



الهجمات الإلكترونية باستعمال تسجيل الدخول بالمواقع الاجتماعية.

لعل أبرز مشكل في استعمال الشبكة المعلوماتية هو الهجمات الإلكترونية التي أصبحت اليوم هاجسا يؤرق جل المستخدمين للفضاء الافتراضي.



شرح مبسط لثغرة "SpoofedMe"

سنتكلم اليوم عن الهجوم على الحياة الخاصة باستعمال المعلومات الشخصية للمواقع الاجتماعية و بالتحديد استعمال تسجيل الدخول الاجتماعي Social login □ وسنكشف عن الثغرة الجديدة المسماة "SpoofedMe" التي أعلن عنها فريق من الباحثين في مختبر IBM X-Force's Application Security Research يوم الخميس الماضي .

يستعين العديد من مستخدمي الشبكة العنكبوتية بخدمة أصبحت منتشرة وهي خدمة الدخول باستعمال معلومات الدخول للمواقع الاجتماعية. هذه الخدمة تمكن المتوفرين على حساب في أحد المواقع الاجتماعية المعروفة من الدخول و استعمال مواقع أخرى بدون الحاجة الى التسجيل او إنشاء حساب جديد.

ولاستغلال هذه الثغرة يكفي معرفة بريد الضحية الإلكتروني الذي يستخدمه للدخول مثلا إلى Google و بعد ذلك يقوم المتجسس بإنشاء حساب في "لينكت إن" LinkedIn باستعمال بريد الضحية (بشرط عدم توفر الضحية على حساب سابق في نفس الموقع) وبعد إنشاء الحساب يعمد المتجسس إلى استعماله (دون الحاجة الى تأكيده) في الدخول على مواقع أخرى تدعم خدمة الدخول الاجتماعي مما يسمح للمتجسسين من دخول موقع مثل [ناسداك](#) بمعلومات مزيفة قصد التعليق أو نشر أخبار أو الاستفادة من خدمات معينة و العيب هنا هو أن موقع LinkedIn أنشأ خدمة الدخول الاجتماعي دون الحاجة إلى التأكد من الهوية و تفعيل الحساب .

وأشار التقرير إلى أن الخوادم المعيبة المستخدمة للدخول هي [Amazon](#) و [Linkedin](#) و [mydigipass](#) أما بالنسبة للمواقع "الضحية" فهي [Nasdaq](#) و [Slashdot](#)

الطريقة بسيطة جدا و لا تحتاج إلى معرفة تقنية معينة و الجدير بالذكر أن فريق IBM قام بإبلاغ المواقع المعنية قصد إصلاح الثغرة قبل نشرها للعموم.

شرح الطريقة على اليوتوب:

المصدر: **1**