STORMSHIELD

ARTÍCULOS DE OPINIÓN

CIBERSEGURIDAD Y JUEGOS OLÍMPICOS: COMENTARIOS ANTES DE PARÍS 2024

Victor Poitevin
Editorial & Digital Manager, Stormshield

Los Juegos Olímpicos y Paralímpicos de verano de 2024 en París representan el mayor evento que se celebrará en Francia desde 1900. Las cifras resultan asombrosas: 7000 millones de euros de presupuesto, 4000 millones de telespectadores, 12 millones de espectadores, 30 000 voluntarios, 10 000 atletas, 206 naciones, 40 sedes de competición que se deben proteger... Pero tampoco hay que olvidar las relacionadas con la cuestión cibernética: tras los 500 millones de ataques de 2016 en Río, en los Juegos de Tokio de 2021 fueron más de 4000 millones de ciberataques. De ahí la importancia de la ciberseguridad en este evento mundial.

Recientemente, los incidentes de la final de la Champions League de fútbol en 2022 pusieron de manifiesto las limitaciones de la gestión de los incidentes físicos. Junto con la cuestión cibernética y los posibles incidentes informáticos, llegan incluso a poner en tela de juicio la capacidad de organizar los Juegos Olímpicos de 2024. Pero ¿cómo se prepara Francia para la organización de un acontecimiento así? **¿Qué ciberseguridad se implantará para París 2024?** ¿Qué medidas se han emprendido para hacer frente a los ciberataques y protegerse de ellos?

¿CUÁLES SON LOS RIESGOS CIBERNÉTICOS DE CARA A LOS JUEGOS OLÍMPICOS?

Durante un evento mundial de este tipo, los ciberataques pueden materializarse (y ya lo han hecho) de diferentes formas. *Phishing, spoofing*, denegación de servicio (DDoS), interceptación de flujos Wifi/4G/5G, vulneración de cajeros automáticos... los medios de ataque son numerosos. **Vincent Riou**, socio de Avisa Partners encargado de las actividades de ciberseguridad y coautor de un artículo estratégico sobre el tema, analiza el atractivo de los Juegos Olímpicos para los ciberdelincuentes. «*Los Juegos Olímpicos representan para el país anfitrión el equivalente a la organización de unos 60 mundiales de fútbol al mismo tiempo. Son, por tanto, un formidable potenciador de imagen para el país que los acoge, con miles de millones de telespectadores. No obstante, también significa que el más mínimo problema se transmite a todo el planeta*»**. Porque los Juegos Olímpicos atraen a distintos tipos de ciberdelincuentes con diferentes motivaciones.**

Karim Benslimane, Director de Ciberinteligencia de Darktrace, detalló una triple ciberamenaza durante una conferencia en Lille (Francia) en 2022: «*En primer lugar, tenemos grupos de ciberterroristas afiliados a Estados y con motivaciones geopolíticas con el objetivo de desestabilizar el país. En segundo lugar, tenemos a los ciberdelincuentes oportunistas y mercantiles, tentados por las ganancias financieras. Apuestan, por ejemplo, por la urgencia de los organizadores por restablecer la situación para animarles a pagar el rescate lo antes posible. Y por último, en tercer lugar, los grupos hacktivistas tienen reivindicaciones ideológicas y militantes, que pueden llevar a cabo ataques como la desfiguración de sitios web o la denegación de servicio*».

«Los Juegos Olímpicos representan para el país anfitrión el equivalente a la organización de unos 60 mundiales de fútbol al mismo tiempo. Son, por tanto, un formidable potenciador de imagen para el país que los acoge, con miles de millones de telespectadores. No obstante, también significa que el más mínimo problema se transmite a todo el planeta.»

Vincent Riou, socio de Avisa Partners encargado de las actividades de ciberseguridad

Para los organizadores de este evento extraordinario, los riesgos cibernéticos son omnipresentes. Captura de vídeo para la televisión o los árbitros, cámaras videovigilancia y sistemas de alarma, lectores de tarjetas de identificación y billetes... Cada equipo conectado es un punto de entrada potencial para los ciberdelincuentes. A esto hay que añadir la logística y la cadena de subcontratación, que aumentan considerablemente la superficie de ataque. Además, esta edición de París incluye eventos deportivos en el corazón de las joyas del patrimonio francés, y no solo en estadios cerrados. El tiro con arco en Los Inválidos, el voleibol de playa a los pies de la Torre Eiffel, la esgrima en el Grand Palais, la ceremonia de inauguración en el Sena... Estos escenarios abiertos en la capital conllevan su propia serie de dificultades para su protección. Para Vincent

Riou: «*La celebración de los Juegos Olímpicos en lugares emblemáticos de la ciudad es algo genial para los espectadores. Pero protegerlos resulta muy complejo. Cuando haya multitudes de espectadores en las orillas del Sena, imagine los diferentes puntos de acceso. ¿Cómo protegemos todo eso? Cámaras de videovigilancia, puertas de acceso, bases de datos para ver quién tiene derecho a entrar o no en según las tarjetas de identificación, retransmisiones televisivas... todo está digitalizado y, por tanto, vulnerable a posibles ataques*». El aumento de la digitalización y la desmaterialización augura, por tanto, **un aumento del nivel de riesgos cibernéticos para los organizadores**.

Los aficionados, los espectadores o los telespectadores también son víctimas potenciales en este caso, y pueden sufrir el impacto de los ciberataques que provocan, por ejemplo, la interrupción de las emisiones televisivas. Pero también pueden ser objetivo directo de ciberataques a través de campañas de phishing, como explica **Nicolas Caproni**, responsable del equipo de investigación y detección de amenazas (TDR) de SEKOIA.IO: «*De forma oportunista, los ciberdelincuentes aprovecharán el evento para enviar campañas de phishing, recurriendo a concursos para aumentar las posibilidades de que abran los mensajes y hagan clic en enlaces comprometedores. También pueden esconder malware en un pdf como parte de una estafa para vender o revender entradas. Asimismo, tratarán de recopilar datos personales, datos de tarjetas de crédito que luego tendrán valor en la darknet*». Otra amenaza que se contempla es la difusión de información falsa. «*Algunos grupos de atacantes se han especializado en la desinformación y las noticias falsas. Estas nuevas armas pueden utilizarse para perturbar los eventos mediante la filtración de datos que no deberían haberse comunicado o la falsificación de datos. Debido a la complejidad de la implementación, en este caso se trata más bien de ataques estatales*».

Por último, las amenazas durante los Juegos Olímpicos y Paralímpicos también afectan a los deportistas. Vincent Riou menciona algunos ejemplos de posibles ataques a estos últimos: «*Las llaves de acceso a los hoteles, el aire acondicionado, las alarmas contra incendios, los marcadores digitales, los cronómetros... Todo está digitalizado. Imagínese las consecuencias de una alteración de la cadena de frío en el suministro de alimentos para ciertas delegaciones o la activación de las alarmas de incendio en los hoteles de ciertos deportistas el día antes de una competición importante*».

Organizadores, espectadores, aficionados y deportistas se ven afectados por los riesgos cibernéticos durante los Juegos Olímpicos.

UNA DÉCADA DE CIBERATAQUES EN LOS JUEGOS OLÍMPICOS

La cuestión de la ciberseguridad en los Juegos Olímpicos y Paralímpicos se viene planteando desde hace diez años. De hecho, en 2004, durante los Juegos de Atenas, el principal riesgo de perturbación tecnológica estuvo vinculado con la zona sísmica. En 2008, con motivo de los Juegos Olímpicos de Pekín, se crearon algunos sitios ficticios para la compra de billetes falsos. Pero la ciberseguridad no pasó a ser una de las prioridades de los organizadores hasta el ataque a la ceremonia de apertura de los Juegos de Londres en 2012. **En 10 años, el número de ciberataques se ha multiplicado por 20**, pasando de 212 millones durante los Juegos de Londres 2012 a 4400 millones en los de Tokio en 2021.

Londres 2012 fue el evento que marcó el inicio del enfoque de los ciberdelincuentes en los Juegos Olímpicos. En ese momento, se registraron más de 212 millones de ciberataques el día de la ceremonia de apertura, marcada por múltiples ofensivas, como una denegación de servicio distribuido (DDoS) en la infraestructura eléctrica.

Posteriormente, en 2014, en los Juegos Olímpicos de Invierno **de Sochi,** no se produjo ningún incidente importante de ciberseguridad. ¿Comunicación cerrada del Estado ruso, desinterés de los ciberdelincuentes o miedo a represalias? La pregunta sigue en el aire... Parte de la respuesta se encuentra en las declaraciones del FSB (Servicio Federal de Seguridad), cuyo plan era «*garantizar que ninguna comunicación, ya sea por parte de los competidores o de los espectadores, escapara a la vigilancia*» apoyándose en un sistema de interceptación de las comunicaciones especialmente reforzado para la ocasión. Esto fue suficiente para que el Servicio de Seguridad Diplomática de Estados Unidos pidiera a sus ciudadanos que extremaran la precaución durante los Juegos Olímpicos. Los deportistas y los ciudadanos estadounidenses se concienciaron sobre la no divulgación de datos confidenciales, incluyendo el consejo de quitar la batería del teléfono móvil tan a menudo como fuera posible.

En 2016, en los Juegos de **Río**, las cifras se dispararon, con 500 millones de ciberataques registrados. Esto corresponde a 400 ataques por segundo. Varios meses antes de la ceremonia de apertura, se produjeron ataques DDoS consecutivos y a gran escala contra los sitios web de las organizaciones asociadas a los Juegos Olímpicos. Los ataques efectuados por la red de bots LizardStresser (que ya había sido noticia tras el bloqueo de las plataformas de juego *online* PSN y Xbox Live) se intensificaron durante los Juegos Olímpicos, incluida una campaña de DDoS de más de 500 Gbps.

En 2018, el fenómeno se intensifica para la opinión pública, ya que la ceremonia de apertura de los Juegos de **Pieonchang** fue objeto de ataques. Algunos espectadores no pudieron imprimir sus entradas para entrar en el estadio, hubo un problema con el Wifi en el emplazamiento, la ceremonia no se retransmitió en las pantallas del estadio, el sensor RFID de las puertas de acceso no funcionaba, la aplicación oficial de los Juegos Olímpicos tampoco (es decir, el acceso a las taquillas, los horarios, la información sobre los hoteles, las tarjetas de acceso, etc.). Las consecuencias fueron evidentes desde el primer momento. El *malware* Olympic Destroyer causa estragos, en directo, ante miles de espectadores y periodistas. Los equipos de ciberseguridad necesitan 12 horas de duro trabajo para reconstruir la infraestructura informática de los Juegos Olímpicos a partir de las copias de seguridad. Este inusual ataque se convirtió inmediatamente en un asunto de calado internacional. Atribuido a Rusia, se realizó en represalia por la prohibición de su bandera en esta edición, tras los casos de dopaje en Sochi.

En 2021, los Juegos Olímpicos de **Tokio**, aplazados un año por la pandemia mundial, se celebraron a puerta cerrada. A pesar de ello, esta edición no estuvo exenta de ataques, ya que se lanzaron 4400 millones de ciberataques contra la organización. Según la Nippon Telegraph and Telephone Corporation (NTT), se utilizaron varios medios de ataque, como correos electrónicos de suplantación de identidad y sitios web falsos que imitaban los sitios oficiales de los Juegos. Un alto funcionario japonés indicó que los Juegos Olímpicos fueron víctimas de un ciberataque que provocó una filtración de datos personales de los titulares de entradas y voluntarios del evento (nombre, dirección, número de cuenta bancaria). Estos datos se divulgaron *online*.

Por último, en 2022, durante los Juegos de Invierno **de Pekín,** fue la aplicación oficial de lucha contra la COVID-19, My2022, la que suscitó polémica por el temor al ciberespionaje. Un estudio de ingeniería inversa de la aplicación demostró posteriormente que las conversaciones de los deportistas se recopilaban, analizaban y guardaban en servidores chinos. Para ello, las autoridades de muchos países dieron instrucciones a sus delegaciones, como la recomendación de llevar un dispositivo telefónico desechable.

¿CÓMO SE ESTÁ PREPARANDO LA SEGURIDAD DE LOS JUEGOS OLÍMPICOS DE PARÍS 2024?

El Comité Organizador de los Juegos Olímpicos (COJO) se está preparando para los ciberataques apoyándose en las lecciones aprendidas en ediciones anteriores. **Tony Estanguet,** presidente del COJO de París 2024, fue claro en su entrevista con AFP en abril de 2021: «*No tenemos ninguna duda de que seremos atacados continuamente. No debe haber ningún resquicio de entrada posible en los empleados, el software o el ecosistema*». En el Ministerio del Interior francés, **Ziad Khoury**, prefecto y coordinador nacional de la seguridad de los Juegos Olímpicos y Paralímpicos de 2024 (CNSJ), también insiste en la necesidad de la ciberseguridad durante los grandes eventos y especificó durante una reunión del Cercle des Assises de la Cybersécurité en septiembre de 2021 que «*cada edición de los Juegos Olímpicos es nueva, en el sentido de que no se puede comparar con las anteriores: el contexto cambia, las amenazas evolucionan, son cada vez más variadas y los ataques son más numerosos. Podemos aprender de experiencias anteriores, pero sobre todo debemos estar preparados para lo desconocido, porque algunas de las amenazas de 2024 aún no se conocen*». A esto se suman los conflictos geopolíticos en Ucrania y la recomendación del Comité Olímpico Internacional (COI) en febrero de prohibir a Rusia y Bielorrusia las competiciones deportivas. Según Nicolas Caproni, «*los ataques de ransomware son una de las amenazas para los Juegos Olímpicos. Pero no serían sino una tapadera para actos de sabotaje destinados a perturbar el evento y dañar la imagen del país y de los Juegos. Si Rusia queda excluida del evento en 2024, podemos temer métodos de represalia*».

> *«No tenemos ninguna duda de que seremos atacados continuamente. No debe haber ningún resquicio de entrada posible en los empleados, el software o el ecosistema.»*
>
> **Tony Estanguet,** presidente del COJO de París 2024

Para hacer frente a los ciberataques cada vez más complejos e innovadores, las autoridades francesas se están organizando. Así, la ANSSI ha firmado un acuerdo de cooperación con su homólogo japonés, el NISC (*National center of Incident readiness and Strategy for Cybersecurity*). Se trata de una oportunidad para reforzar

los intercambios y la puesta en común de experiencias en torno a la ciberseguridad para los grandes acontecimientos deportivos, como la Copa del Mundo de Rugby y los Juegos Olímpicos. Al mismo tiempo, la ANSSI está reforzando sus comunicaciones **para concienciar al mayor número posible de personas sobre la higiene digital**. Existen muchos materiales disponibles, como el pasaporte de consejos a los viajeros, las 12 reglas de sentido común para aplicar en la vida digital diaria o la guía de buenas prácticas informáticas. El Ministerio del Interior francés afirma querer desarrollar la denominada «videoprotección inteligente». Estas cámaras serían capaces de detectar comportamientos sospechosos y movimientos de multitudes en tiempo real utilizando la inteligencia artificial. El uso del reconocimiento facial en los espacios públicos, que se había abandonado ante la ausencia de una legislación adecuada sobre las garantías de respeto a las libertades individuales, vuelve a estar en el punto de mira. Según Vincent Riou, que cita el trabajo de la Alliance pour la Confiance Numérique (ACN), «*sería conveniente impulsar nuestras tecnologías nacionales, porque los Juegos Olímpicos representan un magnífico escaparate para nuestra industria cibernética francesa y, más globalmente, para nuestra industria de seguridad digital*».

En cuanto a la organización, el **presupuesto de la edición de París para la ciberseguridad asciende a más de 17 millones de euros.** Este incluye un programa de prevención y defensa con simulaciones a escala real, código de aplicación seguro, un esfuerzo por sellar las capas de la red y servidores en el diseño de las infraestructuras, auditorías de seguridad y la creación de SOC. Asimismo, se aplica un programa de concienciación con formación para empleados, patrocinadores, subcontratistas, deportistas y todas las partes interesadas, y se acompaña de estrictas especificaciones impuestas a toda la cadena de subcontratistas. **Anne Le Hénanff**, titular de la cátedra de ciberseguridad para grandes eventos de la Universidad de Bretaña Sur, insistió en el papel de las autoridades locales que van a acoger a las delegaciones en su territorio y en la importancia de implicarlas en el tema cibernético. Con motivo de una conferencia el pasado febrero sobre «*El éxito de los Juegos Olímpicos de París 2024: una cuestión crucial de ciberseguridad*», destaca lo siguiente: «*Mientras su atención se centra legítimamente en cuestiones de seguridad física y otras de gestión de los flujos de personas, las autoridades locales no están para nada concienciadas sobre las cuestiones de ciberseguridad. Su mayor competencia en este ámbito es un requisito previo para el éxito de los Juegos Olímpicos*».

Al igual que en ediciones anteriores, la amenaza cibernética para los Juegos Olímpicos y Paralímpicos de París 2024 es la perturbación pública. **Ante el riesgo de ataques u otros problemas de seguridad interna, la ciberseguridad no debe considerarse de forma aislada, sino como parte integral del programa de seguridad del evento.** Para Vincent Riou, es impensable separar la seguridad física de la cibernética y se debe tener en cuenta el carácter cada vez más híbrido de las ciberamenazas. «*Algunos delincuentes podrían tener la tentación de atacar ciertos sistemas para acceder a los recintos sin derecho de acceso, o provocar la salida de los espectadores y que se reúnan fuera de los recintos protegidos, facilitando así los ataques terroristas. Los ciberataques pasan pues a ser facilitadores de ataques de alto impacto. La ciberseguridad es una parte integral, no separada, del sistema general de seguridad de los Juegos*».

En el reciente informe de los senadores Meurant y Cardon sobre ciberseguridad, la ambición declarada es claramente «*posicionar a la industria francesa como líder mundial en ciberseguridad y en la seguridad del Internet de las cosas*». Los Juegos Olímpicos de París 2024 serían una gran oportunidad para ello. Las autoridades francesas, el COJO, las empresas colaboradoras y patrocinadoras, las empresas de ciberseguridad... todas las partes se han unido para hacer de este evento un lugar seguro y dar paso a las festividades. Tras el episodio (fallido) de la final de la Champions League, el Mundial de Rugby de 2023 se presenta como una oportunidad de recuperación.