النشرة الشهرية حول الوعي الأمني لمستخدمي الحاسب الآلي

OUCH!

في هذا العدد..

- نظرة عامة
- إصلاح الثغرات (Patching)
- النسخ الاحتياطي
- التصيد الإلكتروني (Phishing)

الدروس المستفادة من هجوم " WannaCry "

نظرة عامة

خلال الايام القليلة الماضية انتشرت الاخبار حول هجوم إلكتروني جديد باسم WannaCry والذي يعني باللغة العربية أرغب في البكاء. تمكن هذا الهجوم من إصابة أكثر من 200,000 جهاز حول العالم في جهات مختلفة تتضمن مستشفيات في بريطانيا. هناك عدة أسباب جعلت هذا الهجوم يحصل على اهتمام كبير: أولاً، أنه انتشر بسرعة بين اجهزة الكمبيوتر التي تعمل بنظام ويندوز مستغلاً إحدى الثغرات المكتشفة في النظام. ثانيا أن الهجوم كان من نوع برامج طلب الفدية وهي برامج تعمل على تشفير الملفات الموجودة في الجهاز المصاب وتمنع الدخول لهذه الملفات. السبيل الوحيد لاستعادة تلك الملفات هو دفع مبلغ 300 دولار للمهاجم لفك التشفير أو استعادتها من النسخ الاحتياطي إن كان يتم بشكل منتظم. ثالثاً أن هذا الهجوم كان المفترض أن لا يحدث لأنه كان يستغل إحدى الثغرات المكتشفة في نظام ويندوز والتي عرفتها الشركة المنتجة للنظام Microsoft وأصدرت تحديث مجاني على موقعها لإصلاح هذه الثغرة منذ عدة أشهر. ما حدث كان بسبب أن بعض المستخدمين لم يقوموا بتحميل وتثبيت التحديث المطلوب، كما أن بعض المستخدمين لا يزال يستخدم نظام تشغيل «ويندوز إكس بي» وهو إصدار قديم جداً وقد أعلنت الشركة عن توقفها عن دعم هذا الاصدار وعن توفير اي تحديثات له منذ عدة سنوات. نذكر هنا ثلاث خطوات بسيطة يمكنك القيام بها لحماية نفسك من هجوم WannaCry.

المحرر الضيف

الدكتور يوهانس أولريش هو "عميد البحوث" بمعهد سانز ومؤسس DShield.org. ومسؤول عن **مركز عاصفة الإنترنت بمعهد سانز** الذي يقوم بمتابعة التهديدات الأمنية الحاسوبية الحالية. يقوم بتدريس مقرر "أمان تطبيقات الانترنت" (**DEV522**)، "كشف الإختراق" (**SEC503**) و "بروتوكول الانترنت الاصدار السادس IPv6" (**SEC546**).

إصلاح الثغرات (Patching)

أولاً وقبل كل شيء، تأكد من تحديث أنظمة التشغيل والتطبيقات المسجلة على جميع الاجهزة المتصلة بالانترنت من أجهزة كمبيوتر وأجهزة نقالة و أجهزة لوحية. مهاجمو الإنترنت يبحثون باستمرار عن ثغرات قد تكون موجودة في أنظمة التشغيل أو التطبيقات المستخدمة. عندما يتم اكتشاف نقطة ضعف معينة يقوم المهاجمون بكتابة برامج تستطيع استغلال تلك الثغرة وتخترق من خلالها الأجهزة التي تستخدمها. وفي الوقت نفسه تقوم الشركة المنتجة للبرنامج الذي تم اكتشاف ثغرة به بالعمل جاهدين لاصلاح تلك الثغرة واصدار تحديث مناسب لذلك. تثبت ذلك التحديث ضروري جداً لمنع أي مهاجم يستغل تلك الغرة من اختراق جهازك. من المزعج أن الثغرة التي استغلها هجوم WannaCry قد تم اكتشافها واصدار تحديث لها من شركة Microsoft قبل حوالي شهرين. ورغم ذلك أبقت بعض الجهات أجهزة الكمبيوتر

الدروس المستفادة من هجوم " WannaCry "

الخاصة بهم دون تحديث. لذا نوصي بتمكين التحديث التلقائي - كلما كان ذلك ممكناً - لجميع الأجهزة المتصلة بشبكة الانترنت ويشمل ذلك أجهزة الكمبيوتر والأجهزة النقالة وأجهزة الجوال وأجهزة توزيع الشبكة وأجهزة الألعاب. كما نوصي باستبدال اي اجهزة قديمة تعمل بنظام التشغيل Windows XP.

المفتاح لحماية نفسك من الهجمات مثل WannaCry ثلاث خطوات بسيطة: التحديث المستمر للأجهزة والحذر من هجمات التصيد الإلكتروني والنسخ الاحتياطي المنتظم.

النسخ الاحتياطية

وفي بعض الحالات، قد تصيب هجمات الإنترنت مثل WannaCry حتى أحدث الأنظمة. من أنجح الوسائل للرجوع لبياناتك في حال تم اختراق جهازك هو وجود نسخة إحتياطية لتلك البيانات. ببساطة النسخ الاحتياطي هو نسخ المعلومات المخزنة إلى مكان آخر للرجوع إليها عند الحاجة. للأسف، لا يقوم الكثير من الناس بتنفيذ النسخ الاحتياطي على الرغم من أنها عملية بسيطة وغير مكلفة. يمكن تخزين النسخ الاحتياطي للبيانات في وسائط مادية أو ارسال النسخة إلى التخزين السحابي. لكل نهج مزاياه وعيوبه. يمكنك استخدام كلا النهجين في نفس الوقت إذا كنت غير متأكد من الطريقة التي يجب عليك استخدامها.

نقصد بالوسائط المادية مثل محركات الأقراص الصلبة الخارجية أو محركات الأقراص الموجودة في الشبكة الداخلية. ميزة استخدام الوسائط المادية أنها تتيح لك النسخ الاحتياطي واستعادة البيانات بسرعة عالية. ومن عيوب هذا النهج إذا أصيب أحد الأجهزة لديك ببرنامج خبيث يمكن للعدوى أن تنتقل إلى النسخ الاحتياطي. إذا كنت تستخدم وسائط مادية للنسخ الاحتياطي يجب تخزين الوسائط المادية بعيداً عن المكان الذي فيه الأجهزة التي تم نسخها وفي مكان أمن. تأكد من أن تتم تسمية النسخ الاحتياطية التي قمت بتخزينها بشكل صحيح. النظام السحابي هي خدمة توفرها شركات مختلفة لتخزين الملفات على شبكة الإنترنت. عادة، يمكنك الاستفادة من هذه الخدمة من خلال تثبيت برنامج خاص بتلك الخدمة على جهاز الكمبيوتر الخاص بك. مزايا التخزين السحابي سهولة الاستخدام بالإضافة إلى ذلك، في حال أصيب جهازك ببرنامج خبيث فلا يمكن للعدوى الانتقال إليه. أهم العيوب هو أن التخزين واستعادة البيانات يستغرق وقتاً طويلاً ويكون عادةً مكلفاً. تأكد من الإطلاع على بنود الخصوصية والأمن الذي توفره الشركة الموفرة للتخزين السحابي وهل توفر خدمة تشفير البيانات وهل تنفذ خاصية المصادقة القوية؟

الدروس المستفادة من هجوم " WannaCry "

التصيد الإلكتروني (Phishing)

يقوم مجرمو الانترنت بتحديث وتغيير أساليب الهجوم باستمرار. أحد الوسائل الحديثة التي يقوم مجرمو الانترنت باستخدامها هو التصيد الإلكتروني (Phishing). يتم التصيد الالكتروني من خلال ارسال رسالة بريد إلكتروني تحاول اقناع المستخدم بفتح مرفق مصاب أو زيارة موقع إلكتروني ضار. هجوم WannaCry لم يستخدم هذا الأسلوب في الهجوم، لكن هناك هجمات عديدة يتم تنفيذها بهذه الطريقة، بما في ذلك معظم أنواع برامج طلب الفدية. وبالإضافة إلى ذلك، سيقوم منفذي هجوم WannaCry بلا شك بتحديث أسلوب الهجوم في الأشهر المقبلة واستخدام تقنيات جديدة مثل التصيد الإلكتروني. المفتاح لحماية نفسك ضد هذه الهجمات هو الحذر عند فتح رسائل البريد الإلكتروني التي تبدو غريبةً أو مشبوهة أو تعد بجوائز أو مبالغ مالية ضخمة.

إعرف أكثر

أوتش الشهرية! نشرة توعوية بالأمن المعلوماتي. للاشتراك والوصول إلى الأعداد السابقة ولمعرفة المزيد حول "سانس" نأمل زيارة securingthehuman.sans.org/ouch/archives.

النسخة العربية

تتم ترجمة هذه النشرة شهريا من قبل مجموعة من الأساتذة و المتخصصين في أمن المعلومات.

مصادر إضافية

عدد أوتش حول ما هي البرامج الضارة—:	https://securingthehuman.sans.org/newsletters/ouch/issues/OUCH-201603_aa.pdf
عدد أوتش حول برامج طلب الفدية:	https://securingthehuman.sans.org/newsletters/ouch/issues/OUCH-201608_aa.pdf
عدد أوتش حول النسخ الاحتياطي:	https://securingthehuman.sans.org/newsletters/ouch/issues/OUCH-201508_aa.pdf
عدد أوتش حول التصيد الالكتروني (باللغة الانجليزية):	https://securingthehuman.sans.org/ouch/2015#december2015
عدد أوتش حول استخدم الحوسبة السحابية بأمان":	https://securingthehuman.sans.org/newsletters/ouch/issues/OUCH-201611_aa.pdf

مجلس التحرير: بيل واميان، والت سكريفن، فيل هوفمان، كاثي كليك، شيريل كونلي
ترجمها إلى العربية: طلال موسى الخروبي، محمد سرور