﴿بِسۡمِ ٱللَّهِ ٱلرَّحۡمَٰنِ ٱلرَّحِيمِ﴾

نبدأ بسم الله:

قبل الخوض في هذا الموضوع أردت أن أعرف لكم هذا الفايروس و مدى تأثيره على نظام التشغيل (Windows)، وعادة مثل أي فايروس يدخل مجلدات نظام التشغيل الاساسية مثل (System32) و مجلد (Windows) ، و تأتي بهذه المسميات او الملفات :

SYSLIB32.DLL
OLEMDB32.DLL
WMIMGR32.DLL
VCMGRD32.DLL
VCMGCD32.DLL
WDMFMC32.DLL

وغيرها من الأسماء .

الكثير من مستخدمي الحاسوب تأثروا بهذا الفايروس حيث أنه مزعج جداً كلما ضرب الويندوز يلجئون الى عمل الفورمات ، وهذا يتطلب الكثير من الوقت و بعد الفورمات يمكن أن يضربه مرة ثانية و ثالثة حتى تتعب من كثرة الفورمات و بعدها يجب عليك تعريف الاجزاء (كارت الشاشة و الصوت و الخ.....) و بعدها تنصيب البرامج الاساسية و البرامج التي تستخدمه في عملك . واذا كان لديك ويندوز أصلي اشتريته بمبلغ كثير يجب عليك بعد الفورمات إعادة تفعيل النظام و من ثم إعادة تحديثه ، على أية حال فهذا يزعجك كثيرا ، و أحببت أن أنصحكم فليكون الفورمات اخر خطوة لكم ، ولكن من خلال بحثي لإزالة هذا الفايروس كن معي سأشرح لك بحول الله و قوته، عدة خطوات للتخلص من هذا الفايروس المزعج و التخلص من الفورمات .

ملحوظة/ بعض المرات يُمسح الملفات النظامية في الويندوز هذا يتطلب الفورمات في كثير من الأحيان. أنا أقول لكم لا تفرمتوا حواسيبكم إذا ضربه هذا الفايروس.

*ما هو فايروس (Sality):

فايروس سريع الانتشار في نظام التشغيل و ذلك من خلال الفلاش ميموري و قرص الصلب الخارجي (USB) أو أي جهاز له ذاكرة.

كيف تعرف أن نظامك مضروب من قبل هذا الفايروس:

إذا حدث هذه الأشياء في نظامك فاعلم بأنه مضروب بالفايروس

١- **الكومبيوتر يصبح غير فعال ، أي عندما تضغط على (Ctrl+Alt+Delete) (Task manager) يظهر لك رسالة بأن (Task manager) غير فعال.**

٢- **الريجستر (Registry Editer) لا يعمل ، أي عندما تكتب في الـ (Run) عبارة (Regedit) فأنه لا يعمل.**

٣- **الملفات المخفية لا يمكن إظهاره ، أي عندما تضغط على (Show hidden files and Folders) و تضغط (Ok) فأنه لا يظهر الملفات المخفية و لو حاولت مليون مرة.**

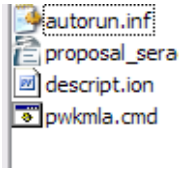
٤- **الجدار الناري المعروف بـ (firewall) و برامج ضد الفايروس (Anti Virus) الذي عندك لا يعمل ، اذا كان لديك (Anti Virus) فعال فأنه يحوله الى غير فعال و إذا كان فعالاً لا يقبل التحديث**

(Update) ، و إذا فحصت الحاسوب من الفايروس يمكن أن يمسك الفايروس و لكن لا يقتله أو لا يمسحه.

٥- كل الملفات التنفيذية التي لها امتداد (exe)في حاسوبك يصبح فايروس أو يحل الفايروس محله و عندما تريد تنصيب ذلك البرنامج فإن البرنامج لا يستجيب و لا يمكنك تنصيبه و تظهر لك رسالة خطأ (error massage).

٦- أيضا الملفات التي لها امتداد com. و scr و بعض الـ dll تصبح فايروس .

٧- عندما تستخدم فلاش ميموري فإنه يزيد ملف داخل الفلاش اسمه autorun.inf اذا ظهر هذا الملف في فلاشك فاعلم أنه فايروس و ايضا يزيد ملفات اخرى اليه بهذه الاسماء:



٨- لا يمكنك دخول (Safe mode) و إذا حاولت الدخول فإن الويندوز يعيد التشغيل (Restart) ولو حاولت مليون مرة.

* البرامج التي تحتاجه لإزالة الفايروس :

هذه مجموعة من البرامج التي تحتاجه لإزالة الفايروس و إذا لم يكن لديك هذه البرامج ، فإليك الروابط التالية:

١- برنامج (Norman Malware Cleaner : و الرابط)

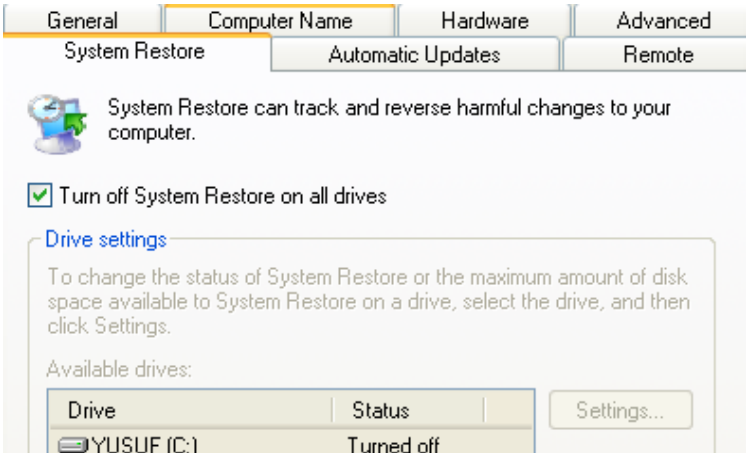
http://normanasa.vo.llnwd.net/o29/public/Norman_Malware_Cleaner.exe

٢- برنامج (Symantec Win32.Sality.AE Removal Tool) و الرابط :

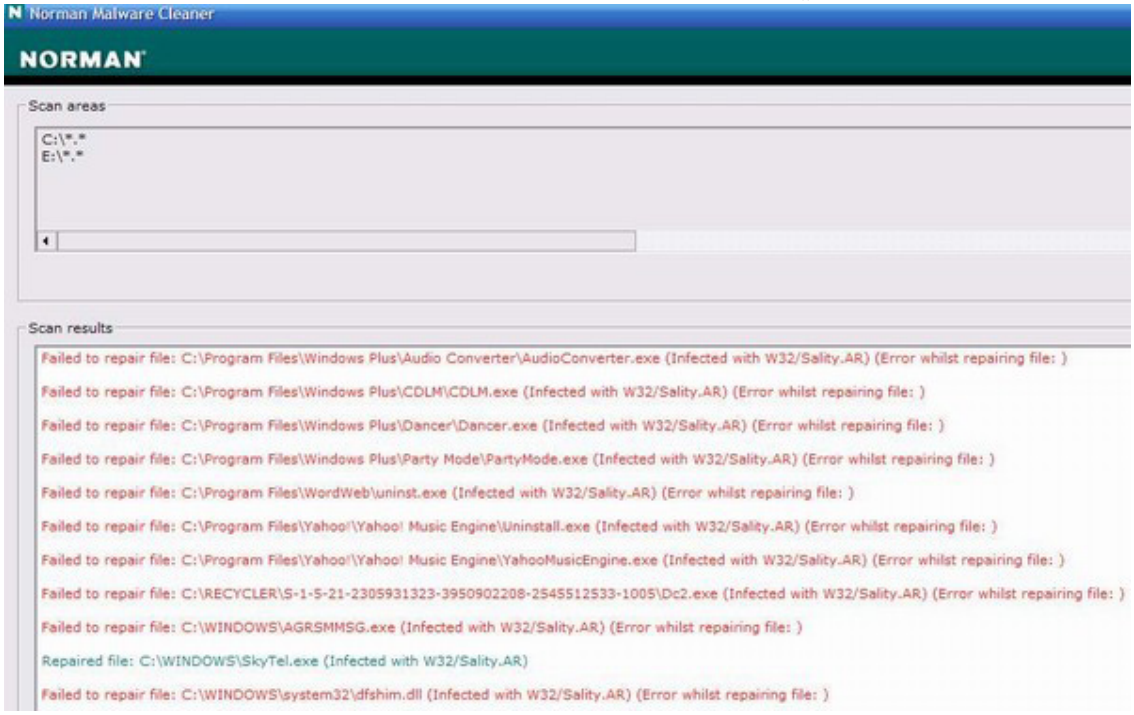
http://www.ziddu.com/download/3653712/FxSltyAE.rar.html

و الآن نشرح كيفية إزالة الفايروس :

١- قبل أي شيء يجب عليك إطفاء خاصية إعادة الويندوز أي (System restore) و ذلك عن طريق النقر على الزر الأيمن للماوس على (My computer) و بعدها تبويب (System restore) و تفعيل الزر المبين في الشكل:



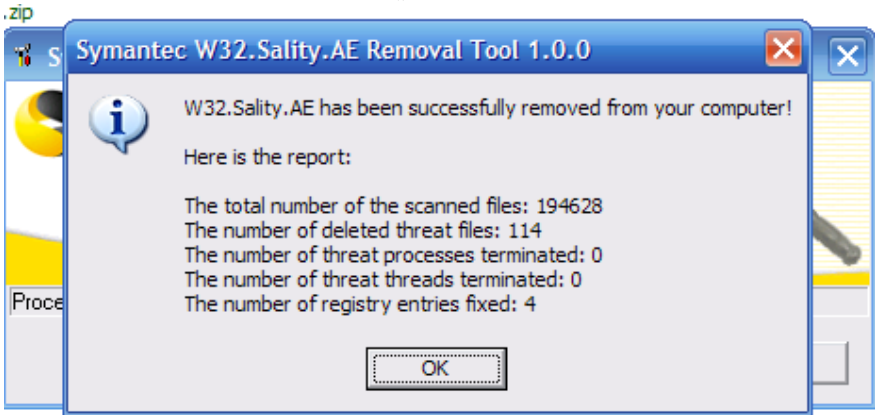
٢- و بعد ذلك نفتح برنامج (Norman Malware Cleaner) و نبدأ بعملية (Scan) حيث البرنامج بنفسه يقوم بمسح كل الفايروسات التي تجدها كما في الشكل:



وبعدها يطلب منك إعادة تشغيل الويندوز ، و أنت إفعل ذلك.

ملا حظة/ قبل إعادة تشغيل النظام يجب عليك التأكد من أن (System restore) غير فعال أي هذه الخاصية منطفئة .

٣- بعد إعادة التشغيل إفتح برنامج (Symantec Win32.Sality.AE Removal Tool) و ابدأ بعملية الـ (Scan) حيث يقوم بإزالة الفايروس كما في البرنامج السابق. ممكن أحد يسأل لماذا نقوم بإزالة الفايروس ببرنامجين و نحن نجيب على هذا السؤال بإختصار ، بعض الفايروسات يقوم البرنامج الأول بإزالته و لا يمكنه إزالة أنواع أخرى من الفايروسات و البرنامج الثاني يقوم بإزالة البعض و ترك البعض يعني البرنامجين مكملين للآخر.



و أيضا يطلب إعادة التشغيل فأعد تشغيل النظام.

٤- قم بإعادة تفعيل خاصية (Task manager) و (Registry Editor) و (Folder Option) بواسطة جروب بوليس (Group police) و ذلك عن طريق كتابة الأمر (gpedit.msc) ، و إذا لم تقدر على ذلك استخدم برنامج (PRT) المعروف لإعادة الخواص الغير فعالة.

٥- قم بتنصيب برنامج انتي فايروس قوي بحسب رغبتك (Kaspersky أو Norton أو Avast) و قم بتفعيله و تحديثه و افحص الكومبيوتر (Scan Virus) و اقض على كل الفايروسات الموجودة.

بعض الملاحضات المهمة حول هذا الموضوع:

١- كل الملفات أو بعض الملفات التي لها امتداد (exe) الموجودة داخل حاسوبك يحذف بسبب الفايروس.

٢- بعض المرات تحتاج الى (Safe mode) لتصليح الويندوز ، نحن قلنا في أول الموضوع ان الفايروس سيسبب الى تعطيل هذه الخاصية و لتصليح هذه الخاصية اليك هذا البرنامج :

الرابط : http://support.kaspersky.com/downloads/utils/sality_regkeys.zip

كاتب الموضوع : عباس محمد الكوردي