SOPHOS

O ESTADO DO RANSOMWARE 2025

Resultados de uma pesquisa independente com 3.400 líderes de TI e segurança cibernética distribuídos em 17 países e cujas organizações foram atingidas por ransomware no último ano.

Documento técnico Sophos. Junho de 2025

Introdução

Bem-vindos à sexta edição do relatório anual da Sophos, O Estado do Ransomware, que expõe a realidade dos ransomwares em 2025.

O relatório deste ano detalha como as experiências com ransomware dasorganizações, tanto causa como consequência, evoluíram nos últimos 12 meses. Também elucida áreas previamente inexploradas, incluindo fatores operacionais que deixaram as organizações expostas aos ataques e o impacto humano dos incidentes nas equipes de TI e segurança cibernética.

Baseado em experiências reais de 3.400 líderes de TI e segurança cibernética distribuídos em 17 países e cujas organizações foram atingidas por ransomware no último ano, o relatório oferece insights únicos sobre:

- Por que as organizações se tornam vítimas de ransomware.
- O que acontece aos dados.
- Resgates: exigências e pagamentos.
- Impacto comercial do ransomware.
- Impacto humano do ransomware.

Observação sobre a data dos relatórios

Para facilitar a comparação de dados entre nossas pesquisas anuais, acrescentamos o ano em que a pesquisa foi realizada ao nome do relatório. Neste caso, 2025. Estamos cientes de que os entrevistados compartilharam conosco suas experiências relativas ao ano anterior, portanto, muitos dos ataques citados ocorreram em 2024.

Sobre a pesquisa

O relatório é embasado nas descobertas reveladas por uma pesquisa realizada por terceiros, e independentemente de fornecedores, sobre as experiências organizacionais com ransomwares. A pesquisa é encomendada pela Sophos e realizada por especialistas terceirizados entre janeiro e março de 2025. 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.

Os participantes estavam localizados em 17 países diferentes e são provenientes de uma ampla gama de setores, assegurando que os resultados da pesquisa reflitam a diversidade das experiências vividas pelos setores público e privado. O relatório inclui comparações ano a ano com os resultados de nossos relatórios anteriores. Todos os dados financeiros são expressos em dólares americanos.

Principais descobertas

Por que as organizações se tornam vítimas de ransomware

- Pelo terceiro ano consecutivo, as vítimas apontaram a **exploração de vulnerabilidades** como a causa técnica primária mais comum dos ataques, usada em 32% dos incidentes.
- Fatores multioperacionais contribuem para que as organizações sejam vítimas de ransomware, sendo o mais comum a **falta de expertise**, citada por 40,2% das vítimas, seguido bem de perto por **lacunas de segurança das quais a organização não tinha conhecimento**, o fator que contribuiu para 40,1% dos ataques. Em terceiro lugar ficou a **falta de pessoas/capacidade**, que contribuiu para 39,4% dos ataques.

O que acontece aos dados

- A **criptografia de dados** atingiu o seu nível mais baixo em seis anos, com 50% dos ataques resultando na criptografia do dados, valor inferior aos 70% em 2024.
- 28% das organizações que tiverem dados criptografados também passaram pela **exfiltração de dados**.
- 97% das que tiverem os dados criptografados conseguiram recuperá-los.
- O uso de **backups** para restaurar dados criptografados atingiu o seu nível mais baixo dos últimos seis anos: apenas 54% dos incidentes utilizaram backups.
- 49% das vítimas **pagaram o resgate** para reaver os dados. Ainda que represente uma leve queda dos 56% do ano anterior, foi o segundo índice de pagamento de resgate mais alto em seis anos.

Resgates: exigências e pagamentos

- A média (mediana) do **pedido de resgate** caiu um terço (34%) durante o último ano, chegando a US$ 1.324.439,00 em 2025 em comparação a US$ 2 milhões em 2024.
- A média (mediana) do **pagamento de resgate** caiu em 50% durante o último ano, de US$ 2 milhões em 2024 para US$ 1 milhão em 2025. O fator primário por trás dessa queda foi a diminuição do percentual de pagamentos de resgate de US$ 5 milhões ou mais: de 31% de pagamentos efetuados em 2024 para 20% em 2025.
- Ao comparar **exigências versus pagamentos**, apenas 29% disseram ter pago o pedido inicial de resgate. 53% pagaram menos do que o valor inicial, enquanto 18% pagaram mais.

Impacto comercial do ransomware

- Salvo os resgates pagos, a média de **custo de recuperação** de um ataque de ransomware caiu em 44% no último ano, chegando a US$ 1,53 milhão em comparação a US$ 2,73 milhões em 2024.
- Analisando a **velocidade de recuperação**, as organizações estão ficando mais rápidas, com 53% delas recuperadas completamente após uma semana em comparação a 35% em 2024.

Impacto humano do ransomware

- Todas as organizações que tiveram os dados criptografados disseram ter havido **repercussões diretas** para as equipes de TI e segurança cibernética:
  - 41% das equipes de TI e segurança cibernética disseram estar sentindo **aumento em ansiedade e estresse** sobre ataques futuros.
  - Um terço (34%) disseram que a equipe ficou com **sentimento de culpa** porque o ataque não foi interrompido a tempo.
  - 40% disseram ter havido **aumento da pressão** pelos líderes seniores, mas 31% relataram o **aumento de reconhecimento**.
  - 31% das equipes passaram por períodos de **licença de pessoal** devido a problemas de estresse e saúde mental relacionados ao ataque.
  - Em um quarto dos casos, as equipes tiveram a **liderança substituída** como consequência do ataque.

Por que as organizações se tornam vítimas de ransomware

Causas técnicas primárias dos ataques

Pelo terceiro ano consecutivo, as vítimas apontaram a **exploração de vulnerabilidades** como a causa primária mais comum dos incidentes de ransomware, usada para se infiltrar em 32% dos ataques às organizações.

O **comprometimento de credenciais** permanece sendo o segundo vetor de ataque mais comum, embora a porcentagem de ataques que utilizou essa abordagem tenha caído de 29% em 2024 para 23% em 2025. E-mails continuam a ser o maior vetor de ataque, com 19% das vítimas que relataram **e-mails maliciosos** como a causa primária e outros 18% que citaram o **phishing** — um salto notável dos 11% do ano anterior.

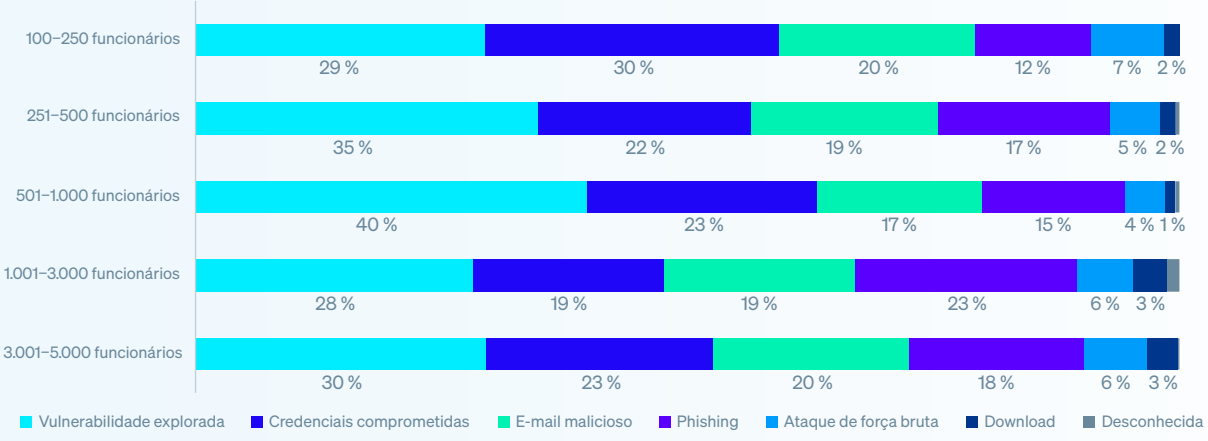
Gráfico 1: Causa técnica primária dos ataques de ransomware 2023–2025

Você sabe a causa primária do ataque de ransomware que a sua organização enfrentou no último ano? Sim. n=3.400 (2025), 2.974 (2024), 1.974 (2023).

A pesquisa revela diferenças nos vetores de ataque com base no tamanho da organização:

- O **comprometimento de credenciais** foi a causa primária mais comum na faixa de 100–250 funcionários, utilizado em 30% dos ataques.
- 40% dos ataques na faixa de 501–1.000 funcionários começou com uma **exploração de vulnerabilidade**.
- Chegando a quase um quarto (23%) dos ataques em organizações com 1.001–3.000 funcionários, os ataques começaram com um **e-mail de phishing**.

Gráfico 2: Causa técnica primária dos ataques de ransomware dividida por tamanho da organização

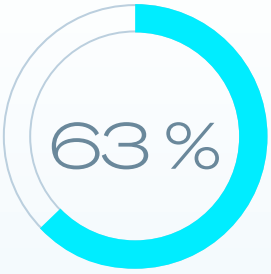


Você sabe a causa primária do ataque de ransomware que a sua organização enfrentou no último ano? Sim. n=3.400

Causa operacional primária dos incidentes

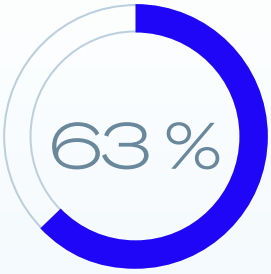
O relatório deste ano explora, pela primeira vez, os fatores organizacionais que deixaram as empresas expostas aos ataques. Os resultados revelam que as vítimas geralmente estão enfrentando várias dificuldades operacionais, com os entrevistados citando 2,7 fatores, em média, que contribuíram para que se tornassem vítimas do ataque de ransomware.

No geral, não há um fator que se destaque dos outros, com as causas organizacionais primárias distribuídas igualmente entre problemas de proteção, problemas de recursos e lacunas de segurança.



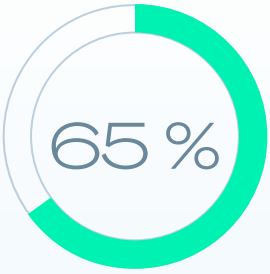
Problemas de proteção

(falta de soluções de proteção ou soluções de baixa qualidade)



Problemas de recursos

(falta de expertise ou pessoas/capacidade)



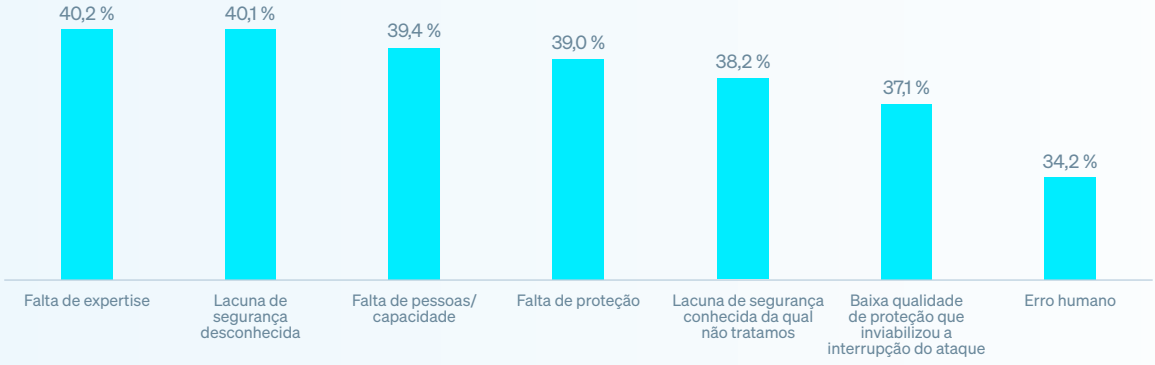
Lacuna de segurança

(conhecida ou desconhecida)

Por que você acha que a sua organização foi vítima de um ataque de ransomware? n=3.400

Falta de expertise (ou seja, não ter habilidades ou conhecimento para detectar e interromper o ataque em tempo hábil) é o motivo operacional mais comum, mencionado por 40,2% dos entrevistados. Seguido bem de perto por **lacunas de segurança das quais a organização não tinha conhecimento**, o fator que contribuiu para 40,1% dos ataques. Em terceiro lugar ficou a **falta de pessoas/capacidade** (ou seja, não ter um número suficiente de peritos de segurança cibernética monitorando seus sistemas no momento do ataque), que contribuiu para 39,4% dos ataques.

Gráfico 3: Causa operacional primária dos ataques de ransomware

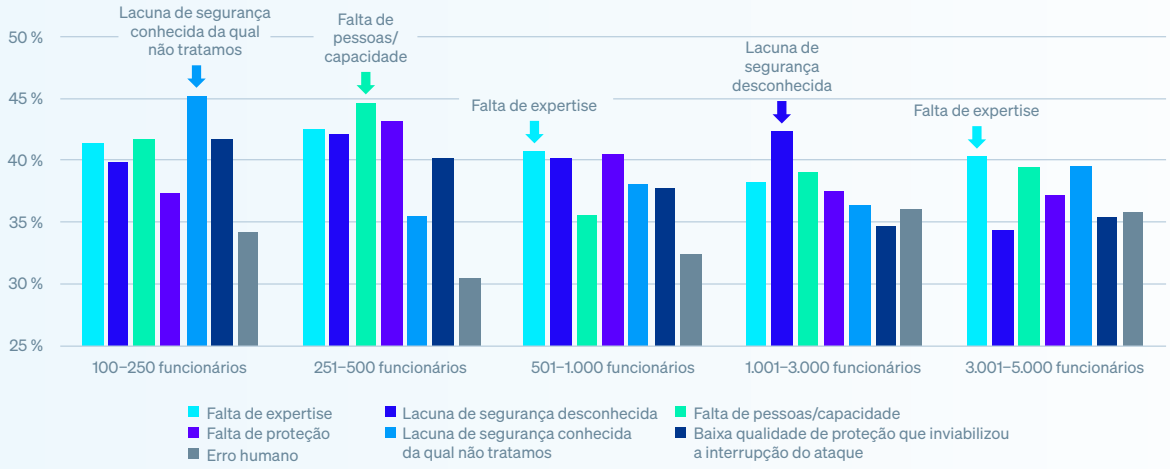


Por que você acha que a sua organização foi vítima de um ataque de ransomware? n=3.400

Causa operacional primária por tamanho da empresa

O motivo organizacional mais comum que torna as empresas vítimas de um ransomware varia de acordo com o tamanho da organização, o que reflete os diferentes desafios que enfrentam. Dentre as cinco faixas de tamanho por funcionários usadas no relatório, quatro desafios diferentes foram destaque entre os fatores que contribuíram para que as empresas fossem vítimas de ataques, como mostra o gráfico abaixo.

Gráfico 4: Causa operacional primária dos ataques de ransomware dividida por tamanho da organização



Por que você acha que a sua organização foi vítima de um ataque de ransomware? n=3.400. Distribuída por tamanho organizacional (número de funcionários)

Causa operacional primária por setor

Aqui também, a causa operacional primária mais comum varia por setor, revelando mais diferenças para enfrentar. Vale notar que nenhum setor apontou o erro humano como o motivo mais comum de terem sido vítimas de um ataque de ransomware.

Gráfico 5: Principal causa operacional primária dos ataques de ransomware por setor

FALTA DE **EXPERTISE**	LACUNA DE **SEGURANÇA DESCONHECIDA**	FALTA DE **PESSOAS/ CAPACIDADE**	FALTA DE **PROTEÇÃO**	LACUNA DE **SEGURANÇA CONHECIDA**	BAIXA **QUALIDADE DE PROTEÇÃO**
Não tínhamos as habilidades ou conhecimento à disposição para detectar e interromper o ataque em tempo hábil	Havia um ponto fraco em nossas defesas do qual não tínhamos conhecimento	Não tínhamos peritos de segurança cibernética suficientes monitorando nossos sistemas no momento do ataque	Não tínhamos os produtos e serviços de segurança cibernética necessários	Havia um ou mais pontos fracos em nossas defesas dos quais tínhamos conhecimento, mas que não tratamos	Nossos produtos e serviços de segurança cibernética não foram capazes de interromper o ataque
Energia, petróleo/ gás e serviços de utilidade (43%)	Ensino superior (18 anos+) (49%)	Ensino básico (42%)*	Serviços financeiros, incl. seguros (44%)*	Governo central/ federal (45%)	Mídia, lazer e entretenimento (41%)
Ensino básico (42%)*	Serviços profissionais e empresariais (46%)	Saúde (42%)	Governo local/ estadual (40%)	TI, tecnologia e telecomunicações [42%]	Distribuição e transporte (41%)
Manufatura e produção (42%)	Varejo (46%)			Construção civil (41%)*	
Construção civil (41%)*	Serviços financeiros, incl. seguros (44%)*				

* indica principal causa primária dos ataques combinada.

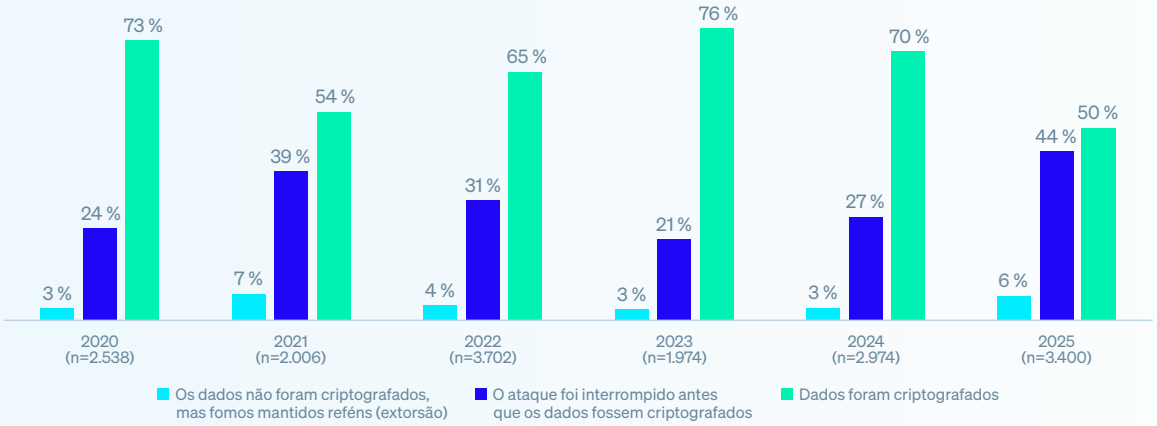
Por que você acha que a sua organização foi vítima de um ataque de ransomware? n=3.400. Distribuída por setor

O que acontece aos dados

Criptografia de dados

A criptografia de dados está no seu índice de presença mais abaixo já relatado durante os seis anos deste estudo, com 50% dos ataques resultando em dados criptografados. Houve uma queda acentuada na porcentagem de ataques que resultaram em dados criptografados no último ano, caindo de 70% na pesquisa de 2024 para 50% na pesquisa de 2025, o que sugere que as organizações estão mais capacitadas a bloquear ataques antes que a carga de criptografia seja lançada.

Gráfico 6: Índice de criptografia de dados em ataques de ransomware 2020–2025



Os criminosos virtuais tiveram sucesso na criptografia de dados da sua organização no ataque de ransomware? Números de base no gráfico.

As grandes organizações entrevistadas mostraram maior probabilidade de ter seus dados criptografados, com 65% dos ataques a organizações com 3.001–5.000 funcionários resultando na criptografia de dados, o maior índice de criptografia relatado entre as coortes de todos os tamanhos. Isso sugere que as grandes organizações estão menos capacitadas a detectar e interromper um ataque antes da criptografia; e/ou estão menos capacitadas a bloquear e reverter a criptografia maliciosa do que as organizações menores.

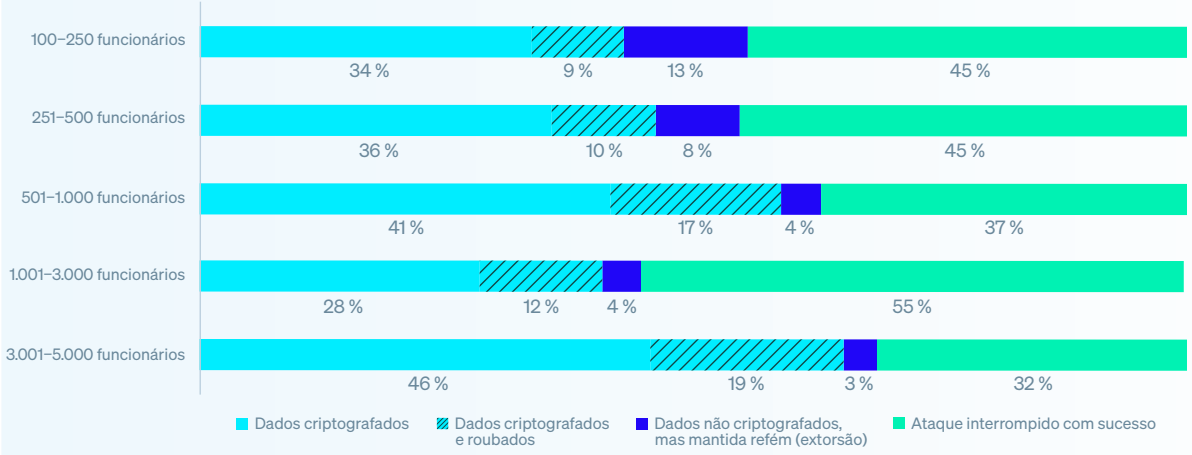
Roubo de dados

Os adversários não apenas criptografam os dados, eles também os roubam. 14% de todas as vítimas de ransomware e 28% das que tiveram seus dados criptografados tiveram seus dados roubados. Examinado os dados por tamanho da empresa, observamos que as organizações menores apresentam quase 40% menos de probabilidade de ter os dados roubados do que as grandes empresas.

- 22% das organizações com 100–500 funcionários que tiverem os dados criptografados também tiveram os dados roubados.
- 30% das organizações com 501–5.000 funcionários que tiverem os dados criptografados também tiveram os dados roubados.

Ainda que seja possível que as pequenas organizações estejam mais bem capacitadas a prevenir o roubo de dados, essa variação provavelmente se deve ao fato de os adversários estarem mais propensos a exfiltrar dados de organizações maiores e/ou de as pequenas empresas estarem menos capacitadas a identificar que os dados foram roubados.

Gráfico 7: Índice de criptografia de dados em ataques de ransomware dividido por tamanho da organização



Os criminosos virtuais tiveram sucesso na criptografia de dados da sua organização no ataque de ransomware? n=3.400

Ataques no estilo extorsão

Como mostra o gráfico 6, a porcentagem de organizações que não tiveram os dados criptografados, mas que foram feitas reféns (extorquidas), duplicou no último ano, fato relatado em 6% de ataques em 2025 comparado a apenas 3% em 2024. As pequenas organizações estão mais propensas a passar por uma situação de resgate sem que os dados sejam criptografados (um ataque no estilo extorsão) do que as grandes empresas:

- 13% das vítimas com 100–250 funcionários passaram por um ataque no estilo extorsão.
- 3% das vítimas com 3.001–5.000 funcionários passaram por um ataque no estilo extorsão.

No geral, as organizações com 1.001–3.000 funcionários estão mais capacitadas a prevenir as repercussões de um ataque de ransomware (ou seja, impedir que os dados sejam criptografados, prevenir a exfiltração de dados e evitar sujeitar-se a uma extorsão). Essas organizações talvez estejam na melhor situação possível: grandes o suficiente para ter um ótimo arsenal de ferramentas de segurança cibernética e expertise, mas sem estarem sujeitas aos mesmos níveis de complexidade organizacional que as grandes empresas.

Recuperação de dados criptografados

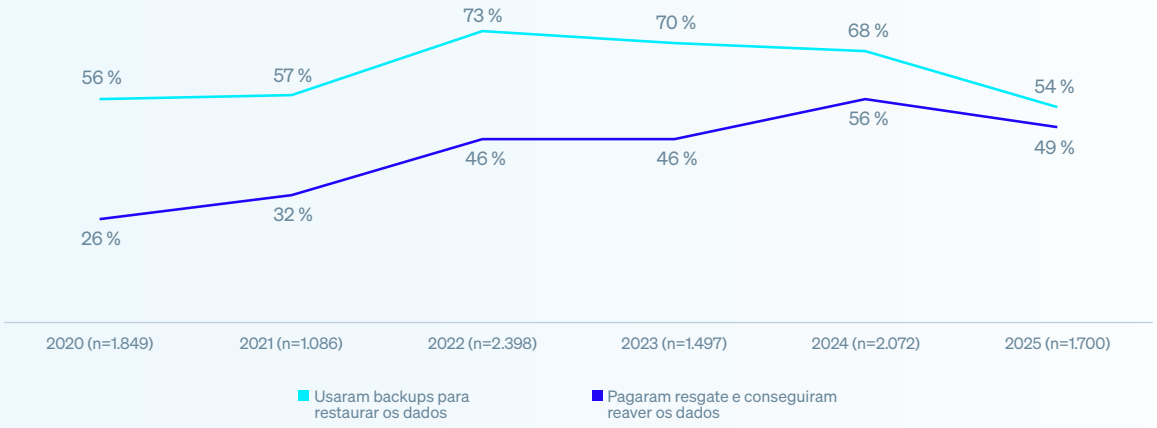
97% das organizações que tiveram os dados criptografados conseguiram recuperá-los.

Apenas um pouco mais da metade (54%) restaurou seus dados usando backups — o terceiro ano consecutivo em que esse número diminui. No geral, a recuperação de dados através de backups atingiu o seu índice mais baixo em seis anos.

Um pouco menos da metade (49%) das vítimas pagou o resgate e conseguiu reaver os dados. Ainda que represente uma pequena redução dos 56% do ano anterior, esse continua a ser o segundo índice de pagamentos de resgate mais alto nos últimos seis anos.

29% das vítimas que tiveram seus dados criptografados disseram ter utilizado “outros meios” para restaurar os dados. Esse valor provavelmente inclui as vítimas que usaram chaves de descriptografia que foram a público anteriormente.

Gráfico 8: Recuperação de dados via backups e pagamentos de resgate 2020–2025



Sua organização conseguiu reaver os dados capturados? Sim, pagamos o resgate e recuperamos os dados; Sim, usamos backups para restaurar os dados.
Números de base no gráfico

Resgates

Pedidos de resgate

A média (mediana) do pedido de resgate caiu um terço (34%) no último ano, chegando a US$ 1.324.439,00: uma queda em relação aos US$ 2 milhões em 2024. Essa redução foi levada, em grande parte, pela diminuição de pedidos de resgate de US$ 5 milhões ou mais: uma queda de 30% para 24%. Ainda que seja uma queda apreciável, é importante lembrar que 57% dos pedidos de resgate foram de US$ 1 milhão ou mais.

As exigências nos resgates aumenta de acordo com a receita da organização, o que sugere que os adversários "precificam" seus pedidos de resgate com base no pressuposto do pagamento ser concretizado pela vítima:

- US$ 109.670: valor mediano de resgate exigido das organizações com US$ 10 milhões–US$ 50 milhões de receita anual.
- US$ 5.500.000: valor mediano de resgate exigido das organizações com US$ 5 milhões e acima de receita anual.

Gráfico 9: Exigências de resgate divididas por receita anual da empresa

Qual foi o valor do pedido de resgate exigido pelos invasores? Números de base no gráfico.

Pagamentos de resgate

A média (mediana) do pagamento de resgate caiu em 50% no último ano, de US$ 2 milhões em 2024 para US$ 1 milhão em 2025. Como acontece com os valores de resgate exigidos, o fator primário por trás da baixa mediana de pagamento de resgate é a diminuição do percentual de pagamentos de US$ 5 milhões ou acima, que caiu de 31% em 2024 para 20% em 2025.

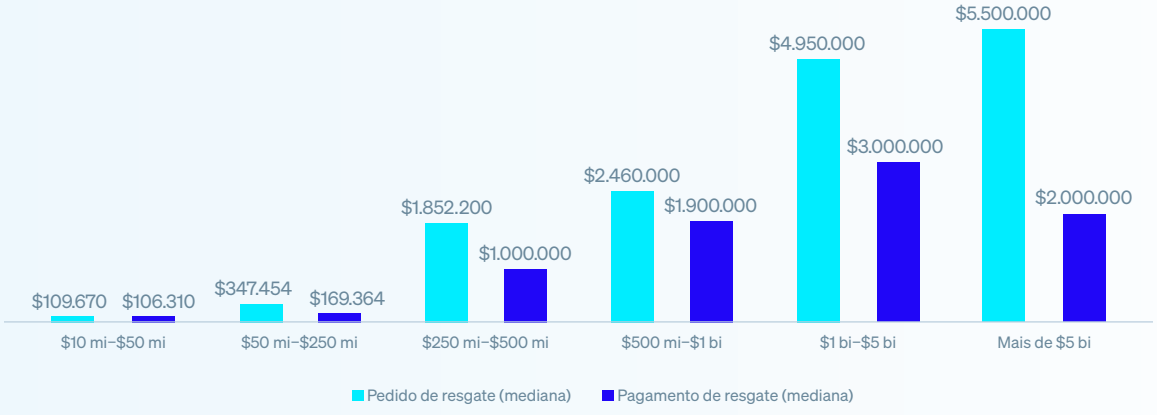
Apesar da queda em pedidos de resgate e pagamentos no último ano, é bom saber que os pagamentos sentiram a maior queda. Ainda assim, US$ 1 milhão é uma grande soma e pode trazer grandes consequências para a maioria das organizações.

Como se parecem os pagamentos reais comparados às exigências iniciais

826 organizações que pagaram o resgate compartilharam conosco os valores inicial e o realmente efetuado, revelando que pagaram, em média, 85% do pedido de resgate inicial. No geral, 53% pagaram menos do que o pedido inicial, 18% pagaram mais e 29% cobriram a exigência inicial.

Dividindo os dados por receita anual, observamos que todas as coortes pagaram, em média, menos do que a exigência inicial. Contudo, as organizações com receitas maiores (US$ 5 bilhões ou mais em receita anual) sentiram maior redução na média de pagamento real (US$ 2 milhões) em apenas 36% das exigências iniciais (US$ 5,5 milhões), excluindo-se os valores atípicos. Por outro lado, as organizações com receita anual de US$ 10 milhões–US$ 50 milhões relataram a menor redução com uma mediana de pagamento de 97% da exigência mediana.

Gráfico 10: Exigência de resgate vs. pagamento do resgate dividido por receita anual da empresa



Qual foi o valor do pedido de resgate exigido pelos invasores? Qual foi o pagamento de resgate que foi efetuado aos invasores? (n=1.552/836)

Por que a maioria dos pagamentos de resgate difere do valor inicial exigido

Este ano, pela primeira vez, examinados por que algumas organizações pagam mais do que o resgate inicial exigido e outras pagam menos, ressaltando uma área importante quando lidamos com um ataque de ransomware.

151 organizações que **pagaram mais** do que o resgate inicial revelaram que:

- 50%: os invasores acreditavam que poderíamos pagar mais.
- 48%: os invasores se deram conta de que éramos um alvo de grande valor.
- 38%: os invasores se irritaram e aumentaram o preço.
- 38%: nossos backups não funcionaram ou apresentaram defeitos.
- 32%: não pagamos rápido o suficiente, então o preço subiu.

No geral, as organizações citaram dois fatores por trás da decisão de pagar mais, revelando os vários desafios que as vítimas enfrentam ao tentar recuperar seus dados.

445 organizações que **pagaram menos** do que a exigência inicial explicaram como conseguiram abaixar o valor do pagamento:

- 47%: negociamos um valor mais baixo com os invasores.
- 45%: os invasores reduziram o valor do resgate devido a pressões externas (por exemplo, da mídia ou de autoridades legais).
- 45%: os invasores reduziram o valor do resgate para nos incentivar a pagar.
- 43%: pagamos o resgate rapidamente, assim conseguimos um desconto.
- 40%: terceiros negociaram um valor mais baixo com os invasores.

Essa coorte também relatou, em média, dois fatores por trás do baixo pagamento de resgate, o que enfatiza ainda mais a complexidade da situação que as vítimas de ransomware enfrentam.

Consequências comerciais do ransomware

Custos de recuperação

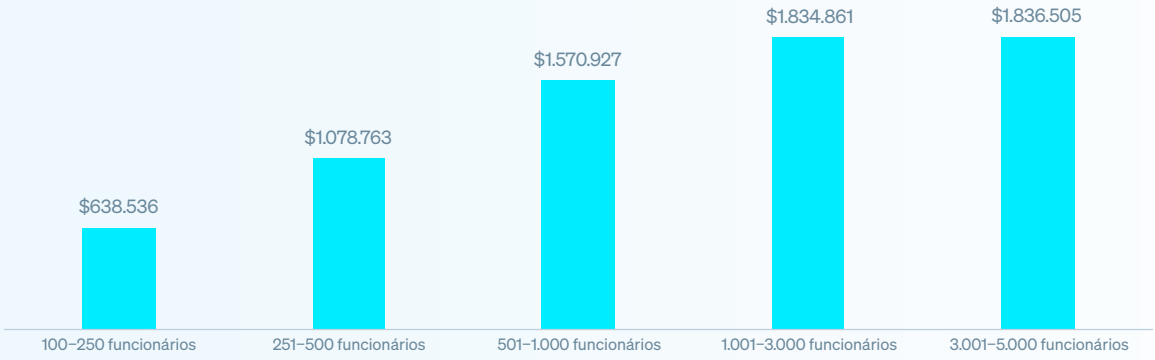
A média do custo de recuperação de um ataque de ransomware (excluindo pagamento de resgate) caiu em 44% no último ano, chegando a US$ 1,53 milhão em comparação a US$ 2,73 milhões em 2024, apenas um pouco mais de US$ 300.000 abaixo da soma registrada em 2023.

2023	2024	2025
$1,82 milhão	$2,83 milhões	$1,53 milhão

Qual foi o custo aproximado para a sua organização retificar o impacto do ataque de ransomware mais significativo (considerando-se período de inatividade, tempo de pessoal, custo dos equipamentos, custo da rede, perda de oportunidades etc.), excluindo pagamentos de resgate realizados? n=3.400 (2025), 2.974 (2024), 1.974 (2023)

Os custos de recuperação aumentaram de acordo com o tamanho da organização, até se equipararem às organizações com entre 1.000 e 5.000 funcionários. As organizações com 100–250 funcionários relataram um custo médio de recuperação de US$ 638.536,00, enquanto as organizações com 1.000–5.000 funcionários incorrem em custos de US$ 1,83 milhão.

Gráfico 11: Custo de recuperação de ransomware dividido por tamanho da empresa

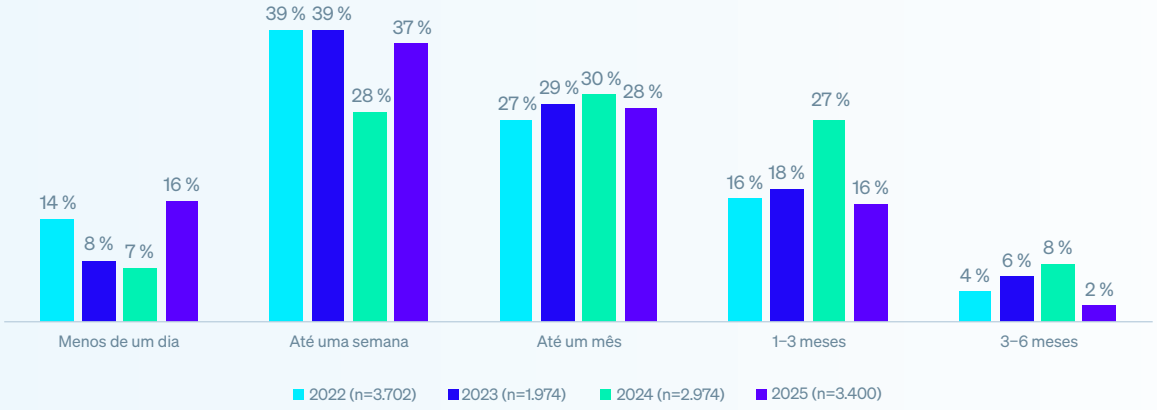


Qual foi o custo aproximado para a sua organização retificar o impacto do ataque de ransomware mais significativo (considerando-se período de inatividade, tempo de pessoal, custo dos equipamentos, custo da rede, perda de oportunidades etc.), excluindo pagamentos de resgate realizados? n=3.400

Tempo de recuperação

Os dados revelam que as organizações estão ficando mais rápidas no processo de recuperação pós-ataque, com 16% delas totalmente recuperadas em um dia – uma subida dos 7% em 2024 e 8% em 2023. Mais da metade (53%) se recuperou em uma semana ou menos, um salto significativo dos 35% registrados em 2024. No geral, quase todas as vítimas (97%) já estavam totalmente recuperadas três meses após o ataque. Essa velocidade de recuperação acelerada indica que as organizações investiram no preparo e recuperação de incidentes cibernéticos durante o último ano.

Gráfico 12: Tempo de recuperação dos ataques de ransomware 2022–2025



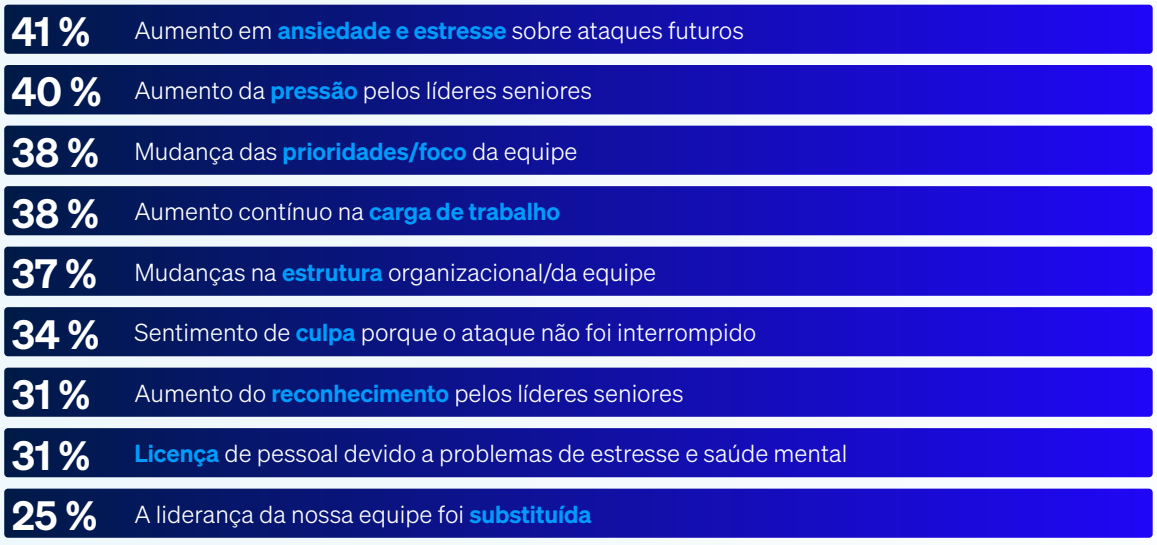
Quanto tempo a sua organização levou para se recuperar por completo do ataque de ransomware? Números de base no gráfico

Não surpreende que as organizações que tiveram seus dados criptografados foram, tipicamente, mais lentas para se recuperar do que aquelas que foram capazes de interromper a criptografia: 9% das organizações que tiveram os dados criptografados estavam totalmente recuperadas em um dia, em comparação aos 24% daquelas em que os adversários foram malsucedidos na criptografia de dados.

Consequências humanas do ransomware

A pesquisa deixa claro que ter os dados criptografados em um ataque de ransomware causa repercussões significativas para as equipes de TI e segurança cibernética, com todos os entrevistados dizendo que suas equipes foram afetadas de alguma forma.

Gráfico 13: As consequências de ter dados criptografados para as equipes de TI e segurança cibernética



Qual a repercussão que o ataque de ransomware teve nas pessoas em sua equipe de TI e segurança cibernética, se alguma? n=1.700

Recomendações

Apesar de ter havido várias mudanças nas experiências vividas pelas organizações com relação a ransomwares no último ano, o ransomware continua a ser uma das maiores ameaças para todas as organizações. Os adversários continuam a repetir e incrementar os seus ataques, sendo essencial que as equipes e suas defesas cibernéticas acompanhem essa evolução de ransomwares e outras ameaças. Utilize os insights deste relatório para fortalecer as suas defesas, moldar as suas respostas às ameaças e limitar o impacto do ransomware nos seus negócios e nas pessoas. Concentre-se nestas quatro áreas para ficar na dianteira dos ataques:

- **Prevenção**. A defesa de maior sucesso contra um ransomware é aquela em que o ataque nunca acontece — porque os adversários não puderam violar a sua organização. Siga os passos ressaltados neste relatório para eliminar as causas técnicas e operacionais primárias.
- **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 backups de qualidade e de praticar a restauração dos dados nesses backups com regularidade para se preparar para uma recuperação mais rápida caso você seja atingido.

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

Saiba mais sobre ransomware e como a Sophos pode ajudar a defender a sua organização.

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.

2025-06-26 WP (DD)

SOPHOS