دعوننا ننظر إلى أحد سيناريوهات الهجوم، المخترق طلال يهدف إلى إضافة جهاز كمبيوتر جديد إلى شبكة الكمبيوترات المخترقة التي يمتلكها في البوتنت (Botnet)*، قام بذلك عن طريق اختراق حساب الضحية سارة على برنامج التواصل الاجتماعي فيسبوك (Facebook)، و نظراً لأنها استخدمت كلمة مرور ضعيفة لحسابها الشخصي، تمكن طلال من تخمين كلمة المرور بسهولة، و قام طلال بانتحال شخصية سارة ليتمكن من إرسال رسالة على فيسبوك (Facebook) إلى صديقتها مريم، و يقوم طلال بإدراج أحد الروابط لتنزيل برنامج مكافحة الفيروسات المجاني في الرسالة المرسلة إلى الضحية مريم، و نظراً لأن مريم تثق في سارة باعتبارها خبيرة في تقنية المعلومات، فإنها تقوم بتنزيل البرنامج الخاص بالكمبيوتر و تثبيته على الكمبيوتر، و يحتوي البرنامج الذي تم تثبيته على فيروس حصان طروادة الذي يسمح لطلال بالاستيلاء على كمبيوتر مريم، و يمكنه من سرقة أي بيانات حساسة قد تكون في كمبيوتر مريم مثل البريد الإلكتروني (Gmail) و كلمة المرور (Password) الخاصة بمريم، لكن الأهم من ذلك أنه بإمكانه استخدام حساب البريد الإلكتروني (Gmail) الخاص بمريم و إرسال رسائل بريدية لجميع أصدقائها في قائمة بريدها الإلكتروني، و تحتوي هذه الرسالة على ملف بصيغة (PDF) المصاب بفيروس حصان طروادة و الذي يظهر على أنه دعوة لحفل عيد ميلاد، مريم لديها كلمة مرور قوية و لكن حفظها لكلمة المرور (Password) على متصفح الانترنت و جهازها يحتوي على الفيروس تمكن طلال من الوصول إليها.

*تعريف البوتنت (Botnet): هي شبكة من أجهزة الكمبيوتر الخاصة المصابة بالبرامج الخبيثة و الضارة و التحكم بها كمجموعة دون علم صاحب الكمبيوتر.

ما الذي يمكنك عمله لحماية نفسك وحماية البيئة الكمبيوترية الخاصة بك؟

بينما يظل حماية البيئة الكمبيوترية الخاصة بك أحد التحديات ضد أي هجمات مقصودة و متعددة الأفرع و متطورة فإنه بإمكانك تقليل المخاطر بإتباع عدد من إجراءات أمن المعلومات الأساسية، و فيما يلي بعض من إجراءات الأمن الرئيسية التي ينبغي عليك إتباعها:

إدارة مكافحة الجرائم الإلكترونية :

هاتف: +(965) 25660142

البريد الالكتروني: Info@cybercrime.gov.kw

حسابنا في مواقع التواصل الاجتماعي: @ECCCD

اعرف عدوك

من المعروف عامة أن الناس أنفسهم هم أضعف وصلة في سلسلة أمن المعلومات

و أن المهاجمون أصبحوا أكثر تطوراً في استغلال هذه الميزة. و حالياً فإن المهاجم المحترف بات أكثر حرفية و يعمل بصورة أكثر سرية و يعتمد بصورة كبيرة على أساليب الهندسة الاجتماعية لاستهداف الضحايا من خلال الخداع و الغواية بدون قصد و أحياناً بصورة متعمدة لتوفير المعلومات و الدخول و الذي قد يكون أصعب كثيراً لو أنه انتزع بالقوة، فهجمات الهندسة الاجتماعية تستهدف و بصورة متزايدة شركات أو أشخاص محددين و يتم تصميمها للاستفادة من واحد أو أكثر من الدوافع(الغرائز) البشرية الأساسية أو العواطف أو نواحي الضعف البشري، و الكثير من هؤلاء الضحايا لن يدركوا على الإطلاق أنهم أو أن أنظمتهم قد تعرضت للهجوم.

و عندما يستهدف المهاجمون الصفحة الرئيسية لبيئة كمبيوترية فإنهم يهدفون عادة إلى سرقة البيانات الشخصية مثل بطاقات الدفع و بيانات التوثيق المصرفي عبر الانترنت و أرقام الهوية الحكومية و يتطلعون أيضاً إلى الدخول إلى الأنظمة الكمبيوترية لجعلها جزء من شبكة البوتنت (Botnet)*،

و هذه العناصر التي يتم الولوج إليها عادة ما يتم بيعها إلى جهاز الاقتصاد السري و التي تقدر قيمتها بحوالي ٢٧٦ مليون دولار أمريكي حسب تقديرات شركة سيمانتك في عام ٢٠٠٨.

قم بحماية نقطة الدخول إلى الواي فاي(Wi-Fi) (تشفير الواب[1] (WAP) و تشفير كلمات المرور الافتراضية على أجهزة الراوتر و فلترة نظام ماك (Mac filter)[2]).

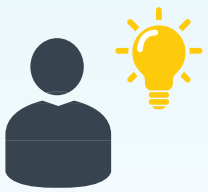
قم بتشغيل حسابات أنظمة التشغيل بالاستفادة من آخر المزايا إن أمكن.

قم بحماية نقاط اتصالك باستخدام برنامج أمني بواسطة أحد برامج مكافحة الفيروسات و جدران الحماية النارية الشخصية، و عليك بتحديث هذا البرنامج بصورة منتظمة.

قم بتحديث نظام التشغيل و برامج التطبيقات الكمبيوترية بصورة منتظمة.

قم بتشفير المعلومات الحساسة أو لا تقم بتخزينها على جهاز الكمبيوتر الشخصي المتصل بالإنترنت، و قم بتشفير المعلومات الحساسة التي ترسلها عبر الانترنت.

قم باختيار كلمات مرور قوية و تغييرها بصورة مستمرة.



فكر قبل القيام بالضغط: و كن حذر من رسائل البريد الإلكتروني و مواقع الإنترنت، فإذا كانت تبدو على أنها مواقع صحيحة بصورة كبيرة فإنه من المحتمل أن تكون مزيفة.

توخي الحذر بشأن المعلومات الشخصية التي تقوم بوضعها على مواقع التواصل الاجتماعي مثل شبكة (Linked-In) و فيسبوك (Facebook).

[1] الواب (WAP): بروتوكول التطبيقات اللاسلكية و هي معيار عالمي مفتوح للتطبيقات التي تستخدم التواصل اللاسلكي و وظيفته الأساسية هي تمكين الاتصال بالإنترنت من خلال الهاتف الذكي.

[2] فلترة نظام ماك (Mac filter): تنقية العناوين الخاصة بالأجهزة.

*تعريف البوتنت (Botnet): هي شبكة من أجهزة الكمبيوتر الخاصة المصابة بالبرامج الخبيثة و الضارة و التحكم بها كمجموعة دون علم صاحب الكمبيوتر.