FACULDADE DE TECNOLOGIA DE AMERICANA – MINISTRO RALPH BIASI

Curso Superior de Tecnologia em Segurança da Informação

Douglas Cordeiro da Graça

Rodrigo Vieira de Souza

Ransomwares: uma ameaça crescente.

Americana, SP

2020

Faculdade de Tecnologia de Americana "Ministro Ralph Biasi"

Curso Superior de Tecnologia em Segurança da Informação

Douglas Cordeiro da Graça

Rodrigo Vieira de Souza

Ransomwares: uma ameaça crescente

Trabalho de Conclusão de Curso desenvolvido em cumprimento à exigência curricular do Curso Superior de Tecnologia em Segurança da Informação, sob a orientação da Prof.(a) Dr. Maria Cristina Aranda.

Área de concentração: Segurança da informação.

Americana, SP.

2020

FICHA CATALOGRÁFICA – Biblioteca Fatec Americana - CEETEPS
Dados Internacionais de Catalogação-na-fonte

G753r GRAÇA, Douglas Cordeiro da

Ransomwares: uma ameaça crescente. / Douglas Cordeiro da Graça, Rodrigo Vieira de Souza. – Americana, 2020.

46f.

Monografia (Curso Superior de Tecnologia em Segurança da Informação) - - Faculdade de Tecnologia de Americana – Centro Estadual de Educação Tecnológica Paula Souza

Orientador: Profa. Dra. Maria Cristina Aranda

1 Segurança em sistemas da informação 2. Ransomware I. SOUZA, Rodrigo Vieira de II. ARANDA, Maria Cristina III. Centro Estadual de Educação Tecnológica Paula Souza – Faculdade de Tecnologia de Americana

CDU: 681.518.5

Douglas Cordeiro da Graça
Rodrigo Vieira de Souza

Ransomwares: uma ameaça crescente.

Trabalho de graduação apresentado como exigência parcial para obtenção do título de Tecnólogo em Segurança da Informação pelo CEETEPS/Faculdade de Tecnologia – FATEC/ Americana.
Área de concentração: Segurança da Informação.

Americana, 22 de julho de 2020.

Banca Examinadora:

_____
Maria Cristina Aranda (Presidente)
Doutora
FATEC de Americana

_____
Paula da Fonte Sanches (Membro)
Mestre
FATEC de Americana

_____
Alberto Martins Junior
Mestre
FATEC de Americana

AGRADECIMENTOS

Eu Rodrigo, agradeço primeiramente a Deus por me proporcionar forças e foco para concluir a minha primeira graduação e este trabalho.

Agradeço à minha querida mãe Elaine Cristina por sempre me apoiar em minhas decisões e nunca me deixar desistir.

Aos amigos Alberto, Douglas e Rafael que me proporcionaram ótimos momentos e me ajudaram a sempre continuar e concluir as tarefas necessárias.

Agradeço à minha namorada Mirella por me aconselhar e nunca me deixar desistir.

E um agradecimento especial para a orientadora Doutora Maria Cristina Aranda por nos ajudar e nos direcionar para que este trabalho fosse concluído.

Eu Douglas, agradeço a Deus que guia cada passo de minha vida, e, se estou aqui é por conta dEle.

Agradeço à minha noiva Bruna, que por muitas e muitas vezes esteve disponível para me ajudar e incentivar, mostrando que a vida, quando vivida por duas pessoas com o mesmo foco é muito mais fácil.

A meus pais, Gilberto e Gisela por me incentivarem a sempre olhar em frente e me ensinarem os princípios para que eu pudesse estar aqui. Agradeço a minha irmã Larissa por me apoiar e ajudar sempre que precisei.

Aos meus amigos Alberto, Rafael e Rodrigo por todos os inesquecíveis momentos que vivemos nesses três anos, que parecem mais terem sidos poucos meses. Todo sucesso para vocês, meus amigos!

Agradeço especialmente a professora Doutora Maria Cristina Aranda que, sempre com um sorriso no rosto, nos ajudou a enxergar que um TCC não é um bicho de sete cabeças.

RESUMO

Nos últimos anos, uma rápida e crescente proliferação de diferentes tipos de *malwares* (softwares maliciosos) direcionados a usuários comuns, empresas e até mesmo às estruturas críticas de infraestrutura está afetando sistemas de informação ou redes inteiras de computadores. Um desses *malwares* é o *ransomware,* que é criado com a finalidade de bloquear arquivos ou computadores, podendo tornar alguns dados e informações inacessíveis a seus proprietários, sendo que só serão desbloqueados a partir do pagamento de resgaste (*ransom*) por parte do usuário. A partir do aumento da propagação desse tipo de virus, o presente trabalho foca a segurança da informação com ênfase no s*oftware* malicioso *ransomware*. A abordagem aqui apresentada contextualizará esse *malware* na segurança da informação e como mitigá-lo. A remoção do mesmo não é simples, necessitando recuperar os dados encriptados através de ferramentas específicas ou mantendo cópias de segurança atualizadas. O trabalho culminará com a demonstração do funcionamento real de um *ransomware* e formas de como remover esse vírus, visando essa apresentação ser de cunho didático.

Palavras Chaves: *Segurança da Informação, Ransomware, Software Malicioso.*

ABSTRACT

In recent years, a rapid and growing proliferation of different types of malware (malicious software) targeting common users, businesses and even critical infrastructure structures is affecting information systems or entire computer networks. One such malware is ransomware, which is created for the purpose of blocking files or computers and can make some data and information inaccessible to its owners and will only be unlocked after the user has paid for ransom. Based on the increase in the spread of this type of virus, this paper focuses on information security with an emphasis on malicious software ransomware. This paper will put this malware in context of information security and how to mitigate it. Remove it is not simple, will be needed to recover encrypted data using specific tools or keeping up-to-date backup copies. The work will culminate with the demonstration of the real functioning of a ransomware and ways on how to remove this virus, aiming this presentation to be didactic.

Keywords: *Information Security, Ransomware, Malicious Software.*

SUMÁRIO

1 INTRODUÇÃO

No dia 27 de abril de 2016 foi emitida a *regulation* [1] (EU) 2016/679, a GDPR (*General Data Protection Regulation*) da União Europeia, dando início a uma era digital totalmente nova, uma era digital de privacidade, *compliance* [2] e proteção de dados e identidades que as organizações possuem de qualquer indivíduo físico ou jurídico. Ao todo, foram dois anos e vinte e oito dias de adequações para a União Europeia e do Espaço Econômico Europeu (EEE) até a sua sanção definitiva, no dia 25 de maio de 2018.

Após a criação da GDPR, a necessidade de criação de uma lei nacional tanto para acompanhar a evolução da proteção dos dados quanto para continuar a comercialização com os países que estão sob regulamentação da GDPR se tornou uma obrigação. Assim foi planejada a implantação da LGPD (Lei Geral de Proteção de Dados), para que as empresas do território nacional se adequassem quanto a proteção de quaisquer dados pessoais que tenham em posse.

Com isso, a preocupação quanto ao vazamento de dados pessoais de seus clientes e colaboradores se elevou e deu espaço a um novo e emergente tipo de ataque às organizações, os *ransomwares* [3].

Os *ransomwares* já existem a décadas e suas variações estão crescendo exponencialmente com o intuito de se espalhar, fugir da detecção, criptografar os arquivos e convencer os usuários a pagar o resgate requerido. Mas os *ransomwares* da atualidade são um pouco mais complexos, com técnicas cada vez mais avançadas de desenvolvimento, dificultando extremamente a probabilidade de que seja executada uma engenharia reversa e, além disso, estão com seus ataques cada vez mais direcionados. Com a chegada da indústria 4.0 e a GDPR/LGPD os ataques desse tipo de código malicioso tem aumentado cada vez mais, porque se tornaram (no caso do Brasil, se tornarão, já que ainda não foi atingida a data limite da *vacatio legis* [4]) uma forma muito lucrativa de ataque, já que os dados vazados por uma empresa acarretariam em uma multa que pode chegar a milhões de dólares,

[1] Regra ou diretiva feita e mantida por uma autoridade.
[2] Conformidade.
[3] Tipo de software malicioso.
[4] Período entre a data de publicação de uma lei e o início de sua vigência.

suspensões das atividades da empresa por determinados período de tempo afetando as porcentagens de faturamento anual. E os atacantes cientes destes fatos, estão adaptando os *ransomwares* para serem capazes de enviar uma cópia de todo o conteúdo desses dados para servidores remotos que seus criadores possuem. Com isso, passam a ter em seu poder muitas informações sensíveis que vazadas, seriam passíveis de multa perante a GDPR/LGPD, potencializando o poder de extorsão dos atacantes.

Partindo desse ponto e de considerações de algumas grandes empresas como a KnowBe4, pode-se prever que os ataques de *ransomware* se tornarão cada vez mais comuns e cada vez mais caros para as organizações, isso se os atacantes não decidirem espalhar os dados sequestrados pela Internet por motivos diversos, como por exemplo, vingança ou diversão.

Outro grande problema é que não se trata apenas de um *malware* [5] criptografando e fazendo cópias de arquivos, mas sim um problema de amplitude similar que surgiu antes dos *ransomwares*, porém, caminham juntos, e é conhecido como *wiper*. No início da Internet, os *wipers* [6] foram um dos primeiros ataques virtuais, que comprometiam o disco rígido de computadores e apagavam todos os seus arquivos. O principal objetivo dos criminosos digitais que fazem esses ataques era a fama na rede. Esse tipo de *malware* pode vir a ser um problema ainda maior, uma vez que ele pode facilmente infectar um banco de dados e destruí-lo. Neste cenário, caso o administrador não tenha um *backup* [7] atualizado deste banco, perderá informações cruciais para a continuidade do negócio.

[5] Software malicioso.
[6] Software de limpeza total de discos rigidos.
[7] Cópia de segurança.

2 REFERENCIAL BIBLIOGRÁFICO

2.1 SEGURANÇA DA INFORMAÇÃO

Segundo Kaspersky [s.d.], a cibersegurança é a prática de defender computadores, servidores, dispositivos móveis, sistemas eletrônicos, redes e dados contra-ataques maliciosos. Também é conhecido como segurança da informação ou segurança da informação eletrônica. O termo se aplica em diversos contextos do mundo tecnológico e pode ser dividido em categorias:

- A segurança do aplicativo: se concentra em manter o *software* e os dispositivos livres de ameaças. Um aplicativo comprometido pode fornecer acesso aos dados aos quais ele foi projetado para proteger. A segurança bem-sucedida começa no estágio de *design*, muito antes de um programa ou dispositivo ser implantado.
- A segurança das informações: protege a integridade e a privacidade dos dados, tanto no armazenamento quanto no transporte.
- Segurança operacional: inclui os processos e decisões para manipular e proteger ativos de dados. As permissões que os usuários têm ao acessar uma rede e os procedimentos que determinam como podem ser armazenados ou compartilhados.
- Um evento que cause perda de dados ou qualquer incidente de segurança cibernética: nas operações, deve ser tratada no plano de recuperação de desastres, que irá definir como uma organização responde a qualquer um desses eventos. A restauração de informações, retornando à mesma capacidade operacional que antecede o evento, são tratadas nas políticas de recuperação de desastres. Continuidade dos negócios é o plano que a organização utiliza quando assume operar sem a totalidade dos seus recursos.
- O fator humano: é o fator mais imprevisível da segurança cibernética, por isso deve ser adotada a “educação do usuário final”. Sem as boas práticas do uso dos recursos computacionais, acidentalmente, o usuário pode introduzir um vírus em um sistema seguro. É vital para qualquer organização, conscientizar os usuários sobre os riscos de abrir anexos de e-mail suspeitos, conectar unidades USB não identificadas e outras lições.

2.1.1 OS PRINCIPAIS ATRIBUTOS DA SEGURANÇA DA INFORMAÇÃO

Na área da segurança da informação, existem os principais atributos (pilares) que necessitam ser rigorosamente seguidos para que se tenha um ambiente com controle e mitigação das ameaças, sejam estas internas ou externas. Segundo Telium (2018), são:

I. Disponibilidade: tem relação com o tempo e à acessibilidade aos dados e sistemas de uma organização, isto é, se estes dados e sistemas podem ser acessados e/ou consultados por qualquer pessoa autorizada sempre que necessite.

> A disponibilidade pode ser garantida de forma mais eficiente por meio da implantação de processos de manutenção rápida de hardwares e eliminação de conflitos de *software* graças à priorização de programas compatíveis. É essencial utilizar uma infraestrutura tecnológica voltada à manutenção e preservação do acesso aos dados. (TELIUM, 2018)

Para garantir a Internet da organização sempre ativa, ou seja, para que os colaboradores naveguem pela *web* ou enviem *e-mails* sem transtorno é indicado contratar um *link* redundante de um outro provedor de Internet. Também é muito importante que se realize as atualizações necessárias dos sistemas e seus aplicativos/programas periodicamente, bem como utilizar um *link* principal com largura de banda de comunicação que atenda a demanda da organização.

É de extrema importância que a organização crie e implemente um Plano de Recuperação de Desastres (*Disaster Recovery* DR) que contenha procedimentos e diretrizes para administrar possíveis crises e manter a continuidade do negócio. A necessidade deste plano, é importante não só para remediar possíveis ataques virtuais, “como para se proteger de catástrofes naturais (enchentes, desmoronamentos de terra etc.) e eventos que podem prejudicar os equipamentos da empresa (incêndios, blecautes, entre outros.” (TELIUM, 2018).

A organização deve sempre contar com um eficiente sistema de *backup* para recuperar os dados caso seja impossível recuperar *hardwares* os dados que estão armazenados neles por qualquer motivo. Um exemplo é o *backup* em nuvem, onde uma outra organização que mantém *data centers* [8], servidores e outros recursos

[8] Centro de processamento de dados.

computacionais necessários provê um serviço de armazenagem dos dados e informações dos sistemas de determinada organização contratante de forma automática e remota, via Internet.

II. Integridade: está relacionada à confiabilidade e precisão da informação, ou seja, garante que nenhuma informação foi alterada, e está correta, verdadeira e não corrompida. “Para garantir a integridade dos dados, é possível implementar soluções de controle de acesso**,** não só para saber quem modificou determinada informação, mas também para garantir que a pessoa que acessou é realmente quem ela disse ser.” (ESET, 2018).

De acordo com Wireshark [s.d], existem vários procedimentos e ferramentas com a finalidade de reforçar a integridade das informações da organização, são elas:

a) Definir permissões nos arquivos e diretórios do sistema, isto é, permitir que estes sejam acessados somente por usuários que realmente necessitem;

b) Usar *checksums* [9] nas transmissões de dados em uma rede geralmente verificam diversos erros, dentre estes erros existem os *bits* [10] duplicados, faltantes e alterados, ou seja, quando os arquivos são transmitidos e ocorrem um ou mais erros como estes, os dados que foram recebidos podem não ser os mesmos que foram enviados pela origem. Este mecanismo checa a integridade dos arquivos que são transmit *bytes* idos pela rede ou antes de serem armazenados através de checagem de em determinado arquivo, uma vez que os *bytes* de saída da origem devem coincidir com os bytes que chegam ao destino.

> O uso de uma soma de verificação reduz drasticamente o número de erros de transmissão não detectados. No entanto, os algoritmos usuais de soma de verificação não podem garantir uma detecção de erro de 100%, portanto, um número muito pequeno de erros de transmissão pode permanecer sem ser detectado. (WIRESHARK, [s/d]).

Além destes mecanismos a serem implementados nos sistemas da organização, Telium (2018), alega que é necessário que existam certas instruções, orientações e políticas para que os colaboradores da empresa não possam fazer

[9] Método de verificação de dados.
[10] Menor unidade de medida para mensurar dados de computador.

alterações em dados que não são de sua autoria ou que não tenham recebido permissão para tal.

III. Confidencialidade: significa que a informação deve ser acessada somente por quem realmente necessita dela para realizar as atividades profissionais estabelecidas pela organização, porém, deve-se existir uma autorização prévia do detentor da informação para que tal acesso seja realizado. De acordo com ESET (2018), existem alguns procedimentos para garantir a confidencialidade dos dados de uma organização que são:

a) Definir acesso às informações de forma hierárquica, isto é, permitir que funcionários com cargos hierárquicos mais elevados na organização tenham mais acessos que os de cargo hierárquico mais baixo, como também separar permissões de acesso a informações por áreas da organização, como recursos humanos, departamento pessoal, expedição, vendas etc. Uma boa forma de se definir esta separação hierárquica de acessos é categorizar os dados conforme o nível de impacto às operações da empresa caso sejam vazados e/ou sequestrados por cibercriminosos;

b) Efetuar treinamentos com os colaboradores que lidam com as informações sensíveis para ensiná-los a operar estes dados com maior perícia e terem as noções devidas dos riscos em casos de quebra de confidencialidade destes dados. Além disto, é necessário conscientizar e incentivar de uma forma geral os colaboradores para que sigam as políticas e os procedimentos estabelecidos de forma adequada;

c) Implementar nas infraestruturas de redes verificações biométricas para acesso a determinadas áreas da organização, usar dois fatores de autenticação para prevenir acessos não autorizados a computadores, dispositivos ou celulares de colaboradores. Também é necessário implementar criptografia nos dados que sejam de alto risco para a organização, assim como o uso de ferramentas de proteção de

rede e sistemas como *firewalls* [11], *honeypots* [12], *hashing* [13], antivírus, *antispywares* [14] dentre outros.

IV. Legalidade: Este pilar define que o uso da informação deve estar de acordo com a lei vigente local, além de seguir os regulamentos, licenças e contratos.

V. Auditabilidade: Garante que seja feito um registro de acesso e uso da informação para identificação de quem fez o acesso e quais foram as alterações feitas na informação, ou seja, deve ser possível conferir o que foi feito com determinada informação, havendo também a possibilidade de rastreamento de quem fez e quando fez.

VI. Não repúdio de autoria: este pilar tem como objetivo provar que um determinado usuário que alterou ou gerou uma informação não possa negar o fato, mediante a existência de algumas ferramentas e mecanismos que garantem a autoria do usuário naquela informação, como por exemplo em contas de usuário, sistema de armazenamento de logs[15], assinaturas digitais, etc.

Todos estes pilares/atributos existem com um único objetivo, minimizar os riscos perante as ameaças que afligem a segurança da informação.

2.1.2 AMEAÇAS À SEGURANÇA DA INFORMAÇÃO

Segundo Bishop e Oliveira (2008), a ameaça é uma potencial violação de segurança. Esta violação não precisa efetivamente ocorrer para ser considerada uma ameaça, ou seja, refere-se a qualquer tipo de ocorrência ou atitude prática indesejada que possa desabilitar, remover ou deletar completamente um dado ou

[11] Parte de um sistema ou rede designada para liberar ou bloquear comunicação.
[12] Técnica utilizada para detectar tentativas de acesso não autorizado.
[13] Método de criptografia.
[14] Programa de computador designado para detectar programas espiões não desejados.
[15] Arquivo de registro que salva as interações com o sistema operacional.

informação. As ameaças geralmente se aproveitam de certas falhas de segurança da informação que existam em uma organização.

Para Gomes (2015), existem algumas categorias de ameaças:

I. Ameaças internas: As ameaças internas muitas vezes podem ser causadas por um tipo de atacante denominado como *insider* [16]. Este tipo de atacante é geralmente um funcionário em atuação na empresa, um ex-funcionário ou até um prestador de serviço que atuou por algum motivo na empresa e teve acesso a informações importantes da empresa. Geralmente os *insiders* motivam-se por descontentamento financeiro ou por uma insatisfação pessoal e roubam informações sensíveis da empresa, com o objetivo de causar prejuízos. Caso este tipo de atacante interno vise vender os dados coletados para conseguir ganhos extras sem a ciência da empresa empregadora, sua ação é considerada uma ameaça intencional, pois ele premedita suas ações com um objetivo pré-estabelecido

Segundo Proof (2018), outro tipo de ameaça interna e é considerada acidental, quando um funcionário mal treinado ou desinformado cai em alguma forma de fraude virtual como por exemplo, o *phishing* [17]. Este funcionário geralmente não tem muito conhecimento em computação e tampouco em segurança da informação, somando isso à falta de treinamento e negligência, pode-se ter um incidente de segurança dentro da organização.

II. Ameaças externas: de acordo com Cruz [s.d], os sistemas modernos de computadores comerciais são complexos e distribuídos. Além da rede interna de uma organização, muitos componentes importantes residem na Internet que é pública. Isso significa que uma cadeia complexa de eventos pode afetar um banco de dados de TI (Tecnologia da Informação) de maneiras imprevisíveis. Por exemplo, uma forte tempestade em uma região do país pode reduzir a energia de um servidor que armazena licenças de *softwares*. Com as licenças indisponíveis, o *software* de *backup* do banco de dados pode não funcionar no horário agendado, deixando o banco de dados aberto à corrupção irreversível. Mas, os ataques mais assustadores vêm de

[16] Programa de computador externo malicioso.
[17] Prática fraudulenta com intuito de induzir o funcionário a revelar informações confidenciais como senhas e números de cartão de créditos.

hackers [18] externos qualificados e sofisticados. Esses invasores podem encontrar vulnerabilidades da rede ou manipular socialmente pessoas internas, por meio da engenharia social para superar as defesas externas da rede. Como os aplicativos de *software* de uma organização mantêm conexões abertas com os bancos de dados de TI, os *hackers* procuram assumir o controle desses aplicativos depois de entrarem, geralmente buscando senhas padrão de aplicativos.

2.2 MALWARE

Segundo Sans [s.d], o termo *malware* deriva das palavras inglesas *malicious* (malicioso) e *software* (programa). Os *malwares* desempenham um papel importante quando se fala em incidentes de segurança e intrusões a computadores. De uma forma geral, os *malwares* são todo tipo de programa de computador que tem como objetivo causar danos a usuários, computadores ou redes. Diversos cibercriminosos instalam este tipo de *software* em computadores para tomar controle ou ganhar acesso aos seus arquivos e sistemas. Uma vez que o *malware* está instalado no computador da vítima, o criador deste tipo de código malicioso pode utilizar-se dele para espionagem de atividades *online* [19] da vítima afetada, roubar suas senhas e arquivos ou utilizar o computador infectado para executar ataques *online* a outros computadores. Um *malware* também pode ser desenvolvido para bloquear o acesso das vítimas aos seus arquivos, requerendo um pagamento *online* para a total liberação do sistema do computador juntamente com todos os arquivos.

2.2.1 TIPOS DE MALWARE

Segundo o CERT.br (2017), existem variados tipos de *malware*, e em geral são programas com códigos maliciosos especificamente desenvolvidos para executar atividades nocivas e atividades maliciosas em um computador. Seus principais tipos

[18] Expert em computação que usa seu conhecimento técnico para encontrar e reportar vulnerabilidades no mundo da computação.
[19] Conectado à rede global de computadores.

são classificados como: vírus, *worm*, *botnet*, *trojan*, spyware, *backdoor*, *rootkit* e *ransomware*.

Vírus: o *malware* classificado como vírus é um programa ou parte de um programa de computador, normalmente malicioso, que se propaga inserindo cópias de si mesmo e tornando-se parte de outros programas e arquivos. Estes vírus se propagam por *e-mails*, *scripts*[20], macros e mensagens MMS (*Multimedia Message Service*[21]). Geralmente este tipo de *malware* procura permanecer oculto no sistema para executar uma série de atividades sem o conhecimento do usuário.

Worm: *malware* do tipo *worm* é um programa malicioso capaz de se propagar automaticamente pelas redes de computadores, enviando cópias de si mesmo de computador para computador. Seu processo de propagação é feito por meio da execução direta de suas cópias ou pela busca e exploração automatizada de vulnerabilidades pré-programadas em seu código, e que sejam existentes em programas instalados nos computadores. O processo de propagação deste tipo de *malware* é bem rápida e ocorre da seguinte forma: após o primeiro computador ser infectado, o *worm* passa a identificar os computadores que estão na mesma rede ou que estão se comunicando com o hospedeiro, então, inicia um processo de envio de cópias de si mesmo para todos os computadores identificados. Assim que os demais computadores recebem as cópias, e estas são ativadas, o ciclo se reinicia.

Bot e *botnet*: Os *bots* são programas feitos para proporcionar comunicação remota entre o invasor e o hospedeiro. Este tipo de *malware* tem sua forma de propagação muito semelhante ao *worm*, ou seja, é capaz de se espalhar de forma automatizada explorando vulnerabilidades nos sistemas e aplicativos dos computadores. Os computadores afetados pelo *bot* são chamados de zumbis, pois podem ser controlados remotamente pelo seu criador, que após infectar centenas ou até milhares de outros computadores cria uma *botnet*, utilizado muitas vezes para ataques DDoS (Distributed Denial Of Service [22]), esse tipo de ataque é feito para derrubar *sites* e servidores enviando múltiplas solicitações até exceder a capacidade

[20] Conjunto de instruções para que uma função seja executada em determinado aplicativo.
[21] Método padrão de envio de mensagem que contém multimídia.
[22] Técnica utilizada para tirar de operação um sistema de comunicação.

que o *site* ou servidor tem de lidar com estas solicitações, fazendo com que parem de funcionar corretamente.

Spyware: *spyware* ou programa espião, é um programa criado para monitorar e capturar as atividades de um sistema de computador e enviá-las a terceiros. Pode ser usado de forma legítima (quando instalado em um computador de uso próprio pelo seu dono ou com o consentimento do mesmo, com o objetivo de verificar se o computador está sendo utilizado de forma errônea ou não autorizada) ou de forma maliciosa (quando é instalado de forma não consentida pelo dono do computador e é utilizado para roubar informações ou dados, quebrando totalmente a privacidade do usuário e a segurança do computador). Alguns tipos específicos de programas *spyware* são os *keyloggers*[23], *screenloggers*[24] e os *adwares*[25].

Backdoor: o *malware* do tipo *backdoor* é um programa que permite ao invasor retornar de forma livre a um computador que foi comprometido anteriormente por meio da inserção de serviços criados ou modificados propositalmente para este fim. Pode ser introduzido no computador alvo por outros programas maliciosos que tenham o infectado anteriormente ou diretamente por atacantes que exploram vulnerabilidades nos programas instalados no computador alvo. Existem ainda os casos dos *backdoors* implementados de forma proposital por fabricantes de aplicativos, com a alegação de que o uso destes seria somente para atividades administrativas, o que é uma forma muito invasiva e que afeta muito a segurança do computador e a privacidade do usuário.

Cavalo de troia ou *trojan-horse*: *malware* chamado de cavalo de troia, *trojan* ou *trojan-horse* é um programa criado para executar as funções para as quais foi feito e, além disso, também executa outras funções que são normalmente mal-intencionadas e sem o consentimento e conhecimento do usuário do computador em que está hospedado. Alguns exemplos deste tipo de *malware* são programas que algum usuário recebe ou faz o *download* de *sites* na Internet e que parecem ser inofensivos, como por exemplo, cartões virtuais animados, jogos ou fotos. São

[23] Programa de computador que registra as interações do usuário com o teclado.
[24] Programa de computador que registra as imagens exibidas no monitor.
[25] Programa de computador que automaticamente exibe ou baixa material de propaganda.

geralmente implantados nesses tipos de arquivos pois necessitam ser executados pelo usuário para que sejam instalados no computador.

Rootkit: o *malware* categorizado como *rootkit* é um conjunto de programas e técnicas que possibilita disfarçar e manter a presença de um atacante ou de outro programa malicioso em um computador alvo. O conjunto deste tipo de *malware* pode ser utilizado para remover evidências em arquivos de *logs* [26]; instalar outros tipos de códigos maliciosos, como os *backdoors* para garantir acesso posterior; esconder atividades e informações dentro de um computador comprometido; mapear a rede em que se encontra o computador comprometido e buscar por vulnerabilidades em outros computadores e executar ferramentas para roubar informações da rede na qual o computador comprometido está, através da interceptação de tráfego.

3 RANSOMWARE

Segundo Mcafee [s/d], o *malware* denominado *ransomware* é um programa malicioso que emprega uma técnica de criptografia de dados de alta complexidade nos arquivos do computador infectado, impossibilitando o acesso do usuário aos seus arquivos, base de dados ou aplicações. Seu nome deriva de *ransom* (resgate) e *software* (programa), pois para que o usuário seja autorizado a acessar seus dados é necessário que pague um valor requerido pelos cibercriminosos. Geralmente, os criadores de um ransomware o projetam para se espalhar por uma rede de computadores e se direcionar a servidores de banco de dados contendo arquivos importantes e de necessidade diária de uma organização ou empresa. É uma ameaça que está se expandindo gradativamente gerando centenas de milhões de dólares de prejuízos em pagamentos de resgate de dados aos cibercriminosos que os criam e em danos e despesas para as organizações afetadas.

[26] Processo de coletar e armazenar dados sobre um período.

3.1 COMO FUNCIONA UM RANSOMWARE

Segundo Mcafee [s/d], o *ransomware* usa criptografia assimétrica. Essa criptografia usa um par de chaves para criptografar e descriptografar um arquivo. O par de chaves público-privado é gerado exclusivamente pelo atacante para a vítima, com a chave privada para descriptografar os arquivos armazenados no servidor do atacante. O atacante disponibiliza a chave privada à vítima somente após o pagamento do resgate, embora, como nas últimas ondas de *ransomwares*, esse nem sempre seja o caso. Sem acesso à chave privada, é quase impossível descriptografar os arquivos que estão sendo retidos para resgate.

Existem muitas variações de *ransomwares*. Geralmente, o *ransomware* é distribuído usando campanhas de *spam* por *e-mail* ou por meio de ataques direcionados. O *malware* precisa de um vetor de ataque (*phishing*, *download* direto, vulnerabilidades em sistemas, etc.) para estabelecer sua presença em um *endpoint* [27] (computador pessoal ou servidor). Depois que tal presença é estabelecida, o *malware* permanece no sistema até que sua tarefa seja concluída.

Após uma exploração bem-sucedida, o *ransomware* descarta e executa um binário malicioso no sistema infectado. Esse binário pesquisa e criptografa arquivos valiosos, como documentos, imagens, bancos de dados e assim por diante. O *ransomware* também pode explorar vulnerabilidades de sistema e rede para se espalhar para outros sistemas e possivelmente para organizações inteiras.

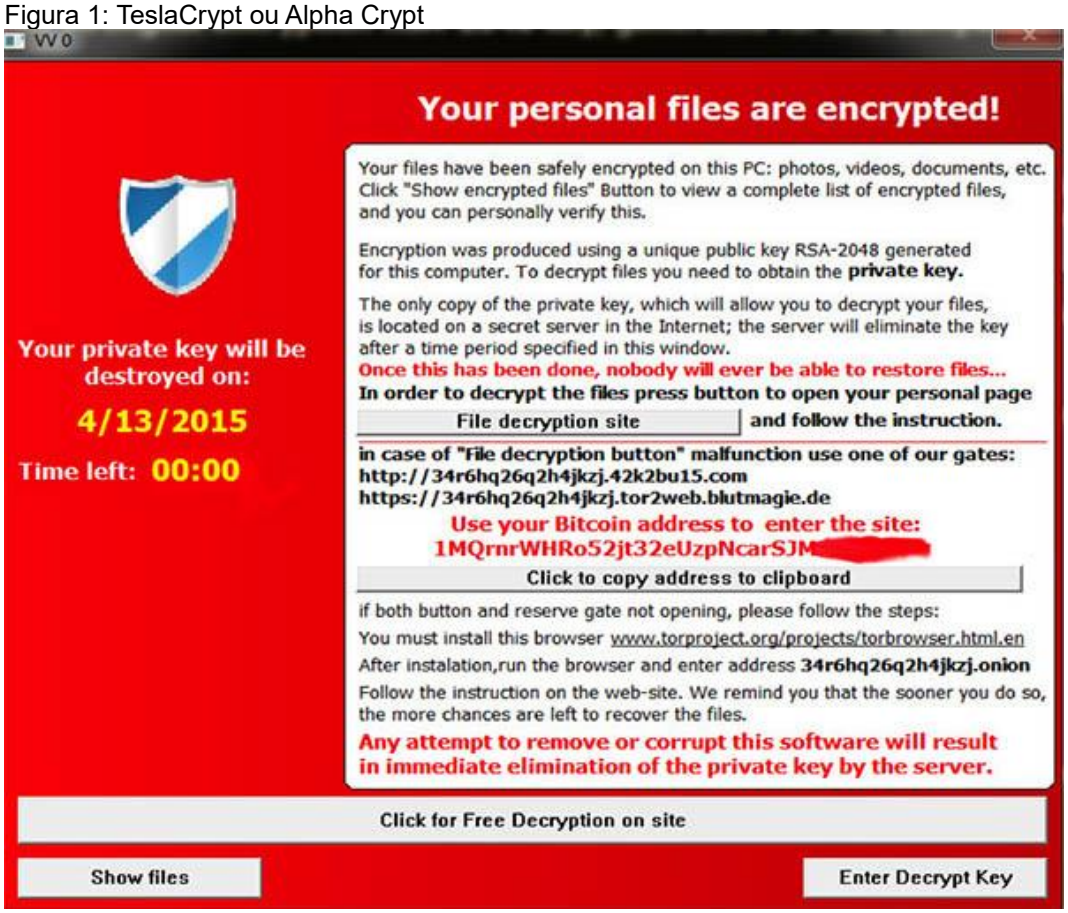
Depois que os arquivos são criptografados, o *ransomware* solicita ao usuário que o resgate seja pago dentro de 24 a 48 horas para descriptografar os arquivos, ou eles serão perdidos para sempre. Se um *backup* de dados não estiver disponível ou esses *backups* forem criptografados, a vítima poderá pagar o resgate para recuperar arquivos pessoais.

[27] Ponto final ou vítima.

3.2 ALGUNS DOS MAIORES RANSOMWARES

Os prejuízos que os *ransomwares* acumulam pelo mundo, já passam dos bilhões de dólares, a seguir serão citados alguns dos maiores *ransomwares* já criados e a quantia que deixaram de prejuízo para as organizações e pessoas.

Figura 1: TeslaCrypt ou Alpha Crypt



Fonte: SECUREWORKS COUNTER THREAT UNIT, 2015.

De acordo com a imagem da figura 1, este *ransomware* foi descoberto em 2015 e continua a evoluir. O *TeslaCrypt* [28] permite que a vítima pague o resgate em *Bitcoin* ou via *PayPal* [29] *My Cash Cards* [30]. O *malware* tem como alvo quase 200 tipos de arquivos e usa uma variedade de criptografia, incluindo AES (*Advanced Encryption*

[28] Tipo de ransomware.
[29] Aplicativo para pagamentos online.
[30] Aplicativo para pagamentos online.

Standard [31]), RSA (*Rivest-Shamir-Adleman* [32]) e ECDH (Elliptic-curve Diffie–Hellman [33]). Novas variantes descobertas no final de 2018 se concentram em arquivos associados a jogos de computador, incluindo os que estão localizados em jogos como: World of Warcraft, *Call of Duty* [34], *Fallout* [35], *Minecraft* [36] *e Half-Life* [37], além de outros (MCAFEE, [s.d.]).

De acordo com Villeneuve (2015), durante uma investigação feita pelo *site fireeye* [38] sobre o *Teslacrypt*, foram descobertos cerca de 1.231 endereços de *bitcoins* usados pelo grupo de crimes cibernéticos. Isso não representa o número total de vítimas, mas as que realmente acessaram o *site TeslaCrypt* e tentaram descriptografar um arquivo. Usamos esses endereços de *bitcoin* para determinar se a vítima pagou o resgate.

Dessas 1.231 vítimas conhecidas, 163 pagaram o resgate, uma taxa de cerca de 13%. Das vítimas que pagaram o resgate, 139 pagaram um intervalo de 0,5 a 2,5 *bitcoin*. Outros 20 pagaram com cartões *PayPal My Cash* e todos, exceto um, pagaram um total de US $ 1.000. Três das vítimas pediram ao grupo de crimes cibernéticos, que então forneceu as chaves de descriptografia de graça, e uma parece ter enganado as pessoas alegando um pagamento de *bitcoin* que parece não ter realmente ocorrido.

No total, o grupo de crimes cibernéticos coletou 254,6 *bitcoins* [39], que foram convertidos para US$ 57.272 em 29 de abril de 2015 e US$ 19.250 em cartões do PayPal, totalizando US$ 76.522 entre 7 de fevereiro de 2015 e 28 de abril de 2015.

[31] Método criptográfico que utiliza um algoritmo de chave simétrica, ou seja, a mesma chave usada para criptografar e descriptografar os dados.
[32] Método criptográfico que utiliza chaves públicas e privadas, ou seja, as chaves de criptografia e descriptografia são diferentes.
[33] Método criptográfico que utiliza uma aproximação para a criptografia de chave pública com base na estrutura algébrica de curvas elípticas sobre corpos finitos.
[34] Jogo digital.
[35] Jogo digital.
[36] Jogo digital.
[37] Jogo digital.
[38] Site da internet.
[39] Moeda digital criptografada.

Figura 2: Wanna Cry

Fonte: WIINNOVA, 2017.

O ataque do *ransomware* WannaCry, foi uma epidemia global que aconteceu em maio de 2017. Ele se espalhou por computadores com o Microsoft Windows e são apresentados na maioria das vezes conforme mostrado na Figura 2. Os arquivos dos usuários eram mantidos como reféns e, para que fossem devolvidos, era exigido um resgate em *bitcoins*. Se não fosse o uso contínuo de sistemas de computador desatualizados e o pouco conhecimento sobre a necessidade de atualizar o *software*, os danos causados por esse ataque poderiam ter sido evitados.

Os cibercriminosos responsáveis pelo ataque se aproveitaram de uma deficiência no sistema operacional Microsoft Windows usando um *exploit* [40] que, supostamente, foi desenvolvido pela Agência de Segurança Nacional dos Estados Unidos. Conhecido como *EternalBlue* esse *exploit* se tornou público por um grupo de *hackers* chamado *Shadow Brokers* [41] antes do ataque do WannaCry. A Microsoft lançou uma correção de segurança que protegia os sistemas de usuários contra esses *exploit* quase dois meses antes do início do ataque do *ransomware* WannaCry. Infelizmente, muitas pessoas e organizações não atualizam regularmente seus sistemas operacionais e, portanto, ficaram expostas ao ataque.

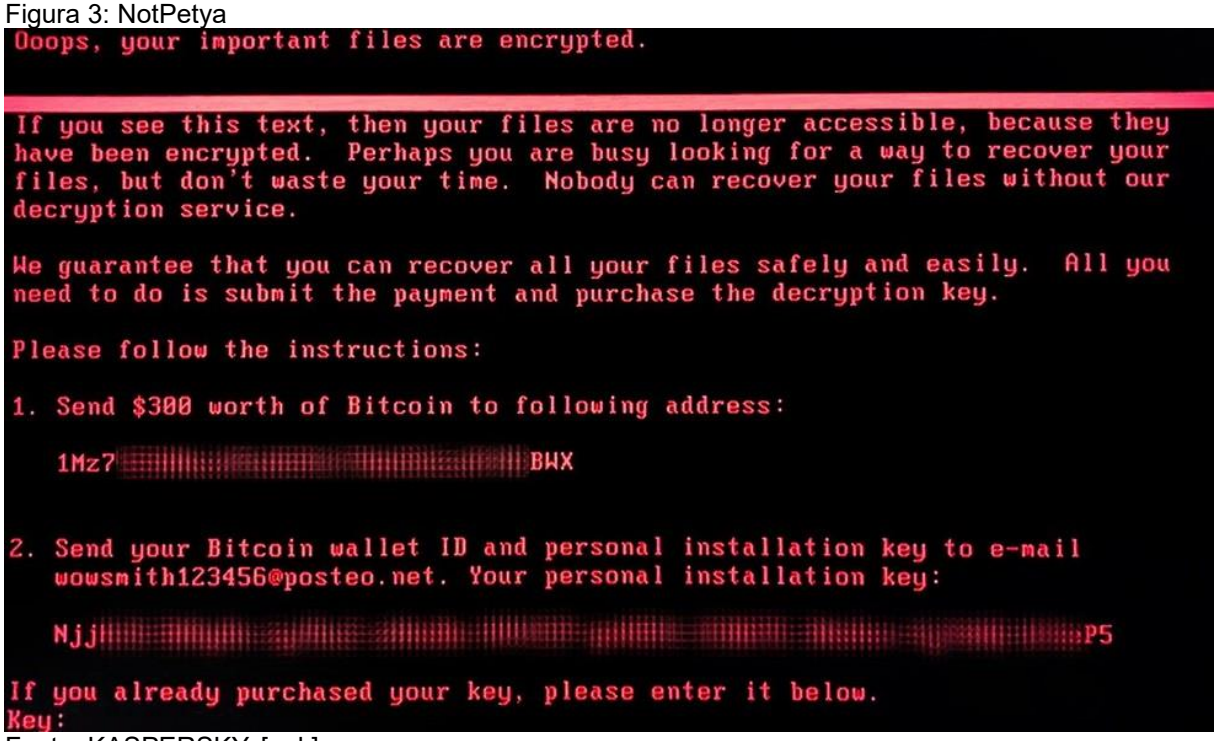
[40] Ferramenta modelada para obter vantagem em um sistema de computador.
[41] Grupo de hackers

Os invasores exigiam a cada ataque US$ 300 em *bitcoins* e, mais tarde, aumentaram o valor do resgate para US$ 600 em *bitcoins*. Se as vítimas não pagassem o resgate dentro de três dias, os responsáveis pelo ataque ameaçavam excluir os arquivos permanentemente.

O ataque do *ransomware WannaCry* atingiu cerca de 230 mil computadores em todo o mundo. Uma das primeiras organizações afetadas foi a empresa espanhola de telefonia móvel, a Telefónica. Em 12 de maio, milhares de consultórios e hospitais do NHS foram afetados em todo o Reino Unido.

Um terço das fundações hospitalares do NHS foram afetadas pelo ataque. Outro acontecimento assustador foi que as ambulâncias desse hospital (foi por causa do *WannaCry*) mudaram de rota e deixaram de atender pessoas que precisavam de cuidados urgentes. O custo estimado para o NHS foi de esmagadores £ 92 milhões após 19 mil consultas terem sido canceladas como resultado do ataque. À medida que o *ransomware* se disseminou para fora da Europa, os sistemas de computadores em 150 países ficaram paralisados. O ataque do *ransomware WannaCry* teve um impacto financeiro considerável em todo o mundo. Estima-se que as perdas causadas por esse crime cibernético tenham somado US$ 4 bilhões em todo o mundo (KASPERSKY, (s.d.]).

Figura 3: NotPetya



Fonte: KASPERSKY, [s.d.]

De acordo com Infotransec, [s.d], o *NotPetya* Ransomware (Figura 4) chegou às manchetes em 27 de junho de 2017, quando o conglomerado empresarial dinamarquês Maersk anunciou que era vítima de uma das variantes mais maliciosas do *ransomware*, o *NotPetya.* Esse *ransomware* também comprometeu inúmeras vítimas, incluindo algumas das maiores empresas do mundo, incluindo Merck, FedEx, Saint-Gobain, Mondelez e Rechitt Benckiser.

O NotPetya recebeu esse nome por sua semelhança com o *ransomware* conhecido como *Petya* que foi centro das atenções no início de 2016 e foi usado para comprometer os computadores das vítimas. O Petya instruía suas vítimas como pagar o resgate em *bitcoin* em troca da chave de descriptografia. Essa nova variante, *NotPetya*, também fez o mesmo, mas incluiu muitos recursos adicionais para permitir a auto propagação e a infecção de sistemas adicionais. O *NotPetya* também tem uma grande semelhança com o *ransomware WannaCry,* que se espalhou pela Internet cerca de seis semanas antes dele, na medida em que ambos utilizaram as ferramentas de exploração conhecidas como *EternalBlue*, que permitiram a propagação do *ransomware* através de compartilhamentos de arquivos abertos na rede interna. Depois que um compartilhamento de arquivo foi identificado, o *malware*

conseguiu se auto copiar no novo *host* e criptografar o MBR (Registro de Inicialização Mestre) do disco rígido, e o processo teve continuidade.

Uma das empresas que sofreu perda financeira significativa como resultado do *NotPetya* foi a Maersk, uma gigante marítima internacional, que é responsável por 76 portos internacionais e transporta quase 20% dos produtos comerciais do mundo. Quando a Maersk respondeu a esse ataque cibernético, desligando toda a sua rede, eles haviam acumulado uma perda de US $ 300 milhões devido a sérias interrupções nos negócios, mas também tiveram força para reinstalar 4.000 servidores e 45.000 estações de trabalho. Isso repercutiu ao redor do mundo e colocou especialistas de segurança em alerta máximo (INFOTRANSEC, ([s.d]).

A perda pela Maersk colocou a empresa em 4º lugar na lista de vítimas mais atingidas pela *NotPetya,* segundo a Casa Branca. A empresa farmacêutica Maersck em função deste *ramsomware* teve uma perda de informações de US$ 870 milhões. Seguido pela FedEx relatando uma perda de US$ 400 milhões e uma empresa de construção francesa Saint-Gobain relata uma perda de US$ 384 milhões de dólares. De acordo com a estimativa fornecida pela Casa Branca, o total de danos estimados do *NotPetya* em 2017 atingiu US$ 10 bilhões (INFOTRANSEC, ([s.d]).

3.3 PREVISÕES DE PREJUÍZOS PARA O FUTURO?

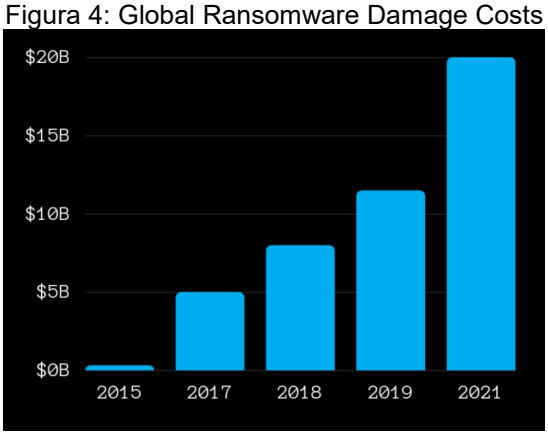
À medida que o estado dos ataques de *ransomware* passa de simples golpes de criptografia de dados a ataques com a intenção de colocar a rede de uma organização como refém, o custo da correção deve aumentar. Esse método de ataque evolui dia-dia, transformando-se em ataques híbridos que utilizam técnicas normalmente encontradas em violações de dados, espionagem, movimento lateral [42]e o método avançado de ataque cibernética *island hopping* estão envolvidos.

De acordo com Sjouwerman [s/d], com as mudanças nos métodos de ataque, o aumento na sofisticação e o aumento no valor do resgate, a *Cybersecurity Ventures*[43] prevê que o *ransomware* gere custos globais acima de US$ 20 bilhões no

[42] Quando o invasor aproveita as instâncias quando usuários confidenciais entram em um computador em que um usuário não confidencial tem direitos locais
[43] Programa internacional de aceleração de cibersegurança.

próximo ano. Parte disso se deve a um aumento na frequência de ataques, que a Cybersecurity Ventures acredita que ocorrerá a cada 11 segundos até 2021. Dado o histórico de serem bastante conservadores com suas previsões, o grande número de US$ 20 bilhões (Figura 4) deve colocar algum medo em organizações que não estão prontas para esses ataques.

Figura 4: Global Ransomware Damage Costs



Fonte: CYBERSECURITYACENTURES, [s.d]

Alguns dos aumentos assumidos (quando os ataques são reconhecidos pelas vítimas) giram em torno do fato de que os danos causados por *ransomwares* não se limitam aos pagamentos do resgate. As organizações precisaram substituir a infraestrutura; executar recuperações em todo o sistema; envolver advogados, relações públicas e investidores; e trabalhar para restaurar a fé de seus clientes após um ataque.

De acordo com Sjouwerman [s.d], outras observações notáveis sobre o estado atual dos *ransomwares*, incluem:

- 55% das pequenas empresas pagam o resgate aos *hackers*;
- Prevê-se que os custos de *ransomwares* alcancem 57 vezes mais que desde seu início até 2021;
- Novas cepas de *ransomwares* estão destruindo *backups*, roubando credenciais, expondo publicamente vítimas, vazando dados roubados e algumas até ameaçam os clientes da vítima;

Além disso Sjouwerman [s.d], estima que a cada 40 segundos uma empresa é vítima de um ataque de *ransomware*, e em um boletim de segurança de dezembro de 2016 publicado pela empresa de segurança cibernética Kaspersky Lab, afirmava que o número de ataques aumentava a cada dois minutos no início daquele ano.

De acordo com Morgan (2019), a *Cybersecurity Ventures* previu que ocorreria um ataque de *ransomware* às empresas a cada 14 segundos até o final de 2019 e a cada 11 segundos até 2021. Isso não inclui ataques a indivíduos, o que ocorre com mais frequência do que às empresas.

3.4 COMO SE PROTEGER OU MITIGAR

Os prejuízos causados por *ransomware* são de fato inevitáveis, mas, as empresas podem mitigar estes danos financeiros através da aplicação das medidas estabelecidas na norma ISO/IEC 27002 (ABNT, 2013). Segundo essa norma, as organizações devem aplicar mecanismos de detecção, prevenção e recuperação para se protegerem contra códigos maliciosos (*malwares*), além de implementar procedimentos apropriados de conscientização do usuário. Estas proteções, contra tais códigos maliciosos devem ser baseados em *softwares* de detecção e reparo de códigos maliciosos, reconhecimento de segurança e controles apropriados de acesso ao sistema de gerenciamento de alterações. As orientações que devem ser consideradas, segundo a referida norma, são:

a) estabelecer uma política formal proibindo o uso de *software* não autorizado;

b) estabelecer uma política formal para proteger a organização quanto aos riscos associados à obtenção de *softwares* e arquivos de redes externas, ou por qualquer intermédio, indicando quais as medidas protetivas que devem ser tomadas;

c) conduzir revisões regulares dos *softwares* e dos conteúdos de dados dos sistemas que suportam processos comerciais considerados críticos; a presença de quaisquer arquivos não aprovados ou alterações não autorizadas, deverão ser formalmente analisados;

d) instalação e atualizações regulares dos *softwares* de detecção e reparo de códigos maliciosos para escanear os computadores e meios de comunicação como controle de precaução ou como base de rotina; as verificações realizadas devem incluir:

1. verificação de arquivos de mídias eletrônicas ou óticas e arquivos recebidos em rede, quanto a códigos maliciosos antes do uso;

2. verificação de anexos em *e-mails* e *downloads* quanto a códigos maliciosos antes do uso; esta verificação deve ser realizada fora e em locais diferentes, e.g. em servidores de correio eletrônico, nos computadores de mesa e ao entrar na organização;

3. Verificação de páginas da *web* quanto a códigos maliciosos;

e) definir procedimentos e responsabilidades para lidar com a proteção de códigos maliciosos nos sistemas, treinamento em seu uso, relatórios e recuperação de códigos maliciosos;

f) preparar um plano de continuidade de negócios apropriado para recuperação quanto a ataques de códigos maliciosos, incluindo todos os arranjos necessários de *backup* e recuperação de dados e *software*;

g) implementar procedimentos para coletar informações regularmente, tais como assinar listas de discussão e/ou verificar sites fornecendo informações sobre novos códigos maliciosos;

h) Implementar procedimentos para verificar informações relacionadas a códigos maliciosos e garantir que os boletins (comunicados) são precisos e informativos; os gerentes devem garantir que fontes qualificadas, e.g. jornais respeitáveis, sites confiáveis da Internet ou fornecedores que produzem *software* de proteção contra códigos maliciosos sejam usados para diferenciar fraudes de reais códigos maliciosos; todos os usuários devem estar cientes das fraudes e o que fazer ao recebê-los.

Seguindo as instruções da norma ISO/IEC 27002 ABNT (2013), é necessário que a empresa adote um sistema de relatos quanto a eventos de segurança e

fraquezas existentes na infraestrutura geral, a fim de garantir que os eventos de segurança da informação e as fraquezas associadas aos sistemas de informação sejam comunicadas de maneira a permitir tomadas as ações corretivas oportunas.

Estes eventos de segurança da informação devem ser relatados por meio de canais de gerenciamento apropriados o mais rapidamente possível. A implementação do procedimento de comunicação formal de relatório de eventos de segurança da informação, deve ser estabelecido em conjunto com um procedimento de respostas a incidentes e escalonamento, definindo as ações a serem tomadas no recebimento de um relatório de evento de segurança da informação. Um ponto de contato também deve ser estabelecido para que sejam enviados os relatos dos eventos de segurança da informação. Deve ser garantido também que este ponto de contato seja conhecido por toda a organização, esteja sempre disponível e que seja capaz de providenciar o tempo adequado de resposta.

Todos os funcionários, contratantes e usuários terceiros devem estar cientes de sua responsabilidade em relatar os eventos de segurança da informação o mais rapidamente possível. Eles também devem estar cientes do procedimento para relatar o evento de segurança da informação e do ponto de contato. Os procedimentos de relato devem incluir:

a) Processos de *feedback* adequados para garantir que esses relatores de eventos de segurança da informação sejam notificados após o problema ter sido tratado e fechado;

b) Formulários de relatório de eventos de segurança da informação para apoiar a ação de relato e para ajudar a pessoa que está relatando a lembrar de todas as ações necessárias no caso de um evento de segurança da informação;

c) O comportamento correto a ser realizado em caso de um evento de segurança da informação, isto é.

1. Anotando todos os detalhes importantes (e.g. tipo de não-conformidade ou violação, mau funcionamento, mensagens na tela, comportamentos estranhos) imediatamente;

2. Não realizar nenhuma ação própria, mas relatar para o ponto de contato imediatamente;

d) Estabelecer um processo disciplinar para lidar com empregados, contratantes ou usuários de terceiros que cometerem violações de segurança.

Alguns exemplos de incidentes e eventos de segurança são:

a) perda de serviço, instalações ou equipamentos;

b) mau funcionamento do sistema ou sobrecarga;

c) erros humanos;

d) não conformidade com as políticas e/ou orientações;

e) violações de disposições de segurança física;

f) alterações não-controladas dos sistemas;

g) mau funcionamento de *hardwares* e *softwares*;

h) violações de acesso.

Ainda de acordo com a norma ISO/IEC 27002 (ABNT, 2013), uma outra forma de prevenção são os relatos de fraquezas de segurança da informação, onde todos os funcionários, contratantes e usuários terceiros de sistemas de informação e serviços devem anotar e relatar quaisquer fraquezas na segurança da informação destes sistemas e serviços, sejam elas observadas ou suspeitas. Eles deverão reportar estas fraquezas para seus administradores ou diretamente ao provedor do serviço o mais rápido possível para prevenir incidentes de segurança da informação. O mecanismo de relato deve ser tão fácil, acessível e disponível quanto possível. Eles também devem ser informados que, em nenhuma circunstância, devem tentar provar uma suspeita de fraqueza de segurança.

4 ESTUDO DE CASO

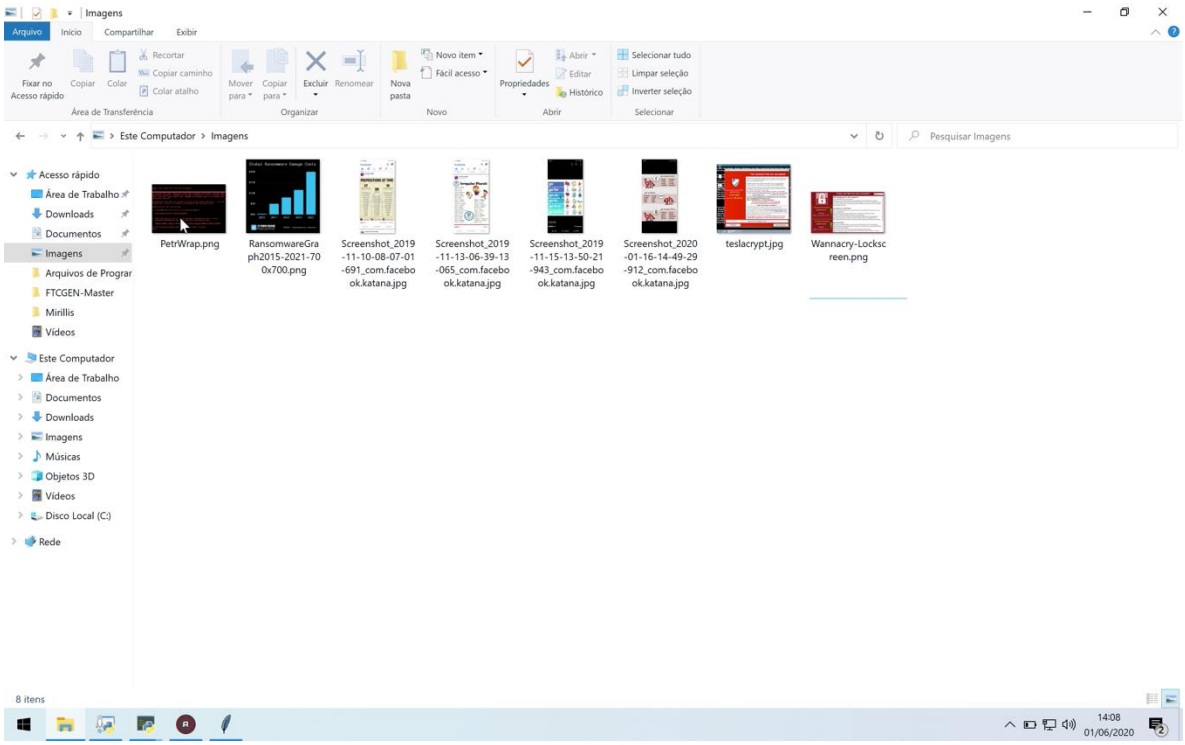
O intuito desse capítulo é apresentar um teste de *malware* do tipo *ransomsware* em um dos sistemas operacionais mais utilizados em ambientes corporativos e domésticos, o *Microsoft Windows*. Para a demonstração do perigo e facilidade que existe em se infectar um computador e causar prejuízos em um alvo, foi criado um ambiente de testes controlado em uma máquina virtual com as seguintes especificações:

- Windows 10 Home Edition Versão 1909 x64 (KB4497165);
- Intel Core I5-6360U;
- 4GB RAM;
- Windows Defender com 100% de funcionamento;
- Avast Free Antivírus;
  Foi escolhido um antivírus gratuito e conhecido por se tratar de uma simulação possível para uma pequena empresa ou computadores pessoais de usuários comuns e sem conhecimentos técnicos e profundos em segurança da informação.

O *ransomware* utilizado foi criado na linguagem de programação denominada python3. Este *ransomware*, pode ser adaptado conforme a necessidade do alvo, ou seja, pode ser alterado facilmente para ler tipos de extensões de arquivos específicas e diretórios específicos em um computador ou servidor alvo. O *ransomware* também pode ser configurado para atacar máquina com os sistemas operacionais Linux/Unix ou OS-X.

Antes do “ataque”, observa-se um ambiente saudável e com os arquivos em seus *status* normais, conforme exemplificado na Figura 5.

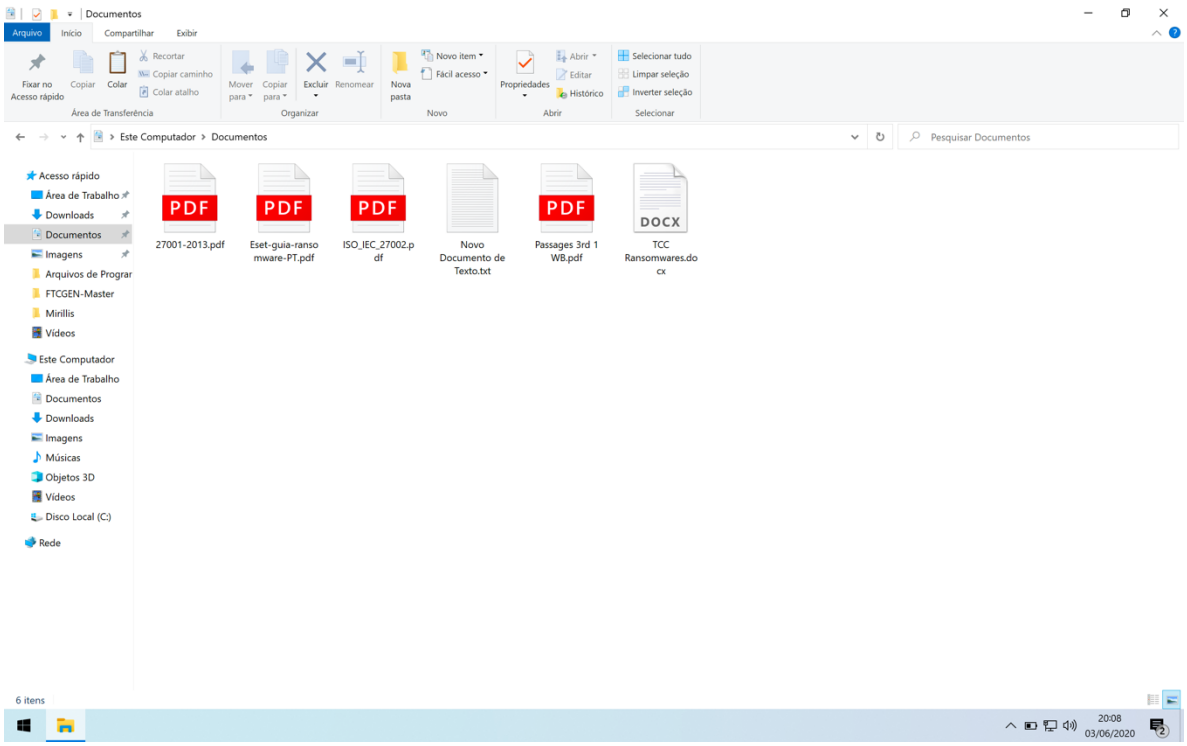
Figura 5 – Diretório “Imagens” antes do ataque.



Fonte: Autoria própria.

Captura de tela do Windows mostrando que os arquivos localizados no diretório “Imagens” no Disco Rígido da máquina estão funcionais (Figura 5).

Figura 6 - Diretório “Documentos” Saudável

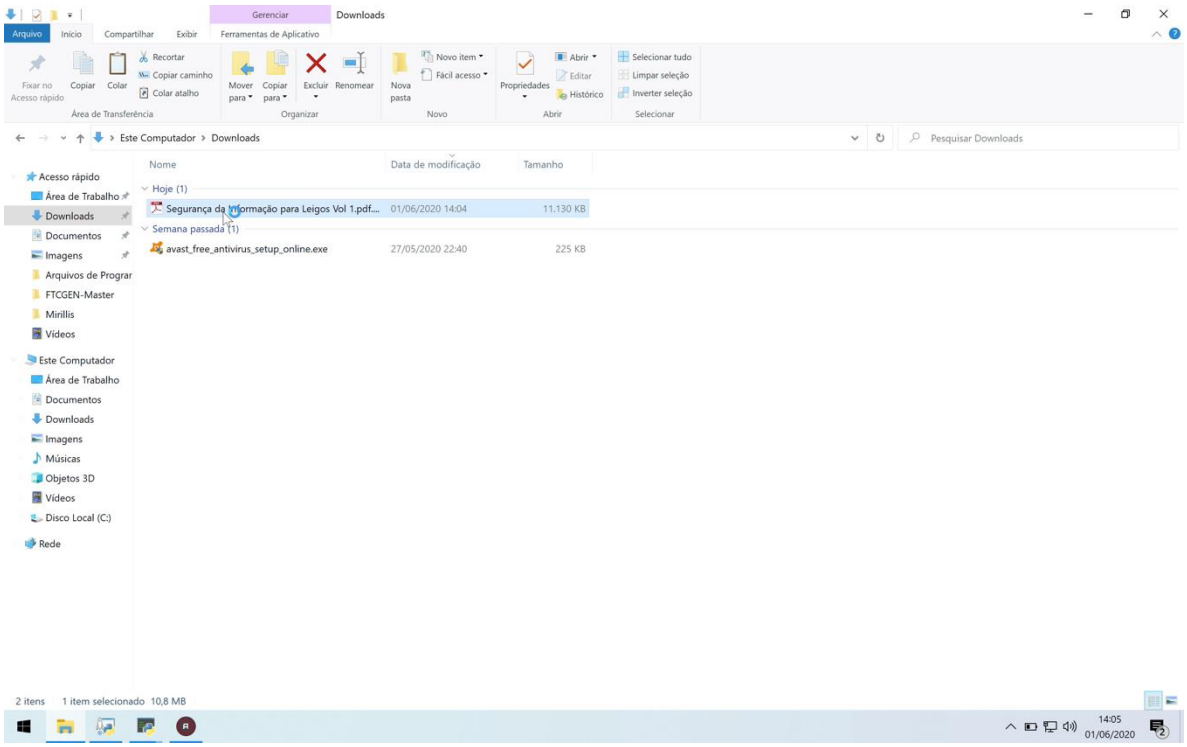


Fonte: Autoria própria.

Captura de tela do Windows mostrando que os arquivos localizados no diretório “Documentos” no Disco Rígido da máquina estão funcionais (Figura 6).

No teste realizado, o arquivo nomeado FATECRANSOMWARE foi camuflado em um documento do formato pdf, onde foi feito *download* da Internet pela vítima como sendo um livro de ensinamentos para leigos em segurança da informação. E após tentar abrir o arquivo, que na verdade é um executável o *ransomware* já começa a agir no computador da vítima e criptografa todos os arquivos encontrados dentro das pastas que foram apontadas como alvo para o *ransomware*.

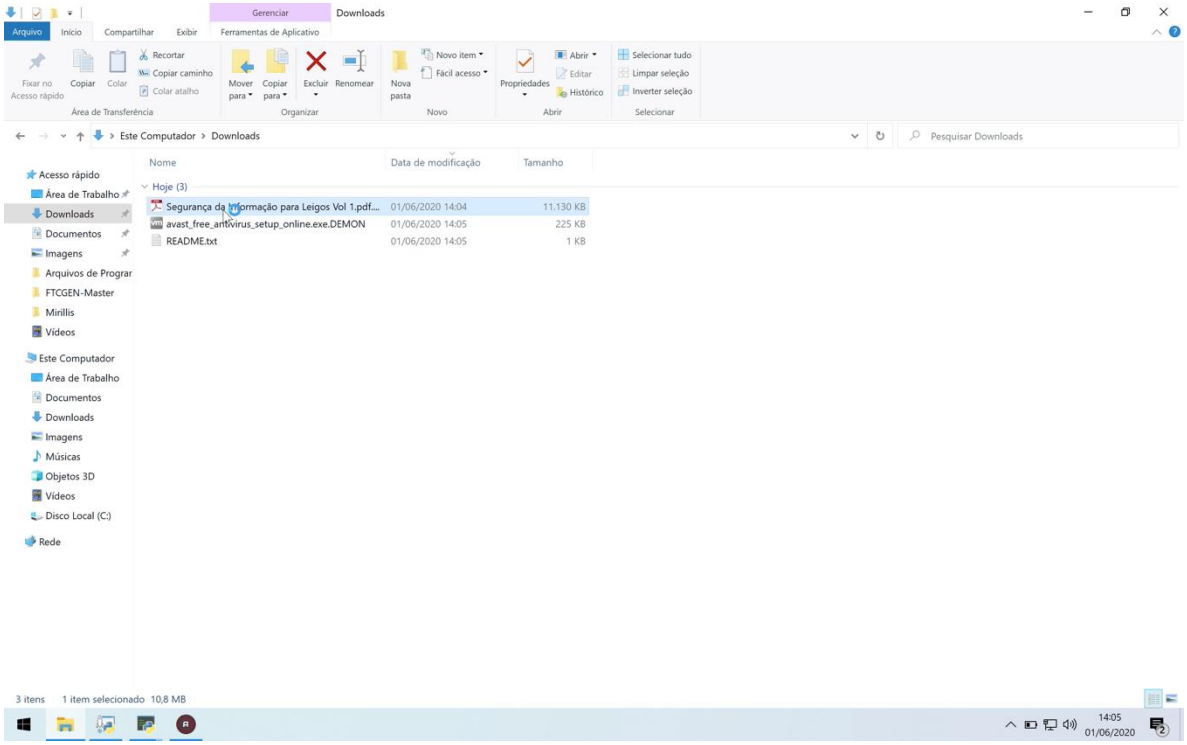
Figura 7 – Abertura e Execução do *Ransomware*



Fonte: Autoria própria.

Captura de tela do Windows mostrando o momento que o arquivo malicioso, camuflado em um arquivo com extensão “.pdf” é executado (Figura 7).

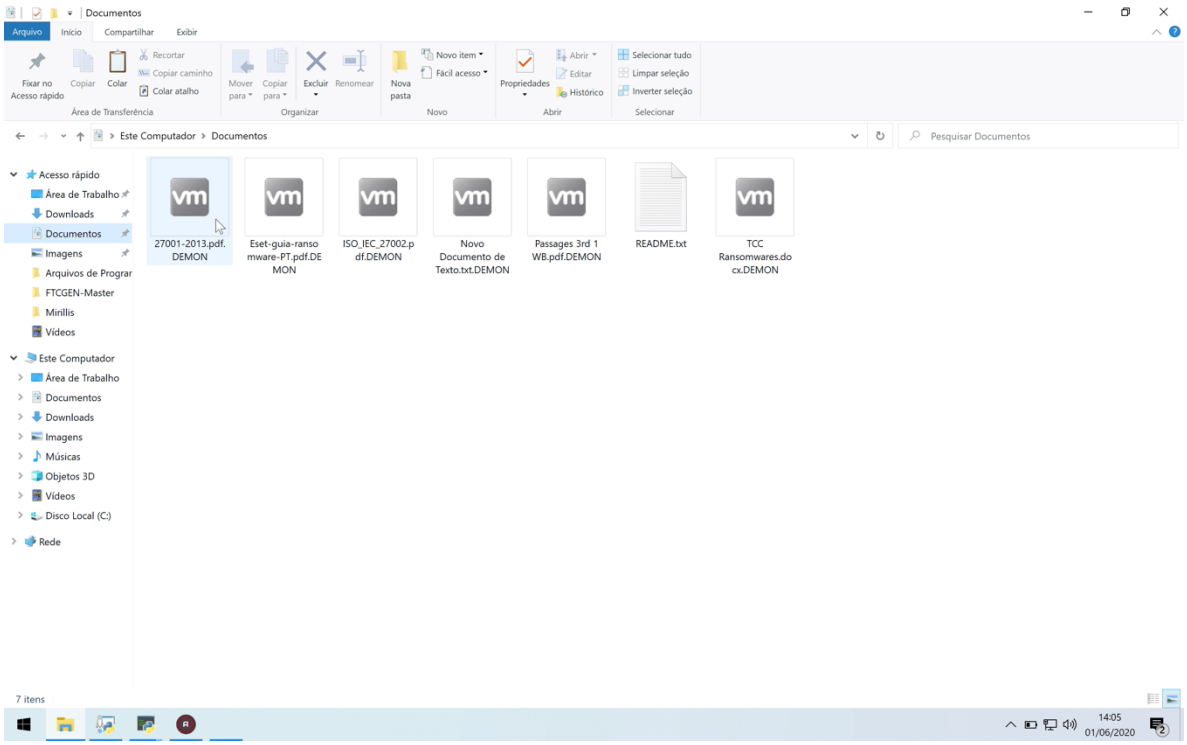
Figura 8 - Diretório “Downloads” Infectado



Fonte: Autoria própria

Captura de tela do Windows mostrando o diretório “Downloads” após a execução do Ransomware (Figura 8).

Figura 9 - Diretório “Documentos” Infectado

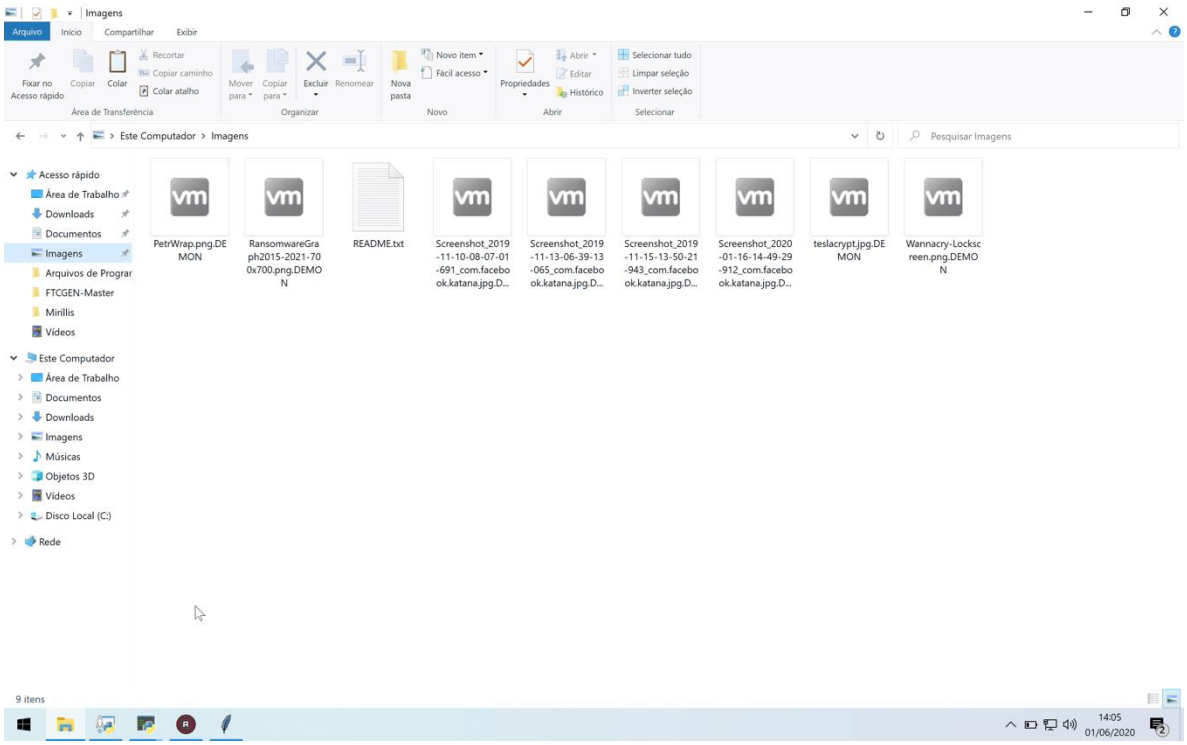


Fonte: Autoria própria

Captura de tela do Windows mostrando o diretório “Downloads” após a execução do ransomware (Figura 9).

Pode-se ver na Figura 8, o resultado após a criptografia dos arquivos encontrados ter sido executada. Como estamos em um ambiente virtualizado, o Microsoft Windows acabou tentando reconhecer os arquivos que agora estão com a extensão “.DEMON”. Isso resultado da ação do *ransomware* injetado no arquivo.

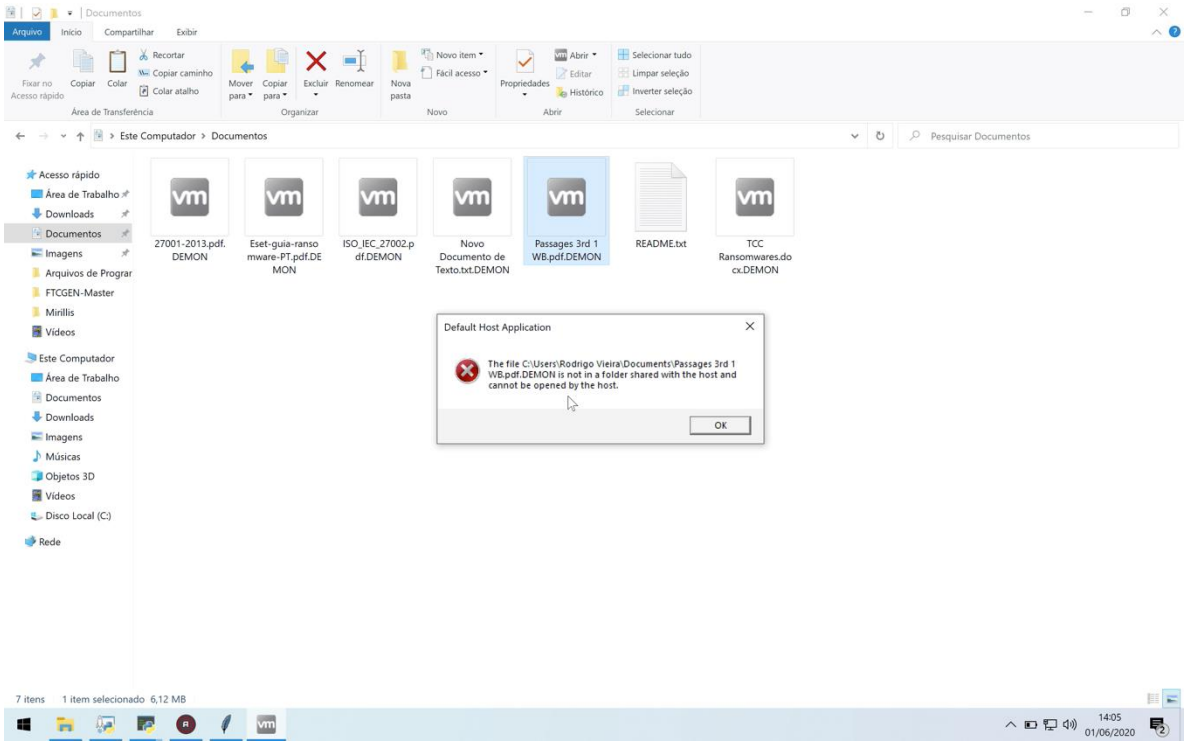
Figura 10 - Diretório “Imagens” Infectado



Fonte: Autoria própria.

Captura de tela do Windows mostrando o diretório “Imagens” após a execução do ransomware (Figura 10).

Figura 11 – Tentativa de Abertura de um Arquivo Infectado

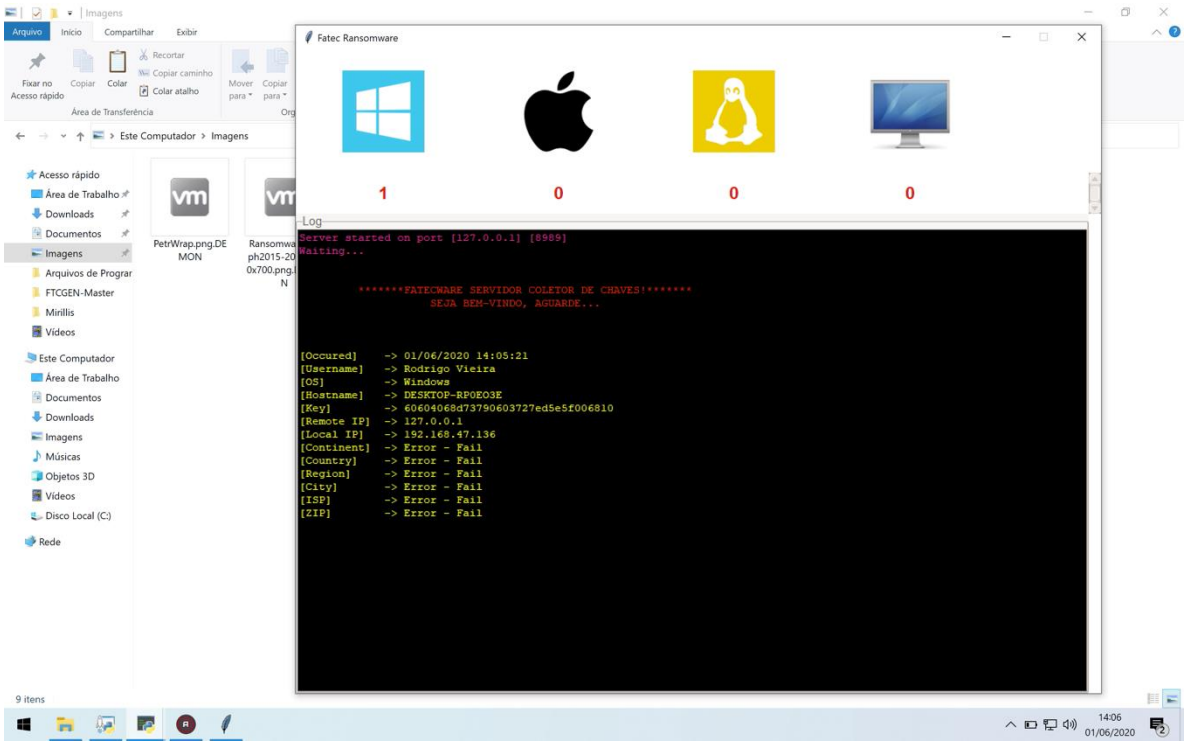


Fonte: Autoria própria.

Captura de tela do Windows exibindo o erro ao tentar abrir arquivo após a infecção (Figura 11).

Ao mesmo tempo em que o *ransomware* está sendo executado, ele efetua o envio da chave para a descriptografar os arquivos afetados para um “servidor remoto”, que no caso deste teste mais controlado foi deixado na própria máquina virtual em que o teste foi realizado.

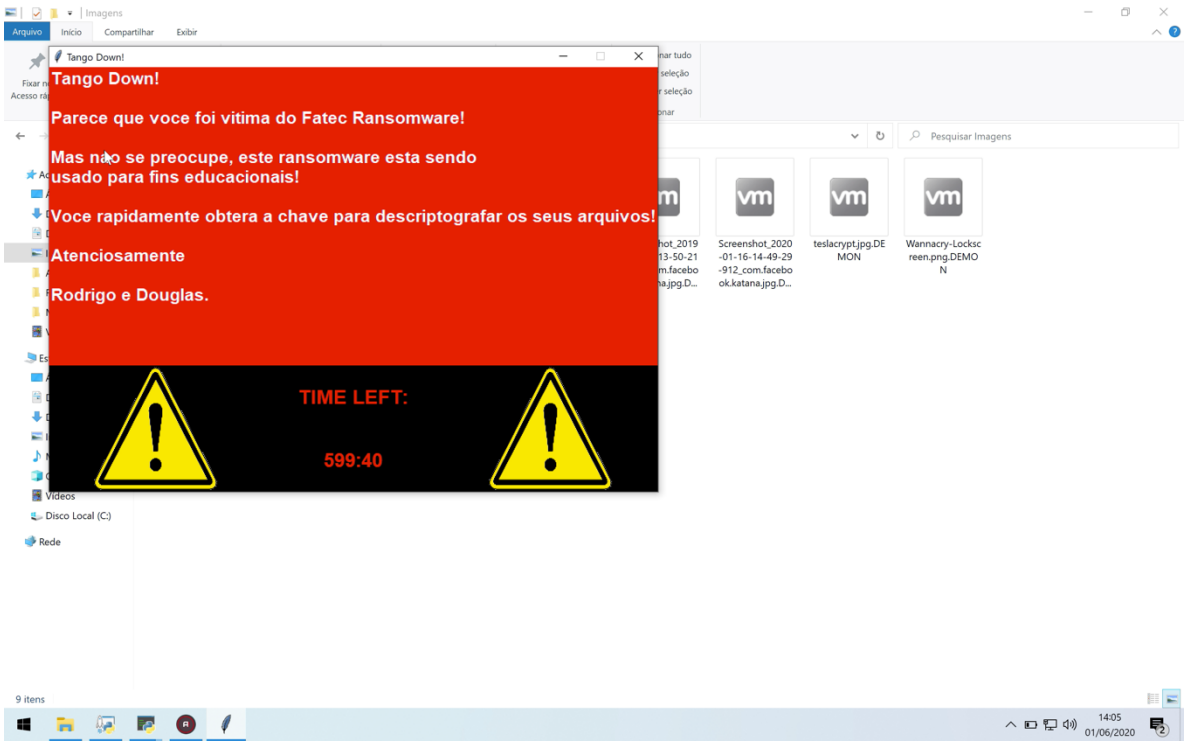
Figura 12 – Servidor Remoto de Chaves



Fonte: Autoria própria.

Quando o *malware* termina a execução e identifica que todos os arquivos foram criptografados, ele executa uma tela no estilo *pop-up* que conteria a informação para que a vítima conseguisse a chave para obter seus arquivos novamente e quanto tempo esta pessoa tem até que seus arquivos sejam destruídos. Mas neste caso apenas foi inserida uma mensagem e um tempo simbólicos para efetuar o teste.

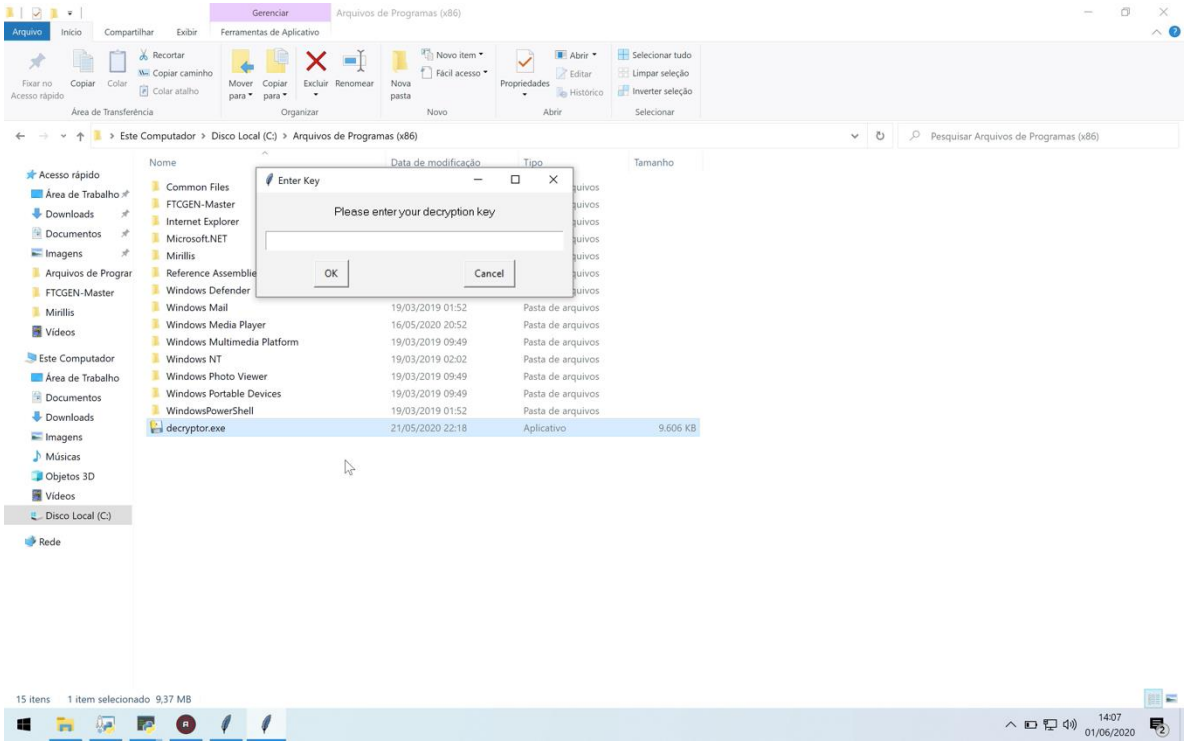
Figura 13 – Tela de Instruções e Aviso de Infecção



Fonte: Autoria própria.

Em uma situação real, a ferramenta parar descriptografar os dados, seria enviada juntamente com a chave após o pagamento de uma quantia previamente calculada em *bitcoins*.

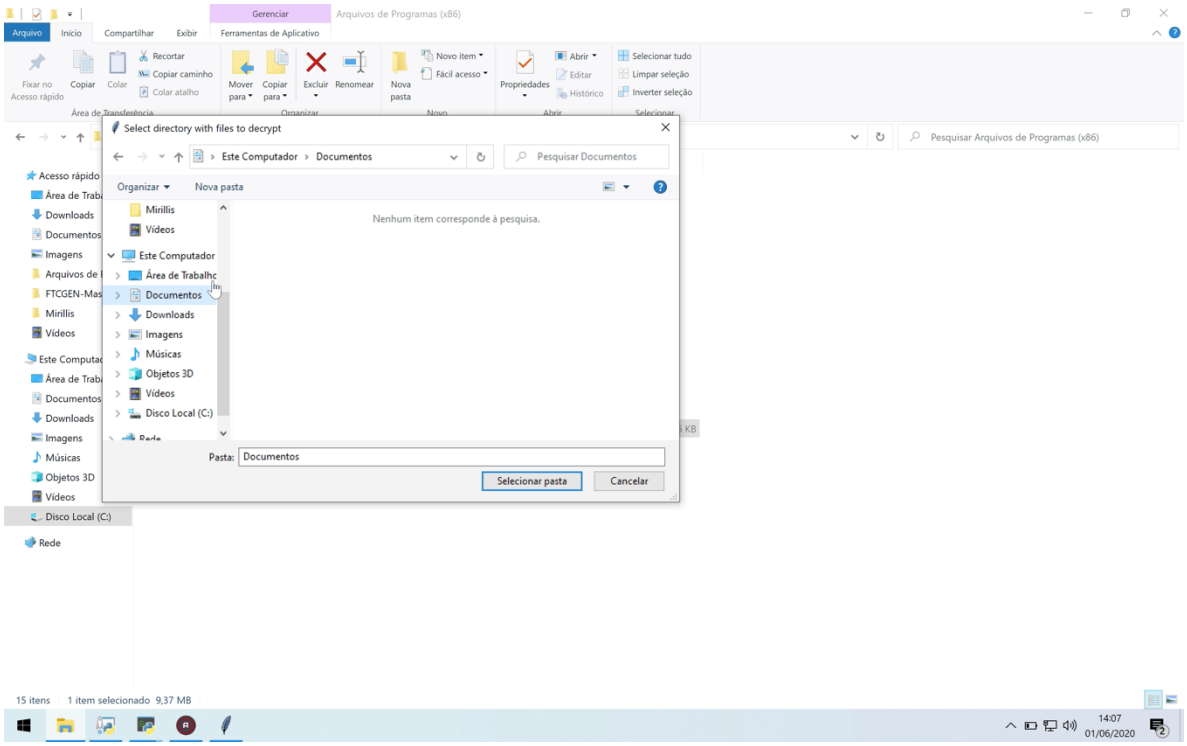
Figura 14 – Executável para descriptografar os Arquivos



Fonte: Autoria própria.

Captura de tela do Windows mostrando a ferramenta usada para gerar a chave de descriptografia dos arquivos (Figura 14).

Figura 15 – Seleção de Diretório para Descriptografar os Arquivos



Fonte: Autoria própria.

Captura de tela do Windows mostrando a etapa de selecionar os arquivos à serem descriptografados (Figura 15).

Como uma das intenções é o uso deste material em ambiente educacional de forma didática, foi gravado um vídeo explicativo da execução prática do teste, o qual pode ser acessado e assistido através do *QR code* ~~abaixo~~ apresentado na Figura 16.

Figura 16 – QR CODE do Vídeo Prático

Fonte: Autoria própria

5 **CONCLUSÃO**

O desenvolvimento deste estudo com base na crescente disseminação de um tipo de *malware* possibilitou uma análise de como um simples *ransomware* criado utilizando a linguagem *python3* pode causar um grande e rápido dano à pequenas e grandes empresas assim como a usuários sem ligação a qualquer tipo de organização.

Também foi comprovado que um *ransomware* pode ser disseminado sem ser detectado pelos antivírus gratuitos que a maioria dos usuários e pequenas empresas possuem.

Além disso o trabalho permitiu a demonstração da um ataque em um ambiente real focando principalmente na forma que computacional é afetado por este tipo de *malware.*

Este trabalho cumpriu com seus objetivos iniciais demonstrando o quanto é importante que o usuário seja bem instruído para verificar o tipo de arquivo que está abrindo, sua fonte e nunca confiar no ícone apresentado ou que a extensão do mesmo seja realmente .pdf, .doc, .txt ou outra que não cause problemas.

REFERÊNCIAS BIBLIOGRÁFICAS

BISHOP. **Riscos, vulnerabilidade e ameaça em segurança da informação. 2008.** Disponível em: https://www.techtem.com.br/seguranca-da-informacao-riscos-vulnerabilidade-e-ameaca/. Acesso em: 28 fev. 2020.

CERTBR. **Códigos maliciosos (malware).** 2017. Disponível em: https://cartilha.cert.br/malware/. Acesso em: 20 fev. 2020.

CRUZ, Michael. **Difference between internal & external threats to an IT database**. ([s.d]). Disponível em: https://smallbusiness.chron.com/difference-between-internal-external-threats-database-74165.html. Acesso em: 08 mar. 2020.

ESET. **Como garantir a confidencialidade, integridade e disponibilidade dos dados?** 2018. Disponível em: https://www.eset.com/br/sobre/blog/corporativo/como-garantir-a-confidencialidade-integridade-e-disponibilidade-dos-dados/ Acesso em: 25 fev. 2020.

GOMES, Maria. **Insiders e a segurança cibernética de empresas**. 2015. Disponível em: http://www.justificando.com/2015/04/27/insiders-e-a-seguranca-cibernetica-de-empresas/. Acesso em: 28 fev. 2020.

INFOTRANSEC. **The impacts of NotPetya Ransomware**: what you need to know. ([s.d]). Disponível em: https://infotransec.com/news/the-impacts-of-notpetya-ransomware-what-you-need-to-know/. Acesso em: 18 mar. 2020.

KASPERSKY. **O que é o Ransomware WannaCry?** ([s.d]). Disponível em: https://www.kaspersky.com.br/resource-center/threats/ransomware-wannacry. Acesso em: 20 mar. 2020.

MCAFEE. **TeslaCrypt**: ransomware. ([s.d]). Disponível em: https://www.mcafee.com/enterprise/en-us/threat-center/threat-landscape-dashboard/ransomware-details.teslacrypt-ransomware.html. Acesso em: 17 mar. 2020.

MORGAN, Steve. **Global ransomware damage costs predicted to reach $20 billion (USD) by 2021**. 21 out. 2019. Disponível em: https://cybersecurityventures.com/global-ransomware-damage-costs-predicted-to-reach-20-billion-usd-by-2021/. Acesso em: 18 mar. 2020.

MORGAN, Steve. **Ransomware predicted to cost $20 Billion (USD) in damages globally by 2021.** ([s.d]). Acesso em: 10 mar. 2020. Disponível em: https://cybersecurityventures.com/global-ransomware-damage-costs-predicted-to-reach-20-billion-usd-by-2021/. Acesso em: 05 abr. 2020.

OLIVEIRA, Valdes. **Riscos, vulnerabilidade e ameaça em segurança da informação**. 2008. Disponível em: https://www.techtem.com.br/seguranca-da-informacao-riscos-vulnerabilidade-e-ameaca/. Acesso em: 28 fev. 2020.

PROOF. **Segurança da informação nas empresas: as diferenças entre educar, treinar e conscientizar.** ([s.d]). Disponível em: https://www.proof.com.br/blog/seguranca-da-informacao-nas-empresas/. Acesso em: 08 mar. 2020.

SANS. **What is malware?** ([s.d]). Disponível em: https://www.sans.org/security-awareness-training/ouch-newsletter/2016/what-malware. Acesso em: 25, fev. 2020.

SIKORSI, Michael; HONIG, Andrew. **Practical malware analysis**: the hands-on guide to dissecting malicious software. San Francisco: No Starch Press, 2012. Acesso em 23 de abr. de 2020.

SJOUWERMAN. **Ransomware predicted to cost $20 Billion (USD) in damages globally by 2021.** ([s.d]). Disponível em: https://cybersecurityventures.com/global-ransomware-damage-costs-predicted-to-reach-20-billion-usd-by-2021/. Acesso em: 05 abr. 2020.

TELIUM. **Confidencialidade, integridade e disponibilidade: os três pilares da segurança da informação**. 2018. Disponível em: https://www.telium.com.br/blog/confidencialidade-integridade-e-disponibilidade-os-tres-pilares-da-seguranca-da-informacao. Acesso em: 25 fev. 2020.

VILLENEUVE, Nart. **TeslaCrypt**: following the money trail and learning the human costs of ransomware. 15 mai. 2015. Disponível em: https://www.fireeye.com/blog/threat-research/2015/05/teslacrypt_followin.html. Acesso em: 17 mar. 2020.

WIRESHARK. **Checksums**. ([s.d]). Disponível em: https://bit.ly/2TrvP7R. Acesso em 08 maio de 2020.