SANS SECURITY AWARENESS

OUCH!

نشرتك الشهريه للتوعية بأمن المعومات

نعم، أنت مستهدف

نظرة عامة

يعتقد الكثير من الناس أنهم ليسوا هدفاً للهجمات الإلكترونية معتقدين أنهم، أو أنظمتهم وحساباتهم لا قيمة لها. وفي حقيقة الامر هذا اعتقاد خاطئ وبعيد عن الحقيقة فإن كنت مستخدماً للتكنولوجيا في البيت أو العمل أو أي مجال آخر فإنك ذو قيمة كبيرة بالنسبة للمهاجمين. وأنت وليس غيرك خط الدفاع لتلك الهجمات الإلكترونية.

لماذا يتم استهدافك؟

تختلف دوافع وطرق مهاجمين الفضاء الإلكتروني لتحقيق أهدافهم من خلال اختراق مستخدمي الانترنت وعلى سبيل المثال لا الحصر سنستعرض مثاليين للمهاجمين عبر الانترنت ولماذا يتم استهدافك:

⚠ **الجريمة الإلكترونية (Cyber Criminal):** يعتبر الانترنت ذا قيمة كبيرة لهم لأنهم من خلاله يستطيعون استهداف أي شخص بالعالم بسهولة ومن خلال العديد من الطرق التي تمكنهم من كسب المال منك على سبيل المثال سرقة الأموال من حسابك المصرفي، حساب التقاعد، بطاقة الائتمان أو إرسال الفواتير إليك بالإضافة أنهم يمكنهم استخدام جهازك الشخصي لاختراق حسابك للتواصل الاجتماعي أو الألعاب وبيعهم لجهات أخرى. ويقدر عدد مجرمي الفضاء الإلكتروني بمئات الآلاف يستيقظون كل صباح بهدف اختراق أكبر عدد ممكن من الأشخاص في كل يوم، بما في ذلك أنت.

☆ **المُهاجمون المُستهدِفون (Targeted Attackers):** هؤلاء المهاجمون مدربين وذو خبرة عالية جداً وهم بالأغلب يتبعون لحكومات أو يتم استغلالهم من قبل مؤسسات لأغراض مخصصة. يعتقد الكثير من الأشخاص أن طبيعة عملهم غير مهمة أو غير ملفتة للاهتمام، ولكنك ستستغرب بأن:

- قيمة المعلومات التي تقوم بالعمل عليها لها أهمية عند الشركات المنافسة أو الحكومات المختلفة.

- قد يتم اختراقك للوصول لزملائك بالعمل أو اختراق الأنظمة.
- قد يتم اختراقك لمعرفة ما تفعله الشركات الأخرى التي تتشارك أو تتعاون معها.

أنا أمتلك برنامجاً للحماية .. فأنا آمن

حسنا، على ما يبدو أنني مستهدف، لا مشكلة. سأقوم بتنصيب برنامج حماية من الفيروسات مع جدار حماية ناري على حاسوبي فأكون محمياً وانتهت المشكلة، أليس كذلك؟ لسوء الحظ، لا. كثيرون هم الذين يعتقدون أن الحماية تتحقق بتنصيب برامج الحماية فقط. وهذا وبكل أسف ليس صحيحً تماماً. فتعقيد وقوه الهجمات الإلكترونية يستمر في التحسن شيئاً فشيئاً وكثير من هذه الهجمات تطورت طرقها لتتجاوز وبسهولة تقنيات الحماية. على سبيل المثال غالباً ما يتمكنون من صناعة برامج خبيثة لا تستطيع برامج الحماية من الفيروسات اكتشافها! أيضا، غالباً ما يتمكنون من خداع فلاتر الحماية للبريد الإلكتروني وإرسال رسائل غير مرغوبة أو رسائل لِتصيُّد المعلومات أو يمكنهم باستخدام مهارات الهندسة الاجتماعية اجراء مكالمة هاتفية معك لخداعك وسحب بياناتك الشخصية وكلمات المرور أو أموالك ورقم بطاقة الائتمان خاصتك. صحيح أن التكنولوجيا وتقنيات الحماية بما فيها من أجهزة وبرمجيات تلعب دوراً مهما، لكن أيضا وعيك الأمني مهم جداً وفي النهاية أنت أفضل دفاع.

لحسن الحظ، أن تكون آمناً ليس بالأمر الصعب، في النهاية الحس والوعي الأمني إضافة إلى بعض السلوكيات الأساسية ستكون أفضل الدفاعات. فعند استلامك بريداً الكترونياً، او رسالة نصية مكالمة هاتفية تُشعِرُك بأنها غاية في الأهمية أو تشعر بأنها غريبة او مشبوهة، قد تكون هجوماً يستهدفك. ولكي تتأكد من سلامة وأمان أجهزتك وحواسيبك احرص على تحديثها باستمرار وحبذا لو فعلت التحديث الالي. أخيراً، استخدم كلمات مرور قوية مختلفة وفريدة لكل حساب. وكونك على وعي واطلاع دائمين بمخاطر الهجمات الإلكترونية هو أفضل وسيلة للحماية. لا تعرف من أين تحصل على هذا الوعي والمعرفة؟ تابع بشكل مستمر نشرة OUCH! الإخبارية الشهرية على sans.org/ouch

الضيف المحرر

مات برومیلي Matt Bromiley يعمل في الاستجابة لحالا الطوارئ الناتجة عن الهجمات الالكترونية، حيث يتعامل مع جميع أنواع الاختراقات وتسريب البيانات. يعمل أيضا مدري لدي SANS لدورة التحقيقات الجنائية الالكترونية المتقدمة والتصرف في حالات الطوارئ FOR508 تابع مات عبر تويتر @mbromileyDFIR.

SANS SECURITY AWARENESS

مصادر إضافية

أوقف البرمجيات الخبيثة(اللغة الانجليزية): https://www.sans.org/u/L1J

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

الهجمات وعمليات الاحتيال عبر الهاتف (اللغة العربية): https://www.sans.org/sites/default/files/2018-07/201807-OUCH-July-Arabic.pdf

بوستر انت مستهدف (اللغة الانجليزية): https://www.sans.org/u/L23