SOTI

10 YEARS
OF SECURITY INSIGHT

V10 EDIÇÃO 06

Análise aprofundada do setor de saúde

Ataques se concentram em aplicativos e APIs

Akamai

State of the Internet/Security

Índice

Da vulnerabilidade à visibilidade, esclarecendo a situação da cibersegurança do setor de saúde

O estado do setor de saúde pode ser resumido a uma palavra: vulnerável. Para abordar isso, o tema principal da saúde em 2024 deve ser a visibilidade. Mais plataformas, software de terceiros e troca de dados em larga escala exigem maior visibilidade, mas a modernização técnica está se movendo tão rapidamente em organizações de saúde que muitas têm dificuldade com a verdadeira visibilidade sobre seu ecossistema. Além da complexidade, existem medidas de conformidade que exigem mais compartilhamento, mas com controles mais rigorosos. Embora esse seja um próximo passo lógico para eliminar fossos de dados e monopólios de rede, ele adiciona elementos de sofisticação técnica que muitas vezes excedem as capacidades de segurança atuais da maioria do setor, com exceção dos principais participantes.

Agentes de ameaças estão vendo uma coisa: oportunidade. Como cada área de saúde está abrindo seus sistemas para trocar informações mais confidenciais da nossa sociedade, estamos combinando novos sistemas e novos padrões com décadas de infraestrutura legada. Assim, além de essa infraestrutura legada criar uma dívida técnica própria potencialmente enorme, ela também fornece um ambiente ideal no qual agentes mal-intencionados podem prosperar.

Infelizmente, a onda cada vez maior de ataques de cibersegurança no setor de saúde não é surpreendente. Nos Estados Unidos, especificamente, muitas organizações de saúde têm tratado a cibersegurança como um exercício protocolar durante solicitações de propostas e avaliações de fornecedores por anos. Em vez de desenvolver conhecimentos internos, as organizações geralmente exigem fornecedores certificados pelo HITRUST, HIPAA, SOC 2 e usam Contratos de Associado Empresarial para transferir os riscos para esses fornecedores. Embora esse seja um começo decente, ainda estamos vendo manchetes alardeando grandes problemas financeiros, incidentes operacionais ou, pior ainda, ameaças à segurança dos pacientes no setor de saúde. Agora, percebemos que isso pode incomodar algumas pessoas, mas quando entre um quarto e metade dos 1.000 principais hospitais e sistemas de saúde usam a mesma "lista de verificação de segurança" baseada em planilha para aprovar e integrar fornecedores, temos um problema.

Vale a pena focar no fato de que as operadoras de serviços de saúde estão mais expostas do que nunca, com medidas de conformidade as puxando para fora de seus antigos sistemas locais em lote para atender aos requisitos de dados baseados em API do ecossistema moderno. Embora essa modernização esteja fornecendo às operadoras de serviços de saúde o acesso a dados clínicos que elas têm procurado há anos, a troca aberta é uma nova maneira de fazer negócios que vem com novos tipos de riscos. Como possuem dados financeiros e dados clínicos, as operadoras de serviços de saúde devem proteger sua infraestrutura e elevar cuidadosamente sua postura de segurança à medida que aderem a cada nova medida de conformidade.

A conclusão: essas mudanças de mercado estão aqui para ficar. O setor de saúde não terá uma reversão dos requisitos de API e nuvem. Embora as preocupações de segurança sobre mudanças sejam normais, essa ênfase na troca de dados aberta é um progresso monumental para um setor historicamente atormentado por silos de dados.

Neil Jennings
Vice-presidente, Untangle Health

Chris Notaro
CEO, Untangle Health

Introdução

O setor de saúde tem alguns desafios únicos quando se trata de cibersegurança.

- Os riscos podem ser vida ou morte.
- O valor da informação está entre os mais altos de qualquer setor.
- A infraestrutura inclui sistemas legados e dispositivos de IoMT (Internet das Coisas Médicas).
- Os sistemas são federados e muitas vezes interdependentes.
- Os requisitos de conformidade estão entre os mais árduos.

Neste relatório SOTI (State of the Internet), analisamos dados de ameaças e tendências relacionadas aos riscos para o ecossistema de saúde. As duas ameaças que estão tendo os maiores impactos nesse setor são ataques a aplicativos da Web e APIs e ataques de DDoS (negação de serviço distribuída).

Os participantes em todo o ecossistema de saúde (operadoras de serviços, prestadoras e empresas farmacêuticas e de ciências da vida) também enfrentam desafios únicos que devem servir como base de informação para sua estratégia de segurança.

As companhias de seguros ou operadoras de serviços de saúde têm acesso robusto a dados clínicos e financeiros para determinar a elegibilidade, a cobertura e os pagamentos, e são um dos principais vínculos de compartilhamento de dados em todo o setor.

As organizações farmacêuticas e de ciências da vida descobriram que os agentes de ameaças estão se concentrando em suas inovações, incluindo o uso de inteligência artificial e aprendizado de máquina para analisar grandes conjuntos de dados para inúmeros aplicativos, o que as colocou firmemente na encruzilhada de inovação e risco.

Os investimentos dos fornecedores de serviços de saúde são canalizados principalmente para inovações clínicas, como a telessaúde e a crescente IoMT, com menos gastos organizacionais em funções mais tradicionais, como a evolução das abordagens de cibersegurança, que são essenciais para a resiliência organizacional.

O impulso para a interoperabilidade permite melhores resultados financeiros e de pacientes, mas também introduz riscos na forma de ataques a aplicativos da Web e APIs.

De uma perspectiva histórica, os agentes de ameaças têm visado o ecossistema de saúde por anos. Em 2024, pelo 13º ano consecutivo, o setor de saúde experimentou os maiores custos de violação de dados de todos os setores, com o custo médio atingindo US$ 9,77 milhões, o que foi substancialmente maior do que o dos serviços financeiros, o setor com custos mais próximos, com US$ 6,08 milhões.

As APIs são uma das principais tecnologias que afetam todos os subverticais do setor de saúde. As APIs possibilitam o compartilhamento de dados entre prestadoras, operadoras de serviços de saúde, pacientes e outras partes, como prontuários médicos eletrônicos, empresas de dispositivos médicos e sistemas de troca de informações de saúde. O impulso para a interoperabilidade permite melhores resultados financeiros e de pacientes, mas também introduz riscos na forma de ataques a aplicativos da Web e APIs.

Outra ameaça comum à camada de aplicativo são ataques de DDoS. Eles são a arma de escolha atual na EMEA (Europa, Oriente Médio e África), que é provavelmente atribuível a desenvolvimentos geopolíticos e grupos hacktivistas pró-russos na região. No entanto, nenhum país ou região está imune a ataques, já que o número de grupos que realizam ataques de DDoS e as táticas, técnicas e procedimentos que usam mudam continuamente.

Principais informações

41%

Porcentagem de ataques a APIs no ecossistema de saúde que visava operadoras de serviços

Os ataques a APIs estão crescendo constantemente no ecossistema de saúde, particularmente ataques a operadoras de serviços e companhias de seguros devido à riqueza de informações que possuem: PHI (informações de saúde protegidas), dados de sinistros e informações financeiras.

A expansão de APIs representa riscos significativos, como acesso não autorizado a dados

A expansão de APIs, ou a proliferação não regulamentada de APIs dentro das organizações, pode criar lacunas de segurança significativas por meio da falta de visibilidade e de seu surgimento fora dos controles de segurança. Como resultado, a expansão de APIs amplia a superfície de ataque de uma organização e apresenta riscos como acesso não autorizado a dados confidenciais.

88%

Percentagem de ataques de DDoS da camada 7 contra organizações farmacêuticas na EMEA

As empresas farmacêuticas da região da EMEA experimentaram o maior volume de ataques de DDoS da camada 7, seguido pela América do Norte e APJ (Ásia-Pacífico e Japão). Um exame mais detalhado de dados do 1° semestre de 2024 revela que o número de ataques contra a EMEA e a América do Norte está no caminho para exceder o total de cada região em 2023.

21 MILHÕES

Média mensal de ataques a aplicativos da Web e APIs contra prestadoras de serviços de saúde

O impulso para a interoperabilidade de dados e outros requisitos de conformidade alimentaram o crescimento do uso de aplicativos da Web e APIs, que por sua vez criou riscos de segurança para prestadoras e pacientes.

415 MILHÕES

Média mensal de ataques de DDoS da camada 7 contra prestadoras de serviços de saúde

O setor da saúde está passando por um aumento nos ataques de DDoS, impulsionados pelo hacktivismo e pelo atual clima geopolítico. Esses ataques podem causar interrupções e falhas que ameaçam os resultados dos pacientes. Em 2023, o Killnet lançou uma campanha de DDoS em grande escala que impactou principalmente as organizações provedoras.

As operadoras de serviços de saúde estão em alto risco de violações de APIs

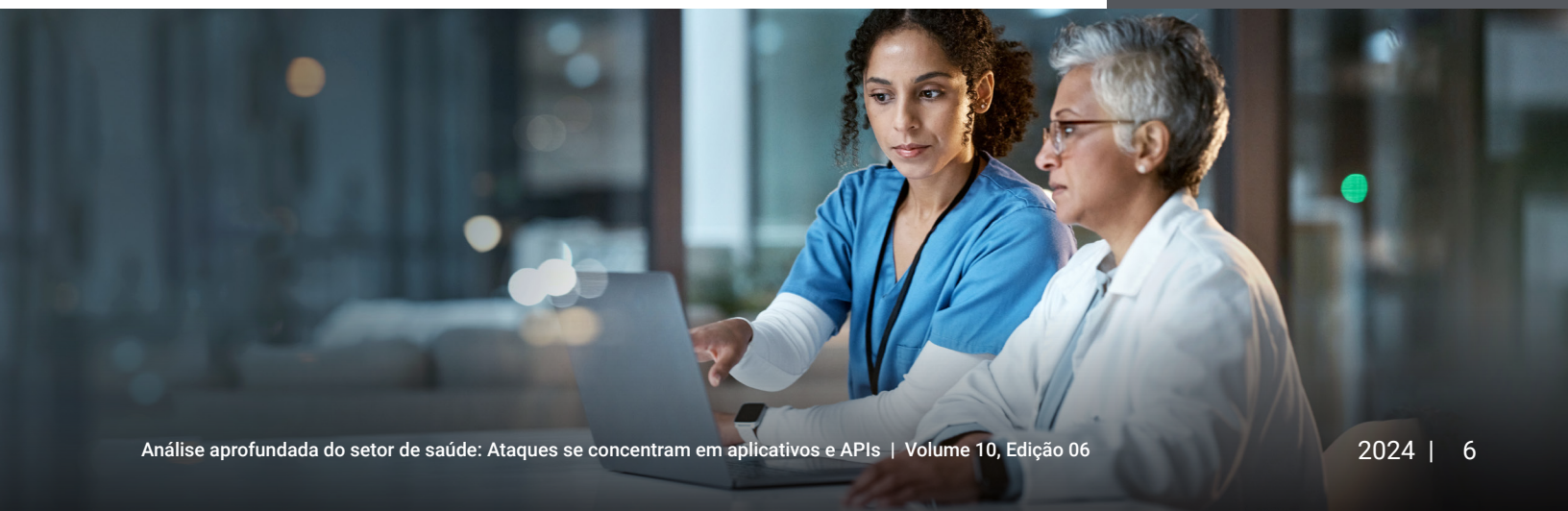
Embora o alto uso de APIs das operadoras de serviços de saúde para coletar e processar dados em todo o ecossistema de saúde ofereça enormes benefícios, ele também vem com compensações, especialmente requisitos de conformidade significativos e riscos de segurança. Os cibercriminosos e os agregadores estão atacando e violando esses recursos, o que pode resultar em problemas de segurança e privacidade.

Para as operadoras de serviços de saúde, os ataques habilitados por APIs também podem resultar em interrupções de serviço que afetam operações de cadastro e sinistro, levam a tempo de inatividade oneroso e prejudicam a marca da empresa. O ataque sistêmico que bloqueou severamente o processamento de pagamentos em farmácias nos Estados Unidos em fevereiro de 2024 é um exemplo recente e doloroso.

Tendências de ataques a APIs

A pesquisa da Akamai descobriu que de janeiro de 2023 a junho de 2024, 41% dos ataques a APIs que visaram o ecossistema de saúde foram contra operadoras de serviços de saúde. Isso indica que as operadoras de serviços de saúde enfrentam um risco mais concentrado de violação de APIs por ataques, o que é consistente com a importância das operadoras para manter o sistema de saúde em movimento, já que aproximadamente 67% das despesas totais de saúde dos EUA passam por operadoras de serviços, conforme dados de 2022.

Vemos uma tendência semelhante em outros setores regulamentados, especialmente naqueles que lidam com sistemas de pagamento. O setor financeiro, por exemplo, está mais adiantado em sua jornada de transformação digital e já está usando APIs mais integradas como parte de seus modelos de negócio. O Open Banking está ampliando seu uso de APIs, o que tem causado mais riscos à segurança. Portanto, o setor financeiro está passando por uma maior concentração de ataques focados em APIs, conforme encontrado em nosso relatório SOTI de segurança de APIs.



Ao analisar mais de perto os dados de ataque a APIs de operadoras de serviços de saúde, os pesquisadores da Akamai observaram flutuações na atividade durante o período de 18 meses, de janeiro de 2023 a junho de 2024, particularmente trimestrais. A tendência geral ascendente dentro de cada trimestre pode refletir a sincronização entre os sistemas no final do trimestre para reconciliar dados previstos e reais, mas o aumento geral no quarto trimestre de 2023 provavelmente pode ser atribuído a invasores que visam os períodos de inscrição para interromper as operações (Figura 1).

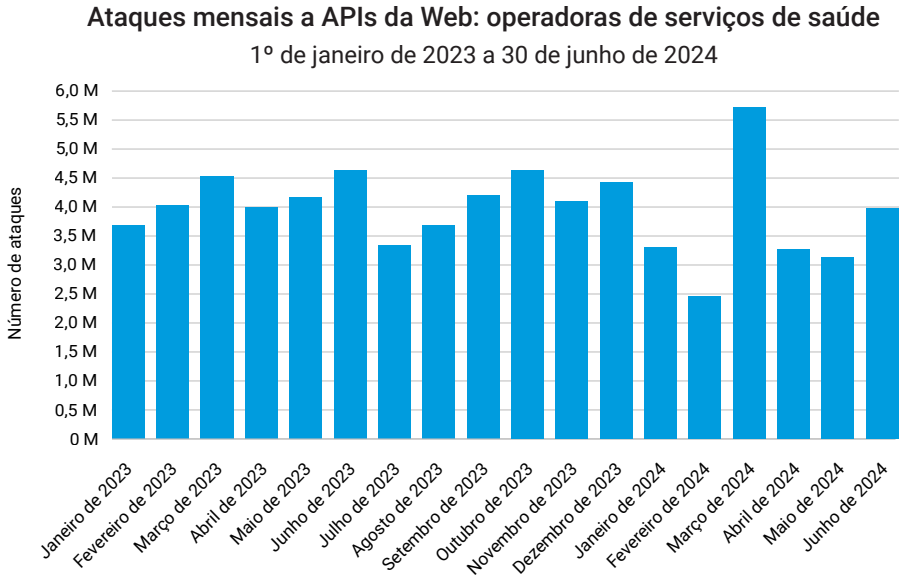


Fig. 1: Os ataques da Web contra APIs aumentaram em cada trimestre, com um aumento geral no quarto trimestre de 2023

Violações de APIs e desafios críticos de segurança em todos os setores

Embora muitos desafios de segurança de APIs sejam exclusivos do setor de saúde, os conceitos básicos de APIs são semelhantes em todos os setores, e vale a pena rever alguns dos riscos mais técnicos que todos precisamos para mitigar. Primeiro, devemos nos concentrar nos riscos de segurança a APIs destacados pelo OWASP Top 10. Mas também precisamos garantir que nossos desenvolvedores e funcionários de TI entendam as vulnerabilidades mais comuns que categorizamos como problemas de postura e problemas de tempo de execução.

- **Problemas de postura** dizem respeito a falhas na implementação da API da empresa. Alertas que indicam problemas de postura ajudam as equipes de segurança a identificarem e corrigirem vulnerabilidades de alta prioridade antes que elas possam ser exploradas pelos invasores. Os problemas de postura comuns incluem pontos de extremidade de sombra e dados confidenciais em um URL.
- **Os problemas de tempo de execução** são ameaças ativas ou comportamentos que exigem uma resposta urgente. Esses alertas críticos são mais sutis do que outros tipos de alertas de segurança, uma vez que eles assumem a forma de violações de APIs (em comparação com tentativas de violação de infraestrutura mais explícitas). Os problemas de tempo de execução comuns incluem tentativas de acesso de recurso não autenticadas e scraping de dados.

Também é fundamental dar um passo atrás e olhar para três desafios mais gerais que as APIs apresentam para garantir que seu programa de segurança cubra exploração e violação de APIs.

1. **Visibilidade**: você tem controles técnicos e de processo para garantir que todas as APIs estejam protegidas por seu programa? Esse é um problema fundamental, pois as APIs são muitas vezes parte da transformação ou incorporadas em novos produtos, portanto, muitas não têm o mesmo nível de direcionamentos, proteções e validações de uma presença na Web tradicional.

2. **Vulnerabilidades**: suas APIs estão seguindo as práticas recomendadas de desenvolvimento? Você está evitando os problemas de codificação mais comuns do OWASP? Além disso, você está monitorando e verificando vulnerabilidades?

3. **Violação de lógica de negócios**: você tem uma linha de base do tráfego esperado? Você estabeleceu o que constitui atividades suspeitas?

As respostas a essas perguntas formam a base do que sua equipe deve entender. Os objetivos gerais devem ser ter a visibilidade e a capacidade de conduzir investigações e estabelecer processos para mitigar rapidamente as ameaças. Isso é verdade tanto para APIs internas quanto para as voltadas para o paciente.

Melhor desempenho pode significar maior risco

O desempenho está se tornando uma preocupação maior, pois os pacientes demandam o mesmo nível de experiência do usuário em todos os seus aplicativos. Isso significa que o ecossistema de saúde precisa ser protegido contra ataques de negação de serviço, bem como contra ataques de violação. Além disso, os fornecedores devem obedecer a requisitos regulatórios de transparência que estão impulsionando a necessidade de disponibilidade imediata de informações.

A expansão de APIs pode levar a uma má visibilidade que se torna ainda mais turva à medida que a superfície de ataque se expande. As APIs geralmente fazem parte de projetos complexos de transformação digital e, por isso, podem não estar no radar das organizações da área de saúde. E os programas de segurança, menos ainda.

Os tipos de dados, tanto médicos quanto financeiros, envolvidos nas atividades de negócios diárias são altamente regulamentados e podem ser alvo de cibercriminosos, o que complementa os desafios para as operadoras de serviços de saúde.

As APIs geralmente fazem parte de projetos complexos de transformação digital e, por isso, podem não estar no radar das organizações da área de saúde. E os programas de segurança, menos ainda.

O número de ataques de DDoS contra organizações de ciências da vida está aumentando

O foco na cibersegurança farmacêutica se tornou preciso durante a pandemia da COVID-19, quando a pesquisa de desenvolvimento de vacinas, dados de teste, fabricação, produção e implementação foram todos considerados alvos fáceis pelos agentes de ameaças. Hoje, a saúde é classificada como infraestrutura crítica dos EUA e o novo financiamento bipartidário eleva os requisitos de resiliência em todos os setores que são considerados críticos. As razões são claras:

- As tensões internacionais continuam a aumentar globalmente, e o clima geopolítico pesa muito sobre os executivos que responderam à 25ª Pesquisa Anual Global com CEOs da PwC. Quase um terço dos entrevistados disse que o conflito geopolítico ameaça o crescimento de suas empresas, e mais de dois terços disseram que é um fator esperado na perturbação da cadeia de suprimentos.
- Abordagens como o sourcing localizado e o uso aprimorado da tecnologia de blockchain podem ajudar as empresas farmacêuticas a aumentarem a resiliência e melhorarem os impactos clínicos e de negócios.
- Os dados globais da Akamai para o setor de ciências da vida sugerem que os ataques de DDoS, e o número de grupos que os realizam, estão apenas crescendo; resiliência é exatamente o que esse setor precisa.

EMEA é alvo de ataques de DDoS em camada de aplicativos contra organizações farmacêuticas

A pesquisa da Akamai descobriu que de janeiro de 2023 a junho de 2024, a região EMEA experimentou 88% de todos os ataques de DDoS de camada de aplicação (camada 7) que visavam organizações farmacêuticas, enquanto a América do Norte e a APJ representaram 7% e 5% desses ataques, respectivamente. Ao olhar para o 1° semestre de 2024, podemos ver que a concentração de ataques na EMEA e na América do Norte estava em ascensão e em um caminho para exceder o número total de ataques de cada região em 2023 (Figura 2).

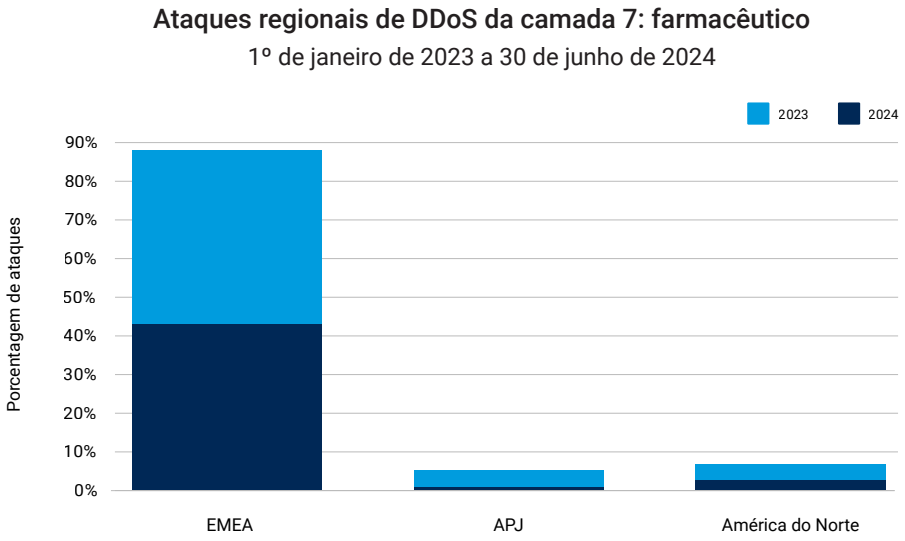


Fig. 2: A concentração de ataques de DDoS da camada 7 na EMEA continua de 2023 para 2024 e aumentou no 1° semestre de 2024, enquanto os ataques na América do Norte também estavam em ascensão

Diferentemente dos ataques de DDoS tradicionais da camada 3 e da camada 4, que visam sobrecarregar a infraestrutura de rede e de camada de transporte, os ataques de DDoS de camada 7 têm como alvo funcionalidades específicas de aplicativos ou o próprio servidor de aplicativos. Eles têm capacidade de causar danos significativos mesmo com uma quantidade relativamente pequena de tráfego mal-intencionado.

Os ataques de DDoS da camada 7 têm como alvo recursos de nível de aplicativo, como CPU e memória, de modo que o aplicativo ou serviço visado pode ficar lento ou totalmente não responsivo, mesmo que a rede permaneça disponível.

Aumento dos ataques de DDoS no setor de saúde e ciências da vida na União Europeia

O relatório ENISA 2023 Threat Landscape: Health Sector confirma um aumento no número de ataques de DDoS no setor de saúde e ciências da vida na União Europeia. É interessante notar que os países "hot spot" para incidentes cibernéticos no relatório (especialmente França, Alemanha e Holanda) se correlacionam positivamente com a concentração geográfica das empresas farmacêuticas e de biotecnologia nas 1.000 principais empresas da União Europeia de 2022.

A ENISA (Agência da União Europeia para a Cibersegurança) atribui o aumento dos ataques de DDoS aos desenvolvimentos geopolíticos e grupos hacktivistas pró-russos, como o Killnet.

Organizações de ciências da vida dos EUA visadas em seguida

O Killnet visou hospitais europeus antes de passar para alvos hospitalares em quase todos os estados dos EUA. Embora esses ataques cibernéticos em hospitais tenham gerado a maior parte das notícias, um relatório de abril de 2023 do Departamento de HHS (Saúde e Serviços Humanos) dos EUA observa que a porcentagem de organizações visadas pelo Killnet com ataques de DDoS foi na verdade mais alta entre as empresas farmacêuticas e de biotecnologia.

Dado que os Estados Unidos têm uma maior participação no mercado global de ciências da vida (50%) do que a EMEA (34%), é compreensível esperar que a ameaça de ataques de DDoS a empresas farmacêuticas sediadas nos Estados Unidos se intensifique.

Mas nenhum país ou localização geográfica está imune. A Índia, um dos maiores produtores e exportadores mundiais de medicamentos genéricos, sofreu grandes consequências no ano passado após uma violação de dados que vazou 17 TB de dados empresariais. A gangue de ransomware e agente de ameaças ALPHV/BlackCat reivindicou a responsabilidade por outro ataque de ransomware que incluía informações confidenciais sobre fornecedores, clientes e documentos de 1.500 funcionários dos EUA.

Quais agentes de ameaça estão usando quais táticas?

O relatório da ENISA cita o ALPHV/BlackCat como um dos principais grupos de invasores contra as ciências da vida na EMEA, o mesmo grupo que atingiu a cadeia de suprimentos dos EUA no início deste ano.

Assim como o Killnet, o Anonymous Sudan é mencionado no relatório como sendo politicamente motivado; essa organização criminosa primeiro visou grupos de prestadoras, mas agora está expandindo suas metas e incluindo outras partes do ecossistema de saúde.

Essa expansão torna os desenvolvimentos recentes, como a reivindicação de responsabilidade do Anonymous Sudan por recentes ataques de DDoS contra o OpenAI, ainda mais preocupantes. O grupo diz que usou o botnet Skynet, que recentemente incorporou suporte para ataques de DDoS da camada 7 para sobrecarregar aplicativos e gerar erros.

Riscos altos exigem uma abordagem conservadora

As empresas farmacêuticas têm sido líderes do setor de saúde no uso de IA (inteligência artificial), especificamente ML (aprendizado de máquina), e se beneficiaram da capacidade da IA de analisar grandes conjuntos de dados para inúmeros aplicativos. Esses benefícios incluem detecção precoce de doença, descoberta mais rápida de medicamentos e melhorias na fabricação de medicamentos. No entanto, semelhante a outros setores que adotaram a transformação digital (como serviços financeiros), as ciências da vida estão na encruzilhada da inovação e do risco.

A porcentagem de organizações visadas pelo Killnet com ataques de DDoS foi na verdade mais alta entre as empresas farmacêuticas e de biotecnologia.

As organizações farmacêuticas estão assumindo uma posição. Ao analisar como outros setores regulamentados lidam com ataques de DDoS da camada 7, os pesquisadores da Akamai descobriram que, quando se trata da porcentagem de ações de "negação" versus "alerta" aplicadas, as empresas farmacêuticas têm políticas conservadoras que negam atividade anômala a uma taxa alta (Figura 3).

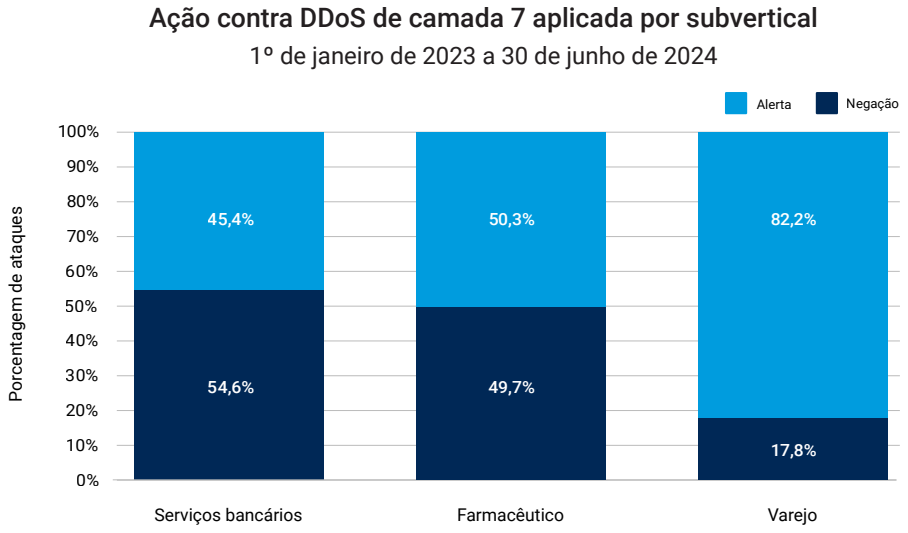


Fig. 3: As empresas farmacêuticas e de ciências da vida têm um alto percentual de ações de negação em comparação com alertas

Desde que relatamos pela primeira vez essa estatística de negação em comparação com alertas de janeiro de 2023 a março de 2024, a taxa aumentou mais de quatro pontos percentuais, com ações de negação subindo de 45,5% para 49,7%, um salto relevante em um curto período.

Outros setores, como serviços financeiros e bancos, compartilham essas políticas igualmente conservadoras; tanto os serviços bancários quanto as ciências da vida são considerados de infraestrutura crítica e, portanto, fortemente regulamentados, o que representa muitos paralelos.

Além disso, no caso de organizações farmacêuticas, as consequências de um ataque de DDoS bem-sucedido podem ser graves, potencialmente ameaçando a vida das pessoas ao atrasar o acesso a medicamentos que sustentam a vida. Faz sentido adotar a aplicação de uma ação de negação e depois investigar a atividade.

Em contraste, o varejo assume uma postura menos agressiva, permitindo mais tempo para receber um alerta e avaliar a atividade anômala antes de agir. Mas podemos ver uma mudança para ações de negação mais frequentes entre os varejistas se novos regulamentos entrarem em jogo, particularmente em torno do uso de IA/ML.

Os pesquisadores da Akamai descobriram que quando se trata da porcentagem de ações de "negação" em comparação com "alerta" aplicadas, as empresas farmacêuticas têm políticas conservadoras que negam atividade anômala a uma taxa comparativamente alta.

As prestadoras de serviços de saúde estão sob cerco

Citando uma análise do HHS sobre violações de dados publicada em dezembro de 2023, o diretor de segurança do Centro de Compartilhamento e Análise de Informações em Saúde (Health-ISAC) disse que, em média, 3.604 prontuários médicos foram violados e relatados ao HHS a cada hora.

O número de ataques cibernéticos a prestadoras de serviços de saúde e hospitais continua a aumentar. Conectividade e interoperabilidade alimentadas por aplicativos da Web e o uso obrigatório de APIs podem expor prestadoras de serviços e pacientes ao risco. As vulnerabilidades não corrigidas e a dívida técnica da tecnologia legada são um desafio caro que os grupos de ransomware usam em seu benefício.

E a ameaça contínua de ataques de DDoS em hospitais atribuídos a grupos hacktivistas e o clima geopolítico estão atrapalhando o atendimento aos pacientes. Tudo isso está levando a violações de dados de PHI, impactos negativos no atendimento ao cliente e, em alguns casos, problemas de segurança do paciente.

Ataques contra prestadoras de serviços de saúde

A pesquisa da Akamai constatou que, durante o período de 18 meses de janeiro de 2023 a junho de 2024, os ataques a aplicativos da Web e APIs contra prestadoras continuaram em um ritmo constante (Figura 4). É provável que essa tendência continue a crescer, com flutuações, à medida que os cibercriminosos aproveitam as vulnerabilidades novas e comprovadas inerentes aos modelos de atendimento em evolução, aos métodos de fornecimento e a sistemas de inovação para atacar e violar aplicativos da Web e APIs.

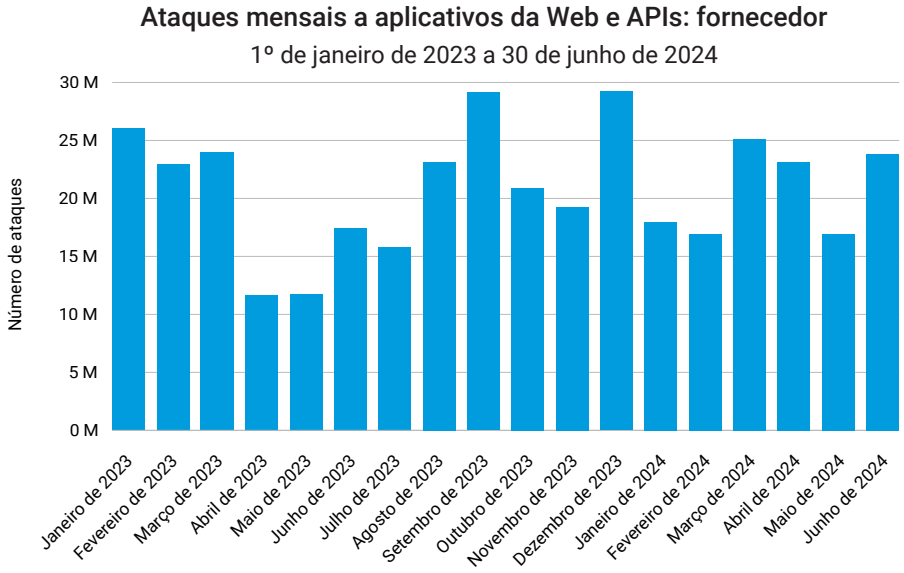
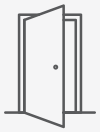


Fig. 4: Os ataques mensais a aplicativos da Web e APIs contra prestadoras de serviços de saúde em todo o mundo atingiram uma média de 21 milhões (NOTA: um cliente distorceu os dados e foi removido em benefício do relatório)



As vulnerabilidades não corrigidas e a dívida técnica da tecnologia legada são um desafio caro que os grupos de ransomware usam em seu benefício.

A coordenação do atendimento possibilitada pelo compartilhamento de dados e pela interoperabilidade por meio do uso de aplicativos da Web e APIs permite melhores resultados clínicos e financeiros. No entanto, isso coloca o setor de saúde em risco significativo, pois as implicações de segurança das APIs ainda não são totalmente compreendidas.

Equilíbrio entre a coordenação ideal dos cuidados e o risco de vulnerabilidades

Devido ao grande número de prontuários médicos e pontos de conectividade do sistema, as prestadoras de serviços de saúde precisam otimizar a coordenação do atendimento e, ao mesmo tempo, implementar controles para fornecer visibilidade e reduzir proativamente o risco de vulnerabilidades. Esse equilíbrio costuma ser desafiador ao implantar novas tecnologias e infraestrutura, como APIs.

Os pesquisadores da Akamai também analisaram os ataques de DDoS da camada 7 contra prestadoras de serviços de saúde durante o mesmo período de 18 meses e encontraram um quadro constante de interrupção após janeiro de 2023 (Figura 5). Podemos atribuir isso, em parte, a uma campanha global de DDoS do grupo hacktivista pró-russo Killnet contra a saúde, com foco em prestadoras de serviços nos Estados Unidos. Ao longo do período, os cibercriminosos continuaram a aproveitar os ataques de DDoS que visavam as funcionalidades de aplicativos ou os próprios aplicativos e introduziram risco ao atendimento ao paciente.

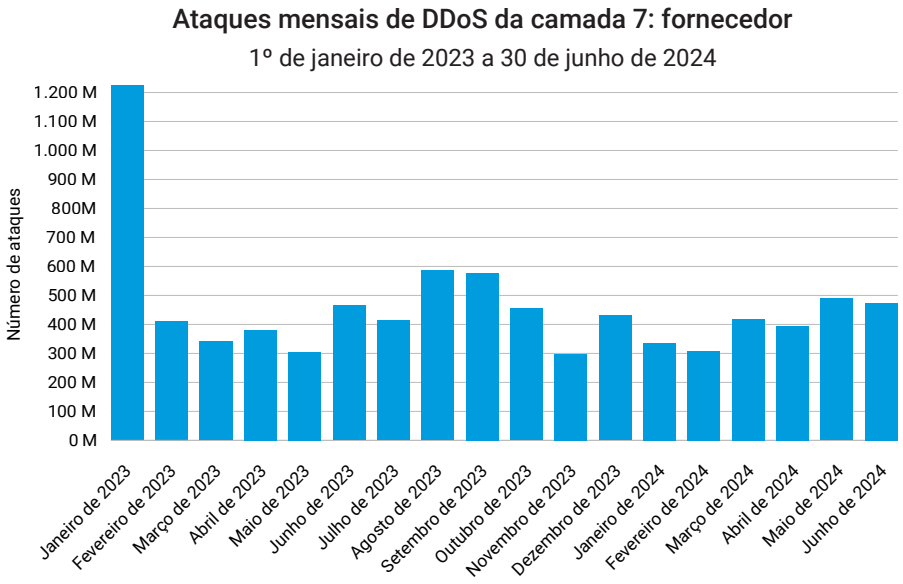


Fig. 5: Com exceção de um aumento isolado em janeiro, os ataques mensais de DDoS da camada 7 contra prestadoras de serviços de saúde globalmente tiveram uma média de 415 milhões

Ataques de DDoS ao setor de saúde estão estabelecendo novos recordes de escala e velocidade

Um aumento na atividade de DDoS, atribuído a desenvolvimentos geopolíticos e grupos hacktivistas causou interrupções que podem ameaçar os resultados dos pacientes. Todo o ecossistema de saúde foi afetado: as prestadoras de serviços foram os alvos mais frequentes nos ataques de DDoS em grande escala do Killnet em 2023. O HC3 alertou que as interrupções de serviços de saúde, mesmo que por apenas algumas horas, podem afetar o espectro das operações diárias, desde as rotineiras até as críticas, com consequências potencialmente significativas.

Com mais interações na área de saúde acontecendo por meio de aplicativos, é cada vez mais importante para a experiência do paciente obter informações e cuidados oportunos. Assim, é igualmente importante se certificar de que você tem proteções e processos em vigor.

Ataques em várias frentes impedem a coordenação dos cuidados

Além de DDoS, as prestadoras de serviços enfrentam outros tipos de ataque populares. Ataques de ransomware que limitam o acesso a prontuários médicos e forçam as ambulâncias a desviarem destacam o fato de que, sem acesso ao histórico médico, é impossível que as prestadoras de serviços de saúde se coordenem. O retorno aos prontuários em papel atrapalha o rastreamento das operações de atendimento ao paciente, a comunicação entre os principais departamentos e todos os serviços de pedidos.

Quando dados confidenciais são afetados, as prestadoras também precisam lidar com o impacto de uma violação de dados. A exploração de vulnerabilidades em ferramentas de software populares permite que agentes de ameaças não autorizados obtenham acesso a um arsenal de dados, desde informações de saúde protegidas até seguro de saúde e informações médicas.

A proteção do paciente deve incluir proteção de dados

A capacidade de proteger e controlar o acesso aos dados do paciente faz parte do atendimento como um todo. Tradicionalmente, os orçamentos e as equipes de cibersegurança do setor de saúde são escassos, o que contribui para os desafios de proteção de dados. Mas à medida que os ataques cibernéticos contra grupos de prestadoras de saúde continuam a ser notícias, os grupos de prestadoras continuam a melhorar as parcerias de proteção terceirizadas e aumentar a cobertura de seguro cibernético.

O impulso para melhorar a proteção continuará a ser construído à medida que as prestadoras de saúde se beneficiam de atualizações de políticas do governo dos EUA, projetadas para aumentar a resiliência em setores críticos de infraestrutura.

As prestadoras foram os alvos mais frequentes nos ataques de DDoS em grande escala do Killnet em 2023.

Considerações de conformidade

O cenário regulatório exige cada vez mais transparência, o que está impulsionando o uso de APIs. As medidas de conformidade estão impondo requisitos amplos de compartilhamento de dados tanto para prestadoras quanto para operadoras de serviços de saúde. Esse compartilhamento de dados tem como objetivo permitir a polinização cruzada de dados clínicos e financeiros, que historicamente tem sido difícil para cada parte, mas é necessário para a execução efetiva do VBC (cuidado baseado em valor).

O movimento em direção ao VBC (ou seja, prestar cuidados com os custos em mente) é um exemplo primordial da quantidade e variedade de informações que agora precisam ser compartilhadas. Há muito tempo, as operadoras de serviços de saúde têm acesso aos dados financeiros de pacientes e prestadoras. Mas mais pontos de dados de VBC, como adesão a medicamentos e internações hospitalares, exigem uma continuidade que não é apenas mais inovadora, mas mais interoperável, e exigem um meio para compartilhar esses dados. As APIs são os canais.

A recente Regra Final de Interoperabilidade do CMS e Acesso ao Paciente exige que as operadoras de serviços de saúde mantenham três categorias principais de APIs para manter as informações fluindo entre operadoras, prestadoras e pacientes:

1. API de acesso de pacientes: aumentará o acesso de membros a seus próprios dados médicos e, provavelmente, aumentará sua satisfação.

2. API de diretório de prestadoras: permite que os membros pesquisem prestadoras e instituições de saúde com base em sua localização e especialidade médica, melhorando o acesso ao atendimento.

3. APIs de pagador-provedor e pagador-pagador: podem ajudar a resolver e reduzir as lacunas no atendimento aos pacientes e, possivelmente, evitar serviços duplicados e dispendiosos.

E, em breve, a Regra Final de Interoperabilidade do CMS e de Autorização Prévia exigirá que as operadoras de serviços de saúde afetadas adotem uma API de autorização prévia adicional.

As medidas de conformidade também estão ditando o formato das APIs por meio do padrão FHIR (Fast Healthcare Interoperability Resources). Esses requisitos e padrões vão simplificar e otimizar a interoperabilidade entre os sistemas enquanto impulsionam a segurança. A expectativa do FHIR é que um programa de segurança exista e inclua recursos básicos, como firewall de aplicativos da Web, autenticação, criptografia, privacidade e microssegmentação.

Embora as prestadoras sejam obrigadas a compartilhar mais dados do que nunca, e em um formato padrão que permita que elas se conectem a aplicativos de saúde do paciente (da escolha dos pacientes) em tempo hábil, a intenção do padrão FHIR é reduzir a carga administrativa e aumentar a transparência. Portanto, os pacientes podem esperar um melhor nível de serviço.

Além disso, os atrasos na troca de dados podem resultar em impactos médicos adversos (geralmente caros), incluindo ser submetidos a penalidades de bloqueio de informações. Portanto, as prestadoras que recentemente se tornaram modernizadas na nuvem estão agora rapidamente implantando APIs externas no novo formato para aderir a essas novas medidas de conformidade.

Além do risco de ataques focados em APIs, ataques de disponibilidade como DDoS e ransomware continuam a ter grandes impactos em todos os setores, e o setor de saúde é um dos que podem ser fortemente afetados. As regulamentações que visam abordar esses tipos de ataques tendem a se concentrar na resiliência. Por exemplo, nos Estados Unidos, o HHS lançou um Guia de DDoS do setor de saúde. Além disso, o Centro de Compartilhamento e Análise de Informações em Saúde (Health-ISAC) sem fins lucrativos publicou um artigo sobre a questão da resiliência no setor de saúde intitulado Resiliência está em nosso DNA.

Adoção de medidas: recomendações de mitigação

A segurança de APIs é mais importante do que nunca de uma perspectiva de gerenciamento de riscos e conformidade. No entanto, devido à proliferação de APIs, tornou-se cada vez mais desafiador identificar, catalogar e proteger as APIs do setor de saúde. Além disso, as organizações de saúde devem se defender contra ataques de DDoS que ameaçam a disponibilidade dos serviços.

Você não pode se defender contra ataques dos quais você não está ciente. Portanto, primeiro, você precisa descobrir todos os ativos para que possa incluí-los em seu programa de segurança. Então, você precisa saber quais vulnerabilidades existem e ter consciência situacional a respeito do que está acontecendo em relação ao desempenho e à segurança. Por fim, você precisa validar a segurança de seus sistemas por meio de testes automatizados e testes de penetração clássicos.

Cumprir os seguintes marcos da estratégia de proteção de APIs e contra DDoS pode ajudar você a alcançar um forte programa de segurança.

Cinco marcos da estratégia de proteção de APIs

Adotar um programa de segurança de APIs forte ajuda você a melhorar a visibilidade de todas as suas APIs e a entender sua exposição ao risco, para que você possa aumentar a proteção.

1. Elimine os pontos cegos da infraestrutura descobrindo sistematicamente APIs não autorizadas ou de sombra e garanta que cada uma delas seja desativada ou incorporada aos controles de segurança de APIs.
2. Determine e fortaleça a postura de risco analisando tipos de alertas comuns e corrigindo falhas no código da API, resolvendo problemas de configuração incorreta e implementando processos para evitar futuras vulnerabilidades com base nas lições aprendidas.
3. Aprimore a detecção de ameaças e respostas compreendendo o comportamento normal e identificando possíveis violações com base em picos de alertas de segurança de APIs. Em seguida, aplique procedimentos de resposta bem definidos para reduzir o risco e o volume de alertas a níveis normais.
4. Faça parceria com fornecedores que fornecem treinamento e experiência. Eles devem oferecer uma gama de serviços, desde suporte baseado em projetos até serviços totalmente gerenciados que podem ajudar a configurar e gerenciar corretamente soluções de cibersegurança complexas e integradas.

Adotar um programa de segurança de APIs forte ajuda você a melhorar a visibilidade de todas as suas APIs e a entender sua exposição ao risco, para que você possa aumentar a proteção.

5. Desenvolva uma ofensiva mais forte ao estabelecer uma disciplina formal de caça a ameaças a APIs com o objetivo de identificar possíveis ameaças antes que elas cheguem a um cenário reativo.

Quatro marcos da estratégia de proteção contra DDoS

Com novos registros sendo definidos para ataques de DDoS contra páginas da Web e APIs da camada 7, infraestrutura das camadas 3 e 4 e sistemas DNS, é fundamental garantir a disponibilidade de seus serviços e recursos. Hoje, isso significa ter proteções ativas em vigor que possam atender ao tamanho, escopo e velocidade dos ataques mais recentes.

1. Tenha um sistema em vigor que forneça visibilidade e resposta rápida aos ataques. Isso deve cobrir as camadas 3, 4 e 7 e a infraestrutura DNS.
2. Faça backup de sua proteção contra DDoS no local com uma plataforma híbrida de mitigação de DDoS que proteja contra ataques que sobrecarregam seus dispositivos no local.
3. Envolva prestadoras ou use sistemas que permitam gerenciar facilmente políticas e manter listas de permissões de IP que fornecem análises práticas em tempo real para ajudar você a adotar uma postura de segurança proativa.
4. Valide seus sistemas de alerta, recursos de proteção e processos de gerenciamento de crises por meio de testes e garanta que toda sua infraestrutura esteja por trás das proteções apropriadas.

Para obter mais informações, leia nossa pesquisa mais recente ou nosso blog.

Com novos registros sendo definidos para ataques de DDoS contra páginas da Web e APIs da camada 7, infraestrutura das camadas 3 e 4 e sistemas DNS, é fundamental garantir a disponibilidade de seus serviços e recursos.

Metodologia

Ataques de DDoS contra aplicativos da Web e da camada 7

Esses dados descrevem alertas da camada de aplicativo sobre o tráfego observado por meio do nosso WAF (firewall de aplicativos da Web). Os alertas de ataques a aplicativos da Web são acionados quando detectamos uma carga útil mal-intencionada em uma solicitação enviada a websites, aplicativos ou APIs protegidos. Os alertas de DDoS de camada 7 são acionados quando detectamos anomalias volumétricas no número de solicitações enviadas a websites, aplicativos ou APIs protegidos. Esses alertas podem ser acionados por solicitações mal-intencionadas e benignas. Normalmente, as próprias solicitações são benignas, mas o alto volume de solicitações indica más intenções. Os alertas não indicam o êxito de um ataque. Embora esses produtos permitam um alto nível de personalização, coletamos os dados apresentados aqui de uma forma que não considera as configurações personalizadas das propriedades protegidas.

Os dados foram extraídos de uma ferramenta interna para análise de eventos de segurança detectados na Akamai Connected Cloud, uma rede de aproximadamente 340 mil servidores em mais de 4 mil locais em quase 1.300 redes em mais de 130 países. Nossas equipes de segurança usam esses dados, medidos em petabytes por mês, para pesquisar ataques, sinalizar comportamentos mal-intencionados e apresentar inteligência adicional às soluções da Akamai.

Esses dados cobriram um período de 18 meses de 1º de janeiro de 2023 a 30 de junho de 2024.

Atualização de dados de 2024

Temos o prazer de anunciar algumas atualizações nos nossos conjuntos de dados para o nosso 10º aniversário. Nossos conjuntos de dados de aplicativo da Web e de ataque de bot receberam algumas atualizações. O método de coleta para cada um foi transformado, simplificado e otimizado. O alcance e a profundidade de nossos insights foram ampliados. Foram adicionadas classificações para vetores de ataque adicionais, como SSRF. A identificação de ataques direcionados a pontos de extremidade de APIs também foi adicionada a cada conjunto de dados. Nós apreciamos destacar algumas dessas novas melhorias neste relatório, e estamos ansiosos para continuar a compartilhar essas atualizações ao longo do ano e além, enquanto celebramos este marco do SOTI/Security com nossos leitores.

Créditos

Diretor de pesquisa
Mitch Mayne

Editorial e redação
Neil Jennings
Chris Notaro
Charlotte Pelliccia
Badette Tribbey
Maria Vlasak
Steve Winterfeld

Análise e contribuição do assunto
Claire Broome
Shane Keats

Análise de dados
Chelsea Tuttle

Materiais promocionais
Barney Beal

Marketing e publicação
Georgina Morales Hampe
Emily Spinks

Mais informações sobre o State of the Internet/Security

Leia as edições anteriores e fique por dentro das próximas versões dos aclamados relatórios State of the Internet/Security da Akamai. **akamai.com/soti/**

Mais informações sobre a pesquisa de ameaças da Akamai

Mantenha-se em dia com as mais recentes análises de inteligência de ameaças, relatórios de segurança e pesquisas sobre cibersegurança. **akamai.com/security-research**

Acesse os dados deste relatório

Visualize versões em alta qualidade das tabelas e dos gráficos mencionados neste relatório. Essas imagens podem ser usadas e consultadas livremente, desde que a Akamai seja devidamente creditada como a fonte e que o logotipo da Akamai seja mantido. **akamai.com/sotidata**

Saiba mais sobre as soluções da Akamai

Para obter mais informações sobre as soluções da Akamai contra ameaças direcionadas ao setor de saúde, visite nossa **página de serviços de saúde e ciências biológicas**.

As soluções de segurança da Akamai protegem os aplicativos que impulsionam seus negócios em cada ponto de interação, sem comprometer o desempenho ou a experiência do cliente. Ao aproveitar a escala de nossa plataforma global e sua visibilidade de ameaças, trabalhamos com você para evitar, detectar e mitigar ameaças, permitindo que você construa a confiança na sua marca e opere de acordo com a sua visão. Saiba mais sobre as soluções de computação em nuvem, segurança e entrega de conteúdo da Akamai em akamai.com e akamai.com/blog, ou siga a Akamai Technologies no X, antigo Twitter, e LinkedIn. Publicado em 10/24.