Fevereiro de 2026

Relatório de ameaças

O Relatório de Ameaças Globais XDR Gerido

Como os atacantes visam as organizações e lacunas de segurança

Barracuda®
Your business, secured.

Conteúdos

Introdução

As ferramentas avançadas e os especialistas do Barracuda Managed XDR monitorizam e protegem as redes dos clientes 24 horas por dia, 365 dias por ano. A cada minuto, a solução deteta e responde a um aviso de segurança. A cada 15 minutos, envia um alerta a um cliente, e a cada 60 minutos, bloqueia automaticamente uma ameaça de alta gravidade, como um dispositivo comprometido ou um incidente de ransomware em desenvolvimento.

Se não for resolvido, um único sinal de alerta pode rapidamente escalar para um incidente generalizado que perturba operações, reduz a produtividade, compromete dados sensíveis e danifica a estabilidade financeira e a reputação da marca. Nenhuma organização é imune; os atacantes visam empresas de todos os tamanhos, em todas as indústrias e geografias.

O que torna os alvos vulneráveis pode ser muitas coisas — lacunas de segurança, dispositivos desonestos, sistemas não corrigidos, descuidos, configurações incorretas — e a falta de tempo e recursos para detectar a intrusão, remover os atacantes e fechar a porta firmemente atrás deles.

O objetivo deste relatório é ajudar os profissionais de TI e segurança em organizações com recursos limitados a compreender melhor como os atacantes visam potenciais vítimas e os pontos fracos de segurança que tentarão explorar.

Fornecemos exemplos de incidentes reais e recomendações sobre como manter-se seguro e ciber-resiliente.

Num mundo de ciberameaças cada vez mais complexas e evasivas, as organizações não enfrentam o desafio sozinhas. O seu fornecedor de segurança tem as ferramentas e o conhecimento para o ajudar a resolver os problemas identificados neste relatório — e estamos consigo em cada passo do caminho.

Os dados subjacentes

As conclusões detalhadas neste relatório baseiam-se no Barracuda Managed XDR's conjunto de dados exclusivo com mais de dois biliões de eventos de TI recolhidos durante 2025, quase 600 000 alertas de segurança e mais de 300 000 terminais protegidos, firewalls, servidores, ativos na nuvem e muito mais. Cerca de 53.000 ameaças de alta gravidade foram triadas pela plataforma de orquestração de segurança e resposta automatizada (SOAR) do Barracuda Managed XDR.

Principais Conclusões

100%

de incidentes de segurança envolveram pelo menos um endpoint não protegido ou desonesto

96%

de incidentes envolvendo movimento lateral terminaram com a libertação de ransomware

66%

dos incidentes envolveram a cadeia de abastecimento ou um terceiro (acima de 45% em 2024)

3 horas

o ataque de ransomware mais rápido, desde a violação até à encriptação

90%

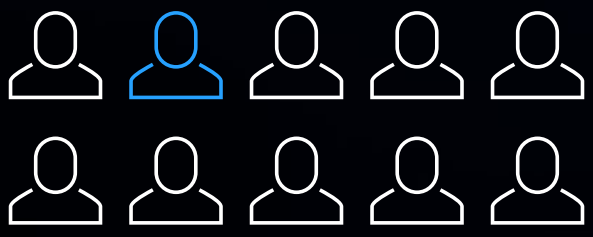
de incidentes de ransomware exploraram firewalls

13 anos

a vulnerabilidade mais detectada é um

1 em 10

vulnerabilidades detetadas têm uma exploração conhecida



Como os atacantes visam as organizações

Soluções eficazes de deteção e resposta alargadas (XDR) são concebidas para intercetar ameaças de entrada na fase mais precoce da cadeia de ataque — o ponto de compromisso e acesso inicial. Barracuda Managed XDR não é exceção. Também proporciona visibilidade adicional nas fases posteriores do ataque, incluindo movimento lateral e impacto. Esta ampla capacidade está refletida no conteúdo deste relatório.

Liderando a lista das ameaças mais detectadas contra organizações nos últimos 12 meses estão os ataques que visam identidades e a segurança de identidade.

Isso inclui logins incomuns ou inesperados numa conta de utilizador. Estas são conexões que não correspondem ao padrão de comportamento típico do utilizador em termos de dispositivo, localização ou horário. Tais detecções são um forte indicador de roubo de credenciais e comprometimento de conta. Outros sinais de alerta são tentativas de conexão a partir de uma geolocalização bloqueada e a regra de 'viagem impossível', onde um utilizador faz login a partir de uma segunda localização que nunca poderia ter alcançado no tempo entre os logins.

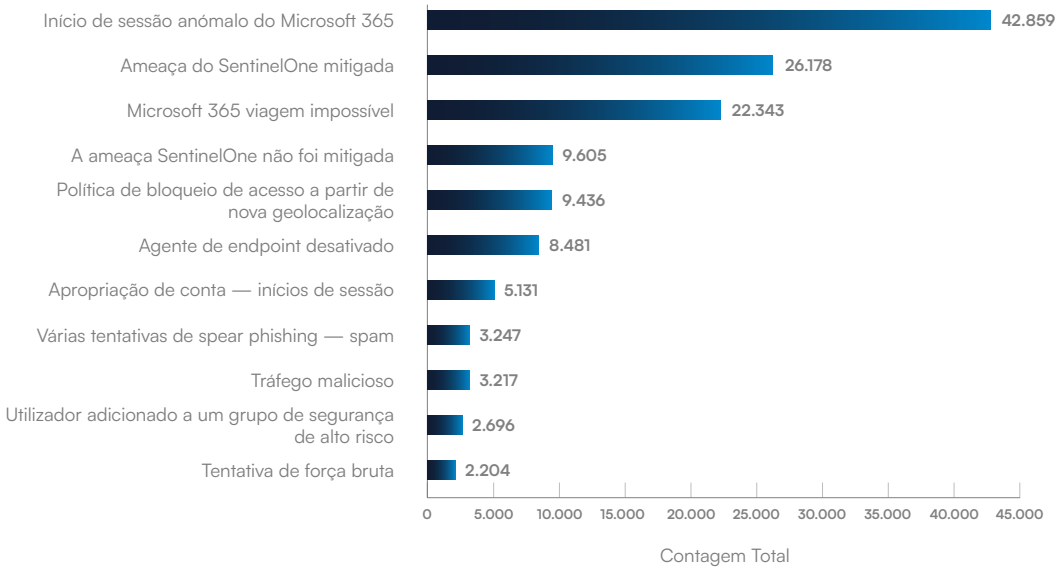


FIGURA 1

Principais deteções de ataques contra organizações

A lista das principais detecções também inclui atividades que podem significar que uma conta foi comprometida e os atacantes estão na rede. As equipas de segurança precisam investigar essas detecções imediatamente. Elas incluem sinais que sugerem que alguém tentou contornar ou desativar a proteção de endpoint e notificações de que um utilizador foi adicionado a um grupo sensível à segurança, o que pode ser um atacante a tentar escalar os seus privilégios.

Como os atacantes manipulam os direitos de privilégio uma vez dentro do sistema

A escalada de privilégios é crucial para os atacantes porque transforma o acesso limitado em controlo administrativo total, permitindo-lhes desativar defesas, mover-se lateralmente entre sistemas e aceder a dados sensíveis. O resultado pode ser um comprometimento em larga escala e a libertação de ransomware.

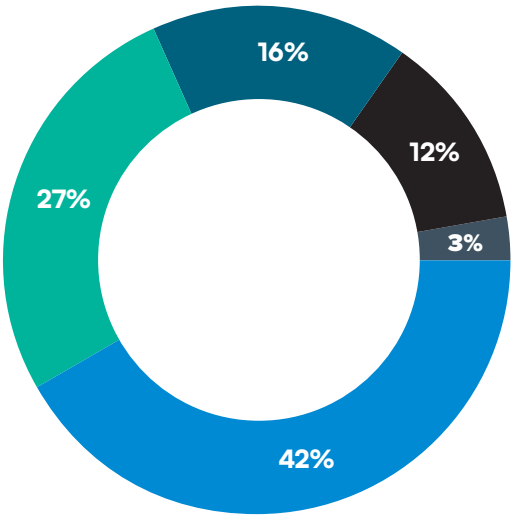


FIGURA 2

Como os atacantes manipulam os direitos de privilégio

- Windows — Adicionou um utilizador a um grupo com direitos de segurança de alto risco
- Windows — Removeu um utilizador de um grupo com direitos de segurança de alto risco
- Microsoft 365 — Adicionado um utilizador como administrador global
- Microsoft 365 — Removeu um utilizador como administrador global
- Firewall FortiGate — Adicionado um utilizador como administrador

As ferramentas de segurança do firewall, Windows e Microsoft 365 do Barracuda Managed XDR detetaram os seguintes comportamentos que indicam uma tentativa de escalonamento de privilégios:

Windows — adicionou um utilizador a um grupo com direitos de segurança de alto risco (representando 42% das escaladas de privilégios suspeitas)

- **O que isto significaa:** Um utilizador foi adicionado a um grupo com permissões poderosas (por exemplo, administradores de domínio).
- **Os invasores podem usá-lo para:** Movimentar-se lateralmente, implantar malware ou extrair dados.
- **Como manter a segurança:** Monitorize as alterações nos grupos e gerencie a atribuição de todos os direitos de acesso privilegiados.

Windows — removeu um utilizador de um grupo com direitos de segurança de alto risco (27%)

- **O que isto significa:** Um utilizador foi retirado de um grupo com privilégios elevados.
- **Os invasores podem usá-lo para:** Cobrir os seus rastos após a escalação de privilégios.
- **Como manter-se seguro:** Investigue o motivo da remoção e verifique se houve algum uso indevido antes da remoção.

Microsoft 365 — adicionou um utilizador como administrador global (16%)

- **O que isto significa:** Alguém recebeu o nível mais alto de acesso no Microsoft 365.
- **Os invasores podem usá-lo para:** Criar novas contas, roubar dados ou desativar a segurança.
- **Como manter a segurança:** Reveja as alterações nas funções dos administradores, imponha a autenticação multifator (MFA) e introduza processos adequados de revisão e aprovação.

Microsoft 365 — removeu um utilizador como administrador global (12%)

- **O que isto significa:** Alguém perdeu os seus direitos de administrador global.
- **Os invasores podem usá-lo para:** Evitar a detecção removendo as contas adicionadas.
- **Como manter a segurança:** Verifique se a alteração foi autorizada e analise os registos de auditoria para detectar atividades suspeitas ou uso indevido.

FortiGate Firewall — adicionou um utilizador como administrador para o firewall (3%)

- **O que isto significa:** Se creó una nueva cuenta de administrador en el firewall.
- **Os atacantes podem usá-lo para:** Desactivar protecciones y abrir puertas traseras.
- **Como manter-se seguro:** Confirme a legitimidade da conta e aplique controlos administrativos rigorosos.

Relatório de Incidente — O anexo malicioso que levou a um RAT

Foi encontrado um Trojan de acesso remoto (RAT) nos sistemas de um cliente depois de um funcionário ter descarregado inadvertidamente um ficheiro executável malicioso. O ficheiro tentou imediatamente estabelecer persistência: pediu para se registar como um serviço do Windows, o que lhe permitiria iniciar automaticamente, executar em segundo plano e operar com acesso ao nível do sistema, para que pudesse controlar o sistema remotamente sem suporte. Também tentou instalar a ferramenta de gestão remota de confiança ScreenConnect através do PowerShell.

Escondido à vista de todos

Adicionar e remover utilizadores de grupos de acesso privilegiado é uma atividade legítima de TI. A capacidade dos atacantes de esconder comportamentos maliciosos entre tarefas e ferramentas normais do dia-a-dia é um dos maiores desafios que as equipas de segurança enfrentam atualmente.

Esta abordagem de viver da terra (LOTL) está em ascensão, com atores de ameaça a aproveitar ferramentas e técnicas de software legítimas para evitar a deteção. Felizmente, a IA está a ajudar sistemas de segurança avançados a detetar anomalias subtis em atividades aparentemente benignas que podem ser investigadas e mitigadas.

Relatório de Incidente — Ransomware Akira vira ferramenta de gestão remota da vítima contra si própria

Os atacantes ganharam acesso ao controlador de domínio (DC) e instalaram o Datto RMM. A sua atividade espelhava de perto o que um agente de backup poderia legitimamente fazer durante trabalhos agendados, o que fez com que tudo parecesse uma atividade normal de TI.

Uma palavra sobre ferramentas de acesso remoto e gestão (RMM)

As ferramentas de acesso remoto são um alvo crescente para atacantes. Comprometer com sucesso uma ferramenta RMM dá aos atacantes uma quantidade significativa de poder, ao mesmo tempo que reduz o risco de serem detetados, porque os RMMs são amplamente utilizados por organizações.

Nos últimos 12 meses, Barracuda Managed XDR mitigou incidentes envolvendo o abuso de, entre outros, SonicWall SSL-VPN, (uma rede privada virtual popular) ScreenConnect, RDP (o Protocolo de Ambiente de Trabalho Remoto), PsExec (uma ferramenta de linha de comandos para executar programas e comandos em computadores remotos), AnyDesk, e outras VPNs de firewall.

Para reduzir o risco, as equipas de segurança precisam de implementar sistemas de deteção que procurem especificamente o abuso de RMM. Por exemplo, a Barracuda Managed XDR desenvolveu uma regra de deteção que utiliza telemetria de endpoints para identificar pedidos enviados do ScreenConnect para domínios de topo (TLDs) suspeitos.

Combinações de bandeira vermelha

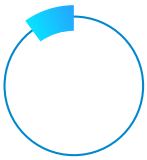
Atividade suspeita também pode ser identificada ao olhar para o quadro geral. Uma análise de incidentes do mundo real envolvendo Barracuda Managed XDR nos últimos 12 meses identificou as seguintes combinações comuns de ferramentas/técnicas e comportamentos:

66%

de casos envolvendo malware sem ficheiros usaram o PowerShell como o método de execução principal. O PowerShell é uma ferramenta independente de plataforma utilizada para automatizar tarefas e gerir configurações.

44%

de incidentes relacionados com firewall envolveram password-spraying — onde os atacantes tentam várias palavras-passe comuns contra nomes de utilizador roubados.



10%

das violações de segurança do servidor envolveram a limpeza dos registos de atividade para encobrir os rastros dos atacantes.

96%

dos casos envolvendo movimento lateral resultaram na implementação de ransomware.

90%

de incidentes de ransomware exploraram firewalls através de um CVE (uma vulnerabilidade de software classificada) ou conta vulnerável.

34%

de incidentes envolveram engenharia social que enganou os utilizadores a descarregar ficheiros potencialmente maliciosos.

Para que os ataques tenham sucesso, os atacantes precisam encontrar e aproveitar lacunas na segurança das suas vítimas pretendidas. Os dados de deteção e a perceção de incidentes do Barracuda Managed XDR destacam alguns dos pontos fracos potenciais que deixaram os alvos vulneráveis a ciberameaças ao longo do último ano.

Como as organizações se deixam expostas

Principais vulnerabilidades de segurança de rede

Métodos de encriptação inadequados ou desatualizados que não protegem o tráfego sensível, bem como a falta de validação adequada — ou certificação — da atividade de rede podem ser utilizados por atacantes para intensificar os seus ataques.

Barracuda Managed XDR identificou os seguintes riscos de segurança de rede no último ano:

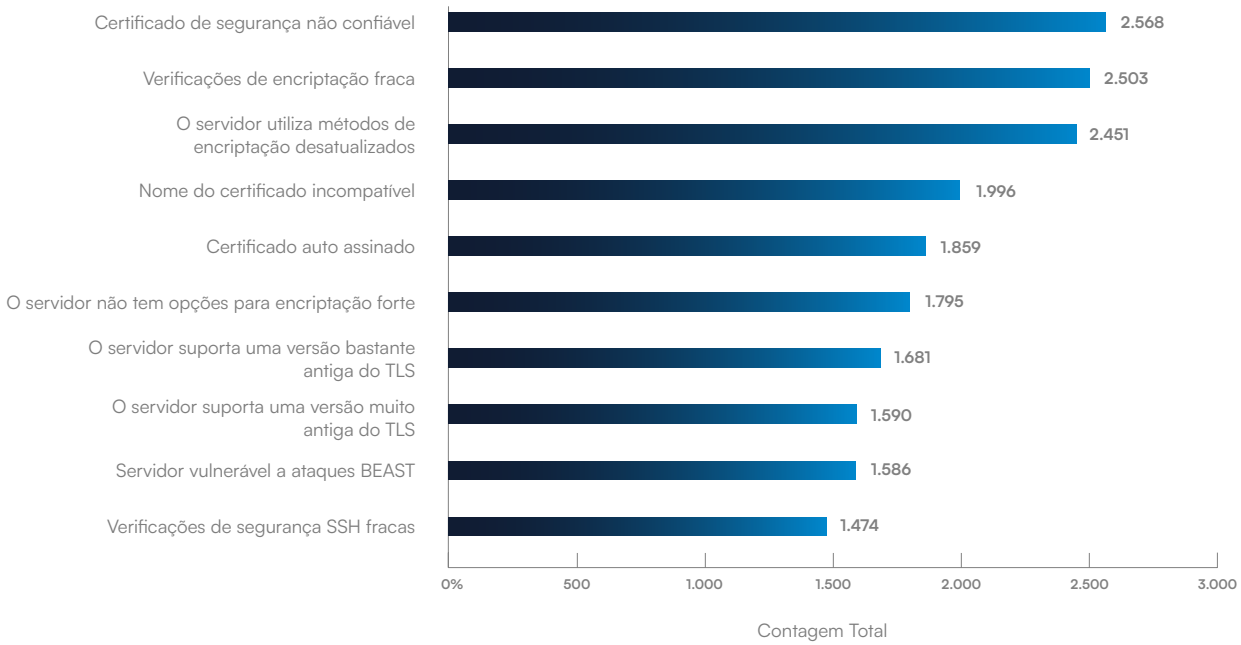


FIGURA 3

Principais vulnerabilidades de segurança de rede

Certificado de segurança não fidedigno

O que isto significa:

O certificado apresentado pelo servidor não foi emitido por uma Autoridade Certificadora (CA) de confiança.

Os atacantes podem usá-lo para:

Falsificar um site legítimo usando um certificado falso, permitindo que atacantes se insiram em comunicações legítimas para roubar dados, contornar a segurança, injetar conteúdo malicioso e muito mais.

Como se manter seguro:

Utilize certificados de ACs reputadas.

Para equipas mais técnicas: Implemente uma validação adequada de certificados e habilite o «certificate pinning» (onde a aplicação só confia num certificado específico ao conectar-se a um servidor). Também é importante verificar se o certificado de uma aplicação foi revogado (usando ferramentas como CRL e OCSP) para evitar confiar em certificados comprometidos. Consulte: OWASP Certificado Validação.

Verificações de encriptação fraca

O que isto significa:

O servidor utiliza algoritmos fracos ou comprimentos de chave insuficientes para encriptação.

Os atacantes podem usá-lo para:

Forçar ou explorar vulnerabilidades para decifrar dados sensíveis, como palavras-passe e informações financeiras. O brute-forcing envolve tentar muitas combinações diferentes de nome de utilizador/palavra-passe para ver se alguma funciona.

Como se manter seguro:

Implemente normas de encriptação fortes, como AES-256, RSA-2048+.

Para equipas mais técnicas: Desative cifras fracas e audite regularmente as configurações. Considere implementar criptografia de curva elíptica (ECC), como ECDSA ou ECDHE, para obter melhor segurança e desempenho (consulte: Recomendações ECC do NIST). Use conjuntos de cifras Perfect Forward Secrecy (PFS) para proteger sessões anteriores se as chaves forem comprometidas.

O servidor utiliza métodos de encriptação desatualizados

O que isto significa:

O servidor depende de algoritmos obsoletos como MD5, SHA-1 ou RC4.

Os atacantes podem usá-lo para:

Explorar vulnerabilidades conhecidas para quebrar encriptação ou falsificar assinaturas, levando a violações de dados.

Como se manter seguro:

Atualize para algoritmos modernos, como SHA-256 ou AES, e siga as melhores práticas da indústria (por exemplo, as diretrizes NIST acima).

Para equipas mais técnicas: Remova o suporte a algoritmos obsoletos (MD5, SHA-1, RC4) de todas as configurações. Teste com ferramentas como o SSL Labs para verificar se nenhum algoritmo desatualizado está ativado. Consulte: SSL Labs Test.

Nome do certificado incompatível

O que isto significa:

O nome de domínio não corresponde ao Nome Comum (CN) ou Nome Alternativo do Sujeito (SAN) do certificado.

Os atacantes podem usá-lo para:

Lançar ataques de interceção redirecionando o tráfego para um servidor malicioso.

Como se manter seguro:

Certifique-se de que os certificados correspondem a todos os domínios/subdomínios em uso.

Para equipas mais técnicas: Use campos SAN para certificados multidomínio. Automatize a gestão de certificados para evitar incompatibilidades durante as renovações.

Certificado auto assinado

O que isto significa:

O certificado é assinado pela mesma entidade que o possui, não por uma CA de confiança.

Os atacantes podem usá-lo para:

Torna mais fácil falsificar servidores, uma vez que qualquer pessoa pode criar certificados autoassinados.

Como se manter seguro:

Utilize certificados emitidos por CA para serviços voltados para o público e restrinja certificados autoassinados a sistemas internos.

Para equipas mais técnicas: Mantenha uma CA privada para uso interno e distribua a sua certidão raiz de forma segura. Monitore certificados autoassinados não autorizados na sua rede.

O servidor não possui opções de encriptação fortes

O que isto significa:

O servidor não oferece conjuntos de cifras modernos e seguros.

Os atacantes podem usá-lo para:

Forçar uma redução para encriptação mais fraca.

Como se manter seguro:

Configure os servidores para suportar conjuntos de cifras fortes, como Transport Layer Security (TLS) 1.2/1.3 com AES-GCM.

Para equipas mais técnicas: Desative o suporte para opções de criptografia TLS fracas ou inseguras, como NULL ou EXPORT, para que apenas conexões fortes, criptografadas e autenticadas sejam permitidas. Atualize regularmente o software do servidor para oferecer suporte aos protocolos e conjuntos de criptografia mais recentes.

O servidor suporta versões mais antigas do TLS

O que isto significa:

A versão do TLS utilizada está desatualizada e vulnerável a ataques.

Os atacantes podem usá-lo para:

Explorar fraquezas do protocolo para ataques de interceção ou de downgrade que enganam o sistema a utilizar um protocolo de segurança mais antigo e mais fraco.

Como se manter seguro:

Atualize a versão do TLS utilizada.

Para equipas mais técnicas: Desative o TLS 1.0 e 1.1. Suporta apenas TLS 1.2 e 1.3. Consulte: Mozilla Recomendações TLS.

O servidor suporta uma versão muito antiga do TLS

O que isto significa:

A versão do TLS em uso é obsoleta e insegura.

Os atacantes podem usá-lo para:

Explorar vulnerabilidades conhecidas

Como se manter seguro:

Atualize a versão do TLS utilizada.

Para equipas mais técnicas: Remova completamente as versões SSLv2, SSLv3 e TLS antigas. Use ferramentas automatizadas para verificar se há suporte a protocolos legados.

Servidor vulnerável a ataque BEAST

O que isto significa:

Ataques BEAST (Browser Exploit Against SSL/TLS) têm como alvo versões mais antigas do TLS que apresentam fraquezas na sua encriptação baseada em blocos.

Os atacantes podem usá-lo para:

Desencriptar HTTPS (Hypertext Transfer Protocol Secure) — uma versão segura do protocolo básico de comunicação web) tráfego e expor dados confidenciais.

Como se manter seguro:

Atualize para a versão mais recente do TLS e utilize conjuntos de cifras seguras.

Para equipas mais técnicas: Considere TLS 1.2+ com conjuntos de cifras AES-GCM ou ChaCha20-Poly1305. Desative as cifras do modo CBC em versões TLS mais antigas.

Verificações de segurança SSH fracas

O que isto significa:

A configuração SSH utiliza algoritmos fracos ou protocolos desatualizados. SSH (Secure Shell) é um protocolo de rede seguro usado para aceder e controlar remotamente computadores através de uma rede não segura, como a internet.

Os atacantes podem usá-lo para:

Credenciais de força bruta ou explorar chaves fracas para obter acesso não autorizado.

Como se manter seguro:

Implemente algoritmos de troca de chaves fortes, desative protocolos SSH fracos, utilize autenticação baseada em chave e implemente ferramentas especializadas de prevenção de intrusões que protejam servidores de ataques de força bruta, como o Fail2Ban ou similar.

Para equipas mais técnicas: Use apenas o protocolo SSH versão 2. Imponha comprimentos mínimos de chave (por exemplo, RSA 4096, Ed25519). Desative a autenticação por palavra-passe, se possível, e utilize a autenticação baseada em chave. Restrinja o acesso SSH por IP e utilize regras de firewall. Atualize regularmente o software do servidor SSH. Consulte: SSH Segurança Melhores Práticas.

As principais vulnerabilidades de software CVE detetadas

Software desatualizado e sem patches é um íman para ameaças cibernéticas. De acordo com a Barracuda Managed Vulnerability Security, estas são as principais vulnerabilidades de software identificadas nas redes dos clientes ao longo do último ano:

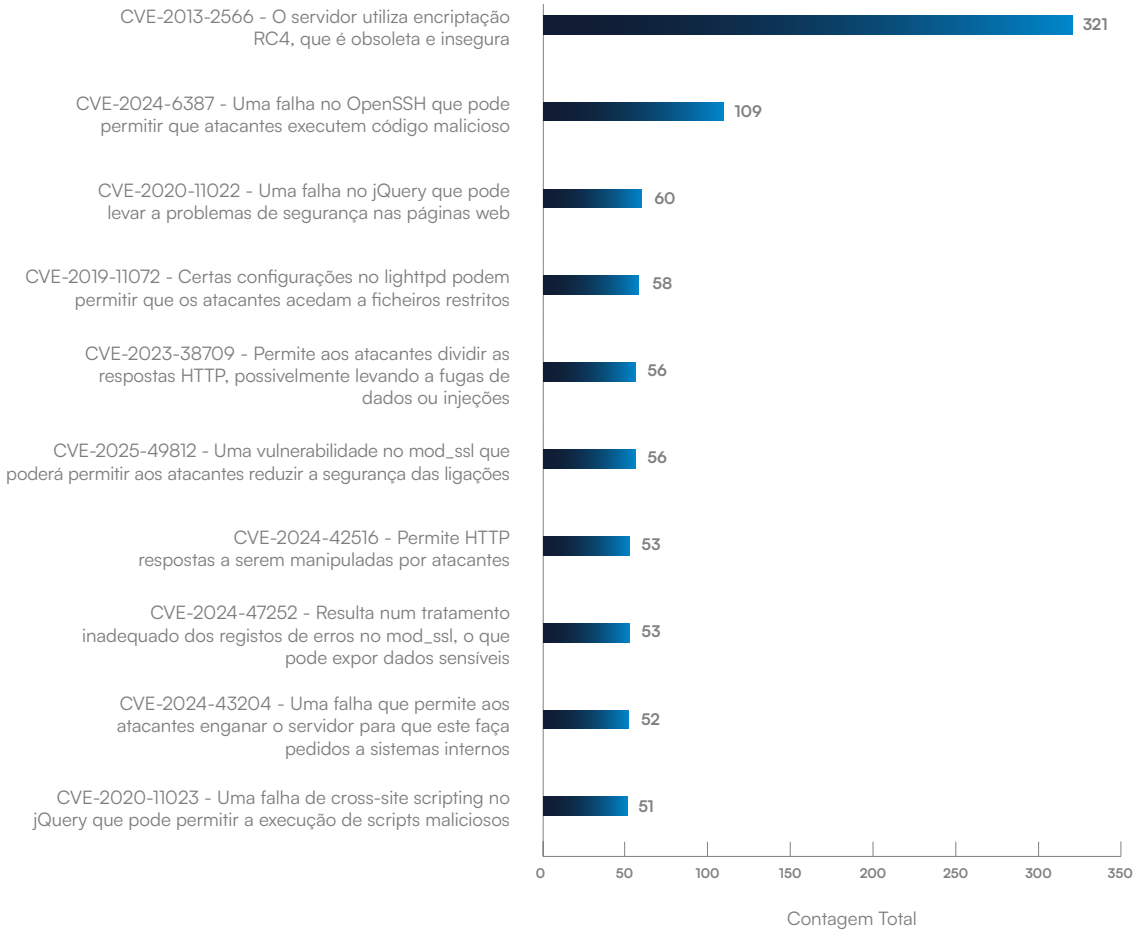


FIGURA 4

Principais Vulnerabilidades com CVE Designado Encontradas em Organizações

A vulnerabilidade mais amplamente detectada é também a mais antiga. A CVE-2013-2566 existe há quase 13 anos e ainda pode ser encontrada em sistemas legados, como servidores antigos, dispositivos incorporados ou aplicações.

Estes sistemas podem estar em uso ativo, mas muitas vezes estão inativos e esquecidos. A prevalência desta vulnerabilidade é um aviso claro sobre o risco de exposição dormente. Quanto mais cedo uma vulnerabilidade for corrigida, menor é a probabilidade de ser ignorada.

Apenas um CVE na lista tem uma classificação de severidade crítica, mas cinco são designados como de alta severidade. A pontuação média de severidade de todas as vulnerabilidades detectadas nos últimos 12 meses foi de 5,9.

CVE-2013-2566 — O servidor depende de encriptação RC4 vulnerável e desatualizada

Gravidade: **MÉDIA**

Os atacantes podem usá-lo para:

Explorar encriptação fraca para decifrar dados sensíveis em texto simples. RC4 é um tipo de cifra de encriptação.

Como se manter seguro:

Desativar RC4 nas configurações de TLS (ver acima) e utilizar cifras modernas como AES, TLS 1.2+.

CVE-2024-6387 — Uma falha no OpenSSH que pode permitir que atacantes executem código malicioso

Gravidade: **CRÍTICA**

Os atacantes podem usá-lo para:

Obtenha controlo total dos sistemas afetados remotamente. SSH é Secure Shell, um protocolo utilizado para conectar-se de forma segura a sistemas remotos através de uma rede não segura como a internet, e OpenSSH é uma versão gratuita e de código aberto.

Como se manter seguro:

Aplique imediatamente os patches mais recentes do OpenSSH e restrinja o acesso SSH.

CVE-2020-11022 — Um bug no jQuery que pode levar a problemas de segurança em páginas web

Gravidade: **MÉDIA**

Os atacantes podem usá-lo para:

Injetar scripts maliciosos em páginas web e roubar sessões e dados. jQuery é uma biblioteca JavaScript que facilita a codificação para os programadores.

Como se manter seguro:

Atualize para a versão mais recente do jQuery e limpe os dados antes de o seu sistema os utilizar.

CVE-2019-11072 — Certas definições no servidor web lighttpd podem permitir que atacantes acedam a ficheiros restritos

Gravidade: **ALTA**

Os atacantes podem usá-lo para:

Aceder a ficheiros restritos no servidor, incluindo configurações ou dados sensíveis. Um servidor lighttpd é um servidor web de código aberto concebido para ambientes críticos em termos de velocidade.

Como se manter seguro:

Atualize o servidor web lighttpd para a versão mais recente e certifique-se de que quaisquer localizações de ficheiros fornecidas pelos utilizadores sejam verificadas e limpas para evitar uso indevido.

CVE-2023-38709 — Permite que atacantes dividam respostas HTTP em servidores web Apache vulneráveis, possivelmente levando a fugas de dados ou injeção

Gravidade: **ALTA**

Os atacantes podem usá-lo para:

Adicione instruções falsas às respostas da web, engane os sistemas para armazenar dados prejudiciais ou injete código malicioso em páginas web, comprometendo a integridade dos dados e a segurança do utilizador.

Como se manter seguro:

Atualize o servidor web Apache e certifique-se de que todas as instruções ou dados de cabeçalho de navegador para servidor sejam devidamente verificados e limpos.

CVE-2025-49812 — Uma vulnerabilidade no mod_ssl que pode permitir que atacantes façam downgrade de conexões seguras

Gravidade: **ALTA**

Os atacantes podem usá-lo para:

Reduzir o nível de encriptação ou intercetar tráfego e expor dados sensíveis. mod_ssl é um módulo do servidor Apache HTTP que adiciona suporte para encriptação.

Como se manter seguro:

Aplique os patches mais recentes do Apache e imponha configurações de encriptação TLS fortes.

CVE-2024-42516 — Uma falha de segurança que permite aos atacantes manipular respostas web HTTP enviadas aos utilizadores

Gravidade: **ALTA**

Os atacantes podem usá-lo para:

Explorar fraquezas na forma como um sistema recebe, verifica e processa dados para injetar conteúdo nocivo ou redirecionamentos que podem levar a phishing, entrega de malware ou roubo de sessões de utilizador.

Como se manter seguro:

Aplique patches de fornecedor prontamente e imponha cabeçalhos de segurança fortes.

CVE-2024-47252 — Resulta em tratamento inadequado de registos de erro no mod_ssl que pode expor dados sensíveis

Gravidade: **MÉDIA**

Os atacantes podem usá-lo para:

Injetar conteúdo malicioso em registos que pode envenenar registos e potencialmente escalar privilégios.

Como se manter seguro:

Atualizar o Apache e restringir o acesso aos logs.

CVE-2024-43204 — Um bug que permite aos atacantes enganar o servidor para fazer pedidos a sistemas internos

Gravidade: **ALTA**

Os atacantes podem usá-lo para:

Forçar um servidor a fazer pedidos a sistemas internos, expondo a rede interna.

Como se manter seguro:

Corrigir o Apache e validar as configurações de cabeçalho.

CVE-2020-11023 — Uma falha de cross-site scripting no jQuery que pode permitir scripts maliciosos

Gravidade: **MÉDIA**

Os atacantes podem usá-lo para:

Injetar scripts maliciosos.

Como se manter seguro:

Atualize o jQuery, limpe as entradas do utilizador e use ferramentas para bloquear código prejudicial.

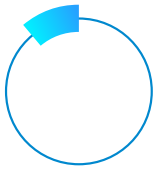
Descobertas adicionais da Segurança de Vulnerabilidades Geridas da Barracuda

4.146

Número total de vulnerabilidades críticas detetadas.

2.525

Número total de vulnerabilidades únicas identificadas.



11%

Proporção de vulnerabilidades que têm um exploit conhecido.

Relatório de Incidente — Firewall não corrigido utilizado na tentativa de RansomHub

Os atacantes exploraram vulnerabilidades não corrigidas num firewall Fortinet. Lançaram uma atividade de força bruta contra a rede de um cliente, mas foram bloqueados. Um mês depois, tentaram um login remoto (SSL VPN), mas foram novamente bloqueados. Dois dias depois, fizeram uma terceira tentativa. O Barracuda Managed XDR detetou atividade de PsExec (comando remoto) e encontrou software malicioso no controlador de domínio primário e no servidor de backup.

Configuração incorreta: Incidentes que envolvem ferramentas de segurança desativadas acidentalmente ou intencionalmente

As ferramentas de segurança que não foram configuradas corretamente representam um grande risco de segurança. O perigo pode ser agravado pela falsa sensação de segurança que advém de ter a ferramenta instalada em primeiro lugar. Nos últimos 12 meses, o Barracuda Managed XDR identificou funcionalidades desativadas que incluíam agentes de proteção de endpoints (representando 94% das deteções de segurança desativadas), MFA (3,62%), link seguro (1,4%) e regras de anexos seguros (0,6%).

Estudos mostram que a maioria das organizações está a tentar gerir demasiadas ferramentas de segurança. Quando os recursos são limitados, erros de configuração podem facilmente surgir. A melhor proteção é uma plataforma de segurança integrada com visibilidade total sobre definições e configurações que pode rapidamente e automaticamente sinalizar lacunas que precisam de ser corrigidas.

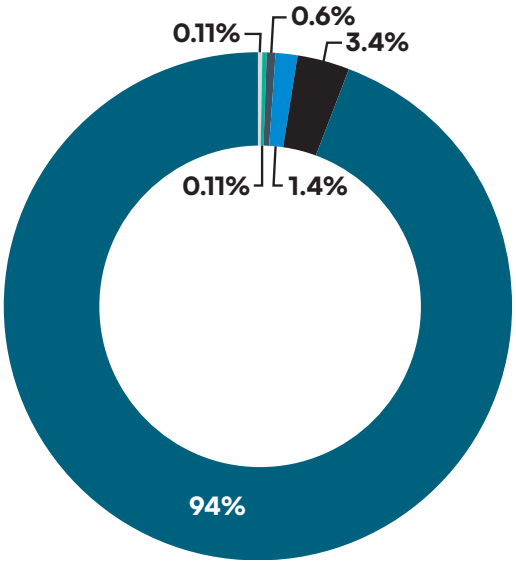


FIGURA 5

Recursos de segurança desativados com mais frequência

- Agente SentinelOne Endpoint desativado
- MFA do Microsoft 365 desativado
- Regra de 'links seguros' do Microsoft 365 ATP desativada
- Regra de «anexos seguros» do Microsoft Office ATP desativada
- MFA do Microsoft Azure desativada
- Google Workspace MFA desativado

100%

Proporção de incidentes a que o Barracuda Managed XDR respondeu que envolveu pelo menos um endpoint não protegido ou desonesto

66%

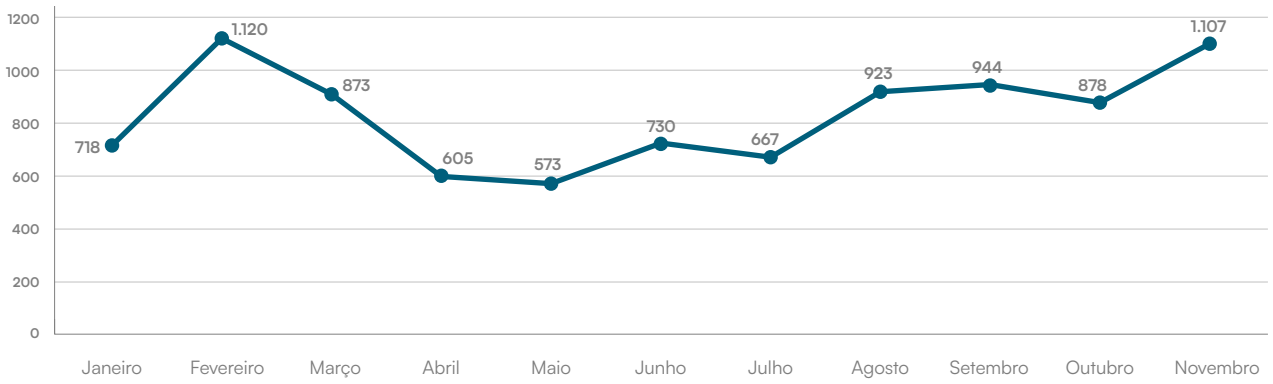
Proporção de incidentes a que o Barracuda Managed XDR respondeu que envolveram a cadeia de abastecimento ou um terceiro (acima de 45% em 2024)

A ameaça duradoura do ransomware

Nos últimos 12 meses, o Barracuda Managed XDR identificou 13.514 indicadores de que um ataque de ransomware estava em curso, incluindo ferramentas, técnicas e comportamentos. Ao contrário dos anos anteriores, já não existem picos ou vales acentuados, mas sim um nível elevado e constante de incidentes ao longo de todo o ano.

FIGURA 6

2025 incidentes relacionados com ransomware



1.5% a 5.6%

Proporção de todas as organizações impactadas por ransomware a cada mês em 2024

5.1% a 10.9%

Proporção de todas as organizações afetadas por ransomware cada mês em 2025

Principais famílias de ransomware encontradas em 2025

Akira

- Akira é um grupo de ransomware relativamente novo, conhecido por atacar organizações com ataques sofisticados. Frequentemente, emprega táticas de dupla extorsão, encriptando dados e ameaçando divulgar informações confidenciais, a menos que um resgate seja pago.
- **Táticas**: Utilização de malware avançado, ataques direcionados e roubo de dados.

Qilin

- Qilin é um grupo de ransomware que ganhou destaque por seus ataques direcionados a infraestruturas críticas e organizações empresariais.
- **Táticas**: Extorsão dupla, exploração de vulnerabilidades e utilização de malware para encriptar dados.

RansomHub

- RansomHub é uma operação de ransomware que funciona como ransomware como serviço (RaaS), permitindo que afiliados implementem ransomware sob a sua marca.
- **Táticas**: Modelo Ransomware-as-a-Service (RaaS), roubo de dados e extorsão.

Cactus

- Cactus é um grupo de ransomware que tem estado envolvido em ataques direcionados, muitas vezes exigindo resgates elevados.
- **Táticas**: Criptografia de dados, dupla extorsão e exploração de vulnerabilidades.

Relatório de Incidente — Várias lacunas de segurança expõem alvo ao Cactus

Os alvos foram enganados a descarregar ficheiros maliciosos através de chamadas do Teams. Os atacantes criaram canais para emitir comandos remotamente, mover-se lateralmente e manter a persistência. Tarefas agendadas maliciosas, edições de registo e DLL sideloading (quando um programa é enganado a carregar um ficheiro de código partilhado falso e prejudicial para que o código do atacante seja executado em vez do real) ajudaram os atacantes a escalar privilégios e a evadir a deteção. A equipa Barracuda Managed XDR encontrou dispositivos desonestos e mais de 1.600 dispositivos desprotegidos na rede, permissões relaxadas do Microsoft Teams, implementações vulneráveis de protocolo de ambiente de trabalho remoto (RDP) e shell seguro, ficheiros não assinados e falta de sensibilização dos funcionários.

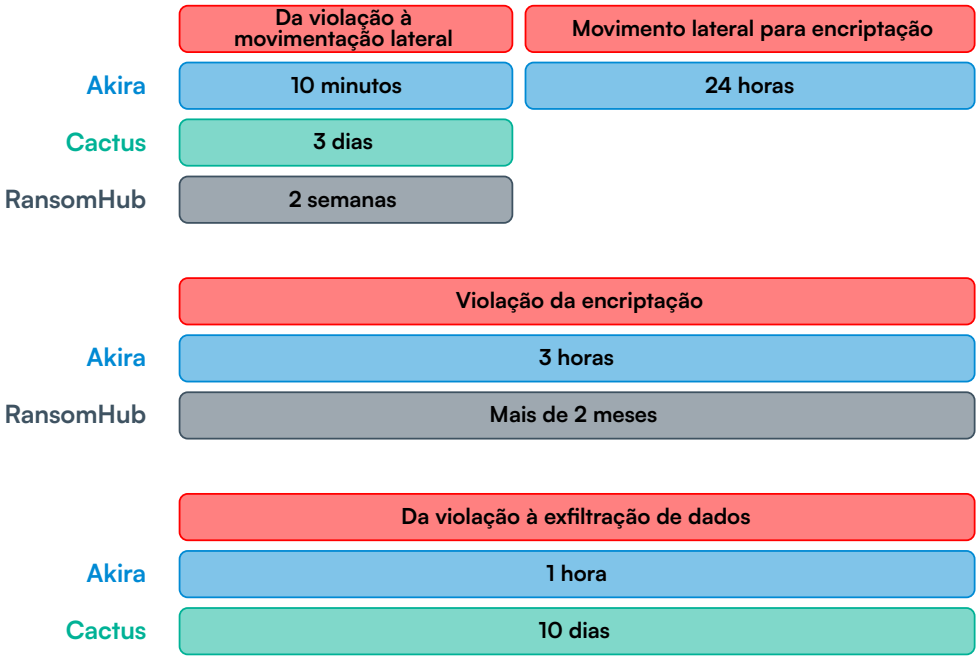
O ransomware move-se a diferentes velocidades

De acordo com os dados de deteção e incidentes do Barracuda Managed XDR, os ataques de ransomware mais rápidos em 2025 levaram apenas horas de ponta a ponta, enquanto os mais longos levaram meses.

Intrusões prolongadas permitem danos máximos, pois os atacantes têm tempo para reconhecimento, exfiltração de dados, sabotagem e mais. Incidentes que se movem a uma velocidade relâmpago podem ser mais difíceis de detectar e conter antes de serem executados e o dano estar feito.

As organizações precisam estar preparadas para ambos os tipos de ataques — e ter ferramentas de segurança implementadas que estejam sempre em alerta.

A velocidade do ransomware — 3 atores



Tempos estimados a partir de incidentes do mundo real

Relatório de Incidente — XDR deteta ransomware Akira a explorar conta 'fantasma' e servidor desprotegido

Os atacantes violaram a rede através de uma conta que foi criada para um fornecedor externo e não foi desativada quando este saiu. Os atacantes tentaram mover-se lateralmente e desativar a segurança de endpoint, mas foram bloqueados. Eles mudaram para um servidor desprotegido, escalaram os seus privilégios e lançaram o ransomware. Todos os dispositivos impactados foram neutralizados. Outros riscos encontrados na rede alvo incluíam dispositivos desprotegidos, um canal VPN aberto no seu firewall e MFA inconsistente.

Conclusão: Como manter-se seguro num mundo de ameaças complexas

As equipas de segurança enfrentam desafios crescentes. Com recursos limitados, devem proteger um panorama cada vez maior de dispositivos, aplicações, vulnerabilidades críticas e ferramentas de segurança fragmentadas, muitas vezes sem a visibilidade unificada necessária para se manterem à frente das ameaças.

Tudo está prestes a tornar-se ainda mais difícil à medida que os atacantes começam a aproveitar a IA agente.

Os sistemas de IA agentica irão automatizar as fases iniciais e repetitivas de um ataque, analisar ambientes sem parar, identificar configurações fracas e lançar explorações direcionadas em minutos. Os atores de ameaças que utilizam agentes de IA serão capazes de tomar decisões, ajustar estratégias e corrigir ou reescrever código malicioso quando algo falha ou encontram um obstáculo. Esta mudança aumentará drasticamente a velocidade, escala e consistência dos ataques.

As organizações precisam de uma estratégia de segurança unificada que integre tecnologias de deteção avançadas, potenciadas por IA, com um SOC totalmente autónomo, complementado por educação do utilizador, resposta automatizada a ameaças e uma cultura de segurança resiliente.

Existem vitórias rápidas, como as descritas ao longo deste relatório. Incluem autenticação multifator consistente e controlos de acesso, uma abordagem robusta à gestão de patches e proteção de dados, e formação regular de sensibilização sobre cibersegurança para os funcionários.

Isto deve ser sustentado por uma plataforma de segurança abrangente e gerida e uma solução XDR gerida 24/7 que integra segurança de rede, endpoint, servidor, cloud e e-mail — proporcionando visibilidade total de ponta a ponta e controlo de gestão suportado por um SOC totalmente autónomo.

A segurança a longo prazo reside na resiliência cibernética. A deteção e a prevenção são os pilares de qualquer estratégia de segurança, mas perante ameaças cada vez mais complexas e evasivas, ser capaz de responder e recuperar de ataques rapidamente e com impacto mínimo é fundamental.

As conclusões deste relatório baseiam-se nos dados de deteção da Barracuda Managed XDR, uma plataforma de visibilidade, detecção e resposta estendidas (XDR), apoiada por um centro de operações de segurança (SOC) que fornece aos clientes serviços de detecção, análise, resposta a incidentes e mitigação de ameaças 24 horas por dia, 7 dias por semana, conduzidos por humanos e IA.

O Barracuda Managed XDR faz parte do BarracudaONE, uma plataforma alimentada por IA que protege e-mails, dados, aplicações e redes com soluções inovadoras e um painel centralizado para maximizar a proteção e fortalecer a resiliência cibernética.

Sobre a Barracuda

A Barracuda é uma empresa líder global em cibersegurança que oferece proteção completa contra ameaças complexas para empresas de todas as dimensões. A nossa plataforma BarracudaONE, potenciada por IA, protege email, dados, aplicações e redes com soluções inovadoras, XDR gerido e um painel centralizado para maximizar a proteção e reforçar a resiliência cibernética. Com a confiança de 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 comprar, implementar e utilizar.