[state of the internet] / security

Retail Attacks and API Traffic (em inglês)

Akamai
Intelligent Security Starts at the Edge

Nota do editor

As equipes de segurança estão se tornando cada vez mais parte integrante da empresa e são mais vitais do que nunca para o sucesso. Elas evoluíram e são vistas cada vez mais como parceiras legítimas de negócios e facilitadoras de crescimento.

Um dos fatores mais importantes para que uma equipe de segurança seja considerada uma parceira de negócios é sua capacidade de identificar os riscos enfrentados pela empresa. A identificação de riscos não é uma ciência exata. Muitas equipes de segurança compreendem as nuances dos riscos associados a várias tecnologias. No entanto, identificar riscos potenciais e entender como eles afetam os negócios pode ser um processo árduo. Isso se torna ainda mais difícil quando as empresas e as equipes de segurança enfrentam fatores desconhecidos sobre os quais a organização não tem praticamente nenhuma visibilidade. Todas as três histórias desta edição do relatório **State of the Internet / Security** abrangem tópicos que provavelmente as organizações não conhecem tão bem quanto deveriam.

Tráfego de API por agente de usuário

TIPO	UA	
Navegador	Chrome	13%
	Mobile Safari	8%
	Firefox	2%
	Internet Explorer	2%
	Edge	1%
	Safari	1%
	IE Mobile	0%
Sem navegador	Outros	66%
	CFNetwork	3%
	Apache HttpClient	2%

Figura 1: a maioria do tráfego de APIs ocorre em aplicações personalizadas e não é facilmente categorizado

Aumento do tráfego de APIs

Nossa pesquisa de outubro de 2018 sobre o tráfego de APIs revelou que 83% dos acessos são direcionados por APIs.

Para os profissionais de segurança, o crescimento no volume de APIs é importante quando se consideram os riscos envolvidos, pois algumas ferramentas não conseguem lidar com isso. Se as ferramentas atuais não conseguem lidar com esse tráfego, é possível que a organização esteja ignorando uma importante origem de tráfego mal-intencionado. Com a proliferação dos dispositivos de IoT, o tráfego de APIs será algo que todas as organizações deverão enfrentar para proteger seus negócios e seus clientes.

Ferramentas de destruição em massa de varejo

Neste relatório, examinamos novamente o preenchimento de credenciais no que se refere ao setor varejista. A Akamai detectou quase 28 bilhões de tentativas de preenchimento de credenciais entre maio e dezembro de 2018. Isso significa mais de 115 milhões de tentativas diárias de comprometer ou efetuar login em contas de usuário.

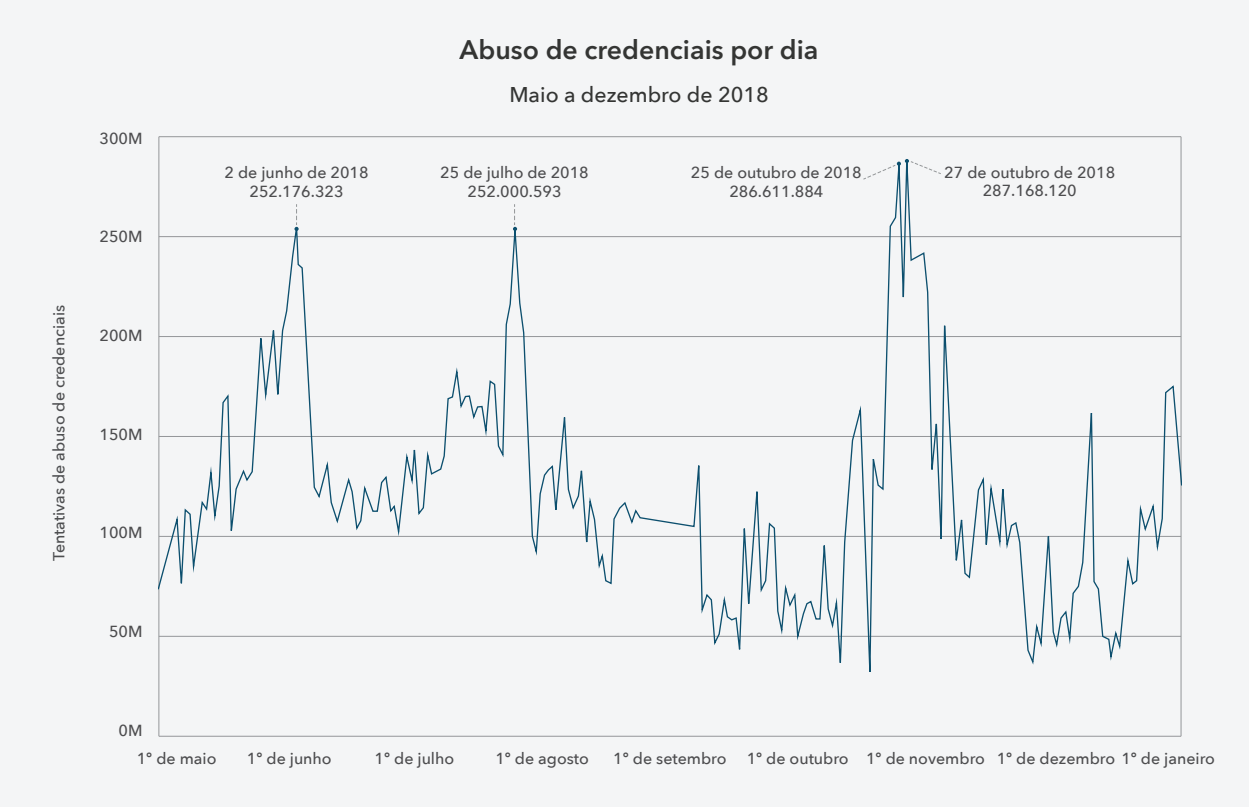

Figura 2: quatro dos principais dias de preenchimento de credenciais são destacados entre 1º de maio e 31 de dezembro de 2018

Qual é o setor mais afetado? O varejo ficou no topo da lista, com 10 bilhões de tentativas de preenchimento de credenciais direcionadas a ele. O setor de vestuário teve 3,7 bilhões de tentativas, sendo a vertical mais atacada do setor varejista no mesmo período. A Akamai também rastreou as tentativas de preenchimento de credenciais no comércio direto (1,427 bilhões), em lojas de departamento (1,426 bilhões), em lojas de material de escritório (1,3 bilhões) e em lojas de acessórios de moda, como joias e relógios (129.725.233).

Os agentes mal-intencionados estão usando ferramentas conhecidas como AIOs, ou bots All-In-One, para acessar contas e automatizar as compras. O uso de alguns AIOs alimenta o mercado de revenda, enquanto outros AIOs são usados para controlar as contas existentes ou coletar informações pessoais e financeiras valiosas.

O IPv6 está sendo subnotificado?

os pesquisadores também examinaram o tráfego de DNS e revelaram um fato interessante: O tráfego IPv6 pode estar sendo subnotificado, pois muitos sistemas capazes de usar o IPv6 ainda preferem o IPv4. Como o IPv6 ainda é visto como minoria de tráfego, ele não é um ponto de venda importante para muitas ferramentas de segurança.

Pensando no futuro

Neste momento, o mundo da segurança engloba praticamente tudo, e a segurança assumiu um papel principal no planejamento e no crescimento das empresas. Estamos longe dos dias em que as empresas podiam tratar a segurança como uma reflexão adicional.

Cada uma das histórias nesta edição do relatório State of the Internet / Security examina aspectos de segurança que podem ser negligenciados, mas são importantes para as operações diárias. Essas histórias criam um pano de fundo para o que esperamos ver nos próximos trimestres e anos.

Se você estiver interessado em saber mais sobre as metodologias utilizadas para selecionar os dados do relatório, incluímos uma seção inteira que analisa isso mais a fundo.

Para uma análise mais detalhada sobre essas histórias, baixe o relatório completo State of the Internet / Security: Retail Attacks and API Traffic (em inglês).

Akamai

A Akamai, a maior e mais confiável plataforma de entrega de serviços em nuvem do mundo, facilita que seus clientes ofereçam as melhores e mais seguras experiências digitais em qualquer dispositivo, a qualquer hora e em qualquer lugar. A plataforma amplamente distribuída da Akamai é incomparável em escala, oferecendo a seus clientes desempenho superior e proteção contra ameaças. O portfólio de soluções de desempenho na Web e em dispositivos móveis, segurança na nuvem, acesso corporativo e entrega de vídeo da Akamai conta com um atendimento ao cliente excepcional e monitoramento 24 horas por dia, 7 dias por semana, 365 dias por ano. Para saber por que as principais instituições financeiras, os líderes de varejo online, os provedores de mídia e de entretenimento e as organizações governamentais confiam na Akamai, acesse www.akamai.com, blogs.akamai.com ou @Akamai no Twitter. Publicado em 02/19.