آوتش! | أغسطس ٢٠١٦

النشرة الشهرية حول الوعي الأمني لمستخدمي الحاسب الآلي

OUCH!

في هذا العدد..

- ماهي برمجيات طلب الفدية
- هل يجب دفع الفدية؟
- النسخ الاحتياطية
- المزيد من التدابير الوقائية

برمجيات طلب الفدية

ماهي برمجيات طلب الفدية؟

برمجيات طلب الفدية (Ransomware) هي نوع خاص من البرمجيات الخبيثة (Malware) التي تنتشر بشكل كبير عبر الإنترنت هذه الأيام، وتهدد بتدمير مستندات الضحايا وملفاتهم الأخرى. البرمجيات الخبيثة هي برمجيات تستهدف مستخدمي الحاسب الآلي وتهدف للتخريب. برمجيات طلب الفدية هي أحد أنواع هذه البرمجيات الخبيثة، ولكنها كسبت شهرة كبيرة مؤخرًا لأنها مربحة بشكل كبير للمخربين. عندما يصاب جهازك بإحدى برمجيات طلب الفدية يتم تشفير القرص الصلب (hard disk) أو عدد من الملفات على جهاز الضحية. بسبب ذلك يصبح الضحية غير قادر على استخدام جهازه أو الوصول إلى ملفاته، وتُظهر رسالة «أن هذا الجهاز تم تشفيره ولن تستطيع الوصول لملفاتك، ولفك التشفير عليك دفع مبلغ ***». تحتوي الرسالة على طريقة دفع هذا المبلغ والتي تكون في الأغلب من خلال عملية إلكترونية (بت كوين أو باي بال مثلا). هذه البرمجيات بدأت تنتشر بشكل كبير، وأشهر طريقة يستخدمها المخربون هي إرسال رابط عبر البريد الإلكتروني ضمن رسالة تحاول اقناع المستخدم – بطريقة أو بأخرى – للنقر على هذا الرابط والذي يأخذ المستخدم الى موقع خبيث يقوم بتنفيذ التشفير لملفات المستخدم.

المحرر الضيف

ليني زيلتر يعمل على حماية بيانات العملاء في شركة NCR Corp ويُدرس كيفية مكافحة البرمجيات الخبيثة في معهد سانس. ليني نشط على تويتر (@lennyzeltser) ويكتب في مدونه عن أمن المعلومات على zeltser.com.

هل يجب دفع الفدية؟

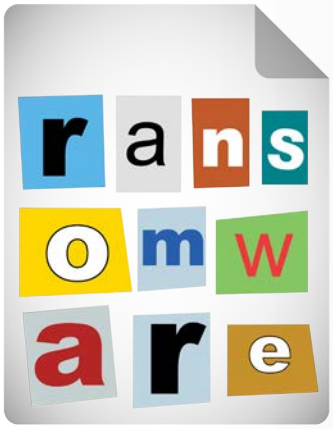
الجواب هنا صعب! المشكلة أن دفع مثل هذه المبالغ للمخترقين يزيد من رغبتهم في اختراق المزيد من الضحايا. من ناحية أخرى، قد لا يكون لديك حل آخر لاسترجاع بياناتك بدون دفع الفدية لهم. في كلا الحالين عليك أن تعلم أنك تتعامل مع مجرمين، ربما تدفع لهم الفدية ولا يعيدون لك أي ملفات، وربما يعيدونها لك باستخدام برنامج يفك التشفير ولكنه يمكنهم من اختراق جهازك مرة أخرى ، لذا فعليك أن تكون حذراً.

النسخ الاحتياطي للملفات

قد تكون أفضل طريقة للحماية من برمجيات طلب الفدية (وغيرها) هي اجراء عملية النسخ الاحتياطي لملفاتك بشكل دوري. بهذه

برمجيات طلب الفدية

الطريقة، حتى إذا حصل وتم تشفير ملفاتك، فستكون قادراً على استرجاعها من النسخة الاحتياطية دون الحاجة لدفع الفدية. طبعاً احرص على ان تكون النسخة الاحتياطية لا يمكن الوصول اليها من الجهاز المصاب. ولذلك، من المناسب جعل النسخ الاحتياطي على مواقع سحابية موثوقة. كما ننصحك بوضع النسخ الاحتياطية على محركات الأقراص الصلبة الخارجية (لا تنسى فصل القرص الخارجي بعد انتهائك من النسخ الاحتياطي). يعتقد الكثير من المستخدمين أن النسخ الاحتياطي مضمون ولا يحتاج لاختباره والتأكد أنه يعمل بشكل صحيح، وهذا خطأ شائع. لذا عليك اختبار النسخ الاحتياطية والتأكد من انك تستطيع فعلا استرداد الملفات. النسخ الاحتياطية تفيد كذلك في حال حصل خلل في القرص الصلب لجهازك أو قمت بحذف الملفات بطريق الخطأ.



برمجيات طلب الفدية هي برمجيات خبيثة تقوم بتشفير كافة الملفات الموجودة على جهاز الحاسب الآلي المصاب وتمنع صاحب الجهاز من الوصول إليها.

المزيد من التدابير الوقائية

علاوة على ذلك، يمكنك حماية نفسك من برمجيات طلب الفدية بنفس الطرق التي تحمي نفسك بها من أنواع البرمجيات الخبيثة الأخرى. إبدأ بالتأكد من أن لديك أحدث تطبيقات مكافحة البرمجيات الخبيثة من مورد موثوق به. تم تصميم هذه الأدوات، لكشف ووقف البرامج الضارة. لكن تذكر أن هذه التطبيقات رغم تطورها لا يمكنها حماية جهازك أو إزالة كافة البرامج الخبيثة. فمجرمي الإنترنت يقومون بتطوير مستمر لبرامجهم وأساليبهم لتجنب الكشف عنها. وفي المقابل، موردي تطبيقات مكافحة البرمجيات الخبيثة يعملون باستمرار على تحديث منتجاتهم لتمكينها من الكشف عن البرامج الضارة الحديثة. من نواح عديدة، أصبح كسباق «التسلح» بين الجانبين. وللأسف، مجرمي الانترنت عادة ما يكونون خطوة واحدة إلى الأمام، ولهذا السبب عليك التأكد من نسخ الملفات احتياطياً، وتنفيذ الخطوات التالية لتوفير حماية إضافية :

- غالبا ما يستطيع مجرمو الانترنت إصابة الأجهزة والحواسيب من خلال نقاط الضعف الموجودة بها. كلما كانت برمجيات هذه الأجهزة محدثة وجديدة كلما قلت المخاطر الموجودة بها، لذا ننصحك بتحديث أنظمة التشغيل وتفعيل التحديثات التلقائية للتطبيقات المختلفة بشكل دوري.
- بدلا من استخدام الجهاز بصلاحيات «Adminstrator» او « Root» أنشئ مستخدم بصلاحيات محدودة واستخدمه دائماً فهذا يؤدي الي حماية إضافية للنظام من أنواع من البرمجيات الخبيثة التي تستطيع إعادة تكرار نفسها والانتشار.

برمجيات طلب الفدية

- يقوم المهاجمون في الغالب بخداع المستخدمين عن طريق تنصيب البرمجيات الخبيثة بأنفسهم. مثلا يقوم المهاجم بإرسال بريد الكتروني قد يبدو عاديا ويحتوي على مرفقات او رابط. ربنا يبدو هذا البريد الإلكتروني قادما من احد البنوك المعروفة او من أحد أصدقائك، وعندما تقوم بفتح المرفقات او الضغط على الرابط، فانت حقيقةً تقوم بتفعيل نص برمجي خبيث يقوم بمهاجمة نظام التشغيل الخاص بك. إذا كان نص الرسالة يطلب منك التصرف بسرعة أو يحاول إرباكك أو كان النص بسيطا جدا أو يحتوي على أخطاء املائية او تعبيرية، فهناك احتمال كبير أن يكون هجوم الكتروني. كن حذراً فالحس السليم هو دفاعك الأفضل.

قم بحماية نفسك من برمجيات الفدية عن طريق بقائك حذرا حين فتح المرفقات في البريد الالكتروني او الضغط على الروابط. تأكد من تحديث برنامج مكافحة البرمجيات الخبيثة والتأكد من أخذ نسخ احتياطية من الملفات بشكل دوري لكي تستطيع استعادتها عند الحاجة.

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 التصيد (باللغة الإنجليزية):	https://securingthehuman.sans.org//ouch/2015#december2015
عدد أوتش حول ما هي البرمجيات الخبيثة:	https://securingthehuman.sans.org/newsletters/ouch/issues/OUCH-201603_aa.pdf
عدد أوتش حول التشفير:	https://securingthehuman.sans.org/newsletters/ouch/issues/OUCH-201606_aa.pdf
عدد أوتش حول النسخ الاحتياطي واستعادة البيانات:	https://securingthehuman.sans.org/newsletters/ouch/issues/OUCH-201508_aa.pdf
مقالة عن برمجيات الفدية من شركة مايكروسوفت (باللغة الإنجليزية):	https://www.microsoft.com/security/portal/mmpc/shared/ransomware.aspx
دورة من SANS عن الهندسة العكسية للبرمجيات الخبيثة (باللغة الإنجليزية):	https://sans.org/for610

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