



هجمات المراسلة

نظرة عامة

واحدة من أكثر الطرق شيوعاً التي يحاول المهاجمون عبر الإنترنت خداعنا من خلالها هي هجمات البريد الإلكتروني (غالباً ما تسمى التصيد phishing) أو محاولة الاحتيال عليك عن طريق المكالمات الهاتفية. ومع ذلك، ومع استمرار تطور التكنولوجيا يحاول المخترقون دائماً استخدام أساليب جديدة ومتطورة لتشمل خداعك مع تقنيات المراسلة مثل الرسائل النصية أو iMessage / Facetime أو WhatsApp أو Slack أو Skype إليك بعض الخطوات البسيطة لحماية نفسك وتحديد هذه الهجمات الشائعة أو إيقافها.

ما هي الهجمات التي تتم عبر برمجيات المراسلة؟

هجمات المراسلة (تسمى أحياناً Smishing، وهي تحوير على كلمة Phishing) عندما يستخدم المخترقون تقنيات الرسائل النصية للتواصل معك ومحاولة خداعك لتتخذ إجراء لا يجب عليك اتخاذه. ربما يريدون خداعك لتضغط على رابط ضار، أو الاتصال بك على رقم هاتف حتى يتمكنوا من الحصول على معلوماتك المصرفية. تماماً كما هو الحال في هجمات البريد الإلكتروني التقليدية، غالباً ما يلعب الأشرار على عواطفك لتفعل أشياء لا يجب عليك القيام بها. ومع ذلك، فإن ما يجعل هجمات المراسلة خطيرة جداً لدرجة أنها غالباً ما تشعر بأنها غير رسمية أو شخصية أكثر من البريد الإلكتروني، مما يجعلك أكثر عرضة أن تقع ضحية لمثل تلك الهجمات. بالإضافة إلى ذلك، مع هجمات الرسائل، يكون هناك معلومات أقل وأقل عددًا من الأدلة التي يمكنك التقاطها بأن هناك شيئاً ما خطأ أو مشبوه. عندما تتلقى رسالة تبدو غريبة أو مشبوهة، ابدأ بسؤال نفسك هل هذه الرسالة منطقية، لماذا أتلقتها؟ فيما يلي بعض الدلائل الأكثر شيوعاً للهجوم.

شعور هائل بالإلحاح، عندما يحاول شخص ما أن يدفعك لاتخاذ إجراء ما.



هل تطلب هذه الرسالة معلومات شخصية أو كلمات مرور أو معلومات حساسة أخرى لا ينبغي لهم الوصول إليها؟



هل تبدو الرسالة جيدة جداً بحيث لا تكون صحيحة؟ لا لم تفز باليانصيب، خاصة في مسابقة لم تدخلها من قبل.





رسالة تظهر على ما يبدو من حساب زميل في العمل أو صديق أو رقم هاتف، لكن الصياغة لا تبدو صحيحة مثل ما تعودت منهم. قد يكون حساب صديقك أو زميلك قد تعرض للاختراق واستولى عليه المهاجم، ثم يحاول المهاجم التظاهر بأنك مالك الحساب الحقيقي، مما يخدعك في اتخاذ إجراء ما.



إذا تلقيت رسالة تحاول إجبارك للقيام برد فعل قوي، فانتظر لحظة وامنح نفسك فرصة لتهدأ والتفكير في الرسالة قبل الرد.

في بعض الأحيان، سيجمع المخترقون بين هجمات البريد الإلكتروني والرسائل. على سبيل المثال، يمكن أن تعمل حيل بطاقات الهدايا بهذه الطريقة. سيرسل لك مهاجم الإنترنت رسالة بريد إلكتروني عاجلة يتظاهر بأنه صديق أو زميل في العمل، ثم يطلب رقم هاتفك الخليوي. بعد ذلك يقومون بإرسال رسائل نصية متكررة، والضغط عليك لشراء بطاقات الهدايا. بمجرد الشراء، يطلب منك المهاجمون كشط الكود الموجود علي ظهر البطاقات وإرسال صورة للرموز إليهم. هجوم اخر شائع يحثك المهاجمون على التحقق من مقطع فيديو أو صورة بعنوان «لن تصدق هذا» إنه يستغل شعورك بالفضول. إذا كانت الرسالة تبدو أنها من شخص تعرفه، اتصل بالشخص على الموجود بالهاتف للتحقق قبل أن تتصرف.

إذا تلقيت رسالة تنبيه من مؤسسة رسمية، فتتحقق منها مباشرةً. على سبيل المثال، إذا تلقيت رسالة نصية من البنك الذي تتعامل معه تفيد بوجود مشكلة في حسابك المصرفي أو بطاقتك الائتمان، فاتصل بالبنك أو شركة بطاقة الائتمان مباشرةً من خلال زيارة موقع الويب الخاص بهم أو الاتصال بهم مباشرة باستخدام رقم الهاتف من الجزء الخلفي من بطاقتك المصرفية لحسابك أو بطاقة ائتمان. ضع في اعتبارك أن معظم الوكالات الحكومية، مثل وكالات الضرائب أو وكالات إنفاذ القانون، لن تطلب منك بيانات عبر رسالة نصية. عندما يتعلق الأمر بهجمات الرسائل، فأنت أفضل دفاع لديك.



الضيف المحرر

جن فوكس الحاصلة على وسام DEF CON 23 الأمني والمختصة بمجال الهندسة الاجتماعية وهي تُوفّر تدريبًا في مجال الوعي الأمني بصفتها المختصة في البرنامج الأمني في سلسلة دومينوز. يُمكنك متابعتها على تويتر عبر حسابها @fox_j.

مصادر إضافية

الهندسة الاجتماعية:

لا تكن فريسة سهلة:

هجمات الاحتيال عبر الهاتف:

التبليغ عن الرسائل النصية الاحتمالية:

<http://www.sans.org/u/XAQ>

<http://www.sans.org/u/XAV>

<http://www.sans.org/u/XB0>

<https://www.consumer.ftc.gov/articles/0350-text-message-spam>

OUCH! من قبل فريق الوعي الأمني في SANS وتوزع 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 سكرينغز، فل هوفمان، ألان واجونير، شيريل كونلي | ترجمها إلى العربية: محمد سرور، فؤاد أبو عويمر، درويش الحلو، اسلام الكرد