النشرة الشهرية حول الوعي الأمني لمستخدمي الحاسب الآلي

OUCH!

في هذا العدد..

- ما هو التشفير ؟
- ما الذي تستطيع تشفيره ؟
- التشفير بالشكل الصحيح

حيلة الرئيس التنفيذي

ماهي حيلة الرئيس التنفيذي؟

مجرمو الإنترنت دائمًا مخادعون، يقومون باستخدام طرق متعددة للحصول على ما يريدون. إحدى الطرق الفعالة لتحقيق أهدافهم هي من خلال استهداف المستخدمين بشكل شخصي. لأن هؤلاء المجرمين يعلمون أن الأشخاص الجاهلين بمخاطر الانترنت هم الحلقة الأضعف في أي منظمة، لكنهم نسوا أن قراء آوتش! المطلّعين سيكونون أقوى حماية لجهات عملهم.

المحرر الضيف

أنجيلا باباس، مديرة التوعية الأمنية والتدريب بوكالة رويترز الإخبارية Thomson Reuters. كجزء من عملها، أنجيلا مسؤولة عن تدريب وتوعية الموظفين بمخاطر الخداع والاصطياد الالكتروني.

مجرمو الإنترنت طوّروا هجوماً جديدًا يسمى «حيلة الرئيس التنفيذي»، وتسمى أيضاً بالاحتيال على أنظمة البريد الإلكترونية الخاصة بالأعمال (Business Email Compromise). في هذه الهجمات، يدعي المهاجم بانه المدير التنفيذي أو أحد كبار المسؤلين في جهة عمل معينة، ثم يقوم بإرسال رسائل بريد إلكتروني لموظفي هذه الجهة ويطلب منهم القيام بعمل معين. هذا النوع من الهجمات فعّال جداً لأن المهاجمين يقومون بجمع معلومات عن ضحاياهم قبل تنفيذ الهجوم لإقناعك بتنفيذ ما يطلبون. يبحثون عن معلومات مثل مكان جهة العمل، وأسماء المسؤولين بها وأسماء الجهات التي تتواصل معها. وغالبًا تكون مصادرهم لهذه المعلومات موقع جهة العمل وحسابات التواصل الاجتماعي الخاصة بموظفيها (فيسبوك، لينكدإن، وتويتر, ...). عندما يجمع المهاجم معلومات كافية حول بعض الموظفين، يبدأ باستهدافهم. يتم تحديد المستهدفين بحسب هدف الاختراق، فإذا كان الهدف الحصول على المال، فيتم استهدف بعض المحاسبين، وإن كان الهدف معرفة بيانات حول الموظفين، فيتم استهدف بعض موظفي الموارد البشرية، وإن كان هدف الاختراق المعلومات المحفوظة في قواعد البيانات، فيتم استهدف بعض موظفي تقنية المعلومات.

عندما يتم تحديد ما يريد ومن يستهدف، يبدأ المهاجم بتوجيه «رماح التصيد» وهي عبارة عن رسائل بريد إلكتروني مخصصة تستهدف عددا محدداً و صغيراً من المستخدمين. هذه الرسائل تبدوا واقعية للغاية ويصعب اكتشاف انها رسائل تصيد. فهي تبدوا وكأنها مرسلة

حيلة الرئيس التنفيذي

من شخص تعرفه أو تعمل معه، مثل موظف أو زميل أو ربما أحد مسؤولي جهة عملك. كما أن هذه الرسائل قد تستخدم نفس المصطلحات التى يستخدمها زملائك فى العمل؛ وقد تستخدم شعار جهة عملك وربما التوقيع الرسمي لأحد المسؤولين. هذه الرسائل غالبا ما تطلب تنفيذ أمر معين بشكل عاجل جداً و دون إخبار أحد بهاذا. يهدف المهاجم من ذلك إلى دفعك الضحية لتنفيذ طلبهم دون التأكد من هوية مرسل الرسالة ومصداقية الطلب. وفيما يلي ثلاثة أمثلة شائعة:

حيلة الرئيس التنفيذي وسيلة هجوم فعالة يمكنها تجاوز أفضل الوسائل الدفاعية – أنت أفضل مدافع ضد هذا الهجوم.

تنفيذ حوالة مصرفية: في هذا المثال يقوم المهاجم باستهداف المال بشكل مباشر. يستهدف المهاجم أحد موظفي قسم المحاسبة ويطلب منه تحويل مبلغ من المال بشكل عاجل الى حساب معين. طبعاً يجب أن تظهر الرسالة وكأنها من رئيس ذلك الموظف حتى يقوم بتنفيذ الطلب.

ارسال بيانات بعض الموظفين: في هذا المثال يقوم المهاجم باستهداف بيانلا الموظفين الشخصية. يستهدف المهاجم أحد موظفي قسم الموارد البشرية ويطلب منه ارسال بيانات بعض الموظفين بشكل عاجل. كذلك يجب أن تظهر الرسالة وكأنها من رئيس ذلك الموظف حتى يقوم بتنفيذ الطلب.

الاحتيال الهاتفي: هذا النوع من الاحتيال يبدأ برسالة تبدوا من الرئيس التنفيذي أو أحد كبار المسؤولين يخبر فيها الضحية بأن شخصاً هاماً سيقوم بالاتصال به للحديث في أمر هام وأن عليه التعاون معه. بعد ذلك سيقوم المهاجم أو أحد معاونيه بالاتصال بهذا الموظف ويقوم بالحصول على المعلومات التي يريدها.

احمي نفسك

الحس السليم هو أفضل وسيلة للدفاع. إذا وصلتك رسالة من مديرك أو أحد زملائك يطلب فيها طلباً غريباً ، فهناك احتمال أن تكون هجوماً يستهدفك أو يستهدف جهة عملك. مما يزيد احتمالية ذلك أن يكون هناك استعجال لتنفيذ الطلب بشكل غير مبرر، أو أن توقيع

حيلة الرئيس التنفيذي

البريد الإلكتروني لا يبدو صحيحاً، أو أن طريقة الرسالة غير متوقعة من المرسل الذي تعرفه. دليل اخر على الاحتيال أن المهاجم يستخدم بريد الكتروني او رقم هاتف لم تشاهدهم من قبل. او يكون مشابها لدرجة كبيرة لكن ليس مطابقا لبريد مديرك في العمل او زميلك. إذا شككت في الامر، قم بالاتصال بمرسل الرسالة من خلال الهاتف أو مقابلته وجه لوجه (لا تقم بالرد أبدا على البريد الالكتروني) واستعلم منه عن موضوع البريد الالكتروني. لا تتجاوز إجراءات وقواعد الامان الخاصة بجهة عملك مثلاً أنظمة صرف الاموال أو إعطاء الصلاحيات أو إرسال البيانات الخاصة بالموظفين. الطلبات التي تحاول تجاوز هذه الإجراءات والقواعد بغض النظر عن مصدرها الظاهر، يجب ان تُعامل بحذر ولا بد من التحقق من مرسلها قبل اتخاذ أي اجراء بخصوصها. إذا استلمت مثل هذه الطلبات ولما تكن متأكدا ماذا تفعل، تواصل مع مديرك، او قسم أمن المعلومات في جهة عملك في الحال.

إعرف أكثر

أوتش الشهرية! نشرة توعوية بالأمن المعلوماتي. للاشتراك والوصول إلى الأعداد السابقة ولمعرفة المزيد حول "سانس" نأمل زيارة securingthehuman.sans.org/ouch/archives.

النسخة العربية

تتم ترجمة هذه النشرة شهريا من قبل مجموعة من الأساتذة و المتخصصين في أمن المعلومات.

مصادر إضافية

عدد أوتش حول "الهندسة الاجتماعية": https://securingthehuman.sans.org/newsletters/ouch/issues/OUCH-201411_aa.pdf

عدد أوتش حول "التصيد" (باللغة الانجليزية): https://securingthehuman.sans.org/resources/newsletters/ouch/2015#december2015

عدد أوتش حول "ما هي البرمجيات الخبيثة ": http://securingthehuman.sans.org/newsletters/ouch/issues/OUCH-201603_aa.pdf

عدد أوتش حول "التحقق باستخدام خطوتين ": http://securingthehuman.sans.org/newsletters/ouch/issues/OUCH-201603_aa.pdf

نصيحة اليوم الأمنية من سانز (باللغة الانجليزية): https://www.sans.org/tip-of-the-day

مجلس التحرير: بيل وايمان، والت سكريفن، فيل هوفمان، لانس سبيتسر، كارمن رويل هاردي، شيريل كونلي
ترجمها إلى العربية: طلال موسى الخروبي، فرج أحمد عز الدين، محمد سرور، زياد الشهري.