الفصل الأول (تاريخهم و بدايتهم)

الهاكرز, هذه الكلمة تخيف الكثير من الناس خصوصا مرتادي شبكة الإنترنت الذين يحملون خصوصياتهم الموجودة في أجهزتهم و يبحرون في هذا البحر, و معظم الأحيان يرجعون و قد تلصص أحدهم على هذه الخصوصيات و ربما استخدمها في أمور غير شرعية.

عالم الهاكرز عالم ضخم غامض, و بدايته كانت قبل الإنترنت بل و قبل الكمبيوتر نفسه, و لربما تسائل البعض, من هو الهاكر؟

تعريف الهاكرز:- الهاكرز, هذا اللفظ المظلوم عربيا, يطلق على المتحمسين في عالم الحاسب و لغات البرمجة وأنظمة التشغيل الجديدة, و يستخدم هذا اللفظ ليصف المبرمجين الذين يعملون دون تدريب مسبق.

لقد انتشر هذا المصطلح انتشارا رهيباً في الآونة الأخيرة و أصبح يشير بصفة أساسية إلى الأفراد الذين يلجئون بطريقة غير شرعية إلى اختراق أنظمة الحاسب بهدف سرقة أو تخريب أو إفساد البيانات الموجودة بها. و في حالة قيام المخترق بتخريب أو حذف أي من البيانات الموجودة يسمى (كراكر), لأن الهاكر يقوم عادة بسرقة ما خف من البرامج و الملفات ولا يقوم بتخريب أو تدمير أجهزة الغير.

بدايتهم :- نعود إلى عام 1878م, في الولايات المتحدة الأمريكية, كان أغلب العاملين في شركات الهاتف المحلية من الشباب المتحمس لمعرفة المزيد عن هذه التقنية الجديدة و التي حولت و غيرت مجرى التاريخ. فقد كانوا يستمعون إلى المكالمات الشخصية و يغيرون الخطوط الهاتفية بغرض التسلية و تعلم المزيد حتى قامت الشركات بتغيير الكوادر العاملة بها من الرجال إلى كوادر نسائية للانتهاء من هذه المشكلة.

مع ظهور الكمبيوتر في الستينات من هذا القرن, انكّب المتحمسون على هذا الصندوق العجيب, و ظهر الهاكرز بشكل ملحوظ, فالهاكر في تلك الفترة هو المبرمج الذكي الذي يقوم بتصميم و تعديل أسرع و أقوى البرامج, و يعتبر كل من (دينيس ريتشي و كين تومسون) أشهر هاكرز على الإطلاق في تلك الفترة لانهم صمموا نظام التشغيل (اليونكس) و الذي كان يعتبر الأسرع في عام 1969م.

و مع ظهور الإنترنت و انتشاره دولياً, أنتجت شركة IBM عام 1981م جهاز أسمته (الكمبيوتر الشخصي) الذي يتميز بصغر حجمه و وزنه الخفيف بالمقارنة مع الكمبيوترات القديمة الضخمة, و أيضا سهولة استخدامه و نقله إلى أي مكان و في أي وقت, و استطاعته الاتصال بالإنترنت في أي وقت. عندها, بدأ الهاكرز عملهم الحقيقي بتعلم كيفية عمل هذه الأجهزة و كيفية برمجة أنظمة التشغيل فيها و كيفية تخريبها, ففي تلك الفترة ظهرت مجموعة منهم قامت بتخريب بعض أجهزة المؤسسات التجارية الموجودة في تلك الفترة. يوماً بعد يوم ظهرت جماعات كبيرة منافسة , تقوم بتخريب أجهزة الشركات و المؤسسات حتى بدأت هذه المجموعات الحرب فيما بينها في التسعينات من هذا القرن و انتهت بإلقاء القبض عليهم .

و من عمليات الاختراق الملفتة للأنظار, قيام مجموعة من الهاكرز مؤخراً بالهجوم على موقع هيئة الكهرباء والمياه في دبي و مكتبة الشارقة العامة و ذلك بنشر كلمات غريبة في الصفحة الرئيسة للموقعين!

كما قامت مجموعة أخرى من البرازيل باختراق 17 موقعاً من الولايات المتحدة الأمريكية إلى بيرو, و من أهمهم موقع (ناسا) تاركة رسالة تقول " لا نرى فارقاً كبيراً بين نظامكم الأمني و نظام حكومة البرازيل...

هل فهمتم؟"

أشهر الهاكرز:- كـــيفن ميتنك, الشخص الذي دوّخ المخابرات الأمريكية المركزية و الفيدرالية FBI كثيراً.

قام بسرقات كبيرة من خلال الإنترنت لم يستطيعوا معرفة الهاكر في أغلبها. و في إحدى اختراقاته، اخترق شبكة الكمبيوترات الخاصة بشركة Digital Equipment Company و سرق بعض البرامج فتم القبض عليه و سجنه لمدة عام.

خرج ميتنك من السجن أكثر ذكاء, فقد كان دائم التغيير في شخصيته كثير المراوغة في الشبكة و كان من الصعب ملاحقته, و من أشهر جرائمه سرقة الأرقام الخاصة ب20000 بطاقة ائتمان و التي كانت آخر جريمة له. و يعتبر ميتنك أول هاكر تقوم ال FBIبنشر منشورات عنه تطالب من لديه أية معلومات عته بإعلامها, حتى تم القبض عليه عام 1995 و حكم عليه بالسجن لمدة عام لكنه لم يخرج إلا أواخر عام 1999 و بشرط عدم اقترابه من أي جهاز كمبيوتر لمسافة 100 متر على الأقل!

الفصل الثاني (وسائلهم و طرقهم)

عالم الهاكرز عالم دائم التطور, فالهاكرز يخترعون برامج و طرق جديدة معقدة يستطيعون من خلالها اختراق الشبكات و الأجهزة مهما كانت محمية. تختلف برامج التجسس في المميزات و طرق الاستخدام, ولكن الطرق التقليدية التي يستعملها الهاكرز المبتدئين جميعها تعتمد على فكرة واحدة و هي ما يسمى (الملف اللاصق (Patch file) (و الذي يرسله المتجسس إلى جهاز الضحية عن طريق البريد الإلكتروني أو برامج المحادثة فيقوم الأخير بفتحه بحسن نية دون دراية منه أنه قام في نفس الوقت بفتح الباب على مصراعيه للمتجسس ليقوم بما يريد في جهازه, و في بعض الأحيان يستطيع المتجسس عمل ما لا يستطيع الضحية عمله في جهازه نفسه.

يتم الاختراق عن طريق معرفة الثغرات الموجودة في ذلك النظام و غالباً ما تكون تلك الثغرات في المنافذ (Ports)الخاصة بالجهاز, و يمكن وصف هذه المنافذ بأنها بوابات للكمبيوتر على الإنترنت. يستخدم الهاكر برامج تعتمد على نظام (الزبون/الخادم (client/server) (حيث أنها تحتوي على ملفين أحدهما هو الخادم (server) الذي يرسل إلى جهاز الضحية الذي يقوم بفتحه و يصبح عرضةً للاختراق حيث أنه تم فتح إحدى المنافذ بواسطة هذا الخادم.

هناك طرق عديدة و مختلفة تمكن المتطفلين من اختراق الأجهزة مباشرة دون الحاجة إلى إرسال ملفات , لدرجة أن جمعية للها كرز في أمريكا ابتكرت طريقة للاختراق تتم عن طريق حزم البيانات التي تتدفق مع الاتصالات الهاتفية عبر الإنترنت حيث يتم اعتراض تلك البيانات و التحكم في جهاز الضحية. كما يستخدم الهاكرز نظام التشغيل (Unix) لأنه نظام أقوى و أصعب من (Windows) بكثير , كما يستخدمون أجهزة خادمة تعمل على الإنترنت و تستخدم خطوط T1 السريعة الاتصال بالشبكة عن طريق الحصول على حساب شل

(Shell Account).

الفصل الثالث (العلاج و الوقاية)

كلنا سمع بالحكمة التي تقول (درهم وقاية خير من قنطار علاج) , و طرق الوقاية عديدة تقي الجهاز من الإصابة بفيروسات أو ملفات لاصقة يرسلها هؤلاء الهاكرز, و منها أن يكون الكمبيوتر محملاً ببرنامج (مضاد للفيروسات) و يفضل أن يتم شراؤه لا تنزيله من الإنترنت و يجب تحديثه عن طريق الإنترنت كلما توفر ذلك.من البرامج المضادة للفيروسات برنامج (Norton AntiVirus) الذي يوفر تحديثات كل أسبوعين.

بما أن الغالبية العظمى من الملفات اللاصقة تحتوي على فيروس التروجان -(Trojan) الذي أُخذ اسمه من حصان طروادة صاحب القصة المشهورة, الذي أُدخل إلى قصر الطرواديين على أنه هدية من اليونانيين و خرج منه الجنود ليلاً- الذي سيكشفه برنامج المضاد للفيروسات مع باقي الفيروسات إن وجدت, و سيقوم بتنظيف الكمبيوتر من تلك الفيروسات و لكنه لن يتمكن من تنظيف الملفات اللاصقة لأنها تكون قيد العمل بذاكرة الكمبيوتر, هذا إن وُجدت طبعاً.

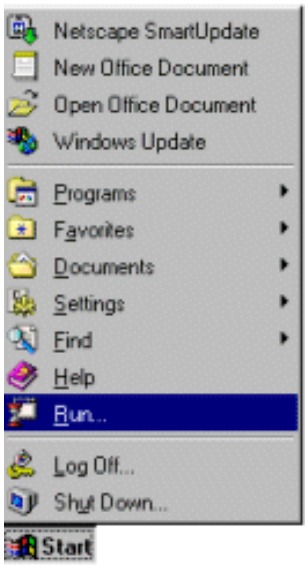
الوقاية:- من الضروري عدم حفظ الملفات الشخصية و الصور العائلية و ملفات تحتوي على أرقام سرية و حسابات في القرص الصلب للجهاز إنما حفظها في أقراص مرنة ,(Floppy Disk) و الابتعاد عن المواقع المشبوهة عدم تنزيل أي ملفات و برامج منها للاحتمال احتوائها على بعض الفيروسات أو الملفات اللاصقة.

العلاج:- يجب فحص الجهاز بإحدى البرامج المضادة للفيروسات, و عند اكتشافها ملفات تجسس يجب تدوين و تسجيل كل المعلومات عنها على ورقة والاحتفاظ بها.

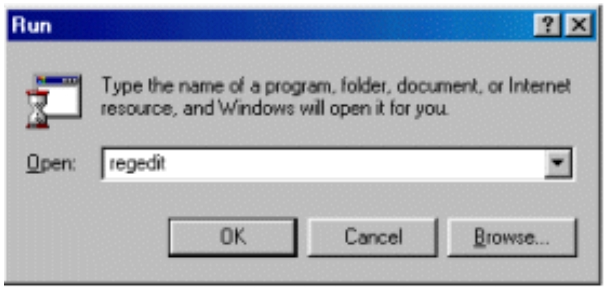
إن عد الملفات اللاصقة كبير خصوصاً بعد ظهور برامج التجسس الجديدة , لذا قد تكون عملية حذفها صعبة خصوصاً إذا قام الهاكر بتغيير اسم الملف باسم آخر, و لكن سيتم قدر الإمكان تضييق الدائرة على ملف التجسس و حذفه من دفتر التسجيل في الجهاز المصاب و بالتالي منه.

بدخول دفتر التسجيل (Registry)و اتباع التالي:

Startو الضغط على زرrun

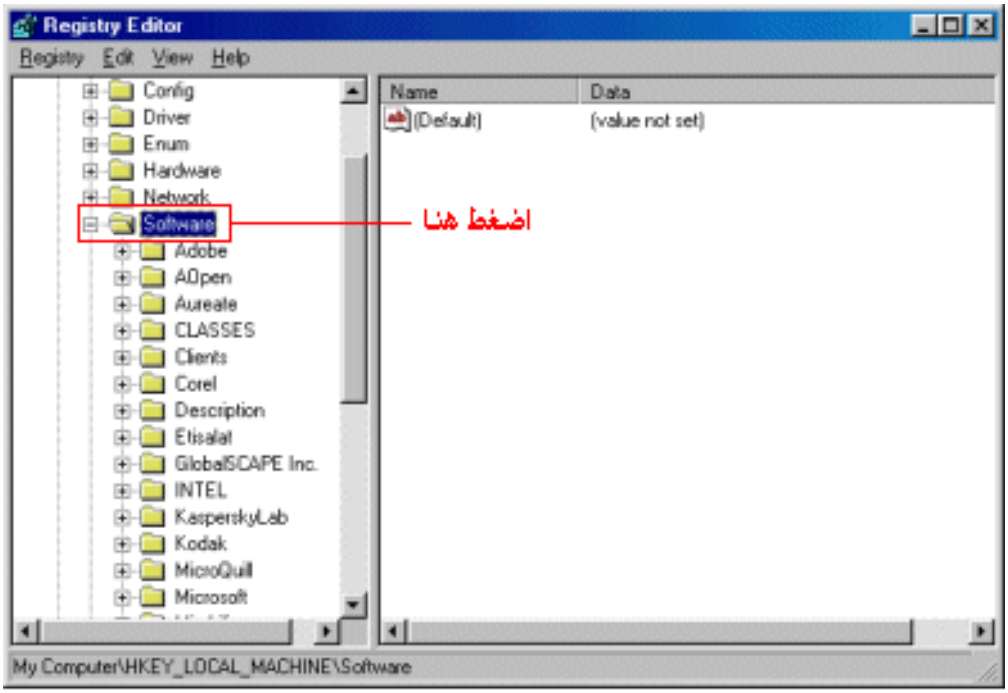


بكتابة (regedit) في المكان المخصص ستظهر نافذة دفتر التسجيل

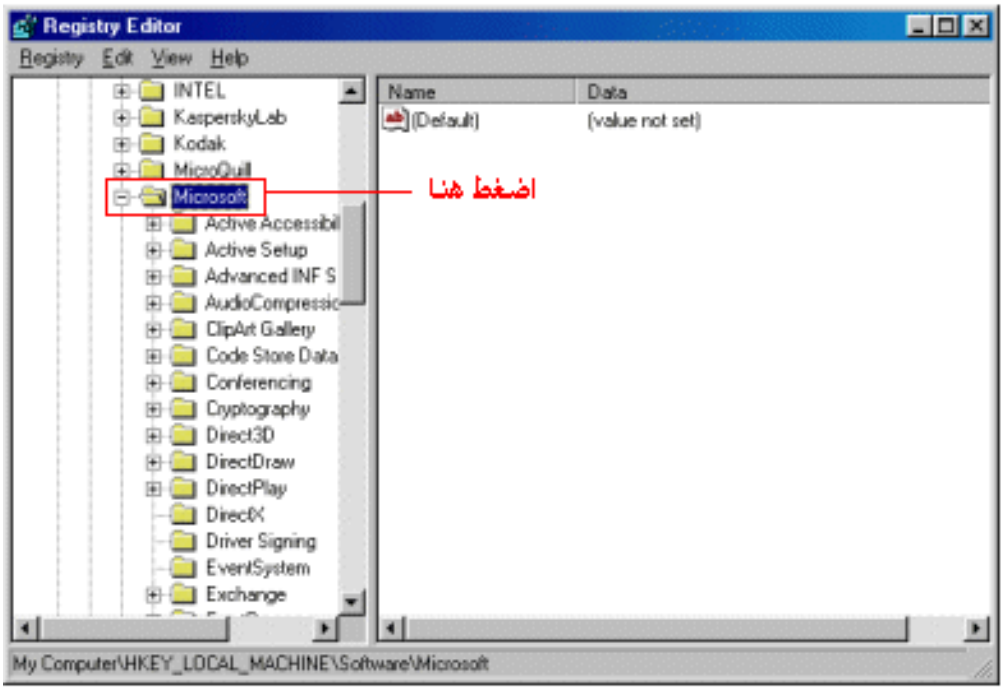


و بالضغط علىHKEY-LOCAL-MACHINE

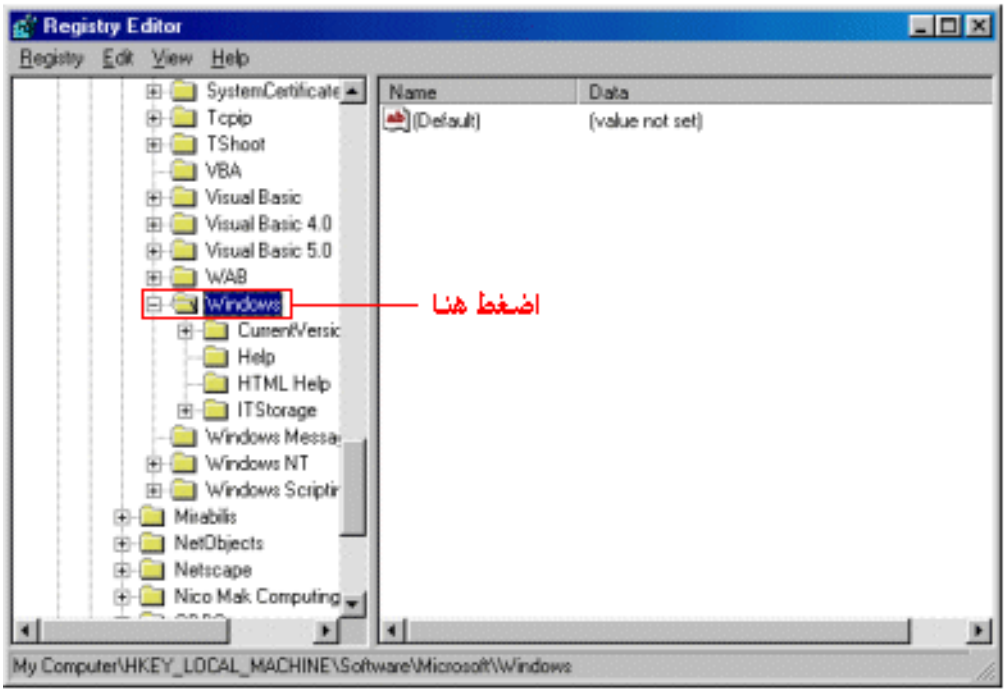
ستظهر قائمة أخرى, و باختيار Software



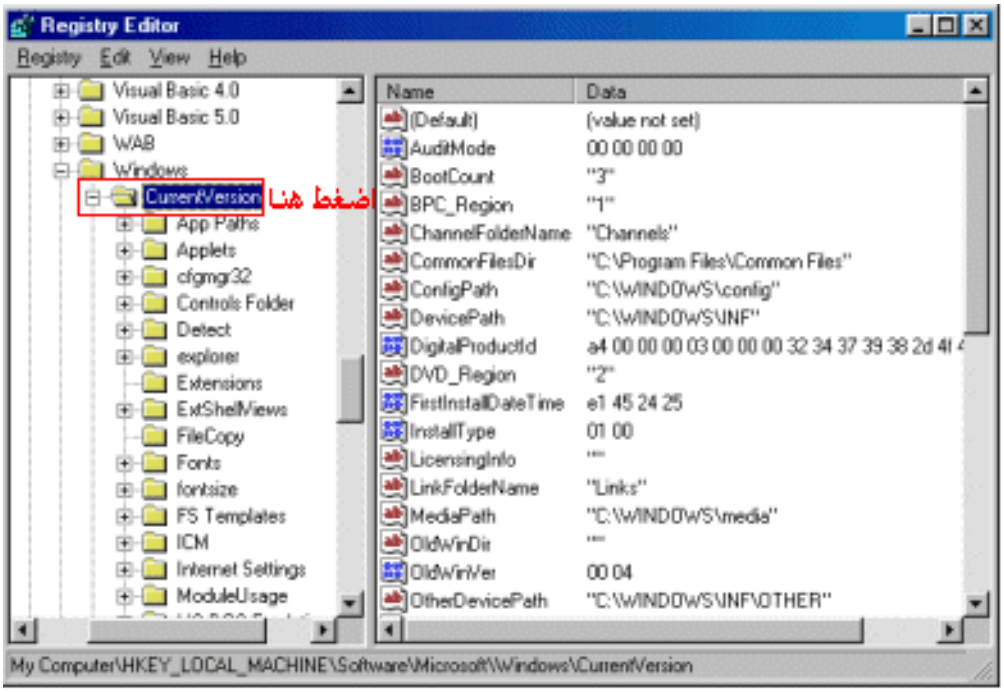
ثم الضغط على زر ال Microsoft ستظهر قائمة أخرى



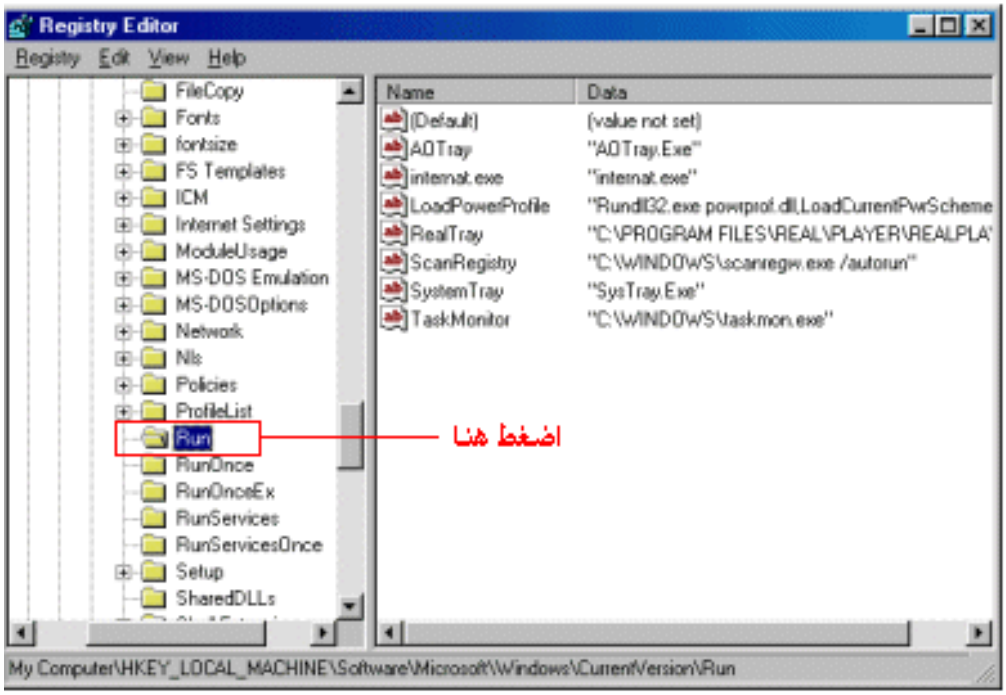
باختيارWindows



ستظهر قائمة أخرى أيضا, بعدها يتم الضغط علىCurrent Version



و أخيراً بالضغط علىRun

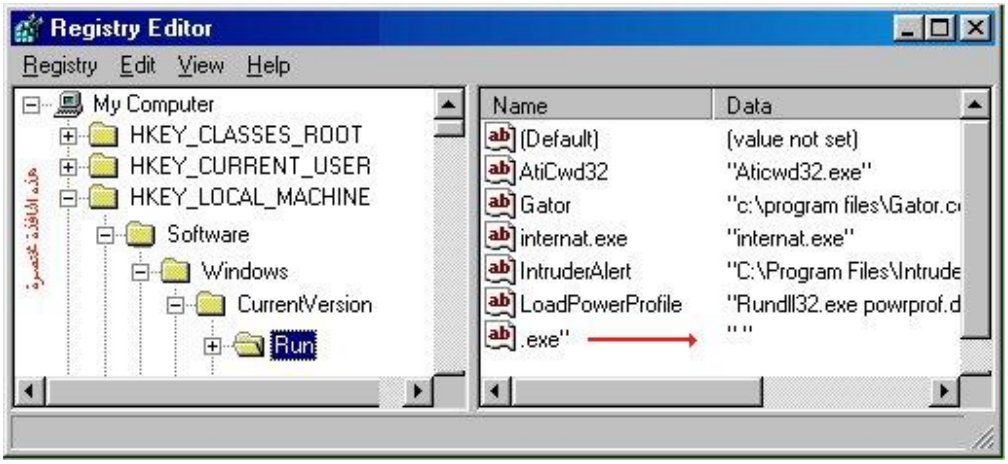


توجد قائمتان

الأولى (Name) و فيها اسم الملفات التي تعمل بقائمة بدء التشغيل للجهاز

الثانية (Data) و فيها معلومات عن الملف و امتداد ه أو البرنامج

من القائمة الثانية نستطيع معرفة ملف التجسس حيث أنه لن تكون له أي معلومات أو امتداد مثل الشكل التالي



فنقوم بحذفه من دفتر التسجيل ثم نقوم بإغلاق النافذة.

الخطوة الأخيرة تكون من خلال الذهاب إلى

Start

Restart at MS- Dos

بالذهاب إلى مكان ملف التجسس الذي غالباً ما يكون ملصوقاً بملفات النظام

C:/windows

أو

C:/windows/systemمتبوعاً باسم الملف , و بحذفه و بإعادة تشغيل الجهاز نكون قد تخلصنا من الملف.

كيف تحمي جهازك من المخترقين

كيف تحمي جهازك من المخترقين أوكد لكم أن المخترقين مزعجين وخصوصا المبتدئون منهم الذين يصرون بعض الاوقات على شيء معين حتى لو كان لا جدوى منه فترى ارقام الاي بي تتردد في برنامج الحماية كثيرا كيف امنعهم وكيف اقفل عليهم جميع الابواب حتى لا يجدون منفذ ؟؟ هذا ما سوف اشرحة في الاسفل أولا: لا بد من تنظيف الجهاز والتاكد من خلوه من جميع الملفات التي تفتح المنافذ للمخترقين كيف يتم ذلك ؟؟ ملفات التجسس دائما تقوم بتغطيه انفسها بعده طرق منها : بناء ملف جديد في نظامك تحت النظام في مجلد الويندز , تغير الاسم وهناك ما يعمل في الخلفية وبعضها ينصب على ان برنامج اعداد والكثير منها اول طريقة : من أبداء أختر تشغيل ثم قم بكتابة هذا الامر اذا كان نظامك ويندز 98 msconfig هذه الاعدادت حساسة للغاية فلا تحاول ان تخطى لانها تسبب في تلف الويندز وأن شاء الله لن يكون هناك اي تلف , واقصد بقول خطيرة لان البعض يحاول أستكشاف المنطقة غير التي نتكلم عنها مما تسبب عنها أضرار من هذه القائمة تجدون بداية التشغيل startup أختروها ثم تفحصو هذه البرامج سوف ترون انها مألوفة لديكم ولكن عندما تشاهدون بعض الاسماء الغريبة أنصحكم بأزالتها ثاني طريقة : هناك برنامج رائع يمكنكم الاعتماد عليه في ازالت جميع ملفات التجسس المخباه في النظام ولكن سوف يمسك بالبرامج ايضا التي تساعدك في الاتصال وأقصد هنا بالبرامج وهي الكلينت مثل السب سيفن والنت سفير وغيرها كونها برامج تجسس أيضا AntiViral ToolKit Pro Version 3.0البرنامج يمكنك الحصول عليه من عده مواقع مخلتفة مثل http://www.download.com وايضا دائما ما أجد هذا البرنامج في الاقراص المدمجة للمجلات كونة برنامج حماية رائع صدقوني لا يوجد برنامج يضاهيه في التعرف على الفيروسات الخاص بالتجسس بعدما تأكدنا من خلو أجهزتنا من جميع الملفات التجسسية وجلبنا برامج لتنظيف الجهاز منها بقي لنا ان نتعرف على افضل الوسائل المتاحة لحماية الاجهزة من هجمات المخترقين أولا: لا تستعمل اي من البرامج التي تلفت انتباه المخترقين لجهازك , نعم هي برامج حماية ولكن تلفت انتباه المخترقين الي جهازك وانت لا تعلم بذلك كيف ؟؟؟ عندما يظهر برنامج الحماية رقم اي بي حاول ان يخترق جهاز فأنه يعرضك للخطر في نفس الوقت ؟؟ ذكرنا من قبل في تعليم أستخدام برنامج النت سنوب ان هناك أرقام اي بي تظهر عند انتهاء العملية وتكون هذه الارقام مراقبه ببرامج حماية , ما الفائدة من برنامج الحماية اذا كان يظهرك للمخترقين ويعلمهم برقم الاي بي الخاص بك ؟؟ فمن بين كل هذه الارقام يظهر رقمك والسبب برنامج الحماية , بعض المخترقين المبتدئين لا يعرفون ما معنى العبارة التي تظهر في برنامج النت سنوب والتي ان مفادها ان هذا الرقم مراقب فيبداء بالمحاولة مرة أخرى على جميع الارقام التي ظهرت بدون أستثناء وهذا سبب تكرر محاولة الاختراق في جهازك اذا ما العمل لكي لا نلفت أنتباه هؤلا المخترقين برقم الاي بي الخاص بك ؟؟؟؟؟ هناك برنامج رائع أستطاع ان يثبت فعاليته وقد كان هذا البرنامج أختياري الاول والاخير منذ زمان والي الان Atguard الحارس : طريقة عمل هذا البرنامج رائعه جدا وعمليه في نفس الوقت , يقوم هذا البرنامج بعمل حاجز ناري في جهازك ثم يعرض لك قائمتين القائمة الاولى : وهي القائمة البيضاء والتي تضيف بها ما تريد ان تسمح لة بالمرور من هذا الجدار مثل : برنامج الشات , المتصفح , بروكسي الشركة , الاي سي كيو , عامة اي برنامج يعمل على الانترنت يكون له عنوان اي بي ومنفذ وما عليك الا الموافقة على البرامج التي تستخدمها القائمة الثانية : وهي القائمة السوداء وتضم هذه القائمة جميع البرامج الممنوعه من المرور من هذا الجدار واي برنامج جديد يحاول المخترق أستخدامة سوف يقوم البرنامج بأخبارك به ومنه تستطيع أضافته الي القائمة بكل سهوله لكي لا يزعجك بالسؤال مرة أخرى هناك اربع أختيارات عن ظهور برنامج جديد يريد التسلل من الجدار وهذه الخيارات تظهر لك أسمح له هذه المرة اسمح له للابد لا تسمح له هذه المرة لا تسمح له للابد عند أختيارك للابد فانة لن يقوم بأزعاجك مرة أخرى بالسؤال كيف ؟؟؟ فرضا لو ظهرت رساله ان رقم الاي بي يحاول الاتصال بجهازك من منفذ 12345 وهو النت بس وأخترت لا تسمح له للابد فانه في المرة الاخرى عندما يحاول اي شخص أستخدام هذا المنفذ للدخول لجهازك لن تظهر لك اي رساله كونه أضيف للقائمة السوداء , والمخترق لن يحصل على اي أشارة من جهازك وكما ان هذا الرقم غير متصل بأي جهاز ولا يعطى اي رد منك فأيهم افضل ان ترشد المخترقين لرقم الاي بي الذي يعمل علية جهازك ام تفضل الهدوء ؟؟ انا أصور المخترق وهو يحاول يخترق جهاز يمتلك هذا البرنامج كا شخص بداخل عازل للصوت لا يسمع الذي ينادية بالخارج ولا يستطيع ان يراه فكل من الاثنين لا يستطعون التواصل موقع هذا البرنامج هو http://www.atguard.com أنتهى

ما هو التروجان و كيف تتخلص منه

ما هو التروجان ؟؟

تعريف:

التروجان هو برنامج تجسس و له أسماء أخرى مثل مخدم (Server) أو اللاصق (Patch) أو الجاسوس (Spy) لكن مبدعين هذا النوع من الملفات يفضلون الأسماء الرنانة و اسم تروجان هو نسبة إلى حصان طروادة. لكن مع اختلاف المسميات فهو برنامج تجسسي يجعل من حاسبك مخدم لحاسب الجاسوس, أي يتمكن الجاسوس (و هو الشخص الذي بعث إليك هذا التروجان) من التحكم بجهازك و كأنه أنت, لكن مع الأخذ بعين الاعتبار أن ذلك فقط في حال أنت متصل بالإنترنت أو الشبكة و ليس هذا فقط بل و عندما يعرف أنك على الإنترنت أما غير ذلك فهو لا حول له ولا قوة.

كيف يلج إلى التروجان إلى حاسبي:

1- عن طريق برامج المحادثة مثل Microsoft chat و ICQ و Mirc و MSN و Yahoo .. الخ.

فلا تستقبل أي ملف مهما يكن و خاصة التي يكون امتدادها exe و حالياً ظهرت برامج تقوم بتغير امتداد الصور إلى exe فبعض الهاكرز يستخدمها في الضحك على الضحايا و يقول لهم أنها صور مغير امتدادها إلى exe و لكنه قد يدس التروجان بداخلها أو قد تكون هي التروجان بحالها.

2- عن طريق البريد الالكتروني:

لذا قم بحذف جميع الرسائل المجهولة و التي لا تعرف من هو مرسلها.

3- عن طريق تحميل برامج من مواقع مشبوهة:

الحل : أن تفعل خاصية الحماية التلقائية لبرنامج Norton Antivirus و الذي هو أقوى برامج الحماية على الإطلاق لأنه يتعامل مع الفيروسات و برامج التجسس على حد سواء.

4- عن طريق المنتديات التي تفعّل خاصية html قد يأتي من هو حاقد على المنتدى و يزرع الكود في رد لموضوع أو في موضوع جديد.

الحل : بسيط جداً لأنه ليس من مسؤوليتك بل من مسؤولية مشرف الموقع.

5- عن طريق الماسنجر بأنواعها هناك برنامج جديد و لكني لا اعلم مدى مصداقية كاتبه و هو يقوم بعمل سرقة الملفات و الصور من جهاز الطرف الآخر إذا كان online و من دون إذنه و اسم البرنامج imesh .

الحل : لا تضيف إلا من تعرفهم و إذا صادفت أي شخص لا تعرفه و شكيت فيه فقم بعمل حظر ثم حذف, لكن إذا كان في جهازك تروجان و حظرته فسوف يدخل و أنت لا تعلم لأن الحظر لن يفيد ما دام الخادم في جهازك يستقبل أوامر العملاء, و أنا لي وقفة بسيطة حول هذا البرنامج قد يكون هذا البرنامج مثل أخواتها من التروجانات .. قد تسمح لمصمم البرنامج أن يتجسس عليك و أنت تحاول أن تتجسس على الآخرين عملاً بشعار افتراس المفترس و هذا هو حال كثير من برامج التجسس.

كيف أتخلص من التروجان إذا أصاب جهازي:

قبل كل شيء يجب أن تعرف أن الملف التجسسي إذا أصاب جهازك فإنه سوف يستوطن في واحد على الأقل من الأماكن التالية:

1- في الريجستري .

2- في الملف Startup .

3- في الملف System.ini .

4- في الملف Win.ini .

أما للتخلص منه فإليك الطريقة..

هناك طريقتين لحذف التروجان و هي مجربة على ويندوز 98 و هي إما بواسطة برامج الحماية و هذه هي الطريقة الأوتوماتيكية, أو الطريقة اليدوية عن طريق DOS و هي الأفضل و الأقوى من خلال التجارب مع Trojans إذا عملت بحث بواسطة برامج الحماية و صدف إنه في بعض الأحيان لا يمكن حذف التروجان بواسطة برامج الحماية لأن التروجان قد يحذف معه ملف مهم من ملفات النظام و في هذه الحالة تضطر إلى استخدام الطريقة الأخرى و هي الأفضل و الأسلم و هي كالتالي:

لنفرض أن التروجان اسمه Server تمكن من معرفته برنامج الحماية, أول خطوة و هي أن تتأكد هل هو يشتغل مع تشغيل الجهاز و ذلك بفعل التالي:

اضغط على زر start

اختر run

اكتب: msconfig

ثم اختر Start UP و من هناك ابحث عن اسم التروجان و غالباً ما يكون اسمه على الاسم الذي تم كشفه, ثم إذا وجدته أزل علامة الصح من أمامه ثم اعد تشغيل الجهاز. يمكنك مراجعة الطرق الاخرى بالضغط على هذه الوصلة

الخطوة الثانية و هي أن تحاول أن تجمع اكبر قدر من المعلومات عن التروجان الذي تم اكتشفاه حتى تتعرف عن أماكن اختبائه في الجهاز و عن تسجيل نفسه في الريجستري أو Win.ini أو System.ini أو جميعها معاً, و أفضل ثلاث مواقع يقدم لك الاستفسار الكامل عن أي تروجان هم

http://www.dark-e.com/archive/trojans/

http://www.google.com/

http://www.moosoft.com/tdbindex.php

الخطوة الثالثة بعد إعادة التشغيل ينبغي أن تكتب اسم التروجان كامل في ورقة خارجية ثم تذهب إلى الدوس عن طريق إعادة التشغيل و اضغط على Ctrl أو F8 أو استخدام قرص الإقلاع اختار Ms-Dos prompt في حال كنت تستخدم Win ME أو عن طريق الدوس الخارجة عن نطاق الويندوز و هي من ابدأ ثم إيقاف التشغيل ثم اختر الرجوع إلى بيئة الدوسRESTART IN MS-DOS MODE و ذلك في حال أنك تستخدم Win 98 ثم اتبع هذه الطريقة لكي تبحث عن التروجان و انتبه إلى المسافة بين الأمر dir و بين اسم التروجان و لا تنسى النجوم *.* :

C:/Windows>dir server *.*

ثم إنتر و إذا وجدت أي ملف اسمه server و امتداده الأخير هو exe فهو مطلبك و عليك أن تحذفه بهذه الطريقة و انتبه إلى المسافة بين deltree و بين اسم التروجان ولا تنسى النجوم *.* :

C:/Windows>Deltree server *.*

ثم إنتر ثم راح تسأل سؤال ضع علامة Y و قد يكون هناك أكثر من برنامج يحمل نفس الاسم و لكن الامتداد يختلف.. أهم شيء انك تبحث عن اسم التروجان server و الذي يكون امتداده exe هذه هي الطريقة اليدوية و الفعالة في حذف التروجان من الجهاز طبعاً تضع بدل من كلمة server الاسم الذي تم رصده من مكافحات التجسس.. ثم اعد تشغيل الجهاز.

ملاحظه مهمة جداً:

هناك أمر أخر للحذف و هو Del و لكني أفضل الأمر Deltree لأنه اشمل في الحذف و يقوم بحذف كل شيء مخفي من اثر التروجان و يتعقبه في كل الأدلة و ليس مثل الأمر Del و الآن نحن في الويندوز و بعدما تم حذف التروجان و بقي أن نزيل بعض من آثاره منwin.ini أو system.ini أو الريجستري. طبعاً بعدما تدخل إلى إحدى المواقع اللي فوق و بعدما تبحث عن اسم التروجان الذي تريده أن تعرفه عنه, و كان تروجانك هو server و حصلت على هذه المعلومات من المواقع السابقة و هي انه من فصيلةSub 7 و أهم شيء من المعلومات هذه من القسم How To Remove و عليك أن تتبع مسار التروجان في مكانه.. و بعد التمحيص عن التروجان وجدناه يسجل نفسه في الريجستري, اذهب إلى المفتاح التالي

HKET_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion

و ابحث عن الأسماء التالية RunDLL32r, EXPLO32, SERVER.EXEC, Explorer32, WINDOWS\EXPL32.EXE, في المفتاحين Run و RunServices و لاحظ على الملفات جيداً فإن لم يقابلها Data أو يظهر أمامها سهم صغير à فهو ملف تجسس إذ ليس له عنوان معيين في الويندوز, و عندما تجد احد تلك الملفات قم بحذفه, و بعدين تسوي إعادة تشغيل, و الآن عليك البحث في الملفين Win.ini و System.ini و اللذين تشغلهما من Run ثم اختر الملف System.ini و ابحث في قسم الـBoot عن أي اسم غريب تحت هذا السطر shell=Explorer.exe ثم أزل منه الصح لكن تحقق من انه تروجان و هكذا. بعض التروجانات قد تحذف معها ملفات مهمة من الجهاز و في هذه الحالة يتطلب منك إرجاعها و طريقة الاسترجاع كالتالي:

في تشغيل Run اكتب SFC ثم إنتر ثم اختر الإعدادات Settings ثم في آخر شيء ضع علامة صح تفقد الملفات المحذوفة Check for deleted files ثم اختر موافق و بعدها اختر Start و اترك البرنامج يقوم بعمل فحص للملفات قد يكون هناك ملف محذوف و يتطلب رجوعه بواسطة ..CD طبعاً على حسب نوع النظام اللي عندك يعني إذا عندك نظام 98 لازم قرص 98 و هكذا إذا وجد ملف محذوف يطلب القرص و أكمل بعدها إجراءات استرجاعه.

كيف أتأكد من وجود اتصال بجهازي

. كيف أتأكد من وجود أي اتصال تام مع جهازي ؟؟

- للاتصال بين جهازين لابد من توفر برنامج لكل من الجهازين و يوجد نوعان من البرامج ففي الجهاز

المستهدف (قد يكون جهازك) يوجد برنامج الخادم server و في الجهاز الآخر يوجد برنامج الزبون client و من خلالهما يتم تبادل المعلومات حسب قوة البرنامج الذي بإمكانه الإطلاع على جميع البيانات الموجودة في جهازك و التحكم بنظام التشغيل لديك إلى درجة أن بعضها يمكن أن يفتح سواقة القرص الليزري و يقفلها أو عرض جميع ملفاتك و سحب أو إلغاء أو إضافة.

أما لمعرفة وجود اتصال فالأمر سهل جداً كل ما عليك انه في حاله التأكد من عدم اتصال أي جهاز آخر مع جهازك أن تتجه إلى الدوس و تكتب الأمر الآتي :

C:\Windows\netstat –n

و معناه البحث عن الاتصال بالأرقام عندها سوف تظهر لك شاشه تأخذ ثواني لإعطائك النتيجة و سوف تكون على النحو الآتي :

Proto Local Address Foreign Address State

كل ما يهمنا في الأمر هو الـ Foreign Address و State و سوف تجد في هذا الأمر أرقام مقدم الخدمة لك مع رقم المنفذ port و هنا يجب أن تنتبه لأن الحالة تكون كالآتي:

Foreign Address State

212.123.234.200:8080 Established

أي أن الأرقام 212.123.234.200 هي أرقام مقدم الخدمة ثم تأتي بعدها نقطتين فوق بعض و يأتي بعدها رقم المنفذ و هو 8080 و هذا وضع طبيعي جداً, ثم تأتي كلمة state أي حالة الاتصال و تحتها كلمة Established أي الاتصال تام, و هذا أيضا طبيعي المهم في الأمر إن وجدت رقمIP غريب و تتأكد من ذلك برقم المنفذ و هو الذي يأتي بعد النقطتين التي فوق بعض, مثال :

Foreign Address State

212.100.97.50:12345 Established

انظر إلى رقم الـIP و رقم المنفذ, رقم الـ IP غريب و رقم المنفذ كذلك, إذاً فهو في الغالب منفذ لبرنامج تجسس, و حاله الاتصال تام مع جهازك أي انه بالفعل يوجد شخص الآن داخل جهازك يتجسس عليك. اكتب رقم المنفذ و هو 12345 ثم اتجه إلى قائمة المنافذ الموجودة في الموقع تحت عنوان أرقام البورتات المستخدمة في برامج التجسس و ابحث عن اسم البرنامج لكي تعرف الملف المصاب به جهازك لتنظيفه

- ثمة طريقة أخرى تختلف قليلاً عن الأولى. اذهب إلى موجه الدوس و اكتب الأمر التالي: netstat –a ثم enter و انتظر قليلاً وسوف ترا جميع المنافذ المفتوحة و هي التي تلي الرمز (:) ما قبل الرمز فهو اسم الكمبيوتر الخاص بك الذي تم تعريفه عند تجهيز شبكة الاتصال. و ضمنها سوف تشاهد الIP الخاص بك و إذا رأيت غير الIP الخاص بك من الممكن ان يدل أن هاكر اخترق جهازك .

المهم قبل ان تكمل يجب ان تغلق جميع المواقع التي تتصفحها لكي لا يعطيكIP المواقع و يخطر على بالك انه هاكرز. المهم ستجد IP واحد هوIP الخاص بك واذا وجدت أكثر منIP احتمال كبير يكون لمخترق, خاصة بعد ان تأكدت انك لا تقوم بتشغيل برنامج محادثة او ليست هناك وسيلة اتصال بين جهازك و بين جهاز اخر على النت, فوجود اتصال آخر غير الذي تعرفه يثير الشك و احتمالية ان يكون لمخترق كبيرة جداً.

ملفات التجسس النصية

الموضوع الذي أريد التحدث فيه يختص بأمن نظام التشغيل, أثناء زيارتي لأحد مواقع البحث، قام هذا الموقع بالوصول إلى المتصفح الذي على جهازي (والذي كباقي المتصفحات على الأجهزة العربية مليء بالثغرات)؛ وقام بتغيير الصفحة الرئيسية (Home Page), وباءت كل المحاولات بالفشل لتغيير الصفحة الرئيسية (Home Page). فقررت أن أقوم بإعادة تنصيب نظام التشغيل. ولكن الأنكى والأمرّ أنني عدت إلى ذلك الموقع بالخطأ فقررت البحث عن حل جدي للمشكلة .

قُمت بحذف جميع الملفات المؤقتة للانترنت(Temporary Internet Files) وتدمير جميع (Cookies) وبقيت المشكلة على حالها, كل دقيقة يتم تغيير الصفحة الرئيسية (Home Page) ورغم إعادة إقلاع الجهاز مرات كثيرة لم تفلح أياً من الطرق في إيقاف هذه الحالة.

رفعت مستوى الأمان. أزلت الإنترنت إكسبلورر (Internet Explorer). أوقفت سكريبت (Script) بجميع أنواعها ولم تتوقف المشكلة.
بعد عملية بحث على الانترنت اكتشفت الحل :
الذي على جهازي برنامج تجسس كُتب بوساطة الجافا سكريبت (Java Script). و هذا البرنامج يحقن الريجستري (Registry) بالكثير من المفاتيح التي تقوم بتوليد الكود مرة أخرى بعد حذف ملفات الإنترنت المؤقتة (Temporary Internet Files) و لحذف هذا البرنامج نتبع ما يلي:

1- اذهب إلى الموقعhttp://www.lavasoft.de و قم بتحميل البرنامج Ad-aware 6.0 فهو مجاني و لا تنسى أن تقوم بعمل ترقية فلم استطع أن احذف البرنامج حتى قمت بالترقية.
2- قم بتغير إعدادات البرنامج إلى ما يلي:
1) الصورة

2) الصورة 2

3- قم بعد ذلك بتغير أعدادات الأمان (Security tab) في انترنت إكسبلورر إلى ما يلي :

1) Download unsigned ActiveX controls – *Disable*
2) Initialize and script ActiveX controls not marked as safe – *Disable*
3) File download – *Disable*
4) Font download – *Disable*
5) Java Permissions – *High safety*
6) Access data sources across domains – Disable
7) Installation of desktop items – *Prompt*
8) Software channel permissions – *High*
9) Allow paste operations via script – *Disable*

4- و من قائمة إعدادات متقدمة (Advanced tab)غير إلى:

1) Check for publisher's certificate revocation.
2) Check for server certificate revocation.
3) Warn about invalid site certificates.
4) Warn if forms submittal is being redirected.

5- بعد ذلك اذهب إلى موقع http://www.zonelabs.com و قم بتحميل ZoneAlarm Pro و ذلك لمنع دخول مثل هذه الملفات على جهازك.

6- بقي أخيراً احتجت لتنصيب Norton AntiVirus 2003 Professional Edition حتى تمكنت من التقاط ملف الجافا سكريبت (Java Script).

تعرف على الفيروسات

ماهي الفيروسات؟

فيروسات الكومبيوتر هي برامج تتم كتابتها بغرض إلحاق الضرر بكومبيوتر آخر، أو السيطرة عليه، تمت كتابتها بطريقة معينة. سُمّيت بالفيروسات، لأنها تشبه تلك الكائنات المتطفلة في صفتين رئيسيتين:

- **تحتاج فيروسات الكومبيوتر دائماً إلى ملف عائل تعيش متستّرةً فيه:**
فالفيروسات، دائماً تتستر خلف ملف آخر، و لكنها تأخذ زمام السيطرة على البرنامج المصاب. بحيث أنه حين يتم تشغيل البرنامج المصاب، يتم تشغيل الفيروس أولاً.

- **تستطيع فيروسات الكومبيوتر أن تنسخ نفسها:**
تتم كتابة هذه البرامج المؤذية بحيث تقوم بنسخ نفسها فوراً بمجرّدتشغيل البرنامج المصاب. و هي تنسخ نفسها للأقراص الأخرى، فإذا كان الكومبيوتر مصاباً ووضعت فيه قرصاً مرناً، يتم نسخ الفيروس اوتوماتيكياً للقرص المرن. و نظراً لهذه الخاصية في الفيروسات، تجد أن القرص المصاب يعطيك علامة أنه ممتلئ تماماً برغم أنك لم تقم بتخزين غير ملفات ذات حجم صغير.

ما الفرق بين الدودة و التروجان و الفيروس؟

- **الدودة:** تصيب الدودة الكمبيوترات الموصلة بالشبكة بشكل اوتوماتيكي و من غير تدخل الانسان و هذا الامر يجعلها تنتشر بشكل اوسع و اسرع عن الفيروسات . الفرق بينهم هو ان الديدان لا تقوم بحذف او تغيير الملفات بل تقوم بتهليك موارد الجهاز و استخدام الذاكرة بشكل فظيع مما يؤدي الى بطء ملحوظ جدا للجهاز , و من المهم تحديث نسخ النظام المستخدم في الجهاز كي يتم تجنب الديدان.

  ومن المهم عند الحديث عن الديدان الإشارة إلى تلك التي تنتشر عن طريق الإيميل. حيث يرفق بالرسالة ملفاً يحتوي على دودة، و عندما يشغّل المرسل إليه الملف المرفق، تقوم الدودة بنشر نفسها إلى جميع الإيميلات الموجودة في دفتر عناوين الضحية.

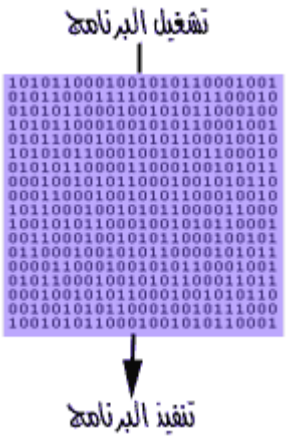
- **التروجان:** وهو عبارة عن برنامج يغري المستخدم باهميته او بشكله او باسمه ان كان جذاباً, و في الواقع هو برنامج يقوم بفتح باب خلفي ان صح التعبير بمجرد تشغيله , و من خلال هذا الباب الخلفي يقوم المخترق باختراق الجهاز و بامكانه التحكم بالجهاز بشكل كبير حتى في بعض الاحيان يستطيع القيام بامور , صاحب الجهاز نفسه لا يستطيع القيام بها , و هذا لا يرجع لملف التروجان, لكن ملف التروجان هو الذي فتح للمخترق الباب ان صح التعبير بتشغيله اياه.

- **الفيروس:** كما ذكرنا , الفيروس عبارة عن برنامج صمم لينشر نفسه بين الملفات و يندمج او يلتصق بالبرامج. عند تشغيل البرنامج المصاب فانه قد يصيب باقي الملفات الموجودة معه في القرص الصلب او المرن, لذا الفيروس يحتاج الى تدخل من جانب المستخدم كي ينتشر , بطبيعة الحال التدخل عبارة عن تشغيله بعد ان تم جلبه من الايميل او تنزيله من الانترنت او من خلال تبادل الاقراص المرنة.

كيف تعمل الفيروسات؟

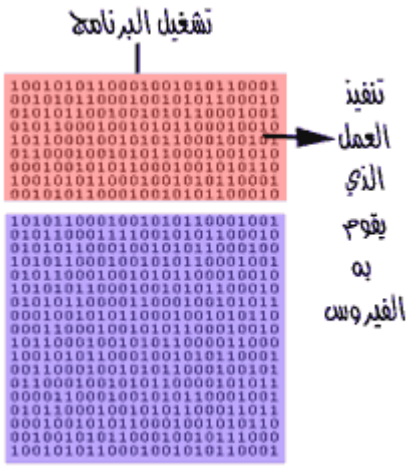
في الواقع يقوم الفيروس في حالة إصابة الملف بإضافة نفسه في بداية أو نهاية الملف المصاب، دون أن

يقوم فعلياً بأي تغيير في مكوّنات الملف الأصلية. لننظر للصورة التالية التي توضّح شكل البرنامج غير المصاب بفيروس:

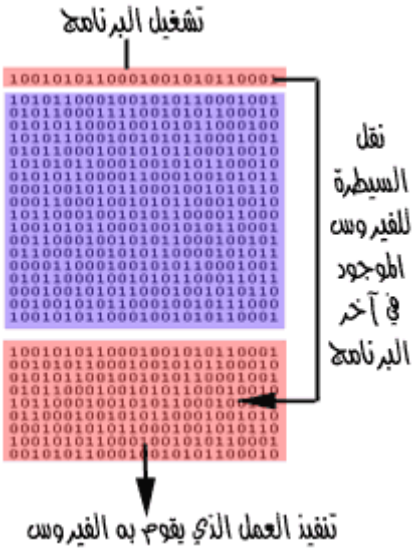


نلاحظ أنه عند استدعاء البرنامج فإنه يعمل بشكل طبيعي.

والآن لنتصوّر أنه تم اصابة البرنامج بفيروس. في الواقع يقوم الفيروس بلصق نفسه في البرنامج كما أسلفنا دون أن يغير في محتويات الملف شيئاً. و طريقة اللصق تكون، إما أنه يقوم بلصق نفسه في بداية البرنامج، بحيث يتم تشغيله هو قبل البرنامج نفسه:



وقد تكون طريقة التحاق الفيروس بالملف بأن يضع نفسه في نهاية البرنامج المصاب. و يضع علامة في بدايته، هكذا:



إن هذا الفيروس، يختبئ في نهاية الملف المصاب، و يضع في مقدّمة البرنامج مؤشّراً بحيث أنه عندما يتم استدعاء البرنامج و تشغيله، يحوّل السيطرة للفيروس بدلاً من تشغيل البرنامج.

وفي الحالتين قد يعود الفيروس بعد الانتهاء من تنفيذ عمله المؤذي لتشغيل البرنامج، و لكنه قد لا يعود أيضاً. و يسبب أضراراً جسيمة للجهاز.

أنواع الفيروسات:

هناك الآف من الفيروسات المنتشرة عبر الانترنت , لكن اغلبها ما يقع تحت هذه النقاط الستة:

1. **فيروسات بدء التشغيل اوBoot Sector Virus**
هذا النوع من الفيروسات يصيب قطاع الاقلاع في الجهاز , و هو المكان المخصص الذي يتجه اليه الكمبيوتر في بداية تشغيل الجهاز. و هذا النوع من الفيروسات قد يمنع المستخدم من الوصول الى النظام ويمنعه من اقلاع الجهاز.

2. **فيروس الملفات اوFile Virus**
يصيب البرامج عادة , و ينتشر بين الملفات الاخرى و البرامج الاخرى عند تشغيله.

3. **فيروس الماكرو اوMacro Virus**
هذه الفيروسات تصيب برامج الميكروسوفت اوفيس مثل الوورد و الاكسل, و تعتبر ذات انتشار واسع جدا تقدر ب 75% من عدد الفيروسات الموجودة. يقوم هذا النوع من الفيروسات بتغيير بعض المستندات الموجودة في القرص الصلب و خصوصا الوورد , قد تجد بعض التصرفات الغير منطقية في بعض الاحيان مثل طلب باسوورد لفتح ملف تعرف انك لم تضع عليه باسوورد , و ايضا تجد بعض الكلمات قد تغير مكانها و اضيفت كلمات جديدة لا علاقة لها بالموضوع . هي اساساً ليست ضارة, لكنها مزعجة نوعاً ما و قد تكون مدمرة احيانا!

4. **الفيروس المتعدد الاجزاء او Multipartite Virus**
و هو الذي يقوم باصابة الملفات مع قطاع الاقلاع في نفس الوقت و يكون مدمراً في كثير من الاحيان اذا لم تتم الوقاية منه.

5. **الفيروس المتطور اوPolymorphic Virus**
هي فيروسات متطورة نوعا ما حيث انها تغير الشفرة كلما انتقلت من جهاز الى آخر. نظريا,

يصعب على مضادات الفيروسات التخلص منها لكن عمليا و مع تطور المضادات فالخطر اصبح غير مخيف.

6. **الفيروس المختفي او Stealth Virus**

تخفي نفسها بان تجعل الملف المصاب سليما و تخدع مضادات الفيروسات بان الملف سليم و ليس مصاباً بفيروس. مع تطور مضادات الفيروسات اصبح من السهل كشف هذا النوع.

ماهي العلامات الشائعة لوجود فيروس في الجهاز:

- بطء الجهاز الشديد، بما لا يتناسب مع عدد البرامج التي تعمل في نفس الوقت.
- امتلاء القرص بما لا يتناسب مع عدد و حجم الملفات الموجودة عليه.
- ظهور مربّعات حوار غريبة اثناء العمل على الجهاز.
- اضاءة لمبة القرص الصلب أو القرص المرن، دون أن تقوم بعملية فتح أو حفظ ملف.

لابد أن تعرف أن هذه العلامات لا تعني بالضرورة وجود فيروس، فقد يكون بعضها بسبب مشكلة في عتاد الجهاز مثلاً.

كيف نحمي أنفسنا من الفيروسات ؟

للحيطة و الحذر من الفيروسات-خاصة إذا كنت معتاداً على تبادل الأقراص المرنة، أو الملفات عبر الانترنت- لابد من اتخاذ الخطوات التالية:

- لابد من موجود برنامج حماية من الفيروسات في جهازك.
- لابد أن تقوم بتحديثه بشكل دوري، وإلا فلا فائدة من وجوده.
- لا تقم بفتح المرفقات في أي إيميل لا تعرف مرسله.
- لا تقم بفتح المرفقات في إيميلات أصدقائك إذا وجدتها تنتهي بـ exe أو bat أو أي امتداد لا تعرفه.
- لا تقبل ملف من شخص لا تعرفه أبداً.
- إذا قبلت ملفاً من شخص تعرفه، افحصه أيضاً ببرنامج الحماية، فقد يكون صديقك نفسه ضحية.
- احرص على فحص جميع البرامج التي تقوم بتنزيلها من الإنترنت، أو تشغيلها من قرص مرن أو سي دي. قبل أن تشغّلها.

داوم على زيارة المواقع التي تهتم بالحماية
من الفيروسات، للإطلاع على كل ما هو جديد في هذا المجال، و لاتخاذ الحيطة، فدرهم وقاية خيرٌ من قنطار علاج.

معلومات عامة عن برامج الحماية من الفيروسات

كما أسلفنا لابد من وجود برنامج الحماية من الفيروسات في الجهاز. ويقوم البرنامج بفحص و تدقيق الملفات و حماية الجهاز كما ينبغي. وهو يقوم بهذا العمل عن طريق البحض عن بصمات الفيروسات. فلكل فيروس بصمة عبارة عن رقم محدد. و برنامج الحماية في الواقع يبحث عن هذه البصمة المحددة فإن وجدها فإنه يعلن عن وجود الفيروس. وهو اذ يقوم بذلك يقارن بين الملفات و بين جدول لبصمات الفيروسات المختلفة.

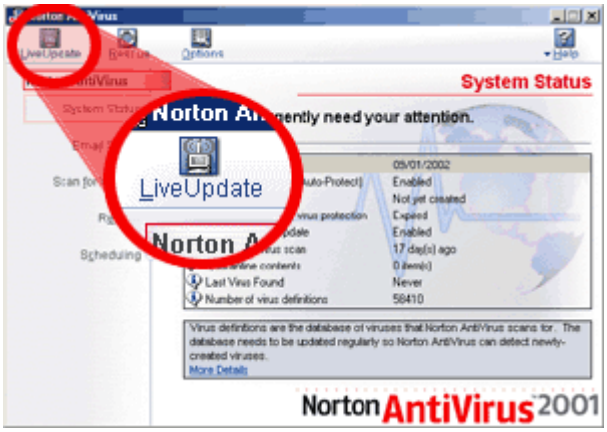
إن الكثير من الفيروسات تتم كتابتها و نشرها في الأسبوع الواحد و هكذا ترى أنه من المهم جداً أن

يكون هذا الجدول محدّثاً باستمرار. لذا فإن وجود برنامج الحماية نفسه ليس كافياً أبداً. بل لابد من تحديثه باستمرار.

بعض برامج الحماية من الفيروسات، تقوم بالحماية من التروجانز و الوورمز أيضاً، و لكن هناك بعض البرامج المتخصصة في مجال الحماية من الاختراق، التي تعمل بمساندة برامج المكافحة لحماية جهازك من أي ضرر.

لعل أشهر برامج مكافحة الفيروسات (أو الحماية من الفيروسات) اثنين، هما برنامج Norton للحماية من الفيروسات، http://www.norton.com و برنامج McAffee للحماية من الفيروسات:
http://www.mcaffee.comوهذا الموقع يوفّر خدمة الفحص عبر الانترنت مقابل سعر معقول.

و في كلا البرنامجين ستجد رزّا واضحاً في النافذة الرئيسية لتحديث قائمة الفيروسات. فمثلاً في النورتون ستجده في الشكل التالي:



فلا تنسَ القيام بتحديث قائمة الفيروسات بشكل دوري(-:

مواقع مفيدة:

مواقع توفّر معلومات عن الفيروسات:

- موقع يقدّم أحدث المعلومات عن الفيروسات مع ملفات التخلّص منها من مكافي
- تعرّف على الفيروسات و طرق الوقاية منها
- Introduction to viruses
- How Computer Viruses Work

مواقع برامج الحماية من الفيروسات:

- McAfee's Virus Information Library
- SARC: Symantec AntiVirus Research Center
- http://www.antivirus.com

يقدم هذا الموقع إمكانية كشف الفيروسات مجاناً مباشرة عبر النت، و لكن لابد من معرفة أن هذه العملية تعني أنّك تعطي الموقع إمكانية حذف الملفات في جهازك، فإذا شئت فقم بها على مسؤوليتك الخاصة.

)إذا ان لديك برنامج لمكافحة الفيروسات، و أردت أن توصي بأن نضع موقعه في هذه القائمة، فراسلنا من فضلك :-) (

ملاحظات مهمّة:

- تتم اصابة جهازك أو قرصك بفيروس فقط حين تقوم بتشغيل برنامج مصاب.
- يمكن لأي قرص أن يصاب بفيروس الـ boot sector.
- مجرّد وجودك في الانترنت لا يعرّضك للاصابة بفيروس. و لكنك تصاب به فقط إذا قمت بتنزيل برنامجاً مصاباً من الانترنت و قمت بتشغيله.
- لابد أن تحرص على استخدام نسخاً قانونية و مسجّلة من البرامج.
- لابد أن تقوم بعمل باك أب لملفاتك المهمة بشكل دوري و ذلك لاسترجاعها في حالة فقدانها لأي سبب تقني أو تعرّضك لفيروس.
- لابد أن يكون في جهازك برنامجاً للحماية من الفيروسات، و لابد أن تقوم بتحديثه بشكل وري.
- لابد أن تقوم بفحص جميع البرامج التي تنوي تشغيلها، و كذلك جميع الأقراص التي تقوم شرائها قبل أن تشغّلها.

غلق البوابات الخلفية للفيروسات داخل نظام تشغيل ويندوز

نظام تشغيل النوافذ به بعض البوابات الخلفية التي يمكن أن تخترقها الفيروسات من هذه الأبواب تقنية تسمى Windows Scripting Host ويطلق عليها اختصارا WSH فإذا لم تسمع عنها من قبل فيجب أن تقرأ هذا الموضوع بعناية .

الفيروسات الشهيرة مثل فيروس الحب I Love You وفيروس الحب الجديد New Love استغلت هذا الباب لكي تقتحم حاسبات ملاين المستخدمين وتصيبها بأعطال خطيرة .

تقنية WHS تستخدم لكي تسمح لصفحات مواقع الإنترنت بأن تقوم بتشغيل برامج على حاسبات المستخدمين بدون تداخل منهم ومادام قد تم السماح بهذه الخصية فيمكن لصفحات الإنترنت التي تحمل فيروسات أن يتم تشغيلها على الحاسب بنفس الطريقة التي يتم بها تشغيل البرنامج العادي . خاصية WSH اختيارية ويمكن للمستخدم أن يلغيها وبذلك يحمى نفسه من الباب الخلفي لدخول الفيروسات ولكن ليست كل وجود هذا التقنية سيئة فهي لم تخترع لكي تصيب حاسباتنا بالفيروسات ولكن لها فوائد أخرى متعددة ولذلك علينا أن نقارن بين فوائدها وعيوبها وبعد ذلك نقرر هل من الأفضل إلغاؤها أم تركها.

ميزات إلغاء WHS

إلغاء هذه الخصية سيمنع صفحات الإنترنت التي تحمل فيروسات مثل فيروس الحب من العمل . وبذلك لن تتمكن من إلحاق الضرر بحاسبك . وبذلك تصبح ملفاتك في مأمن من الإصابة بهذه الفيروسات الخطيرة . أيضا لن يقوم حاسبك بإرسال نسخة من الفيروسات لحاسبات أصدقائك الذي تراسلهم عن طريق البريد الإلكتروني .

إلغاء هذه التقنية ليس له تأثير سريع ومباشر على حاسباتنا فالحاسب سيستمر في العمل بطريقة طبيعية .

برامج المجموعة المكتبية office وبرنامج الاكسبلور لتصفح الإنترنت لا تستخدم هذه التقنية ولذا فان إلغاء هذه الخصية لا يؤثر على استخدام هذه البرامج.

عيوب إلغاء WHS

بعض البرامج الأخرى غير التي ذكرت قد تستخدم هذه الخصية ولو قمنا بإلغائها فقد يؤثر ذلك على الطريقة التي تعمل بها هذه البرامج وللأسف لا توجد طريقة تخبرنا عن هذه البرامج والتطبيقات التي توجد على الحاسب .ولكن يمكنا القول أن أغلبية البرامج لا تستخدمها .

خطوات إيقاف هذه الخاصية:-

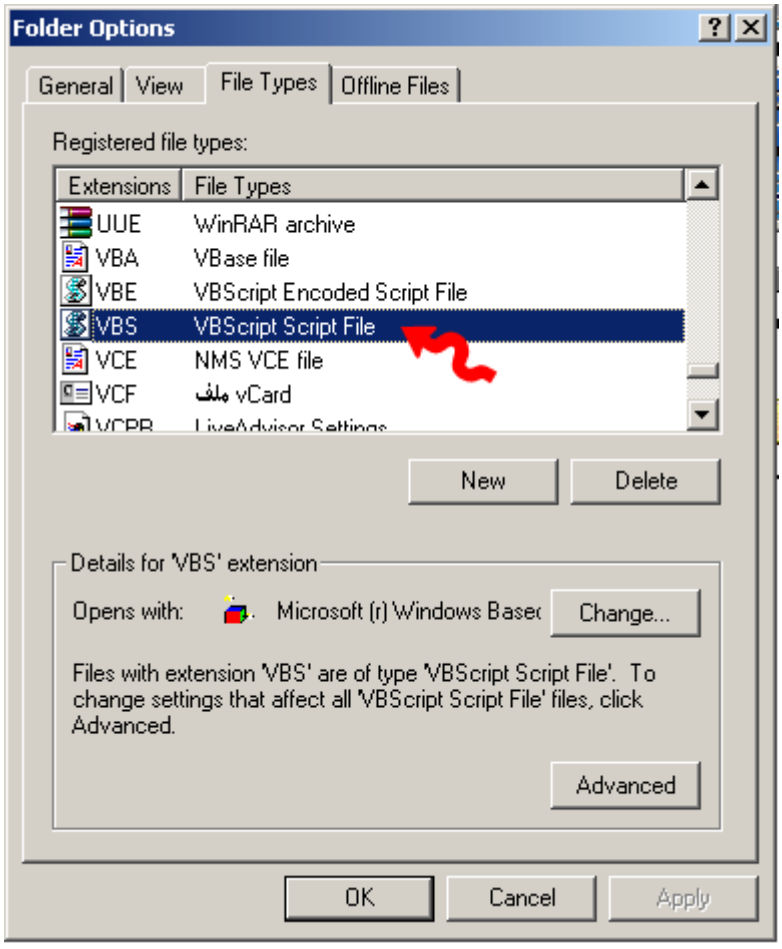
نظام نوافذ 98

- من قائمة البداية اضغط على settings

- اختار التعامل مع لوحة التحكم control panel
- افتح أيقونة Add/remove Programs
- اختار التعامل مع وظيفة windows Setup
- اضغط على مجموعة accessories ثم اضغط على مفتاح details
- الغ العلامة الموضوعة أمام خاصية windows Scripting Host
- اضغط مفتاح ok لتأكيد الاختيار.

نظام نوافذ 2000

- افتح أيقونة حاسبك myComputer والتي توجد على شاشة سطح المكتب.
- من قائمة الأدوات tools اضغط على اختيارات المجلدات folder Option
- اضغط على وظيفة أنواع الملفات File Types .
- ابحث عن VBScript Script File وقم بإلغائه
- اضغط ok لتأكيد الاختيار.



كيف تتخلص من الفيروس html.redlof.a. او folder.htt يدوياً

ما اكتبه هنا هو عبارة عن تجربة مريرة خضتها على مدى عطلة الاسبوع الفائته و احببت ان اشارككم اياها .....

احد زملائي اخبرني بانه يرى ملف اسمه folder.htt في كل مجلد يفتحه على الوندوز و لا يستطيع ان يفتحه ليرى ما في داخلة حيث تظهر له الرسالة المعروفة access denied اي ان الوصول الى هذا الملف ممنوع ..... اضافة للملف folder.htt فانه يجد ايضا ملف اسمه .... desktop.ini وهذا الملف يمكنه فتحه لكنه لا يجد فيه اكثر من 5 سطور ولا تشكل اي خطر من وجهه نظرة .... فكان سؤاله لي هل هذا فيروس او لا ..... واذا كان فيروسا فهل يمكن ازالته و ما مدى الضرر الذي يلحقه بالجهاز .....

طبعا في البداية تذكرت اني قد رايت هذا الملف (folder.htt) في اكثر من جهاز على مقاهي انترنت ولكني لم اكترث حينها له ولم احاول حتى فتحه ..... لهذا وافقت ان اذهب مع صديقي الى غرفته لنكشف على الجهاز ونرى ما المشكلة ....

اول مجموعة ملاحظات كانت التالي ....

-الملفين desktop.ini و folder.htt ملفان مخفيان لكنهما يظهران لان صديقي اختار ان يظهر الملفات المخفية من قائمة ..... tools>>folderOptions ولولا انه اختار اظهار كافة الملفات منذ زمن لما لاحظ وجود الملفين (عندما تختار اظهار كافة الملفات تظهر الملفات المخفية اصلا بلون باهت مقارنه مع بقية الملفات)

-عند انشاء مجلد جديد فارغ في اي مكان على الجهاز ثم فتح المجلد نجد الملفان موجودان في داخله. ولكن عند انشاء مجلد جديد فارغ عن طريق الـ DOS ثم استعراض الملفات التي بداخلة من على الـ DOSايضا لا نجد الملفين ولكن ما ان نستعرض المجلد نفسه من الوندوز ثم نعود و نستعرضه من الدوس حتى نجد انهما اصبحا موجودين في داخله.

-حجم الملف folder.htt حوالي 15. KB

-الملف folder.htt لا يمكن فتحه ولا حذفه لا من الدوس و لا من الوندوز.

-الجهاز اصبح بطيئا بشكل ملحوظ عند فتح مجلد حتى ولو كان فارغا.

-عند ادخال قرص مرن في محرك الاقراص فانك بمجرد فتحه تجد الملفين موجودين في كل مجلد من مجلدات القرص المرن.

الآن بدأت فعليا اشك في انه فيروس,لكن جهاز صديقي عليه McAfee Anti Vairus ولم يعلن عن وجود فيروس في الجهاز ثم انني تذكرت شيئ مهم ....

اذكر منذ زمن انه يمكننا تخصيص مجلد ما من داخل الوندوز بحيث يظهر بشكل مختلف عن بقية المجلدات عندما نفتحه .... اقصد يكون له صورة معينة بدل الخلفية البيضاء العادية و يتغير لون و نوع الخط الذي تظهر به اسماء الملفات..... عندما قرأت اسم الملف folder.htt ربطت بينه و بين هذه الميزة و اعتقدت ان الوندوز تنشئ هذا الملف و تحفظه في اي مجلد نقوم بتخصيصه اي انه ليس فيروسا وانما احد ملفات الوندوز المعروفة ....

وجدت ان استنتاجي المبدئي كان صحيحا عندما عدت الى جهازي السليم و بحثت عن ملف اسمه folder.httووجدته .... لكن المشكلة اني لم اجد سوى عدد قليل من الملفات وكلها لم يقل حجمها عن 20 KB .....

ففكرت بعمل تجربة .... جهازي يعمل عليه.... Norton Anti Vairus 2003

فقررت ان اجازف بادخال القرص المرن الذي جلبته من جهاز صديقي .... وبمجرد ان ادخلته ظهرت لي شاشه الـ Norton المشهورة التي تحذرك من وجود فيروس .... وكانت كما توقعت .... !!
الملف folder.htt مصاب بالفيروس .... html.redlof.a ولا يمكن اصلاحه ....
الآن تأكدت من صحه استنتاجي ..... فضغطت مباشرة على الرابط في الرسالة و الذي يأخذني الى موقع symantec و يقدم شرحا وافيا عن الفيروس المذكور .... وهذه هي الصفحة

http://securityresponse.symantec.com/avcenter/venc/data/html.redlof.a.html

يعتبر هذا الفيروس من اخطر الانواع من ناحية الانتشار وهو يسمى polymorphic اي متعدد التشكل او عديد التشكل .... المهم انه من النوع الذي يقوم بانشاء نسخ من نفسه و ينتشر بهذه الطريقه .....

وهذه بعض المعلومات عنه

هذا الفيروس عبارة عن Visual Basic Script

ينسخ نفسه في مجلد النظام system او system32 باسم kernal.dll اوkernal32.dll

ويصيب الملفات من نوع .... html,htm,php,asp,jsp, vbs

يقول موقع symantec انه يوجد 50 - 999 اصابة مسجلة لديهم مع اني اعتقد ان الرقم الحقيقي اكبر من هذا بكثير خصوصا واني قد رايت اجهزة اخرى مصابة بالفيروس ولم اعرف حينها انه فيروس ....

اهم شيئ انه يقوم بعمل تعديلات معينه في الرجستري لكي يضمن ان يقوم النظام باعتبار اي مجلد هو مجلد مخصص و ينسخ الفيروس اليه .... على الاقل هذا مااعتقد انه يحصل ....

ثم عندما تستعرض المجلد اذا كنت تستخدم اسلوب عرض المجلدات كصفحات ويب .... فانك لن تستطيع رؤية الملفات ولكنك سترى احرف غريبة تملا نافذه متصفح الوندوز ..... ولحسن الحظ ان صديقي لم يكن يستخدم هذا الاسلوب .... لكن المشكلة لا زالت قائمة ..... الفيروس " مبسط في جهاز الرجال و مسوى حفلات كل ليلة .... و سامري و بلوت و كل شي .... يعني ماخذ راحته على الآخر "

الآن ما الحل ..... كيف استطيع ازالته ....

في البداية ..... ادركت انه لا يمكن حذف كل الملفات بكل بساطة .... ولكني بدأت احاول .....

ذهبت لموجة الدوس ثم نفذت المر التالي

edit folder.htt

طبعا امر edit يقوم بعرض محتويات الملف في محرر نصوص عادي على بيئة الدوس ..... لكن هذا لم يفلح فالملف لا يمكن الوصول البه..... تماما نفس الرساله التي تظهر في الوندوز .....

قمت بخدعه اخرى....

نفذت الامر التالي

edit

هذا الامر يفتح لك المحرر فارغا بحيث تستطيع الكتابة ثم حفظ الملف تماما كبرنامج النوت باد ..... وهنا استغليت الموقف و حفظت الملف "الفارغ" باسم folder.htt في نفس المجلد الذي يوجد فيه الملف folder.httمن قبل ..... ماذا تتوقعون انه حدث .....؟!

طبعا سالني المحرر " يوجد ملف اصلا باسم folder.htt هل تريد الحفظ عليه ؟ " فاجبت بنعم ...

وحصل بالضبط ما توقعته ..... لقد تم محو الملف الاصلي ... وبشكل ادق ... اصبح الفيروس عبارة عن ملف فارغ باسم ... folder.htt وغير مخفي ... وطبعا حجمة 0.. kb

فكرت بعدها .... هذه الطريقة لن تكون عملية ... فانا لن استطيع الدخول الى كل مجلدات القرص الصلب و تكرار نفس العملية في كل مرة .... اي اني لن استطيع ان افتح المحرر ثم احفظه بنفس الاسم في كل مجلد في القرص الصلب

ثم و الاهم من هذا انها بمجرد ان تفتح ايا منها من الوندوز مرة اخرى ستجد ان الملف قد عاد على ماهو عليه .... و اصبح الملف حجمه 15 kb مرة اخرى ....
اذا ما العمل....

يجب ان اوقف نشاط الفيروس التكاثري اي ان احاول منعه من نسخ نفسه في كل مجلد يتم فتحه من الوندوز .... و هنا عدت لموقع .... symantec فوجدت هذه التعليمات

لازالة الفيروس يجب ان
-1تحدث تعريفات الفيروسات في برنامج النورتون
-2تعمل فحص شامل للملفات و احذخ كل الملفات المصابة بالفيروس
-3اعكس العمليات التعديلات التي احدثها الفيروس في ملف الرجستري ...

الكلام اسهل من الفعل ... .لاني في البداية اضطررت للبحث عن قرص تركيب برنامج النورتون وبعد ان ازلت McAfee الذي لم يكتشف حتى وجود الفيروس و ركبت Norton بعد جهد جهيد بدا يزعجني بشكل لا يطاق,حيث انني كلما فتحت اي مجلد اجد انه يظه لي رسائل التحذير التي لا تنتهي الى درجة اني فكرت في ان الغي تركيبة من على الجهاز .... لكني فكرت مرة اخرى .... بعد ان لاحظت ان الفيروس لم يعد ينتقل الى المجلدات الجديدة ....
فكل ما حاول ذلك يمنعه النورتون من تنفيذ الكود الخاص بالفيروس
و بالتالي لا يستطيع نسخ نفسه بعد الآن الى المجلدات الجديدة ..... لكن المشكلة ان الجزء الخاص بالفحص الشامل في النورتون و الذي يكتشف كل الملفات المصابة ثم يزيلها لا يعمل !! .... هكذا بكل بساطة لا يعمل !!

كلما ضغطت على الايقونة تظهر لي علامة الساعة الرملية ولكن البرنامج لا يعمل و عندما ابحث عنه في قائمة البرامج Alt+Ctrl+Del لا اجد اي عملية جارية لها علاقة بالنورتون .... هل يعقل ان الفيروس يمنع الجزء المتعلق بالفحص الشامل في نورتون من العمل ؟؟ ....!!! هذا ما لم اجد له جوابا ..... لكني حاولت بكل الطرق و شغلت النورتون عدة مرات .... و اعدت تشغيل الجهاز كذا مرة .... ولم تحل المشكلة النورتون لا يعمل ... الجزء الوحيد الذي يعمل هو الجزء المزعج .... التنبيهات التي لا تتوقف ولا تستطيع لا ازالة الملف ولا حتى احتوائة .... Quarantine ما العمل اذا ...

تركت الملفات المصابة الآن وشغلت الرجستري ...
run > regedit
و تتبعت المسار االتالي
1- HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run

ثم حذفت المدخل Kernel32 من الجزء الايمن ...

2- HKEY_CURRENT_USER\Identities\[Default Use ID]\Software\
Microsoft\Outlook Express\[Outlook Version].0\Mail

ثم حذفت القيم
Compose Use Stationery
Stationery Name
Wide Stationery Name

3- HKEY_CURRENT_USER\Software\Microsoft\Office\9.0\Outlook\Options\Mail

وحذفتEditorPreference

و اخيرا
-4تتبعت هذه المسارات
HKEY_CLASSES_ROOT\dllFile\Shell
HKEY_CLASSES_ROOT\dllFile\ShellEx
HKEY_CLASSES_ROOT\dllFile\ScriptEngine
HKEY_CLASSES_ROOT\dllFile\ScriptHostEncode

و حذفتها كلها ....

الآن المفروض ان الفيروس لا يستطيع التحكم بالمجلدات و نسخ نفسه اليها ....

بقيت امامي العقبة الاخيرة .... وهي ازالة الملفات المصابة .... طبعا الفيروس يصيب الملفات من نوع htmو html و و و لكنني الآن ساركز على الملفات المسماه folder.htt وهي التي
تحمل الفيروس بشكل صريح خصوصا و اني لا استطيع ان اعرف اي الملفات الاخرى تحمل الفيروس بدون ان استخدم برنامج النورتون ..... لكن المشكلة ان المساعدة الواردة في موقع symantec تنتهي عند هذا الحد...
فهي تتطلب استخدام النورتون ..... و النورتون لا يعمل .... و المشكلة لا استطيع الاتصال بالانترنت حاليا .... ماذا افعل ؟

الحل يجب ان يأتي من الدوس ....
عدت مرة اخرى لموجه الدوس ....

وحاولت استخدام امر del مرة اخرى ...
لم ينجح .... استخدمت امر جديدا اسمه erase يقوم بنفس العمل .... ولم ينجح هو الآخر ...

ثم اهديت الى فكرة مجنونة ..... لمذا لا ازيل خاصية الاخفاء من الملف ثم احاول حذفه ..... و جربت
attrib folder.htt -h
فنجح الامر ....
ونفذت بعدها امر
attrib *.*
لاجد ان الملف folder تحول الى R و A اي انه اصبح ملف للقرائه و الحفظ ....

اها ... هل يمكن ان اقرا الملف الآن بواسطة محرر الدوس ..... كنت متشوقا لاعرف كيف كتب الفيروس .... لكن يبدو اني كنت ساذجا .... فلم اتمكن من قرائته حتى ببرنامج... hex editor
لكنه الآن ليس مخفيا.....

اذا لمذا لا احاول ان احذفة مرة اخرى ...
del folder.htt
وكانت المفاجأة لقد تم حذف الملف!!

لم اصدق ما رأيت ....

عندها عملت patch file وهو ملف تنفيذي يحتوى سلسلة من اوامر الدوس التي تنفذ تباعا بدون ان يحتاج المستخدم لكتابتها كل مرة ....
وكتبت فيه الاوامر التاليه

attrib folder.htt -h /s
attrib desktop.ini -h /s
del folder.htt /s
del desktop.ini /s

طبعا الحرف s يعني ان يبحث في كل المجلدات الموجودة في السواقة و المجلدات التي داخل كل مجلد .....

طبعا بعد ان نفذت الملف .... الذي اسميته .... folderhttFixer.bat استغرق وقتا طويلا قبل ان يعلن لي وبكل زهو انه ازال كل ملفات الفيروس :) :)

ولكن مهلا بقيت عدد من المفات من الانواع htm و html و php و غيرها .... ما العمل الآن ؟؟؟

عدت الى النورتون و بمجرد ان ضغطت على ايقونه الفحص الشامل ..... اشتغل البرنامج! و قام بفحص شامل و وجد حوالي 200 ملف من الانواع المذكورة ... وطبعا طلبت منه حذفها جميعا ....

واما الـ patch file الذي عملته .... فقد وجدت مفيدا مع الاقراص المرنه بمجرد ان انسخه الى احدها و انفذه يمسح كل ملفات الفيروس و تعود الاقراص نضيفة مرة اخرى بدون الحاجة الى عمل فورمات و ضياع الملفات الاخرى المفيدة عليها ...

هذه كانت مشكلتي ..... التي شيبت رأسي الى ان حللتها .....لكن بفضل الله تم حلها في النهاية و التخلص منه