[Estado de Internet] / Seguridad

Tráfico de API y ataques al sector retail

Akamai
Intelligent Security Starts at the Edge

Nota del editor

Los equipos de seguridad constituyen, cada vez más, una parte fundamental de las empresas, además de ser más decisivos que nunca para su éxito. Estos equipos han evolucionado y cada vez reciben mayor consideración como partners comerciales legítimos que impulsan el crecimiento.

Uno de los factores más importantes para que un equipo de seguridad sea considerado un partner comercial es su capacidad para identificar los riesgos a los que se enfrenta la empresa. La identificación de riesgos no es una ciencia exacta. Muchos equipos de seguridad comprenden las peculiaridades de los riesgos asociados a las diversas tecnologías; sin embargo, identificar el riesgo y el modo en que este afectará a la empresa puede ser un proceso complejo. Y esto resulta aún más difícil cuando las empresas y los equipos de seguridad se enfrentan a incógnitas de las que la organización no tiene prácticamente ninguna percepción. Las tres historias de esta edición del **informe Estado de Internet en materia de seguridad** cubren temas que creemos que las organizaciones no conocen con la profundidad que debieran.

Tráfico de API por agente de usuario

TIPO	AU	
Navegador	Chrome	13 %
	Safari para móvil	8 %
	Firefox	2 %
	Internet Explorer	2 %
	Edge	1 %
	Safari	1 %
	IE Mobile	0 %
Sin navegador	Otros	66 %
	CFNetwork	3 %
	HttpClient de Apache	2 %

Figura 1: La mayor parte del tráfico de API está dirigido a aplicaciones personalizadas y no es fácilmente categorizable.

Aumento del tráfico de API

Nuestro estudio de octubre de 2018 sobre el tráfico de API reveló que el 83 % de las visitas que vemos proceden de API.

Para los profesionales de la seguridad, el crecimiento del volumen del tráfico de API es importante a la hora de analizar riesgos, ya que algunas herramientas no pueden gestionarlo. Si las herramientas actuales no son capaces de gestionar este tráfico, significa que una organización podría estar ignorando una fuente importante de tráfico malicioso. Con la proliferación de dispositivos del IoT, todas las organizaciones tendrán que enfrentarse al tráfico de API para mantener a sus empresas y clientes protegidos.

Herramientas de destrucción masiva del sector retail

En este informe, hemos observado con mayor detenimiento la relación de los ataques de abuso de credenciales con el sector retail. Akamai detectó cerca de 28 000 millones de ataques de abuso de credenciales entre mayo y diciembre de 2018, lo que se traduce en más de 115 millones de intentos diarios de piratear las cuentas de usuarios o iniciar sesión en ellas.

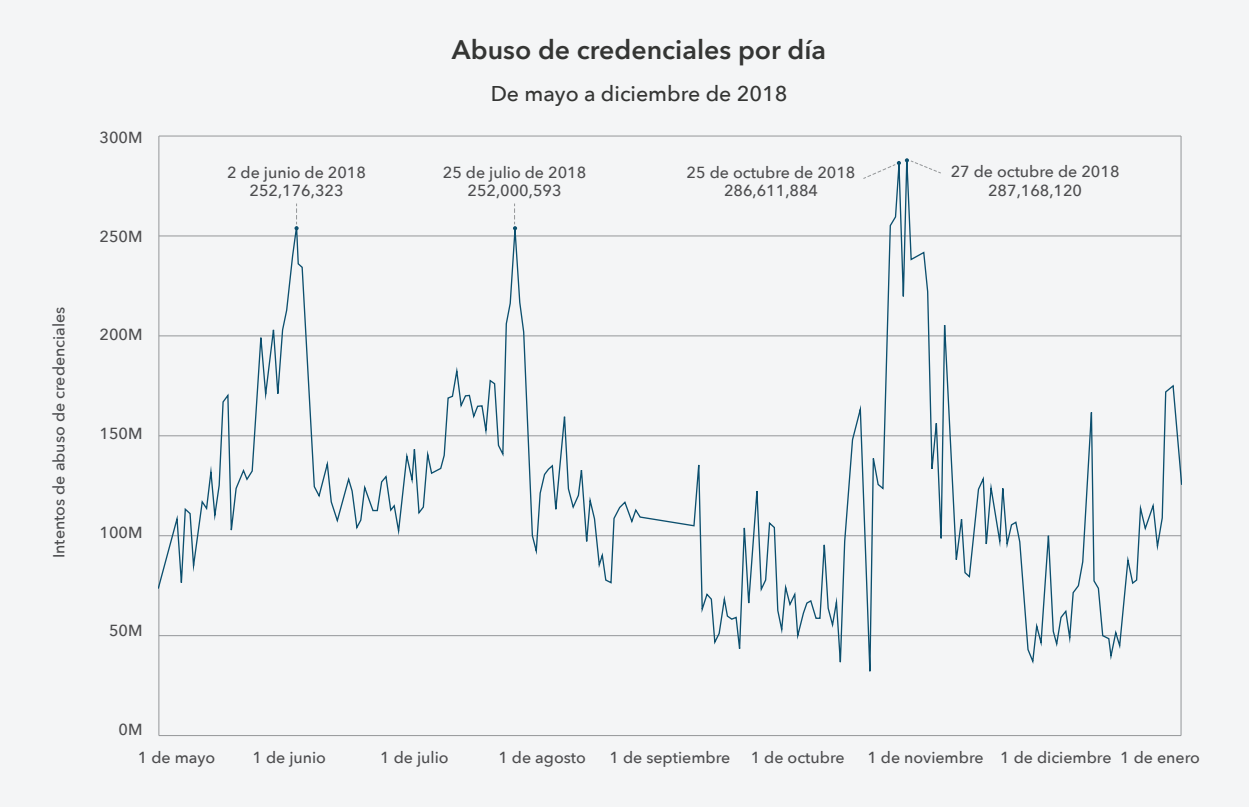

Figura 2: Destacan cuatro días con un mayor número de ataques de abuso de credenciales entre el 1 de mayo y el 31 de diciembre de 2018.

¿Y cuál fue el sector más afectado? El sector retail ocupa el primer puesto del ranking, con 10 000 millones de ataques de abuso de credenciales dirigidos hacia dicha industria. El sector de ropa observó 3700 millones de intentos, lo que lo convierte en el sector más afectado dentro de la industria de retail durante el mismo periodo de tiempo. Akamai también identificó intentos de abuso de credenciales contra sitios web de comercio directo (1427 millones), grandes almacenes (1426 millones), tiendas de material de oficina (1300 millones) y moda, tales como joyas y relojes (129 725 233).

Los agentes maliciosos están utilizando herramientas conocidas como AIO, o bots All-in-One, para acceder a las cuentas y automatizar la compra. Algunos usos de AIO estimulan el mercado de reventa, mientras que otros AIO se utilizan para controlar las cuentas existentes o recopilar información personal y financiera de gran valor.

¿Se ha contabilizado correctamente el tráfico IPv6?

Los investigadores también analizaron el tráfico de DNS y observaron un hecho interesante: el tráfico de IPv6 podría no estar contabilizándose de manera adecuada, ya que muchos sistemas con capacidad para IPv6 todavía prefieren utilizar IPv4. Dado que IPv6 aún se percibe como una solución de tráfico minoritaria, no constituye un punto fuerte de venta para una serie de herramientas de seguridad.

Una mirada hacia el futuro

Actualmente, el sector de la seguridad abarca prácticamente todo, y la seguridad ha adquirido un gran protagonismo en relación con la planificación y el crecimiento empresariales. Los días en que las empresas podían considerar la seguridad como un aspecto de otro orden han pasado a la historia.

Cada una de las historias de esta edición del informe Estado de Internet en materia de seguridad se centra en aspectos de seguridad que podrían estar pasándose por alto y que, sin embargo, son importantes para las operaciones diarias. Estas historias sirven de telón de fondo a nuestras expectativas en relación con los próximos trimestres y años.

Si desea obtener más información sobre las metodologías usadas para recabar los datos del informe, hemos incluido una sección completa con datos detallados.

Para acceder a una perspectiva más pormenorizada de estos datos, consulte el informe Estado de Internet en materia de seguridad: Tráfico de API y ataques al sector retail completo.

Akamai

Akamai, la mayor plataforma de entrega en la nube del mundo y en la que confían más usuarios, ayuda a los clientes a ofrecer las mejores y más seguras experiencias digitales en cualquier dispositivo, en cualquier momento y en cualquier lugar. La plataforma ampliamente distribuida de Akamai ofrece una escala inigualable para garantizar a sus clientes el máximo rendimiento y protección frente a las amenazas. La cartera de soluciones de rendimiento web y móvil, seguridad en la nube, acceso empresarial y distribución de vídeo de Akamai está respaldada por un servicio de atención al cliente excepcional y una supervisión ininterrumpida durante todo el año. Para descubrir por qué las principales instituciones financieras, líderes de retail online, proveedores de contenidos multimedia y de entretenimiento, y organizaciones gubernamentales confían en Akamai, visite www.akamai.com y blogs.akamai.com, o siga a @Akamai en Twitter. Publicado en febrero de 2019.