

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 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-detectação 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 ($\approx 60\text{--}70\%$ dos ataques).

- 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:

- Vulnerabilidades em serviços de rede expostos.
- Falhas em softwares amplamente usados.
- Protocolos de comunicação inseguros.

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.

Referências

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>.

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>.

4 Uso de IA

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

4.1 Busca de artigos

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

Usuário

chat, eu preciso fazer um trabalho de redes da faculdade, meu grupo escolheu o tema "Propagação e modus operandi de ransomware", eu preciso de artigos científicos 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: dissecava 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.

4.2 Projeto no ChatGPT

Nessa seção são apresentados as conversas com um chat que tinha acesso a todos os artigos. 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:
 - animação 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% dos ataques.
 - 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 obfuscção.
 - 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 ($\approx 60\text{--}70\%$) 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, obfuscation).
 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-detectão 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 ($\approx 60\text{--}70\%$) 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 — Destruuição

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!