النشرة الشهرية حول الوعي الأمني لمستخدمي الحاسب الآلي

OUCH!

في هذا العدد..

- نظرة عامة
- مؤشرات حدوث الاختراق
- ماذا تفعل بعد حدوث الاختراق

تم اختراق جهازي، ماذا أفعل الآن؟

نظرة عامة

نحن نعرف أنك تشعر بالقلق و تريد أن تحمي جهازك الحاسوب وتتخذ الخطوات اللازمة لذلك. ومع ذلك، فتماماً مثل قيادة السيارة، مهما كنت تقود بأمان، عاجلاً أو آجلاً قد يحدث لك حادث. في هذه النشرة، سنقوم بتقيم بعض الخطوات لمعرفة ما إذا كان جهازك مخترق أم لا، وإذا كان الأمر كذلك فنقدم لك بعض المقترحات لما يمكنك القيام به حيال ذلك. في نهاية المطاف، كلما أسرعت بالكشف و الإستجابة لإختراق جهازك، كلما كان ذلك أفضل في تخفيف الضرر لك أو لجهة عملك.

المحرر الضيف

جيك ويليامز هو كبير الخبراء في « CSR Group ». وهو أيضا مؤلف مشارك في مقرر «الطب الشرعي للذاكرة» (FOR526) ومقرر «الهندسة العكسية للبرمجيات الخبيثة» (FOR610) لدى معهد سانز.يمكن متابعة ويليامز على (@MalwareJake؛ malwarejake.blogspot.com)

مؤشرات حدوث الاختراق

يجب أن تعرف أنك تحتاج عادةً لعدد من الخطوات للكشف عن حدوث اختراق لجهازك. فعليك مراقبة العديد من المؤشرات لمعرفة أن جهازك قد تم اختراقه. إليك بعض الأمثلة:

- تنبيه من برنامج مكافحة البرمجيات الخبيثة على جهازك بوجود برمجيات خطرة، وخاصة إذا كان ضمن التنبيه أن البرنامج غير قادر على إزالة أو عزل الملفات المتأثرة.
- الصفحة الرئيسية لمتصفح الإنترنت تغيرت بشكل غير متوقع أو أن المتصفح يأخذك إلى مواقع لا تريد الذهاب إليها.
- هناك حسابات جديدة على جهازك لم تقم بإنشائها.
- هناك برامج جديدة مثبتة على جهازك لم تقم بتثبيتها.
- جهازك يتوقف عن العمل بإستمرار أو يعمل بشكل بطيء للغاية.
- النظام يطلب الإذن لإجراء تغييرات على الرغم من أنك لم تثبت أو تحدث أي من التطبيقات.
- تنبيهات من جدار الحماية بأن برنامج غريب يطلب الإذن للوصول إلى الإنترنت.

© The SANS Institute 2014

تم اختراق جهازي، ماذا أفعل الآن؟

ماذا تفعل بعد حدوث الاختراق

إذا عرفت أنه قد تم إختراق جهازك، فعليك أن تتصرف بسرعة. كلما أسرعت بمعالجة الوضع كلما كان ذلك أفضل. إذا كان الجهاز الذي تستخدمه يخص جهة عملك، لا تحاول إصلاح الجهاز بنفسك ولا تطفئ الجهاز. فهذا قد يتسبب في اضرار أكثر، كما يمكن أن يزيل أدلة قيمة يمكن إستخدامها لمعرفة أسباب الإختراق ومن هو المهاجم. عليك أن تبلغ الجهة المختصة بجهة عملك عن الحادث فوراً. إن كنت تشعر بالقلق إزاء تأخر الجهة المختصة بالتصرف قم بفصل الجهاز من الشبكة ومن ثم ضعه في وضعية «sleep» أو «hibernation». إذا كنت تشك في وجود اختراق ولم تكن متأكداً، فمن الأفضل أن تبلغ الجهة المختصة بجهة عملك عن شكوكك، فلديهم على الأرجح إجرائات وفريق للتعامل مع مثل هذه الحالات.

عاجلاً أو أجلاً سيتعرض جهازك للاختراق. كلما تم اكتشاف المشكلة واجراء اللازم بشكل أسرع كلما كنت الاستجابة أفضل.

إذا حدث الاختراق لجهازك الشخصي فهناك عدد من الخطوات التي يمكنك إتخاذها بنفسك:

- **النسخ الإحتياطية**. أهم خطوة يمكنك إتخاذها هي إعداد نسخ إحتياطية مسبقا. تحديدا، أعمل نسخ إحتياطية بشكل منتظم ودوري و تأكد من القدرة على إستعادة الملفات من النسخ الإحتياطية. في كثير من الأحيان، عندما يتم إختراق جهازك، الخيار الأفضل لديك هو مسح القرص الصلب و إعادة تثبيت نظام التشغيل. وعندها تحتاج النسخ الاحتياطية لإسترداد البيانات الشخصية الخاصة بك.
- **تغيير كلمات المرور الخاصة بك**: تأكد من تغيير جميع كلمات المرور الخاصة بك. هذا لا يشمل فقط كلمات المرور على أجهزة الحاسب والأجهزة النقالة، ولكن كل كلمات المرور الخاصة بك على الإنترنت. تأكد من أن تقوم بتغير كلمات المرور من جهاز آخر موثوق وآمن.
- **برامج مكافحة البرمجيات الخبيثة**. إذا أعلمك برنامج مكافحة البرمجيات الخبيثة بإصابة ملف، يمكنك إتباع الإجراءات التي يوصي بها البرنامج. هذه التوصيات عادة تشمل عزل الملف، تنظيفه أو حذفه. معظم برامج مكافحة البرمجيات الخبيثة تعطيك روابط يمكنك إتباعها لمعرفة المزيد حول الإصابة التي تم اكتشافها. إن لم يتمكن البرنامج من عزل أو تنظيف الملف المصاب عليك أن تقوم بحذف الملف.
- **إعادة التثبيت**. إذا لم تتمكن من ازالة البرمجيات الخبيثة بإستخدام برنامج مكافحة البرمجيات الخبيثة ، فإن واحدة من الطرق الأكثر أمانا هي إعادة تثبيت نظام التشغيل. أولا، قم بفصل الجهاز من الشبكة ثم إتبع تعليمات الشركة المصنعة للنظام الخاص بك، في

© The SANS Institute 2014

تم اختراق جهازي، ماذا أفعل الآن؟

معظم الحالات، هذا يعني إستخدام البرنامج المدمج في إعادة تثبيت نظام التشغيل. إذا كان البرنامج مفقود أو مصاب، إتصل بالشركة المصنعة و أطلب منها إرسال البرنامج. لا تعيد تثبيت نظام التشغيل من النسخ الإحتياطية. قد تكون النسخ الإحتياطية بها نقاط الضعف التي سمحت لإختراق جهازك. الشيء الوحيد الذي تستخدمه من النسخ الإحتياطية هو البيانات الشخصية الخاصة بك. أيضا، إذا كان جهازك قديم، فقد يكون أسهل (وربما أرخص) شراء جهاز جديد بدلا من قضاء ساعات للإصلاحه.

- **المساعدة الفنية:** إذا كنت تشعر بالقلق لإختراق جهازك، ولكن تشعر أنك تملك المهارات أو المعرفة اللازمة لإصلاحه، نقترح أن تأخذ الجهاز لشخص أو جهة أكثر مهنية. على سبيل المثال، بعد أن تم إختراق جهازك، أدركت أن النسخ الإحتياطية غير مكتملة أو قديمة. قد تميل لنقل ملفات مهمة مثل الصور والوثائق من الجهاز المصاب والجهاز الجديد. إلى لكن من خلال ذلك، يمكنك عن غير قصد نقل برامج خبيثة وإصابة الجهاز الجديد. ثمة بديل أكثر أماناً بكثير وهو أن تأخذ الجهاز المصاب إلى شخص فني مؤهل لإستعادة الملفات بأمان دون المخاطرة بنقل العدوى إلى جهازك الجديد.

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! حول تطبيقات إدارة كلمات المرور: http://www.securingthehuman.org/newsletters/ouch/issues/OUCH-201310_aa.pdf

عدد أوتش! حول النسخ الاحتياطي واستعادة البيانات الشخصية: http://www.securingthehuman.org/newsletters/ouch/issues/OUCH-201309_aa.pdf

عدد أوتش! حول ما هي البرامج الضارة (باللغة الانجليزية): http://www.securingthehuman.org/newsletters/ouch/issues/OUCH-201402_en.pdf

ملصق: تعرق على الغريب أعرف الشرير – حدد الشر (باللغة الانجليزية): https://digital-forensics.sans.org/media/poster_2014_find_evil.pdf

أوتش! تنشر من قبل برنامج «سانْس» لحماية الإنسان ويتم توزيعها بموجب الرخصة Creative Commons BY-NC-ND 3.0. يسمح بتوزيع هذه النشرة شرط الإشارة للمصدر وعدم تعديل النشرة أو إستخدامها لأغراض تجارية. لترجمة النشرة أو لمزيد من المعلومات، يرجى الإتصال على: ouch@securingthehuman.org

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