FACULDADE DE TECNOLOGIA DE AMERICANA "MINISTRO RALPH BIASI"

CURSO SUPERIOR DE TECNOLOGIA EM SEGURANÇA DA INFORMAÇÃO

Eduardo Peixoto Riccetto

Silvio dos Santos

RANSOMWARE: SUA EVOLUÇÃO HISTÓRICA E COMO FUNCIONA NA PRÁTICA.

Americana-SP

2022

Eduardo Peixoto Riccetto

Silvio dos Santos

RANSOMWARE: SUA EVOLUÇÃO HISTÓRICA E COMO FUNCIONA NA PRÁTICA.

Trabalho de Conclusão do Curso, apresentado para obtenção do grau de Tecnólogo no Curso Superior de Tecnologia em Segurança da Informação da Faculdade "Ministro Ralph Biasi", FATEC Americana.

Orientador(a): Prof. Dra. Maria Cristina Aranda

Americana-SP

2022

Eduardo Peixoto Riccetto
Silvio dos Santos

Ransomwere - sua evolução histórica e como funciona na prática

Trabalho de graduação apresentado como exigência parcial para obtenção do título de Tecnólogo em Curso Superior de Tecnologia em Segurança da Informação pelo Centro Paula Souza – FATEC Faculdade de Tecnologia de Americana – Ministro Ralph Biasi.
Área de concentração: **Segurança da Informação**

Americana, 24 de junho de 2022

Banca Examinadora:

Maria Cristina Aranda (Presidente)
Doutora
Faculdade de Tecnologia de Americana

Rogério Nunes de Freitas (Membro)
Mestre
Faculdade de Tecnologia de Americana

Lucas Serafim Parizotto (Membro)
Especialista
Faculdade de Tecnologia de Americana

RESUMO

Informação é um ativo de extrema importância estratégica e de alto valor econômico para as empresas. A utilização das tecnologias como ferramentas para gerenciar este recurso dentro das organizações se tornou indispensável, auxiliando na tomada de decisões e trazendo vantagens competitivas no mercado. Com o aumento cada vez maior da utilização da tecnologia para gerir este ativo, há também a necessidade de protegê-lo, pois seu valor econômico, é conhecido não só por grandes empresas e corporações, mas também por criminosos que buscam de alguma forma conseguir vantagens econômicas com a posse e chantagens dessas informações sobre as empresas, assim o Ransomware é uma ferramenta utilizada por criminosos para sequestrar dados e extorquir empresas em troca de dinheiro. Sabendo-se disso e da necessidade de proteger estas informações, o presente artigo fez uso de pesquisas bibliográficas, objetivando esclarecer o que é um Ransomware na teoria e como ele atua na prática dentro de um sistema operacional.

Palavras-chave: Segurança da Informação, Ransomware, Engenharia Social.

Abstract: Information is an asset of extreme strategic importance and of high economic value for companies. The use of technologies as tools to manage this resource within organizations has become indispensable, due to its practicality and automation of tasks, helping in decision making and bringing competitive advantages in the market. With the increasing use of technology to manage this asset, there is also a need to protect it, as its economic value is known not only by large companies and corporations, but also by criminals who seek to somehow obtain advantages. With the possession and blackmail of this information about companies, Ransomware is a tool used by criminals to hijack data and extort companies in exchange for money. Knowing this and the need to protect this information, this article made use of bibliographic research, aiming to clarify what a Ransomware is in theory and how it works in practice within an operating system.

Keywords: Information Security, Ransomware, Social Engineering.

1. INTRODUÇÃO

Segundo Paulo Silva (2015, NSC Total). A Informação é um ativo para as empresas, tão importante ou mais que qualquer ativo físico. Por isso, os ambientes e os equipamentos utilizados para seu processamento, seu armazenamento e sua transmissão devem ser protegidos. A informação tem valor para a organização. Sem informação, a organização não realiza seu negócio.

Informação é um dado que tem significado em algum contexto para quem o recebe. Quando a informação é alocada em um computador, ela geralmente está armazenada como um dado. Este que possui valor financeiro e estratégico para as empresas. O conjunto de dados organizados de forma a terem um sentido e valor para o tomador de decisão. São dados com significado e que são processados para um determinado fim, segundo Hintzbergen Jule, Hintzbergen Kees, Smulders e Baars (2018 Fundamentos de segurança da informação). Hoje em dia toda informação tem valor, em um ambiente empresarial o resultado desse processamento dos dados pode significar uma vantagem competitiva frente aos seus concorrentes. Sabendo da importância da informação nas organizações e do seu papel no planejamento e desenvolvimento da empresa, a informação deve ser tratada como um bem do negócio, necessitando de atenção com a segurança, evitando que esses dados sejam perdidos ou fiquem em poder de indivíduos não autorizados.

Informação é muito mais que um conjunto de dados. Transformar esses dados em informação é transformar algo com pouco significado em um recurso de valor para a nossa vida pessoal ou profissional.

Conforme a ISO/IEC 27002 (ABNT, 2013), que fornece diretrizes para padrões organizacionais de segurança da informação e práticas de gerenciamento de segurança, a informação é um ativo de grande importância no processo de negócios de uma organização, e por consequência disso existe a necessidade de proteção desse ativo. Com o aumento da necessidade de tornar

essa informação mais acessível aos utilizadores, a informação acaba ficando mais vulnerável a ameaças.

Os novos recursos tecnológicos para gerenciamento da informação e o uso crescente de sistemas compartilhados abrem a possibilidade para fraudes, vandalismo, desvios, sabotagem, entre outros riscos. A tendência da computação cada vez mais distribuída vem de encontro à eficácia da segurança da informação. O acesso não autorizado a computadores é um dos mais preocupantes e destrutivos problemas de comportamento enfrentados pela sociedade e neste ponto a segurança da informação desempenha papel importante para manter a competitividade da organização, frente à importância da informação no ambiente corporativo. Com esse papel de grande importância da informação no ambiente organizacional isso se traduz em um bem de grande valor financeiro para as empresas, mas também atrai o interesse negativo. Como essas informações têm o poder de garantir o sucesso ou determinar o fracasso dos negócios, proteger estes dados impedindo que pessoas mal-intencionadas tenham acesso a eles e causem danos irreversíveis ou solicitem um retorno financeiro para devolução destas informações, se torna um dos maiores desafios da atualidade. Segundo publicação da TIINSIDE (2022) o Brasil sofreu mais de 33 milhões de tentativas de *ransomware* no ano de 2021. Com o surgimento do *ransomware*, como definição da AVAST ACADEMY (AVAST, [s.d.]), é um tipo de *malware* que criptografa arquivos e até sistemas inteiros de computador, para que posteriormente possa se exigir um valor como resgate destes dados pelas empresas. Este tipo de *malware* afeta sistemas e arquivos da organização, tornando-os inutilizáveis para as vítimas.

Apesar de não ser um problema relativamente novo no cenário empresarial, o sequestro de dados tem se popularizado em grande escala nos últimos anos, tendo como alvos principais empresas e órgãos públicos, incentivados pela grande lucratividade desse tipo de ataque. O aumento no número de ataques desse tipo também está relacionado com o modo de execução dele, ao invés de atacar grandes corporações e pedir altas quantias de resgate, passou-se a realizar uma quantidade maior de ataques contra empresas de menor porte, hospitais e órgãos públicos, como o ocorrido com o TJ do Rio Grande do Sul, que teve 12 mil servidores perdidos em um ataque

ransomware segundo a CISCO *Advisor* (CISCO, 2021). Conclui- se que elas se tornam melhores alvos para estes ataques, pois pequenas instituições possuem menor investimento em segurança digital e mesmo que sejam pedidos valores menores de resgate, devido a facilidade de ataque a estas instituições, vê-se cada vez mais um aumento no volume de ataques no mundo, sendo que em uma escala global atingiu um crescimento de 105% nos números de ataques *ransomwares* de 2020 para 2021. Assim, como já esperado um aumento no índice de crimes cibernéticos, saber como funciona e como se prevenir de um ransomware é essencial. Em pesquisa será abordado a teoria sobre ransomware e segurança da informação, além de uma abordagem prática de como funciona um ransomware dentro do sistema operacional quando realizado um ataque.

2. SEGURANÇA DA INFORMAÇÃO

A Segurança da Informação existe para minimizar os riscos de negócio em relação à dependência do uso dos recursos de informação para o funcionamento da organização. Sem a informação ou com informação incorreta, o negócio pode ter perdas que comprometam o seu funcionamento e o retorno de investimento dos acionistas. Proteger a informação significa garantir os pilares da Segurança da Informação, segundo Edson Fontes (Segurança da Informação - 2003).

Disponibilidade: a informação deve estar acessível para o funcionamento da organização e para o alcance de seus objetivos e missão.

Integridade: a informação deve estar correta, ser verdadeira e não estar corrompida.

Confidencialidade: a informação deve ser acessada e utilizada exclusivamente pelos que necessitam dela para a realização de suas atividades profissionais na organização; para tanto, deve existir uma autorização prévia.

Legalidade: o uso da informação deve estar de acordo com as leis aplicáveis, regulamentos, licenças e contratos, bem como os princípios éticos seguidos pela organização e desejados pela sociedade.

Auditabilidade: o acesso e o uso da informação devem ser registrados, possibilitando a identificação de quem fez o acesso e o que foi feito com a informação.

Não repúdio de autoria: o usuário que gerou ou alterou a informação (arquivo de texto ou mensagem de correio eletrônico) não pode negar o fato, pois existem mecanismos que garantem sua autoria.

O ano de 2021 foi o ano da consolidação das ameaças em relação a ataques cibernéticos, nunca foram tão frequentes estes tipos de ataques quanto nesse ano. Ataques impactantes e sofisticados, vazamentos de informações sigilosas, sequestro de dados, invasões de sistemas e muito dinheiro perdido. Segundo a consultoria alemã Roland Berger, o Brasil foi o 5º país que mais sofreu crimes cibernéticos neste ano de 2021. Apenas no primeiro trimestre houve um total de 9,1 milhões de ocorrências, isso é mais que o ano inteiro de 2020, segundo publicação da revista ISTOÉ DINHEIRO (2021).

Sabe-se que informação é um dos maiores bens de uma empresa e que a evolução da tecnologia está permitindo que essa informação esteja disponível em quase todos os lugares. Nos dias de hoje, as empresas dependem cada vez mais dos sistemas de informação e da Internet para fazer negócios, não podendo se dar ao luxo de sofrer interrupções em suas operações. Um incidente de segurança pode impactar direta e negativamente as receitas de uma corporação, a confiança de seus clientes e o relacionamento com sua rede de parceiros e fornecedores.

Em última instância, um incidente pode impedir, direta ou indiretamente, a organização de cumprir sua missão e deixar de gerar valor para a empresa e para os acionistas. Essa perspectiva traz a segurança da informação para um patamar novo, não apenas relacionada com a esfera da tecnologia e das ferramentas necessárias para proteger a informação, mas também como um dos pilares de suporte à estratégia de negócio de uma corporação. A gestão da segurança assume, então, um novo significado, pois passa a levar em consideração os elementos estratégicos de uma organização e evolui para a extensão da prática de gestão de riscos do negócio, segundo Marcio Zapater e Rodrigo Suzuki (ZAPATER; SUZUKI, 2021).

Os incidentes de segurança da informação vêm aumentando consideravelmente ao longo dos últimos anos e assumem as formas mais variadas, como, por exemplo: infecção por vírus, acesso não autorizado, ataques *denial of service* contra redes e sistemas, furto de informação proprietária, invasão de sistemas, fraudes internas e externas, uso não autorizado de redes sem fio, entre outras.

Um dos principais motivadores desse aumento é a difusão da Internet, que cresceu de alguns milhares de usuários no início da década de 80 para centenas de milhões de usuários ao redor do mundo nos dias de hoje. Ao mesmo tempo que colaborou com a democratização da informação e se tornou um canal *on-line* para fazer negócios, também viabilizou a atuação dos ladrões do mundo digital e a propagação de códigos maliciosos (vírus, *worms*, *trojans* e outros), *spam*, e outros inúmeros inconvenientes que colocam em risco a segurança de uma corporação. Além disso, a facilidade da realização de ataques através da Internet aumentou significativamente com a popularização de ferramentas apropriadas espalhadas ao longo da rede mundial de computadores, habilitando desde *hackers* até leigos mal-intencionados a praticarem investidas contra sistemas de informação corporativos.

O artigo publicado por Edward Uhier Condon (CONDON, 1948), discute temas como a tradição da ciência em compartilhar conhecimentos, em face dos acontecimentos da Segunda Guerra Mundial e do pós-guerra, quando talvez as informações mais bem protegidas tenham sido aquelas relativas à confecção da bomba atômica. O artigo também menciona questões de equilíbrio, para que não ocorram problemas de segurança em excesso, a ponto de não se encontrar, dentro da própria organização, informações necessárias à tomada de decisão. Tal artigo aborda, ainda, questões do custo da proteção, ao se duplicar algo já feito, por receio da perda. Essa política apesar de ser da década de 40, pode ser uma métrica a ser utilizada na área de segurança da informação nos dias de hoje.

Juntamente com a difusão da Internet, outros fatores contribuíram para impulsionar o crescimento dos incidentes de segurança. Um desses fatores é o aumento do número de vulnerabilidades nos sistemas existentes, como, por exemplo, as brechas de segurança nos sistemas operacionais utilizados em

servidores e estações de trabalho. Outro fator é o quão trabalhoso e custoso pode se tornar o processo de mitigar tais vulnerabilidades com a aplicação de correções do sistema, realizadas muitas vezes de forma manual e individual de máquina a máquina. Por último, a complexidade e a sofisticação dos ataques também contribuíram de maneira direta para o aumento dos incidentes, segundo Zapater e Suzuki (2021).

É a conjunção dessas condições que culmina, por exemplo, na parada generalizada de sistemas e redes corporativas ao redor do mundo, causada pela atuação de códigos maliciosos que se propagam pela Internet em questão de minutos. A tendência é que as ameaças à segurança continuem a crescer não apenas em ocorrência, mas também em velocidade, complexidade e alcance, tornando o processo de prevenção e de mitigação de incidentes cada vez mais difícil e sofisticado. E para colaborar com esta difícil tarefa de combater e prevenir danos causados, ainda se enfrenta um alto índice de falta de mão de obra que possa combater esta demanda crescente. Estudo divulgado pela FGV (2022) aponta que a demanda brasileira por profissionais nas áreas de *software*, serviços de TIC e TI *in-house* (que considera outros setores não identificados como tipicamente de TI) deverá alcançar 797 mil vagas em cinco anos (de 2021 a 2025).

3. ENGENHARIA SOCIAL

Engenharia social é uma técnica empregada por criminosos virtuais para induzir usuários desavisados a enviar dados e informações sensíveis e confidenciais, com o intuito de infectar seus computadores com *malwares* ou abrir *links* para *sites* falsos e infectados (Kaspersky, 2022). Este método não é nenhuma novidade do século 21, há muito tempo criminosos fazem uso destas técnicas para ganhar credibilidade de seus alvos e facilitar na aplicação do golpe. Diversos são os golpes aplicados, mas com o crescimento da Internet, este tipo de técnica tem potencializado sua eficácia com a ajuda do anonimato, a facilidade de se passar por outra pessoa, instituição ou órgão, fora a imensa disponibilidade de possíveis vítimas navegando livremente na *web*.

Por meio da engenharia social, criminosos usam a interação humana para manipular o usuário a divulgar informações sensíveis, e como a engenharia social se baseia na natureza humana e nas reações emocionais, os invasores utilizam táticas para tentar enganá-los, segundo publicação do BRNORTON (2021), que demonstra algumas das técnicas utilizadas como *baiting, phishing*, pretextos, *quid pro quo, vishing, farming* etc.

Na técnica ***baiting*** o criminoso deixará um dispositivo infectado à vista em um local público, como um pen drive por exemplo. Quando o usuário encontrar o dispositivo e o conectar em seu computador será infectado por um *malware*.

O truque utilizado no ***phishing*** baseia-se em ludibriar o usuário através de uma mensagem ou *e-mail* que busca conquistar falsamente a confiança de seu alvo, fingindo ser outra pessoa, ou instituição. Existem casos de a mensagem ou *e-mail* tentando enganar o usuário mexendo com seu seus medos e seu senso de urgência da situação, como por exemplo um *e-mail* sobre um saque não autorizado de sua conta pedindo para que altere sua senha rapidamente é claro que o acesso conduzirá a um *site* falso, dando assim acesso a seus dados para o criminoso.

Pretextos são histórias elaboradas inventadas pelos criminosos para criar uma situação que vai "fisgar" suas vítimas. Muitas vezes são histórias tristes sobre alguém perdido em um país estrangeiro ou sobre um príncipe herdeiro de um país desconhecido, que acaba de perder o pai e precisa de 500 dólares para se tornar rei. Essas situações apelam para a inclinação humana natural de ajudar aqueles que necessitam.

"Tomar uma coisa por outra" é o conceito usado no **quid pro quo**, seduzindo o usuário com prêmios ou descontos em produtos de luxo. Este golpe oferece aos usuários "alguma coisa", mas só depois que eles preencherem um formulário que solicita todas as suas informações pessoais.

No ***vishing*** o criminoso liga para o funcionário de uma empresa fingindo ser uma pessoa confiável ou um representante do seu banco ou de uma instituição parceira da empresa em que você trabalha e tenta, durante a conversa, obter informações da vítima.

Um tipo de crime mais elaborado é o ***farming***, no qual o criminoso procura uma maneira de estabelecer um relacionamento com a vítima. Normalmente ele analisa o perfil das vítimas em mídias sociais e tenta estabelecer um relacionamento com ela, com base nas informações obtidas em sua pesquisa. Esse tipo de ataque depende também do pretexto, pois o criminoso tenta enganar a vítima pelo maior tempo possível, a fim de extrair o máximo de dados possíveis.

O desenvolvimento tecnológico proporcionou inúmeros benefícios para a sociedade. Porém, com a evolução das novas tecnologias, cresceram exponencialmente as vulnerabilidades de sistemas. A partir do exposto, nota-se que *hackers* e golpistas exploram essas falhas por meio de aplicação de determinadas técnicas, que, somadas ao poder de persuasão, se transformam em oportunidades para a prática de crimes, causando expressivos prejuízos às vítimas e às empresas.

Define-se engenheiro social (BRADESCO SEGURANÇA, 2017) como aquele que – valendo-se de influência e persuasão, de técnicas psicológicas de convencimento ou de meios tecnológicos – consegue facilmente enganar e manipular as vítimas para que revelem ou concedam acesso a dados pessoais ou informações sigilosas, o que resultará na aplicação de diversos golpes, visando obter benefícios econômicos ou praticar fraudes contra terceiros.

Kevin Mitnick, em seu livro “A Arte de Enganar” (MITNICK, 2003), obra em que explana os artifícios da engenharia social e ilustra os métodos que utilizou enquanto *hacker*, dá um amplo panorama de como conseguir informações e quebrar protocolos utilizados em empresas de maneira simples, principalmente utilizando-se de contatos telefônicos. O próprio Mitnick iniciou a carreira de *hacker* efetuando ataques simples em estações de ônibus.

Mann (2011) ilustra o resultado de vários anos prestando consultoria na área de engenharia social, baseado em estudos empíricos e consultorias, conduz o leitor a quais os processos para leitura comportamental de uma pessoa e como fazer para ganhar sua confiança e enganá-la. Ele ilustra os elementos dos treze comportamentos humanos e como fazer para driblar suas proteções

naturais e explorar possíveis falhas através de mecanismos como confiança, empatia e intimidação.

Mann (2011), salienta ainda que:

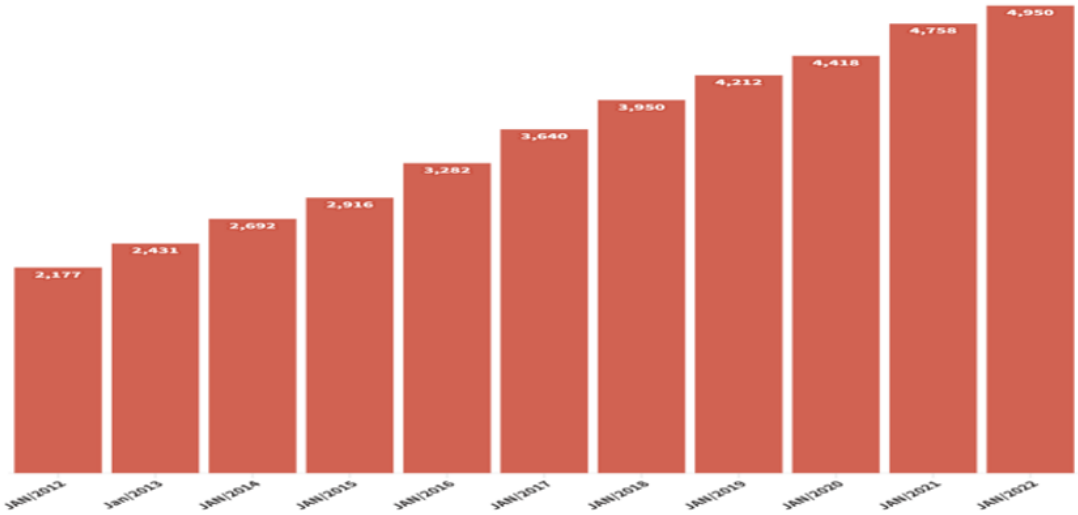
> Muita gente acaba em um cargo de TI porque gosta de tecnologia. Se quisesse trabalhar com pessoal, estaria trabalhando com Recursos Humanos. Assim, se você é executivo, com responsabilidades que incluem segurança da informação, pense nas diferentes pessoas dentro das suas equipes. Elas estão oferecendo a você o equilíbrio correto entre segurança física, de TI e humana? Você pode precisar pensar em recrutar um psicólogo!

Baseado na citação de Mann, pode-se afirmar que a segurança da informação é um processo que conta com a participação de todos os indivíduos da corporação, pois qualquer pessoa envolvida nos assuntos de uma companhia está sujeita a ser alvo de ataques. Sendo assim, é de suma importância a preparação dos profissionais no que tange à possíveis abordagens sociais.

Conhecer, ficar atento ao modo de execução e tentar mitigar possíveis vulnerabilidades são, sem dúvida, os meios mais eficazes de impedir a eficiência do golpe, segundo o BRADESCO SEGURANÇA (2017).

Um dos sinais da sociedade digital moderna é o rápido desenvolvimento das tecnologias da informação e a disseminação da Internet, que está sendo introduzida em todas as esferas da vida, tornando assim, quase todos os atos impessoais interligados à *web*. E a conscientização e cuidado para não cair em golpes é preciso ser cada vez maior. O primeiro *site* da história foi criado em 1991, segundo NEXO JORNAL (2021) e desde então o número de sites e usuários da Internet tem aumentado de maneira quase que exponencial. No ano de 2012 havia cerca de 2 bilhões de usuários na Internet em todo o mundo, hoje em 2022 beira a faixa dos 5 bilhões de usuários em todo o mundo, segundo estatísticas publicadas pelo INSPER (2022), fato este verificado na Figura 1.

Figura *1*- Evolução do número de usuários ativos na Internet.



Fonte: Insper, 2022

4. RANSOMWARE

Neste artigo será abordado o que é o *ransomware*, quais tipos de problemas podem ser causados a partir de sua infecção, como é realizado uma criptografia em dados guardados por instituições e o importante papel da Segurança da Informação nestes novos tempos em que está cada vez mais interligados pela *web.*

Existem dois tipos de *ransomware*:

- *Ransomware Locker*: impede que você acesse o equipamento infectado.
- *Ransomware Crypto*: impede que você acesse aos dados armazenados no equipamento infectado, geralmente usando criptografia.

Além de infectar o equipamento o *ransomware* também costuma buscar outros dispositivos conectados, locais ou em rede, e criptografá-los também.

A primeira demonstração de um *ransomware* foi feita por Joseph Popp em 1989, o *ransomware* chamado AIDS, segundo IET (2018), onde o autor utilizou criptografia de chave simétrica que é o uso de uma única chave, que é compartilhada entre o emissor e o destinatário de um conteúdo. Essa chave é

uma cadeia própria de *bits*, que vai definir a forma como o algoritmo vai cifrar um conteúdo, segundo publicação do CRIPTOID (2017).

De acordo com Sightinformatica (2020), uma vez que algum arquivo foi infectado, o *malware* codifica os dados do usuário, em segundo plano, sem que o sistema ou *softwares* de antivírus possam detectar. Quando tudo estiver pronto, emitirá uma mensagem avisando que o PC está bloqueado e que o usuário não poderá mais usá-lo, a menos que pague o valor exigido para obter a chave para descriptografar e dar acesso novamente aos seus dados. A difícil detecção de um *ransomware* e seus disfarces são os fatores que o tornam tão perigoso. A praga infecta seus alvos de diversas maneiras, através de *sites* maliciosos, *links* suspeitos por *e-mail*, ou instalação de *apps* vulneráveis. O *ransomware* também pode aparecer em *links* enviados por redes sociais, meio muito utilizado para espalhar vírus atualmente.

Todos os usuários e organizações estão sujeitos a este tipo de ataque, desde simples usuários e pequenas empresas até grandes corporações. Exemplos de ataques a alvos inusitados mostram a importância de todos estarem preparados e protegidos contra estas ameaças, como é o caso do "*ransomware* do cemitério" onde consta que um cemitério teve seus dois servidores sequestrados e clientes pagando pelo resgate, pois todos os documentos de operações do lugar só existiam digitalmente e os *backups*, embora tenham sido realizados, também estavam nos servidores afetados, segundo o portal Canal Tech (2021).

Novos tipos de golpes *ransomwares* têm seguido dois padrões encontrados na *web*. O primeiro é a "dupla extorsão", que ocorre principalmente quando uma empresa que sofreu o ataque se recusa a pagar o resgate por possuir *backups* atualizados das informações comprometedoras. Os criminosos então ameaçam vazar estes dados, o que pode trazer complicações para a companhia e multas por quebra da LGPD (Lei Geral de Proteção de Dados). O segundo método é o que promete lucros aos funcionários da empresa que colaborarem com a invasão, seguindo procedimentos descritos em um *e-mail* enviado pelos criminosos. Recentemente um destes casos chegou a oferecer 40% do valor de resgate pelo auxílio do funcionário. Segundo informações obtidas de publicação do portal CANALTECH (2021).

Quando se trata de *ransomware* deve-se ponderar que existem duas categorias principais, o *ransomware* de bloqueio, onde as funções básicas do computador são afetadas, deixando sua usabilidade inoperante. E o *ransomware* de criptografia, onde os arquivos e dados individuais são criptografados tornando inviável sua utilização por usuários e empresas, segundo publicação da Kaspersky (2020).

5. APLICAÇÃO DE UM RANSOMWARE

Para realizar a criptografia dessa aplicação prática foi utilizado o Python que é uma linguagem de programação que auxilia na criptografia das imagens utilizando duas bibliotecas, uma delas é a PYEAS que faz criptografia de arquivos e pastas e outra é a biblioteca OS que fornece funções para interagir com o sistema operacional. Foi definido a linguagem Python para o experimento devido a quantidade de cursos e tutoriais disponíveis sobre o assunto na internet. Uma imagem de formato .png foi usada como exemplo, pois se encontra no diretório do computador da vítima (Figura 2), que será armazenada em uma variável com o nome de *file_name*.

Figura 2- Imagem a ser criptografada

Fonte: Google, 2017

Foi definida uma chave de criptografia de 16 bytes e armazenada em uma variável com o nome de chave. Para um *ransomware* bem elaborado com a finalidade de realizar um ataque real, a ideia seria aplicar essa linha de código para todos os arquivos importantes dentro da máquina alvo. Para isso, deve-se

colocar essa linha de código dentro de um loop que fizesse a navegação pelos diretórios da máquina alvo, como demonstrado na figura 3.

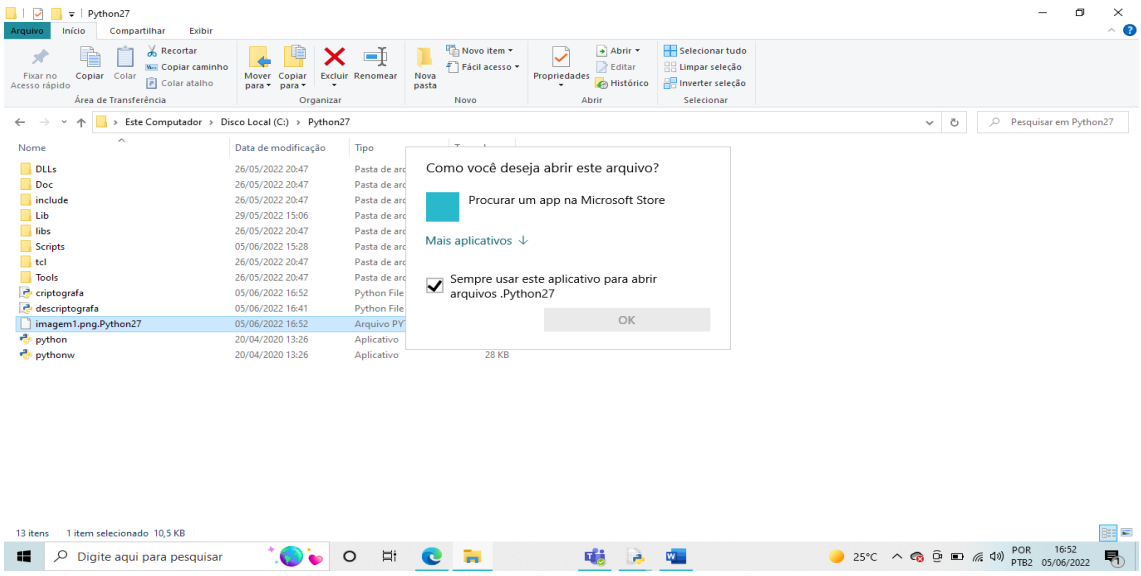
Figura 3 Script antes de ser executado

```
1  import os # Fornece funções para interagir com o sistema operacional
2  import pyaes # Faz a criptografia da imagem ou arquivo
3
4  file_name = "imagem1.png"
5  text = open(file_name, "rb")
6  text_data = file.read()
7  text.close()
8
9  os.remove(file_name)
10
11 chave = "0a5e9d3r1a5v2e9h" # Chave de criptografia de 16 bytes armazenada em variável
12 aes = pyaes.AESModeOfOperationCTR(chave)
13 encripta_dados = aes.encrypt(file_data)
14
15 new_file_name = file_name + ".Python27"
16 new_file = open(new_file_name, "wb")
17 new_file_data = new_file.write(encripta_dados)
18 new_file.close()
```

Fonte: Próprios autores

Depois de executado o script, ao tentar abrir a imagem o Sistema Operacional não encontrará nenhum aplicativo para executar o arquivo, como ostra a Figura 4.

Figura 4 Nenhum arquivo encontrado



Fonte Próprios autores

Após o desenvolvimento do *ransomware*, desenvolve-se um *script* que faça o processo inverso, ou seja, um *script* para descriptografar a imagem. O

passo a passo para construção desse *script* é basicamente o mesmo que o anterior, com alteração em apenas duas linhas.

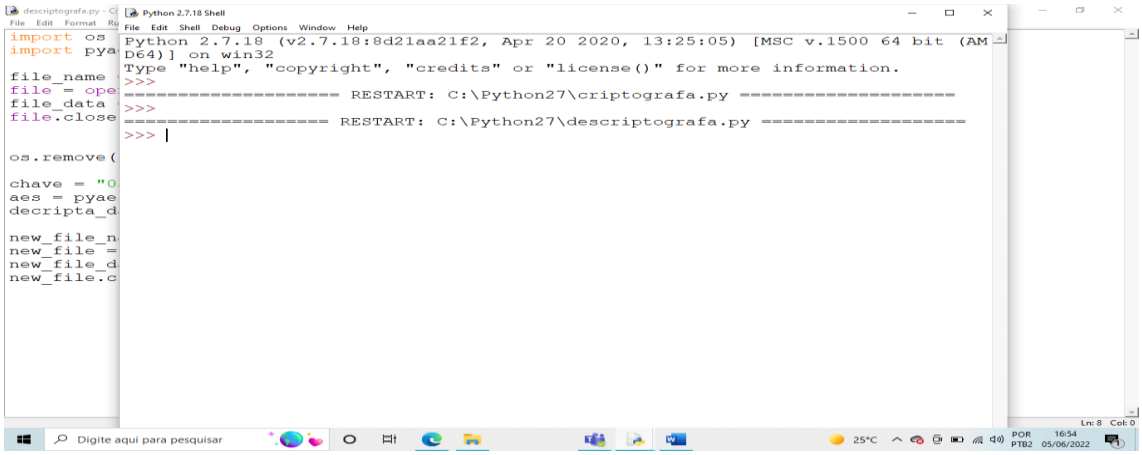
Primeiramente, ao invés de utilizar a biblioteca “pyaes” para criptografar a imagem, utiliza-se para descriptografar e salvar o resultado dessa operação em uma variável chamada “decripta_dados”. Observa-se que foi utilizada a função “.decrypt(arquivo)” ao invés da função “.encrypt(arquivo)”, mostrado na Figura 5 e na Figura 6 o script executado sem nenhum erro.

Figura 5 Alteração da função encrypt para decrypt

```
1  import os # Fornece funções para interagir com o sistema operacional
2  import pyaes # Faz a criptografia da imagem ou arquivo
3
4  file_name = "imagem1.png.Python27"
5  file = open(file_name, "rb")
6  file_data = file.read()
7  text.close()
8
9  os.remove(file_name)
10
11 chave = "0a5e9d3r1a5v2e9h" # Chave de criptografia de 16 bytes armazenada em variável
12 aes = pyaes.AESModeOfOperationCTR(chave)
13 decripta_dados = aes.decrypt(file_data)
14
15 new_file_name = "imagem1.png"
16 new_file = open(new_file_name, "wb")
17 new_file_data = new_file.write(decripta_dados)
18 new_file.close()
```

Fonte: Próprios autores

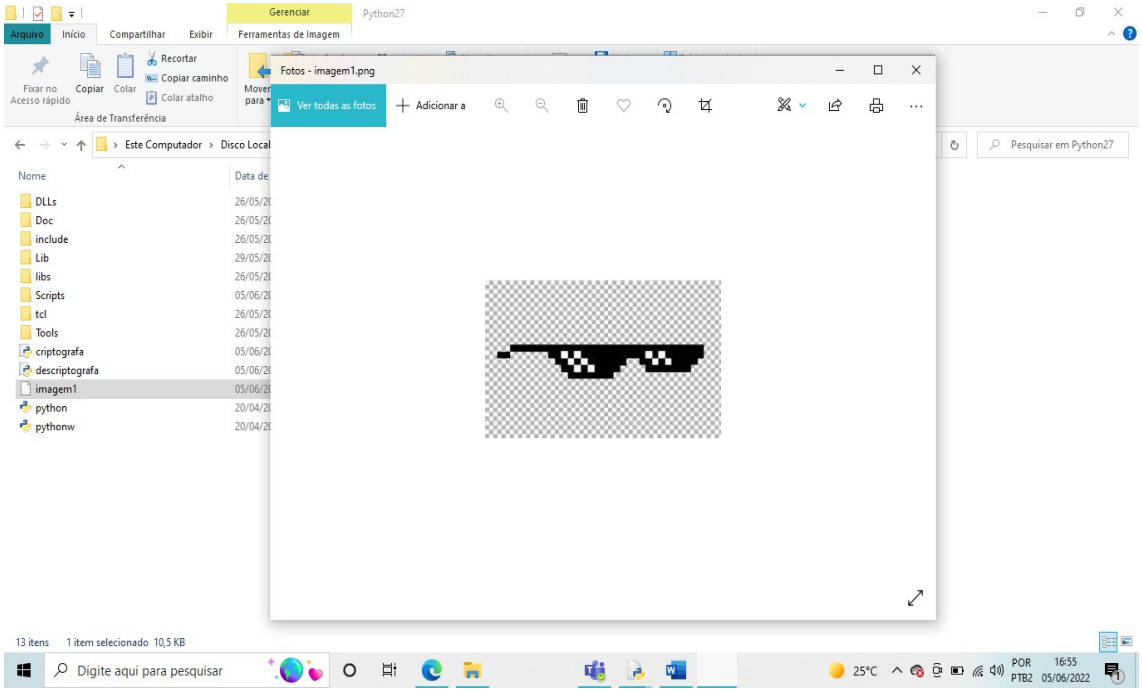
Figura 6 Script executado sem nenhum erro



Fonte: Próprios autores

Ao executar o script a imagem voltará à sua forma original, como mostra a Figura 7.

Figura 7 Imagem recuperada



6. Conclusão

Conclui-se que as políticas de segurança da informação são responsáveis por treinar, esclarecer e tentar prevenir possíveis ataques, além de evoluir e se atualizar juntamente com a técnicas utilizadas por criminosos.

Este trabalho permitiu um aprofundamento no tema, desde seus pontos de evoluções históricas até o atual momento, permitiu uma visão teórica e prática sobre o *Ransomware,* apresentando sua evolução durante os anos e de que forma os criminosos vem se atualizando para continuar extorquindo empresas através do sequestro de dados. Necessita-se também um aprofundamento em relação a vulnerabilidade em relação a engenharia social, que não pode ser sanada por ferramentas automatizadas e necessita de treinamento e conscientização constante dos funcionários sobre os perigos de ataques cibernéticos.

Através do script apresentado como trabalho prático, notou-se que a criptografia bloqueia o arquivo usando chave simétrica, ao aplicar o script que descriptografa a imagem, ele compara a chave e descriptografa a imagem, devolvendo o acesso ao arquivo, utilizando-se das bibliotecas Python apresentadas (PYEAS e OS).

Todos os objetivos propostos foram cumpridos, porém é importante ressaltar que não somente treinamento, conhecimento e conscientização em relação ao tema são suficientes para combater este tipo de ataque, é necessário estar sempre se atualizando, como notado não só este *malware* (*Ransomware*), vem evoluindo e se atualizando e é preciso que a segurança da informação continue fazendo seu papel de se atualizar juntamente, para evitar novos ataques.

REFERÊNCIAS

AVAST. **Guia básico sobre *ransomware***. Avast Academy, publicado em 24 de setembro de 2021. Disponível em: https://www.avast.com/pt-br/c-what-is-ransomware#:~: text=Ransomware%20%C3%A9%20um%20tipo%20de, os%20inutiliz%C3%A1veis%20para%20as%20v%C3%ADtimas. Acesso em: 14 abr. 2022.

CONJUNTURA ECONÔMICA. Déficit de profissionais de TI pode chegar a meio milhão até 2025. **Conjuntura Econômica**, 02 de dezembro de 2021. Disponível em: https://ibre.fgv.br/blog-da-conjuntura-economica/artigos/deficit-de-profissionais-de-ti-pode-chegar-meio-milhao-ate-2025. Acesso em: 14 maio 2022.

CISCO. **Ataques de *ransomware* superam a casa de 623 milhões em 2021**. Cisco Advisor, publicado em 17 de fevereiro de 2022. Disponível em: https://www.avast.com/pt-br/c-what-is-ransomware#:~:text=Ransomware% 20%C3%A9%20um%20tipo%20de,os%20inutiliz%C3%A1veis%20para%20as %20v%C3%ADtimas. Acesso em: 20 maio 2022.

FONTES, Edison. **Segurança da informação**: o usuário faz a diferença. São Paulo: SARAIVA, 2006.

CRIPTOID. **Criptografia simétrica e assimétrica: Qual a diferença entre elas?** Publicado em: 08 de novembro de 2017. Disponível em: https://cryptoid.com.br/banco-de-noticias/29196criptografia-simetrica-e-assimetrica/#:~:text=A%20criptografia%20sim%C3%A9trica%20faz%20uso,algoritmo%20vai%20cifrar%20um%20conte%C3%BAdo. Acesso em: 03 maio 2022.

Hintzbergen Jule, Hintzbergen Kees, Smulders André, Baars Hans. **Fundamentos da Segurança da Informação: definição de informação.** São Paulo: Editora Brasport, 2018.

IET. **Evolution of *ransomware***. Institute of Engineering and Technology. Publicado em 01 de setembro de 2018. Disponível em: https://ietresearch. onlinelibrary.wiley.com/doi/full/10.1049/iet-net.2017.0207 Acesso em: 18 maio 2022.

INSPER. **Mundo se aproxima da marca de 5 bilhões de usuários de internet, 63% da população.** INSPER. Publicado em 15 de fevereiro de 2022. Disponível em: https://www.insper.edu.br/noticias/mundo-se-aproxima-da-marca-de-5-bilhoes-de-usuarios-de-internet-63-da-populacao/ Acesso em: 21 maio 2022.

ISTO É. DINHEIRO. **Brasil foi o 5º país com mais ataques cibernéticos no ano.** Isto é dinheiro. Publicado em 20 de dezembro de 2021. Disponível em: https://www.istoedinheiro.com.br/brasil-foi-5o-pais-com-mais-ataques-ciberneticos-no-ano-relembre-os-principais/ Acesso em: 17 abril 2022.

KASPERSKY**. Engenharia social**: definição. A definição do que é a engenharia social**.** Disponível em: https://www.kaspersky.com.br/resource-center/ center/definitions/what-is-social-engineering Acesso em: 20 maio 2022.

NEXO. **Primeiro site da história entrou no ar há 30 anos.** Nexo Jornal. Publicado em 06 de agosto de 2021. Disponível em: https://www.nexojornal. com.br/extra/2021/08/06/Primeiro-site-da-hist%C3%B3ria-entrou-no-ar-h%C3%A1-30-anos#:~:text=O%20primeiro%20website%20do%20mundo, ar%20em%20sua%20forma%20original. Acesso em: 08 maio 2022.

NORTON. **Ameaças emergentes, informando os tipos de ataques de engenharia social.** Disponível em: https://br.norton.com/internetsecurity-emerging-threats-what-is-social-engineering.html Acesso em: 19 abril 2022.

NSC TOTAL. **Porque a gestão da informação é fundamental para as empresas.** Disponível em: https://www.nsctotal.com.br/noticias/por-que-a-gestao-da-informacao-e-fundamental-para-as-empresas. Acesso em: 09 junho 2022.

SIGHT INFORMÁTICA. **Saiba o que é *malware ransomware* e seus perigos.** Disponível em: www.sightinformatica.com.br. Acesso em: 27 maio 2022.

SIQUEIRA, Fernando. **Sistemas de computação e de informação.** Disponível em: https://sites.google.com/site/uniplisistemasdeinfogerenciais/aulas/1---conceitos-de-tecnologia-de-informacao Acesso em: 18 maio 2022.

TIINSIDE**. Brasil sofreu mais de 33 milhões de tentativas de *ransomware* em 2021**. https://tiinside.com.br/18/02/2022/brasil-sofreu-mais-de-33-milhoes-de-tentativas-de-ransomware-em-2021/. Acesso em: 04 maio 2022.

ZAPATER, Márcio Suzuki Rodrigo. Segurança da informação. **Business & Technology Review**. São Paulo: Editora Promon. Disponível em: https://www.teleco. com.br/promon/pbtr/Seguranca_4WEB.pdf Acesso em: 27 abr. de 2022.