Microsoft

Ponto da situação

Eventos e locais esportivos estão cada vez mais sujeitos a ameaças cibernéticas.

Tentativas de autenticação de

634,6 MM

Durante o período de 10 de novembro a 20 de dezembro de 2022, a Microsoft realizou mais de 634,6 milhões de autenticações e forneceu defesas de segurança cibernética para instalações e organizações no Catar.

Microsoft Threat intelligence

Cyber Signals

Agosto de 2023

Introdução

Os agentes de ameaças estão constantemente em busca de oportunidades para realizar ataques cibernéticos, inclusive em eventos esportivos de grande destaque que ocorrem em ambientes altamente conectados. Isso representa um risco significativo para os organizadores, instalações e participantes desses eventos. O Centro Nacional de Segurança Cibernética do Reino Unido (NCSC) revelou que os ataques cibernéticos contra organizações esportivas estão se tornando cada vez mais comuns, com 70% dos entrevistados relatando pelo menos um ataque por ano, o que é consideravelmente maior do que a média das empresas no Reino Unido.

A pressão para proporcionar uma experiência tranquila e segura em eventos de alcance global coloca novos desafios para os anfitriões e instalações locais. Um único dispositivo mal configurado, uma senha exposta ou uma conexão negligenciada podem resultar em violações de dados ou invasões bem-sucedidas.

Durante a realização da Copa do Mundo da FIFA 2022™, a Microsoft ofereceu suporte de segurança cibernética para instalações de infraestrutura crítica. Neste artigo, compartilharemos insights valiosos sobre como os agentes de ameaças avaliam e infiltram-se nesses ambientes, abrangendo locais, equipes e infraestruturas críticas ao redor do próprio evento.

Todos nós somos defensores

Instantâneo de segurança

Os dados instantâneos representam o número total de entidades e eventos monitorados entre 10 de novembro e 20 de dezembro de 2022. Isso inclui organizações diretamente envolvidas ou afiliadas à infraestrutura do torneio. A atividade inclui buscas de ameaças proativas para identificar ameaças emergentes e rastrear campanhas.

45
Organizações protegidas

100.000
endpoints protegidos

144.000
identidades protegidas

14,6 milhões
de fluxos de e-mail

634,6 milhões
de Tentativas de autenticação

4,35 bilhões
de conexões de rede

Briefing sobre ameaças

Agentes de ameaças oportunistas exploram ambiente rico em alvos

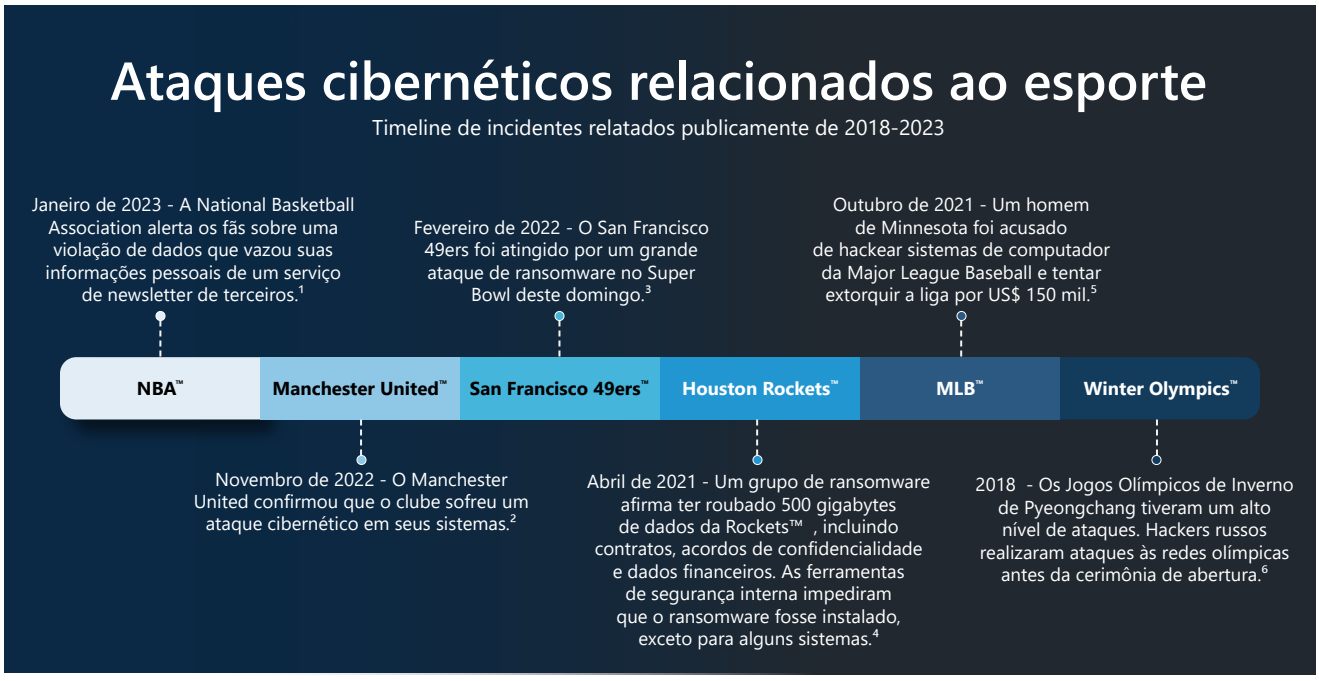
As ameaças de segurança cibernética a eventos e locais esportivos são diversas e complexas. Eles exigem vigilância e colaboração constantes entre as partes interessadas para prevenir e mitigar o seu aumento. Com o mercado esportivo global avaliado em mais de US$ 600 bilhões, tornando-se um alvo ainda mais relevante. Equipes esportivas, grandes ligas e associações esportivas globais e locais de entretenimento abrigam um acervo de informações valiosas desejáveis pelos cibercriminosos.

Informações sobre desempenho atlético, vantagem competitiva e informações pessoais são um alvo lucrativo. Infelizmente, essas informações podem ser vulneráveis em escala, devido ao número de dispositivos conectados e redes interconectadas nesses ambientes. Muitas vezes, essa vulnerabilidade abrange vários proprietários, incluindo equipes, patrocinadores corporativos, autoridades municipais e contratados terceirizados. Treinadores, atletas e torcedores também podem ser vulneráveis à perda de dados e extorsão.

Além disso, arenas esportivas contêm muitas vulnerabilidades conhecidas e desconhecidas que permitem que as ameaças tenham como alvo serviços críticos de negócios, como dispositivos de ponto de venda, infraestruturas de TI e dispositivos de visitantes. Nenhum evento esportivo de alto nível tem o mesmo perfil de risco cibernético, que varia dependendo de fatores como localização, participantes, tamanho e composição.

Para concentrar nossos esforços durante a realização da Copa do Mundo FIFA no Catar 2022™, conduzimos uma avaliação de risco por meio do Defender Experts for Hunting, um serviço gerenciado de busca a ameaças que pesquisa proativamente ameaças em endpoints, sistemas de e-mail, identidades digitais e aplicativos em nuvem. Nesse caso, os fatores incluíram motivação do cibercriminoso, desenvolvimento do perfil e uma estratégia de resposta. Também consideramos a inteligência de ameaças globais sobre agentes de ameaças com motivação geopolítica.

As principais preocupações incluíam o risco de interrupção cibernética de serviços de eventos ou instalações locais. Interrupções como ataques de ransomware e esforços para roubar dados podem afetar negativamente a experiência do evento e as operações de rotina.



Briefing sobre ameaças

A equipe de busca a ameaças operava sob uma filosofia de defesa profunda para inspecionar e proteger dispositivos e redes de clientes. Outro foco foi monitorar o comportamento de identidades, logins e acesso a arquivos. A cobertura abrangeu uma variedade de setores, incluindo clientes envolvidos em transporte, telecomunicações, saúde e outras funções essenciais.

No geral, o número total de entidades e sistemas monitorados ininterruptamente com identificação de ameaças e suporte de resposta abrangeu mais de 100.000 endpoints, 144.000 identidades, 14,6 milhões de e-mail, mais de 634,6 milhões de autenticações e bilhões de conexões de rede.

Como exemplo, quatro unidades de saúde foram designadas como unidades de atendimento de urgência para o evento, incluindo hospitais que oferecem suporte crítico e serviços de saúde para torcedores e jogadores. Como instalações de saúde que possuem dados médicos, elas eram alvos de alto valor. A atividade de identificação de ameaças alimentada por máquinas e humanos da Microsoft aproveitou a inteligência para verificar sinais, isolar ativos infectados e interromper ataques nessas redes. Uma combinação de tecnologia de segurança da Microsoft detectou e colocou em quarentena atividades pré-ransomware visando a rede de saúde. Várias tentativas de entrada malsucedidas foram registradas e outras atividades foram bloqueadas.

A natureza urgente dos serviços de saúde requer que os dispositivos e sistemas mantenham um nível máximo de desempenho. Hospitais e estabelecimentos de saúde têm uma tarefa desafiadora para equilibrar a disponibilidade do serviço e, ao mesmo tempo, manter uma postura saudável de segurança cibernética. Um ataque bem-sucedido, no curto prazo, poderia ter imobilizado as instalações médicas de uma perspectiva digital, deixando os provedores médicos reféns da caneta e do papel ao atualizar os dados dos pacientes e enfraquecendo sua capacidade de realizar cuidados médicos que salvam vidas em uma situação de emergência ou triagem em massa. A longo prazo, o código malicioso plantado para fornecer visibilidade em uma rede poderia ter sido aproveitado para um evento de ransomware mais amplo com o objetivo de mais interrupções. Tal caso poderia ter aberto as portas para roubo de dados e extorsão.

À medida que grandes eventos globais continuam a ser alvos para os criadores de ciberameaças, há uma variedade de motivações que fazem com que os Estados-nação estejam dispostos a absorver danos colaterais de ataques caso estes apoiem interesses geopolíticos mais amplos. Além disso, os grupos cibercriminosos que procuram aproveitar as vastas oportunidades financeiras que existem em ambientes de TI relacionados a esportes e instalações continuarão a vê-los como alvos desejáveis.

Recomendações:

Aumente a equipe do SOC: Tenha um conjunto adicional de olhos monitorando o evento o tempo todo para detectar ameaças de forma proativa e enviar notificações. Isso ajuda a correlacionar mais dados de identificação de ameaças e descobrir os primeiros sinais de intrusão. Ele deve incluir ameaças além do endpoint, como comprometimento de identidade ou pivô de dispositivo para nuvem.

Realizar uma avaliação de risco cibernético focada: identifique ameaças potenciais específicas ao evento, local ou nação onde o evento ocorre. Essa avaliação deve incluir fornecedores, profissionais de TI da equipe e do local, patrocinadores e as principais partes interessadas do evento.

Considere o acesso menos privilegiado uma prática recomendada: conceda acesso a sistemas e serviços apenas àqueles que precisam dele e treine a equipe para entender as camadas de acesso.

Defesa contra ataques

Vastas superfícies de ataque exigem planejamento e supervisão adicionais

Com eventos como a Copa do Mundo FIFA no Catar 2022™ , as Olimpíadas e eventos esportivos em geral, os riscos cibernéticos conhecidos surgem de maneiras únicas, muitas vezes de forma menos perceptível do que em outros ambientes corporativos. Esses eventos podem se formar rapidamente, com novos parceiros e fornecedores adquirindo acesso a redes corporativas e compartilhadas por um período de tempo específico. A natureza pop-up da conectividade em alguns eventos pode dificultar sua visibilidade e o controle de dispositivos e de fluxos de dados. Também promove uma falsa sensação de segurança de que as conexões "temporárias" são de menor risco.

Os sistemas de eventos podem incluir a presença da equipe ou local na web e nas mídias sociais, plataformas de registro ou bilheteria, sistemas de cronometragem e pontuação de jogos, logística, gerenciamento médico e rastreamento de pacientes, rastreamento de incidentes, sistemas de notificação em massa e sinalização eletrônica.

Organizações esportivas, patrocinadores, anfitriões e locais devem colaborar nesses sistemas e desenvolver experiências inteligentes para fãs no ambiente digital. Além disso, a enorme onda de participantes e funcionários que trazem dados e informações por meio de seus próprios dispositivos aumenta a superfície de ataque.

Defesa contra ataques

Fornecer às equipes de segurança as informações de que elas precisam antecipadamente — incluindo serviços críticos que devem permanecer operáveis durante o evento — informará melhor os planos de resposta. Isso é essencial em ambientes de TI e OT que suportam a infraestrutura do local e para manter a segurança física dos participantes. Idealmente, as organizações e as equipes de segurança poderiam configurar seus sistemas antes do evento para concluir os testes, snapshot do sistema e dos dispositivos e disponibilizá-los prontamente para as equipes de TI reimplantarem rapidamente quando necessário. Esses esforços ajudam muito a dissuadir os adversários de tirar proveito de redes ad hoc mal configuradas dentro dos ambientes altamente desejáveis e ricos em alvos de grandes eventos esportivos.

Além disso, alguém na sala deve considerar o risco de privacidade e se as configurações adicionam novos riscos ou vulnerabilidades para as informações pessoais dos participantes ou os dados proprietários das equipes. Essa pessoa pode implementar práticas cibernéticas simples para os fãs, orientando-os, por exemplo, a escanear apenas códigos QR com um logotipo oficial, a rejeitar SMS ou solicitação de texto para a qual não se inscreveram e a evitar o uso de Wi-Fi público gratuito.

Essas políticas e outras podem ajudar o público a entender melhor o risco cibernético em grandes eventos, especificamente, e sua exposição à coleta e roubo de dados. Conhecer práticas seguras pode ajudar fãs e participantes a evitar se tornarem vítimas de ataques de engenharia social, que os cibercriminosos podem travar depois de ganhar uma posição em locais explorados e redes de eventos.

Além das recomendações abaixo, o National Center for Spectator Sports Safety and Security oferece essas considerações para dispositivos conectados e segurança integrada para grandes locais.

Recomendações:

Priorize a implementação de uma estrutura de segurança abrangente e de várias camadas: isso inclui a implantação de firewalls, sistemas de detecção e prevenção de intrusões e protocolos de criptografia fortes para fortalecer a rede contra acesso não autorizado e violações de dados.

Programas de conscientização e treinamento do usuário: instrua funcionários e partes interessadas sobre as melhores práticas de segurança cibernética, como reconhecer e-mails de phishing, usar autenticação multifator ou proteção sem senha e evitar links ou downloads suspeitos.

Faça parcerias com empresas de segurança cibernética respeitáveis: monitore continuamente o tráfego de rede, detecte ameaças potenciais em tempo real e responda rapidamente a quaisquer incidentes de segurança. Realize auditorias de segurança regulares e avaliações de vulnerabilidades para identificar e resolver quaisquer fraquezas na infraestrutura de rede.

Perfil do Especialista

Justin Turner

Gerente Principal de Grupo
da Microsoft Security Research

> **"Você não pode defender algo que não vê ou entende."**

Justin Turner começou sua carreira construindo e quebrando redes de comunicação para o Exército dos Estados Unidos. Isso lhe permitiu viajar pelo mundo e trabalhar em lugares como Iraque, Bahrein e Kuwait. Quando sua aventura no serviço ativo terminou, Justin fez a transição para a vida civil na Flórida em 2006. O trabalho era semelhante – construir, hackear e quebrar coisas – mas, desta vez, ele estava na MITRE Corporation.

Em 2011, ele recebeu uma ligação de um ex-comandante do Exército sobre uma função na SecureWorks focada exclusivamente no lado comercial da segurança cibernética.

Sua função inicial foi na produção de inteligência de ameaças, analisando conjuntos de dados de clientes e respondendo a perguntas sobre arquivos maliciosos ou malware. Isso incluiu fazer análises e investigar campanhas ativas de ameaças.

"Na época, os trojans bancários eram predominantes. Alguns devem se lembrar do Trojan bancário Zeus. Muitas ferramentas de acesso remoto realmente surgiram nessa época. Alguns anos depois, fui convidado a ajudar a desenvolver uma prática de caça a ameaças para a empresa. Isso foi antes de a caça a ameaças existir no mercado como um serviço como acontece agora."

Quando a Microsoft decidiu lançar o Defender Experts for Hunting, Justin recebeu outra ligação de um ex-colega e amigo. Ele disse: "estamos lançando um novo serviço para o Microsoft Security, não consigo pensar em ninguém melhor para essa função".

Justin diz que os três desafios que persistem ao longo de seus 20 anos de experiência em segurança cibernética são gerenciamento de configuração, aplicação de patches e visibilidade de dispositivos.

"Em geral, as configurações equivocadas são um grande desafio. Nosso ambiente de rede mudou drasticamente, passamos de ambientes de mainframe de servidor, que tinham bordas de thin client, para todos possuindo um computador pessoal. Avançando rapidamente até hoje, existem inúmeros dispositivos conectados à rede, de casas inteligentes a ambientes de fabricação e dispositivos pessoais. Manter uma linha de base segura é um desafio, sustentar os níveis de patch adiciona outra camada do problema."

À medida que a complexidade e o tamanho das redes crescem, cresce também o número de vulnerabilidades, explica Justin.

"Nossos clientes com ambientes mistos em expansão tentam acompanhar a aplicação de patches. É fácil para nós dizer, 'apenas um patch', mas é um problema extremamente desafiador que leva muito tempo e investimento contínuo."

O terceiro desafio é a visibilidade. Justin diz que muitas das conversas com clientes que ele tem giraram em torno de um problema que ocorreu porque o cliente não sabia que um sistema vulnerável exposto à Internet estava operando em sua rede.

"Recentemente, para uma conferência, analisei uma invasão cibernética de décadas atrás e outra de uma semana atrás. Coloquei ambas lado a lado e perguntei: 'Qual delas aconteceu em 1986 e qual delea aconteceu na semana passada?'

Ninguém sabia dizer porque eram muito parecidas. O ataque foi uma vulnerabilidade de software que ninguém sabia que existia. Foi uma configuração errada do servidor, auditoria e registro em log ruins, com pouco ou nenhum gerenciamento de patches. Os detalhes técnicos dos problemas são diferentes agora, mas os fundamentos são os mesmos. Como defensor, você não pode defender algo que você não vê ou entende."

Metodologia: para dados de instantâneo, as plataformas e serviços da Microsoft, incluindo Microsoft Extended Detections and Response, Microsoft Defender, Defender Experts for Hunting e Azure Active Directory, forneceram dados anônimos sobre atividades de ameaças, como contas de email mal-intencionadas, emails de phishing e movimentação de invasores dentro das redes. Informações adicionais são provenientes dos 65 trilhões de sinais de segurança diários obtidos em toda a Microsoft, incluindo a nuvem, endpoints, Intelligent Edge e nossas Práticas de Recuperação de Segurança de Comprometimento e Equipes de Detecção e Resposta. A arte da capa não retrata um jogo de futebol, torneio ou esporte individual real. Todas as organizações esportivas referenciadas são marcas registradas de propriedade 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