Utilização de Inteligência de Ameaças Cibernéticas Para Prevenção e Mitigação de Ataques Ransomware: Uma Revisão Sistemática da Literatura

Rennan Luis B. Cabral, Fernando A. A. Lins

Departamento de Computação (DC)
Universidade Federal Rural de Pernambuco(UFRPE) – Recife, PE – Brazil
{rennan.bcabral,fernandoaires}@ufrpe.br

Resumo — O Ransomware se estabeleceu como uma das ameaças cibernéticas mais impactantes dentro de organizações, e tem crescido de forma acentuada nos últimos anos, afetando empresas de diversos domínios e tamanhos. Esse tipo de ataque usa criptografia para sequestrar dados e sistemas, e depois os criminosos exigem resgate para a liberação dos mesmos. A ocorrência deste tipo de ataque resulta em perdas financeiras significativas e danos à reputação da organização. Neste contexto, a inteligência de ameaças cibernéticas (CTI) surge como uma alternativa interessante na defesa contra o ransomware, fornecendo informações detalhadas sobre as táticas, as técnicas e os procedimentos (TTPs) usados pelos atacantes. CTI permite a antecipação, a identificação e a mitigação de ataques por meio da coleta e da análise de dados de ataques prévios, vulnerabilidades conhecidas e comportamentos de malwares. Ao empregar CTI, as organizações podem melhorar a detecção precoce de ameaças, otimizar a resposta a incidentes e implementar medidas preventivas para reduzir a probabilidade de infecção. Contudo, existe uma lacuna de levantamentos bibliográficos ou sistematizados referentes especificamente ao uso de CTI para prevenção e mitigação de ataques Ransomware. Neste contexto, este artigo tem como objetivo apresentar uma revisão sistemática da literatura sobre o uso de CTI para ataques do tipo Ransomware, analisando as abordagens, as ferramentas e as estratégias para prevenir e atenuar ataques desse tipo, com base em dados recentes e nas práticas recomendadas por especialistas em segurança cibernética.

Palavras-chave - Ransomware, Cyber Threat Intelligence, Segurança da Informação, Segurança Cibernética, Resposta a Incidentes.

1. Introdução

Nos últimos anos, o ataque de *Ransomware* emergiu como uma das ameaças cibernéticas mais temidas por organizações, impactando os mais variados tipos de

negócio. Com ataques cada vez mais sofisticados, os cibercriminosos exploram vulnerabilidades pararealizar sequestro de dados, e depois demandam pagamentos elevados para restaurar o acesso. Esse cenário destaca a necessidade de estratégias proativas de defesa, nas quais a Inteligência de Ameaças Cibernéticas (Cyber Threat Intelligence - CTI) desempenha um papel crucial.

O CTI vai além das abordagens reativas, capacitando organizações a antecipar ameaças e mitigar riscos com base em informações previamente coletadas e avaliadas. Ao reunir, analisar e contextualizar dados sobre adversários, ferramentas e táticas utilizadas em ataques de *Ransomware*, CTI permite que empresas adaptem suas defesas, reduzam a superfície de ataque e aprimorem a capacidade de resposta.

Contudo, uma lacuna existente atualmente no estado da arte da área é a falta de revisões bibliográficas ou sistematizadas relacionadas ao uso de CTI na prevenção e mitigação de ataques do tipo *Ransomware*. Esta falta faz com que não exista uma literatura específica, técnica e científica sobre este domínio, o que pode dificultar organizações e usuários a usarem técnicas e ferramentas de CTI na prevenção do citado ataque.

Neste contexto, o objetivo principal deste artigo é realizar uma revisão bibliográfica sobre como a inteligência de ameaças cibernéticas (CTI) vem sendo usada para a prevenção, tratamento e mitigação de ataques do tipo *Ransomware*. Nesta revisão, será dada ênfase especial aos benefícios de se entender o panorama de ameaças, a importância da colaboração e as melhores práticas para implementar um programa eficaz de CTI.

Este artigo está dividido da forma que se segue. A Seção II apresenta os conceitos básicos que são necessários para o entendimento das contribuições desta pesquisa. A Seção III, por sua vez, detalha a metodologia aplicada para a realização da revisão. Na Seção IV os trabalhos selecionados são detalhados e discutidos. Por fim, a Seção V apresenta as conclusões e os trabalhos futuros.

2. Conceitos Básicos

Esta seção apresenta conceitos básicos relacionados às principais temáticas abordadas nesta pesquisa: Inteligência de Ameaças Cibernéticas (*Cyber Threat Intelligence* - CTI) e *Ransomware*.

A. Cyber Threat Intelligence

Cyber Threat Intelligence (CTI), ou Inteligência de Ameaças Cibernéticas, é o processo de coleta, análise e compartilhamento de informações relevantes sobre ameaças e ataques cibernéticos. O objetivo da CTI é capacitar organizações a compreender melhor o panorama de ameaças, antecipar possíveis ataques e tomar decisões informadas para proteger seus ativos.

O CTI engloba dados técnicos, como indicadores de comprometimento (IoCs), além de informações contextuais sobre os métodos, motivos e perfis dos adversários. Essas informações são classificadas em três níveis, que são detalhados a seguir.

Estratégico. A inteligência estratégica de ameaças (STI) é baseada em análises aprofundadas de tendências de segurança cibernética e seus possíveis impactos em uma organização. Ela fornece informações sobre as intenções, capacidades e alvos dos agentes de ameaças, auxiliando executivos e líderes fora da área de TI a compreenderem as potenciais ameaças cibernéticas. Geralmente, como não tem elevado detalhamento técnico, a STI é utilizada na formulação de estratégias e programas de gestão de riscos, com o objetivo de reduzir os efeitos de possíveis ataques no futuro.

Tático. A Inteligência Tática de Ameaças (TTI) concentra-se nas táticas, técnicas e procedimentos (TTPs) empregados pelos agentes de ameaças, buscando compreender como esses indivíduos podem atacar uma organização. Ela também investiga vulnerabilidades, utilizando a caça de ameaças, que visa identificar proativamente ameaças ainda não detectadas dentro da rede da organização. A TTI é mais voltada para aspectos técnicos do que a inteligência estratégica de ameaças (STI) e é geralmente utilizada por equipes de TI ou Centro de Operações de Segurança(SOCs) para reforçar as medidas de segurança cibernética ou otimizar os planos de resposta a incidentes.

Operacional. A inteligência operacional de ameaças (OTI) é mais detalhada em termos técnicos do que a STI e a TTI. Trata-se de dados em tempo real que ajudam na detecção de ameaças e na resposta a incidentes. CISOs, CIOs e membros do SOC costumam usar a OTI para identificar e impedir ataques iminentes.

O CTI é fundamental para aprimorar a postura de segurança cibernética, permitindo uma resposta mais ágil e precisa contra ameaças, especialmente em cenários de alta criticidade como os usualmente encontrados em ataques de *Ransomware*.

B. Ransomware

Ransomware é um tipo de malware projetado para bloquear o acesso a sistemas ou dados, geralmente por meio de criptografia, até que um resgate seja pago. Esse tipo de ataque é atualmente um dos mais lucrativos e visados pelos criminosos, e impactam tanto indivíduos quanto organizações.

Os ataques de *Ransomware* geralmente seguem uma sequência, onde a primeira etapa é a de infecção, onde o malware é introduzido no sistema por meio de phishing, exploração de vulnerabilidades ou outros vetores. Logo em seguida temos a etapa de criptografia, onde os arquivos e sistemas críticos são criptografados, tornando-os inacessíveis. Logo após segue a etapa de extorsão, onde normalmente há uma mensagem exigindo o pagamento de resgate, frequentemente em criptomoedas, em troca da chave de descriptografia. Por fim, vem às consequências, que podem variar e inclusive existir mesmo que o pagamento seja feito (por exemplo, os atacantes podem vazar dados sensíveis ou manter os sistemas bloqueados mesmo com o pagamento).

Além de perdas financeiras, os ataques de *Ransomware* também causam interrupções operacionais, danos à reputação da organização e potenciais sanções regulatórias. O aumento da sofisticação desses ataques, como o modelo *Ransomware-as-a-Service*(RaaS) [9], torna essencial a adoção de estratégias robustas de defesa, nas quais o CTI desempenha um papel relevante.

3. Metodologia

A principal contribuição deste artigo é a realização de uma revisão sistemática dentro do escopo da temática proposta. O fluxo seguido para auxiliar a realização desta revisão sistemática está apresentado na Figura 1. O processo é composto por diversas etapas que norteiam a execução da revisão, desde a definição da questão de pesquisa até a interpretação dos resultados obtidos. É importante ressaltar que não se buscou seguir protocolos mais elaborados de revisão sistemática fielmente; foi instanciado um protocolo, inspirado em outros mais elaborados, que atendesse aos objetivos desta pesquisa.

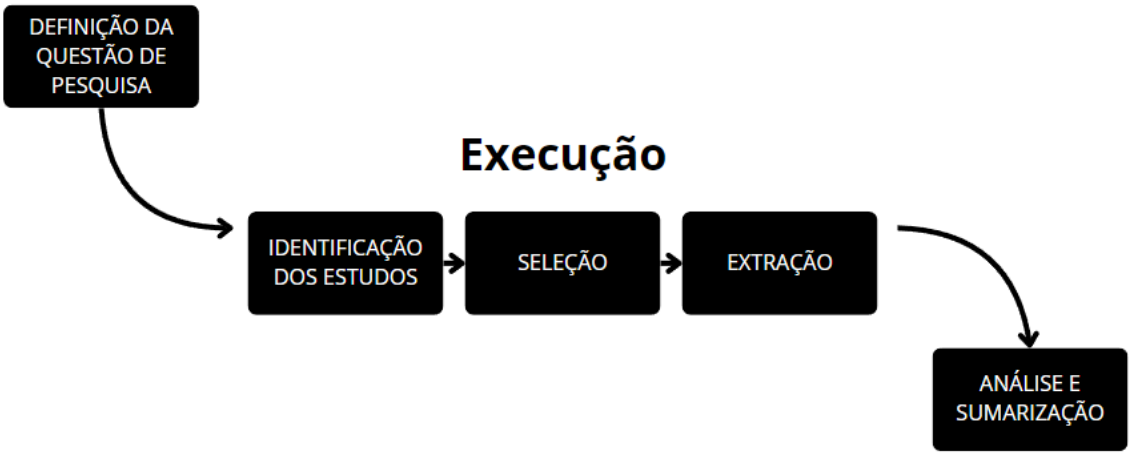

Figura 1. Fluxo da Revisão

O processo tem início na primeira atividade, que consiste na Definição da Questão de Pesquisa, momento em que se determina o objeto de análise e estudo. Em seguida, o fluxo segue para a fase de Execução, que abrange várias atividades: Identificação dos Estudos, onde é realizado o levantamento dos materiais que serão analisados; Seleção, atividade em que ocorre a escolha das referências científicas mais relevantes para o estudo; e a atividade de Extração, dedicada à coleta de informações relevantes dos materiais selecionados. Por fim, o processo é concluído na última atividade, chamada Análise e Sumarização, que envolve a leitura e análise do material seguido da sumarização do documento com os resultados obtidos ao longo das etapas anteriores.

As próximas subseções descrevem a execução deste fluxo tendo em vista os objetivos deste trabalho.

A. Definição da Questão de Pesquisa

De acordo com o escopo proposto para este trabalho, a seguinte pergunta de pesquisa é proposta.

RQ1 - Como a Inteligência de Ameaças Cibernéticas(CTI) tem sido aplicada para a prevenção e mitigação de ataques de *Ransomware*?

B. Identificação dos estudos

A pesquisa foi realizada a partir de termos específicos vinculados ao tema principal do estudo. A coleta de informações ocorreu em plataformas acadêmicas que reúnem artigos, teses, dissertações e publicações científicas. As busca nas bases de dados são realizadas de forma manual, e os resultados obtidos são organizados para serem submetidos às etapas seguintes. Neste estudo, foram importadas referências de bases bibliográficas como ACM, IEEE e Google Acadêmico. A Tabela I exibe as *strings* de busca utilizadas nas buscas de acordo com as bases bibliográficas utilizadas nesta pesquisa.

Tabela I
Bases bibliográficas x Strings de busca

Base bibliográfica	Strings de busca
ACM	”Ransomware”AND ”cyber threat intelligence”AND (cybersecurity OR incident response)
IEEE	”Ransomware”AND ”cyber threat intelligence”AND (cybersecurity OR incident response)
Google acadêmico	”Ransomware”And ”cyber threat intelligence”And (cybersecurity Or incident response)

C. Seleção

Inicialmente, foram eliminados todos os artigos duplicados. Além disso, artigos que não apresentavam informações relevantes no título, resumo ou palavras-chave também foram descartados. A seleção concentrou-se exclusivamente em artigos nos idiomas inglês e português e publicações feitas em até dez anos atrás.

Ainda nesta etapa, foi realizada uma análise consolidada de todos os artigos pertinentes com base nas palavras-chave. Ao revisar os resumos dos artigos, foram destacadas as palavras-chave principais e as referências presentes em cada um deles. Em seguida, foram aplicados filtros e critérios de inclusão e exclusão, demonstrados na Tabela II e III, para selecionar os estudos mais relacionados ao objetivo desta pesquisa. Os trabalhos escolhidos foram analisados para avaliar sua aderência ao escopo, e as informações essenciais, como metodologias e resultados, foram extraídas. Essa fase tem o objetivo de estruturar e processar os dados coletados, buscando possibilitar que a revisão seja consistente e relevante.

Inicialmente, foram reunidos 675 artigos. Após a aplicação dos critérios de exclusão, foram obtidos 35 artigos. Para um melhor direcionamento e qualidade dos materiais estudados, aplicou-se agora os critérios de inclusão, onde através destes foram descartados mais 27 artigos, restando assim 8 artigos que foram selecionados para serem aprofundados neste artigo.

Tabela II
CRITÉRIOS DE INCLUSÃO

CI1	Serão incluídos trabalhos que abordem uso do Cyber Threat Intelligence(CTI) voltadas para *Ransomware*.
CI2	Serão incluídos trabalhos públicos e disponíveis integralmente nas bases científicas buscadas.

Tabela III
CRITÉRIOS DE EXCLUSÃO

CE1	Serão excluídos trabalhos com títulos repetidos.
CE2	Serão excluídos trabalhos duplicados.
CE3	Serão excluídos trabalhos que não apresentam resumo/abstract.
CE4	Serão excluídos trabalhos que não apresentarem a palavra-chave "*Ransomware*" no resumo/abstract
CE5	Serão excluídos trabalhos que não forem encontrados integralmente na base de busca
CE6	Serão excluídos trabalhos publicados a mais de dez anos

D. Extração

Nesta etapa do processo, o objetivo foi extrair as informações essenciais para a análise dos trabalhos, como frameworks, algoritmos, metodologias e estratégias utilizadas para responder a nossa questão de pesquisa.

E. Análise e Sumarização

Por fim, todas as informações relevantes extraídas dos artigos selecionados foram reunidas. A ideia principal desta sumarização é de produzir um material resumido e com informações direcionadas sobre como estes estudos conseguem responder a pergunta de pesquisa proposta neste artigo.

4. Resultados e Discussão

Esta seção apresenta, sumariza e discute as referências bibliográficas encontradas e priorizadas através do protocolo de revisão definido e executado na seção anterior.

Lawall *et al* [1] realizaram um levantamento sobre os ataques de *Ransomware* entre o período de 1º de janeiro de 2023 a 2 de junho de 2023. Neste estudo, foi realizado um perfil para cada grupo de *Ransomware*, buscando suas motivações, capacidades e padrões de ataques. Em seguida foi criado um mapa de calor com base nos TTPs (Táticas, técnicas e procedimentos) dos grupos de *Ransomware* analisados. Após isto, foram analisadas as 10 técnicas e sub técnicas mais comuns nos grupos de *Ransomware* analisados, que foram elas a criptografia dos dados, acesso de contas válidas, inibição de sistemas de recuperação, descobrimento de arquivos e diretórios, *phishing* e entre outras, visando o impacto e a frequência dessas técnicas. Através do Framework MITRE ATT&CK[10], foi feito um mapeamento das mitigações relacionadas às técnicas e sub técnicas mais comuns encontradas no estudo.

Uma das limitações identificadas neste estudo é a ênfase exclusiva na Inteligência de Ameaças Tática (*Tactical CTI*), sem considerar os demais níveis, como Estratégico, Operacional e Técnico. A inclusão desses níveis poderia proporcionar uma visão mais completa e detalhada do panorama de ameaças cibernéticas. Além disso, observa-se que não se utilizaram métricas para avaliar a gravidade e o impacto potencial das Táticas, Técnicas e Procedimentos (TTPs) analisadas. Embora o estudo apresente a frequência e a variação das TTPs identificadas, ele não explora de maneira aprofundada sua relevância e consequências no contexto da segurança cibernética, o que possibilitaria maior profundidade na análise e melhor priorização das ameaças.

Marinho *et al* [2] propuseram uma abordagem para identificar e criar perfis, de forma automática, de ameaças cibernéticas emergentes com base em OSINT [13] (*Open Source Intelligence*), que é uma técnica que consiste em coletar e analisar informações públicas para gerar inteligência, a fim de gerar alertas. Para isso, foi monitorado e coletado continuamente postagens de pessoas e empresas relevantes no Twitter, explorando termos desconhecidos relacionados a ameaças cibernéticas e campanhas maliciosas. Logo em seguida, os autores utilizaram Processamento de Linguagem Natural (PLN) e Aprendizado de Máquina (ML) para identificar os termos com maior probabilidade de serem nomes de ameaças, descartando os menos relevantes. Adicionalmente, os autores empregaram o framework MITRE ATT&CK para identificar

as táticas mais prováveis utilizadas pelas ameaças descobertas, e por fim foram gerados alertas para as ameaças identificadas.

Um possível problema encontrado neste estudo foi a alta taxa de falsos positivos (38,01%) identificada: 38,01%. Os alertas incorretos resultaram na identificação de nomes incomuns que, embora detectados pelo sistema, não estavam necessariamente associados a ameaças reais. Os autores colocaram que este é um desafio a ser explorado em trabalhos futuros.

Tekin *et al* [3] propuseram um método para extrair Inteligência de Ameaças Cibernéticas (CTI) do Twitter. Este método utiliza Processamento de Linguagem Natural (NLP) e Aprendizado Profundo (Deep Learning). A pesquisa foi baseada em 21.000 tweets coletados com a biblioteca Tweepy, utilizando palavras-chave estratégicas para filtrar conteúdos relevantes. Após um aprofundado processo de limpeza e pré-processamento, os dados foram analisados em duas etapas. Uma foi relacionada à classificação dos tweets para determinar se estavam relacionados à inteligência de ameaças cibernéticas (CTI) e a outra foi relacionada a classificação do tipo específico de inteligência de ameaça presente no tweet. Os resultados foram a identificação de tweets relacionados a CTI (88,61% de precisão) e a classificação do tipo de ameaça cibernética (89,09% de precisão). Os resultados demonstram a eficácia da abordagem para identificar ameaças cibernéticas a partir de redes sociais, podendo auxiliar na detecção precoce de ameaças e na tomada de decisões estratégicas em segurança cibernética.

Kante *et al* [5] utilizaram Machine Learning para analisar malware, estruturando o processo em três fases: definição de objetivos, extração de características e aplicação de algoritmos. Duas técnicas principais foram usadas para a classificação de *Ransomware*: a *Decision Tree* (DT), que fornece um modelo interpretável para classificar malware, e a *Random Forest* (RF), que melhora a precisão da detecção. A pesquisa destaca a importância da extração de características, como cálculo de entropia e análise de opcodes, para aprimorar a identificação de malwares. Os resultados demonstram que técnicas modernas, incluindo aprendizado profundo e redes neurais, estão impulsionando a evolução da Inteligência de Ameaças Cibernéticas (CTI) e tornando os processos de detecção e classificação de malwares mais eficientes.

Foi relatado pelos autores que uma dificuldade relevante é a complexidade de identificar ameaças Zero Day(novas ameaças). Para enfrentar esse desafio, será fundamental, no futuro, desenvolver modelos mais flexíveis e adaptáveis, capazes de responder melhor ao surgimento de novas ameaças cibernéticas. Além disso, a integração de redes de informações diversificadas e o uso de conjuntos de dados mais amplos podem ajudar a minimizar algumas das limitações das abordagens tradicionais de Inteligência de Ameaças Cibernéticas (CTI). Um dos principais desafios é garantir a atualização e a relevância dos dados de treinamento, uma vez que as ameaças cibernéticas estão em constante evolução.

Rathod *et al* [6] propuseram o uso combinado do MITRE ATT&CK em conjunto com o Symantec EDR (*Endpoint Detection and Response*) que é uma solução de detecção e resposta a ameaças em endpoints desenvolvida pela Symantec projetada para detectar, investigar e responder a ataques avançados (como, por exemplo, *ransomware*). Nas empresas, as ferramentas de EDR atendem a quatro propósitos principais: detectar

ameaças potenciais, ingestão de log escalável(o processo de recolher, processar e guardar registros de eventos e atividades), investigar ameaças e fornecer orientação para remediação e fornecer orientação para lidar com incidentes de segurança. A proposta dos autores foi utilizar e configurar o Symantec EDR com alertas específicos para as técnicas MITRE para serem detectadas e classificadas através dos registros e análises dos logs. Os autores utilizaram as regras padrão do MITRE para o envio de alertas caso situações específicas fossem detectadas nos logs, que eram coletados em cada host da empresa. Em seguida os logs são transformados em formato JSON para indicar as relações causais entre as entidades do sistema. Foi utilizado o conjunto de dados EMBER, que é um conjunto de dados de benchmark rotulado, para treinar modelos de aprendizado de máquina, com o objetivo de detectar arquivos executáveis portáteis maliciosos. O EMBER consiste em arquivos de linha JSON (onde é incluído os logs). Os autores utilizaram a "*Library to Instrument Executable Formats*" para analisar as informações presentes nos logs. Após esta análise, foi realizada a previsão para identificar arquivos maliciosos, e para isto foi utilizado o modelo de dados "ember-net". De acordo com o estudo, foi apresentada uma precisão de 97% na previsão dos arquivos maliciosos.

Chinmaya *et al* [7] realizaram uma simulação de ataque de *Ransomware*, utilizando o TeamViewer, para realizar a tomada de controle da máquina. Uma vez que o controle é obtido, os autores utilizaram o descompactador de arquivos 7-Zip e o algoritmo de criptografia AES-256 para proteger dados confidenciais. Toda a metodologia da simulação é realizada para mostrar possíveis áreas de aplicações da mesma, como: testes de penetração (*pentests*) para avaliação de vulnerabilidade em organizações e treinamento de conscientização sobre segurança. O estudo descreve também a utilidade do HostedScan, que é uma plataforma de gestão de vulnerabilidades, que permite escanear redes, servidores e sites para identificar riscos de segurança.

Yeboah-Ofori *et al* [8] adotaram a abordagem CTI para reunir e analisar dados de ameaças, além de técnicas de ML para prever possíveis ataques. As técnicas de ML são aplicadas em algoritmos de classificação para treinar modelos com conjuntos de dados, melhorando a precisão das análises preditivas. A justificativa para a integração entre CTI e ML na previsão de ameaças é que o ciclo de vida do CTI fornece parâmetros de entrada para detectar ataques conhecidos, enquanto o ML gera parâmetros de saída para prever tanto ataques conhecidos quanto desconhecidos, auxiliando na identificação de tendências futuras.

O objetivo é detectar vulnerabilidades e indicadores de comprometimento em nós da *Cyber Supply Chain* (CSC) utilizando ataques conhecidos para prever ataques desconhecidos. Para isso, foi aplicado técnicas de CTI na coleta de ameaças (ataques conhecidos) e técnicas de ML para analisar os dados e prever novas ameaças cibernéticas (ataques desconhecidos) em sistemas CSC. Os resultados experimentais mostraram as precisões dos algoritmos Logistic Regression (LG), Decision Tree (DT), Support Vector Machine (SVM) e Random Forest (RF) na Majority Voting e identificaram uma lista de ameaças.

Song *et al* [11] selecionaram 12 incidentes de *Ransomware* conhecidos que ocorreram no período de 2021 e 2022. Para fins de análise, foram transformadas as informações de TTPs (Táticas, Técnicas e Procedimentos) de cada ataque em descrições de técnicas de ataque na estrutura matriz ATT&CK. Após isto, foi feita uma comparação de similaridade entre os TTPs mais encontrados nos ataques estudados. Após esta etapa, foi utilizado e consultado o gráfico de conhecimento D3FEND[12], que é uma ferramenta da MITRE Corporation que ilustra as técnicas de defesa cibernética e as suas relações com as técnicas de ataque. O D3FEND é um complemento do framework ATT&CK, que tem foco específico nas técnicas de ataque, para ajudar na proteção destes TTPs encontrados.

Os autores relataram algumas dificuldades e limitações no desenvolvimento do experimento, como a escassez de fonte de dados de inteligência de ameaças, assim como a confiabilidade delas. Por fim, há limitações associadas aos métodos atuais de extração de informações de TTPs. *"Embora certas abordagens contemporâneas defendam o uso de técnicas de aprendizado profundo para extrair informações de TTPs da inteligência de ameaças, muitos desses métodos sofrem de precisão abaixo do ideal", Song et al* [11].

5. Conclusões e Trabalhos Futuros

A revisão bibliográfica realizada nesta pesquisa demonstra que a aplicação da Inteligência de Ameaças Cibernéticas (CTI) no contexto de Ransomware tem evoluído significativamente, com abordagens inovadoras baseadas em Processamento de Linguagem Natural (PLN), Aprendizado de Máquina (ML) e Aprendizado Profundo (DL) sendo utilizadas. Os estudos analisados destacam a importância da integração entre dados de ameaças, modelagem preditiva e frameworks como o MITRE ATT&CK e D3FEND, permitindo não apenas a detecção de ataques conhecidos, mas também a previsão de novas ameaças emergentes, inclusive ameaças *zero day*.

A contribuição positiva do uso de técnicas e abordagens como extração de informações de CTI a partir de redes sociais, perfilamento de grupos de *Ransomware*, classificação de malwares com ML e simulações de ataques para análise de vulnerabilidades reforça a necessidade de abordagens inovadoras e adaptáveis. O uso de métodos estatísticos, análise de TTPs e mapeamento de mitigação contribui para a criação de estratégias mais eficazes. No entanto, desafios ainda persistem, como a necessidade de grandes volumes de dados rotulados, que são necessários para o aprendizado de máquina, assim como a veracidade desses dados; a interpretabilidade dos modelos de aprendizado profundo, para garantir que esses modelos sejam confiáveis diante de suas previsões e análises; e a evolução constante das táticas de *Ransomware*, já que todo dia há novos e novos ataques, principalmente depois do crescimento exponencial da Inteligência Artificial(IA).

Como trabalhos futuros, se destaca inicialmente o aprofundamento e avaliação de abordagens e ferramentas para a prevenção e resposta proativa a ataques de *Ransomware*, reduzindo impacto relacionado a ocorrência do ataque e fortalecendo a

resiliência cibernética das organizações. Além disso, também se almeja investigar como a inteligência artificial (especialmente LLMs) podem ajudar neste cenário. Por fim, também é vislumbrado a avaliação destas abordagens e técnicas em organizações para possibilitar uma melhor avaliação das mesmas.

Referências

[1] Alexander Lawall and Petra Beenken. 2024. A Threat-Led Approach to Mitigating Ransomware Attacks: Insights from a Comprehensive Analysis of the Ransomware Ecosystem. In Proceedings of the 2024 European Interdisciplinary Cybersecurity Conference (EICC '24). Association for Computing Machinery, New York, NY, USA, 210–216. https://doi.org/10.1145/3655693.3661321

[2] R. Marinho and R. Holanda, "Automated Emerging Cyber Threat Identification and Profiling Based on Natural Language Processing," in IEEE Access, vol. 11, pp. 58915-58936, 2023, doi: 10.1109/ACCESS.2023.3260020.

[3] U. Tekin and E. N. Yilmaz, "Obtaining Cyber Threat Intelligence Data From Twitter With Deep Learning Methods," 2021 5th International Symposium on Multidisciplinary Studies and Innovative Technologies (ISMSIT), Ankara, Turkey, 2021, pp. 82-86, doi: 10.1109/ISMSIT52890.2021.9604715.

[4] F. Aldauiji, O. Batarfi and M. Bayousef, "Utilizing Cyber Threat Hunting Techniques to Find Ransomware Attacks: A Survey of the State of the Art," in IEEE Access, vol. 10, pp. 61695-61706, 2022, doi: 10.1109/ACCESS.2022.3181278.

[5] M. Kante, V. Sharma and K. Gupta, "Mitigating Ransomware Attacks through Cyber Threat Intelligence and Machine Learning: Survey," 2023 International Conference on Research Methodologies in Knowledge Management, Artificial Intelligence and Telecommunication Engineering (RMKMATE), Chennai, India, 2023, pp. 1-5, doi: 10.1109/RMKMATE59243.2023.10369007.

[6] V. Rathod, C. Parekh and D. Dholariya, "AI & ML Based Anamoly Detection and Response Using Ember Dataset," 2021 9th International Conference on Reliability, Infocom Technologies and Optimization (Trends and Future Directions) (ICRITO), Noida, India, 2021, pp. 1-5, doi: 10.1109/ICRITO51393.2021.9596451.

[7] B. J. Chinmaya, S. A. Kudtarkar and Mohana, "Targeted Ransomware Attacks and Detection to Strengthen Cybersecurity Strategies," 2023 2nd International Conference on Automation, Computing and Renewable Systems (ICACRS), Pudukkottai, India, 2023, pp. 1039-1044, doi: 10.1109/ICACRS58579.2023.10404203.

[8] A. Yeboah-Ofori et al., "Cyber Threat Predictive Analytics for Improving Cyber Supply Chain Security," in IEEE Access, vol. 9, pp. 94318-94337, 2021, doi: 10.1109/ACCESS.2021.3087109.

[9] IBM. Ransomware as a Service (RaaS): O que é e como funciona. Disponível em: https://www.ibm.com/br-pt/topics/ransomware-as-a-service. Acesso em: 24 fev. 2025.

[10] MITRE. MITRE ATT&CK Framework. Disponível em: https://attack.mitre.org. Acesso em: 24 fev. 2025.

[11] Z. Song, Y. Tian and J. Zhang, "Similarity Analysis of Ransomware Attacks Based on ATT&CK Matrix," in IEEE Access, vol. 11, pp. 111378-111388, 2023, doi: 10.1109/ACCESS.2023.3322427.

[12] MITRE. MITRE D3FEND Framework. Disponível em: https://d3fend.mitre.org. Acesso em: 24 fev. 2025

[13] OSINT Framework. OSINT Framework: Open Source Intelligence Tools. Disponível em: https://osintframework.com. Acesso em: 24 fev. 2025