NOTA DE PRENSA
28 / 07 / 2021

¿Cómo se ha preparado Japón para combatir los ciberataques durante los Juegos Olímpicos?

> Japón es un país caracterizado por estar siempre a la vanguardia tecnológica, la cual ha aplicado a este evento deportivo a nivel mundial

Los Juegos Olímpicos de Tokio 2020 no solo son el mayor evento deportivo a nivel mundial, también se alzan como una nueva oportunidad para los actores maliciosos, que buscan en los grandes eventos internacionales, así como en días señalados en el calendario global como el Black Friday, un filón para realizar sus ciberataques. Para contrarrestar las posibles amenazas en materia de ciberseguridad Japón, que se ha caracterizado siempre por estar a la vanguardia tecnológica, se ha volcado en la mejora de sus infraestructuras críticas para garantizar unos Juegos ciberseguros del 23 de julio al 8 de agosto.

El aplazamiento de los Juegos, que inicialmente pudiera ser visto como un inconveniente provocado por la Covid-19, finalmente ha permitido al país nipón ganar ventaja a los ciberdelincuentes al tener más tiempo para actualizar su infraestructura digital. De hecho, ya en 2020, para ganar tiempo y estar bien preparado, Japón buscó la cooperación bilateral con Estados Unidos y otras naciones para poner en marcha sus prioridades de ciberseguridad. Asimismo, realizó un nuevo acuerdo con el Departamento de Seguridad Nacional de Estados Unidos con el propósito de mejorar el intercambio de indicadores de ciberamenazas entre gobiernos, con el objetivo de estar preparado de forma cibernética de cara a la celebración de estos Juegos.

Además, el país ha creado un Consejo de Ciberseguridad encargado de coordinar los esfuerzos de defensa y restauración de los sistemas entre las distintas organizaciones y de aplicar la legislación internacional cuando sea necesario durante Tokio 2020. Para estar prevenidos, el Instituto Nacional de Tecnología de la Información y las Comunicaciones nipón inspeccionó más de 200 millones de dispositivos conectados a la red a lo largo de 2019, realizando pruebas para detectar combinaciones

inseguras de nombre de usuario y contraseña principalmente en puntos de acceso público a Internet y a través de proveedores de servicios de Internet.

Por su parte, el Comité Olímpico Internacional (COI) también ha identificado la ciberseguridad como un área prioritaria y ha invertido para proporcionar el mejor entorno ciberseguro para Tokio 2020. Aunque el COI no ha revelado los detalles específicos de su plan de ciberseguridad, debido a su criticidad.

Impacto de los ciberataques

Las amenazas cibernéticas a este tipo de eventos no son nada nuevo. En los Juegos Olímpicos de Invierno de 2018 en PyeongChang (Corea del Sur) se produjo el mayor aluvión de ataques: ciberdelincuentes rusos atacaron las redes olímpicas antes de la ceremonia de apertura, lo que ralentizó la entrada de espectadores y dejó fuera de servicio las redes Wi-Fi, afectando a la retransmisión.

A pesar de esta minuciosa preparación por parte de Japón, cualquiera puede ver en los Juegos Olímpicos una oportunidad para llevar a cabo un ataque. El país del sol naciente ya se ha enfrentado a múltiples amenazas durante los preparativos de Tokio 2020, sobre todo las que provienen de las actividades de reconocimiento cibernético que estarían relacionadas supuestamente con Rusia.

Aunque se han revelado pocos detalles sobre las tácticas, técnicas y procedimientos específicos utilizados para atacar los Juegos Olímpicos de Tokio, sus objetivos abarcaban desde los organizadores, hasta los servicios logísticos y los patrocinadores de los Juegos. Las autoridades creen que se pretendía sabotear los Juegos Olímpicos, de forma similar a los ciberataques llevados a cabo en PyeongChang.

En el caso de Tokio 2020, las operaciones ofensivas podrían ser a través del robo y filtración de datos, la desinformación o la interrupción de los sistemas implicados en los eventos deportivos. Ya en abril de 2021, el Comité Olímpico Japonés sufrió un ataque de ransomware, uno de los principales riesgos durante la celebración de estos Juegos Olímpicos. A esto se le añaden problemas de seguridad física, por ello, los organizadores, los proveedores y los asistentes deben ser conscientes de las posibles amenazas, especialmente en un año tan excepcional como este.

En este sentido, ZeroFox puede ser un buen aliado ya que está especializado en la protección contra riesgos digitales (DRP) que se producen en plataformas de colaboración, redes sociales, redes con contenido no indexable (Deep y Dark Web), correo electrónico y móviles. Concretamente, su solución identifica y remedia los ataques phishing dirigidos, el compromiso de credenciales, la exfiltración de

datos, el secuestro de marcas o las amenazas a ejecutivos, gracias al manejo de diversas fuentes de datos y al análisis basado en la Inteligencia Artificial. Además, su tecnología es capaz de procesar y proteger millones de posts, mensajes y cuentas del panorama social y digital tales como LinkedIn, Facebook, Slack, Instagram, Pastebin y YouTube, así como tiendas de aplicaciones móviles, entre otros.

Contacto de prensa:

JAVIER MODUBAR ALVAREZ
info@ingecom.net
944395678
http://www.ingecom.net