اعداد وتصميم: بنبري أيوب

الفيروسات

نظرة معمقة

مقدمة

عزيزي القارئ...

في ظل التطور الحاصل في مجتمعنا العربي، ومع تعميم تكنلوجيا الإنترنت. ولأن المخترقين بأصنافهم "يتفننون" في إيجاد أحدث الطرق والثغرات للتسلل إلى الأجهزة، تخريبها... أصبح من الواجب على المستخدم العادي معرفة ما يواجه من أخطار قصد حماية نفسه. من هنا جاءت فكرة تأليف هذا الكتيب. لن أطيل عليك ـعزيزي القارئـ وسأتركك مع صفحات هذا الكتيب...

المؤلف،

الفصل الأول

مدخل إلى عالم الفيروسات

أهمية التعرف على الفيروسات

يتحدث أغلب الناس عن الفيروسات وكأنها شيء ضار يمكن القضاء عليه باستخدام مضاد فيروسات. وهذا مفهوم خاطئ كليا. فهناك عدة أنواع من الفيروسات ستتعرف عليها -عزيزي القارئ- في الصفحات القادمة من هذا الكتاب. كما أن مضاد الفيروسات ليس الوسيلة الوحيدة للقضاء عليها، في الواقع لم يتم تصميم مضاد للفيروسات يوفر الحماية بنسبة 100% ضد الفيروسات. لكنه يبقى مكونا أساسيا لا يمكن الاستغناء عنه. ومن جهة أخرى، يتوجب عليك أخذ ولو لمحة بسيطة عن الفيروسات، أنواعها، كيفية اكتشافها والقضاء عليها... لتساعد مضاد الفيروسات على إبقاء حاسوبك آمنا. فبمعرفتك لكيفية عمل الفيروس، ستتجنب الأضرار التي يمكن له التسبب بها أو على الأقل توقعها. لاحظ أن الكثيرين لا يعلمون أن حاسوبهم مصاب بفيروس (أو عدة فيروسات) حتى يفوت الأوان ويصبح القضاء عليه أمرا مستحيلا.

تعريف الفيروس Virus

الفيروس هو ملف تنفيذي غالبا (يحمل اللاحقة exe.)، يكون عادة صغير الحجم. كما أن له القدرة على نسخ نفسه في أماكن

عديدة على جهاز الضحية أو استخدام جهازه كوسيط لنقل نفسه إلى حواسيب أخرى. أيضا، يمكن للفيروس دمج نفسه مع برامج أخرى. والمستخدم العادي لا يمكنه رؤية عملية النقل أو الدمج غالبا حتى يتم تفعيل الفيروس أي بعد فوات الأوان.

ملاحظة

عند تعريفي للفيروس، أخبرتك أنه يحمل اللاحقة exe. غالبا. وقد أضفت "غالبا" لأن هناك فيروسات يقوم مصمموها بتغيير لاحقتها للتمويه. فمثلا، قد تردك صورة كملف مرفق Attachement في رسالة إلكترونية "إيميل" وتفتحها أنت فتجدها حقا صورة وتحمل امتداد صورة أيضا إلا أنها في حقيقة الأمر فيروس.

حصان طروادة [التروجان] Trojan horse

هو برنامج صغير الحجم يتطلب عمله وجود الإنترنت. أين يمكن أن يصلك مدمجا مع برنامج، أو مرفقا في رسالة إلكترونية. حيث يستهدف أماكن محددة في النظام (تحديدا السجلات Registers) كما يختبأ في أحد مجلداته ويدعى هذا الملف بالخادم Server. وعندما يتم تفعيله بأحد الطرق التي سنراها لاحقا يبدأ بإرسال معلومات الضحية إلى مبرمج الفيروس الذي يمكنه التحكم بهذا الأخير وإعطائه أوامر جديدة لتنفيذها عبر برنامج مرتبط به يدعى بالعميل Client. أغلب التروجانات يتم كشفها من طرف برامج

الحماية أياما بعد نشرها، ولتضمن أعلى نسبة حماية لا تكتف بمضاد فيروسات Anti-virus واستخدم جدارا ناريا Firewall (سنتحدث عنه لاحقا).

الديدان Worms

الدودة نوع من الفيروسات يقوم بدمج نفسه تلقائيا مع كل برنامج يتم تشغيله، ليقوم لاحقا بتدمير كل برنامج التصق به تدريجيا. وفي حال نقل الضحية لأحد البرامج المصابة إلى جهاز آخر فسيصاب هذا الجهاز أيضا. بعض الديدان (وأخطرها) تقوم باستخدام جهاز الضحية كوسيط لنقل نفسها إلى أجهزة أخرى أو تقوم بإزالة مضاد الفيروسات ومنع تنصيب آخر.

برامج الـ Keyloggers

لاحظ استخدامي للفظة "برامج" وليس "فيروسات" لأن الـ Keylogger تم تصميمه أساسا لأغراض شرعية. فهو بكل بساطة برنامج يقوم بتسجيل كل زر تم ضغطه باستخدام لوحة المفاتيح. حيث كان يستخدمه الآباء لمراقبة أبناءهم، وأرباب العمل لمراقبة عمالهم... لتأخذ استعمالاته منحى آخر فيما بعد، حيث قام مصممو

الفيروسات بتطوير هذا النوع من البرامج وإضافة خصائص له مثل التخفي والإرسال الفوري للمعلومات... كما أن بعضا منها يتم دمجه مع التروجانات (وأظنك تعرف الآن معنى هذه الكلمة). وعليه، فكل كلمة سر سيتم كشفها، وكل رسالة سرية ستتم قراءتها...

أوجه التشابه بين الفيروسات

من خلال ما سبق، يمكننا القول أن لكل نوع من الفيروسات مميزاته الخاصة، لكن معظمها -إن لم نقل كلها- تتشابه في الخصائص التالية:

1. الحجم: فأغلب الفيروسات حجمها صغير لا يتعدى 1 Mo
2. طريقة إصابة البرامج: يمكن للفيروس إصابة برنامج ما بإحدى الطرق الآتية:

- الاستبدال: هذه أسهل طريقة بالنسبة لمبرمج الفيروس، حيث يقوم ببرمجة فيروسه على حذف البرنامج الأصلي ويعوضه بنسخة منه (من الفيروس) تحمل نفس الاسم ونفس الأيقونة.
- الدمج: هذه الطريقة أكثر تعقيدا من سابقتها، حيث أن الفيروس يقوم بإضافة أسطر برمجية قبل وبعد أسطر

البرنامج. فالأسطر التي قبل البرنامج تقوم بتنفيذ الأسطر الموجودة بعد البرنامج (والتي تحتوي الفيروس) ومن ثمة تعود لتنفيذ أسطر البرنامج الأصلية وكأن شيئا لم يحدث.

ملاحظة

يتكون البرنامج من مجموعة أسطر تدعى بالأسطر البرمجية، هذه الأخيرة يقوم بكتابتها مبرمجون مستخدمين في ذلك أحد لغات البرمجة (غالبا ما تتكون من دوال رياضية) ومن ثم يتم تحويلها إلى لغة الآلة. من جهة أخرى، فمصممو الفيروسات يعملون على إيجاد طرق لكسر حماية البرامج وتعديل أسطرها البرمجية بإضافة أسطر ضارة كما هو موضح في الطريقة السابقة "الدمج".

3. مكان التموضع: قد يتمركز الفيروس في مكان ما على القرص الصلب أين يستهدف أحد مجلدات النظام المهمة و"يخبأ" نفسه على أساس أحد ملفات النظام وذلك بأحد الطرق التي سلف ذكرها (الاستبدال - الدمج). من جهة أخرى، يمكن للفيروس بأنواعه الاختباء في الـ MBR والتي هي اختصار لـ (Master Boot Record) أو في الـ Partition table. والمكانان اللذان ذكرتهما يتم تشغيلهما تلقائيا في كل مرة يقلع الكمبيوتر (لاحظ استعمالي لكلمة "كمبيوتر" وليس "نظام" أي أن الفيروس سيبقى موجودا حتى في حالة مسح النظام وإعادة تنصيبه).

4. التفعيل وتأثيره: بعض الفيروسات يتم تفعيلها في تاريخ ووقت معينين، واللذان يرتبطان عادة بمواعيد مهمة (كفيروس عيد الميلاد، فيروس 11 سبتمبر...)، والبعض الآخر يتم تفعيله تلقائيا عندما يشغل المستخدم برنامجا معينا. إضافة لوجود فئة قليلة تنشط فقط إذا كان الكمبيوتر خاليا من الفيروس، حيث يقوم بإصابته ومن ثمة يكمن منتظرا خلو الحاسوب من الإصابة مجددا ليعيد نفس العملية.

الأضرار المترتبة عن تفعيل الفيروس

أما فيما يخص التأثير المرتبط بالتفعيل Activation فإما أن يكون عاديا (بالأحرى مقلقا) كإظهار رسائل خطأ، إعادة تشغيل النظام وأشياء بسيطة من هذا القبيل. وإما أن يكون مضرا كمسح كل بيانات قرص صلب معين، حذف كل الملفات من نوع معين... بعض الفيروسات مقلقة جدا (نادرا ما تتعرض لهذا النوع) لدرجة أنها تظهر لك رسالة خطأ عادية ولنفرض أن بها خيارين: نعم ولا. فعند اختيارك لنعم ستؤجل التعرض للمشكلة (سيتحين الفيروس وقتا آخر مبرمج سلفا ليصيب حاسوبك) وإن اخترت لا فسيتم تفعيل الفيروس. وهذا ما يعرف بالمزحة السيئة Bad Joke.

الفصل الثاني

التعامل مع الفيروسات

كيف تحدث الإصابة بالفيروسات؟

تتحدث العديد من المنتديات والمواقع العربية -للأسف- عن الفيروس كشيء خطير، حتي يمكن التخلص منه باستخدام برنامج حماية يوفره ذلك الموقع أو المنتدى "لوجه الله"... في حين أن الفيروس مجرد برنامج أسطره البرمجية ضارة، كما أن مضاد الفيروسات أو أي برنامج حماية آخر (سنتعرف عليها لاحقا) متوافر بسعر رمزي. فلماذا تأخذه "مجانا" من موقع لا يعرف حتى كيفية وضع تعريف للفيروس. في الحقيقة، فإن أغلب الكراكات Cracks وغيرها من برامج كسر الحماية، أو البرامج التي يوزعها أشخاص ما "مجانا" هي في الواقع ملغمة. على كل، فالوسائل الوحيدة لتشغيل فيروس هي:

- تشغيل الفيروس بنفسه.
- تشغيل برنامج مصاب بالفيروس.
- تشغيل الفيروس تلقائيا عند إدخال قرص مصاب للكمبيوتر.

الإشارات التي تدل على وجود فيروس

عند تعرض جهازك للإصابة، سيظهر إشارات يمكنك من خلالها التأكد من وجود الفيروس والتعرف عليه مبدئيا.

يمكن تلخيص إشارات وجود فيروس على جهازك في النقاط التالية:

- تغير في حجم الملفات (خاصة ملفات exe.) أو اسمها.
- ظهور ملفات خطأ عند تشغيل برنامج معين (كان يعمل بشكل جيد من قبل) أو عند بدأ تشغيل النظام.
- زيادة في حجم الذاكرة المستهلكة. يمكنك ملاحظة ذلك من خلال ثقل الجهاز.
- رسائل خطأ عديدة تفسيرها الوحيد أنها "بدون سبب".

الحماية من الفيروسات

قبل أن تعتمد على برنامج حماية من الفيروسات وتظن أن هذا كاف لتصفح الإنترنت والبحث في مجلدات جهازك بكل أمان وحرية عليك أن تعلم بأنك مخطئ. بل عليك الاعتماد على معارفك

وذكائك وقدرتك على التعامل مع كل طارئ تواجهه. وحتى لا أطيل عليك، إليك النقاط الأساسية التي تتجنب بها التعرض للفيروسات:

- قم بعمل نسخة احتياطية لملفاتك المهمة بشكل دوري تحسبا لأي طارئ. من الأفضل حفظها على قرص.
- إذا كنت من مستخدمي الإنترنت، تأكد من الرسائل التي تصلك، لا تفتح أي مرفق في رسالة لا تعرف مصدرها. من جهة ثانية، لا تنخدع بتلك الرسائل التي تخبرك أنك ستربح ملايين الدولارات وباقي الخدع الواهية.
- قم بالتحميل من المواقع المعروفة فقط وهذا أمر جد مهم.
- قم بشراء مضاد فيروسات معروف وحدثه بشكل دوري (يمكنك القيام ببرمجة تحديث تلقائي كل أسبوع كمثال)، ولا تنس القيام بفحص شامل بشكل دوري أيضا.
- لا تستخدم غير البرامج الأصلية (في حالة العجز، استخدم المجانية Freeware أو التي تتيح مدة للتجريب Shareware).
- قم بفحص كل قرص قابل للإزالة و-إن أمكن- كل قرص (CD أوDVD) قبل استعماله.
- لا تدع الكمبيوتر يقلع بوجود قرص.

الإجراءات الأولية عند التعرض لفيروس

إذا تأكدت من أن جهازك مصاب بفيروس (أو عدة فيروسات) فلا تقم بإدراج ملفات إضافية. ضع كل ملفاتك المهمة في مكان آمن وهذا يشمل الصور العائلية، كلمات السر... وأنا لا أقصد هنا على قرص ثان، بل على قرص خارجي خال من الفيروسات (تأكد من خلوه عبر فحصه على جهاز سليم). بعد ذلك حاول استخدام أحد برامج الحماية لحذف الفيروس. إن لاحظت عدم تغير أي شيء (وهذا الاحتمال الغالب لأن أغلب الفيروسات تقوم بإيقاف عمل مضاد الفيروسات) فسننتقل -بكل أسف- للحل الأطول. إذ أنه عليك القيام بعملية فورمات Format للقرص الصلب الذي يتواجد به النظام ومن ثم إعادة تنصيبه (أو استعن بخبير صيانة في هذه الخطوة)، قم بتنصيب مضاد الفيروسات وباقي برامج الحماية. وأخيرا أعد فحص ملفاتك المهمة وافحص باقي أقراص الجهاز.

الفصل الثالث

برامج الحماية

مضاد الفيروسات Anti-Virus

مضاد الفيروسات هو برنامج وظيفته الأساسية البحث عن الفيروسات وحذفها. هناك نوعان من مضادات الفيروسات، النوع الأول يوفر الحماية وقت التشغيل On-time protection والثاني يوفر فقط إمكانية فحص النظام (هذا النوع مجاني على الأغلب لكنني لا أنصح باستخدامه). ويعمل أي مضاد فيروسات بالآلية التالية:

- يتم إدراج ملف لفحصه.
- يقوم مضاد الفيروسات بقراءة أسطره البرمجية ومقارنتها مع قاعدة بيانات المضاد Anti-virus Data Base.
- عند توافق أسطر البرنامج مع أسطر قاعدة البيانات فهذا يعني أنه فيروس.
- يقوم مضاد الفيروسات بمحاولة نزع الأسطر الضارة من أسطر البرنامج.
- في حالة الفشل، يضطر المضاد لحذف البرنامج كليا.

تهتم العديد من الشركات اليوم بتصميم وتطوير مضادات الفيروسات. وهذا التنافس انعكس إيجابيا على المستخدم. حيث أن

أغلب المضادات اليوم تحتوي على جدار ناري وأدوات لحذف البرامج الضارة... مما يغنيك عن شراء كل واحد على حدة. شيء آخر، فأنا أنصحك باستخدام مضاد فيروسات يوفر لك مدة معقولة لتجربه (30 يوما غالبا) وفي حال أعجبك ورأيت توافقه مع نظامك وعدم تسببه في بطئ جهازك قم بشرائه. نصيحة أخرى، عند شراءك للبرنامج تأكد من أن الشركة المصنعة توفر خدمة التحديث مجانا Free Update. وإليك بعض الأمثلة عن مضادات فيروسات مشهورة (على سبيل الذكر وليس الحصر):

اسم البرنامج	الموقع الرسمي
AVAST	WWW.AVAST.COM
KASPERSKY ANTI-VIRUS	WWW.KASPERLAB.COM
ESET NOD 32	WWW.ESET.COM

الجدار الناري Firewall

يطلق البعض عليه "جدار اللهب" إلا أن لفظة "الجدار الناري" هي الأكثر شعبية. وظيفة هذا البرنامج الأساسية مراقبة وتنظيم المعلومات المتبادلة في شبكة معينة. وأشهر شبكة هي شبكة الإنترنت. مثال آخر هو الشبكات الداخلية (لا داعي للتعمق في هذا النوع).

وللاستفادة من الجدار الناري بشكل صحيح يجب تعديل خصائصه وهذا ما يتطلب فهما بالشبكات. كما أن العديد من مستخدمي هذا النوع من البرامج يشغلون خيار "السماح دائما" بهدف التخلص من النوافذ التي يرونها "مزعجة". في الحقيقة، عندما يود برنامج ما الدخول إلى جهازك (كمثال) يقوم الجدار الناري بوقف عملية الدخول وتخييرك بين إكمالها وإعطاء هذا البرنامج الحرية أو إيقاف عمله. وعليه فإن اختيار "السماح دائما" سيكون فعلا غير محمود العواقب. أمر آخر، فمن خلال تجوالي بين صفحات الإنترنت المهتمة بالأمن المعلوماتي وجدت أن العديدين يستخدمون برنامج Zone Alarm كجدار ناري. لذلك، إن لم يكن مضاد الفيروسات خاصتك مزودا بواحد فأنا أنصحك بإلقاء نظرة على هذا البرنامج.

البرامج الضارة

يمكن اعتبار كل من:

- السبايوير Spyware
- الأدوير Adware
- الهايجاكرز Hijackers
- المالوير Malware

برامج ضارة تهدد أمن جهازك. هدف البرامج الضارة غالبا ما يكون ربحيا... كيف؟ سأجيبك: يطلق على برنامج ما أنه من النوع Shareware إذا كان يتيح للمستخدم فترة لتجريبه. لكن بعض البرامج وبمجرد تنزيلها تبدأ بإظهار إعلانات مزعجة تنغص عليك جلستك أمام الحاسوب. كما أن بعضها يقوم بإرسال معلومات عنك إلى الشركة المصنعة أو الشخص المبرمج له وهذا دون علمك. من أشهر هذه البرامج Real player و KaZaa. ولتجنب تنصيب هذا النوع من البرامج توجه إلى الموقع: www.spywareguide.com من حين لآخر وستجد هناك قائمة بكل البرامج المشبوهة. وهذه لائحة بأشهر البرامج المختصة في إيجاد، إيقاف وحذف السبايوير بأنواعه:

اسم البرنامج	الموقع الرسمي
SPYBOT SEARCH & DESTROY	WWW.SAFER-NETWORKING.ORG
SPYWARE BLASTER	WWW.WILDERSSECURITY.NET
SPYWARE GUARD	WWW.WILDERSSECURITY.NET

خاتمة

ختاما، أتمنى أن تكون الصفحات القليلة السابقة قد قدمت شيئا مفيدا لرصيدك المعرفي. من جهة أخرى، فلا داعي لأذكرك -عزيزي القارئ- بالتواصل معي إن واجهت أية مشكلة:

dzmaghboun@gmail.com

لمزيد من المقالات، الكتب وبعض المشاريع البرمجية:

www.dzmaghboun.blogspot.com