

Agosto de 2025

Relatório de mercado

O Relatório de Perspetivas sobre Ransomware 2025

Examinando a experiência e o impacto do ransomware nas organizações em todo o mundo

| Conteúdos

Introdução	3
Principais conclusões	5
Ransomwareafetamaisdo quemetadedasorganizações	6
Ransomwarevítimas têm um diferente perfil para segurança ferramentas e prioridades.....	6
Ransomwareganguestêm uma em três hipóteses de receberem o pagamento	8
Dadoscriptação é agora apenas uma parte de um ataque de ransomware ataque	8
Ransomwarevítimas perdem clientes e novos negócios oportunidades	10
Conclusão	11

I Introdução

O ransomware é uma ameaça generalizada e em evolução, potenciada por kits de ransomware-as-a-service que permitem que cada vez mais criminosos cibernéticos lancem ataques. Os incidentes de ransomware podem danificar a reputação da marca e paralisar as operações diárias, causando interrupções, perda de dados, confiança dos clientes e mais. Toda organização é um alvo potencial.

Este relatório explora a experiência e o impacto de ataques de ransomware bem-sucedidos em organizações de todo o mundo nos últimos 12 meses. Baseia-se nas conclusões de um inquérito internacional a 2.000 decisores de TI e segurança realizado pela Barracuda e Vanson Bourne.

As conclusões podem ser agrupadas em três temas gerais, a saber:

- As vítimas de ransomware são mais propensas a ter segurança fragmentada, com demasiadas ferramentas de segurança desconectadas e cobertura insuficiente em áreas de segurança chave.
- Os ataques de ransomware são multidimensionais. Já não se tratam apenas de encriptação de dados, mas agora envolvem roubo e exposição de dados, a

Metodologia

A Barracuda encomendou à empresa independente de estudos de mercado Vanson Bourne a realização de um inquérito global a 2.000 decisores seniores de segurança em funções de TI e negócios em organizações com entre 50 e 2.000 colaboradores de uma ampla gama de indústrias nos EUA, Reino Unido, França, DACH (Alemanha, Áustria, Suíça), Benelux (Bélgica, Países Baixos, Luxemburgo), os Países Nórdicos (Dinamarca, Finlândia, Noruega, Suécia), Austrália, Índia e Japão. O trabalho de campo foi realizado em abril e maio de 2025.

instalação de cargas maliciosas adicionais, e mais.

- A cratera de impacto de um ataque de ransomware bem-sucedido está a expandir-se, incluindo a perda de novas oportunidades de negócio e táticas de pressão de pagamento que se estendem a funcionários, parceiros, clientes e às autoridades.

I Introdução

Esperamos que este relatório ajude organizações de todos os tamanhos e indústrias a compreender a ameaça e o impacto do ransomware em 2025 e a identificar e abordar áreas onde possam potencialmente estar em risco.

| Principais Conclusões

57%



de organizações sofreram um ataque de ransomware bem-sucedido nos últimos 12 meses

71%



das organizações que sofreram uma violação de email também foram atingidas por ransomware

32%



pagaram um resgate para recuperar os seus dados — 41% deles não recuperaram todos os seus dados

65%



das vítimas de ransomware conseguiram restaurar dados a partir de backups

24%



das vítimas de ransomware tiveram dados encriptados — enquanto 27% tiveram dados roubados, e 29% disseram que os atacantes instalaram cargas adicionais

25%



das vítimas de ransomware perderam clientes existentes — a mesma proporção perdeu novas oportunidades de negócio

O ransomware afeta mais de metade das organizações

No geral, 57% das organizações pesquisadas tiveram um ataque de ransomware bem-sucedido nos últimos 12 meses.

Uma em cada três vítimas (31%) foi afetada duas vezes ou mais.

A prevalência de vários ataques bem-sucedidos sugere que as lacunas de segurança não são totalmente investigadas e resolvidas após cada incidente. Ao longo deste relatório, analisamos a diferença entre as organizações afetadas uma vez e aquelas afetadas várias vezes para ver o que pode ser aprendido com os dados e como as organizações podem usar isso para reforçar a sua postura de segurança.

Os setores industriais mais afetados na nossa pesquisa incluíram a saúde (com 67% das organizações afetadas), o governo local (65%) e o retalho (61%). De acordo com os dados, a indústria transformadora foi a menos impactada, com pouco menos de metade (46%) dos inquiridos a reportarem um ataque bem-sucedido.

O tamanho não parece ser um fator quando se trata de ransomware, com os resultados a manterem-se consistentes em todas as faixas de tamanho de empresa pesquisadas, de 50 a 2.000 colaboradores.

71% das organizações que sofreram uma violação de e-mail também foram atingidas por ransomware — destacando a ligação entre os dois tipos de ataques.

As vítimas de ransomware têm um perfil diferente para ferramentas de segurança e prioridades

Proliferação de segurança e o risco de ransomware

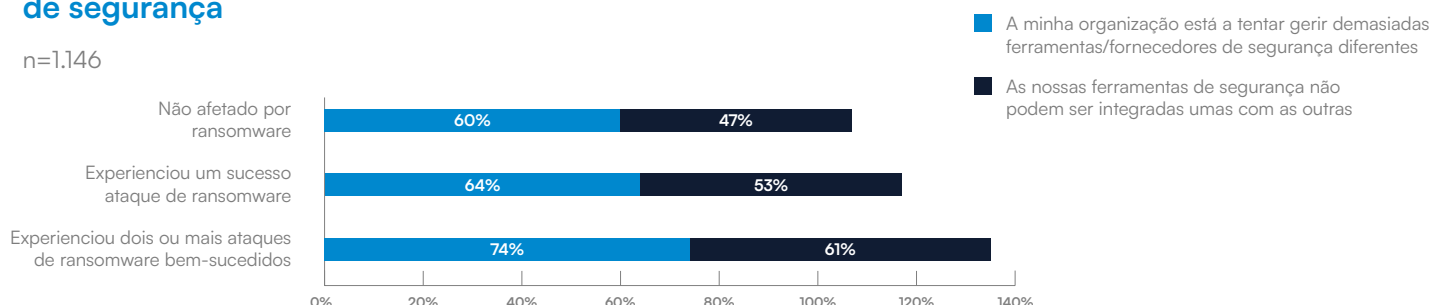
A pesquisa [mostra](#) que ferramentas de segurança em excesso — conhecidas como proliferação de segurança — acompanhadas por falta de integração podem aumentar o risco e criar lacunas na proteção, tornando mais difícil para as organizações detectar e mitigar ameaças ativas, incluindo ransomware.

Os dados mostram que a proporção de organizações afetadas pela proliferação de segurança/falta de integração aumenta em linha com a sua experiência de ransomware.

FIGURA 1

Incidentes de ransomware e proliferação de ferramentas de segurança

n=1.146



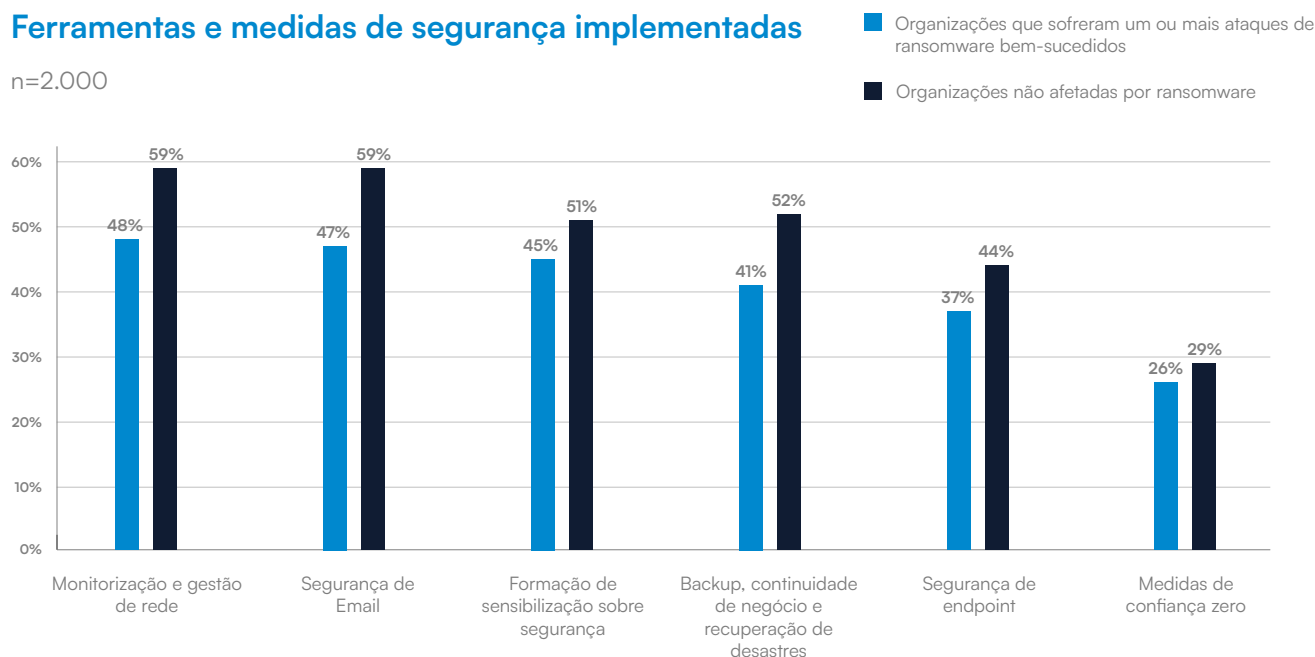
Os diferentes tipos de ferramentas e medidas de segurança

De acordo com os inquiridos, as medidas de segurança mais amplamente implementadas são a segurança de e-mail (implementada por 52%), segurança de rede (52%) e formação de sensibilização sobre segurança (48%). As organizações que relataram um incidente de ransomware bem-sucedido são menos propensas a ter implementado qualquer uma destas.

FIGURA 2

Ferramentas e medidas de segurança implementadas

n=2.000



Por exemplo:

- 47% das vítimas de ransomware tinham implementado uma solução de segurança de e-mail — em comparação com 59% dos não-vítimas
- 48% das vítimas de ransomware tinham gestão e monitorização de rede implementadas — em comparação com 59% dos não-vítimas
- 45% das vítimas de ransomware tinham formação de sensibilização sobre segurança — em comparação com 51% dos não-vítimas
- 37% tinham implementado segurança de endpoint — em comparação com 44% dos não vítimas

Estas conclusões sugerem que as vítimas de ransomware podem estar a investir insuficientemente em áreas de segurança que poderiam ajudar a reduzir a sua exposição ao risco.

Por exemplo, a segurança de e-mail, de rede e de endpoint, juntamente com a formação de sensibilização sobre segurança, proporcionam uma defesa robusta contra ataques de phishing transmitidos por e-mail e de engenharia social concebidos para roubar credenciais e permitir que os atacantes violem redes, comprometam dispositivos e se movam lateralmente — todas técnicas características de um ataque de ransomware.

Os grupos de ransomware têm uma probabilidade de uma em três de serem pagos

32% das vítimas de ransomware pagaram um resgate para recuperar ou restaurar dados.

Os resultados mostram uma correlação entre a propensão de uma organização para pagar um resgate e o número de vezes que são afetadas por ransomware.

As organizações que apenas sofreram um ataque de ransomware bem-sucedido foram ligeiramente menos propensas a pagar o resgate, com 29% a fazê-lo, enquanto entre aquelas afetadas duas vezes ou mais, 37% pagaram o resgate para recuperar os seus dados.

Esses números mudaram pouco desde a [última pesquisa](#) há dois anos. Em 2023, os resultados mostraram que 31% dos afetados uma vez, e 38% dos afetados duas vezes ou mais, pagaram um resgate para recuperar os dados.

Uma possível explicação para uma ligação entre múltiplos ataques e pagamentos de ransomware é que, uma vez que é [demonstrado](#) que uma organização está disposta a pagar, outros atacantes irão visar a mesma vítima, ou o mesmo atacante pode voltar mais de uma vez.

A boa notícia é que a maioria (65%) dos afetados por ransomware conseguiu restaurar os seus dados usando backups.

Como um lembrete claro de que pagar o resgate não compensa: 41% dos que pagaram (13% no total) não recuperaram todos ou sequer alguns dos seus dados.

A encriptação de dados é agora apenas uma parte de um ataque de ransomware

Além do encargo financeiro de pagar um resgate, a pesquisa mostra que o impacto comercial, operacional e até emocional de um ataque de ransomware bem-sucedido é considerável.

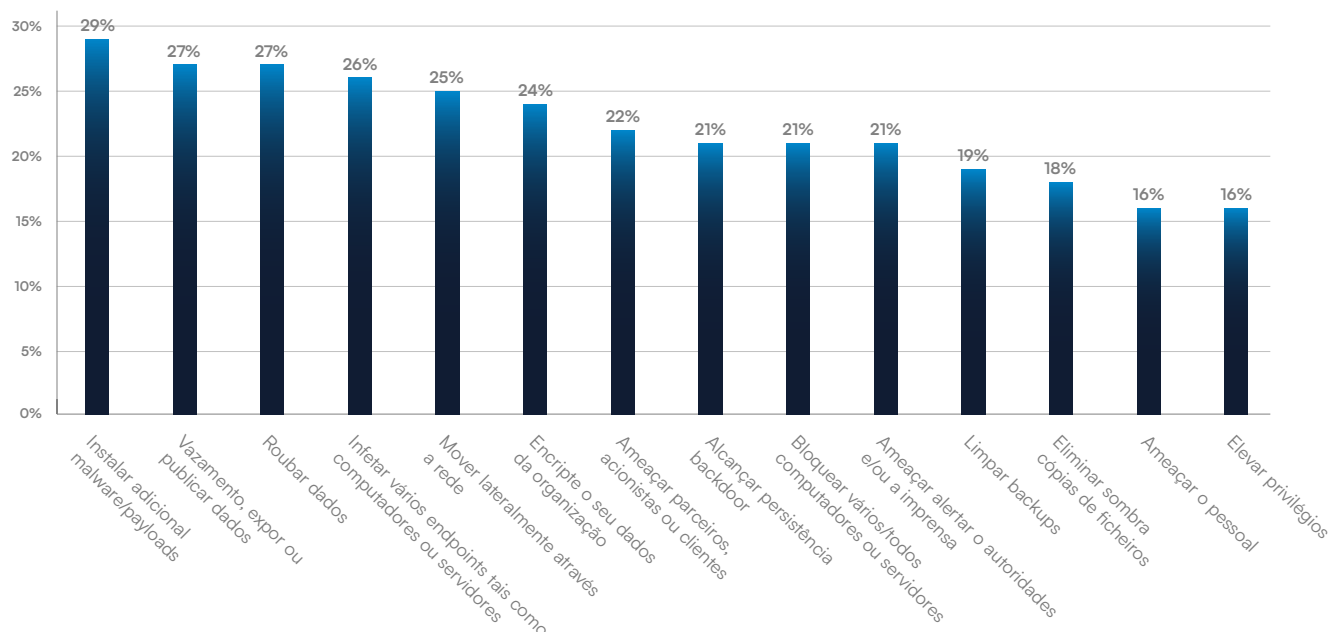
Na maioria dos incidentes de ransomware, a encriptação de dados e o bloqueio de sistemas e computadores é geralmente o objetivo final. Esta é a parte mais visível do ataque e, portanto, a mais provável de revelar a presença de intrusos à equipa de segurança e resultar na contenção e remoção da ameaça.

As conclusões da pesquisa sublinham a amplitude de atividade que ocorre sob o radar antes de o ransomware ser executado, seja para permitir o ataque ou potencialmente abrir caminho para outras atividades.

FIGURA 3

Atividades realizadas por gangues de ransomware durante o incidente mais significativo

n=1.146



Cerca de um quarto dos incidentes de ransomware experimentados pelos inquiridos envolveu a encriptação de dados (24%), bloqueio de endpoints (21%) e roubo de dados (27%).

Os ataques também apresentam movimento lateral através da rede (25%), a infeção de múltiplos endpoints, como computadores ou servidores (26%), a instalação de cargas úteis adicionais maliciosas (29%), elevação de privilégios (16%) e a incorporação de backdoors e outros mecanismos de persistência (21%).

Além disso, para dificultar que as vítimas restaurem os seus dados sem pagar, cerca de um em cada cinco atacantes acedeu e apagou backups e eliminou cópias sombra de ficheiros (ambos experienciados por 19% das vítimas).

As descobertas também mostram que, uma vez que o ransomware foi executado e a exigência de pagamento submetida, os atacantes começam a exercer pressão sobre a vítima através de táticas psicológicas. Estas incluem ameaçar parceiros, acionistas ou clientes (experienciado por 22%), ameaçar alertar a imprensa ou as autoridades (21%) e até mesmo ameaçar o pessoal (16%).

Em 27% dos incidentes de ransomware bem-sucedidos, os atacantes prosseguiram para vazar, expor ou publicar os dados roubados.

As vítimas de ransomware perdem clientes e novas oportunidades comerciais

Após a conclusão do ataque, as vítimas enfrentam repercussões operacionais e comerciais.

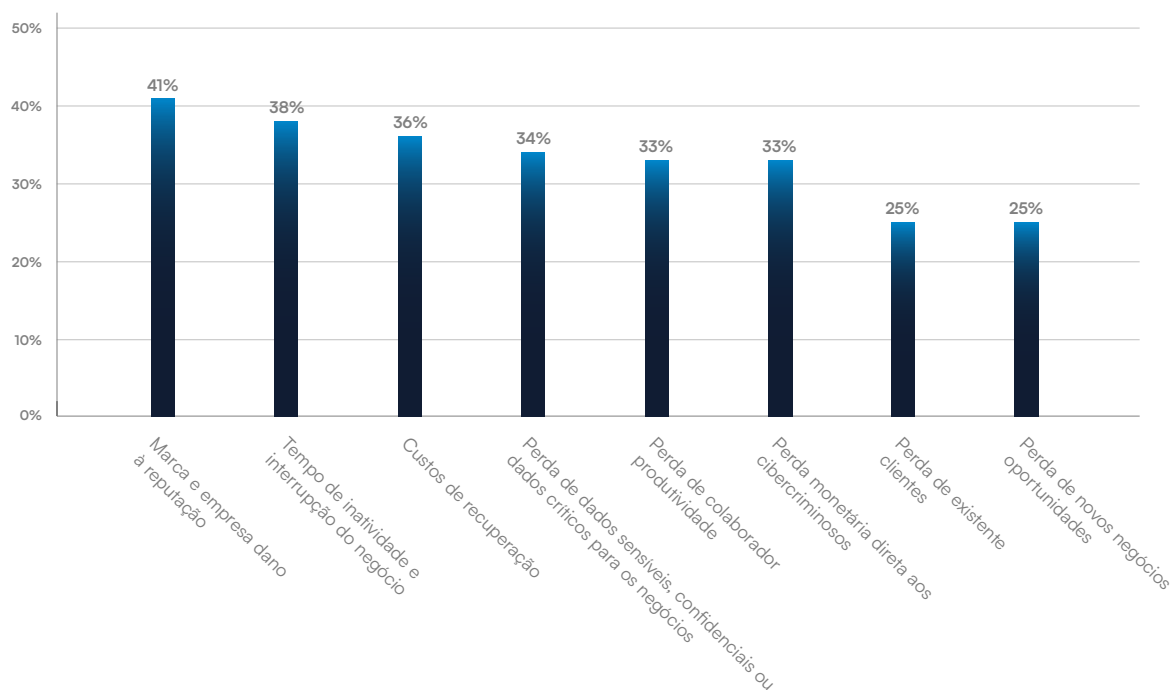
O principal impacto mencionado pelas vítimas de ransomware foi o dano à sua marca e reputação (afetando 41%). Segue-se o tempo de inatividade (38%) e os custos de recuperação (36%). Um terço (34%) admitiu ter perdido dados sensíveis.

Um em cada quatro vítimas de ransomware enfrentou o impacto comercial a longo prazo de perder clientes existentes e novas oportunidades de negócios (ambos 25%).

FIGURA 4

O impacto do ataque de ransomware mais significativo nos últimos 12 meses

n=1,146



| Conclusão

Para serem resilientes a ransomware, as organizações precisam de uma segurança integrada e multinível que proteja a sua superfície de ataque em constante expansão contra ciberameaças.

Os seguintes passos práticos podem ajudar:

- **Certifique-se de que os dados são regularmente e de forma segura**, mantidos offline. Realize testes para garantir que consegue restaurar os dados de forma eficaz.
- **Implemente a autenticação multifator e aplique o princípio do menor privilégio** para limitar o acesso a ativos e aplicações corporativas. Isto impede que atacantes ataquem dados e sistemas de alto valor, mesmo com credenciais roubadas.
- **Mantenha o software atualizado** com os patches de segurança mais recentes para fechar as lacunas de segurança.
- **Forneça formação regular de sensibilização sobre cibersegurança para os funcionários** focando-se nas táticas mais recentes de phishing e ransomware.
- **Segmente a rede**, isolando sistemas críticos para evitar o movimento lateral por atacantes.
- **Verifique todas as configurações**, incluindo na nuvem. Configurações incorretas são um dos principais contribuintes para violações de segurança.
- **Instale uma solução robusta de segurança de e-mail**. O e-mail continua a ser um ponto de entrada principal para ransomware, e a proteção avançada, baseada em IA, pode detetar cargas maliciosas e reconhecer táticas avançadas de engenharia social concebidas para contornar a segurança.
- **Proteja aplicações web, como serviços de partilha de ficheiros, formulários web e sites de comércio eletrónico**. As aplicações são frequentemente alvo através da interface do utilizador ou de uma interface API.
- **Tenha — e ensaie regularmente — um plano de resposta a incidentes**.
- **Considere colaborar com peritos externos**, incluindo fornecedores de serviços geridos e fornecedores de segurança, para suporte adicional. Estes parceiros podem apoiá-lo na implementação de plataformas e soluções de segurança integradas avançadas para detetar, bloquear e responder a ameaças ativas 24/7, contendo e neutralizando incidentes antes que possam causar danos graves.

Sobre a Barracuda

A Barracuda é uma empresa global de cibersegurança líder que oferece proteção completa contra ameaças complexas para empresas de todos os tamanhos. A nossa plataforma potenciada por IA protege e-mail, dados, aplicações e redes com soluções inovadoras, XDR gerido e um painel de controlo centralizado para maximizar a proteção e fortalecer a resiliência cibernética. Confiada por centenas de milhares de profissionais de TI e fornecedores de serviços geridos em todo o mundo, a Barracuda oferece defesas poderosas que são fáceis de adquirir, implementar e utilizar.

Barracuda Networks, Barracuda, BarracudaONE e o logótipo da Barracuda Networks são marcas registadas ou marcas comerciais da Barracuda Networks, Inc. nos EUA e noutros países.

Sobre a Vanson Bourne

A Vanson Bourne é uma empresa independente especializada em estudos de mercado no sector da tecnologia. A sua reputação, baseada em análises de investigação sólidas e credíveis, assenta em princípios de pesquisa rigorosos e na sua capacidade de recolher as opiniões de decisores seniores em funções técnicas e empresariais de todos os sectores de atividade e principais mercados. Para mais informações, visite vansonbourne.com.