Microsoft

# Situación actual

## Los eventos y sedes deportivas atraen amenazas cibernéticas a una tasa cada vez mayor

**634.6** MM

### Intentos de autenticación

Microsoft realizó más de 634.6 millones de autenticaciones al tiempo que proporcionó defensas de ciberseguridad para instalaciones y organizaciones qataríes entre el 10 de noviembre y el 20 de diciembre de 2022.

**Microsoft Threat Intelligence**

# Cyber Signals

Agosto 2023

# Introducción

Los actores de amenazas van donde están los objetivos, capitalizando las oportunidades para lanzar ataques dirigidos u oportunistas generalizados. Esto se extiende a eventos deportivos de alto perfil, especialmente aquellos en entornos cada vez más conectados, introduciendo riesgo cibernético para los organizadores, las instalaciones anfitrionas regionales y los asistentes. El Centro Nacional de Seguridad Cibernética del Reino Unido (NCSC por sus siglas en inglés) descubrió que los ataques cibernéticos contra organizaciones deportivas son cada vez más comunes, con el 70 por ciento de los encuestados experimentando al menos un ataque por año, significativamente más alto que el promedio de las empresas en el Reino Unido.

La presión de ofrecer una experiencia fluida y segura en el escenario mundial introduce nuevas apuestas para anfitriones e instalaciones locales. Un solo dispositivo mal configurado, una contraseña expuesta o una conexión de terceros que pase por alto, puede provocar una violación de datos o una intrusión exitosa.

Microsoft brindó soporte de ciberseguridad a instalaciones de infraestructura crítica durante la organización de la Copa Mundial de la FIFA 2022™. En esta edición, ofrecemos aprendizajes de primera mano sobre cómo los actores de amenazas evalúan e infiltran estos entornos en lugares, equipos e infraestructura crítica en torno al evento en sí.

**Todos somos defensores.**

# Panorama de Seguridad

Los datos del panorama representan el número total de entidades y eventos monitoreados 24/7 entre el 10 de noviembre y el 20 de diciembre de 2022. Esto incluye organizaciones directamente involucradas o afiliadas a la infraestructura del torneo. La actividad incluye búsquedas proactivas de amenazas humanas para identificar amenazas emergentes y realizar un seguimiento de campañas notables.

**45**
Organizaciones protegidas

**100,000**
Endpoints protegidos

**144,000**
Identidades protegidas

**14.6 Millones**
de flujos de email

**634.6 Millones**
de Intentos de autenticación

**4.35 Mil Millones**
de conexiones de red

# Información sobre amenazas

## Los actores de amenazas oportunistas explotan el entorno con muchos objetivos

Las amenazas de ciberseguridad a los eventos y sedes deportivas son diversas y complejas. Requieren vigilancia y colaboración constante entre las partes interesadas para prevenir y mitigar una escalada. Con el mercado deportivo mundial valuado en más de USD600 mil millones, el objetivo es rico. Los equipos deportivos, las grandes ligas y las asociaciones deportivas mundiales, y las sedes de entretenimiento albergan un tesoro de información valiosa deseable para los ciberdelincuentes.

La información sobre el rendimiento deportivo, la ventaja competitiva y la información personal son un objetivo lucrativo. Desafortunadamente, esta información puede ser vulnerable a escala, debido a la cantidad de dispositivos conectados y redes interconectadas en estos entornos. A menudo, esta vulnerabilidad abarca múltiples propietarios, incluidos equipos, patrocinadores corporativos, autoridades municipales y contratistas externos. Los entrenadores, atletas y aficionados también pueden ser vulnerables a la pérdida de datos y la extorsión.

Además, las sedes y arenas contienen muchas vulnerabilidades conocidas y desconocidas que permiten que las amenazas se dirijan a servicios empresariales críticos, como dispositivos de punto de venta, infraestructuras de TI y dispositivos de visitantes. No hay dos eventos deportivos de alto perfil que tengan el mismo perfil de riesgo cibernético, que varía según factores como la ubicación, los participantes, el tamaño y la composición.

Para centrar nuestros esfuerzos en la Copa del Mundo FIFA Qatar 2022™, realizamos una búsqueda proactiva de amenazas a través de la cual evaluamos el riesgo utilizando Defender Experts for Hunting, un servicio gestionado de búsqueda de amenazas que busca de forma proactiva amenazas en endpoints, sistemas de email, identidades digitales y apps en la nube. En este caso, los factores incluyeron la motivación del actor de amenazas, el desarrollo del perfil y una estrategia de respuesta. También consideramos la inteligencia de amenazas globales sobre actores de amenazas y ciberdelincuentes con motivos geopolíticos.

Las principales preocupaciones incluían el riesgo de interrupción cibernética de los servicios de eventos o instalaciones locales. Las disrupciones como los ataques de ransomware y los esfuerzos para robar datos podrían afectar negativamente la experiencia del evento y las operaciones de rutina.

# Información sobre amenazas

El equipo de búsqueda de amenazas operó bajo una filosofía de defensa en profundidad para inspeccionar y proteger los dispositivos y redes de los clientes. Otro enfoque fue monitorear el comportamiento de identidades, inicios de sesión y acceso a archivos. La cobertura abarcó una variedad de sectores, incluidos clientes involucrados en transporte, telecomunicaciones, atención médica y otras funciones esenciales.

En general, la cantidad total de entidades y sistemas monitoreados las 24 horas del día, los siete días de la semana, con soporte de respuesta y búsqueda de amenazas dirigida por humanos abarcó más de 100 mil endpoints, 144 mil identidades, más de 14.6 millones de flujos de email, más de 634.6 millones de intentos de autenticación y miles de millones de conexiones de redes.

Como ejemplo, cuatro centros de salud fueron designados como unidades de atención urgente para el evento, incluidos hospitales que brindan apoyo crítico y servicios de salud para aficionados y jugadores. Como instalaciones de atención médica poseedoras de datos médicos, eran objetivos de alto valor. La búsqueda de amenazas impulsada por máquinas y humanos de Microsoft aprovechó la inteligencia en amenazas para escanear señales, aislar activos infectados e interrumpir ataques en estas redes. Con una combinación de la tecnología de seguridad de Microsoft, el equipo detectó y puso en cuarentena la actividad previa al ransomware dirigido a la red de atención médica. Se registraron varios intentos de inicio de sesión fallidos y se bloqueó la actividad adicional.

La naturaleza urgente de los servicios de atención médica requiere que los dispositivos y sistemas mantengan un nivel máximo de rendimiento. Los hospitales y los centros de salud tienen una tarea desafiante para equilibrar la disponibilidad del servicio mientras mantienen una postura de ciberseguridad saludable. Un ataque exitoso, en el corto plazo, podría haber inmovilizado las instalaciones médicas desde una perspectiva de datos a TI, dejando a los proveedores médicos relegados a lápiz y papel al actualizar los datos de los pacientes y debilitando su capacidad para realizar atención médica que salva vidas en una situación de emergencia o triaje masivo. A largo plazo, el malware plantado para proporcionar visibilidad a través de una red podría haberse aprovechado para un evento de ransomware más amplio destinado a una mayor interrupción. Tal caso podría haber abierto la puerta al robo de datos y la extorsión.

A medida que los grandes eventos globales siguen siendo objetivos deseables para los actores de amenazas, hay una variedad de motivaciones por parte de los estados nación que parecen estar dispuestos a absorber el daño colateral de los ataques si apoyan intereses geopolíticos más amplios. Además, los grupos de ciberdelincuentes que buscan aprovechar las vastas oportunidades financieras que existen en entornos de TI deportivos y relacionados con sedes, continuarán viéndolos como objetivos deseables.

## Recomendaciones:

**Aumente el equipo del Centro de Operaciones de Seguridad:** tenga un par de ojos adicionales que monitoreen el evento durante todo el día para detectar amenazas de manera proactiva y enviar notificaciones. Esto ayuda a correlacionar más datos de búsqueda y descubrir señales tempranas de intrusión. Debe incluir amenazas más allá del punto final, como el compromiso de identidad o el pivote de dispositivo a nube.

**Realice una evaluación de riesgos cibernéticos enfocada:** identifique las amenazas potenciales específicas del evento, sede o nación donde ocurre el evento. Esta evaluación debe incluir proveedores, profesionales de TI del equipo y del lugar, patrocinadores y partes interesadas del evento que sean clave.

**Considere el acceso con privilegios mínimos como una práctica recomendada:** otorgue acceso a los sistemas y servicios solo a aquellos que lo necesiten y capacite al personal para que entienda los niveles de acceso.

# Defensa contra ataques

## Las amplias superficies de ataque requieren planificación y supervisión adicionales

Con eventos como la Copa del Mundo FIFA Qatar 2022™, los Juegos Olímpicos y los eventos deportivos en general, los riesgos cibernéticos conocidos surgen de maneras únicas, a menudo menos perceptibles que en otros entornos empresariales. Estos eventos pueden llevarse a cabo rápidamente, con nuevos socios y proveedores que adquieren acceso a redes empresariales y compartidas durante un período de tiempo específico. La naturaleza emergente de la conectividad en algunos eventos puede dificultar la visibilidad y el control de dispositivos y flujos de datos. También fomenta una falsa sensación de seguridad de que las conexiones "temporales" son de menor riesgo.

Los sistemas durante eventos pueden incluir la presencia web y en las redes sociales del equipo o del lugar, las plataformas de registro o venta de entradas, los sistemas de cronometraje y puntuación de los juegos, la logística, la gestión médica y el seguimiento de pacientes, el seguimiento de incidentes, los sistemas de notificación masiva y la señalización electrónica.

Las organizaciones deportivas, patrocinadores, anfitriones y sedes deben colaborar en estos sistemas y desarrollar experiencias cibernéticas inteligentes para los aficionados. Además, la enorme oleada de asistentes y personal que traen datos e información a través de sus propios dispositivos, aumenta la superficie de ataque.

# Defensa contra ataques

Proporcionar a los equipos de seguridad la información que necesiten por adelantado, incluidos los servicios imprescindibles que deben permanecer operando durante el evento, manifestará mejor los planes de respuesta. Esto es esencial en entornos de TI y OT que respaldan la infraestructura del lugar y para mantener la seguridad física de los asistentes. Idealmente, las organizaciones y los equipos de seguridad podrían configurar sus sistemas antes del evento para completar las pruebas necesarias, captar el estatus del sistema y los dispositivos, y ponerlos a disposición de los equipos de TI para volver a implementarlos rápidamente cuando sea necesario. Estos esfuerzos contribuyen en gran medida a disuadir a los adversarios de aprovechar las redes improvisadas mal configuradas dentro de los entornos altamente deseables y vastos en objetivos de los grandes eventos deportivos.

Además, se debe considerar el riesgo de privacidad y si es que las configuraciones agregan nuevos riesgos o vulnerabilidades para la información personal de los asistentes o los datos de propiedad de los equipos. A partir de esta consideración, se pueden implementar prácticas inteligentes cibernéticas simples para los aficionados, dirigiéndolos, por ejemplo, a escanear solo códigos QR con un logotipo oficial, a ponderar la solicitud de SMS o mensajes de texto para los que no se inscribieron y evitar el uso de Wi-Fi público gratuito.

Estas políticas y otras pueden ayudar al público a comprender mejor el riesgo cibernético específicamente en grandes eventos, y su exposición a la recolección y robo de datos. Conocer las prácticas seguras puede ayudar a los aficionados y asistentes a evitar ser víctimas de ataques de ingeniería social, que los ciberdelincuentes pueden realizar después de afianzarse en las redes de las sedes y eventos explotados.

Además de las recomendaciones a continuación, el Centro Nacional para la Seguridad y Protección de los Deportes de Espectadores ofrece estas consideraciones para dispositivos conectados y seguridad integrada para grandes recintos.

## Recomendaciones:

**Priorizar la implementación de un marco de seguridad integral y de múltiples niveles:** Esto incluye la implementación de firewalls, sistemas de detección y prevención de intrusiones y protocolos de cifrado sólidos para fortalecer la red contra el acceso no autorizado y las violaciones de datos.

**Programas de capacitación y concientización del usuario:** informe a los empleados y partes interesadas sobre las mejores prácticas de ciberseguridad, como reconocer correos electrónicos de phishing, usar autenticación multifactor o protección sin contraseña, y evitar enlaces o descargas sospechosas.

**Asóciese con empresas de ciberseguridad reconocidas:** supervise continuamente el tráfico de red, detecte amenazas potenciales en tiempo real y responda rápidamente a cualquier incidente de seguridad. Realice auditorías de seguridad periódicas y evaluaciones de vulnerabilidad para identificar y abordar cualquier debilidad dentro de la infraestructura de red.

# Perfil del experto

**Justin Turner**
Director General del Grupo de Investigación de Seguridad de Microsoft

> **"No puedes defender algo que no ves o entiendes."**

Justin Turner comenzó su carrera construyendo y rompiendo redes de comunicaciones para el Ejército de los Estados Unidos. Esto le permitió viajar por el mundo y trabajar en lugares como Irak, Bahrein y Kuwait. Cuando su aventura en servicio activo terminó, Justin hizo la transición a la vida civil en Florida en 2006. El trabajo era similar: construir, hackear y romper cosas, pero esta vez, estaba con MITRE Corporation.

En 2011, recibió una llamada de un ex comandante del Ejército sobre una posición en SecureWorks, centrado exclusivamente en el lado comercial de la ciberseguridad.

Su función inicial fue en la producción de inteligencia ante amenazas, mirando a través de los conjuntos de datos de los clientes y respondiendo a preguntas sobre archivos maliciosos o malware. Eso incluyó hacer análisis e investigar campañas de amenazas activas.

"En ese momento, los troyanos bancarios eran frecuentes. Puede que recuerden el troyano bancario Zeus. Muchas herramientas de acceso remoto realmente se aplicaron en ese momento. Un par de años después de eso, me pidieron que ayudara a desarrollar una práctica de caza de amenazas para la compañía. Esto fue antes de que existiera la caza de amenazas en el mercado como un servicio como lo hace ahora".

Cuando Microsoft decidió lanzar Defender Experts for Hunting, Justin recibió otra llamada de un antiguo colega y amigo. Dijo: "Estamos lanzando un nuevo servicio para Microsoft Security, no puedo pensar en nadie mejor para este rol".

Justin dice que los tres desafíos que persisten a lo largo de sus 20 años de experiencia en ciberseguridad son la gestión de la configuración, los parches y la visibilidad del dispositivo.

"En general, las configuraciones erróneas son un desafío monumental. Nuestro entorno de red ha cambiado drásticamente, pasamos de entornos de mainframe de servidor, que tenían entornos de clientes ligeros, a todos los que poseen una computadora personal. Hoy, hay innumerables dispositivos conectados a la red, desde hogares inteligentes hasta entornos de fabricación y dispositivos personales. Mantener una línea de base segura a través de eso es un desafío, mantener los niveles de parches agrega otra capa del problema".

A medida que crece la complejidad y el tamaño de las redes, también lo hace el número de vulnerabilidades, explica Justin.

"Nuestros clientes que cuentan con entornos combinados en expansión intentan mantenerse al día con parches. Es fácil para nosotros decir, 'solo parche', pero es un problema enormemente desafiante que requiere mucho tiempo e inversión continua".

El tercer desafío es la visibilidad. Justin dice que muchas de las conversaciones con los clientes que tiene se centran en un problema que ocurrió porque el cliente no sabía que un sistema vulnerable expuesto a Internet estaba operando en su red.

"Recientemente, para una conferencia, tomé una intrusión de hace décadas y luego miré una intrusión de hace una semana. Puse los dos uno al lado del otro y pregunté: '¿Cuál de estos sucedió en 1986 y cuál de estos sucedió la semana pasada?'

Nadie podía decirlo porque los dos se veían muy similares. El ataque fue una vulnerabilidad de software que nadie sabía que existía. Fue una mala configuración del servidor, una auditoría y un registro deficientes, con poca o ninguna administración de parches. Los detalles técnicos de los problemas son diferentes ahora, pero los fundamentos son los mismos. Como defensor, no puedes defender algo que no ves o entiendes".

**Metodología:** Para los datos del panorama de seguridad, las plataformas y servicios de Microsoft, incluidos Microsoft Extended Detections and Response, Microsoft Defender, Defender Experts for Hunting y Azure Active Directory, proporcionaron datos anónimos sobre la actividad de amenazas, como cuentas de correo electrónico malintencionadas, correos electrónicos de phishing y acciones de atacantes dentro de las redes. La información adicional proviene de los 65 billones de señales de seguridad diarias obtenidas en Microsoft, incluida la nube, los endpoints, el entorno inteligente y nuestros equipos de Práctica de recuperación de seguridad comprometida y Detección y respuesta. La portada no representa un partido de fútbol real, torneo o deporte individual. Todas las organizaciones deportivas a las que se hace referencia son marcas comerciales de propiedad individual.



1: https://www.bleepingcomputer.com/news/security/nba-alerts-fans-of-a-data-breach-exposing-personal-information/

2: https://www.independent.co.uk/sport/football/premier-league/manchester-united/manchester-united-cyber-attack-organised-criminals-data-b1759472.html

3: https://www.espn.com/nfl/story/_/id/33283115/san-francisco-49ers-network-hit-gang-ransomware-attack-team-notifies-law-enforcement

4: https://rocketswire.usatoday.com/2021/04/15/rockets-working-with-fbi-to-investigate-cyberattack-on-team-systems/

5: https://www.cnn.com/2021/10/29/tech/mlb-hack/index.html

6: https://www.nytimes.com/2018/02/12/technology/winter-olympic-games-hack.html