الحماية من الفيروسات:

كما نعلم ان معظم الفيروسات تسبب اضرار جسيمة بالكمبيوتر وتصعب التعامل معها اذا حدث ودخلت الى النظام لذا نقوم بحماية الجهاز عن طريق عدة اشياء تكون بمثابة مفتاح الامان في عالم نظام ويندوز:

(ملاحظة :من الممكن ان تكون بعض الموجودات هنا في بيئة xpلكنها لن تختلف كثيرا في بيئه win7 بإمكانكم البحبشة وايجاد ما يوافق الموجود هنا)

شرح عام عن الفيروسات:

- تقسم الفيروسات الى عده انواع في نظام ويندوز(حسب اللاحقه):

1- فيروسات exe. :بريمجات تقوم بمهام محدده كما البرامج لكن بعض منها قد يقوم بكتابة الكود المخصص له مع وضع الاوتورن له داخل برامج النظام.....قد يقوم بالدخول الى explorer ويقوم بنسخ نفسه عده مرات او قد يقوم بملئ الاقراص بمجلدات منسوخه او اختصارات ....
من الممكن ان نقسم بريمجات ال exe الى عده اقسام لكن سأتحدث عنها لاحقا

2- فيروسات ال vbs : قد تكون من اخطر الفيروسات بالنسبه للفضوليين حيث يقوم الفيروس بنسخ نفسه ويترك التشغيل الى غباء المستخدم ..فيقوم بوضع نسخه exe منه في النظام ويشغل لنفسه التشغيل مع النظام ويلصق نفسه بنظام ويندوز.

3- فيروسات الsrc:وهي فيروسات من نوع شاشه توقف حيث يرفق هذا الفيروس بفيروس اخر ويقوم بتشغيل نفسه او يقوم بتحويل الفيروس المرافق ليلائم بيئه هذا النظام.

4- مكتبه الdll المرافقه للفيروس: لاتكون هناك خطورة من هذه المكتبه لان الفيروس لن يعمل بشكل جيد اذا لم تكون موجوده ....ولكن وجودها لوحدها لن يشكل خطأ على المستخدم.

(*طبعا يوجد انواع اخرى لكن مافي ببالي شي تاني اكتبو*). ;-p

ونستطيع ايضاً تقسيم الفيروسات حسب عملها وطريقه عملها الى الانواع التاليه :

1- الفيروسات العاديه: تقوم بنسخ نفسها وعملها كأي برنامج اخر لكنها تدخل اجزاء من كودها الى البرنامج المصاب بها.

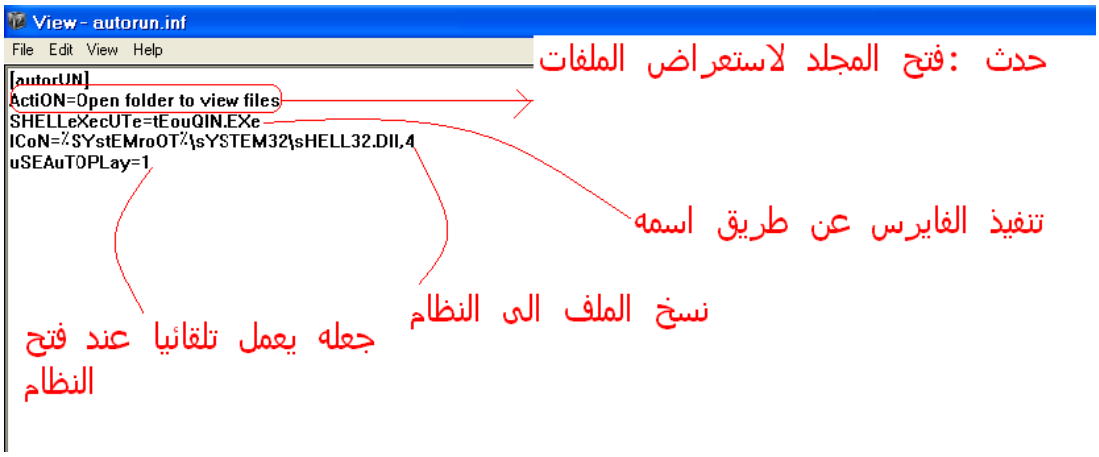
2- فيروسات الوورم (الدوده):تقوم هذه الديدان بنسخ نفسها الى البرامج التي تعمل منذ لحظه دخولها النظام ..ثم تاخذ باكل الملفات وتدميرها جزئياً .
قد لاتقوم الديدان الى بعمل واحد هو ان تعطل عمل الانتي او ان تنسخ الفيروس المرافق لها الذي يكون من النوع المتحول ...وهذه تكون ايضا من اخطر انواع الديدان.

3- الفيروسات المتحولة:من اخطر انواع الفيروسات تقوم بملائمه نفسها مع النظام ونسخ نفسها الى اي جهاز يتم ربطه بالجهاز المصاب

4- التروجانات(احصنة طرواده): وهي فيروسات خاصة بالهاكرز تقوم بعمليات محدد حسب البرنامج (الكلاينت) المربوط بهذا التروجان.
5- طبعا توجد انواع اخرى ايضا لكن كمان هاد يلي خطر ببالي.

الطرق العمليه للحمايه من الفيروسات:

1- ان لا تفتح الفلاشة او اي جهاز نقل بيانات عن طريق كبستين وممكن ان نوضح لماذا عن طريق الصور التالية:

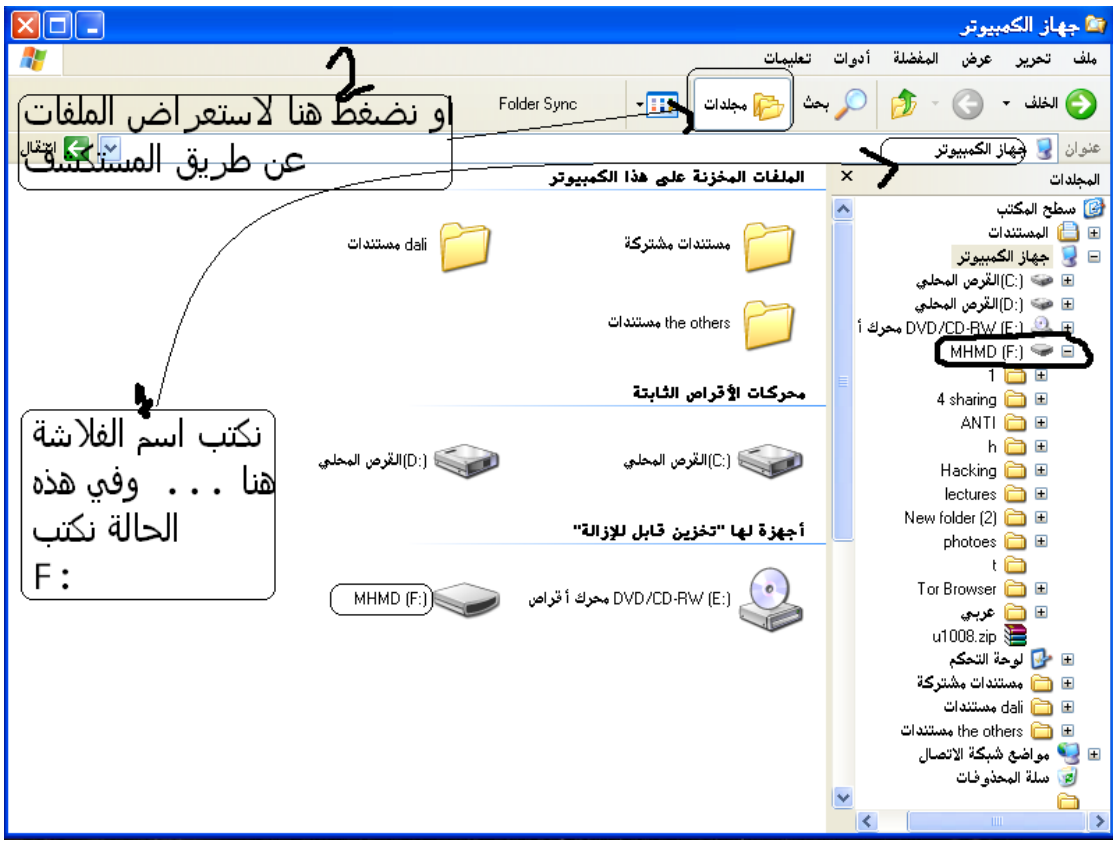


هذه صورة عن فايرس الاوتورن الذي يخيف الجميع
وقد يكون الفايرس مشفر تكون كتابته كالتالي:

من الممكن ان يكون فايرس autorun.inf من اخطر الفايروسات لانه من الممكن ان يشغل عدد من الفايروسات .....وذلك بسبب عدم انتباه المستخدمين الى ان هذا الفايرس عبارة عن ملف نصي غبي من الممكن التعديل عليه اذا كان الكمبيوتر المستخدم غير مصاب...

اذا نرى انه بإمكاننا حماية الجهاز من الاصابة بالفايرس او حتى حذف الفايرس من واسطة النقل المستخدمة.

وللحماية نقدم طريقة فتح الفلاشة عن طريق استعراض الملفات او من الممكن كتابة اسم الفلاشة في شريط المسار :



2- اظهار الملفات المخفية وحتى ملفات النظام المخفية :

الأول :وجود ملفات مخفية يمكن إظهارها كالتالي:

أدوات - خيارات المجلد - عرض: ثم نضع الاشارة على: إظهار الملفات المخفية.

الثاني :وجود ملفات محمية(إخفاء مضاعف) يمكن إظهارها كالتالي:

أدوات - خيارات المجلد - عرض: ثم نزيل التشك(إشارة الصح)عن: إخفاء ملفات النظام المحمية(مستحسن).

بالامكان ان ترى الان جميع الملفات المخفية وملفات النظام المحمية او المحددة بالقراءة التلقائية .

واذا كان الجهاز المستخدم مصاب بأحد الفايروسات من الممكن استعراض هذه الفايروسات من جهاز النقل بالطريقة التالية:

ندخل للرن >نكتب cmd انتر>نكتب اسم الواسطة مثلا ..... M: g: >نكتب السطر التالي : attrib *.* -s –h –r

نقوم بفتح الفلاشة فنجد ان الفايروسات قد ظهرت وبالامكان حذفها.

3- ايقاف تشغيل القرائة التلقائية:
عن طريق الدخول الى رن ثم كتابة gpedit.msc يفتح لنا نهج المجموعة ندخل الى قوالب الاداره>تكوين المستخدم>نظام> ايقاف تشغيل القرائة التلقائية
aDminstration tamplet >all sitings>turnoff autoplay
ونضعها تمكين حتى تتوقف القرائة التلقائية.
4- لا تشغل أي برنامج تنفيذي على جهازك لا تعرف من أين هو وماذا عمله، وهذه المهمة سهلة جدا، فبرامج نظام التشغيل مضمونة ولا تحوي فيروسات، البرامج التي تحتاجها من المحلات مضمونة إلى حد مقبول جدا، بقي عليك البرامج التي تستقبلها من الميل أو الانترنت، وهذه حوادث عرضية قد لا تحدث بالشهر مرة أو مرتين...
من منا يستقبل برامج exeيوميا على ميله , لو حصل ونزلت برنامج من النت فيمكنك فحصه على جهاز زميلك، أو على جهازك ثم ازالة مضاد الفايروسات أو ايقاف تشغيله على الأقل! لكي تحرر موارد جهازك من هذا البلوى المسمى أنتي فيروس.

اذا حدث واصيب الجهاز بالفايرس مالذي من الممكن ان يحدث للجهاز المصاب؟

ذلك يعتمد على نوع الفايرس الذي يصيب الجهاز او تأثير عدد الفايروسات التي تصيب الجهاز ووظيفتها تختلف من فايرس لآخر, بالنسبة للفايروسات حصرا التي تصيب برمجيات تنفيذية ليس بالامكان سوى ازالة جميع البرامج التنفيذية من الاقراص الاخرى وفرمتتة قرص النظام اما بالنسبة للتروجانات والديدان التي تقوم باخفاء الملفات وتعطيل بعض مهام النظام للسماح للفيروسات الاخرى بالعمل بحرية من الممكن ازالتها بالطرق التالية:

1- يتوجب عليك ايقاف عملها من الاماكن التالية:
أ- نطفي الدودة من ادارة المهام لانها تعمل بشكل خفي.
ب- ندخل للرن من الابدأ ثم نكتب msconfig ندخل لبدء التشغيل ونبحث عن البرامج التي تثير الشك من اسمها او من اماكن تواجدها حيث ان كل فايرس يمكن ان يكون اسمه غريب عجيب او مكان وجوده في الويندوز او سلة المهملات او او.....
ثم نزيل التشك عن هذا البرنامج.
ت- ندخل للرن ونكتب regedit ثم ندخل للتسلسل التالي :
hkcu\s\m\w\curr\explorer\advanced
غير قيمة الـ hiddenلـ(0) لإظهار الملفات المخفية.
غير قيمة الـ showsupperhiddenلـ(1) لإظهار المحمي.
طبعا أقصد بالـ :sسوفتوير، :Mمايكروسوفت، :Wوندوز، :Currكارنت فيرجن.
ثم:
hkcu\s\m\w\cur\
احذوف كل القيم يلي بالـ runوالـ runonceوالـ runservices، ماعدا قيم الدفولت طبعا.
2- من ال msconfig عرفت مسار الدودة او التروجان ,ممكن تتوجه للمكان الذي تقيم فيه وتحذفها بكبستين shift+delete حتى لا تعود للنظام.

ومن الممكن الآن معرفة الدودة او الاوتورن اذا كان موجود في الفلاشة او اي شي اخر وممكن ازالته.

بعض المشاكل التي من الممكن ان تواجه اثناء حذف الديدان:

1- من الممكن ان يظهر لك الجهاز المصاب ان اداة ادرة المهام او بدء التشغيل او محرر التسجيل غير مسموح تشغيلها وتحتاج الى صلاحيات .
هذه المشكله من الممكن حلها عن طريق الgpedit.msc .
2- ايضاً قد تعطل الدودة التي تصيب الجهاز وتمنع الدخول الى نهج المجموعه لذلك انصح باستخدام نظام بديل (من نوع اخر مثل لينكس) او استخدام نظام windows XP mini المتخصص في الصيانة الداخلية للنظام والدخول الى اماكن لا تستطيع الدخول اليها ,وتمكنك من الحصول على صلاحيات لا تملكها بدونه.
وخلال ذلك بالامكان التأكد من ان الجهاز يخلو من الديدان الاخرى التي تثير الشك في وجودها في غير اماكنها ونطرح بعض الامثلة:
أ- في القرص المحلي >Documents and Settings >المستخدم الحالي/
هنا تنسخ نفسها معظم الديدان لكن احذر من حذف الملفات الاساسية للنظام لانها قد تؤدي الى نقص في برنامج تشغيل النظام.
ب- من الممكن ان توجد الدودة في السيستم32 بالإمكان التوجه الى مكان تواجدها وحذفها.
3- قد تكون الدودة محمية من الحذف او مخصصة فقط للقراءة:
بالامكان الدخول الى موجه الاوامر وكتابة الامر التاليattrib xxx.eee –s –h –r
حيث ان xxx هو اسم الدودة و eee هو لاحقة الدودة(ليس بالضرورة ان يكون اسم الدودة من ثلاث احرف فقط)
4- عند الحاجة الى تنظيف فلاشة من الديدان الموجودة فيها والاوتورن ينصح بالتوجه الى جهاز نظيف من الفايروسات ولا يوجد فيه انتي فايرس ((لان الانتي من الممكن بغبائه ان يشغل الفايرس وينسخ الفايرس نفسه الى برنامج الانتي)) وايضا انصح بأن تكون القراءة التلقائية في ذلك الجهاز معطله .
5- هذا الشرح يقتصر على نظام ويندوز XP اما بالنسبة للنسخ الاخرى فتختلف بعض الاجراءات والمسارات لان الانظمه التي تلي XP كانت تعطي المستخدم صلاحيات قليلة وليس بإمكانه التعديل على بعض الخصائص في النظام بحجة الامان.
لكن من اراد ان يعلم كيفية الدخول الى المسارات او تعديل بعض الاشياء في نظام ويندوز 7 من الممكن ان يتواضل معنا "لان نظام 7 يختلف بين 32بت و64 بت في معظم الاعدادات العامة"
الآن اصبح من الممكن لمن شارك بأن يتخلى عن الانتي فايرس (الذي ليس له لزوم).
ولكن انصح بأن لا تتم هذه الخطوات في المراحل التجريبية الاولى الا في ظل نظام حماية قوي تجنبا للمشاكل والعوائق التي من الممكن ان تواجه المستخدم المجرب.