SANS SECURITY AWARENESS

OUCH!

نشرتك الشهريه للتوعية بأمن المعومات

الحِيَل الشَخصية

نظرة عامة

يبدع مجرمو الانترنت في تنويع طرق ابتزاز مستخدمي الانترنت من خلال الاحتيال عليهم باستخدام طرق جديدة ومبتكرة من الحيل الشخصية، ومن الطرق الجديدة الذي يتبعها مجرمو الانترنت قيامهم بالحصول على معلومات الملايين من مستخدمي الانترنت عن طريق شرائها أو الحصول عليها من خلال اختراق لمواقع الانترنت. ثم استخدام تلك المعلومات لإضفاء الطابع الشخصي على هجماتهم. سنستعرض لكم كيف تعمل هذه الطرق في الابتزاز والاحتيال على مستخدمي الانترنت. معرفتكم بهذه الطرق سوف تساعدكم على اكتشافها وتجنب وقوعكم ضحية لهذا النوع الجديد من الاختراقات.

كيف تعمل؟

يعتبر استخدام البريد الالكتروني أو المكالمات الهاتفية من الطرق القديمة لعملية الاحتيال على مستخدمي الانترنت، حيث كان مجرمو الانترنت على سبيل المثال لا الحصر يبعثون برسائل اصطياد للضحية ومن أمثلة هذه الرسائل « فزت باليانصيب "دون أن يقوم مجرمو الانترنت بتحديد هوية المستهدف وإنما إرسالها بشكل عام لملايين المستخدمين وهي تكون ضمن رسائل موجهة بشكل عام ومن هنا يسهل اكتشافها.أما الاحتيال الشخصي فهو مختلف كلياً حيث يقوم مجرمو الانترنت بالبحث أولاً عن بيانات مستخدمي الانترنت بشكل مخصص وذلك من خلال الانترنت أو شراء قاعدة بيانات بأسماء الناس، وكلمات المرور (السر)، وأرقام الهاتف أو أي تفاصيل أخرى. كما يُسَهِل عملية الحصول على هذه البيانات كمية المواقع الذي يتم اختراقها بشكل دوري على شبكة الانترنت وما تحتويه من تفاصيل المستخدمين. وهي أيضا متوفرة عادة من خلال منصات التواصل الاجتماعي والمواقع الحكومية العامة. بعد ذلك يتم استهداف جميع هؤلاء الأشخاص بشكل مباشر.

إحدى الحيل الشائعة التي يستخدمها مجرمو الإنترنت في ابتزازك هي الخوف لإجبارك على دفع المال لهم، حيث يقوم مجرمو الانترنت بإرسال بريد الكتروني للضحية يحتوي علي بعض التفاصيل الشخصية مع كلمات مرور لك مما تحصلوا عليها من خلال الانترنت كبرهان وإثبات أنهم يعرفون عنك الكثير وأنهم قد اخترقوا جهازك الشخصي و عندهم تفاصيل دقيقة عن طبيعة تصفحك للإنترنت والمواقع التي تتصفحها و صورك الشخصية التي على جهازك الشخصي وغيرها من المعلومات التي قد توهم الضحية بأنه قد تعرض لعملية اختراق، ومن ثم فإنهم يطلبو منك ان تدفع لهم مقابل عدم نشر هذه البيانات للحفاظ على خصوصيتك وعدم إحراجك أمام الأصدقاء و المجتمع.

الخدعة التي تكمن هنا أنه في أغلب المواقف لم يتمكن مجرمي الانترنت من اختراق جهازك وهم لا يعرفون الكثير عنك ولا يعرفون أنشطتك على الانترنت، ببساطة يحاولون استخدام التفاصيل الشخصية القليلة التي لديهم عنك لإخافتك لتصديق أنهم اخترقوا حاسوبك أو جهازك ويجبروك على أن تدفع لهم مقابل عدم نشر هذه البيانات للحفاظ على خصوصيتك. تذَكَر، مجرمو الانترنت يمكن أن يستعملوا نفس تقنيات الاحتيال من خلال مكالمة هاتفية أيضا لابتزازك.

ماذا يتوجب علي أن أفعل؟

يجب أن تميز هذه الرسائل الالكترونية أو المكالمات أنها خدعة. من الطبيعي أن تشعر بالخوف عندما يكون لدى شخص ما معلومات شخصية عنك يرسلها لك من خلال البريد الالكتروني أو من خلال مكالمة هاتفية لابتزازك، تذَكَر المُرسِل يكذب. الهجوم هو جزء من حملة آلية واسعة النطاق، وليس محاولة لاستهدافك مباشرة. أصبح من السهل على مجرمي الإنترنت اليوم إيجاد أو شراء معلومات شخصية، لذا توقع المزيد من الحيل الشخصية مثل هذه في المستقبل. بعض الأدلة للتأكد:

- **عندما تتلقى رسالة بريد إلكتروني عاجلة جداً، أو رسالة أو مكالمة هاتفية تكون مشبوهة جداً. إذا كان شخص ما يستخدم العواطف مثل الخوف أو الإلحاح، انهم يحاولون إجبارك على التسرع لترتكب خطأ.**
- **عندما يطلب شخص ما الدفع من خلال البيت كوين Bit Coin، بطاقات هدايا، أو طرق أخرى لا يمكن تعقبها.**
- **عندما تتلقى بريداً إلكترونياً مريباً، ابحث في الانترنت من خلال جوجل لمعرفة ما إذا كان هناك أشخاص آخرون أبلغوا عن هجمات مماثلة.**

في نهاية الأمر أفضل وسيلة للدفاع هو الحس السليم وعدم التسرع والخوف، كما نوصيك باستخدام كلمات مرور صعبة وفريدة ومتنوعة لكل من حساباتك على الانترنت وهو ما يعد مرهق لك في تذكرها، فإننا ننصحك باستخدام برنامج مدير كلمات المرور ليساعدك على تذكر كلمات المرور الخاصة بك. كما يفضل استخدام أساليب تحقق متعددة للوصول للبيانات وليس كلمة مرور فقط إن أمكن.

الضيف المحرر

ليني زلتسر (Lenny Zeltser) يعمل في مختبرات منيرفا (Minerva Labs) للمنتجات الأمنية ويدرس أساليب مكافحة البرمجيات الضارة في معهد سانس (SANS) ليني نشيط على تويتر @lennyzeltser كما أنه يكتب على مدونته لأمن المعلومات على وحكومة حول العالم zeltser.com/blog.

مصادر إضافية

الهندسة الاجتماعية(اللغة العربية): https://www.sans.org/sites/default/files/newsletters/ouch/issues/OUCH-201701_aa.pdf
لا تكن فريسة سهلة (اللغة العربية): https://www.sans.org/sites/default/files/2018-04/201804-OUCH-April-Arabic.pdf
ابحث عن نفسك عبر الانترنت (اللغة العربية): https://www.sans.org/sites/default/files/2019-01/201901-OUCH-January-Arabic.pdf
تطبيقات إدارة كلمات المرور(اللغة العربية): https://www.sans.org/sites/default/files/newsletters/ouch/issues/OUCH-201709_aa.pdf

OUCH! من قبل فريق الوعي الأمني في SANS وتُوزّع بموجب Creative Commons BY-NC-ND 4.0. يسمح بتوزيع هذه النشرة شرط الإشارة للمصدر وعدم تعديل النشرة أو إستخدامها لأغراض تجارية. لترجمة النشرة أو لمزيد من المعلومات، يرجى الإتصال على: www.sans.org/security-awareness/ouch-newsletter. | المجلس التحريري: والت سكريفنز، فِل هوفمان، ألان واجونير، شيريل كونلي | ترجمها إلى العربية: محمد سرور، فؤاد أبو عويمر، درويش الحلو، اسلام الكرد