



**Universidade Federal de Ouro Preto
Instituto de Ciências Exatas e Aplicadas
Departamento de Computação e Sistemas**

Trabalho de Conclusão de Curso II

Luiz Carlos Silva Júnior

RANSOMWARE: ANÁLISE TÉCNICA E PREVENÇÃO

ORIENTAÇÃO:
Theo Silva Lins

**Agosto, 2023
João Monlevade—MG**

Luiz Carlos Silva Júnior

Trabalho de Conclusão de Curso II

Orientador: Theo Silva Lins

Monografia apresentada ao curso de Sistemas de Informação do Instituto de Ciências Exatas e Aplicadas, da Universidade Federal de Ouro Preto, como requisito parcial para aprovação na Disciplina “Trabalho de Conclusão de Curso II”.

Universidade Federal de Ouro Preto

João Monlevade

Agosto de 2023

SISBIN - SISTEMA DE BIBLIOTECAS E INFORMAÇÃO

S586r Silva Junior, Luiz Carlos.
Ransomware [manuscrito]: análise técnica e prevenção. / Luiz Carlos
Silva Junior. - 2023.
54 f.: il.: color., gráf..

Orientador: Prof. Dr. Theo Silva Lins.
Monografia (Bacharelado). Universidade Federal de Ouro Preto.
Instituto de Ciências Exatas e Aplicadas. Graduação em Sistemas de
Informação .

1. Cibernética - Segurança de sistemas. 2. Computadores - Medidas de
segurança. 3. Criptografia de dados (Computação). 4. Firewalls (Medidas
de segurança para computadores). 5. Malware - Programas de
computador. 6. Proteção de dados. I. Lins, Theo Silva. II. Universidade
Federal de Ouro Preto. III. Título.

CDU 004.056.52/.57

Bibliotecário(a) Responsável: Flavia Reis - CRB6-2431



MINISTÉRIO DA EDUCAÇÃO
UNIVERSIDADE FEDERAL DE OURO PRETO
REITORIA
INSTITUTO DE CIÊNCIAS EXATAS E APLICADAS
DEPARTAMENTO DE COMPUTAÇÃO E SISTEMAS



FOLHA DE APROVAÇÃO

Luiz Carlos Silva Júnior

Ransomware: Análise Técnica e Prevenção

Monografia apresentada ao Curso de Sistemas de Informação da Universidade Federal de Ouro Preto como requisito parcial para obtenção do título de bacharel em Sistemas de Informação

Aprovada em 01 de setembro de 2023

Membros da banca

Doutor - Theo Silva Lins - Orientador - Universidade Federal de Ouro Preto
Doutor - Helen de Cassia Sousa da Costa Lima - Universidade Federal de Ouro Preto
Doutor - Marlon Paolo Lima - Universidade Federal de Ouro Preto

Theo Silva Lins, orientador do trabalho, aprovou a versão final e autorizou seu depósito na Biblioteca Digital de Trabalhos de Conclusão de Curso da UFOP em 15/09/2023



Documento assinado eletronicamente por **Theo Silva Lins, PROFESSOR DE MAGISTERIO SUPERIOR**, em 15/09/2023, às 09:28, conforme horário oficial de Brasília, com fundamento no art. 6º, § 1º, do [Decreto nº 8.539, de 8 de outubro de 2015](#).



A autenticidade deste documento pode ser conferida no site http://sei.ufop.br/sei/controlador_externo.php?acao=documento_conferir&id_orgao_acesso_externo=0, informando o código verificador **0590325** e o código CRC **579828E9**.

Dedico este trabalho de conclusão de curso com profundo carinho e gratidão à minha amada família, cujo amor e apoio inabaláveis me guiaram ao longo dessa jornada. A Deus, fonte inesgotável de força e inspiração, expresso minha eterna gratidão por sua orientação e proteção. Gostaria de fazer uma menção honrosa especial à memória da minha querida avó Augusta e do meu amado irmão Marcelo, cuja presença e sabedoria continuam a iluminar meu caminho, mesmo ausentes fisicamente. Seus legados de amor, determinação e perseverança sempre estarão comigo, motivando-me a superar desafios e alcançar realizações. Que este trabalho seja uma celebração da dedicação, aprendizado que permeiam minha jornada acadêmica e pessoal. A todos que de alguma forma contribuíram para esta trajetória, meu sincero agradecimento.

Agradecimentos

Gostaria de expressar meus sinceros agradecimentos a todos que contribuíram de maneira significativa para a realização deste trabalho de conclusão de curso.

Ao meu orientador Theo Lins, pela orientação valiosa, paciência e dedicação ao longo de todo o processo de pesquisa e desenvolvimento deste trabalho. Sua expertise e apoio foram fundamentais para o sucesso deste projeto.

À Universidade Federal de Ouro Preto, pela oportunidade de aprendizado e crescimento ao longo da minha jornada acadêmica. Agradeço também aos professores que compartilharam seus conhecimentos e experiências, enriquecendo meu aprendizado.

À minha família, que sempre esteve ao meu lado com amor, incentivo e apoio. Seu suporte foi essencial para enfrentar os desafios e conquistar meus objetivos.

À Deus, por guiar meus passos, me conceder saúde e força para superar obstáculos e alcançar realizações.

Que este trabalho seja uma expressão de minha gratidão a todos que fizeram parte dessa jornada. Obrigado!

Resumo

Este estudo apresenta uma análise sobre o funcionamento de ransomware, com o objetivo de compreender suas características, identificar vulnerabilidades nos sistemas operacionais e nos usuários, e propor soluções de prevenção e proteção de dados contra as ameaças deste malware. Para isso, foi desenvolvido um ambiente de testes seguro e controlado, onde foram simulados ataques de ransomware em diferentes sistemas operacionais e dispositivos. Os principais algoritmos e técnicas utilizados pelo ransomware, como criptografia Fernet, foram incorporados para compreender seu funcionamento e impacto. A eficácia das soluções propostas a nível de rede, como firewalls, sistemas de detecção de intrusões e políticas de acesso restrito, foi validada por meio de testes e análises. O comportamento do ransomware foi analisado, levando em consideração variações nos tipos de ataques, alvos e condições de segurança. Embora este estudo se concentre principalmente na prevenção de ataques de ransomware, entender a importância de estudar os ataques de negação de serviço distribuído também é relevante no contexto da segurança cibernética, pois este ataque representa uma ameaça que pode interromper significativamente a disponibilidade de serviços online e está sendo usado cada vez mais em conjunto com outras ameaças, como o ransomware. Identificou-se as principais vulnerabilidades dos sistemas operacionais e dos usuários que podem ser exploradas pelo ransomware, fornecendo orientações para aprimorar a segurança cibernética, incluindo técnicas de utilização de iptables para bloqueio de portas de entrada no Linux e reforçando medidas de segurança no Windows, incluindo o uso do firewall. Os resultados destacam a importância de implementar medidas de segurança robustas para prevenir e atenuar os riscos do ransomware. Conclui-se que a combinação de abordagens teóricas embasadas em revisões bibliográficas e experimentos práticos é fundamental para oferecer uma visão abrangente do tema e contribuir para o desenvolvimento de estratégias efetivas de defesa contra o ransomware.

Palavras-chaves: ransomware, segurança cibernética, criptografia, iptables, firewall.

Abstract

This study presents an analysis of ransomware operation with the aim of understanding its characteristics, identifying vulnerabilities in operating systems and users, and proposing prevention and data protection solutions against the threats posed by this malware. To achieve this, a secure and controlled testing environment was developed, where ransomware attacks were simulated on different operating systems and devices. The primary algorithms and techniques used by ransomware, such as Fernet encryption, were incorporated to comprehend its functioning and impact. The effectiveness of the proposed network-level solutions, such as firewalls, intrusion detection systems, and restricted access policies, was validated through testing and analysis. The behavior of ransomware was analyzed, considering variations in the types of attacks, targets, and security conditions. While this study primarily focuses on preventing ransomware attacks, understanding the importance of studying distributed denial of service (DDoS) attacks is also relevant in the cybersecurity context, as DDoS attacks can significantly disrupt online service availability and are increasingly used in conjunction with other threats, such as ransomware. The study identified the main vulnerabilities in operating systems and users that ransomware can exploit, providing guidance to enhance cybersecurity, including the use of iptables techniques for blocking entry ports on Linux and strengthening security measures on Windows, including firewall usage. The results underscore the importance of implementing robust security measures to prevent and mitigate ransomware risks. It is concluded that the combination of theory-based approaches grounded in literature reviews and practical experiments is essential to provide a comprehensive understanding of the subject and contribute to the development of effective defense strategies against ransomware.

Key-words: Ransomware, cyber security, encryption, iptables, firewall.

Lista de ilustrações

Figura 1 – Hierarquia de botnets em ataques DDoS	21
Figura 2 – Número de ataques do Ransomware WannaCry em 2017	22
Figura 3 – Mensagem de resgate da família de Ransomware WannaCry	23
Figura 4 – Escolaridade dos participantes	30
Figura 5 – Faixa etária dos participantes	31
Figura 6 – Experiência em computadores	31
Figura 7 – Frequência do uso Internet	32
Figura 8 – Dispositivos conectados à Internet	32
Figura 9 – Backup	33
Figura 10 – Utilização de antivírus	34
Figura 11 – Ransomware o que é	34
Figura 12 – Configuração Disponibilizada para Máquina Virtual	35
Figura 13 – O arquivo txt contém o seguinte texto: Lorem ipsum	36
Figura 14 – Arquivo txt, completamente criptografado pelo ransomware, impossibi- litado de ler os texto original	36
Figura 15 – Descriptografando dados da pasta	37
Figura 16 – Mensagem enviando pedido HTTP GET para URL	39
Figura 17 – Vulnerabilidade explorada	40
Figura 18 – Instalando iptables	42
Figura 19 – Bloqueando tráfego nas portas 445 (SMB) e 135 (RPC)	42
Figura 20 – Bloqueio de tráfego excessivo nas portas 80 (HTTP) e 22 (SSH)	43
Figura 21 – Criando a regra para salvar as alterações no iptables.	43
Figura 22 – Acessando o Firewall	44
Figura 23 – Portas à Serem Bloqueadas	45
Figura 24 – Regra Criada TESTE1TCC	45
Figura 25 – Ferramenta de Remoção de Software Mal-intencionado do Windows x64 - v5.113.	46
Figura 26 – Microsoft Defender Antivírus(verificação offline)	47
Figura 27 – Manter Todas Proteções Ativas	47
Figura 28 – Verificação Completa do Antivírus Para Varredura	48
Figura 29 – Desabilitando execução de macros que não são de fonte confiáveis	49
Figura 30 – Controle de Conta de Usuário	49
Figura 31 – Acessando o Programas e Recursos	50
Figura 32 – Desativando o Suporte Para o Protocolo de Compartilhamento de Arquivos SMB 1.0/CIFS	50
Figura 33 – Verificação Se Há Algum Tráfego Indesejado À Ser Bloqueado	51

Lista de abreviaturas e siglas

3DES - Triple Data Encryption Standard

AES - Advanced Encryption Standard

Crypto - Criptografia

DDoS - Distributed Denial of Service

HTTP - Hypertext Transfer Protocol

HTTPS - Hypertext Transfer Protocol Secure

IP - Internet Protocol

Py - Python

RSA - Rivest, Shamir e Adleman

RPC - Remote Procedure Call Port

SMB - Server Message Block Port

SSH - Secure Shell Port

TCP - Transmission Control Protocol

UDP - User Datagram Protocol

UAC - Controle de Conta de Usuário

URL - Uniform Resource Locator

WCry - WannaCry

Sumário

1	INTRODUÇÃO	12
1.1	Problema de pesquisa	12
1.2	Objetivos	13
1.3	Metodologia	14
1.4	Organização do trabalho	14
2	REVISÃO BIBLIOGRÁFICA	15
2.1	Ransomware	15
2.1.1	História	15
2.1.2	Tipos	16
2.2	Abordagens de Ataque	17
2.3	Métodos de Criptografia	17
2.4	Técnicas e Códigos Maliciosos Utilizados	18
2.5	Ataques Mais Famosos	21
2.6	Normas de Segurança Cibernética	26
2.7	Iptables: Visão Geral	27
2.8	Trabalhos Relacionados	27
3	ESTUDO E ANÁLISE DO RANSOMWARE	29
3.1	Pesquisa: Conscientização e Medidas de Segurança Cibernética em Usuários de Dispositivos Conectados à Internet	29
3.2	Ambiente dos Testes	35
3.3	Ransomware	35
3.4	Negação de serviço distribuída	37
3.5	WannaCry	39
4	SOLUÇÕES PROPOSTAS	41
4.1	Utilização do Iptables para Bloqueio de Portas de Entrada e Prevenção de Ataques WannaCry e DDoS:	41
4.1.1	Utilização do Iptables no Ubuntu	41
4.2	Firewall do Windows	43
4.3	Reforçando a Segurança no Windows	46
4.4	Normas de Segurança da Informação: Orientações para Proteção	51
5	CONCLUSÃO	52
5.1	Limitações e Trabalhos Futuros	52

5.1.1	Limitações do Trabalho Atual	53
5.1.2	Sugestões de Trabalhos Futuros	53

REFERÊNCIAS	54
------------------------------	-----------

1 Introdução

O estudo da segurança cibernética desempenha um papel fundamental na proteção de indivíduos, empresas e instituições em um mundo cada vez mais conectado digitalmente, é de grande importância compreender e diminuir os riscos associados à segurança da informação. O estudo da segurança cibernética permite a identificação e análise de vulnerabilidades em sistemas e redes, além de fornecer as habilidades necessárias para desenvolver estratégias de defesa eficazes.

O termo ransomware representa uma grande ameaça real nos dias de hoje para seu dispositivo, e seus dados, podendo bloquear arquivos e exigir um resgate para desbloqueá-los. Este trabalho propõe realizar uma análise sobre o funcionamento de ransomware, identificando e diferenciando versões desse malware e propõe soluções para prevenir ou atenuar possíveis danos causados por essa ameaça.

O ransomware tem evoluído rapidamente como uma tática de ataque, direcionando cada vez mais alvos estratégicos, incluindo empresas de grande porte e infraestruturas críticas. Isso pode resultar em danos significativos e sem precedentes. Em 2020, houve um aumento significativo nos ataques devido à transição para o trabalho remoto, destacando a urgência de implementar medidas de segurança eficazes. É crucial alertar a sociedade sobre a crescente complexidade do ransomware e a dificuldade de combatê-lo. Isso ressalta a importância de adotar práticas de segurança.

1.1 Problema de pesquisa

Os problemas de segurança cibernética relacionados ao ransomware e suas variações são uma preocupação crescente na atualidade. O ransomware, como uma forma de malware que criptografa os arquivos de um sistema e exige um resgate para a sua liberação, pode causar danos significativos às organizações e indivíduos. Além disso, existem diferentes tipos de variações de ransomware, como ransomware criptográfico, locker, scareware e doxware, cada um com suas próprias características e métodos de infecção. Essa diversidade de ataques coloca em evidência a necessidade de estar constantemente atualizado sobre as novas variantes de ransomware e implementar medidas de segurança para proteger-se contra essas ameaças.

O estudo e compreensão do tema dos ransomwares e dos problemas de segurança cibernética associados a eles, assim como o avanço tecnológico e a crescente dependência de sistemas computacionais tornam as organizações e indivíduos mais vulneráveis a ataques cibernéticos, incluindo o ransomware. Ao estudar o assunto, é possível adquirir

conhecimento sobre as técnicas e os métodos utilizados pelos cibercriminosos, bem como identificar vulnerabilidades e implementar estratégias eficazes de prevenção e resposta a ataques. Além disso, o estudo sobre segurança cibernética e ransomware permite entender as melhores práticas e soluções disponíveis para fortalecer a proteção dos sistemas e minimizar o impacto causado por essas ameaças. Portanto, investir em educação e conscientização sobre segurança cibernética é fundamental para manter a integridade dos dados e garantir a continuidade das operações em um ambiente digital cada vez mais complexo e ameaçador.

1.2 Objetivos

O objetivo geral deste trabalho é realizar uma análise técnica e prevenção sobre o funcionamento de ransomware. Visando compreender as características do ransomware, bem como identificar as vulnerabilidades dos sistemas operacionais e dos usuários que podem ser exploradas por esses ataques. Será proposto soluções a nível de rede para atenuar os riscos e proteger os dados contra as ameaças desse malware.

Este trabalho possui os seguintes objetivos específicos:

- Realizar uma análise das principais abordagens e estratégias de segurança cibernética, investigando suas aplicações com foco na prevenção e resposta a ataques de ransomware.
- Conduzir uma pesquisa sobre conscientização e medidas de segurança cibernética em usuários de dispositivos conectados à internet, explorando a compreensão, percepção e adoção de práticas de segurança, visando identificar lacunas de educação e proteção.
- Compreender criptografia de arquivos vindas de ataques ransomware, a fim de identificar seu funcionamento e impacto.
- Propor soluções em rede de Internet, como firewalls e políticas de acesso restrito, por meio de testes e análises.
- Analisar o comportamento e funcionamento do ransomware, levando em consideração variações nos tipos de ataques, alvos e condições de segurança.

Ao atingir esses objetivos, busca-se contribuir para o avanço do conhecimento na área de segurança cibernética, oferecendo subsídios para o desenvolvimento de estratégias efetivas de defesa e prevenção contra ransomware. O presente trabalho combina uma abordagem teórica embasada em revisões bibliográficas e experimentos práticos, proporcionando uma visão abrangente do tema.

1.3 Metodologia

O estudo adota uma metodologia para estudar o ransomware, testando as técnicas de códigos exemplos simples para simular esse tipo de malware. Os passos para execução deste estudo são definidos em diferentes etapas. A revisão da literatura é realizada para explorar o estado atual do conhecimento sobre o tema, compreender as técnicas de criptografia e os tipos de ataques mais comuns. Em seguida, o estudo e análise do ransomware envolve uma pesquisa sobre conscientização e medidas de segurança cibernética em usuários de dispositivos conectados a internet, a criação de um ambiente de testes e a execução de experimentos para analisar o comportamento do ransomware e suas variantes. As soluções propostas visam oferecer medidas de segurança para prevenir ataques cibernéticos de ransomware. Por fim, a análise e discussão dos resultados obtidos permite identificar as principais descobertas, destacando os pontos críticos da segurança cibernética relacionados ao ransomware. Essa abordagem metodológica visa contribuir para o avanço do conhecimento na área e fornecer subsídios para o desenvolvimento de estratégias efetivas de defesa e prevenção contra esse tipo de ameaça.

1.4 Organização do trabalho

Quanto à estrutura do trabalho, ele está organizado da seguinte forma: No capítulo 2 temos a revisão da literatura onde aborda os principais conceitos, técnicas e estudos relacionados ao ransomware e à segurança cibernética. O capítulo 3 descreve detalhadamente os passos seguidos para a realização do estudo, incluindo os experimentos, testes e análises realizadas. No capítulo 4 são apresentados e discutidos na seção de análise e discussão, destacando as principais descobertas. Por fim, o capítulo 5 enfatiza a importância do estudo e sugere possíveis direções para pesquisas futuras.

2 Revisão bibliográfica

A análise bibliográfica abordada neste estudo compreendeu uma investigação sobre ransomware, explorando suas diferentes variantes, peculiaridades, técnicas de ataque, normas de segurança e abordagens empregadas por essas ameaças cibernéticas. Além disso, foram examinados os elementos e características distintivas do ransomware com o objetivo de obter uma compreensão completa das ameaças cibernéticas mais relevantes nos dias atuais. Por meio dessa análise, buscou-se fornecer uma base para o estudo da prevenção, detecção e mitigação de ameaças ransomware, contribuindo para o desenvolvimento de estratégias eficazes de defesa contra essas crescentes ameaças.

2.1 Ransomware

O ransomware é um tipo de malware que criptografa os dados do sistema ou bloqueia o acesso aos arquivos de um usuário, exigindo o pagamento de um resgate em moeda virtual para restaurar o acesso aos dados. Esse tipo de ataque, amplamente estudado por especialistas em segurança cibernética, tornou-se uma das principais ameaças à segurança digital. Geralmente, o pagamento é solicitado em criptomoedas, como o Bitcoin, dificultando o rastreamento da identidade do autor do ataque.

2.1.1 História

O ransomware tem uma história que remonta aos primórdios da era da internet e evoluiu ao longo do tempo para se tornar uma das ameaças cibernéticas mais persistentes e lucrativas. Esta ameaça surgiu no final da década de 1980, mas realmente se tornou algo relevante após 2005. Isto ocorreu devido às mudanças tecnológicas que aconteceram nesta época ([SAVAGE](#); [COOGAN](#); [LAU](#), 2015). Um dos primeiros casos conhecidos é o ransomware AIDS Trojan, que apareceu em 1989 e se espalhava por meio de disquetes compartilhados. No entanto, foi no início dos anos 2000 que o ransomware começou a se tornar uma ameaça mais prevalente, com o advento de métodos de pagamento online e a maior sofisticação dos ataques. O famoso ransomware CryptoLocker, que surgiu em 2013, foi um marco importante, pois introduziu a criptografia como uma forma eficaz de bloquear o acesso a arquivos. Desde então, várias variantes e modificações de ransomware surgiram, cada uma com suas próprias táticas e alvos. Essa evolução contínua demonstra a adaptabilidade e a rentabilidade do ransomware, tornando-o uma preocupação constante para indivíduos e organizações em todo o mundo.

2.1.2 Tipos

- **Ransomware Criptográfico:** esse tipo de ransomware utiliza algoritmos de criptografia para bloquear arquivos e dados importantes da vítima, tornando-os inacessíveis. Normalmente, exige-se um resgate em criptomoedas para fornecer a chave de descriptografia. Metodologia: o ransomware criptográfico se espalha por meio de anexos de e-mail maliciosos, links infectados, downloads de software comprometido ou exploração de vulnerabilidades em sistemas. Uma vez dentro do sistema, ele criptografa os arquivos identificados e exibe uma mensagem de resgate, fornecendo instruções para o pagamento ([CONTROLENET, 2021](#)).
- **Ransomware Locker:** nesse tipo de ataque, o ransomware impede o acesso ao sistema infectado, bloqueando a área de trabalho e impedindo que a vítima utilize o computador. Ele não criptografa os arquivos, mas limita o acesso ao sistema operacional. Metodologia: o ransomware locker costuma ser distribuído por meio de anexos de e-mail infectados, downloads maliciosos ou explorando vulnerabilidades em sistemas desatualizados. Ao infectar o sistema, ele exibe uma tela de bloqueio com uma mensagem exigindo o pagamento de resgate para liberar o acesso ao sistema ([CONTROLENET, 2021](#)).
- **Ransomware Scareware:** o ransomware scareware utiliza táticas de intimidação para enganar as vítimas, apresentando falsos alertas ou notificações de segurança para fazê-las acreditar que o sistema está comprometido. Ele induz as vítimas a pagar um resgate por uma suposta solução de segurança. Metodologia: esse tipo de ransomware normalmente é disseminado por meio de anúncios enganosos, sites comprometidos ou downloads de software falsos. Ele exibe alertas falsos, como supostas infecções por malware, e instrui as vítimas a pagar por uma ferramenta de remoção de malware falsa ([CONTROLENET, 2021](#)).
- **Ransomware Doxware:** também conhecido como leakware ou extortionware, o ransomware doxware ameaça publicar ou divulgar informações confidenciais da vítima, como dados pessoais, documentos sensíveis ou imagens comprometedoras, a menos que um resgate seja pago. Metodologia: esse tipo de ransomware geralmente é distribuído por meio de links maliciosos, anexos de e-mail infectados ou exploração de vulnerabilidades. Após a infecção, ele coleta dados confidenciais e exibe uma mensagem de ameaça, exigindo pagamento para evitar a divulgação dessas informações ([CONTROLENET, 2021](#)).

2.2 Abordagens de Ataque

Com essa criação e distribuição em massa de novos Ransomwares, ficou evidente que os sistemas atuais estão altamente vulneráveis e, na maioria das vezes, isso ocorre ou pode ocorrer pela falta de conhecimento das pessoas/usuários que utilizam o mundo digital ([ZAGHETTO, 2017](#)). Qualquer sistema, de dispositivos Android a sistemas iOS ou Windows, está sujeito aos riscos impostos por esse tipo de exploração de falhas por meio de Ransomware. Conforme o alvo, o método de comprometimento do dispositivo pode ser diferente e as ações finais serão limitadas pela própria capacidade do dispositivo, mas há também padrões reconhecíveis seguidos por muitos extorsionários ([LISKA; GALLO, 2016](#)).

- Sites de Doxxing corporativo, nesse caso, os cibercriminosos, munidos de dados corporativos e pessoais, os expõem progressivamente em sites específicos a fim de coagir as vítimas, condicionando o fim da exposição ao pagamento do resgate ([FLASHPOINT, 2021](#)).
- Leilões de venda de dados, dependendo do valor das informações, os cibercriminosos podem escolher por vendê-los em leilões de venda online de dados para também garantir que o esforço do ataque seja financeiramente recompensado, caso não lhes seja depositado o resgate. Já ocorreram na história leilões onde foram negociados dados de vítimas de alto status social, como Lady Gaga, Madonna e Donald Trump ([FLASHPOINT, 2021](#)).
- Contato direto e mídia, contra organizações corporativas, os criminosos podem contactar partes interessadas como fornecedores, acionistas, clientes e também jornalistas e mídia especializada para cobrir e expor o ataque, coagindo os executivos a pagar o valor de resgate ([FLASHPOINT, 2021](#)).
- Scareware dentre os existentes, é o menos perigoso. Eles são softwares maliciosos que aparecem inicialmente como avisos – geralmente apelando para nomes de softwares de segurança e antivírus legítimos –, que pedem pagamentos em troca de uma suposta desinfecção. Ele é a porta de entrada para ransomwares mais perigosos que podem bloquear todo o sistema ([4INFRA, 2020](#)).

2.3 Métodos de Criptografia

- AES (Advanced Encryption Standard): o AES é um algoritmo de criptografia simétrica amplamente adotado em todo o mundo. Ele foi selecionado pelo Instituto Nacional de Padrões e Tecnologia (NIST) dos Estados Unidos como um substituto para o antigo padrão de criptografia DES (Data Encryption Standard). O AES opera

em blocos de dados e possui tamanhos de chave de 128, 192 e 256 bits, oferecendo segurança e eficiência em suas operações criptográficas ([DAEMEN; RIJMEN, 2002](#)).

- Fernet: o Fernet é um esquema de criptografia simétrica que utiliza o algoritmo AES em modo de operação CBC (Cipher Block Chaining). Ele é amplamente utilizado em bibliotecas e frameworks Python para proteger informações sensíveis, como tokens de autenticação e chaves de acesso. O Fernet é fácil de implementar e garante autenticação e integridade dos dados criptografados ([FERRIE, 2018](#)).
- O RSA é um algoritmo de criptografia assimétrica muito conhecido, utilizado para criptografia de chaves públicas e assinaturas digitais. Ele se baseia na dificuldade de fatorar grandes números inteiros, tornando a chave privada (fatores primos) difícil de ser determinada a partir da chave pública. O RSA é amplamente utilizado para garantir a troca segura de chaves e a autenticação de entidades em redes públicas ([RIVEST; SHAMIR; ADLEMAN, 1978](#)).
- O Blowfish é um algoritmo de criptografia simétrica criado por Bruce Schneier em 1993. Ele é um algoritmo de chave variável, o que significa que ele pode aceitar chaves de tamanhos variados (de 32 bits a 448 bits). O Blowfish é rápido e eficiente, sendo utilizado em diversos sistemas e aplicativos para proteção de dados ([SCHNEIER, 1994](#)).
- 3DES (Triple Data Encryption Standard): o 3DES é uma versão aprimorada do algoritmo DES (Data Encryption Standard). Ele utiliza três vezes a aplicação do DES, com chaves diferentes, para fornecer maior segurança e uma chave de 168 bits. O 3DES é amplamente utilizado em aplicações legadas e em cenários que requerem maior segurança do que o DES ([National Institute of Standards and Technology \(NIST\), 2001](#)).
- O Serpent é um algoritmo de criptografia simétrica projetado em uma competição realizada em 1997 para encontrar uma substituição segura para o DES. O Serpent é conhecido por sua estrutura matemática sólida e complexidade, o que torna sua implementação eficiente em hardware. Ele é considerado uma das melhores opções para proteger dados sensíveis ([ANDERSON; BIHAM; KNUDSEN, 1998](#)).

2.4 Técnicas e Códigos Maliciosos Utilizados

- Phishing: é um ataque em que os cibercriminosos enganam as pessoas, levando-as a compartilhar informações confidenciais, como senhas e números de cartões de crédito. Esses golpistas utilizam táticas astutas para atrair suas vítimas, sendo o envio de e-mails ou mensagens de texto falsos uma das abordagens mais comuns. Eles se

passam por pessoas ou organizações em quem as vítimas confiam, como colegas de trabalho, bancos ou órgãos governamentais. Ao abrir o e-mail ou mensagem, as vítimas são confrontadas com uma mensagem alarmante que as assusta e induz a agir impulsivamente, ignorando o bom senso, a fim de evitar alguma consequência negativa. A mensagem exige que a vítima acesse um site e tome uma ação imediata ou corra o risco de sofrer algum tipo de dano ([MALWAREBYTES, 2021](#)).

- **Exploits de Software:** exploits são programas ou códigos desenvolvidos para explorar falhas de segurança em software e causar efeitos indesejados. Em um computador ou rede, as vulnerabilidades representam janelas abertas pelas quais os hackers podem instalar softwares maliciosos e obter controle sobre o sistema, com intenções maliciosas e sem o conhecimento do usuário. Esse controle permite que o sistema seja infectado e utilizado para fins ilícitos ([AVAST, 2022](#)).
- **Kits de Exploração:** as explorações costumam ser a etapa inicial de ataques mais complexos. Os hackers buscam por sistemas desatualizados que possuem vulnerabilidades críticas, que são exploradas para implantar malware direcionado. Essas explorações geralmente incluem o shellcode, uma pequena carga de malware utilizada para baixar malware adicional de redes controladas pelos invasores. O shellcode possibilita que os hackers infectem dispositivos e se infiltrem em organizações. Os kits de exploração são ferramentas abrangentes que englobam uma coleção de explorações. Esses kits verificam dispositivos em busca de diferentes tipos de vulnerabilidades de software e, quando encontradas, implantam malware adicional para infectar ainda mais o dispositivo. Os kits podem utilizar explorações direcionadas a diversos softwares, como Adobe Flash Player, Adobe Reader, Internet Explorer, Oracle Java e Sun Java. Essas técnicas permitem que os hackers realizem ataques mais sofisticados e tirem proveito de vulnerabilidades presentes em diferentes sistemas e aplicativos ([DANSIMP, 2023](#)).
- **Engenharia Social:** a engenharia social é uma estratégia utilizada por cibercriminosos para manipular e enganar usuários desavisados, levando-os a divulgar dados confidenciais, infectar seus computadores com malware ou abrir links para sites contaminados. Nesse tipo de abordagem, os hackers exploram a falta de conhecimento e conscientização dos usuários sobre segurança cibernética. Com a rápida evolução da tecnologia, muitos clientes e funcionários podem não compreender completamente o verdadeiro valor de seus dados pessoais e, conseqüentemente, não estão cientes das medidas adequadas para proteger suas informações. Isso torna as pessoas suscetíveis a ataques de engenharia social, onde os criminosos se aproveitam da falta de conhecimento para obter acesso a informações sensíveis de maneira ilícita ([KAPERSKY, 2023](#)).
- **Serviços de Ransomware como Serviço (RaaS):** é um modelo de negócios que trans-

forma o malware de sequestro de dados em um serviço, também conhecido como kit de ransomware. Esse modelo de comercialização tem impulsionado a disseminação e entrega crescente de ameaças ransomware. O RaaS funciona através de transações entre os operadores de ransomware e afiliados, que são pessoas ou organizações que pagam para lançar ataques. Esses ataques são relativamente fáceis de serem realizados por grupos especializados em cibercrime, conhecidos como gangues digitais. Com baixo custo de operação, o RaaS possibilita golpes bem-sucedidos em organizações de todos os tamanhos e setores. Os kits de RaaS são encontrados na *dark web*, uma parte oculta da internet que garante o anonimato tanto para quem oferece o serviço quanto para quem contrata (PROLINX, 2023).

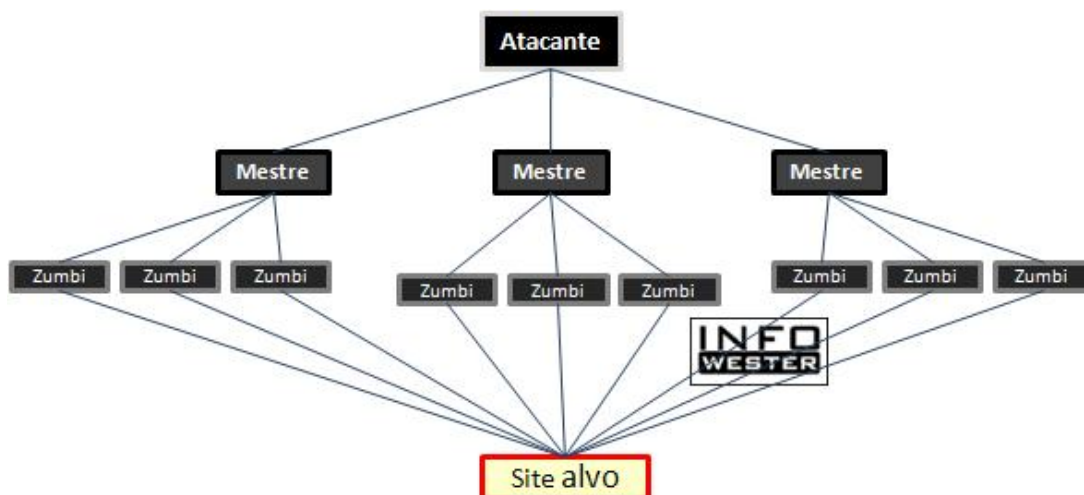
- DDoS no livro do autor Stallings e Brown (2017), o ataque de negação de serviço distribuído (DDoS) é abordado como uma forma de ataque cibernético que tem como objetivo sobrecarregar um serviço ou recurso específico de uma vítima, tornando-o inacessível para os usuários legítimos. Os autores explicam que o ataque DDoS é realizado através da coordenação de um grande número de dispositivos conectados em rede, muitas vezes pertencentes a botnets - redes de computadores zumbis controlados remotamente por um atacante.

Os ataques DDoS são frequentemente usados para prejudicar a disponibilidade e a estabilidade de serviços online, causando prejuízos financeiros e afetando a reputação das vítimas. Os atacantes podem utilizar diferentes técnicas e estratégias para executar um DDoS, explorando vulnerabilidades em protocolos de rede, explorando falhas em aplicativos ou até mesmo combinando múltiplos ataques de diferentes origens (STALLINGS; BROWN, 2017).

Os ataques DDoS podem ser classificados em diferentes tipos, como ataques de volume, que visam sobrecarregar a largura de banda do servidor, ataques de exaustão de recursos, que exploram vulnerabilidades nos serviços do servidor, e ataques de camada de aplicação, que alvejam aplicativos específicos para esgotar recursos do servidor.

Uma forma de ataque bastante comum faz uso de botnets mostrado na figura 1, em poucas palavras, um tipo de rede formada por computadores infectados que pode ser controlada remotamente pelo atacante. Assim, os computadores que a compõem passam a trabalhar da já mencionada maneira escravizada.

Figura 1 – Hierarquia de botnets em ataques DDoS



Fonte: (ALECRIM, 2004)

Nesta forma de ataque, é comum o uso de computadores domésticos, já que estes são maioria e, muitas vezes, não são devidamente protegidos. Assim, é mais fácil infectá-los com um malware que possui instruções para fazer com que a máquina participe de um ataque DDoS.

Quando o computador passa a fazer parte de uma botnet, esta máquina pode ser chamado de zumbi. Após a contaminação, os zumbis podem entrar em contato com máquinas mestres, que por sua vez recebem orientações (quando, em qual site/computador, tipo de ataque, entre outros) de um computador atacante ou líder.

Um computador mestre pode ter sob sua responsabilidade até milhares de computadores. Nestes casos, as tarefas de ataque DoS são distribuídas a um exército de máquinas escravizadas, fazendo jus ao nome Distributed Denial of Service (Negação de Serviço Distribuído). Uma vez infectados, os computadores passam a executar as ordens que recebem, como enviar constantemente pacotes de dados a um determinado servidor até que este não consiga mais responder a tantas requisições. Para tornar o ataque ainda mais eficiente, várias técnicas podem ser utilizadas. Em uma delas, o IP de origem dos pacotes utilizados é alterado para uma sequência falsa, dificultando a descoberta da origem da ação (ALECRIM, 2004).

2.5 Ataques Mais Famosos

- WannaCry ou WCry ou WanaCrypt0r é o crypto-ransomware mais famoso mundialmente, por ter sido utilizado no ataque de maior rede infecciosa da história, conhecido como O ataque do ransomware WannaCry, ocorrido em maio de 2017. Ele

infecta os sistemas operacionais Microsoft Windows desatualizados, sequestrando os arquivos do usuário, que seriam liberados apenas após pagamento de resgate em bitcoins. Foi utilizado em larga escala contra organizações tanto públicas ou privadas, como empresas de telecomunicações e organizações governamentais, mas também contra computadores pessoais (CRUZ, 2017).

O ataque WannaCry ficou conhecido por sua rápida disseminação e impacto massivo em todo o mundo. Esse ataque cibernético começou a se propagar em 12 de maio de 2017 e se espalhou por mais de 150 países em apenas alguns dias. se espalhou rapidamente e afetou principalmente sistemas operacionais Windows. Ele explorou uma vulnerabilidade conhecida do Windows chamada EternalBlue, que havia sido desenvolvida pela Agência de Segurança Nacional dos Estados Unidos (NSA) e posteriormente vazada publicamente por um grupo chamado Shadow Brokers.

O Ransomware WannaCry teve sua grande aparição em 12 de maio de 2017 em um grandioso ataque que se espalhou e infectou em primeiro momento 45 mil máquinas em 11 países, mas como ninguém estava preparado para tal ataque, ele continuou a se propagar, no qual em 17 de maio de 2017 ele já tinha infectado 345 mil máquinas em mais de 150 países, assim como mostra a a figura 2 a seguir (PROOF, 2017).

Figura 2 – Número de ataques do Ransomware WannaCry em 2017



Fonte: (PROOF, 2017)

Essa imagem é um lembrete das consequências que um ataque de ransomware pode ter e da necessidade crítica de estar preparado para enfrentar tais ameaças. O

WannaCry serviu como um alerta sobre a importância de medidas de segurança cibernética robustas e da colaboração global para combater ameaças cibernéticas em escala global.

O Ransomware utiliza-se de criptografia do tipo assimétrica. De acordo com (BERRY; HOMAN; EITZMAN, 2017), o mesmo se utiliza de uma lista de chaves do tipo Rivest-Shamir Adleman (RSA) para realizar a encriptação dos dados e arquivos da vítima, sendo que esta lista possui chaves públicas e genéricas.

A rápida propagação e o impacto do WannaCry chamaram a atenção da mídia e da comunidade de segurança cibernética em todo o mundo. Esforços de respostas de prevenção foram realizados para conter a disseminação do ransomware e fornecer soluções para descriptografar os arquivos afetados sem pagar o resgate.

A mensagem de resgate da família de ransomware WannaCry na figura 3 é uma representação desse ataque cibernético que ocorreu em maio de 2017. A imagem geralmente mostra um fundo vermelho ou preto com texto branco, informando às vítimas que seus arquivos foram criptografados e que eles precisam pagar um resgate em criptomoeda para recuperá-los.

Figura 3 – Mensagem de resgate da família de Ransomware WannaCry



Fonte: (OLIVEIRA, 2018)

Essa imagem foi amplamente divulgada na mídia e tornou-se um símbolo dos ataques de ransomware em escala global. Ela ilustra de forma clara e direta a natureza do

ataque, em que os atacantes impõem um prazo limitado para o pagamento do resgate, propagando pânico e urgência nas vítimas.

- BadRabbit é um crypto-ransomware que infecta a partir de uma falsa requisição de atualização do Adobe Flash, confirmada pela vítima no momento que permite a instalação, encontrada principalmente em sites de notícias comprometidos. Uma vez dentro do computador hospedeiro, o cibercriminoso tem acesso a credenciais do usuário que o possibilitam disseminar a infecção para toda rede local nativa do computador. Após isso os arquivos são encriptados e é exigido um resgate em bitcoins no qual os valores progridem conforme o prazo de pagamento atual expira ([KASPERSKY, 2017](#)).
- Cerber é um crypto-ransomware oferecido como Ransomware-as-a-service ou Ransomware como serviço. Nesse modelo de negócio, o software é cedido pelo desenvolvedor para utilização de outros cibercriminosos, dos quais exige-se comissões dos resgates bem-sucedidos. É difundido pela disseminação de arquivos maliciosos anexados em correspondências de e-mail que quando abertos infectam a máquina e conectam-se a um site malicioso, de onde é instalado o ransomware em si. Após a infecção os arquivos são encriptados e uma nota de resgate será exibida para a vítima. Os valores também progridem conforme o prazo de pagamento atual expira ([LABS, 2021a](#)).
- Darkside é um Ransomware-as-a-service (RaaS) é desenvolvido por Darkside o ransomware para cibercriminosos e recebe uma parte dos lucros dos ataques. Em maio de 2021 um dos maiores incidentes de cibersegurança na história dos Estados Unidos, envolvendo a empresa Colonial Pipeline, que opera o maior gasoduto do país, foi atribuído ao grupo. O ataque teria tido origem por uma invasão na rede corporativa por meio de uma VPN inativa, cuja senha estava na darkweb ([LOIK, 2021](#)).
- Crysis é um crypto-ransomware que dissemina-se também através arquivos maliciosos anexados a correspondências de e-mails, propagados pelo disparo de campanhas de SPAM e infecta apenas sistemas operacionais Microsoft Windows. Quando instalado e terminado o processo de encriptação, é exibida uma nota de resgate que pode disfarçar-se de mecanismo de proteção e segurança do próprio sistema ([LABS, 2021b](#)).
- Locky é um tipo de crypto-ransomware ainda mais perigoso pois encripta uma grande variedade de arquivos de uso ordinário, o que causa bloqueio da maioria das funções regulares da máquina. É disseminado também a partir de campanhas de e-mail SPAM, mas apresenta-se como faturas de pagamento, tendo anexadas mensagens sem sentido para que solicitando permissão para ativar um macro, a vítima seja enganada a pensar que está autorizando a decodificação da mensagem. Nesse

momento, o malware é instalado no computador, realiza a encriptação e bloqueia a maioria das funções comuns, para depois exibir a nota de resgate ([BELCIC, 2019a](#)).

- Jigsaw é um tipo de crypto-ransomware dos mais destrutivos pois exclui os arquivos encriptados na regularidade de hora em hora, até o prazo de 72 horas da infecção se não pago o resgate, quando todos os arquivos são deletados completamente. O malware também intimida a vítima a não reiniciar o computador, ameaçando deletar os arquivos caso feito. É facilmente identificável, pois o programa exibe na sua nota de resgate a imagem de Jigsaw, icônico vilão da série Jogos Mortais ([MESKAUSKAS, 2023](#)).
- Petya é uma família de crypto-ransomwares que foi descoberta em 2016 pela grande campanha de engenharia social empreendida no mesmo ano. Por ela inúmeros e-mails anexados com arquivos infecciosos propagaram variantes do malware Petya por todo o mundo culminando em 2017 com um dos maiores ciber-ataques da história do mundo. O software se beneficia de uma vulnerabilidade nos sistemas operacionais Microsoft Windows para infectá-lo e assim encriptar os arquivos e exibir uma mensagem de resgate. No entanto, após estudos, especialistas dizem o Petya ter adquirido características de wiper, ou seja, um software malicioso cujo objetivo é destruir os arquivos ao invés de criptografá-los, sem chance de recuperação ([BELCIC, 2019b](#)).
- GoldenEye é um tipo de crypto-ransomware da família Petya, muito semelhante ao próprio. O malware é distribuído por meio de campanhas maliciosas de e-mail massivas contendo dois tipos de arquivos. O conteúdo da correspondência geralmente é uma oferta de emprego e está escrito em alemão. Em anexo há dois tipos de arquivos: um currículo falso e o outro, um arquivo excel malicioso que se aberto abre uma requisição para que o usuário habilite os macros de seu sistema operacional ([MESKAUSKAS, 2022](#)).
- Reveton é um tipo de locky-ransomware dos mais antigos conhecidos, que ao invés de criptografar os arquivos, bloqueia a tela do computador. Apesar de inacessíveis, os arquivos mantém-se íntegros e são recuperados mediante a um resgate. Na tela de bloqueio, é exibida uma falsa comunicação de crime, cujo procurador seria o governo, alegando que a máquina fora bloqueada por ter sido utilizada para fins ilícitos, exigindo portanto uma quantia em dinheiro para ser desbloqueada ([CONTROLENET, 2021](#)).
- Maze ransomware é um crypto-ransomware que em 2019 tornou-se famoso por prejudicar diversas instituições ao longo do mundo, principalmente na área da saúde. É também distribuído como um RaaS, no esquema de desenvolvedor-afiliado, no qual os desenvolvedores vendem os softwares para criminosos e exigem uma porcentagem

da quantia do resgate. Os ataques eram direcionados principalmente a grandes corporações pois o grupo de desenvolvedores se especializou na extorsão por meio da ameaça de vazamento de dados sensíveis extraídos dos sistemas de informação das instituições vítimas ([GALAXKEY, 2021](#)).

2.6 Normas de Segurança Cibernética

Existem várias normas e padrões relacionados à segurança cibernética e segurança da informação. Alguns exemplos importantes incluem:

1. ABNT NBR ISO/IEC 27001: esta norma estabelece os requisitos para um sistema de gestão de segurança da informação (SGSI). Ela define os critérios para identificar, analisar e tratar os riscos à segurança da informação, além de estabelecer diretrizes para implementar controles de segurança adequados ([ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS, 2006](#)).
2. ABNT NBR ISO/IEC 27002: também conhecida como ISO 27002, esta norma fornece um conjunto abrangente de controles de segurança da informação. Ela oferece orientações detalhadas sobre práticas de segurança, abordando áreas como políticas de segurança, gestão de ativos, controle de acesso, criptografia, segurança física, continuidade de negócios, entre outros ([ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS, 2005](#)).
3. A ABNT NBR ISO/IEC 27003: é uma norma técnica que fornece diretrizes para implementação de um sistema de gestão da segurança da informação, com base nas orientações da ABNT NBR ISO/IEC 27001. Ela auxilia as organizações na elaboração de um plano de implementação do sistema de gestão, considerando a contextualização do ambiente, a identificação de requisitos e a definição de processos e controles adequados para proteger a informação ([ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS, 2011](#)).
4. ABNT NBR ISO/IEC 27004: é voltada para a medição e avaliação da gestão da segurança da informação. Ela fornece diretrizes e orientações para a definição e implementação de um programa de medição da segurança da informação, com o objetivo de avaliar a eficácia dos controles de segurança implementados e melhorar continuamente o sistema de gestão ([ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS, 2010](#)).
5. ABNT NBR ISO/IEC 27005: a ISO 27005 é uma norma voltada para a gestão de riscos de segurança da informação. Ela fornece diretrizes e métodos para identificar, avaliar e tratar os riscos relacionados à segurança da informação, ajudando as organizações

a implementar medidas adequadas de gerenciamento de riscos ([ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS, 2008](#)).

6. ABNT NBR ISO/IEC 27017: esta norma aborda aspectos específicos da segurança da informação na computação em nuvem. Ela oferece orientações e controles para garantir a proteção dos dados e dos serviços em ambientes de computação em nuvem ([ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS, 2015](#)).

Essas normas são amplamente reconhecidas internacionalmente e fornecem diretrizes valiosas para ajudar as organizações a estabelecer práticas eficazes de segurança da informação e proteger seus ativos contra ameaças cibernéticas. É importante observar que essas normas podem ser adotadas e adaptadas de acordo com as necessidades específicas de cada organização, visando sempre garantir a confidencialidade, integridade e disponibilidade das informações.

2.7 Iptables: Visão Geral

O iptables é uma solução de firewall baseada em linha de comando amplamente utilizada em sistemas Linux. Sua funcionalidade principal é controlar o tráfego de pacotes em uma rede, permitindo o estabelecimento de políticas de segurança personalizadas. O iptables divide as regras de filtragem em tabelas e cadeias, proporcionando uma abordagem modular para configurar a proteção do sistema contra ameaças e ataques maliciosos. O iptables é uma ferramenta de linha de comando e, por ser extremamente flexível e poderosa, requer um conhecimento sólido para utilizá-la adequadamente. A configuração do iptables é realizada através da criação de tabelas (*chains*) de filtragem e do estabelecimento de regras que especificam como os pacotes devem ser tratados. Lembrando que o iptables faz parte da pilha de rede do sistema operacional e, portanto, requer privilégios de superusuário (*root*) para ser configurado. É importante ter cuidado ao configurar regras no iptables, pois configurações incorretas podem resultar em bloqueios indesejados ou problemas de conectividade. ([PROJECT, 2023](#))

2.8 Trabalhos Relacionados

O trabalho de [Morais \(2021\)](#) teve como objetivo apresentar as normas ABNT NBR ISO/IEC 27002 e ABNT NBR ISO/IEC 27005, exemplificar um ataque de ransomware e sugerir medidas preventivas para proteger os dados de um computador. Utilizando pesquisa bibliográfica e experimental, foi possível demonstrar um passo a passo para criar um ransomware usando o sistema operacional Kali Linux e a ferramenta The Fat Rat. Concluiu-se que a aplicação das normas de segurança mencionadas pode tornar as redes mais seguras contra ataques cibernéticos, incluindo a prevenção de malwares.

O autor [Zaghetto \(2017\)](#) aborda a segurança das redes de interconexão e da internet em um mundo cada vez mais conectado. Destaca-se a ameaça dos malwares, que são códigos maliciosos que exploram vulnerabilidades dos usuários para controlar e manipular os computadores atacados. Um tipo específico de malware, o ransomware, é destacado como uma ameaça em ascensão. O ransomware sequestra os dados do usuário e exige um resgate para liberá-los. O artigo fornece uma explicação detalhada sobre a origem e o funcionamento dos ransomwares, além de apresentar medidas para se proteger contra esse tipo de ataque. Também são abordadas ações a serem tomadas caso ocorra uma infecção por ransomware.

O artigo de [Pimentel, Cabrera e Forte \(2021\)](#) aborda o aumento do uso de ransomwares por grupos especializados em cibercrime, que se mostram eficientes para realizar extorsões. É explorado nesse estudo a evolução dos ransomwares, suas diferentes formas de ataque e destaca a modalidade as a service, que representa um desafio ainda maior. Além disso, são apresentadas medidas específicas de defesa contra ransomwares recomendadas pela comunidade de segurança cibernética, proporcionando uma visão abrangente sobre o assunto.

Nesse presente estudo de Análise Técnica e Prevenção, se distingue dos demais ao adotar uma abordagem das técnicas de entrada empregadas no ataque, explorando vulnerabilidades tanto nos sistemas quanto nos usuários envolvidos. Isso permite uma análise sobre a execução desses ataques. Além disso, oferece soluções no âmbito de redes, destacando medidas preventivas que podem ser adotadas para reforçar a segurança cibernética e reduzir os riscos associados aos ataques de ransomware. Tais propostas visam fornecer um guia prático e abrangente para profissionais de segurança lidarem com essas ameaças de forma eficaz.

3 Estudo e Análise do Ransomware

O desenvolvimento deste estudo seguiu várias etapas para garantir a sua efetividade. Inicialmente, foi coletado em uma pesquisa sobre conscientização sobre segurança cibernética que será mostrada em detalhes na Seção 3.1, em seguida um ambiente de testes seguro e controlado foi criado para utilizar uma máquina virtual baseada em Linux Ubuntu. Nesse ambiente, foram criadas pastas contendo arquivos de texto, permitindo a realização dos testes de forma segura, sem prejudicar sistemas ou dados reais.

Os códigos apresentados neste trabalho são exemplos simples de técnicas de criptografia, adaptados de várias fontes disponíveis na Internet, tutoriais e fóruns de debate sobre segurança cibernética, nosso objetivo é demonstrar a execução de códigos relacionados aos principais ataques estudados para compreender a ideia de funcionamento dos ransomwares, e em seguida, demonstrar técnicas que podem ser utilizadas para combater ransomware. Ressalta-se que esses códigos foram utilizados apenas para fins educacionais e não têm a intenção de serem empregados para fins maliciosos. Em relação a fontes confiáveis sobre Ransomware, destacam-se os seguintes materiais acadêmicos de criptografia Fernet ([FERRIE, 2018](#)), assim como foi citado as principais fontes que agregaram nesse estudo no capítulo 2.

Além disso, foram realizados testes e análises para validar soluções de segurança em rede. Foram avaliados firewalls, sistemas de detecção de intrusões e políticas de acesso restrito, com o intuito de verificar sua eficácia na detecção e prevenção de ataques de ransomware. Todas essas etapas foram fundamentais para a realização de um estudo abrangente sobre ransomware e segurança cibernética, visando contribuir para a compreensão do funcionamento desses ataques, bem como para o desenvolvimento de estratégias eficazes de prevenção e proteção.

3.1 Pesquisa: Conscientização e Medidas de Segurança Cibernética em Usuários de Dispositivos Conectados à Internet

A presente pesquisa Conscientização e Medidas de Segurança Cibernética em Usuários de Dispositivos Conectados à Internet foi realizada através de questionário online, disponibilizado na plataforma Google Forms, perguntas sobre o conhecimento em segurança cibernética, as práticas de segurança ao utilizar dispositivos conectados à Internet e as percepções sobre ameaças cibernéticas. Além disso, foram coletadas informações demográficas para compreender o perfil dos participantes.

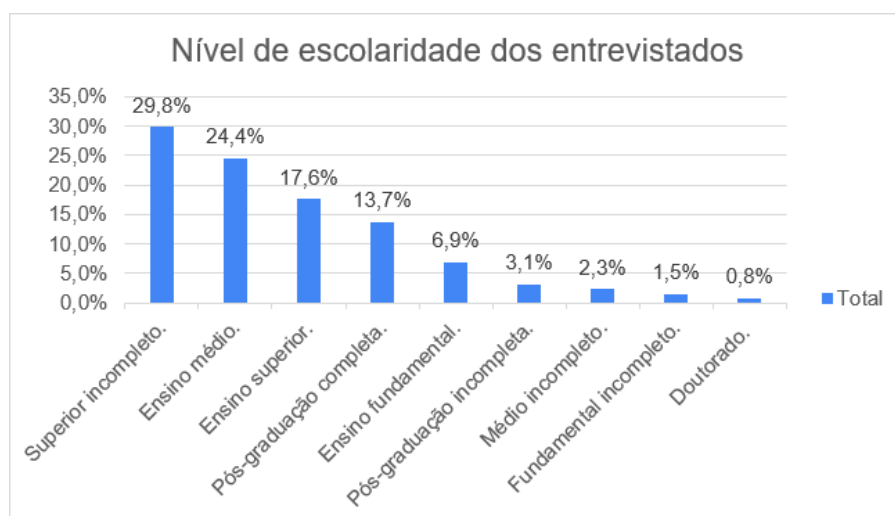
A pesquisa foi conduzida entre os dias 17/07/2023 e 24/07/2023, com a participação

de 131 respondentes. Para garantir uma amostra diversificada, o formulário foi amplamente divulgado em vários canais de comunicação, incluindo grupos de WhatsApp de alunos da universidade, meio corporativo, perfis de redes sociais e até mesmo em círculos familiares. Um link de acesso ao questionário foi compartilhado com os participantes por esses meios, permitindo uma abrangente participação na pesquisa.

A relevância deste estudo reside no seu propósito de fornecer percepções sobre o grau de preparo dos usuários frente às ameaças cibernéticas, além de identificar áreas de melhoria na conscientização e práticas de segurança online. Com base nas informações obtidas, espera-se aprimorar as medidas de proteção e prevenção contra possíveis ataques, contribuindo assim para a segurança dos usuários e de suas informações em um cenário cada vez mais digital e conectado.

Após a análise dos dados coletados, mostrados na figura 4 constatou-se que a maioria dos participantes da pesquisa são predominantemente formada por indivíduos cursando ensino superior (29,8%) e com ensino médio completo (24,4%).

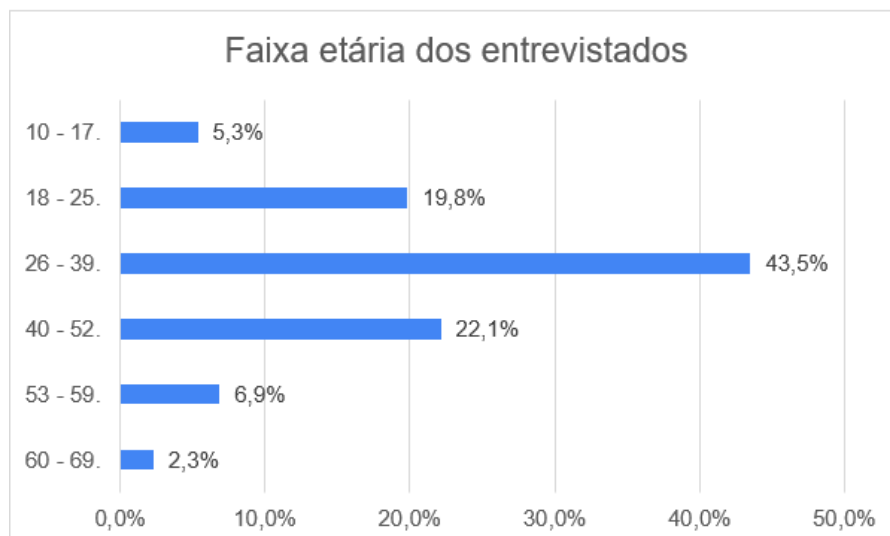
Figura 4 – Escolaridade dos participantes



Fonte: Autor

Quanto à faixa etária dos participantes, a figura 5 pesquisa englobou uma ampla distribuição, destacando-se os seguintes grupos etários: 18-25 anos (19,8%), 26-39 anos (43,5%) e 40-52 anos (22,1%).

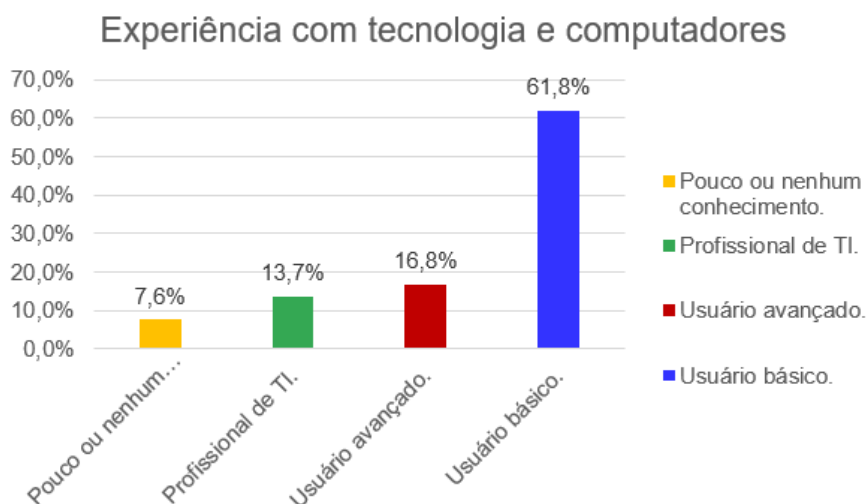
Figura 5 – Faixa etária dos participantes



Fonte: Autor

Os resultados da pesquisa mostrados na figura 6 revelam um panorama sobre o conhecimento e práticas de segurança cibernética dos participantes. Em relação à experiência com tecnologia e computadores, a maioria dos entrevistados se classificou como usuários básicos (61,8%), seguidos pelos usuários avançados (16,8%) e profissionais de TI (13,7%). Um pequeno percentual relatou ter pouco ou nenhum conhecimento (7,6%), o que destaca a necessidade de conscientização e educação em segurança digital.

Figura 6 – Experiência em computadores

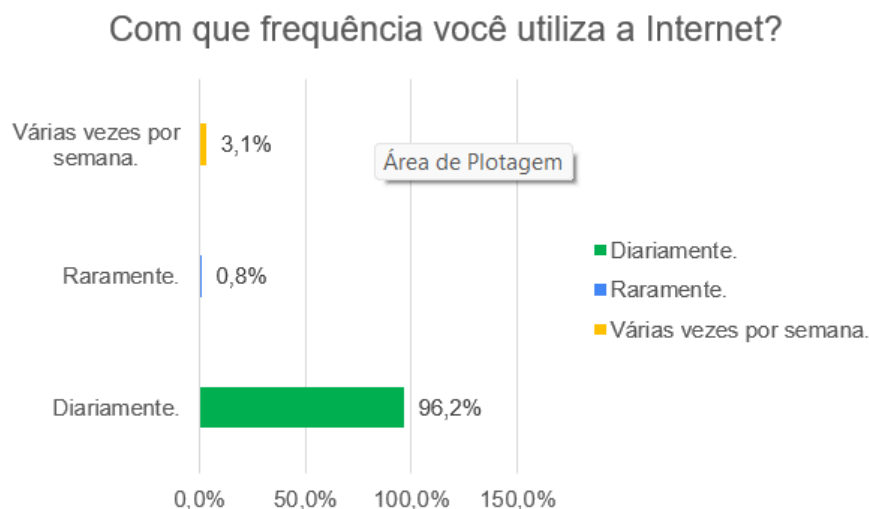


Fonte: Autor

Quanto à frequência de utilização da Internet diário como ferramenta de trabalho, estudo, entretenimento, podendo ser observado na figura 7, a grande maioria dos participantes declarou fazer uso diário (96,2%). Por outro lado, apenas um pequeno grupo

afirmou utilizar a Internet várias vezes por semana (3,1%), e ninguém relatou acessá-la apenas algumas vezes por mês. Essa alta frequência de uso pode impactar diretamente a exposição a possíveis ameaças cibernéticas.

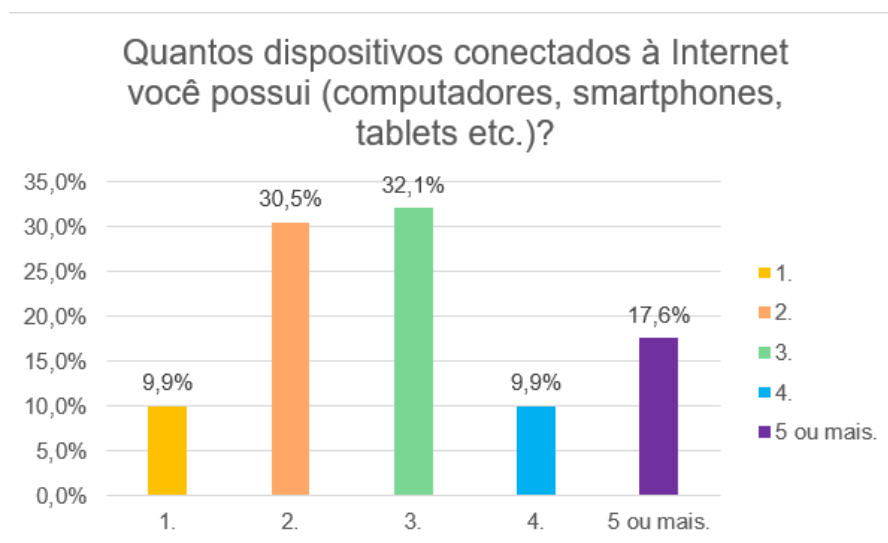
Figura 7 – Frequência do uso Internet



Fonte: Autor

Em relação à quantidade de dispositivos conectados à Internet, a figura 8 indica que a pesquisa revelou que a maioria possui múltiplos dispositivos. Cerca de um terço dos participantes possui 3 dispositivos (32,1%), seguidos por 2 dispositivos (30,5%) e 5 ou mais dispositivos (17,6%). Esse cenário aumenta a superfície de ataque e ressalta a importância de medidas de segurança adequadas para cada um dos aparelhos.

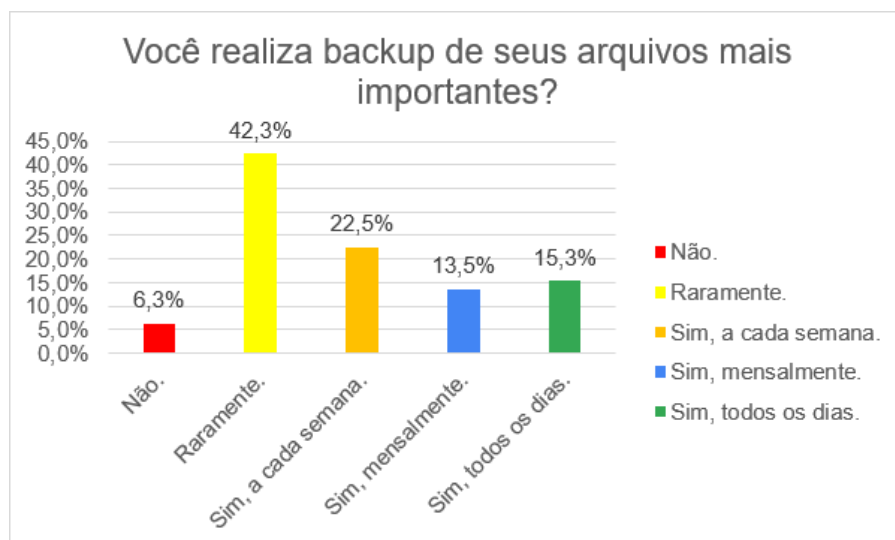
Figura 8 – Dispositivos conectados à Internet



Fonte: Autor

Quando se trata de realizar backups de arquivos importantes, a figura 9 mostra uma porcentagem significativa não possui essa prática. O maior grupo (42,3%) relatou realizar backups raramente, enquanto 22,5% o fazem semanalmente e 13,5% mensalmente. Apenas 15,3% dos participantes realizam backup diariamente, e 6,3% não realizam backup algum. Essa estatística evidencia uma oportunidade para conscientizar sobre a importância de backups regulares para evitar a perda de dados em caso de incidentes.

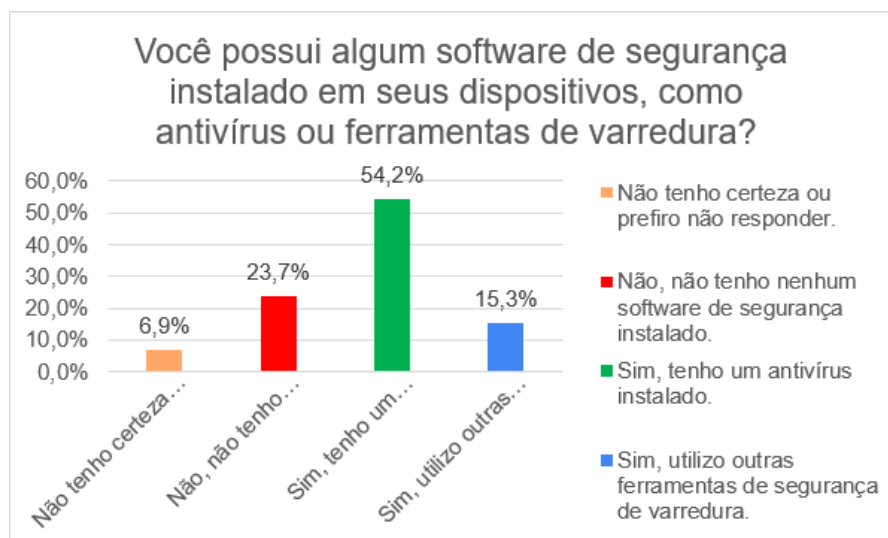
Figura 9 – Backup



Fonte: Autor

Em relação à presença de software de segurança, na figura 10 que indica 54,2% afirmaram ter um antivírus instalado, enquanto 15,3% utilizam outras ferramentas de varredura. Por outro lado, 23,7% não possuem software de segurança instalado, e 6,9% não souberam responder. Esses resultados sugerem que há espaço para aumentar a adoção de soluções de segurança em dispositivos conectados à Internet.

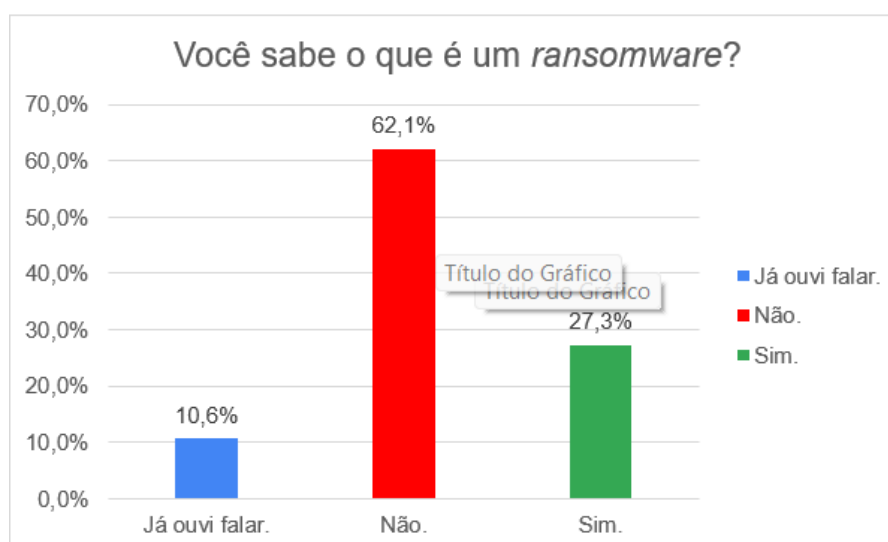
Figura 10 – Utilização de antivírus



Fonte: Autor

Quando questionados sobre o conhecimento em relação ao Ransomware, a figura 11 indica que os resultados foram diversos. Apenas 27,3% afirmaram saber o que é um Ransomware, enquanto a maioria dos participantes (62,1%) não possui conhecimento sobre o tema. No entanto, é relevante notar que 10,6% já ouviram falar sobre o assunto. Ressalta a importância dos usuários se educarem sobre os riscos associados a ameaças cibernéticas.

Figura 11 – Ransomware o que é



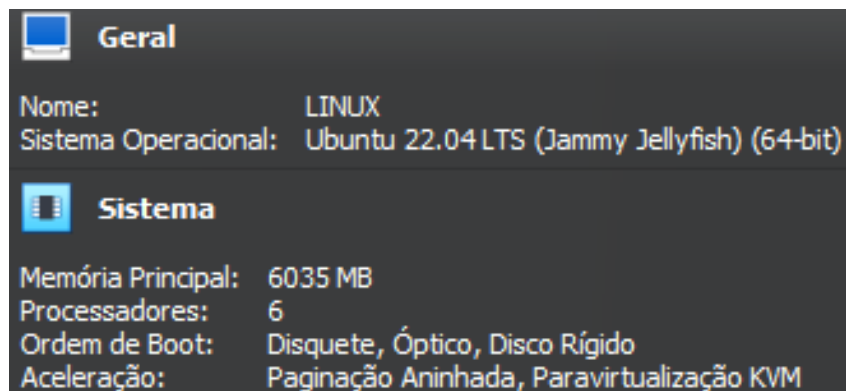
Fonte: Autor

Para consultar os resultados da, acesse o link: <https://docs.google.com/forms/d/e/1FAIpQLSd2M7Y7p56FW95VXMoCzvIjA1F23j8g6Nf1bsAITCFyJ8TV8A/viewanalytics>

3.2 Ambiente dos Testes

Utilizamos uma máquina virtual hospedada no Oracle VM VirtualBox 7.0.8, mostrado na figura 12 com o sistema operacional Linux Ubuntu 22.04 (Jammy Jellyfish) de 64 bits. Para possibilitar a execução adequada da máquina virtual, configuramos a BIOS habilitando a opção *Intel Virtualization*. No contexto do estudo, desenvolvemos uma amostra educativa de ransomware usando o Fernet (criado pelos próprios desenvolvedores do python.org) usando a linguagem Python 3.11.4. Utilizamos o compilador PyCharm *Community Edition 2023.2 1.3* para criar e executar o código.

Figura 12 – Configuração Disponibilizada para Máquina Virtual



Fonte: Autor

3.3 Ransomware

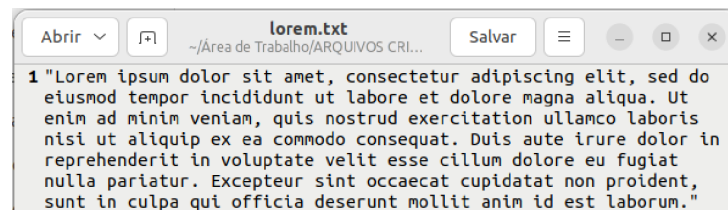
Foi utilizado um algoritmo para realizar a criptografia de arquivos em um diretório. Ele gera uma chave de criptografia aleatória usando o algoritmo Fernet e a armazena em "thekey.key". Em seguida, percorre os arquivos no diretório, lê o conteúdo de cada arquivo, criptografa esse conteúdo usando a chave gerada e sobrescreve o arquivo original com o conteúdo criptografado. O resultado final é a criptografia de todos os arquivos no diretório, e uma mensagem é impressa indicando que todos os arquivos foram criptografados.

- Identificação dos arquivos: O primeiro trecho cria uma lista de arquivos a serem criptografados, excluindo três arquivos específicos ("malware.py", "thekey.key" e "decrypt.py") e adicionando todos os outros arquivos encontrados no diretório atual à lista.
- Geração da chave de criptografia: O código gera uma chave de criptografia usando o Fernet e a salva no arquivo "thekey.key". Essa chave é essencial para a criptografia e posterior descriptografia dos arquivos.

- Criptografia dos arquivos: Esta seção é a parte central do código, onde cada arquivo na lista "arquivos" é lido, o seu conteúdo é criptografado usando a chave gerada anteriormente e, em seguida, o arquivo original é sobrescrito com o conteúdo criptografado. Isso é a essência do processo de criptografia de arquivos em um ataque de ransomware.
- Mensagem de conclusão: O código imprime uma mensagem indicando que todos os arquivos foram criptografados. Essa mensagem geralmente é exibida para a vítima como parte do ataque, informando que seus arquivos foram bloqueados.

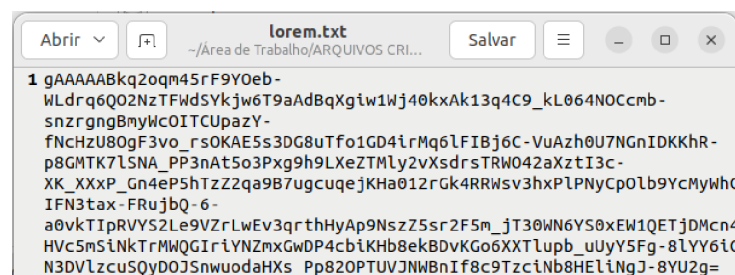
O algoritmo foi executado em um arquivo de texto exemplo "lorem ipsum" que estava alocado na pasta onde foi executado o código, resultando na criação de arquivos criptografados representados na imagem subsequente. As imagens a seguir ilustram os arquivos resultantes da criptografia, sem a possibilidade de visualização do conteúdo original, em seguida mostra todos os arquivos contidos na pasta, representados na figura 13, 14:

Figura 13 – O arquivo txt contém o seguinte texto: Lorem ipsum



Fonte: Autor

Figura 14 – Arquivo txt, completamente criptografado pelo ransomware, impossibilitado de ler os texto original



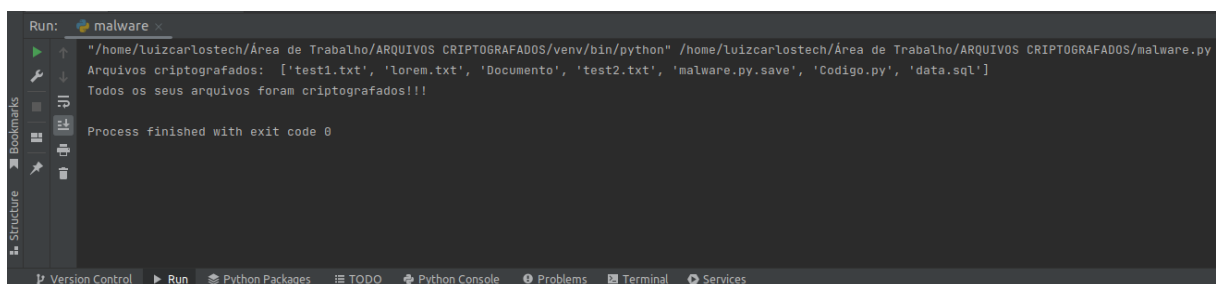
Fonte: Autor

Agora vamos demonstrar em seguida executado na figura 15 um processo de descriptografia de arquivos criptografados por um ransomware. Primeiro, ele lista os arquivos no diretório atual, excluindo arquivos específicos ("malware.py", "thekey.key" e "decrypt.py"). Em seguida, lê a chave secreta de um arquivo chamado "thekey.key". O

usuário é solicitado a inserir uma senha, e se a senha estiver correta, os arquivos são descriptografados usando a chave secreta. Para cada arquivo na lista de arquivos, o conteúdo criptografado é lido, descriptografado usando a chave secreta e, em seguida, o arquivo original é sobrescrito com o conteúdo descriptografado. O resultado final é a recuperação dos arquivos descriptografados, e uma mensagem é impressa indicando que todos os arquivos foram recuperados.

- Identificação dos arquivos: O início do código é semelhante ao anterior, onde uma lista de arquivos a serem descriptografados é criada. Novamente, os arquivos "malware.py", "thekey.key" e "decrypt.py" são excluídos.
- Leitura da chave de descriptografia: O código lê a chave de descriptografia armazenada no arquivo "thekey.key". Essa chave é necessária para a descriptografia dos arquivos e deve corresponder à chave usada para criptografá-los.
- Solicitação de senha: O código solicita uma senha ao usuário para descriptografar os arquivos. A senha é comparada com uma "frase secreta" pré-definida (variável "cript"). Se a senha estiver correta, o processo de descriptografia é realizado.
- Descriptografia dos arquivos: O código percorre a lista de arquivos a serem descriptografados, lê o conteúdo criptografado de cada arquivo, descriptografa-o usando a chave secreta e, em seguida, substitui o conteúdo criptografado pelo conteúdo descriptografado no próprio arquivo.
- Mensagem de conclusão: Após a descriptografia de todos os arquivos, uma mensagem é exibida indicando que todos os arquivos foram recuperados com sucesso.

Figura 15 – Descriptografando dados da pasta



Fonte: Autor

3.4 Negação de serviço distribuída

Fizemos uma representação executando o script no compilador como uma demonstração visual das solicitações simultâneas enviadas às URLs-alvo. Foi feita a utilização de

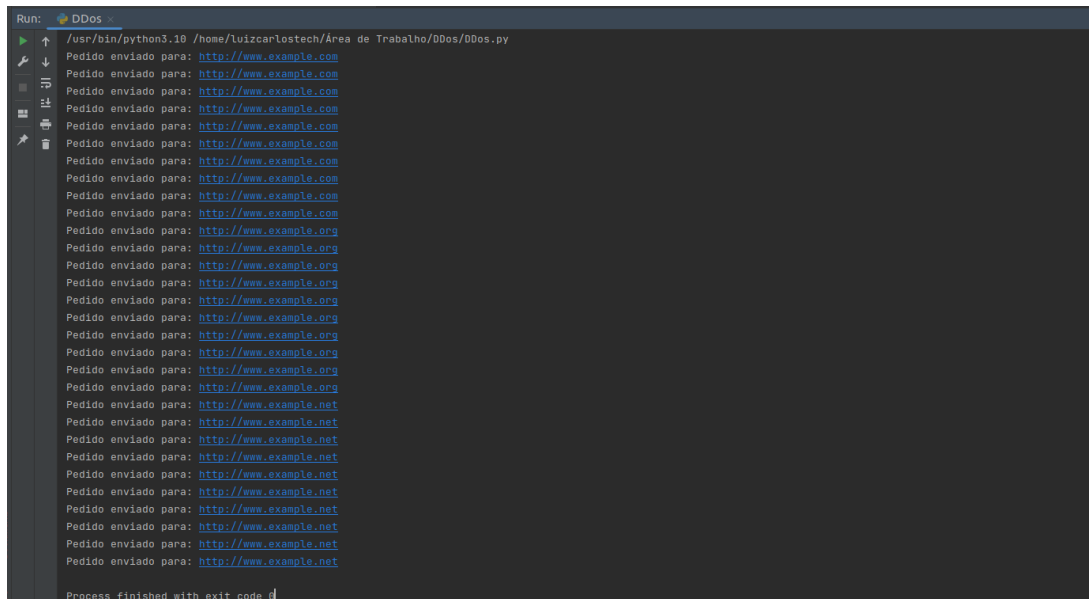
url's de forma simbólica. O experimento tem como objetivo compreender a natureza dos ataques DDoS e explorar medidas de mitigação e prevenção.

O algoritmo envia pedidos HTTP simultaneamente para um conjunto de URLs-alvo usando threads. Ele importa os módulos "requests" e "threading" para enviar os pedidos e criar as threads, respectivamente. A função `send_request(url)` envia um pedido HTTP GET para uma URL específica, exibindo uma mensagem de sucesso ou erro. O algoritmo tem uma lista de URLs-alvo e define o número de threads como 10. Para cada URL, ele cria threads que executam a função "sendrequest". Após a criação e início das threads, outro loop aguarda o término de todas as threads usando o método "join()". Isso permite o envio concorrente de pedidos HTTP para as URLs-alvo, processando vários pedidos simultaneamente por meio de threads.

- O algoritmo realiza o envio simultâneo de pedidos HTTP para um conjunto de URLs-alvo utilizando *threads*.
- Primeiro, o algoritmo importa os módulos *requests*, *threading* necessários para o envio dos pedidos e a criação das *threads*, respectivamente.
- Em seguida, é definida a função *send_request(url)*, que realiza o envio de um pedido HTTP GET para uma URL específica. Se o pedido for bem-sucedido, exibe uma mensagem indicando que o pedido foi enviado para a URL. Caso ocorra algum erro durante o envio do pedido, exibe uma mensagem de erro informando o problema.
- O algoritmo possui uma lista de URLs-alvo, representada pela variável *urls*. Essas URLs são os destinos para os quais os pedidos serão enviados.
- A variável *num_threads* indica o número de *threads* que serão criadas para enviar os pedidos simultaneamente. Neste caso, o valor é definido como 10.
- Em seguida, há um loop que percorre cada URL-alvo da lista *urls*. Para cada URL, é criada uma lista de *threads* vazia. Em seguida, um novo loop é executado *num_threads* vezes, criando uma nova *thread* para cada iteração. Cada *thread* é direcionada para a função *send_request* com a URL-alvo correspondente como argumento. As *threads* são adicionadas à lista de *threads* e iniciadas.
- Após o término do *loop* de criação e início das *threads*, um novo loop é executado para aguardar o término de todas as *threads*. Isso é feito utilizando o método *join()* em cada *thread*, que bloqueia a execução até que a *thread* termine.
- Dessa forma, o algoritmo realiza o envio concorrente de pedidos HTTP para as URLs-alvo, permitindo que múltiplos pedidos sejam processados simultaneamente por meio do uso de *threads*.

Execução dos envios das URLs alvos na figura 16:

Figura 16 – Mensagem enviando pedido HTTP GET para URL



```
Run: DDos
/usr/bin/python3.10 /home/luizcarlostech/Área de Trabalho/DDos/DDos.py
Pedido enviado para: http://www.example.com
Pedido enviado para: http://www.example.com
Pedido enviado para: http://www.example.com
Pedido enviado para: http://www.example.com
Pedido enviado para: http://www.example.com
Pedido enviado para: http://www.example.com
Pedido enviado para: http://www.example.com
Pedido enviado para: http://www.example.com
Pedido enviado para: http://www.example.com
Pedido enviado para: http://www.example.com
Pedido enviado para: http://www.example.org
Pedido enviado para: http://www.example.org
Pedido enviado para: http://www.example.org
Pedido enviado para: http://www.example.org
Pedido enviado para: http://www.example.org
Pedido enviado para: http://www.example.org
Pedido enviado para: http://www.example.org
Pedido enviado para: http://www.example.org
Pedido enviado para: http://www.example.org
Pedido enviado para: http://www.example.net
Pedido enviado para: http://www.example.net
Pedido enviado para: http://www.example.net
Pedido enviado para: http://www.example.net
Pedido enviado para: http://www.example.net
Pedido enviado para: http://www.example.net
Pedido enviado para: http://www.example.net
Pedido enviado para: http://www.example.net
Pedido enviado para: http://www.example.net
Process finished with exit code 0
```

Fonte: Autor

3.5 WannaCry

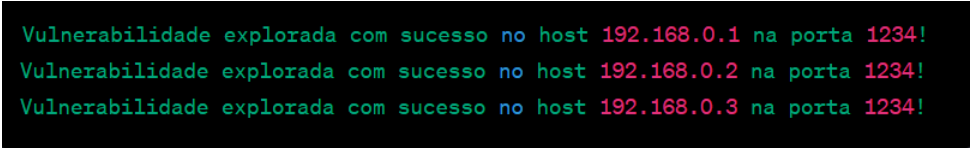
O WannaCry é um tipo de ransomware que explorava uma vulnerabilidade no sistema Windows conhecida como MS17-010. Essa vulnerabilidade permitia que o ransomware se propagasse rapidamente pela rede, infectando outros computadores desprotegidos.

Para criar uma representação com o código Python, podemos usar uma simulação de propagação de um malware por meio de uma vulnerabilidade específica. Por exemplo, podemos criar um código Python que explora uma vulnerabilidade de um serviço em execução em um determinado *host* na rede e, em seguida, se espalha para outros *hosts* desprotegidos. Neste exemplo, temos uma função *exploit vulnerability* que simula a exploração de uma vulnerabilidade em um serviço em execução em um *host* específico. Em seguida, a função *propagate malware* representa a propagação do malware para outros *hosts* vulneráveis na rede.

- A função *exploit vulnerability* representa a exploração de uma vulnerabilidade em um serviço em execução em um determinado *host* e porta. Ela cria um *socket*, conecta ao *host* e envia um *payload* malicioso para explorar a vulnerabilidade.
- A função *propagate malware* simula a propagação do malware para outros *hosts* vulneráveis na rede. Ela itera sobre uma lista de *hosts* vulneráveis e chama a função *exploit vulnerability* para cada um deles após um intervalo de 1 segundo.

Suponha que os hosts 192.168.0.1, 192.168.0.2 e 192.168.0.3 sejam vulneráveis e estejam com um serviço na porta 1234. Nesse caso, a função *propagate* malware será executada, e a função *exploit vulnerability* será chamada para cada um desses *hosts* após um intervalo de 1 segundo mostrado na figura 17.

Figura 17 – Vulnerabilidade explorada



```
Vulnerabilidade explorada com sucesso no host 192.168.0.1 na porta 1234!  
Vulnerabilidade explorada com sucesso no host 192.168.0.2 na porta 1234!  
Vulnerabilidade explorada com sucesso no host 192.168.0.3 na porta 1234!
```

Fonte: Autor

4 Soluções Propostas

Serão apresentados as percepções e descobertas decorrentes das simulações controladas de ataques ransomware, bem como os dados coletados por meio da pesquisa de avaliação sobre segurança cibernética. Será demonstrada a eficácia das medidas de proteção adotadas, como o uso do iptables para bloquear portas de entrada e o reforço do firewall do Windows, a fim de fortalecer a segurança contra essas ameaças. A análise desses resultados fornecerá uma visão abrangente da conscientização geral sobre segurança cibernética e destacará a importância de estratégias proativas na defesa contra ameaças em um ambiente digital em constante evolução.

4.1 Utilização do Iptables para Bloqueio de Portas de Entrada e Prevenção de Ataques WannaCry e DDoS:

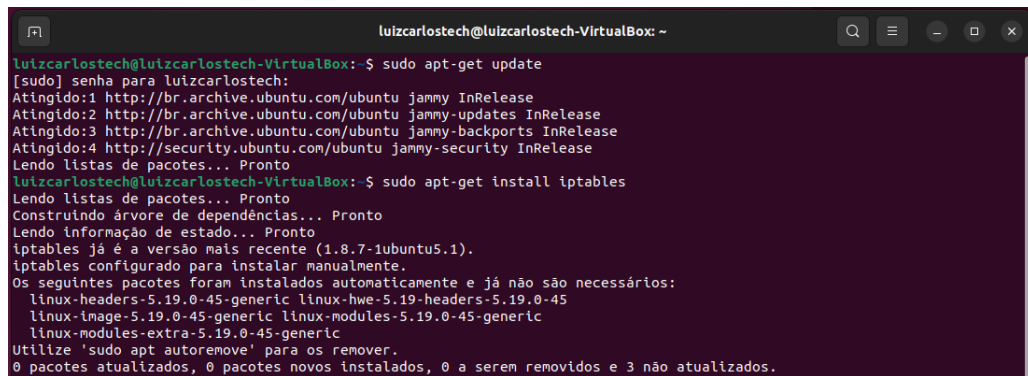
Apresentação de estratégias e medidas de segurança a nível de rede para prevenir e mitigar ataques de ransomware. Nesta seção, abordaremos o uso do iptables como uma ferramenta de firewall no sistema operacional Linux Ubuntu 22.04 (Jammy Jellyfish) 64 bits. Primeiramente, apresentaremos uma breve explicação sobre o iptables e sua importância na segurança cibernética.

4.1.1 Utilização do Iptables no Ubuntu

A seguir, detalharemos as etapas que seguimos para bloquear as portas de entrada do WannaCry e implementar medidas de prevenção contra ataques DDoS e ransomware usando o iptables:

- **Instalação do iptables:** acessamos o terminal do Ubuntu com permissões de superusuário (*root*) para executar comandos com privilégios de administrador na figura 18.

Figura 18 – Instalando iptables

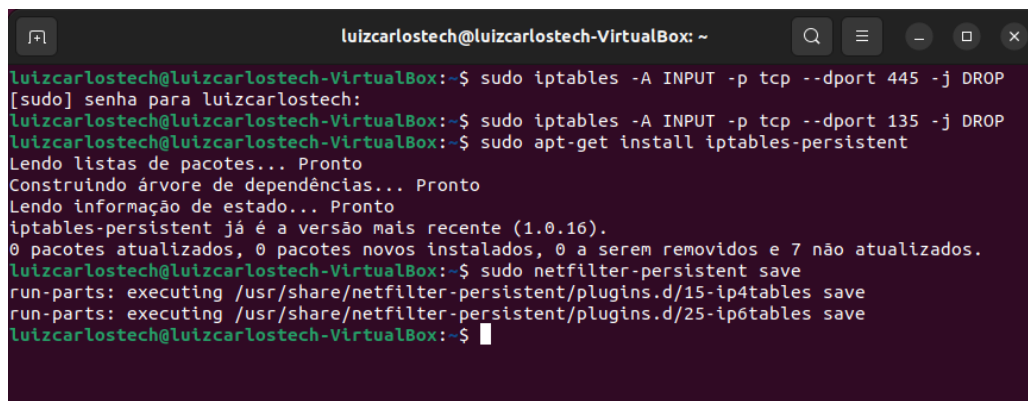


```
luizcarloste@luizcarloste-VirtualBox: ~  
luizcarloste@luizcarloste-VirtualBox:~$ sudo apt-get update  
[sudo] senha para luizcarloste:  
Atingido:1 http://br.archive.ubuntu.com/ubuntu jammy InRelease  
Atingido:2 http://br.archive.ubuntu.com/ubuntu jammy-updates InRelease  
Atingido:3 http://br.archive.ubuntu.com/ubuntu jammy-backports InRelease  
Atingido:4 http://security.ubuntu.com/ubuntu jammy-security InRelease  
Lendo listas de pacotes... Pronto  
luizcarloste@luizcarloste-VirtualBox:~$ sudo apt-get install iptables  
Lendo listas de pacotes... Pronto  
Construindo árvore de dependências... Pronto  
Lendo informação de estado... Pronto  
iptables já é a versão mais recente (1.8.7-1ubuntu5.1).  
iptables configurado para instalar manualmente.  
Os seguintes pacotes foram instalados automaticamente e já não são necessários:  
  linux-headers-5.19.0-45-generic linux-hwe-5.19-headers-5.19.0-45  
  linux-image-5.19.0-45-generic linux-modules-5.19.0-45-generic  
  linux-modules-extra-5.19.0-45-generic  
Utilize 'sudo apt autoremove' para os remover.  
0 pacotes atualizados, 0 pacotes novos instalados, 0 a serem removidos e 3 não atualizados.
```

Fonte: Autor

- **Bloqueio das Portas Exploradas pelo WannaCry:** o ransomware WannaCry, em sua propagação, explora vulnerabilidades nas portas de entrada dos sistemas. Utilizando o iptables, implementamos regras específicas para bloquear o tráfego nas portas 445 (SMB) e 135 (RPC), que são conhecidas por serem exploradas pelo WannaCry. Essas regras direcionadas impedem o tráfego malicioso relacionado a esse ransomware, mitigando a possibilidade de infecção em nosso ambiente de estudo na figura 19.

Figura 19 – Bloqueando tráfego nas portas 445 (SMB) e 135 (RPC)

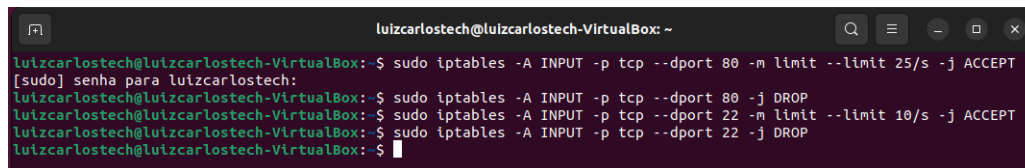


```
luizcarloste@luizcarloste-VirtualBox: ~  
luizcarloste@luizcarloste-VirtualBox:~$ sudo iptables -A INPUT -p tcp --dport 445 -j DROP  
[sudo] senha para luizcarloste:  
luizcarloste@luizcarloste-VirtualBox:~$ sudo iptables -A INPUT -p tcp --dport 135 -j DROP  
luizcarloste@luizcarloste-VirtualBox:~$ sudo apt-get install iptables-persistent  
Lendo listas de pacotes... Pronto  
Construindo árvore de dependências... Pronto  
Lendo informação de estado... Pronto  
iptables-persistent já é a versão mais recente (1.0.16).  
0 pacotes atualizados, 0 pacotes novos instalados, 0 a serem removidos e 7 não atualizados.  
luizcarloste@luizcarloste-VirtualBox:~$ sudo netfilter-persistent save  
run-parts: executing /usr/share/netfilter-persistent/plugins.d/15-ip4tables save  
run-parts: executing /usr/share/netfilter-persistent/plugins.d/25-ip6tables save  
luizcarloste@luizcarloste-VirtualBox:~$
```

Fonte: Autor

- **Limitar Tráfego nas Portas Para Prevenir o DDoS:** aplicamos regras no iptables para limitar a quantidade de pacotes por segundo em portas específicas. Neste caso, exemplificamos o bloqueio de tráfego excessivo nas portas 80 (HTTP) e 22 (SSH) como medida preventiva contra ataques volumétricos na figura 20.

Figura 20 – Bloqueio de tráfego excessivo nas portas 80 (HTTP) e 22 (SSH)

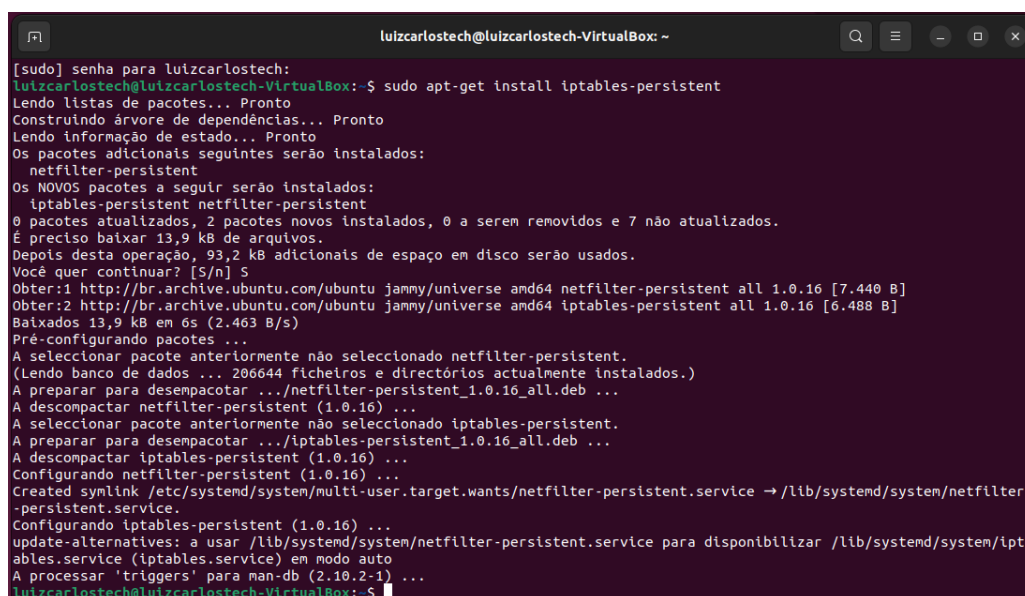


```
luizcarloste@luizcarloste-VirtualBox: ~  
luizcarloste@luizcarloste-VirtualBox:~$ sudo iptables -A INPUT -p tcp --dport 80 -m limit --limit 25/s -j ACCEPT  
[sudo] senha para luizcarloste:  
luizcarloste@luizcarloste-VirtualBox:~$ sudo iptables -A INPUT -p tcp --dport 80 -j DROP  
luizcarloste@luizcarloste-VirtualBox:~$ sudo iptables -A INPUT -p tcp --dport 22 -m limit --limit 10/s -j ACCEPT  
luizcarloste@luizcarloste-VirtualBox:~$ sudo iptables -A INPUT -p tcp --dport 22 -j DROP  
luizcarloste@luizcarloste-VirtualBox:~$
```

Fonte: Autor

- Para garantir que as regras sejam aplicadas sempre que o sistema for reiniciado, você pode salvar as regras do iptables em um arquivo na figura 21.

Figura 21 – Criando a regra para salvar as alterações no iptables.



```
[sudo] senha para luizcarloste:  
luizcarloste@luizcarloste-VirtualBox:~$ sudo apt-get install iptables-persistent  
Lendo listas de pacotes... Pronto  
Construindo árvore de dependências... Pronto  
Lendo informação de estado... Pronto  
Os pacotes adicionais seguintes serão instalados:  
  netfilter-persistent  
Os NOVOS pacotes a seguir serão instalados:  
  iptables-persistent netfilter-persistent  
0 pacotes atualizados, 2 pacotes novos instalados, 0 a serem removidos e 7 não atualizados.  
É preciso baixar 13,9 kB de arquivos.  
Depois desta operação, 93,2 kB adicionais de espaço em disco serão usados.  
Você quer continuar? [S/n] S  
Obter:1 http://br.archive.ubuntu.com/ubuntu jammy/universe amd64 netfilter-persistent all 1.0.16 [7.440 B]  
Obter:2 http://br.archive.ubuntu.com/ubuntu jammy/universe amd64 iptables-persistent all 1.0.16 [6.488 B]  
Baixados 13,9 kB em 6s (2.463 B/s)  
Pré-configurando pacotes ...  
A seleccionar pacote anteriormente não seleccionado netfilter-persistent.  
(Lendo banco de dados ... 206644 ficheiros e directórios actualmente instalados.)  
A preparar para descompactar .../netfilter-persistent_1.0.16_all.deb ...  
A descompactar netfilter-persistent (1.0.16) ...  
A seleccionar pacote anteriormente não seleccionado iptables-persistent.  
A preparar para descompactar .../iptables-persistent_1.0.16_all.deb ...  
A descompactar iptables-persistent (1.0.16) ...  
Configurando netfilter-persistent (1.0.16) ...  
Created symlink /etc/systemd/system/multi-user.target.wants/netfilter-persistent.service → /lib/systemd/system/netfilter-persistent.service.  
Configurando iptables-persistent (1.0.16) ...  
update-alternatives: a usar /lib/systemd/system/netfilter-persistent.service para disponibilizar /lib/systemd/system/iptables.service (iptables.service) em modo auto  
A processar 'triggers' para man-db (2.10.2-1) ...  
luizcarloste@luizcarloste-VirtualBox:~$
```

Fonte: Autor

- Para que as regras criadas sejam carregadas automaticamente durante a inicialização do sistema, salvamos as configurações iptables persistent.

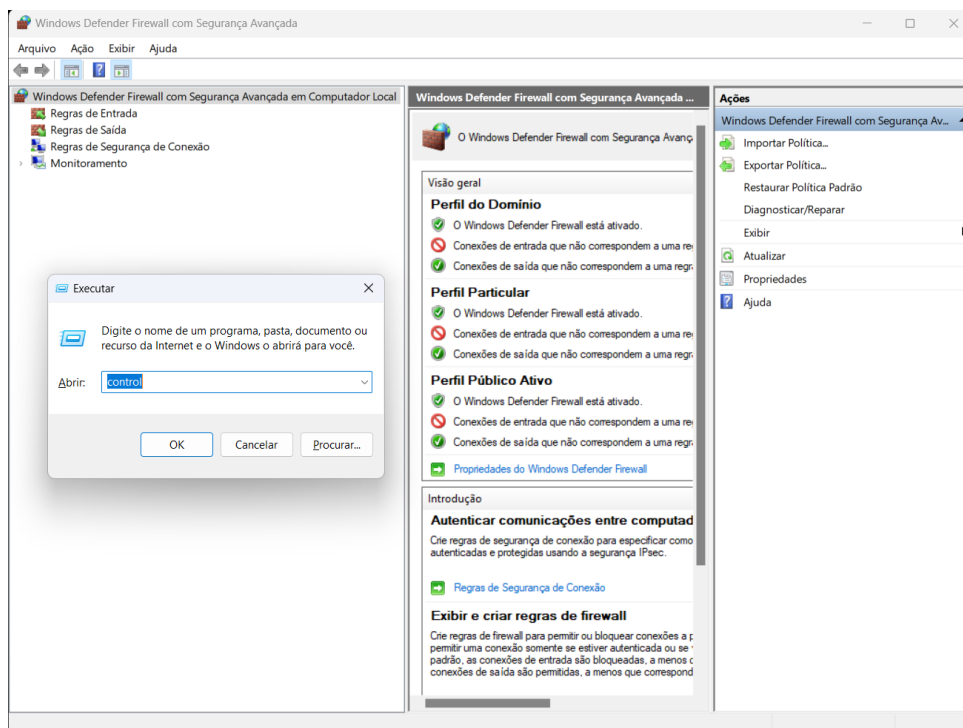
4.2 Firewall do Windows

Nesta seção, exploramos como o Firewall do Windows 11 foi configurado para bloquear portas de entrada específicas, impedindo a propagação de Ransomware, e como foram aplicadas regras para limitar o tráfego malicioso e atenuar ataques.

- **Bloquear o tráfego de portas vulneráveis, como a porta 445, que é explorada pelo WannaCry:** para fazer isso, iremos logar com o usuário administrador do sistema operacional Windows e acessaremos o Windows Defender Firewall com segurança avançada. Para isso seguramos a tecla WIN+R para abrir o executar e

digitaremos control para abrir o painel de controle. Em seguida vamos em Sistema e Segurança e encontraremos a opção Windows Defender Firewall, nela vamos abrir as configurações avançadas e encontraremos a segurança avançada do computador local como mostra a figura 31.

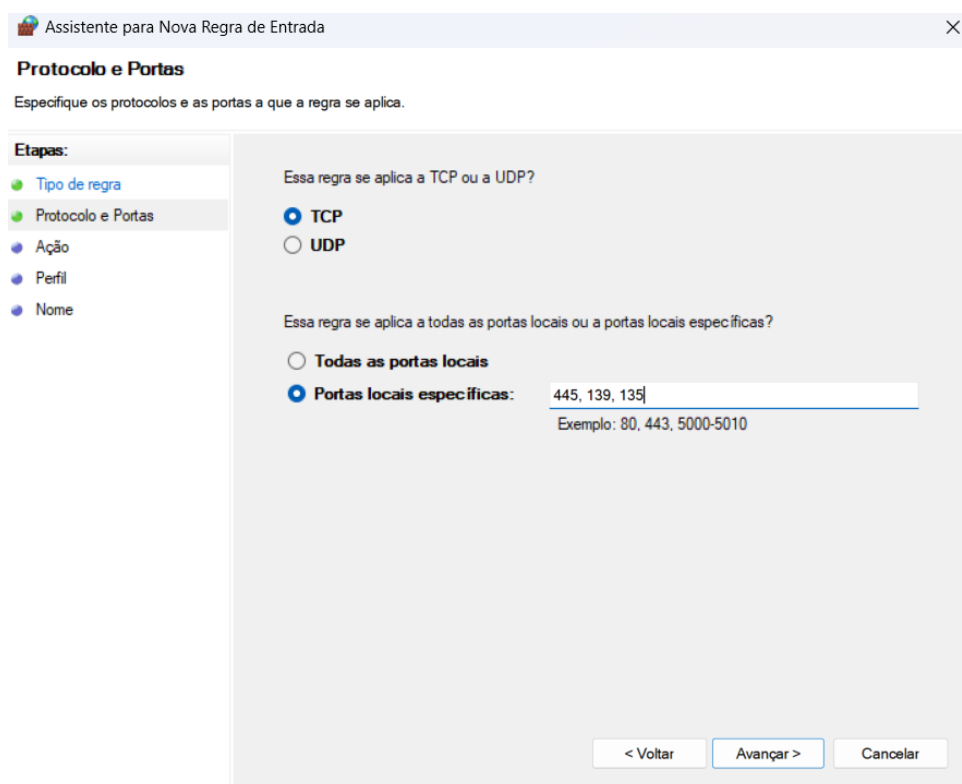
Figura 22 – Acessando o Firewall



Fonte: Autor

Em regras de entrada iremos criar uma nova regra e selecionaremos a opção Porta (regra que controla conexões para uma porta TCP ou UDP), selecionamos a opção TCP e portas locais específicas e colocamos as portas a serem bloqueadas na figura 23.

Figura 23 – Portas à Serem Bloqueadas



Fonte: Autor

Selecionamos a opção de bloquear a conexão e deixamos selecionado as opções de domínio, particular e público, e damos um nome a regra, no nosso caso TESTE1TCC, como pode ser visto na figura 24.

Figura 24 – Regra Criada TESTE1TCC



Fonte: Autor

As portas exploradas pelo WannaCry são as portas TCP 445 (usada para o protocolo SMB) e portas TCP 139 e 135 (também associadas ao compartilhamento de arquivos no Windows). Portanto, essas portas foram usadas pelo ransomware para propagar-se e infectar outras máquinas na rede local.

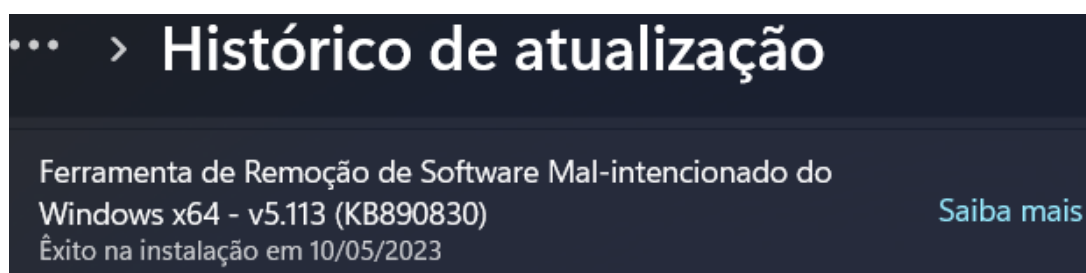
- **Utilizar firewalls de rede para filtrar e bloquear pacotes suspeitos:** ainda nas configurações do Firewall devemos manter ativado a proteção de rede deixando habilitado o Microsoft defender firewall, como mostra as imagens.

4.3 Reforçando a Segurança no Windows

Nesta seção, enfatizamos a importância de adotar uma abordagem na proteção do sistema operacional Windows 11, combinando ações do Antivírus e outras soluções de segurança para garantir uma defesa robusta contra ameaças cibernéticas em constante evolução. Descrevemos como as políticas de segurança do Antivírus do Windows 11 foram ajustadas para restringir a execução de scripts e macros não confiáveis.

- **Utilizar balanceadores de carga para distribuir o tráfego entre servidores e evitar sobrecargas.**
- **Implementar serviços de proteção DDoS fornecidos por provedores de rede especializados.**
- **Fazer farreduras da Ferramenta de Remoção do Windows mantendo os últimos patches de segurança atualizados, podemos ver na figura 25.**

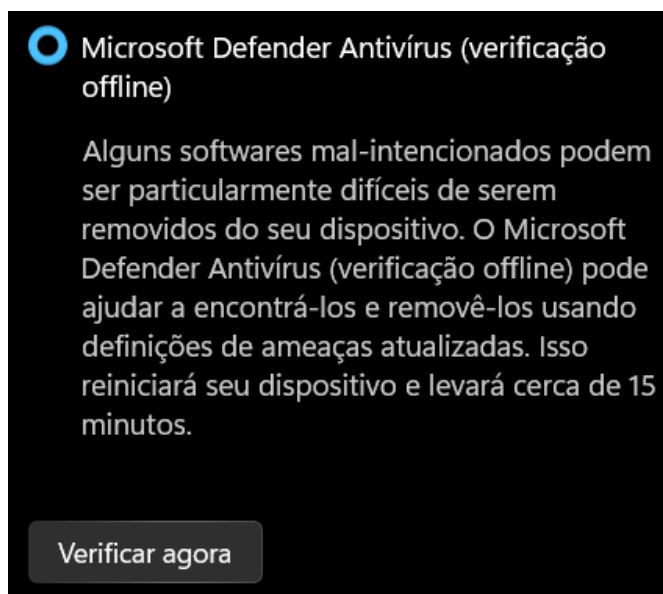
Figura 25 – Ferramenta de Remoção de Software Mal-intencionado do Windows x64 - v5.113.



Fonte: Autor

- **Utilizar softwares de segurança, como o Windows Defender, para proteger contra malware conhecidos e desconhecidos na figura 26.**

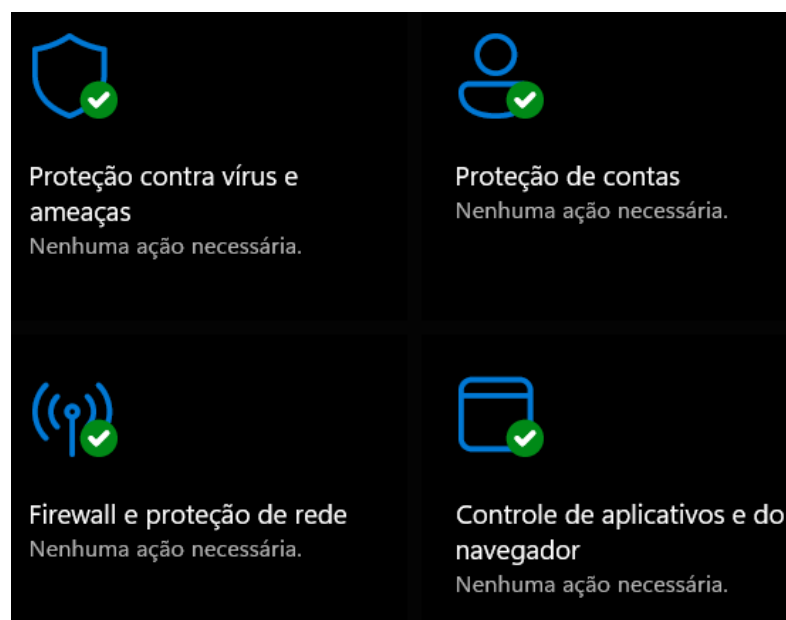
Figura 26 – Microsoft Defender Antivírus(verificação offline)



Fonte: Autor

- Instalar e manter um antivírus atualizado para identificar e bloquear arquivos maliciosos na figura 27.

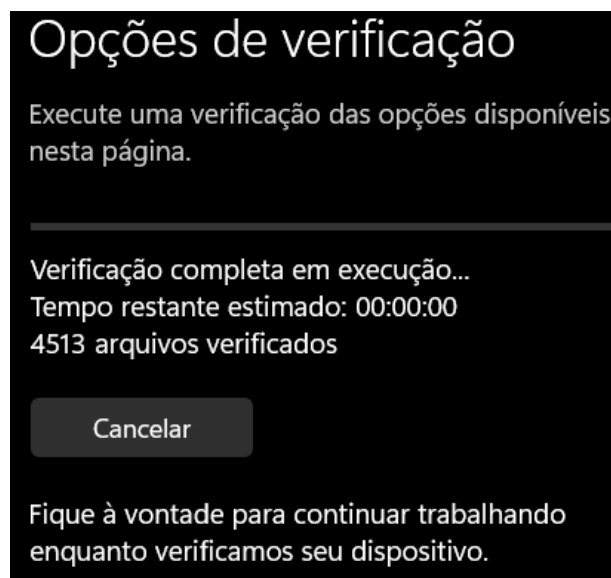
Figura 27 – Manter Todas Proteções Ativas



Fonte: Autor

- Fazer varreduras completas, a fim de verificar possíveis ameaças na figura 28.

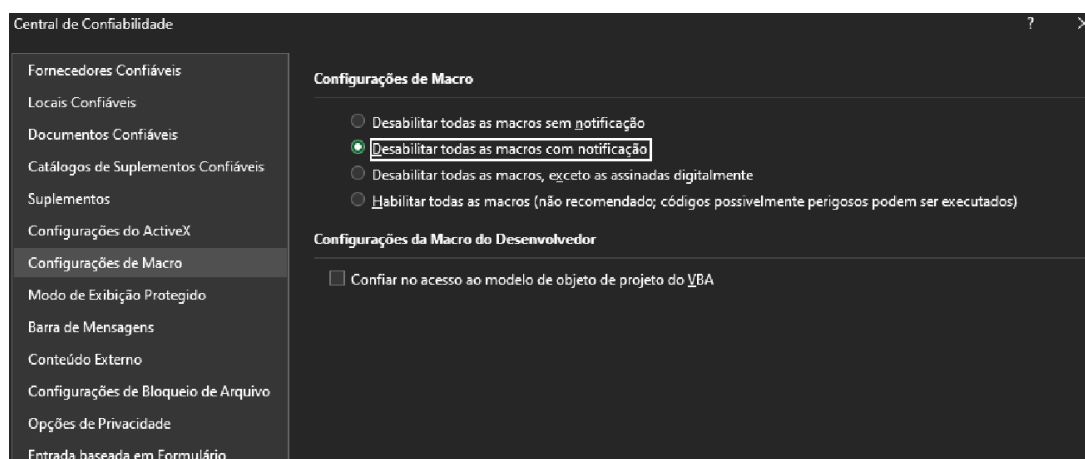
Figura 28 – Verificação Completa do Antivírus Para Varredura



Fonte: Autor

- **Defina permissões apropriadas para arquivos e pastas:** a fim de garantir que apenas usuários autorizados possam acessá-los.
- **Fazer backup regular de dados importantes:** faça backup regularmente de dados importantes e sensíveis em sistemas isolados, como unidades de armazenamento externas ou servidores de backup.
- **Manter o sistema operacional e os aplicativos atualizados.**
- **Usar políticas de segurança do Microsoft Office:** vamos configurar políticas de segurança para o Microsoft Office, na seção configurações da central de confiabilidade, vamos desabilitar a execução de macros ou habilitar apenas macros assinados digitalmente e confiáveis. Afim de restringir a execução de scripts e macros não confiáveis em aplicativos do Microsoft Office como vemos na figura 29.

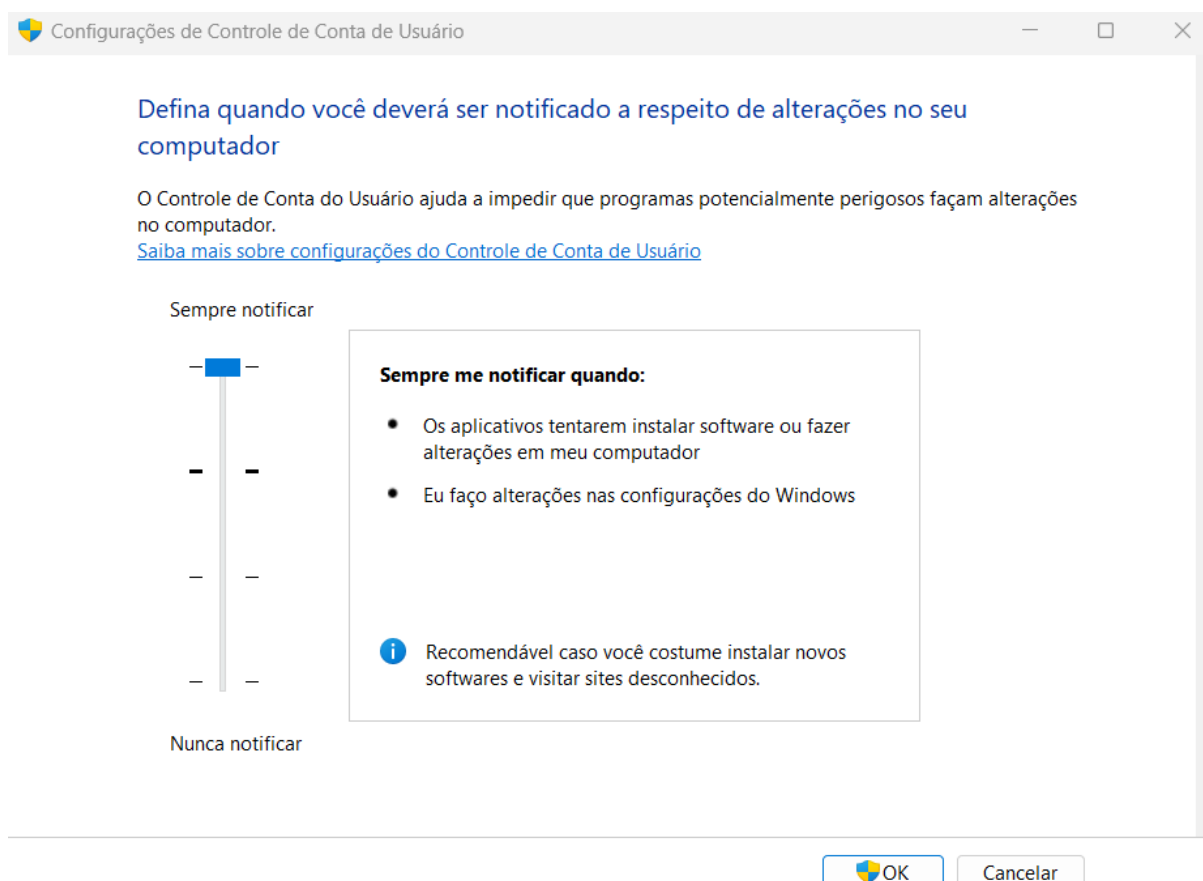
Figura 29 – Desabilitando execução de macros que não são de fonte confiáveis



Fonte: Autor

- **Ativar o recurso Controle de Conta de Usuário (UAC):** vamos ativar o UAC para evitar alterações não autorizadas no sistema e configurações importantes. O Windows solicitará a permissão do usuário sempre que uma alteração significativa estiver prestes a ser feita na figura 30.

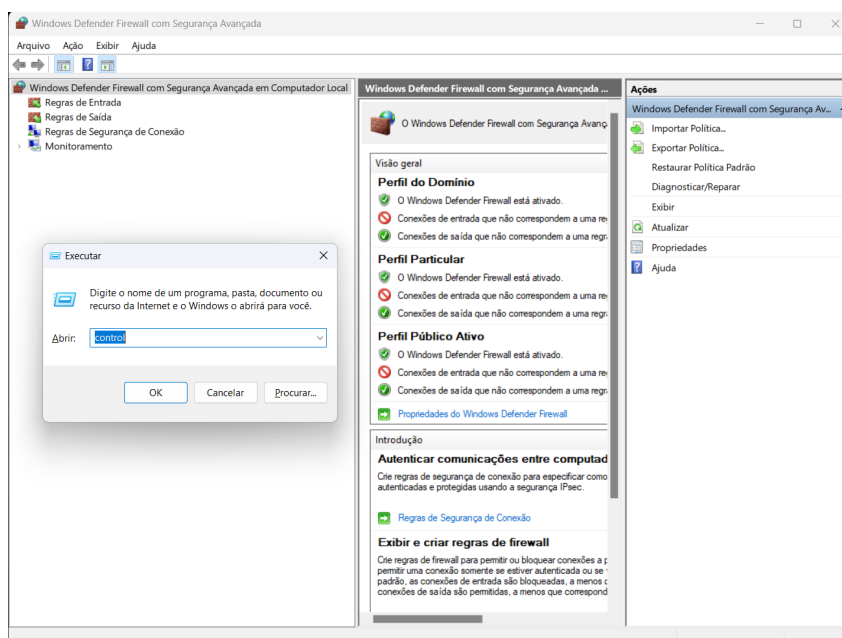
Figura 30 – Controle de Conta de Usuário



Fonte: Autor

- **Desabilitar o protocolo SMBv1, que é explorado pelo WannaCry:** para isso, vamos pressionar as teclas Win+R para abrir a caixa de diálogo Executar e vamos digitar `appwiz.cpl` para abrir os Programas e Recursos na figura 31.

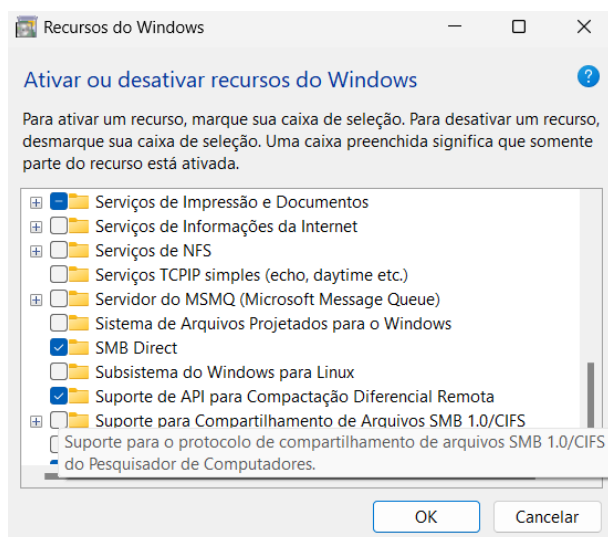
Figura 31 – Acessando o Programas e Recursos



Fonte: Autor

Em Seguida iremos desativar o suporte para compartilhamento de arquivos SMB 1.0/CIFS desmarcando a caixa, e vamos reiniciar o computador como vemos na figura 32.

Figura 32 – Desativando o Suporte Para o Protocolo de Compartilhamento de Arquivos SMB 1.0/CIFS



Fonte: Autor

- Configurar o firewall do Windows para bloquear tráfego indesejado mostrado na figura 33.

Figura 33 – Verificação Se Há Algum Tráfego Indesejado À Ser Bloqueado

Permitir que aplicativos se comuniquem através do Windows Defender Firewall

Para adicionar, alterar ou remover portas e aplicativos permitidos, clique em [Alterar configurações](#).

Quais são os riscos de permitir que um aplicativo se comunique?



Aplicativos e recursos permitidos:

Nome

Privada

Público

Fonte: Autor

4.4 Normas de Segurança da Informação: Orientações para Proteção

As duas normas relacionadas à esse trabalho seriam a ABNT NBR ISO/IEC 27001 e a ABNT NBR ISO/IEC 27002. Podemos pensar nessas normas como guias de navegação. A ABNT NBR ISO/IEC 27001 seria como um mapa geral, definindo os princípios e requisitos para conduzir e fornecer uma visão geral das rotas possíveis para manter a segurança da informação.

Agora, a ABNT NBR ISO/IEC 27002 seria semelhante a um conjunto detalhado de instruções de navegação. Ela oferece diretrizes específicas para práticas de segurança da informação, descrevendo as ações precisas que deve seguir para proteger seu sistema. Isso inclui orientações sobre como configurar o firewall, proteger sistemas Windows e usar o iptables com eficácia.

O estudo dessas normas, desempenham um papel fundamental na definição das melhores práticas para a segurança cibernética, fornecendo um guia para a implementação de soluções de segurança em resposta às ameaças do ransomware. Essas normas oferecem estabelecer políticas de segurança sólidas, configurar soluções de firewall e no Windows e garantir a proteção dos dados contra ameaças cibernéticas.

5 Conclusão

Através desta pesquisa e revisão bibliográfica abrangente sobre ransomware, explorando suas tipologias, curiosidades, algoritmos de ataque, normas de segurança e abordagens de ataque. A análise do ransomware, proporcionou uma compreensão das ameaças cibernéticas enfrentadas atualmente. A implementação de uma pesquisa para medir o nível de conhecimento das pessoas sobre segurança cibernética proporcionou percepções valiosas, destacando a importância da conscientização sobre esse tema crucial. A realização de simulações controladas de ataques ransomware e ataque de negação de serviço distribuído em um ambiente seguro permitiu observar os mecanismos desses ataques e seus efeitos.

As simulações da execução dos códigos de ataque, ao poder ser executado e explorar vulnerabilidades, enfatizam a necessidade de adotar abordagens de proteção multicamadas contra ameaças cibernéticas, empregando ferramentas como o iptables para bloquear as portas de entrada de ataques WannaCry e DDoS. Além disso, foram aplicadas melhorias no firewall do Windows, fortalecendo ainda mais a segurança e bloqueando as principais portas vulneráveis.

Este estudo destaca a importância contínua de medidas proativas para proteger os sistemas e dados contra ameaças cibernéticas cada vez mais sofisticadas. A conscientização sobre segurança cibernética é crucial, assim como a implementação de práticas de segurança, como atualização de sistemas e softwares, uso de antivírus e firewalls, e a educação do usuário, desempenham papel crucial na defesa contra ameaças em constante evolução.

É fundamental ressaltar que a pesquisa e o estudo sobre ransomware devem ser guiados por princípios éticos e legais. A disseminação de conhecimentos deve ser feita com responsabilidade, evitando o uso de informações para fins maliciosos.

Por fim, este trabalho busca contribuir para a área de segurança cibernética, promovendo a conscientização, o desenvolvimento de soluções eficazes e a adoção de medidas de segurança responsáveis. Ao fazê-lo, visa proteger a segurança e a privacidade das pessoas e organizações, auxiliando na prevenção e mitigação de ameaças cibernéticas, incluindo o ransomware. É fundamental enfrentar esses desafios, protegendo ativamente nossos sistemas e dados em um cenário cada vez mais digital e interconectado.

5.1 Limitações e Trabalhos Futuros

Áreas de pesquisa adicionais podem contribuir para um entendimento mais abrangente das ameaças de ransomware e fornecer orientações práticas para aprimorar a segu-

rança cibernética em diferentes contextos.

5.1.1 Limitações do Trabalho Atual

Neste estudo, focamos principalmente em analisar e entender o Ransomware e suas implicações em sistemas e dispositivos específicos. No entanto, existem alguns pontos que este trabalho não abordou ou poderia ter aprofundado:

- Implementação de soluções de segurança de e-mail: O e-mail continua sendo uma das principais portas de entrada para ataques de ransomware. Portanto, um estudo mais aprofundado poderia se concentrar em implementações eficazes de soluções de segurança de e-mail para identificar e bloquear tentativas de phishing e ransomware.
- Prevenção em sites e aplicações web: Com a crescente sofisticação dos ataques cibernéticos, é fundamental proteger sites e aplicativos da web contra ransomware e outras ameaças. Um estudo futuro poderia investigar soluções práticas para proteger sistemas web contra ataques de ransomware.

5.1.2 Sugestões de Trabalhos Futuros

À medida que continuamos a pesquisar ransomware e segurança cibernética, além de enriquecer esse estudo com implementação de soluções de segurança de email, sites e aplicações web, existem várias direções promissoras para trabalhos futuros:

- Malware para smartphones: Uma área de pesquisa interessante seria explorar ransomware direcionado a smartphones. Isso envolve examinar as vulnerabilidades do sistema operacional Android, identificar como os usuários podem detectar comprometimento de segurança em seus telefones e abordar problemas específicos de ransomware para dispositivos móveis, como WannaLocker, DoubleLocker e LeakerLocker.
- Soluções de segurança para smartphones: Além de identificar vulnerabilidades, seria benéfico investigar e apresentar soluções de segurança eficazes para proteger smartphones e tablets contra ransomware.
- Medidas de segurança em redes locais: Considerando a prevenção a nível de rede, explorar como as configurações de segurança em roteadores e em redes locais podem ajudar a mitigar ameaças de ransomware seria um campo valioso de pesquisa. Isso pode incluir políticas de firewall personalizadas e outras medidas de proteção de rede.

Referências

- 4INFRA, R. *Tipos de Ransomware que podem atacar a empresa*. 2020. Acessado em abril de 2023. Disponível em: <<https://4infra.com.br/tipos-de-ransomware-que-podem-atacar-a-empresa>>. Citado na página 17.
- ALECRIM, E. *DDoS - Negação de Serviço Distribuído*. 2004. Disponível em: <<https://www.infowester.com/ddos.php>>. Citado na página 21.
- ANDERSON, R.; BIHAM, E.; KNUDSEN, L. *Serpent: A proposal for the Advanced Encryption Standard*. 1998. Fonte online. Disponível em: <<https://www.cl.cam.ac.uk/~rja14/Papers/serpent.pdf>>. Citado na página 18.
- ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. *ABNT NBR ISO/IEC 27002*. Rio de Janeiro, 2005. Tecnologia da Informação – Técnicas de Segurança – Código de Prática para a Gestão da Segurança da Informação. Citado na página 26.
- ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. *ABNT NBR ISO/IEC 27001*. Rio de Janeiro, 2006. Tecnologia da Informação – Técnicas de Segurança – Sistemas de Gestão de Segurança da Informação – Requisitos. Citado na página 26.
- ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. *ABNT NBR ISO/IEC 27005*. Rio de Janeiro, 2008. Tecnologia da Informação – Técnicas de Segurança – Gestão de Riscos de Segurança da Informação. Citado na página 27.
- ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. *ABNT NBR ISO/IEC 27004*. Rio de Janeiro, 2010. Tecnologia da Informação – Técnicas de Segurança – Gestão da Segurança da Informação — Medição. Citado na página 26.
- ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. *ABNT NBR ISO/IEC 27003*. Rio de Janeiro, 2011. Tecnologia da Informação – Técnicas de Segurança – Diretrizes para Implantação de um Sistema de Gestão da Segurança da Informação. Citado na página 26.
- ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. *ABNT NBR ISO/IEC 27017*. Rio de Janeiro, 2015. Tecnologia da Informação – Técnicas de Segurança – Código de Prática para Controles de Segurança da Informação para o Ambiente em Nuvem. Citado na página 27.
- AVAST. *O que são exploits?* 2022. Acessado em Março de 2023. Disponível em: <<https://www.avast.com/pt-br/c-exploits>>. Citado na página 19.
- BELCIC, I. *O que é o ransomware Locky?* 2019. Acessado em Março de 2023. Disponível em: <<https://www.avast.com/pt-br/c-locky>>. Citado na página 25.
- BELCIC, I. *Ransomware Petya: Como funciona e como se proteger*. 2019. Acessado em Maio de 2023. Disponível em: <<https://www.avast.com/pt-br/c-petya>>. Citado na página 25.
- BERRY, A.; HOMAN, J.; EITZMAN, R. *Threat Research: WannaCry Malware Profile*. 2017. S. 1. Citado na página 23.

- CONTROLENET. *Os 9 tipos de ataque Ransomware mais conhecidos na internet*. 2021. Acessado em Maio de 2023. Disponível em: <<https://www.controle.net/faq/9-tipos-de-ransomware-mais-conhecidos-na-internet#Reveton>>. Citado 2 vezes nas páginas 16 e 25.
- CRUZ, M. *O que é ransomware? Aprenda tudo sobre a ameaça e como removê-la*. 2017. Acessado em de Maio de 2017. Disponível em: <<https://www.techtudo.com.br/listas/2017/05/o-que-voce-precisa-saber-sobre-o-ransomware-wannacrypt.ghhtml>>. Citado na página 22.
- DAEMEN, J.; RIJMEN, V. *The Design of Rijndael: AES - The Advanced Encryption Standard*. [S.l.]: Springer, 2002. Citado na página 18.
- DANSIMP. *Como as explorações e os kits de exploração funcionam*. 2023. Acessado em abril de 2023. Disponível em: <<https://learn.microsoft.com/pt-br/microsoft-365/security/intelligence/exploits-malware?view=o365-worldwide>>. Citado na página 19.
- FERRIE, A. *Cryptography With Python - Fernet (Tutorial)*. 2018. Fonte online. Disponível em: <<https://cryptography.io/en/latest/fernet.html>>. Citado 2 vezes nas páginas 18 e 29.
- FLASHPOINT. *Facing Five Types of Ransomware and Cyber Extortion*. 2021. Acessado em Maio de 2023. Disponível em: <<https://flashpoint.io/blog/facing-five-types-of-ransomware-and-cyber-extortion/>>. Citado na página 17.
- GALAXKEY. *HOW DOES THE MAZE RANSOMWARE WORK?* 2021. Acessado em Maio de 2023. Disponível em: <<https://www.galaxkey.com/blog/how-does-the-maze-ransomware-work/>>. Citado na página 26.
- KAPERSKY. *Engenharia social - Definição*. 2023. Acessado em Maio de 2023. Disponível em: <<https://www.kaspersky.com.br/resource-center/definitions/what-is-social-engineeringview=o365-worldwide>>. Citado na página 19.
- KASPERSKY. *Bad Rabbit: nova epidemia de ransomware usa sites contaminados*. 2017. Acessado em Março de 2023. Disponível em: <<https://www.kaspersky.com.br/blog/bad-rabbit-nova-epidemia-de-ransomware-usa-sites-contaminados/9783/>>. Citado na página 24.
- LABS, M. B. *Ransom.Cerber*. 2021. Acessado em Março de 2023. Disponível em: <<https://www.malwarebytes.com/blog/detections/ransom-cerber>>. Citado na página 24.
- LABS, M. B. *Ransom.Crysis*. 2021. Acessado em Março de 2023. Disponível em: <<https://www.malwarebytes.com/blog/detections/ransom-crysis>>. Citado na página 24.
- LISKA, A.; GALLO, T. Ransomware: Defending against digital extortion. p. 1–18, 2016. Citado na página 17.
- LOIK, N. *Lições para equipes de segurança cibernética*. 2021. Acessado em Março de 2023. Disponível em: <<https://blogs.manageengine.com/portugues/2021/08/25/ransomware-colonial-pipeline-lico-es-para-equipes-de-seguranca-cibernetica.html>>. Citado na página 24.

- MALWAREBYTES. *Tudo sobre phishing*. 2021. Acessado em Maio de 2023. Disponível em: <<https://br.malwarebytes.com/phishing/>>. Citado na página 19.
- MESKAUSKAS, T. *What kind of malware is GoldenEye?* 2022. Acessado em Maio de 2023. Disponível em: <<https://www.pcrisk.com/removal-guides/10733-goldeneye-ransomware>>. Citado na página 25.
- MESKAUSKAS, T. *Instruções de remoção do ransomware .Fun*. 2023. Acessado em Abril de 2023. Disponível em: <<https://www.pcrisk.pt/guias-de-remocao/8343-fun-ransomware>>. Citado na página 25.
- MORAIS, C. H. J. P. Ransomware: segurança da informação e prevenção. Pontifícia Universidade Católica de Goiás, 2021. Citado na página 27.
- National Institute of Standards and Technology (NIST). *FIPS PUB 46-3: Data Encryption Standard (DES)*. 2001. Fonte online. Disponível em: <<https://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.46-3.pdf>>. Citado na página 18.
- OLIVEIRA, J. C. d. *Ransomware - Laboratório de Ataque do WannaCry*. 2018. Acessado Junho de 2023. Disponível em: <https://bdm.unb.br/bitstream/10483/23052/1/2018_JessicaCristinaDeOliveira_tcc.pdf>. Citado na página 23.
- PIMENTEL, J. E. de S.; CABRERA, D. A.; FORTE, C. E. Ransomware: do surgimento aos ataques “as a service”. In: *FatecSeg-Congresso de Segurança da Informação*. [S.l.: s.n.], 2021. Citado na página 28.
- PROJECT, N. *Netfilter Project - Documentação do iptables*. 2023. Acessado em Junho de 2023. Disponível em: <<https://netfilter.org/documentation/>>. Citado na página 27.
- PROLINX. *Ransomware As A Service: Conheça A Ameaça E Proteja Sua Empresa*. 2023. Acessado em fevereiro de 2023. Disponível em: <<https://prolinx.com.br/ransomware-as-a-service/>>. Citado na página 20.
- PROOF. *Wannacry: O primeiro ransomworm na indústria de cibersegurança*. 2017. P. 1. Citado na página 22.
- RIVEST, R. L.; SHAMIR, A.; ADLEMAN, L. A method for obtaining digital signatures and public-key cryptosystems. *Communications of the ACM*, v. 21, n. 2, p. 120–126, 1978. Citado na página 18.
- SAVAGE, K.; COOGAN, P.; LAU, H. The evolution of ransomware. *Symantec SECURITY RESPONSE*, p. 57, 2015. Disponível em: <<https://www.infowester.com/ransomware.php>>. Citado na página 15.
- SCHNEIER, B. *Description of a New Variable-Length Key, 64-Bit Block Cipher (Blowfish)*. 1994. Fonte online. Disponível em: <https://www.schneier.com/academic/archives/1994/09/description_of_a_new.html>. Citado na página 18.
- STALLINGS, W.; BROWN, L. *Computer Security: Principles and Practice*. [S.l.]: Pearson Education, 2017. Citado na página 20.
- ZAGHETTO, C. Ransomware: Este problema também pode ser seu. *TECNOLOGIAS EM PROJEÇÃO*, v. 8, n. 2, p. 1–18, 2017. Citado 2 vezes nas páginas 17 e 28.