SOPHOS

O ESTADO DO RANSOMWARE NO VAREJO 2025

Resultados de uma pesquisa independente com 3.400 líderes de TI e segurança cibernética, incluindo 361 profissionais do setor de varejo, distribuídos em 16 países e cujas organizações foram atingidas por ransomware no último ano.

Documento técnico Sophos. 2025 Ago

Apresentação

Bem-vindos à quinta edição do relatório anual da Sophos, O Estado do Ransomware no Varejo, que expõe a realidade dos ransomwares para as organizações de varejo em 2025.

O relatório deste ano revela como as experiências com ransomware dos varejistas, tanto causas como consequências, evoluíram no último ano. Também elucida áreas previamente inexploradas, incluindo fatores operacionais que deixaram as organizações do varejo expostas aos ataques e o impacto humano dos incidentes nas equipes de TI e segurança cibernética varejista.

Baseado em experiências reais de 361 líderes de TI e segurança cibernética do setor do varejo distribuídos em 16 países e cujas organizações foram atingidas por ransomware no último ano, o relatório oferece insights únicos sobre:

- Por que as organizações do varejo se tornam vítimas de ransomware
- O que acontece aos dados
- Pedidos de resgate 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, que, no caso, é 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 361 entrevistados do varejo estavam distribuídos em 16 países, assegurando que os resultados do estudo reflitam a grande diversidade e abrangência de experiências. O relatório inclui comparações ano a ano, justapondo 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 do setor varejista apontaram a **exploração de vulnerabilidades** como a causa técnica primária mais comum dos ataques, usada em 30% dos incidentes.
- Fatores multioperacionais contribuem para que as organizações do varejo sejam vítimas de ransomware, sendo o mais comum as **lacunas de segurança das quais a organização não tinha conhecimento**, citada por 46% das vítimas. Seguido bem de perto pela **falta de expertise,** fator que contribuiu para 45% dos ataques (o mais alto índice registrado dentre todos os setores estudados). Em terceiro lugar ficou a **falta de proteção**, que contribuiu para 44% dos ataques.

O que acontece aos dados

- A taxa de **criptografia de dados** no setor de varejo atingiu o seu nível mais baixo em cinco anos, com 48% dos ataques resultando na criptografia de dados, valor inferior ao pico de 71% em 2023.
- 29% das organizações de varejo que tiveram dados criptografados também passaram pela **exfiltração de dados**.
- 98% das organizações de varejo que tiveram os dados criptografados conseguiram recuperá-los.
- O uso de **backups** pelos varejistas para restaurar dados criptografados atingiu o seu nível mais baixo dos últimos quatro anos: 62% dos incidentes utilizaram backups.
- 58% das vítimas do varejo **pagaram o resgate** para reaver os dados. Ainda que represente uma leve queda dos 60% do ano anterior, foi o segundo índice de pagamento de resgate mais alto em cinco anos.

Resgates: exigências e pagamentos

- A média (mediana) do **pedido de resgate** exigido das organizações do varejo dobrou no último ano, chegando a US$ 2 milhões em 2025 em comparação a US$ 1 milhão em 2024. O fator primário por trás dessa variação significativa foi o aumento de 59% em pagamentos de resgates de US$ 5 milhões ou mais: de 17% de pagamentos efetuados em 2024 para 27% em 2025.
- Apesar disso, a média (mediana) do **pagamento de resgate** subiu em apenas 5% no último ano, de US$ 950 mil em 2024 para US$ 1 milhão em 2025. Isso sugere que as organizações de varejo estão resistindo mais às inflacionadas demandas de regaste.
- A **proporção de resgates pagos** pelos varejistas caiu de 85% em 2024 para 81% in 2025.
- Examinando em mais detalhes as **exigências versus pagamentos**, apenas 29% dos varejistas disseram que pagaram o pedido inicial de resgate. 59% pagaram menos do que o valor inicial, enquanto 11% pagaram mais.

Impacto comercial do ransomware

- A média de **custo para as organizações de varejo se recuperarem** de um ataque de ransomware caiu 40% no último ano, chegando a US$ 1,65 milhão em comparação a US$ 2,73 milhões em 2024.
- Analisando a **velocidade de recuperação**, as organizações de varejo estão se recuperando mais rapidamente, com 51% delas recuperadas em uma semana em 2025 em comparação a 46% em 2024.

Impacto humano do ransomware

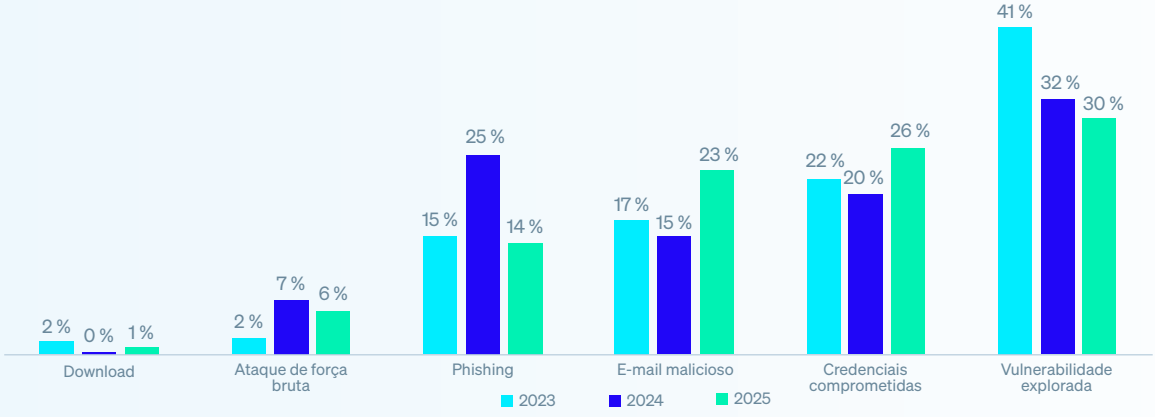
- Todas as organizações de varejo que tiveram os dados criptografados disseram ter havido **repercussões diretas** para as equipes de TI e segurança cibernética:
  - Quase metade (47%) das equipes de TI e segurança cibernética do varejo disseram ter havido **aumento da pressão** pelos líderes seniores, enquanto 30% relataram o **aumento de reconhecimento**.
  - 43% dos entrevistados do varejo citaram o aumento em ansiedade ou estresse sobre ataques futuros e um **aumento contínuo** na carga de trabalho como fatores de impacto em suas equipes de TI e segurança cibernética.
  - 41% relataram mudanças à **estrutura organizacional/da equipe** como uma consequência do incidente.
  - 37% das equipes passaram por períodos de **licença de pessoal** devido a problemas de estresse e saúde mental relacionados ao ataque.
  - Um terço (34%) disseram que a equipe ficou com **sentimento de culpa** porque o ataque não foi interrompido a tempo.
  - Em um quarto dos casos (26%), as equipes tiveram a **liderança substituída** por causa do ataque.

Por que as organizações se tornam vítimas de ransomware

Causas técnicas primárias dos ataques

Pelo terceiro ano consecutivo, as vítimas do varejo apontaram a exploração de vulnerabilidades como a causa primária mais comum dos incidentes de ransomware, usada para se infiltrar em 30% dos ataques às organizações. O comprometimento de credenciais permanece sendo o segundo vetor de ataque mais comum, com a porcentagem de ataques que utilizou essa abordagem aumentando de 20% em 2024 para 26% em 2025. O e-mail mantém a *poli position* entre os vetores de ataque, com 23% dos varejistas relatando o phishing como causa primária (uma salto imenso dos 15% relatados em 2024) e outros 14% mencionando os e-mails maliciosos.

Gráfico 1: Causa técnica primária dos ataques de ransomware no varejo 2023 – 2025



Você sabe a causa primária do ataque de ransomware que a sua organização enfrentou no último ano? Sim. n=359 (2025), 261 (2024), 243 (2023).

A pesquisa revela que as causas primárias variam por setor, mas a exploração de vulnerabilidades é apontada como o maior vetor de ataque pela maioria dos setores. Vale ressaltar aqui:

- O **phishing** foi a causa primária mais comum citada por instituições de **ensino básico** (22%) e fornecedores de **energia, petróleo/gás e serviços de utilidade** (29%).
- O **comprometimento de credenciais** foi o vetor de ataque mais observado pelas organizações do **governo local/estadual**, atribuído a quase um terço dos incidentes (32%).

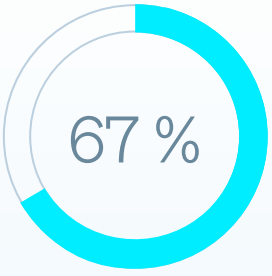
Gráfico 2: Causa técnica primária dos ataques de ransomware dividida por setor

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

Causa organizacional primária dos incidentes no varejo

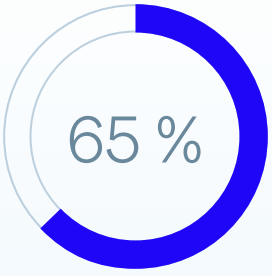
O relatório deste ano explora, pela primeira vez, os fatores organizacionais que deixaram as organizações do varejo expostas aos ataques. Os resultados revelam que as vítimas no setor do varejo geralmente estão enfrentando várias dificuldades organizacionais, com os entrevistados citando 2,9 fatores, em média, que contribuíram para que se tornassem vítimas do ataque de ransomware.

No geral, as causas organizacionais primárias são distribuídas igualmente entre problemas de proteção, dificuldades com recursos e lacunas de segurança. Contudo, as organizações de varejo estão um pouco mais propensas a apontar a lacuna de segurança (conhecida e desconhecida) como o fator primário.



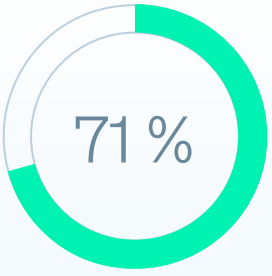
Desafios à proteção

Falta de proteção ou baixa qualidade das soluções de proteção que inviabilizou a interrupção do ataque



Problemas de recursos

Falta de expertise humana (habilidades ou capacidade) para detectar e interromper o ataque em tempo hábil



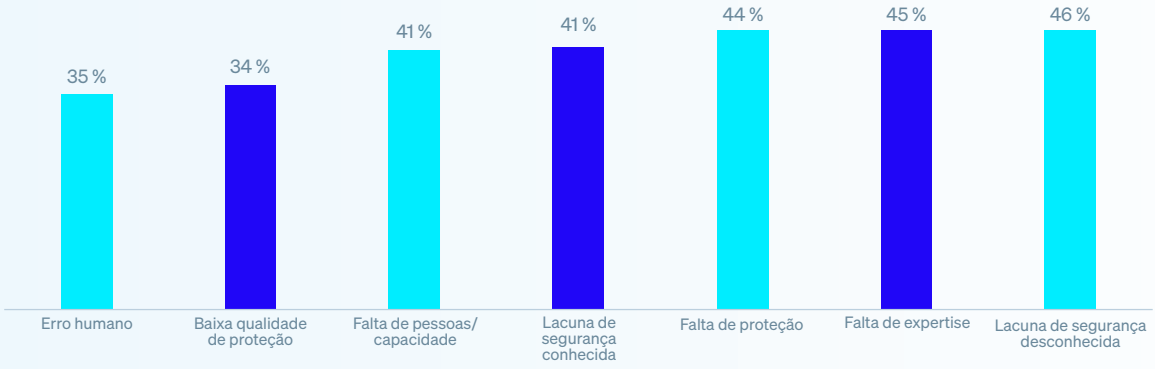
Lacuna de segurança

Presença de pontos fracos conhecidos ou desconhecidos em suas defesas

Por que você acha que a sua organização foi vítima de um ataque de ransomware? n=361. Respostas consolidadas.

Lacunas de segurança desconhecidas (ou seja, pontos fracos na defesa dos quais a organização não tinha conhecimento) são o motivo mais comum, apontado por 46% dos entrevistados. Logo em seguida temos a **falta de expertise** (ou seja, habilidades ou conhecimento insuficientes para interromper um ataque em tempo hábil), que contribuiu para 45% dos ataques — a mais alta taxa registrada entre todos os setores referente a essa causa organizacional primária em particular. Em terceiro lugar ficou a falta de proteção (ou seja, não ter os produtos e serviços de segurança cibernética necessários em operação), que contribuiu para 44% dos ataques.

Gráfico 3: Causa operacional primária dos ataques de ransomware nas organizações de varejo



Por que você acha que a sua organização foi vítima de um ataque de ransomware? n=361.

Causa organizacional primária por setor

A causa organizacional primária mais comum também 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 4: Principal causa operacional primária dos ataques de ransomware por setor

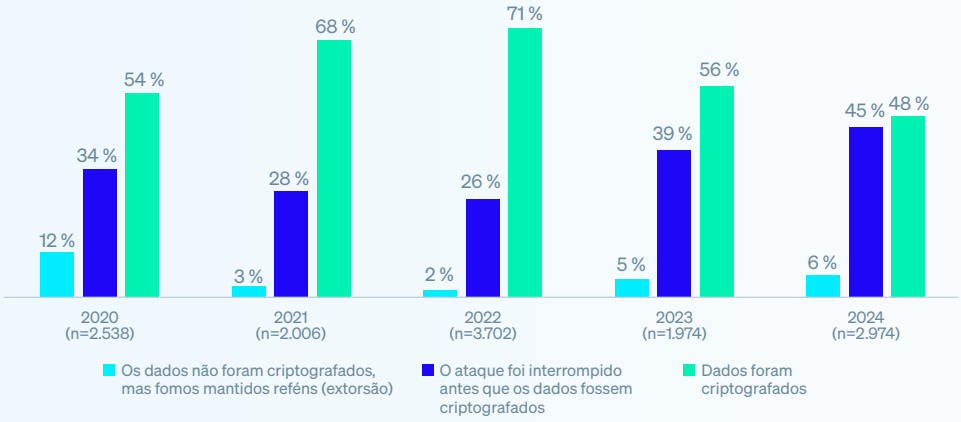
Por que você acha que a sua organização foi vítima de um ataque de ransomware? n=3.400. Distribuída por setor.

O que acontece aos dados

Criptografia de dados no varejo

A criptografia de dados nas organizações de varejo está no seu índice de presença mais abaixo já relatado durante os cinco anos deste estudo, com quase metade (48%) dos ataques resultando em dados criptografados. Houve uma queda acentuada na porcentagem de ataques que resultaram em dados criptografados nos últimos dois anos, caindo dos 71% na pesquisa de 2023, o que sugere que os varejistas estão mais capacitados a bloquear ataques antes que os dados sejam criptografados.

Gráfico 5: Índice de criptografia de dados em ataques de ransomware nas organizações de varejo 2021 – 2025



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

Índice de criptografia de dados por setor

As organizações do setor de **distribuição e transporte** estão mais propensas a ter seus dados criptografados (64%), o que indica que as organizações desse setor têm menor capacidade de detectar e interromper um ataque antes da criptografia e/ou têm menor capacidade de bloquear e reverter a criptografia maliciosa. Enquanto isso, as instituições de **ensino básico** registraram o índice mais baixo de criptografia de dados: 29% — bem abaixo da média de 50% entre setores.

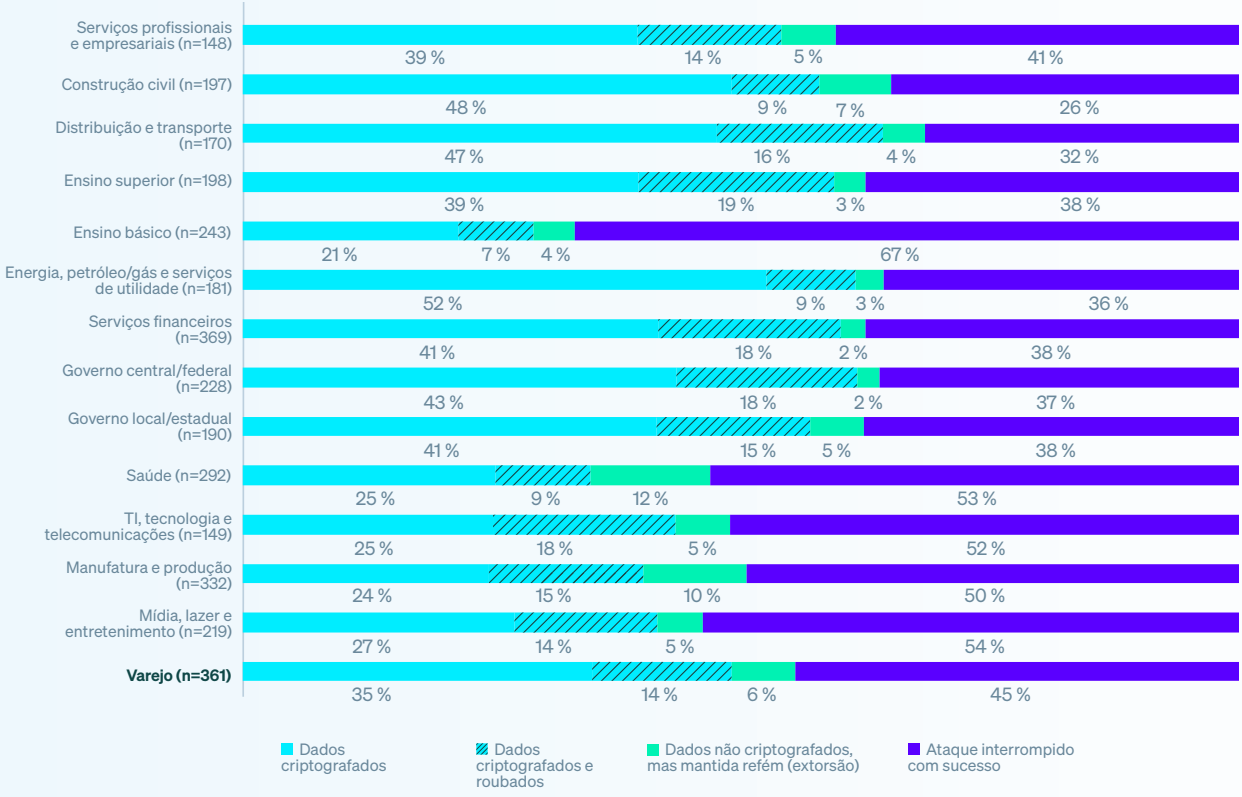
Roubo de dados

Os adversários não apenas criptografam os dados, eles também os roubam. No setor do varejo, 14% de todas as vítimas de ransomware e 29% das que tiveram seus dados criptografados tiveram seus dados roubados. Ao detalharmos os dados por setor, vemos que:

- Em um extremo, 42% das organizações do setor de **TI, tecnologia e telecomunicações** que passaram pela criptografia de dados também tiveram dados roubados.
- Já no outro extremo, apenas 15% das organizações nos setores de construção civil e de **energia, petróleo/gás e serviços de utilidade** tiveram seus dados roubados além de criptografados.

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 6: Criptografia de dados e roubo por setor



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

Ataques no estilo extorsão

Como mostra o gráfico 5, a porcentagem de organizações de varejo que não tiveram os dados criptografados, mas que foram feitas reféns (extorquidas), atingiu a sua maior marca dos últimos três anos, triplicando dos apenas 2% dos ataques em 2024 para 6% em 2025.

Dividindo os dados por setores, vemos que os **provedores da área de saúde** passaram por grande parte dos ataques no estilo extorsão (12%). Isso se deve muito provavelmente à alta confidencialidade dos dados médicos, como prontuário de pacientes, etc. Já os provedores de **serviços financeiros** e as organizações do **governo central/federal** registraram o menor percentual de ataques: apenas 2%.

No geral, as instituições de **ensino básico** 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). Isso sugere que os provedores do ensino básico estão se mostrando supreendentemente eficazes na detecção e intervenção antecipadas, mesmo com seus orçamentos limitados.

Recuperação de dados criptografados no varejo

98% das organizações de varejo que tiveram os dados criptografados conseguiram recuperá-los.

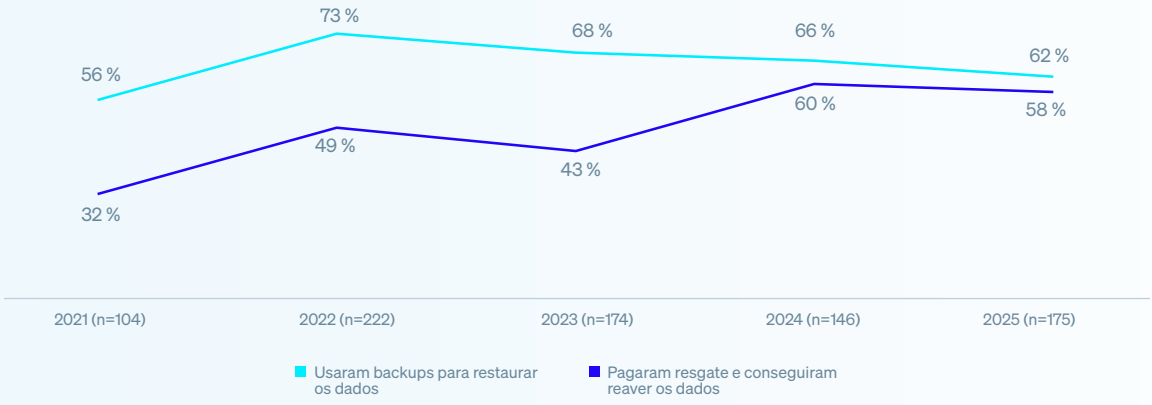
62% das organizações de varejo recuperaram seus dados **usando backups** — a mais baixa taxa em quatro anos, ainda assim um dos três principais setores em uso de backup.

58% do setor **pagaram o resgate e conseguiram reaver os dados**. Ainda que represente uma pequena redução dos 60% do ano anterior, esse continua a ser o segundo índice de pagamentos de resgate mais alto dos últimos cinco anos feito por varejistas.

A pequena diferença entre os varejistas que pagaram o resgate para recuperar os dados e os que usaram backups para recuperar os dados sugere um aumento na dependência de diferentes métodos de recuperação alternativos.

Constatamos isso com a revelação de que 39% das organizações de varejo que tiveram seus dados criptografados disseram ter utilizado mais de um método para restaurar seus dados. Nenhum outro setor relatou uma porcentagem tão alta.

Gráfico 7: Recuperação de dados criptografados no varejo 2021 – 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 no varejo

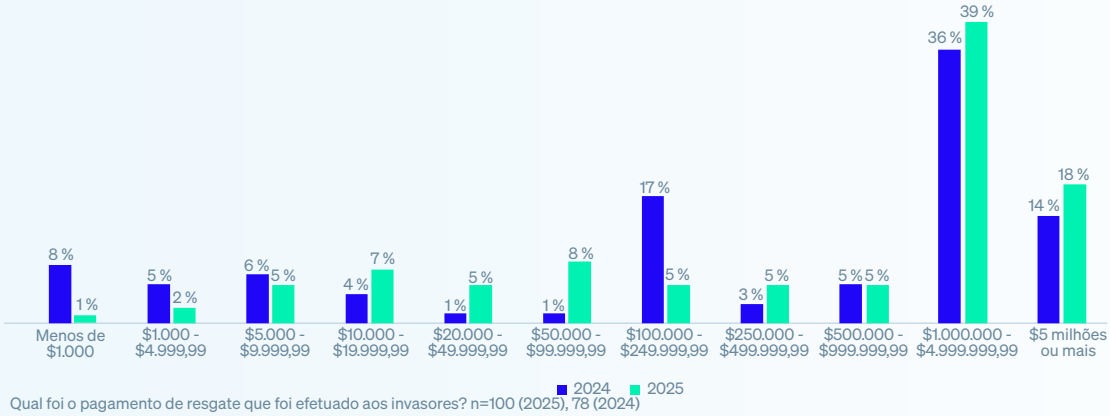
A média (mediana) do pedido de resgate às organizações do varejo dobrou no último ano: de US$ 1 milhão em 2024 para US$ 2 milhões em 2025. O aumento nos pedidos de resgate aos varejistas se deve em grande parte ao aumento de 59% nas exigências de pagamentos de US$ 5 milhões ou acima feitas no último ano. Além disso, 63% de todos os pedidos de resgate feitos aos varejistas ultrapassou US$ 1 milhão, um aumento acentuado dos 50% registrados em 2024.

Por outro lado, a média entre setores diminuiu em um terço (34%): de US$ 2 milhões em 2024 para US$ 1,32 milhão em 2025.

Pagamentos de resgate no varejo

Apesar do aumento acentuado do valor dos resgates, a média (mediana) de resgate pago pelas organizações de varejo subiu apenas 5%, o que sugere que as empresas do setor estão resistindo mais às inflacionadas demandas de regaste. Ainda assim, mesmo com um modesto aumento na mediana de pagamento de resgaste, a distribuição mostra uma tendência generalizada a pagamentos de resgate mais elevados, com uma queda evidente em pequenos valores e um aumento no número de organizações que pagam mais de US$ 1 milhão.

Gráfico 8: Pagamentos de resgate no varejo | Distribuição por faixas

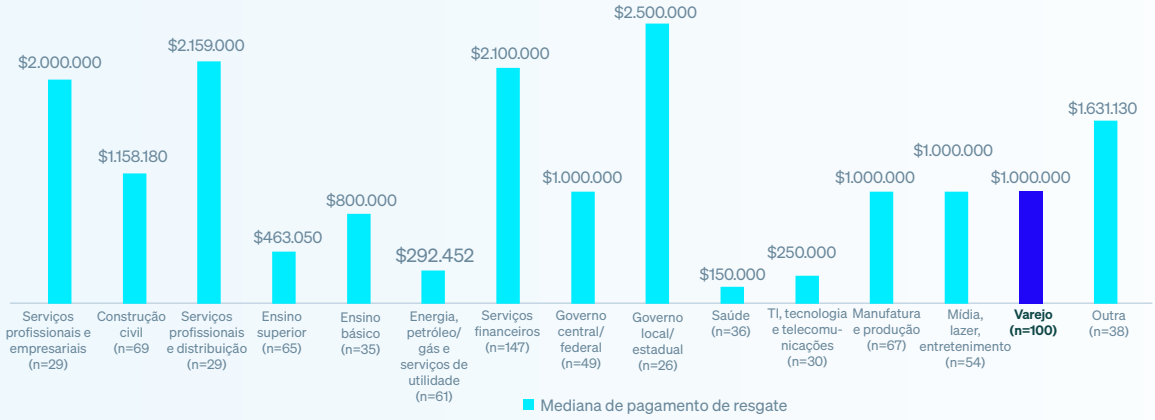


Qual foi o pagamento de resgate que foi efetuado aos invasores? n=100 (2025), 78 (2024)

Pagamentos de resgate por setor

Os pagamentos de resgate variam consideravelmente por setor, com as organizações do **governo estadual e local** pagando aos invasores a mais alta média de resgate: US$ 2,5 milhões. Isso talvez se deva a pressões a serviços críticos, resiliência cibernética limitada e invasores que exploram a urgência do setor em se recuperar prontamente. Já os provedores da área de **saúde** pagaram o mais baixo valor, US$ 150 mil.

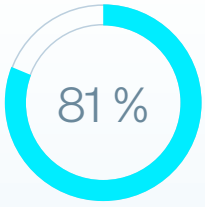
Gráfico 9: Pagamentos de resgate por setor



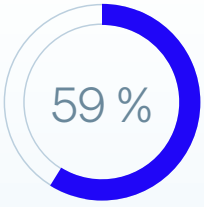
Qual foi o pagamento de resgate que foi efetuado aos invasores? Números de base no gráfico. Nota: Serviços profissionais e empresariais e Governo local/estadual oferecem um número de base baixo no estudo, portanto, os resultados devem ser considerados meros indicativos.

Como se parecem os pagamentos reais feitos pelos varejistas comparados às exigências iniciais

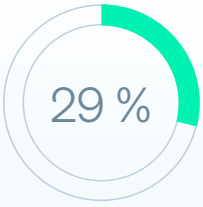
100 organizações do varejo que pagaram o resgate compartilharam conosco os valores inicial e o realmente efetuado, revelando que pagaram, em média, 81% do pedido de resgate inicial, uma queda muito bem-vinda dos 85% registrados em 2024. No geral, 59% pagaram menos do que o pedido inicial (acima da média de 53% entre setores), 11% pagaram mais e 29% cobriram a exigência inicial.



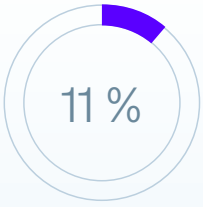
dos pedidos de resgate **foram pagos**, em média



dos pagamentos foram **inferiores** ao pedido de resgate inicial



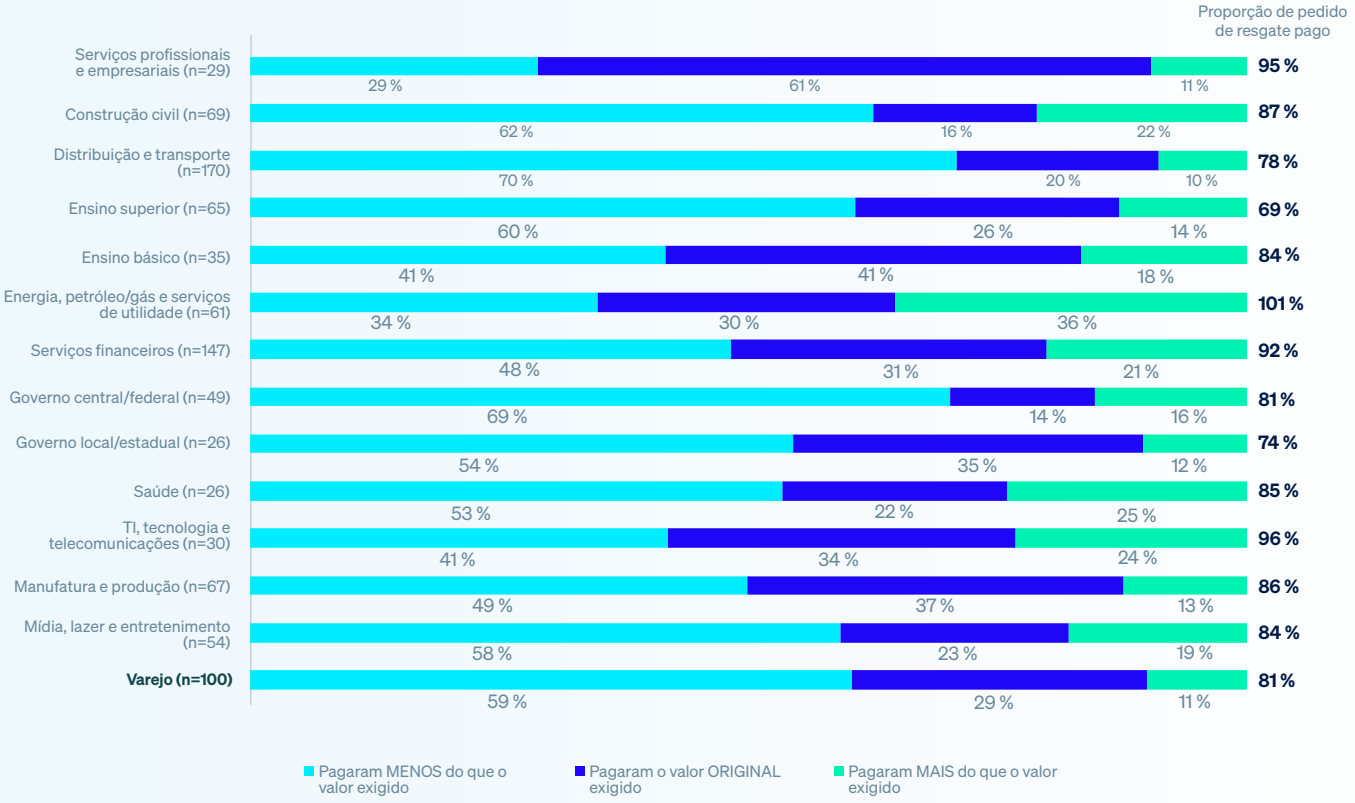
dos pagamentos **cobriram** o pedido de resgate inicial



dos pagamentos foram **superiores** ao pedido de resgate inicial

Distribuindo os dados por setor, vemos que a maioria dos setores pagou menos do que o pedido de resgate original na maior parte das negociações. As organizações no setor de **distribuição e transporte** foram as mais propensas a pagar valores abaixo das exigências iniciais (70%), o que sugere uma grande resistência aos pedidos de resgate. Por outro lado, os fornecedores de **energia, petróleo/gás e serviços de utilidade** foram os mais propensos a pagar valores mais elevados do que os exigidos inicialmente (36%), enquanto os **serviços profissionais e empresariais** atenderam, em sua maioria, às exigências iniciais (61%).

Gráfico 10: Como as organizações respondem às demandas por setor



Qual foi o pagamento de resgate que foi efetuado aos invasores? Nota: Serviços profissionais e empresariais e Governo local/estadual oferecem um número de base baixo no estudo, portanto, os resultados devem ser considerados meros indicativos. Números de base no gráfico.

Por que a maioria dos pagamentos de resgate feitos pelas organizações de varejo difere do valor inicial exigido

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

11 organizações* de varejo que **pagaram mais** do que o resgate inicial revelaram que:

- 45%: os invasores se deram conta de que éramos um alvo de grande valor.
- 45%: os invasores se irritaram e aumentaram o preço.
- 45%: nossos backups não funcionaram ou apresentaram defeitos.
- 36%: os invasores acreditavam que poderíamos pagar mais.
- 18%: não pagamos rápido o suficiente, então o preço subiu.

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

*Nota: devido a um número de base muito baixo, os resultados são meros indicativos.

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

- 60%: os invasores reduziram o valor do resgate devido a pressões externas (por exemplo, da mídia ou de autoridades legais).
- 47%: os invasores reduziram o valor do resgate para nos incentivar a pagar.
- 43%: terceiros negociaram um valor mais baixo com os invasores.
- 42%: pagamos o resgate rapidamente, assim conseguimos um desconto.
- 35%: negociamos 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

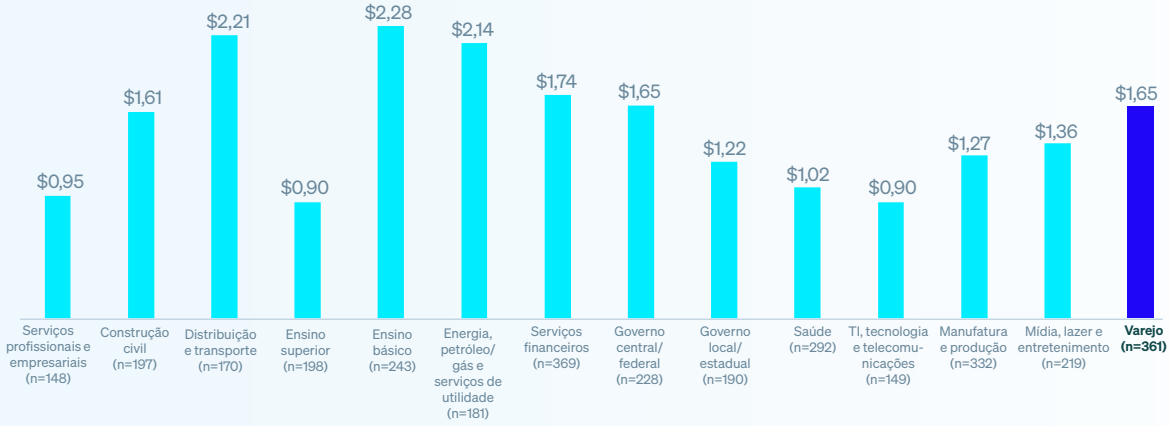
Custos de recuperação no varejo

A média do custo de recuperação de um ataque de ransomware pelas organizações de varejo (excluindo pagamento de resgate) atingiu o ponto mais baixo dos últimos três anos, marcando uma queda de 40%, dos US$ 2,73 milhões em 2024 para US$ 1,65 milhão. Além disso, o valor está US$ 200.000 mais baixo do que a soma registrada em 2023.

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=361 (2025), 261 (2024), 244 (2023).

Quando examinamos a distribuição por setor, observamos que a recuperação varia consideravelmente. As instituições de **ensino básico** registraram o custo médio mais alto para retificar incidentes, US$ 2,28 milhões. Em contrapartida, as instituições de **ensino superior** e as organizações do setor de **TI, tecnologia e telecomunicações** registraram igualmente o mais baixo custo, US$ 900 mil.

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

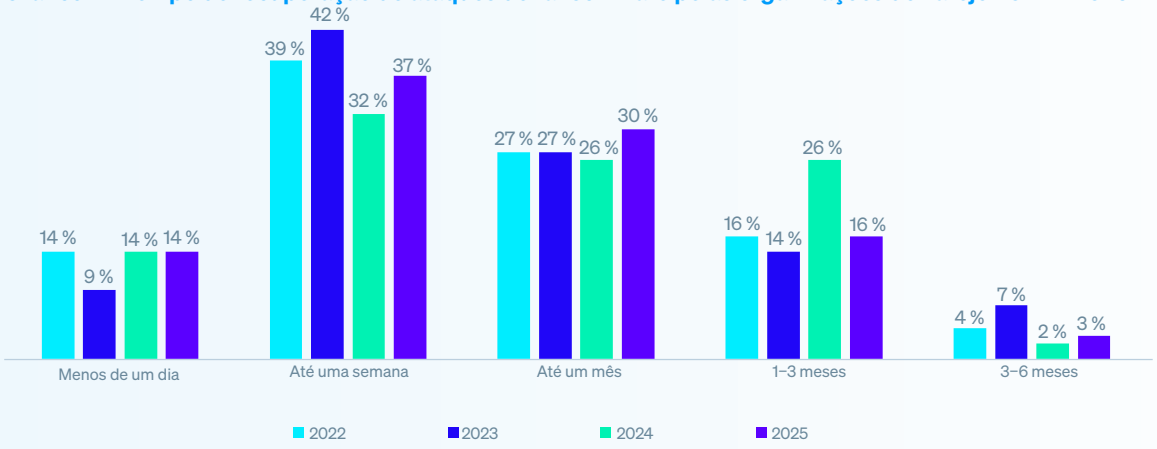


Qual foi o custo aproximado para a sua organização retificar o impacto do ataque de ransomware mais significativo (considerando-se período de inatividade, tempo de pessoal, custo dos equipamentos, custo da rede, perda de oportunidades etc.), excluindo pagamentos de resgate realizados? Números de base no gráfico.

Tempo de recuperação

Os dados revelam que, em 2025, as organizações de varejo mostraram sinais de uma recuperação mais rápida após ataques de ransomware. Mais da metade (51%) se recuperou em uma semana, comparado aos 46% registrados em 2024. Ao mesmo tempo, a proporção que precisou de um a três meses para se recuperar caiu acentuadamente para 16%, comparado aos 26% registrados em 2024. No geral, 96% das vítimas do varejo se recuperaram em três meses, demonstrando a crescente resiliência e capacidade de recuperação do setor.

Gráfico 12: Tempo de recuperação de ataques de ransomware pelas organizações do varejo 2022 – 2025



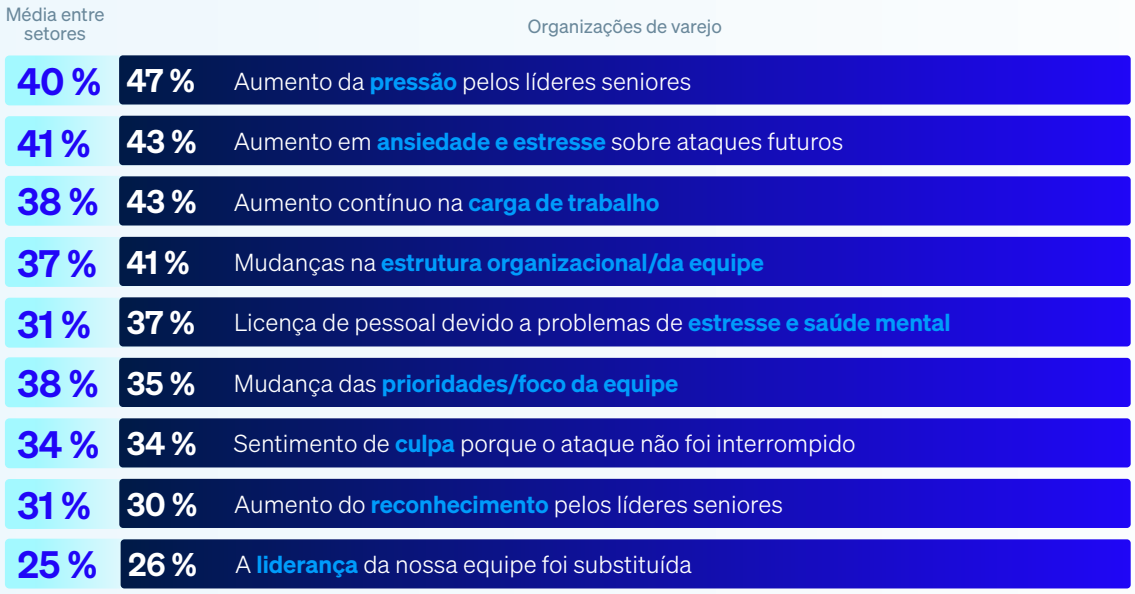
Quanto tempo a sua organização levou para se recuperar por completo do ataque de ransomware? Números de base no gráfico.

Não surpreende que as organizações de varejo que tiveram seus dados criptografados foram, tipicamente, mais lentas para se recuperar do que aquelas que foram capazes de interromper a criptografia: 6% das organizações que tiveram os dados criptografados estavam totalmente recuperadas em um dia, em comparação aos 22% 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 no setor varejista, com todos os entrevistados dizendo que suas equipes foram afetadas de alguma forma.

Gráfico 13: Consequências às equipes de segurança cibernética e TI por terem os dados criptografados



Qual a repercussão que o ataque de ransomware teve nas pessoas em sua equipe de TI e segurança cibernética, se alguma? n=175

Recomendações

Embora as organizações de varejo tenham passado por várias mudanças com relação a ransomwares no último ano, a ameaça continua significante. 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.

2025-08-04 WP (MP)

SOPHOS