INSTITUTO FEDERAL
São Paulo
Câmpus Birigui

Ransomware: Um Estudo Abrangente sobre Ameaças, Estratégias de Defesa e Processos de Recuperação

José Augusto Cenci Castilho
Graduando em Engenharia de Computação, IFSP, Câmpus Birigui, j.cenci@aluno.ifsp.edu.br.

Área de conhecimento (Tabela CNPq): 1.03.03.04-9 Sistemas de Informação.

RESUMO: O ransomware consolidou-se como uma ameaça cibernética proeminente, impactando severamente organizações e indivíduos ao negar acesso a dados críticos mediante exigência de resgate. Este artigo apresenta uma análise abrangente do ransomware, englobando sua definição, evolução histórica desde os precursores até as táticas de extorsão múltipla e modelos como Ransomware-as-a-Service (RaaS). São detalhadas as técnicas de ataque, vetores de infecção comuns, e as fases subsequentes de um ataque. Adicionalmente, explora as principais famílias de ransomware, as estratégias de proteção multicamadas – incluindo conscientização, higiene cibernética e backups robustos – e as complexas metodologias de recuperação de dados, incluindo o dilema do pagamento de resgate. O estudo é complementado por dados e tendências recentes (2024-2025) que ilustram a persistência e adaptação contínua desta ameaça.

PALAVRAS-CHAVE: ciberataque; extorsão digital; proteção de dados; resposta a incidentes; malware evolutivo

Ransomware: A Comprehensive Study of Threats, Defense Strategies, and Recovery Processes

ABSTRACT: Ransomware has established itself as a prominent cyber threat, severely impacting organizations and individuals by denying access to critical data through ransom demands. This article presents a comprehensive analysis of ransomware, encompassing its definition, historical evolution from early precursors to multiple extortion tactics and models like Ransomware-as-a-Service (RaaS). Attack techniques, common infection vectors, and subsequent attack phases are detailed. Additionally, it explores major ransomware families, multi-layered protection strategies – including awareness, cyber hygiene, and robust backups – and complex data recovery methodologies, including the ransom payment dilemma. The study is complemented by

recent data and trends (2024-2025) illustrating the persistence and continuous adaptation of this threat.

KEYWORDS: cyberattack; digital extortion; data protection; incident response; evolving malware

1 INTRODUÇÃO

O ransomware emergiu como uma das ameaças cibernéticas mais proeminentes e disruptivas da atualidade, afetando organizações de todos os tamanhos e setores, bem como usuários individuais. Caracterizado pela sua capacidade de negar acesso a sistemas ou dados críticos, exigindo um resgate para a sua restauração, o ransomware não só causa perdas financeiras diretas, mas também interrupções operacionais significativas, danos à reputação e potenciais violações de dados sensíveis. A sua evolução constante, desde os primeiros exemplares rudimentares até às sofisticadas variantes atuais que empregam táticas de extorsão múltipla e modelos de negócio como Ransomware-as-a-Service (RaaS), sublinha a necessidade de uma compreensão aprofundada desta ameaça. Este artigo tem como objetivo fornecer uma análise abrangente do ransomware, abordando a sua definição, histórico evolutivo, as técnicas de ataque empregadas, as famílias mais notórias, as estratégias de proteção e as metodologias de recuperação, complementada por dados e tendências recentes.

2 O QUE É RANSOMWARE?

Ransomware é uma categoria de software malicioso (malware) que impede ou limita o acesso dos usuários aos seus próprios sistemas ou arquivos pessoais. Para que o acesso seja restabelecido, os perpetradores exigem o pagamento de um resgate. De forma mais técnica, o ransomware é projetado para criptografar arquivos em um dispositivo, tornando quaisquer arquivos e os sistemas que dependem deles inutilizáveis. Os atores maliciosos então exigem um resgate em troca da chave de decriptografia. Frequentemente, esses atores também ameaçam vender ou vazar dados exfiltrados ou informações de autenticação caso o resgate não seja pago, uma tática conhecida como dupla extorsão.

Existem duas categorias principais de ransomware:

- **Locker ransomware:** Este tipo bloqueia as funções básicas do computador, como o acesso ao desktop, e pode desabilitar parcialmente o mouse e o teclado, permitindo interação apenas com a janela de exigência de resgate. Geralmente, não visa arquivos críticos, mas sim bloquear o acesso.

- **Crypto ransomware:** Este tipo criptografa dados importantes como documentos, imagens e vídeos, mas não interfere nas funções básicas do computador. Isso causa pânico, pois os usuários podem ver seus arquivos, mas não acessá-los. Os desenvolvedores frequentemente incluem uma contagem regressiva, ameaçando deletar todos os arquivos se o resgate não for pago dentro do prazo.

A Agência da União Europeia para a Cibersegurança (ENISA) define ransomware como um tipo de ataque onde os atores da ameaça tomam o controle dos ativos de um alvo e exigem um resgate em troca da devolução da disponibilidade do ativo ou em troca de não expor publicamente os dados do alvo. Esta definição abrange o cenário em evolução da ameaça, a prevalência de múltiplas técnicas de extorsão e os vários objetivos dos perpetradores, para além dos ganhos meramente financeiros. Desde o início de 2016, ocorreram, em média, mais de 4.000 ataques de ransomware diariamente.

3 HISTÓRICO DO RANSOMWARE

A história do ransomware, embora relativamente curta, demonstra uma evolução significativa em termos de sofisticação e impacto.

3.1 O Pioneiro: AIDS Trojan (PC Cyborg)

O primeiro caso documentado de ransomware remonta a dezembro de 1989, com o surgimento do AIDS Trojan, também conhecido como PC Cyborg. Criado pelo Dr. Joseph Popp, um biólogo educado em Harvard, este malware foi distribuído através de aproximadamente 20.000 disquetes enviados pelo correio para pesquisadores da AIDS e assinantes de revistas científicas em cerca de 90 países. O malware não criptografava o conteúdo dos arquivos, mas sim os nomes dos arquivos e ocultava diretórios no disco C: após o sistema ser reiniciado 90 vezes. Uma nota de resgate exigia o pagamento de $189 ou $378 para uma caixa postal no Panamá para "renovar a licença"do software.

Embora rudimentar pelos padrões atuais – escrito em QUICKBASIC 3.0 e utilizando uma cifra de substituição simétrica simples nos nomes dos arquivos – o AIDS Trojan estabeleceu o precedente para a extorsão digital. Ferramentas de remoção e decriptografia (AIDSOUT, AIDSCLEAR e CLEARAID) foram rapidamente desenvolvidas por Jim Bates e John Sutcliffe. O Dr. Popp foi preso, mas nunca cumpriu pena, e acredita-se que suas ações foram um catalisador para a criação do Computer Misuse Act de 1990 no Reino Unido, país escolhido para a distribuição dos disquetes devido à ausência de leis específicas contra o uso indevido de computadores na época. Este primeiro ransomware, apesar de sua simplicidade e do alto custo de distribuição, demonstrou o potencial de dano e lançou as bases conceituais para futuras táticas de extorsão cibernética, mesmo que sua execução técnica fosse primitiva e o impacto financeiro para o perpetrador, insignificante. A tentativa de extorsão foi dificultada pelo uso limitado de computadores na época.

3.2 Evolução e Sofisticação

Após o AIDS Trojan, o cenário de ransomware permaneceu relativamente quiescente até meados dos anos 2000, quando os criminosos cibernéticos começaram a experimentar métodos de criptografia mais robustos e mecanismos de pagamento anônimos.

Primeiros Lockers e Scareware (Meados dos anos 2000 - Início dos anos 2010): Surgiram os ransomware lockers, que bloqueavam o acesso ao sistema operacional ou a arquivos essenciais, e o scareware, que exibia falsos alertas de infecção por vírus, exigindo pagamento para "limpeza". Em 2006-2007, variantes como o GPCode utilizavam criptografia simétrica falha, mas versões posteriores empregaram métodos mais fortes e chaves mais longas (1024 ou 2048 bits), dificultando a recuperação.

A Era da Criptografia Forte e Criptomoedas (A partir de 2013): O ano de 2013 marcou um ponto de inflexão com o surgimento do CryptoLocker. Este foi um dos primeiros a utilizar criptografia assimétrica forte (RSA-2048) para tornar os arquivos inacessíveis e exigia pagamento em Bitcoin, garantindo maior anonimato aos criminosos. O CryptoLocker se disseminava principalmente por meio de e-mails de phishing com anexos maliciosos e, até o final de 2015, teria rendido aos seus operadores cerca de $27 milhões. Este sucesso financeiro demonstrou a lucratividade do modelo e impulsionou o desenvolvimento de novas famílias de ransomware.

Ransomware-as-a-Service (RaaS) e Dupla Extorsão (Final dos anos 2010 - Presente): O modelo de Ransomware-as-a-Service (RaaS) democratizou o acesso a ferramentas de ransomware, permitindo que indivíduos com menos conhecimento técnico lançassem ataques em troca de uma porcentagem do resgate pago pelas vítimas. Isso levou a um aumento exponencial no volume de ataques. Em 2020, o custo global do ransomware atingiu $20 bilhões. A tática de dupla extorsão, popularizada pelo grupo Maze em 2020, adicionou uma nova camada de pressão: além de criptografar os dados, os atacantes os exfiltram e ameaçam publicá-los caso o resgate não seja pago. Esta abordagem torna os backups, por si só, insuficientes para mitigar completamente o risco, pois não impedem a exposição de dados sensíveis. Dados da BlackFog para 2024 indicam que mais de 93% dos ataques de ransomware incluem um elemento de exfiltração de dados.

A sofisticação crescente dos ataques e a profissionalização dos grupos de ransomware, evidenciada por vazamentos como os do grupo Conti em 2022, que revelaram suas ferramentas internas, guias de ataque e estruturas operacionais, demonstram a natureza empresarial dessas operações criminosas. A adaptação contínua dos criminosos, como o desenvolvimento de variantes para sistemas Linux e ESXi, visa ampliar a superfície de ataque e maximizar o impacto e as demandas de resgate.

4 TÉCNICAS DE ATAQUE

Os ataques de ransomware envolvem um ciclo de vida com múltiplas fases, desde a penetração inicial até a extorsão. Compreender as técnicas empregadas em cada fase é crucial para desenvolver defesas eficazes.

4.1 Vetores de Infecção Comuns

Os atores de ransomware utilizam diversos vetores para obter acesso inicial aos sistemas das vítimas:

Tabela 1: Evolução Histórica do Ransomware

Período	**Marco Principal**	**Características Notáveis**	**Impacto Significativo**
1989	AIDS Trojan (PC Cyborg)	Distribuição via disquetes, ocultação de diretórios, nomes de arquivos criptografados (simples), resgate por correio postal.	Primeiro ransomware documentado; catalisador para leis de crimes cibernéticos. (JACKSON, 2024; MUNIANDY et al., 2024; WatchGuard Technologies, 2024)
Meados dos anos 2000	Surgimento de *Lockers* e *Scareware*	Bloqueio de tela/sistema; falsos alertas de vírus; criptografia simétrica fraca (e.g., GPCode).	Aumento gradual da atividade; experimentação com modelos de extorsão. (TANNI; HEIKES; HADI, 2022; MasterDC, 2024; ROBB, 2024)
2013	CryptoLocker	Criptografia assimétrica forte (RSA); uso de Bitcoin para pagamento; disseminação via *phishing*.	Revolucionou o ransomware, tornando a recuperação quase impossível sem a chave; alta lucratividade. (JACKSON, 2024; MUNIANDY et al., 2024; ROBB, 2024)
Fim de 2010	Ascensão do *Ransomware-as-a-Service* (RaaS)	Plataformas oferecem ransomware a afiliados; divisão de lucros; proliferação de ataques.	Redução da barreira de entrada para cibercriminosos; aumento massivo no volume de ataques. (JACKSON, 2024; ROBB, 2024)
2017	WannaCry	Exploração da vulnerabilidade EternalBlue (SMB); propagação tipo *worm*; impacto global em larga escala.	Demonstrou a capacidade de interrupção massiva e a vulnerabilidade de sistemas não corrigidos. (JACKSON, 2024; Wikipedia contributors, 2025b)
2020	Predominância da Dupla e Tripla Extorsão	Exfiltração de dados antes da criptografia; ameaça de vazamento público; ataques DDoS adicionais.	Aumenta a pressão sobre as vítimas; *backups* sozinhos não são suficientes. (JACKSON, 2024; ROBB, 2024; ThreatDown by Malwarebytes, 2025; Akamai Technologies, 2024)
2021	Foco em Alvos de Alto Valor e Infraestruturas Críticas	Ataques direcionados a grandes corporações, hospitais, governos; demandas de resgate milionárias.	Interrupções severas em serviços essenciais; aumento do impacto econômico e social. (JACKSON, 2024; ROBB, 2024)
2023	Uso Crescente de IA e Exploração de Novas Vulnerabilidades	Desenvolvimento de ransomware assistido por IA; exploração de vulnerabilidades em dispositivos IoT e *firmware*.	Potencial para ataques mais sofisticados, evasivos e automatizados. (European Union Agency for Cybersecurity (ENISA), 2023; Kaspersky Lab, 2025)

- **E-mails de Phishing e Spear-Phishing:** Continuam sendo os vetores mais comuns. E-mails fraudulentos, muitas vezes com um senso de urgência ou disfarçados de comunicações legítimas, contêm links maliciosos ou anexos infectados (e.g., documentos PDF, ZIP, Microsoft Office com macros). Ao clicar no link ou abrir o anexo, o usuário pode ser redirecionado para sites falsos que baixam o ransomware ou exploit kits. A ENISA aponta que o phishing permanece como o principal vetor de infecção inicial, especialmente na região EMEA (40% das violações).

- **Exploração de Vulnerabilidades em Software:** Sistemas e softwares desatualizados ou não corrigidos são alvos frequentes. Os atacantes exploram vulnerabilidades conhecidas (CVEs) em aplicações voltadas para a internet, como servidores web, VPNs e protocolos de desktop remoto. O relatório da Unit 42 de 2022 indicou que 48% dos casos de ransomware começaram com vulnerabilidades de software. A exploração da vulnerabilidade CVE-2023-0669 no software GoAnywhere MFT pela Cl0p resultou em um aumento nos ataques em março de 2023.

- **Protocolo de Desktop Remoto (RDP) e Outros Serviços Remotos Mal Configurados:** Credenciais RDP fracas ou expostas são um alvo comum para ataques de força bruta ou compra em mercados clandestinos. Uma vez obtido o acesso RDP, os atacantes podem implantar o ransomware diretamente.

- **Malvertising e Drive-by Downloads:** Anúncios maliciosos em sites legítimos ou comprometidos podem redirecionar usuários para sites que hospedam exploit kits ou iniciam o download automático de ransomware sem a interação do usuário.

- **Credenciais Comprometidas:** O uso de credenciais roubadas (obtidas através de violações de dados anteriores, infostealers ou phishing) permite que os atacantes acessem sistemas como usuários legítimos, contornando algumas defesas. O relatório DBIR 2025 da Verizon destaca que o abuso de credenciais (22%) é um dos principais vetores de ataque inicial.

- **Ataques à Cadeia de Suprimentos:** Comprometimento de fornecedores de software ou provedores de serviços gerenciados (MSPs) para distribuir ransomware aos seus clientes, como no ataque à Kaseya pelo REvil.

- **Dispositivos USB Infectados:** Embora menos comum para ataques em larga escala, o uso de dispositivos USB infectados ainda pode ser um vetor, especialmente em ambientes com controles de segurança física deficientes.

Relatórios recentes da ENISA (2023) indicam uma mudança, com links URL e navegação na web emergindo como métodos dominantes para entrega de ransomware, respondendo por mais de 77% dos casos, superando os anexos de e-mail.

4.2 Fases do Ataque Após a Infecção Inicial

Uma vez que o acesso inicial é obtido, o ataque de ransomware normalmente progride através das seguintes fases (MasterDC, 2024; ResearchGate (various authors, specific paper not fully identified in snippet), 2024; CASINO et al., 2025):

1. **Reconhecimento e Movimentação Lateral**: O atacante explora a rede para identificar ativos críticos, dados valiosos e sistemas adicionais para comprometer (MasterDC, 2024; ThreatDown by Malwarebytes, 2025; ResearchGate (various authors, specific paper not fully identified in snippet), 2024; CASINO et al., 2025). Ferramentas como `Mimikatz` podem ser usadas para extrair credenciais e escalar privilégios (Wikipedia contributors, 2025a). A movimentação lateral visa expandir o controle sobre a rede da vítima.

2. **Exfiltração de Dados (Dupla Extorsão)**: Antes da criptografia, os atacantes frequentemente exfiltram grandes volumes de dados sensíveis para servidores sob seu controle (JACKSON, 2024; ROBB, 2024; ThreatDown by Malwarebytes, 2025; SADAYAPPAN et al., 2024). Ferramentas comuns de exfiltração incluem `Rclone`, `MEGASync`, `FileZilla` e `WinSCP`, além de ferramentas personalizadas como `EXMATTER` e `EXBYTE` (SADAYAPPAN et al., 2024). Esta etapa é fundamental para a tática de dupla extorsão.

3. **Criptografia de Dados**: Esta é a fase central do ataque de *crypto ransomware*. O *malware* procura e criptografa arquivos com extensões específicas (e.g., `.doc`, `.jpg`, `.pdf`, bancos de dados) (TANNI; HEIKES; HADI, 2022). Algoritmos de criptografia fortes são empregados:

    - **Criptografia Simétrica**: Utiliza uma única chave tanto para criptografar quanto para decriptografar os dados. É rápida, mas a chave precisa ser distribuída ou armazenada no *malware*, tornando-a vulnerável à engenharia reversa se não for protegida adequadamente (TANNI; HEIKES; HADI, 2022).
    - **Criptografia Assimétrica (Chave Pública)**: Utiliza um par de chaves: uma pública para criptografar e uma privada para decriptografar. A chave pública pode ser distribuída abertamente, enquanto a chave privada é mantida em segredo pelo atacante. É mais lenta que a simétrica para grandes volumes de dados (TANNI; HEIKES; HADI, 2022).
    - **Criptografia Híbrida**: Combina a eficiência da criptografia simétrica com a segurança da assimétrica. Tipicamente, o ransomware gera uma chave simétrica aleatória para cada arquivo (ou um conjunto de arquivos), criptografa os dados com essa chave simétrica, e então criptografa a chave simétrica com a chave pública do atacante. A chave privada do atacante, necessária para decriptografar a chave simétrica (e, por conseguinte, os arquivos), é mantida no servidor de Comando e Controle (C2) (TANNI; HEIKES; HADI, 2022). Este é o método mais comum e robusto.

O ransomware pode chamar APIs criptográficas do sistema operacional da vítima para gerar chaves (TANNI; HEIKES; HADI, 2022). Algumas variantes, como o Ryuk, incorporam chaves públicas RSA (e.g., RSA-2048) e usam AES-256 para a criptografia de arquivos (CrowdStrike, 2019). O objetivo é tornar a recuperação sem a chave privada do atacante computacionalmente inviável.

4. **Comunicação com Servidor de Comando e Controle (C2)**: Muitos ransomwares se comunicam com servidores C2 para enviar informações da vítima, baixar módulos adicionais, e, crucialmente, obter ou enviar chaves de criptografia (TANNI; HEIKES; HADI, 2022). A chave simétrica usada para criptografar os arquivos da vítima é frequentemente criptografada com a chave pública do C2, e a chave privada correspondente permanece com os atacantes (TANNI; HEIKES; HADI, 2022).

5. **Exibição da Nota de Resgate e Exigência de Pagamento**: Após a criptografia, uma nota de resgate é exibida na tela da vítima ou em arquivos de texto (`.txt`, `.html`) deixados nos diretórios afetados (MUNIANDY et al., 2024; Wikipedia contributors, 2025a). A nota instrui a vítima sobre como pagar o resgate (geralmente em criptomoedas como Bitcoin ou Monero devido ao seu pseudo-anonimato) para obter a ferramenta de decriptografia (TANNI; HEIKES; HADI, 2022; JACKSON, 2024). As notas podem incluir ameaças de aumento do valor do resgate com o tempo ou de publicação dos dados exfiltrados (Wikipedia contributors, 2025b).

A detecção precoce e o bloqueio do processo de criptografia são cruciais. Abordagens de detecção podem monitorar eventos de escrita no sistema de arquivos, procurando por arquivos com alta entropia (característica de dados criptografados ou comprimidos), embora diferenciar entre os dois possa ser um desafio (CASINO et al., 2025).

5 OS RANSOMWARES MAIS CONHECIDOS

Diversas famílias de ransomware ganharam notoriedade devido ao seu impacto, sofisticação ou volume de ataques. Abaixo, detalhamos algumas das mais conhecidas:

5.1 LockBit

Modelo e Operação: LockBit é um grupo cibercriminoso que opera um proeminente modelo de Ransomware-as-a-Service (RaaS) desde sua aparição em fóruns de cibercrime de língua russa em janeiro de 2020. Ele recruta afiliados para conduzir ataques, utilizando táticas de dupla extorsão: criptografia de dados e ameaça de vazamento público.

Evolução: Conhecido anteriormente como ".abcd"(devido à extensão de arquivo adicionada aos arquivos criptografados), evoluiu para LockBit 2.0 em 2021 e LockBit 3.0 (ou LockBit Black) em março de 2022, com recursos aprimorados e criptografia mais robusta. Em janeiro de 2023, foi lançado o LockBit Green, incorporando código do ransomware Conti.

Técnicas: O LockBit se auto-propaga dentro de uma rede usando Windows PowerShell e Server Message Block (SMB). Utiliza ferramentas como Mimikatz para coletar credenciais, desabilita produtos de segurança e evade defesas. A criptografia é realizada com AES e RSA, criptografando apenas os primeiros kilobytes de cada arquivo para maior velocidade e adicionando a extensão ".lockbit". Notas de resgate são exibidas como papel de parede e podem ser impressas.

Alvos e Impacto: O LockBit foi o ransomware mais prolífico em 2022, responsável por 44% de todos os incidentes de ransomware globalmente no início de 2023. Entre janeiro de 2020 e maio de 2023, foi usado em aproximadamente 1.700 ataques nos EUA, resultando em $91 milhões pagos em resgates. Alvos notáveis incluem Accenture (julho de 2021), Thales (janeiro de 2022), o hospital de Corbeil Essonnes na França (setembro de 2022, resgate de $10 milhões), e o Hospital for Sick Children de Toronto (dezembro de 2022), onde o grupo pediu desculpas e ofereceu a solução de decriptografia gratuitamente, alegando uma política contra atacar hospitais.

Status Atual: Em fevereiro de 2024, agências de aplicação da lei apreenderam o controle dos sites da dark web do LockBit. Apesar das ações policiais, variantes e afiliados podem continuar ativos.

5.2 Conti

Modelo e Operação: Conti foi um grupo de RaaS altamente ativo entre dezembro de 2019 e maio de 2022, acreditado ser operado pelo grupo russo Wizard Spider e possivelmente evoluído do Ryuk. Os desenvolvedores alugavam seu malware para afiliados, que realizavam os ataques e dividiam os lucros.

Técnicas: Conti utilizava diversas técnicas de infecção, incluindo e-mails de phishing (com malware BazarLoader), exploração de vulnerabilidades de software (como no protocolo SMB), e o uso de outros malwares como o TrickBot e ferramentas legítimas de simulação de adversário como Cobalt Strike. Após o acesso inicial, desabilitava ferramentas de segurança, movia-se lateralmente, exfiltrava dados valiosos e utilizava criptografia multi-threaded para rápida encriptação de arquivos, podendo também deletar backups. Empregava táticas de dupla extorsão, com um site de vazamento para publicar dados roubados.

Alvos e Impacto: Conti era conhecido por ataques agressivos a uma vasta gama de organizações públicas e privadas, incluindo saúde, educação, governos e infraestruturas críticas. Ataques notáveis incluem JVCKenwood (setembro de 2021), o Health Service Executive (HSE) da Irlanda (maio de 2021, forçando o desligamento do sistema), o governo da Costa Rica (abril de 2022, levando à declaração de emergência nacional) e a cidade de Tulsa (maio de 2021).

Status Atual: O grupo sofreu um grande golpe em fevereiro de 2022, quando declarou apoio à invasão da Ucrânia pela Rússia, o que reduziu sua receita, pois as vítimas se tornaram relutantes em pagar. Concomitantemente, um insider vazou conversas internas e código-fonte, expondo as operações do grupo. Embora o Conti tenha encerrado seu site e ataques sob essa marca em 2022, acredita-se que seus membros se reorganizaram em outras operações de

ransomware.

5.3 Ryuk

Origem e Operação: Ryuk surgiu em agosto de 2018, sendo operado pelo sofisticado grupo de eCrime WIZARD SPIDER. É derivado do código-fonte do Hermes, um ransomware comercial, mas Ryuk foi especificamente adaptado para ataques direcionados a grandes organizações ("big game hunting") em busca de resgates elevados.

Técnicas: Ryuk é conhecido por sua capacidade de identificar e criptografar unidades de rede e recursos, além de deletar cópias de sombra (shadow copies) no endpoint, impossibilitando a restauração do sistema Windows sem backups externos. A criptografia utiliza RSA-2048 e AES-256, com chaves armazenadas no executável no formato Microsoft SIMPLEBLOB e um marcador de arquivo "HERMES". Uma diferença notável em relação ao Hermes é que o Ryuk incorpora duas chaves RSA públicas no executável e não gera um par de chaves RSA específico da vítima no host; em vez disso, a chave privada da "vítima"(usada para proteger a chave AES de criptografia de arquivo) é também criptografada e embutida, sugerindo que pares de chaves RSA são pré-gerados para cada vítima/executável. A entrega frequentemente ocorre após infecções pelos trojans Emotet e TrickBot, que fornecem o acesso inicial e as credenciais administrativas.

Alvos e Impacto: Ryuk visa organizações de alto perfil onde os atacantes esperam pagamentos significativos, como EMCOR, hospitais UHS e diversos jornais. Estima-se que tenha gerado $61 milhões para seus operadores entre fevereiro de 2018 e outubro de 2019. O valor do resgate varia consideravelmente, sugerindo um cálculo baseado no tamanho e valor da organização vítima.

Status Atual: Embora grupos como WIZARD SPIDER possam adaptar suas ferramentas, o Ryuk como marca específica pode ter sido sucedido por outras variantes ou operações do mesmo grupo.

5.4 WannaCry

Origem e Propagação: O ataque WannaCry em maio de 2017 foi um evento global que explorou a vulnerabilidade EternalBlue no protocolo SMB do Microsoft Windows. O EternalBlue, um exploit desenvolvido pela NSA dos EUA, foi vazado pelo grupo The Shadow Brokers um mês antes do ataque. WannaCry agia como um cryptoworm, espalhando-se automaticamente para computadores vulneráveis na mesma rede e aleatoriamente pela Internet.

Técnicas: Ao ser executado, verificava um "kill switch"(um nome de domínio específico); se não encontrado, criptografava os dados do computador e tentava se propagar. Utilizava a ferramenta DoublePulsar para instalar e executar cópias de si mesmo. Exigia resgate em Bitcoin, cerca de US$300 a US$600.

Impacto: Infectou mais de 230.000 computadores em mais de 150 países em um dia. Organizações que não haviam aplicado o patch de segurança da Microsoft de março de 2017

foram afetadas, com um impacto particularmente severo em sistemas Windows não suportados como o XP (embora estudos da Kaspersky Lab tenham indicado que 98% dos computadores afetados rodavam Windows 7). O Serviço Nacional de Saúde (NHS) do Reino Unido foi um dos mais atingidos, com até 70.000 dispositivos afetados e um custo de recuperação de $100 milhões. As perdas econômicas globais foram estimadas em mais de $4 bilhões. O ataque foi interrompido algumas horas após seu início pela descoberta e registro do domínio kill switch por Marcus Hutchins.

Status Atual: Embora o WannaCry original tenha sido contido, a vulnerabilidade EternalBlue continuou a ser explorada por outros malwares, e variantes do WannaCry podem ter surgido.

5.5 CryptoLocker

Contexto Histórico: Surgiu em setembro de 2013 e operou principalmente até maio de 2014. Foi um dos primeiros ransomwares a usar criptografia assimétrica forte (RSA-2048) de forma eficaz e a exigir pagamento em Bitcoin.

Técnicas: Disseminava-se através de anexos de e-mail infectados (frequentemente arquivos ZIP disfarçados de notificações de empresas de logística ou faturas). Após a infecção, buscava e criptografava arquivos com extensões comuns (documentos, imagens). As chaves de decriptografia eram armazenadas nos servidores dos atacantes.

Impacto: Estima-se que tenha infectado cerca de 500.000 máquinas. A operação foi significativamente desmantelada pela Operação Tovar, que derrubou a botnet Gameover ZeuS, usada para distribuir o CryptoLocker. Um portal online foi criado por autoridades e empresas de segurança para que as vítimas pudessem obter chaves de decriptografia gratuitamente, após a apreensão de parte da infraestrutura dos criminosos.

Status Atual: Inativo, mas seu sucesso pavimentou o caminho para muitos outros crypto ransomwares.

5.6 REvil (Sodinokibi)

Modelo e Operação: REvil, também conhecido como Sodinokibi, surgiu em abril de 2019 e operava como um RaaS. Era conhecido por suas altas demandas de resgate e por visar uma ampla gama de setores, incluindo empresas privadas, agências governamentais e instituições médicas e educacionais.

Técnicas: Os afiliados do REvil usavam diversos métodos de intrusão. No notório ataque à Kaseya VSA (uma plataforma de gerenciamento de TI para MSPs) em julho de 2021, o REvil explorou uma vulnerabilidade de dia zero para distribuir o ransomware a jusante para os clientes dos MSPs. O ataque à Kaseya envolveu o uso de PowerShell para desabilitar o Windows Defender, copiar e renomear certutil.exe para evadir detecções baseadas em nome (mascaramento), e então usar o cert.exe modificado para decodificar e executar a carga útil do ransomware (agent.exe). O agent.exe era assinado digitalmente com um certificado válido e

utilizava DLL side-loading com uma versão antiga do MsMpEng.exe para executar o encriptador mpsvc.dll. Empregava táticas de dupla extorsão.

Alvos e Impacto: Além do ataque à Kaseya, que afetou milhares de pequenas empresas e MSPs, o REvil foi responsável pelo ataque à JBS Foods, um grande fornecedor de produtos agrícolas, impactando 98% de sua rede de mais de 5.000 servidores e causando grande interrupção no processamento e entrega de alimentos.

Status Atual: O grupo REvil desapareceu abruptamente em julho de 2021, após o ataque à Kaseya, mas ressurgiu brevemente antes de ser alvo de uma operação policial internacional que levou à prisão de alguns membros e ao desmantelamento de parte de sua infraestrutura no final de 2021 e início de 2022. O Departamento de Estado dos EUA ofereceu recompensas de até $10 milhões por informações sobre líderes do grupo.

5.7 ALPHV (BlackCat)

Modelo e Operação: ALPHV, também conhecido como BlackCat ou Noberus, é um grupo de RaaS que surgiu no final de 2021, supostamente com membros ligados aos extintos grupos DarkSide e BlackMatter. É notável por ser um dos primeiros ransomwares escritos na linguagem de programação Rust, o que lhe confere vantagens como compatibilidade multiplataforma (Windows e Linux), velocidade de criptografia e maior dificuldade de engenharia reversa.

Técnicas: Ganha acesso inicial através de RDP, credenciais comprometidas e vulnerabilidades de servidores Exchange. Após a infecção, criptografa arquivos e exfiltra dados para táticas de dupla ou tripla extorsão (ameaça adicional de ataques DDoS). O ALPHV é altamente personalizável, permitindo que os operadores escolham algoritmos de criptografia, personalizem a nota de resgate e especifiquem arquivos a serem ignorados ou processos a serem encerrados. Oferece um pagamento mais alto aos afiliados (80-90%). Possui um site público de vazamento de dados para aumentar a pressão sobre as vítimas. Uma nova variante chamada "Sphynx"é considerada ainda mais rápida e eficiente.

Alvos e Impacto: Tem como alvo diversas indústrias, incluindo saúde, finanças e governo.

Status Atual: Permanece uma ameaça ativa e significativa.

5.8 Clop (Cl0p)

Modelo e Operação: O Clop (ou Cl0p) é um grupo de ransomware conhecido por explorar vulnerabilidades de dia zero em softwares de transferência de arquivos para realizar ataques em massa, com foco principal na exfiltração de dados para extorsão, em vez de apenas criptografia. Formado em 2019, opera como RaaS.

Técnicas: Notabilizou-se pelos ataques que exploraram vulnerabilidades nos softwares Accellion FTA (2020-2021), Fortra GoAnywhere MFT (CVE-2023-0669 em 2023) e Progress MOVEit Transfer (CVE-2023-34362, CVE-2023-35036, CVE-2023-35708 em 2023). No caso do MOVEit, o Clop explorou vulnerabilidades de injeção SQL para instalar um webshell, permitindo listar pastas/arquivos/usuários, baixar qualquer arquivo e adicionar um usuário backdoor

administrativo. Recentemente (outubro de 2024), o Clop também foi associado à exploração de vulnerabilidades (CVE-2024-50623, CVE-2024-55956) em produtos de compartilhamento de arquivos da Cleo, implantando um backdoor Java chamado Malichus.

Alvos e Impacto: Os ataques do Clop têm um vasto alcance devido à natureza das vulnerabilidades exploradas em softwares amplamente utilizados. O ataque ao MOVEit afetou centenas de organizações globalmente, incluindo grandes empresas como BBC, British Airways (via o fornecedor de folha de pagamento Zellis), CalPERS (Sistema de Aposentadoria dos Funcionários Públicos da Califórnia, via o fornecedor PBI Research Services), Shell, Siemens Energy, entre muitas outras. O grupo alega deletar dados de entidades governamentais, policiais ou de pesquisa sem pagamento.

Status Atual: O FBI ofereceu uma recompensa de $10 milhões por informações sobre o grupo. Continua sendo uma ameaça altamente ativa e perigosa, especializada em ataques à cadeia de suprimentos via softwares de transferência de arquivos.

A compreensão das características e táticas dessas famílias de ransomware é essencial para o desenvolvimento de contramedidas e estratégias de defesa mais eficazes. A tendência de profissionalização, a adoção de modelos RaaS e a contínua busca por novas vulnerabilidades e métodos de extorsão indicam que o cenário de ransomware permanecerá dinâmico e desafiador.

6 TÉCNICAS DE PROTEÇÃO CONTRA RANSOMWARE

A proteção eficaz contra ransomware requer uma abordagem multifacetada, combinando defesas tecnológicas, processos robustos e conscientização contínua dos usuários. Nenhuma medida isolada é suficiente; a resiliência é construída através de camadas de segurança.

6.1 Conscientização e Treinamento de Segurança

O elemento humano é frequentemente o elo mais fraco explorado pelos atacantes de ransomware, principalmente através de e-mails de phishing e engenharia social.

- **Treinamento Regular:** Todos os funcionários devem receber treinamento de conscientização sobre segurança cibernética que cubra a identificação de e-mails de phishing, links e anexos suspeitos, e os perigos de clicar em conteúdo não solicitado. O treinamento deve ser contínuo e atualizado para refletir as táticas mais recentes dos atacantes.

- **Simulações de Phishing:** Campanhas de simulação de phishing ajudam a avaliar a eficácia do treinamento e a reforçar o aprendizado, medindo o quão bem os usuários identificam e reportam tentativas de phishing. A KnowBe4 recomenda iniciar com um módulo abrangente que cubra tópicos como engenharia social, phishing, malware e ransomware, e automatizar o processo para novos funcionários.

- **Cultura de Segurança:** Promover uma cultura organizacional onde a segurança é responsabilidade de todos e onde os funcionários se sintam confortáveis para reportar incidentes ou atividades suspeitas sem receio de punição.

6.2 Higiene Cibernética e Controles Técnicos Preventivos

Práticas sólidas de higiene cibernética e a implementação de controles técnicos são fundamentais para reduzir a superfície de ataque.

- **Atualizações e Gerenciamento de Patches:** Manter sistemas operacionais, softwares e firmwares constantemente atualizados com os últimos patches de segurança é crucial para corrigir vulnerabilidades conhecidas que podem ser exploradas por ransomware. Priorizar patches para vulnerabilidades críticas e aquelas em sistemas voltados para a Internet.

- **Senhas Fortes e Autenticação Multifator (MFA):** Exigir o uso de senhas complexas e únicas para todas as contas e, fundamentalmente, habilitar a MFA para todos os acessos, especialmente para contas administrativas e acesso remoto. A MFA adiciona uma camada crítica de segurança contra o comprometimento de credenciais.

- **Segmentação de Rede:** Dividir a rede em segmentos menores e isolados pode ajudar a conter a propagação do ransomware caso um segmento seja comprometido. O princípio do Zero Trust, que assume que nenhuma confiança implícita deve ser dada, deve ser aplicado ao acesso entre segmentos.

- **Controle de Acesso e Princípio do Menor Privilégio:** Conceder aos usuários e serviços apenas os níveis de acesso estritamente necessários para realizar suas funções. Limitar privilégios administrativos reduz o impacto potencial de uma conta comprometida.

- **Segurança de Endpoints:** Utilizar soluções de segurança de endpoint robustas, como software antivírus/antimalware de próxima geração (NGAV), Endpoint Detection and Response (EDR) e Extended Detection and Response (XDR). Essas ferramentas podem detectar e bloquear atividades maliciosas e comportamentos anômalos associados ao ransomware. O EDR/XDR fornece visibilidade e capacidade de resposta em endpoints e outras camadas da pilha de segurança.

- **Filtragem de E-mail e Web:** Implementar filtros de e-mail para bloquear spam, phishing e anexos maliciosos. Utilizar soluções de segurança da web para bloquear o acesso a sites maliciosos conhecidos. A implementação do DMARC (Domain-based Message Authentication, Reporting and Conformance) ajuda a proteger contra e-mails falsificados.

- **Desabilitar Macros e Protocolos Desnecessários:** Desabilitar macros de arquivos do Microsoft Office transmitidos por e-mail. Desabilitar portas e protocolos não utilizados para fins comerciais, como o RDP (Porta TCP 3389) quando não necessário, ou protegê-lo adequadamente com MFA e limitação de acesso. Desabilitar ou bloquear o protocolo SMB (Server Message Block) na saída da rede e remover ou desabilitar versões desatualizadas do SMB (SMBv1, SMBv2).

- **Lista de Permissões de Aplicativos (Application Whitelisting):** Permitir que apenas aplicativos aprovados e verificados sejam executados nos endpoints, impedindo a execução de malware desconhecido.

6.3 Estratégias de Backup e Plano de Recuperação de Dados

Backups robustos e testados são a última linha de defesa mais crítica contra a perda de dados por ransomware, permitindo a restauração sem o pagamento do resgate.

- **Regularidade e Abrangência:** Realizar backups regulares de todos os dados críticos e configurações de sistema. A frequência deve ser determinada pela criticidade dos dados e pelos objetivos de ponto de recuperação (RPO).
- **Regra 3-2-1 (ou Variações):** Manter pelo menos três cópias dos dados, em dois tipos diferentes de mídia, com uma cópia armazenada offline ou externamente (fora do local ou na nuvem).
- **Backups Offline e Imutáveis:** É crucial que os backups sejam mantidos offline (desconectados da rede) ou em armazenamento imutável (que não pode ser alterado ou excluído por um período definido). Isso é vital porque os atacantes de ransomware tentam ativamente encontrar e excluir ou criptografar backups acessíveis. A Microsoft recomenda proteção forte, exigindo etapas fora de banda (MFA ou PIN) antes de modificar backups online, ou armazenamento imutável como o Blob do Azure.
- **Testes de Restauração:** Testar regularmente os procedimentos de restauração de backup para garantir que os dados possam ser recuperados de forma eficaz e dentro do tempo esperado (objetivo de tempo de recuperação - RTO).
- **Proteção da Documentação de Recuperação:** Manter cópias offline de documentos de suporte necessários para a recuperação, como procedimentos de restauração, diagramas de rede e bancos de dados de gerenciamento de configuração (CMDBs).

A crescente tática dos atacantes de visar os backups (94% das organizações atingidas por ransomware em 2023 relataram tentativas de comprometimento de seus backups, segundo o Data Protection Trends Report 2024) torna a resiliência dos próprios backups um campo de batalha crítico. A simples existência de backups não é mais suficiente; sua integridade, imutabilidade e isolamento são fundamentais. Falhar em proteger os backups pode deixar o pagamento do resgate como a única opção percebida, mesmo que indesejável.

6.4 Planejamento de Resposta a Incidentes (IRP)

Um Plano de Resposta a Incidentes (IRP) bem definido e testado é essencial para gerenciar um ataque de ransomware de forma eficaz, minimizando o impacto e o tempo de inatividade.

- **Fases do IRP:** O plano deve abranger as fases clássicas de resposta a incidentes, como as definidas pelo SANS Institute ou NIST: Preparação, Identificação, Contenção, Erradicação, Recuperação e Lições Aprendidas.
- **Equipe de Resposta a Incidentes (IRT):** Designar uma equipe de resposta a incidentes com funções e responsabilidades claramente definidas, incluindo membros de TI, segurança, jurídico, comunicação e gestão executiva.
- **Playbooks de Resposta:** Desenvolver playbooks específicos para cenários de ransomware, detalhando os passos a serem seguidos.
- **Comunicação:** Estabelecer canais de comunicação claros para equipes internas, partes interessadas externas, órgãos reguladores e clientes.
- **Testes e Simulações:** Realizar testes e simulações regulares do IRP para garantir que a equipe esteja preparada e que o plano seja eficaz.
- **Revisão e Atualização:** Revisar e atualizar o IRP continuamente com base nas lições aprendidas de incidentes reais ou simulados e na evolução das ameaças.

6.5 Utilização de Frameworks de Segurança Cibernética

Adotar frameworks de segurança cibernética estabelecidos pode ajudar as organizações a estruturar suas defesas contra ransomware.

- **NIST Cybersecurity Framework (CSF) 2.0:** O NIST CSF fornece uma estrutura de padrões, diretrizes e melhores práticas para gerenciar o risco de segurança cibernética. A Revisão 1 do NIST IR 8374, "Ransomware Risk Management: A Cybersecurity Framework 2.0 Community Profile", alinha os objetivos de segurança do CSF 2.0 (Governar, Identificar, Proteger, Detectar, Responder e Recuperar) com os desafios específicos do ransomware.
- **Diretrizes da CISA:** A Cybersecurity and Infrastructure Security Agency (CISA) dos EUA oferece recursos valiosos, como o guia #StopRansomware, que compila melhores práticas de prevenção, resposta e mitigação. As recomendações incluem manter backups offline e criptografados, aplicar patches regularmente, usar MFA e realizar varreduras de vulnerabilidade.
- **Recomendações da ENISA:** A Agência da União Europeia para a Cibersegurança (ENISA) publica relatórios anuais sobre o panorama de ameaças (ETL), que frequentemente destacam o ransomware como uma ameaça principal e fornecem recomendações. As recomendações incluem a regra de backup 3-2-1, uso de software de segurança, restrição de privilégios administrativos e não pagamento do resgate.

A eficácia das estratégias de proteção está intrinsecamente ligada à sua implementação holística e à adaptação contínua. Frameworks como o NIST CSF 2.0 e o planejamento de resposta a incidentes enfatizam essa abordagem cíclica de avaliação, melhoria e adaptação, refletindo a natureza dinâmica da ameaça ransomware. A segurança contra ransomware não é um estado final, mas um processo contínuo de gerenciamento de risco que exige vigilância, investimento e adaptação constantes.

7 COMO RECUPERAR DADOS E SISTEMAS APÓS UM ATAQUE DE RANSOMWARE (QUANDO POSSÍVEL)

A recuperação após um ataque de ransomware é um processo complexo e multifásico, que exige uma resposta rápida e coordenada. O objetivo principal é restaurar as operações normais com o mínimo de perda de dados e impacto nos negócios.

7.1 Passos Imediatos Após a Detecção

Ao detectar um possível ataque de ransomware, as seguintes ações imediatas são cruciais:

- **Isolar os Sistemas Infectados:** Desconectar imediatamente os computadores, servidores ou segmentos de rede afetados da rede para prevenir a propagação do ransomware para outros sistemas. Isso inclui desabilitar conexões Wi-Fi, Bluetooth e desconectar cabos de rede.
- **Ativar o Plano de Resposta a Incidentes (IRP):** Notificar a equipe de resposta a incidentes designada e iniciar os procedimentos definidos no IRP.
- **Avaliar a Extensão do Dano:** Determinar quais sistemas e dados foram afetados e criptografados. Tentar identificar a variante específica do ransomware, se possível, analisando a nota de resgate, as extensões dos arquivos criptografados ou usando ferramentas de identificação. Ferramentas como a Bitdefender Ransomware Recognition Tool ou as listas de características de ransomware da Avast podem ajudar.
- **Preservar Evidências:** Se possível e relevante para investigações futuras ou reivindicações de seguro, preservar os sistemas afetados (ou imagens forenses deles) antes de qualquer tentativa de limpeza ou restauração.
- **Não Desligar Imediatamente (Consideração):** Algumas fontes recomendam deixar o dispositivo ligado, mas desconectado da rede, para preservar evidências voláteis na memória RAM, que podem ser úteis para a análise forense. No entanto, se o ransomware estiver ativamente criptografando, o desligamento pode interromper o processo. A decisão deve ser baseada no IRP e na situação específica.

7.2 Restauração a Partir de Backups

A restauração a partir de backups é o método preferencial e mais confiável para recuperar dados sem pagar o resgate.

- **Verificar a Integridade dos Backups:** Antes de restaurar, é fundamental garantir que os backups estejam limpos, não corrompidos e não infectados pelo ransomware. Restaure os dados para um ambiente limpo e isolado para verificação.
- **Priorizar a Restauração:** Restaurar primeiro os sistemas e dados mais críticos para os negócios para minimizar o tempo de inatividade das operações essenciais.
- **Processo de Restauração:** Seguir os procedimentos documentados no plano de recuperação de desastres. O NIST SP 1800-11 foca na integridade dos dados durante a recuperação, e a Microsoft oferece guias para restauração, incluindo arquivos do OneDrive.

7.3 Ferramentas de Decriptografia

Em alguns casos, pode ser possível decriptografar arquivos sem pagar o resgate usando ferramentas desenvolvidas por empresas de segurança ou iniciativas colaborativas.

- **Projeto "No More Ransom":** Uma iniciativa conjunta da Europol, Polícia Nacional Holandesa, Kaspersky e McAfee (e outros parceiros), que oferece uma coleção de ferramentas de decriptografia gratuitas para diversas famílias de ransomware. É importante verificar se existe uma ferramenta para a variante específica que afetou os sistemas. O site lista ferramentas para ransomwares como 777 Ransom, AES_NI, Akira, GandCrab, LockBit 3.0 (um verificador de decriptografia), Maze, REvil/Sodinokibi, Shade, TeslaCrypt, entre outros.
- **Ferramentas de Fornecedores de Segurança:** Empresas como Avast, Bitdefender, Emsisoft, Trend Micro e Kaspersky também disponibilizam decriptadores gratuitos para certas variantes de ransomware. A Bitdefender Ransomware Recognition Tool pode ajudar a identificar a família do ransomware e indicar uma ferramenta de decriptografia, se disponivel.

A disponibilidade dessas ferramentas é um testemunho do esforço colaborativo entre o setor privado e as autoridades para combater o ransomware. No entanto, sua eficácia é inerentemente reativa; elas geralmente surgem após a análise de uma variante específica, a descoberta de uma falha na criptografia implementada pelos criminosos, ou a apreensão de chaves mestras (frequentemente resultado de ações policiais). Isso implica um atraso inevitável entre o surgimento de uma nova ameaça e a potencial disponibilidade de um decriptador. Portanto, embora valiosas, as ferramentas de decriptografia não substituem a necessidade de medidas preventivas robustas e, crucialmente, de backups seguros e testados. Elas representam um último recurso com sucesso variável.

7.4 O Dilema do Pagamento do Resgate

A decisão de pagar ou não o resgate é uma das mais difíceis e controversas enfrentadas pelas vítimas de ransomware.

Recomendações Oficiais: Agências de aplicação da lei como o FBI, a CISA e a Europol geralmente desaconselham veementemente o pagamento do resgate. As razões incluem:

- Não há garantia de recuperação dos dados: Pagar não assegura que os criminosos fornecerão a chave de decriptografia correta ou funcional.
- Incentivo ao crime: O pagamento financia os criminosos, encorajando-os a realizar mais ataques e a desenvolver ransomwares mais sofisticados.
- Alvo para futuros ataques: Vítimas que pagam podem ser vistas como alvos dispostos a pagar novamente.
- Questões éticas e legais: Pagar pode financiar outras atividades criminosas ou terroristas, e em algumas jurisdições, pode haver implicações legais.

Estatísticas de Recuperação Pós-Pagamento: Dados recentes indicam que o pagamento do resgate é uma aposta arriscada.

- O relatório CyberEdge Group 2025 (dados de 2024) revelou que apenas 54% das vítimas que pagaram o resgate recuperaram seus dados, uma queda em relação aos 73% de dois anos antes.
- Um relatório da Halcyon, citando dados de 2021, indicou que apenas 8% das vítimas que pagaram recuperaram todos os seus dados, e uma pesquisa de 2023 mostrou que 21% não recuperaram dados mesmo após o pagamento.
- A Sprinto cita uma estatística alarmante de que "75% pagaram o resgate, mas não receberam seus dados de volta", embora este número pareça destoar de outras fontes e deva ser interpretado com cautela.

Custos Totais: O valor do resgate é apenas uma fração do custo total de um ataque de ransomware. Os custos adicionais incluem tempo de inatividade, perda de receita, custos de restauração e remediação, danos à reputação, possíveis multas regulatórias e perda de clientes. O custo médio de uma violação de dados por ransomware foi de $4,91 milhões em 2024, segundo a IBM.

A Tabela 2 apresenta um resumo dos prós e contras do pagamento do resgate.

De acordo com (Halcyon, 2024), a decisão de pagar ou não o resgate é um cálculo de risco complexo. As recomendações oficiais de não pagamento frequentemente colidem com as pressões operacionais e financeiras imediatas enfrentadas pela organização atacada, especialmente quando dados sensíveis foram exfiltrados (dupla extorsão). Mesmo com backups, a ameaça de vazamento de dados persiste, aumentando a tentação de pagar. No entanto, as estatísticas de

Tabela 2: Prós e Contras do Pagamento de Resgate

Argumentos a Favor do Pagamento (Perspectiva da Vítima)	**Argumentos Contra o Pagamento (Perspectiva de Segurança/Legal)**	**Realidade Estatística/Riscos Associados**
Potencial recuperação rápida de dados e sistemas críticos.	Não há garantia de recebimento da chave de decriptografia ou de sua funcionalidade.	Apenas 54% das vítimas que pagaram em 2024 recuperaram dados (queda de 73% em 2 anos). Chaves podem ser defeituosas ou incompletas.
Evitar o vazamento público de dados sensíveis exfiltrados (dupla extorsão).	Os dados já podem ter sido copiados, vendidos ou vazados antes ou mesmo após o pagamento. Pagar não garante o sigilo.	Criminosos podem não cumprir a promessa de não vazar os dados.
Retomar rapidamente as operações comerciais e minimizar perdas financeiras por inatividade.	O pagamento financia atividades criminosas e incentiva futuros ataques contra a própria organização e outras.	O custo total do incidente geralmente excede em muito o valor do resgate, incluindo custos de recuperação, tempo de inatividade e danos à reputação.
Percepção de ser a única ou a mais rápida opção quando os backups falharam ou foram comprometidos.	Pode marcar a organização como um alvo disposto a pagar, levando a futuros ataques.	21% das organizações que pagaram em 2023 ainda não conseguiram recuperar seus dados.
Evitar danos à reputação associados à perda de dados ou interrupção prolongada.	Implicações éticas e potenciais sanções legais por negociar com criminosos ou entidades sancionadas.	A notícia do pagamento do resgate pode, por si só, causar dano reputacional.

recuperação pós-pagamento e a possibilidade de os criminosos não cumprirem suas promessas tornam essa decisão ainda mais arriscada. As organizações precisam se preparar para esse dilema em seus IRPs, considerando não apenas a recuperação técnica, mas também as implicações legais, de conformidade e de relações públicas de um vazamento de dados, e ter estratégias para mitigar esses riscos independentemente da decisão de pagamento. A existência de seguros cibernéticos também pode influenciar essa decisão, embora a cobertura possa ser limitada ou condicionada.

7.5 Reconstrução de Sistemas e Validação Pós-Recuperação

Após a erradicação do malware (seja por ferramentas, restauração ou, em último caso, pagamento) e a restauração dos dados, seguem-se etapas críticas:

- **Reconstrução Segura:** Reconstruir os sistemas afetados a partir de imagens limpas (*gold images*) ou reinstalar sistemas operacionais e aplicativos. Aplicar todos os patches de segurança e corrigir as vulnerabilidades que foram exploradas no ataque inicial.
- **Restauração de Dados Verificada:** Restaurar dados a partir de backups limpos e verificados. Garantir que os dados restaurados estejam íntegros e livres de malware.
- **Validação e Testes:** Testar exaustivamente os sistemas e aplicativos restaurados para garantir que estão funcionando normalmente e de forma segura antes de serem colocados de volta em produção.
- **Monitoramento Contínuo:** Implementar monitoramento reforçado nos sistemas recuperados para detectar qualquer atividade anômala ou sinais de reinfecção.
- **Análise Forense e Lições Aprendidas:** Conduzir uma análise forense detalhada para entender completamente o vetor de ataque, a linha do tempo, o escopo e as táticas do invasor. Documentar as lições aprendidas para melhorar o IRP, as defesas e o treinamento de conscientização. Esta fase é crucial e alinha-se com as recomendações do NIST SP 800-61r3.

A recuperação de um ataque de ransomware é uma oportunidade para fortalecer a postura de segurança da organização e aumentar a resiliência contra futuras ameaças.

8 DADOS ATUAIS E TENDÊNCIAS (2024-2025)

O cenário de ransomware continua a evoluir rapidamente, com novas táticas, alvos e tendências emergindo constantemente. Dados de relatórios recentes fornecem um panorama da situação atual:

8.1 Frequência e Prevalência de Ataques

- **Sophos (State of Ransomware 2024):** 59% das organizações foram atingidas por ransomware no último ano (Sophos, 2024).
- **Sprinto (2024/2025):** Algumas estatísticas citam até 90% das organizações atingidas, mas um valor mais alinhado com outras fontes indica que 72,7% das empresas globalmente foram vitimadas em 2023 (Sprinto, 2024).
- **Verizon (DBIR 2025):** Houve um aumento de 37% nos incidentes de ransomware em relação ao ano anterior, estando presente em 44% de todas as violações analisadas. As PMEs são desproporcionalmente afetadas, com ransomware presente em 88% das suas violações (Verizon Business, 2025).
- **Mandiant (2023):** Observou-se um aumento de 75% em postagens em sites de vazamento de dados (DLS) e mais de 20% nas investigações envolvendo ransomware, comparando 2022 com 2023 (SADAYAPPAN et al., 2024).

8.2 Custos e Demandas de Resgate

- **IBM (Cost of a Data Breach Report 2024):** O custo médio global de uma violação de dados atingiu $4,88 milhões. Para ransomware, o custo médio foi de $4,91 milhões ().
- **Sophos (2024):** Relatou aumento de 5 vezes nas contas de resgate nos últimos 12 meses (Sophos, 2024).
- **Halcyon (2024):** O pagamento médio de resgate foi de $2 milhões (aumento de 500% em relação ao ano anterior). O custo médio de recuperação, excluindo o resgate, foi de $2,73 milhões (Halcyon, 2024).
- **Verizon DBIR (2025):** A mediana do pagamento de resgate caiu para $115.000 em 2024 (de $150.000 em 2023). 64% das vítimas agora se recusam a pagar, um aumento em relação aos 50% de dois anos atrás (Verizon Business, 2025).
- **Chainalysis (2025 Crypto Crime Report):** O volume total de pagamentos de resgate em criptomoedas diminuiu aproximadamente 35% em relação ao ano anterior, atribuído ao aumento das ações de aplicação da lei, melhor colaboração internacional e crescente recusa das vítimas em pagar (Chainalysis, 2025).

A aparente contradição nos dados sobre o volume de pagamentos de resgate pode ser reflexo de diferentes metodologias de pesquisa, escopos de amostragem distintos, ou uma possível bifurcação no mercado de ransomware. Alguns grupos podem estar exigindo valores astronômicos de grandes alvos, enquanto outros focam em um volume maior de ataques menores com demandas mais baixas. O impacto de operações de desmantelamento de grandes grupos e a crescente taxa de recusa em pagar também influenciam essas cifras. Estatísticas isoladas devem ser interpretadas com cautela.

8.3 Taxas de Criptografia e Exfiltração de Dados

- **Sophos (2024):** 70% dos ataques de ransomware resultam na criptografia dos dados da vítima (Sophos, 2024).
- **BlackFog (2024):** Mais de 93% dos ataques de ransomware incluem um componente de exfiltração de dados, evidenciando a prevalência da tática de dupla extorsão (BlackFog, 2025).

8.4 Vetores de Ataque e Alvos

- **Sophos (2024):** 32% dos ataques de ransomware começaram com a exploração de uma vulnerabilidade não corrigida (Sophos, 2024).
- **ENISA (2023-2024):** No setor financeiro europeu, os bancos foram os mais afetados (46% dos 488 incidentes analisados). O ransomware afetou principalmente provedores de serviços (29%) e seguradoras (17%) dentro deste setor (European Union Agency for Cybersecurity (ENISA), 2024).
- **Kaspersky (2025):** Tendências emergentes incluem o uso crescente de IA no desenvolvimento de ransomware (e.g., grupo FunkSec) e a exploração de vulnerabilidades não convencionais, como webcams para contornar EDR (e.g., grupo Akira) (Kaspersky Lab, 2025).
- **Mandiant (2023):** Aumento de variantes de ransomware visando sistemas Linux e ESXi, expandindo a superfície de ataque além do Windows (SADAYAPPAN et al., 2024).
- **Verizon DBIR (2025):** O envolvimento de terceiros em violações de dados dobrou para 30%. A exploração de vulnerabilidades aumentou 34%, com foco em exploits de dia zero em dispositivos de perímetro e VPNs. O abuso de credenciais (22%) e a exploração de vulnerabilidades (20%) continuam sendo os principais vetores de ataque inicial (Verizon Business, 2025).

O aumento significativo no comprometimento de terceiros e o uso de infostealers como precursores de ataques de ransomware indicam uma expansão da superfície de ataque para além do perímetro direto da organização. Isso sugere que os atacantes estão explorando elos mais fracos na cadeia de suprimentos ou utilizando credenciais roubadas de funcionários para obter acesso inicial. Consequentemente, a segurança da cadeia de suprimentos e o gerenciamento robusto de identidades e credenciais tornam-se ainda mais críticos.

8.5 Recuperação e Taxas de Pagamento

- **CyberEdge Group (2025):** Apenas 54% das vítimas que pagaram resgate em 2024 recuperaram seus dados, uma queda significativa em relação aos 73% de dois anos antes.

41% das organizações vitimadas optaram por pagar em 2024, uma redução em relação aos 63% de três anos antes (CyberEdge Group, 2025).

- **Sophos:** Em 2022, 41% das vítimas pagaram o resgate, enquanto 73% utilizaram backups para recuperar seus dados (Sophos, 2024).
- **Sprinto (Data Protection Trends Report 2024):** 94% das organizações atingidas por ransomware relataram que os cibercriminosos tentaram comprometer seus backups durante o ataque (Sprinto, 2024).

Esses dados ressaltam a importância de backups seguros e testados, bem como a crescente relutância das organizações em pagar resgates, possivelmente devido à maior conscientização sobre a incerteza da recuperação dos dados e às recomendações das autoridades.

CONCLUSÕES

O ransomware permanece uma ameaça cibernética persistente, dinâmica e de alto impacto, evoluindo continuamente em suas táticas, alvos e modelos de negócios. Desde o rudimentar AIDS Trojan até as sofisticadas operações de RaaS atuais que empregam dupla e tripla extorsão, os atores de ransomware demonstraram uma capacidade notável de adaptação e inovação. A análise histórica revela uma trajetória de crescente complexidade técnica, exploração de novas vulnerabilidades e uma profissionalização das atividades criminosas.

As técnicas de ataque continuam a explorar tanto falhas tecnológicas quanto o fator humano, com phishing, exploração de vulnerabilidades não corrigidas e comprometimento de credenciais permanecendo vetores de infecção proeminentes. A mudança para alvos de alto valor, infraestruturas críticas e a expansão para plataformas não-Windows, como Linux e ESXi, demonstram a ambição e o alcance crescentes desses grupos. A exfiltração de dados tornou-se um componente padrão, aumentando a pressão sobre as vítimas e complicando as estratégias de recuperação baseadas apenas em backups.

As estratégias de proteção devem, portanto, ser abrangentes e multicamadas, integrando rigorosa higiene cibernética, conscientização e treinamento contínuo dos usuários, tecnologias avançadas de detecção e prevenção, e, crucialmente, planos robustos de backup e recuperação de desastres. A resiliência dos próprios backups, através de imutabilidade e isolamento, emergiu como um diferencial crítico, dado o foco dos atacantes em neutralizar essa linha de defesa. A adoção de frameworks de segurança como o NIST CSF 2.0 e o desenvolvimento de Planos de Resposta a Incidentes detalhados e testados são fundamentais para uma postura de segurança proativa e adaptativa.

A decisão de pagar o resgate continua sendo um dilema complexo, com autoridades desaconselhando veementemente o pagamento, enquanto as vítimas enfrentam pressões operacionais e o risco de vazamento de dados. As estatísticas indicam que o pagamento não garante a recuperação e pode perpetuar o ciclo de ataques.

Olhando para o futuro, espera-se que o ransomware continue a evoluir, possivelmente alavancando a Inteligência Artificial tanto para aprimorar ataques (e.g., phishing mais convincente,

desenvolvimento de malware mais evasivo) quanto para fortalecer as defesas. A exploração de vulnerabilidades em um espectro cada vez maior de dispositivos conectados (IoT, OT) e a contínua sofisticação das táticas de extorsão exigirão vigilância constante. A colaboração internacional entre governos, agências de aplicação da lei e o setor privado, juntamente com a partilha de informações sobre ameaças, será indispensável para combater eficazmente esta ameaça global. Em última análise, o investimento contínuo em pesquisa, tecnologia, treinamento e, acima de tudo, em uma cultura de resiliência cibernética, é essencial para que as organizações possam enfrentar os desafios impostos pelo ransomware.

REFERÊNCIAS

Akamai Technologies. *What Is BlackCat Ransomware?* 2024. Accessed: 2024-11-26. Source: [15]. Disponível em: <https://www.akamai.com/glossary/what-is-blackcat-ransomware>.

BlackFog. *2024 State of Ransomware Annual Report*. [S.l.], 2025. Acessado em 27 de maio de 2025. Este relatório cobre dados do ano de 2024 e afirma que 94% dos ataques de ransomware envolveram exfiltração de dados. Disponível em: <https://privacy.blackfog.com/wp-content/uploads/2025/02/2024-State-of-Ransomware-Annual-Report_v1.pdf>.

CASINO, F. et al. Not on my watch: ransomware detection through classification of high-entropy file segments. *Journal of Cybersecurity*, Oxford University Press, v. 11, p. tyaf009, April 2025. Accessed: 2024-11-26. Source: [25]. Disponível em: <https://doi.org/10.1093/cybsec/tyaf009>.

Chainalysis. *The 2025 Crypto Crime Report*. [S.l.], 2025. Accessed: 2024-11-26. Data for 2024. Source: [79]. Disponível em: <https://www.chainalysis.com/wp-content/uploads/2025/02/the-2025-crypto-crime-report-release.pdf>.

CrowdStrike. *Big Game Hunting with Ryuk: Another Lucrative Targeted Ransomware*. 2019. Accessed: 2024-11-26. Source: [27]. Disponível em: <https://www.crowdstrike.com/en-us/blog/big-game-hunting-with-ryuk-another-lucrative-targeted-ransomware/>.

CyberEdge Group. *Only Half of Ransomware Victims Recover Data After Paying, Finds CyberEdge Group's 2025 Cyberthreat Defense Report*. 2025. Accessed: 2024-11-26. Source: [73]. Disponível em: <https://www.businesswire.com/news/home/20250415839378/en/Only-Half-of-Ransomware-Victims-Recover-Data-After-Paying-Finds-CyberEdge-Groups-2025-Cyberthre

European Union Agency for Cybersecurity (ENISA). *ENISA Threat Landscape 2023*. [S.l.], 2023. Reporting period: July 2022 to June 2023. Accessed: 2024-11-26. Source: [5]. Disponível em: <https://www.enisa.europa.eu/publications/enisa-threat-landscape-2023>.

European Union Agency for Cybersecurity (ENISA). *ENISA Threat Landscape: Finance Sector*. 2024. Accessed: 2024-11-26. Original report likely on ENISA website. Source: [61]. Disponível em: <https://circle.cloudsecurityalliance.org/discussion/enisa-threat-landscape-finance-sector-1>.

Halcyon. *Beyond Ransoms: The Financial Impact of Ransomware Attacks*. 2024. Accessed: 2024-11-26. Source: [74]. Disponível em: <https://www.halcyon.ai/blog/beyond-ransoms-the-financial-impact-of-ransomware-attacks>.

JACKSON, C. *Tracing the History of Ransomware: Major Attacks and Developments*. 2024. Accessed: 2024-11-26. Source: [7]. Disponível em: <https://www.cybermaxx.com/resources/tracing-the-history-of-ransomware-major-attacks-and-developments/>.

Kaspersky Lab. *Kaspersky State of Ransomware Report 2025: Global and regional insights for International Anti-Ransomware Day*. 2025. Accessed: 2024-11-26. See also: https://securelist.com/state-of-ransomware-in-2025/116475/. Source: [16]. Disponível em: <https://www.kaspersky.com/about/press-releases/kaspersky-state-of-ransomware-report-2025-global-and-regional-insights-for-international-anti-ransomwar

MasterDC. *Ransomware: How it Works and What to Do to Prevent it*. 2024. Accessed: 2024-11-26. Source: [10]. Disponível em: <https://www.masterdc.com/blog/ransomware-how-it-works-and-what-to-do-to-prevent-it/>.

MUNIANDY, M. et al. Evolution and impact of ransomware: Patterns, prevention, and recommendations for organizational resilience. *International Journal of Academic Research in Business and Social Sciences*, v. 14, n. 1, p. 2668–2687, January 2024. Accessed: 2024-11-26. Source: [8].

ResearchGate (various authors, specific paper not fully identified in snippet). *Ransomware infection vector (Figure from a research paper)*. 2024. Accessed: 2024-11-26. Snippet refers to multiple papers. Source: [18]. Disponível em: <https://www.researchgate.net/figure/Ransomware-infection-vector_fig2_336339807>.

ROBB, B. The history and evolution of ransomware. *BlackFog Blog*, September 2024. Last Updated: September 5th, 2024. Accessed: 2024-11-26. Source: [11]. Disponível em: <https://www.blackfog.com/the-history-and-evolution-of-ransomware/>.

SADAYAPPAN, B. et al. *Ransomware Rebounds: Extortion Threat Surges in 2023, Attackers Rely on Publicly Available and Legitimate Tools*. 2024. Accessed: 2024-11-26. Source: [17]. Disponível em: <https://cloud.google.com/blog/topics/threat-intelligence/ransomware-attacks-surge-rely-on-public-legitimate-tools>.

Sophos. *The State of Ransomware 2024*. 2024. Accessed: 2024-11-26. Source: [51]. Disponível em: <https://www.sophos.com/en-us/content/state-of-ransomware>.

Sprinto. *The State Of Ransomware Attacks: Top Ransomware Statistics 2025*. 2024. Accessed: 2024-11-26. Source: [52]. Disponível em: <https://sprinto.com/blog/ransomware-statistics/>.

TANNI, T. I.; HEIKES, N.; HADI, K. S. A technical analysis of redalert ransomware - targeting virtual machine files. In: *Proceedings of the ACM Conference on Computer and Communications Security (CCS '22)*. New York, NY, USA: ACM, 2022. p. 1–8. Source:.[4] The original is a student project paper, so conference details are illustrative.

ThreatDown by Malwarebytes. *What is ALPHV/BlackCat Ransomware?* 2025. Accessed: 2024-11-26. Source: [14]. Disponível em: <https://www.threatdown.com/glossary/what-is-alphv-blackcat-ransomware/>.

Verizon Business. *Verizon's 2025 Data Breach Investigations Report: Alarming surge in cyberattacks through third-parties*. 2025. Accessed: 2024-11-26. Source:.[21] Also see [77] for Rhymetec summary. Disponível em: <https://www.verizon.com/about/news/2025-data-breach-investigations-report>.

WatchGuard Technologies. *Ransomware - AIDS Trojan*. 2024. Accessed: 2024-11-26. Source: [9]. Disponível em: <https://www.watchguard.com/wgrd-ransomware/aids-trojan>.

Wikipedia contributors. *LockBit — Wikipedia, The Free Encyclopedia*. 2025. Accessed: 2024-11-26. Source: [26]. Disponível em: <https://en.wikipedia.org/wiki/LockBit>.

Wikipedia contributors. *WannaCry ransomware attack — Wikipedia, The Free Encyclopedia*. 2025. Accessed: 2024-11-26. Source: [13]. Disponível em: <https://en.wikipedia.org/wiki/WannaCry_ransomware_attack>.