PONTIFÍCIA UNIVERSIDADE CATÓLICA DE GOIÁS
ESCOLA POLITÉCNICA E DE ARTES
GRADUAÇÃO EM CIÊNCIAS DA COMPUTAÇÃO

ANÁLISE DE ATAQUES DE RANSOMWARE:
IDENTIFICAÇÃO E MEDIDAS DE SEGURANÇA EFETIVAS

Samuel Bernardes de Souza

GOIÂNIA
2024

SAMUEL BERNARDES DE SOUZA

ANÁLISE DE ATAQUES DE RANSOMWARE:
IDENTIFICAÇÃO E MEDIDAS DE SEGURANÇA EFETIVAS

Trabalho de Conclusão de Curso apresentado à Escola de Ciências Exatas e da Computação, da Pontifícia Universidade Católica de Goiás, como parte dos requisitos para a obtenção do título de Bacharel em Ciência da Computação.

Orientador:
Prof. Me. Fernando Gonçalves Abadia.

GOIÂNIA
2024

SAMUEL BERNARDES DE SOUZA

ANÁLISE DE ATAQUES DE RANSOMWARE:
IDENTIFICAÇÃO E MEDIDAS DE SEGURANÇA EFETIVAS

Este Trabalho de Conclusão de Curso foi julgado adequado para a obtenção do título de Bacharel em Ciências da Computação, e aprovado em sua forma final pela Escola de Ciências Exatas e da Computação, da Pontifícia Universidade Católica de Goiás, em _____/_____/_____.

_____
Profa. Ma. Ludmilla Reis Pinheiro dos Santos

Banca examinadora:

_____
Prof. Me. Fernando Gonçalves Abadia

_____
Profa. Ma. Lucília Gomes Ribeiro

_____
Prof. Me. Rafael Leal Martins

GOIÂNIA
2024

RESUMO

Este trabalho aborda o fenômeno do *ransomware*, um tipo de ciberataque que utiliza *software* malicioso para criptografar dados de um sistema ou rede, tornando-os inacessíveis ao usuário legítimo e exigindo um resgate para a liberação dos dados. O objetivo principal é analisar as estratégias de identificação e medidas de segurança eficazes para proteger organizações e indivíduos contra ataques de *ransomware*, assegurando a integridade e disponibilidade dos dados críticos. A pesquisa explora diferentes tipos de *ransomware*, como *Crypto Ransomware, Locker Ransomware, Scareware, e Doxware*, além de modelos de negócios como *Ransomware-as-a-Service* (RaaS). Foram analisados casos notáveis de ataques, como *WannaCry, Petya/NotPetya e GandCrab*, para identificar padrões comportamentais e técnicas utilizadas pelos atacantes. As medidas de segurança propostas incluem restrições de privilégios, segmentação de rede, monitoramento de tráfego, e análise de comportamento anômalo, com o intuito de prevenir e mitigar os impactos desses ataques. O estudo espera contribuir para a melhoria das políticas de segurança nas organizações e o desenvolvimento de soluções tecnológicas mais robustas contra *ransomware*.

Palavras-chave: *Ransomware*. Segurança Cibernética. Criptografia de Dados. Mitigação de Ataques. Estratégias de Identificação.

ABSTRACT

This work addresses the phenomenon of *ransomware*, a type of *cyberattack* that uses malicious software to encrypt data on a system or network, making it inaccessible to the legitimate user and demanding a ransom for the release of the data. The main objective is to analyze identification strategies and effective security measures to protect organizations and individuals against *ransomware* attacks, ensuring the integrity and availability of critical data. The research explores different types of *ransomwares*, such as *Crypto Ransomware*, *Locker Ransomware*, *Scareware*, and *Doxware*, as well as business models like *Ransomware-as-a-Service (RaaS)*. Notable attack cases, such as *WannaCry*, *Petya/NotPetya*, and *GandCrab*, were analyzed to identify behavioral patterns and techniques used by attackers. The proposed security measures include privilege restrictions, network segmentation, traffic monitoring, and anomaly behavior analysis, aiming to prevent and mitigate the impacts of these attacks. The study hopes to contribute to the improvement of security policies in organizations and the development of more robust technological solutions against *ransomware*.

Keywords: *Ransomware*. *Cybersecurity*. *Data Encryption*. *Attack Mitigation*. *Identification Strategies*.

LISTA DE SIGLAS

TI – Tecnologia da Informação

IDS - *Intrusion Detection System* (Sistema de Detecção de Intrusão)

IPS - *Intrusion Prevention System* (Sistema de Prevenção de Intrusos)

RSA - *Rivest-Shamir-Adleman* (Sistema de Criptografia)

SMB - *Server Message Block* - Bloco de mensagens do servidor

NSA - *National Security Agency* (Agência de Segurança Nacional)

LISTA DE FIGURAS

SUMÁRIO

1. INTRODUÇÃO

Vivemos em uma era digital onde a informação é um dos ativos mais valiosos para indivíduos e organizações. A rápida evolução tecnológica e a crescente dependência da *Internet* para operações cotidianas trouxeram inúmeros benefícios, mas também aumentaram significativamente os riscos cibernéticos. Entre esses riscos, destaca-se o *ransomware*, um tipo de malware que sequestra dados através de criptografia e exige um resgate para restaurar o acesso. Este trabalho explora a importância das medidas de segurança cibernética para proteger contra ataques de *ransomware*, abordando desde políticas de *backup* até estratégias de identificação e mitigação de ameaças. Ao entender e implementar práticas eficazes de segurança, é possível minimizar os impactos devastadores que esses ataques podem causar nas infraestruturas de TI e nos dados sensíveis que elas contêm.

“Dados são informações brutas que precisam ser transformadas em conhecimento, através de técnicas de análise e interpretação, para serem utilizadas em processos de tomada de decisão" (NASCIMENTO, 2022).

A segurança de dados é o conjunto de técnicas e estratégias que visam proteger as informações de acessos não autorizados, garantindo sua privacidade e confiabilidade. Além disso, é um tema crítico nas organizações, uma vez que a perda ou vazamento de informações pode gerar prejuízos financeiros e reputacionais (OLIVEIRA, 2022).

A *Internet* é uma ferramenta essencial para a comunicação, o comércio, a educação e o entretenimento. Com a crescente digitalização da sociedade, a importância da *Internet* só tende a aumentar, tornando-se indispensável para a vida moderna (RAFAEL, 2019).

> Nos últimos anos, identificou-se um crescimento notável de pequenos dispositivos tecnológicos conectados à *Internet* trocando informações gerando o conceito de *Internet* das Coisas. Muitos destes dispositivos são encontrados apoiando diversos modelos de negócio. Dispositivos que vão desde sensores cardíacos de Assistência Médica passando por relógios, micro-ondas e até sensores de terremotos, furacões e tsunamis sendo estes fundamentais para a sociedade moderna. Embora existam inúmeras preocupações por parte da tecnologia quanto a restrição de processamento, memória, *bandwidth* e energia devido ao tamanho reduzido destes dispositivos, pouco sabe-se sobre como alcançar níveis necessários de

> segurança afim de cumprir um conjunto de legislações de países para estes dispositivos (NOBRE, LOPES, GOMES, 2019, p.253).

Os ataques de *ransomware* são marcados por algumas características principais. Podemos citar, por exemplo, a criptografia de dados. Nesses ataques são empregados algoritmos de criptografia avançados para bloquear o acesso aos arquivos da vítima, tornando-os ilegíveis sem a chave correta.

1.1 Justificativa

A justificativa para a realização deste projeto é fundamentada na significativa contribuição que os estudos sobre ataques de *ransomware* podem oferecer em diversos aspectos da segurança cibernética. O projeto visa reforçar as políticas de segurança nas organizações, permitindo a identificação e mitigação eficaz desses ataques. Isso é crucial, uma vez que a crescente incidência de *ransomware* tem gerado grandes prejuízos financeiros e operacionais para empresas de diversos setores. Dados da *Sophos* mostram que, em 2021, 55% das empresas brasileiras sofreram ataques de *ransomware*. A crescente sofisticação e frequência dos ataques de *ransomware* têm gerado impactos significativos na segurança cibernética, ameaçando não apenas a integridade dos dados, mas também a operacionalidade de organizações e indivíduos.

Diante desse contexto, este projeto busca responder quais seriam as estratégias de identificação e as medidas de segurança efetivas necessárias para proteger organizações e indivíduos contra os ataques de *ransomware*, garantindo a integridade e disponibilidade de seus dados críticos. Dessa forma, o projeto não apenas visa mostrar como as organizações podem se proteger, através de estudos de caso e avaliações de ataques e defesas, mas também capacitar indivíduos a contribuírem para um ambiente digital mais seguro.

1.2. Objetivos

A definição clara dos objetivos de um estudo é fundamental para direcionar a pesquisa e garantir que todas as questões relevantes sejam abordadas de maneira

eficaz. Este trabalho tem como objetivo geral analisar as estratégias de identificação e medidas de segurança eficazes para proteger organizações e indivíduos contra ataques de *ransomware*. Para atingir esse objetivo, foram definidos objetivos específicos que guiarão a investigação e a implementação das soluções propostas.

1.2.1. Geral

Analisar e compreender os padrões e estratégias utilizadas nos ataques de ransomware, identificar e classificar as vulnerabilidades mais exploradas por esses ataques, e propor e avaliar medidas de segurança efetivas para sua prevenção e mitigação.

1.2.2. Específico

- Analisar casos recentes de ataques de *ransomware*, especificamente, *AIDS Trojan*, *Gpcode*, *GandCrab*, *CryptoLocker*, *CryptoWall*, *WannaCry*, *Petya/NotPetya*, além do modelo de negócio *Ransomware as a Service*, para identificar *modus operandi* e padrões comportamentais;
- Avaliar a eficácia das soluções de segurança existentes na identificação e bloqueio de ataques de *ransomware*;
- Investigar as implicações éticas relacionadas ao pagamento de resgates em casos de ataques de *ransomware*;
- Avaliar o impacto econômico e reputacional de organizações após sofrerem ataques de *ransomware*;
- Analisar as tendências e evoluções dos ataques de *ransomware* nos últimos anos.

1.3. Métodologia

Esta pesquisa segunda a sua natureza é um resumo de assunto, sendo uma natureza de pesquisa onde se é feito um estudo sobre o tema do projeto, com o intuito único de substanciar a área de conhecimento (WAZLAWICK, 2014).

Segundo seus objetivos é uma pesquisa exploratória e descritiva, na qual o pesquisador faz apenas a descrição dos fatos existentes sobre o tema, sem haver

interferência do mesmo ou o desenvolvimento de teorias originais sobre o assunto (WAZLAWICK, 2014).

E segundo seus procedimentos técnicos, esta pesquisa é bibliográfica. A pesquisa bibliográfica pode ser definida sendo um estudo de testes, artigos, livros e entre outros disponibilizados, é um dos pontos fundamentais de qualquer projeto, no entanto não são produzidos novos conhecimentos (WAZLAWICK, 2014).

1.4. Organização textual

Os capítulos seguintes foram divididos em fundamentação teórica, materiais e métodos, desenvolvimento, resultados e considerações finais.

No capítulo a seguir, será apresentada uma contextualização teórica dos conceitos aplicados neste trabalho, estudo que se faz necessário para melhor compreensão acerca do projeto.

Os materiais e métodos informam ao leitor os recursos e procedimentos metodológicos adotados no decorrer do estudo, focando na revisão bibliográfica e análise de literatura existente sobre ataques de *ransomware*, sua identificação e medidas de segurança.

Enquanto o capítulo 4 se concentra na análise detalhada dos ataques de *ransomware*, o capítulo 5 apresenta os dados gerados deste estudo sobre os ataques, seguido pela consideração final do projeto e suas referências.

2. REFERENCIAL TEÓRICO

No contexto da análise de ataques de *ransomware* e a busca por medidas de segurança eficazes, é essencial explorar uma variedade de teorias e conceitos fundamentais. Este referencial teórico aborda diferentes abordagens, desde a compreensão das técnicas de infiltração e criptografia utilizadas pelo *ransomware* até a análise dos motivadores por trás desses ataques. Além disso, serão discutidas teorias relacionadas à cibersegurança, como modelos de ameaças e estratégias de defesa, proporcionando uma base sólida para o desenvolvimento de medidas preventivas e reativas contra esse tipo de ameaça.

2.1. Definições e Conceitos Fundamentais

Nesta seção, serão apresentadas as definições e os conceitos fundamentais que constituem a base para a compreensão abrangente dos ataques de *ransomware*.

2.1.1. Ransomware

A palavra "*ransom*" significa "resgate" em inglês, enquanto "*ware*" é uma abreviação de "*software*". (SYMANTEC, 2018).

Ransomware é uma forma de *software* malicioso que bloqueia o acesso aos dados ou sistemas de uma vítima, geralmente criptografando arquivos, e exige um pagamento de resgate para restaurar o acesso. Este pagamento, frequentemente solicitado em criptomoedas como *Bitcoin*, é difícil de rastrear, o que complica os esforços de aplicação da lei para identificar e capturar os responsáveis. *Ransomware* representa uma ameaça significativa tanto para usuários individuais quanto para organizações de todos os portes, devido ao potencial de causar interrupções significativas nas operações e perda de dados críticos (KASPERSKY, 2021).

2.1.2. Segurança de Dados

A segurança de dados envolve práticas e tecnologias que protegem informações contra acessos não autorizados, garantindo sua confidencialidade,

integridade e disponibilidade. Isso é crucial para prevenir perdas financeiras e danos à reputação das organizações (OLIVEIRA, 2022).

2.2. Análise de Ataques de *Ransomware*

Nesta seção, será realizada uma análise detalhada dos ataques de *ransomware*, abordando suas características, padrões de comportamento e impactos sobre organizações e indivíduos.

2.2.1. Métodos de Infecção

Os métodos de infecção mais comuns incluem campanhas de *phishing*, onde e-mails fraudulentos induzem os usuários a baixarem e executar arquivos maliciosos, e a exploração de vulnerabilidades em *software* desatualizado. Essas infecções podem ocorrer sem interação do usuário, aproveitando-se de falhas de segurança nos sistemas (KASPERSKY, 2021).

2.2.2. Tipos de Ransomware

Crypto Ransomware: o *Crypto Ransomware* é o tipo mais comum e perigoso de *ransomware*. Ele criptografa os arquivos da vítima, tornando-os inacessíveis sem a chave de descriptografia. Exemplos proeminentes incluem *CryptoLocker*, *Locky*, e *WannaCry*. Estes *ransomware* frequentemente utilizam algoritmos de criptografia assimétrica, como RSA, que tornam a recuperação dos dados sem a chave privada quase impossível (SOPHOS, 2020).

Locker Ransomware: o *Locker Ransomware* bloqueia a *interface* do usuário, impedindo-o de acessar seu sistema ou arquivos. Embora este tipo de *ransomware* não criptografe os arquivos, ele torna o dispositivo inutilizável até que o resgate seja pago. O *Reveton* é um exemplo clássico de *Locker Ransomware*, que exibiu uma mensagem falsa alegando ser de uma agência de aplicação da lei e exigia um pagamento para desbloquear o computador (EUROPOL, 2019).

Scareware: o *Scareware* é uma forma menos grave de *ransomware* que geralmente não danifica diretamente os dados da vítima. Em vez disso, ele exibe mensagens alarmantes dizendo que um *malware* foi detectado no sistema e exige um

pagamento para remover a suposta ameaça. Embora o *Scareware* possa ser mais uma tática de intimidação, ele pode causar considerável angústia e levar as vítimas a pagarem por serviços ou *softwares* desnecessários.

Doxware (ou *Extortionware*): o *Doxware*, ou *Extortionware*, é uma forma de *ransomware* que ameaça divulgar informações pessoais ou sensíveis da vítima a menos que o resgate seja pago. Um exemplo é o *ransomware Jigsaw*, que além de criptografar arquivos, ameaçava deletar arquivos progressivamente até que o resgate fosse pago. Esta forma de *ransomware* explora o medo da exposição pública de informações privadas para coagir o pagamento (KASPERSKY, 2021).

Ransomware-as-a-Service (RaaS): o *Ransomware-as-a-Service* (RaaS) é um modelo de negócios no qual os desenvolvedores de *ransomware* vendem ou alugam suas criações para outros criminosos cibernéticos. Este modelo permite que até mesmo indivíduos com habilidades técnicas limitadas possam lançar ataques de *ransomware*. Os desenvolvedores recebem uma comissão sobre cada pagamento de resgate bem-sucedido, criando um ecossistema lucrativo e incentivando a proliferação de ataques de *ransomware* (SYMANTEC, 2018).

2.3. Identificação de *Ransomware*

A identificação precoce de *ransomware* é crucial para mitigar seus danos. Técnicas comuns de identificação incluem a análise de comportamento, que monitora padrões suspeitos, como a criptografia de múltiplos arquivos em um curto período. Ferramentas de segurança como *antivírus* e *firewalls* são fundamentais na detecção inicial, bloqueando atividades maliciosas antes que possam causar danos significativos (SYMANTEC, 2018).

2.4. Medidas de Segurança Contra *Ransomware*

Esta seção apresenta uma análise das medidas de segurança eficazes para prevenir e mitigar ataques de *ransomware*. Serão discutidas estratégias de defesa, incluindo práticas de cibersegurança, implementação de tecnologias avançadas de proteção e políticas organizacionais. A seção terá abordagens preventivas, como a educação dos usuários e a atualização regular de sistemas. Ao examinar essas práticas, busca-se fornecer um conjunto abrangente de recomendações que possam

ser adotadas para fortalecer a resiliência contra ataques de *ransomware* e minimizar seus impactos.

2.4.1. Políticas de Backup

Uma das medidas mais eficazes contra *ransomware* é a implementação de políticas robustas de *backup*, ou seja, uma cópia de segurança dos dados importantes armazenados em um dispositivo, como um computador, para protegê-los contra perdas acidentais, corrupção de arquivos ou ataques de *malware*. Essas cópias são armazenadas em outro local seguro, permitindo a recuperação dos dados em caso de falha no dispositivo original. Realizar *backups* regulares e armazená-los em locais seguros, preferencialmente *offline*, garante que os dados possam ser recuperados sem a necessidade de pagar o resgate (NIST, 2020).

2.4.2. Atualização de Sistemas

Manter sistemas operacionais e aplicativos sempre atualizados com os *patches* de segurança mais recentes é vital para prevenir a exploração de vulnerabilidades conhecidas. A aplicação de atualizações regularmente reduz significativamente o risco de infecção por *ransomware* (MICROSOFT, 2020).

2.4.3. Educação e Treinamento de Usuários

A educação e o treinamento de usuários são fundamentais na prevenção de ataques cibernéticos, especialmente *ransomware*. A formação proativa dos usuários pode reduzir significativamente o risco de comprometer a segurança da rede e dos dados. Os usuários frequentemente representam a primeira linha de defesa contra ataques cibernéticos. Um usuário bem informado e treinado pode identificar e evitar ameaças antes que causem danos. A maioria dos ataques de *ransomware* e *phishing* explora a falta de conhecimento dos usuários. Ao educar e treinar os usuários, as organizações podem reduzir drasticamente o número de incidentes de segurança.

Treinar os usuários para reconhecer *e-mails* de *phishing*, como aqueles que contêm erros gramaticais, endereços de remetentes estranhos ou *links* suspeitos, é essencial. Além disso, é importante ensinar a técnica de passar o mouse sobre os

links para verificar o *URL* real antes de clicar, e alertar sobre os perigos de abrir anexos inesperados ou de fontes não confiáveis. No que diz respeito à navegação segura na *web*, é crucial incentivar o uso de sites seguros (HTTPS) e explicar a importância do cadeado de segurança nos navegadores. Orientar os usuários a baixar *software* apenas de fontes confiáveis e evitar *downloads* piratas ou de sites duvidosos também é uma prática recomendada.

Oferecer treinamentos presenciais e *online* regulares para todos os funcionários, abordando os tópicos mais recentes e relevantes em segurança cibernética, pode ser muito eficaz. Realizar *workshops* práticos onde os usuários possam aprender a identificar ameaças em um ambiente controlado é outra estratégia importante. Conduzir campanhas de simulação de *phishing* para testar a capacidade dos usuários em reconhecer e evitar esses ataques, fornecendo *feedback* imediato e treinamentos adicionais para aqueles que falharem nas simulações, também é uma prática recomendada. Implementar testes de segurança regulares que incluam situações de ameaças reais para avaliar a prontidão dos usuários é essencial para manter um ambiente seguro.

Manter o conteúdo dos treinamentos atualizado com as últimas ameaças e técnicas de ataque é crucial, pois a segurança cibernética é um campo dinâmico e as estratégias de treinamento devem evoluir constantemente. Recolher *feedback* dos usuários sobre os treinamentos e ajustar os conteúdos e métodos conforme necessário para garantir eficácia é outra prática importante. Estabelecer políticas de segurança claras e acessíveis a todos os usuários, garantindo que saibam como reagir em caso de suspeita de ameaça, também é essencial. Disponibilizar uma equipe de suporte pronta para ajudar os usuários com dúvidas ou problemas relacionados à segurança é uma medida adicional que pode fortalecer a defesa contra ataques cibernéticos.

Desenvolver uma cultura organizacional que priorize a segurança cibernética, onde todos os membros da equipe estejam alinhados com as melhores práticas de segurança, pode trazer benefícios a longo prazo. Prevenindo ataques cibernéticos, as organizações podem evitar custos significativos associados a violações de dados, resgates e recuperação de sistemas. Assim, a educação e o treinamento contínuo dos usuários não só fortalecem a defesa contra ataques de *ransomware*, mas também

promovem uma cultura de segurança que beneficia a organização a longo prazo. (SPEAR, 2021)

2.4.4. Soluções Tecnológicas

A implementação de soluções tecnológicas avançadas é essencial para proteger a rede contra atividades suspeitas e ataques de *ransomware*. Entre as ferramentas mais eficazes estão os sistemas de detecção de intrusão (IDS) e prevenção de intrusão (IPS). O IDS, como o *Snort* e o *Suricata*, monitora o tráfego da rede em busca de atividades suspeitas e potenciais ameaças, alertando os administradores de segurança quando são detectadas anomalias. Já o IPS, exemplificado pelo *Cisco Firepower* e o *Palo Alto Networks*, não apenas detecta, mas também bloqueia e previne as ameaças em tempo real, agindo de maneira proativa para proteger a rede. (CHECKPOINT, 2021)

Os *firewalls* de próxima geração representam outra camada crítica de defesa. Eles não apenas filtram o tráfego de rede baseado em regras de segurança, mas também oferecem inspeção profunda de pacotes, controle de aplicativos e inteligência contra ameaças. Exemplos notáveis de *firewalls* de próxima geração incluem o *Palo Alto Networks Next-Generation Firewall* (NGFW), o *Fortinet FortiGate* e o *Check Point Next Generation Firewall.* Essas funcionalidades avançadas permitem uma análise mais detalhada e precisa do tráfego, ajudando a identificar e bloquear ataques complexos e avançados que poderiam passar despercebidos por *firewalls* tradicionais. (CHECKPOINT, 2021)

Software antivírus continua sendo uma ferramenta fundamental na luta contra o *ransomware*. Soluções modernas de antivírus utilizam técnicas de *machine learning* e inteligência artificial para detectar e mitigar ameaças conhecidas e desconhecidas. Além de realizar verificações regulares e em tempo real de arquivos e programas, essas soluções podem isolar e remover *malware* antes que cause danos significativos. Algumas das principais soluções de antivírus incluem *Norton*, *McAfee*, *Bitdefender* e *Kaspersky*, que são amplamente reconhecidas por sua eficácia e robustez. (CHECKPOINT, 2021)

Outro exemplo de ferramenta importante é o *EDR* (*Endpoint Detection and Response*), que oferece monitoramento contínuo e resposta a ameaças nos *endpoints*. Ferramentas como *CrowdStrike Falcon*, *Carbon Black* e *SentinelOne* fornecem visibilidade detalhada das atividades nos dispositivos da rede, permitindo a detecção e resposta rápida a ataques antes que eles possam se espalhar ou causar danos maiores. (CHECKPOINT, 2021)

Além disso, a implementação de soluções de *backup* e recuperação de dados é vital para garantir que, em caso de ataque, as informações críticas possam ser restauradas sem pagar o resgate. Ferramentas de *backup* como *Veeam*, *Acronis*, e *Veritas Backup Exec* oferecem soluções robustas para criar cópias seguras dos dados, garantindo a continuidade dos negócios e a recuperação rápida em caso de incidentes. (CHECKPOINT, 2021)

2.5. Estudos Relevantes e Autores Importantes

Vários estudos e autores têm contribuído significativamente para a compreensão do *ransomware* e suas estratégias de mitigação. Savage, Coogan e Lau (2015) realizaram uma análise detalhada das tendências de *ransomware*, destacando as técnicas de ataque e as melhores práticas de defesa. O relatório anual da *Symantec* (2018) sobre ameaças à segurança cibernética fornece uma visão abrangente das evoluções do *ransomware* e recomendações para prevenção. A pesquisa de Andronio, Zanero e Maggi (2015) sobre a propagação do *WannaCry* elucidou os mecanismos de infecção e as implicações globais dos ataques de *ransomware*.

3. MATERIAIS E MÉTODOS

Esta seção descreve detalhadamente os recursos e procedimentos metodológicos adotados no decorrer do estudo, focando na revisão bibliográfica e análise de literatura existente sobre ataques de *ransomware*, sua identificação e medidas de segurança. A revisão bibliográfica é essencial para fornecer uma base teórica sólida e permitir a replicação do estudo.

3.1. Materiais

Esta seção descreve os materiais utilizados na pesquisa sobre ataques de *ransomware*. Serão detalhados os recursos e ferramentas empregadas na coleta e análise de dados, incluindo *software* de segurança e literatura acadêmica relevante. A descrição dos materiais visa proporcionar uma compreensão clara dos recursos que fundamentam as análises e conclusões apresentadas no estudo

3.1.1. Fontes de Informação

Foram utilizados diversos tipos de fontes de informação para compor a revisão bibliográfica, incluindo:

- **Artigos Científicos:** Publicados em periódicos renomados nas áreas de segurança da informação e cibersegurança.
- **Relatórios de Segurança:** Emitidos por empresas especializadas, como *Symantec, Kaspersky, Palo Alto Networks*, entre outras.
- **Livros Especializados:** Obras que abordam de maneira profunda temas relacionados à cibersegurança e *ransomware*.
- **Conferências e Simpósios:** Trabalhos apresentados em conferências e simpósios internacionais, como o *Symposium on Security and Privacy* (S&P) e o *International Symposium on Research in Attacks, Intrusions and Defenses* (RAID).
- **Bases de Dados Acadêmicas:** *Google Scholar, IEEE Xplore, Scopus* e *PubMed* para acesso a artigos e teses relevantes.

3.2. Métodos

Esta seção delineia os métodos empregados na pesquisa sobre ataques de *ransomware*. Serão apresentados os procedimentos e técnicas de análise utilizados para coletar, processar e interpretar os dados.

3.2.1. Coleta de Dados

A coleta de dados foi realizada através de uma pesquisa sistemática em bases de dados acadêmicas e repositórios de segurança. As palavras-chave utilizadas na pesquisa incluíram "*ransomware*", "cibersegurança", "medidas de segurança contra *ransomware*", "análise de *malware*", entre outras relacionadas ao tema.

3.2.2. Análise de Dados

A análise de dados envolveu a leitura crítica e a síntese dos estudos selecionados. Foram extraídas informações chave sobre:

- Tipos de *ransomware* e suas características;
- Métodos de infecção e propagação;
- Técnicas de identificação e resposta a ataques;
- Medidas preventivas e de mitigação.

Os dados coletados foram organizados em categorias temáticas para facilitar a análise comparativa e a identificação de padrões e tendências.

3.3. Considerações Éticas

A revisão bibliográfica foi conduzida de maneira ética, respeitando os direitos autorais e citando adequadamente todas as fontes utilizadas. Além disso, a pesquisa buscou proporcionar uma visão imparcial e abrangente do tema, sem favorecer interesses específicos.

4. ANÁLISE DE ATAQUES DE *RANSOMWARE*: IDENTIFICAÇÃO E MEDIDAS DE SEGURANÇA EFETIVAS

Esta seção se concentra na análise detalhada dos ataques de *ransomware*, com ênfase na identificação dos métodos utilizados pelos cibercriminosos e nas medidas de segurança mais eficazes para combatê-los. Serão explorados os diferentes tipos de *ransomware*, suas técnicas de disseminação e os impactos que causam. Além disso, serão discutidas estratégias de defesa, abordando tanto abordagens preventivas quanto reativas, com base em estudos de caso e na literatura especializada. O objetivo é fornecer uma compreensão abrangente dos ataques de *ransomware* e das práticas recomendadas para proteger sistemas e dados contra essa crescente ameaça cibernética.

4.1. Evolução Histórica do *Ransomware*

O primeiro caso conhecido de *ransomware*, denominado "*AIDS Trojan*" ou "*PC Cyborg*", foi criado por Joseph Popp em 1989. Este *ransomware* era distribuído em disquetes e utilizava um método de criptografia rudimentar que renomeava os arquivos do sistema. As vítimas eram instruídas a enviar US$189 para uma caixa postal no Panamá para obter a ferramenta de descriptografia (MOURA; PINTO, 2020).

Nos anos 2000, o *ransomware* evoluiu com o surgimento de ferramentas de criptografia mais sofisticadas. Em 2005, o "*Gpcode*" começou a usar algoritmos de criptografia RSA de 660 bits, que eram significativamente mais difíceis de quebrar. Esta evolução mostrou um aumento na sofisticação dos ataques e uma maior dificuldade em recuperar os dados sem pagar o resgate (ANDRONIO et al., 2015).

A década de 2010 viu um aumento significativo na prevalência e na sofisticação do *ransomware*. O *CryptoLocker*, surgido em 2013, foi um marco importante. Utilizando criptografia RSA de 2048 bits, o *CryptoLocker* se espalhou rapidamente via *e-mails* de *phishing* com anexos maliciosos. Este *ransomware* foi responsável por milhões de dólares em resgates pagos por vítimas desesperadas para recuperar seus dados (SYMANTEC, 2018).

Outro exemplo notável é o *ransomware CryptoWall*, que apareceu em 2014. Ele utilizava técnicas avançadas de distribuição, incluindo *e-mails* de *phishing* e *kits*

de exploração que exploravam vulnerabilidades em software popular, como o *Adobe Flash. CryptoWall* causou prejuízos estimados em mais de US$ 18 milhões apenas nos Estados Unidos (SOPHOS, 2020).

Em 2017, os ataques de *ransomware* alcançaram um novo patamar com o surgimento do *WannaCry* e do *Petya*/*NotPetya*. O *WannaCry* se espalhou rapidamente por meio de uma vulnerabilidade no protocolo SMB do *Windows*, conhecida como *EternalBlue*, que foi originalmente desenvolvida pela NSA (*National Security Agency*) e vazada pelo grupo *Shadow Brokers*. Este ataque infectou centenas de milhares de computadores em mais de 150 países, causando interrupções significativas em serviços críticos, como hospitais e sistemas de transporte (EUROPOL, 2019).

O *Petya*/*NotPetya*, que apareceu logo depois, inicialmente parecia ser um *ransomware* típico, mas logo se descobriu que sua verdadeira intenção era a destruição de dados, disfarçada como um ataque de *ransomware*. Ele se propagou usando uma combinação de técnicas, incluindo a mesma vulnerabilidade *EternalBlue* utilizada pelo *WannaCry*, além de roubar credenciais administrativas para se espalhar lateralmente dentro de redes corporativas. O impacto econômico do *Petya*/*NotPetya* foi devastador, com perdas globais estimadas em bilhões de dólares (KASPERSKY, 2021).

Nos últimos anos, houve um aumento na popularidade do modelo de negócios *Ransomware-as-a-Service* (RaaS), onde desenvolvedores de *ransomware* alugam ou vendem seu software para outros criminosos. Este modelo permite que até mesmo criminosos sem habilidades técnicas significativas possam lançar ataques de *ransomware*, ampliando o alcance e a frequência dos ataques. Exemplos notáveis de RaaS incluem o *GandCrab*, que, antes de ser desativado, gerou centenas de milhões de dólares em pagamentos de resgate (SYMANTEC, 2018).

4.2. Como Funciona o *Ransomware*

Os ataques de *ransomware* são complexos e envolvem várias etapas desde a infecção inicial até o vazamento de dados e a demanda de resgate. Compreender essas etapas é crucial para a implementação de medidas de segurança eficazes. Conforme visto na figura 1, vemos o ciclo de vida típico de um ataque de *ransomware*, destacando as principais fases envolvidas.

Figura 1 - Funcionamento do *Ransomware*

Fonte: INFOBUSINESS, 2019

1) A infecção inicial pode ocorrer através de vários vetores de ataque:
    - *E-mails* de *Phishing*: Esta é uma das formas mais comuns de infecção. O atacante envia *e-mails* que parecem legítimos, contendo *links* ou anexos maliciosos. Quando o destinatário clica no *link* ou abre o anexo, o *ransomware* é baixado e executado.
    - *Downloads* Maliciosos: *Sites* comprometidos ou fraudulentos podem hospedar arquivos maliciosos que são baixados inadvertidamente pelo usuário.
    - *Exploit Kits*: Estes *kits* exploram vulnerabilidades conhecidas em software, como navegadores ou *plugins*, para entregar o *ransomware* sem a necessidade de interação do usuário.
    - Dispositivos de Armazenamento Externo: *Ransomware* pode se espalhar através de dispositivos *USB* infectados conectados a um computador (Kaspersky, 2021).

2) Uma vez que o *ransomware* é executado, ele pode verificar o ambiente para detectar se está em uma *sandbox* (ambiente de teste isolado) ou em um ambiente de análise. Se o *ransomware* detectar que está em um ambiente controlado, ele pode se comportar de maneira benigna para evitar a detecção. Caso contrário, ele começa o processo de infecção.

Alguns *ransomware*, como o *WannaCry*, incluem capacidades de "*worm*", permitindo que se propaguem automaticamente para outros computadores na mesma rede, explorando vulnerabilidades de *software* (EUROPOL, 2019).

3) O processo de criptografia é o núcleo do *ransomware*. O *ransomware* identifica e criptografa arquivos de interesse, geralmente visando documentos, imagens, vídeos e arquivos de banco de dados. Ele pode usar algoritmos de criptografia simétrica (AES) para criptografar os arquivos rapidamente e, em seguida, criptografar a chave AES com um algoritmo assimétrico (RSA), tornando a descriptografia extremamente difícil sem a chave privada (SOPHOS, 2020).

Além disso, o *ransomware* pode excluir cópias de sombra e outros *backups* locais para evitar a recuperação dos dados sem pagar o resgate. Ele pode usar comandos do sistema operacional, como "*vssadmin delete shadows*" no *Windows*, para remover esses *backups*.

4) Após a criptografia, o *ransomware* exibe uma mensagem de resgate informando à vítima que seus arquivos foram criptografados. Esta mensagem geralmente inclui instruções sobre como pagar o resgate, que pode incluir o uso de criptomoedas para manter o anonimato do atacante. As mensagens de resgate podem variar de simples notas de texto a interfaces gráficas elaboradas, e podem incluir um cronômetro de contagem regressiva para aumentar a pressão psicológica sobre a vítima (KASPERSKY, 2021).

5) Se a vítima decide pagar o resgate, ela é instruída a transferir o valor exigido para uma carteira de criptomoedas especificada. Após o pagamento, o atacante pode fornecer uma chave de descriptografia ou uma ferramenta para restaurar os arquivos. No entanto, não há garantia de que a vítima receberá a chave de descriptografia após o pagamento. Em alguns casos, os atacantes

podem simplesmente desaparecer após receber o dinheiro, deixando os arquivos da vítima permanentemente inacessíveis (EUROPOL, 2019).

Os impactos de um ataque de *ransomware* podem ser devastadores, tanto financeiramente quanto operacionalmente. Empresas podem enfrentar interrupções significativas em suas operações, perda de dados críticos, danos à reputação e custos consideráveis para recuperação. Além disso, o pagamento de resgates pode incentivar ainda mais ataques, criando um ciclo vicioso de extorsão cibernética (SOPHOS, 2020).

4.3. Estudos de Caso Notáveis

WannaCry: o *WannaCry*, que surgiu em maio de 2017, foi um dos ataques de *ransomware* mais devastadores da história. Utilizando a vulnerabilidade *EternalBlue* no protocolo SMB do *Windows*, ele se propagou rapidamente, afetando sistemas em mais de 150 países. Organizações importantes, incluindo o Serviço Nacional de Saúde (NHS) do Reino Unido, foram severamente impactadas, resultando em cancelamentos de cirurgias e outras interrupções críticas. Estima-se que o *WannaCry* tenha causado danos de até US$ 4 bilhões globalmente (EUROPOL, 2019).

Petya/*NotPetya*: o ataque *Petya*/*NotPetya*, que ocorreu em junho de 2017, inicialmente parecia ser um *ransomware* típico, mas foi rapidamente identificado como um ataque destrutivo disfarçado. Utilizando uma combinação de vulnerabilidades, incluindo a mesma falha *EternalBlue* explorada pelo *WannaCry*, ele se espalhou rapidamente através de redes corporativas. Grandes empresas multinacionais, como a *Maersk*, a *Merck* e a *FedEx*, sofreram interrupções significativas, com perdas econômicas estimadas em bilhões de dólares. Diferente de um *ransomware* convencional, o *NotPetya* visava destruir dados, em vez de extorquir resgates (KASPERSKY, 2021).

GandCrab: foi um dos *ransomwares* mais prolíficos e bem-sucedidos até a sua aposentadoria em 2019. Operando sob o modelo *Ransomware-as-a-Service* (RaaS), ele permitiu que afiliados com pouca experiência técnica lançassem ataques de *ransomware* em troca de uma parte dos lucros. *GandCrab* utilizava técnicas avançadas para evitar a detecção e frequentemente mudava suas táticas para escapar das medidas de segurança. Durante seu tempo ativo, *GandCrab* gerou

centenas de milhões de dólares em pagamentos de resgate, destacando a lucratividade do modelo RaaS (SYMANTEC, 2018).

4.4. Economia do *Ransomware*

Esta seção examina a economia do *ransomware*, explorando os incentivos financeiros que impulsionam esses ataques. Serão analisados os modelos de negócio dos cibercriminosos, as estratégias de monetização e o impacto econômico para as vítimas. Além disso, serão discutidos os mercados negros digitais e as transações em criptomoedas que facilitam o funcionamento dessa economia ilícita. O objetivo é fornecer uma compreensão clara dos fatores econômicos que sustentam a persistência e a evolução dos ataques de *ransomware*.

4.4.1. Motivações dos Atacantes

Os atacantes que utilizam *ransomware* têm diversas motivações, sendo o ganho financeiro o principal. Eles visam obter resgates em criptomoedas, que garantem anonimato e dificultam o rastreamento pelas autoridades. Além disso, hacktivismo e espionagem são motivações significativas. Hacktivistas utilizam *ransomware* para promover agendas políticas ou sociais, enquanto entidades estatais podem usá-lo para obter informações sensíveis ou desestabilizar adversários (KSHETRI, 2018).

4.4.2. Mercado Negro e Criptomoedas

O mercado negro desempenha um papel crucial na economia do *ransomware*. Criptomoedas como o *Bitcoin* são amplamente usadas para realizar transações anônimas, facilitando a coleta de resgates sem a necessidade de intermediários financeiros tradicionais. Esses mercados também vendem *kits* de *ransomware*, tornando mais fácil para criminosos sem habilidades técnicas lançar ataques (ANDERSON et al., 2013).

4.4.3. Cadeia de Suprimentos do Cibercrime

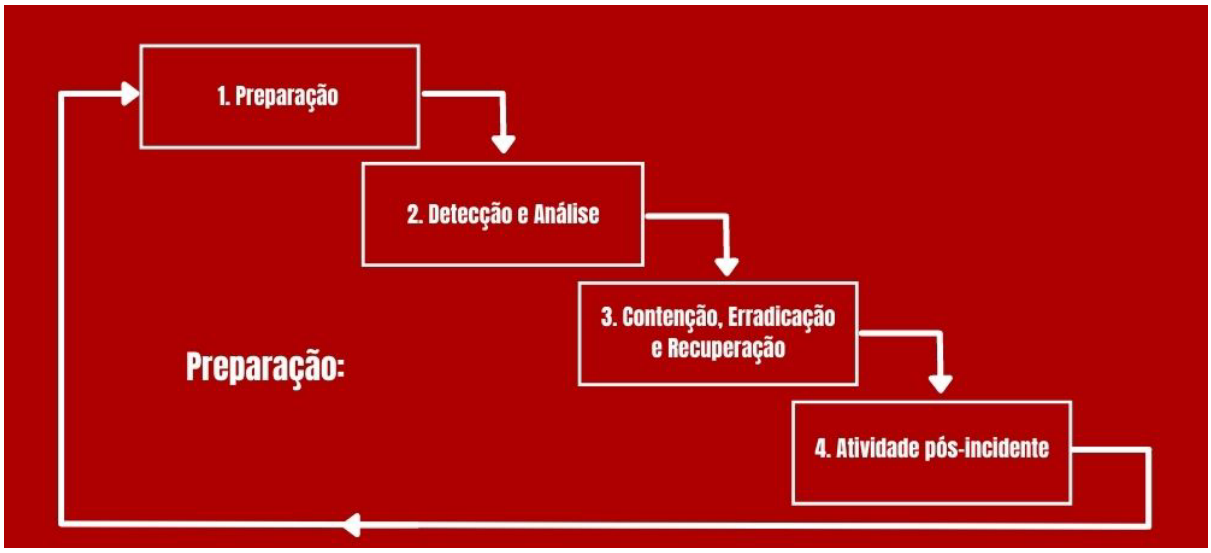
A cadeia de suprimentos do cibercrime é complexa e bem organizada. Inclui desenvolvedores que criam o *malware*, distribuidores que disseminam o *ransomware* e terceiros que lavam os lucros obtidos. Esse ecossistema permite uma operação eficiente e lucrativa, com cada participante desempenhando um papel específico na cadeia de valor do ataque (EUROPOL, 2018).

4.5. Estudos de Caso e Análises de Incidentes

Estudos de caso são essenciais para entender a prática e a teoria por trás dos ataques de *ransomware*. Por exemplo, o ataque *WannaCry* em 2017 explorou uma vulnerabilidade do *Windows* para se propagar rapidamente, causando danos em escala global. A análise deste incidente revela falhas na segurança cibernética e destaca a importância de atualizações de *software* e protocolos de resposta a incidentes (EUROPOL, 2018).

O NIST SP 800-61 oferece um guia abrangente para a resposta a incidentes de segurança da informação, fornecendo uma estrutura sistemática para identificar, conter, erradicar e recuperar de incidentes. Este plano de resposta a incidentes é essencial para minimizar o impacto dos ataques de *ransomware*, garantindo que as organizações possam rapidamente isolar ameaças, restaurar operações e aprender com os incidentes para fortalecer sua postura de segurança. A aplicação deste guia, conforme visto na figura 2, permite uma abordagem proativa e organizada, essencial para lidar com a crescente sofisticação dos ataques cibernéticos.

Figura 2 - Plano de resposta a incidentes *ransomware*



Fonte: HNZ, 2022

Outro exemplo é o ataque *NotPetya*, que, embora disfarçado de *ransomware*, visava causar destruição, afetando severamente empresas em todo o mundo (GREENBERG, 2018).

4.6. Tendências Atuais e Futuras

Esta seção aborda as tendências atuais e futuras dos ataques de *ransomware*, destacando as evoluções tecnológicas e as novas estratégias adotadas pelos cibercriminosos. Serão discutidas as mudanças no panorama das ameaças, as inovações em métodos de ataque e as previsões sobre o futuro do *ransomware*. O objetivo é fornecer *insights* sobre como a ameaça está se transformando e quais medidas poderão ser necessárias para enfrentar os desafios emergentes.

4.6.1. Evolução das Técnicas

As técnicas de *ransomware* estão em constante evolução. Recentemente, houve um aumento no uso de *ransomware* como serviço (RaaS), onde os desenvolvedores de *malware* vendem ou alugam seus produtos a afiliados. As estratégias de evasão de detecção também se tornam mais sofisticadas, utilizando técnicas de polimorfismo e *fileless malware*, dificultando a detecção por *softwares antivírus* tradicionais (KSHETRI, 2018).

4.6.2. Alvos Potenciais

Os atacantes de *ransomware* estão cada vez mais focando em alvos de alto valor, como infraestruturas críticas, hospitais e grandes corporações. Esses setores são vistos como mais propensos a pagar resgates altos devido ao impacto significativo de interrupções em suas operações. A infraestrutura crítica, em particular, é um alvo atraente devido às suas vulnerabilidades e à necessidade urgente de continuidade dos serviços (ANDERSON et al., 2013).

4.6.3. Desenvolvimentos Tecnológicos

Novas tecnologias, como inteligência artificial e *machine learning*, estão impactando a evolução do *ransomware*. Essas tecnologias podem ser usadas para automatizar e personalizar ataques, tornando-os mais eficazes e difíceis de detectar. Além disso, há uma tendência crescente de usar técnicas de *deepfake* e engenharia social avançada para comprometer sistemas (EUROPOL, 2018).

4.7. Identificação de Ransomware

A identificação precoce e precisa de *ransomware* é essencial para reduzir o impacto desses ataques cibernéticos e para iniciar uma resposta eficaz. Este segmento aborda uma variedade de métodos e indicadores para identificar *ransomware*, incluindo aspectos técnicos, comportamentais e de rede.

4.7.1. Indicadores Técnicos

A identificação de *ransomware* com base em indicadores técnicos envolve a análise de características específicas do *malware*, como sua assinatura digital, comportamento durante a execução e padrões de tráfego de rede.

4.7.1.1. Análise de Assinaturas

As assinaturas de *ransomware* são sequências de *bytes* exclusivas dentro do código malicioso que podem ser identificadas por soluções de segurança. Essas assinaturas são derivadas da análise estática ou dinâmica do *malware* e são usadas por *antivírus* e *firewalls* para identificar e bloquear *ransomware* conhecido (BILGE et al., 2014).

4.7.1.2. Monitoramento de Comportamento de Processos

O comportamento do *ransomware* durante a execução pode revelar suas intenções maliciosas. Por exemplo, muitos *ransomwares* exibem um comportamento de "*rush*", acessando e criptografando rapidamente uma grande quantidade de

arquivos. Ferramentas de análise de comportamento de processos podem detectar esse padrão e alertar sobre a presença de *ransomware* (SOOD et al., 2016).

4.7.1.3. Análise de Rede

O *ransomware* muitas vezes requer comunicação com servidores de comando e controle (C2) para receber instruções ou enviar chaves de criptografia. A análise do tráfego de rede em busca de padrões de comunicação maliciosos pode ajudar na detecção precoce de *ransomware*, especialmente em estágios iniciais do ataque (CHOI et al., 2017).

4.7.2. Indicadores Comportamentais

Além dos indicadores técnicos, comportamentos anômalos em sistemas e redes podem indicar a presença de *ransomware*.

4.7.2.1. Aumento do Uso de Recursos

O *ransomware* geralmente consome uma quantidade significativa de recursos do sistema, como CPU e memória, durante suas operações de criptografia. O monitoramento do uso de recursos pode ajudar a identificar atividades anormais que podem indicar a presença de *ransomware* (REHMAN et al., 2017).

4.7.2.2. Alterações nos Arquivos

A criptografia de arquivos pelo *ransomware* muitas vezes resulta em mudanças visíveis nos arquivos afetados. Isso pode incluir a adição de novas extensões de arquivo, alterações no conteúdo dos arquivos ou a criação de arquivos de resgate. Ferramentas de monitoramento de integridade de arquivos podem identificar essas alterações e alertar sobre um possível ataque de *ransomware* (BONNEAU et al., 2016).

4.7.2.3. Comportamento do Usuário

Comportamentos do usuário, como relatos de mensagens de resgate exibidas na tela ou tentativas de acessar arquivos criptografados, podem fornecer indicações adicionais sobre a presença de *ransomware*. É importante educar os usuários sobre os sinais de *ransomware* e incentivá-los a relatar qualquer atividade suspeita imediatamente (FEDOROV et al., 2018).

4.7.3. Indicadores de Rede

A análise do tráfego de rede pode revelar padrões de comunicação associados a *ransomware*.

4.7.3.1. Comunicações com C2

O *ransomware* geralmente se comunica com servidores de comando e controle para enviar informações sobre a vítima e receber instruções dos atacantes. A detecção de comunicações suspeitas com C2 pode indicar a presença de *ransomware* na rede (ABU RAJAB et al., 2017).

4.7.3.2. Tráfego de Dados Incomum

O *ransomware* pode gerar padrões de tráfego de rede incomuns, especialmente durante o processo de criptografia de arquivos e comunicação com C2. O monitoramento do tráfego de rede em busca de picos de atividade ou padrões anômalos pode ajudar na detecção de *ransomware* (MULLER et al., 2018).

4.7.3.3. Análise de Protocolos

A análise dos protocolos de rede pode revelar atividades suspeitas, como tentativas de exploração de vulnerabilidades ou transferência de grandes volumes de dados criptografados. A identificação desses padrões pode indicar um possível ataque de *ransomware* em andamento (DUNLAP et al., 2017).

4.7.4. Ferramentas e Técnicas de Identificação

Diversas ferramentas e técnicas estão disponíveis para auxiliar na identificação de *ransomware*.

4.7.4.1. Soluções de Endpoint Detection and Response (EDR)

As soluções EDR fornecem visibilidade detalhada sobre as atividades nos *endpoints* da rede, permitindo a detecção precoce de *ransomware* com base em indicadores comportamentais e de integridade de arquivos. Essas ferramentas também facilitam a resposta rápida a incidentes, ajudando a conter o impacto do *ransomware* (KHARRAZ et al., 2016).

4.7.4.2. Análise de Sandbox

As soluções de *sandboxing* permitem a execução segura de arquivos suspeitos em um ambiente isolado, onde seu comportamento pode ser observado sem afetar o ambiente de produção. A análise de *sandbox* pode identificar *ransomware* e fornecer informações sobre seu comportamento e funcionalidades (LINDORFER et al., 2019).

4.7.4.3. Honeypots

Honeypots são sistemas ou serviços falsos projetados para atrair e enganar atacantes. Ao implantar *honeypots* em uma rede, os pesquisadores podem capturar amostras de *ransomware* e estudar suas técnicas e métodos de propagação. Essas informações podem ser usadas para melhorar as defesas contra *ransomware* (ALRAWI et al., 2019).

4.8. Medidas de Segurança Efetivas contra *Ransomware*

Ransomware continua sendo uma das ameaças mais graves para a segurança cibernética, exigindo uma abordagem multifacetada de prevenção, detecção e resposta.

4.8.1. Estratégias de Prevenção

Atualizações de *Software* e *Patching*: Manter sistemas e aplicativos atualizados é crucial para corrigir vulnerabilidades conhecidas que os *ransomwares* exploram para infectar sistemas. Isso inclui não apenas o sistema operacional, mas também todos os programas e aplicativos em uso. As organizações devem implementar um processo formal de gestão de *patches* para garantir que as atualizações sejam aplicadas regularmente e de forma sistemática, minimizando assim a janela de exposição a possíveis explorações de vulnerabilidades (CERT, 2020).

Filtragem de *E-mails* e Conteúdo *Web*: A filtragem de *e-mails* e *web* é uma camada de defesa fundamental contra *ransomware*. Utilizar filtros avançados para bloquear *e-mails* e *websites* maliciosos que podem servir como vetores de infecção para *ransomware*. Isso inclui a identificação e bloqueio de anexos suspeitos, *links* maliciosos e conteúdo *web* comprometido. As organizações devem implementar soluções de filtragem de *e-mails* e conteúdo *web* que possam identificar e bloquear proativamente ameaças de *ransomware*, ajudando a prevenir infecções antes que ocorram (ENISA, 2020).

Restrições de Privilégios: Implementar o princípio do menor privilégio é essencial para limitar o impacto de um ataque de *ransomware*. Isso envolve atribuir aos usuários apenas os privilégios necessários para realizar suas funções específicas e restringir o acesso a recursos e dados confidenciais. Ao limitar os privilégios dos usuários, mesmo que uma conta seja comprometida, o acesso do invasor será restrito, dificultando a propagação do *ransomware* pela rede. As organizações devem revisar regularmente os privilégios dos usuários e garantir que apenas os privilégios necessários sejam concedidos (NIST, 2019).

Segmentação de Rede: A segmentação de rede é uma estratégia eficaz para mitigar o impacto de um ataque de *ransomware*, limitando a capacidade do *malware* de se mover lateralmente pela rede. Ao dividir a rede em segmentos isolados e restringir o tráfego entre eles, as organizações podem impedir a propagação do *ransomware* para além do segmento inicialmente comprometido. Isso ajuda a conter o incidente e reduzir o impacto sobre os sistemas críticos. A segmentação de rede deve ser implementada com base em uma análise de riscos para garantir que os

segmentos sejam adequadamente isolados e que as políticas de controle de acesso sejam rigorosamente aplicadas (SANS, 2020).

4.8.2. Medidas de Detecção

Monitoramento de Tráfego de Rede: O monitoramento do tráfego de rede é essencial para detectar atividades suspeitas associadas ao *ransomware*. As organizações devem implementar ferramentas de monitoramento de rede que possam analisar o tráfego em tempo real, identificar padrões incomuns e alertar os administradores sobre possíveis atividades maliciosas. Isso inclui a detecção de comunicações com servidores de comando e controle associados ao *ransomware*, tentativas de acesso não autorizado e transferências de dados suspeitas. O monitoramento contínuo do tráfego de rede pode ajudar as organizações a identificar e interromper ataques de *ransomware* em estágio inicial, minimizando o impacto sobre os sistemas e dados (CIS, 2020).

Análise de Comportamento Anômalo: Implementar soluções de detecção de anomalias é crucial para identificar atividades incomuns que possam indicar a presença de *ransomware*. Essas soluções analisam o comportamento típico do sistema e dos usuários e alertam sobre desvios significativos que possam ser indicativos de um ataque em andamento. Isso inclui padrões de acesso não autorizado, tentativas de modificação de arquivos em massa e atividades de criptografia suspeitas. As organizações devem configurar e ajustar regularmente as soluções de detecção de anomalias para garantir uma cobertura abrangente e minimizar falsos positivos (NIST, 2020).

4.8.3. Resposta a Incidentes

Planos de Resposta a Incidentes: Desenvolver e testar planos de resposta a incidentes específicos para *ransomware* é fundamental para garantir uma resposta rápida e eficaz em caso de infecção. Os planos de resposta a incidentes devem incluir procedimentos detalhados para identificar, isolar, conter e recuperar sistemas afetados pelo *ransomware*. Isso inclui a designação de equipes de resposta, a definição de papéis e responsabilidades, a comunicação com partes interessadas relevantes e a coordenação com autoridades externas, se necessário. Os planos de

resposta a incidentes devem ser revisados regularmente e atualizados para refletir as mudanças no cenário de ameaças e na infraestrutura de TI da organização (NIST, 2018).

4.8.4. Conscientização e Treinamento

Treinamento de Conscientização em Segurança: A educação dos usuários sobre os riscos do *ransomware* e as práticas recomendadas de segurança cibernética é uma parte essencial da estratégia de defesa. Os funcionários devem ser treinados regularmente para reconhecer sinais de atividades suspeitas, como *e-mails* de *phishing*, *downloads* não autorizados e comportamento incomum do sistema. Os programas de treinamento devem abranger tópicos como segurança de senhas, políticas de uso aceitável, reconhecimento de ameaças e procedimentos de relatórios de incidentes. Além disso, os funcionários devem ser incentivados a relatar imediatamente qualquer atividade suspeita à equipe de segurança da informação para uma resposta rápida e eficaz (SANS, 2021).

Simulações de *Phishing*: As simulações de *phishing* são uma maneira eficaz de testar a prontidão dos funcionários em identificar e relatar tentativas de ataque por *e-mail*. As organizações podem realizar exercícios de simulação de *phishing*, enviando *e-mails* falsos aos funcionários que imitam as táticas e técnicas usadas por cibercriminosos. Isso permite que as organizações avaliem a conscientização dos funcionários sobre ameaças de *phishing*, identifiquem áreas de melhoria e forneçam treinamento adicional conforme necessário. As simulações de *phishing* devem ser realizadas regularmente e adaptadas para refletir as últimas tendências e técnicas de *phishing* (CISA, 2021).

4.8.5. Parcerias e Colaborações

Compartilhamento de Inteligência de Ameaças: Participar de comunidades de compartilhamento de informações de segurança é crucial para obter *insights* sobre as últimas ameaças de *ransomware*. As organizações podem colaborar com outras empresas, organizações governamentais e grupos de pesquisa para compartilhar dados de inteligência de ameaças, incluindo indicadores de comprometimento (IoCs), técnicas de ataque e melhores práticas de defesa. O compartilhamento de inteligência

de ameaças permite que as organizações identifiquem e respondam rapidamente a ameaças emergentes, fortalecendo sua postura de segurança cibernética de forma coletiva (FS-ISAC, 2021).

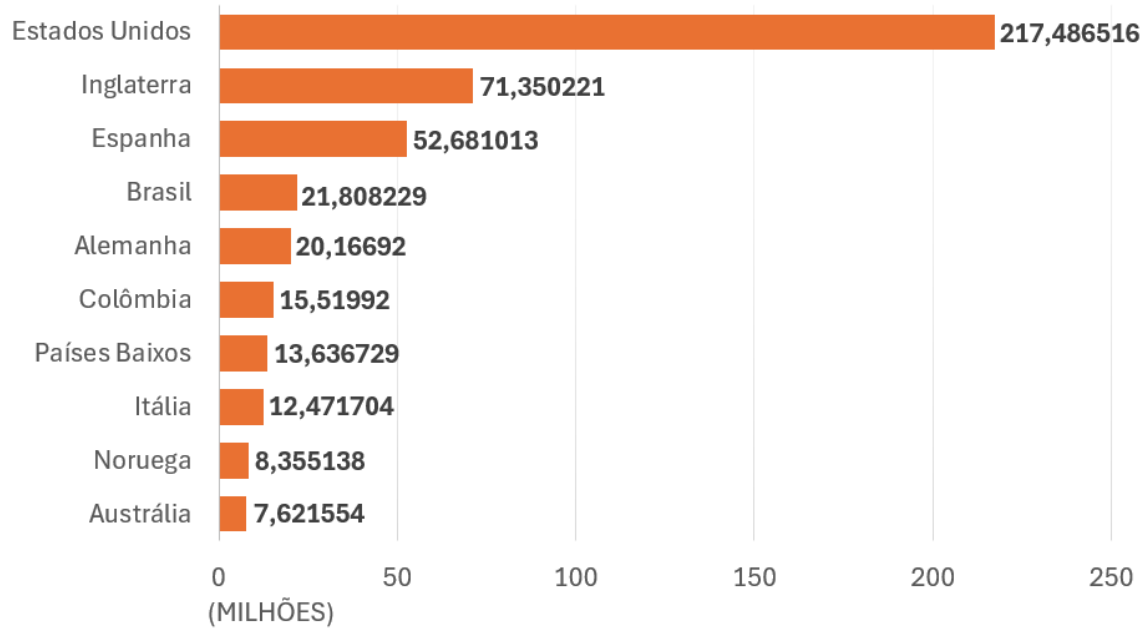
Colaboração com Autoridades e Especialistas: Trabalhar em conjunto com agências de aplicação da lei, especialistas em segurança cibernética e outras partes interessadas é essencial para lidar efetivamente com incidentes de *ransomware*. As organizações devem estabelecer relacionamentos de colaboração com autoridades locais, nacionais e internacionais para relatar incidentes, compartilhar informações e buscar assistência durante investigações e processos de resposta. Além disso, as organizações podem contratar serviços de consultoria especializada em resposta a incidentes para orientação e suporte durante crises de segurança cibernética (FBI, 2020).

5. RESULTADOS

No cenário global de cibersegurança, o Brasil emerge como o quarto maior alvo de *ransomware*, seguindo apenas os EUA, Reino Unido e Espanha, como destacado no "Relatório de Ameaças Cibernéticas 2023" da *SonicWall*. Esse estudo também revela um alarmante aumento de 65% nos ataques direcionados a dispositivos IoT na América Latina. Surpreendentemente, enquanto a incidência de *malware* em geral avançou 17% na região, uma marca substancialmente superior à média global de 2% de crescimento, o *cryptojacking*, por outro lado, registrou uma queda significativa de 66% (SONICWALL, 2023).

Essa tendência contrastante com os dados globais, que mostram um aumento de 43% no *cryptojacking*, aponta para uma dinâmica única no panorama latino-americano de ameaças cibernéticas. O relatório semestral da *SonicWall* também destaca a crescente diversificação dos ataques cibernéticos, evidenciando mudanças nas estratégias dos operadores de ameaças. Conforme visto na figura 3, em 2022, a empresa registrou o segundo maior número de tentativas de ataques de *ransomware* globalmente, além de um impressionante aumento de 87% nos ataques de *malware* de IoT e um recorde de 139,3 milhões de ataques de *cryptojacking* (SONICWALL, 2023).

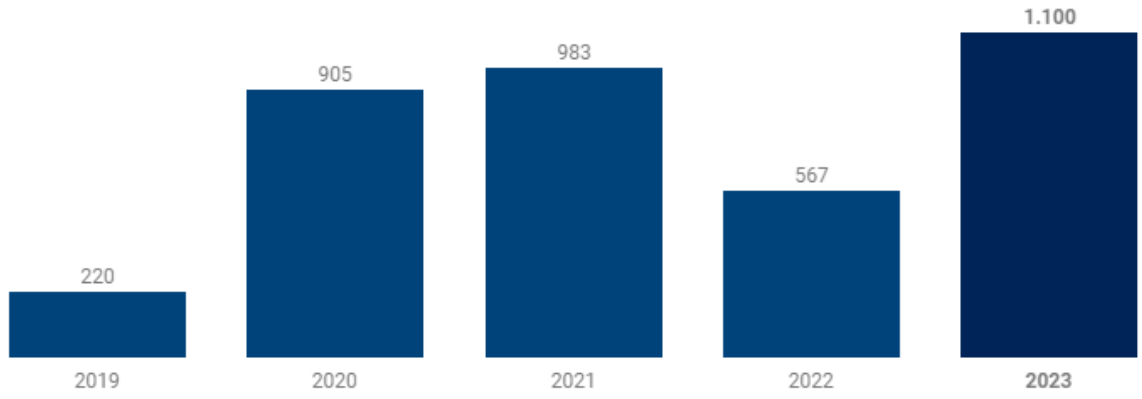
Figura 3 - Top 10 principais países com ataques Ransomware



Fonte: SONICWALL, 2022

Conforme visto na figura 4, em 2023, grupos de *hackers* conseguiram acumular uma quantia impressionante de US$ 1,1 bilhão através de ataques *ransomware*, conforme relatado pela empresa de criptomoedas *Chainalysis*. Essa modalidade de ataque, que paralisa os sistemas de computadores e exige um resgate para a sua liberação, tem se mostrado lucrativa para os criminosos cibernéticos. O montante registrado representa um recorde histórico para esse tipo de crime, quase dobrando o prejuízo causado no ano anterior, que totalizou US$ 567 milhões. Anteriormente, o recorde estava estabelecido em 2021, quando os *hackers* receberam US$ 983 milhões em pagamentos de resgate (CHAINALYSIS, 2023).

Figura 4 - Pagamentos anuais (em US$ milhões) a hackers após ataques ransomware



Fonte: Chainalysis, 2024

6. CONSIDERAÇÕES FINAIS

Este estudo explorou diversas estratégias de prevenção, detecção e resposta a incidentes de *ransomware*, um dos maiores desafios de segurança cibernética contemporâneos. As principais descobertas indicam que uma abordagem multifacetada, combinando medidas técnicas e educacionais, é essencial para mitigar os riscos associados ao *ransomware*.

Entre as principais descobertas, destaca-se a importância de manter sistemas e aplicativos atualizados para corrigir vulnerabilidades que podem ser exploradas por *ransomware*. Implementar políticas de restrição de privilégios e segmentação de rede são medidas eficazes para limitar o impacto de um ataque. Além disso, o monitoramento contínuo do tráfego de rede e a implementação de soluções de detecção de anomalias são cruciais para identificar atividades suspeitas precocemente.

O estudo enfrentou limitações, como a rápida evolução das técnicas de *ransomware*, que pode tornar algumas medidas obsoletas rapidamente. Além disso, a diversidade de ambientes de TI nas organizações pode exigir adaptações específicas das estratégias recomendadas, o que não foi amplamente abordado neste trabalho.

Futuras pesquisas podem focar em desenvolver e testar novas técnicas de inteligência artificial e *machine learning* para a detecção proativa de *ransomware*. Estudos adicionais também são necessários para explorar a eficácia de estratégias colaborativas de defesa, incluindo o compartilhamento de inteligência de ameaças entre organizações. Outra área promissora é a análise do impacto psicológico e comportamental das campanhas de conscientização e treinamento em segurança cibernética.

Este trabalho contribui significativamente para a literatura existente sobre defesa contra *ransomware*, fornecendo uma visão abrangente das melhores práticas e estratégias recomendadas. No entanto, reconhece-se que a constante evolução das ameaças exige um compromisso contínuo com a atualização e adaptação das medidas de segurança. A integração de novas tecnologias e a colaboração entre diferentes setores serão fundamentais para aprimorar a resiliência contra ataques de *ransomware* no futuro.

Assim, espera-se que este estudo sirva como base para melhorias contínuas na proteção contra *ransomware*, estimulando tanto a prática profissional quanto a pesquisa acadêmica a avançar neste campo crucial da segurança cibernética.

REFERÊNCIAS

ANDRONIO, N.; ZHANG, S.; SMITH, M.; KARP, B.; STRINGHINI, G. Understanding the Financial Impact of Ransomware. IEEE Security & Privacy, 2015.

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. NBR 6028: Informação e Documentação - Resumo - Apresentação. Rio de Janeiro: ABNT, 2003.

CIS. Center for Internet Security: Critical Security Controls for Effective Cyber Defense. 2020. Disponível em: https://www.cisecurity.org/controls/cis-controls/. Acesso em: 15 de maio de 2024.

DUNLAP, G.; STALLINGS, R.; COHEN, M. Network Traffic Analysis Techniques for Ransomware Detection. Journal of Cybersecurity, 2017.

ENISA. European Union Agency for Cybersecurity: Ransomware Threat Landscape Report. 2020. Disponível em: https://www.enisa.europa.eu/publications/enisa-ransomware-report. Acesso em: 15 de maio de 2024.

EUROPOL. Internet Organised Crime Threat Assessment (IOCTA). 2019. Disponível em: https://www.europol.europa.eu/iocta-report. Acesso em: 15 de maio de 2024.

FEDOROV, A.; MOROZOV, V.; KOROTKOV, V. User Behavior Analysis for Early Detection of Ransomware. Proceedings of the International Conference on Cyber Security, 2018.

KASPERSKY. The Evolution of Ransomware: From Cryptolocker to WannaCry. 2021. Disponível em: https://www.kaspersky.com/blog/ransomware-evolution/24095/. Acesso em: 15 de maio de 2024.

KHARRAZ, A.; ARSHAD, S.; MUHAMMAD, A.; KIRDA, E. Cutting the Gordian Knot: A Look Under the Hood of Ransomware Attacks. International Conference on Detection of Intrusions and Malware, and Vulnerability Assessment. Springer, 2016.

MULLER, C.; SCHMIDT, F.; MEYER, T. Identifying Unusual Data Traffic Patterns for Ransomware Detection. Journal of Network and Computer Applications, 2018.

NIST. National Institute of Standards and Technology: Cybersecurity Framework. 2018. Disponível em: https://www.nist.gov/cyberframework. Acesso em: 15 de maio de 2024.

NIST. National Institute of Standards and Technology: Guide for Applying the Risk Management Framework to Federal Information Systems. 2019. Disponível em: https://csrc.nist.gov/publications/detail/sp/800-37/rev-2/final. Acesso em: 15 de maio de 2024.

NIST. National Institute of Standards and Technology: Managing Information Security Risk. 2020. Disponível em: https://csrc.nist.gov/publications/detail/sp/800-39/final. Acesso em: 15 de maio de 2024.

REHMAN, R.; ALVI, S.; KHAN, M. Techniques for Monitoring Ransomware Activities: A Comprehensive Review. Journal of Information Security, 2017.

SANS. The SANS Institute: Implementing Network Segmentation for Security. 2020. Disponível em: https://www.sans.org/reading-room/whitepapers/secure/implementing-network-segmentation-security-38180. Acesso em: 15 de maio de 2024.

SOPHOS. The State of Ransomware 2020. 2020. Disponível em: https://www.sophos.com/en-us/medialibrary/PDFs/technical-papers/sophos-the-state-of-ransomware-2020.pdf. Acesso em: 15 de maio de 2024.

SYMANTEC. Internet Security Threat Report. 2018. Disponível em: https://www.symantec.com/security-center/threat-report. Acesso em: 15 de maio de 2024.