تخلص من ملفات التجسس

تختلف برامج ((التجسس)) في المميزات وطريقة الإستخدام .. لكنها جميعاً تعتمد على فكرةٍ واحده وهي ما يسمى ((الملف اللاصق .. ((Patch File - والذي يرسله (المتجسس) إلى جهاز (الضحيه) فيقوم الأخير بحسن نيه بتشغيل هذا الملف ظناً منه بأنه برنامج ظريف أو لعبةٍ جميله سيقضي وقتاً ممتعاً عليها .. لكنه غالباً ما سيتفاجأ بعدم عمل الملف بعد الضغط عليه وسينسى الأمر أو سيظن أن الملف معطوب .. لكنه لن ينسى أن يقوم بشكر المرسل على الأقل 3 مرات ((مثل بعض الناس ((بينما في ذلك الوقت يكون ((صاحبنا المتجسس)) يتمشى بين ملفات جهازك مسيطراً على ما فيه من برامج وملفات شخصيه وخاصه وبإمكانه إتلاف ملفات نظام التشغيل ((بضغطة زر من جهازه)) لو كان من عديمي الضمير والأخلاق .. ولكن معظمهم يكتفي بسرقة ((ماخف وزنه)) كالصور والملفات .. وإزعاجك ببعض الحركات السخيفه كالتحكم بمؤشر الماوس ولوحة المفاتيح .. ألخ .. كما يمكنه ((في بعض البرامج)) الإستماع إليك إن كنت تتحدث أو قراءة ما تقوم بكتابته على جهازك . بعد هذه المقدمه .. يتضح لنا خطورة هذه البرامج وما يمكنها فعله من كشفٍ للخصوصيات .. والذي يهمنا هنا كيفية الوقايه أولاً .. وثانياً العلاج في حالة وجود الإصابه . الوقاية: تقول الحكمه ((درهم وقايه خيرٌ من قنطار علاج)) .. وغالباً ما تكون صعبة التنفيذ حيث ان كثير من الأمور التي ستذكر لاحقاً قد يصعب تنفيذها .. لكن لا بأس من تنفيذ ما يمكن منها إن كان جهازك يحتوي على ما يستحق الخوف عليه من ((المتلصصين و الطفيليين)) .

1. لا بد من وجود برنامج ((مضاد للفيروسات)) ويفضل أن يتم شراؤه .. ويجب عليك تحديثه عن طريق النت كلما توفر ذلك . ((بعض هذه البرامج تتوفر التحديثات لها كل أسبوعين كبرنامج Norton AntiVirus)) . 2. لا تستقبل ملفات إلا ممن تثق بهم .. وإن إستدعى الأمر ((لتجنب الإحراج)) إستقبل لكن لا تقم بتشغيلها .. حيث أن معظم ملفات الباتش والتي تحوي فيروسات التروجان Trojan .. ترسل دائماً بطريقه مباشره عن طريق برنامج الـ .. ICQ أو الـ .. FreeTel وكذلك الـ Mirc . 3. إفحص جهازك بشكل دوري في موقع HouseCall AntiVirus حيث يوفر هذا الموقع الفحص على الفيروسات وملفات التروجان مجاناً(وقد ذكرت هذا الموقع سابقا) .. ويمكنه كشف جميع أنواعه وحذفها من جهازك .. ويحدث هذا الموقع بإستمرار . سيكشف هذا الموقع جميع الفيروسات والباتش بجهازك .. لكنه لن ينظف إلا الفيروسات فقط .. أما ملفات الباتش فلن يستطيع ((لأنها تكون قيد العمل بالذاكره)) .. هذا أن وجدت طبعاً . 4. لا تحفظ الآتي على القرص الصلب للجهاز) : الملفات الشخصيه - الصور العائليه - ملفات تحتوي على كلمات سريه أو أرقام بطاقات إئتمان أو

حسابات بنوك .. إلخ) . بل إحفظها على ((أقراص مرنـه .. ((Floppy Disk - أو على CD إن كانت إمكانياتك تسمح بشراء .5 . CD Writer إبتعد عن المواقع المشبوهه .. ولا تقم بتنزيل أي ملفات من تلك المواقع . 6. توكل على الله . العلاج: قبل أن نبدأ أرجو منك الضغط هنا وستظهر لك شاشة جديده لموقع HouseCall AntiVirus .. قم بإتباع التعليمات السهله فيها وإفحص جهازك .. وسجل المعلومات عن كل الفيروسات وملفات الباتش على ورقه .. وأحتفظ بها معك . أو إنك قمت بفحص جهازك .. وتأكدت بأنه مصاب بملف تجسس ..!! وبدون شك أنك تود الخلاص منه بدون أن تلجأ لتهيئة القرص الصلب . (Format) طبعاً قد تكون العمليه معقده بعض الشيء .. لأننا نتعامل مع ملفات باتش عديده لبرامج مختلفه .. ويزيد الأمر صعوبه هو إختلاف اسماء تلك الملفات .. حيث أن ((المرسل)) بإمكانه قبل الإرسال تغيير إسم الملف بأي أسم يشاؤه .. لكننا سنحاول قدر الإمكان تضييق الدائرة على ملف التجسس .. ومن ثم حذفه من ((دفتر الريجستري ((Registry وبالتالي من الجهاز .. وذلك بإتباع التالي : 1 Start . 2. Run 3. أكتب في المكان المخصص التالي 4. regedit : إضغط على المفاتيح التاليه بالترتيب : HKEY_LOCAL_MACHINE Software Microsoft Windows CurrentVersion Run 5. والآن بنافذة ((دفتر الريجستري)) على يمينك بالشاشه ستشاهد قائمتين : * الأولى قائمة : Name وفيها إسم الملفات التي تشتغل بقائمة بدء التشغيل للجهاز . * الثانيه قائمة Data وفيها معلومات عن الملف .. وإمتداد هذا الملف أو البرنامج . ومن قائمة Data: سنستطيع التعرف على ملف التجسس .. حيث أنه لن تكون له أي معلومات أو إمتداد مثل الصورة أعلاه ((لاحظ إشارة اليد)) . 6. الآن حدد هذا الملف وإضغط على Del بلوحة المفاتيح واختر .7 . Ok لزيادة الأطمئنان إذهب أيضاً للمفاتيح التاليه .. Run Once Run Services Run Services Onc : وكرر معها نفس الخطوه السابقه بالبند 5 . 8. أغلق برنامج الريجستري وإلى الخطوه الأخيره . الآن للخطوه الأخيره .. وهي إلغاء ملف التجسس من مجلد الويندوز ((وهو نفس الأسم الذي سجلته بالورقه عند فحص الجهاز 1. Start 2. Restart :)) 3. إذهب إلى المجلد الذي به ملف الباتش ... وغالباً ما يكون : at Ms-Dos c:\windows أو c:\windows\system 4. وأحذفه بالأمر del متبوعاً بأسم ملف الباتش . 5. أعد تشغيل الجهاز بالضغط على المفاتيح ctrl+alt+del : وبهذا تكون قد تخلصت من ملف التجسس اللعين .. ولو أنك أتبعت تعليمات ((الوقايه)) ستكون بإذن الله محمياً من (((الجواسيس والطفيليين))) ولن تحتاج إلى أي من تلك التي (((تسمى ببرامج الحمايه))) وحتى بإمكانك إلغاؤها من جهازك وأنت مطمئن . وقبل أن أريح بالكم اريد أن أخبركم معلومه خطيره بأن الملفات المستقبلة عن طريق الريل بلير لا يمكن التخلص منها فيوجد بالريل بلير ثغرة للاسف لا يمكن التخلص منهاولا يوجد حل الا عمل الفورمات من جديد.

==========

مقدمه لكم

م/محمد زايد محمد

01217583666