النشرة الشهرية حول الوعي الأمني لمستخدمي الحاسب الآلي

OUCH!

في هذا العدد..

- ماهي البرمجيات الخبيثة
- من الذي يصدر البرمجيات الخبيثة
- كيف تحمي نفسك منها

ما هي البرمجيات الخبيثة

لمحة عامة

ربما سمعت بعض المصطلحات عندما يتناقش الناس عن أمن المعلومات، مثل فايروس (Virus)، حصان الطروادة (Trojan)، برمجيات طلب الفدية (Ransomware)، وأدوات التحكم الخفي (Rootkit). كل هذه المصطلحات تنتمي لمجموعة برمجيات يستخدمها مجرمو المعلومات لمهاجمة أجهزة مستخدمي الانترنت. البرمجيات الخبيثة (Malware) هو المصطلح الأشمل الذي يعبر عن جميع هذه الأنواع، وفي هذه النشرة سنشرح مما تتكون هذه البرمجيات، ومن يصدرها ولماذا، والأهم من ذلك ما الذي يمكنك فعله للحماية منها.

المحرر الضيف

ليني زيلتسير متخصص في حماية عمليات تقنية المعلومات للعملاء في شركة NCR Corp ، بالإضافة لتدريسه مكافحة البرمجيات الخبيثة في معهد سانس. يمكن التواصل مع ليني عبر تويتر (@lennyzelter) وكذلك الاطلاع على مدونته عن أمن المعلومات عبر (zeltser.com).

ماهي البرمجيات الخبيثة؟

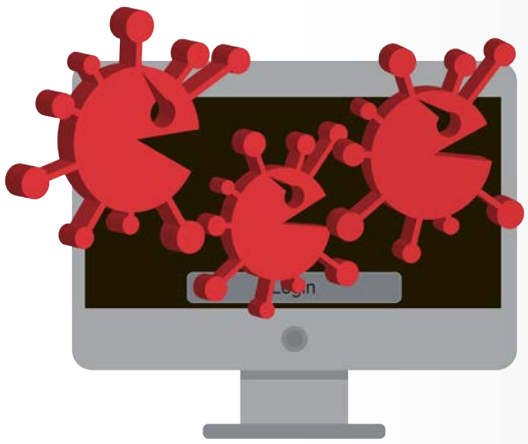
بكل بساطة، البرمجيات الخبيثة (Mal-ware) هي نتاج دمج كلمتي برمجيات Software مع كلمة خبيث Malicious، وبالتالي فهي برمجيات تهدف لإحداث ضرر بالأجهزة المصابة. مجرمو الإنترنت يحاولون تثبيت هذه البرمجيات في أجهزة الحواسيب بغرض التحكم بها أو الاطلاع على البيانات التي تحتويها هذه الاجهزة. عندما تثبّت هذه البرمجيات، يستطيع مجرمو الانترنت استخدامها للتجسس عليك وعلى استخدامك للإنترنت، سرقة كلمات المرور أو الملفات، أو حتى استخدام جهازك لاختراق الآخرين. هذه البرمجيات تستطيع كذلك منعك من الوصول لبعض ملفاتك، وطلب فدية مالية عليك أن تدفعها لشخص معين ليعيد لك صلاحية الوصول لملفاتك.

العديد من الأشخاص لديهم التصور الخاطئ عن البرمجيات الخبيثة بأنها تصيب الأجهزة التي تعمل بنظام ويندوز فقط. الأجهزة التي تعمل بنظام ويندوز تعد الهدف الأهم لأنها تستخدم بكثرة، ولكن هذه البرمجيات قد تصيب الأجهزة التي تعمل بالانظمة الأخرى كذلك، سواء كان من الحواسيب التي تعمل بنظام ماكنتوش، الهواتف الذكية و الاجهزة اللوحية التي تعمل بنظام أبل أو أندرويد. وكلما زاد عدد الأجهزة التي يتمكن مجرمو الانترنت من اختراقها كلما زاد قدر المال الذي يستطيعون جمعه. لذا فالجميع مستهدف من قبلهم، بما فيهم أنت.

ما هي البرمجيات الخبيثة

من الذي يصدر البرمجيات الخبيثة

لم يعد إصدار البرمجيات الخبيثة من قبل الهواة فقط ، فمجرمو الإنترنت يقومون بإصدار برمجيات خبيثة أكثر تطورا وخطورة. هدفهم هو كسب المال من صاحب الجهاز الذي يتم اختراقه، وربما عن طريق بيع البيانات التي يمكنهم سرقتها من الأجهزة المختلفة حول الشبكة، كما يقومون بإرسال رسائل بريد الإلكتروني مخادعة ويطلقون هجمات تعطيل الخدمة من الأجهزة المخترقة. مجرمو الانترنت قد يكونوا افرادا يعملون لانفسهم وربما يكونوا ضمن مجموعات صغيرة وربما جزء من جماعات إجرامية منظمة تنظيما جيداً وقد يكونوا يعملون لحساب مؤسسات حكومية في دولهم. البرمجيات الخبيثة أصبحت أكثر تطورا من ذي قبل وأصبح هناك من عمله الأساسي هو إصدار مثل هذه البرمجيات. بالإضافة إلى ذلك، يقوم بعض مصدري البرمجيات الخبيثة ببيعها للأفراد أو المنظمات الأخرى ويقوم بتوفير تحديثات منتظمة لاصداراته.



لحماية نفسك من البرمجيات الخبيثة عليك تثبيت أحد برامج مكافحة البرمجيات الخبيثة والتحديث المستمر لكافة التطبيقات على جميع الاجهزة التي تستخدمها والحذر من الرسائل المشبوهة.

كيف تحمي نفسك منها

أحد أهم خطوات الحماية هي تثبيت أحد برامج مكافحة البرمجيات الخبيثة من أحد المنتجين الموثوق بهم. بالرغم من أن هذه البرامج تم تصميمها لكشف ووقف البرمجيات الخبيثة إلا أنها لا يمكن أن تمنع أو تزيل جميع البرامج الخبيثة. مجرمو الإنترنت يعملون على ابتكار وتطوير البرمجيات الخبيثة بشكل مستمر ويحرصون على تصميمها بحيث لا يتم كشفها. بدورهم يقوم منتجو برامج مكافحة البرمجيات الخبيثة بتطويرها وتحديثها باستمرار لزيادة القدرة على كشف البرامج الخبيثة وازالتها. أصبح الوضع يشبه إلى حد بعيد سباق التسلح بين الجانبين. ولكن للأسف دائما ما يكون مجرمو الانترنت هم المتقدمون. وبذلك لا يمكنك الاعتماد على برامج مكافحة البرمجيات الخبيثة وحدها، فعلينا اتباع الخطوات الخطوات التالية لتعزيز الحماية:

- مجرمو الانترنت غالباً ما يحاولون استغلال نقاط الضعف في أنظمة التشغيل والتطبيقات المختلفة. لذلك، تأكد من تمكين خاصية التحديث التلقائي لأنظمة التشغيل والتطبيقات لمختلف الاجهزة التي تستخدمها.
- أحد الطرق الشائعة التي يستخدمها مجرمو الإنترنت لمهاجمة الهواتف الذكية هي عن طريق إنشاء تطبيقات خبيثة ووضعها على شبكة الإنترنت، ومن ثم خداع الناس لاقناعهم بتحميل وتثبيت هذه التطبيقات. لذلك عليك تحميل وتثبيت التطبيقات من المواقع الموثوق بها فقط. بالإضافة إلى ذلك، تثبيت التطبيقات التي تم نشرها على الانترنت لفترة طويلة، وتم تحميلها من قبل عدد كبير من المستخدمين، ولها العديد من الملاحظات الإيجابية.

ما هي البرمجيات الخبيثة

- أحرص على أن لا تستخدم جهاز الحاسب الخاص بك من خلال حساب administrator أو root ولكن انشأ حساب بصلاحيات محدودة وقم باستخدامه لعملك اليومي. هذا الاجراء سيوفر حماية إضافية من خلال منع أنواع عديدة من البرامج الضارة من أن تكون قادرة على تثبيت نفسها.
- غالبا ما يقوم مجرمو الانترنت بخداع الناس لاقناعهم بتثبيت البرمجيات الخبيثة على اجهزتهم. على سبيل المثال قد يصلك بريد الكتروني يظهر أنه من البنك الذي تتعامل معه أو من أحد أصدقائك أو زملائك في العمل وقد يحتوي على رابط يظهر أنه منطقي أو مرفق معه ملف أو أكثر، إذا قمت بالضغط على الرابط او فتح أحد الملفات المرفقة فسوف يتم تفعيل برمجية خبيثة وتثبيتها على جهازك
- إذا كانت الرسالة غير منطقية أو تطلب منك التصرف بسرعة كبيرة فالاحتمال قوي أنك تتعرض للاحتيال. كن حذراً فالحس السليم هو من أفضل طرق الدفاع .

قم بعمل نسخ احتياطي لبياناتك بشكل منتظم فهذا يتيح لك الرجوع الى بياناتك اذا تعرض جهازك للهجوم وتم تشفير بياناتك أو محوها.

إعرف أكثر

أوتش الشهرية! نشرة توعوية بالأمن المعلوماتي. للاشتراك والوصول إلى الأعداد السابقة ولمعرفة المزيد حول "سانس" نأمل زيارة

http://www.securingthehuman.org.

النسخة العربية

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

مصادر إضافية

عدد أوتش حول "التصيد" باللغة الانجليزية:	https://securingthehuman.sans.org/ouch/2015#december2015
عدد أوتش حول "الهندسة الاجتماعية":	https://securingthehuman.sans.org/newsletters/ouch/issues/OUCH-201411_aa.pdf
عدد أوتش حول "استخدام تطبيقات الجوال بشكل أمن":	https://securingthehuman.sans.org/newsletters/ouch/issues/OUCH-201501_aa.pdf
عدد أوتش حول "تأمين الجهاز اللوحي الجديد" باللغة الانجليزية:	https://securingthehuman.sans.org/ouch/2016#january2016
عدد أوتش حول " النسخ ا احتياطي واستعادة البيانات":	https://securingthehuman.sans.org/newsletters/ouch/issues/OUCH-201508_aa.pdf

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