SANS SECURITY AWARENESS

OUCH!

نشرة الوعي الأمني الإخبارية الشهرية للجميع

حيلة الرئيس التنفيذي /اختراق البريد الالكتروني للعمل

ما هي حيلة الرئيس التنفيذي /اختراق البريد الالكتروني للعمل؟

مهاجمو الانترنت مستمرون في تطوير نوع من هجمات البريد الإلكتروني يدعي حيلة الرئيس التنفيذي او اختراق البريد الالكتروني للعمل. وهي عباره عن هجمات بريد الكتروني موجهه لإيقاع ضحاياها في فخ القيام بأمور لا يجب فعلها. في الغالب يسعى الأشرار خلف المال. وما يجعل هذه الهجمات خطيره للغاية هو ان المهاجمين يستبقون هجومهم بعمل بحث ودراسة عن الضحايا. والحقيقة أيضا أن تقنيات الأمان والحماية يصعب جدا عليها ايقاف مثل هذه الهجمات لأنها لا تحتوي أي ملفات مرفقه مشبوهة او روابط ملغمه لتكتشفها.

فلننظر سويا كيف يتم الهجوم؟

في البداية يقوم المهاجم بالبحث عبر الانترنت عن الضحية الهدف وعن كل من يتفاعل الضحية معهم , على سبيل المثال لو كنت أنت المستهدف فسوف يبحثون عن مدرائك وأقرانك في العمل أو وكيل عقارات تعمل معه من بيتك. عندها يقوم المهاجم بصياغة ايميل مخادع وارساله لك متظاهرا بأنه أحد هؤلاء الأشخاص الموثوقين لديك. تحت عنوان رسالة طارئه جدا يطلب المهاجم منك ان تتخذ إجراءات عاجله وفوريةً، كقيامك بدفع فاتورةً، وتغيير بيانات المدفوع له أو إقناعك بأن ترد عليه ببيانات ووثائق حساسة. معتمدا في رسالته على أسلوب الضغط. واليك مثالان يوضحان كيف ينجح مثل هذا الهجوم

التحويلات المالية: مجرمو الانترنت يسعون خلف الاموال، فيقومون بالبحث عن الشركة التي تعمل بها مثلا ويحددون من يعمل فيها في دائرة المالية او الحوالات من زملائك. من ثم يقوم المجرمون بصياغة وارسال بريد باسم المشرف او المدير التنفيذي مطالبا إياهم بأنه وبشكل عاجل وطارئ يتعين عليهم الدفع أو تحويل الأموال لحساب ما في البنك، مستخدما أساليب الضغط والالحاح ليوقعهم في الخطأ وبالتالي ارسال الاموال لحساب المجرمين.

الاحتيال الضريبي: هنا مجرمو الانترنت يسعون خلف المعلومات الشخصية للضحايا لاستخدامها في التحايل الضريبي. أحد أسرع الطرق لهذا التحايل هي سرقه بيانات كل الموظفين في الشركة. فمثلا يقوم المجرمون بالبحث وتحديد هويه من يعمل في دائرة شؤون الموظفين وعندها يرسلون له رسائل الكترونيه مفبركة تظهر وكأنها من مديره المباشر أو أحد موظفي الشؤون القانونية تطالبه بضرورة إرسال البيانات الضريبة للموظفين فورا وبشكل عاجل فيقوم الضحية بالتنفيذ ليكون بذلك قد أرسلها لمجرمي الانترنت.

كيف تحمي نفسك

ما هي الإجراءات اللازمة لحماية نفسك؟ الوعي الأمني هو أفضل طريقة لحمايتك من الجرائم الالكترونية، سنعرض لك الأدلة الأكثر شيوعا لمعرفة الهجمات الالكترونية التي تتعرض لها:

البريد الإلكتروني يكون قصير جدًا وعاجل (غالبًا ما يكون جملتين فقط) والتوقيع يشير إلى أنه تم إرسال الرسالة الإلكترونية من جهاز هاتف محمول.

هناك شعور قوي بالإلحاح، مما يضغط عليك لتجاهل سياسات صاحب العمل أو تجاوزها. اتبع دائمًا السياسات والإجراءات المتعلقة بالعمل، حتى لو ظهر البريد الإلكتروني من رئيسك أو حتى الرئيس التنفيذي.

الرسالة الإلكترونية مرتبطة بالعمل، ولكنها تستخدم عنوان بريد إلكتروني شخصي، مثل @gmail.com أو @hotmail.com.

يبدو أن الرسالة الإلكترونية تأتي من أحد كبار القادة، أو زملاء العمل أو الموردين الذين تعرفهم أو يعملون معهم، ولكن لا تبدو صياغة الرسالة مثلهم وإنما صيغتها عامة.

يتم توفير إرشادات الدفع وتختلف هذه التعليمات عن تلك التي تلقيتها بالفعل، مثل طلب الدفع الفوري إلى حساب بنكي مختلف.

إذا كنت تشعر في استهدافك داخل العمل، قم بإيقاف كل التفاعل مع المهاجم وإبلاغ المسؤول المباشر بك بذلك. أما إذا كنت قد استهدفت في المنزل أو وقعت ضحية وتم إرسال حوالة مصرفية، يجب عليك ابلاغ البنك عل الفور وذلك لتطبيق القانون.

الضيف المحرر

دان كافندر، عميل سابق في مكتب التحقيقات الفدرالي، خبره 22 عاما في مجال التحريات الرقمية وجرائم الانترنت. يستهدف مؤخرا منظمات الجرائم الالكترونية كمنسق لملاحقه اختراقات ايميل الاعمال في العاصمة واشنطن. يعمل في مجال التدريب والأبحاث في مجال التحريات الرقمية وجرائم الانترنت. تابع دان علي @don_cavender. https://www.linkedin.com/in/donald-cavender

مصادر إضافية

الهندسة الاجتماعية (باللغة العربية): https://www.sans.org/sites/default/files/newsletters/ouch/issues/OUCH-201701_aa.pdf

لا تكن فريسة سهلة (باللغة العربية): https://www.sans.org/sites/default/files/2018-04/201804-OUCH-April-Arabic.pdf

أوقف البرمجيات الخبيثة(باللغة الانجليزية): https://www.sans.org/security-awareness-training/resources/stop-malware

تأمين بيانات الدخول(باللغة العربية): https://www.sans.org/sites/default/files/newsletters/ouch/issues/OUCH-201712_aa.pdf