KEEPER | Pressemitteilung

Im Abseits: Mit dem illegalen Streaming der Fußball-Europameisterschaft gibt es nichts zu gewinnen

von: Darren Guccione, CEO und Mitbegründer, Keeper Security

Eine weitere Fußballmeisterschaft ist zu Ende und mit ihr die schönen, einzigartigen, erinnerungswürdigen und besonderen Momente, die ein solches Event mit sich bringt. Aber es war nicht alles Gold, was glänzt. Zwar stand der Fußball im Juni in Europa wieder einmal im Fokus, doch nicht alles lief glatt. Fußballfans in Singapur beispielsweise konnten zwar die Spiele live verfolgen – allerdings nur im Bezahlfernsehen und das war vielen zu teuer. Da das Turnier in Deutschland ausgetragen wurde, fanden die Spiele für die Fans in Singapur während der Nachtstunden statt. Viele der Fans waren daher wählerisch bei der Auswahl der Spiele und bleiben nur für die großen Matches während des einmonatigen Wettbewerbs wach. Das wiederum veranlasste viele Singapurer dazu, auf illegale Streamingdienste zurückzugreifen, anstatt sich über teure legale Quellen mit Fußball zu versorgen. Dabei geriet ihre digitale Sicherheit ins Abseits.

Zu schön, um wahr zu sein

Auf lokaler Ebene bieten Streaming-Sites "kostenlose" Alternativen zu den saftigen Abonnementgebühren der Pay-TV-Sender an. Doch auch was nichts kostet, kann einen hohen Preis haben. In einer von der englischen Premier League in Auftrag gegebenen Studie mit dem Titel "Scams, Cyber Threats and Illicit Sports Streaming in Singapore" aus dem Jahr 2024 wurde festgestellt, dass die Wahrscheinlichkeit, auf Streaming-Seiten auf eine Cyber-Bedrohung zu stoßen, im Durchschnitt bei 48 Prozent liegt. Das geht mit einem 3,5-mal höheren Risiko für die Besucher der Streaming-Plattformen einhergeht. Darüber hinaus wurden 54 Prozent der Werbeanzeigen auf solchen Websites als hochriskant eingestuft.

Die Cyberkriminalität weltweit und damit auch in Singapur nimmt zu. Und das illegale Streaming öffnet eine weitere Tür für Cyberkriminelle, die ungebeten in persönliche digitale Räume eindringen. Erst im letzten Jahr meldete die Polizei von Singapur, dass die Zahl der Fälle von Betrug und Cyberkriminalität um 69,4 Prozent auf 24.525 gestiegen ist, was zu Verlusten in Höhe von S$ 334,5 Millionen führte.

Fans, die sich Spiele auf diesen illegalen Streaming-Seiten ansehen, setzen sich großen Sicherheitsrisiken aus, darunter Malware, Datendiebstahl und Finanzbetrug. Dies gilt nicht nur für Fußballfans, sondern für alle, die auf der Suche nach Unterhaltung, Filmen oder Fernsehserien über illegale Streaming-Seiten raubkopieren.

Die Cyber-Bedrohungslandschaft des illegalen Streamings

Es gibt mehrere gängige Tools, die von Cyberkriminellen auf illegalen Streaming-Seiten eingesetzt werden. Malvertising-Angriffe sind komplex und können verschiedene Techniken verwenden. In der Regel beginnt der Angreifer damit, einen Server eines Drittanbieters zu hacken, um bösartigen Code in eine Werbung, beispielsweise ein Banner oder ein Video, einzuschleusen. Wenn ein Nutzer auf die Werbung klickt, installiert der Code Malware oder Adware auf seinem Computer. Bei diesen Angriffen kann ein Exploit-Kit eingesetzt werden,

um Systemschwachstellen zu scannen und auszunutzen. Sobald die Malware installiert ist, kann sie Dateien beschädigen, den Datenverkehr umleiten, Aktivitäten überwachen, Daten stehlen oder einen Backdoor-Zugang schaffen. Die gestohlenen Daten werden meist gelöscht, gesperrt, geändert, weitergegeben, kopiert und gegen Lösegeld oder im Dark Web verkauft.

Redirect-Phishing ist ein weiteres Instrument, mit dem Cyberkriminelle Internetbesucher auf schädliche Websites locken, indem sie vertrauenswürdige Domänen ausnutzen. Sie nutzen Schwachstellen in Webanwendungen aus, die benutzergesteuerte Weiterleitungen ermöglichen. Im schlimmsten Fall führen diese Umleitungen zu Websites mit gefährlicher Malware, die in sichere Datensysteme eindringen kann.

Wenn jemand auf einen Phishing-Link klickt, wird er auf eine gefälschte Website weitergeleitet, die einer seriösen Website ähnelt und auf der er unwissentlich sensible Informationen wie Anmeldedaten, persönliche Informationen oder Finanzdaten eingeben kann, die die Cyberkriminellen dann stehlen.

Browser-Hijacking liegt vor, wenn unerwünschte Software oder bösartige Entitäten die Browsereinstellungen ohne Zustimmung des Benutzers ändern. Diese Änderungen zielen darauf ab, den Verkehr auf bestimmte Websites zu lenken und können sich auf Startseiten, Suchmaschinen, Fehlerseiten und Sicherheitseinstellungen auswirken.

Oft sind Hijacker in kostenlosen Downloads versteckt oder geben sich auf Streaming-Sites als hilfreiche Erweiterungen aus, so dass die Benutzer sie unwissentlich installieren. Die heimliche Natur des Browser-Hijackings bedeutet, dass es oft unbemerkt bleibt, bis unerwartete Änderungen beim Surfen auftreten.

Browser-Hijacker können sensible Daten stehlen, indem sie Tracking-Cookies installieren, um den Browserverlauf, Suchgewohnheiten und persönliche Informationen wie Anmeldedaten und Finanzdaten zu sammeln. Diese Informationen können für gezielte Werbung und Identitätsdiebstahl verwendet oder an Dritte verkauft werden, wodurch die Online-Privatsphäre und Sicherheit ernsthaft gefährdet werden.

Wiederherstellung nach einer Kompromittierung

Wenn durch eine Datenschutzverletzung sensible Informationen preisgegeben werden, müssen die betroffenen Parteien sofort benachrichtigt werden, damit sie geeignete Maßnahmen ergreifen können. Wenn beispielsweise Kreditkarteninformationen bekannt werden, muss die Bank kontaktiert werden, um die Karte zu sperren und Geldverluste zu verhindern. Wenn ein Online-Konto kompromittiert wurde, müssen die Anmeldedaten aktualisiert werden. Wenn Unternehmensdaten preisgegeben wurden, sollten sofort Updates, Patches und Sicherheitsmaßnahmen implementiert werden, um das Sicherheitsproblem zu beheben.

Wenn Betroffene feststellen, dass vertrauliche Informationen bei einem Datenschutzverstoß preisgegeben wurden, müssen sie ihr Passwort für das kompromittierte Konto sowie für alle anderen Konten, die das gleiche Passwort oder eine Version davon verwenden, sofort ändern. Die Erstellung neuer, eindeutiger Passwörter ist von entscheidender Bedeutung, um Wiederholungen zu vermeiden, und die Verwendung eines Passwortmanagers kann diesen

Prozess vereinfachen. Ein Passwort-Manager speichert und verwaltet Passwörter in einem verschlüsselten Tresor. Er speichert alle verwendeten Passwörter sicher und kann bei der Erstellung neuer Passwörter helfen, was die Aktualisierung gefährdeter Konten erleichtert.

Die Multi-Faktor-Authentifizierung (MFA) sollte bei allen Konten für die zusätzliche Sicherheit aktiviert sein. MFA ist eine Sicherheitsmaßnahme, die zusätzliche Überprüfungsschritte für den Zugriff auf digitale Konten erfordert. Mit MFA werden für jede Anmeldung sowohl die Anmeldedaten als auch mindestens eine weitere Form der Identifizierung benötigt, was eine weitere wichtige Sicherheitsebene darstellt. Damit stellt MFA sicher, dass Hacker, selbst wenn sie in den Besitz von Anmeldedaten gelangen, ohne die zusätzliche Identifizierung, die sie nicht umgehen können, keinen Zugang zu Konten erhalten. Dadurch wird es für sie viel schwieriger, ein Konto zu kompromittieren.

Abpfiff
Es ist nachvollziehbar, dass es sich in weit entfernten Zeitzonen nicht gelohnt hat, in das Streaming der Europameisterschaft zu investieren. Fußballfans in Singapur und in anderen Zeitzonen könnten natürlich grundsätzlich auf offizielle Streaming-Angebot verzichten. Das Verlangen, ein paar wichtige Spiele zu sehen, wird jedoch immer bleiben. Aber ist es die potenziellen Cyberrisiken, die mit illegalem Streaming verbunden wert? Stehen die 90 Minuten Aufregung in Relation dazu? Wahrscheinlich nicht.

Starke und sichere Gewohnheiten sind im digitalen Raum vonnöten, da Angreifer ständig neue Taktiken entwickeln, um Anwender online auszunutzen. Abgesehen von ethischen Bedenken sollten sich Fußballfans bei Live-Spielen grundsätzlich an seriöse Quellen halten, um zu vermeiden, dass ihre sensiblen Daten kompromittiert werden und zum Opfer neuester Cybercrime-Attacken werden.
Es lohnt sich nicht, das schöne Spiel durch illegales Streaming zu einem finanziellen Problem werden zu lassen. Die einzigen Gewinner werden immer die Cyberkriminellen sein, die das Ziel verfolgen, die Fans zu hacken und ihrer Daten habhaft zu werden.

###

Über Keeper Security:
Keeper Security verändert weltweit die Cybersicherheit für Menschen und Organisationen. Die intuitiven Lösungen von Keeper basieren auf einer End-to-End-Verschlüsselung, um jeden Anwender auf jedem Gerät und an jedem Standort zu schützen. Die Keeper Zero-Trust-Plattform für die Verwaltung von privilegierten Zugängen ist in wenigen Minuten einsatzbereit. Sie lässt sich nahtlos in jeden Technologie-Stack integrieren, um Sicherheitsverletzungen zu verhindern, Helpdesk-Kosten zu senken und Compliance zu gewährleisten. Keeper genießt das Vertrauen von Millionen von Einzelnutzern und Tausenden von Unternehmen und ist führend bei der Verwaltung von Passwörtern, Passkeys und Geheimnissen, privilegiertem Zugriff, sicherem Fernzugriff und verschlüsseltem Messaging. Erfahren Sie, wie die Zero-Trust- und Zero-Knowledge-Lösungen vor Cyber-Bedrohungen schützen auf KeeperSecurity.com.

Folgen Sie Keeper auf Facebook Instagram LinkedIn X YouTube TikTok

Pressekontakt für Keeper in DACH:
Alexandra Schmidt, +49 170 387 10 64
Thilo Christ, +49 171 622 06 10
keeper@tc-communications.de