البرامج الخبيثة

وطرق الوقاية منها

البرامج الخبيثة

وطرق الوقاية منها

حررها لكم
خالد بن عبدالله العمري
techeditor@hotmail.com

راجعها لغوياً وإملائياً
أ/ ناصر بن أحمد الزهراني
أ/ عبدالله مسواك

المحتويات

البرامج الخبيثة وطرق الوقاية منها

جاءني أحد الزملاء يوما وهو مبتهج أشد الابتهاج ، حيث ارتسمت على محياه ابتسامة عريضة (بطول اثنين متر ونصف)، أذكر أن شفتيه (براطمه) كادت تتقطع من شدة الفرح ، وبعدما حادثته عن سبب هذه الفرحة المفرطة ، أجابني أنه قام بشراء حاسوب جديد ، وينوي أن يصبح (فلتة زمانه) في هذا المجال، فباركت له على هذا الإنجاز، وتمنيت له أن يحقق مراده ، وأنا أقول في نفسي (الله يستر على الجهاز منك).

المهم أن أخانا هذا اختفى عني فترة من الزمان، ويبدو أنه كان خلال هذه الفترة ضيفا (ثقيل الظل) على جهازه الذي اشتراه. قابلته بعد مدة مصادفة وسألته عن أخباره وأخبار (الضحية) الجديد ، ولكنني تفاجأت عندما علمت منه أنه عرضه للبيع !! ، فسألته مستغربا ولماذا! فأجابني أن (المرحوم) كان يعمل معه بدون أي مشاكل ، إلا أنه أصبح في الآونة الأخيرة كثير التضجر من العمل -يعني جهازه- حيث إنه ينطفئ لوحده من دون أي مقدمات (يبدو أن جهازه من النوع الذي يهوى العناد) ويعيد التشغيل من نفسه بدون أن يأمره بذلك (على المزاج) ، ويجمد أو (يعلق) في أحيان أخرى، بل إنه قد يطلب الاتصال بالإنترنت تلقائيا بدون أن يطلب منه ذلك (يموووون) ، ويبدو أن صاحبي قد قسا على جهازه ، فأبى الجهاز إلا أن ينتقم منه ، ويلقنه درسا في أصول المعاملة الحسنة ، فأعلن حالة التمرد ، وأصبح يأتمر بنفسه ، ويفعل ما بدا له من أعمال (الشغب) من دون أن يرجع إلى صاحبه.

أظن أن هذا السيناريو يتكرر كثيرا مع بعض من يتعاملون مع جهاز الحاسوب عموماً ، ومرجع هذه المشاكل وغيرها يعود إلى أسباب عديدة بعضها برمجي (يتعلق بالبرامج) والآخر عتادي (يتعلق بمكونات الحاسوب المادية) وسوف أتعرض في هذا المقال إلى الجانب البرمجي ، وخصوصاً ما يتعلق بالبرامج الخبيثة Malwares ابتداءً بالفيروسات Viruses وانتهاءً بالمتصلات التلقائية Dialers.

كل الطرق تؤدي إلى الهاوية

كثرت في الآونة الأخيرة البرامج الخبيثة التي تصيب الحاسوب وتؤدي إلى إيذائه أو استغلاله لإيذاء الآخرين ، ومع كثرة أنواع هذه البرامج ، قام الباحثون في هذا المجال بتصنيفها حسب الفعل الذي تقوم به ، فهناك البريمجات الخطرة كالفيروسات Viruses ، وأحصنة طروادة Trojan Horses ، والديدان Worms ، وهناك منتهكات الخصوصية كبرامج التلصص Spywares ، وبرامج الدعاية Adwares ، ومختطفات الصفحة الرئيسية للمتصفح Browser Hijackers ، وهناك المستغلات الدنيئة لموارد المستخدم كالمتصلات التلقائية Dialers ، وأخيراً هناك صنف لا يندرج تحت مسمى البرامج الخبيثة لكنه قد يكون مؤذيا في بعض الأحيان وهو الشائعات Hoaxes التي قد تؤدي بالمستخدم إلى التصرف بشكل خاطئ تجاه جهازه.

وعلاوة على ما سبق من التصنيفات فإن بعض البرامج (الشريرة) قد تحمل أكثر من تصنيف وذلك لتنوع الأعمال التي يمكن أن تقوم بها ، ولذا فقد عمد أصحاب الاختصاص إلى جمع هذه التصنيفات في مسمى واحد باسم البرامج الخبيثة Malwares ، فالبرنامج الخبيث هو كل كود برمجي يعمل لأجل إيذاء المستخدم ، أو إيذاء حاسوبه ، أو إيذاء الشبكة الحاسوبية ، أو إيذاء الآخرين ، ولذا فإذا احترت بين تصنيف ما يصيب جهازك من ضرر فيمكنك أن تقول: جهازي به (كوكتيل) من البرامج الخبيثة ، أما إذا كنت تريد أن تفرد عضلاتك أمام زملائك وتثبت لهم أنك (فلتة زمانك) فيمكنك أن تخبرهم أن جهازك أصبح (مستنقعا) للفيروسات (والطحالب الخضراء).

١) فيوز ... فيروز ... أم فيروس ؟؟

يحلو للكثير من الناس أن يسمي كل ما يصيب جهازه من بلاء بالفيروس ، والحقيقة أن ذلك كان صحيحا حتى عهد قريب ، إذ أن التطور التقني الهائل في العقد الأخير من الزمان ، ودخول الإنترنت في كل مكان (إلا في حارتنا) أدى إلى تطور الأساليب التي يستخدمها (الهاكرز) في كتابة برامجهم الخبيثة ، فطوروا من برامجهم ، وجعلوها تستخدم التقنيات الحديثة ووسائل الاتصال لتنتشر ، بل وتحدث أضرارا أكثر من ذي قبل ، ولذا فإنها لم تعد تحمل صفات الفيروس وحسب ، بل زادت عليه وتعدته إلى ما هو أبعد من ذلك بكثير ، وهذا يقودنا إلى معرفة ماهية فيروس الكمبيوتر ، وطرق الإصابة به.

البرامج الخبيثة وطرق الوقاية منها

لماذا سمي الفيروس بهذا الاسم؟

سمي الفيروس بهذا الاسم لأنه يشبه في عمله الفيروسات الطبيعية التي تصيب جسم الإنسان ، فالفيروسات الطبيعية تتميز بصغر حجمها وعظم ضررها ، وصعوبة اكتشافها ، وسرعة تكاثرها ، إضافة إلى إمكانية انتقالها إلى أجسام أخرى سليمة وإصابتها بالعدوى ، وهذه الخصائص تنطبق تماما على فيروسات الكمبيوتر، ويبدو أن أوائل مبرمجي الفيروسات قد استوحوا فكرة هذه البرمجيات الخبيثة من الفيروسات البشرية.

أ) ما هو فيروس الكمبيوتر Computer Virus؟

فيروس الكمبيوتر هو عبارة عن برنامج صغير -لايتجاوز غالبا ١٠٠ كيلوبايت- يضيف نفسه إلى جميع الملفات التي يريد تلويثها ، الهدف منه هو إما تدمير بيانات معينة في الجهاز المصاب بعدة طرق وأشكال ، يحددها مبرمج الفيروس نفسه ، أو إزعاج المستخدم من خلال إبطاء عمل الجهاز ، وجعله يعمل بشكل غير طبيعي.

ب) مميزاته:

أهم ما يميز الفيروس عن بقية أصناف البرامج الخبيثة هو مقدرته على التكاثر بشكل كبير وتلويث أكبر قدر من الملفات والبرامج في جهاز الكمبيوتر (يمكن أن يصبح جهازك وكيل معتمد لتوريد الفيروسات لأصحابك وبالمجان !!) ، وهو في هذه المرحلة قد يكون في طور الانتشار والتكاثر ولكن بدون أن يحدث أي فعل تدميري (فترة الحضانة) ، وقد يبدأ فعله التدميري أو (مسلسل) الإزعاج ، في وقت محدد أو زمن محدد -مثل فيروس تشيرنوبل- أومن خلال تشغيل المستخدم لأحد البرامج أو الملفات الملوثة بهذا الفيروس (ويا حافظ لك الله).

ج) طرق انتشاره:

يمكن للفيروس أن ينتقل إلى جهاز المستخدم بدون علمه ، عن طريق ملف ملوث بالفيروس ، قام المستخدم بإحضاره (من شخص ظريف) إما عن طريق أحد وسائط التخزين (قرص ليزري ، قرص ممغنط ، هارديسك خارجي .... الخ) أو عن طريق شبكة الكمبيوتر (الشبكة المحلية أو شبكة الإنترنت) حيث يظهر في شكل ملف مفيد ينصح أحد مواقع الإنترنت بتحميله (قد يكون الملف مفيداً ولكنه ملوث بالفيروس) أو على شكل رسالة بريدية معها ملف مرفق (ملوث بالفيروس) ، تحث هذه الرسالة على وجوب فتح هذا الملف المرفق ، أو عن طريق مواقع الدردشة Chatting Rooms حيث يطلب منك بعض المحاورين استقبال ملف وفتحه من غير أن تعرف محتواه.

د) أضراره:

كما ذكرت سابقا ، فالأضرار قد تتراوح بين تدمير جميع محتويات الجهاز (يعني يفتح الله على جهازك) وبين حدوث مشاكل قد لاتصل إلى حد الإعطاب ، كبطء أداء الجهاز عموما ، أو ظهور رسائل خطأ بشكل متكرر ، أو تجمد الجهاز عن العمل ، أو إعادة التشغيل التلقائي للجهاز ، و ذلك كله يعتمد على هدف مبرمج الفيروس منه ، ومدى الضرر الذي يود إلحاقه بالجهاز (المسكين).

٢) ذئاب تلبس جلود الضأن:

عفوا ، هذه الفقرة ليست لسرد حكاية من كتاب كليلة ودمنة ، وإنما لتبيين خطورة هذا النوع من البرامج الخبيثة ، الذي يمكن أن يكون له نتائج مدمرة لجهازك (يعني يفتح الله على الجهاز) ، بل وأكثر من ذلك أنه يمكن أن يوقعك فريسة لابتزاز المجرم الذي صنعه ، فهذا النوع يمكن أن يقبع في جهازك لشهور عديدة من دون أن تعلم عنه ومن دون أن يحدث شيئا ، ولكنه خلال هذه الفترة يكون قد (نشر غسيلك) نيابة عنك ، وفضح جميع أسرارك (هذا إن كان عندك أسرار) للشخص الذي قام ببرمجته (الحرامي الكبير) ، وهو مع صغر حجمه إلا أنه يعتبر من اللصوص المحترفين ذوي الأوزان الثقيلة.

أ) ما هو حصان طروادة Trojan Horse:

حصان طروادة هو عبارة عن برنامج صغير ، يظهر بشكل برنامج (أليف) أو ملف ، يتظاهر بأنه يقوم بأعمال مفيدة لك ، أو بعمل تحديثات مهمة لجهازك ويوهمك بأن هذه التحديثات لا غنى لك عنها ، وبهذا الأسلوب فإنه يستحثك لتشغيله ويبدأ فور تشغيله بفعله التدميري أو التجسسي مباشرة وبدون أي مقدمات .

ب) مميزاته:

يتميز حصان طروادة -علاوة على صغر حجمه- بكونه لا ينتشر ولا يتكاثر بين الملفات والبرامج ولا يلوث أياً منها كالفيروس ، فحصان طروادة يؤدي فعله التخريبي بدون أن يرتبط بأي ملف سليم ، إلا أن عمله التخريبي يفوق في بعض الأحيان معظم الفيروسات، فعلاوة على مقدرته على تخريب ملفات وبرامج الكمبيوتر ، وحذف وتخريب ما شاء منها ، يتمتع بعض أحصنة طروادة بخاصية التجسس، حيث يقوم بالتلصص على الضحية ، بصمت مُطْبِقْ ، لعدة أشهر أو سنوات من دون أن يعلم بذلك ، ولك أن تتخيل أين سوف تكون أرقام

البرامج الخبيثة وطرق الوقاية منها

لماذا سمى حصان طرواده بهذا الاسم؟

سمي حصان طرواده بهذا الاسم نسبة للقصة التي وردت في التراث الإغريقي ، حيث يقال أن الإغريق حصلت حرب بينهم وبين قوم يقال لهم الطرواديون ، واستمرت هذه الحرب مدة من الزمان ، مما أضعف من جيش الإغريق وجعله يعقد الهدنة مع الطرواديين ، وعندما وافق الطرفان على الهدنة ، قام الإغريق بإرسال هدية عظيمة لملك الطرواديين وهي عبارة عن مجسم عظيم على شكل حصان ، فقبل الملك الهدية ، وما علم أن السم قد وضع له في الدسم ، فمجسم الحصان كان يختبئ بداخله العديد من الجنود الذين خرجوا من المجسم ليلا وقاموا بمهاجمة الطرواديين ، الذين قتل عدد كبير منهم جراء هذه الخدعة ، ومن هنا جاءت تسمية هذا النوع من البرامج الخبيثة التي تتظاهر أنها تقوم بأعمال مفيدة ، وهي في حقيقتها تخبئ سما زعافا.

بطاقات ائتمانك (إذا كنت من أصحاب الدراهم الكثيرة) أو كلمات المرور الخاصة ببريدك الإلكتروني أو الخاصة بالمواقع التي تشارك بها (خصوصا إذا كنت من فئة أبو طقطق الذين يتسابقون لإنشاء حسابات بريدية كثيرة ، ظنا منهم أنها سوف تتحول في يوم من الأيام إلى حسابات بنكية مليئة بالكنوز!!!)

ج) طرق انتشاره:

غالبا ما ينتقل حصان طروادة إلى جهاز المستخدم بعلمه ، خصوصا إذا علمنا أنه لا ينتشر تلقائيا ولا يلوث ملفات أخرى كما هو الحال بالنسبة للفيروسات ، فقد يصل عن طريق ملف أو برنامج قام المستخدم بإحضاره –من شخص آخر– إما عن طريق أحد وسائط التخزين (قرص ليزري ، قرص ممغنط ، هارديسك خارجي .... الخ) ، وإما عن طريق شبكة الكمبيوتر (الشبكة المحلية أو شبكة الإنترنت) حيث يظهر في شكل ملف مفيد ينصح أحد مواقع الإنترنت بتحميله ، وقد ينتشر حصان طرواده أيضا عن طريق البريد الإليكتروني حيث تصل للمستخدم رسالة معها ملف مرفق ، تحث المستخدم على فتح هذا المرفق ، علاوة على أن لغرف الدردشة والحوار Chatting Rooms دوراً كبير في انتشار هذا النوع من البرامج الخبيثة ، حيث أنه كثيرا ما يتلقى المستخدم دعوات باستقبال ملفات من أشخاص (مشبوهين) أو غير معروفين في غرف الدردشة ، وهذه الملفات في حقيقتها ما هي إلى أحصنة طروادة.

د) أضراره:

تتراوح أضرار هذا النوع من البرمجيات الخبيثة بين فقدان المستخدم للبيانات الموجودة على الجهاز وبين انتهاك خصوصياته ، فبعض الأنواع يقوم بتدمير البيانات والمعلومات الموجودة في الجهاز ، أو يقوم بإبطاء عمل الجهاز وخلق مشاكل كثيرة تؤدي إلى (تجمد) الجهاز عن العمل وانهياره ، وهو في ذلك مشابه للفيروس إلى حد ما ، أما البعض الآخر فيعمل بصمت حيث يقوم بالتجسس لحساب صانعه ومبرمجه ، فيقوم بإرسال معلومات قد تكون سرية ، كأرقام بطاقات الائتمان أو كلمات المرور الخاصة بحساباتك البريدية أو كل ما تقوم بإدخاله عن طريق لوحة المفاتيح ، وقد تكون هذه المعلومات خاصة مثل أسماء المواقع التي تزورها أو أسماء البرامج التي تستخدمها وأسماء الملفات التي قمت بإنشائها أو فتحها مؤخراً ، والأدهى من ذلك هو أن بعضها لديه المقدرة على التقاط صور لسطح المكتب ، تقوم بإظهار ما تقوم بفعله الآن ومن ثم إرسال هذه الصور إلى مبرمجه ، بل إن بعضها يمكن أن يعمل كالخادم المطيع لمبرمجه ، فيمنحه إمكانية التحكم الكامل بجهازك وكأنه أمامه ، فيمكنه من حذف وتعديل وتغيير الملفات ، وتغيير نمط عمل الجهاز ، بل ويمكنه من تحويل حاسوبك إلى جهاز عدائي يُستخدم للإطاحة بخوادم انترنت معينة من خلال **هجمات حجب الخدمة الموزعة Distributed Denial of Service** التي يمكن أن يشارك فيها جهازك من دون علمك ، ولذا فإن ضرره قد يكون أكبر بمرات كثيرة من ضرر الفيروسات.

٣) ابتسم فأنت مع السيدة (دودي) :

السيدة دودي هي كائن(برمجي) من النوع الثقيل الذي لا يطاق ، والذي لا يمكن أن تصبر عليه ولو للحظات (مثل بعض الآدميين) ، فهي من عائلة عريقة في مجال (الإجرام) ، فشقيقها شبه التوأم هو (المستر) فيروس ، أما ابن عمها (المقرف) فهو حصان طرواده ، ولذا فأنا أنصحكم الآن بالاستعداد معنويا للخوض في (مستنقع) الديدان البرمجية حتى نتعرف على مميزاتها وكيف تصيب الحاسوب.

أ) ما هي الديدان البرمجية:

الديدان البرمجية Worms هي عبارة عن بُريمجات صغيرة الحجم ، يتم استقبالها غالبا عن طريق شبكة الكمبيوتر –سواء الشبكة المحلية أم شبكة الانترنت– وتهدف غالبا إلى إزعاج المستخدم أو تدمير المعلومات المخزنة في جهازه ، بالإضافة إلى إحداث حركة مرور كبيرة في الشبكة

البرامج الخبيثة وطرق الوقاية منها

-بإرسال واستقبال بيانات كبيرة وبشكل متواصل- قد تؤدي إلى انهيار الشبكة أو بطئها عموما ، وسميت بذلك لأنها تشابه الديدان الطبيعية في سرعة التوالد والانتشار.

ب) مميزاتها:

تتميز الديدان الحاسوبية بسرعة انتشارها المذهلة ، فيمكن للدودة البرمجية أن تصيب ملايين الأجهزة في غضون مدة زمنية قصيرة جدا ، ويعود السبب في ذلك إلى اعتمادها على الشبكة الحاسوبية في الانتشار ، وتتشابه الديدان مع الفيروسات في الكثير من الخصائص والصفات ، فالديدان البرمجية صغيرة الحجم، ولديها مقدرة على التوالد والانتشار كالفيروسات ، ولكنها لا تلوث الملفات أو البرامج أو تضيف نفسها إليها -كما هو الحال بالنسبة للفيروسات- بل إن ملف الدودة البرمجية يتكاثر ويتضاعف إلى أعداد كبيرة ، ويأخذ بعدها في الانتشار في الشبكة التي يرتبط بها الجهاز الملوث ، وهذا أهم ما يميزها عن الفيروس ، فالفيروس يكون توالده وانتشاره ضمن نطاق الجهاز الملوث نفسه أو جهاز آخر تم وصول الفيروس إليه عبر طرق التخزين التقليدية (القرص المرن أو أقراص التخزين الخارجية ..الخ) بينما الدودة البرمجية يتعدى انتشارها الجهاز نفسه ليصل إلى الآخرين عبر شبكة الحاسوب.

ج) طرق انتشارها:

تنتشر الدودة البرمجية عن طريق شبكة الإنترنت أو الشبكة المحلية ، ويكون الانتشار إما عن طريق رسالة بريدية معها ملف مرفق يحتوي على الدودة نفسها ، وإما عن طريق أحد الثغرات الأمنية الموجودة في نظام التشغيل [شركة مايكرو(زفت) بالمناسبة هي الموزع الحصري والمعتمد للثغرات الأمنية ، ولذلك فبرامجها تزخر بطيف واسع من هذه الثغرات ، ابتداء من (الفأر الصغير) ماسنجر وانتهاء (بالقط الكبير) اكسبلورير].

هجمات حجب الخدمة الموزعة
Distributed Denial of Service

هي عبارة عن هجمات تقوم على مبدأ إغراق أحد الخوادم Servers الموجودة في الإنترنت (أو في أي شبكة عموما) بسيل كبير من طلبات التصفح في لحظة معينة ، مما يؤدي في النهاية إلى انهيار الخادم ، وبالتالي تعذر أو بطء الوصول إلى المواقع المستضافة عليه ، بسبب كثرة الطلبات الهجومية عليه ، وحتى تكون الصورة أوضح في ذهنك خذ هذا المثال: لو أن ١٠٠٠٠ مستخدم ، قاموا بطلب صفحة معينة من أحد المواقع ،بمعدل صفحة كل ثانية ، فهذا يعني أنه خلال ٦٠ ثانية يجب أن يلبي الخادم (السيرفر) ما مقداره ١٠٠٠٠×٦٠= ستمائة ألف طلب !! أو ستة ملايين طلب خلال ١٠ دقائق فقط !!! بالطبع فإن الموقع إذا لم يكن مستضاف على عدد من الخوادم الكبيرة والمرتبطة بسعات اتصال كبيرة بالإنترنت ، فإما أنه سوف ينهار جراء عدم مقدرته على تلبية هذا السيل الهائل من الطلبات في لحظة واحدة ، أو أن تصفح الموقع سوف يكون بطيئا للغاية لأولئك الأشخاص الذين يقومون بتصفح الموقع الآن.

ويمكن أن يتم هذا النوع من الهجوم بعدة طرق من أهمها:

١ أحصنة طروادة:

حيث يقوم مبرمج حصان طرواده ، أو من قام بنشره ابتداء، بإرسال أوامره من خلال الإنترنت إلى جميع الأجهزة المصابة بهذا الحصان ، يأمرهم فيها بمهاجمة موقع معين والإطاحة به من خلال إغراق الموقع بسيل كبير من طلبات التصفح.

٢ الاتفاق المسبق:

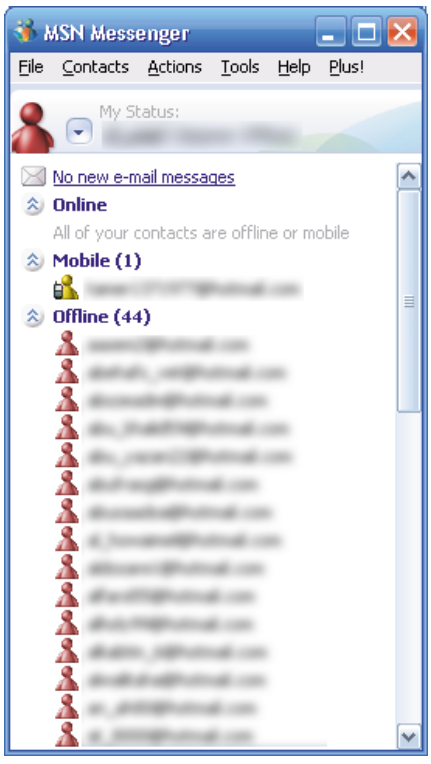
فيمكن أن يتفق مجموعة كبيرة من مستخدمي الإنترنت على إغراق موقع معين بسيل من طلبات التصفح في آن واحد.

٣ الديدان البرمجية:

إذ تعمد بعض الديدان البرمجية إلى إغراق مواقع معينة بسيل من الطلبات بهدف الإطاحة بها ، كما حصل ذلك في دودة بلاستر Blaster مثلا.

البرامج الخبيثة وطرق الوقاية منها

❖ الانتشار عبر البريد الإلكتروني:
يحصل الانتشار عبر البريد الإلكتروني عندما يقوم المستقبل (الدلخ) بفتح الملف المرفق مع الرسالة (ظناً منه أنه سوف يحصل على سيارة رولزرويس بفعله هذا !!) وعندها تبدأ الدودة بعملها التدميري بدون أن يعلم الشخص (الضحية) عنها ، حيث تبدأ بالتكاثر وإرسال نفسها إلى كل الموجودين في قائمة برامج المحادثة (مثل الماسنجر وغيره) أو الموجودين في قائمة دفتر العناوين Address Book ، بل وقد يصل حد الإجرام بالدودة إلى أن تستخدم أحد محركات البحث مثل جوجل أو ياهو ، وتبحث -بدون علم المستخدم طبعا- عن حسابات بريد إليكتروني أخرى في الإنترنت ، وثَمَّ تقوم بإرسال نفسها إلى هذه العناوين لتصيب أكبر قدر ممكن من الأجهزة أو الحواسيب .



تعتبر قوائم المتصلين في برامج المحادثة صيدا ثمينا لمعظم البرامج الخبيثة

تعمد الديدان الحاسوبية إلى إرسال نفسها إلى أكبر قدر ممكن من العناوين البريدية [الإيميل] ، من خلال السطو عليها من جهاز المستخدم [الضحية] ، سواء أكانت العناوين موجودة في قائمة برامج المحادثة –الماسنجر مثلاً– أو كانت موجودة في دفتر العناوين الخاص ببرنامج معين –مثل الآوت لوك Outlook- وحتى تتحايل على الشخص المستقبل ، وتجعله يطمئن لفتح الملف المرفق ، فإنها تستخدم حيلة خبيثة وماكرة ،تكمن في تغيير عنوان المرسل منه From وتجعله يظهر وكأنه لأحد معارفك أو أصدقائك ، ويتم ذلك عبر انتقائها لأحد هذه العناوين –وبشكل عشوائي– من دفتر العناوين أو قائمة برامج المحادثة الموجودة في جهاز الضحية ، فيظهر عنوان المرسل منه وكأنه لأحد أصدقائك ، ويدفعك هذا بالطبع إلى فتح الرسالة وفتح مرفقاتها كذلك ، ظنا منك أن صديقك لن يخونك في يوم من الأيام ويرسل لك بريمجا خبيثا كهذا.
وحتى تتضح الصورة بشكل أفضل لنفرض أن جهازك أصيب بأحد الديدان الحاسوبية ، وقامت هذه الدودة بالسطو على عناوين الحسابات البريدية [الإيميل] الموجودة في جهازك والخاصة برفقائك في العمل ، ولنفرض أن أحد هؤلاء الزملاء هو (عنتر) ، والآخر هو (عبسي) وبالطبع فكلكم تعرفون بعضكم جيدا بحكم العمل الذي يجمعكم ، وبما أن جهازك هو المصاب فإن الدودة سوف ترسل نفسها بهذا الشكل:

❖ رسالة تظهر باسمك ترسل إلى عنتر
❖ رسالة تظهر باسمك ترسل إلى عبسي
❖ رسالة تظهر باسمك ترسل إليك أنت [إذا كان عنوانك من ضمن القائمة التي تم السطو عليها]

وبالرغم أن أياً من جهازي عنتر أو عبسي لم يُصب بهذه الدودة ، إلا أنها تواصل خداعها عبر إرسال نفسها من جهازك أنت (الملوث) إلى عناوينهم البريدية بهذه الطريقة:

❖ رسالة تظهر باسم عنتر ترسل إليك [والذي يحصل هو أن الرسالة ترسل باسم زميلك ولكن من جهازك أنت ثم تعود مرة أخرى إليك].
❖ رسالة تظهر باسم عنتر إلى عبسي
❖ رسالة تظهر باسم عنتر إلى عنتر نفسه [هذا بالطبع إذا لم تكن الدودة على درجة كافية من الذكاء].

ونفس الأمر يحصل لعبسي ، فتقوم بإرسال رسالة إليه شخصيا ، وإليك أنت ، وإلى عنتر ، وتظهر الرسائل كلها على أنها قادمة من عبسي .
لذلك فلا تستغرب مثلا إذا جاءتك في يوم من الأيام رسالة انجليزية من صديقك (مرداح بن مرطاخ) – الذي تعلم يقينا أنه بالكاد يستطيع أن (يفك) الحروف العربية فضلا أن يعرف الانجليزية– تخبرك بأنك قد فزت بمبلغ مليون ريال وسيارة وبيت في جُزُرْ (واكو ماكو)، وحتى تحصل على تفاصيل استلام الجائزة فإنه يجب عليك أن تفتح الملف المرفق ، لتتفاجأ فيما بعد أن الملف لا يحتوي على تفاصيل ولا على (بطيخ) وإنما يحتوي على (السيدة دودي) التي تنتظرك بوافر الشوق داخل الملف.

البرامج الخبيثة وطرق الوقاية منها

❖ الانتشار عبر الثغرات الأمنية Security Holes:

انتشار الديدان عن طريق الثغرات الأمنية ، يتم بدون أن يستقبل (الضحية) أي ملف أو رسالة ، حيث تقوم الدودة بالبحث في الشبكة (الإنترنت مثلا) عن جهاز به ثغرة أمنية معينة ، وفي حال أنها وجدت هذا الجهاز ، فأنها سرعان ما تباشر هجومها بتحميل نفسها على الجهاز (بالطبع وصاحبه نايم في العسل) ، وعند هذه النقطة يبدأ (فيلم الرعب) الذي تقوم ببطولته السيدة دودي ، حيث تقوم ببث نفسها مرة أخرى من خلال جهاز الضحية إلى جميع من هم في قائمة برامج المحادثة -مثل الماسنجر وغيره- أو الموجودين في قائمة دفتر العناوين Address Book أو تقوم بالبحث في الشبكة -سواء شبكة الإنترنت أو الشبكة المحلية- عن كل من لديه ثغرة أمنية معينة وتنتقل إليه مباشرة.

د) أضرارها:

ضرر هذا النوع من البرامج الخبيثة يتوزع بين جهاز المستخدم (الضحية) وبين الشبكة التي يرتبط بها هذا الجهاز ، فبالنسبة للضرر الذي يمكن أن تحدثه في جهاز المستخدم فيتراوح بين تدمير البيانات أو المعلومات في الجهاز -إذا كانت الدودة من النوع التدميري- وبين المساهمة في بطء الجهاز وجعله يجمد أو يتوقف عن العمل ، وذلك من خلال استهلاكها لموارد الجهاز -كالذاكرة مثلا- من غير فائدة ، إضافة إلى جعلها للحاسوب مصدرا لإيذاء الغير وذلك من خلال انتشارها عن طريقه إلى أجهزة أخرى سليمة (وكيل معتمد لتصدير الديدان) ، سواء أكانت هذه الأجهزة مرتبطة بشكل مباشر مع الجهاز الملوث (كالشبكة المحلية) أو غير مباشر (كالإنترنت) ، [بالمناسبة ، هذا يعني أن جهازا ملوثا في جزر (الواق واق) يستطيع وبكل سهولة أن يصيب جهازك (بالمغص) إذا كان الجهاز مهيئا لاستقبال (السيدة دودي)].

أما بالنسبة لضررها على الشبكة فهو يتلخص في إثقالها للشبكة بحركة مرور كبيرة ، من خلال إرسال نفسها إلى أكبر قدر ممكن من العناوين البريدية (الإيميل) ، وبالطبع فإن هذه الإرساليات لابد وأن تمر عبر الشبكة (بغض النظر عن كونها ضارة أم نافعة) ومع كثرة هذه الإرساليات فإن الشبكة تصبح مثقلة بزخم هائل من حركة المرور التي لا فائدة منها ، مما قد يؤدي في النهاية إلى بطء الشبكة عموما ، إضافة إلى أن بعض الديدان مصمم ليقوم بالإطاحة بمواقع معينة ، من خلال هجمات حجب الخدمة الموزعة DDoS ، حيث تقوم بإغراق الموقع بسيل من طلبات التصفح التي تؤدي في النهاية إلى صعوبة الوصول للموقع أو انهياره بالكلية.

أصبحت شركة مايكروسوفت مضرب المثل في الثغرات الأمنية ، ويبدوا أنها دخلت موسوعة جينيس للأرقام القياسية (من أكبر أبوابها) ، فلا يكاد يمر أسبوع إلا وتقرأ أو تسمع عن اكتشاف ثغرة أمنية في أحد برامجها (وما خفي أعظم) ، والمصيبة (والطامة) أن بعض المخربين يقوم باستغلال عدم معرفة معظم الناس بوجود هذه الثغرات ، حتى بعد الإعلان عنها وإيجاد الرقعة المناسبة لها من قبل مايكروسوفت ، فيقوم المخرب ببرمجة دودة تقوم باستغلال هذه الثغرات وإيذاء كل من لم يقم بتحديث جهازه بالرقع المناسبة ، وأكبر مثال على ذلك هو دودة بلاستر Blaster التي أقضت مضاجع كثير من مستخدمي الكمبيوتر ، بالرغم أنها كانت مزعجه أكثر من كونها مدمرة (كانت تظهر رسالة تفيد أن الجهاز سوف ينطفئ بعد ٦٠ ثانية ثم يبدأ العد التنازلي حتى الصفر وينطفيء الجهاز بعدها) ، والطريف في الأمر أن هذه الدودة قد استغلت ثغرة أمنية كانت (مايكروزفت) قد أعلنت عنها قبل أكثر من شهر من ظهور الدودة ، بل وقامت بتزويد المستخدمين بالتحديثات اللازمة لسدها آنذاك ، ومع ذلك كله فإنها أصابت ملايين الأجهزة المرتبطة بالإنترنت حول العالم في غضون ساعات ، والسبب في ذلك أن كثير من الناس يحجم عن تحديث نظام التشغيل أولا بأول ، إما تكاسلا وإما جهلاً بوجود ثغرة أمنية أصلا ، أو لكون تنزيل التحديثات يستغرق وقتاً كبيرا. [أذكر أن بعض الناس أصيب بـ (لحسة) أو (لوثة) في عقله ، حيث أصبح يعيد تشغيل الجهاز بنفسه قبل أن تسبقه الدودة إلى ذلك ، ظنا منه أن هذا الفعل يمكن أن يغيظ الدودة ، ويجعلها تموت قهرا !!].

٤) دعاية ثم دعاية ثم دعاية ... شئت هذا أم أبيت:

هذا العنوان هو جزء من قصيدة أسميتها (دعاية بالغصب) وهي نوع من الشعر (المهترئ والمكسر) من بحر (وسع صدرك) ، وما دعاني لكتابة هذه القصيدة (العصماء طبعا) ، هو تضجري من شركات الدعاية التي تتسابق في هذه الأيام على حشر (أنوفها) في كل شيء حتى في الأحلام ، فيصبح الإنسان لا يرى إلا دعاية ولا يتحلم إلا بالدعاية ، ولايسمع إلا دعاية ، ولايستنشق إلا دعاية

البرامج الخبيثة وطرق الوقاية منها

(هذه دعاية آخر موديل) ، (ولايتمضمض) إلا دعاية (هذا النوع من الدعايات هو النوع الذي يفضله عبود ابن الجيران) ، وليت أن كل هذا يكون باختيار الإنسان ورضاه ، بل هو شيء قسري (يعني عاوز وإلا اضرب راسك في الحيطة) ، وأكبر دليل على هذا التطفل الدعائي هو برامج الدعاية الحاسوبية Adwares التي ظهرت مؤخرا في عالم الحاسوب ، وبدأت تحشر نفسها (على وزن تحشر خشمها) مع معظم البرامج (التي تدعي) أنها مجانية. في هذا الجزء سوف أتطرق إلى هذه (الكوابيس) الدعائية بشيء من التفصيل وأبين ضررها على المستخدم.

أ) ماهي البرامج الدعائية Adwares؟

البرامج الدعائية هي عبارة عن بريمجات صغيرة الحجم (وثقيلة الدم) غالبا ما تكون مرتبطة مع البرامج التي (تدعي) أنها مجانية Freewares ، حيث تقوم بتركيب نفسها مع هذه البرامج ، أو أنه يتم تحميلها من الإنترنت عن طريق بعض المواقع التي تقدم خدمات مجانية (كاستضافة المواقع وغيره) ، ومهمتها الأساسية هي إظهار الدعايات بشكل مستمر (وبصورة مقرفة) لمنتجات مختلفة ، سواء رغب بها المستخدم أم لم يرغب (يعني بالغصب) .

ب) مميزاتها:

تتميز هذه البرامج (الغثيثة) بصغر حجمها ومقدرتها على حشر نفسها في جهاز المستخدم سواء بعلمه أو بغير علمه ، حيث تقوم باستجلاب الدعايات التي (تمطر) بها المستخدم صباح مساء ، عن طريق خوادم مخصصة للدعايات موجودة في شبكة الإنترنت ، وتقوم هذه البرامج الدعائية باستجلاب الدعاية من هذه الخوادم عندما يتصل المستخدم بالإنترنت ، وغالبا ما يتم ذلك بدون علمه ، أما الميزة الأخرى والتي قد تصيب معظم المستخدمين بالحنق والغيظ فهي أن معظم الشركات المعنية بإنتاج البرامج أو السلع تعتبر هذه البرامج نظامية - بالطبع لأنها تروج لمنتجاتهم بشكل مباشر- حيث يزعم معظمهم أنها لا تحدث أضراراً بجهاز المستخدم ، وأن عملها على جهاز المستخدم مرتبط بموافقته على تحميلها على جهازه إما مباشرة عن طريق مواقع الانترنت أو بشكل غير مباشر عن طريق البرامج المجانية ، لذا فإن بعض مضادات الفيروسات -أو بالأصح مضادات البرامج الخبيثة- لا يكتشف هذه البرامج الدعائية ولا يصنفها على أنها برامج خبيثة.

ج) طرق انتشارها:

تنتشر هذه البرامج عن طريق البرامج المجانية التي يحمِّلها المستخدم من الإنترنت أو عن طريق برامج مشاركة الملفات -مثل برنامج كازا Kaza أو أوفرنت Overnet- أو عن طريق مواقع الإنترنت التي تطالب المستخدم بالموافقة على تحميل هذه البرامج الدعائية على جهازه ، حتى يستطيع الاستفادة من خدمات الموقع المجانية .

د) أضرارها:

تتراوح أضرار هذا النوع من البرامج الخبيثة -بتقديري الشخصي- بين الأضرار المعنوية و الأضرار الحسية ، فالأضرار المعنوية تكمن في إجبار المستخدم على مطالعة دعايات لم يطلبها أصلا أو لم يرض أن تظهر في جهازه بهذا الشكل وبهذه الطريقة ، إضافة إلى الكم الهائل من الإيذاء الذي سوف يشعر به عندما تظهر صور مخلة أو دعايات لمواقع إباحية أو مواقع مقززة ، خصوصا إذا كان يجهل كيفية إزالة هذا النوع من البرامج .
إما بالنسبة للأضرار الحسية فتظهر في الانخفاض الملحوظ لأداء الجهاز ، بسبب أن هذه البرامج تعمل بشكل مستمر على الجهاز وتستهلك قدرا كبيراً من موارده -كالذاكرة مثلا- وقد تتسبب في تعطل الجهاز أو بطئه ، بل وقد تتسبب أيضا في ظهور رسائل خطأ بشكل مستمر بسبب خلل في طريقة برمجتها أو عملها ، إضافة إلى كون هذه البرامج تستهلك جزءً ليس يسيراً من سرعة الاتصال بالإنترنت ، وذلك بسبب تحميلها المستمر للدعايات من الإنترنت ،مما يبطئ الاتصال بالإنترنت عموما.

ه) لصوص في وضح النهار (عينك عينك):

هذا ما ينطبق تماما على برامج التلصص Spywares، فبالرغم من أنها برامج تتلصص وتتجسس على خصوصيات المستخدم ، إلا أنها تتخذ وضعا قانونيا صحيحا (بحد زعم معظم الشركات) يجعلك تشعر بالحنق والضيق على كل من يسمها بذلك ، فهذه البرامج تسرقك في وضح النهار ، وأمام مرأى ومسمع بعض برامج الحماية من غير أن تحرك ساكناً ، ومن غير أن يكون لك حول أو قوة في منعها ، بحكم أنك وافقت مسبقا وبشكل أو بآخر على تركيبها في جهازك.

أ) ما هي برامج التجسس Spywares ؟

برامج التجسس هي عبارة عن بريمجات تقوم بجمع معلومات شخصية عنك وعن المواقع التي تزورها في الإنترنت وتقوم بإرسالها بدون علمك (غالبا) إلى جهة معينة ، لأهداف تسويقية أو تطويرية أو تجسسية أو غير ذلك من الأهداف غير المعلنة .[بالمناسبة هذه البرامج لو حصل لها أن تسرق مقاسات أو نوعية ملابسك لفعلت (وكأنه العيد) ، لأنها سوف تستفيد منها طبعا في إظهار الدعايات التي تلائمك ، عندها سوف تظهر لك دعاية تقول: اشتر فنيلة (علّاقي)

البرامج الخبيثة وطرق الوقاية منها

واحصل على سروال (أبو جرس) مجاناً].

ب) مميزاتها:

تتميز برامج التجسس بأنها لصيقة جدا ببرامج الدعاية Adware إذ أنها غالبا ما تعمل جنبا إلى جنب معها ، بل وتقوم بتركيب نفسها معها ، لأن برامج الدعاية غالبا ما (تقتات) على ما تغذيه بها هذه البرامج التلصصية من معلومات حول سلوك المستخدم وطريقة تصفحه للشبكة والمواقع التي يفضلها ، والصفحات التي يزورها بكثرة ، والمجال الذي يميل إليه ،وكل ذلك في الخفاء وبدون علم المستخدم ومن ثم تقوم بإرسال هذه المعلومات إلى جهات معينة ، تقوم بدراسة وتقييم هذه المعلومات وتستفيد منها في نواحي كثيرة غالبا ما تكون تسويقية ، وبالتالي فإنها تقوم بتغذية برامج الدعاية Adware الموجودة في جهاز المستخدم بما يتلائم مع ميول المستخدم.

وقد لا يتوقف الحد عند التجسس وحسب ، فبعض هذه البرامج يقوم بتركيب شريط في المتصفح يحتوي على دعايات تتغير بشكل مستمر بحسب المعلومات التي تم جمعها عن المستخدم ، وقد يتطور الأمر بها إلى إجبارك على فتح مواقع معينة عندما تحاول البحث في الانترنت عن طريق أحد محركات البحث -مثل قوقل Google- فبمجرد أن يعلم برنامج التجسس انك تحاول استخدام أحد محركات البحث فإنه سرعان ما يظهر لك نافذة منبثقة لأحد محركات البحث الذي يقوم بانتقائها هو ، والذي غالبا ما يكون مليئا بالدعايات والإعلانات التي سوف تصيبك (بالمغص)، ومن ثم فإنه يقوم بالبحث عن الكلمة التي أدخلتها نيابة عنك في تلك المحركات.

ومن الميزات المهمة لهذه البرامج هو مقدرتها على التخفي بشكل جيد في جهاز المستخدم، بحيث تصعب إزالتها بشكل يدوي ، وحتى لو تمكن المستخدم من إزالتها ، فإنها سرعان ما تعود لتركيب نفسها ، بسبب وجود بريمجات صغيرة تختبئ في أماكن متفرقة من الجهاز ، وظيفتها الأساسية هي استرجاع ملفات التجسس عندما يقوم المستخدم بحذفها.

ج) طرق انتشارها:

تنتشر برامج التجسس إما عن طريق بعض البرامج المجانية ، كالبرامج الخدمية وبرامج التسلية وبرامج مشاركة الملفات File Sharing Programs -مثل كازا Kaza و أوفرنت Overnet و إي دونكي Edonky- وإما عن طريق تحميلها من الإنترنت عبر بعض المواقع التي تطالب المستخدم بتركيب بريمجات معينة أو متحكمات (أكتيف اكس) Active X كشرط لدخول الموقع أو الاستفادة من خدماته.

❖ الانتشار عبر البرامج:

ويتم ذلك عن طريق تركيب برنامج معين بحيث تكون برامج التجسس مصاحبه له ، وتقوم بتركيب نفسها معه سواء بعلم المستخدم ، عن طريق موافقته على اتفاقية تركيب البرنامج ، أو من غير علمه، خصوصا إذا كانت تخدم جهات مشبوهة أو كان هدفها تخريبي كما سوف يأتي في الأضرار ، وحتى تكون الشركات المنتجة لهذه البرامج في منأىً عن مخالفة قوانين الخصوصية التي تشرعها الكثير من المنظمات والدول ، فإن بعض هذه الشركات تذكر بشكل مبهم وغير مباشر في اتفاقية تركيب البرنامج المرافقة له ، أنها تقوم بجمع معلومات عن المستخدم ، وأنها تقوم بإرسال هذه المعلومات لجهات معينة بقصد تطوير برامجها ، أو من أجل تخصيص الدعايات التي تقوم برامج الدعاية ببثها عليك ، وغير ذلك من الأهداف ، وبالطبع فإن معظم المستخدمين لا يقرأ هذه الاتفاقيات أصلا ، إما لطولها أو لتعمد بعض الشركات كتابة اتفاقيات مبهمة تجعل القارئ في حيرة من أمره حول مقصد الشركة من هذه الفقرة أو تلك ، لتستغلها الشركة فيما بعد لصالحها عند حدوث خلاف بينها وبين المستخدم حول انتهاك الخصوصية.

❖ الانتشار عبر مواقع الإنترنت:

ويتم ذلك عن طريق زيارة بعض المواقع في الإنترنت التي تطلب من المستخدم تركيب برامج معينة لدخول الموقع أو الاستفادة من خدماته ، وغالبا ما تكون هذه البرامج عبارة عن متحكمات أكتف إكس Active X ، فبمجرد أن يوافق المستخدم على ذلك ، فإنها سرعان ما تقوم بتركيب نفسها على جهازه ، ومن ثم تبدأ عملها في الخفاء وبدون أن يشعر المستخدم بها. (بالمناسبة هذا لا يعني أن كل متحكمات أكتف اكس التي تقوم المواقع بتركيبها ضارة ، فمنها

وماهي اتفاقية استخدام البرنامج؟

اتفاقية استخدام البرنامج هي عبارة عن النص الانجليزي الطويل الذي يظهر مع بداية تشغيل معظم البرامج ويأتي في أسفلها زرين أحدهما مكتوب عليه أوافق Agree والآخر مكتوب عليه لا أوافق Disagree ، وبالطبع فإن كثيرا من المستخدمين (يتسلى) باختيار زر الموافقة على الاتفاقية ، لأنه لا يقرأها (ولا يمر عليها أصلا) بل إن بعضهم قد تكون هذه هي المرة الأولى التي يعرف فيها أن هناك اتفاقية لتشغيل البرامج !!

البرامج الخبيثة وطرق الوقاية منها

ما هو ضروري وهام للاستفادة من خدمات موقع معين ، كتلك الموجودة مثلا في موقع التحديثات الخاص بشركة مايكروسوفت (windowsupdate.microsoft.com)

أضرارها:

من أهم الأضرار التي تحملها هذه البرامج ، هو جمعها للمعلومات عنك وإرسالها بدون علمك إلى جهات خارجية ، بغض النظر عن أهداف ومقاصد تلك الجهات ، والمصيبة أن تلك الجهات قد لا تكون جهات دعائية أو تسويقية ، بل قد تكون جهات مشبوهة يكون مقصدها هو التخريب ، فقد لوحظ في الآونة الأخيرة أن بعض البرامج التجسسية تعود بالمعلومات التي يتم جمعها عنك إلى بعض المخربين (الهاكرز) ، وقد تكون هذه المعلومات عبارة عن بريدك الشخصي أو كلمات المرور التي تقوم بإدخالها في مواقع الإنترنت أو أرقام البطاقات الائتمانية الخاصة بك ، بل وقد يتعدى الأمر ذلك إلى جعل هذه البرامج التجسسية أداه في يد (الهاكر) أو المخرب، يستخدمها لتركيب برامج خبيثة على جهازك. [لا تستغرب إذا أتتك رسائل على بريدك الشخصي تحييك باسمك وتطلب منك زيارة مواقع معينة ، بالرغم إنك لا تعرف هذه الجهات من قبل ولم تقم بإعطائها بريدك الشخصي أصلا].

ومن المضار أيضا أن هذه البرامج غالبا ما تسبب بطءً عاما في أداء الجهاز ، قد يصاحبه ظهور رسائل خطأ بشكل متكرر وذلك بسبب استهلاكها جزء كبيرا من موارد النظام من غير فائدة تعود على المستخدم ، إضافة إلى كونها مصدراً للبطء الحاصل عند تصفح الإنترنت جراء استخدام هذه البرامج جزء من سرعة الارتباط بالإنترنت في تحميل الدعايات أو إرسال المعلومات التي تم جمعها عن المستخدم.

وإضافة إلى ما ذكرنا سابقا ، فإن بعض هذه البرامج التجسسية يقوم بمنعك من الوصول إلى المواقع التي تعينك على إزالتها أو تقدم مضادات لها ، وذلك من خلال إقفالها -وبشكل قسري- لنوافذ المتصفح التي تشير إلى تلك المواقع.

٦) اختطاف حتى في الحاسوب!!

يبدو أن مسلسل الإجرام والمكر ليس له حدود مع هذه البرامج الخبيثة ، فمن تخريب إلى تجسس إلى سطو ثم أخيرا إلى اختطاف ، وهذا أكبر دليل على أن عفاريت البرمجة قد استفادوا جيداً من عفاريت الإنس هذه الأيام ، وعلموهم أن الاختطاف لا يكون دوماً للطائرات وحسب ، بل يمكن أن يكون لأجهزة الحواسيب ، وبالطبع فكل ذلك يجعلك (تموت قهراً) خصوصا إذا كنت ترى عملية السطو والاختطاف لجهازك أمام ناظريك ، ولا تستطيع أن تفعل شيئا سوى ترديد عبارة (سمعنا و أطعنا) للبرنامج المختطف.

أ) ما هي مختطفات المتصفح Browser Hijackers:

هذه البرامج تدخل ضمن البرامج المتطفلة على خصوصيات المستخدم حيث تقوم بأفعالها المشينة عن طريق تغيير سلوك متصفح إنترنت ، وجعله مستنقعا للدعايات ، إضافة إلى اختطاف الصفحة الرئيسية للمتصفح (من بين يدي المستخدم) وجعلها تشير دائماً إلى أحد المواقع الدعائية.

ب) مميزاتها:

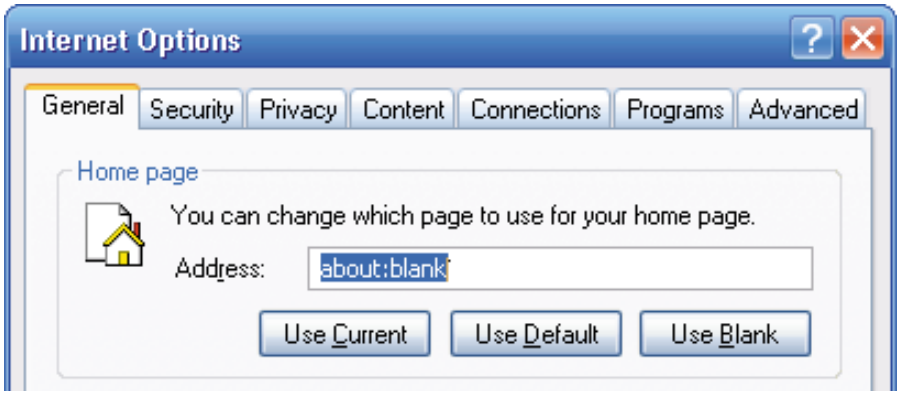
تمتاز هذه البرامج (كأغلب البرامج الخبيثة) بصغر حجمها ، وسهولة انتشارها في جهاز المستخدم ، وقدرتها على التخفي في أنواع كثيرة من الملفات ، مما يؤدي إلى صعوبة إزالتها يدوياً ، خصوصا وإنها غالبا ما تقوم بإحداث بعض التغييرات في ملف سجل النظام System Registry File.

ج) طرق انتشارها:

غالبا ما ينتشر هذا النوع من البرامج التطفلية الخبيثة عن طريق مواقع الإنترنت ، حيث يعرض الموقع على زواره ضرورة تركيب برنامج معين (من نوع أكتيف اكس Active X مثلا) حتى يعمل الموقع بشكل جيد ، وحالما يوافق الزائر على ذلك فسرعان ما يقوم هذا البرنامج الخبيث بتحميل نفسه على جهاز المستخدم ، وتبدأ بعدها عملية السطو والاختطاف (وأي حركة حنضرب بالمليان).

د) أضرارها:

يجمع هذا النوع من البرامج بين مضار



تعمد برامج الاختطاف إلى تغيير عنوان الصفحة الرئيسية للمتصفح

البرامج الخبيثة وطرق الوقاية منها

البرامج الدعائية Adwares وبرامج التلصص Spywares (حشفٌ وسوءُ كيل) ، فهي تقوم بالتلصص على سلوك المستخدم وعلى المواقع التي يقوم بزيارتها دائماً ، ثم تقوم بإظهار الدعاية تبعا لذلك ، إضافة إلى اختطافها للصفحة الرئيسية للمتصفح وجعلها تشير دائماً إلى مواقع دعائية أو إباحية ، وحتى لو حاول المستخدم تغيير هذه الصفحة فإنها سرعان ما ترجع لتشير إلى الصفحة الدعائية مرة أخرى ، ولا ينتهي الأمر عند هذا الحد بل إن هذه البرامج الخبيثة تقوم بإضافة شريط أدوات جديد في متصفح الإنترنت -إكسبلورير مثلاً- يحتوي على بعض الأزرار التي تؤدي إلى مواقع بحث مليئة بالدعايات أو مواقع دعائية عامة أو مواقع فاضحة (وكل ذلك يعتمد على هدف البرنامج) ، علاوة على وضع وصلات على سطح المكتب أو في المفضلة تؤدي إلى مواقع دعائية أو إباحية ، وكل ذلك طبعا من غير علم المستخدم أو رضاه ، ويصاحب هذه الأفعال (المشينة) بالطبع بطء في جهاز الحاسوب عموما ، وانهيار متكرر لنظام التشغيل أو ظهور رسائل الخطأ بشكل كبير، إضافة إلى بطء في تصفح الإنترنت ، لأن تحميل الدعايات بشكل متكرر ينهك موارد الجهاز ويؤثر على سرعة الاتصال بالإنترنت.

٧) المتصلات التلقائية .... القاتل الصامت:

الكثير منا حريص على أن تكون مصروفاته الخاصة بالهاتف متزنة ، فتجده يحاول جاهدا أن يضع سقفاً محدوداً للمكالمات يتعهد بأن لا يتعداه كل شهر ، بل وتراه ينصح أهله وأبناءه وإخوانه بعدم التبذير في استخدام الهاتف فيما لا ينفع ، وكل من يخالف ذلك فمصيره ركلات من النوع الصاروخي (بووووووز) ، أو أنه سوف يصبح (دمية) يتم تجربة آخر ضربات (الكاراتيه) عليها ، ولكن ماذا لو جاءت فاتورة الهاتف وفوجئت أن هناك مكالمات بآلاف الريالات إلى مناطق لم تسمع بها من قبل (مثل جزيرة (الديك ابو رفسه) ، أو منطقة (إذا في راسك حب ما انطحن نطحنه لك)) قد أجريت من هاتفك وأن أحداً من أهلك أو أقاربك لا يعلم عنها أو لم يقم بإجرائها؟؟ في السطور القادمة سوف نعرف من الذي قام بهذه الفعله ، ولماذا فعل ذلك.

أ) ما هي المتصلات التلقائية Dialers :

المتصلات التلقائية هي عبارة عن بريمجات ، تقوم باستخدام حاسوبك الموصول بالهاتف -عن طريق المودم- لإجراء مكالمات (من غير علمك) إلى عدد من الأرقام الهاتفية ذات التكلفة المرتفعة جدا ، بهدف الحصول على عوائد مالية جراء هذا الاتصال.

ب) مميزاتها:

تمتاز هذه البريمجات بأنها تعمل في الخفاء لتحقق مآربها الشيطانية ، إذ أنها تجري الاتصال عندما تحس بأنك لا تعمل حاليا على الجهاز (بالطبع وجهازك موصول بالهاتف)، فتغتنم هذه الفرصة لتقوم بالاتصال بأرقام دولية عالية التكلفة لمدة معينة ، يذهب جزء كبير من ريعها إلى منتج البرنامج المتصل (مثل أرقام ٧٠٠).

ج) طرق انتشارها :

كغيرها من البرامج الخبيثة ، يمكن أن تنتقل هذه البرمجيات كمرفقات عن طريق البريد الإلكتروني ، أو كمتحكمات أكتيف اكس تطالب مواقع معينة بتركيبها (وهذا الغالب) ، أو بتحميل نفسها تلقائيا عن طريق استخدام ثغرات أمنية موجودة في برنامج معين أو في نظام التشغيل (تم اكتشاف مثل هذه الحالات مؤخراً).

د) أضرارها:

تتلخص أضرار هذه النوعية من البرامج الخبيثة في إجبارها للمستخدم على دفع قيمة مكالمات هاتفية لم يقم بإجرائها أصلا ، من خلال الاتصال خلسة بأرقام معينة بهدف تحصيل جزء من ريع هذه المكالمات.

٨) وراك وراك والزمن طويل:

يبدو أن صانعي البرامج لم ييأسوا بعد من بث سمومهم إلى الناس ، فإن لم تطلك برامجهم الخبيثة ، فإنك لن تسلم حتما من شائعاتهم الماكرة ، التي تستحثك في بعض الأحيان على إيذاء نفسك أو إيذاء الآخرين (وبكل دلاخة) ، وهذا كله بالطبع وأنت في كامل قواك العقلية ، ولكن كيف يمكن أن يحصل ذلك؟؟ تابع معنا وسوف تعرف السر (لا تعلم أحد !!)

أ) ما هي الشائعات الحاسوبية:

هي عبارة عن خبر كاذب ، غالبا ما ينتشر عن طريق الإنترنت ، يشير إلى أن هناك ملفات تجسس مزروعة في جهازك ويجب عليك حذفها -قد تكون من ملفات النظام الأساسية- أو أن هناك ثغرات أمنية في نظام التشغيل قد تستغل من قبل الهاكرز ويجب عليك حذف ملفات معينة حتى تقي نفسك منهم ، كما ويستحثك الخبر على نشر هذه الرسالة بين أصدقائك ومعارفك حتى يتجنبوا هذا البلاء من خلال حذف تلك الملفات .

ب) مميزاتها:

تتميز هذه الشائعات باحتوائها على أمرين ، أحدهما المطالبة بحذف ملفات معينة غير مرغوب فيها إما لكونها ملفات تجسس أو لكونها قد تستغل من قبل الهكر ، والأمر الآخر أنها دائما ما تنصح بتوزيع هذا الخبر أو التحذير وإرساله إلى أكبر قدر ممكن من مستخدمي الحاسوب وذلك بقصد النصح -زعموا-.

ج) طرق انتشارها:

تنتشر هذه الشائعات عموما عن طريق مواقع الإنترنت (المنتديات الحوارية أو ساحات النقاش) ، أو عن طريق البريد الإلكتروني أو عن طريق مواقع الدردشة ، أو عن طريق قوائم النقاش والحوار News Groups ، أو عن طريق الطرق التقليدية كأن يخبر شخص مجموعة من الزملاء أو الجيران بهذا الخبر.

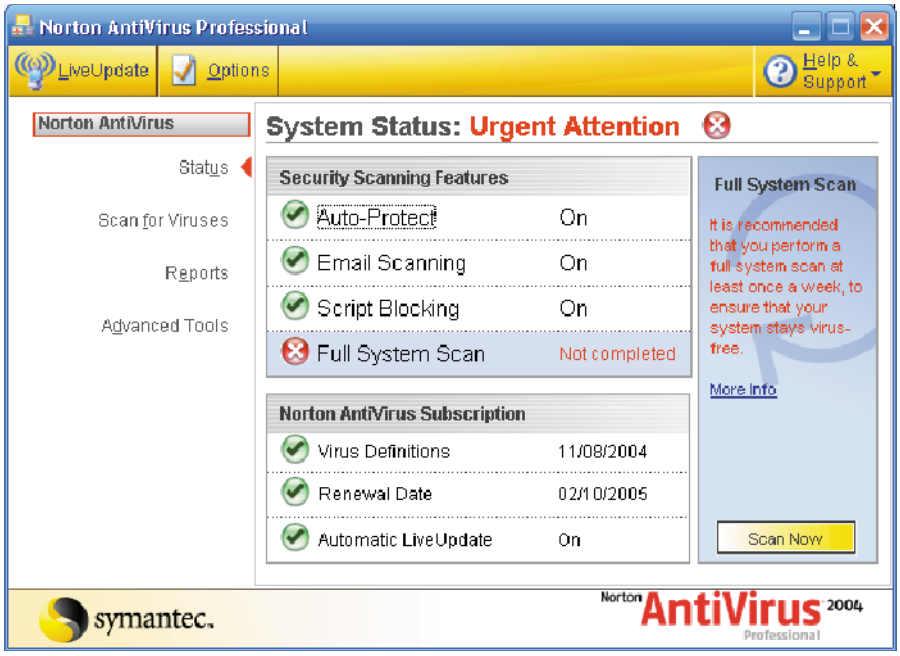
د) أضرارها:

أكبر ضرر يجنيه المستخدم هو أنه قد يقوم بحذف ملفات مهمة لتشغيل النظام أو ضرورية لأحد البرامج الرئيسية -كمضادات الفيروسات مثلاً- ويعطل بذلك عملها ، مما يؤدي في النهاية إلى انهيار النظام و تعطله ، أو توقف أحد البرامج المهمة عن العمل -كمضاد الفيروسات- بسبب عملية الحذف هذه ، فيستفيد الخبثاء (الهكرز) من ذلك في بث برامجهم الخبيثة ، علاوة على أن انتشار الشائعة سوف يؤدي بدوره إلى حصول حركة مرور كبيرة في الإنترنت خصوصا مع بدء نشر المستخدمين لها عن طريق البريد الإليكتروني أو مواقع الحوار ، مما يؤدي (في بعض الأحيان) إلى بطء عام في تصفح الإنترنت أو انهيار بعض مزودات (خوادم) Servers البريد الإلكتروني في الإنترنت بسبب الضغط الحاصل عليها جراء تراسل المستخدمين لهذه الشائعة أو (الشلخة).

إذاً كيف السبيل للخلاص من ذلك كله؟؟

السبيل هو أن تقوم بعرض جهازك للبيع في أقرب محل (تشليح) ، وإذا لم تفلح في بيعه في التشليح فعليك (بالتشليخ) أي تكسير الجهاز ولكن بطريقة مبتكرة ، وذلك بإعطائه لـ (غميص) ابن الجيران ليتولى هو تلك المهمة ووفق أحدث التقنيات وذلك باستخدام نوع من العصي يسمى (العجرة) غالبا ما يستخدم في المشاجرات الثقيلة ، وإذا لم ترُقْ لك أي من هذه الطرق ، فأني أنصحك عندها بان تقوم بتحويل جهازك لمصيدة ولكن للقطط من شاكلة القط (أبو عنتر وباقي الشلة) ، وهذه المصيدة سوف تضمن لك التخلص من سيمفونية (المواء) التي يتحفك بها (ابوعنتر) يوميا ، عندها سوف تحس أنك استفدت من جهازك حق الاستفادة حتى بعد التخلص منه !!!

بالطبع هذه الطرق وغيرها (يوجد لدي الكثير منها) تعتبر حلا جيداً يمكنك تطبيقه ، إذا وصل بك اليأس إلى مراحل كبيرة ، تجعلك تحس بالنشوة وأنت تفعل ماسبق ، ولكن قبل أن تُقْدِم على أي من هذه الأعمال (الانتحارية !!) أنصحكً أن تتريث قليلاً ، وتقرأ بعض النصائح التي سوف تعينك على المحافظة على جهازك لأكبر مدة ممكنة وبقدر قليل من المشاكل.



احرص دائما على تحديث برنامج مكافحة الفيروسات حتى تقي نفسك شر الإصابة بالفيروسات حديثة الانتشار

هناك الكثير من الشركات التي تنتج برامج الحماية من الفيروسات ، ومن أشهرها شركة سيمانتك Symantec التي تنتج برنامج نورتون Norton Antivirus (موقعها: www.symantec.com) ، وشركة مكافي McAfee التي تنتج برنامج McAfee Antivirus (موقعها: www.mcafee.com).

البرامج الخبيثة وطرق الوقاية منها

من المؤسف حقاً أن تقوم بعض الشركات باستخدام أساليب دنيئة وجبانة للإطاحة بمستخدمي الحاسوب ، ومن هذه الأساليب هو أن بعض الشركات تقوم بتسويق برامج على أنها تفحص الجهاز ضد المتلصصات والبرامج الدعائية (وتدعي) أنها تقوم بإزالتها ، وفي حقيقة الأمر فإنها تفعل ذلك جزئيا ، حيث تقوم بإزالة بعض هذه البرامج الخبيثة ، ولكن الدناءة تكمن في أنها (أي هذه البرامج المضادة للمتلصصات) تقوم بزرع متلصصات خاصة بها في جهاز المستخدم لتستخدمها فيما بعد في عرض الدعايات (وترجع حليمة لعادتها القديمة) ، فيجب الحذر منها ، وتركيب ما هو معروف ومشهور من البرامج (البرامج التي ذكرتها في المقالة هي برامج موثوقة ومأمونة بإذن الله).

درهم وقاية خير من قنطار علاج:

هذا المثل القديم ، يصلح لأن يكون شعارك في كل شيء ، فمتى ما استطعت أن تكون في منأى عن الكوارث والنكبات ، وكنت استباقيا في حلها عندما تظهر بوادرها الأولى ، كلما كان بوسعك النوم قرير العين وأنت ترفل (بشخير) هادئ ، وأحلام سعيدة. وحتى تحصل على ذلك فإليك هذه النصائح:

١) ركب برنامجا مضاد للفيروسات :

برامج مكافحة الفيروسات هي خط دفاعك الأول ، خصوصا وأنها تعمل طوال الوقت وفي الزمن الحقيقي Real Time لتفحص ملفاتك ضد الفيروسات وأحصنة طروادة والديدان ، فقم بتركيب أحدها واحرص دائما على تحديثه (تأكد دائما من حداثة ملف تعريف الفيروسات عن طريق تاريخ الملف الذي يعرضه برنامج مضاد الفيروسات) ، فقد تصاب ببرنامج خبيث ظهر حديثاً ، وإذا لم يكن مضاد الفيروسات محدثاً فإنه حتماً لن يكتشف ذلك البرنامج).

٢) لا تقم بتركيب أي برنامج على جهازك حتى تتأكد منه:

احذر تركيب أي برنامج على جهازك ما لم تكن واثقا بمحتواه والجهة التي أنتجته ، واحرص على البرامج المشهورة ذات السمعة الجيدة ، وافحصها قبل التركيب ببرامج مكافحة الفيروسات والبرامج المكملة لها.

٣) لا تقم بتركيب أي من متحكمات أكتيف اكس Active X إلا من المواقع المأمونة:

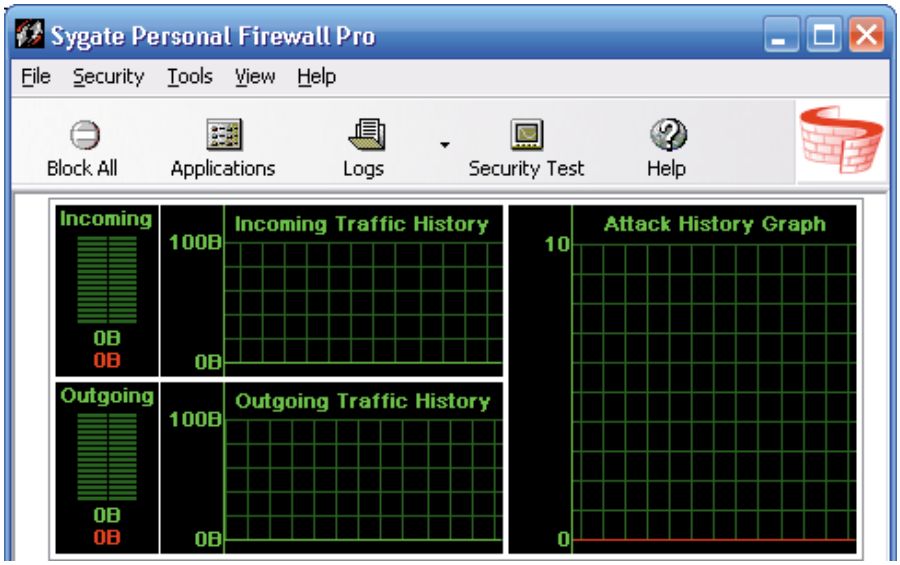
متحكمات أكتف إكس سلاح ذو حدين ، فقد تستخدم لمصلحتك وقد تستخدم ضدك ، وأنا أنصحك شخصيا بأن لا تقوم بتركيب أي منها (إلا تلك الخاصة بالمواقع المشهورة مثل موقع مايكروسوفت وماكروميديا وغيرها ..) لأن نسبة كبيرة منها قد ثبت استغلاله في الآونة الأخيرة، استغلالاً سيئا لبث المتلصصات والبرامج الدعائية والفيروسات عموما.

٤) حدث ثم حدث ثم حدث:

بين الفترة والأخرى يتم اكتشاف ثغرات أمنية في نظام التشغيل لديك ، وقد تستخدم هذه الثغرات ضدك ، فقم بتحديث نظام التشغيل لديك مرة على الأقل كل أسبوع حتى تكون في مأمن من بعض هذه البرامج الخبيثة ، ويمكنك جعل ويندوز يحدث نفسه تلقائيا بمجرد اتصالك بالإنترنت عن طريق تفعيلك لخاصية التحديث التلقائي من: ابدأ> لوحة التحكم> النظام> التحديثات التلقائية ثم التأشير على خيار تلقائي [موقع تحديثات ويندوز: (windowsupdate.microsoft.com)]

٥) قم بتركيب جدار ناري Firewall على جهازك :

الجدر النارية هي أنجع طريقة لسد جميع منافذ الاتصال Ports غير المستخدمة في جهازك ، وبالتالي تقليص القاعدة التي



تحميك الجدر النارية من العديد من الهجمات القادمة من الانترنت ، بالإضافة إلى أنها لاتسمح لأي برنامج في جهازك بالاتصال بالإنترنت إلا بعد أخذ موافقتك.

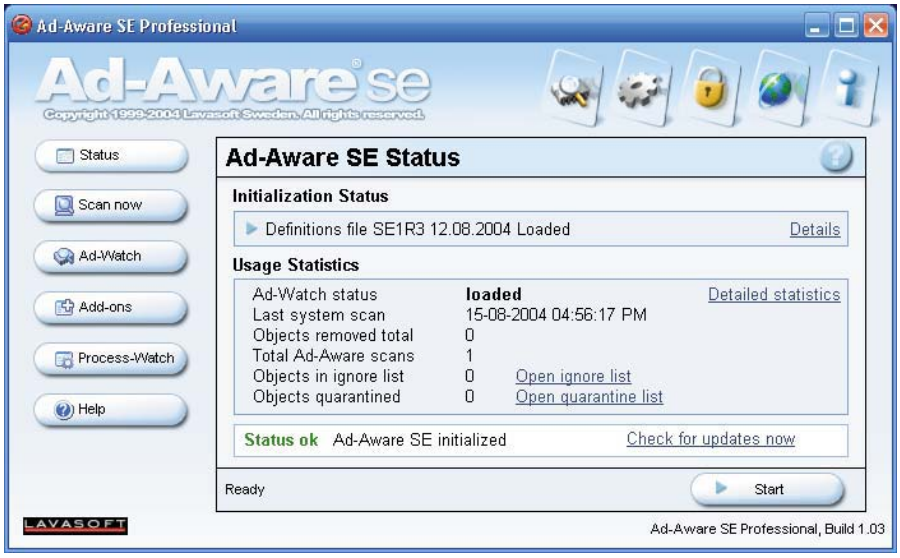
قد يستخدمها المخربون للولوج إلى جهازك ، إضافة إلى قيامها بترشيح حركة مرور البيانات من وإلى جهازك واستبعاد ما كان ضاراً منها ، علاوة على كونها سداً منيعاً في حجب أي اتصال خارج من جهازك إلى الإنترنت ما لم تأذن به ، فلو أصبت مثلا بحصان طروادة في جهازك ، فلن يسمح الجدار الناري لهذا البرنامج الخبيث بالاتصال ما لم تأذن له ، وهذا يقيك -بإذن الله - من أن يتمكن أحد هذه البرامج من إرسال البيانات الخاصة بك ، أو التوالد وإرسال نفسه حتى بعد إصابتك به. (من الجدر النارية الجيدة والموثوقة برنامج Sygate Personal Firwall الذي تنتجه شركة Sygate المشهورة ببرامج ومعدات الجدر النارية [عنوان موقع الشركة: www.sygate.com].

٦) لا تقم بفتح الملفات المرفقة مع البريد الإلكتروني إلا إذا كان مصدرها موثوقا:

الكثير من البرامج الخبيثة يستخدم الإنترنت والبريد الإلكتروني كناقل له ، لذلك لا تقم أبدا وتحت أي ظرف من الظروف بفتح أي ملف يأتي مرفقا مع البريد الإلكتروني ما لم تكن متوثقا من المرسل [تذكر أن بعض الديدان الحاسوبية قد تستخدم اسم صديقك لإرسال نفسها إليك ، عندها يجب التأكد من المرسل شخصيا عن طريق مهاتفته إذا استلزم الأمر ذلك ، أو الاتفاق على رمز سري بينك وبينه بحيث يكون في نص الرسالة أو في موضوعها حتى تتوثق أن من قام بإرسال الرسالة إليك هو فلان وليس البرنامج الخبيث].

٧) قم بتركيب البرامج المكملة لمضاد الفيروسات:

برامج مضاد الفيروسات لا تكفي وحدها لحمايتك حماية كاملة ، خصوصا وأن أغلبها لا يتعرف على البرامج الدعائية



مضادات البرامج الدعائية وبرامج التجسس ، تحميك من العديد من البرامج الخبيثة التي لايكتشفها الكثير من مضادات الفيروسات في العادة.

أو المتلصصات أو المتصلات التلقائية أو مختطفات المتصفح ، لذا فيجب عليك أن تقوم بتركيب أحد البرنامج المكملة لمضاد الفيروسات ، ومنها على سبيل المثال لا الحصر برنامج Ad-Aware SE Professional من شركة Lavasoft [عنوان موقع الشركة: www.lavasoftusa.com] أو البرنامج الرائع والمجاني Spybot-S&D من شركة Safer Networking [عنوان موقع الشركة: www.safer-etworking.org]

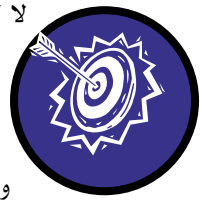
٨) اشترك في أحد النشرات الدورية المتخصصة في أمن المعلومات:

هناك الكثير والكثير من النشرات الإلكترونية والمجانية التي تناقش موضوع أمن الحاسوب الشخصي ، وتطلعك على آخر المستجدات والمخاطر ، قم بالاشتراك في إحداها حتى تكون ملما بآخر التطورات في هذا المجال ، أو لتتعرف على آخر المخاطر أو الثغرات الأمنية التي تم اكتشافها وكيفية الوقاية من أضرارها.

٩) لا تقم بنشر أي تحذير يحثك على حذف ملفات معينة حتى تتوثق من الخبر:

فالكثير من لصوص الحاسوب والمخربين يعز عليهم أن تنعم بجهاز مستقر وآمن ، ولذلك فإذا استقبلت أحد هذه الشائعات أو الأخبار التي تحثك لحذف ملفات معينة من جهازك فلا تقم بذلك أبدا ، وبادر بزيارة أحد مواقع الشركات المشهورة والمتخصصة في مكافحة الفيروسات مثل شركة مكافي (www.mcafee.com) أو شركة سيمانتك (www.symantec.com) ، وتأكد من ذلك الخبر بنفسك ، أو شاور أهل الخبرة والاختصاص قبل أن تقدم على ذلك العمل.

ماذا لو وقع الفأس في الرأس:



لا أظن أن اتصالك بالرقم ٩٩٩ لطلب النجدة ، قد يفيدك أو يجديك في هذه الحالة ، لأن المخربين واللصوص في هذه الحالة من نوع آخر ، يتعذر على النجدة أو الشرطة الإمساك بهم ، ولكن يمكنك أن تتعلم كيف تدافع عن نفسك منهم في حالة حدوث سطو أو تسلل لجهازك عن طريق أحد هذه البرامج الخبيثة.

البرامج الخبيثة وطرق الوقاية منها

إذا أصاب جهازك أي من هذه البرامج الخبيثة أو شككت بذلك فقم بعمل الآتي:

١) تأكد من أن الجدار الناري لديك يعمل بشكل سليم.

٢) حدث نظام التشغيل لديك بشكل كامل.

٣) حدث برنامج مضاد الفيروسات الذي تستخدمه بالإضافة إلى البرامج الأخرى المكملة له.

٤) قم بقطع اتصال جهازك بالإنترنت.

٥) قم بعمل فحص شامل لجهازك عن طريق برنامج مكافحة الفيروسات والبرامج الأخرى المصاحبة له (برامج إزالة ملفات الدعاية والتجسس التي ذكرناها سابقا)

٦) إذا كان الجهاز ينهار ويعيد التشغيل بمجرد اتصالك بالإنترنت ، فقم بقطع الاتصال بالإنترنت ، وقم بتحميل التحديثات المذكورة سابقا عن طريق جهاز أحد زملائك ، ثم قم بتركيبها في جهازك واعمل فحصا شاملا لجهازك كما ورد سابقا.

٧) إذا لم تفلح أي من الخطوات أعلاه في حل مشكلتك ، فقم بعرض جهازك على فني مختص بالحاسوب.

ختاما:

أتمنى أن أكون قد وفقت في استعراض أهم أنواع (المنغصات) الحاسوبية التي قد تصيبك (بالأرق) طوال الليل ، وتصيب جهازك (بالمغص والحمى)، وطرق الوقاية منها والعلاج ، حتى تنعم بحوسبة آمنة وموثوقة بإذن الله تعالى.

يسعدني استقبال ملاحظاتكم وآرائكم حول هذه المقالة ، أو اقتراحاتكم حول المواضيع التي تودون التطرق إليها ومناقشتها مستقبلا على البريد الإليكتروني:

techeditor@hotmail.com