

Coupe du monde 2014 : le match Hackers vs Fans ne fait que commencer

S curit 

Post  par : JPilo

Publi e le : 11/6/2014 11:30:00

Alors que le coup d'envoi du premier match de la Coupe du monde de football va  tre donn  ce jeudi 12 juin   Sao Paulo au Br sil, le risque de cyber-attaques semble bel et bien  tre de la partie. Selon un r cent communiqu  publi  par Reuters, le groupe de pirates informatiques Anonymous se pr pare en effet   lancer des attaques contre les sites Internet des grands sponsors de ce mondial, parmi lesquels Adidas, Emirates Airline, Coca-Cola ou encore Budweiser. Mais ce n'est pas tout. Les hackers comptent  galement profiter de l'intensit  que suscite un tel  v nement pour s'emparer des donn es sensibles de fans et acc der   leurs comptes bancaires, notamment via des sites publiant les scores en direct ou les toutes derni res actualit s relatives aux matchs.

Les internautes vont, sans le savoir,  tre expos s   des sites corrompus ainsi qu'  des campagnes de phishing et de malwares, bien souvent invisibles, capables d'infecter leurs ordinateurs, de voler leurs mots de passe et d'acc der   leurs informations personnelles.



Il y a également fort à parier que les pirates informatiques se serviront du Clickbait, une technique qui consiste à inciter les internautes à se rendre sur un site par le biais d'une vidéo ou d'un titre très accrocheur, et qui cache souvent des liens corrompus initiant l'installation de programmes malveillants tels qu'un cheval de Troie par exemple.

Une fois redirigés sur le site en question, l'internaute va activer le logiciel malveillant par un simple clic et devenir ainsi la proie des hackers.

De plus, les menaces actuelles s'étendent au-delà de la sphère personnelle puisque de nombreux fans vont se connecter à des sites liés à la Coupe du monde de football depuis leur lieu de travail et mettront ainsi potentiellement en danger les ressources et les données de l'entreprise.

Jean-Pierre Carlin, Directeur Europe du Sud chez LogRhythm, a fait les commentaires suivants :

« De nombreux cybercriminels profitent de l'engouement autour de la Coupe du monde, qui représente aujourd'hui l'événement sportif le plus important au niveau international. Les internautes ne vont pas forcément se méfier et seront plus enclin à remplir des formulaires d'inscriptions pour gagner des cadeaux par exemple, ou encore pour accéder à la retransmission des matchs.

En visitant ces sites et en communiquant leurs informations personnelles depuis leur poste de travail, les utilisateurs offrent la possibilité aux hackers de prendre le contrôle de leur ordinateur à distance et d'accéder au réseau de l'entreprise. Dès lors, les cyber-attaquants peuvent récupérer les informations confidentielles liées à l'entreprise mais aussi à celles de leurs clients ainsi qu'à des données bancaires. Si une attaque de grande envergure nuit à l'image d'une organisation, elle peut également avoir des conséquences très lourdes sur le plan économique.

Les entreprises doivent impérativement prendre les mesures nécessaires pour détecter et éliminer les menaces dans le cadre de cet événement majeur. Aujourd'hui, pour lutter contre les cyber-attaques de plus en plus sophistiquées telles que les menaces persistantes avancées (APT), les organisations utilisent des solutions de protection traditionnelles telles que des antivirus et firewall.

Si ces outils doivent faire partie intégrante de la stratégie de sécurité informatique, ils ne sont cependant pas assez performants et puissants pour pouvoir être utilisés seuls. Ils ne sont en effet pas en mesure de détecter toutes les menaces sur le réseau et n'offrent pas la possibilité d'analyser et remédier en temps réel.

Les solutions SIEM permettent en revanche de répondre à ces problématiques de sécurité en étant capable de surveiller tous les événements du réseau en temps réel et de les corriger à d'autres données. Cela permet aux organisations d'être alertées immédiatement en cas d'activité suspecte et de réagir avant qu'elle ne s'étende et cause des dommages durables. Avec une solution SIEM, les entreprises disposent d'une surveillance proactive, la clé absolue pour la sécurité de leurs données. »