SOPHOS

O ESTADO DO RANSOMWARE NO BRASIL 2025

Resultados de uma pesquisa realizada por terceiros, e desvinculada de fornecedores, com 110 organizações no Brasil que foram atingidas por ransomware no último ano.

DOCUMENTO TÉCNICO SOPHOS – JUNHO DE 2025

Sobre o relatório

O relatório se baseia em levantamentos feitos por uma pesquisa independente e totalmente desvinculada com 3.400 líderes ativos de segurança cibernética e TI de organizações que foram atingidas por ransomware no último ano, incluindo 110 do Brasil.

A pesquisa foi encomendada pela Sophos e realizada entre janeiro e março de 2025 por uma empresa especializada independente.

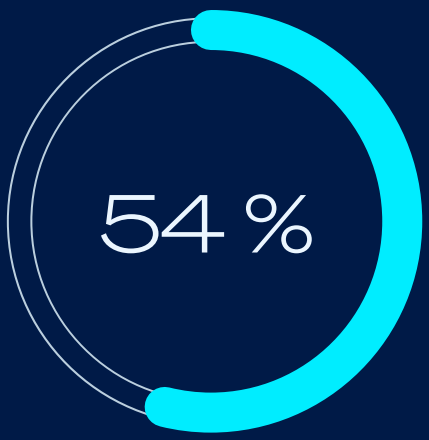
Todos os entrevistados trabalham em organizações com entre 100 e 5.000 funcionários e foram solicitados a responder com base na experiência que tiveram nos 12 meses anteriores.

O relatório inclui comparações com os resultados da pesquisa de 2024. Todos os dados financeiros são expressos em dólares americanos.

Pesquisa com

110

líderes ativos de segurança cibernética e TI de organizações no Brasil que foram atingidas por ransomware no último ano



Porcentagem de ataques que resultaram em dados criptografados.

Mediana de pagamento de resgate no Brasil no último ano.

Custo médio para recuperar-se de um ataque de ransomware.

Por que as organizações brasileiras se tornam vítimas de ransomware

- **A exploração de vulnerabilidades foi a causa técnica primária mais comum,** usada em 44% dos ataques, seguida por credenciais comprometidas, que foram o ponto de partida de 20% dos ataques. E-mails maliciosos foram usados em 18% dos ataques.
- **Uma lacuna de segurança conhecida foi a causa operacional primária mais comum,** citada por 47% dos entrevistados brasileiros, seguida pela falta de pessoas/capacidade, conforme relatado por 39% das organizações. 35% disseram que um erro/falha de suas equipes ao seguir os processos de forma adequada foi um fator determinante para que suas organizações fossem vítimas de ransomware.

O que acontece aos dados

- **54% dos ataques resultaram em dados criptografados.** Esse valor está acima da média global de 50%, porém uma queda significativa dos 77% relatados pelos entrevistados brasileiros em 2024.
- **Os dados também foram roubados em 22% dos ataques em que os dados foram criptografados,** uma queda dos 26% relatados no último ano.
- **Todas as organizações brasileiras que tiverem seus dados criptografados conseguiram reavê-los,** acima da média global.
- **66% das organizações brasileiras pagaram o resgate e conseguiram reaver os dados,** uma leve queda dos 67% relatados no último ano.
- **73% das organizações brasileiras usaram backups para recuperar os dados criptografados,** uma queda notável dos 81% registrados no último ano.

Resgates: exigências e pagamentos

- A **exigência mediana de resgate no Brasil** no último ano foi de US$ 392.500, uma queda de 53% dos US$ 840.000 registrados em nossa pesquisa de 2024.

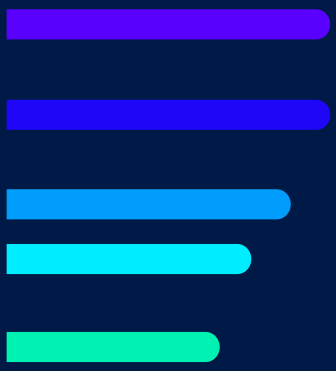
Mediana de exigência de resgate no Brasil no último ano.

- 40% dos **pedidos de resgate foram de US$ 1 milhão ou mais,** acima do dobro dos 16% registrados em 2024.
- O **pagamento mediano de resgate no Brasil** no último ano foi de US$ 400.000, uma queda de 52% dos US$ 840.000 registrados no ano anterior.
- **Em geral, as organizações brasileiras pagaram** 86% das exigências de resgate, alinhada com a média global de 85%.
  - 55% **pagaram MENOS DO QUE o pedido de resgate inicial** (média global: 53%).
  - 11% **pagaram O MESMO QUE o pedido de resgate inicial** (média global: 29%).
  - 34% **pagaram MAIS DO QUE o pedido de resgate inicial** (média global: 18%).

Impacto comercial do ransomware

- Excluindo os pagamentos de resgate, a **conta média incorrida pelas organizações brasileiras para recuperar-se de um ataque de ransomware no último ano foi de US$ 1,19 milhão,** uma queda dos US$ 2,73 milhões reportados pelos entrevistados brasileiros em 2024. Isso inclui custos do período de inatividade, tempo de pessoal, custo dos equipamentos, custo da rede, perda de oportunidades etc.
- **As organizações brasileiras estão ficando mais rápidas no processo de recuperação de um ataque de ransomware,** com 55% delas se recuperando em até uma semana — um aumento significativo dos 28% registrados no último ano. 20% levaram entre um e seis meses para recuperar-se — uma queda notável dos 38% do último ano.

Impacto humano do ransomware nas equipes de segurança cibernética e TI cujas organizações tiverem seus dados criptografados



41% relataram **sentimento de culpa** porque o ataque não foi interrompido.

41% observaram **pedido de licença de pessoal** devido a problemas de estresse/saúde mental.

36% relataram **aumento da pressão** pelos líderes seniores.

31% relataram **aumento em ansiedade e estresse** sobre ataques futuros.

27% disseram que, desde o ataque, houve um **aumento da carga de trabalho** para a equipe.

Recomendações

O ransomware continua a ser uma das principais ameaças às organizações brasileiras. Os adversários continuam a repetir e incrementar os seus ataques, sendo essencial que as equipes e suas defesas cibernéticas acompanhem essa evolução. As lições tiradas deste relatório indicam as áreas-chave de enfoque para 2025 e além.

- **Prevenção.** O melhor ataque de ransomware é aquele que não aconteceu poque os adversários não conseguiram invadir a sua organização. Procure reduzir as causas técnicas primárias do ataque e também as operacionais levantadas neste relatório.
- **Proteção.** Uma segurança básica forte é essencial. Endpoints (incluindo servidores) são o destino principal dos agentes de ransomware, portanto, assegure que apresentem uma boa defesa, incluindo proteção dedicada contra ransomware para interromper e reverter a criptografia maliciosa.
- **Detecção e resposta.** Quanto mais cedo um ataque for interrompido, melhor o resultado final. A detecção e resposta a ameaças 24 horas passou a ser um componente essencial da defesa. Se você não tem pessoal interno ou competências para isso, trabalhe com um provedor de MDR confiável para a detecção e resposta gerenciadas.
- **Planejamento e preparação.** Ter um plano de resposta a incidentes implementado e que você conheça muito bem vai melhorar imensamente os resultados caso o pior aconteça e você enfrente um ataque grave. Certifique-se de fazer bons backups e de praticar a sua restauração com regularidade.

SOPHOS

Para explorar as formas como a Sophos pode ajudar você a otimizar suas defesas contra ransomware, fale com um consultor ou acesse **sophos.com/ransomware2025**

A Sophos oferece soluções de segurança cibernética líder do setor para empresas de todos os tamanhos, protegendo-as em tempo real de ameaças avançadas como malware, ransomware e phishing. Com recursos comprovados de última geração, seus dados comerciais ficam protegidos de modo eficiente por produtos que incorporam inteligência artificial e machine learning.

2025-07-11 PTBR-WP (DD)