SOTI

10 YEARS
OF SECURITY INSIGHT

V10 EDIÇÃO 05

Enfrentando a maré

Tendências de ataque em serviços financeiros

Akamai

State of the Internet/Security

Índice

Introdução

O setor de serviços financeiros não é apenas um pilar da economia global, é a força vital do crescimento e desenvolvimento econômico. Englobando uma gama diversificada de setores, tais como bancos comerciais, processadores de pagamento, empresas de gestão de ativos, bancos de investimento e seguradoras, os serviços financeiros estão em constante estado de evolução.

Os avanços tecnológicos continuam a remodelar o cenário dos serviços financeiros, dando origem a inovações de tecnologia financeira (fintech), como bancos digitais, consultores robôs e ativos criptográficos. O número de empresas fintech aumentou globalmente, com os Estados Unidos e a China saindo na frente. Em janeiro de 2024, oito das dez maiores empresas de fintech estavam sediadas nesses dois países. Essa mudança tecnológica também se reflete no crescimento das transações sem dinheiro, o que deverá aumentar significativamente, em especial nos locais onde o acesso financeiro é limitado. Mas com a inovação vem a vulnerabilidade.

Os cibercriminosos estão atacando incansavelmente as instituições financeiras, e o impacto desses ataques vai muito além da perda financeira. Interrupções operacionais, danos à reputação e penalidades regulatórias devastadoras podem prejudicar a base da confiança sobre a qual o setor de serviços financeiros é construído. Como as instituições financeiras podem estabelecer defesas eficazes em um momento em que a velocidade da transformação digital é alcançada apenas pela sofisticação das ciberameaças?

Este relatório State of the Internet foi concebido especificamente para ajudar profissionais de serviços financeiros em todo o mundo, clientes Akamai, pesquisadores de cibersegurança e líderes do setor, a navegar pelo cenário de ameaças cada vez mais complexo. Como principal alvo dos cibercriminosos, o setor de serviços financeiros requer um esforço colaborativo para proteger sua infraestrutura crítica, proteger empresas e clientes, garantir a estabilidade dos mercados financeiros e evitar problemas econômicos. A pesquisa apresentada neste relatório é uma leitura essencial para quem quer ficar à frente dos invasores, fortalecer os ativos críticos do setor e garantir a confiança e a confiabilidade contínuas que sustentam as relações financeiras globais.

Fortalecer os serviços financeiros com conformidade, resiliência operacional e cibersegurança

Um dos principais desafios que o setor financeiro global enfrenta hoje é a obrigatoriedade de aumentar a conformidade e a resiliência operacional. À medida que o cenário das regulamentações evolui, as instituições financeiras devem se adaptar proativamente para atender a essas novas demandas. A introdução da DORA (Digital Operational Resilience Act, Lei de Resiliência Operacional Digital), por exemplo, ressalta a necessidade de uma estrutura sólida capaz de suportar interrupções relacionadas à tecnologia da informação e comunicação (TIC, Information and Communication Technology). Prevista para entrar em vigor em janeiro de 2025, a DORA exige estratégias abrangentes de resiliência para as entidades financeiras e seus fornecedores terceirizados de TIC, o que está obrigando as empresas a elevar seus recursos de segurança e resposta a incidentes.

As diretrizes atualizadas da Comissão de Valores Mobiliários dos EUA ampliam ainda mais a necessidade de uma abordagem holística de cibersegurança. As instituições financeiras agora são obrigadas a integrar resiliência operacional e recuperação de desastres em suas estratégias, colocando ênfase significativa na materialidade dos riscos cibernéticos. Isso envolve uma compreensão profunda de como ameaças e incidentes significativos podem afetar a estabilidade financeira e as operações. As determinações para divulgação imediata de incidentes relevantes de cibersegurança e articulação detalhada de estratégias de gerenciamento de riscos em relatórios anuais significam uma mudança de paradigma nas expectativas regulamentares. Navegar por esses cenários regulamentares exige que as instituições financeiras façam parcerias com entidades que oferecem soluções de segurança e visibilidade de última geração. Como mostrado nesta pesquisa, a experiência da Akamai pode ajudar a garantir que as organizações de serviços financeiros não apenas alcancem a conformidade, mas também mantenham a integridade operacional em meio a requisitos regulamentares rigorosos.

Considerando esses desdobramentos, as instituições financeiras devem adotar uma abordagem abrangente para lidar com as complexidades da conformidade e resiliência operacional. Isso envolve identificar e priorizar riscos relevantes, os que podem impactar significativamente o processo de tomada de decisão de um investidor. As instituições financeiras devem incorporar esses riscos relevantes em suas estruturas de gerenciamento de riscos e garantir que planos robustos de resposta a incidentes estejam em vigor. O caminho para uma resiliência operacional eficaz é pavimentado com a adoção de uma estratégia de defesa em profundidade de várias camadas. Isso inclui reduzir a superfície de ataque por meio de segmentação e microssegmentação de rede, implementar criptografia de dados em repouso, fortificar servidores e usar firewalls de aplicativos da Web juntamente com sistemas avançados de detecção de ameaças. O monitoramento contínuo e as avaliações periódicas de segurança são cruciais para identificar e mitigar os riscos prontamente.

Exercícios de planejamento de resposta a incidentes, baseados em inteligência e pesquisa de ameaças atuais, como os relatórios SOTI (State of the Internet) da Akamai, são essenciais para as instituições financeiras. Esses exercícios ajudam a construir cenários plausíveis e garantem que as instituições possam se adaptar a novas ferramentas, técnicas e procedimentos à medida que surgirem. Essa postura proativa é vital para garantir a resiliência operacional e manter a confiança dos clientes em um cenário de ameaças cada vez mais volátil. À medida que o setor de serviços financeiros evolui, a intersecção de conformidade, resiliência operacional e cibersegurança continuará a moldar seu futuro. Ao adotar medidas de segurança avançadas e aumentar a visibilidade, as instituições financeiras podem navegar as complexidades regulamentares e proteger suas operações para manter a confiança essencial para os negócios.

Teresa Walsh
diretora global de inteligência, FS-ISAC

Principais informações

34%

Porcentagem de eventos de ataque DDoS das camadas 3 e 4 sofridos por instituições de serviços financeiros

Os serviços financeiros continuam sendo o setor mais frequentemente atacado por eventos de ataque de DDoS (Distributed Denial-of-Service, Negação de serviço distribuída) nas camadas 3 e 4. Em seguida, está o setor de jogos, com 18%, e o de alta tecnologia, com 15%. Essa ameaça predominante provavelmente decorre das tensões geopolíticas em andamento, particularmente as guerras Israel-Hamas e Rússia-Ucrânia, que impulsionaram um aumento na atividade hacktivista em todo o mundo.

O crescimento de APIs impulsiona o aumento dos ataques de DDoS na camada 7

Embora os aplicativos da Web tenham sido tradicionalmente os principais alvos de ataques cibernéticos, os ataques de DDoS da camada 7 em APIs têm picos notáveis durante o período do relatório. Isso é impulsionado em grande parte pela crescente adoção de APIs em serviços financeiros para atender às exigências regulamentares e de conformidade em evolução. À medida que as organizações dependem mais das APIs, os adversários estão adaptando suas táticas, tornando a segurança de APIs uma prioridade imprescindível para as empresas modernas.

Os picos de tráfego destacam a necessidade de avaliar o DDoS por frequência e volume

Ataques de DDoS em serviços financeiros revelam um insight crítico: A frequência dos eventos nem sempre se correlaciona com a intensidade dos ataques. Embora alguns meses apresentem poucos ataques, os dados de Gbps correspondentes indicam picos de tráfego significativos, enfatizando a necessidade de considerar tanto a frequência quanto o volume dos ataques ao avaliar ataques de DDoS.

36%

Porcentagem de domínios suspeitos direcionados a instituições financeiras

Os ataques de phishing têm sido cada vez mais direcionados aos clientes de serviços financeiros, elevando os riscos de roubo de identidade e apropriação indevida de contas. Essa tendência de ataque expõe as instituições financeiras a um maior escrutínio dos reguladores, e as violações levantam preocupações de confiança dos clientes.

30%

Porcentagem de visitas a páginas direcionadas a websites de phishing e de apropriação indevida de marcas

Os invasores conduzem o tráfego com sucesso para websites fraudulentos, imitando websites e aplicativos de serviços financeiros legítimos. Eles continuam a atacar as instituições financeiras com phishing para obter as arcas do tesouro de informações confidenciais mantidas por essas organizações.

Os serviços financeiros continuam sendo o principal alvo para ataques de DDoS das camadas 3 e 4

Os ataques de DDoS (negação de serviço distribuída) das camadas 3 e 4 têm como alvo as camadas de rede e de transporte, sobrecarregando a estrutura de rede e esgotando os recursos do servidor e a largura de banda. Esses ataques enviam uma enorme quantidade de tráfego com o objetivo de consumir a capacidade da rede e degradar o desempenho para usuários legítimos. Entre todos os setores, o setor de serviços financeiros tem sido o principal alvo para ataques de DDoS de camada 3 e camada 4 (Figura 1). Essa tendência é impulsionada por vários fatores interconectados que criaram uma tempestade perfeita de vulnerabilidades e oportunidades para os invasores.

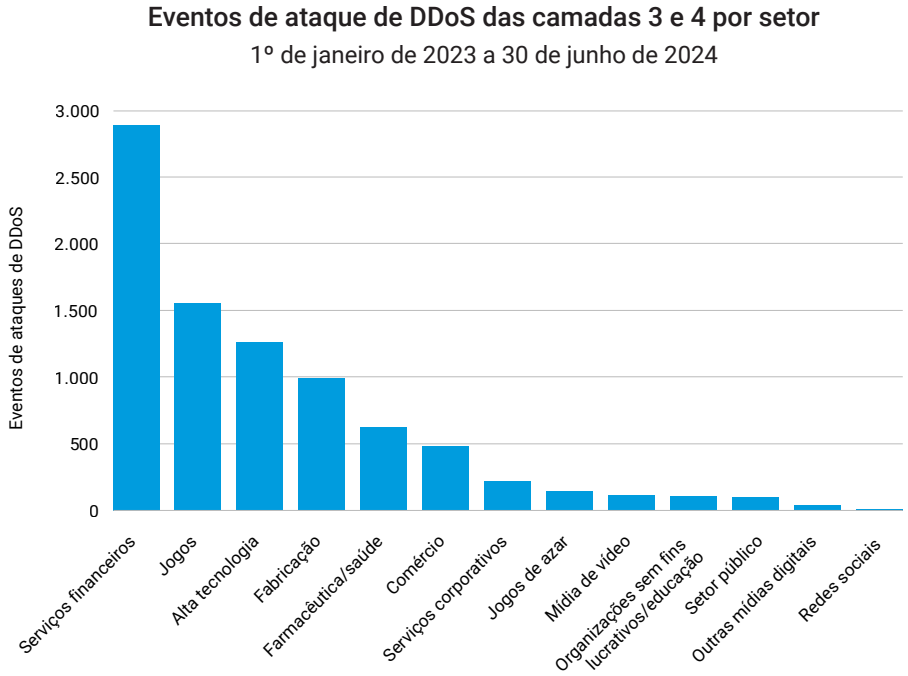


Fig. 1: o setor de serviços financeiros tem uma liderança elevada sobre outros setores em eventos de ataque de DDoS nas camadas 3 e 4

As tensões geopolíticas têm desempenhado um papel significativo no aumento dos ataques de DDoS às instituições financeiras. As atuais guerras Rússia-Ucrânia e Israel-Hamas coincidiram com aumentos significativos no hacktivismo pró-russo e pró-palestino. Esses conflitos estimularam um aumento nos ataques de DDoS, visando particularmente bancos europeus com afiliações à Ucrânia. A natureza politicamente motivada desses ataques acrescenta uma camada adicional de complexidade ao cenário de ameaças.

As instituições financeiras são alvos especialmente atraentes para os invasores de DDoS devido aos altos riscos envolvidos. A interrupção bem-sucedida das operações pode levar a um impacto financeiro grave, danos significativos na reputação e uma perda de confiança no sistema financeiro global. O potencial de propagação das consequências torna os serviços financeiros um alvo primordial para quem procura causar o máximo de danos ou fazer uma declaração política.

Os avanços tecnológicos aumentaram drasticamente o poder e os recursos dos invasores de DDoS, que agora podem implantar botnets de máquina virtual (VM) para realizar ataques de forma mais eficiente, aproveitando recursos computacionais em inúmeras VMs e dispositivos de Internet das Coisas (IoT). Essa abordagem explora a natureza distribuída dos serviços de nuvem, tornando os ataques mais difíceis de mitigar e rastrear. Os invasores podem aproveitar a alta disponibilidade de largura de banda e recursos computacionais vastos, possibilitando que eles iniciem ataques de DDoS adaptáveis, poderosos e economicamente vantajosos usando várias estratégias.

A expansão da superfície de ataque no setor de serviços financeiros também contribuiu para o aumento dos ataques de DDoS. O uso crescente de serviços digitais e APIs abriu mais pontos de entrada para os invasores. Essa mudança trouxe mais complexidade aos sistemas financeiros e introduziu inúmeras vulnerabilidades potenciais para os invasores explorarem. APIs sombra não documentadas são de particular preocupação, pois muitas vezes são desprotegidas porque as equipes de segurança da informação não têm conhecimento de sua existência. Os invasores podem explorar essas APIs para exfiltrar dados, burlar controles de autenticação ou executar atos destrutivos.

As pressões regulamentares aumentaram inadvertidamente a vulnerabilidade das instituições financeiras aos ataques de DDoS. Requisitos como a Diretiva de Serviços de Pagamento 2 (PSD2), introduzida pela União Europeia, exigiram que os bancos abram seus sistemas a fornecedores terceirizados, como empresas fintech, por meio de APIs. Embora isso permita que os bancos respondam às crescentes expectativas dos clientes por meio da integração com fintech, aplicativos móveis e outras plataformas, aumenta também os riscos de segurança e expande a superfície de ataque. O uso adicional de APIs entre essas várias entidades cria mais possíveis pontos de falha para os invasores atacarem.

Coletivamente, esses fatores contribuíram para o setor de serviços financeiros receber o título constante de principal alvo dos ataques de DDoS de camada 3 e camada 4. A combinação de motivações geopolíticas, metas de alto valor, avanços tecnológicos, uma presença digital em expansão e pressões regulamentares criou um ambiente no qual os ataques de DDoS às instituições financeiras não são apenas mais frequentes, mas também potencialmente mais prejudiciais do que nunca. À medida que o setor continua a evoluir, também é necessário que evoluam as suas defesas contra essas ameaças cada vez mais sofisticadas e persistentes.

Os invasores podem aproveitar a alta disponibilidade de largura de banda e recursos computacionais vastos, possibilitando que eles iniciem ataques de DDoS adaptáveis, poderosos e economicamente vantajosos usando várias estratégias.

Eventos de ataques de DDoS das camadas 3 e 4: um passeio de montanha-russa

Embora o setor de serviços financeiros apresente a maior frequência de eventos de ataque de DDoS de camada 3 e camada 4, a taxa desses ataques flutua ao longo do ano (Figura 2).

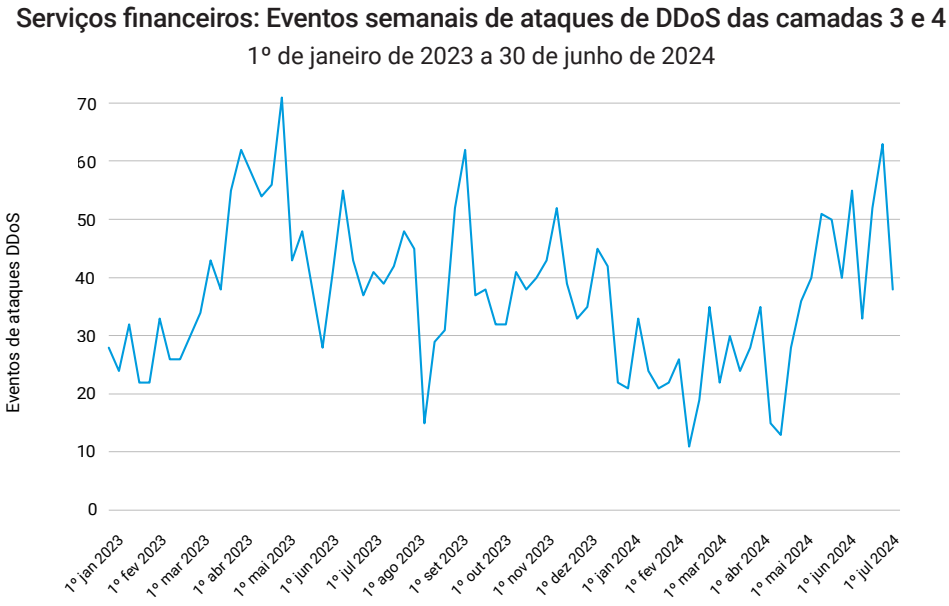


Fig. 2: um padrão de aumento e queda para os eventos de ataque de DDoS das camadas 3 e 4 no setor de serviços financeiros

Os ataques de DDoS da camada 3 e da camada 4 contra o setor de serviços financeiros durante março/abril de 2023, agosto/setembro de 2023, e abril/maio de 2024 podem ser atribuídos a vários fatores específicos.

A primavera, de março a abril no hemisfério norte, marca a temporada ativa de imposto de renda dos EUA, apresentando uma oportunidade atraente para os invasores de DDoS. Houve um aumento significativo em ataques de violação de contas nos bancos nacionais e regionais a partir de 16 de abril, o que coincide com a divulgação dos resultados financeiros do primeiro trimestre de muitos bancos. Durante esse período, o gerenciamento de identidade e acesso (IAM) e os provedores de rede, como Okta e Cisco, também relataram ataques crescentes e consideráveis de preenchimento de credenciais direcionados a serviços online.

Em abril de 2023, especificamente, a descoberta da vulnerabilidade de alta gravidade do Service Location Protocol (SLP) (CVE-2023-29552) provavelmente contribuiu para o aumento das atividades de ataque. Essa vulnerabilidade, que pode amplificar ataques de DDoS tanto nas camadas de rede quanto de aplicativos, teria afetado mais de 2.000 organizações em todo o mundo e mais de 54.000 instâncias do SLP na Internet. Ao explorar essa vulnerabilidade, os invasores podem usar as instâncias comprometidas para iniciar ataques de amplificação de DDoS em grande escala. Com um fator de amplificação de até 2.200 vezes, essa vulnerabilidade permitiu um dos ataques de amplificação mais significativos já documentados.

Identificamos um evento importante examinando o período de agosto/setembro de 2023. A Akamai observou e frustrou o maior ataque de DDoS registrado em uma instituição financeira dos EUA em 5 de setembro de 2023. Esse ataque combinou técnicas de inundação ACK, PUSH, RESET e SYN, atingindo intensidades de pico de 633,7 gigabits por segundo (Gbps) e 55,1 milhões de pacotes por segundo (Mpps). Apesar de sua alta intensidade, o ataque foi breve, com duração de menos de dois minutos.

Destaque de segurança

Intensidade de ataques de DDoS das camadas 3 e 4: eventos vs. Gbps

Para entender completamente a ameaça que os ataques de DDoS representam para o setor de serviços financeiros, é fundamental entender sua complexidade e escala. Esses incidentes não são simples e isolados; cada ataque geralmente envolve múltiplas tentativas de alto volume que inundam redes com gigabits de dados e milhões de pacotes por segundo. A sofisticação, a intensidade e a duração dos ataques estão aumentando, e os atacantes estão usando técnicas mais variadas, o que aumenta o risco para as instituições financeiras (Figura 3).

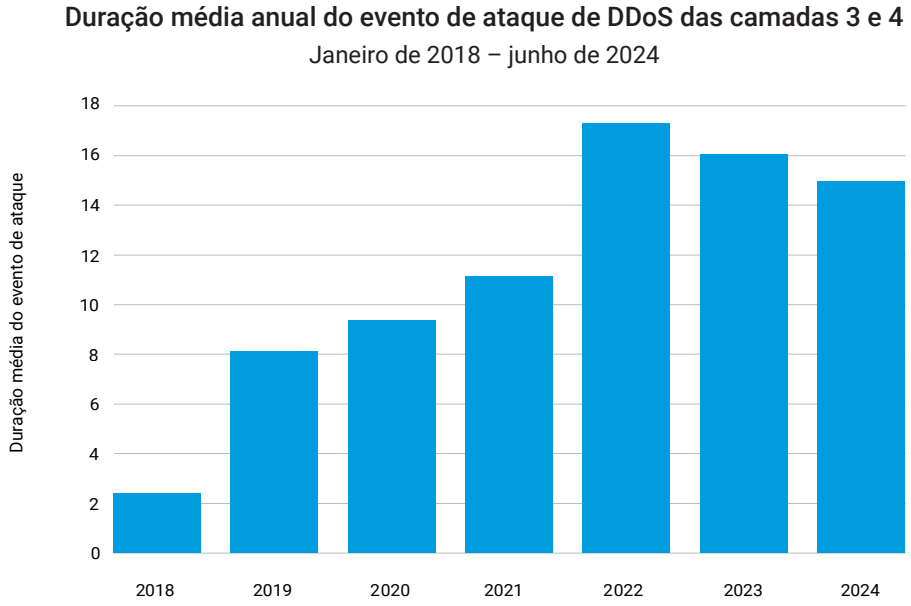


Fig. 3: a tendência global da duração do ataque de DDoS da camada 3 e 4 está aumentando

Além disso, ao comparar o gráfico do número de eventos de ataque de DDoS da camada 3 e 4 no setor de serviços financeiros com os dados correspondentes de DDoS em Gbps, nota-se uma discrepância significativa (Figura 4). O gráfico de Gbps mostra aumentos nítidos que não são refletidos no gráfico de eventos de ataque. Essa disparidade destaca um conceito importante: mesmo um mês com relativamente poucos eventos de ataque ainda pode ter um volume extremamente alto de tráfego DDoS em termos de Gbps.

Serviços financeiros: comparação de eventos semanais de ataque de DDoS das camadas 3 e 4

1º de janeiro de 2023 a 30 de junho de 2024

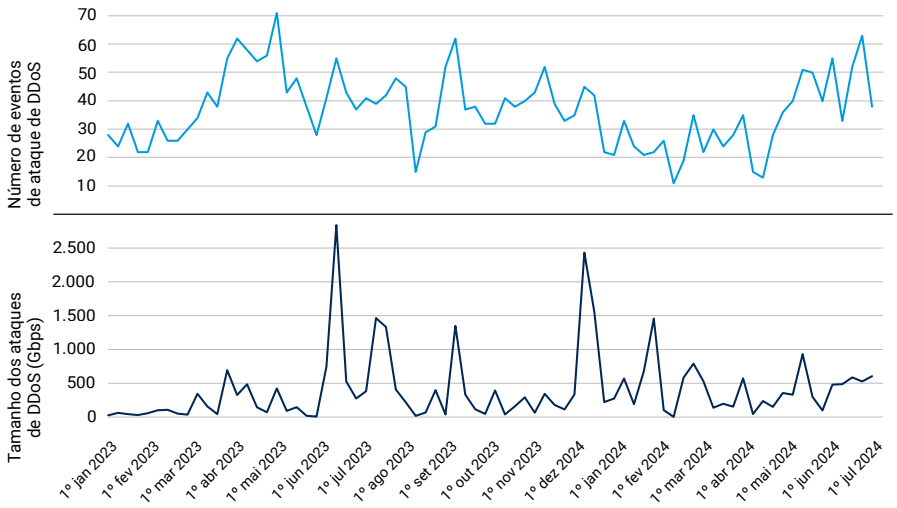


Fig. 4: os eventos de ataque de DDoS das camadas 3 e 4 do setor de serviços financeiros comparados com as respectivas medições em Gbps

Essa observação destaca um ponto crítico: basear-se exclusivamente na frequência de eventos de ataque subestima severamente a verdadeira ameaça. É essencial considerar tanto o volume quanto a intensidade do tráfego em cada ataque. Um pequeno número de ataques de DDoS altamente intensos pode causar muito mais danos do que um número maior de eventos de menor escala, tornando imperativo avaliar o escopo completo de cada ameaça.

Uma tendência de ataque direcionado: ataques de DDoS de vetor único das camadas 3 e 4 em serviços financeiros

Ataques multivetor sobre aplicativos ou redes são uma estratégia comum para os cibercriminosos que estão tentando corromper ou obter acesso não autorizado a um sistema. No entanto, os invasores focados no setor de serviços financeiros parecem tentar fazer ataques de vetor único com mais frequência quando se trata de DDoS nas camadas 3 e 4 (Figura 5).

Contagem de vetores de ataque de DDoS das camadas 3 e 4 por evento de ataque

1º de janeiro de 2023 a 30 de junho de 2024

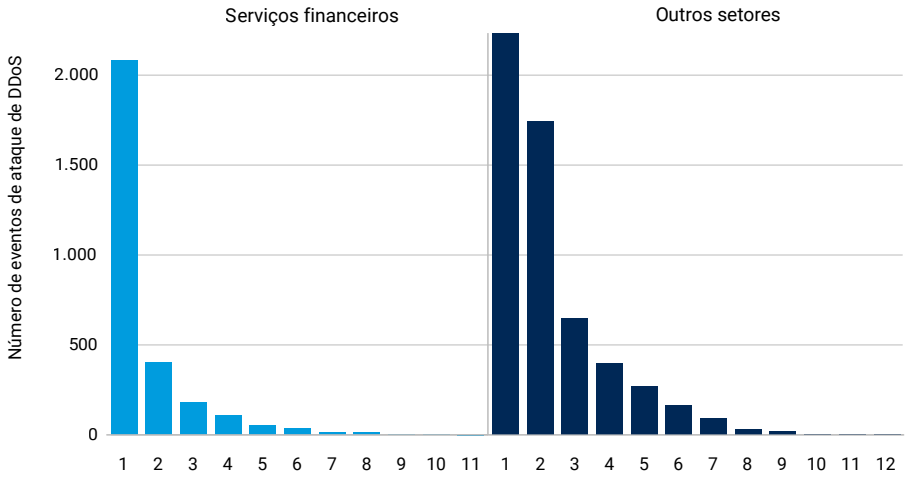


Fig. 5: os ataques de vetor único são mais amplamente utilizados para ataques de DDoS das camadas 3 e 4 no setor de serviços financeiros

Ataques de DDoS de vetor único direcionados às camadas 3 e 4 exigem menos recursos e podem ser altamente eficazes por si só, especialmente contra instituições financeiras que podem ter defesas robustas contra ataques mais complexos. Eles geralmente são mais fáceis de executar e exigem menos coordenação do que ataques multivetor. Também pode haver algumas vulnerabilidades especificamente conhecidas que as instituições financeiras têm nas camadas 3 e 4 que poderiam ser exploradas de forma eficaz com um único ataque vetorial sem o risco de tentar outros vetores de ataque que poderiam ser detectados pela segurança.

Essa preferência por ataques de um único vetor no setor de serviços financeiros apresenta um desafio exclusivo para equipes de cibersegurança. Embora seja importante permanecer vigilante contra ataques complexos e multivetoriais, é crucial garantir que todas as defesas possam resistir a ataques focados em um único vetor nas camadas 3 e 4.

Aumento dos ataques de DDoS da camada 7 em APIs

Os ataques de DDoS da camada de aplicativos (camada 7), também conhecidos como ataques HTTP ou de camada de tráfego da Web, tornaram-se cada vez mais predominantes e são agora um método preferido para os agentes de ameaças que visam o setor de serviços financeiros. Esses ataques focam especificamente nos componentes com uso mais intenso de recursos dos aplicativos, negando efetivamente o acesso a usuários legítimos. Ao contrário dos ataques de DDoS das camadas 3 e 4, que muitas vezes são mitigados por firewalls e proteção de rede, os ataques da camada 7 contornam essas defesas se disfarçando de solicitações legítimas ao atacar páginas de aplicativos ou funções de pesquisa específicas, com o objetivo de sobrecarregar o servidor de aplicativos.

Embora os aplicativos da Web no setor de serviços financeiros tenham sido geralmente visados com mais frequência do que as APIs, observamos aumentos acentuados no número de ataques de DDoS da camada 7 que visam especificamente as APIs (Figura 6). Esses picos são notavelmente mais significativos e variados do que o padrão geral de ataque a API em outros setores.

Serviços financeiros: ataques diários de DDoS da camada 7

1º de janeiro de 2023 a 30 de junho de 2024

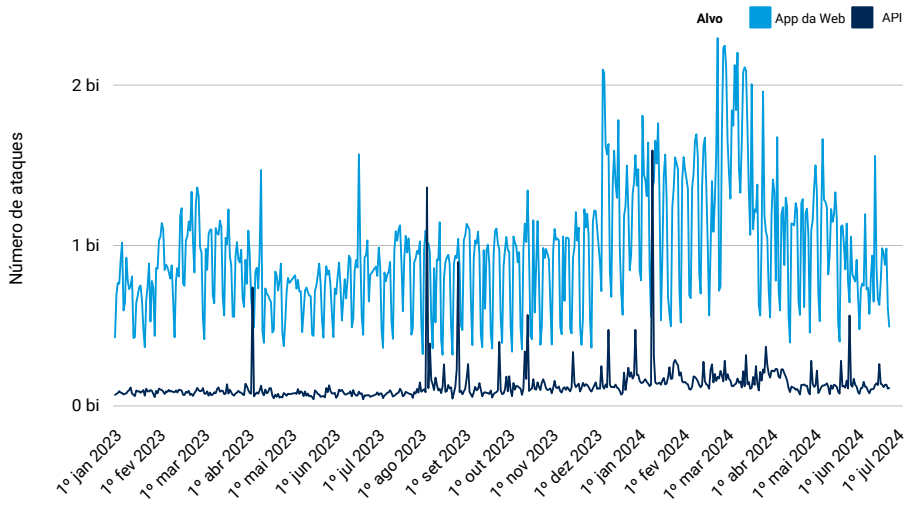
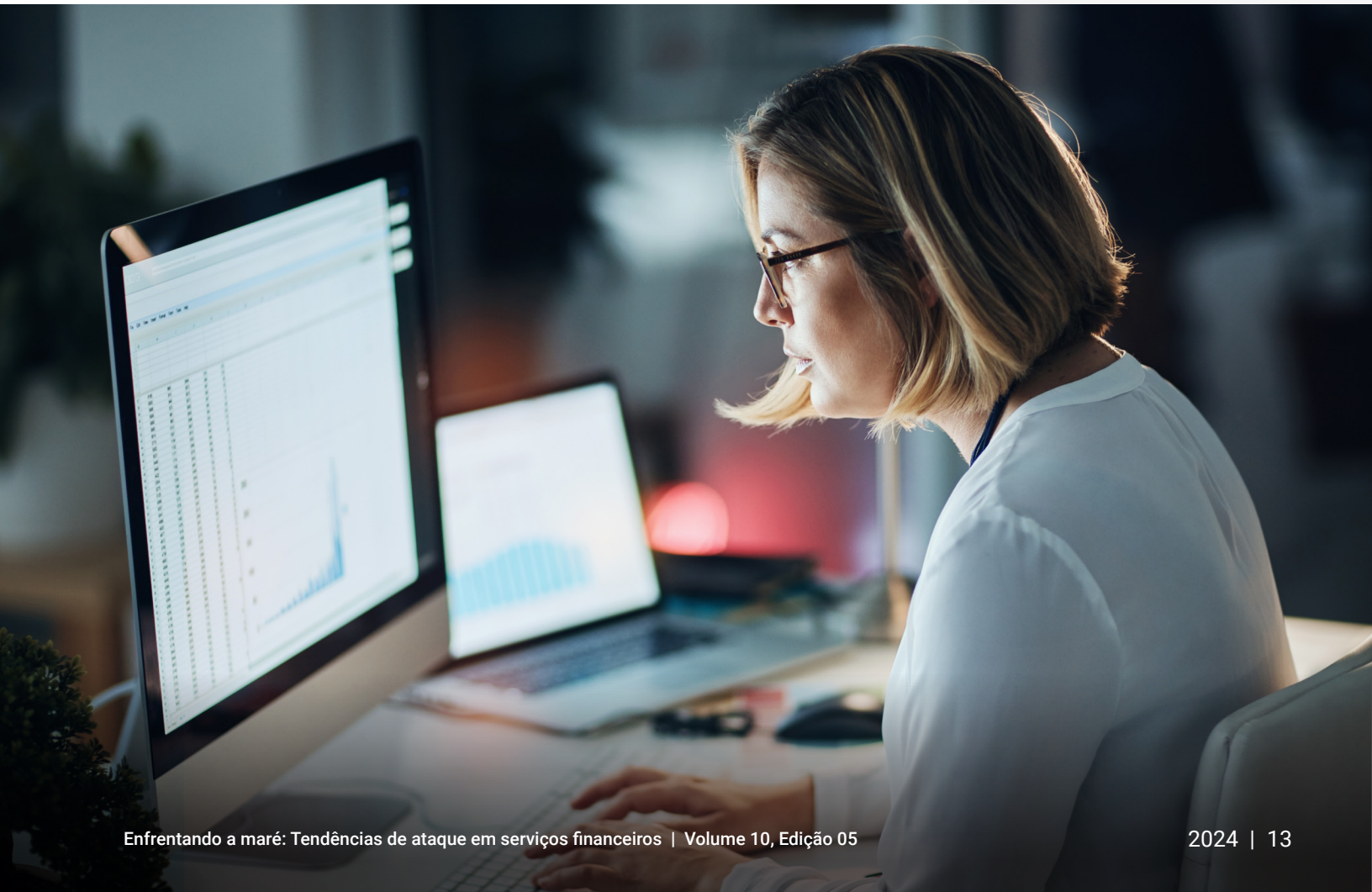


Fig. 6: os padrões de ataque variam significativamente entre aplicativos da Web e APIs visados em ataques de DDoS da camada 7 no setor de serviços financeiros

Esses aumentos acentuados ocorreram especificamente em abril de 2023, agosto de 2023 e janeiro de 2024. Atribuímos esses picos a fatores semelhantes aos que afetam os ataques das camadas 3 e 4, juntamente com elementos específicos adicionais da camada 7.

Os invasores buscam continuamente novas vulnerabilidades para explorar, e a descoberta de tais fraquezas pode levar a aumentos repentinos na frequência de ataque. Por exemplo, a vulnerabilidade HTTP/2 Rapid Reset (CVE-2023-44487), identificada pela primeira vez em agosto de 2023, permitiu ataques de DDoS altamente eficazes da camada 7. Essa vulnerabilidade permitiu que os invasores explorassem lógica aparentemente benigna e agrupassem várias solicitações em um stream, que sobrecarregava servidores e aplicativos. Isso resultou no maior ataque de DDoS da camada 7 registrado até o momento.

Além disso, os ataques de DDoS baseados na sazonalidade continuam sendo uma tática popular para os cibercriminosos que visam instituições financeiras, com picos notáveis durante o período de entrega do Imposto de Renda e períodos de festas de fim de ano. O aumento significativo em janeiro de 2024, após a movimentada temporada de compras de fim de ano, sugere que os invasores estavam se preparando para atacar durante períodos de maior atividade das transações online.



Ransomware e hacktivismo em serviços financeiros

O setor de serviços financeiros é muitas vezes alvo de agentes de ameaças altamente sofisticados, como grupos de ransomware. Esses grupos empregam uma vasta gama de técnicas para se infiltrar em instituições financeiras, roubar informações confidenciais e exigir grandes resgates. Embora as operações se concentrem principalmente nas motivações financeiras, elas também podem se cruzar com contextos geopolíticos, visando instituições financeiras que podem ter laços políticos. Esse foi o caso com o grupo de ransomware baseado na Rússia conhecido como REvil (aka Sodinokibi). O BlackCat (ALPHV) também esteve envolvido dessa forma, como visto por seu ataque a um banco renomado.

Um dos grupos de ransomware mais ativos conhecidos por seus ataques a grandes organizações, incluindo instituições financeiras, continua sendo o LockBit. Isso apesar das recentes ações das autoridades de aplicação da lei contra o grupo. A Operação Cronos, que incluiu uma colaboração entre a Europol e a Eurojust para coordenar uma força-tarefa internacional pioneira, foi superada por novas infraestruturas estabelecidas pelo LockBit. O grupo de ransomware ressurgiu com uma nova infraestrutura e um website de vazamento na dark web poucos dias após a operação das autoridades de aplicação da lei ter apreendido seus servidores em fevereiro de 2024. E o LockBit afirmou que revidaria aumentando os ataques às redes governamentais em resposta à Operação Cronos.

O grupo de ransomware CL0P também continua ativo e tem sido especialmente conhecido por explorar vulnerabilidades no software de transferência de arquivos amplamente utilizado em organizações, incluindo instituições financeiras. Um exemplo notável foi com a vulnerabilidade de dia zero CVE-2023-34362 que afetou o software MOVEit Transfer e começou com uma injeção de SQL para se infiltrar no aplicativo da Web MOVEit Transfer. Pelo menos 15 bancos e cooperativas de crédito confirmaram violações de dados como resultado da vulnerabilidade do MOVEit. O CL0P também ganhou acesso inicial por meio de outras técnicas, incluindo phishing, e continua sendo executado como um modelo de ransomware como serviço (RaaS). Recentemente, o grupo evoluiu suas táticas para empregar extorsão quádrupla em alvos como instituições financeiras. Além das técnicas envolvidas na extorsão tripla, a extorsão quádrupla inclui o envio de mensagens para assediar parceiros de negócios, funcionários, clientes, executivos de alto nível e a mídia para informá-los de que a organização foi hackeada. E essa tática levou a um aumento na média dos pagamentos de ransomware.

Outros agentes de ameaças hacktivistas que visam instituições financeiras, mas não são classificados como grupos de ransomware incluem Anonymous Sudan, KillNet e NoName057(16). Todos eles são notáveis por suas atividades relacionadas à guerra Rússia-Ucrânia, e o Anonymous Sudan também alegou ter sido envolvido com ataques cibernéticos em resposta à guerra Israel-Hamas. No ano passado, esses grupos, além de vários outros grupos de agentes de ameaças, alavancaram o caos provocado pela guerra Rússia-Ucrânia e voltaram sua atenção para a infraestrutura bancária crítica.

Existem muitos outros agentes de ameaça prolíficos que não são classificados como grupos de ransomware, mas são conhecidos por visarem o setor de serviços financeiros, como o Lazarus Group, MoneyTaker, Carbanak/FIN7, Cobalt e APT41.

Dadas as ameaças em curso representadas por esses atores, é fundamental que as instituições financeiras estejam cientes do atual cenário de ameaças e entendam melhor as motivações e técnicas dos invasores para desenvolver estratégias de defesa mais eficazes. Consulte a nossa seção de mitigação mais adiante neste relatório para obter medidas de salvaguarda recomendadas.

Surto recente de hacktivismo DDoS no Oriente Médio entre as instituições financeiras

O setor de serviços financeiros no Oriente Médio experimentou recentemente um aumento em ataques de DDoS sofisticados e prolongados, impulsionados pelas tensões geopolíticas. Essa tendência é particularmente predominante na região da Europa, Oriente Médio e África (EMEA) e exemplifica a ameaça crescente de ataques de DDoS com motivações políticas em instituições financeiras.

Um exemplo notável dessa tendência ocorreu no início deste ano, quando o BlackMeta (também conhecido como DarkMeta), um grupo hacktivista pró-palestino, lançou um ataque de DDoS de camada 7 de seis dias contra uma instituição financeira nos Emirados Árabes Unidos (EAU). O ataque foi facilitado pelo InfraShutdown, um serviço de DDoS por encomenda, destacando a crescente acessibilidade dessas ferramentas de ataque. O BlackMeta, que atua desde novembro de 2023, tem uma história de ataques a organizações em Israel, nos Emirados Árabes Unidos e nos Estados Unidos.

O ataque à instituição financeira dos Emirados Árabes Unidos foi significativo tanto na duração quanto na intensidade. Ele durou aproximadamente 100 horas, com ondas de solicitação da Web com duração de 4 a 20 horas, e média de 4,5 milhões de solicitações por segundo. O ataque colocou o banco sob ataque 70% do tempo, impactando substancialmente seus serviços. A campanha do BlackMeta contra o banco fez parte de um esforço mais amplo para protestar contra as injustiças observadas contra palestinos e muçulmanos, e demonstrou táticas semelhantes às empregadas pelo Anonymous Sudan.

Felizmente, os esforços de mitigação da instituição financeira impediram uma interrupção mais significativa, mas esse incidente ressalta a tendência crescente de ataques cibernéticos com motivação política. Ele também destaca a crescente disponibilidade de serviços de DDoS por encomenda, o que reduz a barreira para grupos hacktivistas lançarem ataques em larga escala. Esse desenvolvimento enfatiza a necessidade de medidas robustas de cibersegurança para proteger contra ameaças persistentes e de alto volume.

Outro ataque de DDoS recente e suspeito motivado politicamente ocorreu em 15 de julho de 2024 e teve como alvo uma grande empresa de serviços financeiros em Israel. Esse ataque maciço, que se originou de um botnet distribuído globalmente, durou quase 24 horas e atingiu um pico de 798 Gbps. A Akamai mitigou com sucesso esse ataque de DDoS nas camadas 3 e 4 que incluiu vários vetores, como reflexão de DNS e inundação UDP.

Durante este ataque, a Akamai bloqueou aproximadamente 389 terabytes de tráfego mal-intencionado em uma fase intensiva de três horas, com o tráfego bloqueado total atingindo aproximadamente 419 terabytes por toda a duração. A ocorrência de outras interrupções enfrentadas pelas instituições financeiras israelenses no mesmo dia sugere um ataque coordenado, destacando ainda mais a ameaça crescente representada por ataques de DDoS avançados.

Vale a pena notar que este invasor bem engenhoso tinha visado anteriormente o mesmo cliente de serviços financeiros 27 vezes nos 90 dias anteriores. O cliente tem sido repetidamente alvo de ataques de DDoS desde o quarto trimestre de 2023, coincidindo com a guerra Israel-Hamas. O grupo interno de inteligência de ameaças de DDoS da Akamai relata que instituições e empresas em Israel experimentaram um número sem precedentes de ataques de DDoS em 2024. Essa campanha agressiva e prolongada destaca a crescente escala e intensidade dessas ameaças, deixando claro que os invasores estão se tornando mais persistentes e engenhosos.

Apostando na familiaridade: abuso de marca em serviços financeiros

À medida que os serviços financeiros adotam abordagens digitais para melhorar a experiência do cliente, a eficiência operacional, a inovação, a receita geral e a visibilidade, os adversários cibernéticos estão explorando a confiança inerente entre as organizações e seus clientes por meio de esquemas de apropriação indevida de marcas. A Figura 7 mostra exemplos de websites fraudulentos que imitam instituições financeiras conhecidas. Embora o phishing e a apropriação indevida de marcas sejam métodos comuns, o número alarmante de websites fraudulentos e o ritmo rápido em que os invasores podem criar novos domínios depois que seus websites originais são colocados offline são particularmente preocupantes. Essa rápida proliferação representa uma ameaça crescente e implacável para o setor de serviços financeiros.

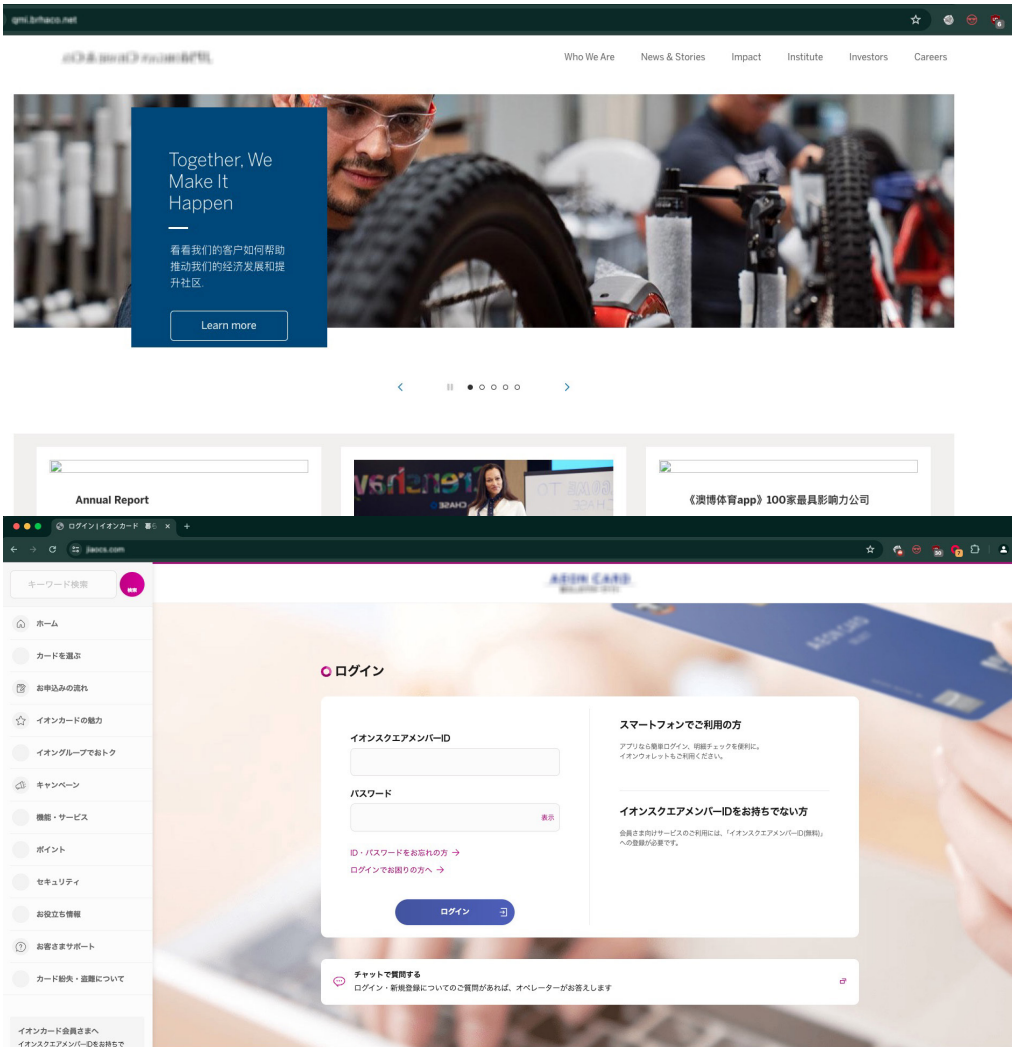


Fig. 7: amostras de websites fraudulentos de phishing que imitam instituições financeiras conhecidas

O cenário do abuso de marca foi significativamente alterado pelo surgimento de plataformas e kits de ferramentas de phishing como serviço. Esses recursos reduziram a barreira à entrada de cibercriminosos, impactando drasticamente a escala e a magnitude dos ataques de phishing contra serviços financeiros e seus clientes. Para colocar isso em perspectiva, o Grupo de Trabalho Anti-Phishing registrou quase cinco milhões de ataques de phishing em 2023, designando-o como o "pior ano já registrado para phishing".

A violação de marca pode ser um impulso para aumentar os riscos, como roubo de identidade e violação de contas. Os invasores geralmente pegam informações do cliente na dark web ou as usam na apropriação indevida de contas. Do ponto de vista da segurança, a intervenção precoce em ataques de marca é crucial. Ao frustrar o ciclo de vida do ataque no início, você pode impedir que os invasores coletem credenciais para fins nefastos.

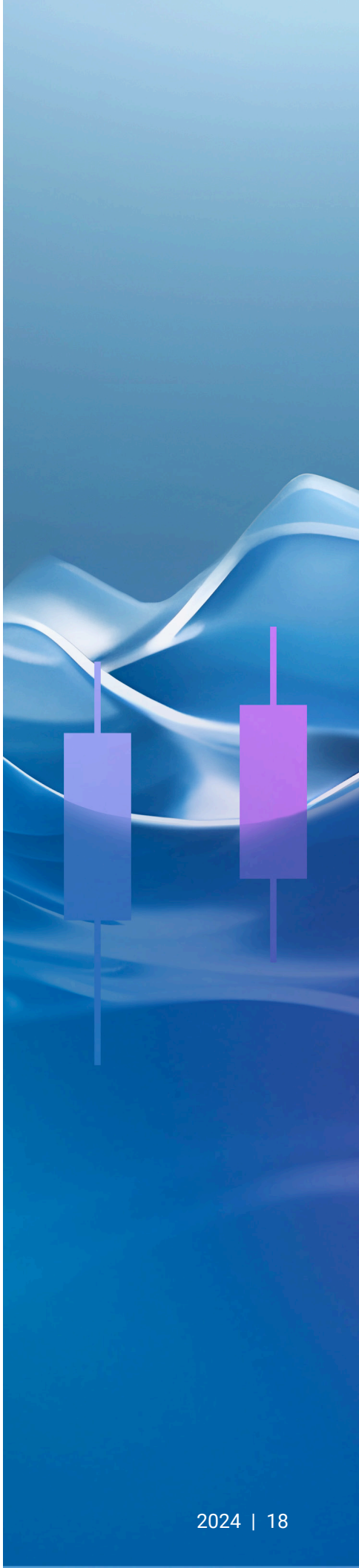
As ramificações do abuso de marca vão além das preocupações imediatas de segurança. Uma organização pode sofrer perdas financeiras substanciais devido a danos à reputação, problemas de conformidade e legais, e até mesmo perda de vendas devido a produtos falsificados. No cenário digital de hoje, a detecção precoce de ataques de apropriação indevida de marcas é fundamental para manter a confiança do cliente e a continuidade dos negócios.

Ponto de fraude: um olhar mais atento aos ataques de apropriação indevida

As equipes de segurança enfrentam o desafio assustador de se defender contra o abuso de marca que pode ocorrer em várias plataformas online. Isso torna os ativos digitais difíceis de proteger, pois tanto usuários legítimos quanto invasores podem acessá-los. Os invasores muitas vezes capturam o conteúdo de ativos públicos, como portais bancários online, para criar seu próprio website falsificado e registrar um domínio com erros ortográficos para enganar usuários desavisados. Além disso, os adversários cibernéticos lançam campanhas envolvendo e-mails de phishing, publicações de rede social e outros canais digitais para atrair potenciais vítimas para seus websites mal-intencionados ou aplicativos falsos.

Para este relatório, analisamos as atividades de apropriação indevida de marcas e phishing observadas em domínios ativos nos últimos 12 meses para fornecer insights sobre a predominância de apropriação indevida de marcas em todos os setores, com um foco particular em serviços financeiros. A visibilidade abrangente e a solução proprietária da Akamai nos permitem:

- Rastrear o tráfego através de websites de phishing e apropriação indevida de marcas, incluindo marketplaces
- Identificar o número de domínios mal-intencionados ativos
- Avaliar as pontuações de gravidade dos domínios mal-intencionados



Os serviços financeiros foram o setor que mais sofreu ataques de apropriação indevida de marcas (36,25%) entre todos os websites suspeitos monitorados pela Akamai (Figura 8). Essa descoberta ressalta particularmente a vulnerabilidade do setor de serviços financeiros à apropriação indevida e à violação de marcas. As organizações de comércio (26,41%) e de serviços empresariais (18,90%) seguiram em segundo e terceiro lugares, respectivamente.

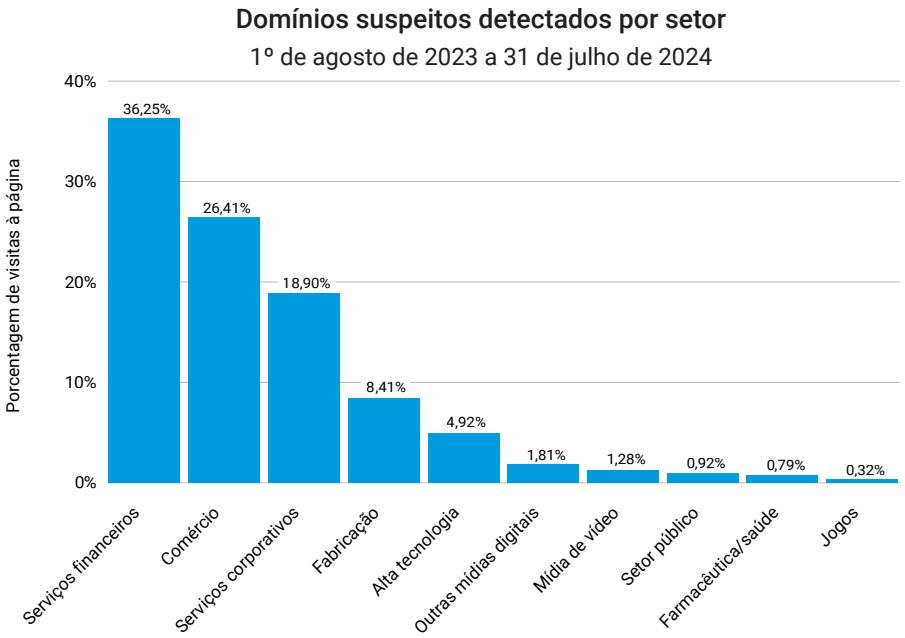


Fig. 8: os serviços financeiros representaram 36,3% dos domínios de phishing e/ou apropriação indevida de marcas

O setor de serviços financeiros é um alvo principal de ataques de apropriação indevida de marcas devido às grandes quantidades de dados confidenciais e altamente valiosos que detém, como credenciais bancárias e informações de identificação pessoal (PII). As informações obtidas de websites bancários falsificados permitem que os cibercriminosos acessem facilmente e, posteriormente, drenem contas. Da mesma forma, outras informações financeiras de alto valor, como credenciais para carteiras eletrônicas e contas de criptomoedas (os preços variam de US$ 120 a US$ 400 na dark web), podem ser obtidas, permitindo que os invasores transfiram o que está na conta ou vendam as informações em marketplaces da dark web. A alta compensação monetária de tais esquemas torna os serviços financeiros alvos principais de violação de marca e ataques de phishing.

Da mesma forma, as organizações de comércio se tornaram alvos lucrativos de violação de marca desde o surgimento do comércio eletrônico e compras online, que apresenta oportunidades de desvio de credenciais e outras informações pessoais. Empresas de manufatura e fornecedores terceirizados que prestam serviços são igualmente vulneráveis à violação de marca. Embora a digitalização melhore o crescimento geral dos negócios, ela se tornou um ponto fraco vulnerável para muitas organizações, levando à proliferação de ataques de apropriação indevida de marcas e ao aumento das tentativas de phishing.

A alta compensação monetária de esquemas [apropriação indevida de marcas] torna os serviços financeiros alvos principais de violação de marca e ataques de phishing.

As organizações devem permanecer vigilantes e implementar medidas de segurança para proteger marcas e clientes neste cenário digital em evolução. Isso inclui monitoramento contínuo para detectar uso indevido de marcas, procedimentos de remoção rápida de websites fraudulentos e a informação aos clientes para reconhecer possíveis tentativas de apropriação indevida. Ao priorizar esses esforços, as organizações podem proteger melhor sua reputação e a confiança de seus clientes em um ambiente de ameaça cada vez mais complexo.

Serviços financeiros na mira da violação de marca

Para obter uma visão holística do impacto da apropriação indevida de marcas e do phishing, também analisamos o número de visitas a páginas de websites suspeitos. Nossos resultados revelam que os websites que se disfarçam como instituições financeiras receberam 30% das visitas, enquanto as empresas que imitam comércio seguem com 20% das visitas (Figura 9). Esses resultados colocam consistentemente os serviços financeiros e o comércio nas principais classificações, seja pela medida de solicitações ou de domínios. Essa consistência destaca seu status como alvos principais de violação e apropriação indevida de marcas, e por uma boa razão.

Os serviços financeiros abrangem uma ampla gama de alvos, desde bancos bem estabelecidos até instituições menores com menos recursos de segurança, todos com alto risco. O comércio, outro setor sob escrutínio semelhante por fóruns de conformidade (por exemplo, o Conselho de normas de segurança do setor de cartões de pagamento) como serviços, também enfrenta riscos significativos devido à riqueza de informações de clientes que possui.

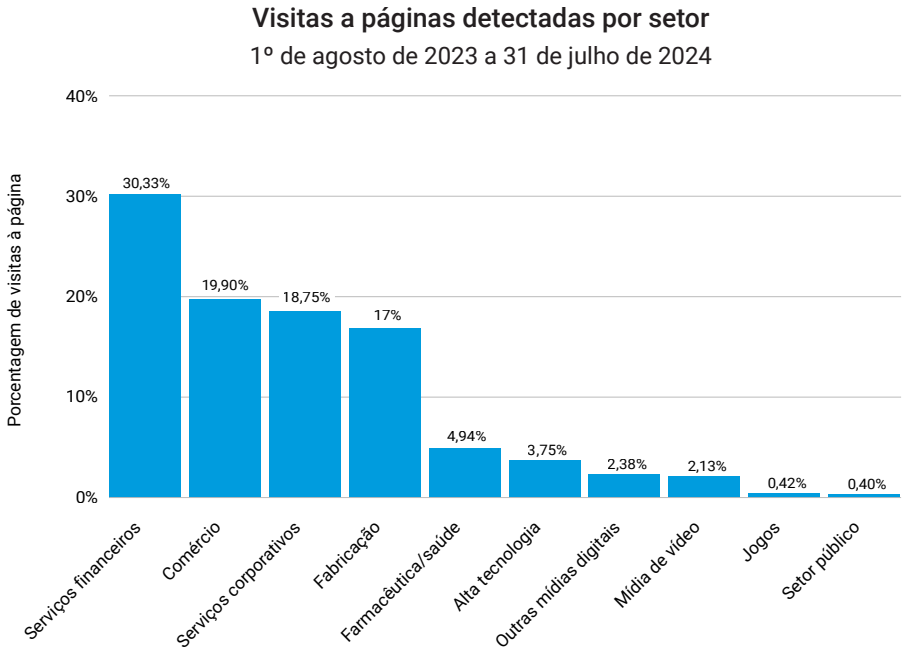


Fig. 9: mais de 30% das visitas de página durante o período de relatórios (agosto de 2023 a julho de 2024) foram para websites suspeitos que estavam se disfarçando como websites de serviços financeiros legítimos

Curiosamente, observamos algumas disparidades entre os rankings de apropriação indevida de domínios e números de visitas reais em todos os setores. Por exemplo, a alta tecnologia está entre os cinco primeiros para apropriação indevida de domínios, mas cai para o sexto lugar em termos de visitas reais. Da mesma forma, há menos domínios posando como serviços de saúde/farmacêuticos, mas as visitas a esses domínios são maiores.

Phishing para credenciais

A violação de marca assume muitas formas, incluindo websites semelhantes que replicam o logotipo e o design exatos da empresa legítima, aplicativos fraudulentos e perfis falsos de rede social imitando contas corporativas oficiais. Para entender a extensão desse problema, analisamos páginas falsas e as classificamos em tipos: apropriação indevida de marcas, phishing, aplicativos não confiáveis, lojas falsas, violadores de cobrança por conteúdo, além de perfis sociais e de lojas falsos. É importante notar que o domínio de uma única organização pode cair em várias classificações com base nas páginas que monitoramos.

Nossa análise revelou que o phishing é o campeão dos domínios falsificados que estão visando instituições de serviços financeiros, representando impressionantes 68% de todas as instâncias registradas (Figura 10). A apropriação indevida de marcas aparece em segundo lugar, representando 24% de todos os domínios registrados. Entre os websites frequentados pelo usuário, o phishing e a apropriação indevida de marcas novamente se classificam em primeiro e em segundo lugar, respectivamente. Outras formas de violação de marca, como falsos perfis de rede social e de lojas, são menos significativas dentro das instituições financeiras do que em outros setores. Apesar de menos ataques direcionados a aplicativos não confiáveis, é importante notar que os invasores estão adotando métodos cada vez mais criativos para ampliar seu alcance.

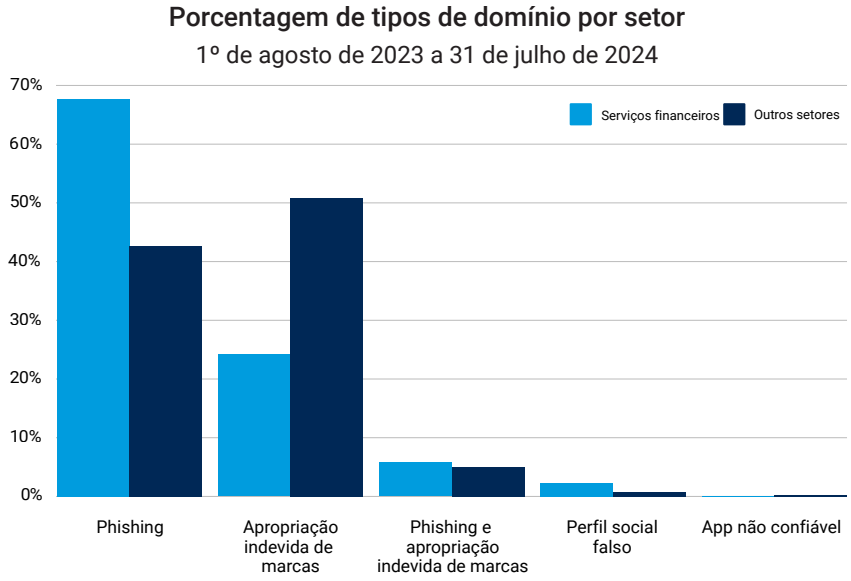


Fig. 10: a maioria dos domínios que registramos para serviços financeiros são websites de phishing, excedendo até mesmo o total de todos os outros setores combinados

As instituições financeiras são vistas como entidades altamente confiáveis, tornando-as alvos principais para fraudadores que exploram essa confiança.

Apesar do aumento da conscientização sobre os riscos representados pelo phishing, o elemento humano continua sendo uma lacuna de segurança significativa. Essa lacuna é exacerbada por técnicas sofisticadas usadas pelos invasores (leia a seção A anatomia da violação de marcas para ver mais detalhes), que dificultam a identificação de uma página falsa pelo olho não treinado. As instituições financeiras são vistas como entidades altamente confiáveis, tornando-as metas principais para fraudadores que exploram essa confiança. Ao se passar por essas instituições, os invasores levam os usuários a entregar suas credenciais de bom grado, aproveitando a reputação da instituição para tornar seus golpes mais convincentes e eficazes.

Para proteger uma organização e seus clientes, é crucial usar tecnologias de segurança com recursos de monitoramento de marca que podem monitorar proativamente qualquer uso não autorizado da marca, seja um nome de domínio, app para dispositivo móvel ou comunicação por e-mail. Uma vez identificados os usos indevidos, o próximo passo é realizar manobras para impedir o tráfego, o que potencialmente expõe os clientes aos perigos (como roubo de dados) causados por violação de marca e phishing.

Estudo de caso: a crescente sofisticação dos ataques de preenchimento de credenciais contra instituições financeiras

Uma empresa de fintech dos EUA sofreu ataques implacáveis de preenchimento de credenciais ao longo de 2023 e 2024 que visavam um de seus aplicativos voltados para o cliente. A magnitude desses ataques é impressionante. Durante um período de 24 horas, a Akamai detectou mais de 3.000 alertas de diferentes endereços IP que estavam tentando se infiltrar em contas usando credenciais roubadas. Observamos um único endereço IP tentando pelo menos 115 combinações de nome de usuário e senha. No total, registramos mais de 100.000 alertas em julho de 2024.

Websites de serviços financeiros fraudulentos em nível crítico de risco

A inteligência exclusiva da nossa edge global, combinada com feeds de dados adicionais de inteligência de ameaças de terceiros, nos dá uma vantagem distinta na detecção de personificações de marcas. Usamos este sistema abrangente para examinar e classificar meticulosamente cada domínio com base em sua pontuação de ameaça.

Calculamos a pontuação da ameaça usando três fatores-chave:

1. **A pontuação de confiança**: nossa certeza de que um evento é uma tentativa de phishing
2. **O nível de gravidade**: o grau de risco (crítico, alto, médio ou baixo) associado a um evento
3. **O fator de frequência**: o número de eventos/sessões associados ao website dentro de um determinado período de tempo

Nosso sistema de pontuação equilibra os três fatores-chave: confiança, gravidade e frequência. Combinamos essas pontuações para gerar uma pontuação de ameaça abrangente para cada domínio suspeito, limitada a 99, para garantir uma avaliação holística das ameaças potenciais.

Nossa análise mais recente revela que o setor de serviços financeiros possui uma pontuação de ameaça mediana alarmante de 85, destacando os riscos significativos que o setor continua enfrentando (Figura 11). Essa pontuação coloca as instituições financeiras diretamente na mira dos cibercriminosos, que estão atacando incansavelmente seus vastos armazenamentos de dados confidenciais.

Pontuações de ameaça por setor

Setor	Pontuação mediana de ameaça	Setor	Pontuação mediana de ameaça
Setor público	**95**	Jogos	**65**
Serviços financeiros	**85**	Fabricação	**64**
Serviços corporativos	**85**	Outras mídias digitais	**62**
Farmacêutica/saúde	**85**	Comércio	**61**
Mídia de vídeo	**71**	Alta tecnologia	**60**

Fig. 11: nosso cálculo de pontuações medianas de ameaças mostra serviços financeiros com uma pontuação alarmantemente alta

Enquanto o setor público registrou a maior pontuação mediana de ameaças, provavelmente devido à sua riqueza de informações confidenciais e recursos de segurança limitados, os serviços financeiros continuam sendo um alvo igualmente atraente, com os invasores atraídos pelo potencial de enorme ganho financeiro. Setores como serviços comerciais e de saúde/farmacêuticos também pontuam de forma semelhante, indicando que os cibercriminosos estão diversificando seus alvos. Mas as instituições financeiras continuam sendo um foco principal devido à natureza crítica de seus dados.

Esse alto nível de ameaça exige ações imediatas para fortalecer as defesas e mitigar as ameaças em evolução antes que elas levem a danos financeiros e à reputação significativos.

A anatomia da violação de marcas

A magnitude das campanhas de phishing e de apropriação indevida é agravada pela existência de kits de ferramentas de phishing.

O sucesso da fraude e da violação de marca depende fortemente do poder da marca como um chamariz de engenharia social. Os invasores capitalizam o senso de familiaridade e a confiança inerente que os consumidores têm em relação a marcas conhecidas, criando websites falsos que imitam quase perfeitamente os legítimos. Em alguns casos, os fraudadores até copiam o código exato, fazendo com que esses websites ilegítimos pareçam quase idênticos aos reais. Com o surgimento de ferramentas de IA generativas, que ajudam os fraudadores a eliminar erros ortográficos e gramaticais, tornou-se ainda mais difícil para os consumidores distinguir entre websites autênticos e falsos.

A magnitude das campanhas de phishing e de apropriação indevida é agravada pela existência de kits de ferramentas de phishing. Por menos de US$ 50, os invasores podem comprar kits de ferramentas de phishing que lhes permitem criar websites de phishing convincentes. A empresa cibercriminosa de desenvolvimento, criação e venda de kits de ferramentas de phishing reduz significativamente a barreira de entrada para a realização de campanhas de phishing e de apropriação indevida. Kr3pto e 16Shop são dois exemplos de kits de ferramentas de phishing predominantes. A Kr3pto visou os bancos do Reino Unido ignorando a autenticação de dois fatores, enquanto a 16Shop se concentrou em grandes marcas como PayPal e Amazon, entre outras. Em agosto de 2023, uma operação internacional de aplicação da lei resultou na prisão dos criadores da 16Shop. Esses casos destacam a sofisticação evolutiva dos ataques de phishing e os esforços coordenados para combater o crime cibernético.

Subestimado, mas eficaz: combosquatting

Outra faceta importante da violação de marca é o uso de nomes de domínio que se assemelham a websites legítimos. Normalmente, os invasores registram seus domínios depois de comprar ou construir seu próprio website de phishing. É aqui que técnicas testadas e aprovadas como o cybersquatting e suas muitas variantes desempenham um papel importante. Uma tática comum é o typosquatting, no qual os invasores registram um domínio com uma ortografia ligeiramente incorreta do nome da empresa (por exemplo, acamai[.]com), esperando que o consumidor faça um erro de digitação. Outro método, o combosquatting, envolve adicionar palavras-chave extras, como "suporte", "login" ou "ajuda", ao nome de domínio. Essa tática aproveita os microsites frequentemente encontrados em websites legítimos da empresa.

De acordo com a pesquisa Akamai, apesar de ser uma tática subnotificada, o comboquatting (a adição de uma palavra-chave) excede o typosquatting (a adição, remoção ou substituição de um caractere) no número de domínios ativos. Curiosamente, "com" surgiu como uma das principais palavras-chave adicionadas em websites fraudulentos.

Mecanismo de distribuição

Websites falsificados e de phishing são entregues e impingidos por meio de vários mecanismos, o principal entre eles é o e-mail. Essas mensagens de e-mail parecem convincentes através do uso de um logotipo legítimo e contêm mensagens urgentes, como solicitações para atualizar as informações da conta. No entanto, o abuso de marca não se limita a websites e e-mails, os invasores também espalham ameaças por meio das redes sociais, expandindo ainda mais seu alcance e táticas de engodo.

Ocultos (links) à plena vista

Existem outras táticas observadas no meio real que dificultam ainda mais para os consumidores identificarem um website de apropriação indevida e que podem aumentar a taxa de sucesso desses ataques. Por exemplo, o uso de URLs encurtados, códigos QR, hiperlinks de imagem e links de texto em SMS ofuscam os links mal-intencionados. Ao contrário do e-mail com filtros de spam que fornecem proteção contra esse abuso, os golpes de texto provavelmente não são bloqueados e têm maior chance de serem lidos ou abertos.

Existem outras táticas observadas no meio real que dificultam ainda mais para os consumidores identificarem um website de apropriação indevida e que podem aumentar a taxa de sucesso desses ataques.

Ataques regionais de phishing e apropriação indevida de marcas em serviços financeiros

A violação de marcas afeta organizações e consumidores em todo o mundo, mas algumas regiões apresentam uma maior vulnerabilidade à fraude e a violação devido à concentração de tráfego para websites de apropriação indevida de marcas e phishing. Nossa análise revela que a região EMEA experimentou o maior volume de tráfego para websites de phishing e de apropriação indevida detectados nos últimos 12 meses, superando até mesmo os na América do Norte (Figura 12). Este ranking abrange serviços financeiros e outros setores.

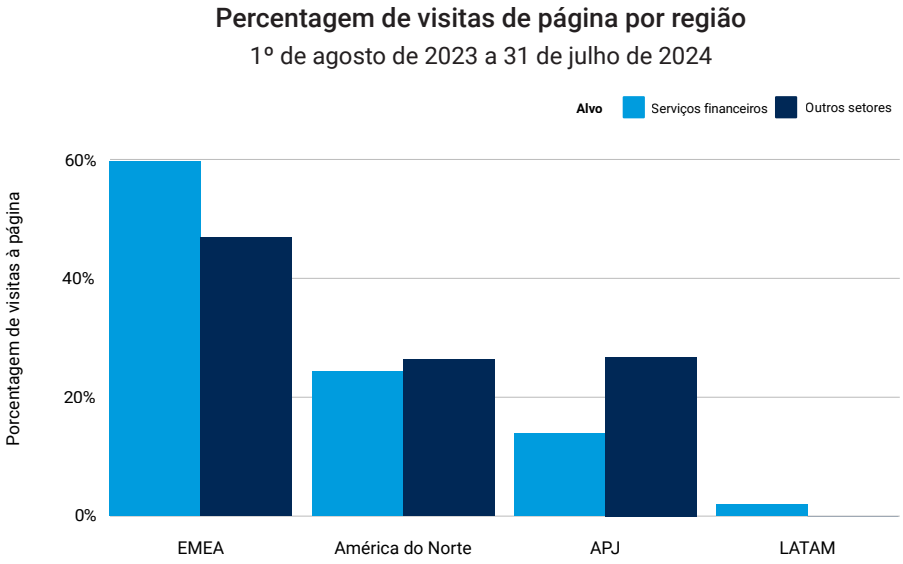
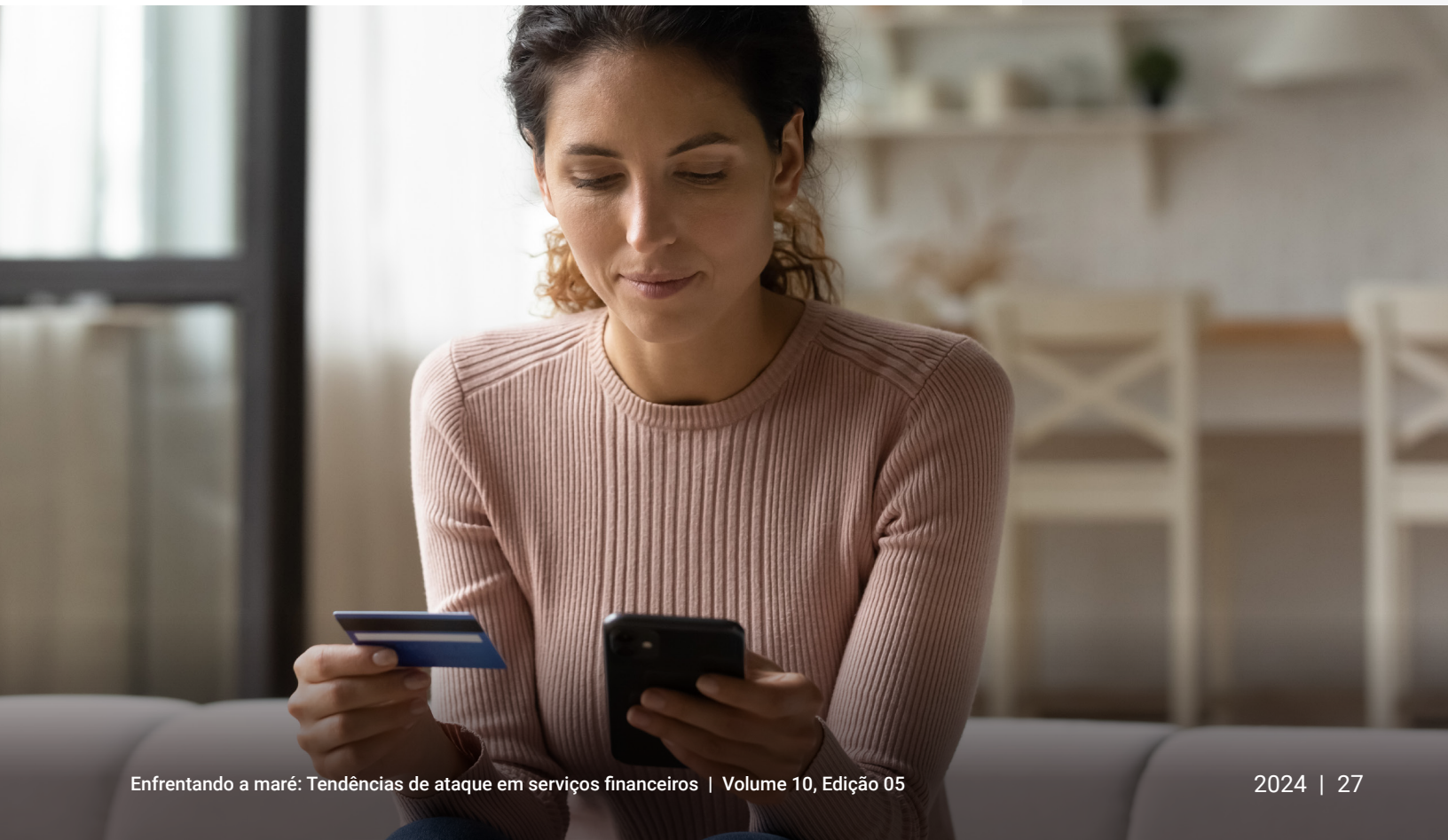


Fig. 12: a EMEA ultrapassou a América do Norte como a região mais afetada pelo phishing e violação de marca em serviços financeiros

Embora as regiões da América Latina e Ásia-Pacífico e Japão (APJ) tenham registrado um número relativamente menor de visitas a páginas, isso não indica menos ataques. Em vez disso, essas descobertas provavelmente refletem a concentração de marcas globais com grandes bases de clientes na América do Norte e na EMEA. Isso cria uma maior quantidade de potenciais vítimas para adversários. Também podemos atribuir essa descoberta ao surgimento de kits de ferramentas de phishing como V3B, que tem especificamente visado os bancos da UE desde 2023.

Embora a EMEA ultrapasse a maioria das regiões em número de domínios suspeitos e visitas de página, a APJ tem a maior pontuação mediana de ameaça: 97. A América Latina, apesar de ter o menor número de visitas a websites, recebe uma surpreendente pontuação mediana de ameaça de 94. Isso indica que os consumidores na América Latina e na região APJ estão em maior risco de ter suas informações bancárias e outros dados confidenciais roubados ao visitar websites.

Vários fatores contribuem para o aumento dos perigos de violação de marca contra serviços financeiros na APJ. Primeiro, a maioria das instituições de serviços financeiros da APJ está altamente digitalizada, quase todas as ofertas de serviços podem ser feitas online sem nunca visitar uma filial física. A taxa de penetração da Internet e a adoção digital na APJ é uma das mais altas globalmente, tornando essa região um alvo atraente para os cibercriminosos aproveitarem. Em segundo lugar, essa região abriga alguns dos países mais ativos do mundo nas redes sociais. E as instituições de serviços financeiros intensificaram o engajamento dos clientes por meio dessas plataformas para competir por participação de mercado e ganhar uma melhor fidelidade do cliente. O uso generalizado de aplicativos de rede social e mensagens na região APJ proporciona aos cibercriminosos vetores adicionais para promover ataques de phishing e de apropriação indevida, muitas vezes abusando da confiança que as pessoas depositam nessas plataformas.



Evolução da conformidade: como as regulamentações globais de cibersegurança estão moldando as instituições financeiras

Quando perguntado por que roubava bancos, o conhecido ladrão de bancos Willie Sutton deu uma resposta famosa: "Porque é aí que o dinheiro está". A declaração de Sutton, é claro, pode ser facilmente aplicada a ataques cibernéticos contra instituições financeiras hoje em dia. A motivação do ganho financeiro, no entanto, conta apenas uma parte da história. As instituições financeiras encontram-se cada vez mais na mira de invasores que são motivados por preocupações políticas, bem como por motivos estratégicos geopolíticos. Essas motivações, aliadas ao fato de que "é aí que o dinheiro está", criam uma combinação perfeita para os ataques às instituições financeiras, pois elas saem na frente como o setor mais atacado da indústria.

Isso não deveria nos surpreender. O setor financeiro sempre desempenhou um papel crucial e central na sociedade e tem sido objeto de regulamentação significativa. Embora a regulamentação das instituições financeiras no passado tenha se concentrado em proteger os clientes em suas relações com as instituições financeiras, os órgãos reguladores estão agora buscando aplicar a segurança crítica no âmbito da infraestrutura e regulamentação de resiliência a instituições financeiras e empresas de serviços. Esta tendência mais recente inclui requisitos não só para a própria instituição financeira, mas também para os seus fornecedores de tecnologia de informação e comunicação (TIC).

Existem inúmeros exemplos de regulamentos de cibersegurança e resiliência operacional. Na União Europeia, a DORA (Lei de Resiliência Operacional Digital) determina que as entidades financeiras e seus fornecedores tenham estruturas sólidas de gestão de risco de TIC e realizem testes contínuos e emitam relatórios de incidentes. Nos Estados Unidos, a SEC (Securities and Exchange Commission) introduziu regulamentos de materialidade cibernética que exigem que empresas públicas, incluindo instituições financeiras, divulguem incidentes cibernéticos que poderiam impactar de forma relevante suas operações. Na Austrália, a APRA (Australian Prudential Regulation Authority, Autoridade Australiana de Regulação Prudencial) estabeleceu normas exigindo que as entidades mantenham recursos de segurança da informação compatíveis com o tamanho e a extensão das ameaças aos seus ativos de informação (regulamento CPS 234). Esses exemplos ilustram a tendência global para melhorar a cibersegurança e a resiliência operacional dos setores financeiros para proteger contra os riscos em evolução e garantir a estabilidade financeira.

Tendo em conta esses regulamentos, compete às instituições financeiras realizar as devidas averiguações ao comprar serviços de TIC e segurança para garantir que os fornecedores cumpram esses padrões de desenvolvimento rigorosos. Elas devem escolher fornecedores que não só prestem um serviço resiliente, mas que também entendam as regulamentações relevantes, forneçam a visibilidade necessária para identificar e mitigar ameaças em evolução e ajudem a aplicar essa inteligência às operações em curso.

A visibilidade é fundamental porque você não pode proteger o que não sabe que tem (ou com o que você se conecta) e você não pode se proteger contra uma ameaça que não sabe que existe. Serviços como a Plataforma Akamai Guardicore fornecem não apenas proteções contra ataques, mas também ajudam os clientes a entender fluxos de dados, identificar anomalias e segmentar adequadamente ativos de rede para mitigar ameaças. Da mesma forma, seus serviços de segurança de APIs são projetados para identificar o tráfego de APIs para ajudar com APIs sombra, bem como reconhecer possíveis ataques por meio de APIs.

Talvez os bancos devam adicionar visibilidade à tríade tradicional CIA (confidencialidade, integridade, disponibilidade) para refletir essa nova tendência: a VCIA — visibilidade, confidencialidade, integridade e disponibilidade.

James Casey
Vice-presidente, diretor de privacidade,
Akamai

Aumento das defesas com o Zero Trust

A confiança forma a base sobre a qual as instituições financeiras constroem sua reputação. No entanto, quando se trata de proteger ambientes complexos e dados confidenciais, a confiança pode facilmente se tornar uma desvantagem significativa. Os adversários muitas vezes aproveitam a confiança implícita de inúmeras maneiras, incluindo:

- Ataques de phishing para se passarem por indivíduos dentro da organização
- Ataques que exploram vulnerabilidades de segurança em fornecedores terceirizados para acessar alvos de alto valor
- Ameaças internas que abusam do acesso para fins nefastos

A crescente sofisticação dos ataques tornou a segurança tradicional baseada em perímetro inadequada, pois ela considera todo o tráfego de dentro como confiável. Considerando os altos riscos nos serviços financeiros, manter uma postura de segurança resiliente é fundamental. É aqui que a estrutura Zero Trust se torna obrigatória. Essa abordagem de segurança opera com o princípio de que qualquer solicitação de conexão, usuário ou dispositivo é um perigo potencial. Ela implementa a verificação contínua e remove a confiança implícita, negando o acesso aos recursos por padrão, a menos que o solicitante seja autenticado e autorizado.

O Zero Trust aumenta a conformidade com os requisitos regulamentares em evolução para as instituições financeiras, garantindo sistemas que lidam com dados regulamentados, permitindo assim que uma organização evite penalidades de reprovação de auditorias. Ele fornece controles adicionais para sistemas legados, oferecendo visibilidade granular para detectar usuários não autorizados que estão tentando acessar aplicativos críticos.

O modelo Zero Trust restringe o tráfego horizontal, limitando o acesso da rede a sistemas críticos e impedindo o movimento lateral de ameaças como ransomware. Essa estratégia de contenção protege dados e ativos essenciais isolando sistemas infectados. Como o número de ataques de ransomware em serviços financeiros aumentou significativamente, a importância do Zero Trust na proteção de informações confidenciais não pode ser ignorada. Com sua visibilidade granular, o Zero Trust ajuda você a detectar e neutralizar ameaças em ambientes complexos, o que é crucial para evitar a disseminação de ransomware e proteger ativos críticos.

Outra vantagem crucial do Zero Trust é sua capacidade de proteger fluxos de dados entre aplicativos, o que é essencial para a implantação segura de aplicativos baseados em nuvem. Isso não só facilita a modernização, mas também garante a proteção de informações confidenciais em um cenário de ameaças em constante mudança, permitindo que as instituições financeiras inovem sem comprometer a segurança. A implementação de uma estrutura Zero Trust aumenta a postura de segurança e prepara uma instituição para o futuro contra ameaças em evolução.

A segmentação é boa. A microssegmentação é melhor.

A segmentação é uma abordagem arquitetônica que divide uma rede em segmentos menores com o objetivo de melhorar o desempenho e a segurança. A microssegmentação é uma técnica de segurança que permite dividir logicamente uma rede em segmentos de segurança distintos até o nível da carga de trabalho individual. Os controles de segurança e a prestação de serviços podem então ser definidos para cada segmento exclusivo.

A microssegmentação também é a espinha dorsal do Zero Trust. Em um relatório recente da Akamai, os líderes de cibersegurança de serviços financeiros citaram o avanço do Zero Trust como o motor mais frequente da implementação de um projeto de segmentação. Na realidade, quase todos os líderes que segmentaram estão implantando ou já implantaram uma estrutura de segurança Zero Trust (99%), embora menos da metade (47%) informe que essa estrutura está totalmente completa e definida e, portanto, madura.

A microssegmentação funciona com sistemas existentes e é implantada mais rapidamente que os métodos tradicionais, como firewalls. Essa abordagem acelera a resposta de ransomware em até 13 horas e simplifica o gerenciamento em todos os ambientes de TI. Ela também ajuda a atender às necessidades de conformidade por meio de controle de dados preciso.

Um exemplo do mundo real mostra o impacto da microssegmentação moderna: um projeto reduziu o tempo de implementação de 2 anos para 6 semanas, usou apenas um engenheiro e reduziu os custos em 85%. Esse caso ilustra como a microssegmentação pode economizar tempo e dinheiro das organizações. Os diretores de TI devem comparar esses resultados com seus custos de segurança e tempo de implementação atuais.

Para fortalecer sua postura de cibersegurança, as instituições financeiras devem priorizar a implementação de estratégias avançadas de segmentação. Os CISOs devem liderar esforços para alinhar as medidas de segurança com os padrões da indústria em evolução, integrando a microssegmentação como o pilar de uma arquitetura robusta do Zero Trust. Os diretores de TI devem estabelecer uma cadência de auditorias de segurança contínuas e de atualizações de estratégia para garantir que suas defesas permaneçam resilientes contra ciberameaças sofisticadas.

Essa abordagem proativa não só ajuda a mitigar as vulnerabilidades atuais, mas também posiciona as organizações para combater de forma eficaz os desafios emergentes da cibersegurança. Ao adotar essas medidas, as instituições financeiras criam uma estrutura de segurança abrangente que aborda preocupações imediatas e gestão de risco a longo prazo.

[A microssegmentação] não só ajuda a mitigar as vulnerabilidades atuais, mas também posiciona as organizações para combater eficazmente os desafios emergentes da cibersegurança.

Mitigação

Quando se trata de proteger sua instituição financeira de várias ciberameaças, você precisa implementar uma abordagem multifacetada. Vamos explorar as principais estratégias de mitigação para phishing, apropriação indevida de marcas, ataques de DDoS e ransomware.

Proteção contra phishing e apropriação indevida de marcas

Para proteger sua instituição contra phishing e apropriação indevida de marcas, considere usar serviços de proteção de marca de terceiros para detectar e remover conteúdo fraudulento rapidamente. Também é importante instruir seus funcionários e clientes. Realize treinamento regular de conscientização de segurança para sua equipe sobre como reconhecer tentativas de phishing e de apropriação indevida. Forneça orientações claras sobre como identificar comunicações legítimas da sua instituição. Estabeleça um plano de resposta rápida para tentativas de apropriação indevida, incluindo um processo para notificar parceiros e clientes sobre fraudes de identidade.

Além disso, implemente estas técnicas de proteção:

- Registre nomes de domínio semelhantes para evitar o typosquatting e use serviços de monitoramento de domínio para detectar domínios semelhantes.
- Fortaleça os protocolos de autenticação usando senhas e gerenciadores de senhas fortes e exclusivos e implemente autenticação multifator (MFA) para todas as contas e sistemas.
- Implemente protocolos de autenticação de e-mail, como o SPF (Sender Policy Framework), o DKIM (DomainKeys Identified Mail) e a DMARC (Autenticação, Relatórios e Conformidade de Mensagens Baseadas em Domínio) para evitar a falsificação de e-mails. Use soluções anti-phishing e filtragem avançada de e-mail para detectar e bloquear e-mails mal-intencionados.
- Proteja seu website e canais digitais obtendo certificados SSL (Secure Sockets Layer), implementando HTTPS e usando ferramentas antifraude para detectar atividades suspeitas em seu website e aplicativos móveis.
- Proteja os canais de comunicação fornecendo portais seguros e implementando mensagens criptografadas para correspondência confidencial.

Proteção contra DDoS

Proteger sua instituição financeira contra ataques de DDoS requer uma estratégia de defesa em várias camadas. Implemente estratégias proativas, como o uso de produtos especializados de detecção, mitigação e proteção contra DDoS; configuração de limitação de taxa; e armazenamento de conteúdo em cache em uma CDN (Rede de Entrega de Conteúdo). Além disso, mantenha-se informado sobre medidas de segurança, como gerenciamento de patches, planos de resposta a incidentes, controles de mitigação para endereços IP expostos a DDoS e sub-redes críticas, políticas de controle de acesso, segmentação de rede e firewalls. Implemente estratégias proativas, como configurar limitação de taxa; armazenar conteúdo em cache em uma CDN (Rede de Entrega de Conteúdo); e usar produtos especializados de detecção, mitigação e proteção contra DDoS.

Para proteger sua infraestrutura de DNS, monitore e analise continuamente o tráfego de DNS de entrada e use uma plataforma híbrida em vez de um firewall de DNS tradicional. Entender as táticas, técnicas e procedimentos usados pelos invasores ajudará você a se proteger melhor contra ataques de DDoS.

Proteção contra ransomware

Como mencionado anteriormente neste relatório, alcançar o Zero Trust com segmentação de rede, especialmente a microssegmentação, é essencial para limitar a disseminação de ransomware em toda a sua instituição financeira. A implementação de medidas robustas de cibersegurança, como essa, ajudará a combater as técnicas avançadas que os invasores de ransomware estão utilizando. Além disso, seja vigilante e use a estrutura MITRE ATT&CK para obter insights sobre táticas e técnicas predominantes usadas pelos invasores e fortalecer seus manuais adequadamente para quebrar a cadeia de destruição de ransomware.

Atualize continuamente suas defesas e instrua sua equipe para reconhecer e responder efetivamente a ameaças potenciais. Incorpore defesas de perímetro fortes, proteção de ponto de extremidade, filtragem de e-mail e gerenciamento regular de patches. Estabeleça monitoramento contínuo do tráfego de rede, logs do sistema e comportamento do usuário e implemente práticas de detecção de ameaças para identificar proativamente ameaças de ransomware.

Implemente backups de dados regulares e seguros, incluindo backups isolados, para garantir que as informações críticas possam ser restauradas rapidamente em caso de um ataque de ransomware. Implemente a MFA para todas as contas de usuário para adicionar uma camada extra de segurança.

Ao implementar essas estratégias abrangentes de mitigação, você pode melhorar significativamente a capacidade de sua instituição financeira de se defender contra várias ciberameaças, garantir a continuidade operacional, proteger sua reputação e preservar a confiança do cliente.

Conclusão

À medida que sua instituição financeira adapta a transformação digital para melhorar a experiência do cliente, a eficiência operacional e o posicionamento competitivo, os desafios de segurança se intensificam, juntamente com a pressão crescente para navegar em um cenário regulamentar em evolução. Nesta edição do relatório SOTI, exploramos as ameaças persistentes e emergentes que o setor de serviços financeiros está enfrentando, ressaltando a necessidade de avaliação contínua e aprimoramento de soluções de segurança. À medida que as ameaças se tornam mais sofisticadas, é fundamental manter-se à frente, fortalecendo as defesas e refinando as estratégias de segurança.

Com os ataques de DDoS em instituições financeiras superando agora os do setor de jogos, há muito tempo considerado o principal alvo, essa tendência alarmante ressalta os riscos crescentes. Fatores como o hacktivismo e o clima geopolítico tornaram os serviços financeiros mais vulneráveis do que nunca. Em paralelo, a escala e a gravidade do tráfego gerado por websites de apropriação indevida de marcas e phishing que visam instituições financeiras, juntamente com a velocidade com que os invasores podem gerar novos domínios após os websites iniciais serem derrubados, são notáveis. O rastreamento dessas atividades pode ter um uso intenso dos recursos das organizações, e as equipes de segurança precisam de soluções que incluem serviços de remoção, inteligência de ameaças e detecção de apropriação indevida de marcas e phishing em vários canais digitais.

Os consumidores e reguladores muitas vezes responsabilizam as instituições financeiras, mesmo quando não são diretamente culpadas, após serem vítimas de phishing e outros golpes. Mais importante, o phishing e a apropriação indevida de marcas frequentemente servem como precursores de ataques mais perigosos, tornando crucial interromper o ciclo de ataque antecipadamente. Tomar medidas decisivas pode significar a diferença entre se tornar a notícia dos jornais de amanhã devido a uma violação e proteger a reputação da sua instituição e a confiança do cliente.

Dada a natureza implacável dos ataques contra as instituições financeiras, a proteção de informações confidenciais para evitar fraudes e abusos continua a ser um enorme desafio. Adotar uma estrutura de segurança como o Zero Trust é essencial para se defender efetivamente contra ataques de phishing que visam funcionários e impedir que ransomware se espalhe dentro das redes para alcançar ativos críticos, tudo isso garantindo a conformidade com as regulamentações globais existentes e emergentes.

Este relatório fornece insights acionáveis sobre as últimas tendências de ataque no setor de serviços financeiros, capacitando você a fortalecer suas defesas. Mantendo-se vigilante e implementando as estratégias descritas neste relatório, você pode proteger melhor sua organização e seus clientes do crescente cenário de ameaças.

Fique por dentro das nossas pesquisas mais recentes conferindo nosso hub de pesquisa de segurança.

Metodologia

DDoS (camada 7)

Esses dados descrevem alertas da camada de aplicativo sobre o tráfego observado através do nosso firewall de aplicativos da Web (WAF). Os alertas de DDoS L7 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.

DDoS (camadas 3 e 4)

O Prolexic Routed da Akamai defende as organizações contra ataques de DDoS interrompendo os ataques e outros tráfegos indesejados ou mal-intencionados antes que atinjam aplicativos, data centers e infraestrutura de nuvem e híbrida voltada para a Internet (pública ou privada), incluindo todas as portas e protocolos. Os especialistas do SOCC (Centro de comando de operações de segurança) da Akamai personalizam controles proativos de mitigação para detectar e interromper ataques instantaneamente, além de realizar análises em tempo real do tráfego restante para determinar se é necessário adotar mais medidas de mitigação. Esses ataques mitigados são organizados e agrupados em eventos de ataque, e todos os dados associados são registrados pelo SOCC para serem analisados.

Esses dados neste relatório cobriram o período de 18 meses de 1° de janeiro de 2023 a 30 de junho de 2024, salvo indicação em contrário.

Ataques de apropriação indevida de marcas

O Akamai Brand Protector é uma solução antiviolação projetada para proteger as empresas e seus clientes contra ataques de apropriação indevida de marcas, como phishing, websites falsificados, contas sociais falsas e aplicativos não confiáveis. Ele usa a rede de edge global da Akamai, analisando mais de 900 TB de dados diariamente, para detectar ameaças antes que elas afetem os clientes. Essa inteligência é aprimorada com feeds de terceiros de parceiros para oferecer uma visão ampla das ameaças potenciais em várias plataformas online.

Várias caraterísticas de cada domínio suspeito detectado são analisadas, e seus níveis determinados de risco contribuem para a pontuação de ameaça calculada do domínio. Esses domínios suspeitos são monitorados, os dados associados são rastreados e os clientes afetados são alertados sobre essas campanhas mal-intencionadas que tentam explorar a identidade da marca.

Os dados neste relatório cobriram domínios suspeitos detectados no período de 12 meses de 1° de agosto de 2023 a 31 de julho de 2024.

Créditos

Diretor de pesquisa

Mitch Mayne

Editorial e redação

James Casey
Badette Tribbey
Lance Rhodes

Análise e contribuição da matéria

Cheryl Chiodi
Gal Meiri
Ziv Eli
Richard Meeus
Reuben Koh
Steve Winterfeld

Análise de dados

Chelsea Tuttle

Materiais promocionais

Barney Beal

Marketing e publicação

Georgina Morales
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.
www.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 serviços financeiros, visite nossa **página de serviços financeiros**.

Publicado em 09/24.