Juan Antonio Calles. Doctor en informática y CEO de Zerolynx.
Helena Jalain. Ingeniera de Telecomunicación y analista de ciberseguridad de Zerolynx.

La ciberdelincuencia pone el foco en los eSports

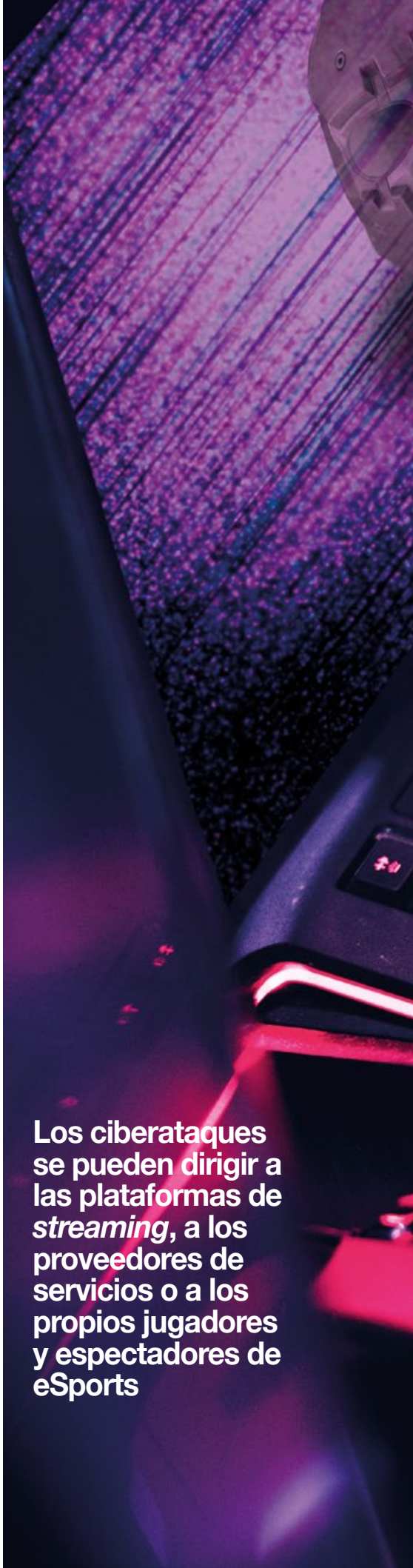
Los deportes electrónicos, conocidos mundialmente como eSports, atraen cada día a más jugadores, seguidores y ciberdelincuentes. El sector mueve cifras millonarias, pero por ahora no ha invertido lo suficiente para garantizar la seguridad de unas infraestructuras que ya han sufrido algunos grandes ataques en los últimos meses.

El mercado de los eSports se encuentra en plena expansión, tanto en España como en el resto del mundo. Desde el año 1997, momento en el que nació la Electronic Sports League (ESL), la primera liga independiente de eSports y la más grande del mundo, el sector ha crecido a pasos agigantados, cobrando adeptos, amantes del *gaming* competitivo, cuyas edades pueden diferir hasta en varias décadas. Si bien la pandemia propiciada por la Covid-19 frenó el crecimiento de los eSports, que con la cancelación de los torneos presenciales y, según datos del diario Palco23, cayeron un 23%, se trata de un sector en crecimiento que en España genera ya un negocio de más de 35 millones de euros, y en el mundo, de casi 800 millones de euros.

España, referente en eSports

España es referencia en el sector, representa en torno al 4% del mercado mundial de los eSports. Tiene tres millones de aficionados y cuenta con su propia federación, la Federación Española de Jugadores de Videojuegos y eSports (FEJUVES), afiliada a la Federación Internacional de eSports (IESF) y encargada de escoger a la selección nacional de los diferentes títulos. Recientemente, el representante español José Carlos Sánchez, y jugador del FC Bayern Munchen Esports, consiguió la medalla de bronce en la competición con el videojuego Pro Evolution Soccer. Así mismo, cuenta con numerosos campeones del mundo en diferentes disciplinas, como es el caso de Akawonder (Esteban), dos veces campeón del mundo de Hearthstone, o Alfonso Ramos, doble campeón del Mundo de FIFA, y con numerosos equipos de referencia internacional, como Riders, Heretics, Giants o Mad Lions.

Sin embargo, los deportes electrónicos no son el único exponente del sector *gaming*, dado que son también muy populares los torneos ajenos a las ligas, en muchas ocasiones privados y orga-



Los ciberataques se pueden dirigir a las plataformas de *streaming*, a los proveedores de servicios o a los propios jugadores y espectadores de eSports

nizados por *influencers*. Estos torneos, *hosteados* generalmente sobre servidores de *roleplay*, son muy populares entre la comunidad de la red social Twitch, dado que cuentan con *owners* de la entidad de Ibai Llanos, Grefg, Auronplay o Rubius, *influencers* con millones de seguidores que, con torneos como SquidCraft, Egoland o Tortillaland, han logrado índices de audiencia equiparables al *prime time* de varios canales de televisión.

Objetivo de la ciberdelincuencia

Citando al ilustre poeta y dramaturgo español Francisco de Quevedo, "poderoso caballero es don dinero". Y es que donde hay éxito suele haber dinero, y donde hay dinero se despierta el interés de la delincuencia, en este caso, ciberdelincuencia, dado que no conviene olvidar que los eSports se sostienen sobre videojuegos *(software)*, y estos sobre servidores y redes.

Las vías de ciberataque que pueden afectar al sector son múltiples. En primer lugar, destacarían los ciberataques contra las propias plataformas de *streaming*. Este fue el caso por ejemplo de la plataforma Twitch, *hackeada* en octubre de 2021 y a la que consiguieron robar gran cantidad de datos, incluyendo su código fuente e incluso los pagos realizados a los *streamers*. También son destacados los ciberataques contra los proveedores de servicios, por ejemplo, de internet, como el reciente ataque masivo de DDoS que sufrió Andorra Telecom en enero de 2022, y que afectó a varios torneos organizados por *influencers* de Andorra como El Rubius o AuronPlay. Se trató de un ataque dirigido a los *youtubers* que residen en ese país, y únicamente afectó de forma puntual a parte de la infraestructura de la operadora gracias a que tenían contratados escudos anti DDoS. Así mismo, también son habituales los ciberataques contra los propios *streamers* o jugadores, a los que habitualmente extorsionan tras hacerse con el control de sus cuentas, solicitándoles rescates para poder recuperarlas. Generalmente estos ataques suelen propiciarse tras un *phishing*, una exfiltración de credenciales o, simplemente, por el uso de contraseñas débiles y la ausencia de medidas básicas de seguridad. Finalmente, no se puede olvidar al consumidor final, el espectador o aficionado, la víctima más invisible y que suele sufrir estafas de diferente índole.

Los ciberataques contra los *streamers* o jugadores suelen ser de extorsión tras hacerse con el control de sus cuentas

Las trampas o *chetos* son también un problema para los fabricantes de videojuegos

Falta de madurez

Todos estos problemas denotan que se trata de un sector inmaduro en ciertos aspectos y que precisa de seguir evolucionando a la par que crece. Debe adaptarse a la realidad actual haciendo frente a la ciberdelincuencia, como ya han hecho otros múltiples sectores más veteranos como la banca, las aseguradoras o el sector de las apuestas deportivas, los tres también con una fuerte presencia en internet. En estos casos las medidas de ciberseguridad son más acordes a la realidad delincuencial, y tratan de reducir el impacto de cualquier ataque exitoso con el fin de dar las máximas garantías posibles a sus clientes, dentro de unos criterios lógicos de coste/beneficio.

Son muchos los aspectos en los que el sector debería poner foco en materia de ciberseguridad. En primer lugar, debería centrar esfuerzos para intentar derrotar al enemigo anónimo oculto tras los ataques que sufren los equipos de eSports, las plataformas que *hostean* los torneos y, en resumen, los diferentes agentes que intervienen en la cadena de valor. De muchos de estos ciberataques surgen filtraciones de datos personales, datos de tarjetas de crédito y credenciales que pueden ocasionar infinidad de ataques posteriores contra los usuarios finales. Es cierto que existen mecanismos para proteger al usuario de un robo de identidad en caso de filtrarse y utilizarse sus contraseñas, como es el caso del doble factor de autenticación (2FA), pero no es una medida de ciberseguridad infalible. El 2FA es un mecanismo útil y necesario para proteger las diferentes cuentas utilizadas en internet, como el correo, las redes sociales o las plataformas de videojuegos de un usuario, pero no se puede olvidar que en determinadas circunstancias también puede ser *hackeado*, como ha ocurrido en reiteradas ocasiones con los 2FA enviados por SMS y que muchos delincuentes han logrado evadir mediante duplicados de tarjetas SIM realizados en tiendas de telefonía fraudulentas. Precisamente, y por esta razón, la AEPD sancionó con una multa de 5,81 millones a varias operadoras españolas el pasado mes de febrero de 2022.

El problema de los *chetos*

El sector, y en especial los fabricantes de los videojuegos, tienen también numerosos problemas con las trampas o, como se los conoce en el sector, con los *chetos*. Es un problema que crece en gran medida cuando los videojuegos van teniendo cierta edad, dado que mediante técnicas de ingeniería inversa se consigue estudiar su código fuente, lo que facilita el camino para que se desarrollen aplicaciones que alteren el comportamiento del juego en tiempo real. Estas mejoras suelen introducir ventajas y facilidades en el juego, como los *wall hacks*, con los que los jugadores pueden ver a través de las paredes, o el *aim*, con el que los jugadores pueden apuntar automáticamente a un enemigo. Los fabricantes y las plataformas de torneos suelen diseñar sistemas para verificar que, mediante firma, las librerías y el resto de binarios de los videojuegos no han sido alterados, pero no siempre son eficaces. Además, se sabe que existen también modificaciones basadas en *hardware*, que suelen ser aún más difíciles de detectar ya que el *software* en sí no se altera, sino que se añaden periféricos o chips integrados que permiten leer y escribir directamente en la memoria del sistema o permiten emular el comportamiento del ratón o teclado. Así mismo, la ciberdelincuencia suele aprovechar que estas aplicaciones fraudulentas suelen requerir inhabilitar el antivirus o, como mínimo, crear una regla para permitir su uso, para desplegar en ellas *malware* de todo tipo, de manera que en muchas ocasiones los jugadores que hacen trampas pueden acabar *hackeados*.

Los juegos *freemium* y aquellos que cuentan con un mercado de *skins* también son muy populares entre los jugadores, tanto profesionales como amateurs. Muchas de estas *skins*, como las de algunas armas de videojuegos como Valorant o CSGO, pueden alcanzar precios de cuatro y cinco cifras, en especial aquellas a las que su exclusividad, por ser una edición limitada de un torneo, o simplemente por su bajo número de unidades, las hace especialmente golosas. Recordando al gran Quevedo de nuevo, la ciberdelincuencia ha puesto el diente en este mercado y se cuentan por cientos las páginas de *phishing* que son creadas diariamente con el fin de hacer pensar a los usuarios que son páginas lícitas, y que estos entreguen sus datos de tarjeta o, simplemente, para que compren un activo virtual que nunca les llegará.

El blanco perfecto

Como conclusión, se podría decir que el sector de los eSports lo tiene todo para considerarse un blanco perfecto para la ciberdelincuencia: mueve mucho dinero, su negocio es completamente digital, y todavía no ha alcanzado la madurez de otros sectores que dedican grandes esfuerzos en ciberseguridad. Aunque se han dado importantes avances en los últimos años, tanto los creadores de videojuegos como las ligas, asociaciones y las compañías que *hostean* la infraestructura y servidores, deben aprender a afrontar los nuevos retos que introduce un negocio de estas características.

REFERENCIAS

1. https://hipertextual.com/2022/01/streamers-andorra-hacker-squidcraft-games
2. https://www.palco23.com/entorno/los-esports-en-espana-un-negocio-de-27-millones-de-euros-listo-para-el-despegue
3. https://www.20minutos.es/tecnologia/ciberseguridad/hackeo-masivo-a-twitch-como-han-conseguido-acceder-al-codigo-fuente-y-los-pagos-a-streamers-de-la-plataforma-4847277/
4. https://www.elespanol.com/invertia/empresas/tecnologia/20220203/proteccion-millones-operadoras-duplicados-fraudulentos-tarjetas-sim/647185524_0.html
5. https://blog.esea.net/esea-hardware-cheats/