SANS SECURITY AWARENESS

اكتشاف وإيقاف هجمات برمجيات المراسلة

ما هي الهجمات التي تتم عبر برمجيات المراسلة؟

Smishing (كلمة ممتزجة تجمع بين الرسائل القصيرة والتصيد الاحتيالي) هي هجمات تحدث عندما يستخدم المهاجمون الإلكترونيون الرسائل النصية القصيرة أو المراسلة أو غيرها من التقنيات المماثلة في خداعك لاتخاذ إجراء لا يجب عليك اتخاذه. ربما يخدعونك بتقديم تفاصيل بطاقتك الائتمانية، أو يحثونك على الاتصال برقم هاتف للحصول على معلوماتك المصرفية، أو يقنعونك بملء استبيان على الإنترنت لجمع معلوماتك الشخصية. تمامًا كما هو الحال في هجمات التصيد الاحتيالي عبر البريد الإلكتروني، غالبًا ما يلعب مجرمو الإنترنت على مشاعرك لحثك على التصرف من خلال خلق شعور بالإلحاح أو الفضول، على سبيل المثال. ومع ذلك، فإن ما يجعل هجمات الرسائل خطيرة للغاية هو وجود معلومات أقل بكثير وأدلة أقل في النص مقارنة بنصّ البريد الإلكتروني، وهذا يُصعّب عليك اكتشاف وجود خطأ ما.

من أمثلة الخداع الشائعة تلقّيك رسالة تخبرك أنك ربحت جهاز Phone، وما عليك سوى النقر على رابط وملء استبيان للمطالبة به. في الواقع، لا يوجد هاتف ولقد جرى تصميم الاستبيان لجمع معلوماتك الشخصية. مثال آخر هو رسالة تفيد بأنه لا يمكن تسليم الحزمة إلى عنوانك، ويترافق هذا مع رابط إلى موقع ويب حيث يُطلب منك تقديم المعلومات اللازمة لإكمال التسليم، بما في ذلك تفاصيل بطاقة الائتمان الخاصة بك لتغطية "رسوم الخدمة". في بعض الحالات، قد تطلب منك هذه المواقع تثبيت تطبيق جوال غير مصرح به يصيب جهازك بفيروس يؤدّي للاستيلاء عليه.

في بعض الأحيان، يجمع مجرمو الإنترنت هجمات الهاتف والرسائل. على سبيل المثال، قد تتلقى رسالة نصية عاجلة من البنك الذي تتعامل معه تسألك عما إذا كنت قد سمحت بدفع دفعة مالية واحدة. تطلب منك الرسالة الرد بنعم أو لا لتأكيد الدفع. إذا رددت، يعرف مجرم الإنترنت الآن أنك على استعداد للمشاركة وسيتصل بك متظاهرًا بأنّه من قسم الاحتيال في البنك. سيحاول بعد ذلك الحصول منك على معلوماتك المالية ومعلومات بطاقتك الائتمانية، أو حتى معلومات تسجيل الدخول وكلمة المرور الخاصة بحسابك المصرفي.

اكتشاف وإيقاف هجمات برمجيات المراسلة

فيما يلي بعض الأسئلة التي يجب أن تطرحها على نفسك لتحديد الأدلة الأكثر شيوعًا لهجوم الرسائل:

- هل تخلق الرسالة إحساسًا هائلاً بالإلحاح في محاولة الاستعجال أو الضغط عليك لاتخاذ إجراء ما؟
- هل تنقلك الرسالة إلى مواقع الويب التي تطلب معلوماتك الشخصية أو بطاقتك الائتمانية أو كلمات المرور أو غيرها من المعلومات الحساسة التي لا ينبغي لهم الوصول إليها؟
- هل تبدو الرسالة جيدة جدًا بحيث لا تكون صحيحة؟ لا، لم تفز بالفعل بجهاز iPhone جديد مجانًا.
- هل يجبرك الموقع أو الخدمة المرتبطة على الدفع باستخدام طرق غير قياسية مثل Bitcoin أو بطاقات الهدايا أو تحويلات Western Union؟

- هل تطالبك الرسالة برمز المصادقة متعدد العوامل الذي تم إرساله إلى هاتفك أو تم إنشاؤه بواسطة تطبيقك المصرفي؟
- هل تبدو الرسالة مكافئة لـ "رقم خاطئ؟" إذا كان الأمر كذلك، فلا ترد عليه أو تحاول الاتصال بالمرسل؛ بل احذفه.

إذا تلقيت رسالة تنبيه من مؤسسة رسمية، فتحقق منها مباشرةً. لا تستخدم رقم الهاتف المضمن في الرسالة، استخدم رقم هاتف موثوق به بدلاً من ذلك. 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. تذكر أيضًا أن معظم الوكالات الحكومية، مثل وكالات الضرائب أو إنفاذ القانون، لن تتصل بك أبدًا عبر الرسائل النصية، وستتصل بك فقط عن طريق البريد المعتاد.

عندما يتعلق الأمر بهجمات الرسائل، فأنت أفضل من سيدافع عنك.

المحرّر الضيف

جيف لوماس هو محقق لمجموعة التحقيقات الإلكترونية التابعة لإدارة شرطة العاصمة في لاس فيجاس، ويقوم بتدريس دورة SANS SEC487 لجمع وتحليل الاستخبارات مفتوحة المصدر (OSINT). يحقق جيف في الجرائم المالية عالية التقنية، بما في ذلك تسويات البريد الإلكتروني للأعمال، والتصيد الاحتيالي، وبرامج الفدية، وقضايا سرقة العملات المشفرة المعقدة وغسيل الأموال.

الموارد

لا تكن فريسة سهلة: https://www.sans.org/sites/default/files/2018-04/201804-OUCH-April-Arabic.pdf

الهندسة الاجتماعية: https://www.sans.org/newsletters/ouch/social-engineering-attacks/

التصيّد - هجمات المكالمات الهاتفية الاحتيالي: https://www.sans.org/newsletters/ouch/vishing

ترجمها للعربية: محمد سرور، فؤاد أبو عويمر، جهاد أبو نعمة، اسلام الكرد