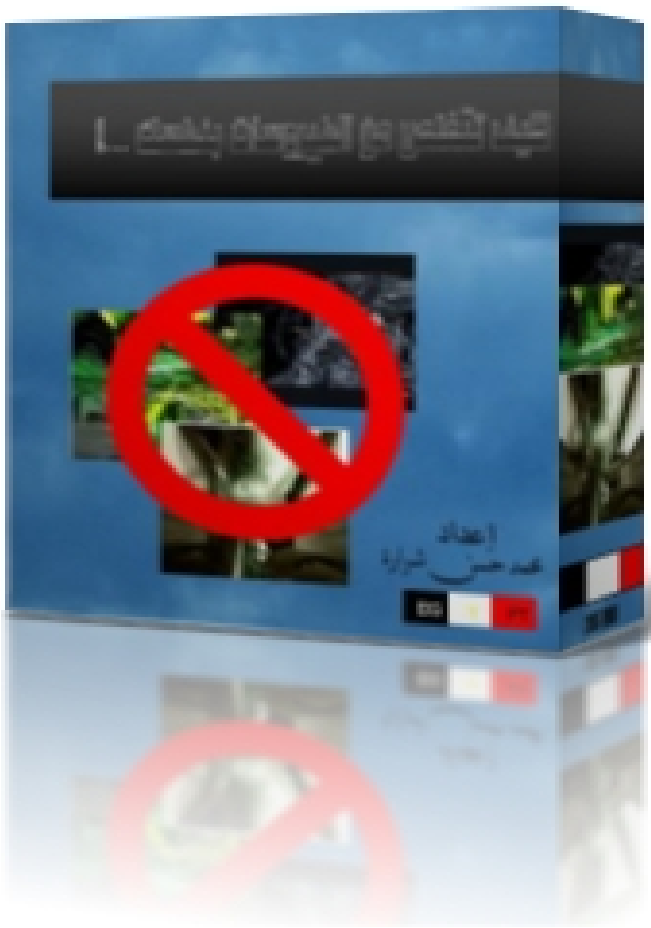
بسم الله الرحمن الرحيم

اقم لكم اليوم كتابى الاول وهو بعنوان " كيف تحمى نفسك من الفيروسات " واترككم مع الكتاب .

واسال الله ان يعود عليكم بالفائدة .....



اعداد /

م . محمد حسن عبد المعطى شرارة

الكتاب

مقدمة

قمت بتاليف هذا الكتاب ارضاء لله ورسوله و يعتبر الكتاب نتيجة لرحلة طويلة ومتعبة مع الفيروسات حيث تعرض جهازى لكثير من هجمات الفيروسات الخطيرة والتى كانت تضعنى فى حرب معها للتخلص منها فكنت ابحث كثيرا على الحل والجا اكثر الى البرامج المضادة للفيروسات والتى كانت تعتبر كمسكن او مخدر ليس الا للفيروس وفى نهاية الامر بعد ان خسرت الكثير من البيانات DATA التى كنت احتفظ بها على جهازى نتيجة لهجمات الفيروسات المتوالية لذا فهناك حل قد يلجا بعضكم اليه الا وهو عمل فورمات للهارد حتى اتخلص من كل البيانات هذا فى سبيل التخلص من الفيروس فى حين اننى لم اقم بعمل BACK UP نسخة للبيانات وانا اعلم انه من الصعب الحصول على جميع البيانات التى كانت لدى وكنت ارى فى هذا الامر او هذا الحل انه ليس بحل بل انه مشكلة ادت الى مشكلة اكبر وهى استعادة البيانات لذا فانى ارى انه لا يوجد افضل من ان تتخلص من الفيروس بنفسك بدون برامج لا تفيد لذا حتى لا اطول عليكم هيا بنا لنجوب فى صفحات هذا الكتاب .....

المؤلف

محمد حسن عبد المعطى شرارة




سنقوم بعرض اشهر الفيروسات التى نتعرض لها وطريقة علاجها واشهر اسماءها التى نعرفها ومن هذه الفيروسات :-

فيروس WORM_CHIR.A

النوع : ينتمى هذا الفيروس إلى قائمة ديدان البريد الإلكتروني.

أسماء الشهرة الأخرى :

W32/Chir@MM

I-Worm.Runouce

Win32/Chir.A@mm

درجة الخطورة : متوسطة

الوصف : ينتقل هذا الفيروس عبر رسائل البريد الإلكتروني ومن خلال الملفات المرفقة Attachments على الهيئة :-

From: iloveyou @ btamail.net.cn

Message Body:< >

Subject: Hi, i am

Attachment: P.exe

طريقة العلاج :

١- افتح قائمة Start واختر الأمر Run ثم اكتب Regedit وانقر Ok.

٢- ستظهر النافذة كما بالشكل رقم (١) من القائمة اليسرى افتح المجلدات الآتية:

HKEY_LOCAL_MACHINE <Software <Microsoft <Windows <CurrentVersion <Run

٣- إذا وجدت في القائمة اليمنى ملف التسجيل Runouce حدده ثم قم بإلغائه.

٤- أعد تشغيل الجهاز.

٥- امسح الجهاز باستخدام برنامج مسح وإزالة الفيروسات واحذف جميع ملفات WORM_CHIR.A




فيروس PE_PERRUN.A

النوع : ينتمى هذا الفيروس إلى قائمة فيروسات الملفات.

أسماء الشهرة الأخرى :

W32.Perrun

W32/Perrun

درجة الخطورة : متوسطة

الوصف : ينتقل هذا الفيروس عبر ملفات الصور ذات الإمتداد JPEG وتعتبر درجة خطورته فى أغلب الأحيان بسيطة وتنحصر على ملفات الصور فقط.

طريقة العلاج :

١- افتح قائمة Start واختر الأمر Run ثم اكتب Regedit وانقر Ok.
٢- ستظهر النافذة من القائمة اليسرى افتح المجلدات الآتية:

command<open<shell <jpegfile<HKEY_CLASSES_ROOT

٣- من القائمة اليمنى حدد الملف Default ثم انقر عليه نقرا مزدوجا حتى يظهر مسار الملف.

٤- تستطيع من هذا المسار أن تحدد ما إذا كانت ملفات الصور تحت الإمتداد JPEG متأثرة بوجود فيروس أم لا، إذا كان متأثرا فانقر بزر الماوس الأيمن على الملف ثم اختر Modify.

٥- من مربع الحوار الذى سيظهر أدخل القيمة الآتية إذا كانت غير موجودة

System%\SHIMGVW.DLL,ImageView_Fullscreen% rundll32.exe

٦- امسح الجهاز باستخدام برنامج مسح وإزالة الفيروسات واحذف جميع ملفات PE_PERRUN.A

فيروس WORM_KELINO.A

النوع : ينتمى هذا الفيروس إلى قائمة ديدان البريد الإلكتروني.




أسماء الشهرة الأخرى :

KELINO.A ،I-Worm.Kelino

درجة الخطورة : خطيرة

الوصف : يصل هذا الفيروس إلي هدفه بواسطة ١٨ رسالة مختلفة كملف ملحق Attachment. ويهاجم البريد الإلكتروني ويرسل نفسه إلى أي عنوان يعثر عليه في دفتر العناوين في الجهاز الذي يصيبه كما يبطل مفعول البرامج المضادة للفيروسات. كما يستغل نقاط الضعف الموجودة في برنامجي البريد الإلكتروني Outlook و Outlook Express ومنذ تشخيصه للمرة الأولى، عثرت شركة Mcaffee المنتجة للبرامج المضادة للفيروسات على ٧٧٥ ألف نسخة منه، ويصل عدد النسخ اليومية إلى نحو ٢٠ ألف نسخة. ويعتبر هذا الفيروس مراوغ بقدر كبير وقادر على اختيار الأسماء بصورة عشوائية من دفتر العناوين ويستحدث انواعا كثيرة من الملفات نصوصا وملحقات، مما يجعل من الصعوبة بمكان تحديد مكانه وملاحقته. إضافة إلى قدرته على جعل برامج مكافحة الفيروسات عاجزة عن أداء دورها.

طريقة العلاج :

١- افتح قائمة Start واختر الأمر Run ثم اكتب Regedit وانقر Ok.

٢- ستظهر النافذة من القائمة اليسرى افتح المجلدات الآتية:

Run <CurrentVersion <Windows <Microsoft <Software <HKEY_LOCAL_MACHINE

٣- من القائمة اليمنى حدد الملف %windir% الذى يأتي غالبا على الصورة :

"C:\Windows:"netpatch" "%windir%\netbiospatch10.exe

٤- أعد تشغيل الجهاز.

٥- افتح قائمة Start واختر الأمر Run ثم اكتب EXPLORER.EXE ثم انقر Ok.

٦- انقر من الشاشة الجديدة View ثم اخنر الأمر Folder Options .

٧- انقر التبويب View ثم نشط الاختيار All Files Show ثم Ok .

٨- من مجلد التسجيل Registry احذف الملف netbiospatch10.exe ثم أعد تشغيل الجهاز.

٩- امسح الجهاز باستخدام برنامج مسح وإزالة الفيروسات واحذف جميع ملفات WORM_KELINO.A




فيروس VBS_LOVELETTR.AS

النوع : ينتمى هذا الفيروس إلى قائمة فيروسات Basic Visual

أسماء الشهرة الأخرى :

LOVELETTR.AS

LOVELETTER.AS

VBS_COLOMBIA

COLOMBIA

PRESIDENT AND FBI SECRETS

درجة الخطورة : عالية

الوصف : ينتقل هذا الفيروس عبر رسائل البريد الإلكتروني وبرنامج Microsoft Outlook ومن خلال الملفات المرفقة Attachments وبالأخص يوم ١٧ من كل شهر ويقوم بإلغاء جميع برامج تشغيل الشبكة وبرامج تصفح الإنترنت من النظام كما يسبب:

* زيادة الوقت اللازم لتنفيذ بعض العمليات عن الوقت المعتاد

*تأخر في تحميل البرامج إلي ذاكرة الكمبيوتر، وعدم تشغيلها بالكفاءة المعتادة.

* ظهور رسائل تفيد بأنه لا توجد ذاكرة كافية لتشغيل البرامج، بالرغم من أن الذاكرة المتاحة كافية.

طريقة العلاج :

١- افتح قائمة Start واختر الأمر Run ثم اكتب Regedit وانقر Ok.

٢- ستظهر النافذة من القائمة اليسرى افتح المجلدات الآتية:

Run <CurrentVersion <Windows <Microsoft <Software <HKEY_LOCAL_MACHINE

٣- احذف الملف LINUX32 من القائمة اليمنى.

٤- افتح قائمة Start مرة أخرى واختر الأمر Run ثم اكتب Regedit وانقر Ok.

٥- ستظهر النافذة من القائمة اليسرى افتح المجلدات الآتية:

\HKEY_LOCAL_MACHINE\Software\Microsoft\Windows

Services\reload CurrentVersion\Run

\HKEY_LOCAL_MACHINE\Software\Microsoft\Windows

columbia CurrentVersion\Run\plan

٦- كرر نفس ما سبق ثم أعد تشغيل الجهاز.

٧- امسح الجهاز باستخدام برنامج مسح وإزالة الفيروسات واحذف جميع ملفات VBS_LOVELETTR.AS ثم حدد هذه الملفات أيضا وقم بمسحها:

c:\Windows\System\LINUX32.vbs

c:\Windows\reload.vbs

c:\Windows\important_note.txt




c:\Windows\System\US-PRESIDENT-AND-FBI-SECRETS.HTM

فيروس VBS_PETIK.I

النوع : ينتمى هذا الفيروس إلى قائمة فيروسات Visual Basic

أسماء الشهرة الأخرى :

I-Worm.Petik.I

درجة الخطورة : متوسطة

الوصف : ينتقل هذا الفيروس عبر رسائل البريد الإلكتروني وبرنامج Microsoft Outlook ومن خلال الملفات المرفقة Attachments على الهيئة:

Subject: What is the seven sins؟؟

Message Body: Look at this file and learn them.

Attachment: Seven.vbs

ويقوم بإلغاء جميع خواص الماوس ولوحة المفاتيح من النظام.

طريقة العلاج :

١- افتح قائمة Start واختر الأمر Run ثم اكتب Regedit وانقر Ok.

٢- من النافذة التى ستظهر، ومن القائمة اليسرى افتح المجلدات الآتية :

HKEY_LOCAL_MACHINE<Software<Microsoft<Windows<CurrentVersion<Run

٣- احذف الملف C:\Windows\System من القائمة اليمنى، أو الملف :

C:\WinNT\System32:Envy = %system%\envy.vbs

٤- افتح المجلد الآتي :

HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\

CurrentVersion\Run\Services

ثم احذف ملف التسجيل الآتى Lust = %system%\lust.vbs

٥- افتح المجلد الآتي :

HKEY_CURRENT_USER > txtfile > shell > open > command

ثم انقر ملف التسجيل Default من القائمة اليمنى وقم بالتعديل الآتي من :

{Default} = wscript %windows%\Seven.vbs

إلى :

{Default} = %1% %windows%\NOTEPAD.EXE




حيث أن %windows% هو مسار برنامج Windowsوهو عادة على هيئةC:\Windows or C:\WinNT

٦- افتح المجلد الآتي :

DefaultIcon < VBSfile < HKEY_CURRENT_USER

ثم انقر الملف Default من القائمة اليمنى وقم بالتعديل الآتي من :

shell32.dll,-152oldicon = %windows%\Wscript.exe,2 = {Default}

إلى :

windows%\Wscript.exe,2% = Default} = %windows%\Wscript.exe,2oldicon}

ثم إلغ الملف oldicon.

٧- احذف الملف الآتي من سطح المكتب COPYRIGHT.txt.vbs ثم أعد تشغيل الجهاز.

٨- امسح الجهاز باستخدام برنامج مسح وإزالة الفيروسات واحذف جميع ملفات VBS_PETIK.I




فيروس PE_MOE.A

النوع : ينتمى هذا الفيروس إلى قائمة ديدان البريد الإلكتروني التي تستخدم بروتوكول Simple Mail Transfer Protocol في التنقل تحت الإمتداد *.exe و *.scr

أسماء الشهرة الأخرى : MOE.A

درجة الخطورة : متوسطة

الوصف : يقوم هذا الفيروس بالتنقل عبر البريد الإلكترونى كملف مرفق وينتج نسخة من نفسه عبر كل رسالة. ولقد وصل هذا الفيروس إلى العالم العربي قادما من استراليا والشرق الأقصى، وبدأ أول تأثير له على مؤسسات المال والإعلام في العاصمة البريطانية. وتعتقد الشركات المتخصصة بمكافحة فيروسات الكمبيوتر أن الوباء الجديد سيكون من أوسع أوبئة الكمبيوتر انتشارا هذا العام ويشك بعض خبراء مكافحة الفيروسات ممن فحصوا الفيروس الجديد والصفحات التي يقوم بإرسال المستخدمين إليها، أنه ليس سوى محاولة قام بها البعض لزيادة عدد الزوار إلى مواقعهم الإباحية. ويأتي انتشار الفيروس الجديد بعد مرور سنة واحدة بالضبط على انتشار فيروس مدمر آخر هو فيروس الحب الذي أدى إلى أضرار كبيرة في العديد من المؤسسات في شتى أرجاء العالم. ومن الجدير ذكره أن الفيروس الجديد لا يصيب سوى مستخدمي برنامج Outlook Express فقط.

طريقة العلاج :

١- افتح قائمة Start واختر الأمر Run ثم اكتب Regedit وانقر Ok.

٢- ستظهر النافذة من القائمة اليسرى افتح المجلدات الآتية:

Run <CurrentVersion <Windows <Microsoft <Software <HKEY_LOCAL_MACHINE

٣- قارن من القائمة اليمنى قيم ملفات التسجيل.

٤- احذف جميع الملفات التي تحتوي على قيم غير صحيحة.

٥- أعد تشغيل الجهاز.

٦- قم بمسح الجهاز باستخدام برنامج مسح وإزالة الفيروسات واحذف جميع ملفات PE_MOE.A

فيروس BKDR_LITMUS.002

النوع : ينتمى هذا الفيروس إلى قائمة فيروسات Backdoor

أسماء الشهرة الأخرى :

TROJ_BCKDR.JZ-1

BACKDOOR.JZ

TROJ_BCKDR.JZ-2

LITMUS.002

LITMUS

درجة الخطورة : عالية

الوصف : هذا الفيروس المدمر يتيح الفرصة لمخترقى أجهزة الكمبيوتر من استغلال أجهزة المصابين به في التحكم الكامل بالجهاز وإجراء أي تصرف كما لو كان جهازه.

طريقة العلاج :

١- افتح قائمة Start واختر الأمر Run ثم اكتب Regedit وانقر Ok.

٢- ستظهر النافذة من القائمة اليسرى افتح المجلدات الآتية:




Run<entVersion Curr<Windows<Microsoft<Software<HKEY_LOCAL_MACHINE

٣- احذف ملف التسجيل Taskschd من القائمة اليمنى.

٤- احذف المجلد TRAYWND.EXE.

٥- أعد تشغيل الجهاز.

٦- امسح الجهاز باستخدام برنامج مسح وإزالة الفيروسات واحذف جميع ملفات BKDR_LITMUS.002.

****

فيروس VBS_JADRA.A

النوع : ينتمى هذا الفيروس إلى قائمة فيروسات VBScript.

أسماء الشهرة الأخرى :

VBS.Jadra

VBS.Madonna.a

درجة الخطورة : عالية

الوصف : يقوم هذا الفيروس المدمر بالتمكن من جميع ملفات VBS ويقوم بإضافة ملفات تسجيل أخرى إليها لعمل على تشغيل الملفات الآتية عند بداية عمل Windows

* DEFRAG.EXE

* WINFILE.EXE

* EXPLORER.EXE

* CDPLAYER.EXE

* COMMAND.COM

طريقة العلاج :

١- افتح قائمة Start واختر الأمر Run ثم اكتب Regedit وانقر Ok.

٢- ستظهر النافذة من القائمة اليسرى افتح المجلدات الآتية:

Run<entVersion Curr<Windows<Microsoft<Software<HKEY_LOCAL_MACHINE

٣- احذف جميع ملفات التسجيل الآتية من القائمة اليمنى:

% Explorer.exe c:\windows\Explorer.exe = Don't_Cry_for_me_Argentina

% Command.com c:\windows\Command.com = JadraquerKiller

% c:\windows\Cdplayer.exe ZoneAlarm Pro = Cdplayer.exe

% AVPCC = Defrag.exe c:\windows\Defrag.exe

% AVP_Monitor = Scandskw.exe c:\windows\Scandskw.exe

% NAVDefAlert = Winfile.exe c:\windows\Winfile.exe

% McAfeeVirusScanService = Winfile.exe c:\windows\Winfile.exe




٤- افتح المجلد HKEY_CURRENT_USER ثم احذف الملف MyRegKey.

٥- أعد تشغيل الجهاز.

٦- امسح الجهاز باستخدام برنامج مسح وإزالة الفيروسات واحذف جميع ملفات VBS_JADRA.A.

****

فيروس WORM_APLORE.A

النوع : ينتمى هذا الفيروس إلى قائمة ديدان البريد الإلكتروني

أسماء الشهرة الأخرى :

APLORE.A

Worm.Psecure

APLORE

درجة الخطورة : متوسطة

الوصف : ينتقل هذا الفيروس عبر رسائل البريد الإلكتروني ومن خلال الملفات المرفقة Attachments كما ينتقل أيضا عبر الملفات المحملة Downloaded من مواقع الإنترنت، ويقوم بإنشاء مفتاح تشغيل ذاتي لملف التسجيل Redegit عن بداية تشغيل الجهاز كما إنه يستقر بالذاكرة الداخلية للجهاز وينشر نفسه إلى المواقع الأخرى عن الدخول على الإنترنت

طريقة العلاج :

١- افتح قائمة Start واختر الأمر Run ثم اكتب Regedit وانقر Ok.

٢- ستظهر النافذة من القائمة اليسرى افتح المجلدات الآتية:

Run <CurrentVersion <Windows <Microsoft <Software <HKEY_LOCAL_MACHINE

٣- احذف ملف التسجيل Explorer=%SYSTEM%\explorer.exe من القائمة اليمنى.

٤-أعد تشغيل الجهاز.

٥- احذف جميع الملفات الآتية من Directory Windows System:

(EXPLORER.EXE (copy of itself

(PSECURE20X-CGI-INSTALL.VERSION6.01.BIN.HX.COM (copy of itself

(EMAIL.VBS (detected as VBS_PSECURE.A

(as HTML_PSECURE.A INDEX.HTML (detected

(APHEX.JPG (image

(usually truncates to 0 byte HWND32.DLL (program

٦- امسح الجهاز باستخدام برنامج مسح وإزالة الفيروسات واحذف جميع ملفات WORM_APLORE.A

EG Y PT
2007-2008
Email mohamedhassen2008@yahoo.com