النشرة الشهرية حول الوعي الأمني لمستخدمي الحاسب الآلي

OUCH!

في هذا العدد..

- ماهي الهندسة الاجتماعية.
- إكتشاف وإيقاف هجمات الهندسة الاجتماعية.

الهندسة الاجتماعية

تمهيد

ثمة مفهوم خاطئ شائع لدى معظم الناس حول هجمات الانترنت هو أنها تستخدم أدوات وتقنيات متقدمة للغاية لاختراق أجهزة الكمبيوتر وحسابات المستخدمين. هذا ببساطة غير صحيح. يعلم مجرمو الانترنت أن أسهل الطرق لسرقة المعلومات الخاصة بك، أو إختراق حساباتك أو إلحاق الضرر بالأنظمة الخاص بك هو ببساطة عن طريق خداعك لكي ترتكب الاخطاء. في هذه النشرة سوف نتعلم كيف تُنفذ هذه الهجمات، والتي تسمى الهندسة الاجتماعية وما يمكنك القيام به للحماية منها.

المحرر الضيف

جيمس لين (@jameslyne) مدرب معتمد من سانز SANS ورئيس فريق الابحاث الدولي في شركة Sophos. قام باكتشاف العديد من الهجمات. قام بتأليف مقرر Metasploit (SEC580) حول اختبارات الاختراق و مقرر الهندسة الاجتماعية (SEC567) في معهد سانز SANS.

ما هي الهندسة الاجتماعية

الهندسة الاجتماعية هي هجوم نفسي حيث يقوم المهاجم بخداع الضحية للقيام بعمل لا ينبغي عمله. مفهوم الهندسة الاجتماعية ليس جديداً، فمنذ القدم وُجِد المحتالون و المخادعون. هم يسيرون على نفس النهج لكن الذي يجعل هذه الهجمات أكثر فاعلية هو أن الضحية لا يرى المهاجم غالباً، وعليه يمكن للمهاجم أن يدعي بسهولة أن يكون أي شخص يريد وبذلك يستهدف الملايين من الناس في جميع أنحاء العالم، بما فيهم أنت. بالإضافة إلى ذلك، يمكن لهجمات الهندسة الاجتماعية تجاوز العديد من التقنيات الأمنية. إن أبسط طريقة لفهم كيفية عمل هذه الهجمات وحماية نفسك منها هو أن نلقي نظرة على أمثلة حقيقة لتلك الهجمات.

تتلقى مكالمة هاتفية من شخص يدعي أنه من شركة دعم فني لاحدى شركات الحاسب أو مزودي خدمة الإنترنت أو ربما دعم فني لشركة مايكروسوفت. يشرح المتصل أن جهاز الكمبيوتر الخاص بك يقوم بنشاط مشبوه على شبكة الإنترنت، وأنهم يعتقدون أن الحاسوب مصاب بإحدى البرمجيات الخبيثة وأنه قد تم تكليفه بالقيام بمساعدتك على تأمين جهازك. بعد ذلك يستخدم مجموعة متنوعة من المصطلحات التقنية ويحاول إقناعك من خلال عدة خطوات مربكة أن جهازك مخترق. على سبيل المثال، قد يطلب منك التحقق مما إذا كان لديك بعض الملفات على حاسوبك ، ويدلك على كيفية العثور عليها. عند تحديد موقع هذه الملفات، المتصل يؤكد لك أن هذه الملفات تثبت أن حاسوبك مصاب ، بينما في الواقع هذه الملفات هي بعض ملفات نظام التشغيل الموجودة على كل جهاز تقريباً. وبعد أن يكونوا قد خدعوك بالاعتقاد أن جهازك مصاب، يحاولون اقناعك بشراء إحدى البرمجيات منهم أو منحهم الوصول عن بعد إلى جهازك حتى يتمكنوا من

الهندسة الاجتماعية

إصلاحه. البرامج التي يقومون ببيعها هي في الواقع برامج خبيثة. إذا قمت بشرائها وتثبيتها فتأكد انك قد خدعت وتم إصابة جهازك ، وأنك من دفع لهم لإصابة جهازك. إذا أتحت لهم الوصول عن بعد إلى جهازك فقد أتحت لهم الإستيلاء عليه، وسرقة البيانات الخاصة بك واستخدامها.

الحس السليم هو دفاعك الأقوى لايقاف معظم هجمات الهندسة الاجتماعية.

مثال آخر هو هجوم الكتروني يدعى حيلة الرئيس التنفيذي ، والتي غالبا ما تحدث في العمل. يبحث فيها المهاجم عن معلومات عن مؤسستك ومدرائها وأسمائهم وزملائك في العمل وألقابهم. بعد ذلك يرسل المهاجم بريد الكتروني لك متظاهرا انه شخص من مؤسستك. البريد الإلكتروني يطلب منك بشكل عاجل إتخاذ إجراء، مثل إجراء حوالة مصرفية أو ان ترسل له معلومات سرية وحساسة عبر البريد الإلكتروني. في كثير من الأحيان هذه الرسائل تتظاهر أن هناك حالة طارئة تتطلب على وجه السرعة تجاوز الإجراءات الأمنية المتبعة، على سبيل المثال قد يطلب منك إرسال معلومات حساسة للغاية لحساب شخصي علي بريد gmail.com. ما الذي يجعل هذه الهجمات المستهدفة عالية الخطورة أن المهاجمين قاموا بجمع معلومات حول الضحية قبل البدء بالهجوم. وبالإضافة إلى ذلك، التقنيات الأمنية مثل مكافحة الفيروسات أو جدران الحماية لا يمكنها كشف أو وقف هذه الهجمات بسبب عدم وجود برامج ضارة أو روابط خبيثة.

تذكر دائما، هجمات الهندسة الاجتماعية مثل هذه لا تقتصر على المكالمات الهاتفية أو البريد الإلكتروني؛ فإنها يمكن أن تحدث في أي شكل بما في ذلك الرسائل النصية على هاتفك المحمول، وعلى وسائل التواصل الاجتماعية أو حتى شخصياً. فالحذر هو افضل وسيلة دفاع بالنسبة لك.

إكتشاف وإيقاف هجمات الهندسة الاجتماعية.

لحسن الحظ إيقاف مثل هذه الهجمات أبسط مما نعتقد الحس السليم هو أفضل دفاع. اذ تشككت في أمر ما أو بدا لك مريباً فقد يكون هجوما إلكترونياً. الخصائص الاكثر شيوعاً لهجمات الهندسة الاجتماعية هي:

- شخص ما يخلق شعور من الارباك والاستعجال لمحاولة خداعك لكي ترتكب خطأ.
- شخص يسأل عن معلومات خاصة ينبغي أن يعرفها مثلاً رقم حسابك البنكي وهو يدعي أنه أحد موظفي البنك الخاص بك.

الهندسة الاجتماعية

- شخص يسأل عن كلمة المرور الخاصة بك، لا يحق لاحد أن يطلب ذلك.
- شخص يضغط عليك لتجاوز أو تجاهل التعمليات الأمنية أو الإجراءات المتبعة في عملك.
- خبر فوزك بجائزة مالية ضخمة أو بجهاز حديث، حتى ولو لم تكن شاركت في أي مسابقة أصلاً .
- تتلقى رسالة بريد إلكتروني غريب من صديق أو زميل في العمل، تحتوي على صيغة لا يبدو أنها حقا لهم. مهاجم الإنترنت قد اخترق حسابه ويحاول خداعك. لحماية نفسك، تحقق من هذه الطلبات من خلال التواصل مع صديقك باستخدام طريقة اتصال مختلفة، عبر الهاتف مثلاً.

اذا كنت تشك ان أحداً ما يحاول خداعك، لا تتواصل معه أكثر. اذا كان الهجوم يتعلق بالعمل، تأكد من اعلام فريق أمن المعلومات في جهة عملك بالحادثة في الحال, تذكر الحس السليم هو أفضل دفاعاتك.

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 التصيد (باللغة الانجليزية):	https://securingthehuman.sans.org/ouch/2015#december2015
عدد أوتش حيلة الرئيس التنفيذي:	https://securingthehuman.sans.org/newsletters/ouch/issues/OUCH-201607_aa.pdf
عدد أوتش برمجيات طلب الفدية:	https://securingthehuman.sans.org/newsletters/ouch/issues/OUCH-201608_aa.pdf
ارشيف أعداد نشرة سانس:	https://securingthehuman.sans.org/ouch/archives

مجلس التحرير: بيل وايمان، والت سكريفن، فيل هوفمان، لانس سبيتسنر، كارمن رويل هاردي، شيريل كونلي
ترجمها إلى العربية: طلال موسى الخروبي، محمد سرور