Volume 5, 6ª edição

[state of the internet]/segurança

Um ano em análise

Sumário

01 Carta do Editor

02 12 Meses da Akamai Research

03 Outubro de 2018

03 Novembro de 2018

04 Dezembro de 2018/Janeiro de 2019

05 Fevereiro de 2019

07 Março de 2019

07 Abril de 2019

08 Maio de 2019

08 Junho de 2019

10 Julho de 2019

11 Agosto de 2019

11 Setembro de 2019

13 Olhando para o futuro

14 Apêndice

24 Créditos

Carta do Editor

Martin McKeay
Diretor editorial

No final de 2019, queremos agradecer a vocês, leitores, por continuarem a apoiar o relatório SOTI (State of the Internet)/Segurança da Akamai. Tanto a equipe quanto o relatório evoluíram significativamente este ano, e planejamos continuar a crescer e a evoluir nos próximos anos. Queremos que seja um relatório para o qual você retorne várias vezes para fazer pesquisas importantes.

Por que a Akamai produz o relatório SOTI e realiza pesquisas de segurança em geral?

De um ponto de vista interno, o relatório SOTI e suas pesquisas são excelentes materiais de marketing. Uma boa pesquisa traz boas histórias, e boas histórias geram conscientização sobre o que uma empresa considera importante. De certa forma, o tipo de pesquisa que qualquer empresa de segurança publica é quase tão importante para construir sua reputação quanto os tipos de produtos que ela vende.

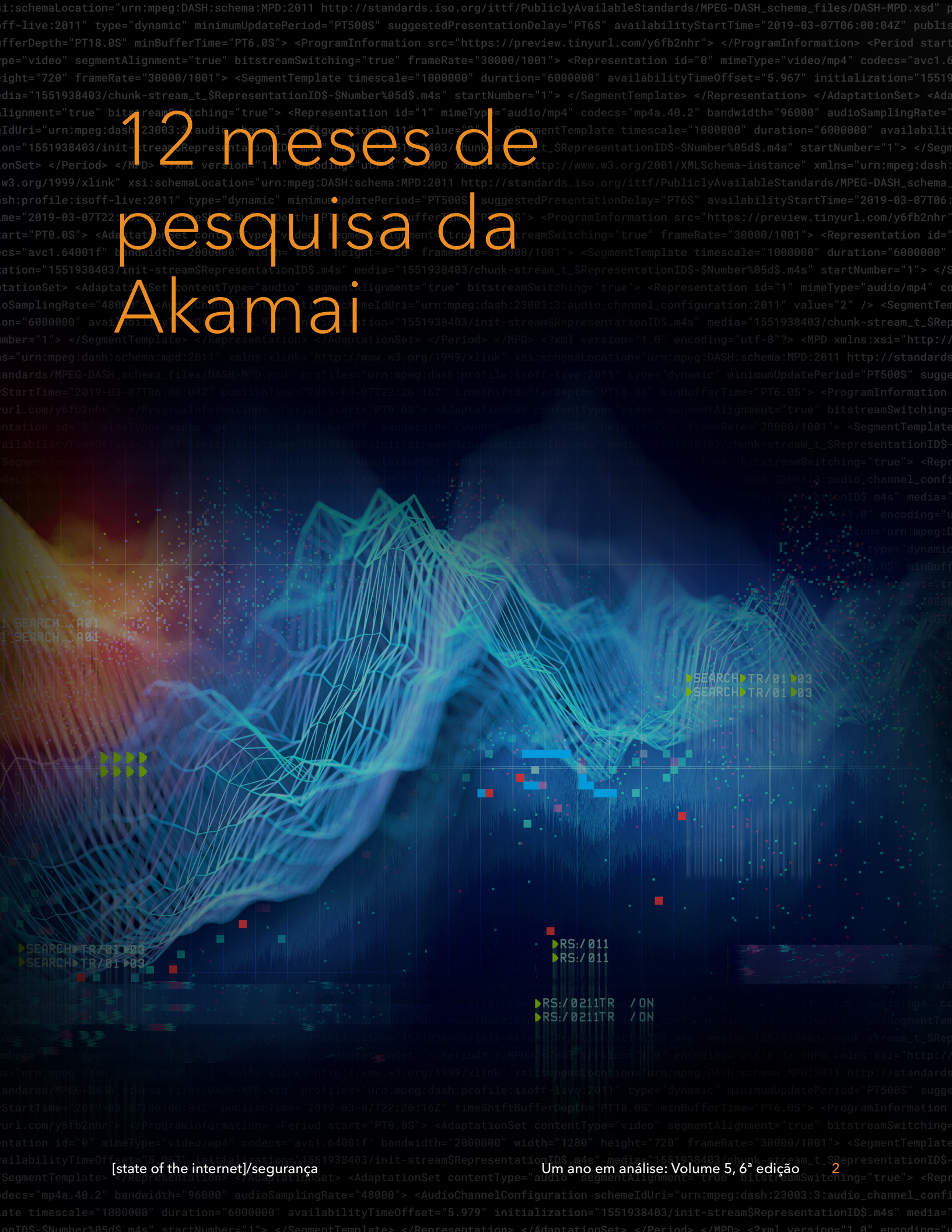
Por que um grupo global de pesquisadores acredita no valor da pesquisa e da publicação? A maioria das respostas individuais que recebemos pode ser resumida em dois motivadores. Primeiro, ser reconhecido como líder e fonte de inteligência no campo escolhido é bom, não importa quem você seja. Segundo, o trabalho que nossas equipes estão fazendo é importante. A área da segurança ainda é jovem, e cada informação, cada porção de sabedoria que contribui para o conhecimento global, é valiosa.

Para a minha equipe – os redatores, cientistas de dados e editores que desenvolvem o relatório e muito mais – nosso trabalho é a nossa paixão. Juntos, temos mais de quatro décadas de experiência em segurança. Percebemos o quanto resta a descobrir e o pouco que essa descoberta é quantificada. Trabalhar com nossos pesquisadores nos permite fazer a diferença, tornando o trabalho deles acessível e interessante para você.

O relatório SOTI foi originalmente baseado apenas em ataques DDoS e a aplicações Web, mas nós o desenvolvemos para cobrir uma ampla variedade de problemas de segurança urgentes. À medida que a Akamai continua sua própria evolução como uma empresa de segurança, os tipos de dados que temos disponíveis só aumentarão. Já começamos a nos planejar para 2020, em todos os sentidos da palavra.

Vocês, nossos leitores, são importantes para nós. Sem vocês, este relatório não existiria. Obrigado por lê-lo, e esperamos que continuem a encontrar valor em nossos relatórios no ano que se aproxima. Recebemos de braços abertos seu feedback e suas perguntas.

12 meses de pesquisa da Akamai



As importantes histórias dos últimos 12 meses

Bem-vindo ao sexto relatório SOTI (State of the Internet)/Segurança do ano. Com o final de 2019 se aproximando, queremos olhar para trás e examinar as pesquisas que a Akamai fez nos últimos 12 meses. Desde o início de outubro de 2018 até o final de setembro de 2019, prestamos atenção especial às pesquisas que saíram da SIRT (Equipe de Resposta de Inteligência de Segurança) da Akamai. Além disso, destacamos uma seleção das notícias mais importantes que afetaram o setor de segurança no ano passado.

Pode parecer clichê dizer que está sendo um ano interessante, mas é verdade. Mais do que nunca, as histórias sobre segurança se tornaram cada vez mais importantes e estão se tornando parte das principais notícias. Com as eleições preocupando a maior parte da população dos Estados Unidos, esperamos que a segurança desempenhe um papel ainda maior no ano que vem por aí.

Outubro de 2018

Que mês! Começou com uma violação de dados que afetou milhões de pessoas no Facebook. Um pouco depois, a Bloomberg publicou uma história centrada nos hacks da cadeia de suprimentos de estados-nações. Cada fornecedor na história, bem como o Departamento de Segurança Interna dos EUA, rejeitou as afirmações, mas a Bloomberg se manteve firme com suas notícias.

Outubro também foi um mês movimentado para nossas equipes de segurança. Ryan Barnett, da Akamai, publicou uma postagem no blog sobre cabeçalhos de resposta de segurança e por que líderes de negócios e gerentes de segurança devem se importar com eles. Um dia depois, Larry Cashdollar publicou uma análise do kit de phishing Luis, incluindo algumas de suas técnicas de evasão.

Cashdollar também quebrou as notícias sobre a vulnerabilidade de carregamento do arquivo jQuery (CVE-2018-9206). Embora o problema tenha sido resolvido, as ramificações do código e o uso reciclado espalham seu impacto em outras bases de código. Isso significava que o problema tinha potencial para afetar 7.800 projetos. Em uma publicação de acompanhamento, Cashdollar testou 1.000 projetos ramificados usando o código jQuery, e descobriu que 970 deles estavam vulneráveis.

Com as eleições preocupando a maior parte da população dos Estados Unidos, esperamos que a segurança desempenhe um papel ainda maior no ano que vem por aí.

Novembro de 2018

Novembro começou com a notícia de que a Biblioteca do Congresso e o Escritório de Direitos Autorais dos EUA haviam dado isenções à DMCA (Digital Millennium Copyright Act). Uma isenção permite que os pesquisadores exponham falhas no software sem medo de processos criminais. Essa notícia foi seguida por relatos de que cerca de 60 milhões de cartões de pagamento dos EUA foram comprometidos entre 2017 e 2018, e 93% deles foram habilitados para EMV.

Neste meio tempo, Kaan Onarlioglu, da Akamai, publicou um blog para discutir avaliações de vulnerabilidades de terceiros na Akamai Intelligent Edge Platform e a existência de resultados falsos positivos que poderiam gerar confusão. Logo depois, Ryan Barnett publicou um relatório detalhado sobre as providências a serem tomadas para se proteger contra ataques Magecart e Or Katz publicou uma análise detalhada de um golpe de phishing com 78 variações diferentes. O software Magecart continua sendo uma ameaça significativa à medida que encerramos 2019, em grande parte devido às vulnerabilidades tanto no software quanto em plug-ins de terceiros usados em muitos websites.

Dezembro de 2018/Janeiro de 2019

Até o final de 2018, as equipes de publicação e pesquisa também deram os toques finais no primeiro relatório State of the Internet/Segurança para 2019, publicado em 30 de janeiro. Parece que pesquisadores, e até mesmo criminosos, tiveram uma folga em dezembro.

Antes que o relatório SOTI fosse à público, Larry Cashdollar publicou um blog focado na vulnerabilidade do ThinkPHP (CVE-2018-20062), que foi descoberta enquanto estava pesquisando sobre ataques de skimming da Magecart. Lukasz Orzechowski seguiu esse post, falando sobre um experimento com ferramentas CAT (Computer-Aided Translation, Tradução assistida por computador). Traduções entre idiomas são difíceis, especialmente quando você está traduzindo um script de computador com escrita técnica.

State of the Internet/Segurança: Volume 5, 1ª edição

Ataques DDoS e a aplicações

Esse tema explorou a saúde mental, com um artigo de Amanda Berlin. Desde janeiro, o número de workshops sobre Mental Health Hackers em conferências de segurança aumentou nos Estados Unidos.

Nós nos aprofundamos em um incidente que, à primeira vista, parecia um enorme ataque DDoS, com mais de 4 bilhões de solicitações, em mais de 15.582 endereços IP. No entanto, "o ataque que não foi" acabou sendo uma aplicação com defeito.

Também exploramos o tópico dos bots de varejo e como as aplicações AIO (All-in-One) podem afetar seriamente as vendas e promoções on-line. Embora nem todos os bots sejam ruins, alguns podem certamente ser mais problemáticos do que valem.

Em resumo

- Problemas de saúde mental custam às empresas dos EUA mais de **US$ 190 bilhões** por ano em lucros perdidos.
- Às vezes, um "ataque" não é exatamente o que parece. Especialistas no SOCC da Akamai observaram **4 bilhões de solicitações** impactando um website importante e interferindo na real causa.
- **Os bots geram muito dinheiro para os invasores**, e eles estão em constante evolução para burlar novas defesas. Um invasor ofereceu US$ 15.000 em sua pesquisa para desenvolvedores com experiência em buscar defesas específicas para empresas.

Fevereiro de 2019

Fevereiro foi frio, assim como o ciclo de notícias. No entanto, houve algumas histórias interessantes, incluindo um caso de alguém que registrou uma ação judicial contra a Apple por forçar a autenticação de dois fatores em contas de usuário.

Uma carta de notificação de incidente arquivada no Gabinete do Procurador Geral de Vermont [PDF] também chamou atenção. O incidente em questão foi mais um ataque de preenchimento de credenciais que visava os usuários da TurboTax, do que uma violação dos sistemas da Intuit. Exemplos como esse são um dos motivos pelos quais a autenticação multifator e o preenchimento de credenciais foram temas que a Akamai acompanhou ao longo de 2019. Outro motivo é o grande volume de ataques de preenchimento de credenciais que a Akamai continua a ver.

Pouco antes da segunda edição do relatório SOTI ter sido publicada este mês, Larry Cashdollar publicou uma postagem no blog examinando o uso do Google Tradutor em ataques de phishing contra o Facebook. LPT: Não provoque pesquisadores com tentativas de phishing, pois eles ganham a vida se aprofundando em padrões estranhos e incomuns.

A autenticação multifator e o preenchimento de credenciais foram temas que a Akamai acompanhou ao longo de 2019.

State of the Internet/Segurança: Volume 5, 2ª edição

Ataques ao varejo e tráfego de API

Essa foi a primeira vez no ano em que a Akamai mergulhou em nossos dados de preenchimento de credenciais. Até o momento em que este relatório foi apresentado, a Akamai havia observado 10 bilhões de tentativas de preenchimento de credenciais contra o setor de varejo entre maio e dezembro de 2018. O relatório também se deparou com bots AIO no setor de varejo, segurança de APIs e possíveis problemas de IPv6.

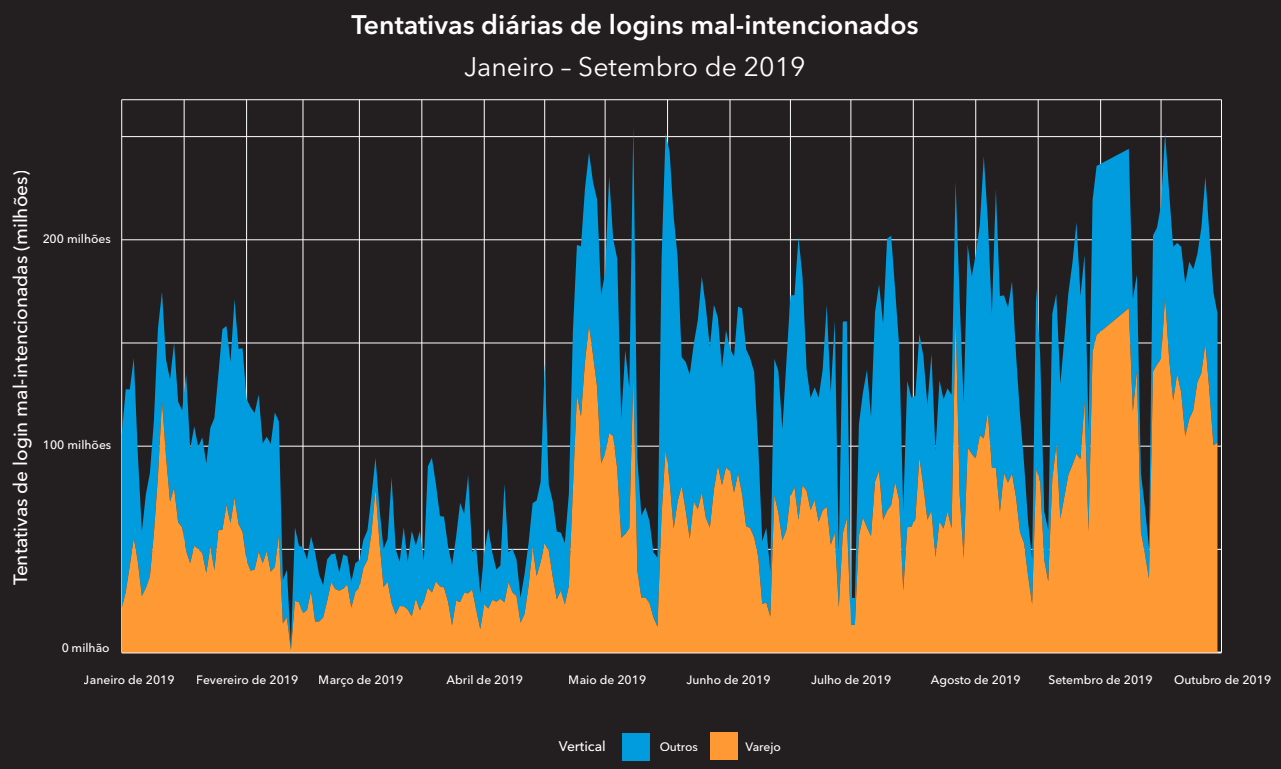


Fig. 1 (Atualização do gráfico publicado na 2ª edição) - O preenchimento de credenciais continua a ser amplamente direcionado ao setor de varejo, com 16,5 bilhões de tentativas nos primeiros nove meses de 2019, comparado com 11,5 bilhões nos últimos nove meses de 2018

Em resumo

- Cobrindo todos os setores (não apenas o varejo), a Akamai detectou quase 28 bilhões de tentativas de preenchimento de credenciais entre maio e dezembro de 2018.
- O uso de IPv6 pode ser subnotificado com base na análise da Akamai. Isso leva a uma suposição perigosa de que o IPv6 não vale a pena ser monitorado.
- Uma análise da ESSL (Rede Segura de Entrega de Conteúdo) da Akamai revelou uma divisão de 83% a 17% entre o tráfego de API e HTML por meio de nossa CDN (Rede de Entrega de Conteúdo). Esse é um aumento significativo desde que a mesma pesquisa foi realizada em 2014.

Março de 2019

Ao discutir tentativas de preenchimento de credenciais, um dos principais temas é o uso de senhas fáceis de adivinhar ou fracas. Além disso, muitos usuários reciclam suas senhas em várias redes e serviços. No início de março, surgiram histórias sobre o serviço de telefone Xfinity Mobile da Comcast, com um PIN padrão de 0000 nas contas de clientes. Essa história circulou logo após o rapper e magnata dos negócios Kanye West ter definido a senha em seu iPhone X como 000000.

Fora do ciclo de notícias, Jonathan Respeto, da Akamai, publicou um blog sobre o uso de programas Capture the Flag para promover o treinamento contínuo no SOCC (Security Operations Command Center, Centro de comando de operações de segurança).

Abril de 2019

Abril chegou e, enquanto a equipe se recuperava da RSA Conference, começaram a espalhar notícias na Web sobre um trio de vulnerabilidades contra dia zero do WordPress, levando a uma série de comprometimentos de websites. Os pesquisadores da Akamai frequentemente observam que os criminosos usam websites comprometidos para hospedar kits de phishing. Isso também ajuda na evasão; um website legítimo, mas comprometido, provavelmente não levanta suspeitas nem aciona alarmes de defesa terminal.

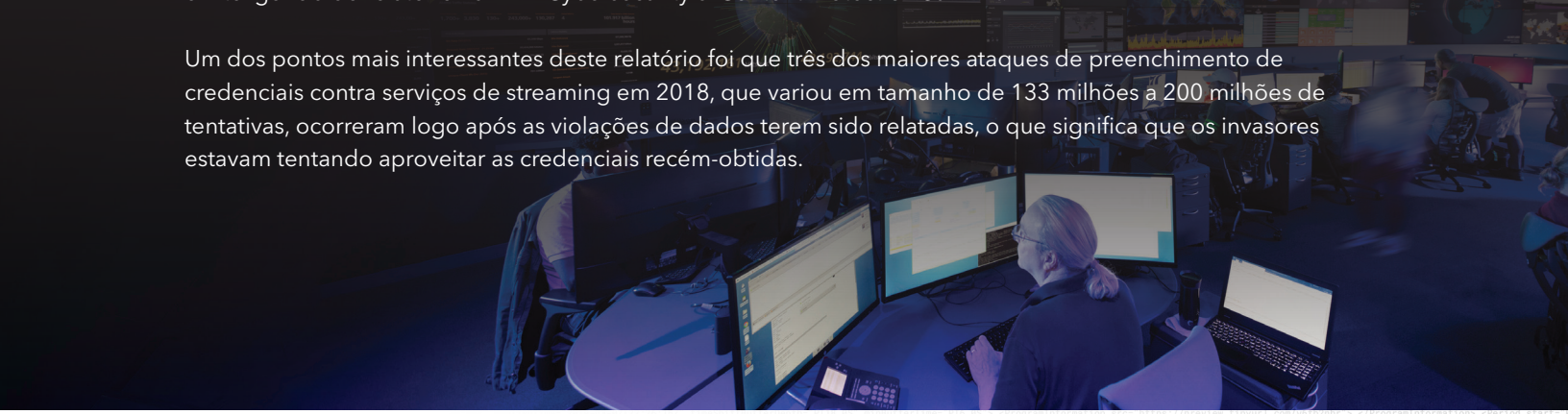
Em outras notícias sobre vulnerabilidade, Larry Cashdollar publicou um blog advertindo sobre várias vulnerabilidades no Magento. O aviso, publicado para chamar a atenção para o problema, revelou mais de 30 vulnerabilidades na plataforma, incluindo uma que tinha na época uma prova de conceito em funcionamento. No final do mês, o pesquisador Yael Daihes publicou no blog com Craig Sprocs sobre como adicionar dados de DNS (Sistema de Nomes de Domínio) do mundo real a modelos de aprendizagem profunda para aumentar a eficiência.

State of the Internet/Segurança: Edição especial de mídia

Preenchimento de credenciais – Ataques e economias

Lançada em 8 de abril de 2019, esta edição especial do relatório SOTI foi publicada para o público de mídia na conferência da NAB (Associação Nacional de Emissoras). Patrick Sullivan, da Akamai, apresentou dados e inteligência do relatório na NAB Cybersecurity & Content Protection Summit.

Um dos pontos mais interessantes deste relatório foi que três dos maiores ataques de preenchimento de credenciais contra serviços de streaming em 2018, que variou em tamanho de 133 milhões a 200 milhões de tentativas, ocorreram logo após as violações de dados terem sido relatadas, o que significa que os invasores estavam tentando aproveitar as credenciais recém-obtidas.



Maio de 2019

Os destaques de maio incluem patches da Cisco que solucionaram sérias vulnerabilidades de roteador e as dificuldades contra ransomwares em Baltimore e seus esforços de recuperação. O ransomware tem sido um tema comum no último ano, e o uso do ransomware mostra pouca evidência de diminuição.

Amiram Cohen, da Akamai, com pesquisa adicional da Or Katz, publicou uma visão detalhada do kit de phishing da 16Shop, que visa usuários da Apple. O kit em si é avançado, constantemente atualizado, e usa várias técnicas de evasão. A Equipe de Pesquisa de Ameaças da Akamai também publicou um blog relacionado ao Cipher Stunting, que é uma ameaça crescente que envolve a randomização de assinaturas SSL/TLS em uma tentativa de burlar a detecção.

Junho de 2019

Em geral, junho é um mês agitado para notícias sobre segurança, e este ano não foi exceção. Houve ataques contra plugins da WordPress, violações de dados e incidentes envolvendo malware POS em 102 restaurantes Checkers and Rally's de 20 estados. Em notícias mais leves, foi publicado um estudo alegando que o viés cognitivo afeta decisões de segurança.

Larry Cashdollar e Steve Ragan começaram o mês escrevendo um blog sobre a identificação de vulnerabilidades em kits de phishing, que, se explorados, poderiam levar a problemas adicionais para administradores de servidores. Or Katz, que se apresentou durante a conferência Edge World da Akamai, também publicou blogs relacionados a técnicas de evasão contra kits de phishing e análises de phishing. Cashdollar também publicou dois blogs adicionais naquele mês. O primeiro, em 13 de junho, abordou 26 vetores de infecção na versão mais recente (na época) do Echobot. No final do mês, ele postou sobre um bot chamado Silex que realizava bricks em sistemas, após infectados.

State of the Internet/Segurança: Volume 5, 3ª edição

Ataques na Web e violação de jogos

Esta edição do relatório SOTI abordou os jogos e a economia criminosa por trás deles. Os jogos são um alvo intenso, e os criminosos têm vários caminhos disponíveis para alcançar jogadores e as empresas responsáveis por alguns dos títulos mais populares da Web. No que diz respeito aos dados, o relatório observou que houve 12 bilhões de ataques de preenchimento de credenciais contra websites de jogos entre novembro de 2017 e março de 2019. Em todos os setores, ocorreram mais de 55 bilhões de ataques de preenchimento de credenciais durante o mesmo período. As aplicações Web também foram alvos populares, como destaca o relatório, com ataques de SQLi (Injeção de SQL) representando quase dois terços de todos os ataques a aplicações Web.

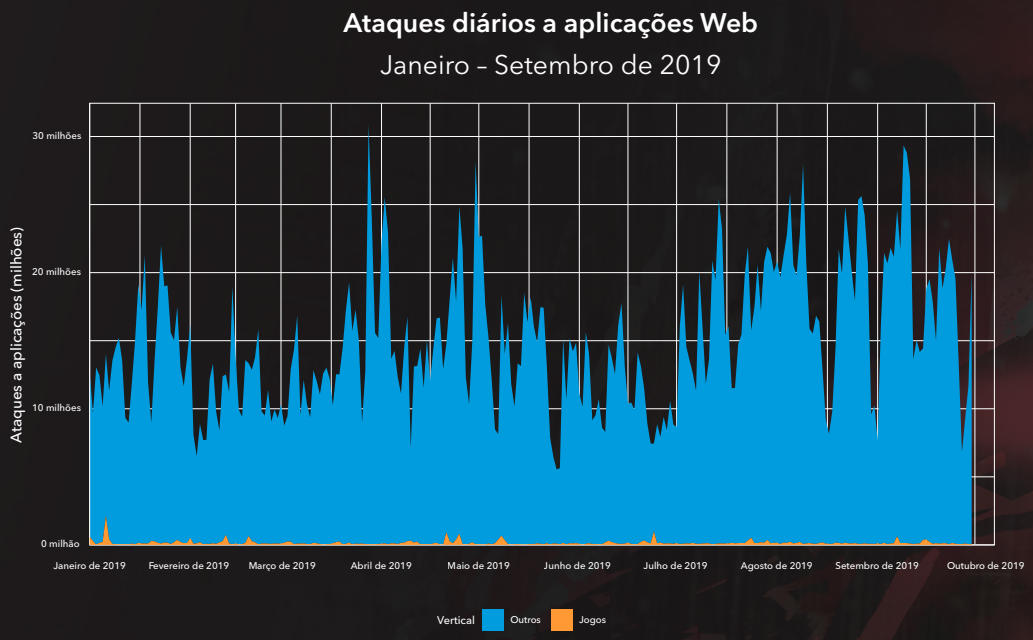


Fig. 2 - Embora as empresas de jogos sejam apenas alvo de uma pequena porcentagem dos ataques que a Akamai vê, elas ainda foram alvo de mais de 35 milhões de tentativas nos primeiros nove meses de 2019

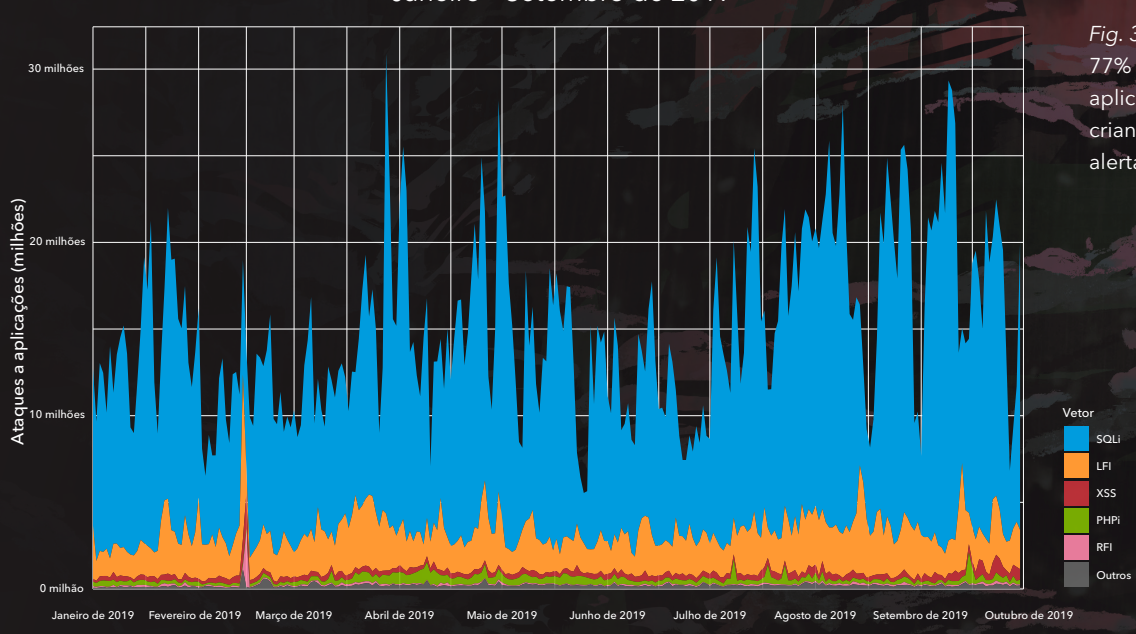


Fig. 3 - Os ataques SQLi representam 77% de todos os ataques a aplicações até o momento em 2019, criando mais de 3,1 bilhões de alertas na plataforma da Akamai

Em resumo

- A Akamai observou 55 bilhões de ataques de preenchimento de credenciais ao longo de 17 meses, e 12 bilhões deles visaram diretamente o segmento de jogos.
- A SQLi é a principal ameaça quando se trata de riscos a aplicações Web, sendo responsável por quase dois terços de todos os ataques.
- No geral, os Estados Unidos ainda são a principal fonte de preenchimento de credenciais, seguidos pela Rússia. Mas, ao analisar somente os dados de jogos, a Rússia é a fonte número um.

Julho de 2019

Em julho, a maioria das pessoas da indústria da segurança, incluindo muitos de nós da Akamai, estava se preparando para eventos em Las Vegas. As empresas de segurança falam muito sobre riscos e superfícies de ataque. Uma das superfícies de ataque mais comuns é o navegador; por isso, quando a notícia de que o *Bundesamt für Sicherheit in der Informationstechnik* (BSI) da Alemanha estava elaborando diretrizes para a segurança de navegadores, as pessoas notaram.

Internamente, no lado da pesquisa, Chad Seaman, da Akamai, publicou um blog sobre ataques SYN-ACK. Lior Lahav e Asaf Nadler discutiram alterações recentes no DGA (Algoritmo de Geração de Domínio) para Pykspa v2, seguido de uma segunda postagem que explorou atenuações de DGA. Por fim, Larry Cashdollar publicou em 29 de julho um blog sobre criminosos que aproveitam as vulnerabilidades de RFI (Remote File Inclusion) em suas campanhas de phishing.

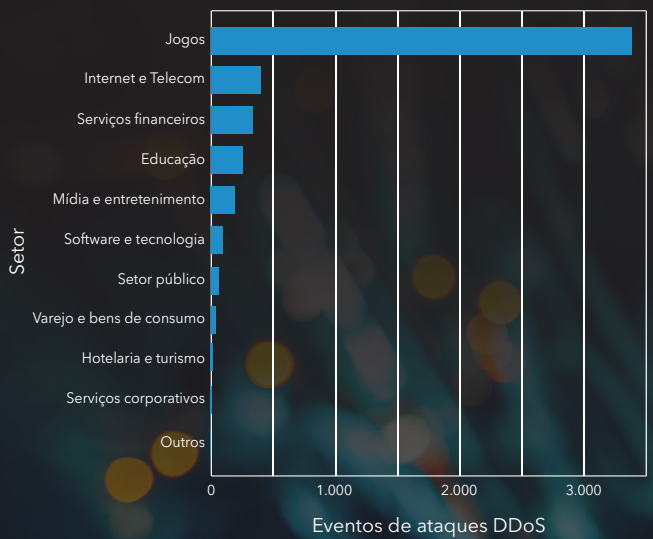
State of the Internet/Segurança: Volume 5, 4ª edição

Economia de ataque dos serviços financeiros

Esta edição do relatório SOTI explorou os ataques e as ferramentas que estão sendo usados contra serviços financeiros, e como eles fazem parte de um ecossistema maior e mais complexo. O relatório analisou os mercados criminosos e examinou como eles visam as organizações financeiras, bem como o que acontece após um ataque bem-sucedido.

DDOS – Eventos de ataques

Janeiro de 2019 – Setembro de 2019



DDoS – Alvos únicos

Janeiro de 2019 – Setembro de 2019

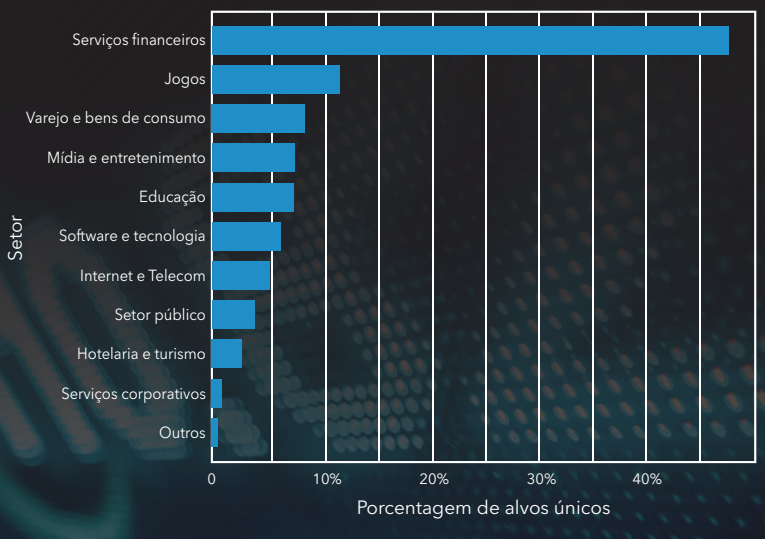


Fig. 4 (Atualização do gráfico publicado na 4ª edição) - Os ataques DDoS têm como alvo mais as empresas de jogos, mas os ataques contra o setor de serviços financeiros são muito mais dispersos em vários alvos

Em resumo

- Metade de todas as organizações exclusivas imitadas por domínios de phishing estava no setor de serviços financeiros, de acordo com os dados da Akamai.
- Mais de 6% das tentativas de logins mal-intencionados foram direcionadas globalmente ao setor financeiro.
- 94% dos ataques contra o setor financeiro vieram de ataques SQLi, LFI, XSS (Cross-Site Scripting) e injeções de Java OGNL.

Agosto de 2019

No início de agosto, a Black Hat, DEF CON e BSides Las Vegas estavam acontecendo, e muitas das primeiras manchetes faziam parte do que a jornalista Violet Blue chama de "Temporada de Clickbaits". Mas a notícia que causou mais rumores não estava nem mesmo relacionada à segurança. Era sobre um homem que usava uma TV na cabeça e que foi flagrado por câmeras deixando TVs em varandas no Estado da Virgínia. Após evitarem por pouco uma praga de gafanhotos em Las Vegas, aqueles que participaram da Black Hat souberam que poderiam ter sido expostos ao sarampo se estiveram na região entre 3 e 5 de agosto.

No departamento de pesquisa, Or Katz, da Akamai, publicou um blog sobre golpes de phishing que visam destinos populares de férias, e Larry Cashdollar escreveu sobre o software de mineração de criptomoeda XMR que vem se espalhando.

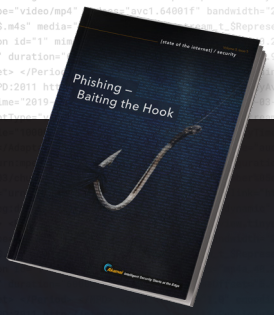
Setembro de 2019

Jonathan Respeto e Chad Seaman, da Akamai, publicaram um blog que trata de um novo vetor DDoS que pode atingir 35/Gbps. O vetor, que aproveita uma técnica de amplificação UDP conhecida como WSD (WS-Discovery), pode ser usado para obter taxas de amplificação de até 15.300%.

State of the Internet/Segurança: Edição especial de mídia

A mídia sob ataque

Lançada em apoio à feira de mídia, entretenimento e tecnologia do IBC, esta edição especial do relatório SOTI continuou a tendência de acompanhar atividades de preenchimento de credenciais, com uma visão detalhada de como elas impactam as empresas de mídia e tecnologia. De janeiro de 2018 a junho de 2019, a Akamai registrou mais de 61 bilhões de tentativas de preenchimento de credenciais e mais de 4 bilhões de ataques a aplicações Web.



State of the Internet/Segurança: Volume 5, 5ª edição

Phishing: Mordendo a isca

O último relatório SOTI do ano, focado em pesquisa, abordou sobre phishing e a economia e os métodos que o apoiam. Essa questão também inclui, pela primeira vez, os dados do próprio rastreamento interno da Akamai sobre tentativas de phishing que visavam nossos funcionários.

Em resumo

- 60% dos kits de phishing monitorados pela Akamai ficaram ativos por 20 dias ou menos.
- A alta tecnologia é o principal setor visado por phishing, de acordo com os dados da Akamai.
- Microsoft, PayPal, DHL, Dropbox, DocuSign e LinkedIn são todos principais alvos de phishing, segundo o monitoramento da Akamai.

Fontes de notícias

Além das fontes vinculadas neste relatório, veja abaixo uma lista de algumas fontes de notícias que os contribuintes deste relatório leem regularmente para análise criteriosa e cobertura do setor.

- Violet Blue
- Zack Whitaker
- Dark Reading
- Ars Technica
- Motherboard
- CyberScoop
- CSO Online
- WIRED
- TechCrunch
- ZDNet
- SecurityWeek
- Forbes

Pensando no futuro

Esta é a temporada de "previsões de segurança". Nós odiamos previsões de segurança.

Futuristas e escritores de ficção científica fazem previsões sobre o futuro. Gene Roddenberry e sua criação *Star Trek* se tornaram elementos básicos da consciência coletiva e previram ou levaram à criação de muitos dos gadgets que usamos diariamente, como telefones celulares e fones de ouvido Bluetooth. Mas somos profissionais de segurança, não futuristas, e nunca conseguimos fazer previsões com um ano de antecedência com qualquer precisão.

Que você viva tempos interessantes.

—Antiga maldição chinesa

O que podemos fazer é analisar os dados que temos hoje e extrapolar tendências. Você pode se perguntar como isso difere de uma previsão. E a resposta é, principalmente, perspectiva. Extrapolação e previsão são tentativas de encontrar tendências emergentes, mas a previsão tem um viés mais sensacional.

Quando alguém solicita uma previsão, existe uma necessidade presumida de que a resposta seja nova e diferente do que os outros apontaram; extrapolação é baseada mais nas tendências do mundo real. Sim, é polêmico e pedante, mas esse nível de especificidade é o que devemos esperar de pesquisadores e editores.

Então, o que podemos extrapolar das tendências de 2019? Primeiro, o abuso de credenciais, o phishing e a exploração de vulnerabilidades em sistemas populares continuarão a crescer. Parece óbvio, mas a diferença é que estamos vendo uma "profissionalização" cada vez maior desses ataques. Na verdade, veremos mais "profissionalização" e mais diversidade nos ataques.

Há uma década, as vulnerabilidades eram geralmente encontradas por um criminoso e, em seguida, incorporadas a ataques. Há cinco anos, tornou-se muito mais comum ver equipes profissionais de criminosos que descobriram e desenvolveram softwares de ataque. A tendência agora é uma sobreposição entre os desenvolvedores criminosos e a APT (ameaça persistente avançada), ou agentes de estados-nações, para criar um fluxo constante de ferramentas de dia zero direcionadas a organizações e indivíduos específicos.

Isso não é mera especulação. No início de outubro, a NSA chegou ao extremo ao emitir um aviso de que agentes conhecidos do estado-nação estavam focando plataformas de VPN vulneráveis. Há vários outros canais de comunicação nos quais esses avisos normalmente chegariam, portanto, isso mostra que a NSA vê isso como um perigo claro e presente.

Estamos nos afastando de uma época em que os consultores de segurança de uma empresa eram vistos como alarmistas, até mesmo quando somos pegos desprevenidos pela gravidade e pelo impacto dos ataques. Tópicos esotéricos sobre segurança que costumavam ser o reino de especialistas e tecnólogos agora fazem parte do ciclo diário de notícias e da consciência coletiva. Muitas das previsões de uma década atrás estão se tornando reais, mesmo que as ameaças não se pareçam com o que a maioria de nós esperava.

Uma previsão que podemos fazer é que 2020 será interessante.

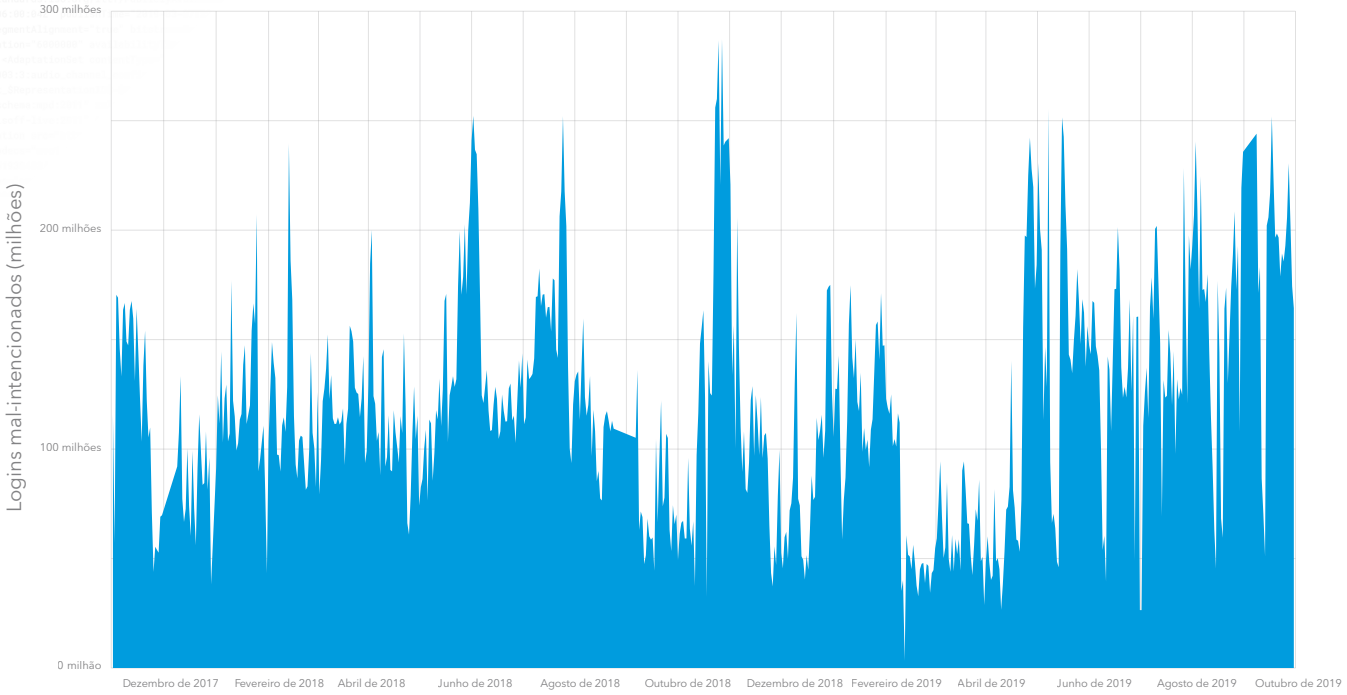
Apêndice

Atualizações importantes de nossas grandes histórias

As seguintes plotagens são atualizações do trabalho em edições anteriores do volume 5 do relatório State of the Internet/Segurança. Estamos fornecendo aos leitores como informações complementares com texto de suporte e explicação mínimos. Todas as plotagens e tabelas abrangem o período de novembro de 2017 a setembro de 2019.

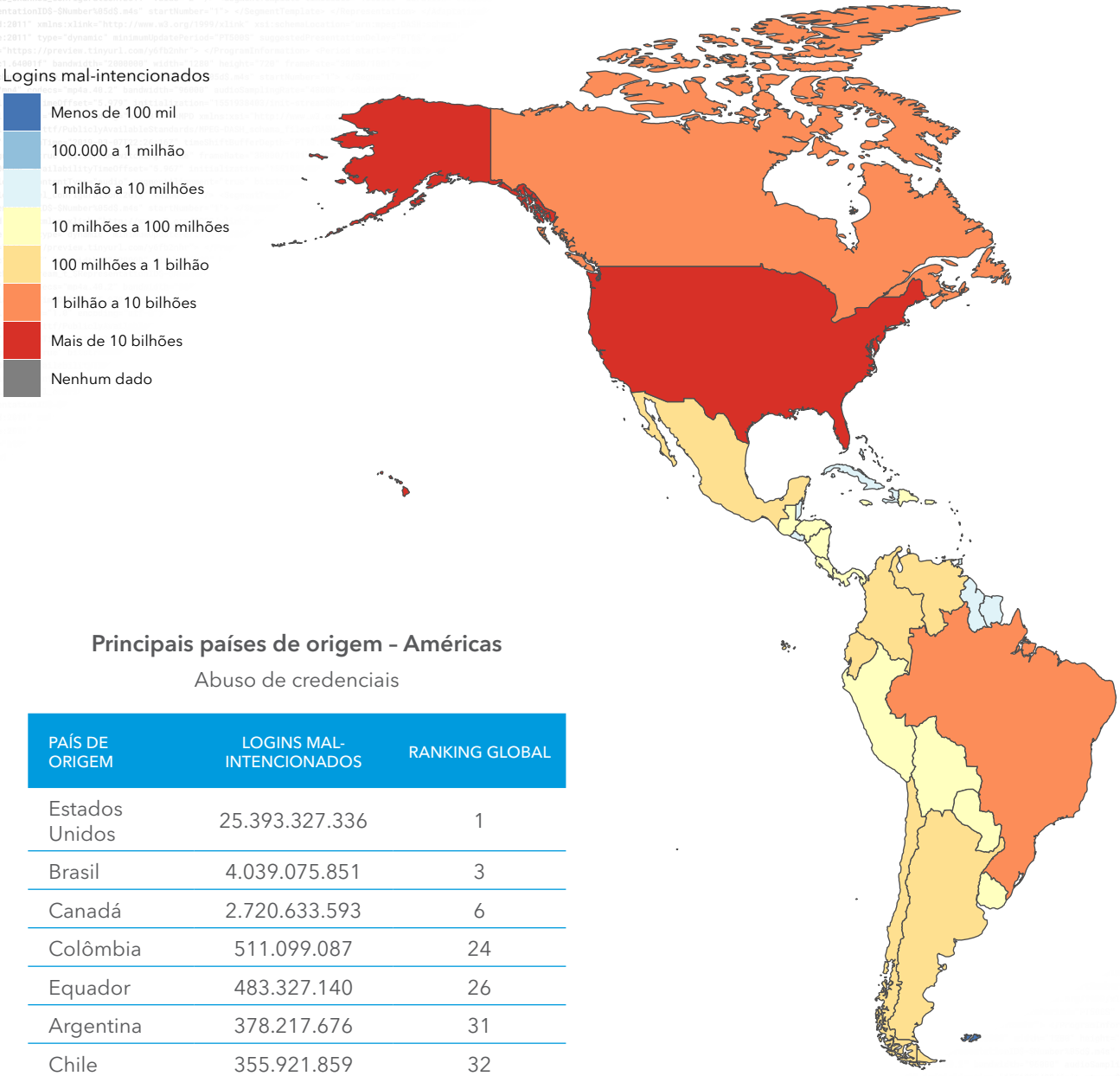
Tentativas diárias de logins mal-intencionados

Novembro de 2017 – Setembro de 2019



Fontes de ataques de abuso de credenciais – Américas

Novembro de 2017 – Setembro de 2019



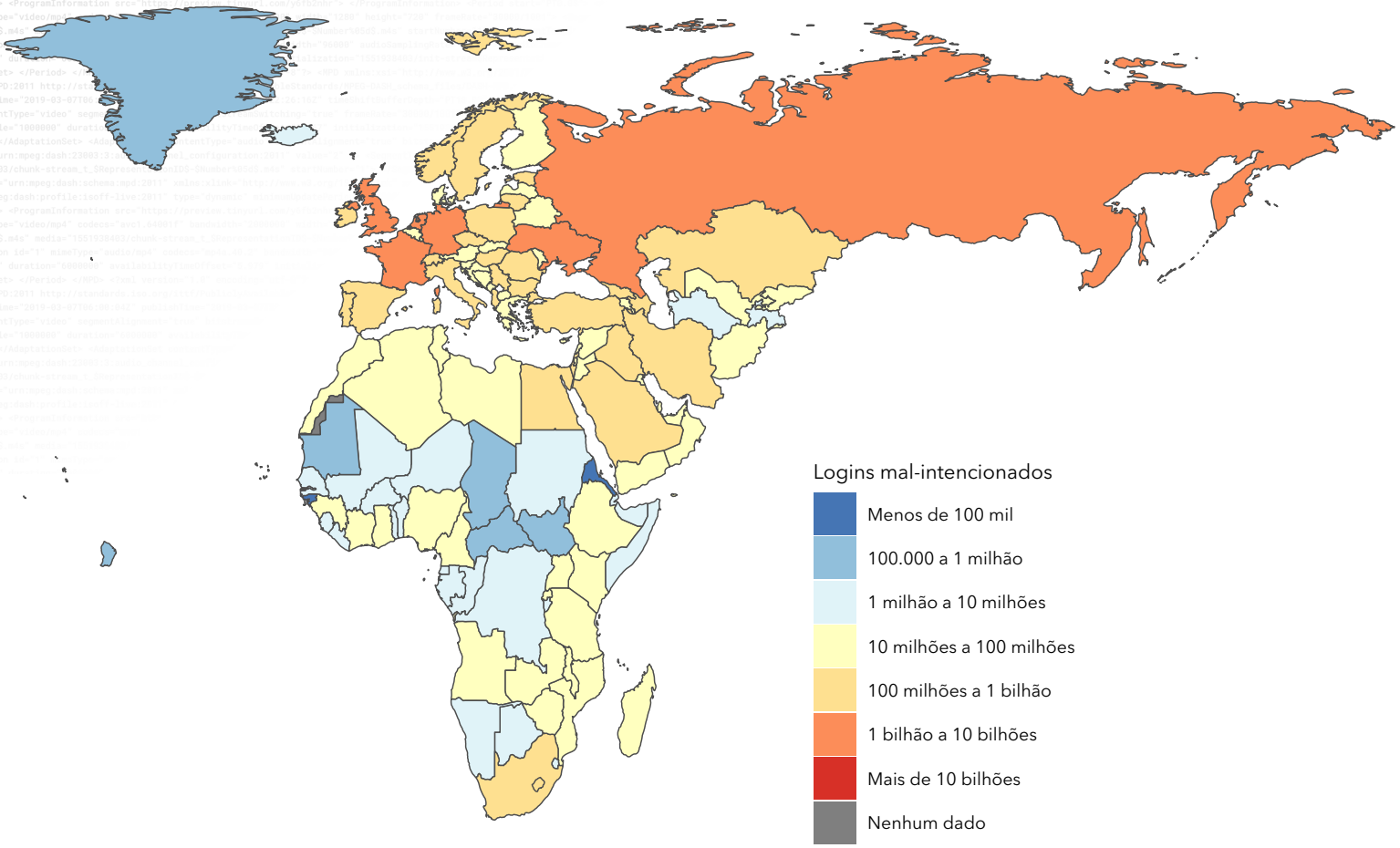
Principais países de origem – Américas

Abuso de credenciais

PAÍS DE ORIGEM	LOGINS MAL-INTENCIONADOS	RANKING GLOBAL
Estados Unidos	25.393.327.336	1
Brasil	4.039.075.851	3
Canadá	2.720.633.593	6
Colômbia	511.099.087	24
Equador	483.327.140	26
Argentina	378.217.676	31
Chile	355.921.859	32
México	344.094.629	34
Venezuela	177.795.687	47
Peru	90.149.099	65

Fontes de ataques de abuso de credenciais – EMEA

Novembro de 2017 – Setembro de 2019



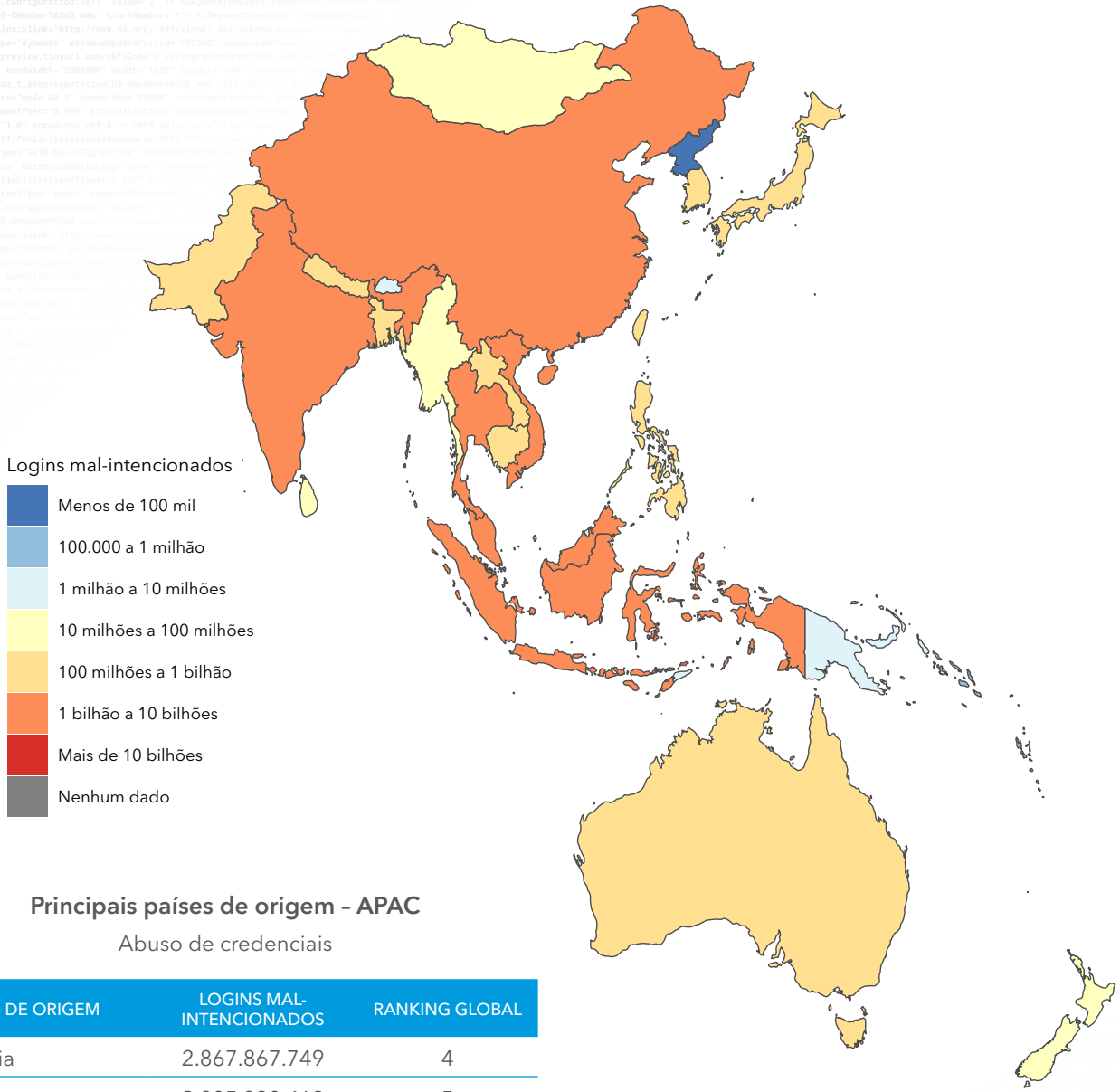
Principais países de origem – EMEA

Abuso de credenciais

PAÍS DE ORIGEM	LOGINS MAL-INTENCIONADOS	RANKING GLOBAL
Rússia	6.114.186.048	2
Alemanha	2.129.388.432	10
França	2.081.826.451	11
Países Baixos	1.723.393.319	12
Reino Unido	1.559.263.043	14
Ucrânia	1.097.729.730	16
Itália	879.866.419	17
Estônia	652.938.763	21
Polônia	571.536.319	23
Espanha	490.167.797	25

Fontes de ataques de abuso de credenciais – APAC

Novembro de 2017 – Setembro de 2019



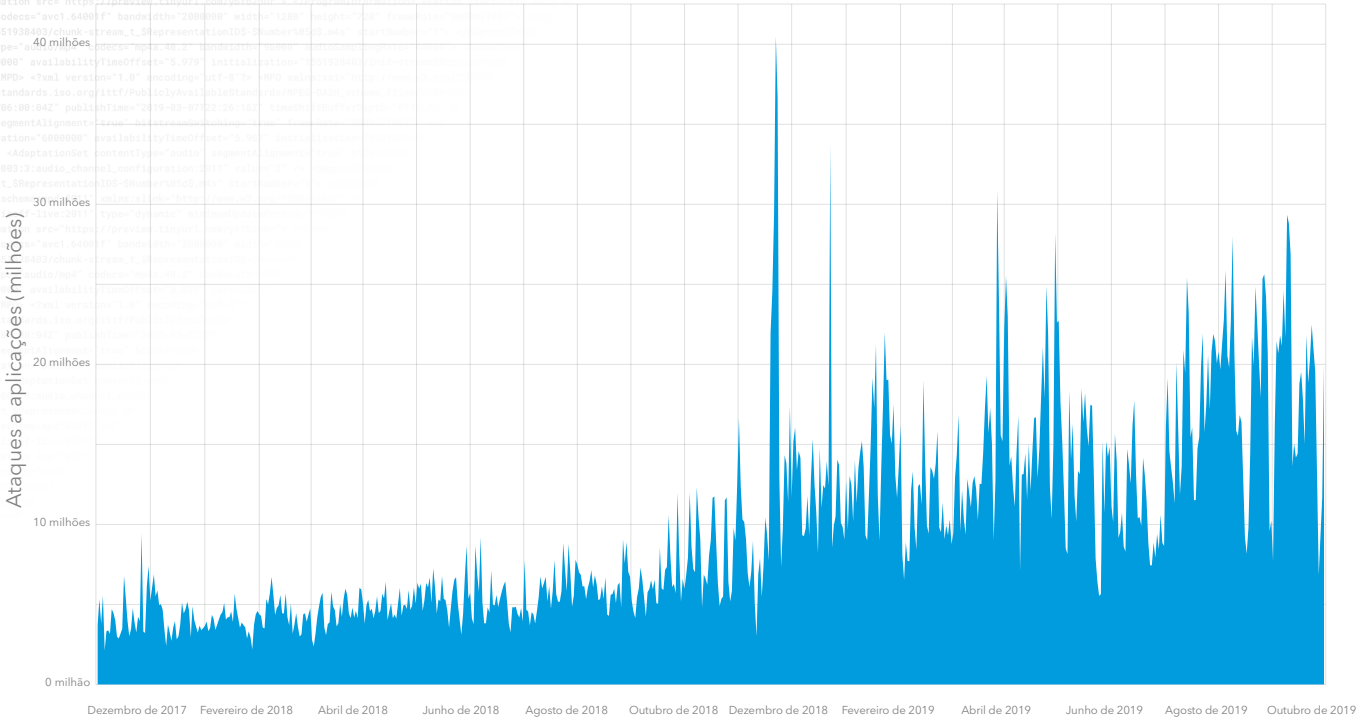
Principais países de origem – APAC

Abuso de credenciais

PAÍS DE ORIGEM	LOGINS MAL-INTENCIONADOS	RANKING GLOBAL
Índia	2.867.867.749	4
China	2.805.330.412	5
Tailândia	2.626.767.167	7
Indonésia	2.328.720.242	8
Vietnã	2.166.055.670	9
Cingapura	1.568.843.384	13
Malásia	1.547.306.924	15
Japão	845.793.217	18
Taiwan	817.736.419	19
Coreia do Sul	737.126.412	20

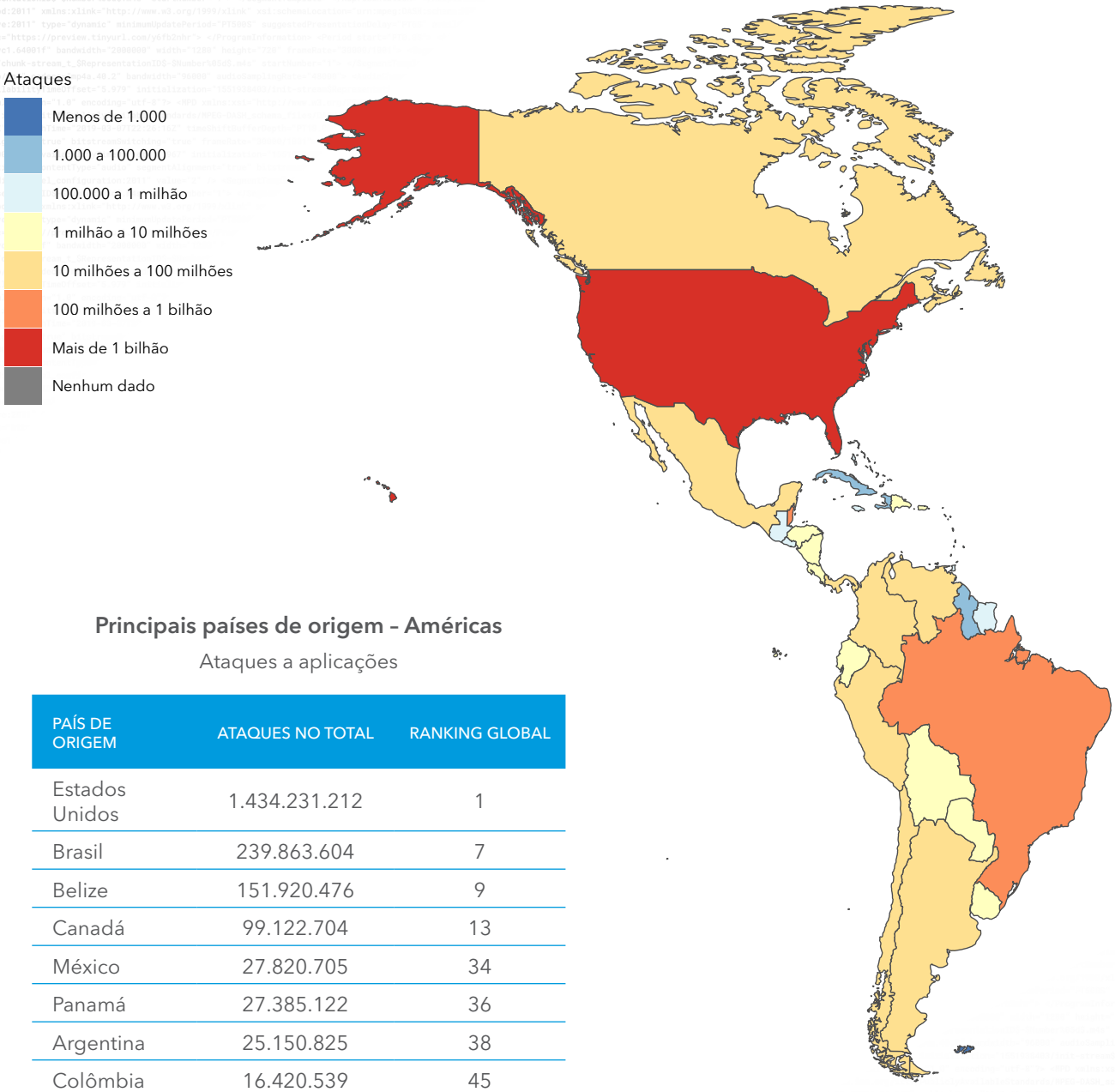
Ataques diários a aplicações Web

Novembro de 2017 – Setembro de 2019



Fontes de ataques a aplicações Web – Américas

Novembro de 2017 – Setembro de 2019



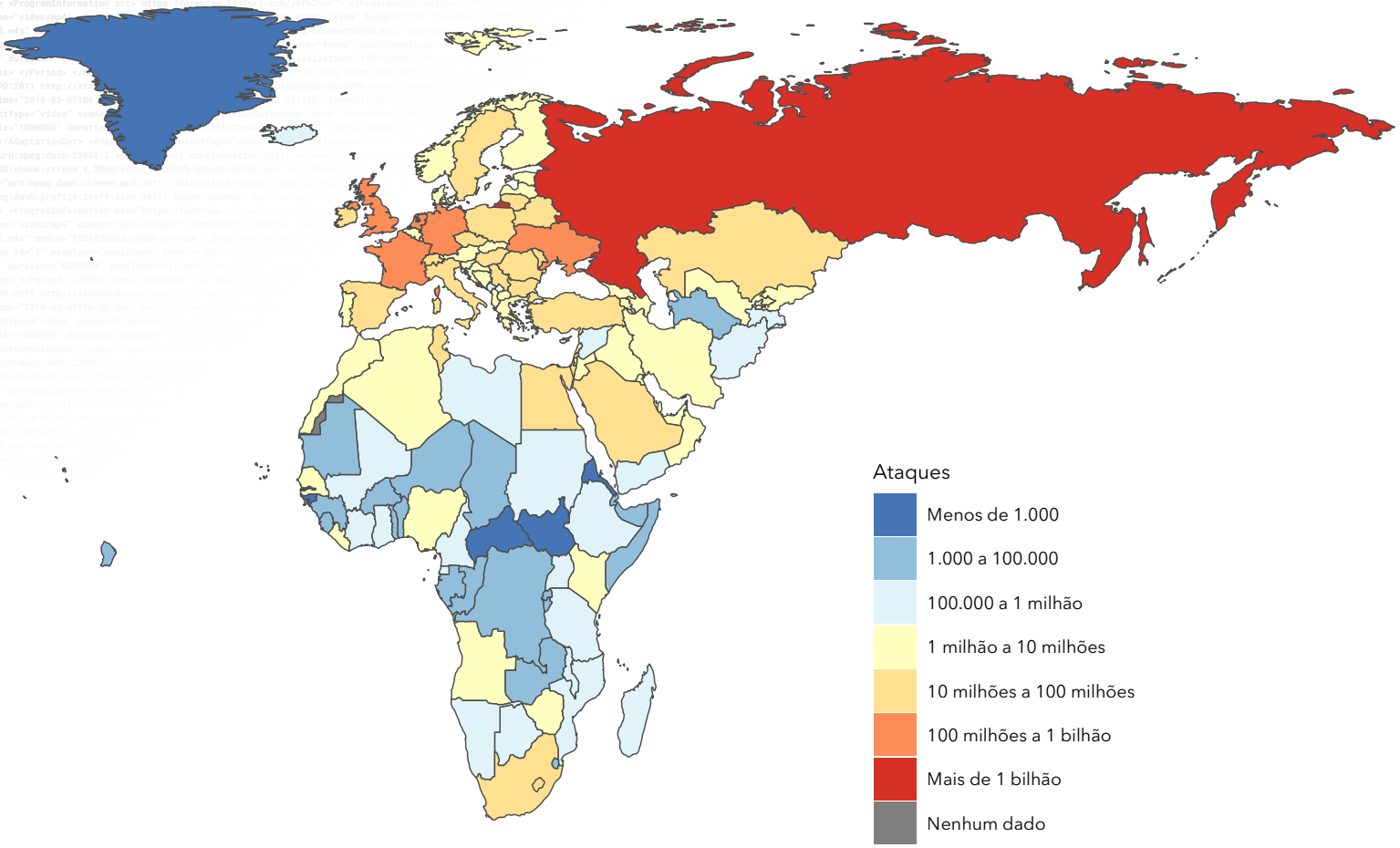
Principais países de origem – Américas

Ataques a aplicações

PAÍS DE ORIGEM	ATAQUES NO TOTAL	RANKING GLOBAL
Estados Unidos	1.434.231.212	1
Brasil	239.863.604	7
Belize	151.920.476	9
Canadá	99.122.704	13
México	27.820.705	34
Panamá	27.385.122	36
Argentina	25.150.825	38
Colômbia	16.420.539	45
Venezuela	16.147.307	47
Chile	12.827.683	50

Fontes de ataques a aplicações Web – EMEA

Novembro de 2017 – Setembro de 2019



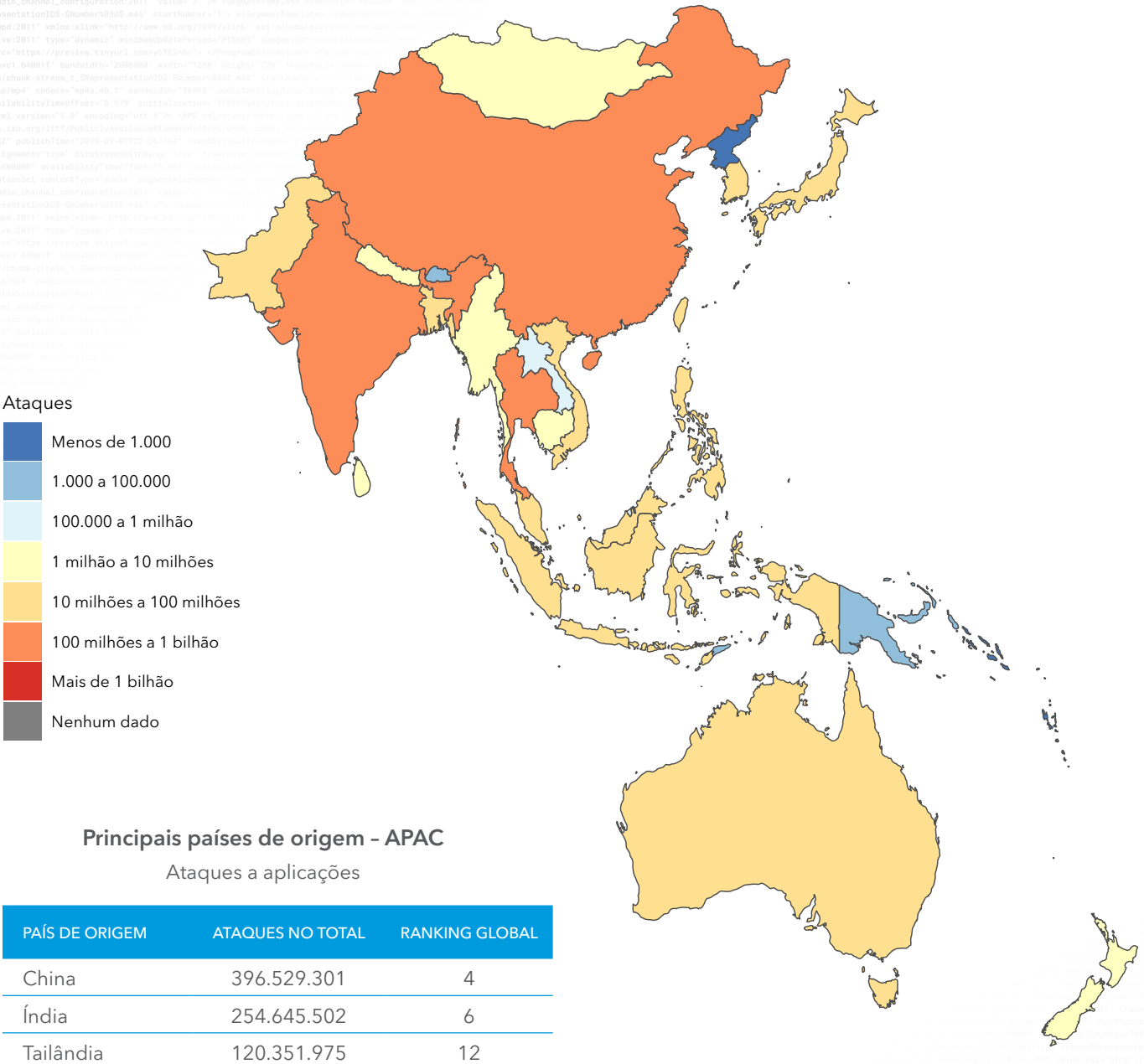
Principais países de origem – EMEA

Ataques a aplicações

PAÍS DE ORIGEM	ATAQUES NO TOTAL	RANKING GLOBAL
Rússia	1.093.219.355	2
Países Baixos	414.257.266	3
Ucrânia	288.844.085	5
Alemanha	200.129.170	8
França	148.147.042	10
Reino Unido	141.076.862	11
Irlanda	93.537.634	14
Turquia	88.376.455	16
Romênia	69.929.767	20
Itália	52.615.647	24

Fontes de ataques a aplicações Web – APAC

Novembro de 2017 – Setembro de 2019



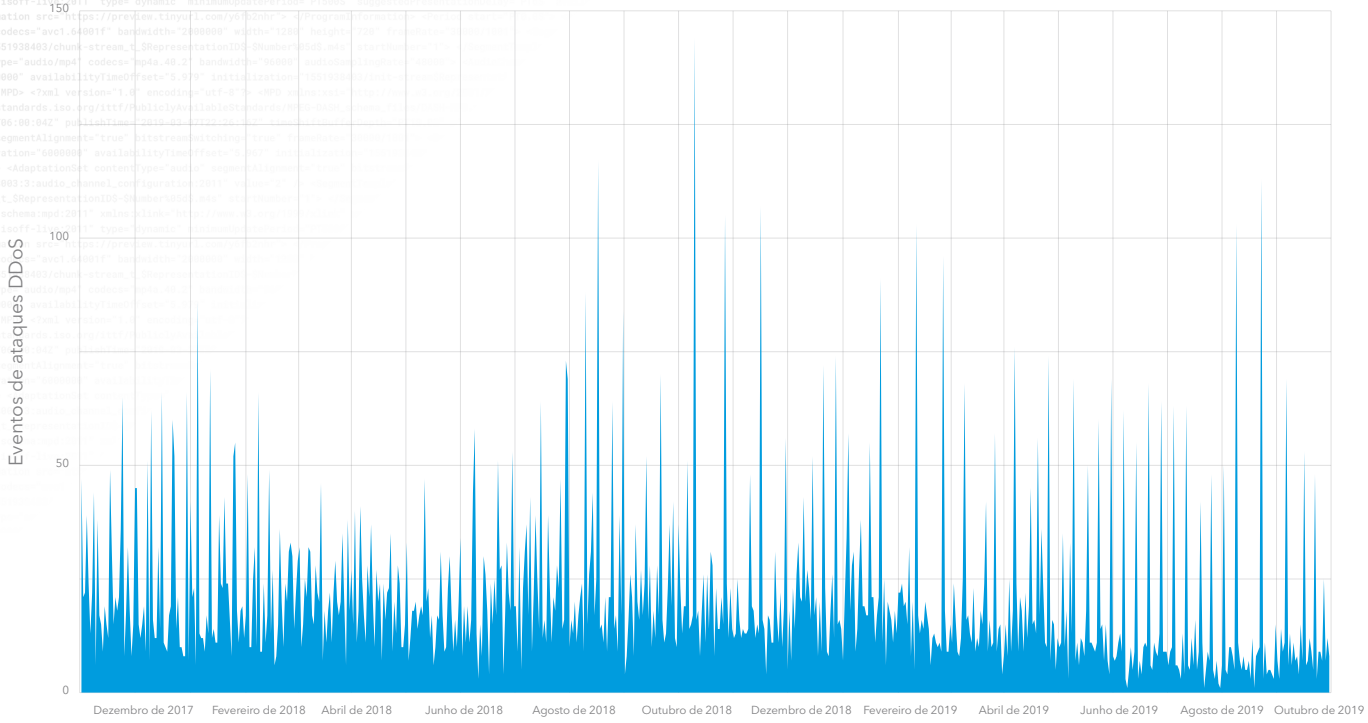
Principais países de origem – APAC

Ataques a aplicações

PAÍS DE ORIGEM	ATAQUES NO TOTAL	RANKING GLOBAL
China	396.529.301	4
Índia	254.645.502	6
Tailândia	120.351.975	12
Cingapura	91.057.766	15
Indonésia	83.441.813	17
Japão	76.396.164	18
Vietnã	63.455.055	22
Taiwan	57.639.687	23
Hong Kong	49.977.066	25
Coreia do Sul	43.552.997	27

Eventos de ataques DDoS diários

Novembro de 2017 – Setembro de 2019



Créditos

Colaboradores do State of the Internet/Segurança

VOLUME 5, 1ª EDIÇÃO

Ben Tang
Cientista de dados

Elad Shuster
Pesquisador sênior de segurança

Chad Seaman
Equipe de resposta de inteligência de segurança, Sênior II

Larry Cashdollar
Equipe de resposta de inteligência de segurança, Sênior II

Moshe Zioni
Pesquisa de ameaças, Diretor

Gabriel Bellas
Gerente de prática, Serviços globais

Autor convidado: Amanda Berlin
Mental Health Hackers

VOLUME 5, 2ª EDIÇÃO

Tony Lauro
Gerente sênior, Estratégia de segurança

Moritz Steiner
Arquiteto principal

Kyle Schomp
Engenheiro de desempenho, Sênior II

Rami Al-Dalky
Estagiário

VOLUME 5, EDIÇÃO ESPECIAL DE MÍDIA: PREENCHIMENTO DE CREDENCIAIS – ATAQUES E ECONOMIAS

Shane Keats
Diretor de marketing global da indústria, mídia e entretenimento

Steve Ragan
Pesquisador, redator técnico sênior

Martin McKeay
Diretor editorial

VOLUME 5, 3ª EDIÇÃO

Elad Shuster
Pesquisador sênior de segurança

Lydia LaSeur
Cientista de dados

Tim April
Arquiteto principal

Steve Ragan
Redator técnico sênior

Martin McKeay
Diretor editorial

VOLUME 5, 4ª EDIÇÃO

Elad Shuster
Pesquisador sênior de segurança

Or Katz
Principal pesquisador de segurança

Tim April
Arquiteto principal

Colaboradores do State of the Internet/Segurança

VOLUME 5, 4ª EDIÇÃO (CONT.)

Lydia LaSeur
Cientista de dados

Steve Ragan
Redator técnico sênior

VOLUME 5, EDIÇÃO ESPECIAL DE MÍDIA: A MÍDIA SOB ATAQUE

Omri Hering
Analista de dados sênior

Lydia LaSeur
Cientista de dados

VOLUME 5, 5ª EDIÇÃO

Eric Kloster
Diretor de engenharia

Lorenz Glaser
Engenheiro de segurança sênior II

Or Katz
Principal pesquisador de segurança

Lydia LaSeur
Cientista de dados

Paul O'Leary
Cientista de dados principal,
Engenharia de inteligência de ameaças

EQUIPE EDITORIAL DO VOLUME 5, EDIÇÕES 1 A 6

Martin McKeay
Diretor editorial

Amanda Fakhreddine,
Editora-chefe, Redatora técnica sênior

Steve Ragan
Redator técnico sênior

Lydia LaSeur
Cientista de dados

EQUIPE DE CRIAÇÃO E MARKETING DO VOLUME 5, EDIÇÕES 1 A 6

Benedikt Van Holt
Direção de arte

Brendan John O'Hara
Design gráfico

Georgina Morales Hampe
Gerente de projetos

Kylee McRae
Gerente de programas

Murali Venukumar
Gerente de programas