Akamai

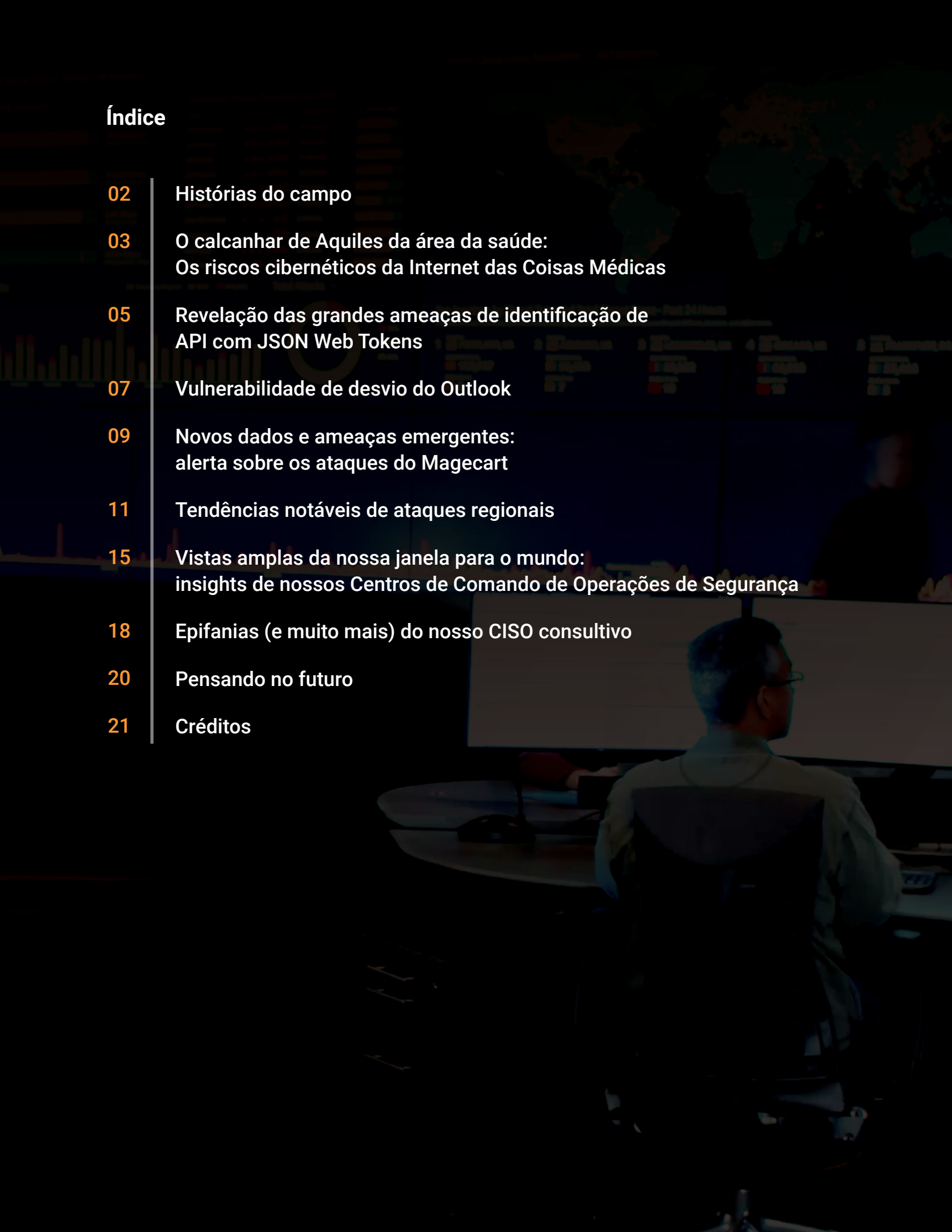
State of the Internet

Volume 9 | Edição 6

Um ano em análise

As tendências cibernéticas de 2023 e o que está por vir

Índice



Histórias do campo

Para este relatório SOTI (State of the Internet), deixamos de lado a típica análise de fim de ano, na qual discutimos cada um dos relatórios anteriores que publicamos este ano, e nos concentramos neste tema central: qual é sua história de segurança favorita do ano? Pedimos aos redatores e a um cientista de dados do Security Intelligence Group (SIG) da Akamai para fazer uma avaliação de final de ano de qualquer história que tenhamos coberto nos últimos 10 meses. Deve ter sido um desafio para eles escolher apenas uma das muitas histórias marcantes e novas descobertas que divulgamos no nosso blog de pesquisa de segurança e nos relatórios SOTI em 2023. Também pedimos ao nosso CISO consultivo e a um vice-presidente dos nossos SOCCs (Centros de comando de operações de segurança) que avaliassem as tendências de ataque deste ano e os principais aprendizados que podemos levar para 2024.

Aconteceu muita coisa este ano no mundo da segurança e na pesquisas da Akamai sobre segurança. As contribuições de pesquisa dos nossos especialistas em segurança são evidentemente inestimáveis para a comunidade. Por meio de nosso hub dedicado, os profissionais de segurança podem acessar recursos confiáveis que contêm insights, estratégias de mitigação e tendências de ataque que podem ajudá-los na defesa de suas organizações. Eles também podem acessar ferramentas gratuitas, como nosso conjunto de ferramentas RPC, bem como nossa plataforma gratuita e de código aberto de emulação de adversários, o Infection Monkey. Agindo exatamente como um malware, o Infection Monkey propaga e "criptografa" os arquivos que pode acessar ao inverter os bits, dando ao profissional uma visão realista de como um invasor poderia (ou não) se movimentar nesse ambiente. A velocidade na qual as ameaças estão evoluindo torna necessária a realização de testes contínuos. Os profissionais precisam conhecer a situação atual de sua rede, e não apenas como ela estava durante o último teste.

Se uma palavra pudesse traduzir o cenário de 2023, essa palavra seria *dinâmico*. Os invasores mudaram suas táticas para burlar as medidas de segurança, procurando novas superfícies de ataque e alvos inexplorados para causar estragos em organizações de todos os tamanhos e setores. O mesmo pode ser dito dos defensores da segurança que continuam a recalibrar e a aprender novas formas de mitigar ataques e proteger melhor as organizações. Nós alternamos soluções, pesquisas e ferramentas com este objetivo: fornecer insights acionáveis e estratégias de mitigação para profissionais de segurança que combatem as mesmas ameaças de segurança que nós.

Boa leitura!

O calcanhar de Aquiles da área da saúde: Os riscos cibernéticos da Internet das Coisas Médicas

Meu nome é Badette Tribbey, uma das contadoras de histórias por trás dos relatórios SOTI, e colaboro com especialistas em segurança e cientistas de dados para transformar as descobertas técnicas e os dados em insights significativos. Odeio matemática, mas adoro como os números podem revelar tendências de ataque convincentes.

Um dos tópicos mais importantes que cobrimos é algo familiar para nós: os riscos elevados da Internet das Coisas Médicas (IoMT). Nos relatórios Invasão pelas brechas na segurança e Ramsomware à espreita, examinamos o cenário de riscos da área da saúde e das ciências biológicas e o que torna esse setor suscetível a ataques. Uma das coisas que mais me impressionou foi como os ativos da IoMT, como aparelhos de ressonância magnética, bombas de insulina e dispositivos vestíveis, embora altamente benéficos para os pacientes, aumentaram significativamente os riscos dos provedores de serviços de saúde. Essas organizações já enfrentavam desafios para proteger seu perímetro devido à complexidade em todo o ecossistema de saúde, à tecnologia legada vulnerável e aos problemas de equipe de TI e cibersegurança. Além disso, a aplicação de patches em tempo hábil nesse ambiente pode ser uma tarefa hercúlea, com atualizações provenientes de vários fornecedores para vários sistemas ou aplicativos, o que dificulta o rastreamento.

Os dispositivos de IoMT sem patches são alguns dos ativos mais vulneráveis entre todos os setores e podem introduzir ameaças mais nefastas, como ransomware. À medida que a IoMT cresce exponencialmente (e com ela, a utilização de APIs), suas vulnerabilidades também crescem e podem se tornar caminhos para os invasores ganharem uma porta de entrada para seus alvos ou resultar em abusos e vazamento de dados (Figura 1). Um relatório conjunto da Cynerio e do Ponemon Institute sobre um estudo realizado com vários hospitais e sistemas de saúde nos Estados Unidos indicou que mais da metade sofreu ataques cibernéticos como resultado de falhas de segurança em dispositivos IoMT.

> “A aplicação oportuna de patches no ambiente (da área de saúde) pode ser uma tarefa hercúlea, com atualizações provenientes de vários fornecedores para vários sistemas ou aplicações, o que dificulta o rastreamento.
>
> **– Badette Tribbey, redatora técnica sênior, Akamai**

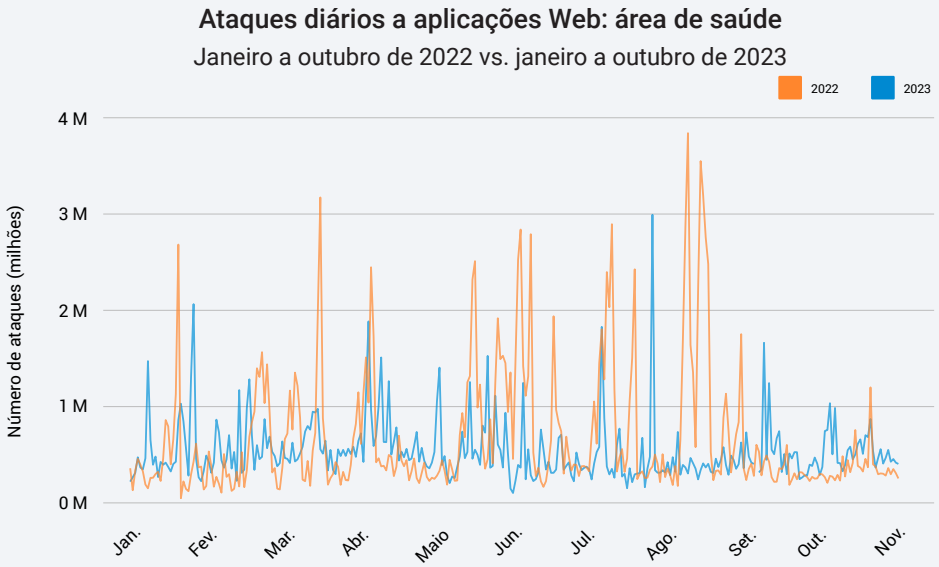


Fig. 1: Os ataques a aplicações Web e API na indústria farmacêutica/da saúde mostram uma atividade constante, com picos esporádicos entre 2022 e 2023. Embora os ataques tenham diminuído 21% em relação ao ano anterior, o número médio de ataques por dia em 2023 é maior do que em 2022.

O que vem a seguir para a área da saúde?

À medida que a área da saúde expande sua IoMT, as APIs continuarão a desempenhar um papel crítico na acessibilidade dos serviços médicos (por exemplo, telessaúde e monitorização remota de pacientes), levando a melhores resultados clínicos e financeiros. E os ataques contra a área da saúde provavelmente não diminuirão, devido ao alto valor dos registros de saúde e dos dados dos pacientes na Dark Web.

Conforme mudamos nossa visão do que está acontecendo para o que devemos esperar, fica claro que os invasores continuarão inovando e aumentando o escopo e a complexidade de seus ataques. É provável que tenhamos um impulso contínuo em direção a ataques mais técnicos que aproveitam as vulnerabilidades de dia zero. Além disso, o cenário regulatório, incluindo, entre outros, a Lei [PATCH] (Lei da Proteção e Transformação da Saúde Cibernética de 2022) está mudando, portanto, precisamos garantir que nossas soluções possam ajudar a cumprir um grande volume de leis iminentes de privacidade, relatórios, pagamentos, soberania de dados e resiliência. Por fim, esperamos ver mais interrupções nos ataques para os CISOs que mudarem os orçamentos para consolidar menos fornecedores e usar soluções que minimizem o tempo de permanência dos hackers que conseguiram entrar.

Revelação das grandes ameaças de identificação de API com JSON Web Tokens

Meu nome é Lance Rhodes e adoro atuar como redator de cibersegurança na equipe do SIG da Akamai desde março de 2023! Grande parte do meu trabalho serve como "tecido conjuntivo" entre nossos relatórios e blogs, já que tenho trabalhado nos aspectos de publicação e redação das postagens do blog e na pesquisa seccional e na redação de conteúdo e materiais de marketing para os relatórios SOTI. E tudo isso está vinculado à minha colaboração com a equipe em nossos boletins informativos internos e externos mensais e em envios para conferências sobre segurança.

Devo dizer que uma das postagens mais interessantes em que trabalhei este ano foi a postagem sobre JWT (JSON Web Token). Essa postagem tinha uma conexão direta com o relatório SOTI de apps e APIs (Invasão pelas brechas na segurança), na medida em que expandia a autenticação interrompida em JWTs, um dos métodos padrão de identificação para APIs. Então, foi divertido obter uma compreensão mais aprofundada dos JWTs.

Depois de trabalhar no relatório SOTI de apps e APIs no início deste ano, comecei a trabalhar com Nitzan Namer na postagem sobre o JWT, que se concentrou no JWT como um vetor de ataque para autenticação de usuário interrompida, um Top 10 em segurança de API do OWASP (Open Web Application Security Project). O relatório SOTI tinha uma seção específica dedicada a isso, mas a postagem do blog se aprofundou na estrutura do JWT e nas práticas recomendadas para proteção contra as maiores ameaças, incluindo escalonamento de privilégios, vazamento de dados e controle de contas.

Lembro-me de conversar com Nitzan sobre como esperávamos que a postagem fosse usada como um recurso contínuo para pesquisadores de segurança, profissionais técnicos e usuários e administradores de JWT. A postagem atende a essa esperança por meio de seu estilo estrutural: os fundamentos do JWT são listados primeiro, seguidos por seis cenários de caso, que incluem ilustrações e exemplificam algumas ameaças comuns e indicam as práticas recomendadas para cada uma. Os princípios básicos fornecem informações sobre como os JWTs protegem APIs emitindo tokens que contêm informações a serem compartilhadas como objetos JSON. Cada token é codificado, embora não seja criptografado, e consiste em um cabeçalho, carga útil e assinatura de verificação (atestando que os dados não foram alterados desde que o servidor criou o token).

> “A postagem do blog analisou mais detalhadamente a estrutura do JWT e as práticas recomendadas para proteção contra as maiores ameaças, incluindo escalonamento de privilégios, vazamento de dados e controle de contas.
>
> **– Lance Rhodes, redator de cibersegurança, Akamai**

Os seis cenários de caso consistem em:

1. Permitir que o servidor use um token sem validação
2. Usar a mesma chave privada para diferentes aplicações
3. Usar um algoritmo de assinatura fraco
4. Usar uma chave privada curta e/ou de baixa entropia
5. Manter dados confidenciais em uma carga útil de JWT
6. Confundir as chaves

Os JWTs são um dos formatos de verificação mais comuns. Medidas de segurança adequadas são cruciais, pois o formato oferece uma grande superfície de ataque com muito espaço para erros. Embora esses cenários apresentem algumas das ameaças mais comuns aos JWTs, ainda existem muitas mais por aí e as técnicas de ataque estão em constante evolução.

Os JWTs não são criptografados nem implementados levando em consideração a segurança

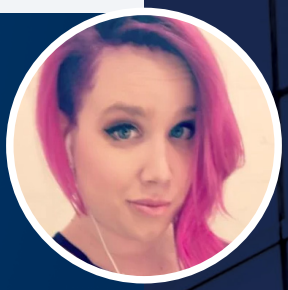
Uma das minhas maiores conclusões da postagem do blog é que os JWTs não são criptografados nem implementados levando em consideração a segurança. É difícil acreditar que um token de autenticação tão popular possa ser tão vulnerável. Parte do apelo dos JWTs é que eles permitem o uso de muitas aplicações da web e APIs sem a necessidade de fazer login com frequência. Tanto o relatório SOTI quanto a postagem do blog de JWT analisaram os algoritmos de JWT no tráfego da Akamai e determinaram que os algoritmos simétricos são os mais comuns, mesmo que sejam teoricamente menos seguros que os algoritmos assimétricos. Por exemplo, ambas as publicações mostram que 54,8% dos clientes da Akamai usam o algoritmo HS256, que é simétrico.

É provável que os algoritmos simétricos sejam escolhidos com mais frequência porque o usuário precisa apenas de uma chave, e algoritmos assimétricos requerem uma quantidade maior de recursos computacionais. O JSON Web Encryption, a versão criptografada do JWT, também não costuma ser usado. A maioria das empresas opta pelo JWT para economizar energia de computação.

A conclusão: a conveniência, o custo e a velocidade geralmente são priorizados em relação à segurança. Este é um lembrete valioso da importância do nosso trabalho como pesquisadores e redatores de segurança. Boas práticas de pesquisa e de segurança são necessárias para um equilíbrio satisfatório entre eficiência e segurança.

> É difícil acreditar que um token de autenticação tão popular possa ser tão vulnerável.
>
> **– Lance Rhodes, redator de cibersegurança, Akamai**

Vulnerabilidade de desvio do Outlook



Olá! Espero que você tenha sorrido hoje! Meu nome é Tricia Howard e eu trabalho no blog do SIG. Vivo no mundo minucioso das redações técnicas e trabalho com nossos pesquisadores, nossa equipe de comunicação corporativa e nosso departamento jurídico (entre outros) para divulgar os materiais de maneira oportuna e eficaz. A melhor parte do meu trabalho é poder me gabar dos nossos pesquisadores porque eles fazem coisas muito legais!

De tudo o que me pediram para escrever este ano, este talvez seja a mais difícil. No meio de todas as coisas extremamente bacanas que nossa equipe fez nos últimos 12 meses, como eu poderia escolher uma favorita? Mas, como tenho que escolher apenas uma, escolhi o trabalho de Ben Barnea sobre a infame vulnerabilidade de desvio do Outlook. Ben é um dos pesquisadores mais brilhantes que conheço e conseguiu encontrar uma maneira de quebrar um patch inteiro... com apenas uma barra. Sei que parece absurdo, até mesmo impossível, mas era possível, e ele conseguiu.

A vulnerabilidade original permitia que um invasor não autorizado enviasse um convite do Outlook com um som de notificação personalizado. Esse som agia como um caminho de ataque que permitia uma conexão com o servidor do invasor, fornecendo credenciais NTLM. Isso é um problema e tanto. A partir daí, o invasor pode forçar as credenciais ou executar um ataque de retransmissão. Tudo isso pode, é claro, levar ao escalonamento de privilégios, e todos sabemos o que pode acontecer a partir daí. A pior parte de tudo é que essa vulnerabilidade foi de clique zero, o que significa que nenhuma ação foi exigida do usuário para executar esse ataque. Isso pega algo poderoso e o torna totalmente perigoso, especialmente quando você fica sabendo que ele se originou na Rússia e foi usado de forma selvagem, infiltrando-se em várias agências governamentais europeias.

O patch foi publicado em março. Ele removeu a capacidade de usar o *PidLidReminderFileParameter*, que estava permitindo que o invasor especificasse o caminho personalizado (ou seja, se conectasse ao servidor da pessoa mal-intencionada). Em vez disso, o patch utiliza o recurso *MapURLtoZone*, que verifica se o caminho estava tentando se conectar à Internet. Se houvesse uma tentativa de conexão, o som de notificação tradicional seria reproduzido, eliminando a opção de caminho do arquivo para a notificação personalizada. Teoricamente, isso impediria que um invasor remoto tirasse proveito dessa vulnerabilidade, pois ele teria que acessar a Internet para estabelecer uma conexão entre o invasor e a vítima.

> “Os defensores já têm um prato cheio com que se preocupar todos os dias, sem contar as novas vulnerabilidades de escalonamento de privilégios de clique zero.
>
> **– Tricia Howard, redatora técnica sênior, Akamai**

Frustrar o patch

É aqui que as coisas ficam interessantes e, sendo bem sincera, bastante engraçadas. Como qualquer grande pesquisador, Ben quis verificar se a vulnerabilidade realmente não era mais explorável. Esta é uma forma muito simplista de explicar, mas há essencialmente duas opções para o *MapURLtoZone*: permitir ou negar. Ele acessa a Internet ou não? Na maioria das vezes, o patch agiu como esperado. Mesmo quando o caminho parecia ser local, o *MapURLtoZone* reconheceu que o caminho pretendia chegar à Internet e o impediu de fazê-lo.

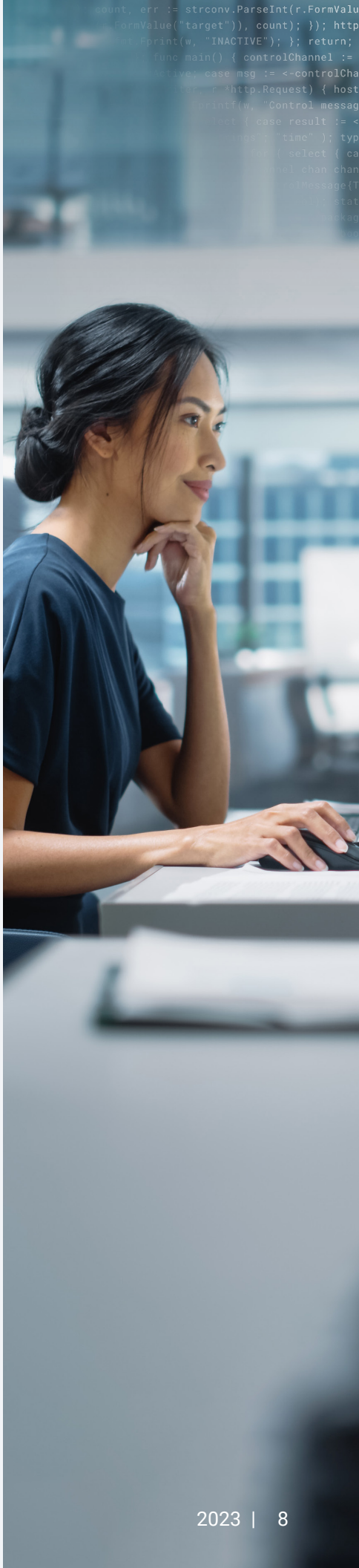
Ben decidiu brincar com o nome do caminho adicionando "/" ao final. Quando se fornece algo que o *MapURLtoZone* não está esperando, ele ainda precisa decidir se deve permitir ou negar. A barra adicional não era reconhecida, que por sua vez retornava um 0, que a função lê como local e confiável. Depois disso, o restante da vulnerabilidade era capaz de funcionar exatamente como esperado, aproveitando o *CreateFile* para o caminho personalizado.

E pronto! Uma mísera barra foi adicionada e um patch completo para uma vulnerabilidade **crítica** de repente deixou de ser uma solução eficaz. Esse patch provavelmente foi criado após dias, possivelmente semanas ou meses, de tempo e energia dos profissionais de cibersegurança para eliminar essa ameaça... e tudo desabou por causa de uma única barra.

A sofisticação absoluta do ataque original é bastante surpreendente quando ela é analisada. O invasor está jogando a longo prazo ao estilo Magnus Carlsen. Considerando que foi necessária apenas uma barra para inutilizar o patch, é lógico que os invasores teriam, mais cedo ou mais tarde, descoberto um desvio por conta própria. É muito bom que tenha sido o Ben quem o descobriu, que foi bem criativo.

É por isso que os pesquisadores que descobrem esses bugs são realmente a força vital da comunidade de segurança. Os defensores já têm um prato cheio com que se preocupar todos os dias, sem contar as novas vulnerabilidades de escalonamento de privilégios de clique zero. Os pesquisadores de segurança estão fazendo uma diferença real no mundo, especialmente à medida que nos tornamos cada vez mais dependentes da tecnologia e da Internet para a nossa vida quotidiana.

Tenho muito orgulho de fazer parte desta equipe incrível e de trabalhar com algumas das mentes mais brilhantes deste planeta. Para qualquer pessoa que tenha lido nossos blogs, nossos tweets, nossos SOTIs: obrigada. E para os pesquisadores, dentro e fora do SIG da Akamai: obrigada por tudo o que fazem, desvendam e encontram. Vamos ver o que o próximo ano nos reserva, certo?



Novos dados e ameaças emergentes: alerta sobre os ataques do Magecart

Meu nome é Chelsea Tuttle e estou na Akamai há quase oito anos. Como cientista de dados responsável pelos dados representados no SOTI nos últimos quatro anos, passo a maior parte do meu tempo limpando, explorando, analisando e visualizando nossos dados. Quando não estou olhando para os dados, estou trabalhando de perto com os redatores da SOTI para ajudá-los a comunicar as histórias que nossos dados nos dizem. Devido às complexidades do big data e aos benefícios de gerar relatórios sobre dados históricos, não é comum adicionarmos um novo conjunto de dados, mas este ano sim! Quando olho para 2023, penso nas histórias que publicamos com base neste novo conjunto de dados como algumas das minhas favoritas porque adorei as oportunidades de aprendizagem que acompanharam este empreendimento.

Muitas vezes, no nosso mundo, nos concentramos em relatar o número de tentativas de ataque que vemos na nossa rede e perdemos oportunidades importantes de reportar dados relevantes para proteger potenciais vulnerabilidades e prevenir ataques. Um conjunto de dados que adicionamos aos nossos relatórios SOTI este ano se destaca porque é o único que realça uma área potencial de vulnerabilidade, em vez de focar no volume de ataques. Esse conjunto de dados é derivado de observações fornecidas pelo Akamai Client-Side Protection & Compliance a partir de sua visão detalhada de bilhões de scripts de páginas da Web diariamente. Uma das áreas de vulnerabilidade potencial que observamos é o número de scripts próprios e de terceiros utilizados nos websites. Embora o uso de um script próprio não garanta segurança e o uso de um script de terceiros não garanta uma vulnerabilidade, quanto maior a confiança depositada em outra pessoa, como confiar em um terceiro para hospedar um script de página da Web, mais risco será adicionado a um perfil de segurança. A Akamai está trabalhando para preencher a lacuna entre conveniência e segurança criada pelo uso crescente de scripts de terceiros em todos os setores.

> A Akamai está trabalhando para preencher a lacuna entre conveniência e segurança criada pelo uso crescente de scripts de terceiros em todos os setores.
>
> **– Chelsea Tuttle, cientista de dados sênior, Akamai**

Como mostramos em nosso relatório SOTI Entrando pela loja de presentes: ataques no comércio de junho de 2023, uma área de foco da pesquisa da Akamai este ano foram os recentes ataques de skimming na Web no estilo Magecart. Em particular, observando como os ataques do Magecart continuam a invadir o setor de comércio digital. Esse tipo de ataque tenta roubar credenciais confidenciais de usuários, como informações de cartão de crédito, do carrinho de compras de um website de comércio digital usando injeção maliciosa de código JavaScript. Esse tipo de ataque tende a ser fácil para os adversários, mas representa grandes riscos para os consumidores, ao mesmo tempo que se torna cada vez mais difícil de detectar.

Esses ataques de Magecart, ou Web skimming, geralmente ocorrem sem que o usuário ou proprietário do website perceba, e os invasores geralmente escolhem websites de comércio digital que usam software vulnerável ou desatualizado.

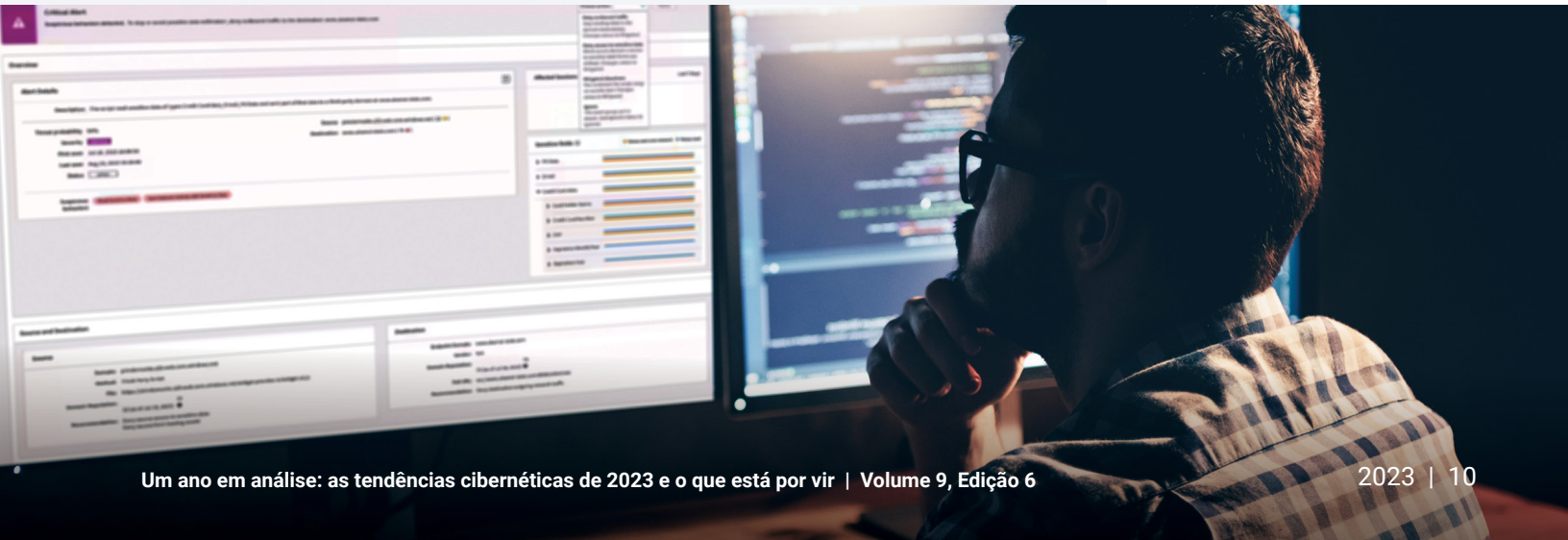
Variantes de Magecart recentes

Diversas variantes do Magecart podem ser vistas nas campanhas mais recentes do Magecart que os pesquisadores da Akamai exploraram. Nosso relatório SOTI de junho de 2023 se concentrou nos ataques Magecart do lado do cliente e observou vulnerabilidades exploradas encontradas em scripts de terceiros de bibliotecas de código aberto que poderiam levar a ataques à cadeia de suprimentos. Logo após a redação do relatório SOTI, publicamos uma postagem no blog sobre como os pesquisadores da Akamai descobriram uma nova campanha no estilo Magecart que usava websites legítimos para atacar outros. Nessa campanha, existiam essencialmente dois conjuntos de websites de vítimas: os websites legítimos sequestrados para hospedagem, que atuam como servidores controlados pelo invasor, e os websites de comércio vulneráveisatacados com Web skimming do lado do cliente. Uma segunda postagem no blog foi publicada em agosto, descrevendo como os pesquisadores da Akamai descobriram uma outra nova campanha Magento com uma injeção oculta de modelo no servidor que explorava websites de comércio digital para coletar estatísticas de pagamento das vítimas.

Os pesquisadores da Akamai descobriram uma nova campanha no estilo Magecart que estava explorando websites legítimos para atacar outros

A última postagem de Magecart do blog do SIG da Akamai revela uma nova técnica de ofuscação na qual os invasores manipulam a página de erro 404 padrão do website para ocultar código malicioso. Os pesquisadores da Akamai descobriram que essa nova campanha consiste em duas técnicas avançadas de ocultação adicionais e apresentam as táticas em desenvolvimento que os invasores estão usando para prolongar a cadeia de ataque e evitar a detecção.

Conforme nos aproximamos do fim de 2023 e eu relembro todas as oportunidades de investigação e elaboração de relatórios que tivemos graças aos novos dados e às ameaças emergentes, penso também nos novos dados e oportunidades de aprendizagem que temos pela frente em 2024.



Tendências notáveis de ataques regionais

Meu nome é Charlotte Pelliccia e entrei para a equipe SOTI em 2023 para chamar a atenção para histórias das regiões Ásia-Pacífico e Japão (APJ) e das regiões Europa, Oriente Médio e África (EMEA). Nossos retratos da APJ e EMEA são peças complementares aos nossos relatórios SOTI globais. Aqui, revisitarei algumas das tendências de ataque mais significativas que abordamos em 2023, atualizando dados de retratos publicados no início do ano.

Ataques a aplicações da Web e API: uma história de dois setores verticais

Consistente com nossos mais recentes relatórios SOTI de serviços financeiros e comércio, os serviços financeiros permaneceram como o principal setor vertical para ataques a aplicações Web e API na região APJ, seguidos pelo comércio. Desde o nosso relatório de junho de 2023, os ataques a serviços financeiros ultrapassaram 4,5 bilhões (de 3,7 bilhões, um aumento de 22%). E desde o nosso relatório de março de 2023, os ataques ao comércio aumentaram de 1,2 bilhão para 1,9 bilhão, um aumento de 58%. As divisões entre subverticais permanecem relativamente consistentes (Figura 2).

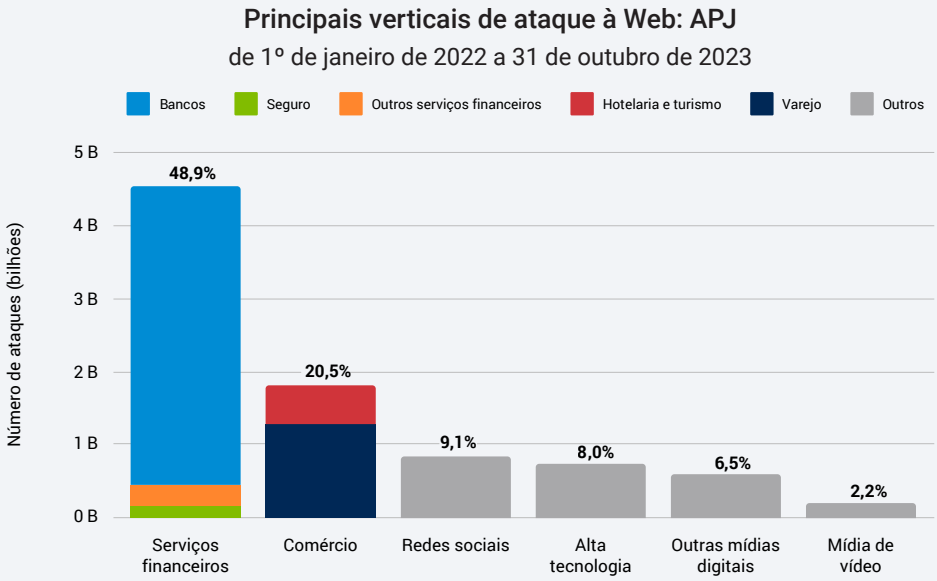


Fig. 2: Mercados verticais de ataques na Web na APJ em outubro de 2023

> A visibilidade das tendências de ataques regionais é vital para ajudar as organizações a entender melhor seus riscos e ajustar suas ferramentas e práticas recomendadas.
>
> **– Charlotte Pelliccia, redatora de cibersegurança, Akamai**

Enquanto isso, na EMEA, o comércio continua sendo o principal setor vertical para ataques a aplicações da Web e API, com ataques que agora ultrapassam os 6,5 bilhões (eram 4,6 bilhões, um aumento de 41%) desde a publicação do nosso relatório de março de 2023. Embora o setor de manufatura tenha subido da quarta posição, substituindo os serviços financeiros na terceira posição, os ataques contra serviços financeiros aumentaram 70% desde a publicação do relatório de junho de 2023, chegando a 1,7 bilhão, ante 1 bilhão. Aqui, novamente, as divisões entre subverticais permaneceram relativamente consistentes (Figura 3).

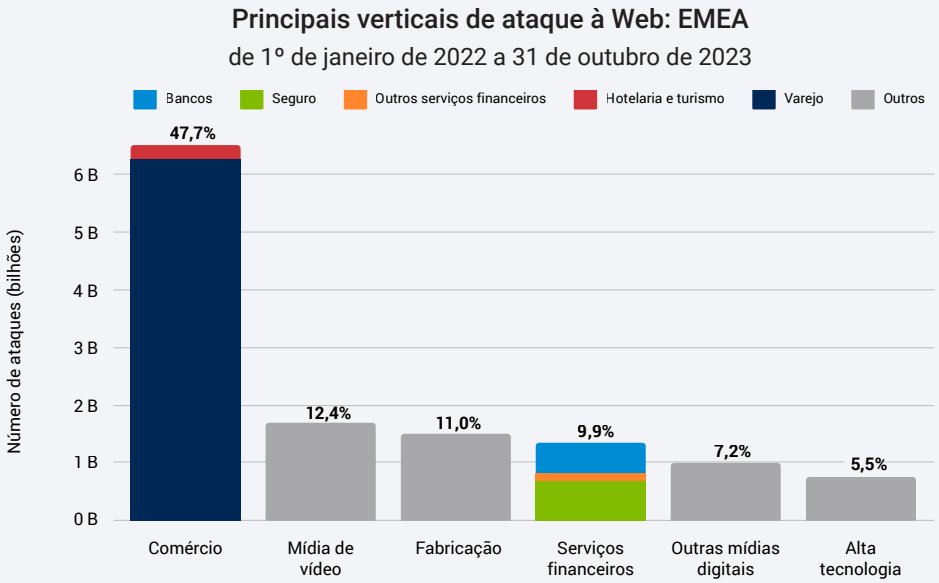
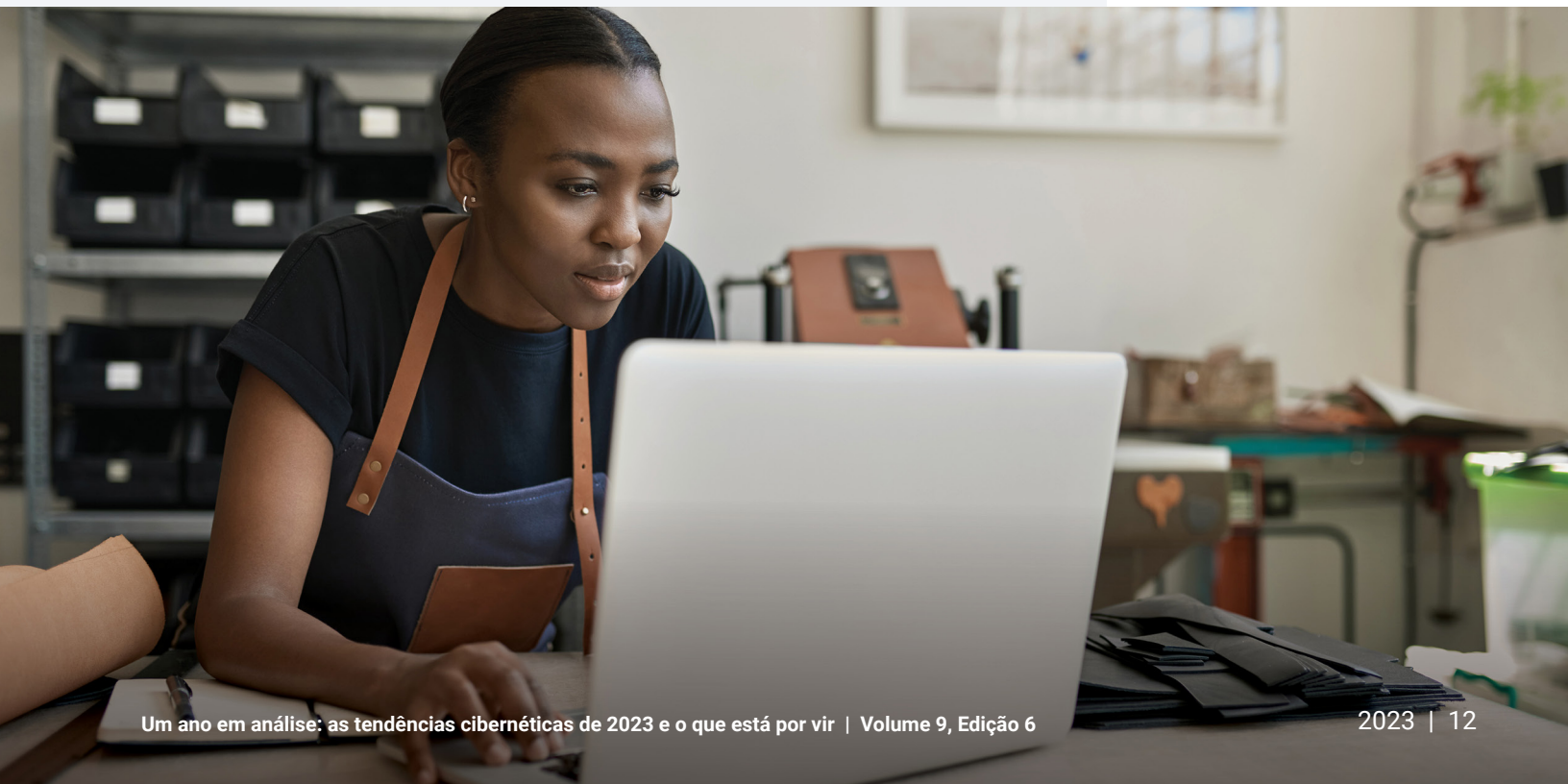


Fig. 3: Mercados verticais de ataques na Web na EMEA em outubro de 2023



Bots mal-intencionados são uma arma de escolha

Continuando o que vimos nos relatórios anteriores, a APJ fica atrás da América do Norte em atividade de bots mal-intencionados. Os três principais setores de ataque de janeiro de 2022 a outubro de 2023 no APJ são comércio (27,4%), mídia de vídeo (15,0%) e serviços financeiros (14,3%). Na EMEA, metade (50,1%) de todas as atividades de bots mal-intencionados visava o comércio, seguido por outras mídias digitais a 15,3% e mídia de vídeo a 12,2% (Figura 4).

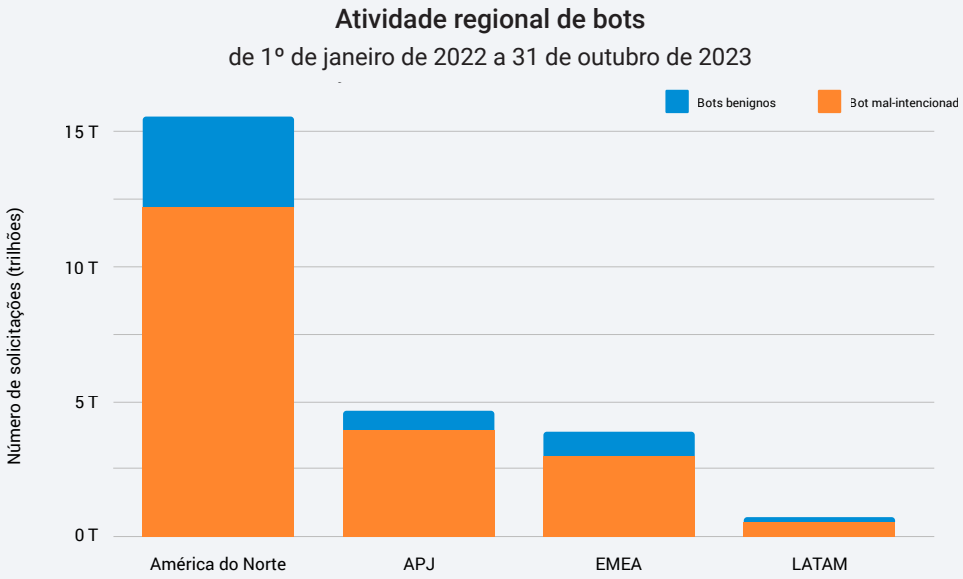


Fig. 4: O uso de bots mal-intencionados prevalece em todas as regiões, excedendo em muito o uso de bots benignos

Consulte o artigo a seguir para obter insights do nosso SOCC sobre como os ataques de bots e DDoS estão mudando.

EMEA sob a mira da mudança regional nos ataques DDoS

Nosso relatório de 2023 deixou bem claro que os agentes de ameaça estão de olho na EMEA, o que se deve, em parte, ao clima geopolítico atual. Um ótimo exemplo: o número de eventos de ataque de negação de serviço distribuída (DDoS) contra os setores de serviços financeiros, jogos de azar e manufatura na EMEA excedeu os números em todas as outras regiões combinadas (Figura 5).

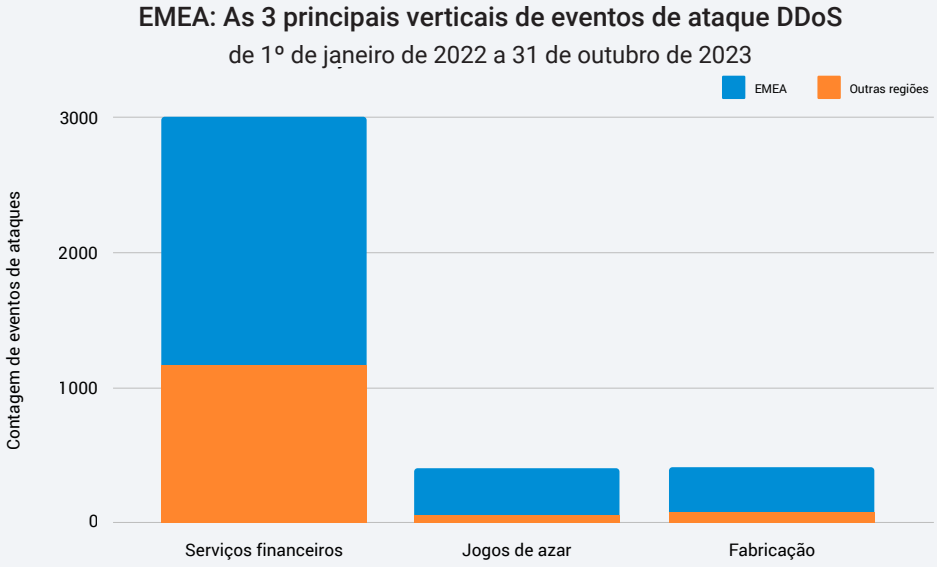


Fig. 5: A EMEA sofreu mais eventos de ataque DDoS nessas verticais do que todas as outras regiões combinadas

Perspectivas futuras

Enquanto os agentes de ameaças obtiverem sucesso com ataques Web, bot e DDoS, é razoável esperar que esses três continuem sendo suas armas de preferência. Na verdade, esses três vetores já estão evoluindo para manter ou ganhar força. As explorações de dia zero de aplicações Web estão sendo interligadas com técnicas de ransomware (por grupos de ransomware como o CL0P) e incluem ataques DDoS para criar uma tática de extorsão tripla. O Web scalping por meio de bots se tornou o novo normal para quase todos os grandes eventos de companhias aéreas ou vendas de passagens. E estão surgindo ataques de API direcionados à lógica de negócios da API.

Em resposta, a supervisão regulamentar e as obrigações de comunicação continuam aumentando em todo o mundo e em todos os setores, uma vez que nenhuma região ou setor está a salvo dos ataques. O objetivo é manter a legislação de cibersegurança atualizada com o cenário de ameaças em evolução. As organizações precisam permanecer vigilantes quanto ao cumprimento dos requisitos de relatórios e preparadas para mitigar riscos através de uma defesa de várias camadas.

Vistas amplas da nossa janela para o mundo: insights de nossos Centros de Comando de Operações de Segurança

Meu nome é Roger Barranco, vice-presidente de operações de segurança global. Estou na Akamai há quase doze anos e sou responsável pelas operações de segurança gerenciadas da empresa, que são atendidas por seis SOCCs posicionados em todo o mundo e facilitadas por uma equipe fantástica. Comecei minha carreira em cibersegurança e fui atraído para a área porque é um mercado interessante e em constante mudança, e 2023 é um ótimo exemplo disso.

O SOCC da Akamai nunca esteve tão ocupado: até o final de 2023, teremos processado aproximadamente 30% mais tíquetes relacionados à segurança do que no ano passado. Aqui estão os principais insights que obtivemos ao trabalhar com nossos clientes de serviços de segurança gerenciados que as organizações devem ter em mente para 2024.

Os ataques DDoS estão mudando

Embora o número de clientes que estão sendo atacados tenha aumentado historicamente ano após ano, o "como" é diferente hoje. Primeiro, o tipo e o volume das propriedades do cliente que estão sendo atacadas mudaram. Por exemplo, em vez de 10 ataques contra pontos de extremidade iguais ou semelhantes, agora estamos vendo 100 ataques, todos direcionados a diferentes IPs no espaço de rede do cliente. E esses ataques não visam apenas a Camada 3, mas também a Camada 7 ao mesmo tempo. Além disso, os ataques contra DNS (Sistema de Nomes de Domínio) aumentaram drasticamente e a maior parte são ataques de consulta válidos que podem facilmente cansar a infraestrutura DNS do cliente. Apenas alguns megabits de tráfego DNS indesejado podem causar uma pressão significativa em uma empresa. Também estamos começando a observar um ressurgimento preocupante da atividade na frente Mirai, que ganhou notoriedade por aproveitar o poder da Internet das Coisas para causar interrupções em larga escala.

No cenário de ameaças de hoje, não basta colocar um equipamento forte na edge para acompanhar o ritmo dos ataques. As organizações precisam de um serviço de segurança robusto no nível da nuvem para assumir essa carga de trabalho, mantendo o estado e ao mesmo tempo implementando proteções exclusivas para cada um desses pontos de extremidade. É aqui que a Akamai se destaca tanto de um ponto de vista de plataforma quanto de serviços. Podemos aplicar várias camadas de segurança para a defesa contra todo o espectro de ataques cibernéticos. E nossos especialistas práticos examinam as nuances e tendências de cada cliente, a fim de monitorar e mitigar de uma forma muito específica que impede os problemas, mas permite a passagem do tráfego esperado e limpo.

> O SOCC da Akamai nunca esteve tão ocupado: até o final de 2023, teremos processado aproximadamente 30% mais tíquetes relacionados à segurança do que no ano passado.
>
> **– Roger Barranco, vice-presidente de operações de segurança global, Akamai**

Combater bots pode ser brutal

O abuso de credenciais é difícil de mitigar porque é complicado distinguir o tráfego indesejado do desejado, e os clientes têm back-ends bastante exclusivos que podem exigir mitigações muito diferentes. Além disso, os invasores que cometem abuso de credenciais são alguns dos mais qualificados e vigilantes porque o abuso de credenciais bem-sucedido é a maneira mais fácil de lucrar. A natureza perigosa e dispendiosa desses ataques de bots torna importante ter uma solução de prevenção contra o abuso de credenciais, especialmente nos setores de serviços financeiros e comércio onde o uso mal-intencionado de bots continua aumentando.

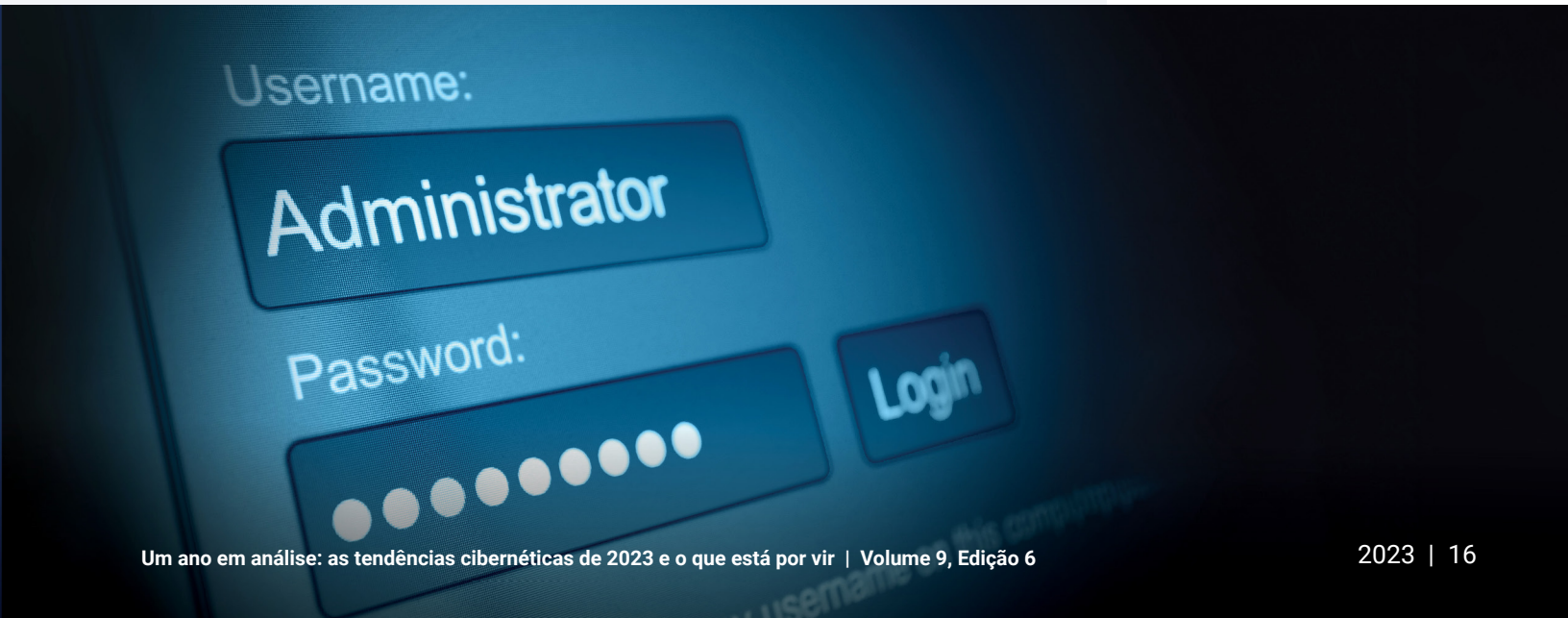
Os websites dos invasores continuam mirando a EMEA

Desde a incursão ucraniana, a EMEA (Europa, em particular) desbancou os Estados Unidos como a principal região de ataques cibernéticos em vários mercados verticais e categorias diferentes de tipos de ataques, principalmente DDoS. Essa mudança destaca o fato de que muitos agressores são Estados-nação ou simpatizantes de Estados-nação e seu foco na Europa não está diminuindo.

A sofisticação dos invasores está aumentando

Já se passaram os dias em que os scripts de garotada representavam a principal ameaça, aproveitando ferramentas genéricas para lançar um ataque na esperança de ter sorte, ou alugando uma botnet DDoS por US$ 10 por hora para derrubar um competidor de videogame. Hoje, os invasores são mais sofisticados e parece que se concentram detalhadamente em alvos específicos, planejam sua estratégia, realizam reconhecimentos às vezes com um ano de antecedência e elaboram ataques para tirar vantagem de possíveis fraquezas percebidas. Como resultado do trabalho de base que os agressores estão implementando, hoje os ataques estão se tornando mais longos do que os ataques dos últimos anos, que costumavam durar apenas alguns minutos.

> Como resultado do trabalho de base que os agressores estão implementando, hoje os ataques estão se tornando mais longos do que os ataques dos últimos anos, que costumavam durar apenas alguns minutos.
>
> **– Roger Barranco, vice-presidente de operações de segurança global, Akamai**



Práticas recomendadas para o alinhamento cibernético e operacional

Apesar desses desafios, os clientes podem aumentar a eficácia de seus esforços para se proteger seguindo duas práticas recomendadas para o alinhamento cibernético e operacional que permitem que a Akamai trabalhe como uma extensão de sua equipe cibernética. Em primeiro lugar, eles precisam estabelecer parcerias com o SOCC durante tempos de paz para construir proativamente sua postura defensiva, em vez de tentar fazer isso durante um ataque. Dessa forma, os ataques podem ser pré-mitigados, sem impacto na produção, e os clientes receberão um relatório de acompanhamento que detalha o ataque evitado.

Em segundo lugar, eles devem trabalhar proativamente na prontidão operacional e nos planos de backup. Por exemplo, eles devem se certificar de que saibam fazer o roteamento em diferentes plataformas durante os testes. Um ataque de cinco minutos pode prejudicar um cliente por uma hora devido a problemas operacionais, portanto, estar preparado operacionalmente é tão importante quanto estar preparado para responder a um problema puramente cibernético.

Este ano ressaltou como a cibersegurança está em constante mudança e esperamos que isso continue. A boa notícia é que, ao aplicar esses insights, os clientes poderão se antecipar e se proteger em 2024.

Epifanias (e muito mais) do nosso CISO Consultivo

Meu nome é Steve Winterfeld e eu sou o CISO Consultivo da Akamai. Atuei como CISO do Nordstrom Bank e como diretor de resposta a incidentes e inteligência de ameaças na Charles Schwab. O meu papel é garantir que os nossos parceiros tenham sucesso na defesa dos seus clientes e determinar onde devemos concentrar as nossas capacidades.

Este ano, observamos algumas tendências que me surpreenderam e algumas que foram confirmadas por dados que podem ser utilizados para atualizar a nossa estratégia. Minhas nove principais histórias deste ano incluíram algumas epifanias, algumas notícias esperadas e algumas coisas que parecem que nunca mudam.

Epifanias

- Um total de 10% a 16% das organizações encontraram tráfego de C2 (comando e controle) em sua rede pelo menos uma vez por trimestre. Além disso, 26% dos dispositivos infectados acessaram domínios relacionados a uma corretora de acesso inicial.
- O cenário de ameaças de ransomware viu uma mudança preocupante nas técnicas de ataque com o abuso desenfreado de vulnerabilidades de dia zero e de um dia nos últimos seis meses.
- A pesquisa da Akamai descobriu que as vítimas de vários grupos de ransomware têm quase seis vezes mais chances de sofrer um ataque subsequente nos primeiros três meses após o ataque inicial.

Notícias esperadas

- Os ataques à API direcionados à lógica de negócios da API não são fáceis de detectar e mitigar. Por esse motivo, eles são difíceis de determinar a nível individual.
- As organizações precisam garantir a conformidade com os novos requisitos do DSS PCI (Padrão de Segurança de Dados da Indústria de Cartões de Pagamento) v4.0 e com os regulamentos da DORA (Lei de Resiliência Operacional Digital).

> Esses insights são ótimos guias para ajudar você a controlar seu programa de segurança e ver onde há ferramentas redundantes ou lacunas.
>
> **– Steve Winterfeld, CISO consultivo, Akamai**

Fatores que parecem nunca mudar

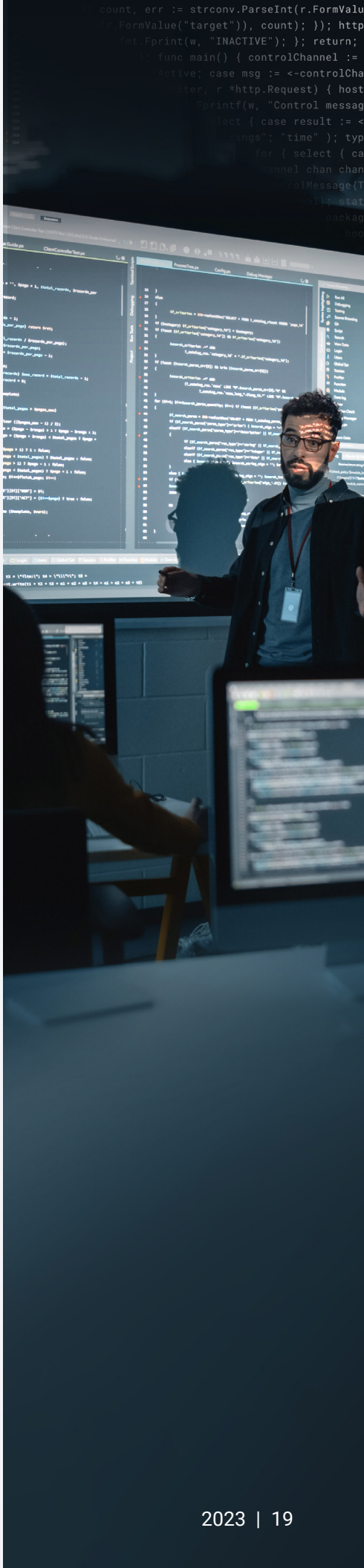
- O número de bots e ataques de API continua crescendo e novos recordes estão sendo estabelecidos para ataques DDoS.
- Os setores mais atacados tendem a ser serviços financeiros, alta tecnologia e comércio.
- A LFI (Inclusão de Arquivos Locais) é a técnica de ataque mais utilizada.
- Há uma mudança contínua da América do Norte para a Europa como a região com mais ataques DDoS.

Os indicadores validados de comprometimento da comunicação C2 foram uma descoberta fundamental que me fez pensar. O que foi particularmente perturbador foi a alta frequência de detecção inicial ocorrida depois que o malware já havia comprometido os sistemas com sucesso e estava estabelecendo comunicação. Isso enfatiza o equilíbrio crítico necessário entre medidas preventivas e detecção rápida para minimizar o impacto.

A história que mais me surpreendeu foi a mudança do ataque às pessoas por meio de engenharia social para o uso de dia zero. Nos últimos anos, senti que nossas defesas técnicas estavam ficando mais fortes e eu precisava reforçar o quadro de funcionários com treinamento e monitoramento. Porém, depois da mudança deste ano para o dia zero, preciso analisar com atenção onde implantarei os recursos no próximo ano.

Os ataques que parecem mais injustos são aqueles que ocorrem enquanto sua organização já está lidando ou se recuperando de um ataque de ransomware. É fácil concentrar-se profundamente na crise e retirar recursos da monitorização defensiva contínua. Esta pesquisa foi um poderoso lembrete de que você NÃO pode se dar ao luxo de baixar suas defesas!

Esses insights são ótimos guias para ajudar você a controlar seu programa de segurança e ver onde há ferramentas redundantes ou lacunas. Eles podem motivar exercícios para atualizar manuais/processos, orientar treinamentos, aprimorar planos de teste de penetração ou apoiar análises de portfólio de risco. A cibersegurança é um esporte de equipe, portanto, esses insights também são úteis para impulsionar discussões com parceiros internos (como equipes jurídicas ou de TI) e fornecedores. Como sempre, referências/ferramentas como o NIST (Instituto Nacional de Padrões e Tecnologia), a base de conhecimento MITRE ATT&CK e o OWASP Top 10 são ótimos recursos.



Pensando no futuro

É impossível prever o futuro, mas podemos antecipar que os ataques DDoS e API dominarão 2024. Os esforços contínuos para construir exércitos maiores de botnets e desenvolver novas técnicas, combinados com a influência dos Estados-nação, farão com que a DDoS cresça. Esse fator, juntamente com a evolução do ransomware, será a gênese da legislação e da resiliência.

A transformação continua sendo a força motriz para a implementação de APIs na maioria dos setores. Esse rápido crescimento levará inadvertidamente a superfícies de ataque maiores e mais vulnerabilidades, APIs de sombra, APIs zumbis e abuso de APIs. Esperamos ver um crescimento significativo nos ataques a aplicações Web e APIs. Isso virá de ataques padrão, como LFI, e de técnicas emergentes, como Server-Side Request Forgery (SSRF) e Server-Side Template Injections (SSTI), que exigirão ferramentas que possam detectar movimentos laterais e mitigar impactos.

Por fim, com exceção de algumas tendências específicas da indústria e da região, esperamos ver uma escassez geral de profissionais qualificados em cibersegurança. Haverá alguma redução no machine learning e na inteligência artificial de grandes modelos de linguagem, mas no geral será extremamente difícil encontrar e reter o talento de que precisamos. Isso levará à parceria com fornecedores para contratação de pessoal sob demanda ou serviços gerenciados para funções não essenciais.

Quanto ao SIG da Akamai, continuaremos alertando para ameaças predominantes e riscos de segurança emergentes no horizonte. Vamos interagir com a comunidade de segurança por meio das nossas plataformas e canais para incrementar os esforços de inteligência contra ameaças. E, em 2024, comemoraremos o aniversário de 10 anos de nossos relatórios SOTI! Estamos empolgados para continuar melhorando nossos relatórios, introduzindo novos conjuntos de dados, recursos visuais e insights importantes que podem apoiar os profissionais de segurança em sua busca de manter suas organizações protegidas.

Esperamos compartilhar mais insights de pesquisa no próximo ano. Enquanto isso, fique em segurança!

Créditos

Editorial e redação

Roger Barranco
Tricia Howard
Charlotte Pelliccia
Lance Rhodes
Badette Tribbey
Chelsea Tuttle
Steve Winterfeld

Análise e contribuição do assunto

Kimberly Gomez
Reuben Koh
Emily Lyons
Richard Meeus
Carley Thornell

Análise de dados

Chelsea Tuttle

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 atualizado 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 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, visite nossa **página de solução de segurança**.

A Akamai protege sua experiência do cliente, sua força de trabalho, seus sistemas e seus dados ajudando a incorporar a segurança em tudo o que você criar, em qualquer lugar que você criar e entregar. A visibilidade da nossa plataforma em relação às ameaças globais nos ajuda a adaptar e desenvolver sua postura de segurança para permitir Zero Trust, interromper ransomware, proteger aplicações e APIs ou combater ataques DDoS, dando a você a confiança para inovar, expandir e transformar continuamente o que é possível. 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 11/23.