SOPHOS

O Estado do Ransomware 2024

Resultados de uma pesquisa independente e totalmente desvinculada com 5.000 líderes responsáveis pela segurança cibernética e de TI distribuídos em 14 países realizada entre janeiro e fevereiro de 2024.

Documento técnico Sophos. Abril, 2024

Apresentação

O quinto estudo anual da Sophos sobre experiências reais com ransomwares que as organizações enfrentaram mundo afora trata da jornada completa das vítimas, desde o momento que caracterizou a causa primária até o nível de gravidade do ataque, seu impacto financeiro e tempo de recuperação. Insights novos e inusitados combinados com as lições aprendidas em nossos estudos anteriores revelam a realidade que as empresas enfrentam hoje e como o impacto do ransomware evoluiu no decorrer dos últimos cinco anos.

O relatório deste ano também incorpora novas áreas de estudo, que incluem a exploração de pedidos de resgate comparada a pagamentos de resgate, além de focar no impacto que a receita das organizações tem nos resultados do ransomware. Também, pela primeira vez, mostramos o papel das autoridades legais na remediação 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 2024. Estamos cientes de que os entrevistados compartilharam conosco suas experiências relativas ao ano anterior, portanto, muitos dos ataques citados ocorreram em 2023.

Sobre a pesquisa

O relatório se baseia em levantamentos feitos por uma pesquisa independente e totalmente desvinculada encomendada pela Sophos com 5.000 líderes de segurança cibernética e TI distribuídos em 14 países nas Américas, EMEA e Ásia-Pacífico. Todos os entrevistados representaram organizações com entre 100 e 5.000 funcionários. A pesquisa foi realizada pela empresa especializada Vanson Bourne e ocorreu entre os meses de janeiro e fevereiro de 2024, e os participantes 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).

Índice de ataques de ransomware

59% das organizações foram atingidas por ransomware no último ano: uma queda pequena, mas muito bem-vinda em comparação aos 66% registrados nos dois anos anteriores. Mesmo com essa diminuição, mais da metade das organizações passou por um ataque, portanto, não podemos nunca baixar a guarda.

2020	2021	2022	2023	2024
51 %	37 %	66 %	66 %	59 %

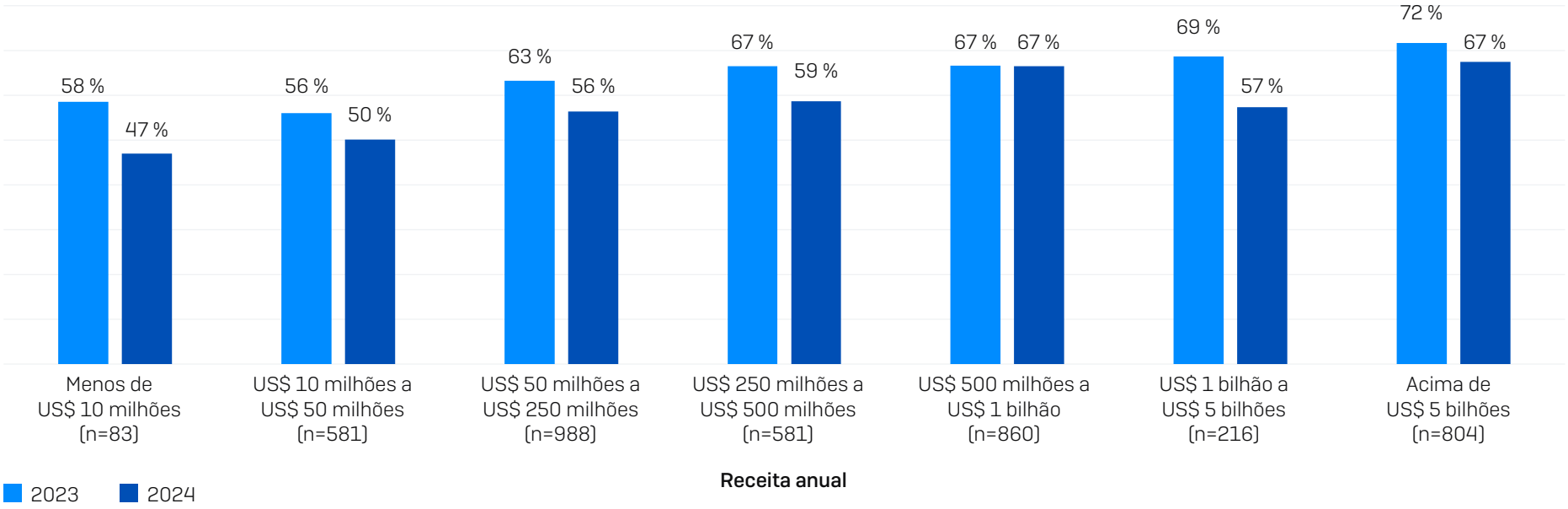
Sua organização foi atingida por ransomware neste último ano?
Sim. n=5.000 (2024), 3.000 (2023), 5.600 (2022), 5.400 (2021), 5.000 (2020).

Ataques por receita

Todas as faixas de receita registraram uma redução no índice de ataques de ransomware no último ano (embora na faixa de US$ 500 milhões a US$ 1 bilhão, esse valor tenha chegado ao mero 1%).

A propensão de ser atingido por um ransomware geralmente aumenta com a receita, com as organizações na faixa acima de US$ 5 bilhões registrando, em conjunto, o mais alto índice de ataques: 67%. Contudo, mesmo as menores organizações (com receita inferior a US$ 10 milhões) são regularmente vitimizadas, com quase metade delas (47%) tendo sido atingida por ransomware no último ano. Muitos ataques de ransomware são executados por quadrilhas sofisticadas e bem-equipadas, mas o uso de ransomwares baratos e grosseiros por bandidos menos qualificados está em ascensão.

Porcentagem de organizações atingidas por ransomwares no ano passado



Sua organização foi atingida por ransomware neste último ano? Sim. n=5.000 (2024), 3.000 (2023). Números de base do segmento de 2024 no gráfico.

Ataques por setor

Com algumas poucas exceções, os índices de ataques de ransomwares foram altamente consistentes entre os diferentes setores, com entre 60% e 68% das organizações atingidas em 11 dos 15 setores cobertos. Os vencedores no estudo deste ano foram os setores do *governo estadual/local* (34%) e do *varejo* (45%), em que menos da metade dos entrevistados relatou ter sido atingida no último ano.

É interessante observar que os dois setores governamentais ocuparam posições opostas, com organizações do *governo central/federal* registrando o mais alto índice de ataques entre todos os setores (68%), o dobro do valor registrado pelas organizações do *governo estadual/local* (34%). Seguindo essa tendência geral de queda em ataques, o valor registrado pelo *governo central/federal* foi mais baixo do que o valor registrado em 2023 de 70%.

Há vários motivos possíveis por trás dessa variação apresentada pelos setores governamentais. Em um ano de grande inquietação, os governos centrais certamente sentiram um aumento nos ataques motivados por facções políticas. Os resultados também podem refletir o empenho das organizações do governo estadual/local em fortalecer sua resiliência a ataques, ou uma guinada na abordagem dos adversários em resposta à capacidade limitada do setor do governo estadual/local em pagar resgates.

Outras mudanças notáveis no setor no último ano incluem:

- Redução na mais alta taxa individual de ataques registrada: de 80% (*ensino fundamental*) para 69% (*governo central/federal*)
- O setor da educação não mais apresenta os dois índices de ataque mais altos, com 66% (*ensino superior*) e 63% (*ensino fundamental*) registrados este ano em comparação a 79% e 80% no ano anterior, respectivamente
- *Saúde* foi um dos cinco setores que registraram um aumento no índice de ataques no último ano, subindo de 60% para 67%
- *TI, tecnologia e telecomunicações* não é mais o setor com o mais baixo índice de ataques, com 55% das organizações atingidas no último ano, registrando um aumento dos 50% relatados em 2023

Consulte o apêndice para ver os índices de ataques de ransomware por setor em mais detalhes.

Ataques por país

A França registrou o mais alto índice de ataques de ransomware em 2024, com 74% dos entrevistados dizendo que foram atingidos no último ano, seguida pela África do Sul (69%) e Itália (68%). Em contrapartida, o Brasil (44%), o Japão (51%) e a Austrália (54%) apresentaram os menores índices de ataque relatados pelos entrevistados.

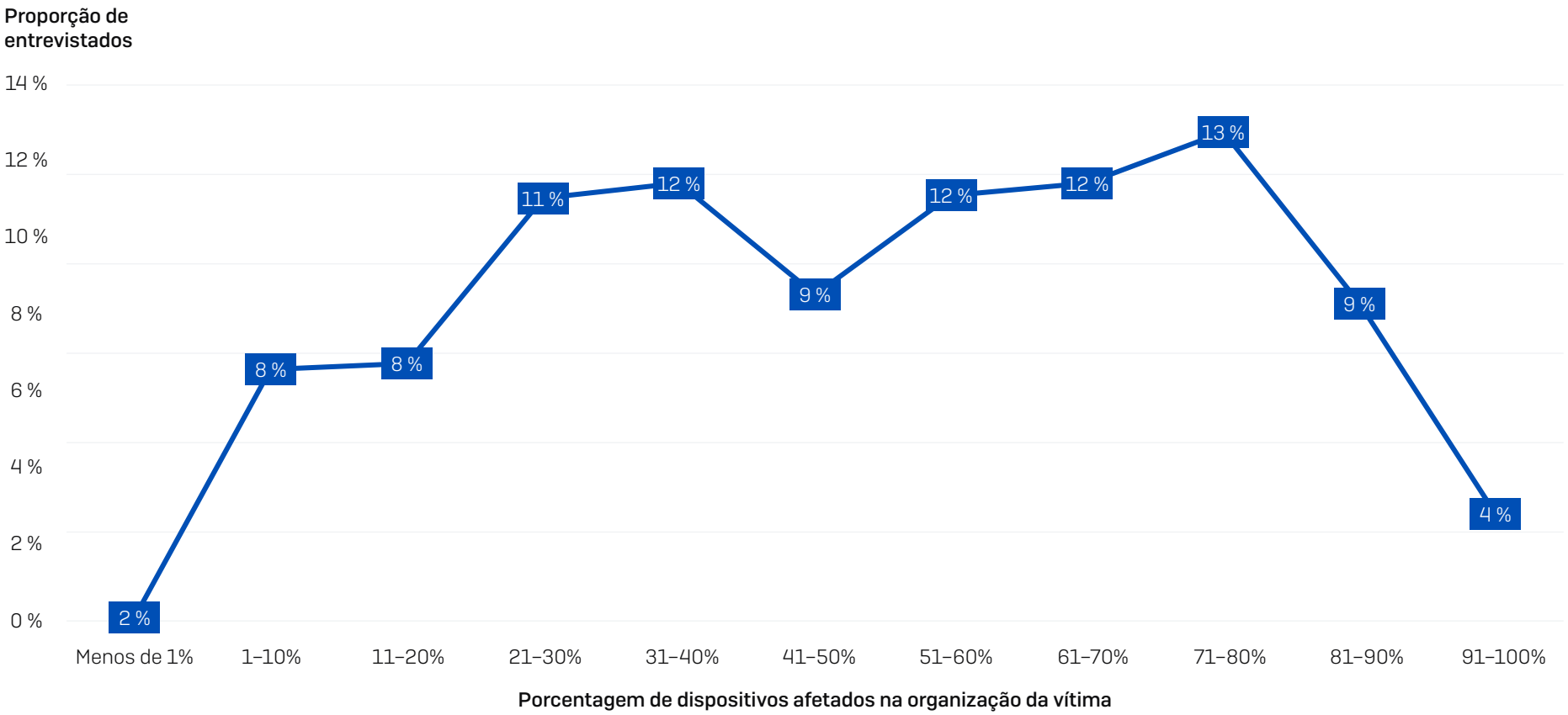
No geral, nove países relataram um índice menor de ataques do que em 2023. Os cinco países que registraram um índice mais alto de ataques do que em 2023 estão todos na Europa: Áustria, França, Alemanha, Itália e Reino Unido (a Alemanha registrou um aumento de menos de 1%). Talvez isso reflita um aumento no direcionamento de ameaças a organizações europeias, ou que as defesas na Europa não conseguiram acompanhar a evolução no comportamento dos invasores do que em outras áreas geográficas.

Consulte o apêndice para ver os índices de ataques de ransomware por país em mais detalhes.

Porcentagem de computadores afetados

Em média, quase metade (49%) dos computadores das organizações foi afetada por um ataque de ransomware. Ter seu ambiente completamente criptografado é extremamente raro, com apenas 4% das organizações relatando que 91% ou mais de seus dispositivos foram afetados. Tal qual, alguns ataques afetaram apenas alguns poucos dispositivos, o que também é bastante incomum, com apenas 2% das organizações impactadas dizendo que menos de 1% de seus dispositivos foi afetado.

Porcentagem de dispositivos afetados na organização da vítima



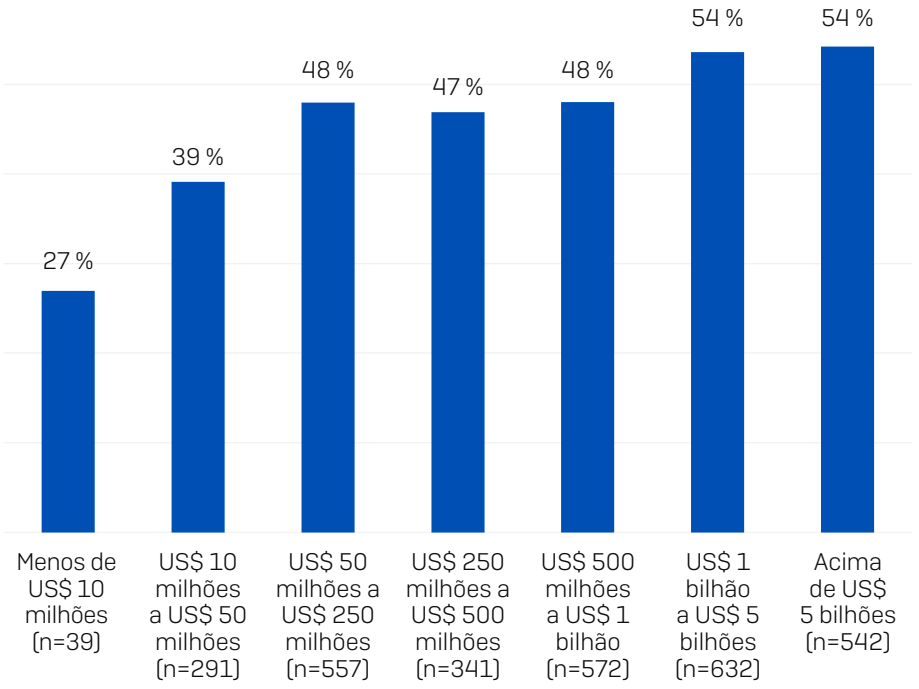
Qual a porcentagem de computadores da sua organização que foi afetada por ransomware no último ano? n=2.974 organizações atingidas por ransomware.

Porcentagem de computadores afetados por receita

Mundialmente, houve uma distribuição plena entre todos os entrevistados, mas observamos uma variação considerável em dispositivos afetados por tamanho da organização e setor.

Conforme a receita aumenta, aumenta também a proporção do patrimônio digital que foi impactada pelo ataque de ransomware, com as organizações menores (abaixo de US$ 10 milhões) registrando metade da porcentagem de dispositivos afetados comparativamente com as organizações com receita de US$ 1 bilhão ou mais (27% x 54%).

Existem vários fatores que podem ter contribuído para isso. Organizações menores são menos propensas a centralizar o gerenciamento de seus dispositivos, diminuindo as chances dos ataques se espalharem por todo o seu patrimônio digital. Além disso, muitas das pequenas empresas e startups são grandes usuárias de plataformas SaaS, o que reduz o risco de interrupção dos negócios por ameaças como ransomware.



Qual a porcentagem de computadores da sua organização que foi afetada por ransomware no último ano? n=2.974 organizações atingidas por ransomware.

Porcentagem de computadores afetados por setor

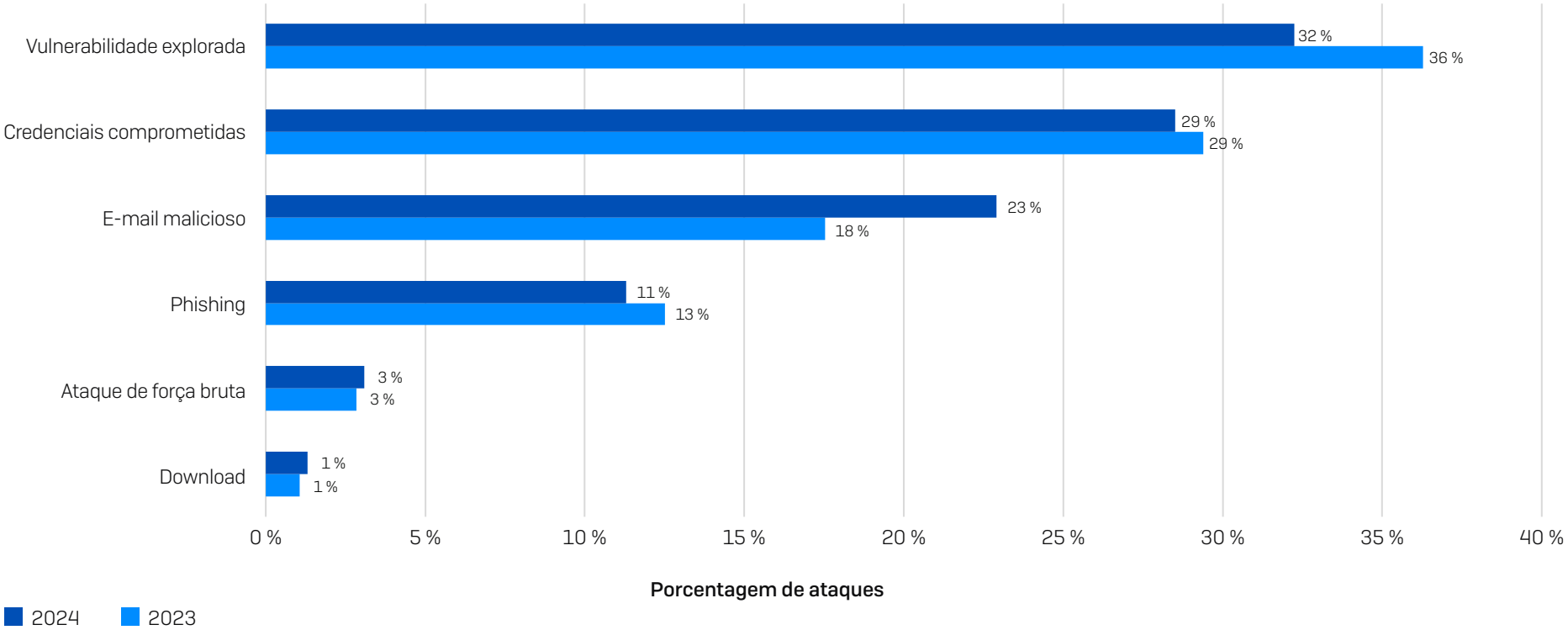
TI, tecnologia e telecomunicações registrou o menor índice percentual de dispositivos afetados (33%), refletindo a forte postura cibernética geralmente observada no setor. Em contrapartida, o setor de *energia, petróleo/gás e serviços de utilidade* foi o que mais sentiu os efeitos dos ataques, com 62% de dispositivos afetados, em média, seguido pelo setor de *saúde* (58%). Os dois setores lutam contra o alto volume de controles estruturais e tecnologias legados do que a maioria dos outros setores, o que dificulta proteger os dispositivos, limitar os movimentos laterais e evitar que os ataques se propaguem.

Consulte o apêndice para ver a porcentagem de computadores afetados por setor em mais detalhes.

Causas primárias dos ataques de ransomware

99% das organizações atingidas por ransomware foram capazes de identificar a causa primária do ataque, tendo a exploração de vulnerabilidades como a causa mais comumente identificada como ponto de partida pelo segundo ano consecutivo. No geral, as ocorrências se mantiveram consistentes com o nosso estudo de 2023.

Abordagens baseadas em e-mails foram identificadas como causa primária do ataque por 34% dos entrevistados, com cerca do dobro de ocorrências começando com e-mails maliciosos (uma mensagem com links maliciosos ou anexos que baixam malwares) como phishing (uma mensagem projetada para enganar os destinatários a revelarem informações). Vale observar que o phishing é normalmente usado para roubar detalhes de logon, podendo, assim, ser considerado o primeiro passo em um ataque com credenciais comprometidas.



Você sabe a causa primária do ataque de ransomware que a sua organização enfrentou no último ano? Sim. n=2.974 organizações atingidas por ransomware.

Ataques de exploração de vulnerabilidades

Embora todos os ataques de ransomware resultem em impactos negativos, alguns são mais devastadores do que outros. As organizações cujos ataques começam com a exploração de uma vulnerabilidade sem patch relatam resultados mais graves do que aquelas cujos ataques começaram com credenciais comprometidas, incluindo uma maior propensão a:

- Ter seus backups comprometidos
  (índice de sucesso de 75% x 54% para credenciais comprometidas)
- Ter seus dados criptografados
  (índice de criptografia de 67% x 43% para credenciais comprometidas)
- Pagar o resgate
  (índice de pagamento de 71% x 45% para credenciais comprometidas)
- Cobrir os custos totais do resgate internamente (custeio total do resgate internamente de 31% x 2% para credenciais comprometidas)

Também relatam:

- Custos gerais de recuperação pós-ataque 4 vezes maior
  (US$ 3 milhões x US$ 750 mil para credenciais comprometidas)
- Tempo de recuperação mais lento (45% levaram mais de um mês x 37% para credenciais comprometidas)

Para obter mais detalhes, leia Vulnerabilidades sem patches: o vetor de ataque de ransomware mais cruel.

Causa primária por setor

Alguns pontos fracos nas defesas cibernéticas são mais predominantes em alguns setores do que em outros, e os adversários sabem muito bem disso. Consequentemente, a causa primária dos ataques de ransomware varia consideravelmente por setor:

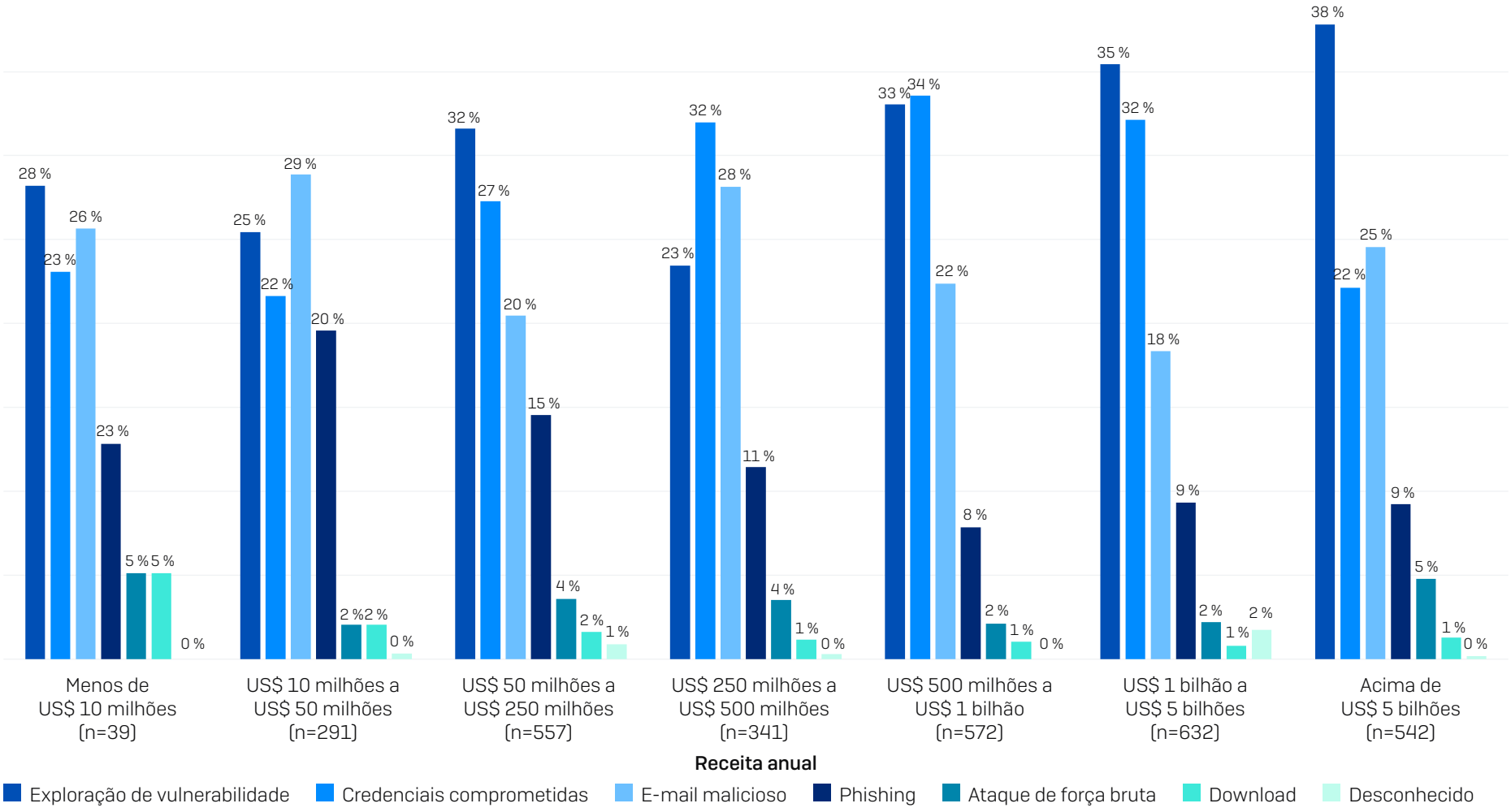
- *Energia, petróleo/gás e serviços de utilidade* é o setor com maior probabilidade de ser vítima da exploração de uma vulnerabilidade por falta de patches, e quase metade (49%) dos ataques começa dessa forma. Esse setor costuma utilizar uma proporção mais alta de tecnologias obsoletas que estão mais propensas a apresentar falhas de segurança do que muitos dos outros setores, o que significa que talvez não haja patches disponíveis para as soluções legadas e no fim de sua vida útil.
- As organizações do governo são particularmente vulneráveis a ataques que começam com o abuso de credenciais comprometidas: 49% (*estadual/local*) e 47% (*central/federal*) dos ataques começaram com o uso de dados de logon roubados
- *TI, tecnologia e telecomunicações* e *varejo* relataram que 7% dos incidentes de ransomware começaram com um ataque de força bruta — isso talvez porque a exposição desses setores a vulnerabilidades sem patches e comprometimento de credenciais seja tão improvável que os adversários se veem obrigados a buscar outras frentes de ataque

Consulte o apêndice para ver os índices de causa primária de ataque por setor em mais detalhes.

Causa primária por receita

Em termos gerais, as grandes organizações são mais propensas a passar por um ataque que comece com uma vulnerabilidade sem patch, com aquelas na faixa acima de US$ 5 bilhões relatando o mais alto porcentual de ataques que começaram dessa forma (38%). Provavelmente porque, conforme as organizações crescem, suas infraestruturas de TI também aumentam em tamanho e complexidade, dificultando para as equipes de TI ter uma amplitude de visão que abranja todos os seus pontos de exposição para aplicar patches antes que eles sejam explorados.

Credenciais comprometidas são um vetor de ataque de ransomware que se intensifica nos coortes formados por empresas de receita média e alta, sendo a principal causa dos ataques nas faixas de receita de US$ 250 milhões a US$ 500 milhões e de US$ 500 milhões a US$ 1 bilhão. As vulnerabilidades e credenciais comprometidas recebem grande foco e atenção, mas os e-mails maliciosos são a causa primária relatada pelas organizações na faixa de US$ 10 milhões a US$ 50 milhões. No geral, ameaças baseadas em e-mails são responsáveis por quase metade (49%) dos ataques nesse segmento.



Você sabe a causa primária do ataque de ransomware que a sua organização enfrentou no último ano? n=2.974 organizações atingidas por ransomware.

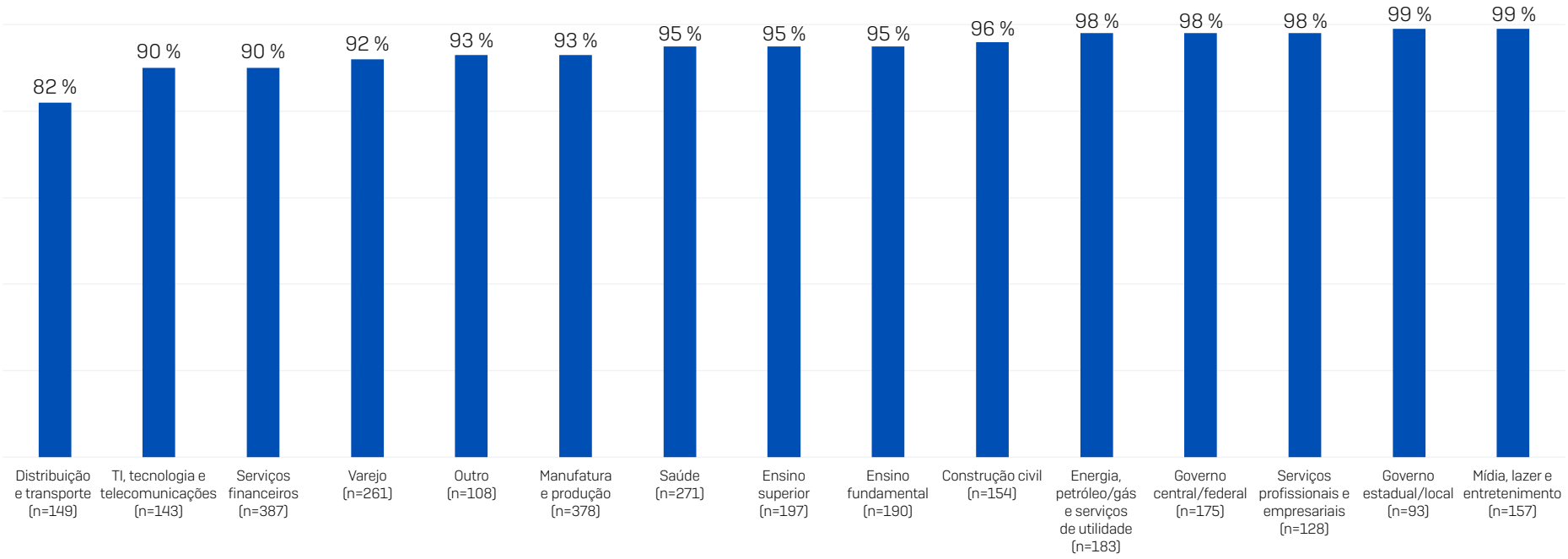
Comprometimento de backup

As duas maneiras mais frequentes de recuperar dados criptografados em um ataque de ransomware são: restaurá-los de backups e pagar pelo resgate. Com o comprometimento dos backups das organizações, os adversários podem restringir a capacidade de suas vítimas recuperarem seus dados criptografados e aumentar a pressão para o pagamento do resgate.

Tentativas de comprometimento de backup

94% das organizações atingidas por ransomware no último ano disseram que os criminosos cibernéticos tentaram comprometer seus backups durante o ataque. Esse índice sobe para 99% quando se trata do setor do *governo estadual/local* e do setor de *mídia, lazer e entretenimento*. O mais baixo índice de tentativa de comprometimento foi relatado pelo setor de *distribuição e transporte*, contudo, mesmo nele, mais de oito em cada dez (82%) organizações atingidas pelo ransomware disseram que os invasores tentaram acessar seus backups.

Porcentagem de ataques que foram tentativas de adversários de comprometer backups



Os criminosos cibernéticos tentaram comprometer os backups da sua organização? Sim. Número de base no gráfico.

Taxa de sucesso de tentativas de comprometimento de backup

Entre todos os setores, 57% das tentativas de comprometimento de backup foram bem-sucedidas, o que significa que os adversários foram capazes de afetar as operações de recuperação pós-ransomware em mais da metade de suas vítimas. A análise revela uma variação marcante na taxa de sucesso do adversário por setor:

- Os invasores demonstraram maior probabilidade de sucesso no comprometimento dos backups de suas vítimas nos setores de *energia, petróleo/gás e serviços de utilidade* (79% de taxa de sucesso) e da *educação* (71% de taxa de sucesso)
- Os setores de *TI, tecnologia e telecomunicações* (30% de taxa de sucesso) e do *varejo* (47% de taxa de sucesso) registraram as menores taxas de sucesso no comprometimento de backups

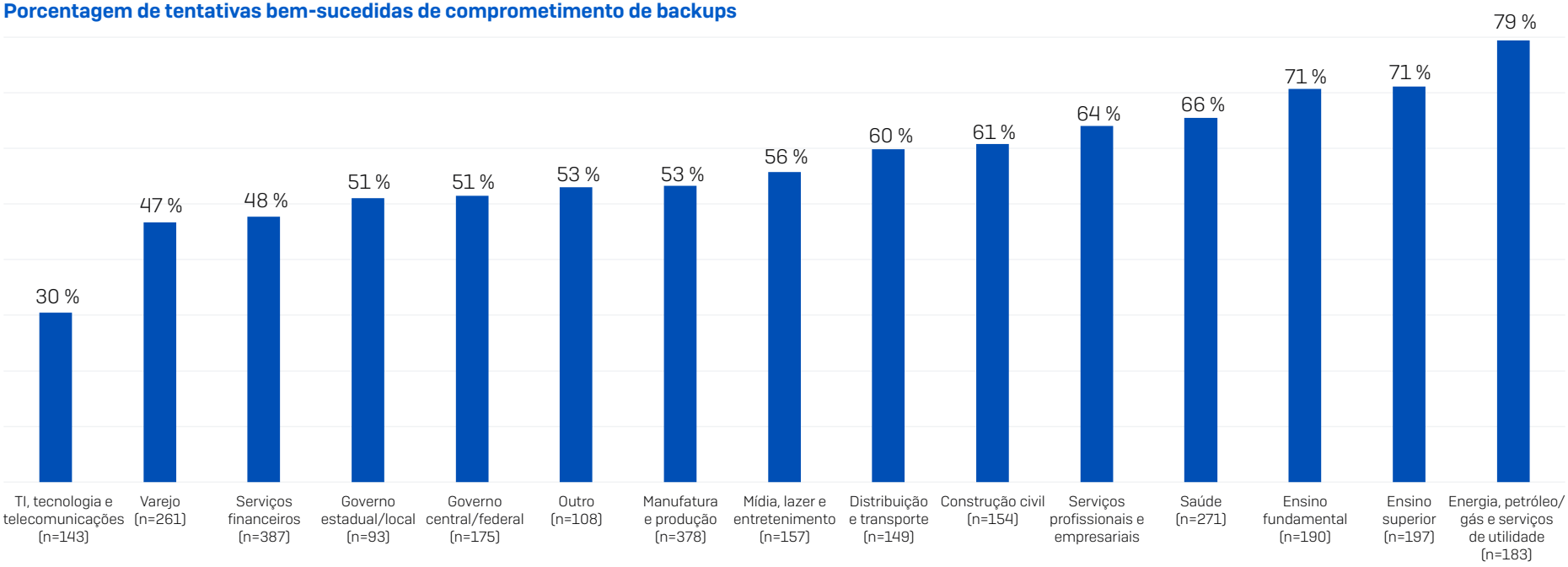
Há vários motivos possíveis por trás das diferentes taxas de sucesso. Um deles pode ser porque o setor de *TI, tecnologia e telecomunicações* apresentou uma proteção de backup mais resiliente contra ataques do que outros setores. Outro motivo pode ter sido a melhor eficiência na detecção e bloqueio das tentativas de comprometimento antes que os invasores conseguissem avançar.

Seja qual for a causa, as organizações que têm backups comprometidos relatam consequências consideravelmente piores do que aquelas cujos backups ficaram ilesos:

- Os pedidos de resgate foram, em média, mais do que o dobro do valor exigido daquelas que não tiveram seus backups afetados, apresentando uma mediana de US$ 2,3 milhões x US$ 1 milhão nos valores de resgate inicial
- As organizações cujos backups foram comprometidos apresentaram quase o dobro de probabilidade de pagar o resgaste para recuperar os dados criptografados (67% x 36%)
- Os custos gerais medianos de recuperação foram oito vezes mais altos (US$ 3 milhões x US$ 375 mil) para as organizações cujos backups foram comprometidos

Para saber mais a fundo, leia O impacto do comprometimento de backups nos resultados de ransomware.

Porcentagem de tentativas bem-sucedidas de comprometimento de backups



Os criminosos cibernéticos tentaram comprometer os backups da sua organização? Sim. Número de base no gráfico.

Índice de criptografia de dados

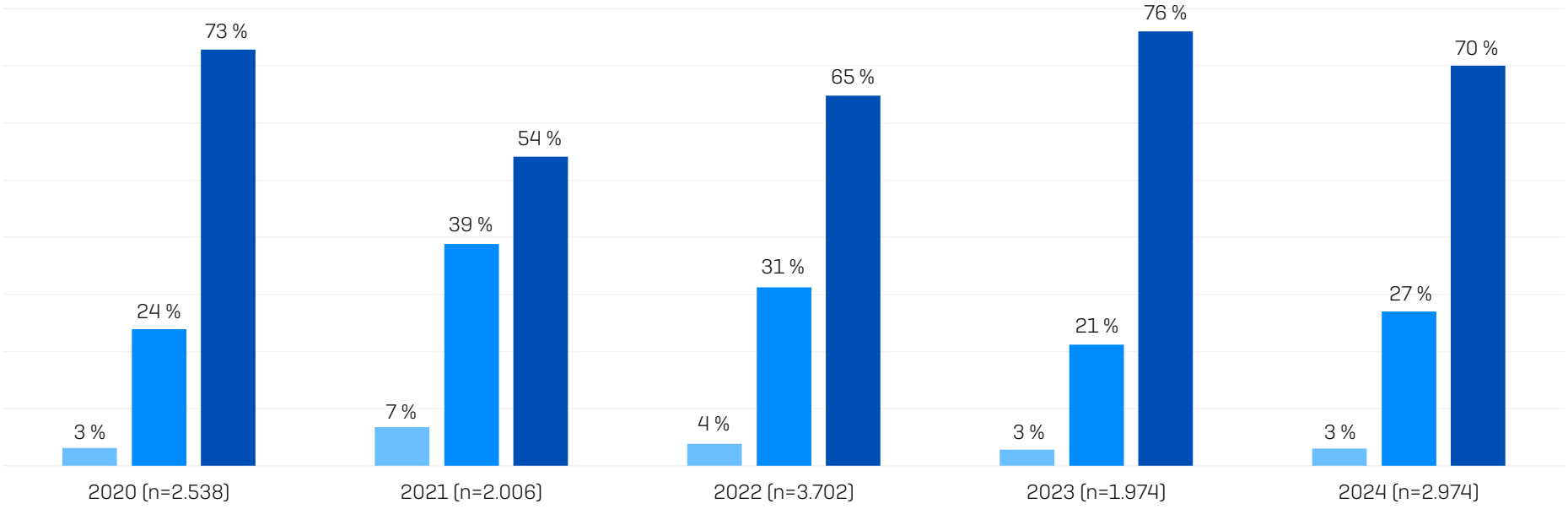
Sete em cada dez (70%) ataques de ransomware no último ano resultaram na criptografia de dados. Ainda que alto, esse valor representa uma pequena queda em relação aos 76% de ataques em que os adversários foram bem-sucedidos na criptografia dos dados conforme relatado em 2023.

Índice de criptografia de dados por setor

A pesquisa de 2024 revela uma variação considerável no índice de criptografa entre os setores.

- O setor de *governo estadual/local* registrou a mais baixa frequência de ataques este ano (34% atingidos por ransomware), mas também registrou o **mais alto índice de criptografia de dados**, com 98% dos ataques resultando em dados criptografados
- O setor de *serviços financeiros* (49%), seguido pelo varejo (56%), apresentou os **mais baixos índices de criptografia de dados**
- *Distribuição e transporte* é o setor que mais provavelmente passou por **ataques de extorsão**, com 17% dizendo que seus dados não foram criptografados, mas que foram feitos reféns mesmo assim — quase três vezes mais do que qualquer outro setor

Consulte o apêndice para ver os índices de criptografia de dados por setor em mais detalhes.



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

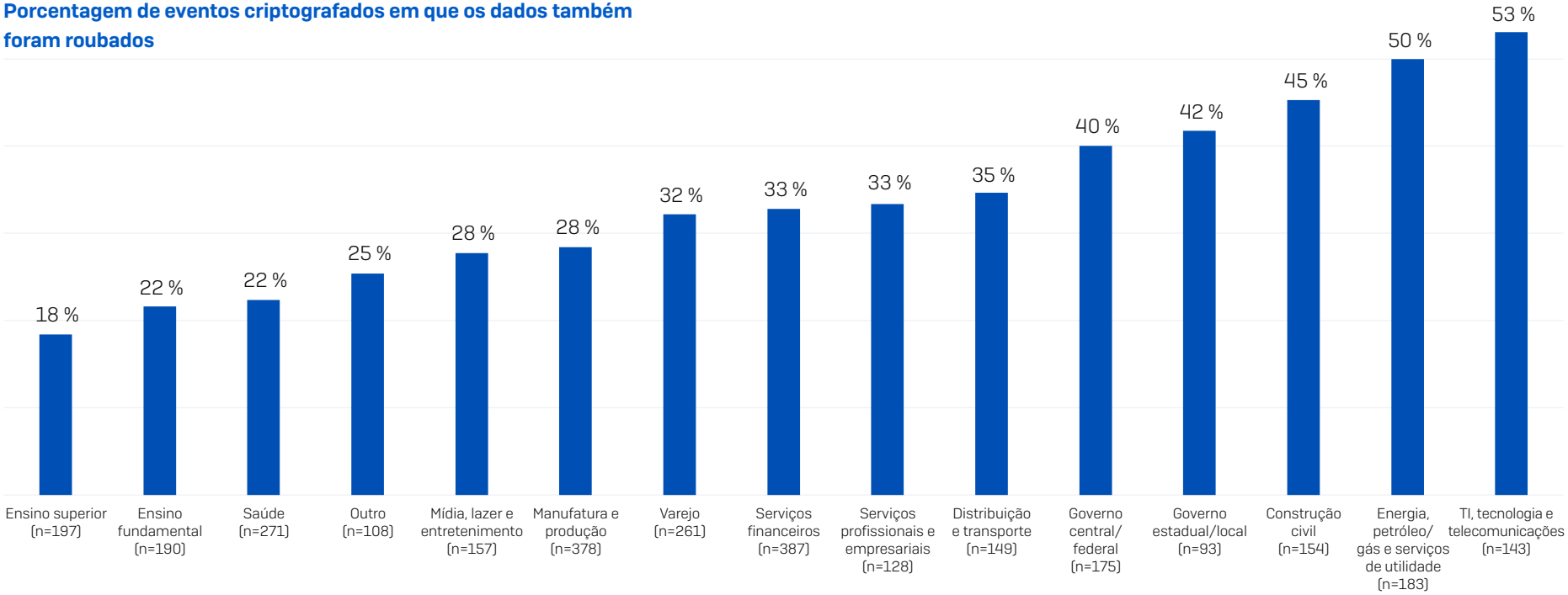
Roubo de dados

Os adversários não apenas criptografam os dados, eles também os roubam. Em 32% dos incidentes em que os dados foram criptografados, eles também foram roubados — ligeiramente acima da taxa do ano passado de 30%. O roubo de dados aumenta a capacidade dos invasores extorquirem dinheiro de suas vítimas, ao mesmo tempo em que lhes permite monetizar o ataque com a venda dos dados roubados na dark Web.

Aqui também, a variação por setor foi considerável. Superficialmente, o setor de *TI, tecnologia e telecomunicações* teve o pior desempenho, com 53% dos ataques em que os dados foram criptografados relatando que eles também foram roubados. O setor de *energia, petróleo/gás e serviços de utilidade* ficou em segundo lugar, tendo seus dados roubados em 50% dos eventos de criptografia. Por outro lado, o setor de educação é o menos propenso a relatar o roubo de dados em um ataque, com o *ensino superior* registrando a mais baixa propensão geral de dados criptografados e roubados (18%), seguido pelo *ensino fundamental*, que divide o segundo lugar com o setor de saúde (ambos com um índice de 22%).

Esses resultados refletem os diferentes níveis de capacidade de investigação entre os setores e suas diferenças em prioridade. Determinar se os dados foram ou não exfiltrados exige altos níveis de habilidades forenses e, frequentemente, conta com os logs registrados por ferramentas EDR/XDR. Pode ser também que o setor de *TI, tecnologia e telecomunicações* simplesmente esteja mais bem preparado para identificar o roubo de dados do que outros setores. A simplicidade de muitos ambientes como os de *energia, petróleo/gás e serviços de utilidade* também facilita a detecção de roubo no setor. Inversamente, as escolas geralmente carecem de competências e ferramentas para determinar se os dados foram ou não foram roubados. Além disso, algumas organizações talvez prefiram não saber se seus dados foram exfiltrados, pois a violação de dados exigiria delas caros processos de divulgação.

Porcentagem de eventos criptografados em que os dados também foram roubados



Os criminosos virtuais tiveram sucesso na criptografia de dados da sua organização no ataque de ransomware? Sim. Sim, e os dados também foram roubados. Número de base no gráfico.

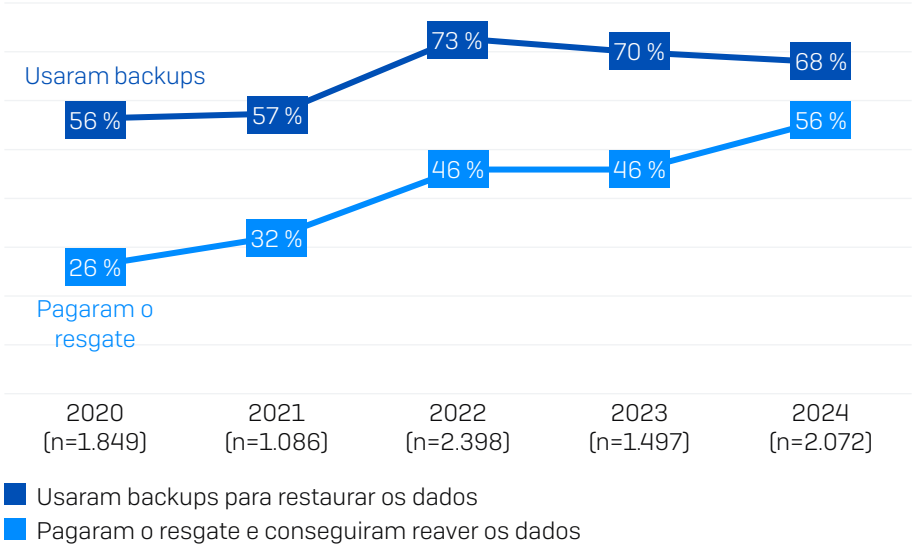
Recuperação dos dados

98% das organizações que tiverem seus dados criptografados conseguiram reavê-los. As duas formas principais de recuperar dados foram restaurá-los de backups (68%) e pagar o resgate para obter a chave de descriptografia (56%). 26% das organizações que tiveram dados criptografados indicaram que usaram "outros meios" para reaver seus dados — a pesquisa não explorou essa área em profundidade, mas esses meios incluiriam trabalhar em colaboração com as autoridades legais ou usar chaves de descriptografia que já tinham sido publicadas.

Usam backups para restaurar dados	Pagaram resgate e conseguiram reaver os dados	Usam outros meios para reaver os dados
68 %	**56 %**	**26 %**

Uma mudança que se nota em comparação ao último ano é o aumento na propensão das vítimas usarem diferentes abordagens para recuperar os dados criptografados, como, por exemplo, pagar o resgate e usar backups. Quase metade das organizações que tiveram seus dados criptografados disse ter usado mais de um método (47%), mais do que o dobro de 2023 (21%).

Este gráfico cobre um intervalo de cinco anos e mostra que a diferença entre o uso de backups e o pagamento de resgate continua a diminuir. O uso de backups caiu levemente pelo segundo ano consecutivo. Concomitantemente, houve um aumento de 10 pontos percentuais no pagamento de resgaste desde o estudo de 2023. A propensão a pagar o resgate depende de muitos fatores, incluindo a disponibilidade de backups. Contudo, essa é uma tendência preocupante e indica que mais da metade das vítimas está predisposta a pagar pela chave de descriptografia.



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 receita

A propensão a pagar o resgate para recuperar os dados geralmente aumenta com a receita. As organizações com baixas receitas (menos de US$ 10 milhões) relataram o mais baixo índice de pagamento de resgaste (25%), enquanto as organizações com as maiores receitas (acima de US$ 5 bilhões) apresentaram o mais alto índice de pagamento (61%). A disponibilidade de fundos para cobrir o resgate é um dos fatores de maior peso nesse cenário, já que muitas das pequenas empresas simplesmente não têm como levantar o dinheiro para pagar o resgate.

Contudo, como se vê, a recuperação de dados não é uma questão de backups ou resgates. As nuanças por trás dos métodos de recuperação de dados se tornam aparentes quando nos aprofundamos nos dados e comparamos os valores de 2024 com os resultados do ano anterior.

Excluindo-se o grupo daqueles abaixo de US$ 10 milhões, todos os segmentos de receita mostraram um aumento no índice de pagamento de resgate em comparação ao último ano, e três deles também mostraram um aumento no uso de backups para restaurar os dados. O grupo de menor receita relatou o mais alto índice de uso de backups (88%), seguido de perto pelo grupo de US$ 250 milhões a US$ 500 milhões (85%).

Recuperação de dados por setor

Como seria de se esperar, o setor do *governo central/federal* é o menos propenso a pagar um resgate para reaver dados — e devido a regulamentações, sua capacidade de pagá-lo é altamente limitada — e o que relatou o mais alto uso de backups para restaurar dados (39% e 81%, respectivamente).

No geral, não há uma correlação direta entre o uso de backups e o pagamento de resgates:

- *Mídia, lazer e entretenimento* registrou o mais alto índice de pagamento de resgate para recuperar dados (69%) e também um dos mais altos índices de uso de backups (74%)
- *Energia, petróleo/gás e serviços de utilidade* apresenta o mais baixo índice de uso de backups (51%) e um índice de pagamento de resgate de 61%, mais baixo do que outros quatro setores

Consulte o apêndice para ver o método de recuperação de dados por setor em mais detalhes.

	RECEITA ANUAL													
	Menos de US$ 10 milhões (n=39)		US$ 10 milhões a US$ 50 milhões (n=291)		US$ 50 milhões a US$ 250 milhões (n=557)		US$ 250 milhões a US$ 500 milhões (n=341)		US$ 500 milhões a US$ 1 bilhão (n=572)		US$ 1 bilhão a US$ 5 bilhões (n=632)		Acima de US$ 5 bilhões (n=542)	
Método de recuperação de dados usado	2023	2024	2023	2024	2023	2024	2023	2024	2023	2024	2023	2024	2023	2024
Usaram backups para restaurar os dados	80 %	88 % ▲	72 %	68 % ▼	77 %	60 % ▼	75 %	85 % ▲	68 %	70 % ▲	66 %	65 % ▼	63 %	66 % ▲
Pagaram resgate e conseguiram reaver os dados	36 %	25 % ▼	41 %	49 % ▲	42 %	57 % ▲	33 %	50 % ▲	51 %	59 % ▲	52 %	56 % ▲	55 %	61 % ▲

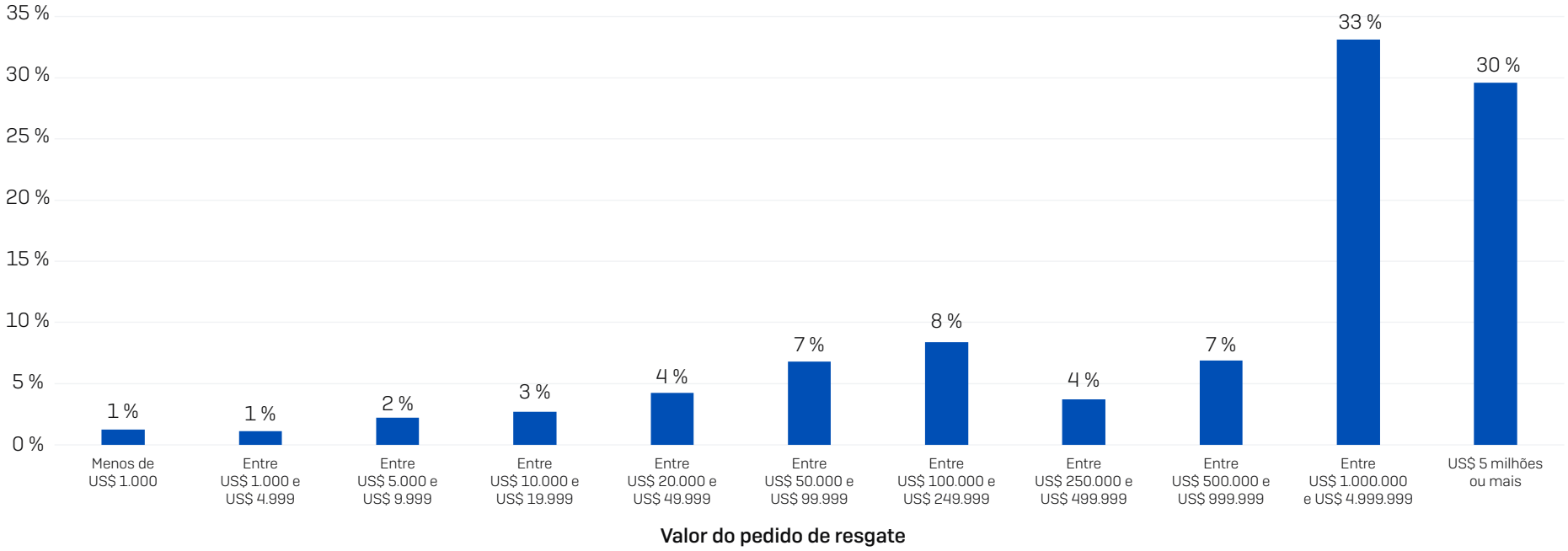
Sua organização conseguiu reaver os dados capturados? Sim, pagamos o resgate e recuperamos os dados; Sim, usamos backups para restaurar os dados. Números de base de 2024 no gráfico. As setas indicam acréscimo/decréscimo em relação a 2023.

Pedidos de resgate

Este é o primeiro ano que incluímos pedidos e pagamentos de resgate no relatório. Entre as 1.701 organizações que tiveram seus dados criptografados e que puderam mencionar o resgate inicial exigido pelos invasores, o valor médio exigido foi US$ 4.321.880 e a mediana foi US$ 2 milhões.

Uma das descobertas mais notáveis no estudo deste ano é que 63% dos pedidos de resgate foram de US$ 1 milhão ou mais, com 30% dos pedidos acima dos US$ 5 milhões. Ainda que um pequeno número de entrevistados tenha relatado pedidos de resgate de quatro dígitos, esses se categorizam como extrema minoria.

Porcentagem dos pedidos do valor do resgate



Qual foi o valor do pedido de resgate exigido pelos invasores? n=1.701

Pedido de resgate por receita

Analisando os dados de média e mediana, a tendência em pedidos de resgate sobe de acordo com a receita, o que indica que os adversários ajustam o valor do resgate com base, ao menos parcialmente, na capacidade de pagamento.

Grandes pedidos de resgate não são mais privilégio exclusivo das organizações com altas receitas, e valores de US$ 1 milhão ou mais agora são corriqueiros: 47% das organizações com receita de US$ 10 milhões a US$ 50 milhões receberam pedidos de resgate de sete dígitos no último ano.

Pedido de resgate por setor

Nesta disputa não há vencedores, com todos os setores, exceto o que denominamos "outro", relatando pedidos de resgate em uma faixa mediana de US$ 1 milhão ou mais.

- *Varejo* e *TI, tecnologia e telecomunicações* receberam pedidos de resgate abaixo da faixa mediana (US$ 1 milhão), seguidos pela *construção civil* (US$ 1,1 milhão)
- O setor do *governo central/federal* é o alvo mais comum, registrando os mais altos valores de regaste, tanto em mediana (US$ 7,7 milhões) como na média (US$ 9,9 milhões)

Consulte o apêndice para ver os pedidos de resgate por setor em mais detalhes.

	RECEITA ANUAL					
Pedido de resgate	**US$ 10 milhões a US$ 50 milhões (n=207)**	**US$ 50 milhões a US$ 250 milhões (n=288)**	**US$ 250 milhões a US$ 500 milhões (n=158)**	**US$ 500 milhões a US$ 1 bilhão (n=268)**	**US$ 1 bilhão a US$ 5 bilhões (n=366)**	**Acima de US$ 5 bilhões (n=398)**
Valor médio	$1.774.941	$1.704.853	$3.407.796	$5.184.024	$4.281.258	$7.467.294
Valor mediano	$330.000	$220.000	$840.000	$2.000.000	$3.000.000	$6.600.000

Qual foi o valor do pedido de resgate exigido pelos invasores? Números de base no gráfico. N.B. "Menos de US$ 10 milhões" foi removido da tabela devido ao baixo número de entrevistados nesta faixa de receita.

Pagamentos de resgate

1.097 entrevistados cujas organizações pagaram o resgate informaram a quantia real que foi paga. Analisando os valores de média e mediana, observamos que os pagamentos de resgate aumentaram consideravelmente no último ano:

- Mediana de pagamento: US$ 2.000.000 (aumento de 5 vezes sobre os US$ 400.000 registrados em 2023)
- Média de pagamento: US$ 3.960.917 (aumento de 2,6 vezes sobre os US$ 1.542.330 registrados em 2023)

O gráfico abaixo deixa claro como a proporção de pagamentos de resgate baixos diminuiu gradualmente nos últimos três anos, enquanto a proporção de pagamentos elevados subiu drasticamente. A norma agora são valores de resgate de sete dígitos ou mais.

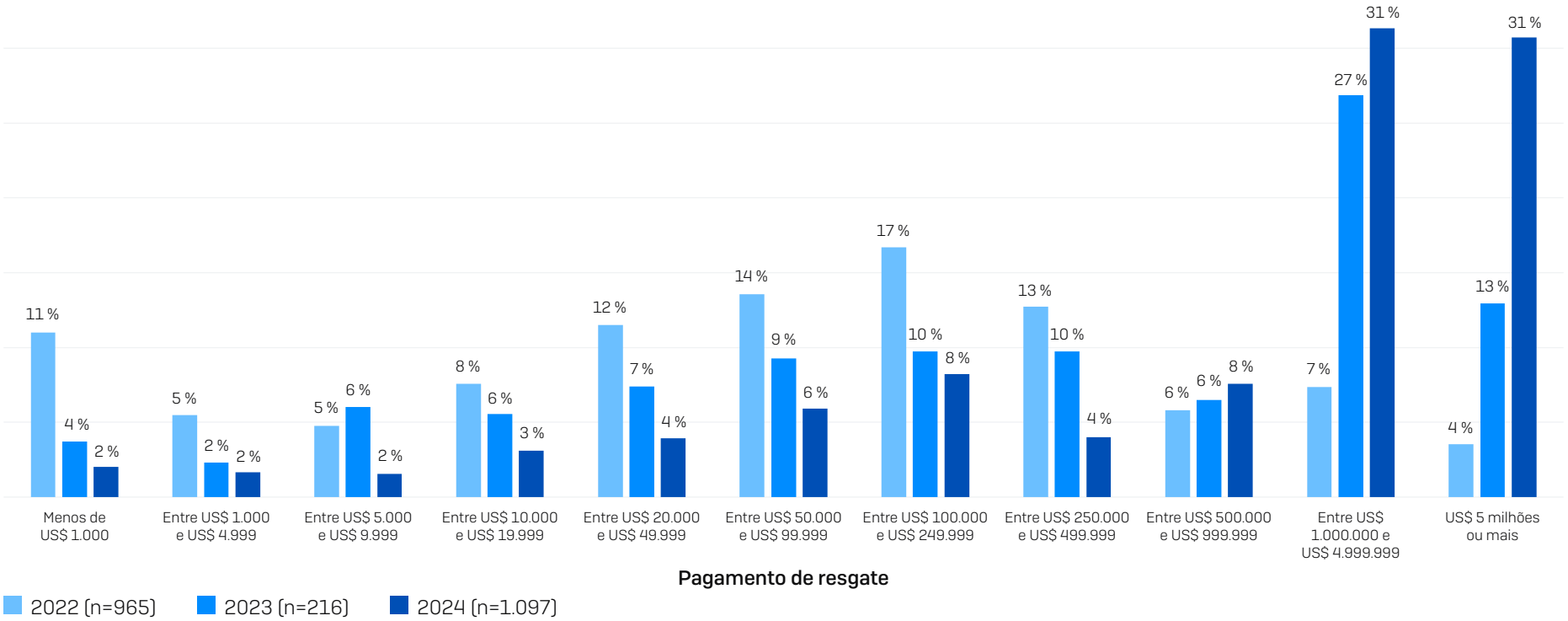
Distribuição dos pagamentos de resgate, 2022-24

Pagamentos de resgate por setor

Da mesma forma que a média dos pedidos de resgate varia consideravelmente por setor, variam também os pagamentos de resgate. O setor de *TI, tecnologia e telecomunicações* registrou a mais baixa mediana de pagamento de resgate (US$ 300.000), seguido por *distribuição e transporte* (US$ 440.000). No outro lado da balança se encontram os setores de *ensino fundamental* e *governo central/federal*, com uma mediana de resgates pagos de US$ 6,6 milhões.

Existe uma ampla correlação entre baixas demandas e baixos pagamentos, mas também há exceções: *distribuição e transporte*, cujo pedido mediano de resgate ficou acima dos US$ 2,8 milhões, pagou, em média, US$ 440.000.

Consulte o apêndice para ver os pagamentos médios de resgate por setor em mais detalhes.



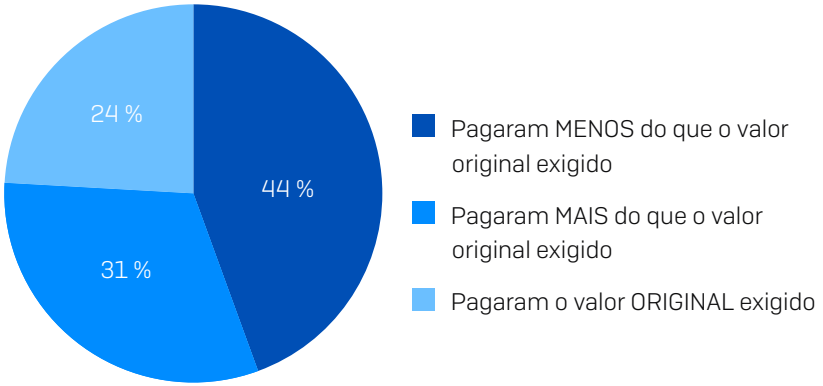
Qual foi o pagamento de resgate que foi efetuado aos invasores? Números de base no gráfico.

Pedido de resgate x Pagamento de resgate

Quando os dados são criptografados, começa a corrida contra o tempo para os envolvidos, com ambos os lados querendo obter os melhores resultados possíveis. As organizações cujos dados foram criptografados tentam minimizar o impacto financeiro, enquanto os adversários tentam assegurar o mais alto retorno monetário possível no mais curto espaço de tempo, ameaçando subir o valor do resgate se o pagamento não for realizado até determinada data, aumentando ainda mais a pressão.

Propensão a negociar o valor do resgate

O estudo revelou que as vítimas raramente pagam a soma inicialmente exigida pelos invasores, com apenas 24% dos entrevistados dizendo que pagaram o valor original do resgate. 44% pagaram menos do que o valor original exigido, enquanto 31% pagaram mais.



Qual foi o valor do pedido de resgate exigido pelos invasores? Qual foi o pagamento de resgate que foi efetuado aos invasores? n=1.097.

Analisando os dados por setor, observamos que dois setores de serviços, *Serviços profissionais e empresariais* e *Serviços financeiros*, foram os mais propensos a tentar negociar o valor do resgate, com 67% dizendo que pagaram menos do que o valor original exigido. O setor de *manufatura e produção* ficou logo atrás, com 65% das organizações que pagaram menos do que o valor inicialmente exigido.

Por outro lado, os setores mais propensos a pagar mais do que o valor original exigido foram aqueles com a mais alta proporção de organizações do setor público:

- *Ensino superior* é o setor mais propenso a pagar valores mais altos do que os exigidos inicialmente (67% pagaram mais) e o menos propenso a pagar valores mais baixos do que os exigidos inicialmente (20% pagaram menos)
- *Saúde* foi o segundo setor mais propenso a pagar valores mais altos do que os exigidos inicialmente (57% pagaram mais), seguido pelo *ensino fundamental* (55% pagaram mais)

Isso pode ser devido aos setores serem menos hábeis para obter acesso a profissionais de negociação de resgate para ajudar a reduzir os custos. Pode ser também que tenham uma maior necessidade de recuperar os dados "a qualquer custo" devido às suas obrigações públicas. Qualquer que seja o motivo, fica claro que existe a possibilidade de negociação entre o valor original exigido e o pagamento final.

Consulte o apêndice para ver pedidos de resgate x pagamentos de resgate por setor em mais detalhes.

Proporção de pedido de resgate pago

Enquanto a negociação do valor do resgate ocorre na maioria dos casos, a oscilação entre o valor exigido e o valor pago foi, em média, muito baixa entre os coortes: 94% dos entrevistados pagaram o montante total exigido.

Aprofundando-nos mais, notamos que todas as faixas de receita, exceto a mais alta de todas, foram capazes de reduzir o valor do pagamento do resgate. A faixa de US$ 50 milhões a US$ 250 milhões pagou a proporção mais baixa do pedido inicial (84%). O único grupo a pagar mais do que o valor inicialmente exigido foi na faixa acima de US$ 5 bilhões, que abrange, em média, 115% do pedido de resgate.

	RECEITA ANUAL					
Coorte	**US$ 10 milhões a US$ 50 milhões (n=100)**	**US$ 50 milhões a US$ 250 milhões (n=206)**	**US$ 250 milhões a US$ 500 milhões (n=104)**	**US$ 500 milhões a US$ 1 bilhão (n=175)**	**US$ 1 bilhão a US$ 5 bilhões (n=233)**	**Acima de US$ 5 bilhões (n=275)**
Proporção de pedido de resgate pago	93 %	84 %	90 %	88 %	85 %	115 %

Qual foi o valor do pedido de resgate exigido pelos invasores? Qual foi o pagamento de resgate que foi efetuado aos invasores? n=1.097. Observação: o coorte "menos de US$ 10 milhões" foi removido do detalhamento por receita anual devido ao baixo número de respostas.

Proporção de pedido de resgate pago por setor

No nível de indústria, vemos que os setores mais propensos a negociar o montante do resgate pagaram o mais baixo percentual do valor exigido inicialmente e vice-versa.

MENOS DE 100%	MAIS DE 100%
Manufatura e produção (70%)	Ensino superior (122%)
Serviços profissionais e empresariais (74%)	Ensino fundamental (115%)
Serviços financeiros (75%)	Saúde (111%)
Outro (79%)	Governo estadual/local (104%)
TI, tecnologia e telecomunicações (82%)	Governo central/federal (103%)
Varejo (84%)	Energia, petróleo/gás e serviços de utilidade (101%)
Construção civil (95%)	
Distribuição e transporte (95%)	
Mídia, lazer e entretenimento (95%)	

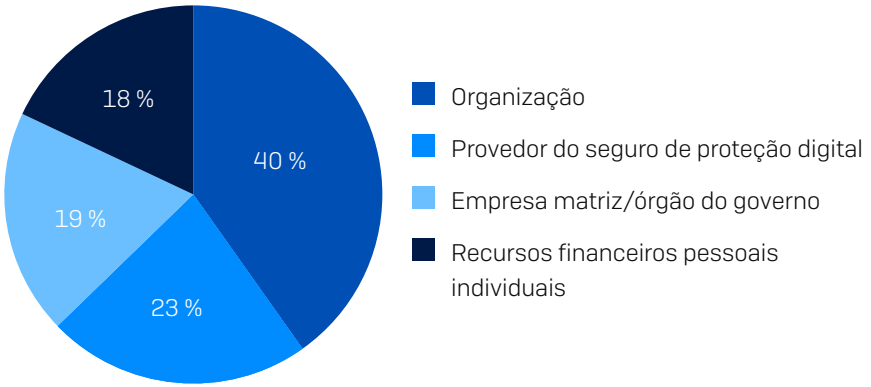
Qual foi o valor do pedido de resgate exigido pelos invasores? Qual foi o pagamento de resgate que foi efetuado aos invasores? n=1.097.

Origem dos fundos de resgate

Quem fornece o dinheiro para pagar o resgate é um assunto de grande interesse, e o estudo revelou vários insights nesta área:

- A coleta de fundos para cobrir o resgate é um esforço colaborativo, com entrevistados relatando várias fontes financeiras em mais de quatro quintos (82%) dos casos
- A principal fonte de recursos financeiros para o resgate é a própria organização, que, em média, cobre 40% do pagamento; a empresa matriz da organização e/ou um órgão do governo geralmente fornece 19%
- As seguradoras são amplamente envolvidas nos pagamentos de resgate
  - 23% dos fundos para o pagamento do resgate se origina das seguradoras
  - As seguradoras contribuem para o resgate em 83% dos ataques
  - Contudo, as seguradoras raramente (1%) cobrem o valor cheio, e, em 79% dos casos, com o segurado custeando menos da metade do pagamento total

Origem dos fundos para o pagamento do resgate



De quais das seguintes fontes o dinheiro para o pagamento do resgate foi obtido? n=1.168.

Execução da transação do resgate

Vários departamentos podem contribuir para o resgate, mas, normalmente, os fundos são transferidos em um único pagamento por apenas uma das partes envolvidas.

Mundialmente, a ordem natural é que as seguradoras transfiram os fundos em quase metade dos pagamentos de resgate, seja diretamente (26%) ou através de um especialista indicado de resposta a incidentes (21%). As organizações vitimizadas fizeram 37% dos pagamentos, enquanto 8% foram executados pelos representantes legais das vítimas.

No geral, 28% (arredondados) das transferências foram realizadas por especialistas em resposta a incidentes, apontados pela seguradora (21%) ou por outra parte envolvida, normalmente a vítima (6%).

Executor da transferência do pagamento do resgate

Quem fez a transação do pagamento do resgate, ou seja, quem transferiu o dinheiro para a conta do invasor? n=1.168.

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, em 2024, as organizações relataram um custo médio de recuperação de um ataque de ransomware de US$ 2,73 milhões, um aumento de quase US$ 1 milhão do valor de US$ 1,82 milhão relatado em 2023.

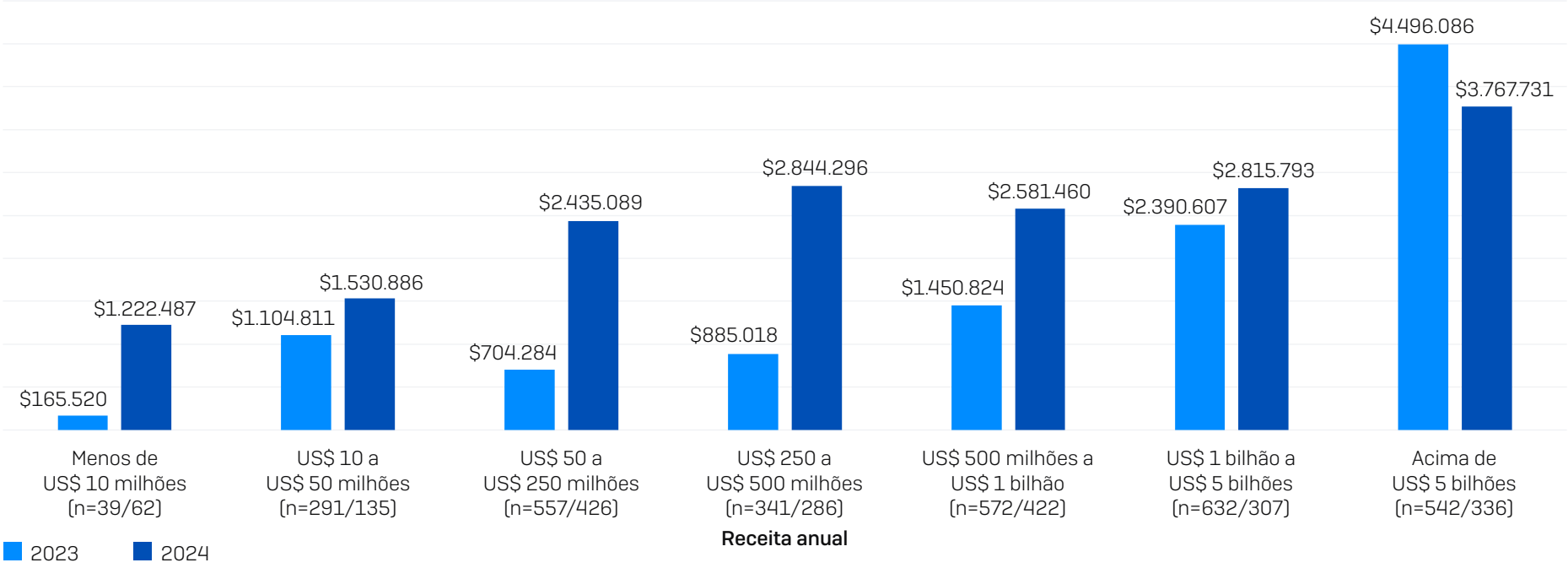
2021	2022	2023	2024
US$ 1,85 milhão	US$ 1,4 milhão	US$ 1,82 milhão	US$ 2,73 milhões

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.)? n=2.974 (2024), 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".

O maior aumento nos custos gerais de recuperação foi sentido pelas empresas nas faixas de receita média e baixa, com o coorte de US$ 250 milhões a US$ 500 milhões relatando o maior aumento individual, de US$ 2 milhões (de US$ 885.018 a US$ 2.885.296).

Organizações com receita de US$ 1 bilhão a US$ 5 bilhões relataram um aumento (relativamente) pequeno de um pouco mais de US$ 400.000, enquanto as organizações maiores, com receita anual de mais de US$ 5 bilhões, foram o único coorte a notar a redução no custo de recuperação, de US$ 4.496.096 a US$ 3.767.731.

A análise dos dados de custo mediano de recuperação confirma essa tendência. Mundialmente, os custos medianos com a recuperação dobraram no último ano: de US$ 375.000 para US$ 750.000. Os aumentos se concentraram mais especificamente nos cinco coortes de receita mais baixa, que relataram um aumento considerável nos custos, mantendo-se relativamente estáveis para os dois maiores.



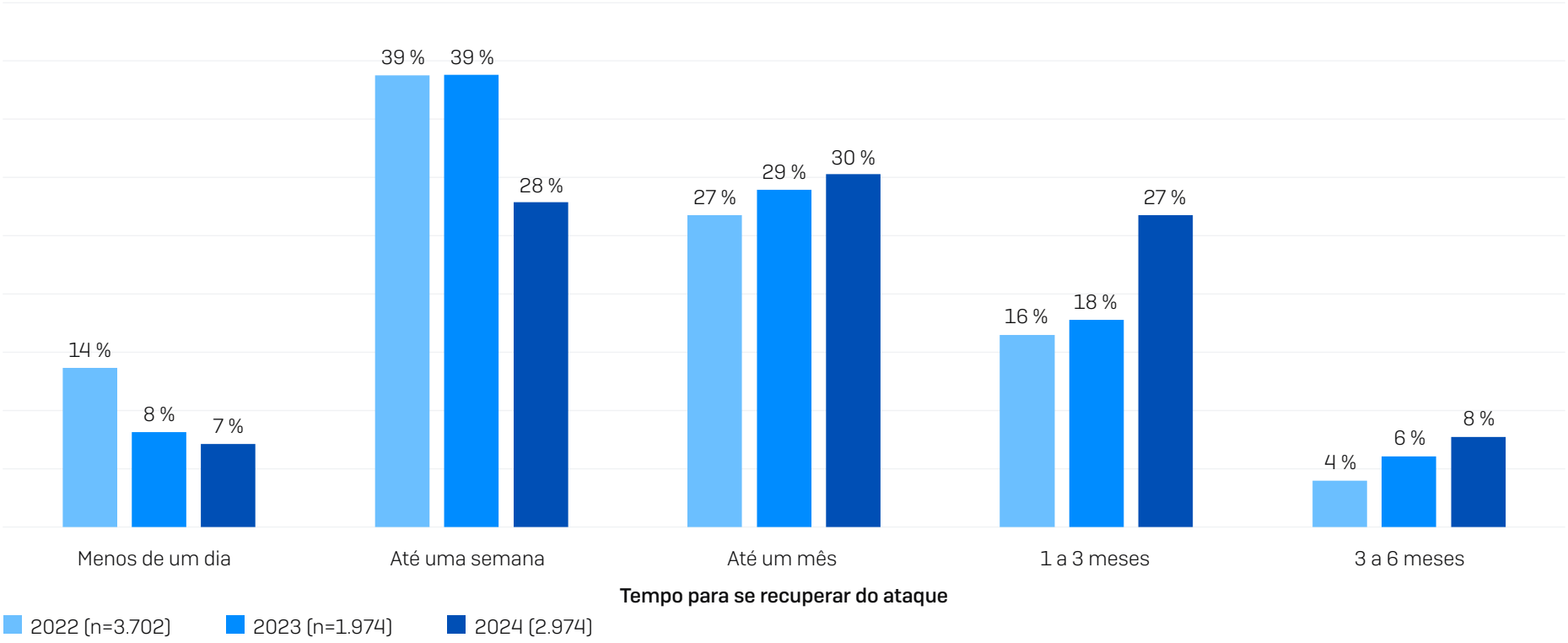
Qual foi o custo aproximado para a sua organização retificar o impacto do ataque de ransomware mais significativo (considerando-se período de inatividade, tempo de pessoal, custo dos equipamentos, custo da rede, perda de oportunidades etc.)? n=2.974 (2024), 1.974 (2023). Números de base de 2024/2023 por receita no gráfico

Tempo de recuperação

O tempo necessário para se recuperar de um ataque de ransomware está aumentando com regularidade. Nossa pesquisa de 2024 revelou que:

- 35% das vítimas de ransomware se recuperam totalmente em uma semana ou menos, caindo de 47% em 2023 e 52% em 2022
- Agora, um terço (34%) demora mais de um mês para se recuperar, subindo de 24% em 2023 e 20% em 2022

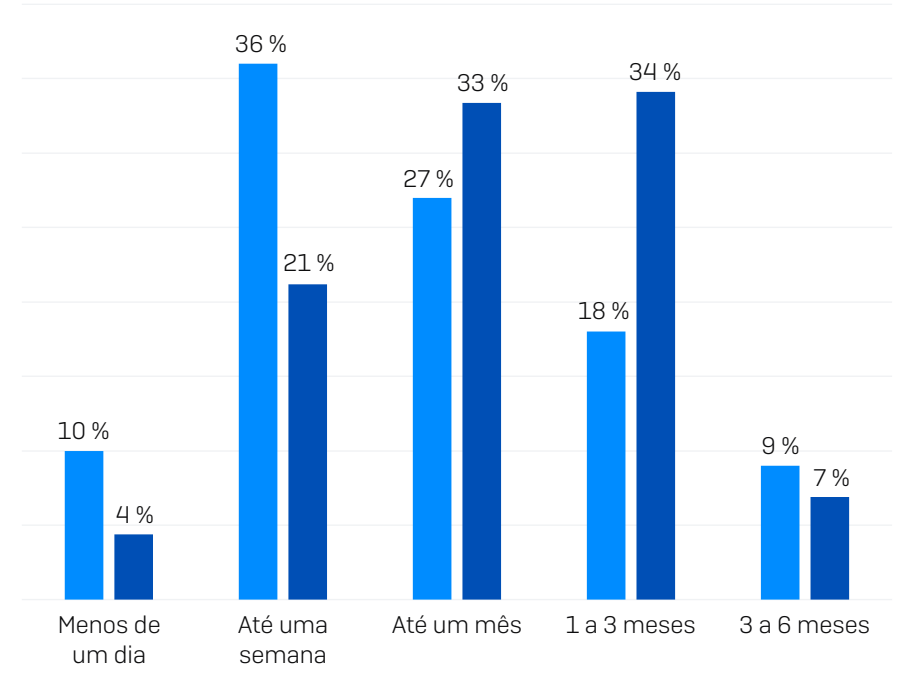
Essa lentidão pode ser reflexo do aumento em complexidade e gravidade dos ataques, exigindo mais esforços de recuperação. Pode indicar também a falta de preparo no processo de recuperação.



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

Tempo de recuperação: impacto do comprometimento de backup

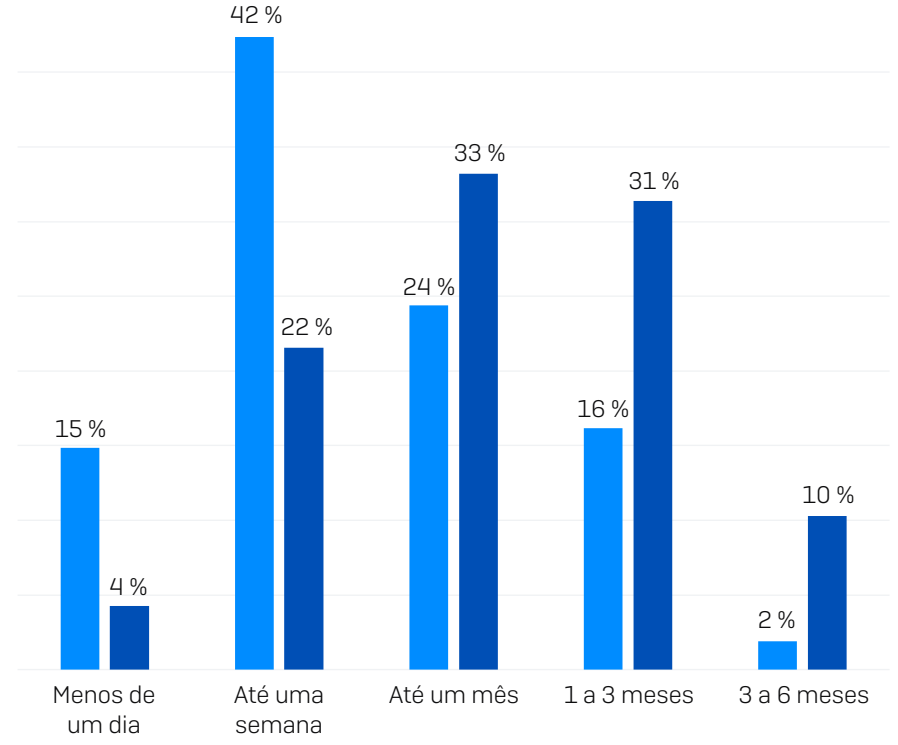
Backups comprometidos têm um impacto imenso no tempo de recuperação geral. Quase metade das organizações cujos backups não foram comprometidos se recuperaram em uma semana ou menos (46%) em comparação a um quarto (25%) daquelas cujos backups foram afetados. Backups comprometidos aumentam a complexidade da recuperação de dados criptografados e adicionam o encargo extra de ter que criar e proteger backups novos e imaculados.



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

Tempo de recuperação: impacto da criptografia de dados

Não surpreende que os dados criptografados em um ataque aumentem significativamente o tempo de recuperação. 57% dos que não tiveram seus dados criptografados se recuperaram totalmente em uma semana, comparado aos 25% dos que tiverem seus dados criptografados.

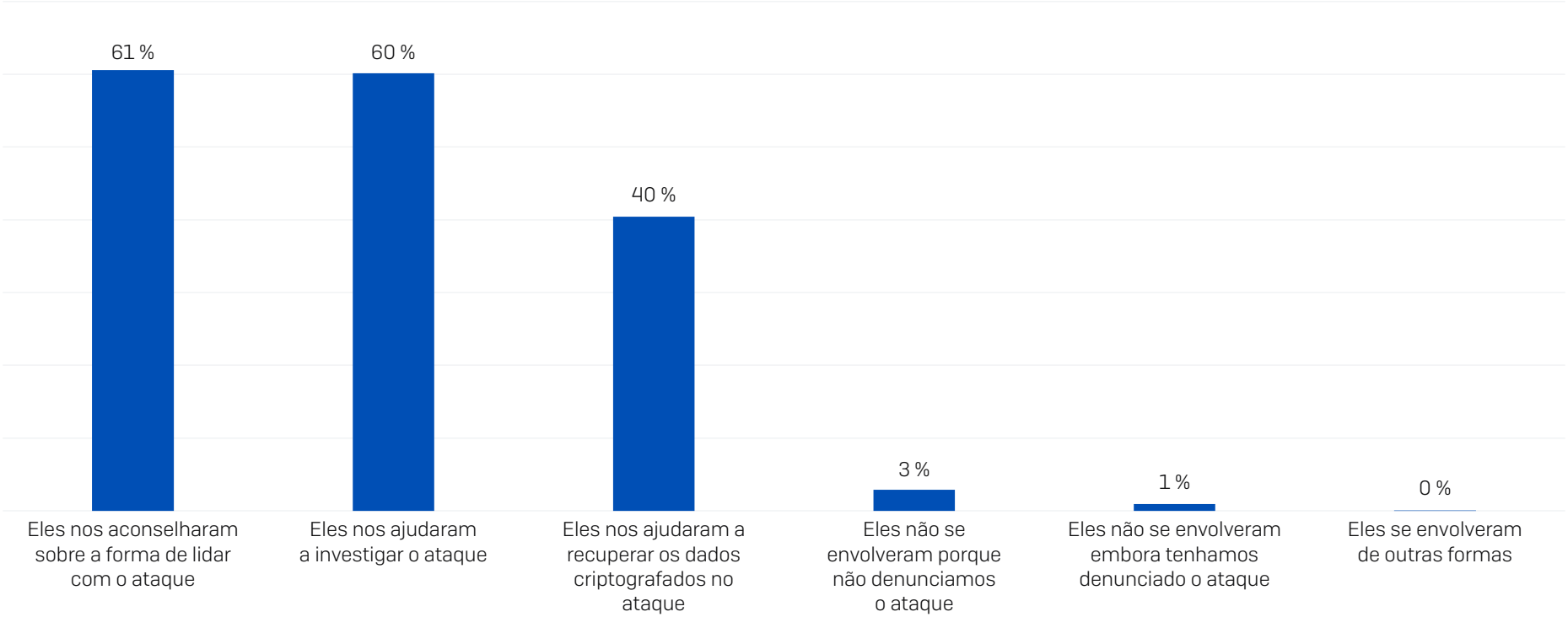


Quanto tempo a sua organização levou para se recuperar por completo do ataque de ransomware? Números de base no gráfico.

Envolvimento das leis e ordem pública

A natureza e disponibilidade do apoio oficial ao lidar com um ataque de ransomware varia de país para país, tal qual os meios para denunciar um ataque cibernético. Por exemplo, nos EUA, as vítimas podem utilizar o CISA (Cybersecurity and Infrastructure Security Agency). No Reino Unido, elas podem procurar o NCSC (National Cyber Security Centre). Na Austrália, o contato se dá pelo ACSC (Australian Cyber Security Center).

Um reflexo da normalização do ransomware é que 97% das organizações em âmbito mundial que foram atingidas por ransomware contataram as autoridades legais e/ou órgãos do governo devido ao ataque. 61% disseram ter recebido aconselhamento sobre como lidar com o ataque, 60% receberam ajuda para investigar o ataque e 40% disseram ter recebido ajuda para se recuperar do ataque.

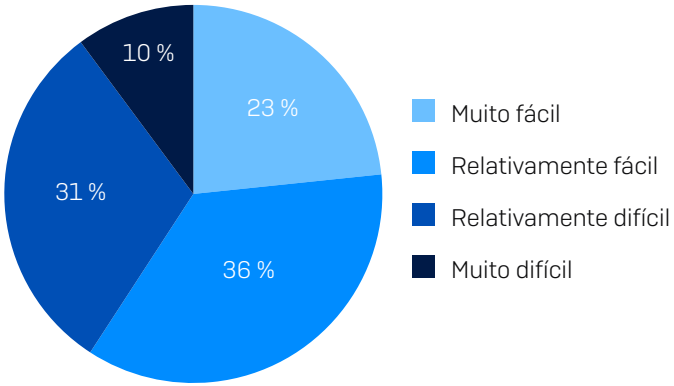


Como as autoridades legais e/ou órgãos do governo se envolveram

Se a sua organização denunciou o ataque a uma autoridade legal e/ou órgão oficial do governo, qual foi o envolvimento deles? n=2.974.

Facilidade de engajamento

Mais da metade (59%) dos que buscaram o engajamento de autoridades legais e/ou órgãos do governo em relação a um ataque disseram que o processo foi fácil (23% muito fácil; 36% relativamente fácil). Apenas 10% disseram que o processo foi muito difícil, e 31% o descreveram como relativamente difícil.



Qual foi o grau de facilidade ou dificuldade para a sua organização se engajar com as autoridades legais e/ou órgãos do governo em relação ao ataque? n=2.874 (excluindo respostas "não sei").

Não envolvimento de órgãos oficiais

São vários os motivos para 3% (86 entrevistados) não denunciarem o ataque, sendo as duas preocupações mais frequentes: que teria um impacto negativo na organização, como multas, encargos e trabalho extra (27%), e porque não acharam que a denúncia os beneficiaria (também 27%). Vários entrevistados disseram em seus feedbacks que não envolveram órgãos oficiais porque foram capazes de resolver o problema internamente.

Ficamos preocupados que haveria um impacto negativo em nossa organização, como multas, encargos, trabalho extra	27 %
Não achamos que beneficiaria nossa organização se denunciássemos o ataque	27 %
Não achamos que teriam interesse no ataque	22 %
Estávamos ocupados lidando com o ataque para pensar em envolvê-los	21 %
Os invasores nos avisaram para não os envolver	19 %
Não sabíamos quais autoridades legais ou órgãos oficiais contatar	10 %
Não havia obrigação legal de que denunciássemos o ataque	9 %
Outro (especifique)	3 %
Não sabe	1 %

Por que você não denunciou o ataque às autoridades legais e/ou a órgãos oficiais? (n=86).

Conclusão

Ransomwares continuam a ser a principal ameaça contra as organizações de todos os tamanhos em âmbito mundial. Mesmo com a queda geral do índice de ataques nos últimos dois anos, o impacto de um ataque para as vítimas aumentou. Os adversários continuam a repetir e incrementar os seus ataques, sendo essencial que as equipes e suas defesas cibernéticas acompanhem essa evolução.

Prevenção. O melhor ataque de ransomware é aquele que não aconteceu poque os adversários não conseguiram invadir a sua organização. Como um terço dos ataques começa com a exploração de vulnerabilidades sem patches, é importante assumir o controle da sua superfície de ataque e implantar um processo de correção baseado na priorização de risco. O uso de MFA para limitar o abuso de credenciais deve ser uma prioridade para todas as organizações. Treinamento constante de usuários sobre como detectar phishing e e-mails maliciosos continua essencial.

Proteção. Uma segurança básica forte é essencial, incluindo tecnologias de firewall, endpoint e e-mail. 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. Ferramentas de segurança precisam ser configuradas e implantadas corretamente para oferecer a proteção ideal. Portanto, busque soluções prontas que possam ser implantadas diretamente e que ofereçam simplicidade de controle. Proteção complicada e difícil de implantar pode facilmente aumentar o risco, em vez de reduzi-lo.

Detecção e resposta. Quanto mais cedo um ataque for interrompido, melhor. Detectar e neutralizar um adversário no seu ambiente antes que ele possa comprometer seus backups ou criptografar seus dados vai melhorar consideravelmente os resultados atingidos.

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. Pratique regularmente a restauração de dados a partir de backups para garantir velocidade e fluidez no caso de ser necessário executá-la após um ataque.

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

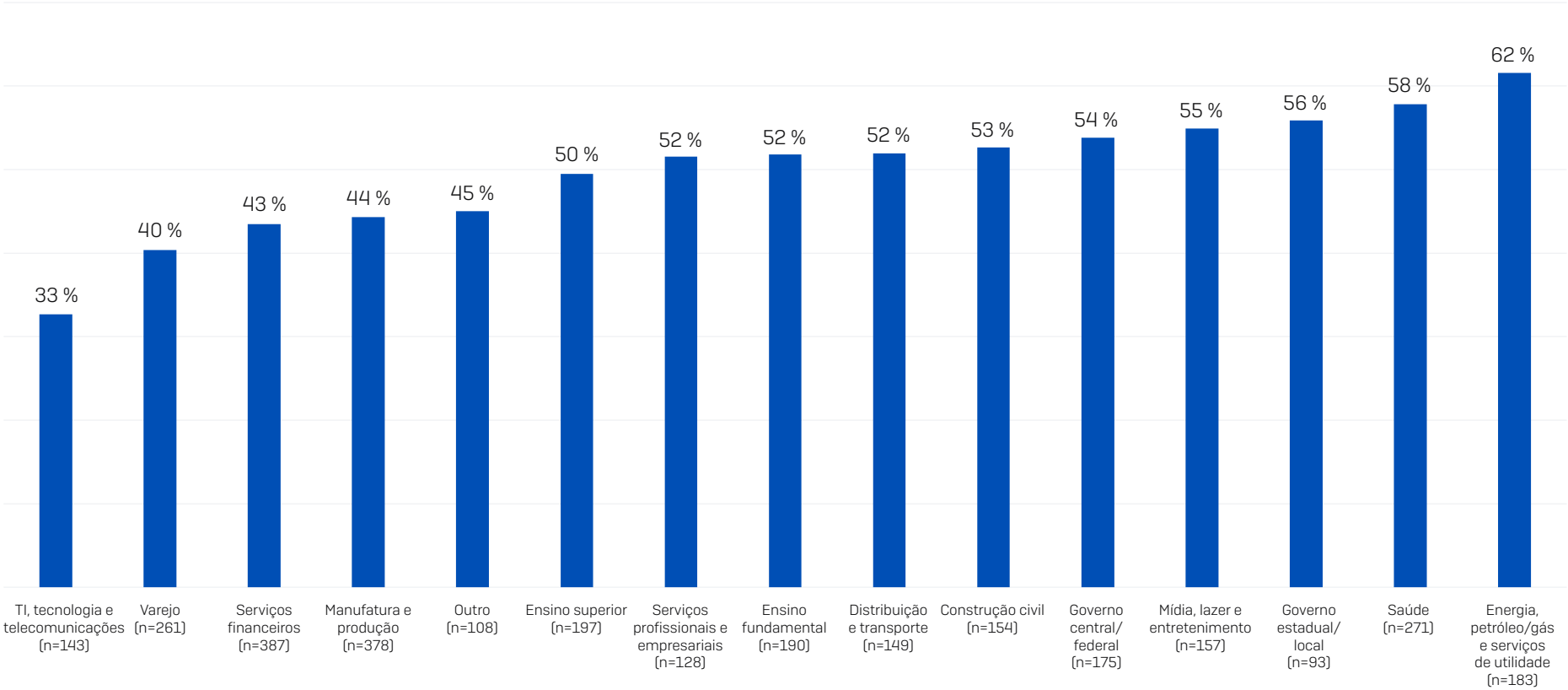
Sobre a Vanson Bourne

A Vanson Bourne é uma firma independente especializada em pesquisa de mercado para o setor tecnológico. A forte reputação e credibilidade incontestável de suas análises de mercado são fundamentadas em rigorosos princípios de pesquisa e na habilidade de buscar opiniões de tomadores de decisão seniores em todos os cargos técnicos e comerciais, em todos os setores de negócio e em todos os grandes mercados. Para obter mais informações, acesse www.vansonbourne.com

Apêndice

Porcentagem de computadores afetados por setor

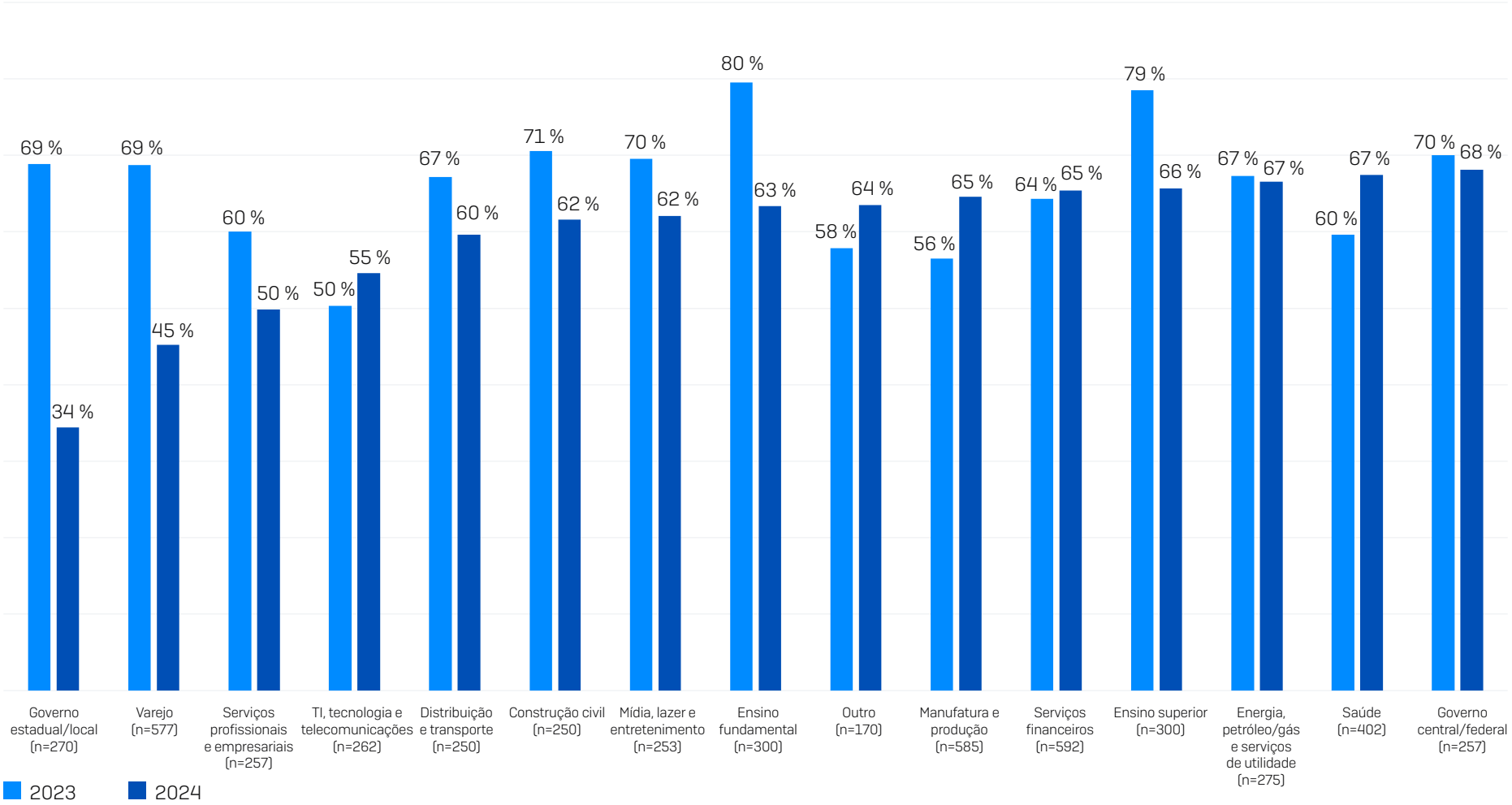
Porcentagem de dispositivos afetados



Qual a porcentagem de computadores da sua organização que foi afetada por ransomware no último ano? n=2.974 organizações atingidas por ransomware. Números de base do setor no gráfico.

Índice de ataques de ransomware por setor

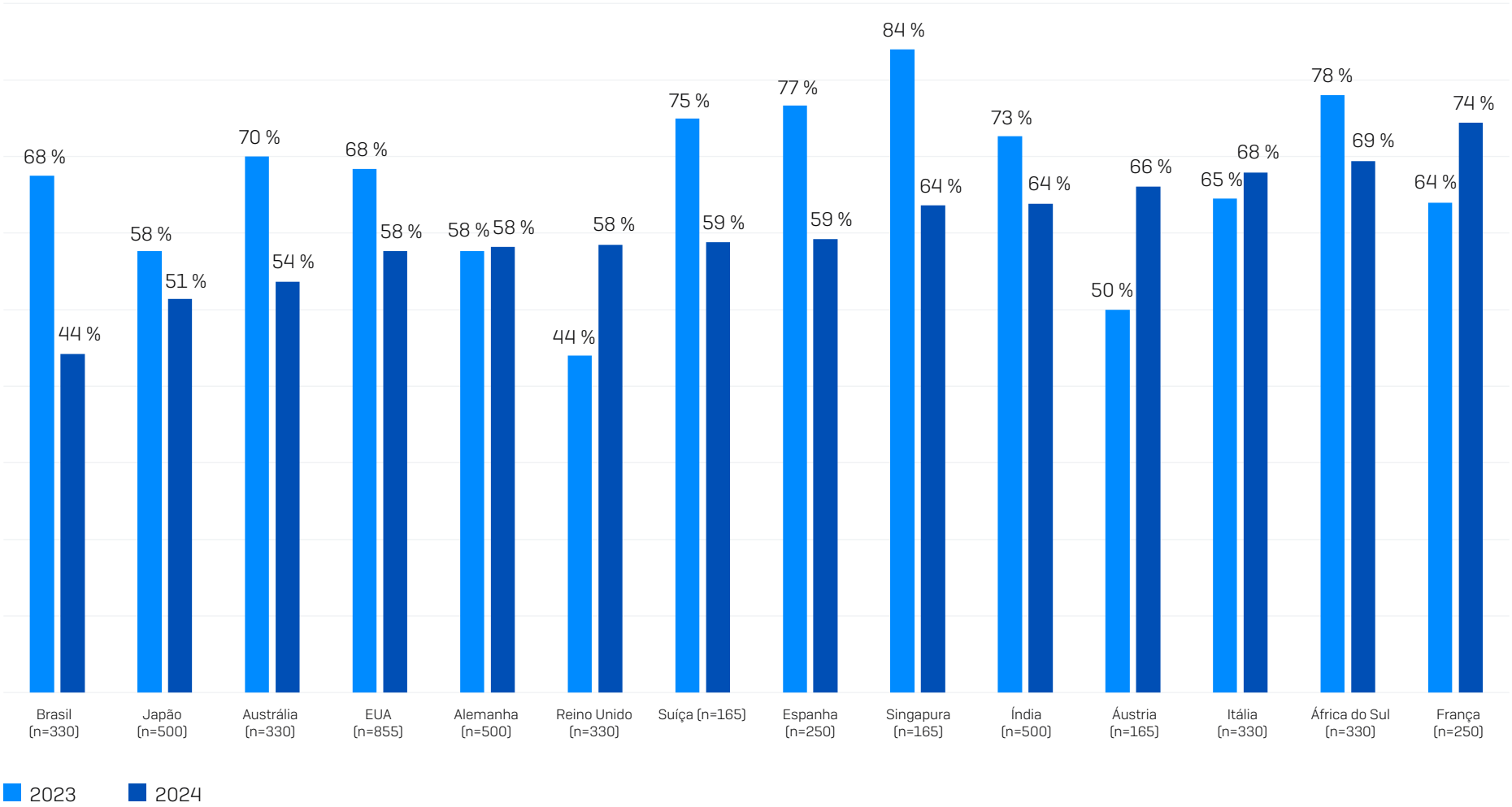
Porcentagem de organizações atingidas por ransomwares no ano passado



Sua organização foi atingida por ransomware neste último ano? Sim. n=5.000 (2024) n=3.000 (2023), 5.600 (2022). Números de base do setor de 2024 no gráfico.

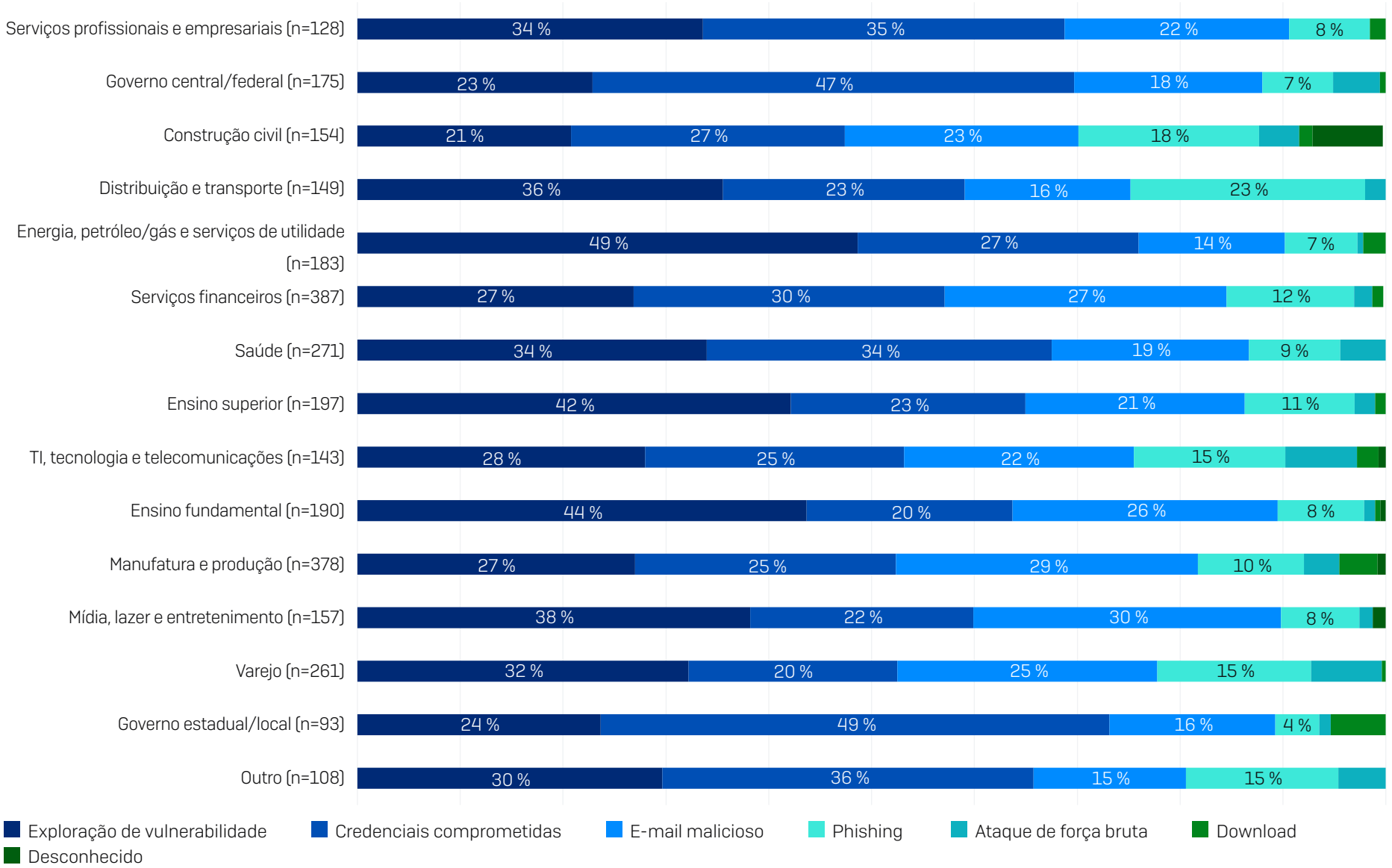
Índice de ataques de ransomware por país

Porcentagem de organizações atingidas por ransomwares no ano passado



Sua organização foi atingida por ransomware neste último ano? Sim. n=5.000 (2024), n=3.000 (2023). Números de base do país de 2024 no gráfico.

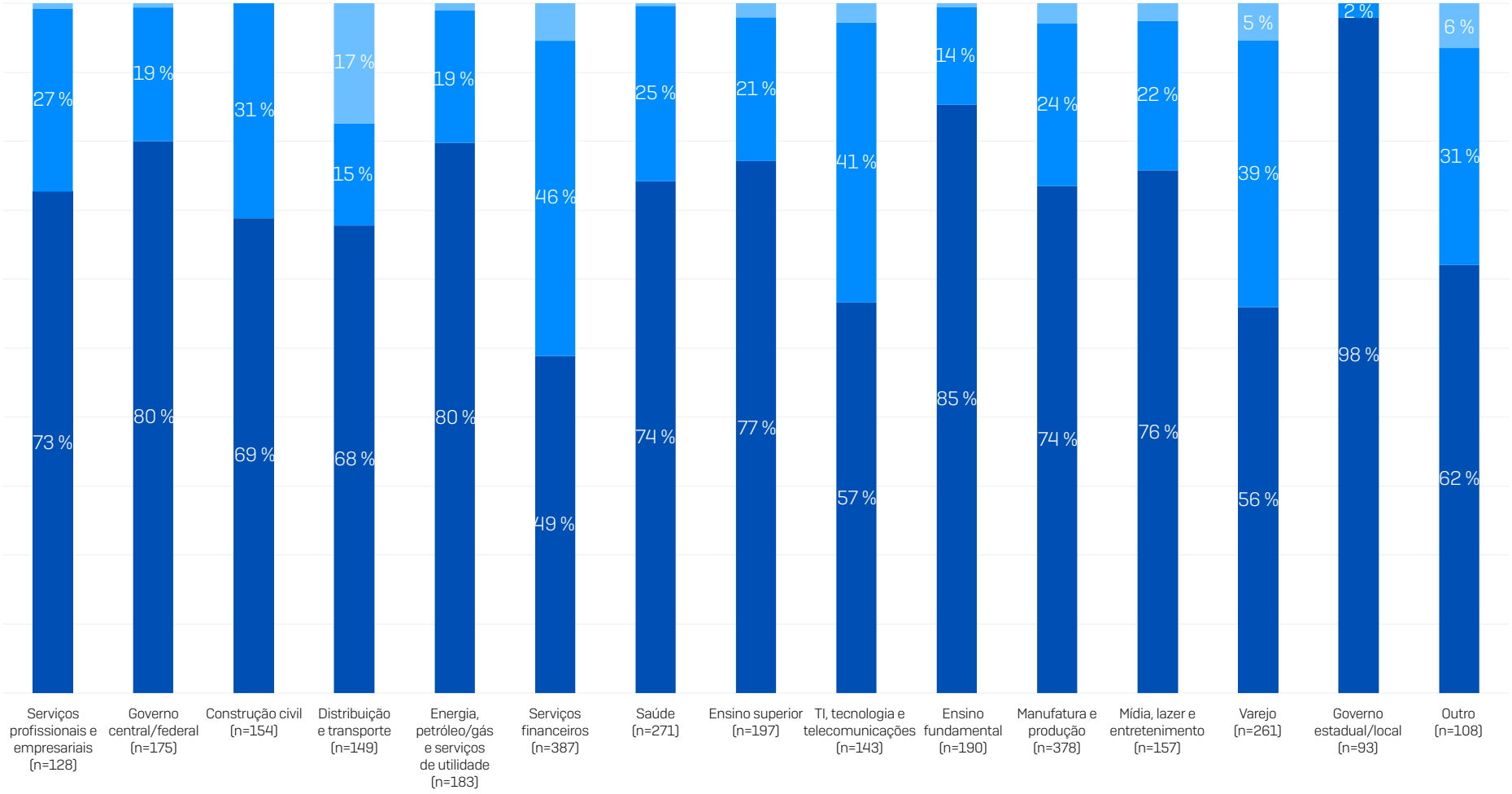
Causa primária do ataque por setor



Você sabe a causa primária do ataque de ransomware que a sua organização enfrentou no último ano? n=2.974 organizações atingidas por ransomware.

Índice de criptografia de dados por setor

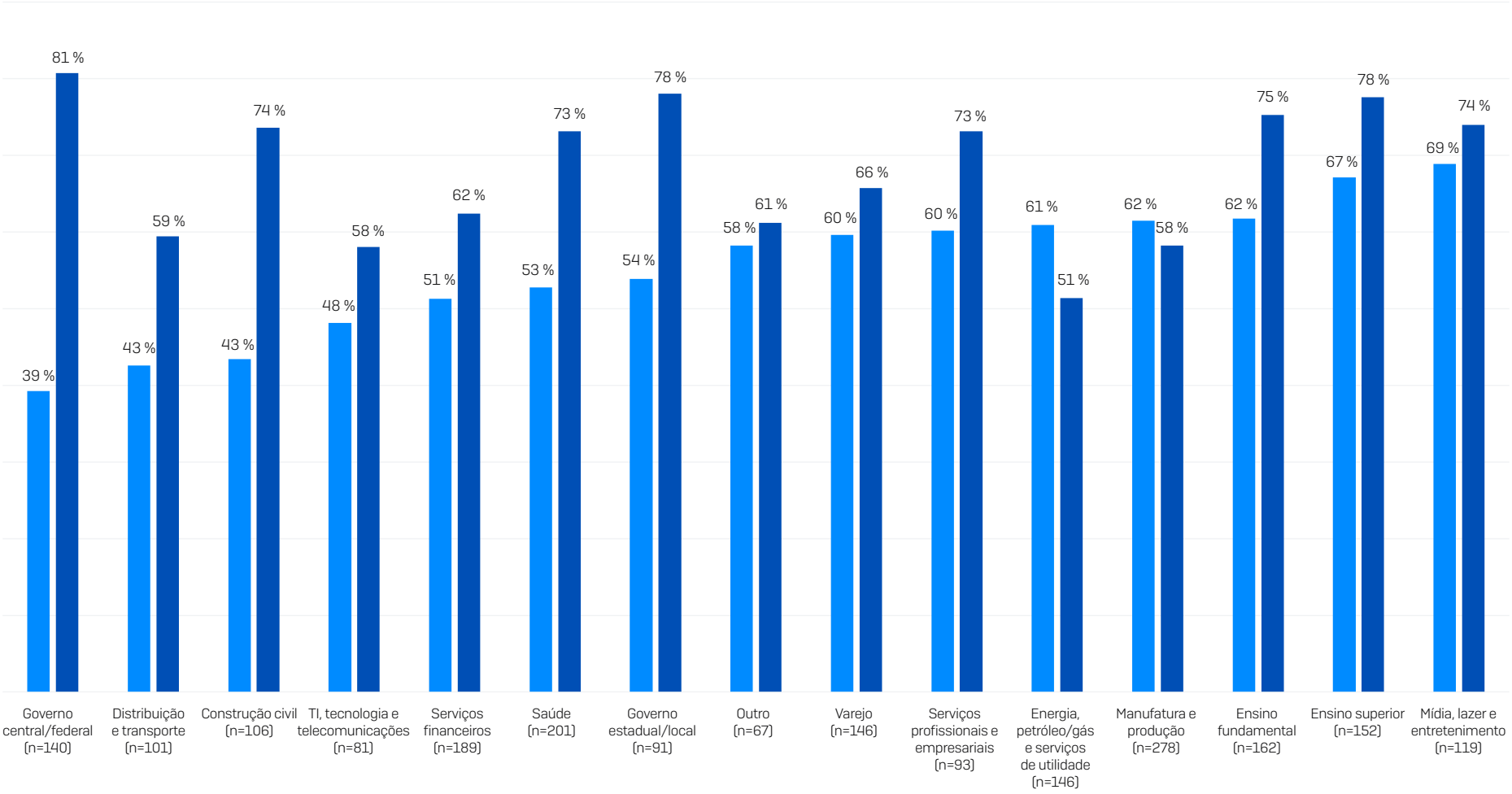
Propensão a ter os dados criptografados em um ataque



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

Método de recuperação de dados por setor

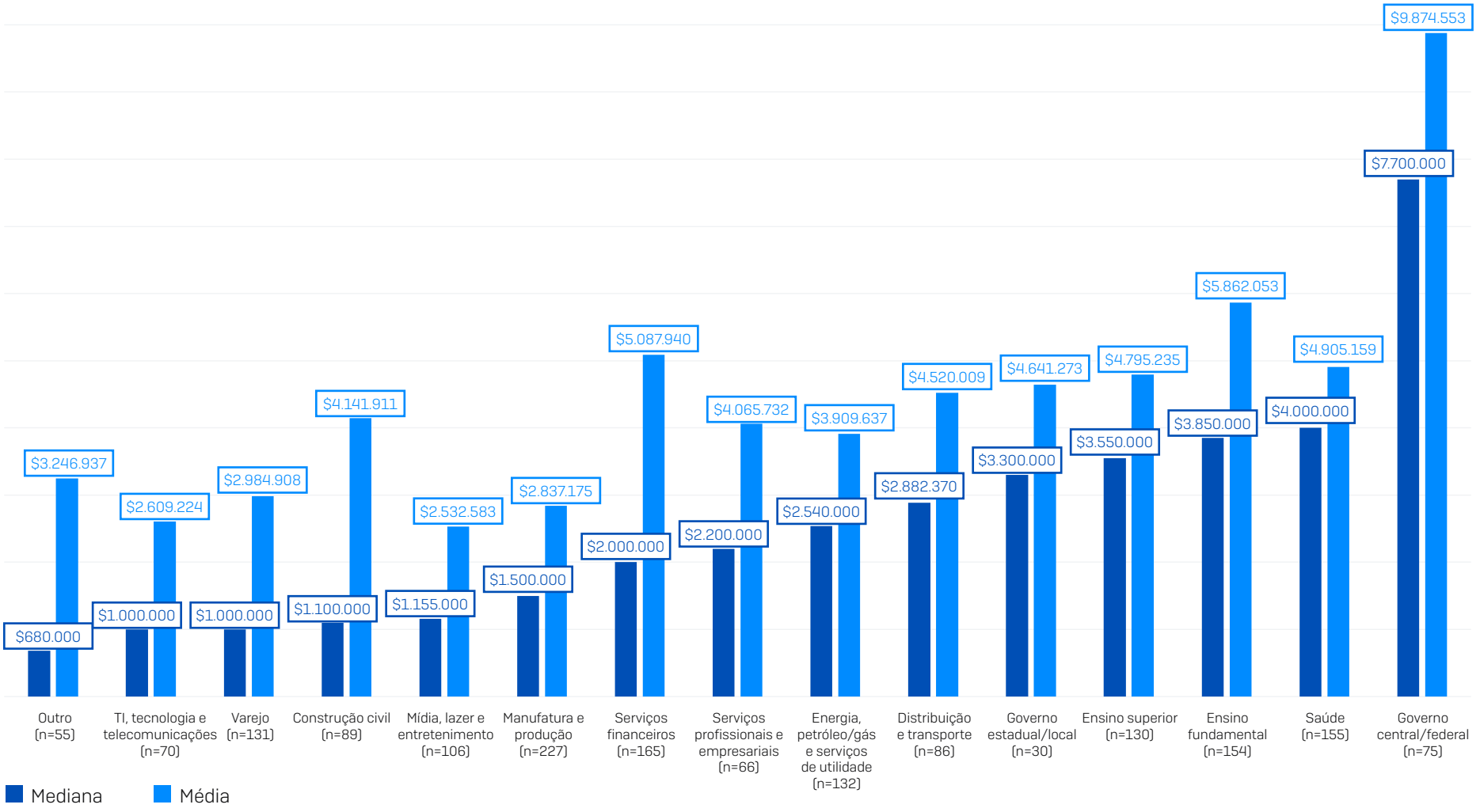
Frequência com que os dados são recuperados usando backups e pagando o resgate



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. Ordenados por propensão a pagar o resgate

Pedido de resgate por setor

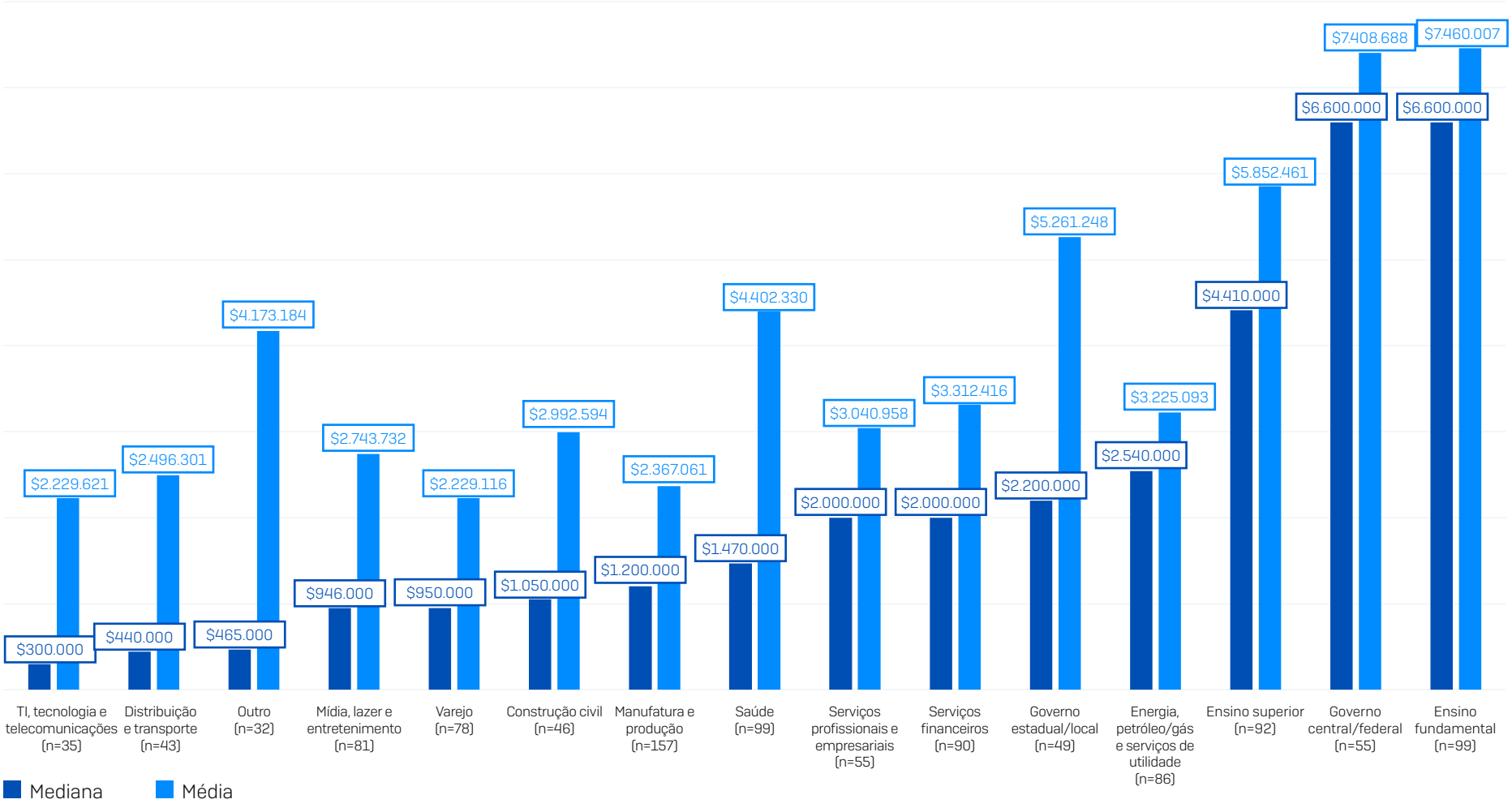
Pedido de resgate



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

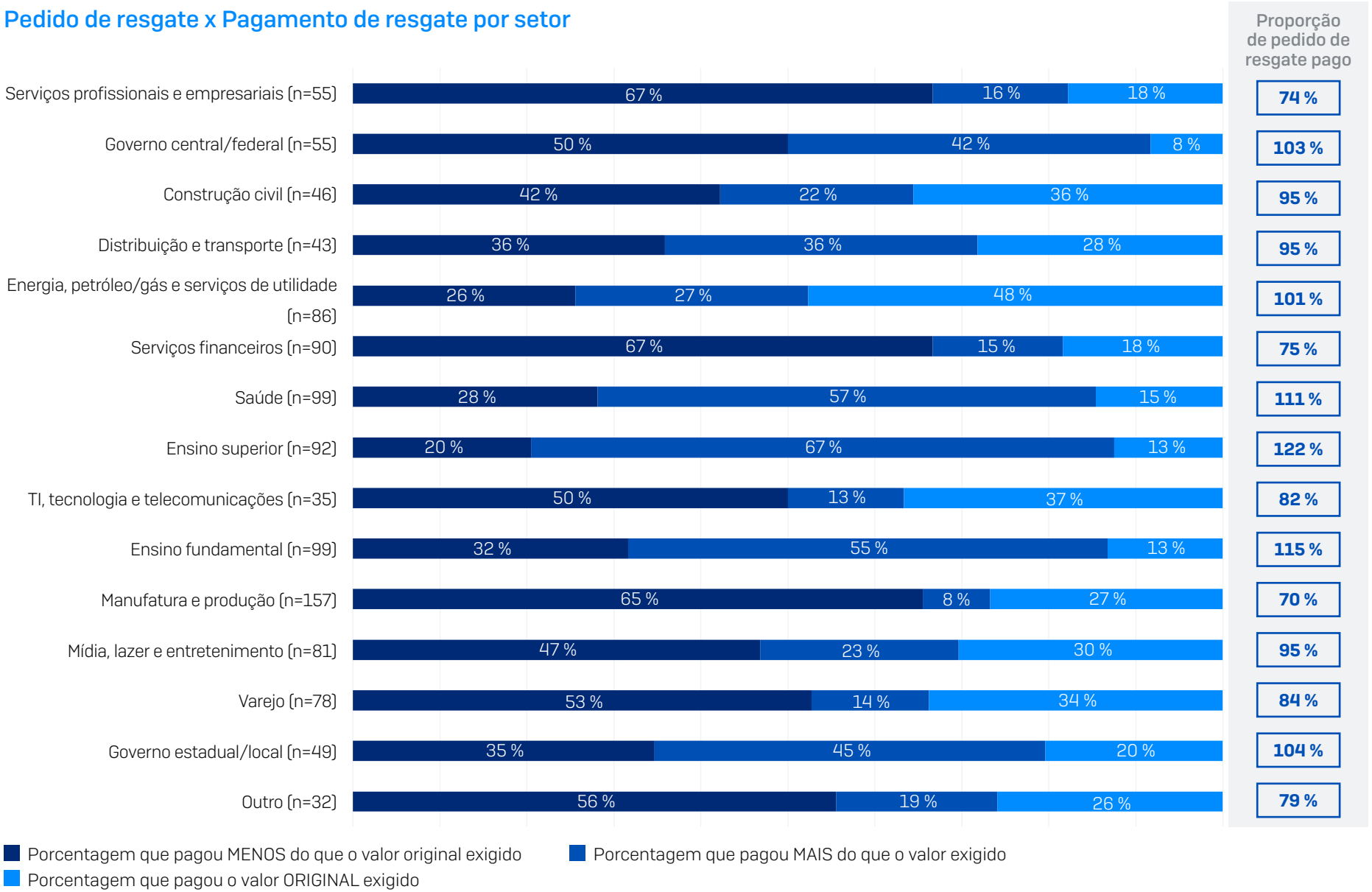
Pagamento de resgate por setor

Pagamento de resgate



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

Pedido de resgate x Pagamento de resgate por setor



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

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.

2024-04-16 (WP-PC)

SOPHOS