Journal of Technology & Information

Ransomware: A Evolução Dos Ataques Na Contemporaneidade e Seus Desafios para a Segurança Digital

Ransomware: The Evolution of Attacks in the Contemporary and Their Challenges for Digital Security

Recebido: 26/06/2023 | Revisado: 02/07/2023 | Aceito: 05/07/2023 | Publicado: 06/07/2023

https://www.doi.org/10.5281/zenodo.8125271

Stephany Victoria Nascimento da Silva
FATEC Santana de Parnaíba
https://orcid.org/0000-0003-2089-0517
stephanynascimento@outlook.pt

Irapuan Glória Junior
FATEC Santana de Parnaíba
https://orcid.org/0000-0003-2973-3470
ijunior@ndsgn.com.br

Resumo

Os ataques de *Ransomware* podem ser devastadores para empresas e indivíduos, causando perda de dados, tempo de inatividade, custos de recuperação e até mesmo danos à reputação. Na atualidade, o *Ransomware* se tornou uma das ameaças cibernéticas mais perigosas e disseminadas. Os criminosos usam diversas técnicas para infectar computadores e redes, incluindo *e-mails* de *phishing*, *downloads* de *softwares* maliciosos, vulnerabilidades em sistemas operacionais e aplicativos, entre outros. Por mais que se desenvolvam estratégias de prevenção os criminosos que usam *Ransomware* estão constantemente desenvolvendo novas táticas e técnicas, além disso existem inúmeras limitações legislativas e práticas na localização e punição desses autores. Este trabalho utilizou a metodologia de pesquisa bibliográfica com o objetivo de identificar os tipos de *Ransomware* que estão fazendo ataques às empresas. Os resultados foram a identificação dos principais tipos de *Ransomware*, como o *Crypto malware*, *Locker* e *Scareware*, e um framework com a forma de identificá-los. A contribuição para a teoria está em apresentar as formas de ataques dos principais tipos de Ransomware. A contribuição para a prática é alertar os gestores e gerentes de segurança da informação das formas de ataques.

Palavras-chave: Ransomware; Ataque; Cibernético; Malware.

Journal of Technology & Information

Abstract

Ransomware attacks can be devastating for companies and individuals, causing data loss, downtime, recovery costs, and even reputation damage. Nowadays, Ransomware has become one of the most dangerous and widespread cyber threats. Criminals employ various techniques to infect computers and networks, including phishing emails, malicious software downloads, vulnerabilities in operating systems and applications, among others. Despite the development of prevention strategies, criminals utilizing Ransomware are constantly devising new tactics and techniques. Moreover, there are numerous legislative and practical limitations in locating and punishing these perpetrators. This study employed a bibliographic research methodology to identify the types of *Ransomware* targeting companies. The results included the identification of key types of *Ransomware*, such as Crypto malware, Locker, and Scareware, along with a framework for their identification. The theoretical contribution lies in presenting the attack methods of the main types of *Ransomware*. The practical contribution aims to raise awareness among managers and information security professionals about these attack methods.

Keywords: Ransomware; Attack; Cybernetic; Malware.

1. Introdução

Ao longo dos anos, os crimes cibernéticos têm chamado cada vez mais a atenção da mídia. Isso devido ao seu crescimento rápido e as táticas de engenharia social empregadas para fazer suas vítimas. Entre eles, um dos mais incidentes nas organizações do Brasil e do mundo está o *Ransomware*, que por ter seu público-alvo voltado às empresas, é um dos que mais causa prejuízos financeiros no mundo (Biancamano, 2021)

O *Ransomware* é um tipo de *malware* que sequestra os arquivos de um computador, exigindo um pagamento para liberá-los. Por meio de técnicas sofisticadas de engenharia social, exploração de vulnerabilidades em sistemas operacionais e aplicativos, e uso de criptografia avançada, os cibercriminosos têm sido capazes de lançar ataques *Ransomware* cada vez mais perigosos e disseminados, incluindo a propagação por meio de *e-mails* de *phishing*, *downloads* de *software* malicioso, vulnerabilidades em sistemas operacionais e aplicativos, entre outras práticas fraudulentas (Inside, 2023)

As tendências nas empresas de utilizar o formato de trabalho remoto e o aumento da digitalização de processos têm proporcionado novas oportunidades para os criminosos propagarem o *Ransomware*, resultando em consequências graves para empresas e indivíduos, incluindo perda de dados, tempo de inatividade, custos de recuperação e danos à reputação. Algumas das variantes mais conhecidas de *Ransomware* incluem o *WannaCry,* o *Petya,* o *Locky,* e o *Ryuk* (Report, 2022).

Diante desse cenário, torna-se imprescindível compreender a evolução do *Ransomware* ao longo dos anos, desde suas primeiras aparições até as variantes mais recentes, com o objetivo de desenvolver estratégias de defesa mais eficazes contra esse tipo de ameaça e até mesmo prever tendências futuras (Souza, 2023). Nesse sentido, o presente artigo possui como questão de pesquisa: "Quais os tipos de *Ransomware* identificados?". Os objetivos do presente estudo são: (1) Identificar quais os tipos de *Ransomware* descritos na literatura (2) Apresentar um diagrama de identificação a partir do comportamento do ataque.

2. Referencial Teórico

2.1. Ransomware

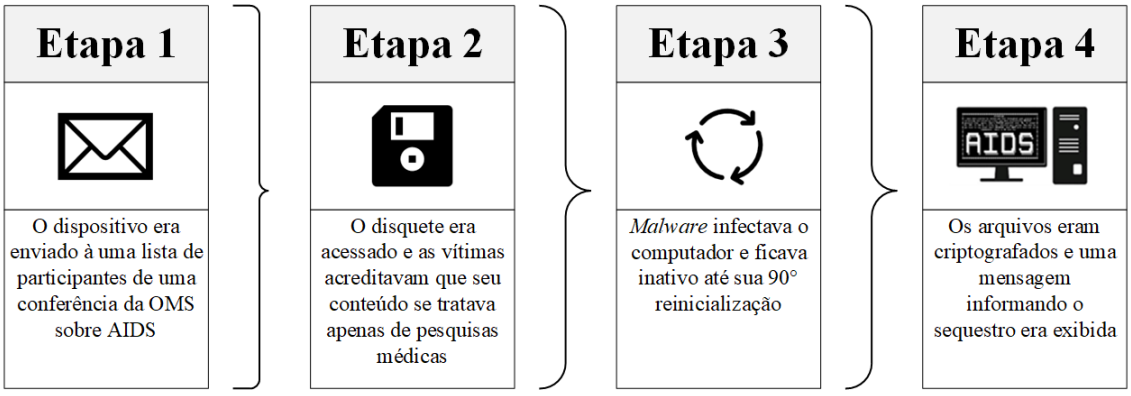
Entender o fenômeno criminógeno, que representa as origens de um crime, é essencial para a sua compreensão, assim como suas condicionantes e possibilita a análise e definição de possíveis tendências, para viabilizar seu combate e prevenção (Souza, 2018).

A escala evolutiva do *Ransomware* (Figura 2) iniciou em 1989 com a primeira versão do vírus que foi criado pelo Doutor em biologia Joseph Popp de Harvard, e disseminado por meio de uma tática de Engenharia Social: foi enviado um disco nomeado AIDS, acrônico para *Acquired Immunodeficiency Syndrome* (Prabhu & Van Wagoner, 2023), para uma lista de participantes de uma confraternização da Organização Mundial de Saúde (OMS) sobre a doença, fazendo mais de 20.000 pessoas serem vítimas de sequestro de dados por acreditarem se tratar de pesquisas médicas (Mujezinovic, 2019).

Por meio de seu primeiro caso, é possível estabelecer como inicia o fluxo de infecção do *Ransomware*, por uma estratégia social, convencendo suas vítimas de que o arquivo malicioso se trata de algo de seu interesse e não por meio de uma força técnica (Guedes, 2021).

A atuação do *Ransomware* AIDS, conforme Figura 1, inicia com o envio de um dispositivo até a vítima (Etapa 1) que insere no computador e acessa o arquivo infectado (Etapa 2). Após o acesso, é realizada a instalação do *malware* (Etapa 3), e quando perfizer a nonagésima inicialização do sistema operacional (Etapa 4), o vírus criptografa os dados do computador e a visualização do sistema era substituída por um alerta de solicitação de pagamento para a corporação *PC Cyborg* pela liberação dos dados (Kelly, 2021).

Figura 1 – Esquema de Infecção do AIDS Baseado em Kelly (2020)



Especialistas da segurança da informação conseguiram rastrear o autor facilmente, revertendo o processo e permitindo o rastreamento e prisão do autor dos crimes. Isso foi possível devido ao fato que a criptografia ser realizada através de chaves simétricas (Kelly, 2021).

Apesar de demonstrar aptidão suficiente para arquitetar o vírus e sua forma de propagação, Popp foi julgado inapto mentalmente para responder por seus atos (Lessing, 2020).

O ataque interrompeu a operação de várias instituições e organizações médicas, no qual algumas vítimas entraram em pânico e apagaram seus *hard-drivers*, perdendo dados de pesquisas de valores imensuráveis e insubstituíveis (Mujezinovic, 2021).

Diferente das vítimas, cuja percepção da realidade acontece imediatamente e suas consequências podem ser inúmeras visto que estes casos podem acarretar demissões nas empresas afetadas, a. Isso ocorre porque as empresas podem sofrer perda de dados, interrupção de negócios e danos à reputação, o que pode afetar sua situação financeira e consequentemente a capacidade de manter funcionários, levando à necessidade de cortes de custos. Em alguns casos a demissão pode ocorrer até mesmo pela culpabilização do funcionário que foi enganado pelos criminosos e acabou servindo como "porta de entrada" (Bertolluci, 2019).

Algumas das consequências psicológicas de um ataque de *Ransomware* incluem ansiedade devido à pressão de tomar decisões rapidamente, raiva e irritação decorrentes da sensação de injustiça, perda de confiança e habilidades tecnológicas resultante da perda de acesso a informações importantes, e depressão devido ao impacto significativo na vida das vítimas. Além disso, algumas vítimas podem desenvolver sintomas de estresse pós-traumático, como *flashbacks*, pesadelos e evitação de situações relacionadas ao ataque (Laccelva, 2021).

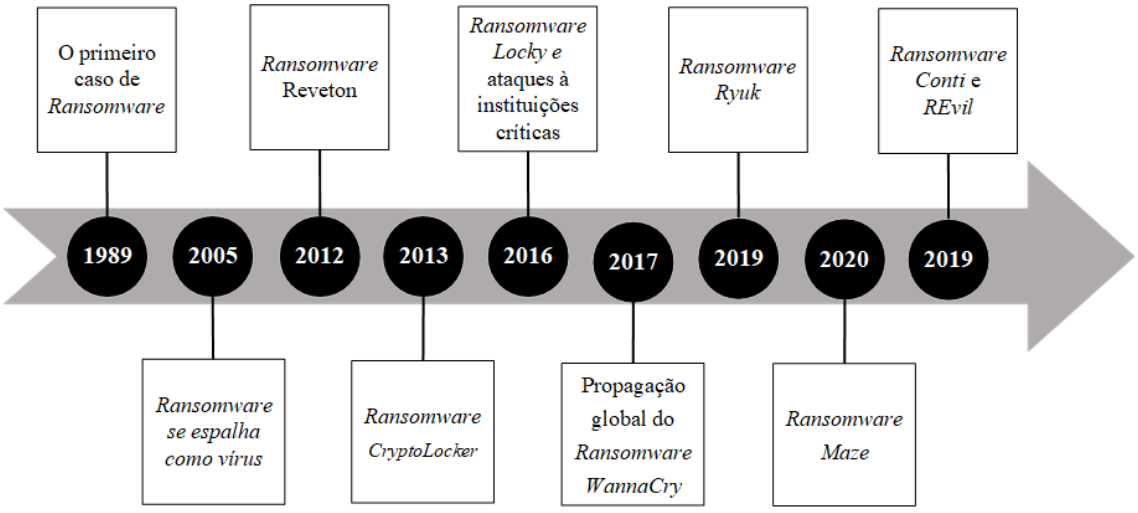
Wilhem, a primeira vítima de *Ransomware* conseguiu contornar a situação e começou a receber ligações de instituições e organizações médicas perguntando como ele o fez. Devido à sua experiência, ele atualmente trabalha como profissional de Segurança da Informação (CNN, 2021).

Apesar de sua investigação ter sido consideravelmente rápida e o autor encontrado, a história do *Ransomware* não acabou por aí. Como principais exemplos, em 2005, o *Ransomware* começou a se espalhar pela internet como um vírus. Já em 2012, o *Ransomware* Reveton se mostrou uma versão mais evoluída e sofisticada ao se disfarçar como uma mensagem de aplicação da lei (Lemos, 2017).

Em 2013, o *Ransomware* CryptoLocker se espalhou rapidamente por e-mail e exigia o pagamento em Bitcoin, dificultando a investigação da transação, tática que é utilizada até os dias atuais. Já em 2016, o *Ransomware* Locky se tornou uma das formas mais populares, atingindo hospitais e outras instituições críticas pois a venda de seus dados possui grande retorno financeiro. Em 2017, o *Ransomware WannaCry* se espalhou globalmente, infectando mais de 200.000 computadores em 150 países (FireEye, 2018).

Em 2019, o *Ransomware Ryuk* se tornou cada vez mais sofisticado e direcionado a grandes empresas. Em 2020, o *Ransomware Maze* se tornou ainda mais direcionado e perigoso ao exfiltrar os arquivos do usuário e ameaçar divulgá-los publicamente. E à partir de 2021, o *Ransomware* continua sendo uma ameaça significativa com ataques como o *Ransomware* Conti e REvil, enquanto surge o aparecimento de grupos de *Ransomware*, que trabalhando desta forma se tornam mais organizados e profissionais (McAffe, 2021).

Figura 2 – Linha do tempo da evolução do Ransomware baseado em McAffe (2021)



Na evolução e história do *Ransomware* foi possível separá-lo em categorias e tipos mais incidentes. Primeiramente é necessário compreender que é frequente haver confusão ao considerar o *Ransomware* como um vírus comum. Tal equívoco ocorre devido a uma imagem ultrapassada que muitas pessoas têm, segundo a qual todo malware é um vírus genérico, pois este é o tipo de malware mais conhecido e difundido, graças à sua habilidade de se replicar e incidência no dia a dia da população (AVG, 2022).

Um malware é uma categoria formada por programas desenvolvidos para prejudicar um computador (PagBank, 2023). Portanto, *Ransomwares*, cavalos de tróias, *spywares*, *adwares*, entre outros, são todos pertencentes às famílias de malwares (Ximenes, 2022).

Os meios mais utilizados para infecção de *Ransomware* utilizam táticas de Engenharia Social, como por exemplo, convencendo o usuário a baixar um arquivo infectado, convencendo-o que na verdade, seja algo de seu interesse (AVG, 2021).

Isso ocorre principalmente via e-mail, convencendo o usuário de que o arquivo malicioso enviado à ele é referente a algum site que este fez inscrição, ou até mesmo em corporações fingindo que é algum comando de um superior na cadeia hierárquica da empresa (Srinivas, 2021).

Existem também, infecções por *Malvertising*, que envolve a incorporação de *malware* em anúncios em sites populares, e kits de *exploit*, que são ferramentas de *hacking* que exploram vulnerabilidades em software desatualizado. Além disso, alguns sites maliciosos aproveitam navegadores desatualizados para baixar *malwares* em segundo plano (Rivera, 2023).

2.2. Incidência Global e Nacional

Em relação aos ataques cibernéticos as maiores vítimas estão nos setores empresariais, sobretudo no setor de Varejo. Baseado nas estatísticas, é possível constatar que o índice está direcionado ao segmento do comércio varejista representando 11% acima da média dos ataques observados em outros setores, e tem levado os agentes varejistas a não encararem a ação de ciberataque de *Ransomware* como uma simples hipótese, mas sim um fato eminente (Inside, 2022).

O setor que registrou a segunda maior incidência de ataques foi o governamental, devido ao fato de que estas realizam a coleta e o armazenamento de vastas quantidades de informações, que compreendem dados de cidadãos individuais que podem ser comercializados na *deep web*. Ademais, há o perigo de utilização de dados militares e de segurança nacional por organizações terroristas (Inside, 2023).

Apesar de não lidarem com dados financeiros ou bancários, a indústria da saúde não está a salvo. No ano de 2022, o setor da saúde sofreu o terceiro maior número de ataques por *Ransomware*. As informações contidas no histórico médico de um paciente podem ter um valor de até 50 vezes mais do que dados bancários no mercado negro da internet. Isso se deve à durabilidade dos dados e à capacidade de cometer fraudes mais lucrativas, como seguros de vida, ao invés de simples compras e empréstimos *online* (Pacete, 2022).

No cenário global, o ano de 2017 passou por três grandes ataques de *Ransomware*. Em maio, o *WannaCry* afetou cerca de 200 mil computadores em mais de 150 países, com prejuízo estimado em US$ 1 bilhão. No final de junho, mais um ataque global foi realizado, desta vez chamado *Petya*, que impactou mais de 12 mil computadores, encriptando *hard-drives* e os tornando inúteis. Por fim, em outubro, e com menor alcance, o *Bad Rabbit* afetou sistemas de aeroportos, metrôs e empresas de países como Rússia, Ucrânia, Turquia e Alemanha (Kapersky 2017).

O WannaCry surgiu porque a Agência de Segurança Nacional dos Estados Unidos desenvolveu uma exploração chamada *EternalBlue*, que se torna uma vulnerabilidade presente na implementação do protocolo *Server Message Block* (SMB) da Microsoft. Esta vulnerabilidade pode ser explorada devido ao fato de que muitas versões do Sistema Operacional *Windows* não manipulam pacotes especialmente criados corretamente, desta forma, um invasor pode criar pacotes especiais enviados ao dispositivo de destino, desencadeando uma exploração que pode ser usada para realizar ataques de *malware* no computador da vítima (Burdova, 2020).

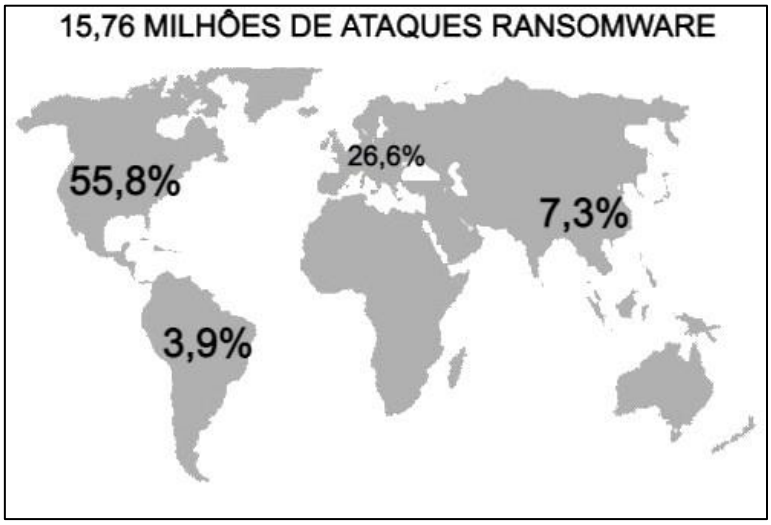
A Microsoft lançou uma atualização para correção desta vulnerabilidade meses antes do ocorrido, porém como não foi divulgada a importância da instalação, muitos usuários acabaram não realizando-a, o que permitiu o grande alcance do *WannaCry* (Root, 2022).

No ano de 2019 houve um aumento de 60% em relação ao ano anterior. Esses ataques, diferente de 2017, foram principalmente concentrados em municípios, e pelo menos 174 instituições municipais, com mais de 3.000 sub-organizações foram atacadas (Kapersky,2019).

Um dos casos conhecidos pela mídia de infecção de *Ransomware* em 2019, foi do *malware Bitpaymer* que vitimou várias empresas espanholas e uma rádio (Chieco, 2019). As empresas conseguiram reverter o problema e mitigar seus impactos sem pagar aos criminosos. Dessa forma o *Bitpaymer* modificou seu código de acordo com estes aprendizados, evoluiu e atualmente é conhecido como *FriedEx* (Poslušný, 2021).

O ano de 2022 foi marcado com um grande acréscimo de ataques *Ransomware* (Figura 3) visto que estes quase dobraram comparado ao ano anterior. A américa do norte foi a maior vítima, com 55,9% dos ataques, em segundo lugar ficou a Europa com 26,6% dos ataques, seguida pela Ásia com 7,3% e por último a América do Sul com 3,9% (Abranet,2023).

Figura 3 – Ataques *Ransomware* em 2022 divididos por continente baseado em Abranet (2023)



No Brasil, os ataques *Ransomware* começaram a tomar conta do mercado a partir de 2018, quando um *malware* brasileiro chamado *Cry Brazil* (Figura 4) chamou a atenção de pesquisadores, criptografando dados de usuários brasileiros e tendo como principal característica a troca do papel de parede do Windows com uma mensagem em português pedindo resgate para liberar o acesso dos documentos armazenados (Perrone, 2018).

Figura 4 - Papel de Parede Cry Brazil baseado em Perrone (2018)

A versão do *Ransomware Cry Brazil* não fez nenhuma grande empresa de vítima, seu foco foi principalmente usuários comuns. Este foi apenas o início de um cenário que colocaria o Brasil no *ranking* mundial como um dos países mais afetados pelo vírus no mundo (Perrone, 2018).

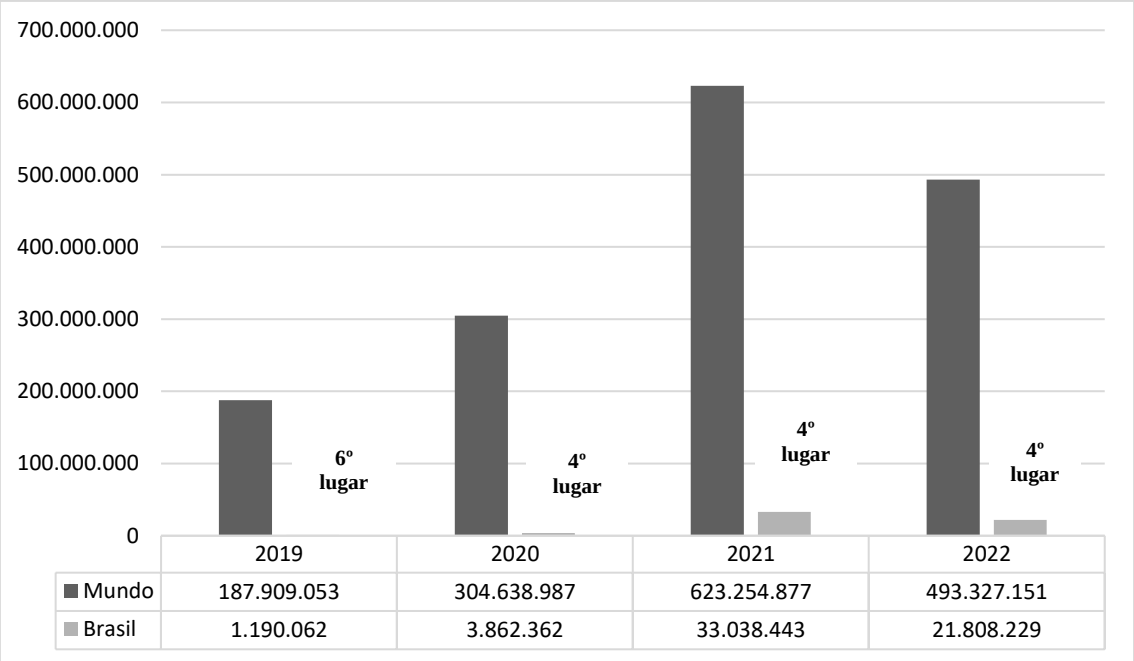
Em 2020, o Brasil sofreu o total de 187.909.053 ataques (Figura 5) ocupando o 6° lugar no ranking de países mais afetados por *Ransomware* no mundo (Report, 2021). Em 2022 essa marca ultrapassou o número de 21.808.229 ataques, consolidando o país no 4 lugar deste ranking, visto que este já o ocupava desde 2020 (SonicWall, 2023).

O ano de 2021, além de trazer o Brasil para o quarto lugar no ranking global de ataques *Ransomware*, também foi marcado pela vitimização de duas grandes empresas brasileiras: As lojas Renner, do ramo de vestuários e a CVC, do mercado de turismo, trouxeram visibilidade à problemática de Segurança da Informação (Pacete, 2021).

O ataque sofrido pela Renner foi um grande marco na segurança da informação nacional, pois graças a sua repercussão, o assunto ganhou visibilidade (Gaidargi, 2021). A empresa divulgou um comunicado informando que havia ocorrido um ataque cibernético em seu ambiente de TI e que este causou indisponibilidade em parte de seus sistemas e operação. Esta também ressaltou que rapidamente acionou os protocolos e

procedimentos existentes de controle e segurança para bloquear o ataque e minimizar eventuais impactos (Upx, 2021).

Figura 5 – Ataques *Ransomware* no Brasil baseado em SonicWall (2023)



	2019	2020	2021	2022
Mundo	187.909.053	304.638.987	623.254.877	493.327.151
Brasil	1.190.062	3.862.362	33.038.443	21.808.229

O caso da empresa de viagens CVC também é outro caso importante para a segurança da informação nacional pois diferente da Renner, esta só conseguiu obter o reestabelecimento normal das operações 10 dias após o ataque cibernético (ABC, 2019).

Consequente deste cenário cerca de 850 lojistas da CVC informaram dúvidas e inseguranças relatadas por clientes que compraram na empresa antes da invasão cibernética, e demonstraram preocupação, se seus dados de cartões e pessoais, estavam seguros após a invasão ou se foram violados, comprometidos ou vendidos pelos criminosos. Apesar de a empresa não ter exposto os prejuízos causados durante esse período de interrupção, estima-se que este foi extremamente alto, visto que o prejuízo aumenta de acordo com o tempo que a organização fica fora do ar (Branco, 2021).

Para evitar estes cenários é extremamente importante que nas organizações sejam disseminadas formas de prevenção através da conscientização e treinamento de funcionários. É importante que eles estejam cientes dos riscos associados ao *Ransomware* e saibam como identificar e evitar possíveis ameaças. Além disso, é fundamental manter os sistemas operacionais e aplicativos atualizados e utilizar programas de antivírus e *anti-malware* (Kapersky, 2022)

É importante que existam backups e estes sejam armazenados em locais seguros e que os procedimentos de recuperação de dados sejam testados regularmente. Caso a empresa seja vítima de um ataque de *Ransomware*, é fundamental ter um plano de contingência para mitigar os danos (McAfee, 2023).

Em resumo, a prevenção e mitigação de ataques de *Ransomware* em empresas exigem uma abordagem holística, envolvendo a conscientização dos funcionários, a atualização de sistemas e aplicativos, o backup regular de dados e a criação de um plano de contingência eficaz. A implementação dessas medidas pode ajudar a reduzir significativamente o risco de ataques de *Ransomware* e minimizar os danos em caso de ocorrência (Paiva, 2023).

Em 2020 foi identificado que o fato de que as empresas não pagaram o resgate, não torna o trabalho dos criminosos em vão, já que há uma nova abordagem híbrida onde a tática de leiloar informações roubadas foi adotada. Os criminosos se unem em organizações tipo cartel para realização destas atividades e compartilhamento de seu conhecimento (Grustniy, 2021).

2.3. Ransomware e a Legislação

Uma grande problemática relacionada aos *Ransomwares* é que estes são extremamente rentáveis para seus autores. Das organizações afetadas por ataques cibernéticos no país, 92% delas possuíam uma apólice de seguro cibernético. Além disso, o estudo constatou que 93% das seguradoras estavam dispostas a pagar o resgate exigido pelos criminosos para descriptografar os arquivos comprometidos. É importante ressaltar que sete em cada 10 organizações conseguiram recuperar o acesso aos seus dados após efetuarem o pagamento do resgate exigido pelos criminosos (Auler & Justo, 2022)

Além disso, o pagamento aos criminosos encoraja os hackers a criarem mais ataques desse tipo. Mesmo que a vítima não pague, estes ainda ganham dinheiro com a venda de dados na internet, prática que inclui até mesmo organização em cartéis (Elsad, 2022).

O principal problema em relação aos ataques *Ramsomware* é a dificuldade em punir seus autores. Em muitos casos, os responsáveis operam em países onde as leis são mais brandas em relação a crimes cibernéticos. Em outros casos, utilizam técnicas para dificultar a identificação da origem do ataque, como o uso de redes virtuais privadas e a utilização de criptomoedas para receber o pagamento do resgate (Finelli, 2016).

Além disso, muitas vezes os órgãos de investigação não possuem recursos suficientes para realizar uma investigação efetiva e identificar os responsáveis pelo ataque. Como resultado, muitos casos de ataques *Ransomware* acabam ficando impunes, o que incentiva ainda mais sua prática (Biales, 2020).

Outro fator que dificulta a punição dos autores de ataques *Ransomware* é a falta de cooperação entre países em relação a crimes cibernéticos. Como o ataque pode ter origem em um país e o resgate ser pago em outro, é necessário que haja uma cooperação internacional para que seja possível identificar os responsáveis e aplicar as leis de cada país (Garcez, 2022)

Portanto, a dificuldade na punição dos autores de ataques *Ransomware* é um grande desafio para as autoridades e empresas de segurança cibernética. É preciso investir em tecnologias e recursos para identificar e punir esses criminosos, além de buscar uma maior cooperação internacional para combater esse tipo de crime de forma efetiva (Lemos, 2020).

No Brasil, não existe uma lei específica que trate exclusivamente do crime de *Ransomware*. No entanto, algumas legislações podem ser aplicadas para punir os responsáveis por essa prática criminosa (Schettini, 2022).

Em território brasileiro, a legislação de combate a crimes cibernéticos é composta, principalmente, pela Lei nº 12.737/2012, também conhecida como Lei Carolina Dieckmann, e pela Lei nº 13.709/2018, Lei Geral de Proteção de Dados Pessoais (LGPD). Ambas as leis trazem dispositivos que visam a prevenção e repressão de atividades ilícitas no ambiente virtual (Araujo, 2023).

O Código Penal Brasileiro prevê sanções criminais para quem produz, oferece, distribui, vende ou difunde programa de computador com o intuito de causar dano à integridade de dados, programas ou sistemas de computador, sem autorização ou consentimento do titular. Essa conduta pode ser enquadrada no artigo 154-A do Código Penal, que trata do crime de invasão de dispositivo informático (Cabette, 2014).

Além disso, a LGPD estabelece normas para proteção de dados pessoais, o que inclui a prevenção de vazamento ou sequestro de informações sensíveis. Dessa forma, empresas e organizações que não implementam medidas adequadas de segurança cibernética podem ser responsabilizadas por eventuais danos causados aos titulares de dados (Nones, 2022).

Por fim, é importante mencionar que o Brasil é signatário da Convenção de Budapeste sobre o Cibercrime, tratado internacional que estabelece cooperação entre países no combate a crimes cometidos no ambiente virtual. Através dessa convenção, é possível aprimorar a troca de informações e a investigação de casos de *Ransomware* que transcendem as fronteiras nacionais (Berbert, 2021).

3. Metodologia

A metodologia aplicada foi estudo de caso (YIN, 2021), pois o estudo tem como objetivo, entender as experiências de profissionais de Segurança da Informação com *Ransomware*, lições aprendidas e estratégias de mitigação apoiadas atualmente por estes. Na Tabela 1 são apresentadas as características utilizadas para a realização do estudo.

Tabela 1 – Características do Estudo

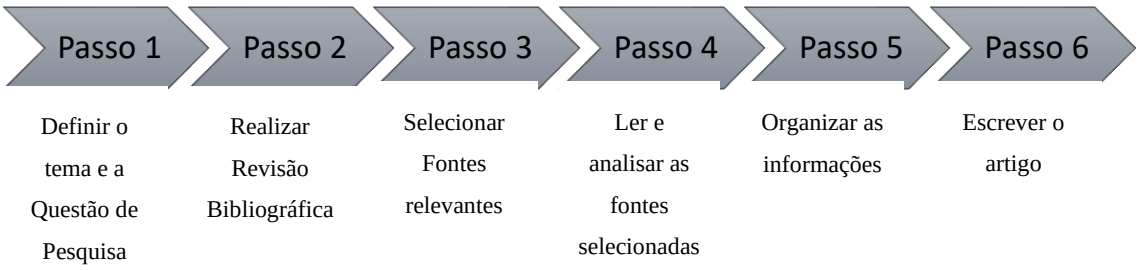
Item	Descrição	Autor(es)
Questão de Pesquisa	"As ações de prevenção, contenção e recuperação conhecidas por profissionais da área de Segurança da Informação evoluíram junto com o Ransomware?"	
Natureza	- Qualitativa	GIL (2022)
Metodologia	- Análise Bibliográfica	ECO (1997)
Coleta de Dados	- Análise documental	TEÓPHILO; MARTINS (2016)
Unidade de análise	- Artigos, publicações e notícias relacionadas à ataques *Ransomware*	

3.1. Processo Metodológico

As etapas desta pesquisa, conforme Figura 6, são:

- **Passo 1: Definir o tema e a questão de pesquisa.** O tema de pesquisa foi definido e uma questão de pesquisa clara foi formulada;
- **Passo 2: Realizar revisão bibliográfica inicial.** Foi realizada uma pesquisa inicial em bases de dados acadêmicas, bibliotecas e outras fontes confiáveis para obter uma visão geral do estado atual do conhecimento sobre o tema;
- **Passo 3: Selecionar as fontes relevantes.** As fontes bibliográficas foram avaliadas e selecionadas com base em sua relevância para o tema de pesquisa;
- **Passo 4: Ler e analisar as fontes selecionadas.** As fontes selecionadas foram lidas atentamente e analisadas, fazendo anotações sobre os principais conceitos, argumentos, metodologias e resultados apresentados;
- **Passo 5: Organizar as informações.** As informações obtidas das fontes bibliográficas foram organizadas de acordo com uma estrutura lógica ou esquema previamente definido; e
- **Passo 6: Escrever o artigo.** Com base na estrutura organizada e nas informações

Figura 6 - Procedimentos Metodológicos



4. Análise e Interpretação dos Resultados

4.1. Identificação do Tipo de Ransomware

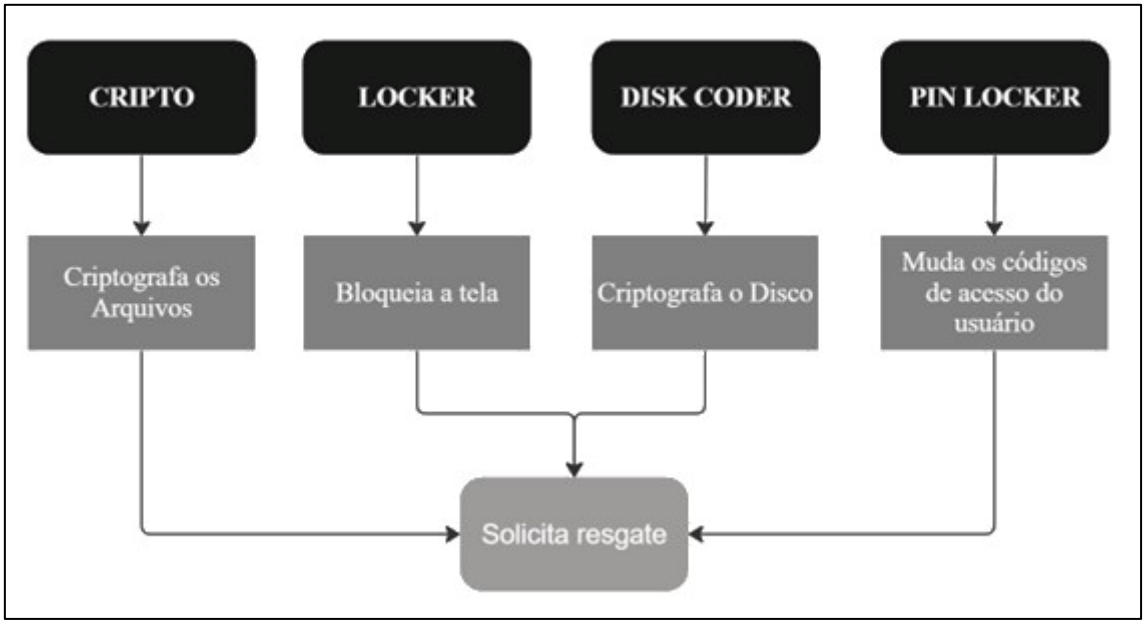
A partir da literatura foi possível identificar os tipos de *Ransomwares: Crypto malware* (Burdova, 2022), *Locker* (Moura,2022), *Scareware* (Ramos, 2021), *Doxware* (Klusaité,2022) *Spora* (Mekauskas, 2020), *Petya* (Belcic, 2017) e *Reveton* (Lessing, 2020) e seu modo de infecção conforme apresentado na Figura 8.

Os *Ransomwares* podem ser divididos em quatro categorias principais (Figura 7): O *Crypto Ransomware* criptografa arquivos da vítima, o dispositivo continua funcionando normalmente, porém estes arquivos não podem ser abertos (Meskauskas, 2021). O *Locker Ransomware* que não realiza criptografia, mas bloqueia funções básicas do dispositivo como não permitir o acesso a área de trabalho ou bloquear parcialmente o teclado (Moura, 2022).

Em relação ao "*disk coder*" criptografa os arquivos no disco rígido da vítima impedindo o acesso aos dados. Esse tipo de *Ransomware* pode se espalhar por toda a rede da vítima, criptografando arquivos em outros dispositivos conectados. Esse tipo de *Ransomware* é mais comumente encontrado em computadores de mesa e laptops (Cossetti, 2023).

Desde seu surgimento era comum o pensamento da existência de *Ransomwares* somente em computadores, mas estes já evoluíram e se sofisticaram, atualmente o *Ransomware "Pin Locker"* bloqueia a tela do dispositivo com um código PIN, e é comum em dispositivos móveis (Osborne, 2015).

Figura 7 – Principais Tipos de Ransomware baseado em Moura (2022) e AVG (2021)



A variante de *Ramsomware Locker* infecta os computadores das vítimas através de arquivos baixados da internet - geralmente versões piratas de jogos. Quando infiltrado e executado com sucesso, este encripta os arquivos do computador e estabelece um prazo de 72 horas para resgate. Caso este prazo não seja cumprido o malware apaga as Cópias Shadow Volume tornando a recuperação dos arquivos impossível (Moura, 2022).

Já o *ScareWare* tem como intuito manipular o usuário através do medo. Este exibe uma mensagem na tela se passando por um antivírus informando falsamente a vítima de que há algo errado em seu dispositivo e que é necessária a instalação de uma aplicação para resolução do problema. Essa aplicação na verdade é um malware que pode acessar as informações pessoais, financeiras e de navegação da vítima (Ramos, 2021).

Uma das variantes mais temidas é o *DoxWare* pois este chantageia o usuário ameaçando-o a expor seus arquivos e informações confidenciais publicamente. Geralmente infecta redes e computadores através de *phishing* com links e anexos maliciosos ou através de sites que contém códigos capazes de explorar vulnerabilidades de segurança não corrigidas no sistema de um visitante (Klusaitė, 2022).

O Spora é um *Ramsomware* que trabalha através do *JavaScript.* Um executável é enviado por e-mail para a vítima que baixa e o executa, desta forma uma pasta é extraída e um documento em *JavaScript* chamado ("closed.js") é colocado no sistema de pasta "%temp%". A pasta em *JavaScript* extrai outro executável com nome aleatório que sai encriptando as pastas da vítima. O Spora não necessita de internet para trabalhar (Meskauskas, 2020).

Um dos *Malwares* mais difíceis de remediar é o Petya, que criptografa o guia de referência rápida do computador para cada arquivo em seu HD (MFT) fazendo com que o computador não consiga inicializar ou funcionar normalmente. Em um computador Windows, ele infecta o MBR que é responsável por carregar o sistema operacional. Desta forma, o Malware obriga o computador a reinicializar enquanto criptografa o MFT, a partir disto o computador não consegue acessar nada do disco rígido, nem o próprio sistema operacional (Belcic, 2019)

O *Ramsomware* Reveton ficou famoso por se apresentar como agências policiais e governamentais, sendo personalizado para cada país. Este bloqueava a tela e exigia que os usuários pagassem uma "multa" sob ameaça de prisão (Lessing, 2020).

Por fim, os tipos *Cerber* e *Locky* são malwares que conseguem criptografar grande variedade de arquivos específicos, geralmente mídias e documentos que o usuário mais acessa, enquanto o *Locky* pode alterar o código-fonte do computador, o que o torna inutilizável (Avast, 2020).

Tabela 2 - Tipos e Características mais comuns de *Ransomware*

Variantes	Características
Crypto malware	Explora uma vulnerabilidade do Windows, deixando a máquina exposta para criptografar os arquivos e pedir resgates (Burdova, 2022).
Locker	Infecta o SO impossibilitando acesso a todos os arquivos e aplicativos (Moura, 2022).
Scareware	Age como um antivírus falso afirmando ter encontrado problemas e solicitando dinheiro para resolver, enchendo a tela de mensagens *pop-up* (Ramos, 2021).
Doxware	Ameaça publicar as informações do usuário on-line caso o resgate não seja pago (Klusaitė, 2022).
Spora	Infecta o sistema através de *phishing*, agindo incialmente como um usuário administrador, mostrando uma janela pop-up que não some até que o usuário a aceite (Meskauskas, 2020).
Petya	Impede o acesso a todo o disco rígido, criptografando a tabela de arquivos mestre (Belcic, 2017).
Reveton	Bloqueia as telas em vez de criptografar os arquivos (LESSING, 2020).
Cerber e Locky	Pesquisam e criptografam tipos específicos de arquivos, geralmente documentos e arquivos de mídia (AVAST, 2021).

O *Ransomware* está em constante evolução, atualmente até mesmo sistemas operacionais como MacOS e Linux já possuem variantes de *Ransomware* adaptadas para si - Assim como os dispositivos *Android* (Avelino, 2023).

Este *Malware* é difundido principalmente por quadrilhas, que se organizam, desenvolvem e realizam os ataques, em um levantamento realizado pela Microsoft, foi estimado que existam pelo menos 100 destas em todo o mundo (Brasiline, 2023). Este mercado é organizado e bem sofisticado porque é bastante lucrativo, uma pesquisa da Tren Micro estima que a Indústria de *Ransomware* já fatura mais de US$ 400 milhões ao ano (Advisor, 2023).

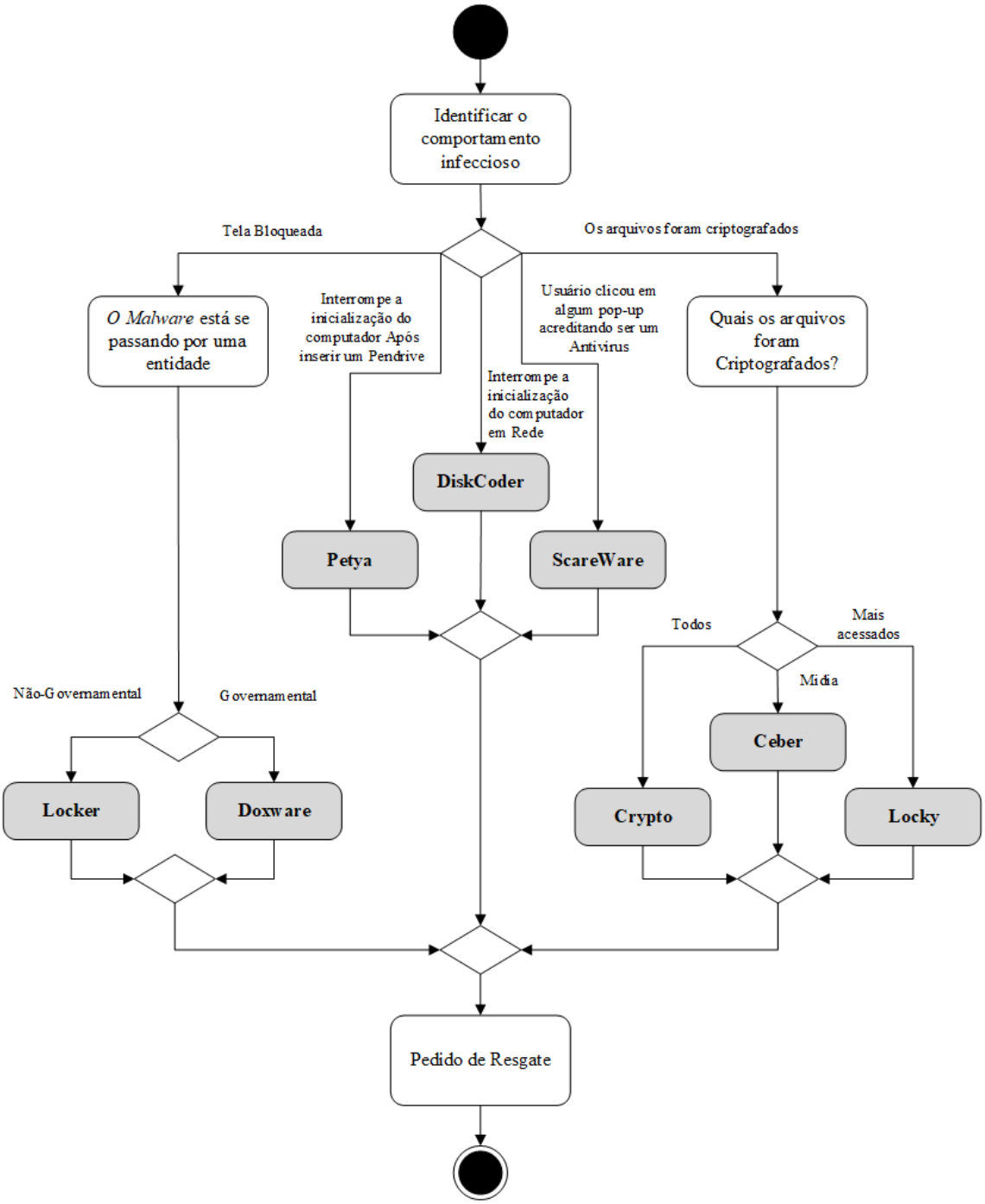
As quadrilhas de *Ransomware* também oferecem na *dark web* o chamado *Ransomware as a Service* (RaaS), ou *Ransomware* como Serviço, que permitem que criminosos cibernéticos sem habilidades técnicas consigam comprar esses kits, que possuem suporte 24 horas e 7 dias por semana, e fazer vítimas sem mesmo precisar desenvolver o *Malware* (Padeiro, 2023).

De acordo com uma pesquisa realizada pelo Relatório Anual de Defesa Cibernética/*Cyber Defense Report* (CDR), cerca de 78% das empresas que foram vítimas de *Ransomware*, mesmo conseguindo mitigar a situação, enfrentaram consequências de ameaças adicionais, como vazamento de dados, notificação à mídia ou outros tipos de ataques conjuntos como por exemplo, *DDoS* (Advisor, 2023).

4.2. Identificação do Tipo de Ransomware

A possibilidade de identificação do tipo de ataque *Ransomware* pode auxiliar os analistas de Tecnologia da Informação (Ramos, 2021; Moura, 2022; Advisor, 2023; Avelino, 2023), desta forma, a partir do referencial teórico foi elaborado um *Framework* de Identificação de *Ransomware* (Figura 8).

Figura 8 – *Framework* de Identificação de Ransomware



4.3. Discussões

É possível inferir que como o crime cibernético não requer ação ou esforço físico e os criminosos não sofrem consequências em suas vidas pessoais, pode reduzir a percepção da gravidade de suas ações (Schreiber, 2022).

5. Conclusões

O mercado do *Ransomware* tem crescido cada vez mais e consequentemente se tornado mais lucrativo para os criminosos, o que ocasiona grande investimento de tempo e dinheiro destes para aprimorar as tecnologias cada vez mais.

As empresas e usuários devem seguir a evolução da criminologia, evoluindo também seus métodos de proteção. É importante investir em métodos de resposta e continuidade à *Ransomware*, mas é muito mais importante que isso investir em conscientização e prevenção. Pois mesmo conseguindo mitigar a ameaça, uma vez que este infecta o computador pode trazer outros tipos de ataque ou ocasionar vazamento de dados.

Decorrente da vergonha ou até mesmo medo ocasionado por um ataque *Ransomware*, grande parte das empresas não divulgam detalhes sobre o ocorrido, mas é importante que isso seja feito para que profissionais de segurança fora desta possam estudar e entender possíveis novas variantes de *Ransomware* ou evoluções e mudanças de comportamento das variantes já existentes.

A contribuição para a teoria está em apresentar as formas de ataques dos principais tipos de *Ransomware*. A contribuição para a prática é alertar os gestores e gerentes de segurança da informação das formas de ataques.

Referencial Bibliográfico

ABC, Diário do (2021). Ataque cibernético prejudica vendas da CVC há cinco dias, SP. Editora Redação. Disponível em: https://www.dgabc.com.br/Noticia/3781374/ataque-cibernetico-prejudica-vendas-da-cvc-ha-cinco-dias

Abranet (2023) Ataques *Ransomwares* Continuam Sendo os Preferidos dos Criminosos, SP. Editora Convergência Digital. Disponível em: https://www.abranet.org.br/Noticias/ Ataques-ransomware-continuam-sendo-os-preferidos-dos-criminosos4212.html?UserActiveTemplate=site#ZCd5kHvMLIU.

Advisor, CISO (2023). Cerca de 4 em cada 5 ataques de *Ransomware* têm outras ameaças. BR. Disponível em: https://www.cisoadvisor.com.br/cerca-de-4-em-cada-5-ataques-de-Ransomware-contem-outras-ameacas/

Advisor, CISO (2023). Indústria de *Ransomwar*e já fatura mais de US$ 400 milhões ao ano. BR. Disponível em: https://www.cisoadvisor.com.br/ industria-de-Ransomware-movimenta-mais-de-us-400-mi-ao-ano

Araujo, J (2023). Dez anos de vigência da Lei Carolina Dieckmann: a primeira a punir crimes cibernéticos. DF. Disponível em: https://www12.senado.leg.br/radio/1/noticia/2023/03/29/dez-anos-de-vigencia-da-lei-carolina-dieckmann-a-primeira-a-punir-crimes-ciberneticos#:~:text=Portanto%2C%20desde%20mar%C3%A7o%20de%202023,dispositivos%20inform%C3%A1ticos%20para%20instalar%20vulnerabilidades

Auler, F & Justo, G (2022). Ataques à propriedade virtual e o seguro cyber. SP. Disponível em: https://www.conjur.com.br/2022-jul-07/seguros-contemporaneos-ataques-propriedade-virtual-seguro-cyber

Avast (2020). *Ransomware Cerber*: Tudo que você precisa saber. Disponível em: https://www.avast.com/pt-br/c-cerber.

Avelino, Y. (2023). *RustBucket*: crackers estariam visando Macs com novo malware. PE. Disponível em: https://macmagazine.com.br/ post/2023/05/05/rustbucket-crackers-estariam-visando-macs-com-novo-malware

AVG (2021). Guia de Proteção e Remoção de *Ransomware*. Disponível em: https://www.avg.com/pt/signal/what-is-Ransomware.

Belcic, I. (2019*). Ransomware Petya:* Como funciona e como se proteger. AVAST. Disponível em: https://www.avast.com/pt-br/c-petya

Berbert. L. (2021). Contra cibercrimes, Brasil passa a ser signatário da Convenção de Budapeste. SP. Disponível em: https://www.telesintese.com.br/brasil-assina-convencao-contra-cibercrimes.

Bertolucci, G. (2019). *Ransomware* causa demissão de 300 funcionários de empresa, MG. Disponível em: https://livecoins.com.br/Ransomware-causa-demissao-300-funcionarios-empresa.

Biancamano, P (2021). 5 prejuízos que um ataque *Ransomware* pode causar a sua empresa. RJ. Disponível em: https://www.psafe.com/blog/5-prejuizos-que-um-ataque-Ransomware-pode-causar-a-sua-empresa/.

Branco, D. (2021). CVC segue com prejuízos em vendas devido a ataque de *Ransomware*. Canaltech. Disponível em: https://canaltech.com.br/ seguranca/cvc-segue-com-prejuizos-em-vendas-devido-a-ataque-de-Ransomware-198352

Brasiline (2023). Microsoft diz rastrear mais de 100 quadrilhas de *Ransomware*. BR. Disponível em: https://brasiline.com.br/blog/microsoft-diz-rastrear-mais-de-100-quadrilhas-de-Ransomware/

Burdova, C. (2022). What Is Eternal Blue and Why Is the MS17-010 Exploit Still Relevant?. London, United Kingdom. Disponível em: https://www.avast.com/c-eternalblue.

Cabette, E (2014). Crime de Invasão de Dispositivo Informático (artigo 154 - A, CP). SP. https://www.jusbrasil.com.br/artigos/crime-de-invasao-de-dispositivo-informatico-artigo-154-a-cp/153070617.

Chieco, B (2019). Everis sofre ataque de *Ransomware*. Disponível em: https://www.mentebinaria.com.br/noticias/portal-mente-bin%C3%A1ria/everis-sofre-ataque-de-Ransomware-r182/.

CNN Brasil (2021). A bizarra história do inventor do *Ransomware;* vírus deixou parte dos EUA sem gás. Disponível em: https://www.cnnbrasil.com.br/economia/a-bizarra-historia-do-inventor-do-Ransomware-virus-deixou-parte-dos-eua-sem-gas/#:~:text= Willems%20esperava%20ver%20pesquisas%20m%C3%A9dicas,dos%20EUA%20na%20semana%20passada.

Cossetti, M. (2023). O que é um *Ransomware*?. RJ. TECNOBLOG. Disponível em: https://tecnoblog.net/responde/o-que-e-um-Ransomware/

Elsad, A. (2022). Threat Assessment: Black Basta Ransomware. USA. Disponível em: https://unit42.paloaltonetworks.com/threat-assessment-black-basta-Ransomware/

Finelli, A. (2016). Por que o *Ransomware* ainda lidera o ranking de ataques?. SP. Conteudo Editorial. Disponível em: https://www.securityreport.com.br/por-que-o-Ransomware-ainda-lidera-o-ranking-de-ataques/

FireEye (2018). Global Ransomware Study, USA. Disponível em: https://www.fireeye.com/content/dam/fireeye-www/global/en/current-threats/pdfs/wp-global-Ransomware-study.pdf.

Gaidargi, J. (2021). Renner é vítima de *Ransomware* – E se fosse você? SP. Disponível em: https://www.infonova.com.br/seguranca/renner-ransonware-consequencias-solucoes/.

Garcez, J. (2022). Breves Anotações Sobre a Cooperação Jurídica Internacional na Convenção de Budapeste e a Investigação e Persecução de Crimes Cibernéticos. RO. Disponível em: http://www.conteudojuridico.com.br/consulta/artigos/58147/breves-anotaes-sobre-a-cooperao-jurdica-internacional-na-conveno-de-budapeste-e-a-investigao-e-persecuo-de-crimes-cibernticos .

Grustniy, L. (2021). A saga do *Ransomware*. RU. Kapersky. Disponível em: https://www.kaspersky.com.br/blog/history-of-Ransomware/17280/.

Guedes, M. (2021). O que é Engenharia Social?, SP. Disponível em: https://www.treinaweb.com.br/blog/o-que-e-engenharia-social.

Inside, TI (2023). Setor Financeiro é o segundo mais atingido por ataque de *Ransomwares*. SP. Disponível em: https://tiinside.com.br/ 06/04/2023/setor-financeiro-e-o-segundo-mais-atingido-por-ataque-de-Ransomwares/.

Inside, TI. (2022). Varejo é o setor mais atacado por *Ransomware*, segundo pesquisa da Sophos. BR. Disponível em: https://tiinside.com.br/ 25/11/2022/cinco-dicas-da-sophos-para-compras-seguras/.

Kapersky (2017). História do Ano de 2017 da Kaspersky Lab: mais de um quarto dos ataques de *Ransomware* visa empresas. SP. Disponível em: https://www.kaspersky.com.br/about/press-releases/2017_kaspersky-lab-more-than-a-quarter-of-Ransomware-attacks-target-companies-in-2017.

Kapersky (2019). *Ransowmare* e cidades: mais de 170 ataques em 2019. SP. Disponível em: https://www.kaspersky.com.br/about/press-releases/2019_ransowmare-e-cidades-mais-de-170-ataques-em-2019 .

Kapersky (2023). Proteção contra *Ransomware*: como manter seus dados seguros em 2023. SP. Disponível em: https://www.kaspersky.com.br/resource-center/threats/how-to-prevent-Ransomware .

Kelly, M. (2021). The bizarre story of the inventor of Ransomware, USA. CNN Business. Disponível em: https://edition.cnn.com/2021/05/16/tech/ Ransomware-joseph-popp/index.html.

Klusaitė, L (2022). *Ransomware:* o que é e como se proteger?. NordVPN. Disponível em: https://nordvpn.com/pt-br/blog/o-que-e-Ransomware/

Laccelva, F. (2021). Os 10 distúrbios psicológicos mais comuns e suas características, SP. Disponível em: https://blog.fepo.com.br/psicologia/os-10-disturbios-psicologicos-mais-comuns-e-suas-caracteristica/.

Lemos, R. (2017). *Ransomware:* O Sequestrador de Dados, RS. Disponível em: https://www.linkedin.com/pulse/Ransomware-o-sequestrador-de-dados-vinicius-m-s-lemos/?originalSubdomain=pt.

Lemos, R. (2020). Ataque ao STJ é sinal de alerta. SP. Folha de São Paulo. Disponível em: https://itsrio.org/pt/artigos/ataque-ao-stj-e-sinal-de-alerta/

Lessing, M. (2020). Case Study: AIDS Trojan Ransomware, USA. Studios Editor. Disponível em: https://www.sdxcentral.com/security/definitions/what-is-Ransomware/case-study-aids-trojan-Ransomware/.

Lessing, M. (2020). Case Study: Reveton Ransomware. USA. Disponível em: https://www.sdxcentral.com/security/definitions/what-is-Ransomware/ case-study-reveton-Ransomware/

McAfee (2022). O que é *Ransomware*?. CA, USA. Disponível em: https://www.mcafee.com/blogs/pt-br/internet-security/8-dicas-para-ficar-protegido-contra-ataques-de-Ransomware/.

McAffe (2021). Threats Report, USA. Disponível em: https://www.mcafee.com/enterprise/en-us/threat-center/threat-reports.html.

Mekauskas, T. (2020). Ransomware Spora. Disponível em: https://www.pcrisk.pt/guias-de-remocao/8473-spora-Ransomware

Meskauskas, T. (2021). Vírus Locker. Lituânia. Disponível em: www.pcrisk.pt/guias-de-remocao/7918-locker-virus.

Moura, B. (2022). Os 14 tipos de *Ransomware* mais perigosos da web. RJ. Disponível em: https://www.psafe.com/blog/os-14-tipos-de-Ransomware-mais-perigosos-da-web/.

Moura, B. (2022). Ransomware Locker: o que é e como evitar. SP. TECNOBLOG. Disponível em: https://www.psafe.com/blog/Ransomware-locker-o-que-e-e-como-evitar/

Mujezinovic, D. (2021) AIDS Trojan: The Story Behind the First Ever Ransomware Attack. Disponível em: https://www.makeuseof.com/aids-trojan-the-first-Ransomware-attack-in-history/.

Nones, F. (2022). LGPD: o que diz a lei de proteção de dados e como ela pode impactar a sua estratégia de marketing e vendas. SP. Disponível em: https://resultadosdigitais.com.br/marketing/o-que-e-lgpd/

Osborne, C. (2015). Lockerpin Ransomware steals PINs, locks Android devices permenantly. USA. Disponível em: https://www.zdnet.com/article/ lockerpin-Ransomware-steals-pins-locks-android-devices-permenantly/

Pacete, L (2022). Dados de saúde valem mais que informações financeiras na dark web. Dísponível em:https://forbes.com.br/forbes-tech/2022/06/dados-de-saude-chegam-a-valer-mais-que-informacoes-financeiras-na-dark-web/.

Pacete, L. (2021). 5 ataques cibernéticos no Brasil em 2021 que geraram alerta. SP. Forbes. Disponível em: https://forbes.com.br/forbes-tech/2021/12/5-ataques-ciberneticos-no-brasil-em-2021-que-geraram-alerta/.

Padeiro (2023) Ransomware As A Service (RaaS) Explained How It Works & Examples, USA. Crowdstrike. Disponível em: https://www.crowdstrike.com/cybersecurity-101/Ransomware/ransom ware-as-a-service-raas/.

PagBank (2023). Malware: saiba o que é e como proteger seus dados!. SP. Disponível em: https://blog.pagseguro.uol.com.br/o-que-e-malware/.

Paiva, C. (2023). Cibersegurança existe responsabilidade e diigencia coletivas. MG. Disponível em: https://www.diariodoaco.com.br/noticia/0106554-opiniao-ciberseguranca-exige-responsabilidade-e-diligencia-coletivas.

Perrone, G. (2018). Cry Brazil: Ransomware sequestra PCs de brasileiros; saiba se proteger, RJ. Disponível em: https://sbackup.online/cry-brazil-Ransomware-sequestra-pcs-de-brasileiros-saiba-se-proteger/.

Poslušný, M (2020). O Ransomware Bitpaymer foi um trabalho dos criadores do Dridex. RJ. Disponível em: https://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=&cad=rja&uact=8&ved=2ahUKEwjMv8eRyfX_AhUKrJUCHf_YAMAQFnoECBAQAQ&url=https%3A%2F%2Fwww.welivesecurity.com%2Fbr%2F2018%2F01%2F31%2Ffriedex-o-Ransomware-bitpaymer-foi-um-trabalho-dos-criadores-do-dridex%2F&usg=AOvVaw1kyot0hs4SuvyOJG7FXLDb&opi=89978449.

Prabhu, S. R., & van Wagoner, N (2023). Human Immunodeficiency Virus Infection and Acquired Immunodeficiency Syndrome (HIV/AIDS): An Overview. Sexually Transmissible Oral Diseases, 51.

Ramos, G. (2021). O que é scareware? Entenda o programa malicioso que 'causa medo'. RJ. Disponível em https://www.techtudo.com.br/listas/2021/03/o-que-e-scareware-entenda-o-programa-malicioso-que-causa-medo.ghtml.

Report, Security (2022). Brasil foi o 5º país com mais ataques cibernéticos em 2021. SP. Conteúdo Editorial. Disponível em: https://www.securityreport.com.br/overview/brasil-foi-o-5o-pais-com-mais-ataques-ciberneticos-em-2021/#.ZCisl3vMLIU

Report, Security (2022). Brasil foi o 5º país com mais ataques cibernéticos em 2021. SP. Conteúdo Editorial. Disponível em: https://www.securityreport.com.br/overview/brasil-foi-o-5o-pais-com-mais-ataques-ciberneticos-em-2021/#.ZCisl3vMLIU.

Rivera, J. (2023). How Big Tech enables cybercriminals via 'malvertising'. TO. TORONTO SUN. Disponível em: https://torontosun.com/opinion/columnists/rivera-how-big-tech-enables-cybercriminals-via-malvertising

Root, E. (2022). As crônicas do WannaCry. Kapersky. Disponível em: https://www.kaspersky.com.br/blog/wannacry-history-lessons/19960/.

Schettini, B. (2022). O crime de invasão de dispositivos informáticos (notebooks, netbooks, tablets, smartphones, etc.). JusBrasil. Disponível em: https://www.jusbrasil.com.br/artigos/o-crime-de-invasao-de-dispositivos-informaticos-notebooks-netbooks-tablets-smartphones-etc/1630463264

Schreiber, A. (2022) O Direito em Tempos de Ciberguerra, RJ. O Globo. Disponível em: https://blogs.oglobo.globo.com/fumus-boni-iuris/post/anderson-schreiber-o-direito-em-tempos-de-ciberguerra.html

Sonicwall. 2023 Cyber Threat Report, CA (USA): Editora SONICWALL. Disponível em: https://www.sonicwall.com/medialibrary/en/white-paper/ 2023-cyber-threat-report.pdf.

Souza (2018) Criminologia - origem e evolução. JusBrasil. Disponível em: https://www.jusbrasil.com.br/artigos/criminologia-origem-e-evolucao/600948002#:~:text=Com%20inicio%20no%20s%C3%A9culo%20XVIII,etiologia%2C%20para%20explicar%20o%20crime.

Srinivas, R (2021). How Cybercriminals Use Phishing Kits, USA. CISO MAG. Disponível em: https://cisomag.com/how-cybercriminals-use-phishing-kits/.

UPX (2021). Ransomware: entenda o caso que abalou a Renner e conheça os diferentes tipos de ciberataques. Disponível em: https://upx.com/ post/Ransomware-renner/.

Ximenes, L (2022). O que é malware? Conheça os tipos mais comuns. Disponível em: https://www.hardware.com.br/artigos/o-que-e-malware-conheca-os-tipos-mais-comuns/#:~:text=Malware%20%C3%A9%20todo%20software%20malicioso,nessa%20categoria%20hoje%20em%20dia.