MARINHA DO BRASIL
DIRETORIA DE ENSINO DA MARINHA
CENTRO DE INSTRUÇÃO ALMIRANTE ALEXANDRINO

CURSO DE APERFEIÇOAMENTO AVANÇADO EM
SEGURANÇA DA INFORMAÇÃO E COMUNICAÇÕES

TRABALHO DE CONCLUSÃO DE CURSO

CIBERCRIME E CIBERTERRORISMO: evolução dos ataques *ransomware* e prejuízos causados

PRIMEIRO-TENENTE HENRIQUE LOUZADA DE BARROS TORTELOTE

Rio de Janeiro
2023

PRIMEIRO-TENENTE HENRIQUE LOUZADA TORTELOTE

CIBERCRIME E CIBERTERRORISMO: evolução dos ataques *ransomware* e prejuízos causados

Monografia apresentada ao Centro de Instrução Almirante Alexandrino como requisito parcial à conclusão do Curso de Aperfeiçoamento Avançado em Segurança da Informação e Comunicações.

Orientadores:
Davidson Rodrigo Boccardo D. Sc.
1T Felipe Brum Aguiar da Costa

CIAA
Rio de Janeiro
2023

PRIMEIRO-TENENTE HENRIQUE LOUZADA TORTELOTE

CIBERCRIME E CIBERTERRORISMO: evolução dos ataques *ransomware* e prejuízos causados

Monografia apresentada ao Centro de Instrução Almirante Alexandrino como requisito parcial à conclusão do Curso de Aperfeiçoamento Avançado em Segurança da Informação e Comunicações.

Aprovada em _____

Banca Examinadora:

Banca Examinadora:

_____

Capitão de Mar e Guerra (RM1-EN) Gian Karlo Huback Macedo de Almeida – CIAA

gov.br Documento assinado digitalmente
DAVIDSON RODRIGO BOCCARDO
Data: 04/12/2023 22:39:43-0300
Verifique em https://validar.iti.gov.br

_____

Davidson Rodrigo Boccardo D. Sc. – Hospital Israelita Albert Einstein

_____

Capitão de Corveta Eclenice Antunes Guarany Dantas – CGAEM

_____

Primeiro-Tenente Felipe Brum Aguiar da Costa – NaPa Gravataí

CIAA
Rio de Janeiro
2023

Dedico esse trabalho aos pesquisadores e técnicos que, em seu trabalho silencioso e incessante, tornam o mundo cibernético um local mais seguro para o mundo. Que seu fogo sagrado brilhe sempre forte nos trazendo grandes inspirações e exemplos.

AGRADECIMENTOS

Agradeço primeiramente a Deus por tudo que tem me acompanhado até agora. Seu incessante amor pelos seus filhos é algo que todo o ser humano criado por ti deve aspirar com fé inabalável.

Segundo a minha esposa, Vivian, cuja compreensão e amor me trazem a alegria de estar vivo e seguir em frente, independente dos desafios que põe à minha frente. Seu apoio me levanta e me sustenta nessa trilha de altos e baixos que chamamos de vida. Obrigado por estar sempre presente ao meu lado.

Aos meus pais, Eliane e Washington, agradeço por toda educação e fé em minha pessoa, mesmo quando eu mesmo não possuía. O exemplo de vida dos dois me mostra o caminho que devo trilhar até hoje e com certeza continuarão a fazê-lo.

À minha irmã, Rebeca, obrigado por sempre conversar comigo em todas as ocasiões que a procurei. Saiba que, embora não mereça, fico muito feliz por você sempre dizer se inspirar em mim. Isso me faz querer ser uma pessoa cada vez melhor para ser digno de ser sua inspiração.

Aos meus grandes amigos que sempre me apoiaram e considero como irmãos, Derek, Felipe, Gabriel e Pedro, agradeço pela irmandade e desejo que nossa amizade continue até nosso perecer, independente da distância que estivermos.

Por último, mas não menos importante, minhas avós, aos meus sogros, minhas primas, meu padrinho, minha tia e todos as outras pessoas que fizeram e fazem parte de minha vida, meus sinceros agradecimentos. Minha jornada apenas começou, mas todos vocês se tornaram parte dela e fazem a diferença em minha vida.

“A melhor parte do futuro é que ele vem um dia de cada vez.”

Abraham Lincoln

CIBERCRIME E CIBERTERRORISMO: evolução dos ataques *ransomware* e prejuízos causados

Resumo

O presente trabalho investiga a evolução dos ataques de ransomware, lançados tanto por cibercriminosos quanto por ciberterroristas, e analisa os impactos diretos e indiretos causados a organizações e indivíduos. O aumento da digitalização global tem proporcionado inúmeros benefícios, mas simultaneamente, abriu portas para ameaças digitais em constante evolução. O estudo, pautado em uma metodologia de revisão bibliográfica de literatura especializada, buscou compreender as nuances desses ataques, desde suas origens e desenvolvimentos técnicos até os danos socioeconômicos e psicológicos resultantes. A pesquisa destaca a crescente sofisticação dos ataques, a transição entre motivações puramente econômicas para agendas ideológicas e políticas e a extensão dos prejuízos que vão além dos pagamentos de resgates, abrangendo despesas de recuperação, interrupções operacionais e danos reputacionais. A pesquisa também sublinha a importância de estratégias abrangentes de prevenção e resposta, salientando a necessidade de medidas técnicas combinadas com educação e treinamento. Como resultado, este estudo contribui para a literatura existente, oferecendo uma visão aprofundada sobre o panorama do ransomware e suas implicações na sociedade contemporânea.

Palavras- chave: cibercrime; ciberterrorismo; *ransomware*.

SUMÁRIO

1 INTRODUÇÃO

No atual cenário da era digital, onde sistemas interconectados permeiam diversos aspectos da vida cotidiana, benefícios incontestáveis são vivenciados diariamente. Por outro lado, essa conectividade trouxe consigo desafios notáveis, sendo o cibercrime e o ciberterrorismo manifestações preocupantes desse cenário. Entre as várias formas de ataques cibernéticos, o *ransomware*, caracterizado como software malicioso que impede o acesso a sistemas até que um resgate seja pago, destaca-se não só por seus impactos imediatos, mas também pela inquietação em torno de seu potencial uso em atividades de ciberterrorismo.

1.1 Justificativa e Relevância

Os ataques de *ransomware* têm registrado um crescimento acentuado, com implicações econômicas, operacionais e reputacionais substanciais para as entidades afetadas. Considerando sua amplitude e os desdobramentos potenciais em contextos de ciberterrorismo, é indispensável um estudo detalhado e profundo sobre o assunto.

1.2 Objetivos

1.2.1 Objetivo Geral

O objetivo geral desta pesquisa é realizar uma análise abrangente da evolução dos ataques de *ransomware* e dos respectivos prejuízos, sejam eles diretos ou indiretos, que impactam organizações e indivíduos.

1.2.2 Objetivos Específicos

Em termos específicos, esta pesquisa visa distinguir entre cibercrime e ciberterrorismo no contexto do *ransomware*, traçar o desenvolvimento histórico e técnico deste tipo de malware, avaliar seus impactos variados em entidades afetadas e explorar sua possível instrumentalização no campo do ciberterrorismo, com ênfase nas implicações geopolíticas.

1.3 Metodologia

A pesquisa se baseará exclusivamente em uma revisão bibliográfica, examinando literaturas acadêmicas, artigos de pesquisa, relatórios de segurança e publicações especializadas no domínio da segurança cibernética. Através dessa abordagem, busca-se consolidar um entendimento teórico e empírico acerca da evolução, impactos e nuances associadas aos ataques de *ransomware*.

2 FUNDAMENTAÇÃO TEÓRICA

A natureza complexa e multifacetada do mundo digital exige um entendimento claro das terminologias e conceitos que o permeiam. Esta seção procura elucidar as definições de cibercrime e ciberterrorismo, bem como diferenciar esses dois conceitos, a fim de estabelecer uma base sólida para análises subsequentes.

2.1Definição de crime cibernético

O cibercrime, ou crime cibernético, refere-se a atividades ilícitas que capitalizam a vulnerabilidade ou a má utilização de sistemas computacionais, redes e dispositivos digitais. Esse tipo de crime possui características únicas, tanto em sua execução quanto em sua dinâmica, derivadas do ambiente digital (ABLON, 2018).

2.1.1 Natureza e Tipos de Ataques Cibernéticos

Na arena digital, os ataques cibernéticos têm se tornado cada vez mais sofisticados, refletindo uma gama diversificada de objetivos dos atacantes e a contínua evolução das tecnologias defensivas. Para entender plenamente este cenário, é importante mergulhar nos conceitos técnicos que fundamentam os principais tipos de ataques.

O cenário global de ataques cibernéticos é complexo, com adversários que empregam uma miríade de técnicas avançadas e frequentemente interligadas. Esta diversidade reflete tanto a gama de possíveis objetivos dos atacantes quanto a evolução das tecnologias defensivas. A seguir estão elencados os principais conceitos técnicos, de acordo com Li e Liu (2021):

I. *Malwares*

a) Vírus: Programas maliciosos que se replicam, anexando-se a outros arquivos executáveis. Utilizam-se de técnicas como polimorfismo (mudança de sua assinatura) e metamorfismo (alterando seu código) para evitar detecção.
b) *Worms*: Operam de forma autônoma sem necessidade de se anexar a programas, e propagam-se explorando falhas na rede.
c) Cavalos de Troia: Disfarçados de programas benignos, não se replicam, mas abrem brechas para que outros malwares entrem.
d) *Ransomware*: Usam criptografia forte para bloquear dados do usuário, e geralmente possuem uma estrutura de comando e controle para gerenciar as infecções.

II. *Phishing*

a) *Phishing* Tradicional: Utiliza-se de técnicas de engenharia social em *e-mails* que imitam organizações legítimas, mas com URLs maliciosas.
b) *Spear Phishing*: Alvo específico, muitas vezes utilizando informações previamente coletadas para persuadir o alvo.
c) *Smishing: Phishing* via SMS, explorando confiança em mensagens de texto.
d) *Vishing*: Utiliza chamadas VOIP para mascarar a origem e persuadir a vítima.

III. Ataques de Força Bruta

Os ataques de força bruta, como o próprio nome sugere, são métodos utilizados por cibercriminosos para tentar obter acesso a um sistema ou informação por meio da tentativa sistemática de todas as combinações possíveis até encontrar a correta. Geralmente, esses ataques são direcionados contra sistemas de autenticação, como logins e senhas, buscando descobrir as credenciais corretas ao testar uma vasta quantidade de combinações em um curto período.

Os algoritmos de força bruta não se baseiam em brechas ou vulnerabilidades específicas do sistema-alvo; em vez disso, confiam no poder de processamento e na velocidade para tentar todas as combinações possíveis. A evolução da tecnologia e o advento das máquinas mais rápidas têm tornado esse tipo de ataque ainda mais eficaz, especialmente contra sistemas com senhas fracas ou padrões de senha previsíveis. Uma variante desse método é o ataque de dicionário, no qual o invasor usa uma lista pré-compilada de palavras ou frases comumente usadas, muitas vezes provenientes de vazamentos de dados anteriores, para tentar ganhar acesso.

IV. Ataques DDoS

a) Amplificação: Abusa de servidores mal configurados para amplificar o tráfego enviado ao alvo.
b) Reflexão: Envolve o uso de terceiros para enviar tráfego ao alvo, mascarando a origem real.
c) *Botnet*s: Redes de dispositivos infectados (como o Mirai) que geram tráfego em massa.

V. *Eavesdropping* e Intercepção

Eavesdropping e interceptação são termos utilizados no contexto da segurança da informação para descrever técnicas de espionagem onde terceiros não autorizados tentam capturar, monitorar ou interferir na comunicação entre duas partes. Estas técnicas podem ser usadas para roubar informações sensíveis, comprometer comunicações ou mesmo realizar ataques mais sofisticados.

O termo "*eavesdropping*", em sua essência, refere-se à prática de escutar secretamente conversas ou comunicações sem o conhecimento ou consentimento das partes envolvidas. No ambiente digital, *eavesdropping* pode ser visualizado como um ator mal-intencionado escutando o "tráfego" entre dois sistemas, buscando capturar dados como senhas, mensagens, informações de cartão de crédito e outros dados sensíveis. Por outro lado, "intercepção" vai além da simples escuta; envolve não apenas capturar a comunicação, mas também pode incluir a alteração ou redirecionamento dessa comunicação. Em termos práticos, um invasor pode interceptar uma mensagem, alterá-la e então enviá-la ao destinatário pretendido, causando todo tipo de consequência nefasta.

Proteger-se contra *eavesdropping* e interceptação é crucial no mundo digital moderno. O uso de protocolos de criptografia robustos, como o TLS (*Transport Layer Security*) e o HTTPS, pode ajudar a garantir que as comunicações entre partes sejam seguras e privadas. Além disso, redes privadas virtuais (VPNs) e outras técnicas de encapsulamento podem ser utilizadas para proteger os dados em trânsito. A conscientização dos usuários e a adoção de práticas de segurança, como verificar certificados digitais e evitar redes Wi-Fi públicas não seguras, são passos adicionais essenciais na luta contra essas formas de espionagem digital.

VI. Ataques *Man-in-the-Middle* (MitM)

a) ARP *Spoofing*: Envolve enviar mensagens ARP falsificadas para associar o MAC *address* do atacante ao IP legítimo de outro *host*.
b) SSL *Strip*: Converte uma conexão HTTPS segura em uma conexão HTTP insegura.

VII. *Exploits*

a) *Zero-Day*: Explora vulnerabilidades não conhecidas publicamente e, portanto, não corrigidas.
b) Injeção de SQL: Insere ou "injeta" um código SQL malicioso em uma *query*.

VIII. *Drive-by Downloads*

Utiliza-se de brechas em navegadores *web* ou *plugins* para executar códigos maliciosos sem interação do usuário. A natureza e a execução destes ataques evidenciam a necessidade de uma postura proativa e bem-informada em relação à segurança cibernética. As defesas devem ser multidimensionais e adaptáveis ao cenário de ameaças em constante evolução.

2.1.2 Mecanismos técnicos dos crimes cibernéticos

O espaço digital, apesar de suas inúmeras vantagens, se tornou um campo fértil para crimes devido à sua natureza expansiva e muitas vezes anônima. Com a sofisticação crescente da tecnologia, os crimes cibernéticos também evoluíram, utilizando uma variedade de mecanismos técnicos para atingir seus objetivos, estes listados a seguir. Explorar esses mecanismos é crucial para entender a complexidade do cenário atual de ameaças cibernéticas (LI & LIU, 2021).

a) Injeção de Código: Esta técnica envolve a inserção de código malicioso em um sistema para comprometê-lo ou extrair informações. Exemplos notáveis incluem Injeção SQL, onde comandos maliciosos são inseridos em uma consulta SQL, e *Cross-Site Scripting* (XSS), que permite que atacantes insiram scripts em páginas web vistas por outros usuários.
b) Engenharia Social: Um método que explora as interações humanas. Em vez de usar falhas técnicas, os criminosos persuadem indivíduos a revelar informações confidenciais. *Phishing*, onde e-mails fraudulentos solicitam informações pessoais, é um exemplo clássico.
c) *Rootkits*: Estes são conjuntos de software que dão acesso privilegiado a um sistema, permanecendo ocultos. Eles podem alterar componentes do sistema operacional ou software antivírus para evitar a detecção.
d) *Botnets:* Redes de computadores comprometidos, ou "zumbis", controlados por cibercriminosos. Eles podem ser usados para uma variedade de propósitos, desde ataques DDoS até mineração de criptomoedas sem o conhecimento do proprietário do sistema.
e) Técnicas de Ocultação: Para evitar a detecção, o malware frequentemente emprega técnicas para se esconder. Isso pode incluir polimorfismo, onde o malware muda seu

código a cada infecção, ou técnicas de evasão, como verificar se está sendo executado em um ambiente de análise.

f) *Exploits* de Dia Zero: Estes são ataques que visam vulnerabilidades desconhecidas nos softwares. Como são desconhecidos para os desenvolvedores e não foram corrigidos, são particularmente perigosos.
g) Técnicas de Propagação: Muitos malwares se propagam explorando vulnerabilidades em sistemas ou redes. Por exemplo, o *ransomware WannaCry* se espalhou explorando uma falha no Windows SMB.
h) *Man-in-the-Middle* (MitM): Nestes ataques, os criminosos interceptam e possivelmente alteram a comunicação entre duas partes. Isso pode ser usado para roubar informações ou inserir mensagens maliciosas.

2.1.3 Impacto e Motivações dos Ataques Cibernéticos

O cenário digital interconectado de hoje, embora uma fonte inestimável de inovação e conectividade, também trouxe consigo vulnerabilidades significativas. A amplitude e profundidade dos ataques cibernéticos têm impactos vastos, desde danos financeiros até perturbações geopolíticas. Para entender esse cenário, é crucial analisar o impacto desses ataques e as motivações por trás deles.

O impacto dos ataques cibernéticos é multifacetado. No nível corporativo, empresas enfrentam perdas financeiras diretas devido a fraudes ou extorsões, como vistas em ataques de *ransomware*. Além disso, danos à reputação após violações de dados podem ter efeitos duradouros na confiança do cliente e valor de mercado. Em uma escala mais ampla, infraestruturas críticas, como redes de energia, transporte e serviços de saúde, podem ser comprometidas, levando a interrupções de serviços essenciais e até mesmo potenciais perigos à vida humana (REINO UNIDO, 2023).

Em termos governamentais, a espionagem cibernética tem o potencial de extrair informações sensíveis, comprometendo a segurança nacional e estratégias geopolíticas. Ademais, ataques cibernéticos bem-sucedidos podem ser usados como ferramentas de desinformação, visando desestabilizar governos ou influenciar opiniões públicas (WEIMANN, 2004).

Por trás desses ataques, as motivações são igualmente variadas. Ganho financeiro continua sendo uma das principais razões para atividades cibernéticas maliciosas. Grupos de

cibercriminosos, frequentemente organizados e sofisticados, buscam lucros através de fraudes, extorsões ou roubo de informações que possuem valor no mercado negro.

Ideologia ou crenças também são impulsionadores significativos. “Hacktivistas”, por exemplo, realizam ataques para promover uma causa política, social ou ambiental. Em uma esfera ainda mais complexa, nações-estado patrocinam atividades cibernéticas para alcançar objetivos geopolíticos, seja através de espionagem, desinformação ou mesmo atos de guerra cibernética.

Também não podemos ignorar os atores que se engajam em atividades maliciosas simplesmente pelo desafio ou pela notoriedade. O mundo digital, com sua natureza interconectada e, muitas vezes, anônima, proporciona um playground para aqueles que buscam testar seus limites técnicos ou causar caos por pura satisfação pessoal.

2.1.4 Desafios de jurisdição e regulamentação em crimes cibernéticos

O cenário cibernético, com sua vastidão e constante evolução, introduz desafios particulares no âmbito da jurisdição e regulamentação. Segundo Ablon (2018), a natureza efêmera e muitas vezes descentralizada das atividades online desafia a aplicação de marcos legais tradicionais. Por exemplo, a ambiguidade territorial do ciberespaço significa que um crime pode ser planejado em um país, usando infraestrutura de vários lugares e atingindo vítimas em uma nação totalmente diferente. Isso complica a determinação da jurisdição aplicável e as nuances da cooperação internacional ou extradição.

Outro obstáculo significativo é a questão da atribuição. Determinar com precisão a origem de um ataque cibernético e seus perpetradores é uma tarefa complexa. A capacidade dos atacantes de usar técnicas de ocultação, servidores *proxy*, VPNs e redes globais de *botnets* significa que a verdadeira origem e intenção por trás de um ataque podem permanecer encobertas. Isso, por sua vez, complica as respostas legais e as possíveis retaliações.

Além disso, a natureza acelerada da inovação tecnológica muitas vezes supera a velocidade de desenvolvimento de leis e regulamentos, resultando em uma lacuna onde novas formas de cibercrime podem operar em zonas cinzentas não abordadas pela legislação em vigor (IST, 2021). A situação é ainda mais complicada pela variedade de interesses nacionais. Alguns países podem buscar rigor na regulamentação cibernética, enquanto outros podem optar por abrigar ou mesmo patrocinar atividades cibernéticas maliciosas, seja por motivos econômicos, geopolíticos ou outros.

Há também uma necessidade urgente de normas e padrões globais. Embora haja movimentos para estabelecer acordos internacionais sobre cibersegurança e crimes cibernéticos, a falta de consenso sobre responsabilidades, definições e sanções apropriadas torna difícil alcançar uma uniformidade global.

Por fim, em meio a todos esses desafios, está a questão premente da privacidade e dos direitos civis. Enquanto a detecção e prevenção de crimes cibernéticos são cruciais, elas devem ser equilibradas com os direitos dos cidadãos à privacidade e proteção contra a vigilância excessiva. Em suma, os desafios de jurisdição e regulamentação no espaço cibernético requerem um equilíbrio cuidadoso, colaboração global e uma abordagem adaptável que reconheça a natureza fluida e complexa do ambiente digital.

2.2Definição de terrorismo cibernético

O terrorismo cibernético marca uma nova fronteira na tapeçaria das ameaças globais, fundindo as motivações tradicionais do terrorismo com a vulnerabilidade do ciberespaço. Esta forma de terrorismo, embora ancorada em princípios ideológicos, políticos ou sociais semelhantes aos do terrorismo convencional, é distinta na sua execução e potencial de dano.

No âmago do terrorismo cibernético, reside a aspiração de causar perturbação. Em vez de se centrar no ganho pessoal, como é comum em muitos crimes cibernéticos, o terrorismo cibernético é motivado por objetivos mais amplos, muitas vezes buscando causar interrupções massivas, semear medo ou promover uma causa particular. Isso pode ser visto em tentativas de desativar redes de comunicação, manipular sistemas de transporte ou energia, ou comprometer estruturas financeiras.

Uma característica particularmente insidiosa do terrorismo cibernético é sua capacidade de influenciar a percepção pública. Semelhante aos atentados terroristas tradicionais que visam incutir medo na população, os ataques cibernéticos podem gerar dúvidas sobre a robustez e confiabilidade dos sistemas digitais dos quais a sociedade moderna é tão dependente. Em algumas instâncias, os ataques são acompanhados de proclamações ou manifestos que buscam justificar ou esclarecer as intenções dos atacantes, aumentando a ressonância de seus atos (WEIMANN, 2004).

Outro aspecto preocupante é a natureza transnacional do terrorismo cibernético. O ciberespaço não conhece fronteiras geográficas, permitindo que indivíduos ou grupos

conduzam operações de qualquer canto do planeta. Isso não só complica os esforços de detecção e prevenção, mas também cria desafios diplomáticos e jurídicos.

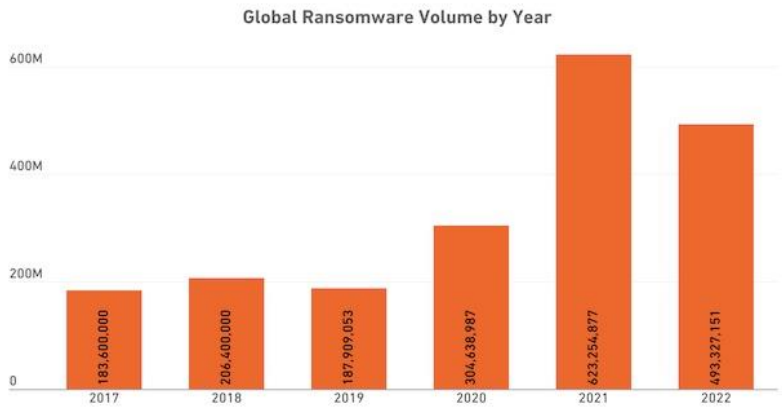
Contudo, é essencial uma abordagem ponderada ao termo "terrorismo cibernético". Segundo Weimann (2004), em uma era de crescente conectividade e sensacionalismo, é fácil rotular prematuramente certos incidentes cibernéticos como "terrorismo". Uma compreensão clara e uma classificação adequada são vitais para garantir que as respostas sejam proporcionais e eficazes.

3 HISTÓRICO DOS ATAQUES DE RANSOMWARE

O *ransomware*, uma das formas mais insidiosas de cibercrime, evoluiu ao longo das décadas, tornando-se uma ameaça crescente para indivíduos, empresas e infraestruturas críticas. Nesta seção, examinaremos as origens dos ataques de *ransomware*, sua evolução técnica e o impacto social e psicológico que causam nas vítimas.

No gráfico abaixo, percebe-se uma evolução constante de ataques de ranswomware em todo o mundo, diminuindo apenas em 2022, mas isso não exime o perigo do aumento no número de casos nos próximos anos.

Figura 1: Gráfico de ataques por ransomware no Relatório de Ameaças Cibernéticas da SonicWall



Fonte: The Channel Company CRN (2023)[1]

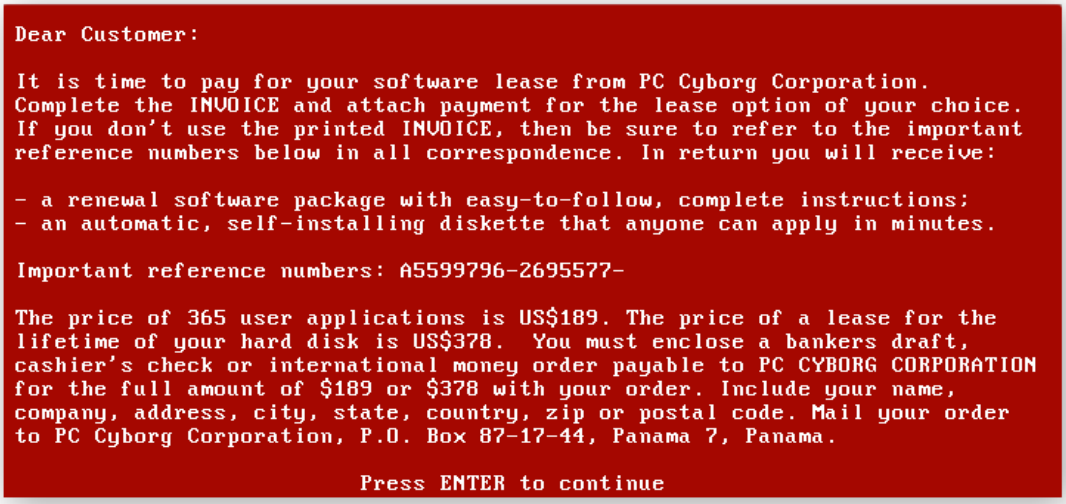
3.1 Origens e Primeiros Casos de *Ransomware*

[1] The Channel Company CRN. Ransomware Attacks Plunged 48 Percent In US Last Year: SonicWall Disponível em: <https://www.crn.com/news/security/ransomware-attacks-plunged-48-percent-in-us-last-year-sonicwall>. Acesso em: 10 out. 2023.

O conceito de *ransomware*, embora pareça um fenômeno recente, remonta a várias décadas atrás. Sua evolução tem sido marcada por notáveis avanços tecnológicos e estratégicos, mas também por ataques de alto perfil que catalisaram a consciência pública sobre a ameaça.

O primeiro exemplo conhecido de *ransomware* foi o "AIDS *Trojan*" de 1989, também referido como "PC *Cyborg*". Criado por Joseph Popp, este malware foi distribuído através de disquetes sob o pretexto de um programa que avaliava o risco de infecção por HIV. Uma vez instalado, o trojan contava o número de vezes que o computador era ligado e, após 90 ciclos, ocultava diretórios e criptografava nomes de arquivos no disco rígido, solicitando ao usuário que pagasse U$189 para "renovar a licença" e, por extensão, descriptografar seus arquivos (O'KANE et al, 2018).

Figura 2: Mensagem exibida na tela de dispositivo infectado com o AIDS Trojan



Fonte: AVAST (2021)[2]

No entanto, foi só no início dos anos 2000, com a popularização da internet e o advento das criptomoedas, que o *ransomware* realmente começou a se estabelecer como uma ferramenta preferida dos cibercriminosos. O aparecimento de variantes como o "*CryptoLocker*" em 2013 marcou uma mudança significativa na paisagem do *ransomware*. Ao contrário de seus predecessores, o *CryptoLocker* usava criptografia RSA de força militar, tornando quase impossível para as vítimas recuperarem seus arquivos sem a chave privada detida pelos cibercriminosos (O'KANE et al, 2018).

[2] AVAST. Guia básico sobre ransomware. Disponível em: <https://www.avast.com/pt-br/c-what-is-ransomware>. Acesso em: 15 out. 2023.

Segundo o trabalho de TrendMicro (2017), outros exemplos emblemáticos de ataques por *ransomware* incluem:

a) *WannaCry* (2017): Talvez um dos ataques de *ransomware* mais notórios, afetou mais de 200.000 computadores em 150 países, com prejuízos estimados em bilhões de dólares. Este *ransomware* se espalhou aproveitando uma vulnerabilidade do Windows que havia sido inicialmente descoberta pela NSA (Agência de Segurança Nacional dos EUA).
b) *NotPetya* (2017): Apesar de se disfarçar como *ransomware*, muitos especialistas acreditam que o principal objetivo do NotPetya era causar disrupção. Ele causou estragos em várias organizações globais, incluindo a Maersk, a maior empresa de transporte de contêineres do mundo.
c) *Bad Rabbit* (2017): Este *ransomware* se espalhou principalmente na Rússia e Ucrânia, afetando infraestruturas importantes, incluindo aeroportos e estações de metrô.
d) *SamSam* (2018): Distinto de outras formas de *ransomware* que se espalharam via *phishing* ou explorações de larga escala, o *SamSam* foi usado em ataques mais direcionados. O município de Atlanta, nos EUA, foi uma das vítimas de destaque, com muitos serviços municipais sendo interrompidos por vários dias.

Estes ataques notáveis representam apenas a "ponta do *iceberg*". À medida que o *ransomware* se tornou mais lucrativo, novas variantes surgiram, cada uma com suas próprias táticas, técnicas e procedimentos. O aumento contínuo desses ataques reforça a necessidade de robustas medidas de segurança cibernética, conscientização do usuário e cooperação internacional para combater essa ameaça crescente (SAVAGE et al, 2015).

Figura 3: Mensagem exibida na tela de dispositivo vítima do WannaCry

Fonte: TechTudo (2017) [3]

3.2Evolução Técnica do *Ransomware*

A evolução técnica do *ransomware* ao longo dos anos reflete o cenário dinâmico e constantemente mutável da segurança cibernética e da ameaça cibernética. O que começou como simples bloqueadores de tela ou códigos que obscureciam diretórios evoluiu para sofisticados malwares que utilizam criptografia de ponta, técnicas de evasão e infraestruturas resilientes para executar e sustentar seus ataques.

De acordo com Beaman et al (2021), a introdução da criptografia foi um divisor de águas na história do *ransomware*. Ao contrário dos primeiros *ransomwares* que apenas bloqueavam o acesso do usuário ao sistema, os criptográficos, como o notório "*CryptoLocker*", utilizam algoritmos robustos para criptografar os dados da vítima. A utilização da criptografia RSA de 2048 bits pelo *CryptoLocker*, por exemplo, tornou quase impossível para as vítimas recuperarem seus dados sem a chave de descriptografia. Este movimento em direção à criptografia avançada significava que as organizações e os

[3] TechTudo. WannaCry: tudo que você precisa saber sobre o ransomware. Disponível em: <https://www.techtudo.com.br/listas/2017/05/o-que-voce-precisa-saber-sobre-o-ransomware-wannacrypt.ghtml>. Acesso em: 15 ago. 2023.

indivíduos não estavam apenas enfrentando uma inconveniência temporária, mas a potencial perda permanente de dados críticos.

Com a proliferação do *ransomware*, o mercado negro também viu a ascensão do *Ransomware as a Service* (RaaS). Esta tendência envolve cibercriminosos oferecendo plataformas de *ransomware* completas para venda ou aluguel. Estes serviços, muitas vezes hospedados em mercados da *dark web*, oferecem uma interface amigável, atualizações regulares e até suporte ao cliente, permitindo até mesmo a criminosos inexperientes lançarem ataques sofisticados com pouco conhecimento técnico.

Outra inovação técnica é a implementação de mecanismos de evasão. Muitos *ransomwares* modernos são projetados para detectar ambientes de análise, como máquinas virtuais ou *sandboxes*, e interromper sua execução nesses contextos para evitar a detecção. Técnicas como empacotamento, ofuscação de código e uso de *exploits* de dia zero também são comuns para evitar soluções de segurança tradicionais.

Além disso, a propagação do *ransomware* também viu uma evolução técnica. Enquanto os primeiros frequentemente dependiam de engenharia social ou campanhas de *phishing* para infecção, variantes mais recentes, como o "WannaCry" e "*NotPetya*", exploraram vulnerabilidades em sistemas operacionais para se propagar automaticamente através de redes (IST, 2021).

O surgimento do *ransomware* de dupla extorsão marca a mais recente evolução no panorama da ameaça. Além de criptografar os dados da vítima, esses *malwares* também roubam informações, ameaçando vazar ou vender os dados se o resgate não for pago. Isso adiciona uma camada adicional de pressão sobre as vítimas e complica as considerações sobre se pagar ou não o resgate.

3.3Principais Variantes de *Ransomware* ao Longo dos Anos

O *ransomware*, como categoria de malware, tem se adaptado e evoluído constantemente, com novas variantes surgindo regularmente para explorar diferentes vulnerabilidades e empregar táticas inovadoras. Ao longo dos anos, algumas destas variantes destacaram-se não apenas por sua sofisticação técnica, mas também pelo impacto e alcance de seus ataques. Nesta seção, exploramos as principais variantes de ransomware que deixaram uma marca indelével na paisagem da segurança cibernética (EGNYTE, 2021):

a) *CryptoLocke*r (2013): Uma das primeiras variantes a usar criptografia de força militar, o *CryptoLocker* representou um marco na história dos ataques de *ransomware*. Distribuído principalmente por meio de anexos de e-mail maliciosos, ele focava em arquivos específicos, como documentos e imagens, e exigia pagamento em Bitcoin.
b) CTB *Locker* (2014): Uma evolução do *CryptoLocker*, o CTB *Locker* diferenciava-se por seu uso de criptografia elíptica, uma abordagem que permitiu ataques mais rápidos. Além disso, a variante oferecia suporte multilíngue, visando vítimas em diferentes regiões geográficas.
c) *TeslaCrypt* (2015): Inicialmente direcionado a gamers, o *TeslaCrypt* visava especificamente arquivos relacionados a mais de 40 videogames. Com o tempo, no entanto, expandiu seu escopo para incluir outros tipos de arquivos e tornou-se uma das variantes dominantes na época.
d) *Locky (*2016): Disseminado por meio de documentos do Microsoft Word contaminados, o *Locky e*ra notório por sua capacidade de criptografar mais de 160 tipos de arquivos. Suas campanhas de distribuição eram massivas, chegando a enviar até 400.000 e-mails maliciosos em um único dia.
e) *WannaCry* (2017): Como mencionado anteriormente, o *WannaCry* foi notável não apenas por sua escala, mas também por sua capacidade de explorar uma vulnerabilidade do Windows conhecida como *EternalBlue*. A velocidade e extensão de sua propagação o tornaram um dos *ransomwares* mais devastadores da história.
f) Ryuk (2018): Originado da Coreia do Norte, o Ryuk é particularmente preocupante devido ao seu foco em organizações de grande porte, especialmente aquelas com infraestruturas críticas, como hospitais e entidades governamentais. É conhecido por suas demandas de resgate exorbitantes, frequentemente chegando a centenas de milhares de dólares.
g) Dharma (2019): Uma variante particularmente prolífica, o Dharma é conhecido por seus múltiplos subtipos e sua capacidade de constantemente se adaptar. Muitas de suas variantes são oferecidas como *Ransomware-as-a-Service* (RaaS), permitindo que outros cibercriminosos realizem ataques sem necessidade de expertise técnico.
h) Maze (2019-2020): Além de suas táticas convencionais de *ransomware*, o Maze introduziu uma abordagem dupla de extorsão. Antes de criptografar os dados das vítimas, ele os extrai, ameaçando divulgá-los publicamente caso o resgate não seja pago.

Estas variantes representam apenas uma fração das inúmeras iterações de *ransomware* que surgiram ao longo dos anos. A contínua evolução destas ameaças sublinha a

importância da adaptação constante das estratégias de defesa e da conscientização sobre segurança cibernética para enfrentar essas ameaças em constante mudança.

4 ANÁLISE DO IMPACTO DOS ATAQUES DE RANSONWARE

O advento e proliferação dos ataques de *ransomware* representam uma das maiores ameaças no panorama atual da segurança cibernética. Estes ataques têm consequências que vão muito além da simples extorsão financeira, afetando a economia, a infraestrutura crítica e o tecido social (TRENDMICRO, 2017). A análise subsequente detalha o impacto multifacetado dos ataques de *ransomware.*

4.1Prejuízos Econômicos Diretos e Indiretos

O impacto financeiro do *ransomware* é monumental, e os custos associados a esses ataques são diversificados e, frequentemente, de longo alcance. Para compreender a magnitude dessas cifras, é crucial analisar tanto os prejuízos diretos quanto os indiretos.

4.1.1 Prejuízos Diretos

a) Pagamento de Resgates: A extorsão financeira por meio de *ransomware* tornou-se uma indústria lucrativa para os criminosos. Segundo estimativas do relatório da *Cybersecurity Ventures*, previa-se que os pagamentos de resgates alcançariam cerca de U$20 bilhões em 2021, representando um aumento dramático em relação aos U$11,5 bilhões em 2019. Esses números, no entanto, só retratam os pagamentos conhecidos. Muitas organizações optam por não divulgar tais pagamentos por receio de danos à reputação ou de futuros ataques.
b) Perda de Dados e Custos de Recuperação: Apesar de muitas vítimas pagarem o resgate, nem sempre os dados são recuperados. Estima-se que 1 em cada 5 empresas que pagam o resgate não recuperam seus dados. Além disso, os custos de restauração dos sistemas podem exceder significativamente o montante do resgate. Por exemplo, a cidade de Atlanta, em 2018, foi atingida por um ataque de *ransomware* com um resgate de U$51.000, mas os custos de recuperação ultrapassaram U$17 milhões, considerando a reconstrução da infraestrutura de TI e outras despesas correlatas.

4.1.2 Prejuízos Indiretos

a) Interrupção Operacional e Perda de Receita: A paralisação das operações comerciais devido a um ataque de *ransomware* pode resultar em perdas de receita significativas. Por exemplo, a gigante global de logística, Maersk, sofreu uma interrupção em 2017 devido ao *ransomware* NotPetya, levando a uma perda estimada de U$300 milhões.
b) Dano à Reputação: O valor da confiança e reputação para uma marca é imensurável. Um ataque bem divulgado pode levar à perda de clientes e depreciação das ações no mercado de valores. Após ataques significativos, algumas empresas observaram quedas significativas em suas avaliações de mercado, refletindo a desconfiança dos investidores e clientes.
c) Custos de Prevenção e Formação: Posteriormente a um ataque, muitas empresas investem consideravelmente em melhorias de segurança e formação de funcionários, incrementando ainda mais os custos indiretos associados ao *ransomware*.

Em perspectiva, enquanto o resgate em si é uma grande despesa, os custos indiretos, muitas vezes, ultrapassam o valor inicialmente exigido pelos atacantes. A somatória de prejuízos diretos e indiretos demonstra o peso econômico que o ransomware impõe ao cenário global, exigindo das organizações uma postura proativa na prevenção e preparação para tais ameaças.

4.2Prejuízos em Serviços de Infraestrutura Crítica

A infraestrutura crítica é indiscutivelmente o pilar que sustenta a funcionalidade e o progresso das sociedades contemporâneas, englobando setores cruciais como energia, água, transportes, saúde e comunicações. Uma perturbação significativa nesses serviços pode gerar consequências devastadoras, tanto economicamente quanto para a segurança e bem-estar das populações (ABLON, 2018).

No setor energético, ataques têm sido frequentes e preocupantes. Em 2017, o *ransomware WannaCry* impactou a empresa estatal de petróleo e gás da Ucrânia, enquanto o NotPetya paralisou operações de empresas de energia em diversas regiões, incluindo a Índia. Além disso, em 2019, um ataque de *ransomware* afetou as operações de uma empresa de serviços de energia nos EUA, causando interrupções no fornecimento de energia para milhares de residências (SULLIVAN, 2021).

A segurança hídrica é uma área de crescente preocupação. Recentemente, um tratamento de água na Flórida foi comprometido por um ataque que tentou alterar os níveis

químicos da água potável. O rápido reconhecimento e resposta impediram um potencial desastre de saúde pública.

Os sistemas de saúde, com sua vasta rede de equipamentos conectados e bancos de dados, têm se mostrado vulneráveis. A paralisação do Serviço Nacional de Saúde do Reino Unido pelo *WannaCry* foi apenas um de muitos ataques que têm perturbado os serviços médicos globalmente.

No âmbito dos transportes, o sistema de transporte de São Francisco foi apenas um dos alvos. A infraestrutura de transporte da cidade de Atlanta, nos EUA, também foi comprometida em 2018, causando grandes interrupções nos serviços de trânsito.

O setor de comunicações é igualmente vulnerável. Em 2020, uma grande empresa de telecomunicações foi vítima de um ataque que interrompeu as comunicações e custou milhões em danos.

Vulnerabilidades em sistemas de infraestrutura crítica muitas vezes se devem a software desatualizado, uso insuficiente de criptografia, redes mal configuradas e falta de treinamento adequado para funcionários. A mitigação passa por atualizações regulares de sistemas, emprego de firewalls avançados, sistemas de detecção de intrusões, treinamento contínuo para o pessoal e estabelecimento de protocolos rigorosos de resposta a incidentes.

Ao olhar para o futuro, torna-se evidente que, enquanto a digitalização da infraestrutura crítica oferece inúmeras vantagens em termos de eficiência e capacidade de resposta, ela também apresenta desafios significativos em termos de segurança. As soluções passam por uma abordagem multifacetada, que combina tecnologia, educação e políticas robustas.

4.3Impacto Social e Psicológico dos Ataques de *Ransomware*

Os ataques de *ransomware* não se limitam apenas a danos técnicos e financeiros; eles também deixam marcas profundas no tecido social e na psicologia das vítimas. Por um lado, o *ransomware* tem o potencial de interromper significativamente a operação de serviços essenciais, como hospitais, transportes públicos e serviços municipais, criando, assim, uma sensação palpável de vulnerabilidade na sociedade. Este tipo de interrupção pode resultar em consequências diretas, como atrasos em tratamentos médicos críticos ou falhas em sistemas de transporte que milhões de pessoas dependem diariamente.

A natureza intrusiva do *ransomware*, que frequentemente envolve a criptografia de dados pessoais e a subsequente demanda de pagamento, também pode levar a um

sentimento generalizado de violação entre as vítimas. Este sentimento é exacerbado pelo dilema moral que as vítimas enfrentam: pagar o resgate e potencialmente financiar atividades criminosas ou não pagar e arriscar perder dados valiosos ou até insubstituíveis.

Em um nível mais amplo, ataques bem-sucedidos de *ransomware* podem abalar a confiança do público nas instituições (LI, 2021). Quando organizações de grande porte ou entidades governamentais caem vítimas de tais ataques, isso pode levar a questionamentos sobre a competência e a capacidade dessas entidades de proteger informações e infraestruturas críticas.

Além disso, o aspecto psicológico se estende além das vítimas imediatas. À medida que os ataques de *ransomware* ganham destaque na mídia, o público em geral pode começar a temer pela sua própria segurança digital, mesmo que não tenham sido diretamente afetados. Essa atmosfera de medo e incerteza pode levar a uma hesitação generalizada em relação à adoção de novas tecnologias ou à desconfiança em relação às redes e sistemas digitais.

Em resposta a esses desafios, diversas entidades, incluindo empresas privadas e agências governamentais, têm intensificado seus esforços para oferecer soluções de segurança e apoio às vítimas. Grupos como *No More Ransom*, uma parceria público-privada, fornecem ferramentas para ajudar vítimas a recuperar seus dados sem pagar resgates, enquanto agências governamentais ao redor do mundo intensificam seus esforços de conscientização e capacitação em segurança cibernética.

5 O *RANSOMWARE* COMO FERRAMENTA DE CIBERTERRORISMO

A ascensão do ciberespaço trouxe consigo uma nova arena para conflitos, competições e, infelizmente, terrorismo. Os ciberataques são cada vez mais comuns, com o *ransomware* tornando-se uma ferramenta potente nas mãos de grupos terroristas. Seus efeitos, que transcendem fronteiras nacionais, têm implicações profundas na geopolítica e exigem uma resposta robusta das nações.

5.1Motivações por trás dos ataques de ciberterrorismo

O ciberterrorismo, uma manifestação digital do terrorismo tradicional, é alimentado por uma confluência de motivações profundamente enraizadas em tensões geopolíticas, ideológicas e econômicas (WEIMANN, 2004). No cerne de muitos atos de ciberterrorismo estão crenças ideológicas profundamente arraigadas, que podem ser de

natureza religiosa, política, étnica ou sociocultural. Atacantes movidos por essas convicções frequentemente buscam transcendência, visando promover uma ideologia, chamar atenção para uma causa ou demonstrar o poder e a capacidade de sua filosofia.

O ciberespaço oferece uma eficaz plataforma para esses atores amplificarem suas mensagens e causar um impacto muito além de sua presença física. Algumas ações de ciberterrorismo, por exemplo, são conduzidas em retaliação a percebidas injustiças ou ações contra um grupo ou comunidade. Nesses casos, os ataques são estruturados para infligir dano como uma forma de "equilibrar" a ofensa original, podendo ser provocados por eventos tanto digitais quanto físicos.

Em outras situações, o ciberterrorismo é uma ferramenta para ganho financeiro (WEIMANN, 2004). Grupos terroristas, reconhecendo a lucratividade potencial do ciberespaço, podem empregar táticas como *ransomware* para acumular recursos. Esses fundos não apenas sustentam as operações digitais do grupo, mas também financiam atividades terroristas no mundo físico.

Além disso, há situações em que o ciberterrorismo serve primordialmente como um meio de propaganda. Grupos, particularmente os menos conhecidos, podem empregar táticas de ciberterrorismo para ganhar reconhecimento, promovendo sua causa e atraindo potenciais recrutas e simpatizantes. O vasto alcance e a capacidade de “viralização” do ciberespaço tornam-no uma plataforma ideal para tal propagação.

Por fim, é crucial compreender que o ciberterrorismo, com suas diversas motivações, representa um desafio contínuo para governos e organizações em todo o mundo. Ao se sobrepor e entrelaçar, essas motivações tornam a tarefa de prevenir e responder a tais ameaças incrivelmente complexa.

5.2 Casos em que *ransomware* foi utilizado como tática de ciberterrorismo

O uso de *ransomware* como uma tática de ciberterrorismo amplia a ameaça desses ataques, já que a motivação por trás deles pode ir além do simples ganho financeiro. Em vez de apenas obter lucro, o ciberterrorismo visa criar medo, incerteza e interrupção em uma escala mais ampla, explorando vulnerabilidades críticas e pressionando governos ou organizações a ceder a demandas específicas (WEIMANN, 2004). Os casos citados abaixo foram retirados da pesquisa de Sullivan (2021).

Um exemplo emblemático é o ataque conhecido como NotPetya, em 2017. Embora inicialmente parecesse um ataque de *ransomware* comum, a natureza destrutiva do

NotPetya rapidamente revelou intenções mais sinistras. Em vez de simplesmente criptografar arquivos e exigir resgate, NotPetya foi projetado para causar destruição em massa nos sistemas que infectou. Especula-se que este ataque teve motivações geopolíticas e foi dirigido principalmente contra a Ucrânia, mas acabou se espalhando globalmente. A sua sofisticação e capacidade de destruição sugeriram que poderia haver um ator estatal ou um grupo com considerável apoio e recursos por trás dele.

Outro caso foi o ataque ao sistema de saúde do Reino Unido pelo *ransomware* WannaCry em 2017. Embora WannaCry tenha afetado várias entidades ao redor do mundo, o impacto no Serviço Nacional de Saúde (NHS) do Reino Unido foi particularmente severo. Hospitais foram forçados a desviar pacientes e procedimentos médicos essenciais foram adiados. Posteriormente, foi revelado que o grupo por trás do ataque, chamado Lazarus, tinha ligações com a Coreia do Norte. A magnitude e o foco deste ataque sugeriram que havia motivações que iam além do simples ganho financeiro.

O ataque Shamoon, que afetou a empresa de petróleo saudita Aramco em 2012, é outro exemplo. Neste caso, o *ransomware* não apenas exigiu resgate, mas também destruiu dados em mais de 30.000 computadores. A magnitude do ataque, associada a tensões geopolíticas na região, levantou suspeitas de motivações de ciberterrorismo.

Estes casos demonstram que o uso de *ransomware* como tática de ciberterrorismo pode ter implicações devastadoras, tanto em termos de dano direto quanto nas repercussões geopolíticas que se seguem. Embora o resgate financeiro possa ser um componente, as ramificações reais desses ataques tendem a ser muito mais amplas, afetando a estabilidade econômica, a segurança nacional e a confiança pública em instituições cruciais.

5.3 Implicações geopolíticas e respostas governamentais

A intersecção do ciberterrorismo com *ransomware* desencadeia implicações geopolíticas que transcendem as fronteiras nacionais, desafiando a ordem global estabelecida (WEIMANN, 2004). Tais ataques não apenas afetam diretamente as vítimas, mas também podem ser usados como instrumentos para avançar agendas políticas, desestabilizar governos e até mesmo criar rupturas em alianças internacionais.

Uma característica fundamental do ciberterrorismo é sua capacidade de obscurecer a atribuição de responsabilidade. Determinar com precisão quem está por trás de um ataque específico é complexo, dada a natureza difusa e interconectada do ciberespaço. Isso oferece uma camada de negação plausível para atores estatais que podem patrocinar ou

encorajar tais ataques sem parecer diretamente envolvidos. Por exemplo, as frequentes acusações e contra-acusações entre nações como Estados Unidos, Rússia, China, Irã e Coreia do Norte em relação a atividades cibernéticas maliciosas ilustram a complexidade desta questão.

Esta ambiguidade em atribuição também tem implicações para a resposta internacional. Enquanto os tratados e convenções tradicionais governam a guerra e o conflito no domínio físico, o ciberespaço permanece uma fronteira amplamente inexplorada em termos de regulamentação internacional. Sem clareza sobre as normas e sem capacidade de atribuição confiável, as nações muitas vezes hesitam em retaliar ou responder de forma assertiva.

Entretanto, à medida que os ataques de *ransomware* com motivações de ciberterrorismo se intensificam, vemos um impulso renovado para uma resposta coordenada. Governos ao redor do mundo estão investindo mais em defesa cibernética, criando agências dedicadas e formando coalizões internacionais para combater essas ameaças. Exemplos incluem a criação do *Cyber Command* nos Estados Unidos e iniciativas semelhantes na União Europeia, bem como o compartilhamento de inteligência entre aliados.

Além das medidas defensivas, há um esforço para estabelecer normas e regulamentos internacionais que definam o comportamento aceitável no ciberespaço. Enquanto as negociações continuam, há um reconhecimento crescente de que o ciberespaço, assim como os mares e o espaço aéreo, é um domínio comum que requer gestão e proteção coletiva.

À medida que o ciberespaço se tornou um elemento central da sociedade global, a necessidade de normas e regulamentos internacionais claros e coesos tornou-se cada vez mais evidente. O ciberespaço, por sua natureza intrinsecamente transfronteiriça, apresenta desafios singulares, muitas vezes tornando as abordagens jurídicas nacionais insuficientes ou inaplicáveis. Diante disso, a comunidade internacional tem se empenhado para estabelecer diretrizes que definam comportamentos aceitáveis, garantam a segurança digital e assegurem a soberania e os direitos humanos no ambiente virtual.

No entanto, esse esforço não é simples. Com diferentes nações possuindo visões distintas sobre controle da informação, privacidade, liberdade de expressão e segurança, encontrar um terreno comum é uma tarefa complexa. Organizações como as Nações Unidas têm desempenhado um papel fundamental nesse diálogo, buscando estabelecer consensos e promover cooperação entre os países. Além disso, iniciativas multilaterais, como o "Diálogo de Budapeste" e convenções como a "Convenção de Budapeste sobre o Cibercrime",

representam tentativas concretas de criar um arcabouço legal que responda aos desafios contemporâneos do ciberespaço.

Ainda estamos nos estágios iniciais de moldar o futuro do ciberespaço, e embora haja avanços, também há resistências e controvérsias. O estabelecimento de normas e regulamentos internacionais requer uma abordagem colaborativa, onde o diálogo e a compreensão mútua são essenciais. Afinal, o objetivo é garantir um ciberespaço que seja seguro, inclusivo e resiliente, preservando os valores e direitos que são caros à comunidade global.

6 ESTRATÉGIAS DE PREVENÇÃO E RESPOSTA

À medida que os ataques de *ransomware* evoluem e se tornam mais sofisticados, é essencial que organizações e indivíduos também aprimorem suas estratégias de prevenção e resposta. Isso exige uma combinação de medidas técnicas, políticas organizacionais e reconhecimento dos desafios inerentes à proteção contra ameaças cibernéticas (EGNYTE, 2021).

6.1Medidas técnicas para prevenção de ataques de *ransomware*

A natureza persistente e evolutiva dos ataques de *ransomware* exige uma abordagem igualmente dinâmica em termos de medidas técnicas de prevenção. As organizações devem adotar uma série de práticas e ferramentas para se proteger contra estas ameaças.

a) Atualizações e *Patches*: Uma das maneiras mais eficazes de proteger os sistemas contra vulnerabilidades conhecidas é garantir que todos os *softwares*, sistemas operacionais e aplicações estejam atualizados com os patches mais recentes. Os criminosos cibernéticos frequentemente exploram vulnerabilidades em softwares desatualizados, tornando essas atualizações cruciais para a segurança.
b) *Backup* de Dados: O valor do *backup* de dados não pode ser subestimado. As organizações devem realizar backups regulares de todos os dados críticos e garantir que esses *backups* sejam armazenados em locais protegidos de acesso à rede, seja *offline* ou em ambientes isolados. Isso permitiria a restauração dos dados em caso de um ataque de *ransomware*, eliminando a necessidade de pagar o resgate.
c) Ferramentas de Detecção e Resposta: Utilizar soluções avançadas de *Endpoint Detection and Response* (EDR) e *Security Information and Event Management* (SIEM) pode

fornecer uma camada adicional de proteção, identificando comportamentos anômalos e atividades suspeitas em tempo real, permitindo uma resposta rápida para isolar e mitigar o ataque.

d) Filtragem de *E-mails*: *E-mails* continuam sendo um dos principais vetores de infecção por *ransomware*. Uma solução de filtragem robusta pode detectar e bloquear *e-mails* de *phishing* ou aqueles que carregam *payloads* maliciosos, prevenindo que cheguem à caixa de entrada dos usuários.
e) Restrição de Acessos: Implementar o princípio do menor privilégio é fundamental. Isso significa que usuários e aplicações devem ter apenas as permissões estritamente necessárias para suas funções, reduzindo a superfície de ataque em caso de comprometimento.
f) Segregação de Redes: Isolar redes críticas e sistemas sensíveis de outras partes da infraestrutura pode impedir que o *ransomware* se propague por toda a organização.
g) Ferramentas *Anti-ransomware*: Além das soluções antivírus convencionais, existem ferramentas especializadas projetadas especificamente para detectar, bloquear e remover *ransomware*.
h) Autenticação multifator: Implementar em todos os pontos de acesso críticos garante que, mesmo que as credenciais sejam comprometidas, um atacante teria dificuldade em ganhar acesso.

Em essência, a proteção contra *ransomware* requer uma combinação holística de várias medidas técnicas que trabalham em conjunto para formar um escudo robusto contra ameaças, garantindo que, mesmo se uma linha de defesa falhar, outras estarão prontas para impedir a infiltração.

6.2Políticas e procedimentos recomendados

A integridade e segurança dos sistemas informáticos de uma organização frequentemente vão além das soluções técnicas, encontrando sua fundação nas políticas e procedimentos bem estabelecidos. A maneira como os funcionários interagem com os recursos digitais, especialmente em um ambiente em que as ameaças cibernéticas estão em constante evolução, desempenha um papel crucial na determinação do nível de vulnerabilidade de uma organização.

Investir em treinamento regular dos funcionários, por exemplo, prepara-os para reconhecer e lidar com tentativas de *phishing* e outros comportamentos suspeitos, tornando-os

a primeira linha de defesa. Uma abordagem proativa envolve não apenas reagir aos incidentes, mas também ter um plano concreto de gestão de incidentes. A rapidez com que uma organização pode identificar, isolar e recuperar-se de uma ameaça de *ransomware* pode ser a diferença entre uma interrupção menor e uma paralisação total.

Um aspecto crucial para a segurança é a regularidade com que os direitos de acesso são revisados. Assegurando que apenas as partes relevantes tenham acesso aos sistemas e dados adequados, e que esses direitos sejam revogados quando não forem mais necessários, minimiza-se a exposição a riscos. Associado a isso, uma política robusta de backup não apenas dita a frequência e os métodos de *backup*, mas também garante que os dados possam ser efetivamente restaurados. Entretanto, não são apenas os funcionários internos que representam um risco. Fornecedores e outros terceiros que têm acesso à rede de uma organização podem ser pontos vulneráveis, o que torna essencial uma política rigorosa de gestão de fornecedores.

Limitar a instalação e execução de *software* e garantir que apenas os administradores tenham o poder de alterar os sistemas fundamentais pode reduzir significativamente o risco de infecções maliciosas. E, dada a natureza dinâmica das ameaças cibernéticas, é imprescindível que as políticas sejam revisadas e atualizadas regularmente, garantindo assim que continuem a ser relevantes e adaptadas ao cenário atual de ameaças.

Por fim, além de todas as precauções e planos de resposta, é fundamental ter em mente a continuidade dos negócios. Independentemente da natureza ou escala do ataque, a capacidade de uma organização de continuar operando é essencial. Um plano robusto de continuidade do negócio garante que, mesmo na pior das hipóteses, a organização possa manter-se resiliente e operacional.

6.3Desafios na implementação de medidas de prevenção e resposta

Os avanços na tecnologia da informação têm permitido às empresas se tornarem mais eficientes, conectadas e ágeis. Contudo, paralelamente a esses benefícios, surgem desafios significativos em termos de segurança cibernética. A implementação de medidas eficazes de prevenção e resposta a ataques cibernéticos, especialmente *ransomware*, é complexa e enfrenta diversos obstáculos.

6.3.1 Cenário em constante mutação

O universo digital, por sua natureza intrínseca, está em constante evolução. Paralelamente a essa evolução, o cenário de ameaças cibernéticas, particularmente relacionado ao *ransomware*, transforma-se de maneira rápida e ininterrupta. Esta natureza mutável do panorama de ameaças tornou-se um dos principais desafios para as organizações e profissionais de segurança cibernética ao tentarem combater esses ataques maliciosos.

A cada dia, novas variantes de *ransomware* são desenvolvidas. Muitas delas são equipadas com técnicas avançadas de evasão, capacidade de propagação autônoma e até mesmo contramedidas para ferramentas de segurança conhecidas. Esse ritmo acelerado de inovação no lado adversário exige uma resposta igualmente ágil por parte das defesas. No entanto, adaptar-se e responder a essas novas variantes em tempo hábil é complexo e, muitas vezes, as organizações encontram-se sempre um passo atrás.

Além disso, o modus operandi dos atacantes também se diversifica. Enquanto inicialmente os ataques de *ransomware* eram em grande parte oportunistas, visando qualquer organização ou indivíduo desprotegido, agora observamos uma tendência crescente de ataques direcionados. Estes são meticulosamente planejados e frequentemente buscam alvos de alto valor, como infraestruturas críticas ou organizações com recursos significativos, aumentando a pressão sobre as vítimas para pagar resgates vultosos.

A combinação desses fatores - a rápida evolução das variantes de *ransomware*, a sofisticação crescente dos ataques e a mudança nas táticas dos atacantes - torna o combate ao *ransomware* um desafio em constante mutação. As soluções de segurança que eram eficazes ontem podem não ser suficientes amanhã.

6.3.2 Complexidade das infraestruturas tecnológicas modernas

A revolução digital transformou a maneira como as organizações operam, tornando-as cada vez mais dependentes de infraestruturas tecnológicas para suas operações cotidianas. No entanto, com os inúmeros benefícios que a tecnologia moderna trouxe, vieram também novos desafios, principalmente no que diz respeito à segurança cibernética e à prevenção de ataques por ransomware.

Uma das principais características das infraestruturas tecnológicas atuais é sua diversidade. As organizações de hoje utilizam uma ampla variedade de dispositivos, sistemas operacionais, aplicativos e soluções de nuvem. Desde servidores tradicionais e *desktops* até dispositivos IoT, *mobile* e infraestruturas de nuvem híbrida, a paisagem tecnológica nunca foi tão vasta.

No entanto, essa diversidade traz consigo um nível significativo de complexidade. Cada componente e sistema tem suas próprias vulnerabilidades, requisitos de configuração e protocolos de segurança. A gestão e a manutenção de todas essas plataformas diferentes, garantindo que estejam sempre atualizadas e configuradas corretamente, tornam-se uma tarefa monumental.

O *ransomware*, por sua natureza, explora pontos fracos e vulnerabilidades. A complexidade e diversidade das infraestruturas modernas proporcionam um terreno fértil para os atacantes encontrarem brechas. Um único dispositivo não atualizado ou uma única configuração malfeita podem servir como porta de entrada para um ataque devastador.

Além disso, a integração de novas tecnologias, como IoT e dispositivos *edge*, amplia ainda mais a superfície de ataque. Muitos desses dispositivos foram projetados com ênfase na funcionalidade, e não na segurança, tornando-os alvos atraentes para os cibercriminosos.

Portanto, enquanto a diversidade e a complexidade das infraestruturas tecnológicas modernas oferecem flexibilidade e eficiência operacional, elas também representam desafios significativos para a prevenção de ataques de *ransomware*. As organizações devem adotar uma abordagem multifacetada e holística, combinando tecnologia, processos e treinamento para garantir que sua infraestrutura esteja protegida contra as ameaças em constante evolução que o *ransomware* representa.

6.3.3 Mentalidade de segurança cibernética

A prevenção de ataques por *ransomware* não se limita apenas à implementação de tecnologias de ponta; a cultura e mentalidade organizacional em relação à segurança cibernética desempenham um papel crucial. Infelizmente, a resistência organizacional e a falta de uma mentalidade adequada muitas vezes se tornam obstáculos significativos para o fortalecimento das defesas contra esses ataques.

A resistência organizacional geralmente se manifesta de diversas maneiras. Pode vir na forma de relutância em investir recursos adequados em segurança, especialmente em organizações que ainda não sofreram ataques significativos e, portanto, não veem a segurança cibernética como uma prioridade. Em outras situações, pode surgir como uma resistência à mudança, onde práticas e sistemas obsoletos são mantidos por conveniência ou familiaridade, apesar de apresentarem vulnerabilidades claras.

Por outro lado, a falta de mentalidade de segurança cibernética refere-se à ausência de consciência e compreensão, por parte dos indivíduos na organização, sobre as ameaças cibernéticas e a importância da segurança. Essa mentalidade limitada pode resultar em comportamentos de risco, como clicar em links suspeitos, compartilhar senhas ou não adotar atualizações de segurança recomendadas.

Ambos os desafios se interconectam e amplificam mutuamente. Por exemplo, sem um comprometimento claro da liderança, os esforços para educar e treinar os funcionários sobre práticas seguras podem ser infrutíferos. Da mesma forma, se os funcionários não reconhecem a importância da segurança, podem resistir às políticas e procedimentos que buscam proteger a organização, vendo-os como inconvenientes.

O resultado desses obstáculos é um ambiente mais vulnerável a ataques de *ransomware*. Em um mundo onde os cibercriminosos estão constantemente aprimorando suas táticas e ferramentas, organizações que não priorizam a segurança cibernética e não cultivam uma mentalidade de segurança entre seus membros correm um risco significativamente maior de serem vítimas de ataques devastadores.

Para superar esses desafios, é essencial que as organizações reconheçam a segurança cibernética como uma responsabilidade coletiva. Isso envolve investir em treinamento, tecnologia e, acima de tudo, promover uma cultura em que a segurança seja valorizada e integrada em todas as operações e decisões.

6.3.4 Desafios legais

O combate ao cibercrime, especialmente em relação aos ataques *ransomware*, apresenta uma gama de desafios legais complexos que transcendem as fronteiras nacionais. O primeiro obstáculo reside na natureza intrinsecamente internacional dos cibercrimes. Muitas vezes, os autores dos ataques estão situados em jurisdições diferentes das suas vítimas, tornando a persecução penal um exercício transnacional. Isso demanda uma cooperação internacional robusta, porém, nem todos os países possuem tratados ou acordos bilaterais para o combate ao cibercrime.

Além disso, a velocidade com que os ataques ocorrem contrasta com o ritmo muitas vezes lento das ações judiciais e investigações. Os criminosos podem rapidamente alterar sua localização digital, utilizar técnicas de ofuscação ou operar através de redes privadas virtuais (VPNs) e outras ferramentas que dificultam o rastreio. A definição legal do que constitui um cibercrime, e mais especificamente um ataque *ransomware*, também pode

variar de um país para outro. Isso pode levar a lacunas legais onde certas atividades podem ser consideradas ilícitas em um país, mas não em outro.

Outro desafio reside na natureza evolutiva do *ransomware*. À medida que a tecnologia avança, os cibercriminosos adaptam-se, desenvolvendo novas formas de malware e táticas de ataque. A legislação precisa ser adaptativa para acompanhar essas mudanças, o que nem sempre acontece de forma ágil.

Por fim, mesmo quando os perpetradores são identificados e processados, a execução de sentenças e a recuperação de ativos pode ser um processo complicado, principalmente se os ativos estiverem em criptomoedas ou em jurisdições com leis de sigilo bancário. Por último, mas certamente não menos importante, o gerenciamento de custos é sempre um desafio. Soluções de segurança de ponta, juntamente com os recursos necessários para implementar e gerenciá-las, podem ser caros. Equilibrar o orçamento com a necessidade de segurança robusta é uma tarefa que muitas organizações encontram difícil.

O ransomware, como muitas outras formas de malware, caracteriza-se por sua capacidade de evoluir rapidamente, adaptando-se às defesas existentes e explorando novas vulnerabilidades. Esta natureza mutável apresenta desafios significativos para a prevenção e combate eficaz desses ataques.

Primeiramente, a evolução constante do ransomware torna difícil para os sistemas de defesa, como antivírus e firewalls, manterem-se atualizados. À medida que novas variantes de ransomware são desenvolvidas, muitas vezes elas são projetadas para evitar detecções comuns, utilizando técnicas de ofuscação, polimorfismo e até mesmo aprendizado de máquina para contornar as soluções de segurança tradicionais.

Além disso, os cibercriminosos estão constantemente aprimorando suas táticas de infiltração. Se antes era comum a dependência de campanhas de phishing para disseminar ransomware, agora vemos uma tendência crescente de ataques direcionados, onde os criminosos identificam e exploram vulnerabilidades específicas em sistemas e redes de uma organização.

A natureza evolutiva do ransomware também dificulta a recuperação pós-ataque. Enquanto versões anteriores de ransomware poderiam ser decifradas com ferramentas de descriptografia disponíveis publicamente, variantes mais recentes muitas vezes utilizam algoritmos de criptografia mais robustos e métodos de entrega que complicam ou impossibilitam a recuperação de dados sem o pagamento do resgate.

Também é preocupante o modo como o modelo de negócio do ransomware tem se adaptado. O surgimento do *Ransomware-as-a-Service* (RaaS) permite que mesmo indivíduos

com habilidades técnicas limitadas lancem ataques sofisticados, alugando infraestruturas de ataque e compartilhando os lucros com os desenvolvedores do *ransomware*.

Para enfrentar a natureza evolutiva do *ransomware*, é crucial que organizações e indivíduos adotem uma abordagem proativa e adaptativa à segurança cibernética. Isso inclui a manutenção regular de sistemas, educação contínua de usuários, monitoramento constante de redes e a implementação de soluções de segurança avançadas capazes de responder dinamicamente às ameaças emergentes.

7 CONCLUSÃO

A crescente digitalização da sociedade tem revolucionado a forma como vivemos, trabalhamos e interagimos. No entanto, essa mesma digitalização tornou-se um campo fértil para ameaças cibernéticas, particularmente ataques de *ransomware* e ciberterrorismo. A presente pesquisa dedicou-se a investigar a evolução dessas ameaças, os prejuízos associados e as estratégias adotadas para enfrentá-las.

7.1 Considerações Finais

O mundo digital em que vivemos oferece inúmeras oportunidades, mas também apresenta desafios significativos em termos de segurança. Esta pesquisa serve como um lembrete de que, para colher os benefícios da digitalização, é imperativo estar ciente das ameaças e equipar-se adequadamente para enfrentá-las. As estratégias de defesa devem ser multifacetadas, combinando tecnologia, políticas, treinamento e cooperação interagências.

7.2 Principais resultados obtidos na pesquisa

Através desta pesquisa, foi possível identificar uma progressão alarmante na sofisticação e escala dos ataques de *ransomware* ao longo dos anos. Não são apenas indivíduos e empresas pequenas que estão em risco, mas também infraestruturas críticas e setores estratégicos da economia global. Os prejuízos econômicos diretos, como pagamentos de resgate, são agravados por perdas indiretas significativas, como interrupções operacionais, danos à reputação e despesas de recuperação.

A linha entre cibercrime e ciberterrorismo tornou-se cada vez mais tênue, com vários atores maliciosos utilizando táticas de *ransomware* para avançar agendas políticas e ideológicas. Esta pesquisa também destacou o papel vital das estratégias de prevenção e

resposta, demonstrando que, enquanto a tecnologia desempenha um papel crucial na defesa contra ameaças, a conscientização e educação dos usuários são igualmente críticas.

7.3 Sugestões para Futuros Trabalhos

Dada a natureza dinâmica dos ciberataques e a rápida evolução do cenário de ameaças, é fundamental que a pesquisa nesse campo continue. Seria valioso investigar mais profundamente os motivos psicológicos por trás dos cibercriminosos e terroristas. Além disso, um foco em tecnologias emergentes, como Inteligência Artificial e Internet das Coisas, e sua intersecção com *ransomware* e ciberterrorismo, poderia oferecer *insights* valiosos. Por fim, estudos de caso detalhados sobre organizações que lidaram com sucesso com essas ameaças poderiam servir como modelos para outras instituições.

REFERÊNCIAS BIBLIOGRÁFICAS

ABLON, L. **Data Thieves: the motivations of cyber threat actors and their use and monetization of stolen data**. Disponível em: <https://www.rand.org/content/dam/rand/pubs/testimonies/CT400/CT490/RAND_CT490.pdf>. Acesso em: 01 set. 2023.

BEAMAN, C. et al. **Ransomware: recent advances analysis, challenges and future research directions.** Disponível em: <https://www.sciencedirect.com/science/article/pii/S016740482100314X>. Acesso em: 03 ago. 2023.

EGNYTE. **The Ultimate Guide to Ransomware**. Disponível em: <https://www.egnyte.com/sites/default/files/2021-01/Egnyte_Ransomeware_White%20Paper_Ultimate_Guide_1.pdf>. Acesso em: 15 ago. 2023

IST, Institute for Security and Technology. **Combating Ransomware.** Disponível em: <https://securityandtechnology.org/wp-content/uploads/2021/09/IST-Ransomware-Task-Force-Report.pdf>. Acesso em: 09 ago. 2023.

LI, Y., LIU, Q. **A comprehensive review study of cyber-attacks and cyber security; Emerging trends and recent developments**. Disponível em: <https://www.sciencedirect.com/science/article/pii/S2352484721007289>. Acesso em: 01 ago. 2023.

O'KANE, P. et al. **Evolution of Ransomware.** Disponível em: <https://ietresearch.onlinelibrary.wiley.com/doi/full/10.1049/iet-net.2017.0207>. Acesso em: 01 set. 2023.

REINO UNIDO, National Cyber Security Centre. **Ransomware, extortion and the cyber crime ecosystem.** Disponível em: <https://www.ncsc.gov.uk/files/White-paper-Ransomware-extortion-and-the-cyber-crime-ecosystem.pdf>. Acesso em: 22 ago. 2023.

SAVAGE, K. et al. **The Evolution of Ransomware.** Symantec, 2015. Disponível em: <https://its.fsu.edu/sites/g/files/imported/storage/images/information-security-and-privacy-office/the-evolution-of-ransomware.pdf>. Acesso em: 02 set. 2023.

SULLIVAN, J., MUIR, J. **Ransomware: a perfect storm.** Disponível em: <https://static.rusi.org/263_ei_ransomware_final_0_0.pdf>. Acesso em: 17 ago. 2023.

TRENDMICRO. **Ransomware: past, present and future.** Disponível em: <https://documents.trendmicro.com/assets/wp/wp-ransomware-past-present-and-future.pdf>. Acesso em: 07 ago. 2023

WEIMANN, G**. Cyberterrorism: how real is the threat?** Disponível em: <https://www.usip.org/sites/default/files/sr119.pdf>. Acesso em: 25 ago. 2023.