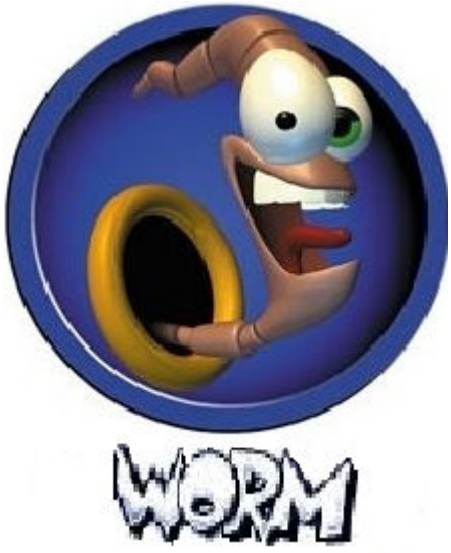
بسم الله الرحمن الرحيم

Sasser

بحث فصلي عن

فيروس دودة ســاسر



تقديم

عبدالرحمن بن علي الخلف

423121670

مـقدمة

ما يجب أن تعرفه عن فيروس دودة ساسر Sasser ؟

فيروس دودة ساسر (Sasser) كأي نوع من ديدان الكمبيوتر الأخرى يهدف للوصول إلى أجهزة الكمبيوتر التي تحمل برمجيات غير محدثة ومحمية من الفيروسات والديدان. فلقد أكد فريق مايكروسوفت Microsoft أن دودة ساسر (من النوع W32.sasser) تقوم باستغلال الثغرة الأمنية في النظام الفرعي لسلطة الأمن المحلي (LSASS).[1]

كيف تعمل دودة سـاسر Sasser؟

عندما تستغل الدودة WIN32.Sasser الثغرة الموجودة في النظام الفرعي لسلطة الأمن المحلي(LSASS) فإنها تقوم أولا بنسخ نفسها إلى مجلد النظام %WINDOWS% ، بل وفي أغلب الأحيان فإنها تعدل على ملف (registry) الموجود في النظام بإضافة هذا الأمر:
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Run[2]

متى تبدأ دودة سـاسر Sasser بالعمل؟

إن ذلك التعديل أو الأمر على ملف registry ، يجعل الدودة تبدأ بالعمل في كل مرة يتم فيها تشغيل النظام Windows. فهي – أي الدودة ساسر- تتقمص شخصية خادم FTP أو (FTP Server) في طريقته بارسال واستقبال البيانات عبر المنفذ الخاص به TCP 5554. ولأي تبادل بيانات على هذا المنفذ، تقوم الدودة ساسر بنسخ نفسها أولا ومن ثم ارسالها إلى الجهاز المتصل على ذلك المنفذ. ولكن يجب أن نعلم أن هذه الدودة لاتنتظر أن يأتي الإتصال من الأجهزة الأخرى عبر منفذ FTP، بل إنها تقوم تلقائيا بذلك كما سيأتي.[3]

---

[1] http://www.microsoft.com/security/incident/sasser.mspx
[2] http://www.microsoft.com/middleeast/arabic/Security/incident/sasser.asp
[3] http://www.microsoft.com/security/incident/sasser.mspx

التحليل الفني لطرية عمل الدودة ســاسـر

تقوم دودة ساسر بإنتاج عناوين عشوائية (Random IP addresses) ومن ثم ارسال شفرة برمجية ناقلة للعدوى (لاحتوائها على الكود الخاص بنقل الفيروس أو الدودة) إلى هذه العناوين باستخدام المنفذ TCP 445. فإن نجحت هذه الشفرة الناقلة للعدوى بالوصول إلى إلى أحد هذه العناوين فسيقوم بريمج موجود في الدودة الأم بالاستماع إلى منفذ TCP للجهاز المصاب بالعدوى (أي سيكون هناك خط اتصال مفتوح بين الجهازين الحامل للدودة الأم والجهاز الاخر المصاب بالعدوى ولكنه لايحمل الدودة). وبالتالي وبكل بساطة يقوم الجاز المستقبل وبواسطة الشفرة المرسلة إليه بتحميل Download الدودة الأم كاملة عن طريق منفذ FTP والذي تسيطر عليه الدودة الأم في الجهاز الأول.

وهكذا يتم نسخ الدودة من الجهاز أ إلى الجهاز ب. [4]

ماهي أبرز أضرار الدودة ساسر؟

إن من أبرز أضراره هو إيقافها لأي محاولة لإيقاف تشغيل الجهاز وذلك باستدعائها لهذا الأمر باستمرار AbortSystemShutdown لكي لايتم إيقاف التشغيل الفجائي أبداً. وبهذه الطريقة تستطيع استكمال النسخ ونقل العدوى بحرية أكثر. والمزعج أكثر في هذا الموضوع أن الدودة ساسر تصدر الأوامر للنظام بإيقاف التشغيل عدة مرات مما يشل حركة الجهاز (نلاحظ هنا أن عملية التشغيل وإيقاف التشغيل للجهاز خرجت عن السيطرة)

البرامج التي تتأثر بالفيروس:

- (Windows XP, Windows XP Service Pack 1 (SP1
- Windows 2000 SP2, Windows 2000 SP3, Windows 2000 SP4

البرامج التي لا تتأثر بالفيروس:

- Windows XP 64-Bit Edition Version 2003
- Windows Server™ 2003
- Windows XP 64-Bit Edition SP1
- Windows Millennium Edition
- Windows 98 Second Edition
- Windows 98
- Windows NT® 4.0 SP6a [5]

---

[4] http://www.microsoft.com/middleeast/arabic/Security/incident/sasser.asp
[5] http://vil.nai.com/vil/content/v_125008.htm

كيف أعلم إن كان جهازي مصابا بالدودة ســاسر أم لا؟[6]

إذا ظهرت لديك إحدى هاتين الرسالتين مرة أو أكثر خلال استخدامك لنظام التشغيل Windows:

[6]

[7]

[6]http://securityresponse.symantec.com/avcenter/venc/data/w32.sasser.removal.tool.htm
[7] http://www.lurhq.com/sasser.html

الخطوات اللازمة لمكافحة فيروس دودة ساسر

الخطوة الأولى: تمكين جدار حماية

قبل القيام بالخطوات التالية، تأكد من تنشيط جدار حماية لديك لحماية جهاز الكمبيوتر الخاص بك من انتقال الفيروس. إذا كان لديك جدار حماية على الأجهزة مستقل للاتصال في المنزل أو في مكان العمل، أو إذا كان لديك جدار حماية ضمن برنامج Microsoft® Windows® XP، فإنه من المحتمل جداً أن لا يتم إصابة الأجهزة لديك بفيروس دودة ساسر. وفي حالة إصابة أي من أجهزة الكمبيوتر لديك، فإن تمكين برنامج جدار الحماية سيساعدك على الحد من تأثير فيروس دودة ساسر على بقية الأجهزة.

الخطوة الثانية: تثبيت التحديث المطلوب

للمساعدة على حماية جهاز الكمبيوتر لديك من فيروس دودة ساسر وأشكاله المختلفة، يجب عليك أولاً تحميل تحديث الأمان 835732 وتثبيته، والذي تم إصداره مع نشرات أمان .Microsoft MS04-011 يمكنك الحصول على تحديث 835732 على موقع تحديث Windows على ويب الموجود على قائمة التحديثات الهامة و قسم حزم الخدمات. يمكنك أيضاً تحميل هذا التحميل وتثبيته يدوياً من مركز تحميلاتMicrosoft.com Download Center. Microsoft

الخطوة الثالثة : البحث التلقائي عن فيروس Sasser وإزالته

يمكنك استخدام هذه الأداة لتفحص جهاز الكمبيوتر الخاص بك بحثاً عن فيروس Sasser ومحاولة إزالته. للقيام بذلك، اضغط على**" تفحص جهاز الكمبيوتر بحثاً عن عن الفيروس. "**

هام لاستخدام هذه الأداة، لابد من تشغيل برنامج Windows XP ، أو Windows 2000 ، ويجب لأن يكون تم تثبيت التحديث الصادر من نشرة Microsoft للأمان.MS04-011

الخطوة الرابعة : مراجعة الموارد الفنية الإضافية

إذا كانت أداة تفحص الفيروسات والتخلص منها لا تعمل لديك، يمكن محاولة استخدام أحد الأدوات المجانية لإزالة فيروس الدودة والمتوفرة في مواقع بائعي برامج مكافحة للفيروسات على ويب التالية:

- Computer Associates
- F-secure
- Network Associates
- Norman
- Panda
- Sophos
- Symantec
- Trend Micro

الخطوة الخامسة : تعلم كيف يمكن حماية جهاز الكمبيوتر الخاص بك[7]

---

[8] http://www.sasserlawfirm.com/Articles_8.shtml

خاتمة

إن ظهور مشاكل الفيروسات انتشار انتشار مروعا مع توفر خدمات الإنترنت والبريد الإلكتروني وذلك لسولة نقل البيانات فيها وتيسير ذلك، فقلما كنا سابقا نشكوا من وجود فيروس أو ديدان في الأجهزة. حيث أن الناقل الوحيد لها هو الدسك Floppy Disks. بل إن أصحاب النوايا غير الحسنة فقط هم الذين يمكنهم نقل فيروس من جهاز إلى اخر عن طريق هذا الدسك. أما اليوم فلن يخلو موقع التحديثات لMicrosoft أسبوعيا من تحذير بوجود ديدان أو فيروسات تنتقل تلقائيا من جهاز إلى اخر ومن شبكة إلى أخرى وبكل بساطة وحرية.

وحيث أن لكل شيء جيد ضريبه، فلنقل أن هذه هي ضريبة الإنترنت التي يسرت على الكثير من المستخدمين من الحصول على المعلومات وتبادلها. ولكن ومع مبدأ المكافحه فإن تحديث البرمجيات واستخدام الجدار الناري وكذلك برامج مكافحة الفيروسات الشهيرة يمكن من القضاء على هذه المشكلة أو تقليل تأثيرها إلى حد كبير.