RELATÓRIO

O Estado do Ransomware 2026

Perspectivas de 2.158 líderes de TI e segurança cibernética em 17 países

SOPHOS

Introdução

O cenário de ransomwares está mudando rapidamente com o avanço da inteligência artificial. As organizações que fazem investimentos contínuos em sua defesa de segurança cibernética mostram resultados concretos, mas os ataques de ransomware ainda custam milhões às empresas.

Esta é a sétima edição do relatório anual da Sophos O Estado do Ransomware, que oferece novos dados sobre ataques de ransomware no último ano. Os resultados foram compilados em seções que abrangem:

- Métodos de ataque e defesa
- Criptografia e recuperação de dados
- Pedidos de resgate e pagamentos
- Impacto nos negócios e nas pessoas

Os dados contam uma história de altos custos combinados com progresso genuíno:

- Os custos de recuperação após ataques de ransomware são elevados, com o valor típico da recuperação atualmente em US$ 1,7 milhão.
- Mais da metade dos ataques de ransomware (56%) ainda consegue criptografar dados, um aumento sobre a taxa de 2025.
- No entanto, os pedidos e pagamentos de resgate estão diminuindo, com as organizações cada vez mais eficientes nas negociações. Nos últimos dois anos, a mediana das exigências de resgate diminuíram 65% e os pagamentos caíram em 62%.
- Após três anos na liderança, as vulnerabilidades exploradas deixaram de ser a causa primária de ataques de ransomware (18%), sendo os ataques baseados em e-mail (phishing 24% ou e-mails maliciosos 26%) os vetores de ataque mais comuns.

2.158

Líderes de TI e segurança de 17 países, cujas organizações foram atingidas por ransomware no último ano, participaram de uma pesquisa global, desvinculada de fornecedores, que serviu de base para a pesquisa deste ano.

Sobre a pesquisa

Este relatório baseia-se nas conclusões de um levantamento independente e totalmente desvinculado de fornecedores encomendado pela Sophos. A pesquisa incluiu perguntas sobre experiências organizacionais com ataques de ransomware e invasões baseadas em identidade, rastreando índices de pagamento de resgate, custos de recuperação, tempo de recuperação e outras métricas ano a ano. As respostas foram coletadas de janeiro a março de 2026 e baseiam-se nas experiências dos entrevistados nos 12 meses anteriores.

Os entrevistados eram provenientes de 17 países, cobriram uma ampla gama de setores, tanto públicos quanto privados, e representaram uma curva de amostragem de empresas com tamanhos entre 100 e 5.000 funcionários, que se mantém proporcionalmente consistente ao longo dos sete anos de histórico da pesquisa. Todos os dados financeiros são expressos em dólares americanos.

Pontos-chave

- **O comprometimento de identidade é o principal mecanismo de distribuição de ransomware**
  - E-mails maliciosos (26%) e phishing (24%) tornaram-se as principais causas primárias de ataques de ransomware.
  - As vulnerabilidades exploradas — a principal causa primária de problemas nos últimos três anos — caíram 14 pontos percentuais no último ano, chegando a 18%.
  - Dois terços das vítimas de ransomware (67%) confirmaram que o incidente de ransomware sofrido foi também o ataque de identidade mais significativo que sofreram.
- **As lacunas em proteção, segurança e recursos deixam as organizações expostas a ataques**
  - As lacunas de segurança (conhecidas ou desconhecidas) foram as causas operacionais primárias mais citadas pelo segundo ano consecutivo, 62%, seguidas pela falta de pessoas ou habilidades (58%) e pela falta de proteção ou baixa qualidade (57%).
- **A implementação da autenticação multifator (MFA) por si só não é suficiente para impedir o ransomware**
  - A autenticação multifator (MFA) foi, de alguma forma, utilizada em 97% dos incidentes em que credenciais comprometidas foram a causa primária dos ataques de ransomware.
- **Em mais da metade dos incidentes, as organizações não conseguem detectar e interromper ataques de ransomware a tempo**
  - Mais da metade dos ataques de ransomware (56%) conseguiu criptografar dados, incluindo 16% em que os dados foram criptografados e roubados.
- **Quando os dados são criptografados, os invasores têm 50% de chance de receber um pagamento de resgate**
  - 48% das organizações que tiverem seus dados criptografados pagaram o resgate.
  - A média de quatro anos é agora de 50% de pagamento de resgate após a criptografia.
- **Os pedidos de resgate estão diminuindo, mas os invasores exigem mais quando conseguem obter o acesso a um sistema privilegiado que é difícil de reverter**
  - O valor mediano dos pedidos de resgate caiu para US$ 698.000, dando continuidade a uma tendência de queda que já dura vários anos, partindo de uma mediana de US$ 1,3 milhão no relatório de 2025 e de US$ 2 milhões no relatório de 2024.
  - 59% dos pedidos de resgate decorrentes de ataques iniciados com a exploração de uma vulnerabilidade no firewall são de US$ 1 milhão ou mais, em comparação com 48% de todos os pedidos.
- **Os pagamentos de resgate estão diminuindo, com as vítimas frequentemente conseguindo negociar um valor menor do que o inicialmente exigido**
  - O valor mediano dos resgates pagos atualmente é de US$ 769.000, uma queda considerável em relação ao valor de US$ 1 milhão registrado no ano passado.
  - Pouco menos da metade (48%) dos pagamentos foi de US$ 1 milhão ou mais, uma queda em relação aos 52% do ano anterior.
  - Quase metade (51%) das organizações que pagaram um resgate pagou menos do que o valor exigido, o que é muito semelhante ao relatório de 2025 (53%) e 7% superior ao relatório de 2024 (44%).
- **O custo para se recuperar de um ataque de ransomware aumentou**
  - O custo médio para recuperação de um ataque de ransomware, excluindo qualquer resgate pago, é agora de US$ 1.700.200, um aumento de 11% em relação à média de US$ 1.525.716 no relatório de 2025.
- **A criptografia de dados quase sempre traz repercussões para os membros da equipe de TI e segurança cibernética**
  - 99% das vítimas de ransomware que tiveram seus dados criptografados afirmaram que isso afetou suas equipes de TI e segurança cibernética.
  - O aumento de ansiedade ou estresse em relação a futuros ataques é o impacto mais comum (41%), seguido pelo aumento da pressão por parte dos líderes seniores (40%).
  - O aumento do reconhecimento por parte dos líderes seniores (36%, contra 31% no relatório de 2025) foi o único impacto que cresceu em relação ao ano anterior.

Métodos de ataque e defesa

Causas primárias dos ataques

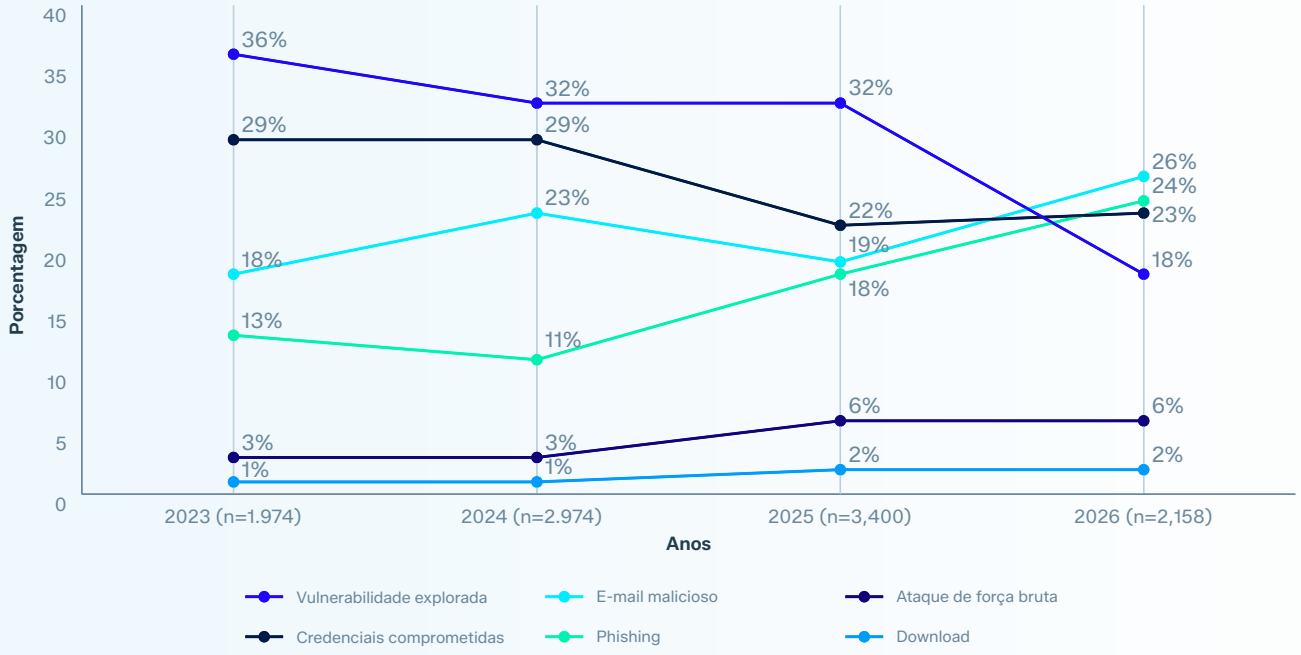
As causas técnicas primárias dos ataques de ransomware mudaram no relatório deste ano. E-mail maliciosos (26%) e phishing (24%) foram as duas principais causas primárias de ataques de ransomware, representando metade de todos os incidentes. Isso representa uma mudança significativa em relação aos anos anteriores, quando as vulnerabilidades exploradas lideravam consistentemente o ranking.

O número de relatos de vulnerabilidades exploradas caiu de 32% no relatório de 2025 para 18% no relatório de 2026. No entanto, dada a velocidade e a escala da capacidade de descoberta de vulnerabilidades da IA fronteiriça, as organizações devem permanecer alertas à possibilidade de um aumento nos ataques de ransomware cuja causa primária seja a exploração de uma vulnerabilidade no próximo ano.

As credenciais comprometidas continuaram sendo a terceira causa primária mais comum, representando 23% dos casos, em consonância com os anos anteriores.

79% dos ataques começaram com uma abordagem baseada em identidade, seja para obter credenciais para uso indevido, seja para explorar credenciais já comprometidas. Isso destaca por que a segurança da identidade é uma peça fundamental em uma postura de segurança holística.

Causa técnica primária dos ataques de ransomware (2023 – 2026)



Você sabe a causa primária do ataque de ransomware que a sua organização enfrentou no último ano? Números de base no gráfico.

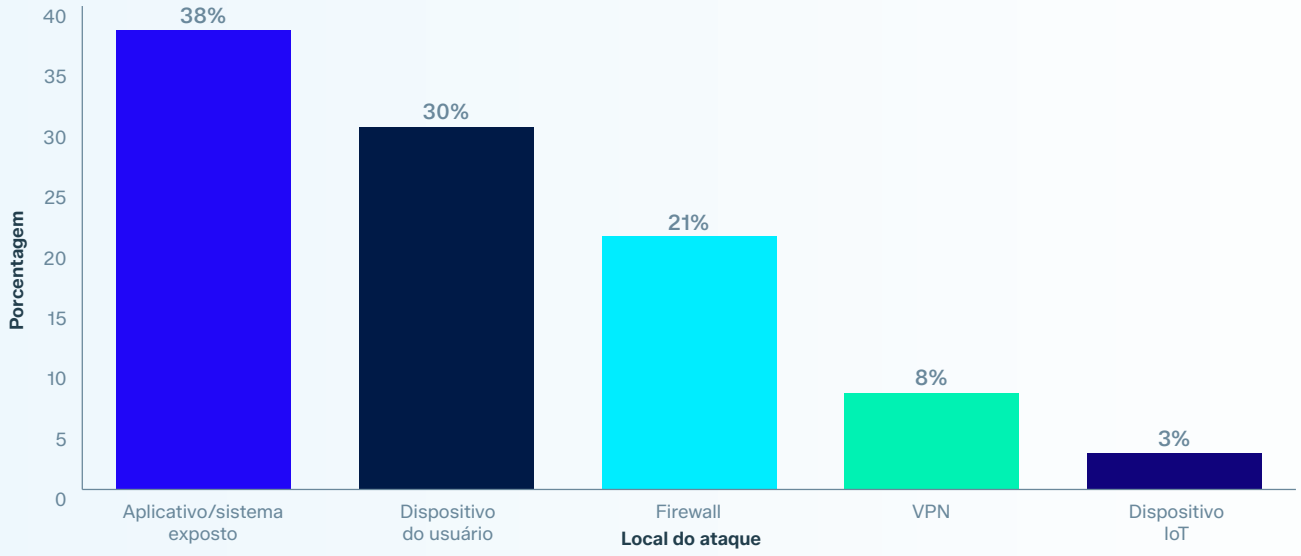
NOVA PESQUISA

Onde começam os ataques

Este ano, pela primeira vez, revelamos onde ocorreu a causa primária dentro do ambiente organizacional. Compreender onde os ataques começam é fundamental para orientar as estratégias de redução de riscos. Em todos os incidentes de ransomware que começaram com uma vulnerabilidade explorada, credenciais comprometidas ou um ataque de força bruta, **os aplicativos e sistemas expostos foram o ponto de entrada de ataque mais comum (38%)**, seguido por dispositivos de usuários (30%) e firewalls (21%).

A proeminência de aplicativos expostos está alinhada com a mudança mais ampla em direção a ambientes de nuvem e SaaS, onde os sistemas voltados para a internet representam uma superfície de ataque grande e crescente.

Locais de ataques de ransomware



Você disse que a causa primária foi uma vulnerabilidade explorada, credenciais comprometidas ou um ataque de força bruta. Onde isso aconteceu no seu ambiente? n=1.022

Analisando mais a fundo, os dados revelam a prevalência de credenciais comprometidas em aplicativos e sistemas expostos, firewalls, VPNs e dispositivos IoT.

Causas primárias mais comuns para cada local

Causa primária	Em um aplicativo ou sistema exposto	Em nosso firewall	Em nossa VPN	Em um dispositivo IoT
Credenciais comprometidas	59%	41%	44%	48%
Uma vulnerabilidade explorada	31%	33%	41%	36%
Ataque de força bruta	10%	26%	15%	16%

Você disse que a causa primária foi uma vulnerabilidade explorada, credenciais comprometidas ou um ataque de força bruta. Onde isso aconteceu no seu ambiente? Seleção de respostas. n=711

Os ataques que exploram credenciais comprometidas foram especialmente predominantes em aplicativos e sistemas expostos (59%), reforçando a importância de proteger controles de identidade e ativos acessíveis externamente.

Ao refazer a comparação dos mesmos dados, foram revelados os alvos mais comuns de comprometimento de credenciais e ataques de força bruta.

Onde começam os ataques de ransomware

Local do ataque	Total (%)	Credenciais comprometidas (%)	Ataque de força bruta (%)
Em um aplicativo ou sistema exposto	38%	46%	30%
No dispositivo do usuário (dentro ou fora da rede; por ex., laptop, desktop)	30%	27%	13%
Em nosso firewall	21%	18%	44%
Em nossa VPN	8%	7%	9%
Em um dispositivo IoT	3%	3%	4%

Você disse que a causa primária foi uma credencial comprometida ou um ataque de força bruta. Onde isso aconteceu no seu ambiente? Seleção de respostas. n=628

Diferentes tipos de ataque visavam locais diferentes.

- Os ataques com credenciais comprometidas concentraram-se em aplicativos e sistemas expostos (46%), seguidos por dispositivos de usuários.
- Os ataques de força bruta visaram mais explicitamente os firewalls (44%), destacando a importância das políticas de limitação de taxa e bloqueio de contas em dispositivos de perímetro de rede.

NOVA PESQUISA

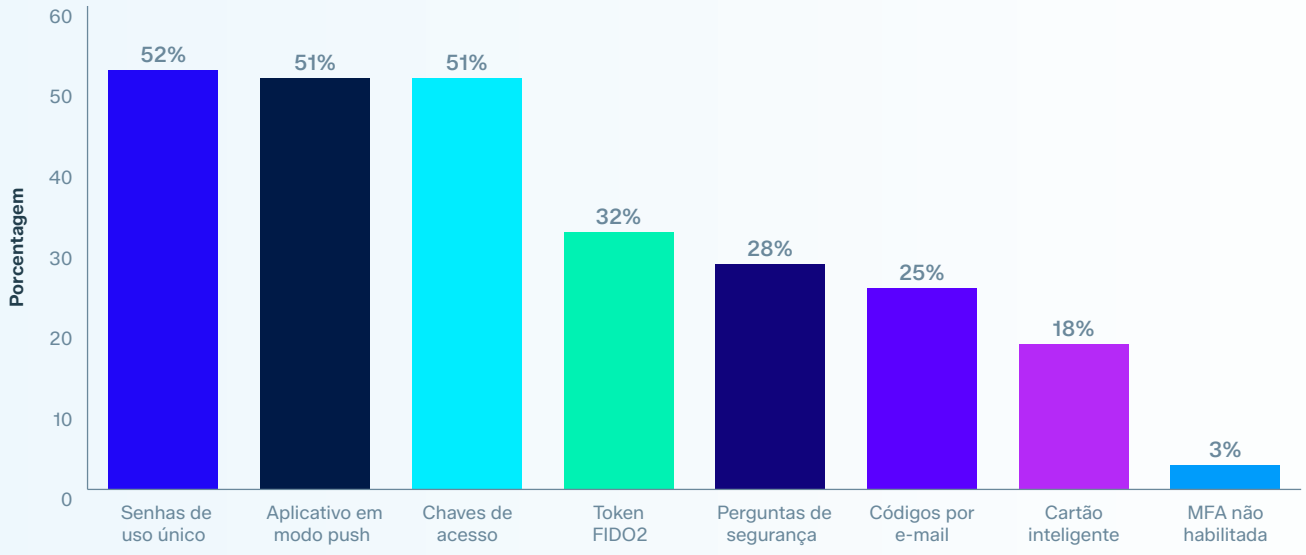
O papel da autenticação multifator (MFA)

Este ano também traz novas perspectivas sobre o papel da autenticação multifator (MFA) em ataques de ransomware.

Entre as organizações em que credenciais comprometidas foram a causa primária do ataque de ransomware, **97% tinham autenticação multifator habilitada de alguma forma no momento do incidente**. Senhas de uso único (52%), aplicativos em modo push (51%) e chaves de acesso (51%) foram os métodos mais amplamente utilizados, com os entrevistados relatando, em média, o uso de 2,5 métodos de MFA.

A alta porcentagem de vítimas de ransomware que tinham a autenticação multifator implementada no momento do ataque indica que a MFA pode não ter sido totalmente implementada em todos os sistemas relevantes, criando brechas que os invasores puderam explorar. Isso também sugere que, embora a MFA continue sendo um elemento essencial de estratégias eficazes de defesa cibernética, ela não é suficiente para impedir ataques baseados em credenciais, visto que as técnicas de evasão continuam a evoluir.

Métodos de MFA habilitados no momento do ataque



Que tipo de autenticação multifator estava habilitada no momento do ataque, se alguma? Base: o ataque ocorreu devido a credenciais comprometidas. n=503

O que deixou as organizações vulneráveis

Pelo segundo ano consecutivo, não houve um fator organizacional dominante único que deixasse as organizações expostas a ataques, com os entrevistados relatando uma ampla gama de desafios, desde proteção inexistente ou de baixa qualidade e escassez de pessoal e habilidades até lacunas na segurança.

35%

Erro humano: a única constante. A única causa operacional primária dos ataques que não diminuiu em relação ao relatório de 2025.

Pelo segundo ano consecutivo, as lacunas de segurança foram a categoria mais citada como causa operacional primária, representando 62% dos casos, seguidas pela falta de pessoas ou habilidades (58%) e pela falta de proteção ou proteção de baixa qualidade (57%).

Felizmente, todos os fatores individuais, exceto um, apresentaram declínio em relação ao ano anterior, com o **erro humano (35%) sendo o único fator operacional que aumentou no último ano**.

Assim como em 2025, as vítimas de ransomware relataram múltiplos desafios organizacionais, com **2,5 fatores citados em média**, valor inferior a 2,7.

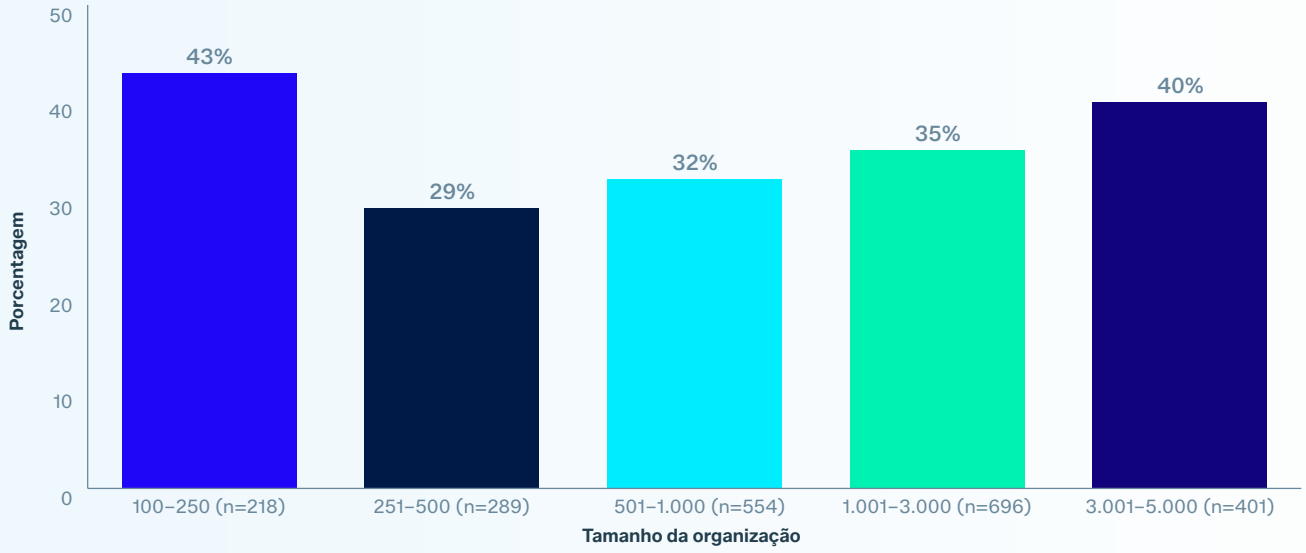
Sete principais causas operacionais primárias de ataques de ransomware

Posição	2025	%	Posição	2026	%
1	Falta de expertise	40,2%	1	Falta de proteção	36,4%
2	Lacuna de segurança desconhecida	40,1%	2	Lacuna de segurança desconhecida	36,3%
3	Falta de pessoas/ capacidade	39,4%	3	Lacuna de segurança conhecida	36,0%
4	Falta de proteção	39,0%	4	Falta de pessoas/ capacidade	35,3%
5	Lacuna de segurança conhecida	38,2%	5	Erro humano	35,3%
6	Baixa qualidade de proteção	37,1%	6	Falta de expertise	35,1%
7	Erro humano	34,2%	7	Baixa qualidade de proteção	32,6%

Por que você acha que a sua organização foi vítima de um ataque de ransomware? n=3.400 (2025), n=2.158 (2026)

Como era de se esperar, a falta de pessoas/capacidade foi citada com frequência por pequenas organizações com 100 a 250 funcionários. No entanto, quatro em cada dez empresas com 3.001 a 5.000 funcionários também citam desafios de capacidade a uma taxa apenas 3% inferior à das organizações com 100 a 250 funcionários, indicando que a alocação de recursos nem sempre se torna mais fácil com o aumento da escala.

A falta de pessoas/capacidade contribuiu para o número de vítimas de ransomware



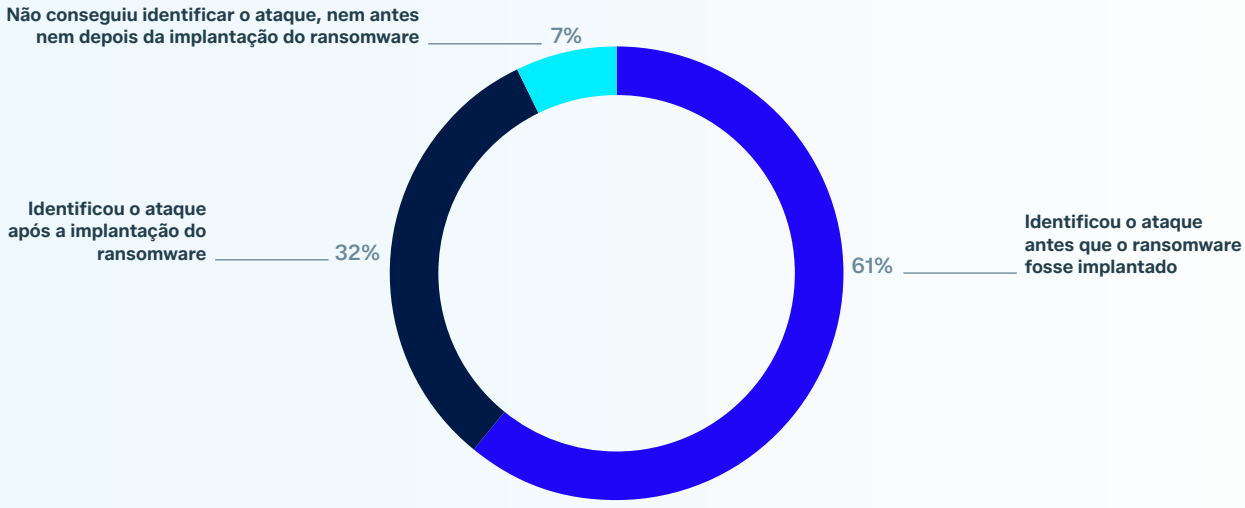
Por que você acha que a sua organização foi vítima de um ataque de ransomware? Não tínhamos um número suficiente de especialistas em segurança cibernética monitorando nossos sistemas no momento do ataque. Números de base no gráfico.

NOVA PESQUISA

O papel dos firewalls na defesa contra ransomware

61% das vítimas relataram que seus firewalls detectaram o ataque de ransomware antes que a carga fosse detonada e 32% disseram que o firewall identificou o ataque depois que o ransomware já havia sido implantado. Apenas 7% relataram que seus firewalls não identificaram o ataque.

Qual foi o papel do seu firewall na identificação do ataque?



Qual foi o papel do seu firewall na identificação do ataque? n=2.158

Os 7% de vítimas cujo firewall não detectou o ataque enfrentaram os piores resultados em termos de criptografia, com 71% tendo seus dados criptografados, em comparação com 50% quando o firewall detectou o ataque antes da implantação do ransomware. A detecção após a implantação do ransomware — normalmente a identificação de sinais pós-incidente que foram posteriormente associados ao ataque de ransomware — apresentou uma correlação com uma taxa de criptografia de 65%.

Os resultados deixam claro que os firewalls desempenham um papel fundamental na detecção de ataques de ransomware, com a telemetria desses dispositivos fornecendo valiosos sinais precoces da atividade do adversário. Quando combinada com informações de todo o ambiente de segurança, por exemplo, de soluções de proteção de endpoints ou segurança e-mail por meio de uma ferramenta XDR ou serviço MDR, a telemetria do firewall pode ajudar as equipes de defesa a detectar e bloquear ataques de ransomware antes que os dados sejam criptografados.

Impacto da identificação de ataques assistida por firewall na taxa de criptografia

	Identificou o ataque antes da implantação do ransomware	Identificou o ataque depois da implantação do ransomware	Não conseguiu identificar o ataque, nem antes nem depois da implantação do ransomware
Criminosos criptografaram seus dados com sucesso	50%	65%	71%
Criminosos não conseguiram criptografar seus dados	50%	35%	29%

Qual foi o papel do seu firewall na identificação do ataque? Os criminosos virtuais tiveram sucesso na criptografia de dados da sua organização no ataque de ransomware? n=2.158

Os firewalls ocupam uma posição privilegiada na infraestrutura organizacional, expondo a empresa a impactos mais significativos quando comprometida, em comparação com outras partes do ambiente. Se os adversários explorarem com sucesso uma vulnerabilidade no firewall, geralmente obterão amplo acesso a toda a empresa. A diferença nos valores dos resgates exigidos nesses cenários corrobora essa afirmação: **59% dos pedidos de resgate decorrentes de ataques iniciados com a exploração de uma vulnerabilidade no firewall são de US$ 1 milhão ou mais**, em comparação com 48% de todos os ataques.

NOVA PESQUISA

A relação entre identidade e ransomware

Uma das descobertas mais surpreendentes da pesquisa deste ano foi a confirmação da ligação direta entre ataques de identidade e ransomware. Entre as organizações que foram atingidas por ransomware no ano passado, dois terços (67%) confirmaram que o incidente de ransomware e o ataque de identidade mais significativo foram o mesmo evento. Embora nem todos os ataques tenham resultado em criptografia de dados, essa descoberta estabelece o comprometimento de identidade como um mecanismo predominante de distribuição de ransomware.

Divisão de dados: No último ano, a sua organização foi atingida por ransomware? n=5.000. Sua organização enfrentou alguma violação de segurança relacionada à identidade nos últimos 12 meses? n=5.000. [Se Sim em ambos os casos] O incidente de ransomware foi o mesmo evento que o seu ataque mais significativo relacionado à identidade?

Criptografia e recuperação de dados

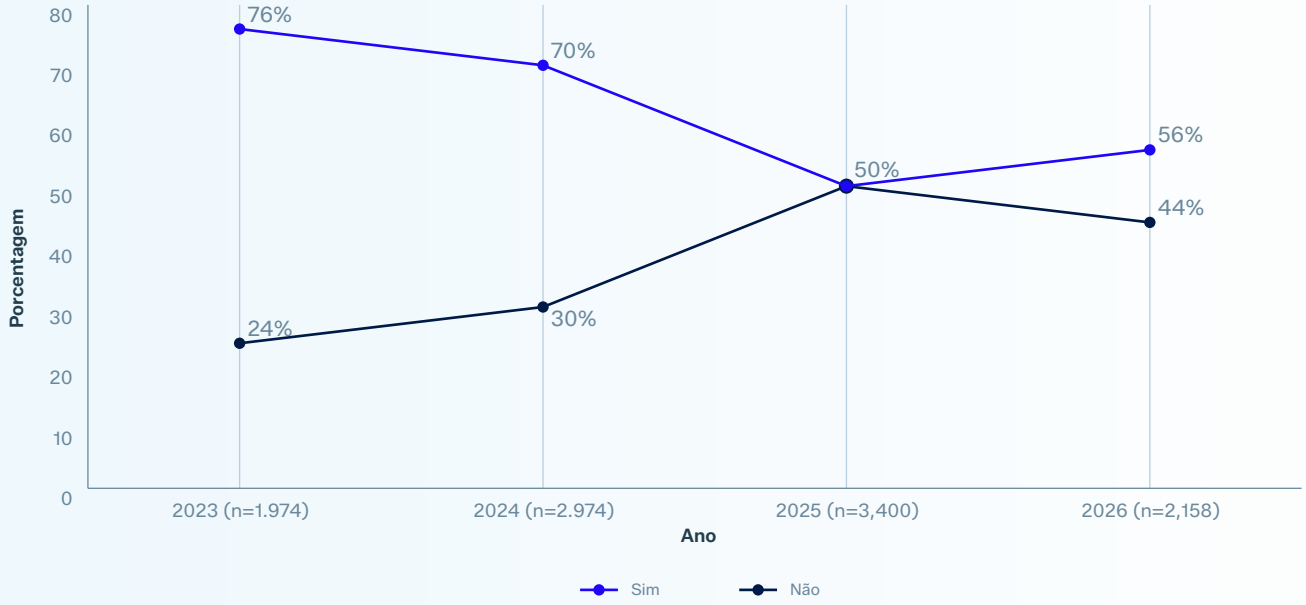
+6%

O aumento na taxa de criptografia por ransomware em relação ao relatório do ano passado.

Taxa de criptografia de dados

Mais da metade dos ataques de ransomware (56%) conseguiu criptografar dados. Isso inclui 40% de casos em que os dados foram apenas criptografados e 16% de casos em que os dados foram criptografados e roubados. 41% dos ataques foram interrompidos antes da criptografia, enquanto 2% envolveram ataques de extorsão sem criptografia.

Os dados foram criptografados durante o ataque? (Resumido: Sim/Não)

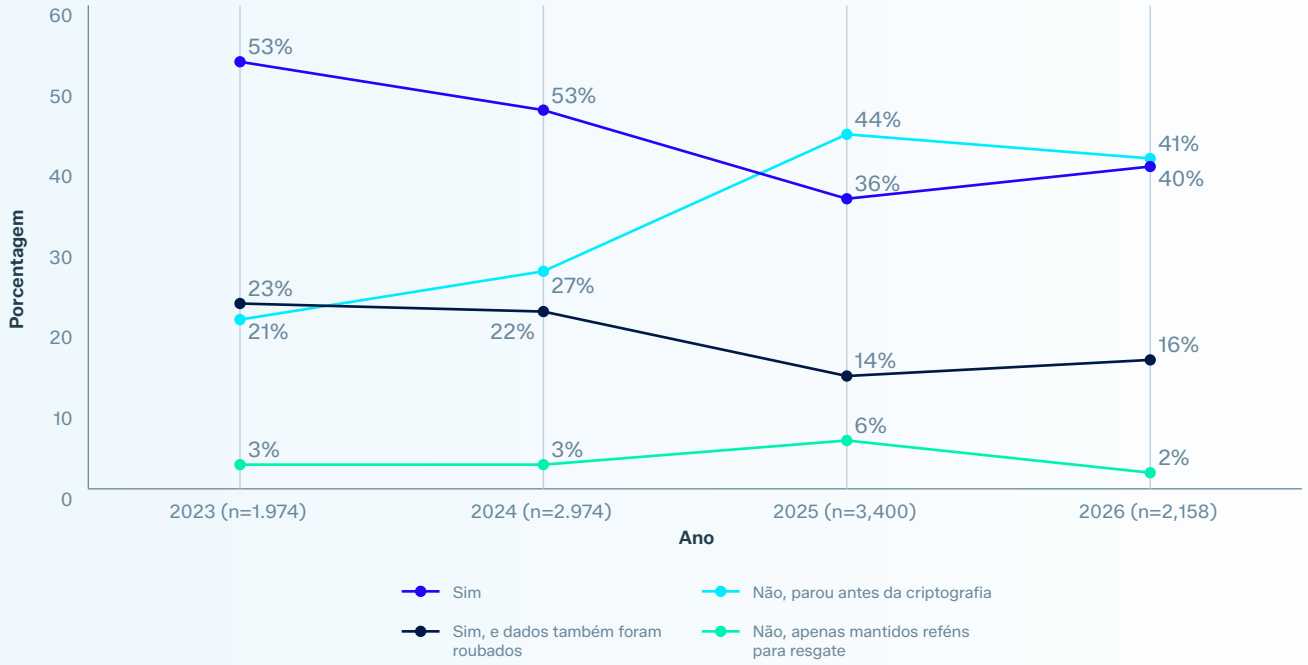


Os criminosos virtuais tiveram sucesso na criptografia de dados da sua organização no ataque de ransomware? Respostas resumidas: Sim/Não. Números de base no gráfico.

Embora a taxa de criptografia permaneça bem abaixo do pico de 76% registrado no relatório de 2023, ela apresentou uma leve alta em relação ao ponto mais baixo de 50% registrado no relatório de 2025. Essa reviravolta merece atenção: após dois anos de declínio no sucesso da criptografia, os invasores parecem estar recuperando terreno.

Os 16% de ataques que envolvem tanto criptografia quanto roubo de dados são particularmente preocupantes, pois esses ataques de duplo impacto oferecem aos invasores múltiplos pontos de alavancagem para extorsão.

Os dados foram criptografados durante o ataque?

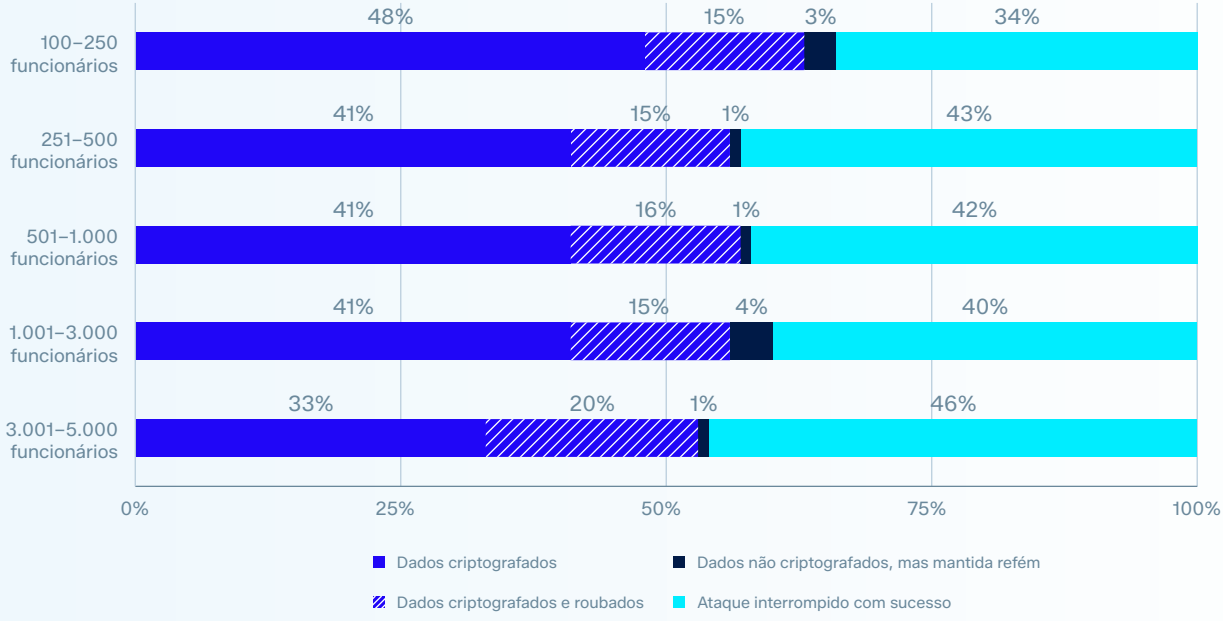


Os criminosos virtuais tiveram sucesso na criptografia de dados da sua organização no ataque de ransomware? (Lista completa de opções de resposta)
Base: organizações atingidas por ransomware. Números de base no gráfico.

Os resultados da criptografia variaram de acordo com o tamanho da organização, com **as maiores organizações pesquisadas (3.001 a 5.000 funcionários) apresentando maior probabilidade de impedir ataques antes da criptografia ou extorsão (46%)** em comparação aos apenas 34% de pequenas empresas (100 a 250 funcionários).

No entanto, quando os ataques conseguiram criptografar dados nas grandes organizações, as vítimas também ficaram mais propensas ao roubo de dados, com a taxa de "dados criptografados e roubados" chegando a 20% entre as empresas de grande porte, contra 15% da maioria das demais. A exfiltração de dados, além da implantação de ransomware, dá aos invasores uma segunda oportunidade de monetizar o ataque.

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=2.158

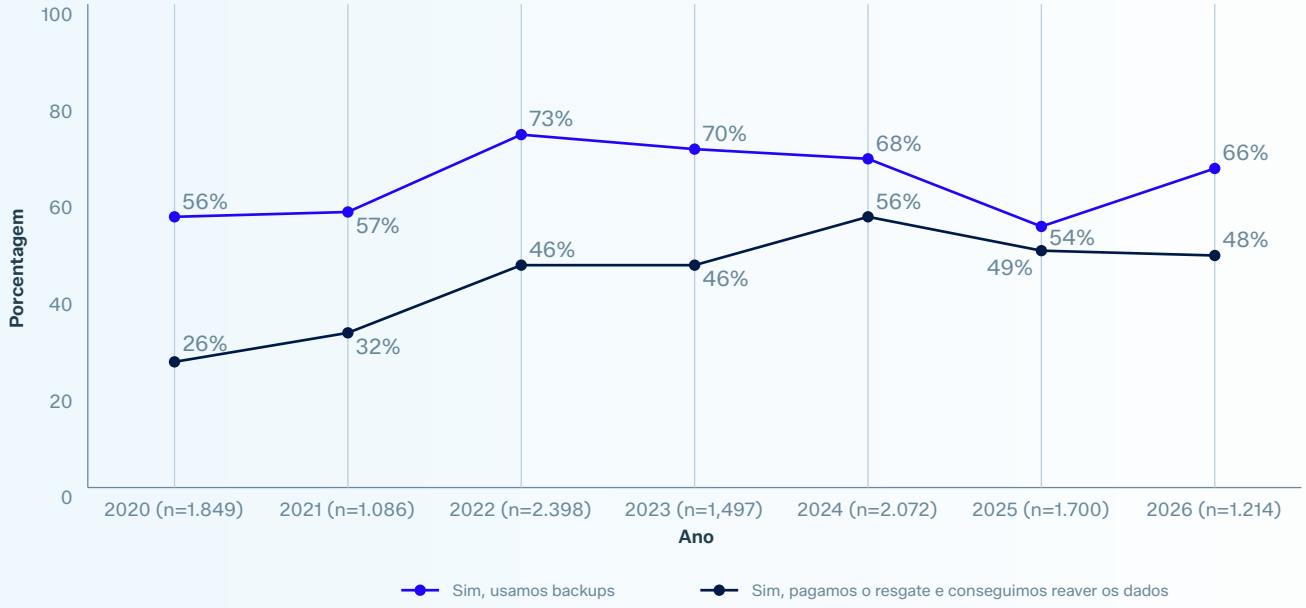
Como as organizações recuperaram dados criptografados

A recuperação baseada em backups subiu para 66% dos ataques em que os dados foram criptografados, em comparação com 54% no relatório de 2025. Essa forte recuperação sugere que as organizações reavaliaram seus investimentos em infraestrutura de backup após uma queda no uso em 2025 e que estão aumentando sua resiliência contra resgates.

+12%

O aumento do uso de backups para recuperar-se de ataques de ransomware entre 2025 e 2026.

Como sua organização recuperou os dados após ataques de ransomware?



Como sua organização recuperou os dados? Base: organizações que tiveram dados criptografados. Números de base no gráfico. São permitidas múltiplas respostas, portanto, as porcentagens podem ultrapassar 100%.

A proporção de organizações que pagaram o resgate para recuperar dados caiu para 48%, a taxa mais baixa dos últimos 3 anos. Apenas 2% das organizações relataram não ter recuperado nenhum dado, o que indica que, quando os dados são criptografados, a recuperação por algum meio é praticamente universal.

Pedidos de resgate e pagamentos

Pedidos de resgate

A mediana dos pedidos de resgate caiu para US$ 698.000 no relatório deste ano, dando continuidade a uma tendência de queda que já dura vários anos. Isso representa uma queda de 65% nos últimos dois anos. O valor médio dos pedidos de resgate também caiu nesse período, ficando em US$ 3.126.372, uma redução de 28% desde o relatório de 2024.

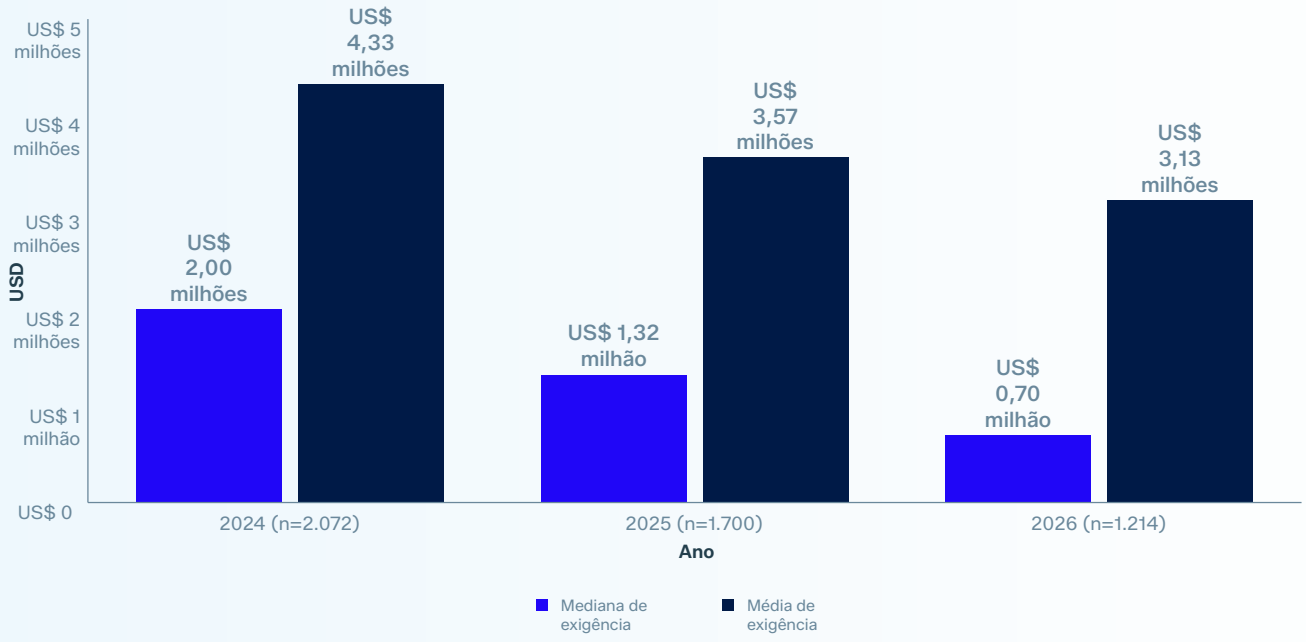
A crescente diferença entre a média e a mediana indica uma distribuição fortemente assimétrica: um pequeno número de grandes resgates infla a média, enquanto a organização típica enfrenta pedidos de resgate de pouco menos de US$ 700.000.

Observação: Valores de resgate atípicos, iguais ou superiores a 40 milhões de dólares, foram removidos desses dados.

US$ 698 mil

A mediana de pedido de resgate de ransomware no último ano.

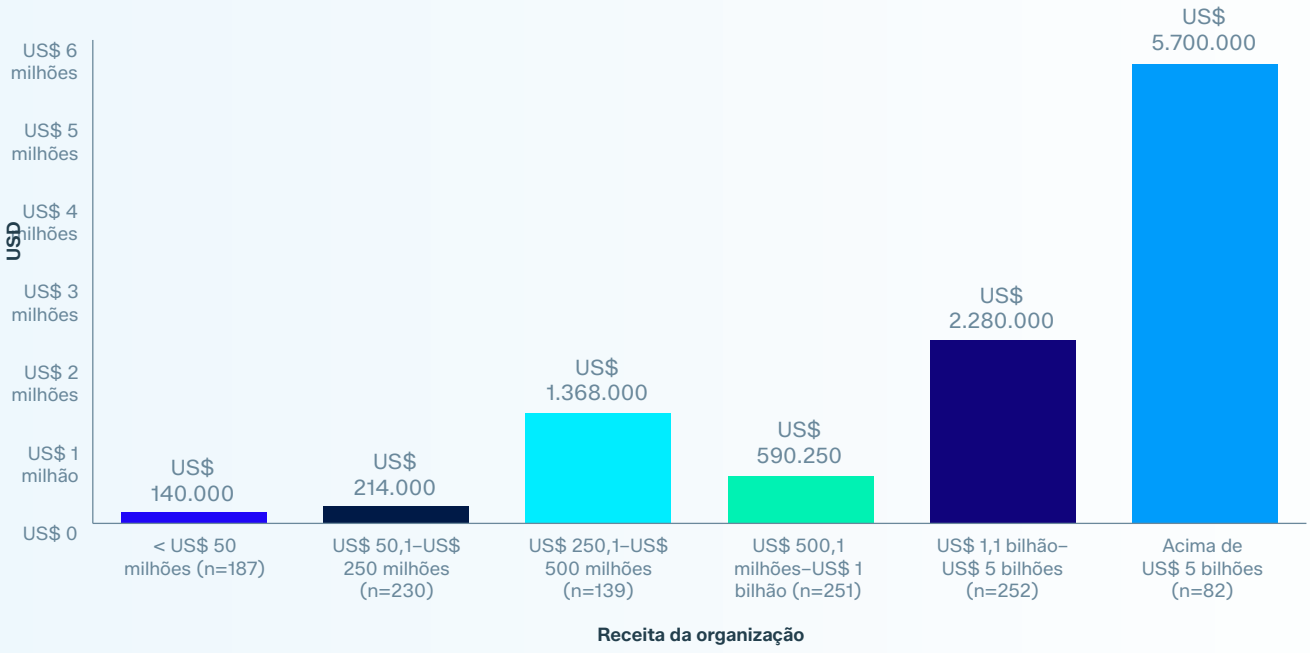
Valores médios e medianos das exigências de resgate



Qual foi o valor do pedido de resgate exigido pelos invasores? Base: organizações que tiveram dados criptografados. Números de base no gráfico. Exclui exigências atípicas de US$ 40 milhões ou mais.

O valor de resgate aumenta drasticamente de acordo com a receita da organização. Organizações com receita inferior a 50 milhões de dólares enfrentaram medianas de resgate de aproximadamente 140 mil dólares, enquanto aquelas com receita superior a 5 bilhões de dólares enfrentaram medianas de 5,7 milhões de dólares. Esse padrão sugere fortemente que os invasores realizam o reconhecimento para calibrar as exigências de resgate com base na percepção da capacidade de pagamento.

Valor mediano do pedido de resgate



Qual foi o valor do resgate exigido? Base: organizações que tiveram dados criptografados. Números de base no gráfico. Exclui exigências atípicas de mais de US$ 40 milhões.

Pagamentos de resgate

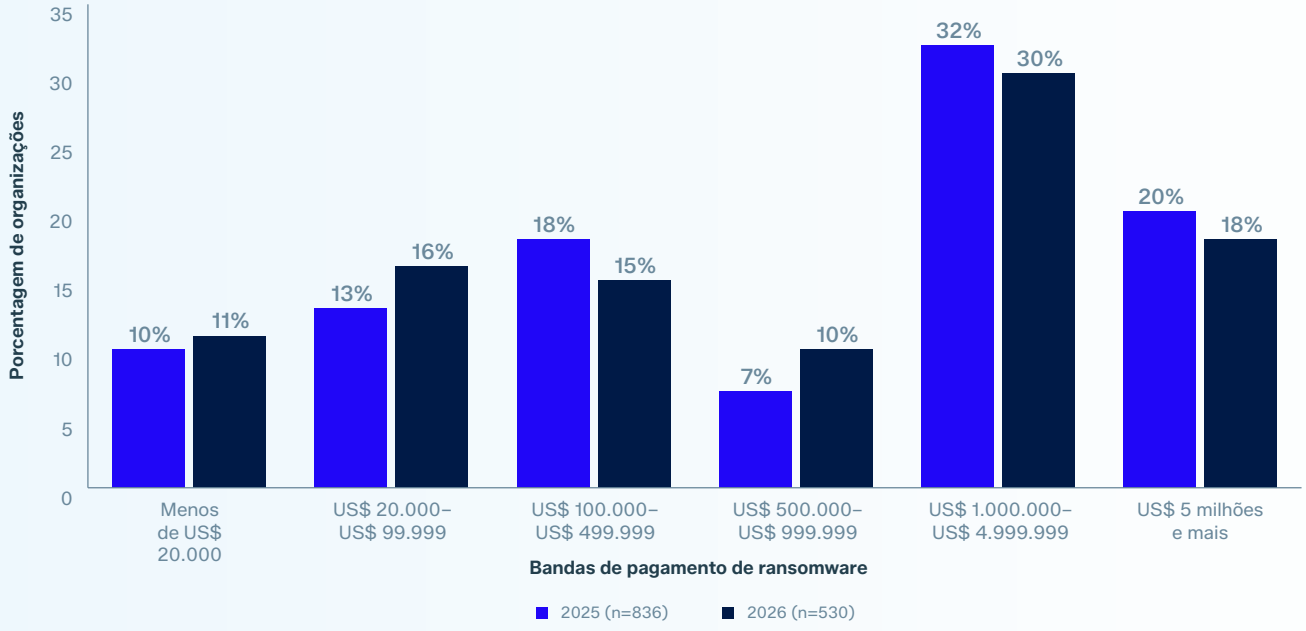
530 organizações que pagaram o resgate compartilharam o montante conosco, revelando que o valor mediano pago em resgates é agora de US$ 769.000, uma queda considerável em relação ao 1 milhão de dólares reportado no ano passado. Pouco menos da metade (48%) dos pagamentos foi de US$ 1 milhão ou mais, uma queda em relação aos 52% do ano anterior.

Ao analisar a distribuição completa dos pagamentos, observa-se uma clara mudança em direção ao meio da faixa de valores. As duas faixas de valores mais altas (US$ 1 milhão a US$ 5 milhões e US$ 5 milhões ou mais) apresentaram queda em relação ao relatório do ano passado, enquanto as faixas de US$ 20.000 a US$ 99.999 e de US$ 500.000 a US$ 999.999 apresentaram uma alta, sugerindo que invasores e vítimas estão cada vez mais se concentrando em pagamentos de valores baixos a médios.

US$ 769 mil

A mediana de pagamento de resgate de ransomware no último ano.

Bandas de pagamento de ransomware

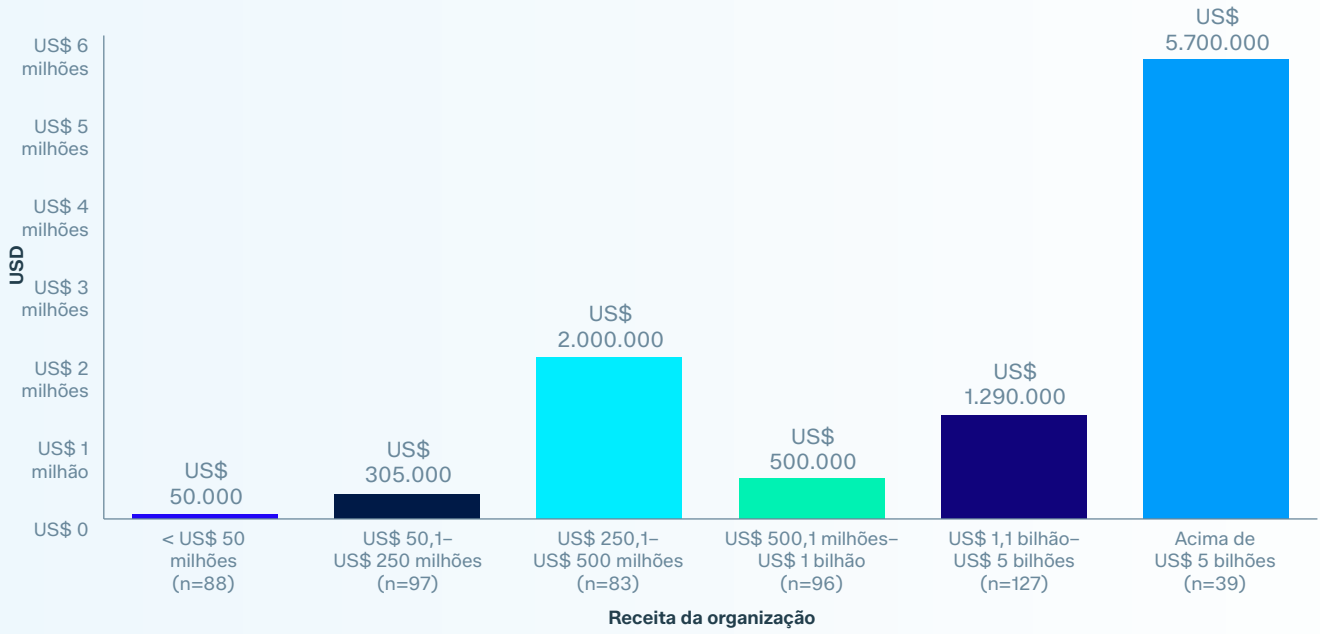


Qual foi o pagamento de resgate que foi efetuado aos invasores? Números de base no gráfico.

A divisão dos pagamentos de resgate pela receita da organização mostrou um pico na faixa de US$ 250,1 milhões a US$ 500 milhões, com as vítimas pagando uma mediana de US$ 2 milhões. Isso representa mais do que qualquer outro segmento, com exceção dos maiores (receita anual acima de US$ 5 bilhões), e é quatro vezes maior do que para organizações com receita entre US$ 500,1 milhões e US$ 1 bilhão.

Os dados sobre pedidos de resgate mostram um pico semelhante, atingindo a faixa de receita de US$ 250,1 milhões a US$ 500 milhões, com médias de pedidos de resgate de US$ 1,37 milhão em comparação com US$ 590 mil da faixa acima, o que sugere que esse segmento está particularmente exposto aos impactos de ataques de ransomware.

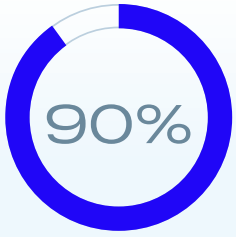
Mediana de pagamento de resgate



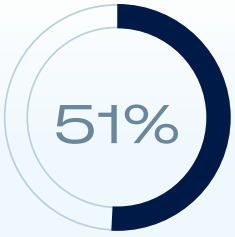
Qual foi o pagamento de resgate que foi efetuado aos invasores? Base: organizações que pagaram o resgate. Números de base no gráfico.

Pagamentos reais versus exigências iniciais

507 organizações compartilharam tanto o valor do resgate exigido quanto o valor pago, revelando a eficácia das organizações em negociar com os invasores. **O pagamento mediano foi de 90% dos valores exigidos (média: 85%)**, com pouco mais da metade (51%) pagando menos do que a exigência inicial, 30% pagando o real pedido de resgate e 18% pagando mais. Esses números são muito próximos dos do ano passado, revelando que a relação entre pedidos de resgate e pagamentos efetivos permaneceu relativamente estável.

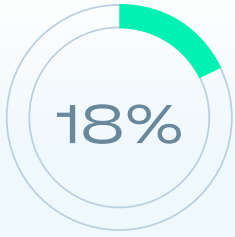


A porcentagem **mediana** de pagamento de resgate



Pagamentos **inferiores** ao pedido de resgate inicial

Pagamentos que se **equipararam** ao pedido de resgate inicial



Pagamentos **superiores** ao pedido de resgate inicial

Qual foi o valor do pedido de resgate exigido pelos invasores? Qual foi o pagamento de resgate que foi efetuado aos invasores? Base: organizações que compartilharam o valor do pedido de resgate e o valor do pagamento de resgate. n=507

Conforme mencionado acima, os valores médios de resgate exigidos geralmente sobem quando a organização visada apresenta maior receita, mas diferentes faixas de receita apresentam níveis variados de sucesso na negociação de valores finais mais baixos.

Organizações de médio porte (receita de US$ 50 milhões a US$ 250 milhões) são as que menos conseguem reduzir os pagamentos de resgate, com 25% delas pagando mais do que o exigido. As grandes maiores (receita acima de US$ 5 bilhões) são as mais eficientes na negociação de resgates menores, com 11% pagando mais do que o valor inicial exigido e 57% pagando menos — a maior porcentagem entre todos os grupos.

As organizações com maior receita (acima de US$ 500 milhões) tiveram mais sucesso em pagar valores inferiores ao exigido pelo resgate, indicando que, para resgates mais altos, os invasores estavam mais dispostos a conceder descontos. Organizações com receita inferior a US$ 50 milhões também obtiveram sucesso moderado na redução dos pagamentos de resgate.

Percentual de resgate pago (mediana) pela receita da organização

Receita	Proporção do resgate pago (Mediana)
< US$ 50 milhões	95%
US$ 50,1 a US$ 250 milhões	100%
US$ 250,1 a US$ 500 milhões	100%
US$ 500,1 milhões a US$ 1 bilhão	83%
US$ 1,1 bilhão a US$ 5 bilhões	83%
US$ 5 bilhões ou mais	83%

Qual foi o valor do pedido de resgate exigido pelos invasores? Qual foi o pagamento de resgate que foi efetuado aos invasores?
Base: organizações que compartilharam o valor do pedido de resgate e o valor do pagamento de resgate. n=507

Pagamentos de resgate por setor

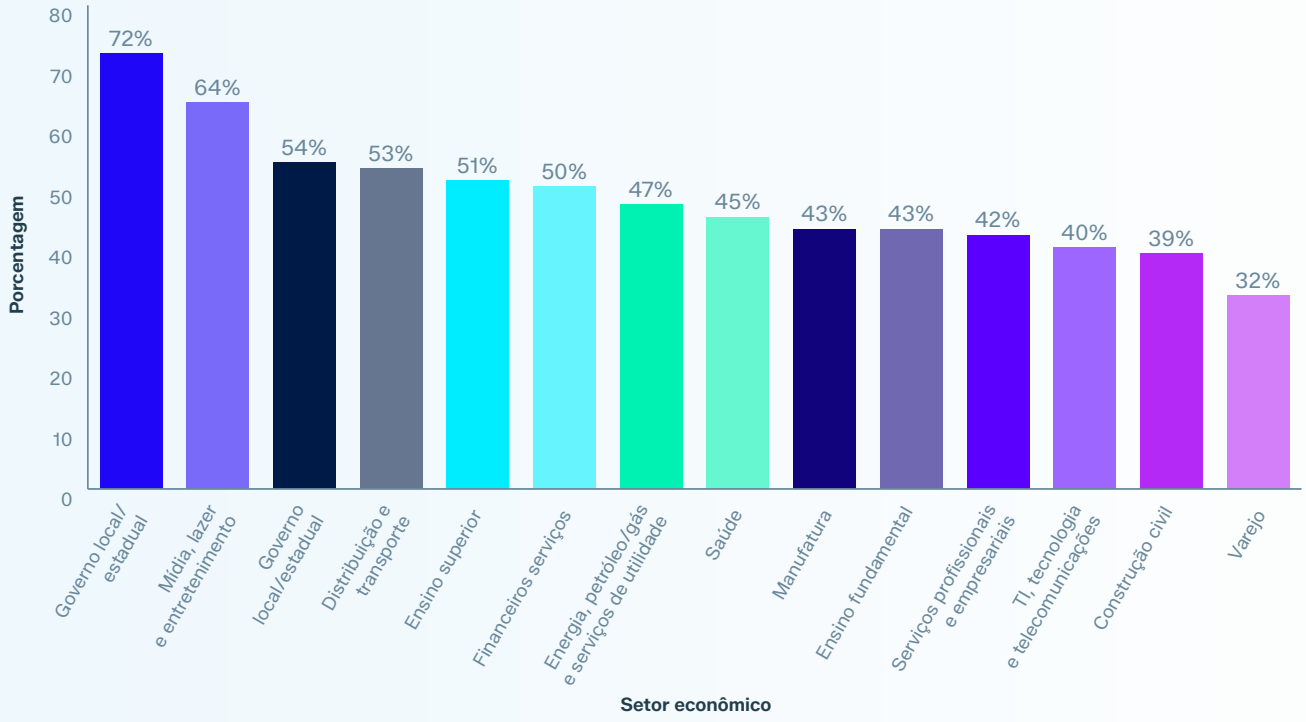
A propensão de pagar o resgate varia por setor. **Governo local/estadual (72%) e o setor de mídia, lazer e entretenimento (64%) foram os mais propensos a pagar o resgate**, relatando mais que o dobro da taxa do setor de varejo (32%).

Organizações do setor público e de mídia frequentemente enfrentam forte pressão para restabelecer rapidamente serviços essenciais ao cidadão ou serviços que exigem agilidade, enquanto organizações do setor varejista podem estar mais dispostas a "esperar a tempestade passar".

Varejo

foi o setor com a menor incidência de pagamento em resposta a ataques de ransomware (32%).

Percentual de organizações que pagaram o resgate por setor



Como sua organização recuperou os dados? Pagamos o resgate. Base: organizações que tiveram dados criptografados. n=1.214

Impacto nos negócios e nas pessoas

Custos de recuperação de ransomware

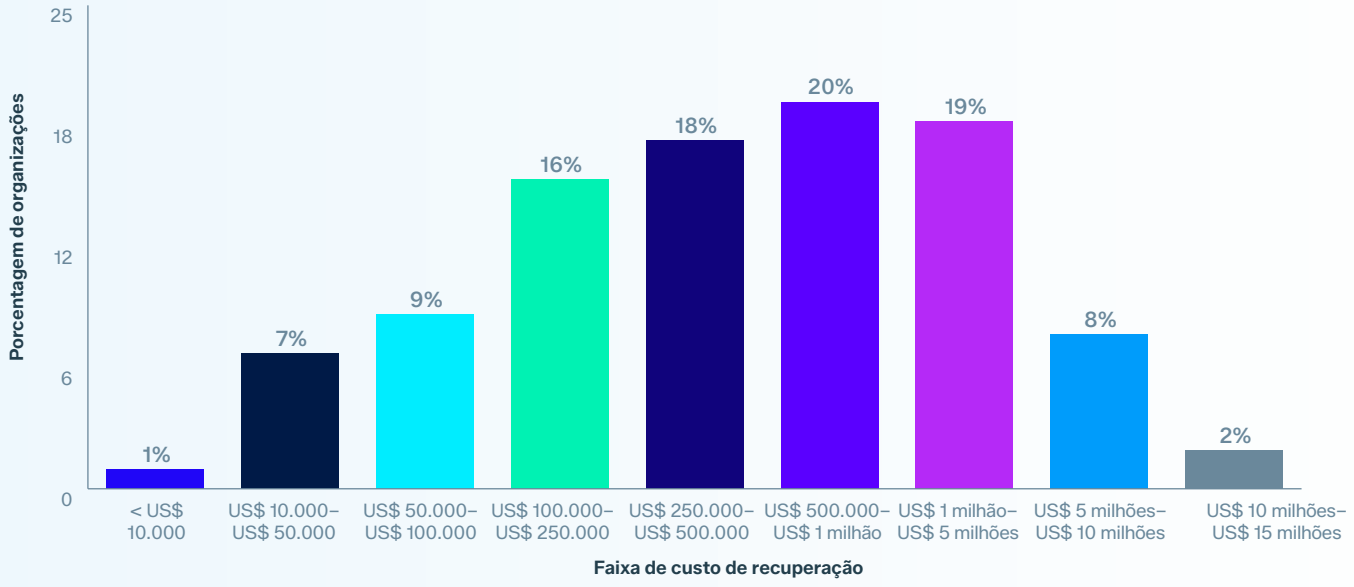
O custo médio para recuperação de um ataque de ransomware, excluindo resgates pagos, foi de US$ 1.700.200 no ano passado. Isso representa um aumento de 11% em relação à média de US$ 1.525.716 do relatório de 2025, mas permanece 38% abaixo do pico de US$ 2.730.684 registrado no relatório de 2024. O custo mediano é de US$ 375.000, inalterado em relação ao relatório do ano passado.

2024	2025	2026
US$ 2,73 milhões	US$ 1,53 milhões	US$ 1,70 milhões

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=2.158 (2026), n=3.400 (2025), 2.974 (2024)

Os custos de recuperação variam bastante: 20% das organizações tiveram

Os custos de recuperação de ataques de ransomware



Qual foi o custo aproximado para sua organização para remediar os impactos do ataque de ransomware mais significativo? n=2.158

Tempo de recuperação

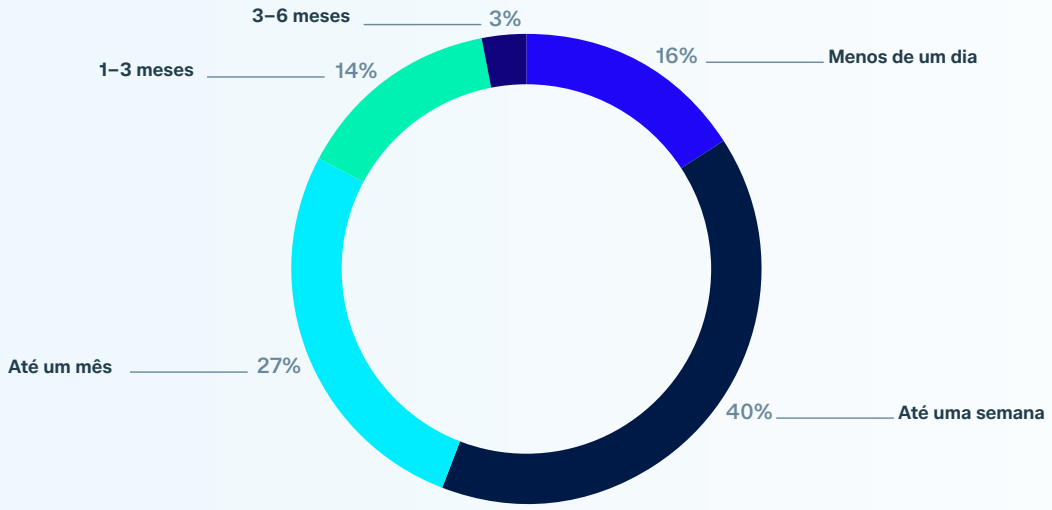
Mais da metade das organizações (55%) se recuperaram do ransomware em uma semana (16% em menos de um dia) e 83% se recuperaram em um mês. Apenas 3% levaram mais de três meses.

A taxa de recuperação de 55% em uma semana representa um aumento de 3% em relação ao ano anterior. O número médio de semanas para recuperação permaneceu em três (relatórios de 2025 e 2026), abaixo das cinco semanas registradas no relatório de 2024.

55%

Porcentagem de organizações que se recuperaram do ataque de ransomware em uma semana.

Quanto tempo levou para se recuperar



Quanto tempo a sua organização levou para se recuperar por completo do ataque de ransomware? n=2.158

Impacto humano do ransomware

Praticamente todas as organizações que tiveram dados criptografados (99%) relataram repercussões duradouras em suas equipes de TI e segurança cibernética. Os impactos mais citados foram o aumento de ansiedade e estresse sobre ataques futuros (41%) e o aumento da pressão por parte dos líderes seniores (40%). Mais de uma em cada cinco vítimas (21%) tiveram a equipe de liderança substituída como resultado direto do ataque.

O aumento do reconhecimento pelos líderes seniores foi o único impacto que cresceu em relação ao ano anterior, subindo de 31% para 36%. Todas as outras repercussões medidas diminuíram, incluindo mudanças das prioridades da equipe (queda de sete pontos), aumentos contínuos na carga de trabalho (queda de sete pontos) e reestruturação da equipe (queda de cinco pontos).

21%

A porcentagem de equipes de liderança de TI e segurança cibernética que foram substituídas devido ao ataque de ransomware.

Como o ransomware afetou as equipes de TI e segurança cibernética

Repercussões	2026	Mudança de 2025
Aumento em ansiedade e estresse sobre ataques futuros	41%	-
Aumento da pressão por parte dos líderes seniores	40%	-
Aumento do reconhecimento pelos líderes seniores	36%	↑ 5pp
Mudanças na estrutura organizacional/da equipe	32%	↓ 5pp
Mudança das prioridades/foco da equipe	32%	↓ 6pp
Sentimento de culpa porque o ataque não foi interrompido	31%	↓ 3pp
Aumento contínuo na carga de trabalho	31%	↓ 7pp
Licença de pessoal devido a problemas de estresse e saúde mental	29%	↓ 2pp
A liderança da equipe foi substituída.	21%	↓ 4pp

Qual a repercussão que o ataque de ransomware teve nas pessoas em sua equipe de TI e segurança cibernética, se alguma?
Base: organizações que tiveram dados criptografados. n=1.214 (2026), n=1.700 (2025)

O aumento do reconhecimento por parte dos executivos pode, por si só, ser um fator que contribuiu para as tendências operacionais positivas observadas em outras partes deste relatório, uma vez que uma maior atenção da liderança pode se traduzir em melhores recursos e apoio organizacional para os programas de segurança cibernética

Recomendações

Reforce a segurança da identidade como uma defesa contra ransomware. Dois terços das vítimas de ransomware confirmaram que o incidente ocorreu no mesmo evento que o ataque de identidade mais significativo que sofreram, o que reforça a forte ligação entre comprometimento de identidade e ransomware. As organizações devem priorizar a detecção e resposta a ameaças de identidade (ITDR), impor a autenticação multifator em todos os pontos de acesso e auditar regularmente as credenciais de identidade, tanto humanas quanto não humanas. Conforme demonstraram os resultados da pesquisa (97% das organizações haviam habilitado a MFA de alguma forma no momento do ataque), a MFA não é suficiente para bloquear ataques, sendo necessário habilitá-la de forma geral.

Reforce a proteção de endpoints para modelos de IA fronteiriça. A IA fronteiriça está acelerando a descoberta e a exploração de vulnerabilidades. Ter defesas robustas nos endpoints que bloqueiem automaticamente ataques baseados em exploits é essencial.

Recorra ao suporte especializado de MDR. A falta de capacidade, habilidades e conhecimento especializado é um tema recorrente tanto para pequenas e médias empresas quanto para grandes corporações. Lidar com ameaças aumentadas por IA exercerá ainda mais pressão sobre essas áreas, à medida que os profissionais de segurança tentam se manter atualizados com a tecnologia de IA em rápida evolução. A menos que você tenha confiança em sua capacidade de formar uma equipe interna de operações de segurança, considere trabalhar com um especialista externo para preencher essa lacuna, seja diretamente com um fornecedor de MDR com cobertura 24 horas por dia, 7 dias por semana, ou com um provedor de serviços gerenciados. Fornecedores que conseguirem resolver mais incidentes de ponta a ponta com IA e automação também serão um fator multiplicador que poderá ajudar a preencher as lacunas de competências e capacidade.

Priorize a segurança de e-mail. Considerando que phishing e e-mails maliciosos representam agora metade de todas as causas primárias de ransomware neste relatório, as organizações deveriam implantar filtragem de e-mail avançada, implementar os protocolos DMARC/DKIM/SPF e investir em treinamento regular de conscientização sobre phishing. A mudança para ataques baseados em e-mail sugere que a aplicação de patches de vulnerabilidades técnicas por si só é insuficiente.

Invista em infraestrutura de backup e recuperação. Organizações que mantiveram sistemas de backup robustos recuperaram dados criptografados em taxas quase recordes no último ano. Os backups devem ser testados regularmente, armazenados offline ou em formatos imutáveis e integrados a um plano de resposta a incidentes documentado que possa ser executado sob pressão.

Mantenha programas de gerenciamento de exposição. A queda de 14 pontos percentuais na exploração de vulnerabilidades como causa primária é encorajadora, mas esses ataques continuam sendo um importante vetor de ataque e provavelmente aumentarão à medida que os modelos de IA fronteiriça encontrarem novas vulnerabilidades mais rapidamente. As organizações devem manter uma frequência rigorosa de aplicação de patches e concentrar-se em medidas de mitigação, incluindo segmentação, Zero Trust Network Access e implementações de MFA/autenticação contínua.

Reduza a exposição através do firewall e utilize a telemetria do firewall para detectar ataques precocemente. Garanta que seu firewall receba atualizações rápidas — o ideal seria recebê-las automaticamente — e minimize serviços expostos à internet, como acesso administrativo e portais de usuários. Conecte firewalls a soluções XDR e MDR para habilitar a telemetria de firewall e ajudar a detectar ataques de ransomware antes que as cargas maliciosas sejam implantadas.

Dê suporte às equipes de segurança cibernética durante o período pós-ataque. Com 99% das equipes afetadas relatando repercussões, o custo humano do ransomware é praticamente universal. As organizações devem estabelecer protocolos claros de suporte pós-incidente e garantir que o crescente reconhecimento da alta administração se traduza em investimento contínuo em pessoas, não apenas em tecnologia.

Conclusão

O Estado do Ransomware 2026 revela um cenário de ameaças em transição.

Há sinais reais de progresso: os pedidos de resgate e pagamentos estão caindo, a recuperação baseada em backups atingiu níveis quase recordes e as organizações estão cada vez mais eficazes na negociação quando decidem pagar. A queda drástica nos ataques que exploram vulnerabilidades sugere que a descoberta orientada por IA e o investimento contínuo no gerenciamento de patches estão dando resultados positivos.

O sinal mais encorajador nos dados pode ser o aumento do reconhecimento das equipes de segurança cibernética por parte da alta administração. Quando a liderança presta atenção, os recursos aparecem. As tendências operacionais positivas neste relatório, desde a melhoria na utilização de backups até negociações mais bem-sucedidas, podem refletir exatamente essa dinâmica.

Ainda assim, os desafios que permanecem são significativos. Mais da metade dos ataques de ransomware conseguem criptografar dados, os custos de recuperação chegam a uma média de US$ 1,7 milhão por incidente e o impacto humano nas equipes de segurança cibernética é quase universal.

A constatação de que dois terços das vítimas de ransomware atribuíram o incidente a um comprometimento de identidade **ressalta o papel crucial que a segurança de identidade desempenha na cadeia de defesa contra ransomwares**. Organizações que tratam a identidade como uma camada fundamental de segurança, em vez de uma reflexão póstuma, estão em melhor posição para impedir que os ataques frutifiquem.

As organizações também precisam se preparar para **o principal desafio de segurança cibernética da próxima década: as ameaças aumentadas por IA**. Os dados já indicam o por quê: 62% das vítimas citaram uma lacuna de segurança, conhecida ou desconhecida, como um fator de ataque, e 58% apontaram para a falta de pessoal ou de habilidades. Ambas as lacunas tornam-se mais relevantes à medida que a IA acelera a velocidade e a escala dos ataques, com os adversários usando a IA para encontrar vulnerabilidades mais rapidamente e orquestrar ataques a múltiplos pontos de controle na velocidade da máquina.

O padrão observado nas descobertas deste ano, que vão de melhores resultados quando os firewalls detectaram ataques precocemente até o aumento na recuperação baseada em backups, aponta para uma direção consistente: **quando as defesas operam em conjunto, em vez de isoladamente, os resultados melhoram**. Reduzir a lacuna nos ataques da era da IA dependerá menos da adição de mais ferramentas e mais da conexão das que já existem, para que o contexto, a detecção e a resposta possam acompanhar a velocidade exigida pelas ameaças atuais.

As organizações que melhor se sairão contra ransomwares nos próximos anos serão aquelas que mantiverem a atenção da alta administração no quesito, adotando sistemas de defesa integrados e baseados em IA e investindo não apenas em tecnologia e processos, mas também nas pessoas que defendem contra essas ameaças diariamente.

Metodologia

Esta pesquisa foi realizada pela Vanson Bourne em nome da Sophos no primeiro trimestre de 2026. Foram entrevistados 2.158 tomadores de decisão de TI e segurança cibernética das organizações que sofreram ataques de ransomware nos 12 meses anteriores, em 17 países. EUA, Brasil, Chile, Colômbia, México, Reino Unido, França, Alemanha, Itália, Espanha, Suíça, Austrália, Índia, Japão, Cingapura, África do Sul e Emirados Árabes Unidos. Os participantes pertenciam a organizações com 100 a 5.000 funcionários, distribuídas em 15 setores de atividade.

SOPHOS

Para saber mais sobre ransomware e como a Sophos pode ajudar a defender a sua organização, visite nosso site.

Vendas na América Latina
E-mail: latamsales@sophos.com

Vendas no Brasil
E-mail: brasil@sophos.com

2026-06-09 PTBR (DD)