G Data press release 2012

Site-urile mai multor cluburi faimoase de fotbal au fost compromise

Din cate se pare, a cazut victima si website-ul unei asociatii nationale de fotbal

Bucuresti (Romania), 15 iunie 2012 – Lovitura in primele zile ale evenimentului fotbalistic al anului! Un atacator, se pare, simpatizant al operatiunilor gruparii Anonymous relateaza despre spargerea unor site-uri de fotbal. El anunta mai multe astfel de spargeri – cea mai recenta nu este mai veche de trei-patru zile.

Atacatorul a sustras mii de date de pe website-uri si le-a dispersat pe Internet. Nume de utilizatori, nume reale, adrese de e-mail, numere de telefon si parole, uneori chiar si informatii despre conturi bancare au fost facute publice si doar arareori criptate. Conform hackerului, el a fost capabil sa extraga numeroase parole de admin cu adresele de host corespunzatoare, pe care le-a si publicat.

Chiar daca atacatorul a declarat initial ca a facut toate lucrurile acestea pentru distractie, a revenit cu un mesaj in care mentioneaza ca, in timp ce criza ruineaza viata oamenilor de clasa mijlocie, cluburile de fotbal castiga sume uriase.
Aceasta forma de protest digital numita de G Data, "Hacktivism", nu este o agresivitate comuna. G Data a avertizat la sfarsitul anului trecut ca asemenea atacuri vor avea loc pe perioada EURO 2012 in G Data preview for 2012.

Victimele sunt cluburi de fotbal de top din Germania, Italia, Olanda, Spania, Cipru si Grecia si o asociatie nationala de fotbal cu o importanta prezenta web, conectata la UEFA Euro 2012 si cu o comunitate de fani pe blog.

Din respect pentru victime, G Data nu va oferi, deocamdata, niciun fel de informatii despre identitatea acestora. G Data a contactat potentialele victime si le-a informat despre aceasta problema, oferind in acelasi timp asistenta si consiliere, acolo unde este cazul.

Cu privire la vulnerabilitatea exploatata:
Din informatiile adunate pana acum, exista suspiciuni ca atacatorul a exploatat vulnerabilitatea pentru a efectua injectari directe ale comenzilor SQL si infiltrarea comenzii CRLF, pentru a sustrage informatiile.

La ce folosesc datele sustrase?
Datele disponibile au un potential important pentru alte activitati frauduloase.

> Un exemplu: Oricine ar detine aceste date, stie ca persoanele din baza de date sunt microbisti si prin urmare, ar putea folosi datele pentru a trimite atacuri de spam cu continut fotbalistic (e-mail-uri cu subiecte gen "Your football ticket invoice" si

atasamente periculoase). Este evident ca datele pot fi folosite, la fel de bine, in orice alta campanie de spam.

Alt exemplu: Atacatorii ar putea pretinde ca sunt angajati ai unuia dintre cluburile atacate si ar putea contacta victimele prin telefon sau e-mail. Ingineria sociala este, din nou, cuvantul cheie.

Mai mult, datele stocate in aceste documente scurse pe Internet ar putea fi folosite pentru a accesa alte servicii web. Multi utilizatori folosesc, inca, aceeasi adresa de e-mail cu aceeasi parola pentru diferite servicii web, ceea ce se dovedeste a nu fi cea mai buna idee!

-###-