محمد عبدالرحمن الخمشي

423102916

CEN 448

1st Paper

Sasser, What, how, when, how to avoid it and what its harm?

Dr. Khaled Al-Ghathber

TA. Mohammed Al-Husain

المحتويات/

 # متى ظهر ساسر ؟

1- مايو – 2004 يوما لن ينساه كل مهتم بالعالم الرقمي. في هذا اليوم كارثة رقمية جديدة تتسبب في كثير من الأضرار لأجهزة الكمبيوتر بأشكالها وتعدد أنواعها . "ساسر" اسم فيروس جديد ظهر في هذا اليوم في تمام الساعة 06:48:08 بتوقيت جرينتش حسب إحصائية شركة sophos . وانتشر منذ ذلك التاريخ بسرعة كبيرة في أنحاء شبكة الانترنت.

 # طبيعة الفيروس

وساسر فيروس كمبيوتر من النوع المعروف "بالدودة" لأنه يبحث عن الأجهزة السليمة ليصيبها بنفسه ودون مساعدة من أي مستخدم، واكتشفت أربع صور مختلفة من فيروس ساسر حتى الآن، وأحدث هذه النسخ المعروفة باسم "ساسر دي" يبحث في شبكة الإنترنت بكل جدية عن أجهزة جديدة ليصيبها وهو ما يحدث تكدسا في المعلومات داخل الشبكات مما يتسبب في إبطاء عملها. و يستمر فيروس ساسر في إشاعة الأعطال بعدد كبير من أجهزة الكمبيوتر التي تعمل بنظام تشغيل ويندوز .وخلافا لغيره من فيروسات الكمبيوتر، لا ينتقل ساسر من جهاز لآخر بالبريد الإلكتروني لكنه يجد طريقه إلى الأجهزة السليمة بنفسه .
وحسب ما أوردته شركة مايكروسوفت فإن البرامج التي تتأثر بالفيروس هي كالتالي:

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

أما البرامج التي لا تتأثر بالفيروس فهي:

- 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

أكد فريق Microsoft أن فيروس دودة ساسر (من النوع W32.Sasser.A وأشكاله المختلفة) ينتشر حالياً من خلال الإنترنت. وقد أكدت شركة Microsoft أن الفيروس يقوم باستغلال مشكلة في النظام الفرعي لسلطة الأمان المحلي (LSASS) التي تم معالجتها من خلال التحديث الصادر في 13 أبريل 2004.

شركة Symantec الشركة الرائدة في مجال أمن المعلومات أصدرت نشرة الكترونية عبر موقعها على الشبكة العنكبوتية بينت من خلاله كيفية عمل ساسر:

1- محاولة إنشاء ثغرة تسمى بـ **Jobaka3l** أو إيجاد مخارج أذا فشلت مهمة البحث عن الثغرة المطلوبة. وذلك للتأكد من انه لاتوجد أي دودة تعمل مع ساسر في الجهاز المطلوب في نفس الوقت.

2- يقوم ساسر بنسخ نفسه كملف من نوع : **%Windir%\avserve.exe**

3- يضيف القيمة **"avserve.exe"="%Windir%\avserve.exe"** وباستخدام أمر معين يتم تمكين الدودة وبداية عملها عند بداية تشغيل ويندوز.

4- يقوم ساسر باستعمال خاصية **AbortSystemShutdown API** لأعاقه أي محاولة لإغلاق الكمبيوتر أو إعادة تشغيله.

5- يستخدم ساسر FTP SERVER على TCP PORT 5554 وذلك لنشر الدودة على أجهزة أخرى. 6- يسترجع ساسر عناوين الـ IP للجهاز المصاب باستخدام **Windows API, gethostbyname.** مع ملاحظة انه يتجاهل مجموعة معينة من الـ IPs.

7- ينشئ ساسر IP جديد بناءً على عناوين الـ IPs السابقة للجهاز.

8- يتصل ساسر بعنوان الجهاز المصاب على TCP port 445 لرؤية ماإذا كان كمبيوتر آخر متصل به.

9- إذا كان هناك أي اتصال مع أي كمبيوتر آخر فانه يرسل كود معين للجهاز المتصل به وهذا ماقد يسبب فتح منفذ TCP port 9996 . 10- ينشئ **ftp script file cmd.ftp** في الجهاز الذي تمت مهاجمته.

11- يقوم بعدها بقطع الاتصال مع FTP server في الجهاز المصاب الأول ويأخذ نسخه من الفيروس على TCP port 4445 هذه النسخة ستحمل اسم من أربعة أو خمسة أرقام متبوعة بـ **up.exe_**

12- بعدها عملية Lsass.exe سوف تتحطم بعد تستغل الدودة الضعف فيها وسيظهر النظام إنذارا انه يجب إغلاق ويندوز خلال دقيقة.

13- سيحذف ملف **cmd.ftp** من الجهاز الذي تمت مهاجمته، وإذا كانت عملية استغلال الكود توقفت فان ملف **cmd.ftp** سيبقى في الجهاز الذي تم الهجوم عليه.

14- سينشئ بعدها ملف في قرص C:\win.log سيحوي هذا الملف عنوان الـ IP للجهاز الذي ستحاول الدودة مهاجمته.

 # تأثر المستخدمين بفيروس ساسر

سأتناول من خلال هذا الجزء مدى التأثير والضرر الذي ألحقه ساسر بمستخدمي الكمبيوتر سواء من المستخدمين العاديين أو من كبيرات القطاعات والشركات في العالم

- **المستخدمون العاديون:**

كما سبق وأن ذكرنا أن ساسر أشاع الأعطال بعدد كبير من أجهزة الكمبيوتر في العالم التي تعمل تحت نظام ويندوز. ويقد بعض الخبراء أن عدد الأجهزة المصابة بساسر يزيد عن المليون جهاز ففيروس ساسر يقتصر ضرره على المستخدمين العاديين بأنه يقوم بإغلاق النظام. وقالت شركة مايكروسوفت إن نحو 1,5 مليون مستخدم زاروا الموقع الذي خصصته الشركة للتخلص من الفيروس خلال 48 ساعة هي الأولى من انتشار الفيروس.

- **القطاعات الخدمية والشركات التجارية:**

قالت شركة إف سيكيور إن عددا من الشركات الكبيرة قامت بالفعل بتحميل التحديثات الأمنية المعالجة للثغرة التي يستغلها ساسر وهو ما قد يحد من انتشار الفيروس. أما الشركات التي لم تحمل التحديثات فقد تضررت بشدة. وأصيب المركز الرئيسي و19 مكتبا إقليميا لوكالة خفر السواحل البريطانية بالفيروس. وقالت الوكالة إن الأعطال لن تعيق أعمال البحث والإنقاذ. وقال مكتب البريد الوطني في تايوان إن 1600 من أجهزته أصيبت بالفيروس وهو ما اضطر أكثر من 400 من أصل 1200 فرع له على استخدام المكاتبات اليدوية. وأفادت تقارير تلفزيونية بأن

هذه الأعطال أدت إلى اصطفاف العملاء في طوابير طويلة عند كثير من مكاتب الشركة. كما أصاب الفيروس وزارتين وعددا من المستشفيات في هونج كونج. وفي استراليا توقفت حركة القطارات في بعض المناطق لما بدا من تعطيل الفيروس لنظم التحكم اللاسلكي مما حال دون اتصال سائقي القطارات بعمال الإشارة. واضطر موظفو بنك ويست باك استراليا إلى استخدام التسجيل اليدوي للمعاملات بعد أن أصاب الفيروس أجهزتهم بالشلل. وسجلت حالات إصابة أخرى في بنكين آخرين. وقال بنك فنلندا إنه أغلق كافة فروعه البالغ عددها 130 بشكل مؤقت كإجراء احترازي ضد ساسر. ورفضت خطوط دلتا الجوية الأمريكية التعليق على تقارير تفيد بأن الفيروس تسبب في توقف لبعض رحلاتها.

 # العلاج لدى مايكروسوفت

وهونت مايكروسوفت من شأن التقارير التي تقول إن ساسر أصاب الملايين من أجهزة الكمبيوتر. وقال الشركة إن عدد المستخدمين الذين يقومون بتحميل التحديثات الأمنية من موقعها ازداد بمقدار أربعة أمثال مقارنة مع خريف 2003. وصدر أول تحديث أمني للحماية من ساسر في 13 من ابريل/نيسان ثم جرى تحديثه في 28 من الشهر نفسه. وربما ساعد تزامن ظهور الفيروس مع العطلات الأسبوعية في بريطانيا وأجزاء من أوروبا واليابان في تقليل انتشار الفيروس. ويقول بعض خبراء أمن الحاسبات إن استخدام برامج التخلص من ساسر قد لا تنهي المشكلة لأن كثيرا من الأجهزة التي أصابها قد أصيبت أيضا بفيروسات أخرى.
وقدمت مايكروسوفت نشرة الكترونية من خلال موقعها على الانترنت أورت خلالها خمس خطوات للتخلص من فيروس ساسر بأشكاله المختلفة والخطوات كالتالي:
الخطوة الأولى: تمكين جدار الحماية : قبل القيام بالخطوات اللاحقة يجب التأكد من تنشيط جدار الحماية لدى المستخدم لحماية جهاز الكمبيوتر من انتقال الفيروس.
الخطوة الثانية: تثبيت التحديث المطلوب: للمساعدة على حماية جهاز الكمبيوتر يجب تحميل تحديث الأمان 835732 وتثبيته والذي تم إصداره مع نشرات أمان MS04-011 Microsoft. .
الخطوة الثالثة: البحث التلقائي عن فيروس Sasser.A وفيروس Sasser.B وإزالته: يمكن استخدام هذه الأداة لتفحص جهاز الكمبيوتر الخاص للبحث عن فيروس Sasser.A وفيروس Sasser.B ولاستخدام هذه الأداة لابد من تشغيل برنامج Windows XP أو Windows 2000.
الخطوة الرابعة: مراجعة الموارد الفنية الإضافية: إذا كانت أداة تفحص الفيروسات والتخلص منها لا تعمل ، 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 كيفية يمكن حماية جهاز الكمبيوتر.

 # الحماية من فيروس ساسر:

معروف عن ساسر كغيره من الفيروسات يمكن اصطياده ومعرفة هجومه باستخدام برامج الانتي فيروس المختلفة وكذلك الحماية من هجومه وتفاديه عن طريق استخدام جدار ناري مناسب في هذا الجزء لن أتحدث عن هذه النقاط لأنها شبه مكررة ومعروفة للجميع.

ماسأتحدث عنه هنا هو كيف نحمي جهاز الكمبيوتر وذلك بمنع عملية إيقاف النظام التي يتسبب بها ساسر وهذه الطريقة أوردتها شركة Symantec وهي كالتالي:

1- إيقاف الاتصال بأي شبكة وخصوصا الانترنت.
2- إعادة تشغيل الكمبيوتر.
3- مع بدء التشغيل نستخدم الخطوات التالية : ابدأ >> تشغيل >> ونكتب الرمز cmd >> نكتب الرمز Shutdown-i .
4- في الشكل الذي سيظهر نختار إضافة >> نكتب اسم الكمبيوتر >> ok >> في الشكل الظاهر الجديد نكتب 9999 >> ثم نكتب النص التالي : Delay Lsass.exe shutdown >> ok
5- نعاود الاتصال بأي شبكة مثل الانترنت.
8- نتصل بالانترنت ونحصل على الـ patch لتغطية الثغرة التي يتوقع دخول الفيروس عن طريقها.

 # تحليل شركة F- Secure لحادثة ساسر !

هذا التحليل نشر بعد انتشار فيروس ساسر بأيام لذا سأذكره كما قرأته:
"وقد نشرت شركة "إف سيكيور" الفنلندية لمكافحة الفيروسات تحليلا لفيروسات "ساسر ونبيتسكاي في" وقالت إن الفيروسين متطابقين. وقد لا يساعد هذا التحليل في العثور على مبتكر فيروس ساسر حيث لا يزال مبتكر فيروس نيتسكاي طليقا. وقد ظهر فيروس ساسر للمرة الأولى في 1 مايو أيار وانتشر بسرعة كبيرة فأصاب عددا كبيرا من الحاسبات. وقال سيمون بيري رئيس قسم استراتيجية أمن الكمبيوتر إن معظم الشركات الكبيرة تجنبت مخاطر فيروس ساسر وتحركت نحو الحد من أضراره في الأجهزة التي أصابها. وأضاف: "أخبرتنا معظم الشركات الكبرى أنها تسيطر على الفيروس." كما أصاب الفيروس العديد من الحاسبات في بنك جودلمان ساشي والمفوضية الأوروبية والخطوط الجوية البريطانية و19 مكتبا إقليميا للبحرية البريطانية. وأغلقت أكثر من 50 مستشفى في نيو أورليانز لساعات عديدة كما أصاب الفيروس أيضا مكاتب الخدمات الصحية في ولاية واشنطن. كما أصاب الفيروس نصف الحاسبات التابعة للخطوط الجوية البريطانية مما أدى إلى تأخير المسافرين صباح يوم الثلاثاء. غير أن التقارير الخاصة بإصابة الحاسبات بفيروس ساسر قد انخفضت كثيرا يوم الأربعاء وهو ما يدل على أن أسوأ مراحل انتشار الفيروس قد انتهت. وقد حذرت العديد من شركات مكافحة الفيروسات من عودة الفيروس مرة أخرى."

 # ختاما ، من هو مطور فيروس ساسر ؟ وكيف كانت النهاية؟

في البداية أعلنت شركة مايكروسوفت انها ستدفع 250 الف دولار لشخصين أسهما فى الكشف عن مخترع فيروس ساسر التى انتشرت عبر الانترنت لتصيب أجهزة كمبيوتر فى مختلف أنحاء العالم.
وذكرت رويترز ان الشخصين اللذين لم يتم الكشف عن هويتهما سيتقاسمان المكافأة التى أعلنت عنها مايكروسوفت والانتربول ومكتب التحقيقات الاتحادى والمخابرات الامريكية.
والقى القبض على سفين ياشان البالغ من العمر19 عاما خلال أسبوع من ظهور فيروس دودة ساسر لاول مرة على الانترنت فى ايار عام 2004 واصابت أكثر من مليون جهاز كمبيوتر يعمل بنظام ويندوز الذى تنتجه مايكروسوفت.
وأصدرت محكمة المانية فى وقت سابق أمس حكما بالسجن 21 شهرا مع إيقاف التنفيذ بحق ياشان بعد اعترافه بابتكار الفيروس.
وتسعى مايكروسوفت التى يوجد مقرها فى ريدموند بولاية واشنطن لجعل برامجها أكثر أمنا وكفاءة وتعهدت بتعقب القراصنة وموءلفى فيروسات الكمبيوتر والبرامج التخريبية الاخرى وملاحقتهم فى المحاكم والاعلان عن مكافات للمساعدة فى الكشف عنهم.

المراجع/

*) موقع بي بي سي العربية
http://news.bbc.co.uk/hi/arabic/sci_tech/newsid_3682000/3682931.stm

*) الموقع الرسمي لشركة مايكروسوفت العربية
http://www.microsoft.com/middleeast/arabic/Security/incident/sasser.asp

*) شبكة ياستر
http://www.yasater.com/news.php?newsid=363&PHPSESSID=8af6f86be195bbb57dcd51af1d0d8071

*) جريدة الوطن السعودية

*) موقع شركة Symantec
http://www.symantec.com/avcenter/venc/data/w32.sasser.worm.html

*) موقع شركة Shopos
http://www.sophos.com/virusinfo/analyses/w32sassera.html

*) موقع شركة F-Secure
http://www.f-secure.com/v-descs/sasser.shtml

*) نشرة مايكروسوفت لامن المعلومات Microsoft Security NewsLetter
http://www.microsoft.com/technet/security/secnews/default.mspx

*) http://vil.nai.com/vil/content/v_125007.htm