxon, usou-se as questões de 6 a 26, de cada respondente de ambos os grupos. Usou-se o quantitativo de resposta por questão, classificados em Segurança e Maior Segurança, conforme é mostrado no Quadro 1.

Quadro 1 - Quantitativos de respondentes de G1 e G2 por questão.

Q	Segurança G1	Maior Segurança G1	TOTAL G1	Segurança G2	Maior Segurança G2	TOTAL G2	d	POSTO	|d|	NOVO POSTO
6	-	12	12	-	14	14	-2	-3	2	-8
7	-	15	15	-	15	15	0	x	x	x
8	13	7	20	14	5	19	1	6	1	6,5
9	-	20	20	-	14	14	6	14	6	14
10	-	19	19	-	16	16	3	12	3	9
11	-	6	6	-	11	11	-5	-1	5	-1
12	-	22	22	-	20	20	2	10	2	8
13	-	13	13	-	4	4	9	18	9	18
14	12	0	12	13	0	13	-1	-4	1	-6,5
15	-	22	22	-	21	21	1	7	1	6,5
16	4	14	18	10	9	19	-1	-5	1	-6,5
17	6	14	20	6	13	19	1	8	1	6,5
18	20	0	20	12	0	12	8	17	8	17
19	5	12	17	1	9	10	7	15	7	15,5
20	4	5	9	3	9	12	-3	-2	3	-9
21	2	10	12	-	5	5	7	16	7	15,5
22	11	0	11	8	0	8	3	13	3	9
23	-	5	5	-	4	4	1	9	1	6,5
24	-	8	8	-	8	8	0	x	x	x
25	8	1	9	7	2	9	0	x	x	x
26	17	0	17	15	0	15	2	11	2	8

Fonte: Próprio autor

O referido Quadro 1, mostra o quantitativos de respondentes de G1 e G2 das questões (Q) de 6 a 26 do questionário dos itens classificados como Segurança e Maior Segurança (Apêndice C) acrescido das diferenças (d = total G1 - total G2) e os postos adotados para o teste de Wilcoxon.

Então, teremos a partir dos dados do Quadro 1 que:

$n=21$

$d=0$ diferença nula (na tabela estão com x)

Com a retirada dos dados que apresentaram diferença nula temos um novo valor para $n=21-3=18$.

Abaixo, temos os novos postos adotados para os respectivos módulos de mesma diferença. Os novos postos correspondem a média aritmética dos postos de mesmas diferenças, em módulo, ou seja, sem levar em conta os sinais das diferenças, para todos os postos cujas diferenças correspondentes foram iguais a 1, por exemplo, fez-se a média aritmética dos postos que resultou em 6,5, então, esse é o novo posto adotado para as referidas diferenças.

$|d|=1$ Novo posto 6,5

$|d|=2$ Novo posto 8

$|d|=3$ Novo posto 9

$|d|=7$ Novo posto 15,5

A seguir, temos a soma dos novos postos:

$T_n=-31$ soma dos postos negativos

$T_p=140$ soma dos postos positivos

Portanto, seja T a menor soma dos valores absolutos dos postos de mesmo sinal. Consultando a tabela G (Anexo), se o valor de T observado superar o valor dado sob determinado nível de significância, deveremos aceitar a Hipótese Nula H_0. Então, para $n=18$, considerando um teste bilateral com nível de significância 0,05, temos que, como $T=T_n=31$ NÃO superou o $T=40$ da tabela G, portanto conclui-se que deveremos rejeitar a Hipótese nula, aceitando a Hipótese Alternativa H_A,

significando que "Uma pessoa que consulta a cartilha, em média, responderá melhor a um questionário com situações usadas por cibercriminosos para a contaminação de computadores e dispositivos móveis por Ransomwares".

5 CONSIDERAÇÕES FINAIS

Notou-se que a cartilha proposta por esse trabalho impactou satisfatoriamente. Foi observado, na análise dos questionários respondidos, que já haviam alguns hábitos defensivos em alguns componentes de G1 e G2, devido aos percentuais analisados não apresentarem diferenças acentuadas para algumas questões propostas. Apesar disso, constatou-se que a cartilha proporcionou mais conscientização relacionada a abertura e compartilhamento de links e arquivos de desconhecidos em Wpp (*Whatsapp*) ou RS (Redes Sociais), adoção de senhas para RS, cadastros em sites e e-mails, o reconhecimento do ícone do cadeado na barra de endereços como um fator a mais na segurança de um site para cadastros de informações pessoais, o uso do serviço Virustotal, disponível na internet, e a necessidade de *Backups* dos arquivos pessoais.

Além disso, após o teste de hipóteses e a consequente rejeição da hipótese nula H0 pode-se ter um argumento a mais para afirmar que a cartilha impactou satisfatoriamente e serve como mais um material de conscientização quanto a algumas situações que podem levar a contaminação de dispositivos informáticos por Ransomwares.

Observou-se, durante as aplicações e análises dos questionários, questões redundantes, a falta de perguntas relacionadas a antivírus, gratuitos ou não, a falta de uma abordagem mais específica sobre *Backups* em serviços de armazenamento na nuvem, no que se refere características como capacidade de armazenamento, nível de proteção de dados do serviço, e procedimentos em caso de identificar ataque de Ransomwares, o que poderão ser focados em trabalhos futuros.

Esse trabalho se mostra relevante como mais uma contribuição social e fonte de informações para que os usuários, leigos ou não, de dispositivos informáticos possam pesquisar, discutir, navegar na internet com um pouco mais de segurança e usá-la, conscientemente, evitando contaminações por Malwares, especialmente do tipo Ransomware.

O presente trabalho não fecha o tema, apenas contribui com subsídios para que hajam mais discussões sobre Malwares, especialmente Ransomwares, e segurança da informações, principalmente para usuários leigos.

REFERÊNCIAS

[1] GIRI, Babu Nath; JYOTI, Nitin; AVERT, McAfee. The Emergence of Ransomware. In: **9th Annual Association of anti-Virus Asia Researchers (AVAR) International Conference–Digital Security: Prevention to Prosecution. Auckland, NZ**. 2006.

[2] COELHO, Cristiano Farias; RASMA, Eline Tourinho; MORALES, Gudelia. **Engenharia Social: Uma Ameaça a Sociedade da Informação**. Exatas & Engenharia, v. 3, n. 05, 2013.

[3] EIRAS, M. C. **Engenharia Social e Estelionato Eletrônico**. 2004. 40f. Monografia (Conclusão de Curso – lato sensu). IBPINET – The internet school e Uni-Rio, Graduação em Segurança da Informação na Internet, Rio de Janeiro.

[4] **Cartilha Cert.br**, Disponível em: <https://cartilha.cert.br/ransomware/>. Acesso em: 21/10/2017.

[5] **Uma História da Ameaça Ransomware: passado, presente e futuro**. Disponível em: <://pt.vpnmentor.com/blog/uma-historia-da-ameaca-Ransomware-passado-presente-e-futuro/>. Acesso em: 07/10/2017.

[6] **Historia del Ransomware: los 15 casos más curiosos**. Disponível em: <http://www.onemagazine.es/historia-del-Ransomware-los-15-que-tienes-que-conocer>. Acesso em: 07/10/2017.

[7] R**ansomware | O que é e como funciona.** Disponível em: <https://cryptoid.com.br/banco-de-noticias/Ransomware/>. Acesso em 12/08/2017.

[8] **Ataque a milhares de computadores teve escala sem precedentes.** Disponível em: <http://g1.globo.com/jornal-hoje/noticia/2017/05/ataque-milhares-de-computadores-teve-escala-sem-precedentes.html>. Acesso em: 12/11/20017.

[9] **'Petya' x WannaCry: veja diferenças do novo ataque cibernético.** Disponível em: <http://g1.globo.com/tecnologia/blog/seguranca-digital/post/petya-x-wannacry-veja-diferencas-do-novo-ataque-cibernetico.html>. Acesso em: 12/11/2017.

[10] **Новый Trojan.Winlock грозит штрафом от имени полиции**. Disponível em: https://3dnews.ru/617164. Acesso em: 15/11/2017.

[11] **Ransomware RECOVERY**. Disponível em: <https://academic.oup.com/itnow/article-abstract/58/4/32/2606459/Ransomware-Recovery>. Acesso em 09/10/2017.

[12] DAMATTO, Felipe César; RALL, Ricardo. **Estudos dos Possíveis Motivos do Aumento de Incidentes de Malware nas Empresas.** Tekhne e Logos, v. 2, n. 2, p. 90-107, 2011.

[13] ZAVARSKY, Pavol et al. **Experimental Analysis of Ransomware on Windows**

and Android Platforms: Evolution and Characterization. Procedia Computer Science, v. 94, p. 465-472, 2016.

[14] SITTIG, Dean F.; SINGH, Hardeep. **A socio-technical approach to preventing, mitigating, and recovering from Ransomware attacks**. Applied clinical informatics, v. 7, n. 2, p. 624, 2016.

[15] **Uma breve história do Ransomware**. Disponível em: <https://www.domosolucoes.com.br/uma-breve-historia-Ransomware/>. Acesso em: 01/10/2017.

[16] SAVAGE, Kevin; COOGAN, Peter; LAU, Hon. **The evolution of Ransomware**. Symantec, Mountain View, 2015.

[17] **Worms**. Disponível em: <https://www.pandasecurity.com/brazil/homeusers/security-info/classic-malware/worm/>. acesso em: 09/12/2017.

[18] **Centro de segurança da Symantec.** Disponível em: <https://www.symantec.com/pt/br/security_response/glossary/define.jsp?letter=t&word=trojan-horse> . Acesso em : 09/12/2017.

[19] ULRICH, Fernando. **Bitcoin: a moeda na era digital**. São Paulo: Instituto Ludwig von Misses Brasil, 2014.

[20] **Phishing e a manipulação do fator humano.** Disponível em: <https://ipnews.com.br/artigo-phishing-e-manipulacao-do-fator-humano/>. Acesso em: 17/12/2017.

[21] OLIVO, CLEBER KIEL; SANTIN, A. O.; OLIVEIRA, L. E. S. **Avaliação de Características para Detecção de Phishing de E-mail**. Pontifícia Universidade Católica do Paraná, Curitiba–PR, Brasil, 2010.

[22] **Cartilha de Segurança para Internet, versão 4.0 / CERT.br** – São Paulo: Comitê Gestor da Internet no Brasil, 2012.

[23] **Ransomware: Como foi o primeiro ataque informático da história.** Disponível em: <http://www.sabado.pt/ciencia---saude/detalhe/ramsomware-o-primeiro-ataque-o-actual-e-o-futuro>. Acesso em: 06/01/2018.

[24] CAVALCANTE, Waldek F. **Crimes Cibernéticos: noções básicas de investigação e ameaças na internet**. v. 22, 2016.

[25] **Ransomware maior praga virtual da atualidade.** Disponível em: <http://thomasdiego.com/ransomware-maior-praga-virtual-da-atualidade/>. Acesso em: 14/01/2018.

[26] **Como desativar o SMBv1 e proteger seu computador com Windows contra ataque.** Disponível em: http://biosbug.com.br/desativar-smbv1-proteger-computador-

windows-ataque/. Acesso em: 21/01/2018.

[27] SÁNCHEZ SOLEDAD, Roberto. **Seguridad en repositorios**. **Jornadas de repositorios institucionales de acceso abierto**, 2018.

[28] KUROSE, James F; ROSS, Keith W. **Redes de Computadores e a Internet: Uma abordagem Top-down.** – 5. ed. – São Paulo: Addison Wesley, 2010.

[29] **Virustotal**. Disponível em: <https://www.virustotal.com/pt/> Acesso em: 03/02/2018.

[30] **Canaltech**. Disponível em: <https://canaltech.com.br/software/o-que-e-api/> Acesso em: 04/04/2018.

[31] **RANSOM.CRYPTOWALL**. Disponível em: <https://www.symantec.com/security_response/writeup.jsp?docid=2014-061923-2824-99>. Acesso em: 04/04/2018.

[32] **Gamers targeted by teslacrypt ransomware 1000 to decrypt games mods steam** disponível em: <https://www.computerworld.com/article/2896408/gamers-targeted-by-teslacrypt-ransomware-1-000-to-decrypt-games-mods-steam.html>. acesso em:17/06/2018.

[33] **What is Tor?** Disponível em: <https://www.torproject.org/index.html.en>. Acesso em: 17/06/2018.

[34] **Apple has shut down the first fully-functional Mac OS X ransomware.** Disponível em: **<**https://techcrunch.com/2016/03/07/apple-has-shut-down-the-first-fully-functional-mac-os-x-ransomware/>. Acesso em: 24/06/2018.

[35] **How To Recover Files Locked By FileCoder, The Mac-Specific Ransomware.** Disponível em: <https://www.lifehacker.com.au/2017/03/heres-how-you-can-recover-files-locked-by-filecoder-the-mac-specific-ransomware/>. Acesso em 24/06/2018.

[36] **O que é ransomware?** Disponível em: <https://www.infowester.com/ransomware.php>. Acesso em: 16/09/2018.

[37] **Jigsaw Ransomware - Como Remover.** Disponível em: <https://malwarerid.com.br/malwares/jigsaw-ransomware/>. Acesso em: 16/09/2018.

[38] **OS X: sobre o Gatekeeper.** Disponível em: <https://support.apple.com/pt-br/HT202491>. Acesso em: 16/09/2018.

[39] **Encriptação**. Disponível em: <https://www.dicio.com.br/encriptacao/>. Acesso em: 16/09/2018.

[40] OLIVEIRA, Ronielton Rezende. **Criptografia simétrica e assimétrica-os**

principais algoritmos de cifragem. Segurança Digital [Revista online], v. 31, p. 11-15, 2012.

[41] ÇELİKTAŞ, Hugo Brito. **INSTITUTO DE INFORMÁTICA DO ISTAMBUL TÉCNICO UNIVERSITY★**. 2018.

[42] SIEGEL, Sidney. **Estatística não-paramétrica para as ciências do comportamento**, São Paulo: Mc Graw Hill, 1975.

GLOSSÁRIO

API é um conjunto de rotinas e padrões de programação para acesso a um aplicativo de software ou plataforma baseado na Web. A sigla API refere-se ao termo em inglês "Application Programming Interface" que significa em tradução para o português "Interface de Programação de Aplicativos" [30].

BITCOIN é uma moeda digital peer-to-peer (de ponto a ponto), de código aberto, que não depende de uma autoridade central, ou seja, é uma forma de dinheiro, assim como o real, o dólar ou o euro, com a diferença de ser puramente digital e não ser emitido por nenhum governo. Entre muitas outras coisas, o que faz o Bitcoin ser único é o fato de ele ser o primeiro sistema de pagamentos global totalmente descentralizado. O seu valor é determinado livremente pelos indivíduos no mercado. Para transações online, é a forma ideal de pagamento, pois é rápido, barato e seguro [19].

CIBERCRIMINOSO pessoa mal intencionada que, entre outras coisas, programa ou faz uso dos chamados malwares para obter vantagens de forma ilícita e prejudicar usuários domésticos ou empresas. Ou seja, é a pessoa que pratica delitos, usando recursos informáticos, que vão desde pornografia infantil, fraudes, falsificações, acesso não autorizado até atividades criminosas contra dados de pessoas ou empresas, muitos dos quais usam malwares para esses fins.

CRIPTOGRAFIA RSA é um algoritmo assimétrico que possui este nome devido a seus inventores: Ron Rivest, Adi Shamir e Len Adleman, que o criaram em 1977 no MIT. Atualmente, é o algoritmo de chave pública mais amplamente utilizado, além de ser uma das mais poderosas formas de criptografia de chave pública conhecidas até o momento [40].

ENCRIPTAÇÃO Ação ou efeito de encriptar, de registrar num código secreto (cifra) que só pode ser lido por quem tem a chave para o decifrar; codificação: encriptação de dados [39].

ENGENHARIA SOCIAL é o termo utilizado para definir a área que estuda as técnicas e práticas utilizadas para a obtenção de informações importantes ou sigilosas de uma organização, através das pessoas, funcionários e colaboradores de uma corporação ou de uma sociedade. Essas informações podem ser obtidas por ingenuidade ou confiança [3].

FIREWALL é a combinação de software e hardware que isola uma rede local de uma empresa da internet, permitindo que alguns pacotes passem e bloqueando outros. Um firewall permite que um administrador de rede controle o acesso entre o mundo externo e os recursos da rede que administra gerenciando o fluxo de tráfego de e para esses recursos [28].

GATEKEEPER é um recurso de sistemas operacionais da Apple, baseado nas verificações de

malware existentes, e que ajudam a proteger o Mac de apps prejudiciais e malware baixados pela Internet, ou seja, baixados por fora Mac App Store [38].

MALWARES são programas de código malicioso que infectam, de forma automática ou não, computadores e dispositivos móveis com a intenção de espioná-los, usá-los para prejudicar outras pessoas e empresas e até deixar arquivos inacessíveis.

PHISHING é uma forma de estelionato que usa engenharia social para fazer vítimas, enganando-as geralmente com o objetivo de obter suas informações pessoais (geralmente de cunho financeiro) e depois causar-lhes prejuízos [21].

SMB é o protocolo Server Message Block que o Windows usa para compartilhamento de arquivos em uma rede local. Foi substituído por SMBv2 e SMBv3. O protocolo SMBv1 mais antigo só está ativado porque existem algumas aplicações antigas que não foram atualizadas para usar SMBv2 ou SMBv3 [26].

TROJAN (TROJAN HORSE OU CAVALO DE TRÓIA) é um arquivo que apresenta-se como programa desejável, mas é maliciosos. Ele contém um código malicioso que, quando acionado, causa a perda ou o roubo dos dados. Para que ele se espalhe, basta convidar esse programa a entrar no computador como, por exemplo, abrindo um anexo de e-mail. Além disso, ele também cria uma porta dos fundos em um computador, o que dá a outro usuário o acesso ao sistema e possivelmente permite o comprometimento de informações confidenciais ou pessoais. O Trojan não se reproduz infectando outros arquivos, nem se autorreplica [18].

TOR (Tor Browser) é software livre e uma rede aberta que ajuda a navegar pela internet de forma anônima, se defendendo contra a análise de tráfego, uma forma de vigilância que ameaça a liberdade pessoal e privacidade. [33].

WORMS são programas que geram cópias de si próprios em diversos locais num computador infectado. O objetivo deste tipo de malware é por norma saturar os computadores e redes, impedindo o seu correto funcionamento. Ao contrário dos vírus, os worms não infectam arquivos. Exploram vulnerabilidades das aplicações e das redes de comunicações para se propagarem, e não necessitam de intervenção das vítimas para se executarem [17].

APÊNDICE A – CARTILHA

José Francisco da Silva Junior

Orientação: Prof. Lucas Amorim - Instituto de Computação - UFAL

Apresentação

Hoje em dia, o uso intensificado da internet tem atraído o interesse de criminosos. Dentre os crimes cometidos na internet, temos a propagação de programas maliciosos cujo objetivo é espionar, boicotar serviços, extorquir dinheiro, etc. Dentre esses tipos de programas, está em evidência o Ransomware que, ao infectar computadores ou smartphones, codificam(criptografam) todos os arquivos(fotos, textos, planilhas, etc), deixando-os inacessíveis. Para o usuário ter acesso a seus arquivos novamente, é exigido um “resgate”, mostrado em mensagem na tela que aparece instantes após a infecção.

Então, para servir como mais um instrumento no auxílio a prevenção, principalmente de Ransomwares, é que surge essa cartilha.

Trata-se de uma cartilha breve, com uma conversação apresentada em forma de estória em quadrinhos no início de cada parte. A primeira parte, Conversando Sobre Ransomwares, mostra alguns conceitos importantes para conhecer o que é o Ransomware e qual seu objetivo. Na segunda parte, Notícias sobre Ransomwares, mostra algumas manchetes recentes sobre Ransomwares, deixando os links disponíveis o leitor acessar e saber mais. A terceira parte, Como Saber se está contaminado por Ransomware?, mostra algumas mensagens típicas indicando que o computador ou dispositivo móvel foi contaminado e os arquivos codificados(criptografados) para que o usuário não acesse até que pague o “resgate” para o acesso ser reestabelecido. A quarta parte, Situações comuns em que se pode pegar Ransomware, trata de algumas situações corriqueiras que podem levar a infecção de computadores ou dispositivos móveis por Ransomwares. A quinta parte, Como se prevenir?, que traz algumas dicas de como se prevenir ou, se ocorrer uma infecção por Ransomware, o prejuízo não ser tão grande. E, por fim, a sexta parte, Ficam as Dicas!, são deixadas dicas finais relativas a Ransomwares.

Sumário

CONVERSANDO SOBRE RANSOMWARES

Alguns Conceitos

Cibercriminoso é quem pratica cibercrime (Crime usando aparelhos informáticos).

Malware: Programa malicioso que se instalam ou são instalados em computadores e dispositivos móveis. Esses programas, a depender do tipo, tem a finalidade de usar computadores ou dispositivos móveis da vítima, para espioná-la e a seus contatos, roubar suas informações, tentar extorquir, etc.

Dispositivos móveis são tecnologias que funcionam como computadores de bolso e permitem acesso à internet. Exemplos: Smartphones e Tablets.

Ransomware é o malware que contamina computadores ou dispositivos móveis para tornar os arquivos inacessíveis e, para a liberação desses arquivos, há a exigência de dinheiro. Ou seja, os arquivos são "sequestrados" e o dinheiro exigido é para pagar o resgate, para tê-los de volta.

Atenção

O Ransomware pode Infectar: computadores, dispositivos Móveis, modens, roteadores, etc.

Notícias sobre Ransomwares

Algumas manchetes pela Internet:

Brasil concentra 92% dos casos de ransomware na América Latina (1)

Brasil é país que mais sofre com ataques de ransomware na América Latina (2)

Ataques de ransomware tendem a crescer em 2018, de acordo com análise (3)

Smartphones com Android são alvos de novo ataque ransomware (4)

Seu celular na mira de um novo tipo de sequestrador (5)

Ataque ransomware atinge novamente computadores no Brasil (6)

Ransomware para smartphones cresceu mais de 3 vezes (7)

Novo ataque de ransomware começa a infectar computadores no Brasil (8)

Quer saber mais? Acesse:

(1)www.canaltech.com.br/seguranca/brasil-concentra-92-dos-casos-de-ransomware-na-america-latina-48259/

(2)www.kaspersky.com.br/blog/brasil-e-pais-que-mais-sofre-com-ataques-de-ransomware-na-al/9626/

(3)www.adrenaline.uol.com.br/2018/02/02/54132/ataques-de-ransomware-tendem-a-crescer-em-2018-de-acordo-com-analise/

(4)www.seguranca.uol.com.br/antivirus/dicas/curiosidades/smartphones_android_sao_alvos_novo_ataque_ransomware.html#rmcl

(5)www.gazetadopovo.com.br/economia/seu-celular-na-mira-de-um-novo-tipo-de-sequestrador-923odv1198jj3osb8mrx9sqpy

(6)www.oficinadanet.com.br/post/19446-ataque-ransomware-atinge-novamente-computadores-no-brasil

(7)/www.oficinadanet.com.br/post/19110-ransomware-para-smartphones-cresceu-mais-de-3-vezes

(8)www.tecmundo.com.br/ataque-hacker/118379-novo-ataque-ransomware-comeca-infectar-computadores-brasil.htm

Como Saber se um dispositivo está contaminado por Ransonware?

Algumas mensagens que podem aparecer num computador ou dispositivo móvel contaminado:

Observações Importantes:

- Nas mensagens que aparecem avisando da contaminação, aparecem, também, instruções de como pagar o “resgate” para ter o acesso a seus arquivos de volta. Em algumas mensagens existem até um cronômetro para pressionar a vítima a fazer o pagamento mais rápido.
- Não há garantias de que, após o pagamento do “resgate” o acesso aos arquivos seja reestabelecido, no computador ou dispositivo móvel da vítima.
- Nunca efetuar o pagamento do “resgate”, para não estimular a prática desse crime.

Atenção

Se você perceber que um computador ou dispositivo móvel foi contaminado por Ransomware, desligue-o imediatamente e chame um técnico.

Situações comuns em que se pode pegar Ransomware

Podem levar a contaminação por Ransomwares ou outros Malwares:

- Acessar e-mails de desconhecidos, ou até clicar em seus links ou baixar seus anexos;
- Usar programas piratas ou baixar programas de sites suspeitos;
- Acessar sites de filmes e seriados gratuitos;
- Acessar site de jogos gratuitos;

Atenção

Submeter o endereço de um Site ao serviço de verificação de segurança VírusTotal(https://www.virustotal.com) é uma dica para Navegação um pouco mais segura.

Como se Prevenir?

Sites Seguros apresentam o Cadeado na barra de endereços:

Serviços de armazenamento na Nuvem:

Google Drive
Quem possui Gmail já tem acesso a esse serviço.

OneDrive
Quem possui Hotmail já tem acesso a esse serviço.

Dropbox
Para ter acesso a esse serviço é só se cadastrar no site https://www.dropbox.com/pt_BR/

box
Para ter acesso a esse serviço é só se cadastrar no site https://account.box.com

Algumas dicas de prevenção

Instale antivírus em seu computador e em seu dispositivo móvel.

Para evitar que o Ransomware se aproveite de alguma vulnerabilidade (Falha) de algum aplicativo instalado:

- instale apenas programas originais e recentes;
- mantenha os aplicativos sempre atualizados;
- evite baixar aplicativos de fontes desconhecidas (prefira baixar da loja de aplicativos do seu sistema operacional);
- delete aplicativos antigos e sem uso.

Para evitar a contaminação por sites ou e-mails:

- evite clicar em links chamativos dos sites ou em links de e-mails;
- prefira digitar os endereços dos sites a serem visitados;
- prefira visitar sites com http**s** (com **s** de seguro), no endereço, ou com a figura do cadeado na barra de endereços do navegador de internet.

Se você for contaminado, poderá, de preferência com a ajuda de um técnico, recuperar seu equipamento e repor seus arquivos, para isso:

- Faça *Backups* (Cópias de segurança) de seus arquivos, fotos, vídeos, etc, em mais de um local e os atualize frequentemente;

Obs.: São opções para fazer *Backups*: serviços de armazenamento na nuvem (Onedrive, Google Drive, Dropbox, Box etc), Hds Externos e Pendrives.

Ficam as Dicas!

APÊNDICE B - QUESTIONÁRIO

UNIVERSIDADE FEDERAL DE ALAGOAS
INSTITUTO DE COMPUTAÇÃO
CURSO DE BACHARELADO EM SISTEMAS DE INFORMAÇÃO

ACADÊMICO: JOSÉ FRANCISCO DA SILVA JUNIOR

ESTE QUESTIONÁRIO TEM COMO OBJETIVO AVALIAR OS RESPONDENTES DE DOIS GRUPOS SOBRE A LEITURA PRÉVIA DA CARTILHA SOBRE PREVENÇÃO DE MALWARES DO TIPO RANSOMWARES. UM DOS GRUPOS LEU A CARTILHA E O OUTRO NÃO LEU. O PRESENTE QUESTIONÁRIO SERVE, TAMBÉM, COMO SUBSÍDIO PARA O TESTE DE HIPÓTESES SOBRE A EFICACIA DA CARTILHA COMO INSTRUMENTO DE CONSCIENTIZAÇÃO.

1. Qual sua profissão: _____ .

2. Qual seu grau de escolaridade?

a) Ensino Fundamental

b) Ensino Fundamental incompleto

c) Ensino Médio

d) Ensino Médio incompleto

e) Ensino Superior

3. Possui computador?

a) Sim b) Não

4. Possui celular, smartphone ou tablet?

a) Sim b) Não

5. Fez algum curso ou treinamento de informática?

a) Sim b) Não

6. Sua senha de e-mail é algum nome conhecido, datas de aniversários ou palavra de dicionário?

a) Sim b) Não

7. Quando recebe um e-mail desconhecido e que contém anexos, como você acredita que deve agir?

a) apaga imediatamente.

b) Abre para ver o conteúdo sem abrir os anexos.

c) abre para ver os conteúdos e abre os anexos.

8. Você recebe um e-mail indicando que você possui um débito num Banco. Como você acredita que deve agir?

a) Ligando para o Banco para saber que débito é esse.

b) Abrindo o email para saber que débto é esse.

c) Abrindo o email para saber que débto é esse, por que seu computador tem antivírus.

d) Ignorando o e-mail , mas não o deletando.

e) Ignorando o email e o deletando.

9. Quando usa o *Whatsapp* e recebe um link, video, gif ou imagem de um desconhecido, como você acredita que deve agir?

a) abre imediatamente. b) apaga imediatamente.

10. Você acredita que deve compartilhar qualquer link, vídeo, gif ou imagem que lhe chame a atenção pelo *Whatsapp*?

a) Sim b) Não

11. Quando recebe vídeo, gif ou imagem pelo *Whatsapp* de um conhecido, como você acredita que deve agir?

a) abre imediatamente. b) apaga imediatamente.

12. Quando você usa uma rede social, acredita que é seguro clicar em qualquer links, vídeos ou imagens?

a) Sim b) Não

13. Como você acredita ser mais adequado para acessar sites?

a) Digitar o endereço na barra de endereços do navegador.

b) Acessar através de um buscador (Google, yahoo, bing, por exemplo).

14. Quando você precisa acessar a internet, para fins pessoais, num computador que não é seu, como você acredita que deve agir?

a) acessando normalmente, como acessa em sua própria casa.

b) acessando numa janela anônima do navegador.

15. Você costuma clicar em links de propagandas em diversos sites?

a) Sim b) Não

16. Suponha que você está interessado em assistir um filme lançado nos cinemas recentemente. Como você acredita que deve agir?

a) Indo ao cinema para assistí-lo.

b) assinando um serviço como Netflix, por exemplo, e aguarda que o filme esteja disponível para assistir.

c) Procurando o filme em sites pela internet para assisti-lo.

d) Procurando o filme em sites pela internet e o assiste, porque seu computador tem antivírus.

17. Você está navegando num site conhecido observando algo de seu interesse. Mas, nesse site, existem links para sites desconhecidos, que lhe chamaram a atenção. Como você acredita que deve agir?

a) Clicando imediatamente em algum desses links.

b) Clicando imediatamente em algum desses links, porque seu computador tem antivírus.

c) Clicando imediatamente em algum desses links, porque esses links são inofensivos.

d) Copiando o endereço do link, para verificar no site Vírustotal, antes de acessar.

e) Ignora os links e continua a navegação.

18. Você navega num site de compras online, se interessa por um produto e decide comprá-lo. Mas para efetuar a compra é preciso fazer um cadastro, onde é pedido informações como nome completo, cpf e endereço. Como você acredita que deve agir?

a) Preenchendo o cadastro normalmente para finalizar a compra.

b) Preenchendo o cadastro normalmente para finalizar a compra, porque seu computador tem antivírus.

c) Preenchendo o cadastro normalmente para finalizar a compra, por já ter feito isso outras vezes e não ter acontecido nada.

d) Verificando se a página do cadastro possui o ícone do cadeado na barra de endereços. Caso contrário, procura outro site.

19. Considerando que você está se cadastrando num site de seu interesse para fazer compras e é pedido para inserir uma senha para seu acesso. Como você acredita que deve agir?

a) colocando sua data de nascimento ou um nome conhecido, para lembrar com mais facilidade.

b) Colocando uma senha que você usa sempre, para lembrar com mais facilidade.

c) planejando uma senha que combina nomes e números conhecidos.

d) Planejando uma senha que contenha letras maiúsculas, minúsculas, números e caracteres especiais.

20. Ao acessar sua rede social, você se depara com um link de promoção de um smartphone de seu interesse, por um preço muito abaixo daqueles que você costuma ver, como você acredita que deve agir?

a) Clicando para fazer a compra, não perdendo a oportunidade.

b) Não clicando porque o preço do smartphone está muito baixo.

c) Não clicando porque não confia em fazer compras pela internet.

d) Copiando o link e o verificando no site Virustotal, antes de comprar.

e) Copiando o link e procurando verificar a reputação da empresa.

21. Com relação às senhas adotadas para redes sociais, e-mail, cadastros em sites, etc, como você acredita que deve agir?

a) Adotando uma mesma senha para todos, pois é mais prático.

b) Adotando senhas simples e diferentes.

c) Adotando algum nome conhecido ou palavra de dicionário.

d) Adotando senhas diferentes que deixa salvas em um arquivo de texto no computador para não esquecer.

e) Planejando uma senha que contenha letras maiúsculas, minúsculas, números e caracteres especiais.

22. Como você acredita ser mais adequado adquirir programas ou aplicativos para seu computador ou smartphone?

a) Baixar da loja de aplicativos.

b) Baixar do site oficial do fabricante do programa ou aplicativo.

b) De site qualquer de downloads (Baixaki, superdownloads, por exemplo).

23. Suponha que você está interessado em um programa, mas pesquisou nas lojas e na internet e viu que tem um preço alto. Um amigo seu indica um site onde você pode baixar esse programa gratuitamente. Diante dessa situação, como você acredita que deve agir?

a) Aceitando a indicação de seu amigo e baixa o programa do site que ele indicou.

b) Aceitando a indicação de seu amigo e baixa o programa do site que ele indicou, porque seu computador tem antivírus.

c) Juntando dinheiro para comprar o programa na loja ou internet.

d) Procurando um software alternativo gratuito ou mais barato de uma empresa ou instituição confiável.

24. Suponha que você esteja interessado em um aplicativo antigo de músicas e cuja versão atual é paga, mas um amigo tem esse aplicativo antigo num CD. Como você acredita que deve agir?

a) Você compra o aplicativo.

b) Você pede a seu amigo para tirar uma cópia do CD para você.

c) Você procura a versão pirata desse aplicativo na internet.

25. Você tem vários arquivos importantes em seu computador ou dispositivo móvel, tais como: fotos e vídeos de melhores momentos de sua vida, repertório de músicas que você levou muito tempo para compor, documentos importantes digitalizados, etc. Como você acredita que deve agir?

a) deixa tudo no computador ou dispositivo móvel.

b) Faz uma cópia de tudo no google drive ou onedrive, por exemplo.

c) Faz cópias em pendrives ou Hds externos.

d) Faz mais de uma cópia de tudo em google drives ou onedrives diferentes.

26. Suponha que você tenha um aplicativo antigo em seu computador ou dispositivo móvel e o utiliza raramente. Como você acredita que deve agir?

a) Deixa esse aplicativo no computador ou dispositivo móvel.

b) Deixa esse aplicativo no computador ou dispositivo móvel, pois os dispositivos possuem antivírus.

c) Deleta esse programa e procura a versão mais atualizada ou equivalente.

APÊNDICE C - Questionário com classificações de riscos nas alternativas

UNIVERSIDADE FEDERAL DE ALAGOAS
INSTITUTO DE COMPUTAÇÃO
CURSO DE BACHARELADO EM SISTEMAS DE INFORMAÇÃO

ACADÊMICO: JOSÉ FRANCISCO DA SILVA JUNIOR

ESTE QUESTIONÁRIO É O MESMO DO APÊNDICE B, ACRESCIDO DAS CLASSIFICAÇÕES DE RISCOS NAS ALTERNATIVAS, A PARTIR DA QUESTÃO 6. ESTE TEM COMO OBJETIVO SERVIR DE INSUMO PARA O TESTE DE HIPÓTESES PROPOSTA NO PRESENTE TRABALHO.

1. Qual sua profissão: _____ .

2. Qual seu grau de escolaridade?

a) Ensino Fundamental

b) Ensino Fundamental incompleto

c) Ensino Médio

d) Ensino Médio incompleto

e) Ensino Superior

3. Possui computAdor?

a) Sim b) Não

4. Possui celular, smartphone ou tablet?

a) Sim b) Não

5. Fez algum curso ou treinamento de informática?

a) Sim b) Não

6. Sua senha de e-mail é algum nome conhecido, datas de aniversários ou palavra de dicionário?

a) Sim (MUITO RISCO) b) Não (MAIOR SEGURANÇA)

7. Quando recebe um e-mail desconhecido e que contém anexos, como você acredita que deve agir?

a) apaga imediatamente. (MAIOR SEGURANÇA)

b) Abre para ver o conteúdo sem abrir os anexos. (LIMITE)

c) abre para ver os conteúdos e abre os anexos. (MAIOR RISCO)

8. Você recebe um e-mail indicando que você possui um débito num Banco. Como você acredita que deve agir?

a) Ligando para o Banco para saber que débito é esse. (SEGURANÇA)

b) Abrindo o email para saber que débto é esse.(MAIOR RISCO)

c) Abrindo o email para saber que débto é esse, por que seu computador tem antivírus. (RISCO)

d) Ignorando o e-mail , mas não o deletando. (LIMITE)

e) Ignorando o email e o deletando. (MAIOR SEGURANÇA)

9. Quando usa o *Whatsapp* e recebe um link, video, gif ou imagem de um desconhecido, como você acredita que deve agir?

a) abre imediatamente.(MAIOR RISCO)

b) apaga imediatamente. (MAIOR SEGURANÇA)

10. Você acredita que deve compartilhar qualquer link, vídeo, gif ou imagem que lhe chame a atenção pelo *Whatsapp*?

a) Sim (MAIOR RISCO) b) Não (MAIOR SEGURANÇA)

11. Quando recebe vídeo, gif ou imagem pelo *Whatsapp* de um conhecido, como você acredita que deve agir?

a) abre imediatamente. (RISCO)

b) apaga imediatamente. (MAIOR SEGURANÇA)

12. Quando você usa uma rede social, acredita que é seguro clicar em qualquer links, vídeos ou imagens?

a) Sim (MAIOR RISCO) b) Não (MAIOR SEGURANÇA)

13. Como você acredita ser mais adequado para acessar sites?

a) Digitar o endereço na barra de endereços do navegador.(MAIOR SEGURANÇA)

b) Acessar através de um buscador (Google, yahoo, bing, por exemplo). (RISCO)

14. Quando você precisa acessar a internet, para fins pessoais, num computador que não é seu, como você acredita que deve agir?

a) acessando normalmente, como acessa em sua própria casa. (RISCO)

b) acessando numa janela anônima do navegador. (SEGURANÇA)

15. Você costuma clicar em links de propagandas em diversos sites?

a) Sim (MUITO RISCO) b) Não (MUITA SEGURANÇA)

16. Suponha que você está interessado em assistir um filme lançado nos cinemas recentemente. Como você acredita que deve agir?

a) Indo ao cinema para assistí-lo. (MUITA SEGURANÇA)

b) assinando um serviço como Netflix, por exemplo, e aguarda que o filme esteja disponível para assistir. (SEGURANÇA)

c) Procurando o filme em sites pela internet para assisti-lo. (MUITO RISCO)

d) Procurando o filme em sites pela internet e o assiste, porque seu computador tem antivírus. (RISCO)

17. Você está navegando num site conhecido observando algo de seu interesse. Mas, nesse site, existem links para sites desconhecidos, que lhe chamaram a atenção. Como você acredita que deve agir?

a) Clicando imediatamente em algum desses links. (MUITO RISCO)

b) Clicando imediatamente em algum desses links, porque seu computador tem antivírus. (LIMITE)

c) Clicando imediatamente em algum desses links, porque esses links são inofensivos.(RISCO)

d) Copiando o endereço do link, para verificar no site Vírustotal, antes de acessar. (SEGURANÇA)

e) Ignora os links e continua a navegação. (MUITA SEGURANÇA)

18. Você navega num site de compras online, se interessa por um produto e decide comprá-lo. Mas para efetuar a compra é preciso fazer um cadastro, onde é pedido informações como nome completo, cpf e endereço. Como você acredita que deve agir?

a) Preenchendo o cadastro normalmente para finalizar a compra. (MUITO RISCO)

b) Preenchendo o cadastro normalmente para finalizar a compra, porque seu computador tem antivírus. (LIMITE)

c) Preenchendo o cadastro normalmente para finalizar a compra, por já ter feito isso outras vezes e não ter acontecido nada. (RISCO)

d) Verificando se a página do cadastro possui o ícone do cadeado na barra de endereços. Caso contrário, procura outro site.(SEGURANÇA)

19. Considerando que você está se cadastrando num site de seu interesse para fazer compras e é pedido para inserir uma senha para seu acesso. Como você acredita que deve agir?

a) colocando sua data de nascimento ou um nome conhecido, para lembrar com mais facilidade. (RISCO)

b) Colocando uma senha que você usa sempre, para lembrar com mais facilidade. (MUITO RISCO)

c) planejando uma senha que combina nomes e números conhecidos. (SEGURANÇA)

d) Planejando uma senha que contenha letras maiúsculas, minúsculas, números e caracteres especiais. (MUITA SEGURANÇA)

20. Ao acessar sua rede social, você se depara com um link de promoção de um smartphone de seu interesse, por um preço muito abaixo daqueles que você costuma ver, como você acredita que deve agir?

a) Clicando para fazer a compra, não perdendo a oportunidade. (MUITO RISCO)

b) Não clicando porque o preço do smartphone está muito baixo. (SEGURANÇA)

c) Não clicando porque não confia em fazer compras pela internet. (MUITA SEGURANÇA)

d) Copiando o link e o verificando no site Virustotal, antes de comprar.

(RISCO)

e) Copiando o link e procurando verificar a reputação da empresa. (LIMITE)

21. Com relação às senhas adotadas para redes sociais, e-mail, cadastros em sites, etc, como você acredita que deve agir?

a) Adotando uma mesma senha para todos, pois é mais prático.(MUITO RISCO)

b) Adotando senhas simples e diferentes. (LIMITE)

c) Adotando algum nome conhecido ou palavra de dicionário. (SEGURANÇA)

d) Adotando senhas diferentes que deixa salvas em um arquivo de texto no computador para não esquecer.(RISCO)

e) Planejando uma senha que contenha letras maiúsculas, minúsculas, números e caracteres especiais. (MUITA SEGURANÇA)

22. Como você acredita ser mais adequado adquirir programas ou aplicativos para seu computador ou smartphone?

a) Baixar da loja de aplicativos. (LIMITE)

b) Baixar do site oficial do fabricante do programa ou aplicativo. (SEGURANÇA)

b) De site qualquer de downloads (Baixaki, superdownloads, por exemplo). (MUITO RISCO)

23. Suponha que você está interessado em um programa, mas pesquisou nas lojas e na internet e viu que tem um preço alto. Um amigo seu indica um site onde você pode baixar esse programa gratuitamente. Diante dessa situação, como você acredita que deve agir?

a) Aceitando a indicação de seu amigo e baixa o programa do site que ele

indicou. (MUITO RISCO)

b) Aceitando a indicação de seu amigo e baixa o programa do site que ele indicou, porque seu computador tem antivírus. (RISCO)

c) Juntando dinheiro para comprar o programa na loja ou internet. (MUITA SEGURANÇA)

d) Procurando um software alternativo gratuito ou mais barato de uma empresa ou instituição confiável. (LIMITE)

24. Suponha que você esteja interessado em um aplicativo antigo de músicas e cuja versão atual é paga, mas um amigo tem esse aplicativo antigo num CD. Como você acredita que deve agir?

a) Você compra o aplicativo. (MUITA SEGURANÇA)

b) Você pede a seu amigo para tirar uma cópia do CD para você. (RISCO)

c) Você procura a versão pirata desse aplicativo na internet.(MUITO RISCO)

25. Você tem vários arquivos importantes em seu computador ou dispositivo móvel, tais como: fotos e vídeos de melhores momentos de sua vida, repertório de músicas que você levou muito tempo para compor, documentos importantes digitalizados, etc. Como você acredita que deve agir?

a) deixa tudo no computador ou dispositivo móvel. (MUITO RISCO)

b) Faz uma cópia de tudo no google drive ou onedrive, por exemplo. (SEGURANÇA)

c) Faz cópias em pendrives ou Hds externos. (LIMITE)

d) Faz mais de uma cópia de tudo em google drives ou onedrives diferentes. (MUITA SEGURANÇA)

26. Suponha que você tenha um aplicativo antigo em seu computador ou dispositivo

móvel e o utiliza raramente. Como você acredita que deve agir?

a) Deixa esse aplicativo no computador ou dispositivo móvel. (MUITO RISCO)

b) Deixa esse aplicativo no computador ou dispositivo móvel, pois os dispositivos possuem antivírus. (RISCO)

c) Deleta esse programa e procura a versão mais atualizada ou equivalente. (SEGURANÇA)

ANEXO – Tabela de Valores de Referência (Prova de Wilcoxon)

Tábua G. Valores Críticos de *T* na Prova de Wilcoxon*

N	Nível de significância para prova unilateral		
	0,025	0,01	0,005
	Nível de significância para prova bilateral		
	0,05	0,02	0,01
6	0	—	—
7	2	0	—
8	4	2	0
9	6	3	2
10	8	5	3
11	11	7	5
12	14	10	7
13	17	13	10
14	21	16	13
15	25	20	16
16	30	24	20
17	35	28	23
18	40	33	28
19	46	38	32
20	52	43	38
21	59	49	43
22	66	56	49
23	73	62	55
24	81	69	61
25	89	77	68

* Adaptado de Table I of Wilcoxon, F. 1949. *Some rapid approximate statistical procedures.* New York: American Cyanamid Company, p. 13, com permissão dos autores e do editor.