كن أنت مضاد الفيروسات

by sasory

لماذا : كن أنت مضاد الفيروسات

الجواب : لأسباب عديدة وهي ....

١ – ليست كل مضادات الفيروسات قادرة على اكتشاف الملف الخبيث وذلك بسبب

@ قد تكون نسخة المضاد قديمة

@ قد يكون الفيروس من نوع جديد

@ قد تكون صلاحية المضاد منتهية

@ قد يكون المضاد متخصص بنوع معين من الفيروسات

@ قد يكون المضاد سيئ الأداء

@ قد يكون المضاد نسخة تجريبية لا تتضمن كل وسائل الحماية

@ قد يكون الفيروس مخادع

٢ – إن مضادات الفيروسات القوية والمشهورة قد تقلل من أداء الكمبيوتر ولذلك لا يرغبها من لديه حاسب بمواصفات متوسطة أو ضعيفة

٣ – قد يكون مضاد الفيروسات من النوع الدموي ، حيث يحجز الملفات الخبيثة والملفات البريئة على حد سواء

٤ – معرفتك عزيزي القارئ بسلوك الفيروسات لن تضرك لذلك يمكنك قراءة هذه المقالة

في الحقيقة لا أقصد من مقالتي هذه مهاجمة مضادات الفيروسات ، فأنا لا أملك ثأرا شخصيا معها ، بل يجب أن يكون هناك مضادات فيروسات مثبتة على الجهاز لضمان الحماية من الفيروسات ومن الاختراق وغيرها من أنواع الأخطار التي لن تتفرغ لها لوحدك ؟؟؟

لم أكتب هذه المقالة من الفراغ ، فأنا قمت ببرمجة عدد لا بأس به من الفيروسات والبرامج الخبيثة ، لذلك أرغب في مشاركتك أيها القارئ الكريم ببعض معلوماتي المتواضعة عن سلوك نسبة كبيرة من البرامج الضارة ، بالإضافة إلى أنني قمت بتجارب على فيروسات ليست من صنعي جلبتها عن طريق(الفلاش ميموري) من الكمبيوترات المصابة

فالكلام الذي سوف أكتبه مجرب وليس (صف حكي)

إن معظم ما نسميه فيروسات أو برامج خبيثة وهذا إن لم تكن كلها ، نستطيع إزالتها يدويا فهي بالنهاية برامج شريرة خارجة عن القانون ، ولكن الذي يصعب إصلاحه هو تأثيرها على جهازك فأحيانا يكون مزعج جدا فقدانك بعض البيانات بسبب هذه المخلوقات المزعجة

إن أكثر أنواعها مقتا تلك التي تكون في كمبيوتر صديقك ، فتذهب أنت بكل سرور الى عنده وتقول له " كيفك أبو الشباب : شوف شو جايبلك " وعندما تضع الفلاش ميموري أو الميموري كارد في كمبيوتره .... يتم تشفير ملفاتك وجعلها غير صالحة للقراءة و الحذف فتضطر الى عمل فورمات .

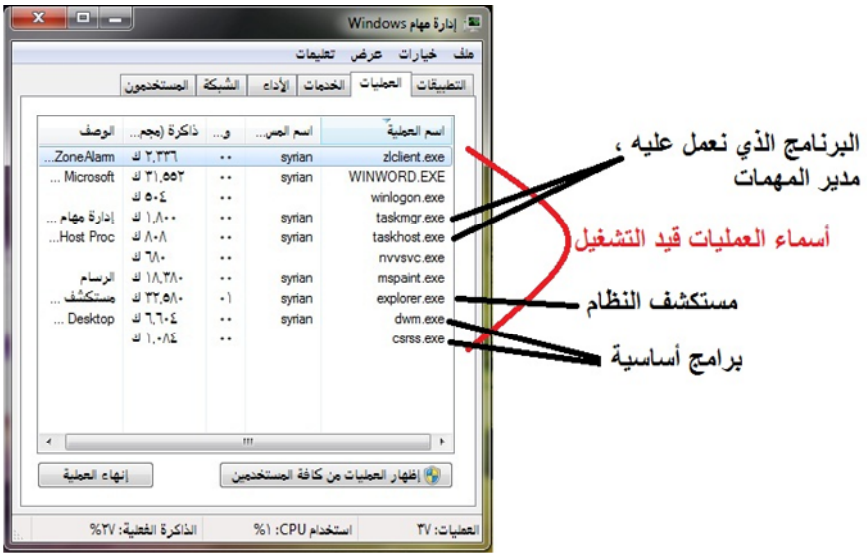
وتشتم الفيروس وصانع الفيروس وكمبيوتر صديقك

إزالة البرامج الخبيثة بالبرامج المتاحة في أي نظام تشغيل

① – استخدم دائما برنامج taskmgr.exe أو إدارة المهام وقم بتفعيل نافذة العمليات process وذلك لتعرف ما هي البرامج التي تعمل حاليا . أفترض أن برنامج إدارة المهام معروف لدى الجميع ، بضغطة يمينية على شريط المهام الموجود في الناحية السفلية من سطح المكتب وستتمكن من تشغيل إدارة المهام وتفيد هذه الخطوة في ملاحظة الأسماء الغريبة لبعض البرامج والتي يشك بأنها فيروسات أو برامج تجسس . مثل : "kjfasvavf.exe" فمثلا هذا الاسم غير منطقي كمتصفح انترنت أو برنامج قراءة كتب الكترونية . فنحن نعلم أن البرامج المعتادة "adobe.exe" "explorer.exe" "mdm.exe" وغيرها من البرامج التي لا نشك في نزاهتها .

وتفيد ادارة المهام في اغلاق بعض البرامج المزعجة التي تتصل بالإنترنت من دون اذن وتأخذ مساحة من ذاكرة التخزين العشوائي مثل برنامج
"realplayer_update" الذي يعمل مع كل تشغيل كمبيوتر ويحاول الاتصال بالإنترنت بدون تهذيب فهو برنامج قليل أدب ، وفي الواقع أغلب البرامج التجارية تحمل هذه الصفة السيئة .

ملاحظة إضافية : إن الفيروسات قد تأخذ أسماء مشابهة للبرامج الخدمية ضمن قائمة المهام ، أنا كنت اسمي بعض فيروساتي "explor.exe" "mdn.exe" "adobe.exe" قد تكون الأسماء متطابقة أو شبيهة ولكن في النهاية هي فيروسات .



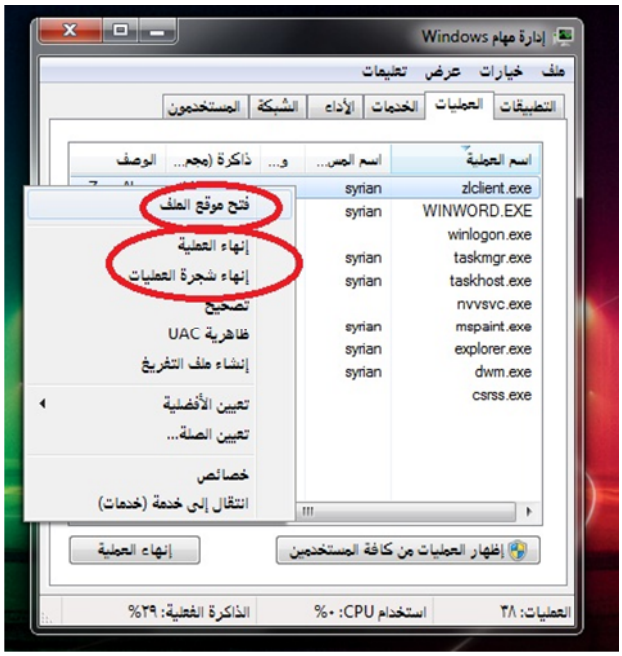
ماذا نفعل بإدارة المهام هذا ؟؟ ؟

أولا وبعد أن نفتح إدارة المهام نقوم بملاحقة الأسماء الغريبة التي نشاهدها ونضغط الزر اليمني للفأرة على اسم البرنامج الغريب ، ثم خيار فتح موقع الملف : إذا كان موقع الملف يثير الشبهة كأن لا يكون في ال program files أو أن يكون في سواقة لا تقوم أنت بالعادة بتحميل البرامج عليها ، نقوم بإنهاء مهمته ثم نحذفه إذا تأكدنا من عدم معرفتنا السابقة به أو لوجوده في مكان لا مبرر له أن يوجد فيه ،

أنتبه أن يكون برنامج يعمل من نواة الويندوز فهذا برنامج نظام ضروري مثل mdm.exe أو explorer.exe

مثال عن برنامج مشبوه

أنا أقوم بتحميل البرامج على السواقة c: فما المبرر لوجود برنامج يعمل من السواقة d: هذا قطعا برنامج خبيث



إذا : مدير المهام هو برنامج أساسي للتعامل مع الفيروسات المحتملة أو المؤكدة

ولكن أعيد وأذكر بالقاعدة التالية : (((يجب أن نعلم دائما ماذا نحمل على الكمبيوتر وفي أي مكان نحمل)))

فأنا عندما أعلم أنني حملت برنامج كذا للموسيقى والبرنامج الفلاني للصور والبرنامج العلتاني للكتب ... الخ هذا يعني أن أي برنامج دخيل سوف أميزه بسهولة .. وحتى ولو كان اسمه يشبه أسماء بعض البرامج الخدمية لدي ، فعندما أقوم بالخطوة الثانية وهي معرفة من أين يعمل هذا البرنامج فسوف أكشفه بكل سهولة إذا كان برنامج خبيث

مثال عن هذه الحالة :

فتحنا إدارة المهام ورأينا كلمة explorer.exe مكررة مرتين ، والحالة الطبيعية أنه يعمل مرة واحد وهو موجود داخل المجلد windows ... نقوم بفتح موقع الملف لكل منهما ونلاحظ الفرق ... الذي يكون خارج المجلد windows يكون هو الفيروس ...قطعا.

المشاكل التي قد تصادفنا وحلها

١ – بعد أن نتأكد أن الملف الذي يعمل هو عبارة عن ملف ضار نقوم بإغلاقه فيقوم بتشغيل نفسه من جديد

٢ – قد يكون هناك عدة ملفات ضارة عندما تغلق أحدها يقوم صديقه بتشغيله من جديد

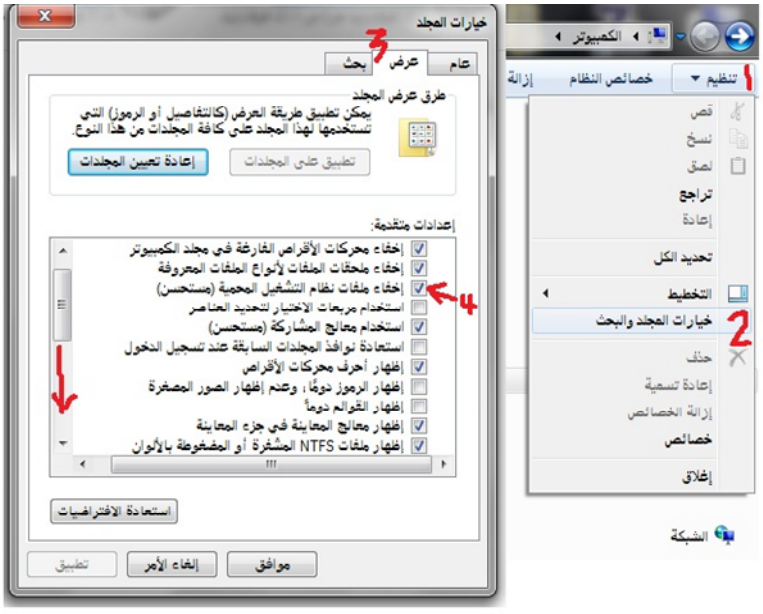
الحل لهذه المشكلة

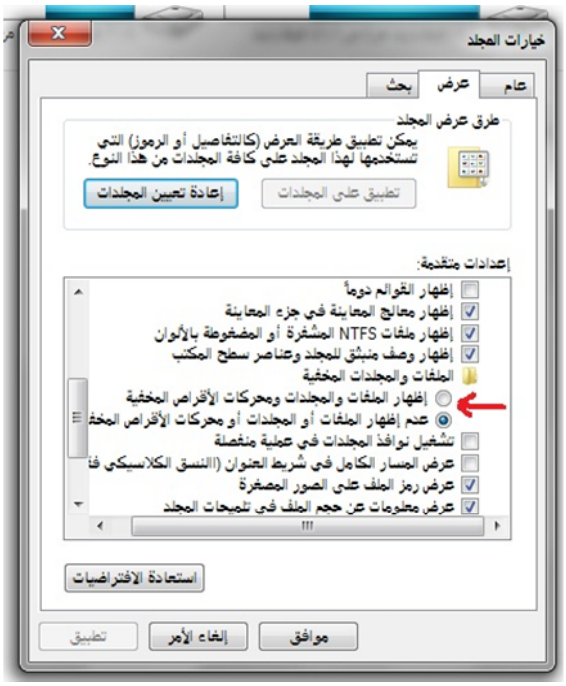
نفتح موقع الملف الخبيث ونحفظ مكانه بالتحديد في ذاكرتنا البشرية أو أين هم إذا كانوا أكثر من ملف ثم نعيد تشغيل الكمبيوتر ولكن بالوضع الآمن safe mode حيث يعمل الكمبيوتر بأقل الموارد وعندها نقوم بحذف الفيروسات بسهولة تامة لأنها لن تعمل في الوضع الآمن

٣ – قد لا يظهر الملف الخبيث عندما نفتح موقع الملف وذلك لأنه مخفي ووضع له سمة ملف نظام

الحل لهذه المشكلة

نقوم بفتح خيارات المجلد ثم إظهار ملفات النظام والملفات المخفية





وعندها سوف ينكشف المستور من الملفات الخبيثة ويمكنك حذفها

ملاحظة هامة : " ليست الفيروسات بأخطر من بعض البرامج الخدمية المستهترة "

ماذا أقصد من كلامي ؟ ؟ نلاحظ أن الشركات المحترمة عندما تطرح برامجها الخدمية في السوق : نقوم نحن بتحميل هذه البرامج على حواسبنا الشخصية

والبروتوكول المعروف أن البرامج تعطي لنفسها مسار للتحميل هو program files وعندما تقوم بالعمل على هذه البرامج وتريد حفظ مشروعك سوف تعطيك هذه البرامج مكانا لحفظ مشروعك ويكون عادة المستندات

وهنا بيت القصيد : البرامج المحترمة لا تقوم بتعقيد أماكن تواجد ملفاتها ونرى في نفس الوقت برامج خدمية غير مرتبة ، تقوم بتحميل ملفاتها في أماكن عشوائية وتنشر ملفاتها الضرورية وغير الضرورية في كل أنحاء الكمبيوتر ، مما يؤدي الى تراكم ملفات فوضوي يأخذ مساحة من الهارد

فما المبرر لبرنامج أن يضع ملفاته على سطح السواقة ويوجد لدينا مجلد ال program files لنضع البرامج داخله .

وما بالك ببعض البرامج التي لا تعمل إلا بشروط أو تلك التي تستخدم موارد النظام وإذا قمت بحذفها قد يذهب بعض من معلومات النظام معها ، من الجيد أن نسخ الأنظمة الحديثة لا تسمح بمثل هذا التسيب

نعود لموضوعنا . . .

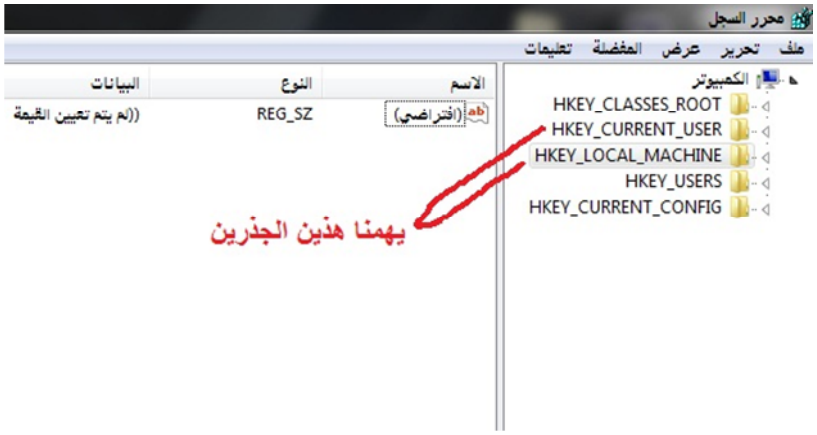
② - استخدام محرر الريجستري regedit.exe

المسار الكلمل c:\windows\regedit.exe

هذا البرنامج يقوم بتحرير بيانات الريجستري ،،، لماذا نحتاجه

لأن الكثير من الفيروسات وبرامج التجسس تحتاج للريجستري لجعل نفسها تقلع في كل إقلاع للكمبيوتر

البرنامج عبارة عن جذور متفرعة كما في الصورة التالية



في هذين الجذرين تتم لعبة إحياء البرنامج الخبيث لنفسه

سوف أكتب لك المسار الكامل للمفاتيح التي تستخدمها الفيروسات لتشغل نفسها مع إقلاع الكمبيوتر

المفتاح الأول

HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run

والمفتاح الثاني

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run

ولكن المفتاح الثاني يحتاج الى صلاحيات أكبر لكي يستطيع الفيروس أن يعدل عليه لذلك فإن أغلب الفيروسات تستخدم المفتاح الأول

كيف نستفيد من هذا المفتاح ؟

ندخل الى المفتاح خطوة تلو خطوة : أولا نفتح HKEY_CURRENT_USER ثم نفتح Software وهكذى حتى نصل الى Run

قبل أن نحذف هذه القيمة الموجودة في المفتاح run نقوم بحفظ موقع الملف الذي سيعيد تشغيل نفسه في ذاكرتنا البشرية لكي نحذفه ، وهو هنا موجود في المسار التالي d:\game\ty.exe

وبذلك نكون قد حذفنا الفيروس ونكون قد حذفنا بياناته في الريجستري

ملاحظة : يجب أن نتأكد من أن الفيروس ليس قيد التشغيل من إدارة المهام

وليس بالضرورة أن يفيدنا الريجستري في معرفة موقع الفيروس ، حيث يمكننا من خلاله إيقاف البرامج المزعجة التي تعمل مع إقلاع الكمبيوتر وذلك بحذف قيمها من المفتاح run

أين ما وجد الفيروس يمكنك من خلال الريجستري معرفة مكانه ولكن هناك مكان أخر غير الريجستري يمكن للفيروس أن يستخدمه ليعيد تشغيل نفسه وهو start up

③ - بدء التشغيل أو start up

مجلد معروف للجميع ، موجود في سواقة النظام ، إن أي نوع من الملفات يوضع في هذا المجلد سوف يقلع مع كل تشغيل للكمبيوتر ، لذلك ما علينا إلا أن ندخل اليه ونحذف كل الملفات الموجودة به ، ولكن يجب أن نظهر الملفات المخفية وملفات النظام أولا ، لأن أغلب الفيروسات تخفي نفسها وتجعل سمتها ملف نظام

يمكن الدخول اليه من : إبدا \ كافة برامج \ بدء التشغيل

④ إذهب إلى لوحة التحكم ثم الأجهزة والصوت ثم تغيير إعدادات التشغيل التلقائي وقم بجعل البرامج والألعاب (السؤال دوما) وبذلك تحمي نفسك من فيروسات ال autorun

إن ميزة نظام ويندوز ٧ أنه لا يشغل تلقائيا كل أنواع البرامج

ففي النسخ القديمة يمكن أن ترفق البرنامج الخبيث بلمف autorun.inf والذي سيقرأه النظام وينفذ التعليمات الموجودة فيه والتي مفادها أن الويندوز سيشغل الملف الخبيث من دون اذنك الشخصي . فهذا الملف نراه في ال cd and dvd فعندما نضعها في السواقة نلاحظ أنها تعمل من تلقاء نفسها وهذا بسبب المعلومات المكتوبة في الملف autorun.inf

وهذا الملف المرفق بالبرامج الخبيثة هو سبب لأنتشارها الكبير في أيام الجد xp

ولكن مع الويندوز ٧ لا يمكن لهذه الملفات أن تساعد في تشغيل الملف الخبيث تلقائيا

يمكنك فتحها بسهولة لمعرفة محتواها

ولكن مبرمجي الفيروسات أصبحوا يخفونها ويجعلون سمة "ملف نظام" عليها . وبعضهم وضع لها لاحقتين مثل "autorun.inf.ran"

⑤ - برامج التنصيب : هناك نسبة كبيرة من برامج التنصيب التي يمكن للمستخدم أن يعرف محتوياتها من دون أن يفتحها بشكل مباشر .

مثل ملفات rar.sfx.exe ذاتية التشغيل كما في الصورة التالية

بسبب مضادات الفيروسات يلجاء بعض صانعي الفيروسات الى جعل ملفهم الخبيث مكون من عدة لواحق وموضوع ضمن ملف رار ذاتي التشغيل ، وكما أشرت يمكنك أن تفتحه باستخدام winrar ثم تفرغ محتوياته من دون تفعيل ما يوجد داخله من برامج .

نصائح مفيدة

@ هناك تطبيقات تحمل اللاحقة exe ولكنها قد تبدو مثل مجلد وذلك ليجعلك مبرمجها تفتحها ، لذلك لا تفتح أي مجلد أو صورة أو ملف صوت أو كتاب الكتروني حتى تتأكد من لاحقته أنها ليست exe

@ لا يهم نوع الفيروس أو درجة خطورته : فقط ابحث مساره في الريجستري وأبحث في بدء التشغيل ثم قم بسحقه

@ تشغيل الكمبيوتر في الوضع الأمن يمكنك من حذف أي فيروس مستعصي عن الحذف

@ عندما تبحث عن الفيروسات قم بإظهار الملفات المخفية وملفات النظام لأن أغلب الفيروسات والبرامج الخبيثة تحاول أن تخفي نفسها

@ البرامج الخبيثة يمكن أن تنتج ملفات مساعدة لها من اللواحق التالية .vbs .wfs .dll .ocx .inf .ini .bat أو قد تكون مرفقة معها ضمن ملف رار ذاتي التشغيل

@ قم بحفظ أسماء البرامج التي قمت بتحميلها على الكمبيوتر لكي تميز الفيروس إذا رأيته

@ اعتبر نفسك محقق وحاول أن تكتشف أين ومن هو المجرم الذي تسلل لجهازك

@ نظام ويندوز ٧ مقاوم للفيروسات بسبب الأذونات التي تفرض على البرامج غير الموثوقة

@ التشغيل التلقائي في الويندوز ٧ مفيد في مكافحة ال autorun

@ لا تحمل أي برنامج يقال أنه برنامج اختراق فأغلبها لا يعمل بالإضافة الى أن الاختراق عن طريق البرامج يحتاج الى تنقيح عشرات المرات ومعظم برامج الإختراق هي للتجسس عليك .. وأغلبها لا يعمل إضافة الى أنه يكشفه مضاد الفيروسات

@عندما تحمل برنامج من الانترنت وتشغله فلا يعمل أو يعطي رسالة خطأ ،، قم بالتأكد من أنه يعمل بشكل خفي ، عن طريق إدارة المهام فإذا كان ضمن العمليات الموجودة أوقفه . وأحذفه ، ثم قم بتفحص الريجستري و بدء التشغيل

@ عندما يتضرر الكمبيوتر بسبب فيروس وتكون الأعراض عدم ظهور سطح المكتب أو ظهوره من دون أيقونات وقائمة ابدأ فهذا يعني أن البرنامج الخبيث أو الفيروس قام بإلغاء عمل ال explorer

الحل : أولا قم بتشغيل الكمبيوتر في الوضع الأمن أو حتى بالوضع العادي ولكن أفضل أن يعمل في الوضع الآمن لأن هذا النوع من الأعراض دليل على فيروس يمكنه العمل في الوضع الأمن لذلك يفضل القضاء عليه في الوضع الأمن

شغل إدارة المهام من خلال الإختصار على لوحة المفاتيح ctrl + alt + delete

اضغط مهمة جديدة new task ثم افتح محرر الريجستري من المسار التالي
c:\windows\regedit.exe

وادخل الى المفتاح التالي

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon

هناك قيمة اسمها shell يجب أن تكون بياناتها Explorer.exe

إذا كان هناك مسار ملف بدلا من هذه القيمة فهذا مسار الفيروس أو ربما يكون موجودا معها ،، قم بحفظ مكانه في ذاكرتك البشرية ثم قم بحذفه وأرجع القيمة Explorer.exe

وإذا لم يكن مسار الفايروس موجودا أرجع القيمة Explorer.exe وابحث عنه في المفتاحين

HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run

يجب أن تغلق البرنامج الخبيث عندما تتعرف عليه ، فليس من الحكمة أن تصلح الضرر الناجم عنه وهوما زال فعالا في قائمة العمليات

معلومات إضافية

١ – وجود الفيروس في الكمبيوتر لا يعني أنه فعال

٢ – إذا كان الفيروس فعال لا يعني أنه يمارس عمله التخريبي

٣ – إذا مارس الفيروس عمله التخريبي هذا لا يعني أنه تمكن من الوصول لغايته

٤ – إذا وصل الفيروس الى غايته وقام بالتخريب هذا لا يعني أن العطل لا يمكن إصلاحه

كل مبرمج له تصنيف خاص به للفيروسات ، وفي الحقيقة لا يوجد تصنيف ثابت لها حيث يمكن تصنيفها حسب درجة الخطورة أو حسب تصنيف مضادات الفيروسات ، حسب الحجم ، حسب السلوك ..... الخ

يمكن الحديث عنها حسب الإحترافية في برمجتها ، لأنه لم يتحدث أحد في هذا النوع من التقييم .

فالمبرمج الهاوي قد يهدف للتدمير : ومعظم فيروساته هدفها إما الحذف أو عمل مقالب بالضحية كعكس أزرار الماوس أو إيقاف بعض الخدمات أو فتح السواقة وإغلاقها أو فيضان ملفات ، وغيرها الكثير من الأشياء المزعجة ،،،، والسبب ناتج عن الرغبة في إظهار الذات ،،،،، والخبر الجيد أن أغلبية هذه البرامج المضرة لا تعمل لأن البرامج في الحالة الطبيعية تحتاج لعملية تدعى التنقيح .. أي يتم تجريبها للعمل على عدة أنظمة تشغيل وبظروف مختلفة لمعرفة الأخطاء البرمجية التي قد تحدث أثناء تنفيذها لعملها أو المرفقات التي يجب أن تكون معها ،،،، وبما أننا نتكلم عن مبرمج هاوي فهذا الشيء هو أول ما يفوته في عالم البرمجة ....لذلك يمكننا أن نضع نسبة كبيرة من البرامج الخبيثة في القمامة لأنها مشاريع فاشلة ... إضافة الى أن هذه النوعية هي المفضلة لدى مضادات الفيروسات حتى الرديئة منها .

أما المبرمجين المتوسطين : هنا تتنوع الرغبات التي يريدونها من فيروساتهم ولدى بعضهم أفكار جديدة ولامعة ، لذلك يمكن لنسبة قليلة منهم أن تبرمج فيروسات خطيرة قادرة على التأثير بالضحية .... ولكن .... يمكن كشف فيروساتهم بالطرق التي ذكرتها .

أما المبرمجين المحترفين : فواحد منهم قد كلف العالم الملايين وذلك عندما برمج دودة بريدية أتلفت آلاف الحواسب حول العالم .... ولكن أغلبهم هدفه تجسسي وليس تخريبي .. لماذا .. لأنه نفسيا راضي عن نفسه أنه قادر على التدمير

ودائما يوجد حلات شاذة فالتصنيف هنا على سبيل المقاربة النفسية وليس كلاما منزلا .

وهذه عبارة عن مقالة خفيفة وليست كتاب متخم بالمعلومات .

Sasory1990@hotmail.com