أوتش! | نيسان/أبريل ٢٠١٤

النشرة الشهرية حول الوعي الأمني لمستخدمي الحاسب الآلي

OUCH!

في هذا العدد..

نعم... في الواقع .. أنت هدف

نظرة عامة

ثمة مفهوم خاطئ شائع بين كثيرا من الناس هو أنهم ليسوا هدفاً للجرائم المعلوماتية، وذلك لأنه يعتقدون أنهم أو أجهزتهم ليس لها أي قيمة وهذا المفهوم غير صحيح. إذا كان لديك جهازحاسب، جهاز محمول، حساب على الإنترنت، عنوان بريد إلكتروني، بطاقات إئتمان، أو لديك أي نشاط آخر على الإنترنت، فأنت تساوي الكثير لدى مجرمي الإنترنت. في هذه النشرة سنفسر لماذا يتم استهدافك، وكيف تتم مهاجمتك، وماذا يمكنك أن تفعل لحماية نفسك.

المحرر الضيف

إريك كونراد - الرئيس والرئيس التنفيذي للتقنية لباك-شور للاتصالات«Backshore Communications» وهو المؤلف الرئيسي لكتاب دليل الدراسة لشهادة أمن المعلومات الإحترفية «CISSP»- الطبعة الثانية، وكتاب أحد عشر ساعة لشهادة أمن المعلومات الإحترفية «CISSP»- الطبعة الثانية. وهو أيضا مؤلف مشارك في مقرر ستة أيام متواصلة من المراقبة والعمليات الأمنية (SEC511) في معهد سانز.

لماذا يتم استهدافك؟

وجدت جرائم الإحتيال وأنتحال الشخصية والإبتزاز منذ بدأت الحضارات، فهي جزء من حياتنا اليومية. هدف المجرم دائما هو: كسب ما أمكن من المال، بأسهل الطرق، ومع أقل قدر ممكن من الخطورة. في السابق كان المجرمين مقيدون بمواقعهم وكان عليهم الذهاب بأنفسهم إلى أماكن تواجد ضحاياهم. وهذا الوضع لم يقلل فقط من الضحايا المتوقعة لهؤلاء المجرمين، لكنه أيضا كان يضع المجرم أمام مخاطر كثيرة. الآن، تغيرت الجريمة جذريا مع ظهور الإنترنت والتكنولوجيا. الآن مجرمو الإنترنت يمكنهم بسهولة إستهداف جميع المستخدمين تقريباً في أي مكان من العالم وبتكلفة ضئيلة أو معدومة، ودون وجود مخاطرة تذكر. بالإضافة إلى ذلك، أصبح مجرمو الإنترنت منظمين ويعملون بكفاءة عالية، مما يتيح لهم أن يكونوا أكثر فعالية من أي وقت مضى.

هدف مجرمي الانترنت هو الحصول على أرباح أعلى وهذا يتأتى بسرقة بيانات بطاقات الائتمان أكثر، اختراق حسابات مصرفية أكثر، كشف كلمات سر أكثر. لهذا، فإنهم يحاولون استهداف أي مستخدم متصل بالإنترنت بما فيهم أنت. مهاجمة ملايين المستخدمين في جميع أنحاء العالم قد يبدو عملاً صعباً، ولكنه فى حقيقة الأمر سهلٌ جداً لأن مجرمي الأنترنت يستخدمون برمجيات خاصة تقوم بالعمل نيابةً عنهم. على سبيل المثال، يقوم مجرموا الانترنت بإعداد قائمة تحتوي على عدة ملايين من عناوين البريد الإلكتروني ثم يقومون باستخدام برنامج بسيط يقوم بارسال رسالة تصيد إلكتروني على كل هذه العناوين. إرسال رسائل البريد الإلكتروني لا تكلف شيئا تقريباً. وقد يستخدم مجرمو الانترنت أجهزة حاسب مخترقة - ربما جهازك - للقيام

نعم... في الواقع .. أنت هدف

بهذا العمل. وهذا يعطينا مثال لأهمية جهازك بالنسبة لمجرمي الانترنت حيث أنهم على أقل تقدير يمكنهم استخدام جهازك لاختراق أو إيذاء الآخرين. في نهاية المطاف، هؤلاء المجرمين لا يعرفون من سيقع ضحية لهجمات التصيد التي يتم ارسالها، لكنهم يعرفون أن إرسال رسائل بريد إلكتروني أكثر يزيد احتمالية وقوع ضحايا. مثال آخر وهو أن يقوم مجرمو الانترنت باختبار كافة الاجهزة على الشبكة بحثا عن ثغرات أمنية، مرة أخرى يتم استخدام أجهزة مخترقة مسبقاً للقيام بهذا العمل. تذكر، لا يجري إستهدافك بشكل خاص، ولكن كما ذكرنا أن هؤلاء المجرمون يستهدفون الجميع.

قد لا تدرك ذلك، ولكن بياناتك والأجهزة الخاصة بك لها قيمة هائلة لدى مجرمي الإنترنت حول العالم.

كيف تحمي نفسك؟

عندما يحاول مجرمو الإنترنت مهاجمة جميع المستخدمين في جميع أنحاء العالم، هم في العادة يستخدمون أساليب بسيطة نسبياً. لحسن الحظ ومن خلال إتباع بعض الخطوات البسيطة التالية يمكنك أن تحمي جهازك وبياناتك من الاختراق أو الكشف:

- **كن حذراً:** أنت خط الدفاع الأول ضد أي هجوم عبر الإنترنت. تبدأ العديد من الهجمات بمحاولة خداعك مثل جعلك تفتح ملف مصاب مرفق مع البريد الإلكتروني أو خداعك لكى تفصح عن كلمة السر الخاصة بك عبر الهاتف. الحدس السليم هو أفضل دفاع لديك: إذا كان هناك شيء يبدو غريباً أو مشبوهاً، فإنه على الأرجح هجوم ضدك.

- **التحديث المستمر للتطبيقات:** تأكد من أن أي جهاز حاسب أو جهاز هاتف نقال تستخدمه يتم تحديثه باستمرار. هذا لا يشمل فقط نظام التشغيل، ولكنه يشمل جميع التطبيقات أو الإضافات التي تستخدمها. بمحافظتك على تحديث النظم والتطبيقات، يمكنك حماية نفسك ضد الهجمات الأكثر شيوعا.

- **كلمات المرور:** إستخدم كلمة مرور قوية ومختلفة لكلٍ من حساباتك. بهذه الطريقة عندما يحصل كشف لاحدى كلمات المرور لاحدى حساباتك تبقى حساباتك الأخرى آمنة. تأكد أيضا أن جميع الأجهزة الخاصة بك محمية بكلمة مرور قوية ومختلفة لكل جهاز. لحفظ كل كلمات المرور الخاصة بك والمحافظة على سريتها نقترح استخدام أحد التطبيقات المسماة»مدير كلمة المرور».

نعم... في الواقع .. أنت هدف

- **بطاقات الإئتمان:** تحقق من البيانات المالية الخاصة بك، نوصي بالتحقق مرة كل أسبوع على الأقل. بمجرد رؤية أي معاملات لم تقم بها في سجل بطاقة الإئتمان، عليك على الفور الأبلاغ عنها. إذا كان مصرفك يتيح لك خدمة إرسال بريد إلكتروني أو رسالة نصية لكل عملية تتم على بطاقتك ننصحك بتفعيل هذه الخدمة.

- **الشبكة الاسلكية في المنزل:** قم بتأمين نقطة الوصول لشبكة ال «واي فاي» المنزلية الخاصة بك بكلمة مرور قوية لكى تضمن أن الوصول للشبكة هو للمصرح لهم فقط. أيضا تأكد من تحديث كافة الأجهزة المتصلة بالشبكة المنزلية.

- **مواقع التواصل الإجتماعي:** كلما قمت بنشر معلومات أكثر على الإنترنت، كلما وضعت نفسك في خطر أكبر. المعلومات التى تنشرها لا تجعل من السهل على مجرمي الإنترنت إستهدافك وخداعك فقط، ولكنها تجعلك هدفا أكثر «جاذبية».

إعرف أكثر

أوتش الشهرية! نشرة توعوية بالأمن المعلوماتي. للاشتراك والوصول الى الأعداد السابقة ولمعرفة المزيد حول "سانس" نأمل زيارة http://www.securingthehuman.org.

النسخة العربية

تتم ترجمة هذه النشرة شهريا من قبل مجموعة من الأساتذة المتخصصين في أمن المعلومات بكلية علوم وهندسة الحاسب الآلي بجامعة الملك فهد للبترول والمعادن.

مصادر إضافية

عدد أوتش! حور تطبيقات إدارة كلمات المرور:	http://www.securingthehuman.org/newsletters/ouch/issues/OUCH-201310_aa.pdf
عدد أوتش! حول تأمين الشبكة المنزلية:	http://www.securingthehuman.org/newsletters/ouch/issues/OUCH-201401_aa.pdf
عدد أوتش! حول هجمات تصيد المعلومات عبر البريد الإلكتروني:	http://www.securingthehuman.org/newsletters/ouch/issues/OUCH-201302_aa.pdf
ملصق: أنت مستهدف:	http://www.securingthehuman.org/media/resources/STH-Poster-YouAreATarget-Arabic.zip

مجلس التحرير: بيل وايمان، والت سكريفن، فيل هوفمان، لانس سبيتسر، كارمن رويل هاردي
ترجمها إلى العربية: طلال موسى الخروبي، فرج أحمد عز الدين.