http://www.silicon.es/ataque-ddos-masivo-dirigido-hacia-rio-2016-nunca-ocurrio-2318627

El ataque DDoS masivo dirigido a las Olimpiadas de Río 2016 que nunca ocurrió

22/09/16

Nerea Bilbao, 22 de septiembre de 2016, 8:52 am
Seguridad

image: http://www.silicon.es/wp-content/uploads/2015/05/Fuente-Shutterstock_Autor-e-X-p-o-s-e_Brasil-684x513.jpg

0 3 1 No hay comentarios

Las empresas de seguridad ocupan un lugar destacado durante la celebración del NetEvents.

Especial desde Silicon Valley

Normalmente la prensa informa de ciberataques que acaban de tener lugar. Pocas veces repara en los ciberataques que pudieron ser pero nunca fueron.

Esta es una historia sobre **prevención**.

Las grandes firmas de seguridad lo predijeron: Río 2016 iba a ser el blanco del cibercrimen. "Los cibercriminales que trabajaron en los Juegos Olímpicos de Londres frente a los que trabajarán en Río son **como comparar un caballo con un Ferrari**", declaró al New York Post el vicepresidente de la unidad de Seguridad de IBM.

Tenía varias razones para semejantes declaraciones. Para empezar, el timing. Los grandes acontecimientos mundiales son siempre un blanco de los hackers. Para seguir: Brasil ocupa la **cuarta plaza en el Top de los principales países receptores de cibercrímenes** a nivel mundial, con un incremento del 274% en el último año.

La firma de seguridad Kaspersky fue más allá al desvelar los detalles sobre el cibermercado negro que iba a surgir a partir de Río 2016. Puso hasta precio de mercado a los servicios de hosting, comprobación de tarjetas de crédito robadas y de codificación.

Pero las Olimpiadas de Río de Janeiro de 2016 no fueron noticia. No al menos por algún ciberataque. Y no fue porque no ocurrió.

"Río fue víctima de ataques DSoS sostenidos, sofisticados y de gran alcance", ha dicho Brian McCann, presidente de la unidad de negocio de Seguridad de NetScout, Arbor Networks, en su intervención durante el NetEvents que tiene lugar estos días en Silicon Valley.

Cuando McCann habla de gran alcance, lo hace refiriéndose a ataques de 540 Gigabits por segundo. "**Una botnet de IoT fue la responsable de la mayoría de ataques preliminares a los juegos"**, nos cuenta en su intervención.

Si no fue noticia es porque el equipo de Arbor Networks trabajó duro antes de la celebración de los Juegos. Estudiaron los servidores, los servicios, las aplicaciones y las políticas de acceso a la red. Integraron herramientas propias de detección de anomalías con otras del equipo de servicios para mitigar de ataques DDoS en la nube. **Crearon equipos virtuales que garantizaran la correcta implementación de la infraestructura de red** (desde canales de comunicación hasta procedimientos operacionales).

Si el equipo de **Arbor Networks** tuviera que enumerar los aspectos que llevaron al éxito la prevención de este ataque masivo, citarían tres: la combinación de un equipo preparado con las mejores soluciones de defensa frente a ataques DDoS y un equipo interorganizacional, que comparte información entre sí para un fin común.

La prevención es la clave, AI es la herramienta

La primera jornada del NetEvents que se celebra estos días en Silicon Valley ha arrancado con dos ponencias sobre Inteligencia Artificial (AI, por sus siglas en inglés) y Ciberseguridad.

Sobre el escenario Kathryn Hume, presidenta de Fast Fordward Labs, y Stuart McClure, CEO de Cylance.

Para Hume **la Inteligencia Artificial es como una fábula.** Hace falta un caso práctico para aplicarla, un lugar en que implementarla de forma efectiva.

Y el segmento de la ciberseguridad es el lugar.

Así, la sesión ha versado sobre las capacidades de las herramientas de inteligencia artificial en general y sobre su aplicación al sector de la ciberseguridad en particular. **"La ciberseguridad es el mejor lugar donde implementar AI"**, ha dicho McClure. "No sé por qué nadie lo había hecho antes".

Cylance es, en efecto, la pionera en implementar tecnologías de inteligencia artificial para la prevención de ciberataques. No les va nada mal. Es una **compañía nacida hace apenas 3 años** que ya tiene un valor de mercado de 1.100 millones de dólares.

Las técnicas tradicionales, sostiene, comparan un comportamiento con otro del pasado. Si se parece a algo del pasado que fue calificado de malicioso, se considera que lo es.

Este enfoque es cojo, defiende el ejecutivo, ex CTO de McAfee. **"Nosotros no necesitamos que haya una víctima para saber que algo es malicioso"**.

Lea más en http://www.silicon.es/ataque-ddos-masivo-dirigido-hacia-rio-2016-nunca-ocurrio-2318627#QI41DqSpvYRepQXK.99