ATAQUE CIBERNÉTICO RANSOMWARE: O QUE É E COMO PREVINIR

RANSOMWARE CYBERATTACK: WHAT IT IS AND HOW TO PREVENT IT

Victor L. L. Silva[1], Rogério L. S. Oliveira[2]

[1]Faculdade de Tecnologia Prof. José Camargo – Fatec Jales, victor.silva208@fatec.sp.gov.br
[2]Faculdade de Tecnologia Prof. José Camargo – Fatec Jales, rogerio.leao@fatec.sp.gov.br

Informação e Comunicação
Subárea: Arquitetura de Computadores, Redes e Segurança

RESUMO

O ransomware é um código malicioso criado com o intuito de sequestrar dados do usuário e extorquir dinheiro dele. Os praticantes de ataques virtuais desse tipo, geralmente solicitam dinheiro em forma de criptomoeda, para não serem rastreados. Esses ataques vêm crescendo cada vez mais em todos os países, inclusive no Brasil estão cada vez mais presentes. No trabalho apresentado, foi realizada uma revisão de literatura, onde os resultados obtidos, incluem, como ocorrem os ataques, com qual frequência, e propostas táticas de prevenção, demonstrando quais as principais vítimas. Concluiu-se por meio deste estudo que este tipo de ataque é muito perigoso, e que geralmente acontece com usuários leigos e despreparados. Mas, ainda serão necessários mais estudos que abranjam de fato, se existe uma maneira preventiva eficaz para que esses ataques não ocorram com a frequência observada nesta revisão.

Palavras-chave: ransomware; ataques; incidentes; segurança; prevenção.

ABSTRACT

Ransomware is malicious code created to hijack user data and extort money from them. Practitioners of cyberattacks of this type, usually request money in the form of cryptocurrency, not to be tracked. These attacks have been increasing more and more in all countries, including in Brazil they are increasingly present. In this presented paper, a literature review was carried out, where the obtained results include, how the attacks occur, how often, and tactical proposals for prevention, demonstrating which are the main victims. It was concluded through this study that this type of attack is very dangerous, and that it usually happens to lay and unprepared users. But, more studies will still be needed that actually cover whether there is an effective preventive way for these attacks not to occur as often as observed in this review.

Keywords: ransomware; attacks; incidents; safety; prevention.

1 INTRODUÇÃO

A Tecnologia da Informação é a área que mais vem crescendo nos últimos anos. Esse advento muito se dá por meio do avanço tecnológico, como o desenvolvimento de sistemas modernos e seguros para o uso de informações pessoais e de negócios. Porém, junto a este tempo, também existe o crescimento exponencial de sistemas não tão seguros, pois, hoje também há o avanço de codificações, gerando oportunidades de grandes experts no assunto conseguirem acessar os sistemas alheios aos seus.

Os ataques cibernéticos elaborados por especialistas em adentrar em sistemas privados(hackers), tem sido cada vez mais comum e evidenciado, tanto no âmbito pessoal como empresarial, causando grande impacto global, e gerando grandes prejuízos, desde perdas financeiras até o sumiço de dados (CHECK POINT, 2023).

Existem várias modalidades de ataques, como o sequestro de dados e vendas de cadastros por meio de links encaminhados aos usuários leigos, que sem notarem, estão entrando numa rede de compartilhamento de informações pessoais.

Os ataques mais evidentes tem sido os de sequestro de dados, onde hackers acessam sistemas, para buscar e sequestrar informações confidenciais e primordiais para a vítima, e depois, solicitarem resgate, para que sejam devolvidos todos esses dados (MACKEY, 2020).

As informações roubadas geram muitos transtornos, porque elas são alvo de um estudo com muita expertise. O hacker responsável pelo sequestro, sabe da necessidade de recuperação rápida dos dados de uma empresa ou pessoa. E para não correr o risco de vazamento da informação roubada, a vítima entra em desespero. O modus operandi dos sequestradores, não se diferem muito, pois, todos fazem uma pressão, baseada em um tempo para o pagamento com ameaça, de logo vazar a informação (MCAFEE, 2022).

Sem opção ou conhecimento, a vítima muitas vezes chega pagar o resgate, e mesmo assim, nada garante a honestidade ou palavra do sequestrador. Além de seus dados confidenciais serem sequestrados e de pagar o resgate, muitas vezes, acontece o pior, e os dados são divulgados de forma a prejudicar a vítima (OLENICK, 2022).

Os tipos de ataques cibernéticos existentes mais comuns no cenário atual são justamente os de sequestro de dados, e o mais utilizado vem sendo o Ransomware (OSBORNE, 2021).

Ransomware é um ataque criado na década de 1980 e seu nome vem baseado na língua inglesa, ransons (resgate).

Este ataque, impede que o usuário autorizado a usar um sistema, consiga ter acesso aos dados deste. E assim o sequestrador solicite um resgate para a recuperação do que foi perdido. Fazem uso de cobrança por meio de cartão de crédito ou cripto moedas (um sistema financeiro de investimento, ainda sem leis de proteção ao investido), o que facilita o recebimento do valor pelos hackers, e oferece uma certa uma segurança, para que esses não sejam localizados e indiciados pelo crime cometido(BAZAN, 2021).

No decorrer do projeto propõe-se, por meio de revisão de literatura, demostrar os meios propostos, por diversos autores, de se mitigar ou evitar os riscos destes ataques. Tendo em vista que na atualidade a inteligência artificial evoluiu bastante, estamos em uma corrida contra o tempo, para cuidar de nossos dados. Pois, até quando, esses ataques serão feitos por humanos?

2 REFERENCIAL TEÓRICO

O ransomware é um tipo de código malicioso (malware) que bloqueia o acesso aos arquivos ou sistemas de computador, exigindo um resgate em troca da liberação (PINTO, 2018).

Com o avanço tecnológico, esses tipos de ataques se tornaram cada vez mais frequentes e sofisticados, afetando organizações em todo o mundo (SILVA, 2020).

A respeito da classificação dos ransomwares, existem duas categorias principais: os criptografadores e os bloqueadores. Os criptografadores utilizam técnicas de criptografia para bloquear o acesso aos arquivos, enquanto os bloqueadores bloqueiam completamente o acesso ao sistema. Em ambos os casos, é exigido um resgate para a liberação do acesso.

O objetivo do ataque é extorquir dinheiro do proprietário do sistema afetado (MAIER, 2022). Eles são projetados para se espalhar rapidamente, afetando o maior número possível de sistemas e arquivos.

Os ataques de ransomware são geralmente distribuídos através de e-mails de phishing, links maliciosos, anexos de e-mail, downloads de software maliciosos, entre outros. Os sistemas operacionais mais comuns, como o Windows, são os mais vulneráveis a esses ataques (MALWAREBYTES LABS, 2020).

Abaixo estão os principais conceitos teóricos relativos ao estudo e uma breve revisão bibliográfica sobre três eventos significativos desses ataques cibernéticos.

Alguns exemplos de ataques:

1. Ataque ao oleoduto da Colonial Pipeline em 2021: Em maio de 2021, a Colonial Pipeline, que fornece cerca de 45% do combustível da Costa Leste dos EUA, foi alvo de um ataque de ransomware. O grupo responsável pelo ataque, DarkSide, exigiu um resgate de cerca de US$ 5 milhões. O ataque causou a interrupção do fornecimento de combustível em grande parte da Costa Leste dos EUA (NEOTEO SEGURANÇA DIGITAL, 2021).
2. Ataque ao provedor de software Kaseya em 2021: Em julho de 2021, a Kaseya, um provedor de software de gerenciamento de TI, foi alvo de um ataque de ransomware que afetou seus clientes em todo o mundo. O grupo responsável pelo ataque, REvil, exigiu um resgate de cerca de US$ 70 milhões. O ataque afetou cerca de 1.500 empresas, incluindo hospitais, escolas e empresas de tecnologia (BRAUN, 2021).
3. Ataque à JBS em 2021: Em junho de 2021, a JBS, o maior processador de carne do mundo, foi alvo de um ataque de ransomware que afetou suas operações nos EUA e na Austrália. O grupo responsável pelo ataque, REvil, exigiu um resgate de cerca de US$ 11 milhões. O ataque afetou o fornecimento de carne em todo o mundo (ARBULO, 2021).
4. Ataque a University Clinic Dusseldorf em 2020: em Setembro de 2020 a University Clinic Dusseldorf Clínica médica da Alemanha, sofreu um ataque de ransoware por engano, os criminosos queriam atacar a Universidade Heinrich Heine que é uma universidade alemã padrão, e a clínica por ser filial da universidade acabou recebendo o ataque, os criminosos ao perceberem que atacaram o alvo errado providenciaram uma chave gratuita de resgate dos dados para a clínica (BANERJEE, 2020).

3 METODOLOGIA

Foi realizado um estudo retrospectivo de ataques com ransomware ocorridos nos últimos anos e utilizados dados de fontes públicas disponíveis online, tais como, como notícias, relatórios de empresas de segurança cibernética e pesquisas acadêmicas.

A técnica utilizada foi de revisão sistemática da literatura, com busca por palavras-chave relacionadas a ransomware, como “ransomware”; “attacks”; “incidentes”; “safety”; “prevention”.

Essa pesquisa foi conduzida utilizando-se um computador com acesso à internet, através de ferramentas de buscas e análise de dados.

É importante destacar que, devido à natureza dos dados coletados, pode haver limitações na precisão e abrangência dos resultados obtidos. Além disso, a pesquisa não tem a intenção de ser uma análise completa e exaustiva de todos os ataques deste tipo, ocorridos no período considerado, mas sim fornecer uma visão geral do cenário e das tendências observadas.

4 ANÁLISE E DISCUSSÃO DOS RESULTADOS

Os resultados foram analisados em termos de número de ataques, setores mais afetados, países mais atingidos, tipos de ransomware mais utilizados, entre outras variáveis consideradas relevantes. Foram apresentadas estatísticas e tendências relevantes para a compreensão do cenário atual desses ataques, bem como recomendações para prevenção e mitigação desses ataques (SENTINELONE, 2022).

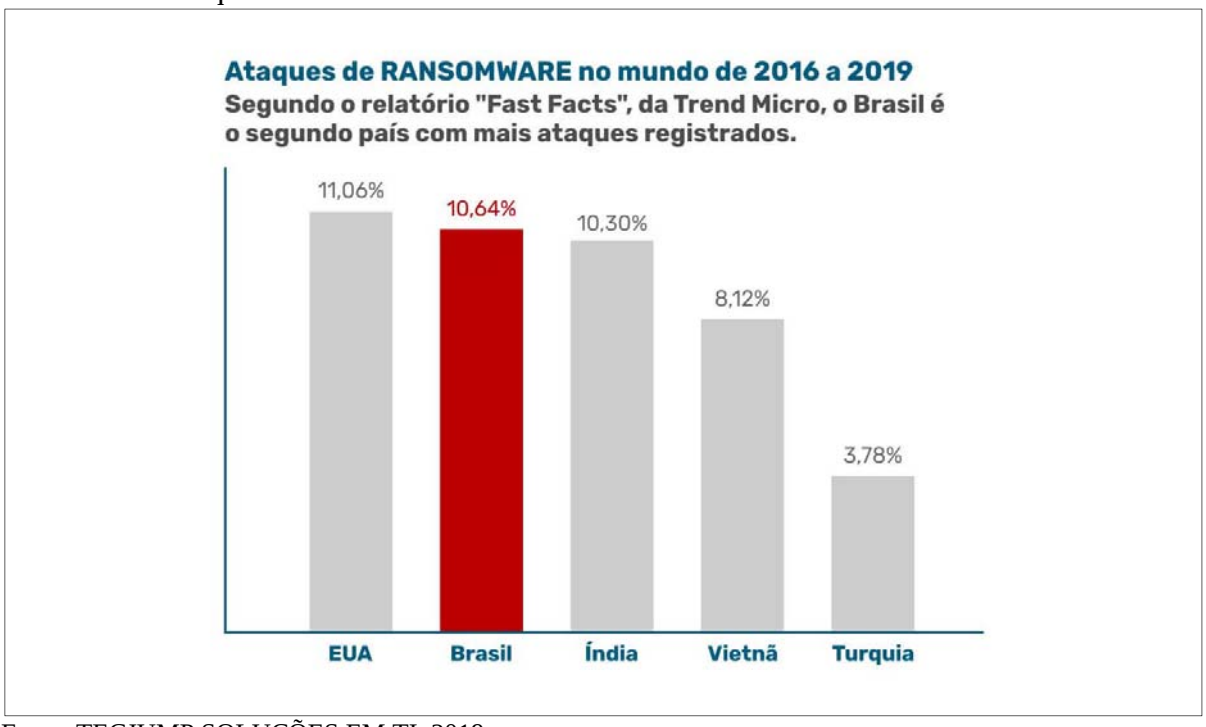
De acordo com as empresas pesquisadas, (SECURITY REPORT, 2023) “Durante o primeiro trimestre de 2023, a média global de ataques semanais aumentou 7% em comparação

com o período correspondente em 2022, com cada organização enfrentando uma média de 1.248 ataques por semana".

Os ataques aumentaram significativamente nos últimos anos, afetando principalmente os setores de saúde, educação e governo. É importante estar ciente das tendências e estatísticas relevantes e implementar medidas preventivas para proteger os dados críticos (GAMBOA, 2020).

Os países mais atingidos por este tipo de ataque, entre 2016 e 2019 foram os Estados Unidos, Brasil, Índia e Vietnã e Turquia (Gráfico 1). O Brasil, em particular, tem sido alvo de ataques com ransomware cada vez mais frequentes nos últimos anos (ASSOLINI, 2021).

Gráfico 1 – Ataques de Ransomware no mundo



Fonte: TECJUMP SOLUÇÕES EM TI, 2019.

Os tipos de ransomware mais utilizados nos últimos anos foram o Ryuk, Sodinokibi e Conti. Esses tipos são conhecidos por serem particularmente muito sofisticados e difíceis de remover.

Além disso, os ataques entre os anos de 2021 e 2023, apresentaram algumas tendências e estatísticas relevantes, tais como, o aumento de ataques de ransomware (onde os cibercriminosos ameaçam divulgar os dados roubados se o resgate não for pago), o aumento do valor médio dos resgates pagos e a utilização cada vez mais frequente de táticas de engenharia social para disseminar esse tipo de ocorrência (COVEWARE, 2021).

Dentro dos artigos selecionados, observou-se que as maiores recomendações para prevenção e mitigação de ataques com ransomware, foram, os backups regulares, instalação de software de segurança como antivírus (mantendo esse sempre atualizado), medidas de autenticação mais forte usando senhas maiores e com caracteres especiais, e a constante educação dos usuários, no sentido de instrui-los a não acessar conteúdos considerados maliciosos ou suspeitos (Gráfico 2).

É importante ressaltar que a prevenção de ataques é um esforço contínuo e requer uma abordagem em camadas, combinando medidas técnicas e educacionais. Além disso, é recomendado ter um plano de resposta a incidentes em caso de ataque, para minimizar os danos e facilitar a recuperação dos dados. A conscientização sobre os riscos e a adoção de boas

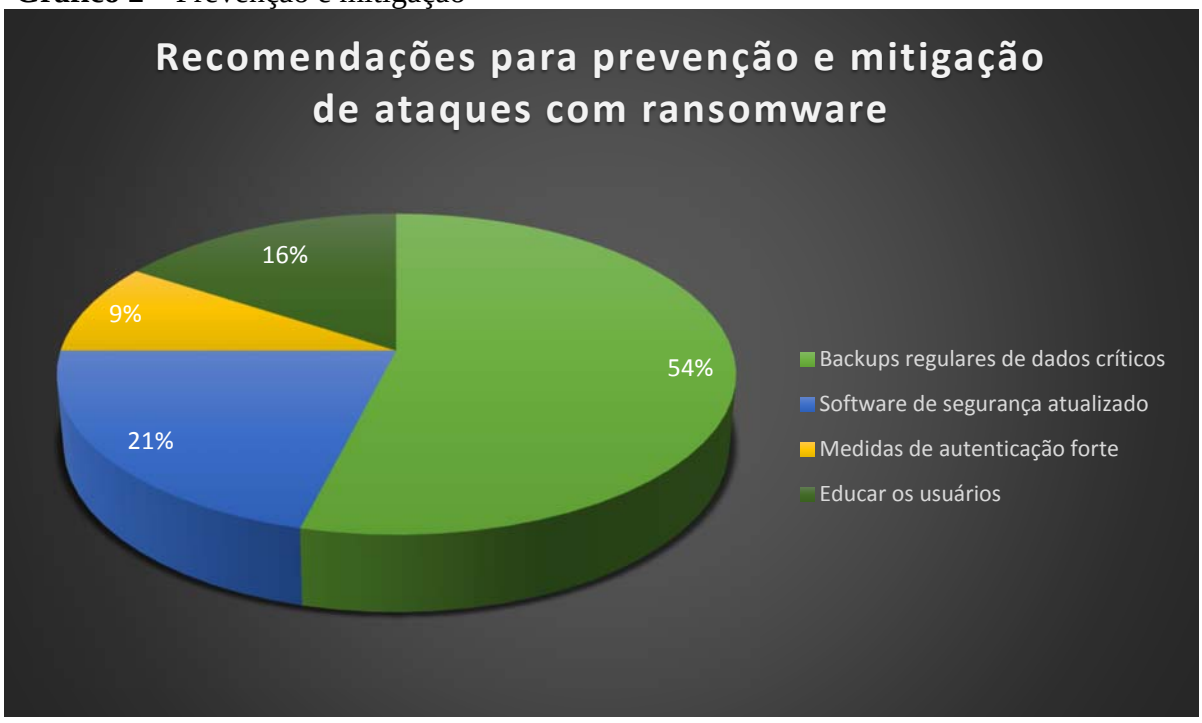
práticas de segurança cibernética são fundamentais para mitigar a ameaça do ransomware (Quadro 1).

Quadro 1 – Ataques, Medidas e Abordagens

Tópico	Descrição
Ataques de ransomware	Causam prejuízos financeiros e impactos negativos em vários setores. Exemplos de ataques famosos: Colonial Pipeline, Kaseya e JBS.
Medidas preventivas	Fazer backups regulares. Instalar software de segurança. Fortalecer autenticação. Educar usuários. Manter sistemas atualizados.
Abordagem em camadas	Combina medidas técnicas e educacionais. Ter plano de resposta a incidentes. Conscientização e boas práticas de segurança cibernética.

Fonte: Elaborado pelos autores.

Gráfico 2 – Prevenção e mitigação



Fonte: Elaborado pelos autores.

5 CONSIDERAÇÕES FINAIS

Após o estudo apresentado, concluiu-se que o ransomware, é um software malicioso muito perigoso, que tem por principal função incapacitar e roubar os dados da vítima. É aplicado para os usuários leigos ou com pouca informação sobre o assunto, e quando são lesadas pelo ataque, sem saber como proceder, acabam pagando o valor ao criminoso. É um ataque que vem tomando força nos últimos anos e o melhor meio de se prevenir deste tipo de ataque, até então, é reconhecendo a necessidade de conscientização (BARRETT, 2020).

Para que se esteja ciente dos diferentes tipos de golpes e ataques que existem, é necessário se manter com senhas seguras, fortes e únicas, para todas as suas contas online, evitando a descoberta delas.

Sugere-se também, atualizações de segurança, onde geralmente se incluem correções de segurança importantes que podem proteger contra vulnerabilidades conhecidas, observando e-mails suspeitos, tendo o cuidado ao abri-los, principalmente de remetentes desconhecidos ou suspeitos. É importante também evitar o acesso a links ou baixar anexos de fontes não confiáveis no conteúdo dos e-mails, ficando atento a erros de ortografia e gramática, pois esses são sinais comuns de e-mails de *phishing*, que são mensagens criadas intencionalmente para enganar usuários desatentos.

Recomenda-se não visitar sites suspeitos ou clicar em links não verificados, usando uma solução de segurança confiável, tais como antivírus, que possa ajudar a bloquear sites maliciosos e fornecer avisos de segurança.

A mais enfática recomendação que se pode fazer está relacionada aos dados armazenados nos dispositivos dos usuários, HDs, Pendrives e outros. Deve-se realizar o *backup* regularmente desses dados e armazenar essas copias em um local seguro, geralmente em servidores de nuvem ou mesmo em discos magnéticos externos.

Por fim, aprender continuamente sobre práticas de segurança cibernética, mantendo-se atualizado sobre as últimas tendências e ameaças de segurança é também extremamente relevante para poder se proteger de forma eficaz.

REFERÊNCIAS

ARBULO, R. **Ataque à JBS foi executado pelo grupo hacker REvil**. 2021. Disponível em: https://www.bbc.com/portuguese/internacional-57344706. Acesso em: 5 abr. 2023.

ASSOLINI, F. **Cybercrime**: ransomware attacks quadruple in Brazil. 2021. Disponível em: https://www.kaspersky.com/blog/ransomware-in-brazil/38334/. Acesso em: 5 abr. 2023.

BANERJEE, K. **Patient dies as ransomware attack cripples University Hospital in Germany**. 2020. Disponível em: https://www.ibtimes.sg/patient-dies-ransomware-attack-cripples-university-hospital-germany-dusseldorf-51651. Acesso em: 17 abr. 2023.

BARRETT, P. M. **Ransomware**: the big business of digital extortion. 2020. Disponível em: https://www.bloomberg.com/features/2020-ransomware-gangs/. Acesso em: 5 abr. 2023.

BAZAN, R. **Ransomware is now the biggest cybersecurity threat in Brazil**. 2021. Disponível em: https://cointelegraph.com.br/news/ransomware-is-now-the-biggest-cybersecurity-threat-in-brazil. Acesso em: 5 abr. 2023.

BRAUN, D. **Cibercriminosos atacam clientes de software da americana Kaseya**. 2021. Disponível em: https://valor.globo.com/empresas/noticia/2021/07/02/cibercriminosos-atacam-clientes-de-software-da-americana-kaseya.ghtml. Acesso em: 5 abr. 2023.

COVEWARE. **The State of Ransomware 2021**: a review of ransomware attack trends and predictions for 2022. 2021. Disponível em: https://www.coveware.com/2021/12/22/the-state-of-ransomware-2021-a-review-of-ransomware-attack-trends-and-predictions-for-2022/. Acesso em: 5 abr. 2023.

CROWDSTRIKE. **2022 CrowdStrike Global Threat Report**. 2022. Disponível em: https://www.crowdstrike.com/resources/reports/2022-crowdstrike-global-threat-report/. Acesso em: 5 abr. 2023.

GAMBOA, L. **The State of Ransomware in Brazil**. 2020**.** Disponível em: https://thehack.com.br/the-state-of-ransomware-in-brazil/. Acesso em: 5 abr. 2023.

MACKEY, T. **Ransomware**: a review of 2020 and what to expect in 2021. 2020. Disponível em: https://securityboulevard.com/2020/12/ransomware-a-review-of-2020-and-what-to-expect-in-2021/. Acesso em: 5 abr. 2023.

MAIER, T. A study of ransomware attacks and payment demands. **IEEE Security e Privacy**, v. 20, n. 1, p. 14-22, jan./fev. 2022. Disponível em: https://doi.org/10.1109/MSEC.2022.3167559. Acesso em: 5 abr. 2023.

MALWAREBYTES LABS. **Ransomware trends in 2020**. 2020. Disponível em: https://resources.malwarebytes.com/files/2020/12/2020-State-of-Ransomware-Report.pdf. Acesso em: 5 abr. 2023.

MCAFEE. **McAfee labs threats report**. 2022. Disponível em: https://www.mcafee.com/enterprise/en-us/assets/reports/rp-labs-threats-report-apr-2022.pdf. Acesso em: 5 abr. 2023.

NEOTEO SEGURANÇA DIGITAL. **Proteção crítica da infraestrutura**: lições aprendidas com o ataque do gasoduto Colonial. 2021. Disponível em: http://blog.neotel.com.br/2021/06/07/protecao-critica-da-infraestrutura-licoes-aprendidas-com-o-ataque-do-gasoduto-colonial/. Acesso em: 5 abr. 2023.

OLENICK, D. **Ransomware**: the cost of redemption. 2022. Disponível em: https://www.scmagazine.com/home/security-news/ransomware/ransomware-the-cost-of-redemption/. Acesso em: 5 abr. 2023.

OSBORNE, C. **Ransomware attacks double in 2020**: These two industries were hardest hit. 2021. Disponível em: https://www.zdnet.com/article/ransomware-attacks-double-in-2020-these-two-industries-were-hardest-hit/. Acesso em: 5 abr. 2023.

PINTO, A. **Ransomware: uma ameaça cibernética em ascensão.** *In*: CONGRESSO BRASILEIRO DE SEGURANÇA DA INFORMAÇÃO E SISTEMAS COMPUTACIONAIS, 1., 2018, Santa Maria. **Anais Congresso Brasileiro de Segurança da Informação e Sistemas Computacionais**. Santa Maria: UFSM, 2018.

SENTINELONE. **State of ransomware**. 2022. Disponívem em: https://go.sentinelone.com/hubfs/2022_State_of_Ransomware_Report.pdf. Acesso em: 5 abr. 2023.

SECURITY REPORT. **Média global de ciberataques semanais aumentou 7% no trimestre**. Disponível em: https://www.securityreport.com.br/overview/brasil-teve-aumento-de-1-em-ataques-ciberneticos-no-primeiro-trimestre-de-2023/#.ZF1YynbMK3A. Acesso em: 25 abr .2023.

SILVA, J. C. Ransomware: a evolução das ameaças cibernéticas. **Revista de Tecnologia da Informação**, v. 6, n. 2, p. 25-38, 2020.

TECJUMP SOLUÇÕES EM TI. **Você já triplicou sua segurança na internet?** 2019. Disponível em: https://blog.tecjump.com.br/voce-ja-triplicou-sua-seguranca-na-internet/. Acesso em: 17 abr. 2023.

AGRADECIMENTOS

Prezados,

Gostaria de expressar minha gratidão a todos que contribuíram para a realização deste trabalho. Primeiramente, agradeço a Deus por me conceder saúde e perseverança para concluir este projeto.

Agradeço ao meu orientador/professor(a) Ms. Rogério Leão Santos de Oliveira, pela paciência, dedicação, conhecimento transmitido e orientações essenciais para o desenvolvimento deste trabalho.

Agradeço aos professores Ms. Alexandre Aparecido Bernardes, Ms. Cristiano Pires Martins, Ms. Fabiana Pupin Masson Caravieri, Ms. Jorge Luis Gregório, Dr. Evanivaldo Castro Silva Júnior, Dr. Edy Carlos Santos de Lima, Ms. Carlos Alberto Gonçalves da Silva, Dra. Elen Dias, Silvio Cesar Lopes, Ms. Welington Luis Codinhoto Garcia, Ms. Rivelino Rodrigues, Tassia da Silva de Carvalho, Ms. Guilherme de Morais, Dra. Andrea Piranhe da Silva, Dra. Ligia Rodrigues Prete, Marcelo Tadeu Boer e Ms. Jefferson Antonio Ribeiro Passerini, pelos ensinamentos adquiridos durante o curso e que foram de fundamental importância para a elaboração deste trabalho.

Aos meus colegas de curso, em especial a Maria do Carmo Camargo, Antenor Barbosa da Silva, Christiane Luci Soares Nagasso, Thiago Alves da Cruz, Mike Andre Camilo de Souza, Daniel Barbosa Aielo e Vinicius Sizilio Boranga, pela ajuda e troca de conhecimento durante o processo de desenvolvimento deste trabalho.

Aos meus amigos e familiares, em especial a minha mãe Lucimara Lopes, por me apoiar em todos os momentos e incentivar a minha formação acadêmica.

Por fim, agradeço a todos que contribuíram direta ou indiretamente para a realização deste trabalho.

Muito obrigado!

Victor Luiz Lopes da Silva