State of Play

Gli eventi sportivi sono sempre più soggetti a minacce Cyber

634.6 MM

Tentativi di Autenticazione

Tra il 10 Novembre ed il 20 Dicembre 2022, Microsoft ha effettuato più di 634.6 milioni di autenticazioni, offrendo servizi di cybersecurity alle strutture presenti in Qatar

.

Microsoft Threat Intelligence

Cyber Signals

Agosto 2023

Introduzione

Gli artefici delle minacce digitali si muovono per colpire obiettivi ben precisi e sferrare attacchi più o meno mirati.

Ciò si estende agli eventi sportivi di alto livello, in particolare quelli che si svolgono in ambienti sempre più connessi, introducendo così rischi Cyber per gli organizzatori, le strutture ospitanti ed i partecipanti.

Il United Kingdom's National Cyber Security Centre (NCSC) ha rilevato che gli attacchi informatici -cyberattacks- contro le organizzazioni sportive sono in aumento, con il 70% degli intervistati che dichiara di aver subito almeno un attacco all'anno. Si tratta di una percentuale di gran lunga superiore rispetto alla media di altri settori del Regno Unito.

L'importanza di assicurare un'esperienza piacevole e sicura per gli spettatori a livello mondiale, introduce nuove sfide per le strutture che ospitano tali eventi. È sufficiente un singolo dispositivo configurato in modo errato, una password non protetta o una connessione poco sicura per esporsi a una violazione dei dati o a un attacco.

Microsoft ha fornito il supporto per la Cybersecurity delle infrastrutture critiche durante la FIFA World Cup Qatar 2022™. In questa edizione presentiamo la nostra esperienza diretta sul modo in cui gli autori delle minacce valutano gli attacchi e infiltrano le sedi, i team e le infrastrutture critiche coivolte in un determinato evento.

We are all defenders

Security Snapshot

Questi dati rappresentano il numero totale di entità ed eventi monitorati 24 ore su 24 tra il 10 novembre e il 20 dicembre 2022. Questi includono le organizzazioni direttamente coinvolte o affiliate alle infrastrutture della competizione. L'attività include la ricerca proattiva e manuale delle minacce, al fine di identificare minacce emergenti e controllare movimenti significativi.

45
Organizzazioniprotette

100,000
Endpoints protetti

144,000
Identità protette

14.6 Million
Email flows

634.6 Million
Tentativi di Autenticazione

4.35 Billion
Connessioni di rete

Gli autori delle minacce sfruttano ambienti ricchi di opportunità di attacco

Le minacce alla sicurezza informatica degli eventi sportivi e le loro sedi possono essere diverse e complesse. Richiedono vigilanza e collaborazione costanti tra gli stakeholders per prevenire e mitigare l'escalation. Con una quotazione superiore ai 600 miliardi di dollari, il mercato globale dello sport è un target ambito. Squadre sportive, major leagues e associazioni sportive globali, e luoghi di intrattenimento ospitano una miniera di informazioni preziose per i criminali informatici.

I dati sulla performance sportiva, il vantaggio competitivo e le informazioni personali sono un target redditizio. Questi dati sono particolarmente vulnerabili su larga scala, a causa del numero di dispositivi collegati e delle reti interconnesse. Spesso questa vulnerabilità riguarda diverse entità, tra cui squadre sportive, sponsor, autorità municipali e terze parti commerciali. Anche allenatori, atleti e tifosi possono essere soggetti alla perdita di dati ed estorsione.

Inoltre, le sedi e le arene sportive sono soggette a vulnerabilità, note o sconosciute, che consentono alle minacce di prendere di mira i servizi aziendali critici, come i dispositivi point of sales (POS), le infrastrutture IT e i dispositivi degli utenti. Gli eventi sportivi di alto profilo non sono mai esposti allo stesso rischio informatico, poiché questo varia a seconda di fattori come la posizione, i partecipanti, le dimensioni e la composizione.

Per concentrare i nostri sforzi durante la FIFA World Cup Qatar 2022™, abbiamo effettuato una ricerca delle minacce per valutare i rischi utilizzando Defender Experts for Hunting, un servizio gestito di ricerca delle minacce che ricerca attivamente le minacce presenti su endpoint, sistemi di posta elettronica, identità digitali e app cloud. I fattori coivolti includevano le motivazioni dell'autore delle minacce, lo sviluppo del suo profilo e una strategia di risposta. Abbiamo anche preso in considerazione l'intelligence globale sugli autori delle minacce con motivazioni geopolitche e sui criminali informatici.

Tra le preoccupazioni principali figurano il rischio di interruzione dei servizi informatici per eventi o strutture locali. Ransomware attacks e tentativi di furto di dati potrebbero infatti impattare negativamente il corso dell'evento e operazioni di routine.

Threat briefing

Il team di ricerca sulle minacce (threat hunting team) si è mosso seguendo una filosofia fortemente difensiva, per ispezionare e tutelare le reti ed i dispositivi dei clienti. In particolare, sono state monitorate le pagine di accesso e le identità.

Complessivamente, il numero totale di sistemi monitorati 24 ore su 24 dal threat hunting team ammontava a più di 100.000 endpoint, 144.000 identità, 14,6 milioni di flussi di posta elettronica, oltre 634,6 milioni di autenticazioni e miliardi di connessioni di rete.

Ad esempio, alcune strutture sanitarie sono state designate come unità di Pronto soccorso per l'evento, ed in quanto strutture sanitarie ospitanti dati medici, sono state obiettivo di attacco. L'attività di ricerca delle minacce da parte di Microsoft -machine e human-powered, ha sfruttato l'intelligence per analizzare ed individuare eventuali segnali di rischio ed interrompere gli attacchi alle reti.

Grazie a una combinazione delle tecnologie di tipo Microsoft Security, il team ha rilevato e messo in quarantena l'attività pre-ransomware che prendeva di mira la rete sanitaria. Sono stati registrati diversi tentativi di accesso (non riusciti), ed ulteriori attività sono state bloccate.

In questo contesto, è necessario che le strutture sanitarie garantiscano elevati livelli di prestazione nell'ambito della sicurezza informatica. Un attacco ben riuscito, nel breve termine, avrebbe potuto creare serie difficoltà alle strutture mediche per quanto riguarda la gestione dei dati e dei processi informatici, rallentando gli operatori sanitari nell'aggiornamento dei dati dei pazienti e minando quindi la loro capacità di operare in situazioni di emergenza.

Nel lungo termine, l'installazione di simili codici dannosi avrebbe potuto rappresentare una leva per eventi ransomware più importanti con il fine di causare danni ulteriori. Questo avrebbe potuto sfociare in successive perdite di dati ed estorsioni. Poiché grandi eventi sportivi rappresentano obiettivi ideali per gli attacchi informatici, possono esserci una serie di motivazioni per cui alcuni Stati sembrano essere più disposti ad assorbire i danni collaterali legati ad attacchi di questo tipo, se ciò sostiene interessi geopolitici più ampi. Inoltre, i gruppi di criminali informatici cercano di sfruttare le vaste opportunità finanziarie degli ambienti IT, legati allo sport e ai luoghi di ritrovo, e continueranno a considerare questi come target di interesse.

Raccomandazioni:

Amplia il SOC team: Assicurati che l'evento venga monitorato 24 ore su 24 e che eventuali minacce vengano rilevate nell'immediato. Inoltre l'utilizzo dei dati ti aiuterà a scoprire i primi segni di intrusione. Il monitoraggio terrà conto di mincacce che vanno oltre l'endpoint, come la compromissione dell'identità o il pivot da dispositivo a cloud.

Conduci una valutazione mirata del rischio informatico:
Identifica le potenziali minacce collegate all'evento e al luogo in cui questo si tiene. Una valutazione di questo tipo dovrebbe tenere conto dei fornitori, dei professionisti IT del team e della sede, degli sponsor e delle principali parti coinvolte nell'evento.

Gestisci gli accessi privilegiati: Garantisci l'accesso a sistemi e a servizi solo a chi ne ha strettamente bisogno, e forma il personale in materia di diritti di accesso.

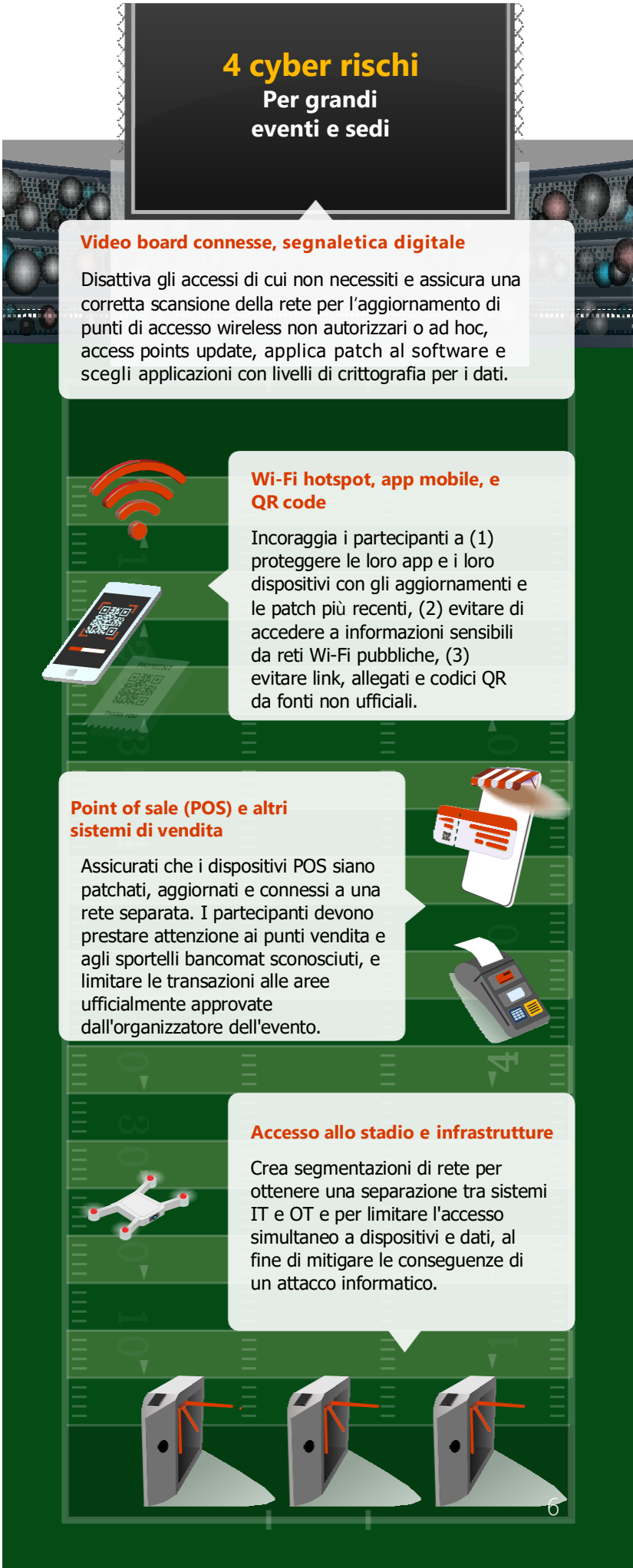
Proteggiti dagli attacchi

Pianificazione e controllo aggiuntivi

In caso di eventi come la FIFA World Cup Qatar 2022™, le Olimpiadi™ invernali, e in generale con gli eventi sportivi, i rischi informatici si presentano inaspettatamente ed in maniera meno evidente rispetto ad altri ambienti aziendali. Spesso si tratta di eventi organizzati rapidamente, con nuovi partner e fornitori che ottengono un accesso temporaneo alle reti aziendali. Ciò può rendere difficile monitorare la visibilità e controllare dispositivi e flussi di dati. Contribuisce inoltre a creare un falso senso di sicurezza, secondo cui le connessioni "temporanee" sono a basso rischio.

I sistemi informatici impiegati includono siti web e social media della squadra o della sede, piattaforme di iscrizione e vendita biglietti, sistemi di monitoraggio dei punteggi della partita, logistica, gestione medica dei pazienti e sistemi globali di notifica.

Le organizzazioni sportive, gli sponsor, gli host e le sedi tipicamente collaborano su questi sistemi, per sviluppare soluzioni informatiche intelligenti per i propri tifosi. Inoltre, il crescente aumento di partecipanti e di personale che porta con sé dati e informazioni attraverso i propri dispositivi, aumenta le probabilità di attacco.



Proteggiti dagli attacchi

Fornire ai team di sicurezza le informazioni necessarie in anticipo, inclusi i servizi critici che devono rimanere operativi durante l'evento, migliorerà la preparazione dei piani di risposta. Questo è essenziale negli ambienti IT e OT che supportano l'infrastruttura della sede e per garantire la sicurezza fisica dei partecipanti. Idealmente, le organizzazioni e i team di sicurezza potrebbero configurare i loro sistemi prima dell'evento per completare i test, acquisire uno snapshot del sistema e dei dispositivi, e renderli prontamente disponibili alle squadre IT per una rapida reimplementazione quando necessario. Questi sforzi contribuiscono in modo significativo a scoraggiare gli avversari dall'approfittare di reti male configurate e ad hoc all'interno degli ambiti altamente desiderabili e ricchi di bersagli dei grandi eventi sportivi.

Inoltre, qualcuno presente dovrebbe considerare il rischio per la privacy e valutare se le configurazioni aggiungono nuovi rischi o vulnerabilità per le informazioni personali dei partecipanti o per i dati confidenziali di proprietà delle squadre.

Questa persona può attuare semplici pratiche di sicurezza informatica per i fan, ad esempio, indirizzandoli a scannerizzare solo i codici QR con un logo ufficiale, a essere critici riguardo a messaggi SMS o richieste di testo a cui non si sono iscritti, e a evitare di utilizzare reti Wi-Fi pubbliche gratuite.

Queste politiche e altre possono aiutare il pubblico a comprendere meglio il rischio cibernetico e la loro esposizione al furto e alla raccolta di dati, in particolare durante eventi di grandi dimensioni. Conoscere le pratiche sicure può aiutare i fan e i partecipanti a evitare di diventare vittime di attacchi di ingegneria sociale, che gli hacker possono lanciare una volta ottenuto un punto d'appoggio nelle reti delle sedi e degli eventi sfruttati.

Oltre alle raccomandazioni di seguito, il National Center for Spectator Sports Safety and Security offre queste considerazioni per i dispositivi connessi e la sicurezza integrata in grandi location.

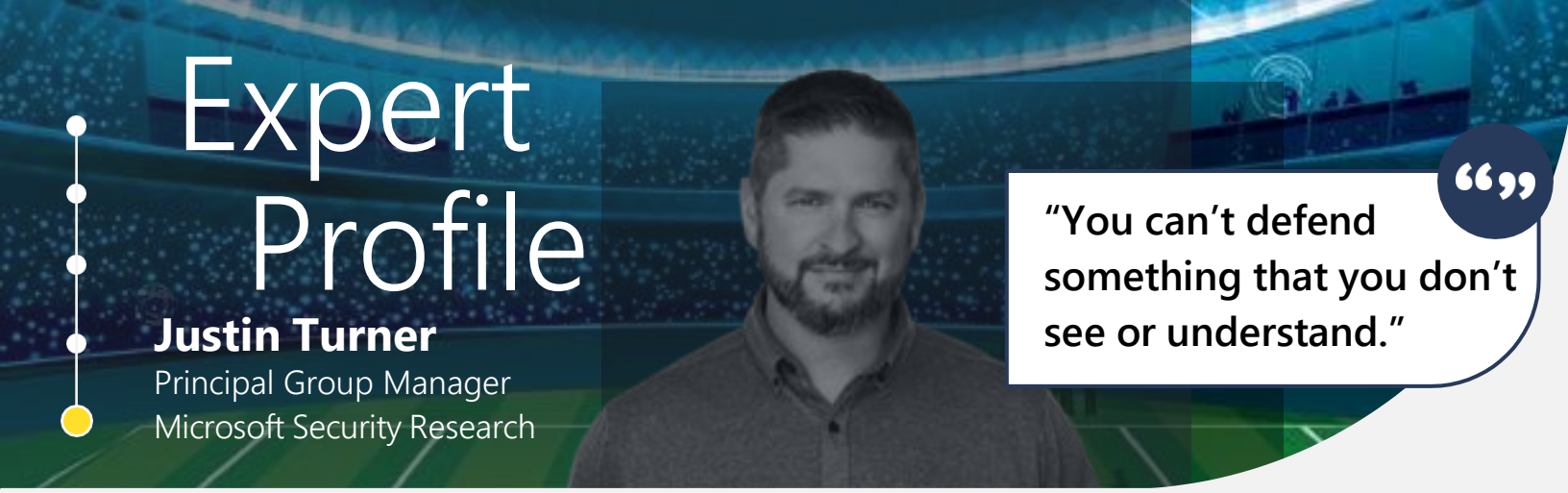
Raccomandazioni:

Dare priorità all'implementazione di un framework di sicurezza completo e multilivello: Ciò include la messa in opera di firewall, sistemi di rilevamento e prevenzione delle intrusioni e protocolli di crittografia robusti per proteggere la rete da accessi non autorizzati e violazioni dei dati.

Programmi di sensibilizzazione e formazione degli utenti: Formare dipendenti e stakeholder sulle migliori pratiche in materia di sicurezza informatica, come il riconoscimento delle email di phishing, l'uso dell'autenticazione a più fattori o della protezione senza password, ed evitare l'apertura di link o download sospetti.

Collaborare con aziende di sicurezza informatica affidabili: Monitorare costantemente il traffico di rete, individua potenziali minacce in tempo reale e rispondi prontamente a eventuali incidenti di sicurezza. Conduci regolari audit di sicurezza e valutazioni delle vulnerabilità per individuare e affrontare eventuali debolezze nell'infrastruttura di rete.

Expert Profile



Justin Turner
Principal Group Manager
Microsoft Security Research

> **"You can't defend something that you don't see or understand."**

Justin Turner ha iniziato la sua carriera costruendo e analizzando reti di comunicazione per l'Esercito degli Stati Uniti. Questo gli ha permesso di viaggiare in tutto il mondo e lavorare in luoghi come l'Iraq, il Bahrein e il Kuwait. Quando la sua avventura nell'attiva militare è terminata, Justin ha fatto la transizione verso la vita civile in Florida nel 2006. Il lavoro era simile: costruire, testare e analizzare cose, ma questa volta era con la MITRE Corporation.

Nel 2011, ha ricevuto una chiamata da un ex comandante dell'Esercito riguardo a un ruolo presso SecureWorks, focalizzato esclusivamente sul lato commerciale della sicurezza informatica.

Il suo ruolo iniziale riguardava la produzione di intelligence sulle minacce, osservando insieme ai dati dei clienti e rispondendo a domande riguardanti file o software dannosi. Questo includeva l'analisi e l'indagine su campagne di minacce attive.

"In quel periodo, i Trojan bancari erano diffusi. Alcuni potrebbero ricordare il Trojan bancario Zeus. Molati strumenti di accesso remoto hanno iniziato a diffondersi in quel periodo. Un paio d'anni dopo, mi è stato chiesto di contribuire a sviluppare una pratica di caccia alle minacce per l'azienda. Questo è successo prima che la caccia alle minacce diventasse un servizio come lo conosciamo oggi."

Quando Microsoft ha deciso di lanciare Defender Experts for Hunting, Justin ha ricevuto un'altra chiamata da un ex collega e amico. Gli ha detto: "stiamo lanciando un nuovo servizio per la sicurezza di Microsoft, e non riesco a pensare a nessuno di migliore per questo ruolo."

Justin afferma che le tre sfide che persistono nei suoi 20 anni di esperienza nella sicurezza informatica sono la gestione delle configurazioni, la distribuzione di patch e la visibilità dei dispositivi.

"In generale, le configurazioni errate rappresentano una sfida monumentale. Il nostro ambiente di rete è cambiato notevolmente, siamo passati da ambienti server mainframe con margini sottili a client personali. Proiettandoci al giorno d'oggi, ci sono innumerevoli dispositivi connessi in rete, dalle case intelligenti agli ambienti di produzione ai dispositivi personali. Mantenere una base sicura tra tutti questi rappresenta una sfida, e il mantenimento dei livelli di patch costituisce un altro livello del problema."

All'aumentare della complessità e delle dimensioni delle reti, cresce anche il numero di vulnerabilità, spiega Justin. "I nostri clienti con ambienti sempre più complessi cercano di tenere il passo con la distribuzione di patch. È facile per noi dire 'basta applicare le patch', ma è un problema estremamente complesso che richiede molto tempo e un investimento continuo".

La terza sfida è la visibilità. Justin spiega che molte delle conversazioni con i clienti ruotano attorno a problemi che si sono verificati perché il cliente non sapeva che un sistema vulnerabile, esposto a Internet, stesse operando nella loro rete. "Recentemente, per una conferenza, ho preso un caso di intrusioni avvenuto decenni fa e l'ho confrontato con un'intrusione avvenuta una settimana fa. Li ho messi uno accanto all'altro e ho chiesto: 'Quale di questi è accaduto nel 1986 e quale la scorsa settimana?' Nessuno avrebbe potuto dirlo perché i due sembravano molto simili. L'attacco era dovuto a una vulnerabilità del software che nessuno sapeva esistesse. Era dovuto a una configurazione errata del server, a una scarsa registrazione e registrazione degli eventi, e a una gestione delle patch limitata o nulla. I dettagli tecnici dei problemi sono diversi ora, ma i fondamentali sono gli stessi. Come difensori, non possiamo difendere ciò che non vediamo o non comprendiamo."

Methodology: For snapshot data, Microsoft platforms and services, including Microsoft Extended Detections and Response, Microsoft Defender, Defender Experts for Hunting, and Microsoft Entra ID, provided anonymized data on threat activity, such as malicious email accounts, phishing emails, and attacker movement within networks. Additional insights are from the 65 trillion daily security signals gained across Microsoft, including the cloud, endpoints, the intelligent edge, and our Compromise Security Recovery Practice and Detection and Response Teams. Cover art does not depict an actual soccer game, tournament, or individual sport. All sports organizations referenced are individually owned trademarks.

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