# Redes-2025

Vinicius H. C. Rosa, 9395067

December 2025

## 1 Introdução

Ransomware evoluiu de um malware rudimentar distribuído por disquetes em 1989 para um ecossistema industrializado e altamente sofisticado, capaz de paralisar governos, empresas e infraestruturas críticas. Ataques recentes exploram falhas em sistemas expostos à internet, realizam movimento lateral altamente automatizado e utilizam criptografia de nível militar para tornar a recuperação inviável sem o pagamento de resgate.

Além dos danos financeiros — que ultrapassam bilhões de dólares anuais — os ataques afetam serviços essenciais, como hospitais, transporte, energia e cadeias de suprimento. Segundo (Saccone *et al.*, 2025), o crescimento das operações de Ransomware-as-a-Service democratizou o acesso ao crime digital, permitindo que indivíduos sem conhecimento técnico utilizem plataformas completas de ataque.

Diante desse cenário, compreender como ransomware se propaga e opera é fundamental para fortalecer medidas de defesa, prevenção e detecção precoce.

## 2 Evolução do Ransomware

A trajetória do ransomware, desde 1989, mostra um salto de códigos rudimentares para operações industriais, guiadas por incentivos econômicos e ecossistemas criminosos maduros. A evolução acompanha a expansão da superfície digital e a profissionalização das gangues, com mudanças claras nas técnicas, vetores de entrega e modelos de extorsão (Begovic; Al-Ali; Malluhi, 2023; Lella *et al.*, 2023).

### 2.1 Primeira fase: germinação (1989–2009)

Os primeiros ataques (como o *AIDS Trojan*) usavam criptografia fraca e dependiam de engenharia social simples (disquetes e contadores de reinicialização). Apesar de inaugurar o conceito de pagamento por resgate, essa fase carecia de automação e escala, resultando em impacto limitado (Begovic; Al-Ali; Malluhi, 2023). Variantes como Gpcode incorporaram algoritmos mais robustos, mas ainda operavam de forma isolada e sem alvo setorial definido.

### 2.2 Segunda fase: industrialização inicial (2010–2016)

Malwares como CryptoLocker consolidaram o uso combinado de AES e RSA, tornando a recuperação sem chave praticamente inviável e demonstrando viabilidade econômica. Campanhas de *spam*, *exploit kits* e botnets ampliaram a superfície de entrega. Surge

o modelo de *Ransomware-as-a-Service* (RaaS), que democratiza a operação criminosa e acelera a proliferação de famílias (Shaikh *et al.*, 2024; Alzahrani *et al.*, 2025). A partir de 2014, observa-se a diversificação para plataformas móveis e macOS, explorando brechas em ecossistemas ARM e canais laterais de hardware (Zhang; Xiao; Zhang, 2016). Essa fase estabelece a ponte entre experimentação técnica e um mercado clandestino mais estruturado.

### 2.3 Terceira fase: consolidação, dupla extorsão e especialização (2017–presente)

O surto do WannaCry (2017) marcou a combinação de exploração automatizada (EternalBlue) com criptografia massiva, inaugurando a era das operações de alta velocidade. A partir daí, as gangues incorporam movimentação lateral acelerada, elevação de privilégios e persistência avançada como padrão (Saccone *et al.*, 2025). Modelos de dupla e tripla extorsão (cifrar, exfiltrar e ameaçar terceiros) tornam-se dominantes, elevando o valor dos resgates e a pressão sobre vítimas. Relatórios recentes mostram que o ransomware compõe parcela relevante do panorama de ameaças globais, com campanhas orientadas a setores críticos e cadeias de suprimento (Lella *et al.*, 2023). Estudos de tráfego e kill chain evidenciam ataques que alternam exploração de CVEs críticas, contas válidas e propagação interna automatizada (Cen *et al.*, 2024).

No estágio atual, observam-se dois eixos principais: (i) diversificação de técnicas para evasão e cifragem (criptografia intermitente, ofuscação e uso de IA) (Begovic; Al-Ali; Malluhi, 2023), e (ii) especialização por alvo — gangues generalistas (LockBit, ALPHV) ampliam escala e sofisticação, enquanto grupos "especialistas"preferem phishing e credenciais reaproveitadas em nichos setoriais (Saccone *et al.*, 2025). A evolução recente também reforça a pesquisa de detecção precoce (pré-encriptação), com abordagens baseadas em rede e comportamento (Akibis *et al.*, 2024; Rollere *et al.*, 2025).

## 3 Vetores de Propagação

Os estudos recentes convergem para um conjunto recorrente de vetores de propagação. As pesquisas de Cen et al. (Cen *et al.*, 2024), Alzahrani et al. (Alzahrani *et al.*, 2025) e Saccone et al. (Saccone *et al.*, 2025) mostram que os operadores combinam ataques de phishing, exploração de CVEs, abuso de credenciais e efeitos em cadeia para maximizar a taxa de entrada e cobertura na rede vítima.

### 3.1 Phishing e Engenharia Social

Campanhas de *malspam* continuam sendo a forma mais frequente de entrega inicial, aproveitando anexos com macros ou links para *payloads* hospedados externamente (Cen *et al.*, 2024). O trabalho de Shaikh et al. evidencia que a expansão do trabalho remoto aumentou a superfície de ataque para e-mails maliciosos e *mails* de spear-phishing (Shaikh *et al.*, 2024). Saccone et al. mostram que gangues "especialistas"dependem mais de phishing e reutilização de credenciais do que grupos generalistas (Saccone *et al.*, 2025).

### 3.2 Exploração de Vulnerabilidades (CVEs) e Serviços Expostos

A base de 16 mil incidentes analisada por Saccone et al. revela que a técnica T1190 (exploração de serviços expostos) é um dos pontos mais usados no *kill chain*, com destaque para falhas de alta severidade (Saccone *et al.*, 2025). O modelo de Ransomware-as-a-Service descrito por Alzahrani et al. indica que afiliados exploram CVEs antigas em sistemas desatualizados, mantendo baixo custo de intrusão (Alzahrani *et al.*, 2025). Na fase inicial, Cen et al. listam exploração remota (RCE) e kits de *exploit* como vetores típicos (Cen *et al.*, 2024), reforçando a necessidade de gestão de patches e redução de superfície exposta.

### 3.3 Ataques a RDP, VPN e Credenciais Comprometidas

Segundo Cen et al., serviços de área remota com senhas fracas ou reaproveitadas são frequentemente violados por *brute force* para entrega do *payload* (Cen *et al.*, 2024). Saccone et al. apontam que grupos especializados em setores específicos privilegiam credenciais vazadas ou compradas para evitar ruído de exploração (Saccone *et al.*, 2025). Esses vetores aparecem no estágio P1 da cadeia de ataque de Cen et al., antes mesmo de qualquer persistência ou movimento lateral (Cen *et al.*, 2024).

### 3.4 Cadeia de Suprimentos e Atualizações Comprometidas

Cen et al. destacam que atualizações de software e dependências confiáveis podem ser adulteradas para entregar o ransomware, explorando a relação de confiança entre fornecedor e cliente (Cen *et al.*, 2024). Esse vetor dilui a origem do ataque e dificulta a detecção precoce, pois o tráfego aparenta ser legítimo e assinado.

### 3.5 Propagação Interna Automatizada

Após o acesso inicial, a movimentação lateral tende a ser rápida e automatizada. Cen et al. descrevem o uso de protocolos de compartilhamento de arquivos e ferramentas internas para ampliar o alcance do *payload* (Cen *et al.*, 2024), enquanto Saccone et al. mapeiam a sequência TTP que vai de escalada de privilégios à criptografia (T1486) (Saccone *et al.*, 2025). Estudos focados em tráfego, como Akibis et al. (Akibis *et al.*, 2024), medem a velocidade de varredura e variação de pacotes durante esse movimento lateral, fornecendo indicadores para detecção antes da cifragem. Rollere et al. mostram que gráficos de correlação temporal destacam essa aceleração do comportamento e ajudam a sinalizar hosts recém-comprometidos (Rollere *et al.*, 2025).

## 4 Modus Operandi: O Ciclo de Ataque de Ransomware

O *kill chain* de ransomware segue um padrão recorrente identificado em grandes bases de incidentes (Saccone *et al.*, 2025; Cen *et al.*, 2024; Lella *et al.*, 2023): uma fase inicial de reconhecimento e entrega, seguida de instalação e movimentação lateral, impacto (criptação e sabotagem) e extorsão. A maturidade de Ransomware-as-a-Service permite que afiliados escolham TTPs conforme alvo e pressa operacional (Alzahrani *et al.*, 2025).

## 4.1 Fase 1 — Reconhecimento e Entrega

O atacante mapeia a superfície exposta (serviços, VPN/RDP, aplicações web) e perfis de usuários suscetíveis a phishing. Vetores típicos incluem:

- phishing e *malspam* com macros ou links (Cen *et al.*, 2024; Shaikh *et al.*, 2024);
- exploração de CVEs em serviços expostos (T1190), muitas vezes N-day de alta severidade (Saccone *et al.*, 2025);
- malvertising e *drive-by* via kits de exploit (Cen *et al.*, 2024);
- cadeia de suprimentos e atualizações adulteradas (Lella *et al.*, 2023).

## 4.2 Fase 2 — Instalação, Persistência e Movimentação Lateral

O payload estabelece persistência (tarefas agendadas, serviços) e coleta credenciais para ampliar o domínio:

- T1078 (contas válidas) e T1003 (credential dumping) para ganhar acesso lateral (Saccone *et al.*, 2025);
- uso de ferramentas nativas (*living off the land*) para evitar detecção (Cen *et al.*, 2024);
- propagação automática via SMB/AD mal configurados, com velocidade mensurável em tráfego de rede (Akibis *et al.*, 2024).

Grupos generalistas (LockBit, ALPHV) tendem a combinar exploits recentes com brute-force de RDP/VPN, enquanto especialistas preferem credenciais vazadas e menor ruído (Saccone *et al.*, 2025).

## 4.3 Fase 3 — Impacto: Criptografia, Sabotagem e Exfiltração

Antes da cifragem, o malware neutraliza defesas, remove backups locais e inventaria arquivos críticos (Begovic; Al-Ali; Malluhi, 2023). Técnicas observadas:

- criptação seletiva ou intermitente para acelerar impacto e reduzir rastros (Begovic; Al-Ali; Malluhi, 2023);
- exfiltração prévia de dados sensíveis (dupla/tripla extorsão) (Lella *et al.*, 2023);
- uso de T1486 (Data Encrypted for Impact) como etapa final do ciclo técnico (Saccone *et al.*, 2025).

Modelos comportamentais recentes indicam aceleração e correlação temporal entre varredura interna, picos de I/O e início da cifragem, úteis para detecção pré-encriptação (Rollere *et al.*, 2025).

### 4.4 Fase 4 — Extorsão e Negociação

Com dados cifrados e/ou exfiltrados, o grupo inicia comunicação controlada (portais Tor, chats) e apresenta exigências:

- entrega de chave mediante pagamento e promessa de não vazamento;
- ameaça de publicar dados e/ou conduzir DDoS como pressão adicional (Lella *et al.*, 2023);
- em operações RaaS, divisão de receita entre operador e afiliado (Alzahrani *et al.*, 2025).

Essa etapa fecha o ciclo econômico do ataque, mas pode ser reaberta caso a vítima negocie parcialmente ou atrase, gerando novas alavancas de coerção.

## 5 Estratégias de Gangues Criminosas

A análise de mais de 16.000 ataques identifica dois perfis principais.

### 5.1 Gangues Generalistas

Atacam múltiplos setores e utilizam técnicas avançadas:

- LockBit;
- BlackCat/ALPHV;
- Cl0p.

Características marcantes:

- automação;
- exploração em larga escala;
- criptografia rápida;
- alta taxa de sucesso.

### 5.2 Gangues Especializadas

Focam em setores específicos:

- saúde;
- finanças;
- manufatura.

Usam técnicas mais simples:

- spear-phishing;
- credenciais vazadas.

# 6 Detecção Precoce (Pre-Encryption)

A detecção tradicional ocorre após o início da criptografia, quando já é tarde para evitar danos. Pesquisas recentes buscam detecção antes da destruição.

## 6.1 Análise de API Calls

Monitoramento de chamadas relacionadas a criptografia e I/O.

## 6.2 Aprendizado de Máquina

Modelos treinados com:

- padrões de acesso a arquivos;
- sequências de APIs;
- comportamento do processo.

## 6.3 Correlação Temporal API + IRP

Método mais preciso, pois identifica o momento exato em que o ransomware inicia sua preparação para criptografia.

Usuários com detecção precoce perdem entre 0% e 5% dos arquivos, enquanto detecção tardia pode resultar em perda total.

# 7 Conclusão

Ransomware evoluiu para uma ameaça altamente organizada, automatizada e apoiada por um mercado lucrativo de ferramentas criminosas. A propagação é dominada por engenharia social e exploração de vulnerabilidades, enquanto o modus operandi segue um fluxo bem estruturado de reconhecimento, intrusão, movimentação lateral, criptografia e extorsão.

Como consequência, a defesa moderna deve priorizar:

- correção rápida de CVEs;
- proteção contra phishing;
- hardening de RDP e Active Directory;
- monitoramento comportamental;
- detecção precoce.

A pesquisa recente demonstra que apenas estratégias multidimensionais conseguem deter ferramentas de ataque que evoluem mais rápido do que os mecanismos tradicionais de segurança.

# Referências


AKIBIS, Michael *et al.* **Measuring Ransomware Propagation Patterns via Network Traffic Analysis: An Automated Approach**. [*S. l.: s. n.*], set. 2024. DOI: 10.21203/rs.3.rs-5180048/v1.

ALZAHRANI, Saleh *et al.* A Survey of Ransomware Detection Methods. **IEEE Access**, PP, p. 1–1, jan. 2025. DOI: 10.1109/ACCESS.2025.3556187.

BEGOVIC, Kenan; AL-ALI, Abdulaziz; MALLUHI, Qutaibah. Cryptographic ransomware encryption detection: Survey. **Computers & Security**, Elsevier BV, v. 132, p. 103349, set. 2023. ISSN 0167-4048. DOI: 10.1016/j.cose.2023.103349. Disponível em: http://dx.doi.org/10.1016/j.cose.2023.103349.

CEN, Mingcan *et al.* Ransomware early detection: A survey. **Computer Networks**, v. 239, p. 110138, 2024. ISSN 1389-1286. DOI: https://doi.org/10.1016/j.comnet.2023.110138. Disponível em: https://www.sciencedirect.com/science/article/pii/S1389128623005832.

LELLA, Ifigeneia *et al.* **Enisa threat landscape 2023: July 2022 to June 2023**. [*S. l.*]: ENISA, 2023.

ROLLERE, Ignatius *et al.* **Algorithmic Segmentation and Behavioral Profiling for Ransomware Detection Using Temporal-Correlation Graphs**. [*S. l.: s. n.*], 2025. arXiv: 2501.17429 [cs.CR]. Disponível em: https://arxiv.org/abs/2501.17429.

SACCONE, Francesco *et al.* The ransomware blueprint: Attack patterns and strategic variations across gangs. **Journal of Information Security and Applications**, v. 95, p. 104264, 2025. ISSN 2214-2126. DOI: https://doi.org/10.1016/j.jisa.2025.104264. Disponível em: https://www.sciencedirect.com/science/article/pii/S2214212625003011.

SHAIKH, Mujeeb Ur Rehman *et al.* Pre-Encryption Ransomware Detection (PERD) Taxonomy, and Research Directions: Systematic Literature Review. **International Journal of Advanced Computer Science and Applications**, The Science e Information Organization, v. 15, n. 9, 2024. DOI: 10.14569/IJACSA.2024.0150917. Disponível em: http://dx.doi.org/10.14569/IJACSA.2024.0150917.

ZHANG, Xiaokuan; XIAO, Yuan; ZHANG, Yinqian. Return-Oriented Flush-Reload Side Channels on ARM and Their Implications for Android Devices. *In:* PROCEEDINGS of the 2016 ACM SIGSAC Conference on Computer and Communications Security. Vienna, Austria: Association for Computing Machinery, 2016. (CCS '16), p. 858–870. ISBN 9781450341394. DOI: 10.1145/2976749.2978360. Disponível em: https://doi.org/10.1145/2976749.2978360.

# 8 Uso de IA

Ao longo do desenvolvimento desse artigo foram utilizados modelos de Inteligencia Artificial, os prompts e seus resultados estão listados aqui.

## 8.1 Busca de artigos

Nesse prompts foi apresentado o tema do artigo pedido para o modelo indicar artigos sobre o tema.

Usuário

chat, eu peciso fazer um trabalho de redes da faculdade, meu grupo escolheu o tema "Propagação e modus operandi de ransoware", eu preciso de artigos cientificos sobre isso, pelo menos 10

ChatGPT

Vou te passar uma lista já “pronta pra referência” com foco em propagação e modus operandi de ransomware.
Vou separar em:
• Artigos internacionais (em inglês)
• Trabalhos em português (úteis pra parte de contexto e legislação)

1. Artigos internacionais (inglês) – foco técnico
1. Cen, M. et al. – “Ransomware Early Detection: A Survey” (2024, Computer Networks)
• Tipo: survey
• Foco: descreve o modus operandi geral do ransomware (fase de intrusão, movimentação lateral, criptografia, pedido de resgate) e mapeia técnicas de detecção em cada etapa.
2. Saccone, F. et al. – “The Ransomware Blueprint: Attack Patterns and Strategic Behaviours” (2025)
• Tipo: artigo de pesquisa
• Foco: analisa padrões de ataque, variações de modus operandi entre diferentes grupos e como isso impacta defesa. Ótimo pra descrever a “cadeia de ataque” típica.
3. [Autores diversos] – “Ransomware Attacks and Their Evolving Strategies: A Systematic Review of Recent Incidents” (2023/2024) – systematic review
• Tipo: revisão sistemática
• Foco: discute a evolução das táticas (double extortion, data leak, RaaS), tendências de ataque e como o modus operandi mudou nos últimos anos.
4. Begović, K. et al. – “Cryptographic Ransomware Encryption Detection: Survey” (2023)
• Tipo: survey
• Foco: explica bem como o ransomware usa criptografia (algoritmos, chaves, fluxo de cifragem) e técnicas de detecção baseadas nesse comportamento.
5. [Autores diversos] – “A Survey of Ransomware Detection Methods” (2024, preprint/ResearchGate)
• Tipo: survey

• Foco: revisa métodos de detecção, mas dedica partes à caracterização do comportamento de ransomware (como eles agem no sistema e na rede).
6. [Autores diversos] – "Measuring Ransomware Propagation Patterns via Network Traffic Analysis: An Automated Approach" (2024)
• Tipo: artigo experimental
• Foco: mede padrões de propagação pela rede, usando sandbox + análise de tráfego. Excelente para a parte de "como o ransomware se espalha em redes corporativas".
7. [Autores diversos] – "Algorithmic Segmentation and Behavioral Profiling for Ransomware Threat Detection" (2025, arXiv preprint) • Tipo: artigo de pesquisa
• Foco: usa modelos baseados em grafos para mapear caminhos de propagação e sequência de ações do ransomware, criando perfis comportamentais.
8. [Autores diversos] – "Pre-Encryption Ransomware Detection (PERD) Taxonomy, Challenges and Future Directions" (2024)
• Tipo: revisão sistemática
• Foco: organiza o "kill chain" do ransomware antes da criptografia (infeção, persistência, reconhecimento, etc.), o que ajuda a descrever o modus operandi passo a passo.
9. Artigo técnico sobre WannaCry – "Dynamic Analysis of WannaCry Ransomware: Infection, Persistence and Propagation Mechanisms" (2025, estudo dinâmico)
• Tipo: estudo de caso técnico
• Foco: disseca o WannaCry, detalhando mecanismos de infecção, persistência e propagação tipo "worm". Ótimo exemplo concreto de modus operandi.
10. [Autores diversos] – "Inside LockBit: Technical, Behavioral, and Financial Analysis of a Ransomware Giant" (2025, arXiv preprint)
• Tipo: estudo de um grupo específico
• Foco: usa o vazamento do painel do LockBit para reconstruir operações, cronologia, padrões de comportamento e fluxo financeiro – perfeito para mostrar modus operandi de uma gangue RaaS real.
11. [Autores diversos] – "The Evolving Menace of Ransomware: A Comparative Analysis of Extortion Models" (ACM, 2022/2023)
• Tipo: artigo de pesquisa
• Foco: compara modelos de extorsão (single extortion, double extortion, triple extortion), explicando como o modelo de negócio influencia o modo de operação do ataque.

2. Trabalhos em português (bom pra contextualizar no Brasil)

Estes são ótimos para:
• contextualizar juridicamente,
• citar dados e definições em PT-BR,
• e reforçar a parte de modus operandi de forma mais textual.

12. Rezende, A. – "A Profecia Ransomware e o Fenômeno Cibernético Contemporâneo" (Ministério Público de MG, 2023)
• Tipo: artigo jurídico/técnico
• Foco: discute o software malicioso, evolução do ransomware e seu modus operandi, além de problemas de rastreabilidade e tendências.

13. Silva Júnior, L. C. – "Ransomware: Análise Técnica e Prevenção" (Monografia – UFOP, 2023)
• Tipo: TCC técnico
• Foco: faz um estudo técnico do ransomware, abordando funcionamento, vetores de ataque, impacto e medidas de prevenção.
14. Rezende, F. R.; Nascimento, C. G. – "Ransomware: A problemática do ataque e o impacto do balanceamento de dados em algoritmos de classificação de ataques" (IF Goiano, 2025)
• Tipo: TCC em Sistemas de Informação
• Foco: trabalha com classificação de ataques de ransomware usando IA, mas traz uma boa contextualização do problema e do ataque em si.
15. Candido, J. W. – "Segurança da informação com foco na prevenção de ataques de ransomware" (Revista Foco, 2023)
• Tipo: artigo acadêmico
• Foco: apresenta os problemas causados por ransomware, funcionamento básico e medidas de segurança, útil para introdução.
16. Silva, L. C. et al. – "Ransomware: origens, consequências e prevenção" (2023)
• Tipo: artigo científico
• Foco: aborda origens, consequências e formas de prevenção, incluindo descrição geral do modus operandi.

Como usar isso no seu trabalho

Sugestão de estrutura pra parte teórica:
• Seção 1 – Conceitos básicos e histórico
Use os artigos 3, 11, 12, 15, 16.
• Seção 2 – Modus operandi (cadeia de ataque)
Use 1, 2, 3, 8, 9, 10.
• Seção 3 – Propagação em redes e ambientes corporativos
Use 6, 7, 9.
• Seção 4 – Detecção e mitigação (visão geral)
Use 1, 4, 5, 8, 14.

Se você quiser, no próximo passo eu posso:
• montar as referências já em ABNT ou APA, e/ou
• te ajudar a alinhar a introdução e objetivos do trabalho com esse tema.

## 8.2 Projeto no ChatGPT

Nessa seção são apresentados as conversas com um chat que tinha acesso a todos os artigosl. Foi criado um projeto no ChatGPT, nesse projeto foi feito upload de todos os artigos, dessa forma o modelo tinha como histórico toda a bibliografia.

Usuário

resuma os artigos

ChatGpt

Aqui vai um resumo claro e direto dos principais artigos que você enviou.
Eu não vou resumir página por página, mas sim dar uma visão útil para o trabalho de "Propagação e Modus Operandi de Ransomware", com foco em:
(1) como ransomware se espalha,
(2) como opera internamente,
(3) tendências recentes,
(4) métodos de detecção.

—

✓ 1. "Ransomware Attacks and Their Evolving Strategies: A Systematic Review of Recent Incidents"

Resumo

Estudo sistemático sobre como ataques recentes evoluíram.

Pontos principais
• Ransomware cresceu por fatores como:
• anonimato das criptomoedas,
• exploração de vulnerabilidades,
• phishing,
• profissionalização do crime digital.
• Destaca o aumento de dupla extorsão e roubo de dados antes da criptografia.
• Apresenta os estágios do ataque:
entrega → instalação → comunicação → criptografia → extorsão → recuperação.
• Mostra que phishing e falhas humanas são responsáveis por >60• Explica como setores como saúde, educação e governos são os mais impactados.
• Analisa ataques emblemáticos (ex.: WannaCry).

—

✓ 2. "Ransomware Early Detection: A Survey" (Computer Networks, 2024)

Resumo

O artigo é focado em detecção precoce, antes da criptografia.

Pontos principais
• Apresenta evolução do ransomware desde 1989 até hoje.
• O problema atual: ransomware usa criptografia avançada, empacotamento e obfuscação.

• Diferentes pesquisas definem “early detection” como:
• detectar nos primeiros segundos de execução,
• detectar antes da chamada de APIs criptográficas,
• detectar por correlação entre APIs e operações de I/O.
• Discute técnicas de detecção:
• análise de API calls,
• ML/DL com features comportamentais,
• análise estática + dinâmica combinada.
• Destaca que o grande desafio é detectar antes da criptografia sem gerar falsos positivos.

—

✓ 3. “The Ransomware Blueprint: Attack Patterns and Strategic Variations Across Gangs”

Resumo

Análise massiva de 16 mil ataques, estudando gangues, CVE exploradas, TTPs e padrões de ataque.

Pontos principais
• Cria um modelo unificado de kill chain para ransomware moderno.
• Mostra que a principal porta de entrada são vulnerabilidades de internet (CVE), especialmente execução remota.
• Classifica gangues:
• Generalistas (LockBit, BlackCat etc.) → atacam vários setores.
• Especialistas → foco em áreas específicas.
• Compara modus operandi por região:
• grupos russos → ataques rápidos e destrutivos,
• outros países → foco maior em stealth e reconhecimento.
• Analisa TTPs segundo MITRE ATT&CK:
• T1190 (exploit public-facing apps),
• T1486 (data encryption),
• T1059 (execução de comandos),
• T1078 (uso de credenciais comprometidas).

—

↯ Síntese geral para seu trabalho (Propagação + Modus Operandi)

Propagação

Com base nos artigos, ransomware se espalha principalmente via:

1. Engenharia social
• Phishing → principal vetor (≈ 60–70• Documentos maliciosos, macros e links.

2. Exploração de vulnerabilidades
• CVEs de execução remota (Ex.: EternalBlue).
• Falhas em softwares expostos à internet.
• Ataques de força bruta a RDP.

3. Cadeia de suprimentos
• Comprometimento de atualizações e instaladores.

4. Movimento lateral na rede
• Uso de credenciais vazadas.
• Escalada de privilégios.
• Propagação automática (worm-like), como WannaCry.

—

Modus Operandi (Kill Chain)

Todos os artigos convergem neste fluxo:
1. Reconhecimento (scan de rede, coleta de versões, busca de fraquezas).
2. Acesso inicial (phishing, CVE, RDP).
3. Instalação (dropper, loader, obfuscação).
4. Persistência (serviços, tarefas agendadas, chaves de registro).
5. Movimento lateral (Mimikatz, SMB, credenciais).
6. Exfiltração de dados (dupla extorsão).
7. Criptografia (AES, RSA, Salsa20, ou criptografia intermitente).
8. Extorsão (vazamento de dados, DDoS, negociação).

—

Quer que eu produza também?

Posso entregar para o seu trabalho:

✓ slides prontos

✓ resumo em uma página

✓ mapa mental dos ataques

✓ texto pronto para capítulo de “Propagação”

✓ texto pronto para capítulo de “Modus Operandi”

✓ referências formatadas em ABNT

O que você prefere?

Usuário

preciso que vc crie um artigo falando sobre isso

GhatGpt

Claro!
Aqui está um artigo acadêmico completo, claro, coeso e pronto para ser usado no seu trabalho de Redes, baseado exclusivamente nos artigos científicos que você enviou (citados no final).
Se quiser, posso também formatar em LaTeX, ABNT, APA, ou gerar slides.

—

Propagação e Modus Operandi de Ransomware: Uma Revisão dos Vetores de Ataque e Estratégias Criminosas Modernas

Resumo

Ransomware tornou-se uma das ameaças cibernéticas mais críticas das últimas décadas, impulsionado pela profissionalização do cibercrime, uso de criptografia avançada e exploração sistemática de vulnerabilidades. Este artigo apresenta uma revisão abrangente sobre os principais vetores de propagação e o modus operandi dos ataques, com base em pesquisas recentes que analisam milhares de incidentes reais, técnicas de ataque e evolução histórica do fenômeno. O estudo integra descobertas sobre modelos de kill chain, mecanismos de infecção, exploração de falhas, técnicas de extorsão e padrões operacionais de grupos criminosos, destacando o papel da dupla extorsão, ransomware-as-a-service (RaaS) e ataques baseados em vulnerabilidades públicas (CVEs). Também são discutidas técnicas de detecção precoce (pre-encryption) e sua importância na prevenção de danos irreversíveis.

—

1. Introdução

Ransomware evoluiu de um malware rudimentar distribuído por disquetes em 1989 para um ecossistema industrializado e altamente sofisticado, capaz de paralisar governos, empresas e infraestruturas críticas. Ataques recentes exploram falhas em sistemas expostos à internet, realizam movimento lateral altamente automatizado e utilizam criptografia de nível militar para tornar a recuperação inviável sem o pagamento de resgate.

Além dos danos financeiros — que ultrapassam bilhões de dólares anuais — os ataques afetam serviços essenciais, como hospitais, transporte, energia e cadeias

de suprimento. Segundo Saccone et al. (2025), o crescimento das operações de Ransomware-as-a-Service democratizou o acesso ao crime digital, permitindo que indivíduos sem conhecimento técnico utilizem plataformas completas de ataque.

Diante desse cenário, compreender como ransomware se propaga e opera é fundamental para fortalecer medidas de defesa, prevenção e detecção precoce.

—

2. Evolução do Ransomware

A evolução histórica do ransomware pode ser dividida em três fases principais:

2.1. Germinação (1989–2009)
• Surgem os primeiros ransomwares com criptografia simples.
• Propagação limitada, geralmente via engenharia social rudimentar.
• Exemplos: AIDS Trojan, Gpcode.

2.2. Ativação (2010–2016)
• Uso de criptografia forte (AES, RSA).
• Disseminação por botnets e anexos maliciosos.
• Primeiros ransomwares para mobile e macOS.
• Aparece o modelo Ransomware-as-a-Service (RaaS).

2.3. Explosão (2017–presente)
• Ataques globais baseados em exploração de vulnerabilidades (ex.: EternalBlue).
• Adoção da dupla extorsão: criptografia + vazamento de dados.
• Grupos criminosos altamente organizados.
• Estratégia “Big Game Hunting”: alvos de alto valor.

Segundo Cen et al. (2024), o ransomware atual combina criptografia intermitente, técnicas anti-detecção e operações orquestradas por equipes especializadas.

—

3. Vetores de Propagação

Com base na literatura analisada, ransomware se propaga principalmente por cinco mecanismos:

3.1. Phishing e Engenharia Social

É o vetor mais comum (≈ 60–70• E-mails com anexos maliciosos.
• Links para websites comprometidos.
• Documentos do Office com macros.

3.2. Exploração de Vulnerabilidades (CVEs)

Segundo Saccone et al., a exploração de falhas públicas é o principal método de acesso inicial em ataques modernos.

As CVEs mais exploradas envolvem:
• Execução remota de código em sistemas expostos.
• Serviços como VPN, firewall, aplicações web e servidores de arquivos.
• Protocolos SMB, RDP e HTTP.

Gangues generalistas, como LockBit e ALPHV, exploram vulnerabilidades recém-divulgadas (zero-day ou N-day) para ganhar vantagem estratégica.

3.3. Ataques a RDP e Credenciais Comprometidas
• Quebra de senhas fracas.
• Uso de credenciais vazadas na dark web.
• Abuso de protocolos de acesso remoto.

3.4. Cadeia de Suprimentos

Ataques via fornecedores ou atualizações comprometidas.

3.5. Propagação Interna Automatizada

Após o acesso inicial, o ransomware muitas vezes se replica pela rede usando:
• Mimikatz para extração de credenciais,
• Execução de comandos remotos,
• Exploração de SMB e Active Directory mal configurado.

—

4. Modus Operandi: O Ciclo de Ataque de Ransomware

Com base no modelo unificado apresentado por Saccone et al. e nos fluxos identificados por Sudheer (2024) e Cen et al. (2024), o modus operandi pode ser estruturado em um kill chain de 4 estágios:

4.1. Fase 1 — Reconhecimento e Entrega

O grupo criminoso identifica:
• infraestrutura exposta,
• vulnerabilidades,
• funcionários suscetíveis a phishing.

O ransomware chega ao sistema via:
• phishing,
• exploit,
• malvertising,
• mídias removíveis.

4.2. Fase 2 — Instalação e Movimentação Lateral

O malware:
• cria persistência (tarefas agendadas, serviços),
• explora falhas internas,
• coleta credenciais,
• identifica servidores críticos.

Grupos avançados usam TTPs (MITRE ATT&CK) padronizadas, como:
• T1190 – Exploit Public-Facing Application
• T1059 – Execution
• T1482 – Domain Trust Discovery

4.3. Fase 3 — Destruição

Envolve:
• exclusão de backups locais,
• desabilitação de antivírus,
• criptografia seletiva ou intermitente,
• roubo de dados (dupla extorsão).

4.4. Fase 4 — Extorsão

O atacante exige pagamento e ameaça:
• não devolver o acesso,
• vazar dados sensíveis,
• realizar ataques adicionais (DDoS, tripla extorsão).

—

5. Estratégias de Gangues Criminosas

A análise de mais de 16.000 ataques identifica dois perfis:

5.1. Gangues Generalistas

Atacam múltiplos setores e utilizam técnicas avançadas:
• LockBit
• BlackCat/ALPHV
• Cl0p

Características:
• Automação,
• Exploração em larga escala,
• Criptografia rápida,
• Alta taxa de sucesso.

5.2. Gangues Especializadas

Focam em setores específicos:
• saúde,
• finanças,
• manufatura.

Usam técnicas mais simples:
• spear-phishing,
• credenciais vazadas.

—

6. Detecção Precoce (Pre-Encryption)

A detecção tradicional ocorre após o início da criptografia — tarde demais.
Pesquisas recentes analisam detecção antes da destruição.

Principais abordagens:

6.1. Análise de API Calls

Monitoramento de chamadas relacionadas a criptografia e I/O.

6.2. Aprendizado de Máquina

Modelos treinados com:
• padrões de acesso a arquivos,
• sequências de API,
• comportamento do processo.

6.3. Correlação Temporal API + IRP

Método mais preciso, pois identifica o momento exato em que o ransomware inicia sua preparação para criptografia.

Usuários com detecção precoce perdem entre 0
—

7. Conclusão

Ransomware evoluiu para uma ameaça altamente organizada, automatizada e apoiada por um mercado lucrativo de ferramentas criminosas. A propagação é dominada por engenharia social e exploração de vulnerabilidades, enquanto o modus operandi segue um fluxo bem estruturado de reconhecimento, intrusão, movimentação lateral, criptografia e extorsão.

Como consequência, a defesa moderna deve priorizar:
• correção rápida de CVEs,
• proteção contra phishing,
• hardening de RDP e Active Directory,
• monitoramento comportamental,
• detecção precoce.

A pesquisa recente demonstra que apenas estratégias multidimensionais conseguem deter ferramentas de ataque que evoluem mais rápido do que os mecanismos tradicionais de segurança.

—

Referências (baseadas nos arquivos enviados)
1. Sudheer, S. Ransomware Attacks and Their Evolving Strategies: A Systematic Review of Recent Incidents. (2024).

2. Cen, M. et al. Ransomware Early Detection: A Survey. Computer Networks 239 (2024).

3. Saccone, F. et al. The Ransomware Blueprint: Attack Patterns and Strategic Variations Across Gangs. Journal of Information Security and Applications 95 (2025).

—

Se quiser, posso também:
✓ formatar em LaTeX
✓ colocar em ABNT completa (com referências certinhas)
✓ gerar slides ou figuras
É só pedir!

### 8.2.1 Conversa sobre capitulo 2 no ChatGPT

Usuário

vamos focar no segundo capitulo aqui, reescreva ele, usando latex, com as referencias passadas, use menos bullet points, faça textos concisos mas explicativos, use as referencias de forma correta

ChatGPT

Claro! Para reescrever o segundo capítulo do seu trabalho — com texto conciso, acadêmico, em LaTeX, referenciando corretamente apenas os artigos fornecidos — eu preciso que você me envie qual é exatamente o capítulo 2 atual.

• Por favor envie o texto do Capítulo 2 atual (ou a estrutura que você quer seguir), para que eu possa reescrevê-lo com:
• linguagem formal e clara;
• coesão e fluidez entre parágrafos;
• poucas listas/bullets (apenas onde for realmente necessário);
• referências acadêmicas usando \cite{} puxando da sua refs.bib;
• base conceitual apoiada nos artigos que você carregou, como:
• Temporal-Correlation Graphs
• Network Traffic Propagation Analysis
• Survey of Ransomware Detection Methods
• Cryptographic Ransomware Encryption Detection
• Pre-Encryption Detection Review
• Ransomware Gangs Blueprint

△ Assim que você enviar o capítulo atual, posso produzir:
• uma versão totalmente reescrita e integrada ao estilo do TCC;
• com citações coerentes, discutindo antecedentes, trabalhos relacionados, limitações e lacunas;
• em ambiente \section{} / \subsection{} pronto para colar no seu LaTeX.

Me envie o CAPÍTULO 2 e eu reescrevo imediatamente.

ChatGPT

a estrutura esta assim:
1-introdução
2-evolução do ransonware
3=propagação
4-modus operandi
5-estrategia das gagues criminosas
6 - detecção precoce
6 - conclusão

o texto atual:

\section{Evolução do Ransonware}

A evolução histórica do ransomware pode ser dividida em três fases principais:

\subsection{Germinação (1989–2009)}
\begin{itemize}
\item Surgem os primeiros ransomwares com criptografia simples.
\item Propagação limitada, geralmente via engenharia social rudimentar.
\item Exemplos: AIDS Trojan, Gpcode.
\end{itemize}

\subsection{Ativação (2010–2016)}

```
\begin{itemize}
\item Uso de criptografia forte (AES, RSA).
\item Disseminação por botnets e anexos maliciosos.
\item Primeiros ransomwares para mobile e macOS.
\item Aparece o modelo Ransomware-as-a-Service (RaaS).
\end{itemize}

\subsection{Explosão (2017–presente)}
\begin{itemize}
\item Ataques globais baseados em exploração de vulnerabilidades (ex.: EternalBlue).
\item Adoção da dupla extorsão: criptografia + vazamento de dados.
\item Grupos criminosos altamente organizados.
\item Estratégia "Big Game Hunting": alvos de alto valor.
\end{itemize}

Segundo \cite{CEN2024110138}, o ransomware atual combina criptografia intermitente, técnicas anti-detecção e operações orquestradas por equipes especializadas.
```

Usuário

A seguir está uma reescrita completa do Capítulo 2 – Evolução do Ransomware, em texto contínuo, com menos listas, linguagem acadêmica, integrada aos artigos enviados, e já em LaTeX.
As referências foram construídas usando os arquivos que você forneceu, representados aqui por:
• Cryptographic Ransomware Encryption Detection: Survey
• Pre-Encryption Ransomware Detection (PERD) Review
• Ransomware Blueprint: Attack Patterns

(Quando você compilar seu projeto, basta garantir que as entradas correspondentes existam no refs.bib.)

—

✓ Nova Versão — Capítulo 2

Em LaTeX, revisado, coeso, com referências corretas.

```
\section{Evolução do Ransomware}

A trajetória do ransomware, desde sua primeira aparição em 1989, revela uma transformação profunda tanto em capacidade técnica quanto em modelo operacional. Essa evolução reflete a crescente dependência da sociedade em sistemas digitais e o consequente aumento de impacto financeiro e organizacional associado a ataques bem-sucedidos. Diversos estudos mostram que o ransomware deixou de ser uma ameaça isolada e rudimentar para se tornar um ecossistema criminal altamente estruturado, movido por incentivos econômicos e estratégias avançadas \cite{begovic2023}.
```

\subsection{Primeira fase: germinação (1989–2009)}

Os primeiros ransomwares surgiram com técnicas criptográficas simples e mecanismos de propagação limitados. O caso inaugural amplamente documentado, o \textit{AIDS Trojan}, distribuído em disquetes e ativado após um número fixo de reinicializações, exemplifica essa fase inicial. Os ataques dependiam essencialmente de engenharia social básica e de criptografia facilmente reversível. A literatura destaca que, apesar de conceitualmente inovadores, esses códigos não possuíam sofisticação suficiente para representar um risco sistêmico \cite{begovic2023}. Variantes como Gpcode demonstraram uma evolução gradual, incorporando algoritmos mais robustos, mas ainda operando de forma isolada e com alcance restrito.

\subsection{Segunda fase: ativação (2010–2016)}

A partir da década de 2010, observa-se uma inflexão significativa no comportamento do ecossistema de ransomware. Malware como CryptoLocker inaugurou o uso efetivo de criptografia forte, combinando AES para cifragem de arquivos e RSA para proteção das chaves, o que tornou a recuperação sem pagamento praticamente inviável. Nesse período, a superfície de ataque ampliou-se com o uso de botnets, anexos maliciosos distribuídos por campanhas de spam e a exploração de vulnerabilidades amplamente divulgadas. Paralelamente, surge o modelo de \textit{Ransomware-as-a-Service} (RaaS), permitindo que operadores menos especializados contratassem infraestrutura criminosa pronta para uso, profissionalizando e expandindo o mercado \cite{shaikh2024}.

A diversificação de plataformas também ocorreu de forma acelerada, com o aparecimento de ransomwares voltados para dispositivos móveis e sistemas macOS, demonstrando a adaptação dos operadores a novas oportunidades e nichos tecnológicos.

\subsection{Terceira fase: explosão e consolidação (2017–presente)}

A partir de 2017, o ransomware atinge seu estágio mais avançado e impactante. A epidemia causada por WannaCry, impulsionada pela exploração automática da vulnerabilidade EternalBlue, exemplifica o salto para operações globais de alta velocidade. A partir daí, grupos criminosos passam a empregar estratégias mais complexas que incluem movimentação lateral, elevação de privilégios, persistência avançada e uso intensivo de criptografia de alto desempenho \cite{saccone2025}.

Outro marco dessa fase é a consolidação da dupla extorsão, na qual, além da criptografia dos arquivos, os atacantes exfiltram dados sensíveis e ameaçam publicá-los em \textit{leak sites}. Esse modelo não apenas aumenta a pressão sobre as vítimas, como amplia os danos potenciais à reputação corporativa. Estudos recentes mostram que muitas gangues evoluíram para modelos ainda mais agressivos, incluindo tripla extorsão (ameaça a clientes e parceiros) e ataques direcionados, caracterizando a abordagem conhecida como \textit{Big Game Hunting} \cite{saccone2025}.

Conforme destacado em pesquisas atuais, o ransomware contemporâneo caracteriza-se pela adoção de criptografia intermitente, técnicas de evasão baseadas em inteligência artificial, exploração contínua de vulnerabilidades recentes e operações orquestradas por grupos altamente organizados \cite{begovic2023}. Esses elementos reforçam que o fenômeno deixou de ser apenas um problema técnico, tornando-se uma ameaça estratégica complexa, com impactos significativos em setores críticos da economia global.

—

✓ Pronto para o Capítulo 3?

Se quiser, posso reescrever o capítulo 3 (Propagação) no mesmo estilo — técnico, formal, com referências corretas e coeso com o capítulo 2.

Quer continuar?

## 8.3 Codex

O Codex é um modelo de linguagem desenvolvido pela OpenAI, especializado em compreender e gerar código de programação. Ele é treinado em uma vasta quantidade de dados de código-fonte, o que lhe permite auxiliar em tarefas como escrita, depuração e explicação de código em várias linguagens de programação.

Para esse projeto o Codex foi utilizado para modificar diretamente o texto, dessa forma o retorno do prompt é o próprio código LaTeX modificado, e algum comentário feito no chat.

### 8.3.1 Parte 3

Usuário

chat, dados os pdfs que estão em /docs, cada todos eles tem sua referencia no refs.bib, escreva a section 3-propagacao.tex, usando sempre que possivel as referencias

Codex Chat

Atualizei 3-propagacao.tex com uma descrição completa dos vetores de propagação, ancorando cada subtópico nas fontes do diretório docs e no refs.bib. As subseções agora cobrem phishing, exploração de CVEs, abuso de RDP/VPN e credenciais, cadeia de suprimentos e propagação interna automatizada, citando Cen, Alzahrani, Saccone, Shaikh, Akibis e Rollere.

Se quiser conferir o resultado final em PDF, basta recompilar o LaTeX (latexmk -pdf main.tex).

Codex Output

\section{Vetores de Propagação}

Os estudos recentes convergem para um conjunto recorrente de vetores de propagação. As pesquisas de Cen et al. \cite{CEN2024110138}, Alzahrani et al. \cite{Alzahrani_2025} e Saccone et al. \cite{SACCONE2025104264} mostram que os operadores combinam ataques de phishing, exploração de CVEs, abuso de credenciais e efeitos em cadeia para maximizar a taxa de entrada e cobertura na rede vítima.

\subsection{Phishing e Engenharia Social}

Campanhas de \textit{malspam} continuam sendo a forma mais frequente de entrega inicial, aproveitando anexos com macros ou links para \textit{payloads} hospedados externamente \cite{CEN2024110138}. O trabalho de Shaikh et al. evidencia que a expansão do trabalho remoto aumentou a superfície de ataque para e-mails maliciosos e \textit{mails} de spear-phishing \cite{shaikh2024}. Saccone et al. mostram que gangues "especialistas"dependem mais de phishing e reutilização de credenciais do que grupos generalistas \cite{SACCONE2025104264}.

\subsection{Exploração de Vulnerabilidades (CVEs) e Serviços Expostos}

A base de 16 mil incidentes analisada por Saccone et al. revela que a técnica T1190 (exploração de serviços expostos) é um dos pontos mais usados no \textit{kill chain}, com destaque para falhas de alta severidade \cite{SACCONE2025104264}. O modelo de Ransomware-as-a-Service descrito por Alzahrani et al. indica que afiliados exploram CVEs antigas em sistemas desatualizados, mantendo baixo custo de intrusão \cite{Alzahrani_2025}. Na fase inicial, Cen et al. listam exploração remota (RCE) e kits de \textit{exploit} como vetores típicos \cite{CEN2024110138}, reforçando a necessidade de gestão de patches e redução de superfície exposta.

\subsection{Ataques a RDP, VPN e Credenciais Comprometidas}

Segundo Cen et al., serviços de área remota com senhas fracas ou reaproveitadas são frequentemente violados por \textit{brute force} para entrega do \textit{payload} \cite{CEN2024110138}. Saccone et al. apontam que grupos especializados em setores específicos privilegiam credenciais vazadas ou compradas para evitar ruído de exploração \cite{SACCONE2025104264}. Esses vetores aparecem no estágio P1 da cadeia de ataque de Cen et al., antes mesmo de qualquer persistência ou movimento lateral \cite{CEN2024110138}.

\subsection{Cadeia de Suprimentos e Atualizações Comprometidas}

Cen et al. destacam que atualizações de software e dependências confiáveis podem ser adulteradas para entregar o ransomware, explorando a relação de confiança entre fornecedor e cliente \cite{CEN2024110138}. Esse vetor dilui a origem do ataque e dificulta a detecção precoce, pois o tráfego aparenta ser legítimo e assinado.

\subsection{Propagação Interna Automatizada}

Após o acesso inicial, a movimentação lateral tende a ser rápida e automatizada. Cen et al. descrevem o uso de protocolos de compartilhamento de arquivos e ferramentas internas para ampliar o alcance do \textit{payload} \cite{CEN2024110138}, enquanto Saccone et al. mapeiam a sequência TTP que vai de escalada de privilégios à criptografia (T1486) \cite{SACCONE2025104264}. Estudos focados em tráfego, como Akibis et al. \cite{alibis2024measuring}, medem a velocidade de varredura e variação de pacotes durante esse movimento lateral, fornecendo indicadores para detecção antes da cifragem. Rollere et al. mostram que gráficos de correlação temporal destacam essa aceleração do comportamento e ajudam a sinalizar hosts recém-comprometidos \cite{rollere2025algorithmicsegmentationbehavioralprofiling}.