vivo empresas

Ransomware em 2025

Como a IA redefine o ciclo de ataque e extorsão – e como **você** pode se defender

O ransomware emergiu no início dos anos 2000 como trojans de criptografia simples, mas seu impacto explodiu globalmente em maio de 2017 com o ataque WannaCry, que contaminou mais de 200.000 sistemas em 150 países – inclusive o Brasil – em apenas 72 horas. Desde então, evoluiu de simples bloqueio de arquivos para esquemas de dupla e até tripla extorsão, combinando criptografia e vazamento de dados, e hoje representa uma das principais preocupações em cibersegurança para organizações de todos os portes.

também conhecidos como cavalo de Troia, é um software malicioso que se disfarça como programas comuns para enganar os usuários e obter acesso aos seus sistemas

Em 2025, o ransomware atingiu patamares sem precedentes: o custo global projetado para o ano é de US$57 bilhões (US$4,8 bilhões/mês; US$156 milhões/dia).

Apenas no início de 2025...

Surto de ameaças (Q12025): Ataques cibernéticos cresceram 47% por organização, somando 1.925 ataques semanais em média.

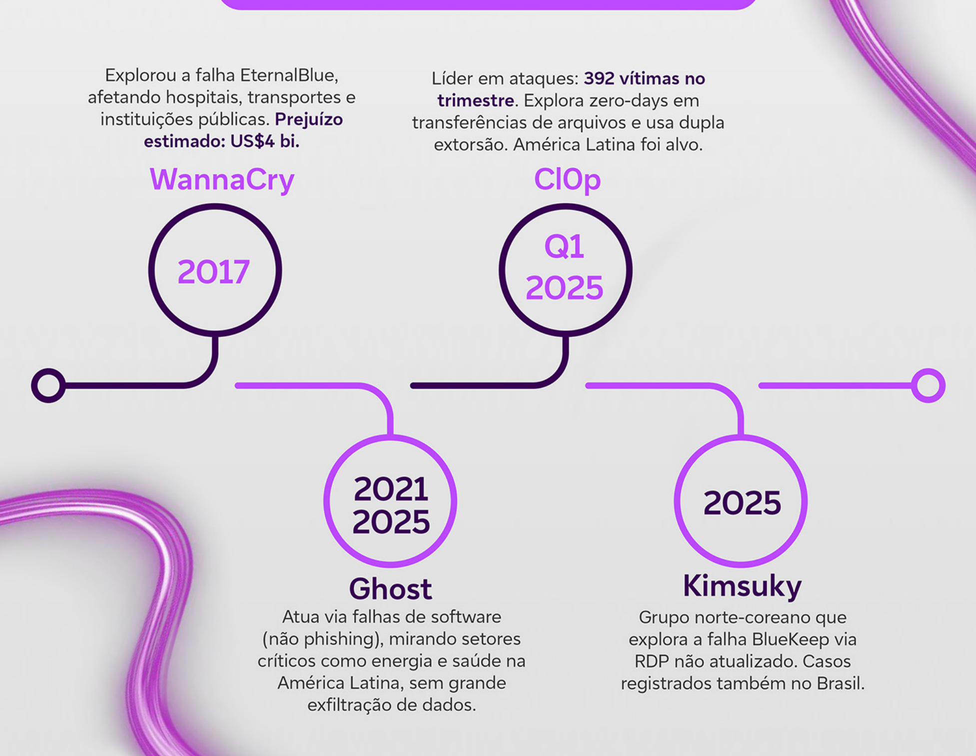
Ransomware em Alta: Crescimento de 126% no número de vítimas extorquidas, batendo recorde histórico. A América Latina responde por 6% dos casos.

Setores mais afetados: Educação lidera com 4.484 ataques semanais, seguida por Governo, com 2.678 ataques.

Impacto Regional: A América Latina teve o maior crescimento ano a ano, com média de 2.640 ataques semanais por organização.

Exploração Zero-Days: Cl0p explorou falhas em softwares de transferência, gerando 83% das vítimas na América do Norte. América Latina responde por 8% do total.

Evolução do Ransomware



2017 – WannaCry
Explorou a falha EternalBlue, afetando hospitais, transportes e instituições públicas. **Prejuízo estimado: US$4 bi.**

2021 2025 – Ghost
Atua via falhas de software (não phishing), mirando setores críticos como energia e saúde na América Latina, sem grande exfiltração de dados.

Q1 2025 – Cl0p
Líder em ataques: **392 vítimas no trimestre**. Explora zero-days em transferências de arquivos e usa dupla extorsão. América Latina foi alvo.

2025 – Kimsuky
Grupo norte-coreano que explora a falha BlueKeep via RDP não atualizado. Casos registrados também no Brasil.

Anatomia de um ataque de Ransomware

1. **Campanha de distribuição:** os criminosos usam técnicas de engenharia social, phishing, exploits e vetores iniciais para instalar o ransomware;
2. **Infecção Inicial:** o malware estabelece um ponto de entrada na rede da vítima, instalando um executável malicioso;
3. **Fase de teste:** o ransomware verifica sua capacidade de funcionamento mapeando permissões e configurações da rede/sistemas;
4. **Escaneamento:** o malware espalha a infecção lateralmente, mapeando compartilhamentos de arquivos e sistemas a serem criptografados;
5. **Criptografia:** os dados previamente escaneados são criptografados com uma chave pública pelo ransomware;
6. **Exigência de resgate:** uma nota de resgate é exibida, demandando o pagamento em criptomoedas pela chave de descriptografia.

Exemplos por Porte/Setor:

Grande Empresa (Saúde): Perda de prontuários e dados críticos; resgate de **US$100 milhões;**

PME (Logística): Paralisia de cadeia de suprimentos, custo médio de **US$2,3 milhões por incidente;**

Administração Pública: Sistemas judiciais fora do ar por 5 dias, **com prejuízos diretos de €4 milhões.**

No Brasil...

Grande Empresa (Automotivo): uma das maiores concessionárias do país teve dados e contratos de clientes roubados. Criminosos exigiram **US$ 1 milhão para não divulgar as informações.**

PME (Logística): a Braspress, referência em encomendas, teve **280 servidores criptografados**, paralisando a operação de entregas por dias

Administração Pública: Em Silveiras (SP), hackers levaram **R$500 mil** dos cofres municipais após invadirem o sistema tributário.

Brechas exploradas e o fator humano

Apesar de ferramentas robustas, o usuário continua sendo o **elo mais vulnerável.**

A engenharia social, potencializada por IA, faz surgir um e-mail malicioso a cada 42 segundos, com 70% de crescimento anual em campanhas de phishing assistidas por IA.

Além disso:

- **Acesso remoto sem múltiplo fator de autenticação (MFA):** em **47% dos ataques**, credenciais roubadas de portais de acesso remoto foram o ponto de partida.
- **Exploração de controladores de domínio ("Domain Controller"): mais de 78% dos ataques humanos** operados comprometem um controlador de domínio antes da criptografia.
- **Deepfakes & Spear-Phishing:** e-mails com áudio e vídeo gerados por IA **crescem 967% desde Q2 2022**, e CISOs apontam spear-phishing assistido por IA e deep-fakes como duas das maiores ameaças. Além disso, **54% das empresas** identificam falhas de gestão de vulnerabilidades (mapeamento e patching) como ponto fraco, permitindo que exploits conhecidos, muitas vezes não corrigidos, sejam vetor de entrada para ransomware.

Sistemas vulneráveis

- **Vulnerabilidades Ativas:** 159 CVEs foram exploradas no wild em Q12025, **sendo 28,3% exploradas em até 24 horas após a divulgação.**
- **Falhas Reportadas:** Mais de **45.000 CVEs** previstas para 2025, um **aumento de 15%** nos primeiros 10 meses de 2024.
- **Painéis de Gestão Expostos:** Acesso administrativo remoto sem segmentação adequada **aumenta em 35%** o risco de escalada de privilégios.

Se o ataque ocorrer...

Estatísticas de resposta mostram que, sem MDR, o MTTD (Mean Time to Detect) pode chegar a 21 dias, dando ao atacante tempo suficiente para criptografar, exfiltrar e preparar saídas. Ferramentas avançadas com:

- **Análise Comportamental por IA:** Detectam padrões anômalos antes da criptografia.
- **Detecção de Artefatos IA-Gerados:** Identificam documentos e e-mails maliciosos criados para enganar.
- **Playbooks Automatizados:** Isolam sistemas comprometidos em segundos, reduzindo o impacto.

Frequência: Um ataque de ransomware ocorre a cada 2 segundos em 2024.

Pagamento Médio de Resgate: US$ 5,2 milhões, em 2024.

Soluções disponíveis no mercado

Com a escalada dos ataques de ransomware – agora potencializados por Inteligência Artificial – as ferramentas tradicionais de cibersegurança já não oferecem respostas suficientes. O cenário atual exige **monitoramento contínuo, resposta rápida e análise de comportamento baseada em IA.**

Antivírus baseados em assinatura são reativos e ineficazes contra ameaças emergentes e variantes IA-assistidas.

Soluções EDR (Endpoint Detection and Response) oferecem visibilidade limitada e exigem equipes internas altamente qualificadas para interpretação e reação.

Firewalls e proxies são essenciais, mas insuficientes frente a ataques que utilizam técnicas evasivas e engenharia social avançada.

Em contrapartida ao crescimento das ameaças, o mercado de MDR alcançou US$4,1 bilhões em 2024 e projeta US$11,8 bilhões até 2029, com CAGR de 23,5%, reposicionando o MDR como defesa estratégica baseada em inteligência

MDR: muito além da detecção

Em um cenário onde os ciberataques evoluem em escala e sofisticação, o MDR da Telefónica Tech se destaca como uma solução completa, robusta, modular e orientada por inteligência artificial, com diferenciais reais frente às alternativas do mercado.

IA preditiva e análise comportamental:
identifica ameaças antes mesmo que causem danos, mesmo sem assinatura conhecida.

Integração com uma plataforma líder em cibersegurança:
acesso a uma base global de threat intelligence constantemente atualizada, com insights acionáveis **para antecipar riscos.**

Monitoramento 24x7 com SOC especializado:
resposta em tempo real por analistas dedicados.

Flexibilidade e integração modular:
compatível com ambientes híbridos, cloud e on-premise.

Relatórios executivos e visão estratégica:
entregas personalizadas para decisões de negócio mais seguras.

Foco na reputação da marca:
proteção que vai além da tecnologia e atua diretamente na preservação da confiança.

A Vivo Empresas e a Telefónica Tech, nossa Unidade de Negócios de Segurança, oferecem soluções customizáveis para as necessidades de sua empresa, através de profissionais capacitados, processos e plataformas inteligentes e parcerias com fabricantes líderes de mercado.

vivo empresas

Para mais informações, fale com nossos especialistas

Fontes Consultadas

Blog CheckPoint Research - https://blog.checkpoint.com/research/the-state-of-ransomware--in-the-first-quarter-of-2025-a-126-increase-in-ransomware-yoy/
Blog CheckPoint Research - https://blog.checkpoint.com/research/q1-2025-global-cyber-attack-report-from-check-point-software-an-almost-50-surge-in-cyber-threats-worldwide-with-a-rise-of-126-in-ransomware-attacks/
Business Insider - https://www.businessinsider.com/ghost-cyberattacks-ransomware--what-you-need-to-know-2025-2
Check Point - https://www.checkpoint.com/cyber-hub/threat-prevention/what-is-phishing/
Comparitech - https://www.comparitech.com/news/ransomware-roundup-h1-2024-stats-on-attacks-ransoms-and-active-gangs/
Cybersecurity Ventures - https://cybersecurityventures.com/ransomware-damage-to-cost-the-world-57b-in-2025/
Cybersecurity Ventures - https://cybersecurityventures.com/cyberwarfare-report-intrusion/
Get Astra - https://www.getastra.com/blog/security-audit/cyber-crime-statistics/
Halcyon AI - https://www.halcyon.ai/blog/rdp-and-vpn-remain-top-ransomware-attack-pathways
Investopedia - https://www.investopedia.com/these-are-cyber-chiefs-biggest-fears-about-ai-8717374
Microsoft Security Blog - https://www.microsoft.com/en-us/security/blog/2025/04/09/how--cyberattackers-exploit-domain-controllers-using-ransomware/
PurpleSec - https://purplesec.us/resources/cybersecurity-statistics/
Securelist - https://securelist.com/state-of-ransomware-in-2025/116475/
The Hacker News - https://thehackernews.com/2025/04/159-cves-exploited-in-q1-2025-283.html
The Hacker News - https://thehackernews.com/2025/04/kimsuky-exploits-bluekeep-rdp.html
VulnCheck - https://vulncheck.com/blog/exploitation-trends-q1-2025

Telefónica