SOPHOS

O Estado do Ransomware 2023

Resultados de uma pesquisa independente e totalmente desvinculada com 3.000 líderes responsáveis pela segurança cibernética e de TI distribuídos em 14 países realizada entre janeiro e março de 2023.

Documento técnico Sophos. Maio de 2023

Introdução

Este estudo anual encomendado pela Sophos sobre as experiências reais com ransomwares enfrentadas pelos líderes em segurança cibernética e TI esclarecem a realidade que as organizações têm pela frente em 2023. Ele revela as causas primárias mais comuns dos ataques e mostra com clareza como as experiências com ransomwares diferem de acordo com a receita das organizações. O relatório revela também o impacto comercial e operacional de pagar o resgate para recuperar dados em vez de usar backups.

Sobre a pesquisa

A Sophos encomendou uma pesquisa independente e totalmente desvinculada com 3.000 líderes de segurança cibernética e TI em organizações com entre 100 e 5.000 funcionários distribuídos em 14 países nas Américas, EMEA e Ásia-Pacífico. A pesquisa ocorreu entre os meses de janeiro e março de 2023, e os entrevistados foram solicitados a responder às questões com base na experiência que tiveram no ano anterior.

No setor da educação, os entrevistados foram divididos em ensino básico fundamental (estudantes até 18 anos) e ensino especializado superior (estudantes acima de 18 anos).

Contents

Índice de ataques de ransomware

A pesquisa revelou que o índice de ataques de ransomware permaneceu estabilizado, com 66% dos entrevistados respondendo que suas organizações foram atingidas por ransomware no ano anterior, o mesmo que constatou a nossa pesquisa de 2022. Com adversários que agora são capazes executar tarefas consistentemente e em grande escala, o ransomware tornou-se, indiscutivelmente, o maior risco cibernético que as organizações enfrentam atualmente.

Os criminosos cibernéticos vêm desenvolvendo e refinando o modelo ransomware-as-a-service já há alguns anos. Esse modelo operacional diminui as exigências para adentrar no mercado de ransomware enquanto aumenta a sofisticação do ataque ao permitir que os agentes adversários se especializem em diferentes estágios de um ataque. Para obter mais informações sobre ransomware-as-a-service, leia o Relatório de Ameaças 2023 da Sophos.

2020	2021	2022	2023
51%	37%	66%	66%

Sua organização foi atingida por ransomware neste último ano? Sim. n=3.000 (2023), 5.600 (2022), 5.400 (2021), 5.000 (2020)

Ataques por país

Ainda que o índice geral de ransomware relatado permaneça estável comparado a 2022, a pesquisa revelou variações no nível de país. Singapura relatou o mais alto índice de ataques de ransomware no estudo deste ano, com 84% das organizações atingidas no ano anterior. Do outro lado da balança está o Reino Unido, que relatou o mais baixo nível de ataques (44%).

A Áustria relatou a maior queda no índice de ataques: de 84% das organizações atingidas para 50%. A África do Sul teve o maior aumento no índice de ataques, com 78% das organizações atingidas em nossa pesquisa de 2023 comparado ao índice de 51% em 2022.

Para ver mais detalhes, consulte o Índice de ataques de ransomware por país: 2022 x 2023, na página 20.

Ataques por setor

O setor da educação foi o que mais sentiu o peso de um ataque de ransomware no último ano, com 80% (ensino fundamental) e 79% (ensino superior) relatando que foram atingidos. Já é costume ver a educação enfrentando dificuldades devido a suas deficiências em recursos e tecnologias – muito mais do que os outros setores – e os dados mostram que os adversários estão explorando essa vulnerabilidade.

TI, tecnologia e telecomunicações registraram o mais baixo índice de ataques (50%), indicando um preparo elevado e boas defesas cibernéticas.

Para ver mais detalhes, consulte o Índice de ataques de ransomware por setor, na página 21.

66% atingidos por ransomware

Singapura mais alto índice de ataques (país)

Reino Unido mais baixo índice de ataques (país)

Educação mais alto índice de ataques (setor)

TI, tecnologia e telecomunicações
mais baixo índice de ataques (setor)

Ataques por tamanho da organização: funcionários x receita

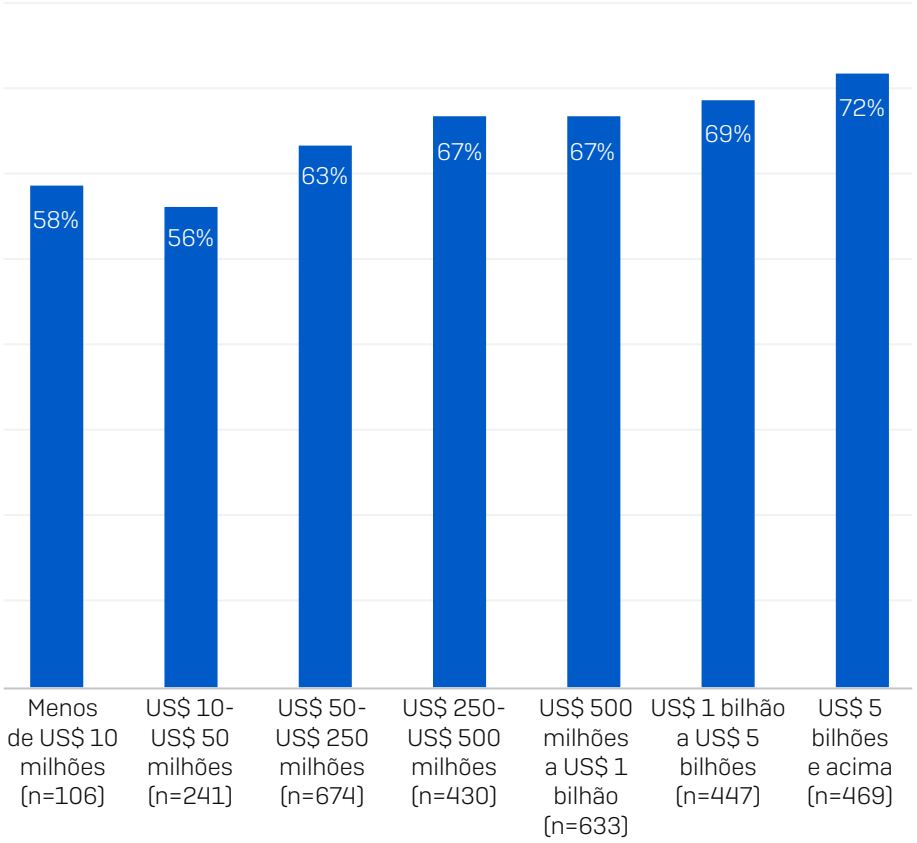
A pesquisa revelou uma clara correlação entre a receita anual e a propensão de passar por um ataque de ransomware, com um aumento progressivo no percentual das organizações atingidas por ransomware quando comparado à receita. 56% das organizações com receita de US$ 10 a US$ 50 milhões passaram por um ataque de ransomware no último ano, subindo para 72% entre as organizações com receita acima de US$ 5 bilhões.

O contrário ocorreu ao correlacionar o número de funcionários em uma organização e um ataque de ransomware, que demonstrou claramente uma relação muito pequena. Até a faixa de 1.001 a 3.000 funcionários, o índice de ataques de ransomware foi bastante consistente:

- 100 a 250 funcionários 62%
- 251 a 500 funcionários 62%
- 501 a 1.000 funcionários 62%
- 1.001 a 3.000 funcionários 73%
- 3.001 a 5.000 funcionários 63%

Os dados deixam claro que, sob a perspectiva de tamanho da organização, a receita anual é um indicador muito mais preciso da possibilidade de passar por um ataque do que o número de funcionários.

Porcentagem de organizações atingidas por ransomware por receita



Sua organização foi atingida por ransomware neste último ano? Sim. Números de base no gráfico

Causas primárias dos ataques de ransomware

Os entrevistados responderam que a exploração de uma vulnerabilidade foi a causa primária mais comum dos ataques de ransomware (36%), seguida pelo comprometimento de credenciais (29%). Essas descobertas se alinham retrospectivamente e quase que exatamente à última análise da Sophos de 152 ataques que as nossas equipes de Incident Response (IR) e Managed Detection and Response (MDR) foram chamadas para controlar, e das quais 37% começaram com a exploração de uma vulnerabilidade e, 30%, com o comprometimento de credenciais.

E-mails foram a causa primária de 30% (valor arredondado) dos ataques: 18% começaram com um e-mail malicioso e 13% com phishing. 3% começaram com um ataque de força bruta e apenas 1% através de downloads.

36%	29%	18%
Vulnerabilidade explorada	Credenciais comprometidas	E-mail malicioso
13%	**3%**	**1%**
Phishing	Ataque de força bruta	Download

Você sabe a causa primária do ataque de ransomware que a sua organização enfrentou no último ano? Se foram atingidos mais de uma vez, pense no ataque mais significativo. (n=1.974 organizações atingidas por ransomwares no ano passado)

Causas primárias por setor

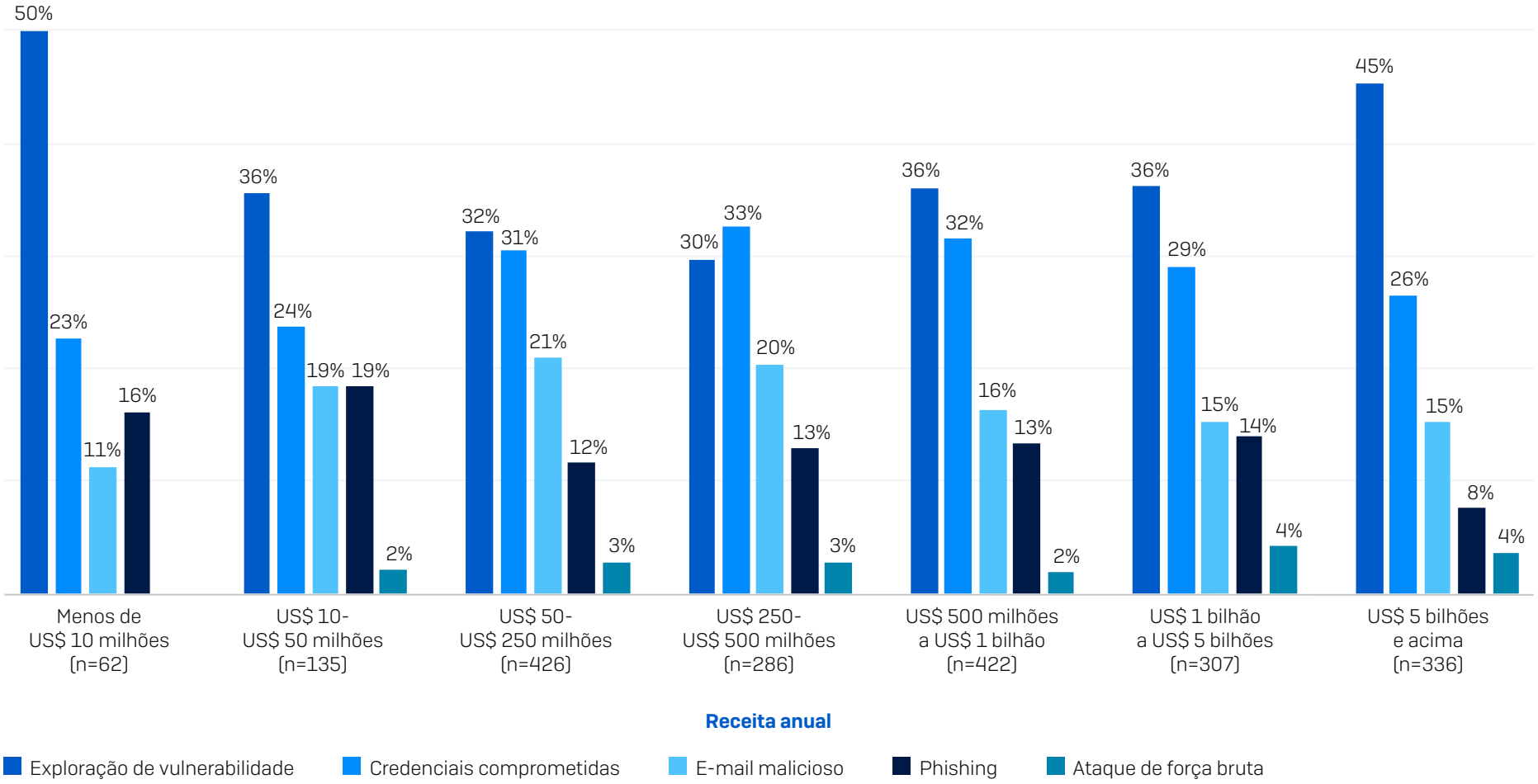
O setor de mídia, lazer e entretenimento registrou a porcentagem mais alta de ataques, tendo como causa primária a exploração de uma vulnerabilidade (55%), indicando grandes lacunas de segurança nessa área. O governo central/federal apresentou a porcentagem mais alta de ataques que iniciaram com o comprometimento de credenciais (41%). Isso pode ser devido ao alto índice de roubo de credenciais registrado, à falta de capacidade de prevenir a exploração das credenciais roubadas ou à combinação desses dois fatores.

TI, tecnologia e telecomunicações registrou o mais baixo índice de vulnerabilidades exploradas (22%) e credenciais comprometidas (22%), o que reflete certamente um grande potencial nas defesas cibernéticas do setor. Contudo, o setor registrou os mais altos índices de ataques relacionados a e-mails, com mais da metade (51%) começando na caixa de entrada dos usuários.

Para ver mais detalhes, consulte as Causas primárias de ataques por setor, na página 22.

Causas primárias por receita

A análise das causas primárias por receita anual revela que as vulnerabilidades exploradas e as credenciais comprometidas seguem curvas de propensão opostas. Os mais altos percentuais de ataques que iniciaram com uma vulnerabilidade explorada foram relatados pelos coortes de receitas mais baixas (menos de US$ 10 milhões: 50%) e mais altas (acima de US$ 5 bilhões: 45%), caindo para 30% no coorte de receita média (US$ 250 a US$ 500 milhões). Já o uso de credenciais comprometidas teve seu pico no coorte de receita média (33%), com o menor uso registrado nos coortes de receita mais baixa (23%) e mais alta (26%).

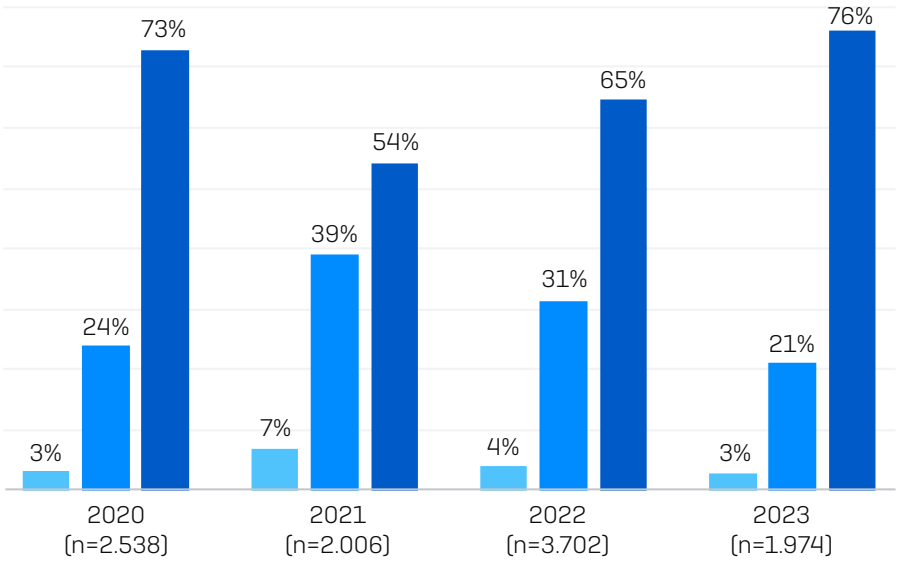


Você sabe a causa primária do ataque de ransomware que a sua organização enfrentou no último ano? Seleção de opções de resposta. Números de base no gráfico

Índice de criptografia de dados

A criptografia de dados continuou subindo, com os adversários se beneficiando da criptografia de dados em mais de três quartos (76%) dos ataques de ransomware. Na verdade, os níveis de criptografia agora estão no auge, considerando-se os últimos quatro anos. Isso é um provável reflexo da crescente especialização dos adversários, que continuam a inovar e refinar suas abordagens.

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



- Não – Os dados não foram criptografados, mas ainda assim fomos feitos reféns (extorsão)
- Não – O ataque foi interrompido antes que os dados fossem criptografados
- Sim – Os dados foram criptografados

Criptografia de dados por setor

Quase todos os setores lutam para bloquear os ataques antes que os dados possam ser criptografados. Com apenas uma exceção, em todos os outros setores, mais de dois terços dos ataques resultaram na criptografia de dados. A mais alta frequência de dados criptografados (92%) foi relatada por serviços profissionais e empresariais.

TI, tecnologia e telecomunicações é o setor que rompe a tendência, onde os adversários obtêm sucesso na criptografia de dados em menos da metade (47%) dos ataques. Esse é outro indicador do alto nível de defesas cibernéticas e preparo de resposta que caracteriza o setor.

Para ver mais detalhes, consulte a Criptografia de dados por setor, na página 23.

Roubo de dados

Em 30% dos ataques em que os dados foram criptografados, os dados também foram roubados. Esse método de "ataque duplo" utilizado pelos adversários tem se tornado bastante comum como um meio de monetizar ainda mais os seus ataques. A ameaça de levar a público os dados roubados pode ser usada para extorquir pagamentos – e os dados também podem ser vendidos. A grande frequência de roubo de dados aumenta a importância de interromper esses ataques o mais rápido possível, antes que as informações possam ser exfiltradas.

30%
dos ataques de ransomware em que os dados foram criptografados também relataram o roubo dos dados

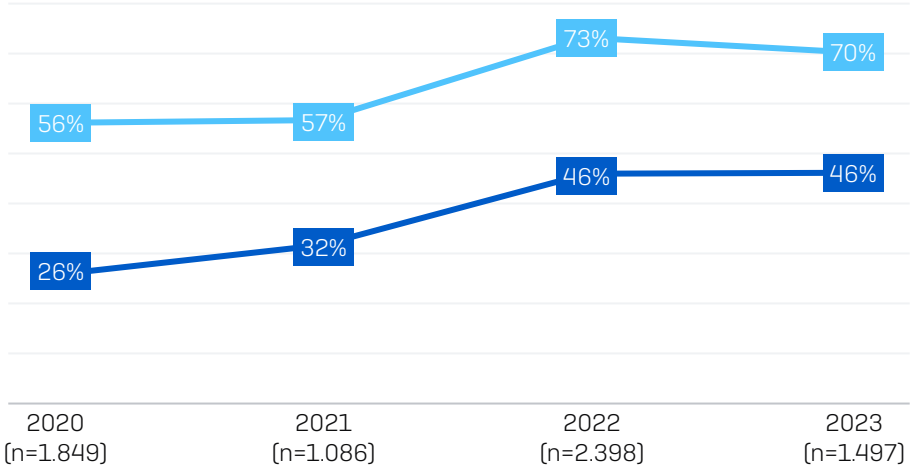
Os criminosos virtuais tiveram sucesso na criptografia de dados da sua organização no ataque de ransomware? Sim, tiveram; Sim, e os dados também foram roubados. n=1.497

Recuperação dos dados

97% das organizações que tiverem seus dados criptografados conseguiram reavê-los. Backup foi o método mais comum utilizado em 70% dos incidentes. 46% pagaram o resgate e recuperaram seus dados, enquanto 2% usaram outros meios. No geral, uma em cinco (21%) usaram vários métodos para restaurar seus dados. 1% das organizações que tiveram seus dados criptografados pagou o resgate, mas não conseguiu reaver os dados.

Usam backups para restaurar dados	Pagaram resgate e conseguiram reaver os dados	Usam outros meios para reaver os dados
70%	**46%**	**2%**

Porém, é preocupante que o uso de backups para recuperar dados tenha caído no último ano, quando foi utilizado em 73% dos casos para recuperar dados. Índice de pagamento de resgate se manteve estável comparado ao último ano.



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

Recuperação de dados por país

No geral, os entrevistados na região EMEA relataram níveis agregados mais altos de uso de backup (75%) e níveis agregados mais baixos de pagamento de resgate (40%) do que nas Américas (65%/55%) e Ásia-Pacífico (67%/49%). No nível de país, a França apresentou o mais alto índice de uso de backup (87%), seguida de perto pela Suíça (84%).

A importância dos backups se mostra quando observamos que os dois países menos capazes de usar backups para restaurar dados – a Itália (55%) e Singapura (57%) –, também são os dois países que relataram o mais baixo índice geral de recuperação de dados (93% e 90%, respectivamente). A Itália registrou também a mais alta propensão a pagar resgate (56%), seguida de perto pelos EUA e o Brasil (ambos 55%).

Na maioria dos casos, as organizações que pagaram o resgate foram capazes de recuperar seus dados. Contudo, na França e no Reino Unido, cerca de uma em cada dez organizações que pagaram o resgate não conseguiu reaver nada de seus dados.

Para ver mais detalhes, consulte a Recuperação de dados por país, na página 24.

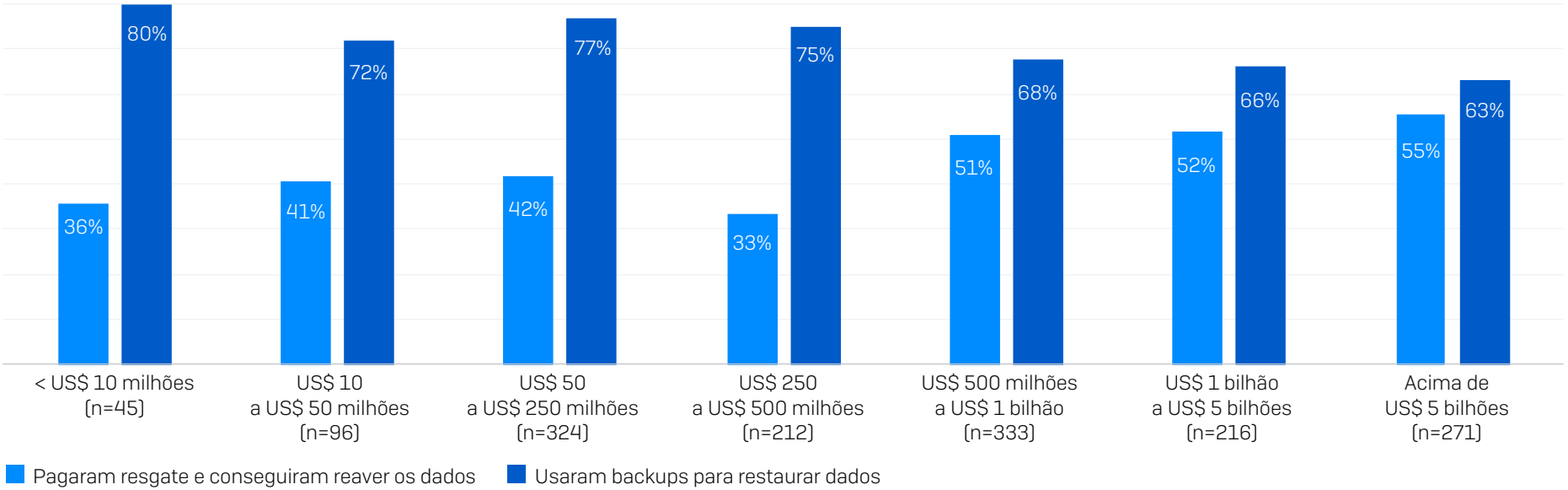
Pagamento de resgate e uso de backup por receita

Em termos gerais, conforme aumenta a receita anual também aumenta a probabilidade de uma organização recuperar seus dados pagando o resgate. Em contrapartida, a frequência do uso de backup cai.

Das organizações com receita acima de US$ 5 bilhões, 55% conseguiram reaver seus dados pagando o resgate e 63% usando backups. Já 36% das organizações com receita inferior a US$ 10 milhões recuperaram seus dados pagando o resgate, enquanto 80% usaram backups – o mais alto índice de uso de backup de todos os coortes de receita.

As organizações com receita anual mais baixa tinham menos fundos para bancar o pagamento de um resgate, o que as forçou a se voltarem aos backups para recuperar seus dados. Já as organizações com receitas maiores normalmente têm infraestruturas de TI mais complexas, o que pode dificultar o uso de backups para recuperar dados com presteza. Elas também são empresas melhor capacitadas a pagar para se saírem de tais situações.

Pagamento de resgate e uso de backup por receita



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

O impacto do seguro de proteção digital na recuperação de dados

As organizações com seguro de proteção digital estavam consideravelmente mais propensas a recuperarem os dados criptografados do que aquelas sem apólices de seguro. Contudo, o tipo de cobertura cibernética fez muito pouca diferença: 98% daquelas cobertas por uma apólice independente e 97% daquelas cobertas por uma apólice de seguro mais ampla conseguiram reaver seus dados. Comparativamente, 84% das organizações sem uma apólice conseguiram reaver seus dados criptografados.

Há uma variedade de fatores prováveis por trás dessa variação. Primeiro, o seguro de proteção digital geralmente exige que as organizações tenham planos de recuperação e backups como condição para a apólice. As seguradoras também são capazes de direcionar as vítimas de ransomware através do processo de recuperação para otimizar os resultados. Além disso, as organizações com seguro de proteção digital estão mais propensas a pagar o resgate para recuperar seus dados do que aquelas sem apólices de seguro.

Porcentagem de vítimas de ransomware que recuperaram os dados criptografados

A sua organização conseguiu reaver os dados capturados? n=1.497 organizações atingidas por ransomware no último ano e que tiveram seus dados criptografados

Impacto do seguro na propensão de pagar o resgate

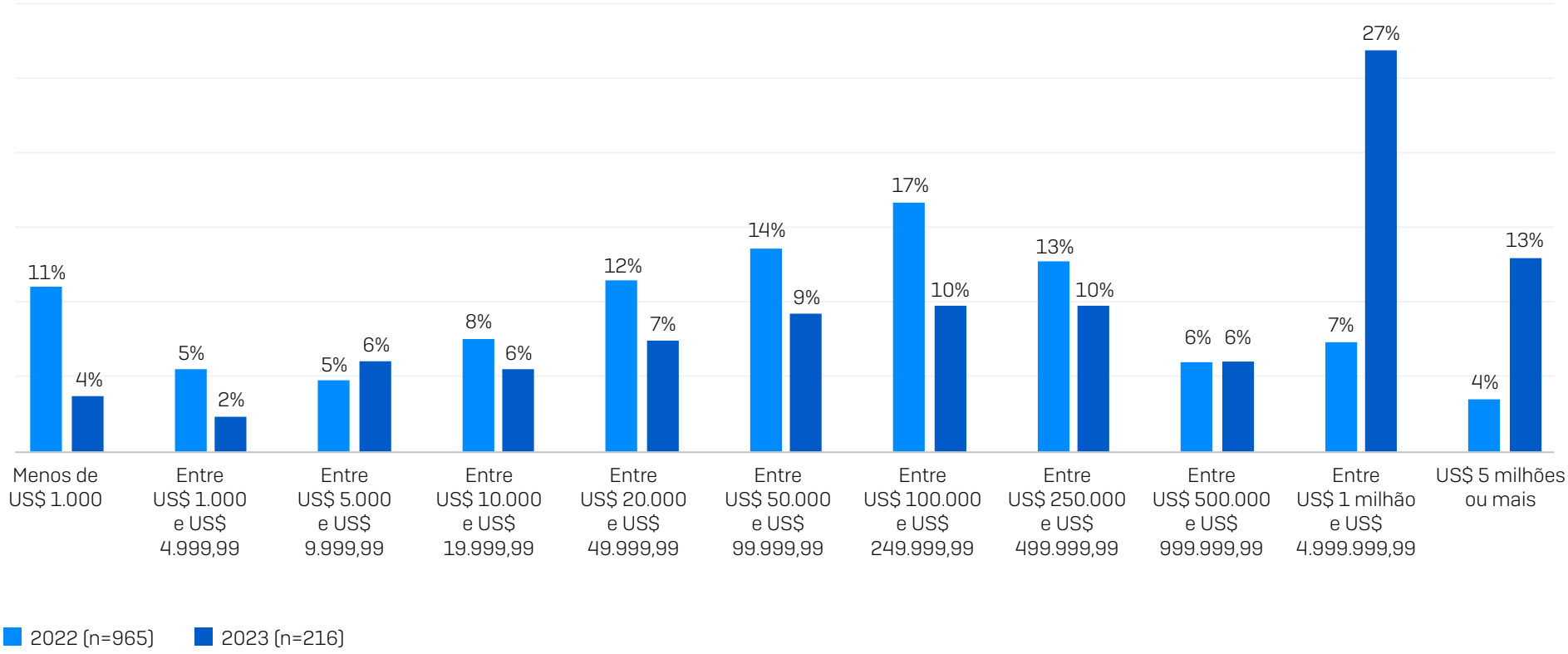
Sua organização conseguiu reaver os dados capturados? Sim, pagamos o resgate e conseguimos reaver os dados. n=1.497 organizações atingidas por ransomware no último ano e que tiveram seus dados criptografados (771 apólices independentes, 658 com proteção de seguro digital como parte de uma apólice mais ampla, 67 sem apólice de seguro de proteção digital)

Pagamentos de resgate

Ainda que a predisposição geral para pagar o resgate permaneça alinhada aos resultados do estudo do ano passado, os pagamentos em si aumentaram consideravelmente em comparação ao último ano, com o pagamento médio de resgate quase dobrando: de US$ 812.380,00 em 2022 para US$ 1.542.333,00 em 2023. A mediana de pagamento de resgate relatada no estudo deste ano foi de US$ 400.00,00.

O estudo revelou uma ampla distribuição dos pagamentos, contudo, a proporção de organizações que pagaram os maiores resgastes aumentou em relação ao nosso estudo de 2022, com 40% relatando pagamentos de US$ 1 milhão ou mais comparado aos 11% do último ano. Inversamente, apenas 34% pagaram menos de US$ 100.000,00, uma queda dos 54% do último ano.

Pagamentos de resgate: 2023 x 2022



Qual foi o pagamento de resgate que foi efetuado aos invasores? Excluindo respostas "Não sei".

Pagamentos de resgate por receita

Provavelmente sem muita surpresa, as organizações com as maiores receitas foram mais propensas a pagar os resgates mais altos, refletindo o ajuste promovido pelos adversários da quantia aceita com base na capacidade de pagar. O estudo não diferenciou entre pagamentos custeados internamente e aqueles custeados pelas seguradoras.

Vale notar que houve uma pequena diferença entre o pagamento médio de resgate e a mediana de pagamentos para as organizações com receita entre US$ 250 milhões e US$ 500 milhões e aquelas com receita entre US$ 500 milhões e US$ 1 bilhão.

	US$ 50-US$ 250 MILHÕES (N=37)	US$ 250-US$ 500 MILHÕES (N=33)	US$ 500 MILHÕES-US$ 1 BILHÃO (N=72)	US$ 1 BILHÃO-US$ 5 BILHÕES (N=45)	ACIMA DE US$ 5 BILHÕES (N=21)
Pagamento médio de resgate	$690.996	$1.523.652	$1.466.240	$2.049.817	$2.464.339
Mediana de pagamento de resgate	$145.000	$428.000	$425.000	$1.000.000	$3.000.000

Qual foi o pagamento de resgate que foi efetuado aos invasores? Excluindo respostas "Não sei". Excluindo organizações com receita anual abaixo de US$ 50 milhões devido a um número de base muito baixo. Números de base no gráfico. Dados para segmentos com menos de 30 entrevistados devem ser considerados um mero indicativo.

Custos de recuperação

Os pagamentos de resgate são apenas um elemento dos custos de recuperação quando tratamos de eventos de ransomware. Excluindo os resgastes pagos, as organizações relataram um custo médio estimado para recuperar-se de ataques de ransomware de US$ 1,82 milhão, um aumento no valor relatado em 2022 de US$ 1,4 milhão, porém alinhado ao valor de US$ 1,85 milhão relatado em 2021.

Observação: a questão formulada no estudo de 2021 e 2022 incluía os pagamentos de resgate nos custos estimados, mas estes foram removidos da pergunta na pesquisa de 2023. Sendo assim, a comparação ano a ano deve ser considerada um mero indicativo.

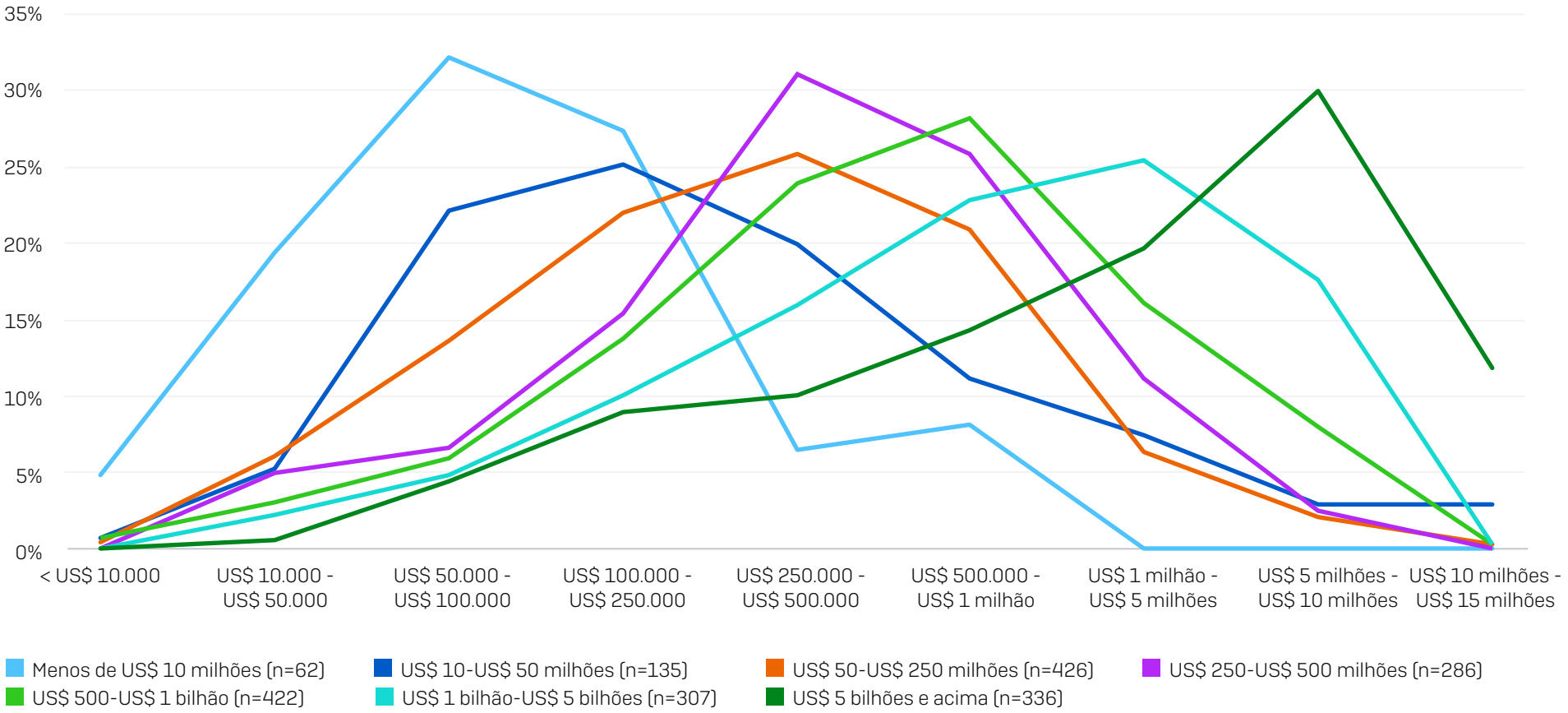
Custo médio de recuperação

2021	2022	2023
US$ 1,85 milhão	US$ 1,4 milhão	US$ 1,82 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.)? n=1.974 (2023); 3.702 (2022); 2.006 (2021). N.B. Em 2022 e 2021, a questão formulada incluía também o termo "resgate pago".

Os custos médios de recuperação relatados começam em US$ 165.520,00 para organizações com receita anual inferior a US$ 10 milhões, subindo para US$ 4.496.086,00 no coorte de US$ 5 bilhões e acima. Ainda que esses números abranjam uma variação de custos de recuperação, há um padrão claro de aumento de custos de recuperação em relação à receita, como indica o gráfico na próxima página.

Custo de recuperação por receita



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.)? Números de base no gráfico

Custo de recuperação por método de recuperação de dados

Qualquer que seja a sua perspectiva frente aos dados, fica consideravelmente mais barato usar backups para se recuperar de um ataque de ransomware do que pagar o resgate. A mediana do custo de recuperação para aquelas que usaram backups (US$ 375.000,00) é metade do custo incorrido por aquelas que pagaram o resgate (US$ 750.000,00). De modo similar, o custo médio de recuperação é quase US$ 1 milhão mais baixo para aquelas que usaram backups. Se havia necessidade de um indício maior para comprovar os benefícios financeiros de se investir em uma estratégia de backup, tome esse fato como final.

Pagaram resgate e conseguiram reaver os dados	Usaram backups para restaurar dados
$750.000	**$375.000**
mediana	mediana
$2,6 milhões	**$1,62 milhão**
média	média

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.)? n=694 que pagaram o resgate e conseguiram reaver os dados e 1.053 que usaram backups para restaurar dados.

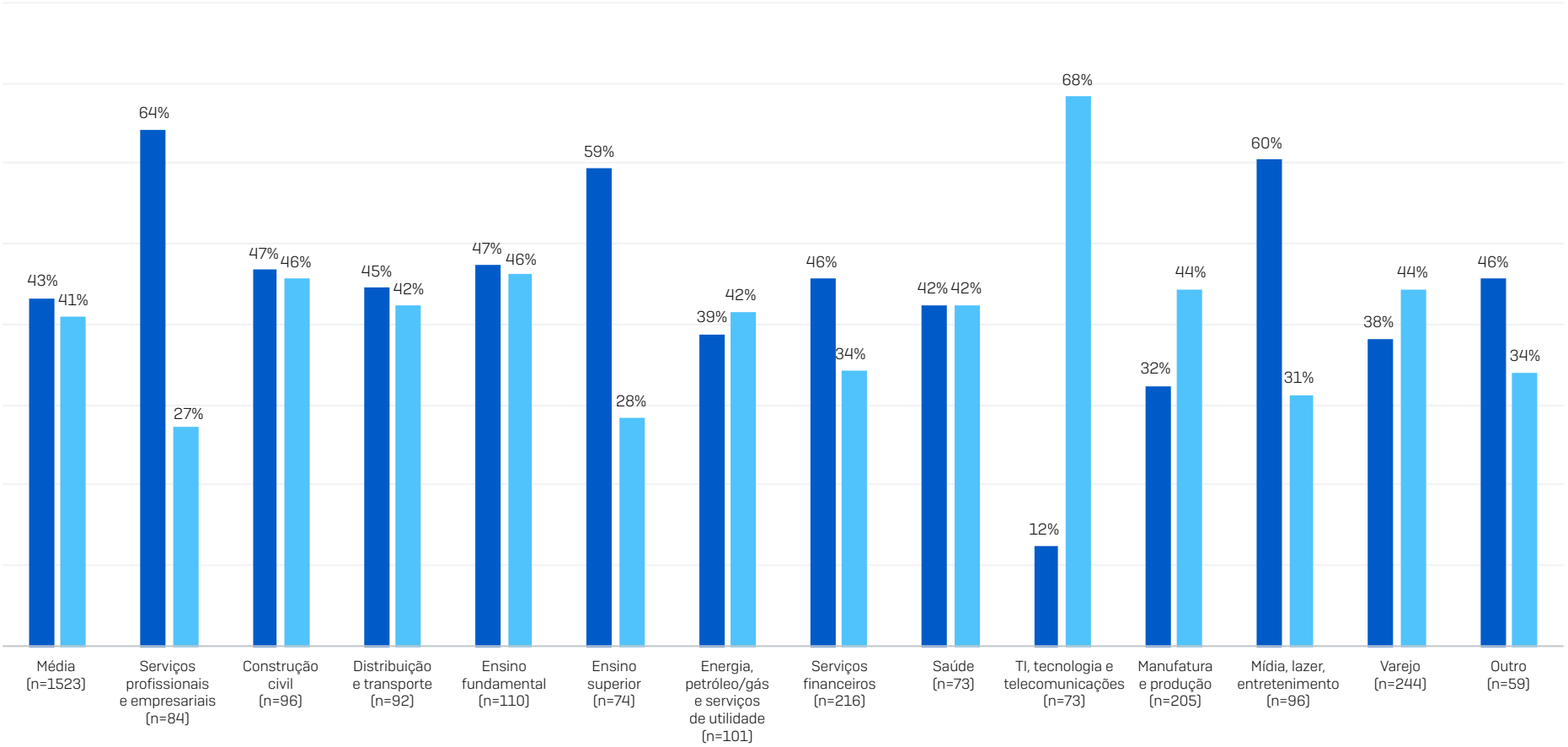
Impacto nos negócios

84% das organizações do setor privado atingidas por ransomware relataram que o ataque causou perdas em negócios/receita. A receita anual teve um impacto relativamente pequeno na perda de negócios, com o índice mais baixo (79%) relatado pelo coorte de US$ 250 milhões a US$ 500 milhões e o índice mais alto (88%) relatado por aquelas com receita abaixo de US$ 10 milhões e acima de US$ 5 bilhões.

O tipo de setor teve um papel muito mais acentuado na propensão de perdas de negócios/receita. No geral, o ensino fundamental (94%) e a construção civil (93%) foram os mais propensos a relatar perdas de negócios/receita devido a ataques, e o setor de manufatura e produção foi o menos afetado (77%).

Aprofundando-se nesse quesito, vemos uma considerável variação nos setores que relataram "muitas" perdas de negócios/receita, com os serviços profissionais e empresariais (64%) mais do que cinco vezes mais propensos a terem sentido esse nível de impacto do que TI, tecnologia e telecomunicações (12%).

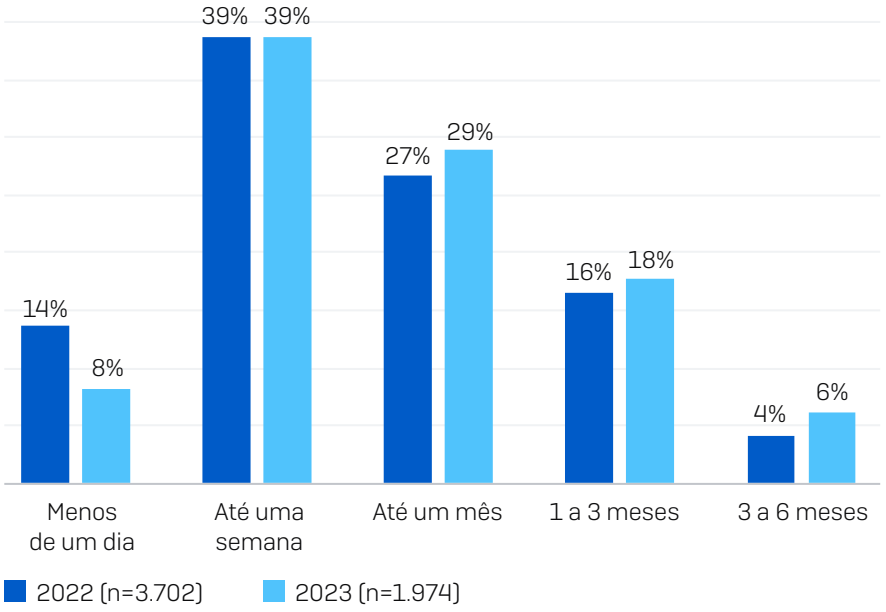
Perda de negócios/receita por setor



O ataque de ransomware causou a perda de negócios/receita à sua organização? Sim, perdemos muitos negócios/receita; Sim, perdemos poucos negócios/receita. Organizações do setor privado que foram atingidas por ransomware no ano, números de base no gráfico

Tempo de recuperação

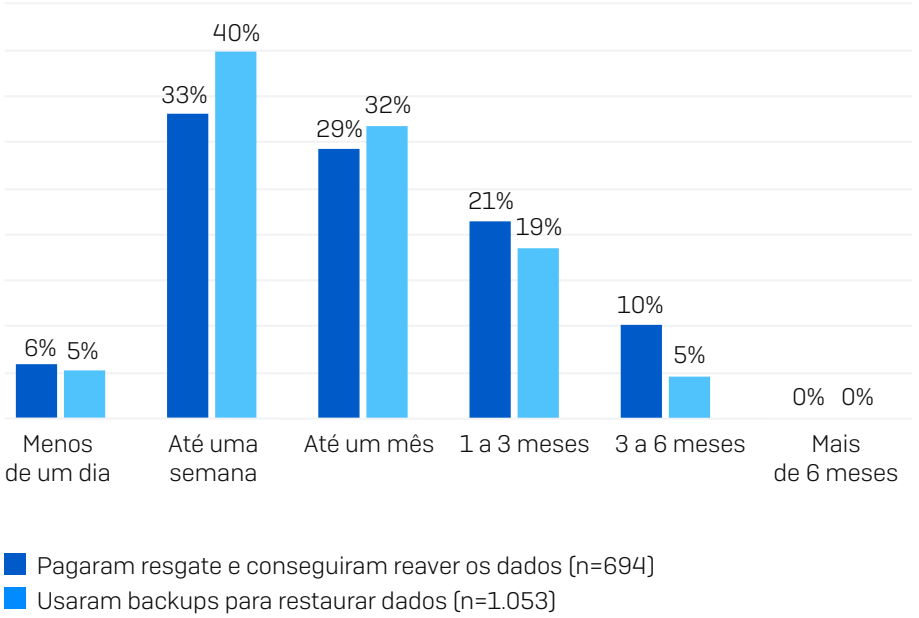
O tempo de recuperação de um ataque de ransomware está amplamente alinhado ao relatório de 2022, porém a porcentagem que foi capaz de se recuperar em menos de um dia caiu de 14% para 8%.



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

Tempo de recuperação por método de recuperação de dados

A pesquisa revelou que as organizações que usam backups para restaurar seus dados de um ataque se recuperam mais rapidamente do que as que pagam o resgaste. 45% daquelas que usaram backups se recuperaram em uma semana, comparado aos 39% daquelas que pagaram o resgate. Quase um terço (32%) daquelas que pagaram o resgate levaram mais de um mês para se recuperar, enquanto que os números mostram que a porcentagem daquelas que usaram backups foi de 23% (valor arredondado). Embora essas duas respostas ao problema não sejam mutuamente exclusivas, e alguns entrevistados tenham pago o resgate e usado backups, as vantagens de backups para o processo de recuperação são nítidas.



Quanto tempo a sua organização levou para se recuperar por completo do ataque de ransomware?
Organizações que pagaram o resgate e/ou usaram backups para recuperar dados. Números de base no gráfico

Conclusão

Independentemente da receita, posição geográfica ou setor, o ransomware continua a ser uma grande ameaça para as organizações. Os adversários continuam a aperfeiçoar suas técnicas, táticas e procedimentos (TTPs) de ataque, com as equipes de defesa se empenhando arduamente para acompanhar o ritmo, resultando no aumento dos índices de criptografia.

A queda no uso de backups para recuperar dados criptografados é um fator consideravelmente preocupante. Se havia necessidade de um indício maior para comprovar os benefícios financeiros e operacionais do investimento em uma estratégia de backup forte, esse relatório é o esclarecimento que faltava.

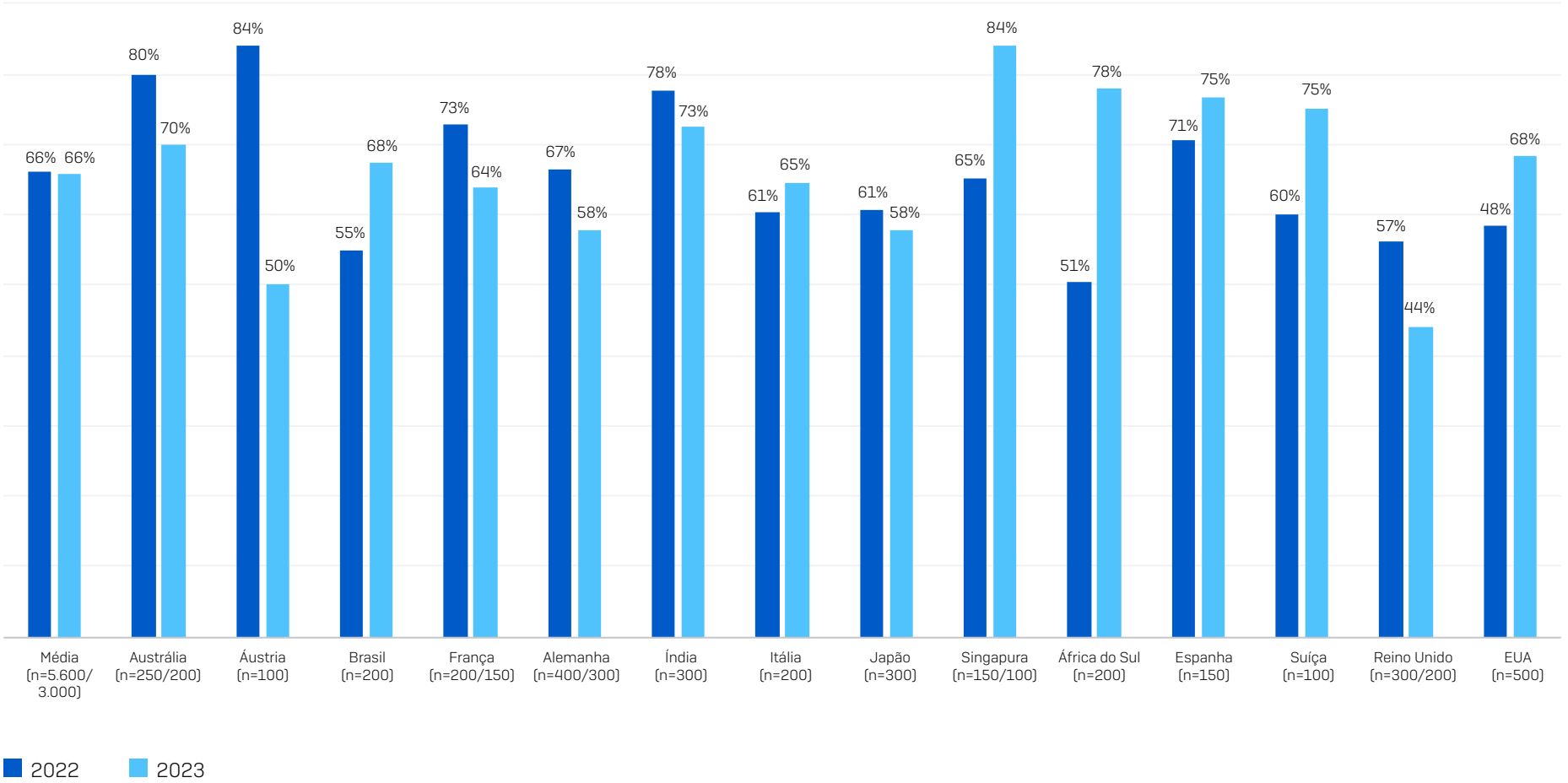
Com o crescimento do modelo de negócio ransomware-as-a-service, não prevemos a diminuição dos ataques para os próximos anos. As organizações deveriam focar em:

- Intensificar seus campos de defesa com:
  - Ferramentas de segurança que as defendam contra os vetores de ataque mais comuns, incluindo proteção de endpoint com intensas capacidades de defesa anti-exploit para prevenir a exploração de vulnerabilidades e Zero Trust Network Access (ZTNA) para frustrar as tentativas de abuso de credenciais comprometidas
  - Tecnologias adaptáveis que respondam automaticamente aos ataques, para interromper a ação dos adversários e ganhar tempo para a resposta de suas defesas
  - Detecção, investigação e resposta 24 horas fornecida internamente ou em parceria com um provedor de serviços especializado em Managed Detection and Response (MDR)
- Preparação otimizada contra ataques, incluindo backups regulares, prática na restauração de dados de backups e manutenção de um plano de resposta a incidentes atualizado
- Manutenção de uma boa higiene de segurança, incluindo configurações de ferramentas de segurança e patches regularmente revistos e atualizados

Gráficos adicionais

Índice de ataques de ransomware por país: 2022 x 2023

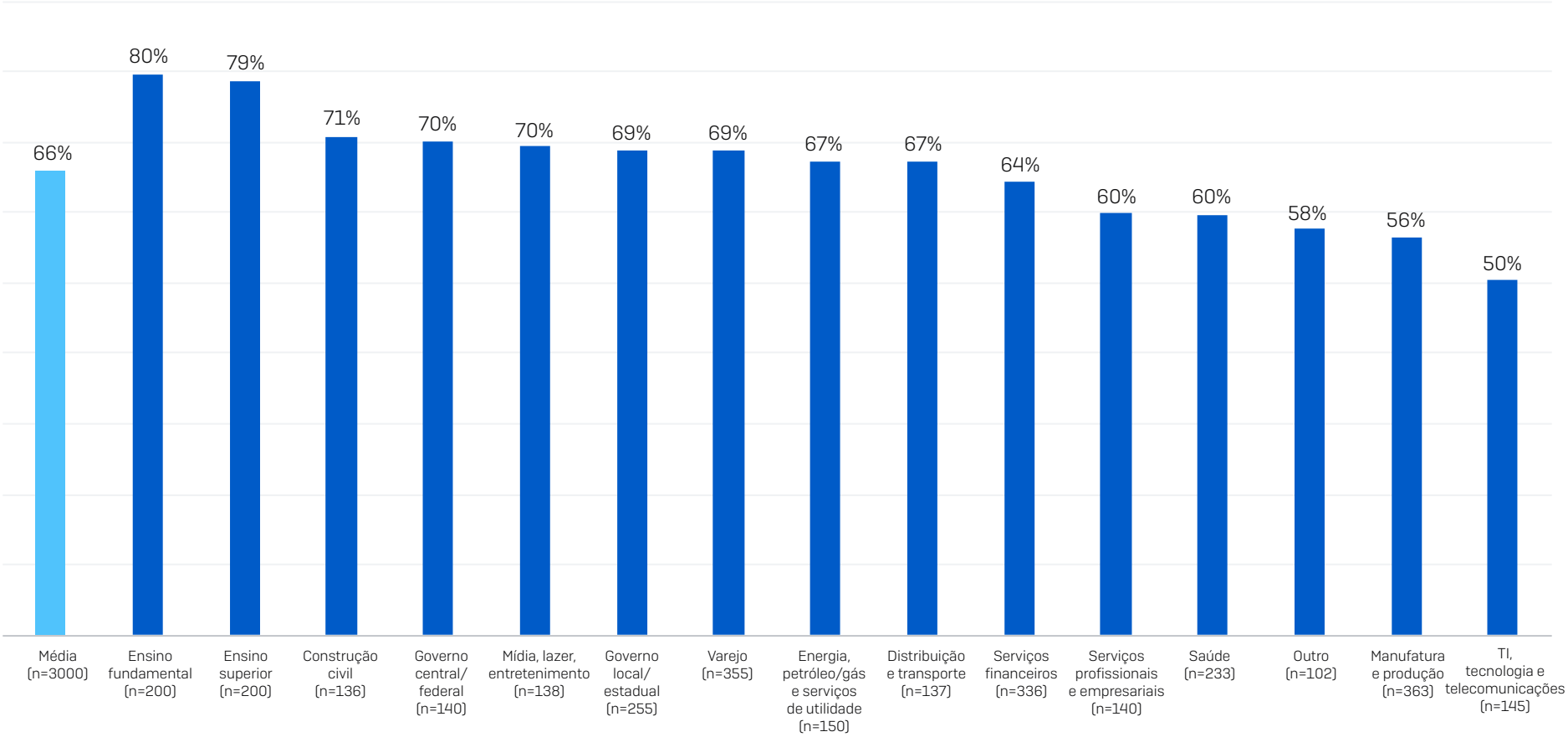
Porcentagem de organizações atingidas por ransomware



Sua organização foi atingida por ransomware neste último ano? Números de base no gráfico

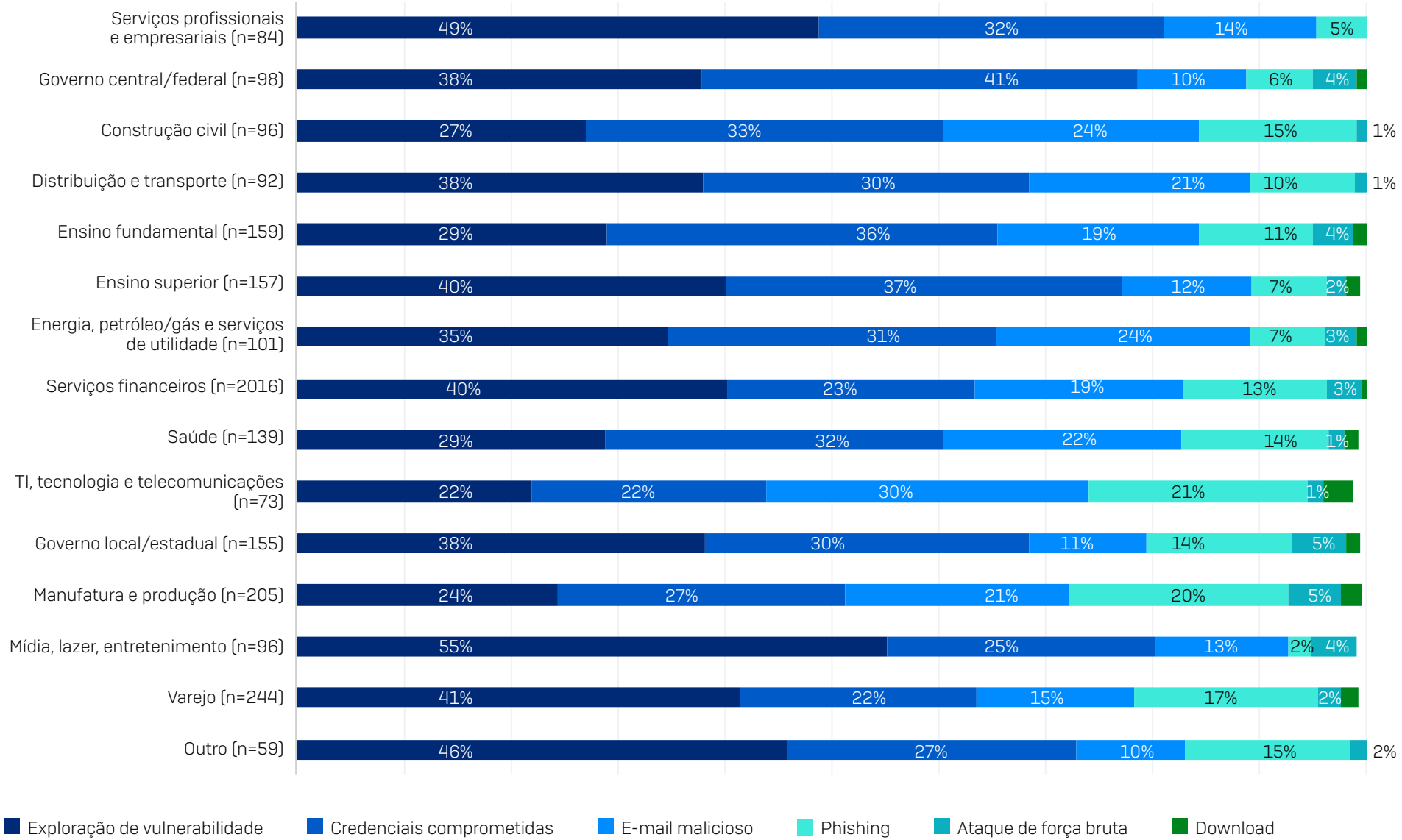
Índice de ataques de ransomware por setor

Porcentagem de organizações atingidas por ransomware



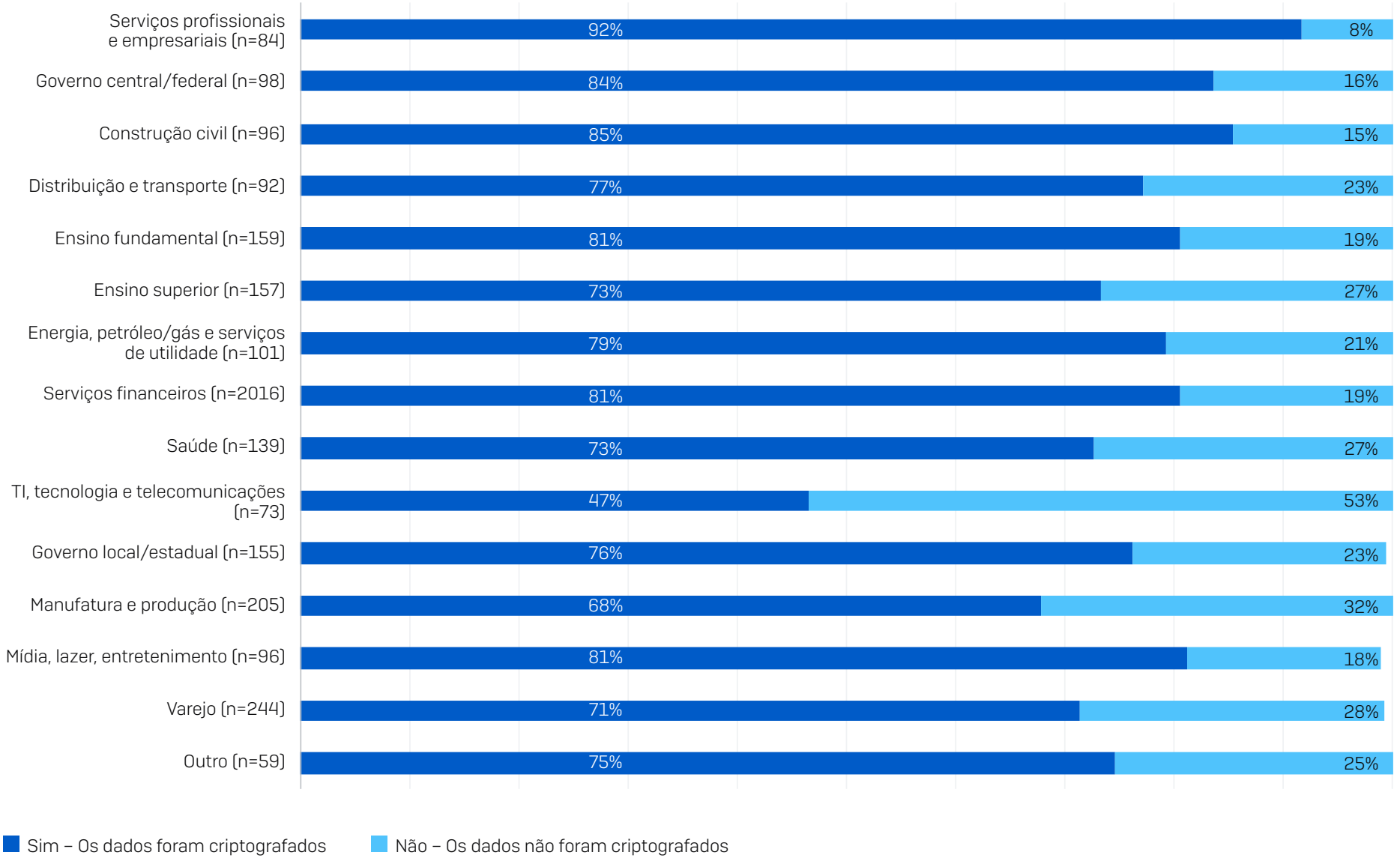
Sua organização foi atingida por ransomware neste último ano? Números de base no gráfico

Causa primária do ataque por setor



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

Criptografia de dados por setor



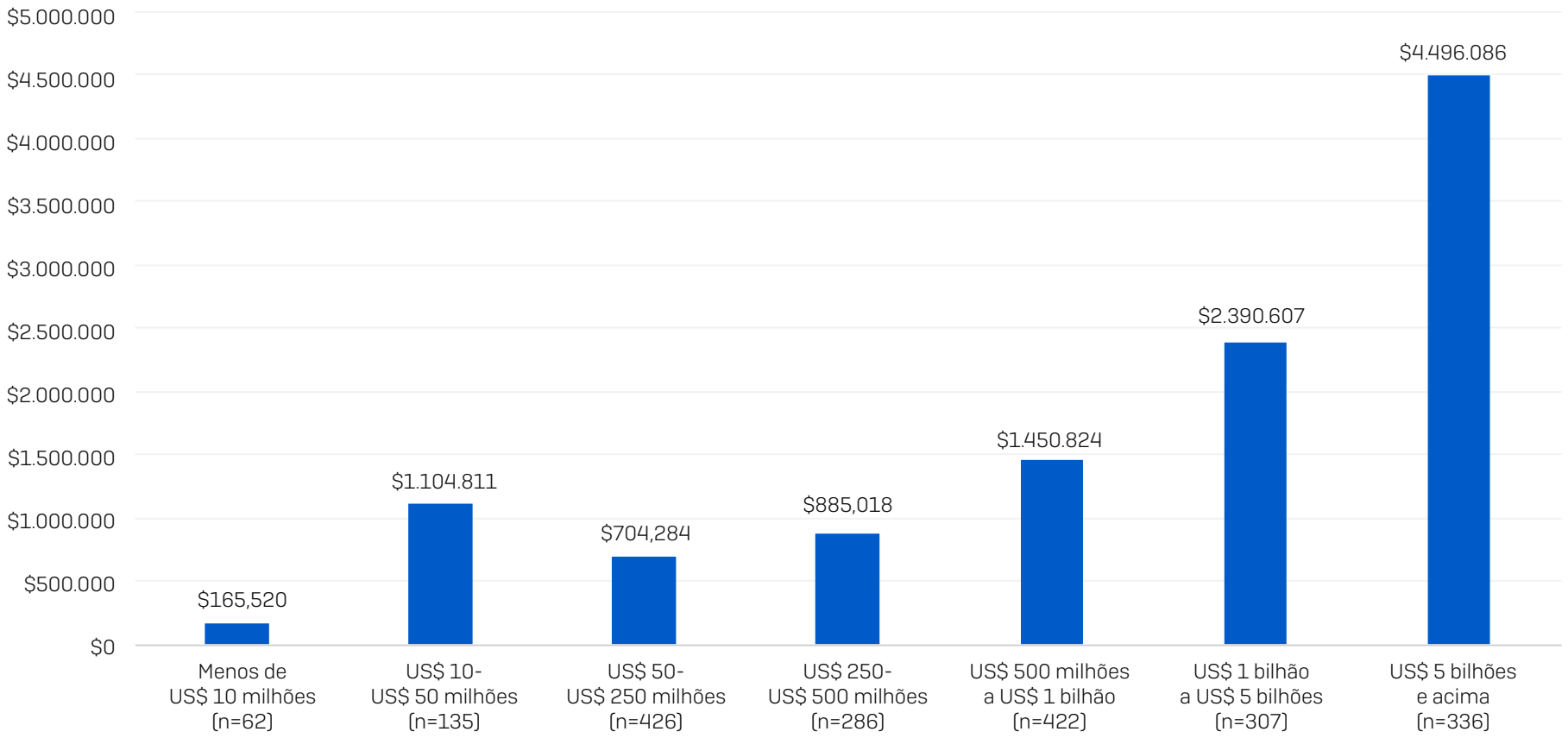
Os criminosos virtuais tiveram sucesso na criptografia de dados da sua organização no ataque de ransomware? Consolidação de opções de resposta. Números de base no gráfico

Recuperação de dados por país

Sua organização conseguiu reaver os dados capturados?

	EUA (N=274)	BRASIL (N=98)	ALEMANHA (N=122)	ÁUSTRIA (N=48)	SUÍÇA (N=68)	REINO UNIDO (N=66)	ITÁLIA (N=82)	ESPANHA (N=93)	FRANÇA (N=68)	ÁFRICA DO SUL (N=139)	ÍNDIA (N=167)	AUSTRÁLIA (N=96)	JAPÃO (N=125)	SINGAPURA (N=51)
Sim, pagamos o resgate e conseguimos reaver os dados	54%	55%	44%	42%	38%	44%	54%	29%	22%	45%	43%	53%	52%	53%
Sim, usamos backups para restaurar os dados	66%	61%	78%	73%	84%	68%	55%	81%	87%	76%	73%	73%	60%	57%
Sim, usamos outros meios para reaver nossos dados	1%	4%	1%	0%	3%	0%	0%	0%	3%	3%	3%	3%	6%	0%
Não, ainda que tenhamos pago o resgate	1%	0%	0%	0%	0%	5%	2%	0%	3%	0%	1%	0%	0%	0%
Não, não pagamos o resgate	0%	1%	2%	2%	1%	2%	5%	2%	0%	0%	1%	1%	5%	10%
Não sabe	0%	0%	2%	0%	0%	0%	0%	0%	0%	0%	0%	0%	0%	0%
Recuperamos os dados usando um método	99%	99%	95%	98%	99%	94%	93%	98%	97%	100%	98%	99%	95%	90%
Usamos mais de um método para recuperar os dados	22%	21%	27%	17%	26%	18%	16%	12%	12%	24%	20%	29%	22%	20%
Pagaram o resgate	55%	55%	44%	42%	38%	48%	56%	29%	25%	45%	44%	53%	52%	53%
Porcentagem dos que pagaram o resgate, mas não conseguiram reaver os dados	1%	0%	0%	0%	0%	9%	4%	0%	12%	0%	3%	0%	0%	0%

Custo médio de recuperação por receita



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.)? Números de base no gráfico.

Metodologia da pesquisa

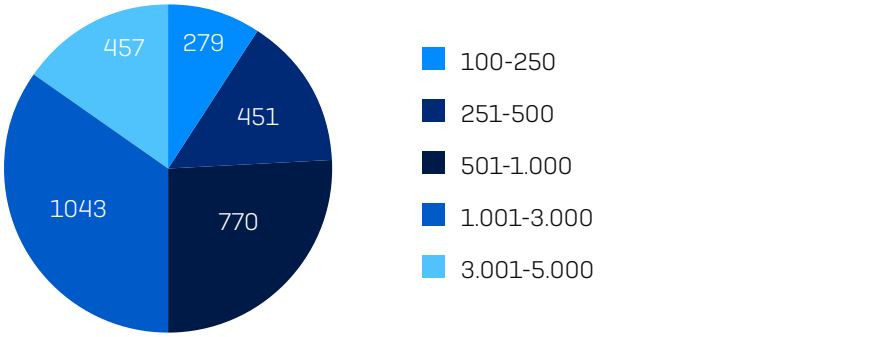
A Sophos encomendou uma pesquisa independente e totalmente desvinculada com 3.000 profissionais na liderança de TI e segurança cibernética que foi realizada entre janeiro e março de 2023. Os entrevistados estavam distribuídos em 14 países entre as Américas, EMEA e Ásia-Pacífico.

Todos os entrevistados eram de organizações com entre 100 e 5.000 funcionários (50% de 100 a 1.000 funcionários, 50% de 1.001-5.000 funcionários). No coorte da pesquisa, a receita anual variou de menos de US$ 10 milhões a mais de US$ 5 bilhões.

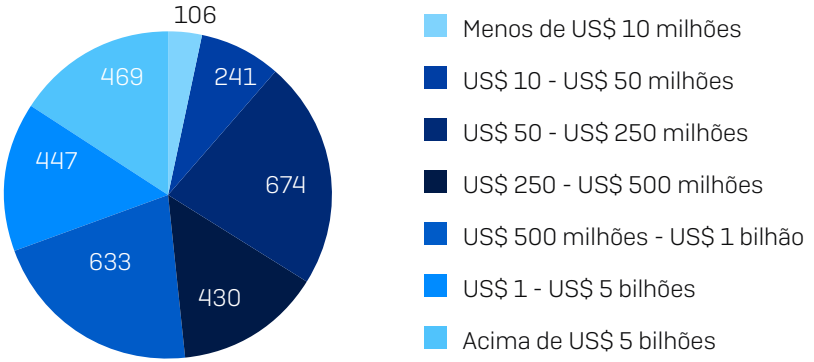
Entrevistados por país

PAÍS	NÚMERO DE ENTREVISTADOS	PAÍS	NÚMERO DE ENTREVISTADOS
Estados Unidos	500	Reino Unido	200
Alemanha	300	África do Sul	200
Índia	300	França	150
Japão	300	Espanha	150
Austrália	200	Áustria	100
Brasil	200	Singapura	100
Itália	200	Suíça	100

Entrevistados por tamanho da organização (nº de funcionários)



Entrevistados por tamanho da organização (receita anual)



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.

2023-05-05 (WP-DD)

SOPHOS