

الفيروسات و الأمن الإلكتروني على الإنترنت



بسم الله الرحمن الرحيم

إعداد : م. محمد الأصبحي

مشرف في عرب هارد وير oneman007@hotmail.com

تم إقتباس بعض الأفكار والفقرات من مصادر مختلفة **v1.3** (ولا تزال الإضافة مستمرة)

والله قد تعبت جدا في إعداد هذا الكتاب راجيا دعوة سالحة في ظهر الغيب



بين كل فترة وأخرى نسمع عن هجمات الفيروسات ومدى الدمار الذي تسببه. كما نسمع عن تسلل أحد المتطفلين إلى قاعدة معلومات عسكرية أو منشآت حكومية. إضافة إلى مجرمي التقنية الحديثة الذين يستخدمون أرقام بطاقات الائتمان بعد رصدتها من شبكة الإنترنت أو بعد اختراقهم لأجهزة بعض المستخدمين. فضلا عن هؤلاء الذين يتسللون إلى شبكات البنوك والشركات الكبرى أو كل ذلك بسبب عدم الأخذ بأسس وقواعد الأمن أو لضعف الإجراءات الأمنية المتخذة. وقد نتج عن ذلك خسائر تقدر بمئات الملايين ولكن الأمور الآن أصبحت أكثر صرامة وصعوبة أمام المخترقين والمتطفلين خاصة بعد سن القوانين التي تجرم من يقوم بتلك الأفعال وتطور مستوى البحث والتحري لتتبع أثر المجرمين على الشبكة. كما لا ننسى أنها أيضا نتيجة مباشرة لزيادة الوعي لدى الشركات والبنوك بأهمية الأمن ولذلك فإن هؤلاء المتطفلين والمجرمين بدؤوا بالبحث عن مستخدمين عاديين. كما أن هناك فئة مريضة بحب التطفل والتجسس على الناس. كذلك هناك مجرمون ممن يريدون إرسال تهديد أو فيروسات فيقومون باستخدام جهازك دون علمك وقيل أن تشعر بهم ومن ثم يضعوك أنت في وجه المدفع أمام الجهات الرسمية. وهذا ما حصل قبل عدة أشهر عندما قام بعض الأشخاص بتعطيل أشهر المواقع الأمريكية مثل ياهوو وأمازون دوت كوم وذلك بتسخير مئات من الكمبيوترات الخاصة بالجامعات وبعض الشركات والأفراد لإرسال كميات هائلة من المعلومات والطلبات حتى تعطلت المواقع وشلت الحركة بها تماما أمام المستخدمين وتسبب في خسائر تقدر بمئات الملايين من الدولارات. هناك عديد من مصادر التهديد الأمني لمستخدمي شبكة الإنترنت تأتي الفيروسات في المرتبة الأولى ومن ثم تليها كل من أحصنة طروادة وديدان الإنترنت. والاختراق (سواء كان اختراقاً لشبكة حاسب أو جهاز شخصي) وتعرف بـ «الهاكينج» (Hacking). والجافاسكريبت والجافا ابليت والأكتف إكس. وجواسيس البريد الإلكتروني. وراصدي لوحة المفاتيح. إضافة إلى مصادر تهديد الخصوصية والتي قد تهدد الأمن مثل: كعكة الإنترنت (Cookies) أو ما يعرف بالكوكيز. ومصادر متعلقة بالبريد الإلكتروني مثل المحولين (رفيرر) ومرسلي الرسائل الإلكترونية الإزعاجية (سبامرز) وغيرهم.

الفيروسات

هي برامج صغيرة قادرة على التناسخ (Replication) والانتشار في نسخ تكون معدلة عنه تصيب الأجهزة وتتسبب في الكثير من المشاكل الخطيرة كمسح الذاكرة الصلبة أو مسح بعض الملفات الهامة في أنظمة التشغيل أو القيام بإصدار الأوامر لبعض البرامج دون علمك أو تدخل مباشر منك مثل ما عمل فيروس الحب. ولمزيد من المعلومات عن أنواع الفيروسات وكيفية عمل البرامج المضادة يمكن الاطلاع على التفاصيل المتوفرة في موقع شركات برنامج الحماية من الفيروسات مثل نورتن ومكافي وغيرها .

وتعتبر الرسائل الإلكترونية أكبر مصدر للفيروسات وذلك لسهولة إضافتها كملفات ملحقة وسرعة انتشارها على الشبكة في زمن قصير جداً. وتعتبر نسخ البرامج المقلدة مصدراً آخر للفيروسات. أما المصدر الأقل انتشاراً فهو الأقراص اللينة ولكنها أخطر بكثير من المصادر الأخرى وذلك لتعاملها المباشر مع نظام بدء التشغيل لجهازك .

أما أحصنة طروادة وديدان الإنترنت فهي شبيهة جداً بالفيروسات ولكنها تختلف في الهدف. **الديدان** تقوم بمسح أو تدمير المعلومات من البرامج التطبيقية كبرامج المحاسبة وقواعد المعلومات فقط كما أن بمقدور هذه الديدان التكاثر حتى تملأ الذاكرة وتعطل الجهاز الضحية.

أحصنة طروادة فهي لا تدمر ولا تمسح المعلومات ولكنها تتجسس وتقوم بجمع المعلومات والبيانات ومن ثم إرسالها لمصدرها (مرسل برنامج حصان طروادة) والذي غالباً ما يكون فرداً أو موقعاً أو منظمة لجمع المعلومات .

ستجد شرحاً مطولاً عن الفيروسات في الصفحة 7

طرق انتقال الفيروسات (العدوى)

ويمكننا أن نميز فئتين من فيروسات الكمبيوتر تبعاً لآلية العدوى وانتشار الفيروس :

1- فيروس العدوى المباشرة Direct Infector

عندما يتم تنفيذ برنامج مصاب بفيروس من هذا النوع فإن ذلك الفيروس يبحث بنشاط عن ملف أو أكثر لينقل العدوى إليه ، ويمكن أن يقتصر البحث على الدليل أو الفهرس الحالي أو أن يتعدى ذلك ليشمل جميع الأدلة الفرعية الموصوفة في جملة المسار PATH و عندما يصيب أحد الملفات بالعدوى فإنه يقوم بتحميله إلى الذاكرة وتشغيله وهذا النوع قليل الانتشار لأن آلية العدوى ليست فعالة كثيراً ، كما في فيروس VIENNA الذي يصيب الملفات من نوع COM. ويخربها بشكل عشوائي بأن يستبدل الرموز الخمسة الأولى بقفزة لإعادة إقلاع الكمبيوتر .

2- فيروس العدوى غير المباشرة Indirect Infector

عندما يتم تنفيذ برنامج مصاب بفيروس من هذا النوع فإن ذلك الفيروس ينتقل إلى ذاكرة الكمبيوتر ويستقر فيها ويتم تنفيذ البرنامج الأصلي ثم يصيب الفيروس بالعدوى كل برنامج يتم تحميله في الذاكرة بعد ذلك إلى أن يتم قطع التغذية الكهربائية عن الكمبيوتر أو إعادة تشغيله . وجميع فيروسات قطاع بدء التشغيل Boot Sector Viruses هي من هذا النوع.

يعمل الفيروس عمله عند تنسيطه حسب كاتب برنامجه ، وتكون النتيجة في حالات عديدة غير مؤذية إطلاقاً مثل:

- كتابة رسالة ماعلى الشاشة كما في فيروس SHAKE الذي يظهر عبارة "Shake well before use" عند تنفيذ ملف COM.

- أو إسماع نغمة موسيقية كما في فيروس FRERE JACQUES الذي يعزف هذه الموسيقى أيام الجمعة.

- وقد يكون التأثير ضاراً كما في فيروس FRIDAY 13 أو JERUSALEM الذي يصيب الملفات من نوع COM. ويحذف أي ملفات تنفذ يوم الجمعة الثالث عشر من أي شهر .

- ويمكن في بعض الحالات أن يتتبع سلوك الفيروس كما في فيروس CHRISTMAS الذي يدمر جدول مواقع الملفات FAT إذا نفذ أي ملف مصاب بها في الأول من نيسان . بينما يعرض صورة لشجرة عيد الميلاد على الشاشة إذا نفذ الملف المصاب به بين 24 كانون الأول وبداية العام الجديد .

- أما الفيروسات الأكثر خطورة فتسبب الضرر في الخفاء بدون أن تسمح لك بمعرفة ما يحدث وعندما يتم كشفها تكون تأثيراتها الضارة المتركمة كارثة حقيقية حتى لو كنت تحتفظ بنسخ احتياطية بشكل منتظم كما في فيروس DATACRIME .

الاختراق

ويعني قيام أحد الأشخاص الخبراء بالتعامل مع الكمبيوتر والإنترنت بمحاولة الوصول الى جهازك أو الشبكة الخاصة بشركتك عن طريق شبكة الإنترنت وذلك باستخدام برامج متخصصة في فك الرموز والكلمات السرية وكسر الحواجز الأمنية واستكشاف مواطن الضعف في جهازك أو شبكة معلوماتك .

وعادة ما تكون المخارج (بوابات العبور للمعلومات) **الراوتر Router** الخاصة بالشبكة المحلية. وهذه أسهل الطرق للوصول إلى جميع ملفاتك وبرامجك. وبالنسبة للمخترقين أصبحت المهمة عسيرة بعض الشيء لاختراق المؤسسات والمواقع الكبيرة بعد تطور نظم الدفاع وبرامج الحماية. ولكن بالنسبة لأجهزة الأفراد مازالت الأبواب مفتوحة .

تقنيات حديثة

جافا سكريبت وجافا أبلتيس والأكتف إكس وكلها تقنيات حديثة ومفيدة ولكن تهدد أمن المستخدمين علما بأن الأخيرتين تعتبران أساسا من الأدوات المهمة جدا لتصميم المواقع الحديثة. غير أن سوء استخدام هذه التكنولوجيا يهدد مستقبلها ومدى انتشار شعبيتها. وذلك لقيام العديد من المستخدمين المتمرسين بتعطيل هذه الخاصية من المتصفح الخاص بها وبالتالي العزوف عن المواقع المصممة على أساس هذه التكنولوجيا مما يؤدي إلى فقدان شريحة كبيرة من المستخدمين لأنها مصدر خطر جدا على الأمن. وعادة تقوم المواقع المشبوهة والعائدة ملكيتها لأحد المحتالين باستخدام هذه التقنية بكثرة لأنها قادرة على رصد كلمات السر والعبور وكذلك تدمير وتعديل الملفات المخزنة أو ملفات البرامج .

ولهذا السبب تتجنب معظم المواقع العالمية الإفراط فيها بينما يقوم أصحاب المواقع الشخصية باستخدامها بكثرة .

جواسيس البريد الإلكتروني

وهم عادة من المخترقين السابقين لجهازك أو ممن يشاركونك الجهاز فعليا سواء في المنزل أو العمل. أو مستخدم آخر للجهاز خاصة إذا كنت في مقهى للإنترنت ولم تخرج من برنامج البريد بشكل صحيح أولم تقم بالخروج من برنامج المتصفح .

راصدو لوحة المفاتيح

وهم من أخطر مصادر التهديد الأمني حيث إنهم قادرون على رصد أي ضغطة على لوحة المفاتيح وبذلك يتمكنون من رصد كل ما يتم كتابته على لوحة المفاتيح خاصة اسم المستخدم وكلمات العبور وذلك حتى قبل أن يتمكن جهازك أو برنامجك من إخفاء وتشفير الكلمة

ولحسن الحظ فإن هذه البرامج غير منتشرة عبر الشبكة لأنها تتطلب الوصول الى جهازك فعليا . ويكثر استخدام هذه البرامج من قبل النساء (الزوجات) لمراقبة درشة الأزواج على الشبكة ! كما يستخدمها بعض ضعاف النفوس لرصد معلومات الغير في مقاهي الإنترنت والأجهزة العامة في المكتبات وغيرها من الأماكن الأخرى. ولذلك يتردد الكثير من المستخدمين ممن يعتمدون على الأجهزة العامة كمقاهي الإنترنت (ولا يمتلكون أجهزة خاصة بهم) من الشراء المباشر من الإنترنت واستخدام بطاقات الائتمان ويفضلون التحويل البنكي أو الاتصال لإملاء الرقم بالهاتف أما إذا كنت تتسوق من جهازك الخاص فلا داعي للقلق .

خطوات وإجراءات بسيطة

هنالك عدة إجراءات بسيطة ينبغي التعود عليها أثناء تصفحك للإنترنت. علما بأن هذه الإجراءات لا تغنيك عن اقتناء برنامج حماية متخصص ولكنها كافية لكي تبدأ ببناء خط دفاعي أول وقوي يصعب من مهمة اللصوص والمتطفلين خاصة إذا كنت تعمل من جهاز شخصي متصل بالإنترنت عن طريق مودم. أما إذا كنت متصلا بالإنترنت بطريقة أسرع كالخطوط الرقمية فأنت بحاجة فورية لبرنامج متخصص للحماية والسبب هو حصولك على رقم أي بي (عنوان بروتوكول الإنترنت) ثابت مخصص لك. ما يسهل عملية تتبعك على الإنترنت. أما لو كنت تستخدم فاكس مودم عاديا للاتصال بالإنترنت فإن مزود

الخدمة لا يخصص لك رقم أي بي محددا ولكنك تحصل على رقم مختلف كلما قمت بالاتصال على الشبكة. أما لو كنت تملك شبكة من الكمبيوترات المتصلة مع بعضها البعض وجهازك يعتبر جزءا من هذه الشبكة المتصلة بالإنترنت فإنك بحاجة فورية لبرنامج حماية متخصص (جدران النيران Firewall) وذلك لأن المخارج المخصصة لمشاركة الملفات تكون مفتوحة وجاهزة ومواتية لدخول الهاكرز .

نصائح

احصل على نسخة أصلية وحديثة من نظام التشغيل لأنه هو أساس الحماية وفي نفس الوقت يمكن أن يكون أكبر نقطة ضعف في جهازك. وفي الحقيقة تقوم الشركات المنتجة لأنظمة التشغيل بتحديث وتعديل هذه الأنظمة كلما يتم اكتشاف خلل أمني. وعادة يتم إخبارك بالبريد الإلكتروني أو بطريقة مباشرة من خلال ارتباطك المباشر بالشركة المنتجة أو زيارة موقع الشركة والبحث عن التحديثات ومن ثم تنزيل الملفات الخاصة بالتحسينات على نظام التشغيل. وعادة لا يتمتع من يملك نسخة مقلدة بهذه الميزة .

قم بتنزيل أحدث نسخة من المتصفح. وذلك لأن الإصدارات القديمة تتخللها العديد من الثغوب الأمنية والتي تجعل منك هدفا سهلا. وطبعاً إذا كنت ممن يشتررون من خلال الشبكة حصل على نسخة مدعومة بقوة تشفير 128 بت. كما ينصح بتعديل مستوى الأمن في المتصفح وذلك بمنع وتعطيل التشغيل المباشر لأكتف إكس وجافا وجافاسكريبت . التحكم بملفات الشبكة المحلية: LAN إذا كنت تملك نظام تشغيل ويندوز ولست متصلاً بشبكة حاسبات آلية داخل المكتب أو المنزل. أي أنك لست بحاجة إلى أي نوع من أنواع الملفات الخاصة بالمشاركة. قم بمسح وإزالة أي نوع من ملفات المشاركة لأن نظام ويندوز يقوم بفتح هذه الملفات بطريقة مباشرة كشيء أساسي في النظام. وتعتبر هذه الملفات أكبر مصدر تهديد أمني لك لأنها تسمح لأي شخص في الإنترنت من الدخول إلى جهازك ومشاركته في ملفاتك ومعلوماتك الموجودة في الجهاز .

احم جهازك بكلمة مرور تمنع الآخرين من الدخول إليه. فهناك عدة كلمات عبور يمكنك إنشاؤها في جهازك، فمثلاً يمكنك وضع كلمة عبور على جهازك لا يمكن لأي أحد غيرك من تشغيل أو استخدام الجهاز إلا بعد كتابتها. وهناك كلمة عبور في نظام التشغيل ويندوز 9895 ولكنها غير مجدية وتحتاج لكثير من الجهد حتى يمكن برمجتها وجعلها مفيدة. وهناك أيضاً كلمة عبور يمكن وضعها إذا كنت متصلاً بشبكة معينة حيث لا يتم الاتصال إلا بعد إدخالها .

عليك بنسخة أصلية وحديثة من برنامج مضاد للفيروسات. وذلك لأنك سوف تتمتع بخدمة مجانية وغالباً ما تكون لمدة عام وهي خدمة التحديث المباشر من موقع الشركة المنتجة وهذا غير متوفر للنسخ المقلدة. واحرص على تجديد وتحديث نسختك كل اسبوع أو عشرة أيام وذلك لظهور فيروسات جديدة أونسخ معدلة من فيروسات قديمة كل يوم . تجنب تنزيل أو تحميل أي برامج أو ملفات ذات طبيعة تنفيذية خاصة من مصادر غير موثوق بها. تجنب فتح الملفات المرفقة في الرسائل الإلكترونية من مصادر غير معروفة لديك وخاصة إذا كانت من الأنواع التالية .exe .com .bat .scr . تجنب تنزيل أي برامج مجانية (إذا لم تكن من مواقع معروفة وذات سمعة بالحفاظ على الخصوصية وكذلك تنزيل البرامج من مصادر المجموعات الإخبارية أو ما يعرف بـ News Group لأن الكثير من الهاكرز يتخفون تحت مظلة هذه البرامج للوصول إلى جهازك .

إذا كنت تملك معلومات في غاية الأهمية أو خاصة جداً. قم باستخدام أي برنامج لتشفير معلوماتك ورسائلك الإلكترونية . لا تقم بأي عملية شراء من شبكة الإنترنت دون التأكد من استخدام سيرفر آمن ووجود علامة القفل المغلق في المتصفح وكذلك تغيير http:// إلى https:// وهنا نلاحظ وجود حرف (s) إضافي. ما يعني أنك تستخدم بروتوكولاً آمناً لنقل المعلومات ولكن عليك التأكد أنك تستخدم قوة تشفير 128 بت وذلك لتوفير الأمان اللازم ويمكنك التأكد من قوة التشفير في متصفحك (انترنت إكسبلورر) وذلك بالنقر على Help وهو موجود على الجانب الأيسر من شاشة المتصفح في أعلى الصفحة ومن ثم اختيار About Internet Explorer وسوف تجد كلمة Ciper 128 bit فإن لم تجد هذا الرقم قم بتنزيل نسخة جديدة من موقع ويندوز .

تجنب الموافقة على حفظ اسم المستخدم وكلمات العبر في أي وقت. لأنك لو وافقت على ذلك فسوف تسهل العملية على الهاكرز لأنه سوف يجدها مخزنة وجاهزة له. وينبغي عليك ألا تسمح لأي كان خاصة من موقع شخصي أو غير متخصص بإجراء تجربة على جهازك ومسح المنافذ المفتوحة فهناك العديد من الهاكرز يتخفون تحت هذا القناع ويخدعونك بهذه الحيلة لتنزيل برامج التجسس والتعرف على نقاط الضعف في جهازك أو شبكتك .

مصادر التهديد الأمني في الرسائل الإلكترونية

أولاً: الملفات المرفقة التي تتطلب الفتح والتحميل:

عليك بالحد من الشدائد عند فتح الملفات المرفقة بالرسائل الإلكترونية لأنها أكثر الطرق استخداماً من قبل أشرار الإنترنت. ولذلك ننصحك بعدم فتح الملفات المرفقة إذا كانت من أحد الأنواع التالية. وخاصة إذا لم تكن من شخص معروف لديك. وهذه الملفات المرفقة الخطيرة تنتهي بأحد هذه الاختصارات :

(COM)=(Command Files) وهذا يعني وجود ملف به أوامر للتنفيذ مرتبطة بأي جزء من الملف وتبدأ بالعمل بعد مرور وقت معين أحيان الضغط على جزء معين .

(BAT)= (Batch Files) وهذا يعني وجود أمر معين موجه لأحد ملفات نظام التشغيل في جهازك .

(APP)= (Application) وهذا يعني وجود ملف به برنامج تطبيقي وهي خطيرة لأنها ممكن أن تكون أحد برامج التجسس **ثانياً: الملفات المرفقة ذاتية التشغيل :**

وهي قادرة على أن تقوم بالعمل حال فتحك لبرنامج البريد الإلكتروني ودون الحاجة لفتح المرفقات وتقوم بإعادة تحميل نظام التشغيل لديك ومن ثم العمل في الخفاء. وتقوم بإضافة نفسها في كل رسالة ترسلها دون علمك لتصيب بها بقية المستخدمين . ومن أهم الأمثلة على ذلك ملف WScript.kak :والطريقة الوحيدة لحماية نفسك من مثل هذه النوع هو إلغاء وحجب خاصية Allow Scripting من متصفحك .

ثالثاً: بقعة نظام التشغيل دوس :

هذا مصدر تهديد يسمح لمرسل الرسالة أو الصفحة من تخريب وتعطيل جهازك حال فتحك لرسالته. التي يتم فيها استخدام لغة الترميز اتش تي إم إل. لأنه من الممكن زرع تعليمات وبرامج مستخدمة في نظام التشغيل القديم وهو ما يعرف بنظام دوس. ليتم تعطيل نظام ويندوز. وأكثر نظم التشغيل التي يمكن أن تتأثر بها هي نظام التشغيل ويندوز 95 و 98 لأنهما يعتمدان على دوس 16 بت. وفي هذا النظام القديم توجد بعض الأوامر التي تمكن نظام التشغيل من التعامل مع بقية المكونات. ومنها على سبيل المثال للتعامل مع الطابعة والمودم وهي COM1. COM2 for communication and Fax :LPT1 for printer modem. وتكمن المشكلة في تعرف نظام التشغيل ويندوز على هذه الأوامر القديمة والتي لا تستخدم في ويندوز حالياً ولكنها في نفس الوقت تتعرف على البرامج والأوامر القديمة إذا ما تم زرعها في لغة الترميز وهي تسبب بعض المشاكل لأنها تجعل نظام ويندوز يتبادل المعلومات والأوامر مع المكونات مثل الفاكس مودم والطابعة بدلاً من القرص الصلب وبالتالي يتوقف الجهاز عن العمل ولذلك ينصح كل من يستخدم ويندوز 98 أو 95 بالقيام بتحديث الملفات من موقع الشركة لتغطية هذا العيب .

من أشهر الفيروسات التي تنتشر عن طريق الرسائل الإلكترونية :

I Love You
Meet Melissa
Buble Boy
Yaha
Nimda
Kletz
Strange Brew

مصادر تهديد الخصوصية والإزعاج

أولاً: المتطفلون والمتجسسون على بريدك الإلكتروني :

كثير من الناس مصابون بإدمان التجسس على الغير. وينشأ معهم حب التتبع لخصوصيات الناس. ويتمكنون من تحقيق ذلك بعدة طرق منها :

برامج التجسس وهي كثيرة ومتنوعة ومتوفرة بالأسواق أو عن طريق الإنترنت . تخمين كلمات العبور السهلة التي قد يستخدمها الأصدقاء كاسم الدولة أو المدينة التي ولدت بها أو اسم المدرسة أو تاريخ الميلاد . استخدام برامج مخصصة للوصول الى كلمات العبور .

وهي عبارة عن برامج تمكن مستخدميها من تجريب عدة آلاف من الكلمات السرية المنطقية والشائعة لدى الناس. وبذلك يمكن لها أن تصيب في بعض الأحيان .

كما يمكن لكل من يستطيع الوصول الى جهازك في المكتب أو المنزل من زملاء أو الأهل أو الأصدقاء من التطفل على رسائلك باستخدام بعض الخصائص المتوفرة في متصفحك ومنها: خاصية الرجوع للخلف في المتصفح. واستخدام خاصية تذكر اسم المستخدم وكلمة العبور. واستخدام خاصية الإكمال التلقائي للاسم وفراغات النماذج. واستخدام خاصية تذكر الصفحات التي تقوم بزيارتها .

ثانياً: المزجون :

وهي عادة الشركات والمواقع التي تحصل على عنوان بريدك الإلكتروني وتقوم بتبادل هذه العناوين فيما بينها أو تقوم ببيع هذه العناوين وكذلك يقوم بعض الأفراد بجمع هذه العناوين للقيام بإزعاج الآخرين أو لغرض بيعها لإحدى الشركات. وقد انتشرت مؤخراً رسائل باللغة العربية تحكي قصص محزنة لأطفال أو كبار تعرضوا لحوادث شخصية أو حوادث سير (طبعاً كلها من نسج الخيال) ويطلب منك صاحب الرسالة بأن تساعد ذلك الطفل المسكين بارسال الرسالة الى كل من تعرف ومن لا تعرف!! وطبعاً أنت من ذوي القلوب الرحيمة والطيبة فتقوم بالعمل نيابة عنه بينما يقوم هو بجمع العناوين وتكوين ثروة من العناوين يقوم ببيعها أو يكون قد أرسل معها فيروساً أو برنامج تجسس أو برنامج للتحكم وتعطيل المواقع وأنت لاتعلم عنها. كما انتشرت في الآونة الأخيرة رسالة تحتوي على معلومات عن أحد مكونات الشامبو وأنها تسبب السرطان . ويذكر فيها منتجاً معيناً ويمدح فيه بينما يذم في بقية الأنواع. ويطلب منك إخبار كل الأصدقاء والمعارف عن طريق تحويل الرسالة. وطبعاً كل هذا الكلام ليس له أساس من الصحة والهدف منه جمع العناوين أو التسويق للشامبو الخاص بهم .

سبل الوقاية

وللوقاية والحماية أثناء استخدام البريد الإلكتروني يجب اتباع الآتي :

استخدام برامج مضادة للفيروسات وبرامج حماية وبرامج التشفير المتخصص .

استخدام (باسورد) سهلة التذكر ولكن صعبة التخمين كأن تتكون من حروف وأرقام أو خليط من الأحرف الكبيرة والصغيرة. غلق المتصفح حال ابتعادك عن الجهاز لتعطيل خاصية الرجوع للخلف في المتصفح .

عدم استخدام خاصية تذكر اسم المستخدم وكلمة العبور .

عدم استخدام خاصية الإكمال الآلي والتلقائي للاسم وفراغات النماذج في المتصفح .

عدم استخدام خاصية تذكر الصفحات التي تقوم بزيارتها لفترات طويلة وتقليل هذه المدة على قدر المستطاع .

عدم فتح الملفات المرفقة إذا كانت من أحد الأنواع التي تم ذكرها في البداية .

عدم تحويل الرسائل المشبوهة الى أصدقائك ومعارفك .

تعديل خاصية الأمن في المتصفح الى المستوى المتوسط أو الأعلى مع تعطيل خاصية الجافا سكريبت . وتعديل مستوى الأمن في خاصية الأكتف إكس .

عند الإنتهاء من قراءة الرسائل عليك بالخروج بطريقة صحيحة من الموقع أو البرنامج ويكون ذلك بتسجيل الخروج

أو ما يعرف ب Sign out. لأن هنالك بعض برامج البريد أو المواقع تتذكرك لمدة تصل الى 8 ساعات وترحب بك مباشرة حال دخول أي شخص آخر للموقع ذاته .

وهكذا. وباطلاعك على هذه المسائل الأمنية وإدراكك الخطر الذي يهدد أمن المعلومات الخاصة بك. ستكون قادراً مستقبلاً على التعامل الأمن مع ثغرات الخطر الكامنة عند استخدامك شبكة الإنترنت بشكل عام بكل ما تحتويه من تطبيقات مفيدة

دخلت في صميم أسلوب الحياة الذي تعيش وخاصة في الفترة الأخيرة

الفيروسات

The Virus

الخطوة الأولى في مكافحة فيروسات الكمبيوتر، هي فهم أنواعها وآليات عملها

تتضمن معظم الكمبيوترات الشخصية المباعة حديثاً برامج لمكافحة الفيروسات، وهذه الحقيقة، أكثر من أي شيء آخر، تدلنا على مدى انتشار الفيروسات، ومدى قبول صناعة الكمبيوتر بها، كقدر لا مفر منه! لقد أصبحت الفيروسات أمراً واقعاً في عالم الكمبيوتر اليوم.

يوجد حالياً الآلاف من فيروسات الكمبيوتر، ويمكن تصنيفها إلى عدة فئات، لكنها جميعاً، على العموم، تخضع لتعريف مشترك بسيط: **الفيروس** هو برنامج كمبيوتر مصمم عمداً ليقترن ببرنامج آخر، بحيث يعمل الفيروس عندما يعمل ذلك البرنامج، ومن ثمَّ يعيد إنتاج نفسه باقترانه ببرنامج أخرى. ويقترن الفيروس بالبرنامج الأصلي بالصاق نفسه به، أو باستبداله أحياناً، وقد يغير الفيروس نفسه عند إعادة الإنتاج، فيظهر كنسخة معدلة عن النسخة التي قبلها، كلما كرر العملية. ويمكن أن تتلوث برامج الماكرو بالفيروس، أو قطاع الإقلاع (boot sector) على القرص، وهو أول برنامج يتم تحميله من قرص يحمل ملفات إقلاع نظام التشغيل. (لا يوجد تعريف رسمي مئة في المئة للفيروسات لأنها في تجدد مستمر لكنني قد وضعت تعريفان مناسبان يكملان بعضهما البعض وضع كل منهما في مكانه المناسب).

لاحظ عبارة "مصمم عمداً" في التعريف، فالفيروسات لا تظهر صدفة، بل يكتبها مبرمجون ذوو مهارات عالية عادة، ثم يجدون طريقة لنشرها في أجهزة المستخدمين الغافلين عنها. وكلما أصبحت برامج مكافحة الفيروسات أقوى، زاد المبرمجون من جهودهم لتطوير فيروسات أذكى، للتحايل عليها. والهدف من تطوير الفيروسات، بالنسبة للكثير من مؤلفيها، ليس أكثر من تحد، والرغبة في إثبات تفوقهم، بينما هو للبعض الآخر التلذذ بإثارة حيرة الآخرين وشكوكهم في الكمبيوتر، أو إزعاجهم، وحتى إيذائهم! وهذا أمر سيئ جداً، إذ يمكنهم أن يجنوا أموالاً طائلة، إذا وجهوا مواهبهم لمساعدة الشركات على حل مشكلة العام 2000، بدلاً من هدرها في أعمال لا طائل منها، مثل تطوير الفيروسات.

اشتهرت فيروسات الكمبيوتر بقدرتها على الأذى وإحداث الأضرار، لكن في الحقيقة، فإن الكثير منها غير مؤذ. صحيح أن بعضها يحذف الملفات، أو يقوم بأعمال تخريبية أخرى، لكن معظمها يسبب إزعاجاً بسيطاً فقط، وبعضها لا يلحظه المستخدم العادي أبداً. ويكفي أن يتمكن البرنامج من إعادة إنتاج نفسه حتى يعتبر فيروساً، بغض النظر عن الأعمال التي ينفذها.

لكن، في الحقيقة، حتى الفيروسات غير المؤذية، تسبب بعض الأذى! فهي تستهلك مساحات تخزين على القرص، وجزءاً من ذاكرة الكمبيوتر، وتشغل جزءاً من طاقة المعالج، وبالتالي فهي تؤثر على سرعة وكفاءة الجهاز. أضف إلى ذلك، أن برامج كشف الفيروسات وإزالتها، تستهلك أيضاً موارد الجهاز. ويرى الكثير من المستخدمين، أن برامج مكافحة الفيروسات تبطئ عمل الجهاز بشكل ملحوظ، وهي أكثر تطفلاً عليه من الفيروسات ذاتها! وبعبارة أخرى، تؤثر الفيروسات في عالم الكمبيوتر، حتى إذا لم تكن تفعل شيئاً.

تصنيف الفيروسات حسب خطورتها

يمكن تصنيف الفيروسات حسب شدة خطورتها والضرر تحدثه في سلم من ست درجات قياساً لمقدار الزمن اللازم لإلغاء التخريب الذي تحدثه وهي :

1. العادي (Trivial)

لا يفعل الفيروس ذو الضرر العادي شيئاً سوى التكاثر REPLICATION ويمكن أن لا يشعرنا بوجوده ولا يسبب ضرراً أو تخريباً معتمداً للمعلومات في الأقراص . وحالما يتم تشخيصه و اكتشافه فكل ما يتوجب هو حذف الفيروس فقط وبجهد قليل باستخدام أحد البرامج المضادة للفيروسات Anti-Virus Programs كما في فيروس STUPID الذي لا يفعل شيئاً سوى البحث عن ملف نظيف وإصابته .

2. الثانوي (Minor)

يسبب للفيروس ذو الضرر الثانوي تغييراً أو مسحاً لواحد أو أكثر من الملف القابلة للتنفيذ Executable والتي تصاب بالفيروس. وبما أن هذه الملفات قد أخذت أساساً من الأقراص الأصلية المقدمة من قبل منتجي البرامج فإن إعادة تركيبها على الكمبيوتر بعد إزالة الفيروس هي عملية بسيطة نسبياً كما يمكن استرجاعها أو من النسخ الاحتياطية للبرنامج كما في فيروس AIDS الذي يصيب الملفات من نوع COM. ويكتب فوق ال 13K الأولى منها .

3. المعتدل (Moderate)

يمكن للفيروس ذو الضرر المعتدل تدمير جميع الملفات الموجودة على القرص الصلب غالباً عن طريق إعادة تهيئة r formatting أو استبدال المعلومات بكتابة معلومات أخرى تافهة فوقها . كما في فيروس DISK KILLER الذي يسبب إعادة تهيئة القرص الصلب عندما يبلغ عدد الأقراص المرنة التي تمت إصابتها عدداً محدداً أو فيروس COLUMBUS الذي يفعل الشيء ذاته إذا تم تنفيذ ملف COM مصاب في تاريخ 12 أكتوبر . وبالرغم أن الكثيرين قد يرون أن هذه المشكلة خطيرة إلا أن مسح جميع الملفات لا يشكل ضرراً حقيقياً طالما كانت عملية النسخ الاحتياطي BACKUP تتم بانتظام .

4. الرئيسي (Major)

يؤدي الفيروس ذو الضرر الرئيسي إلى تخريب المعلومات بشكل تدريجي وبطيء عبر فترة من الزمن كنسخ رسالة معينة أو تشكيل من الرموز في الملفات وبشكل عشوائي ، وبالرغم من أن هذا التخريب قد يجد قد يجد طريقة للنسخ الاحتياطية إلا أنه مرئياً بسهولة بعد تشخيص ومعرفة الإصابة مما يمكن من تحديد الملفات المتضررة ويسهل إصلاحها كما في فيروس RIPPER الذي يتسبب في واحدة من كل ألف عملية كتابة على القرص تسجيل المعلومات بشكل خاطئ مما يؤدي إلى تخريب تدريجي للنظام.

5. الشديد (SEVERE)

يتمكن الفيروس ذو الخطر الشديد من إحداث تغييرات ذكية وبارعة للبيانات دون أن يترك أثراً يشير إلى التغير الحاصل ، كأن يقوم بشكل عشوائي بمبادلة كتل من المعلومات المتماثلة في الطول بين بعض الملفات وإذا تأخر اكتشاف الإصابة به أكثر من بعضة أيام فإن هذا النوع من الضرر يستحيل إزالته لأن المعلومات الأصلية لن تكون موجودة في ذلك الوقت ولأن الضرر قد أستمّر لفترة زمنية قبل تشخيص الفيروس فإن النسخ الاحتياطية ستكون مخربة على الغالب ولا يمكن الوثوق بها .

6. اللامحدود (Unlimited)

يستهدف

الفيروس ذو الضرر اللامحدود شبكات الكمبيوتر Network ويمضي أغلب الوقت في محاولة معرفة كلمة السر Password للمستخدمين الأكثر فاعلية ضمن الشبكة مثل المشرف Supervisor وعندما يتمكن من الحصول عليها فإنه يمررها إلى واحد أو أكثر من مستخدمي الشبكة على أمل أنهم سوف يستخدمونها لأغراض سيئة. وعندما يفقد الشخص المؤهل سيطرته على كلمة السر ورقم الحساب ويتم نقلها إلى شخص آخر يصبح هو المتحكم بكامل الشبكة.

الفيروسات وأشباه الفيروسات

إن الشرح المذكور في الفقرة السابقة عن الفيروس، أكثر تحديداً من الطريقة التي نستخدم فيها كلمة "فيروس" في الواقع. وتوجد أنواع أخرى من البرامج، ينطبق عليها تعريف الفيروس جزئياً. تشترك هذه الأنواع مع الفيروسات في أنها تعمل بدون علم المستخدم، وتقوم بأعمال ضمن الكمبيوتر، مصممة عمداً لتنفيذها. ومن هذه الأنواع: الديدان (worms)، وأحصنة طروادة (Trojan horses) التي تكلمنا عنها سابقاً، وبرامج الإنزال (droppers). وتعتبر كل هذه البرامج، بما فيها الفيروسات، جزءاً من فئة أكبر تدعى البرامج الماكرة (malware)، وهي مشتقة من عبارة malicious-logic software.

الديدان (worms) برنامج يعيد إنتاج نفسه، لكنها لا تلوّث برامج أخرى. تنتسخ الدودة نفسها من وإلى الأقراص المرنّة، أو عبر الشبكات، ويعتمد بعضها على الشبكة في إنجاز عملها. تستخدم إحدى أنواع الديدان -وهي الدودة المضيفة (host worm)- الشبكة لنسخ نفسها، فقط، إلى أجهزة الكمبيوتر المتصلة بالشبكة. بينما توزع الدودة الشبكية (network worm) أجزاءها على عدة كمبيوترات، وتعتمد على الشبكة فيما بعد لتشغيل هذه الأجزاء. ويمكن أن تظهر الديدان على كمبيوترات منفصلة، فتنتسخ نفسها إلى أماكن متعددة على القرص الصلب.

أحصنة طروادة (Trojan horses) وهو النوع الثاني من البرمجيات الماكرة نسبة للأسطورة الإغريقية الواردة في ملحمة الأوديسا لهوميروس، حيث ترك الجيش الإغريقي حصاناً خشبياً ضخماً، كهدية لسكان طروادة، وكان يختبئ ضمنه مجموعة من الجنود الأشداء، بعد أن تظاهروا بإنهاء الحصار الطويل، وعندما رحل الجيش وأدخل السكان الحصان إلى داخل أسوار المدينة، خرج الجند منه وانقضوا على الحامية، وسقطت المدينة في أيدي الإغريق. وتعتمد برامج أحصنة طروادة على المبدأ ذاته، فهي تختبئ ضمن برامج يبدو مظهرها بريئاً، وعندما يشغل المستخدم واحداً من هذه البرامج، ينشط الجزء الماكر ويقوم بعمل معين مصمم له. وتختلف أحصنة طروادة عن الفيروسات العادية، في أنها لا تعيد إنتاج نفسها.

وصممت برامج **الإنزال (droppers)** لمراوغة برامج مكافحة الفيروسات، وتعتمد على **التشفير** غالباً لمنع اكتشافها. ووظيفة هذه البرامج عادة، نقل وتركيب **الفيروسات**، فهي تنتظر لحظة حدوث أمر معين على الكمبيوتر، لكي تتطلق وتلوّثه بالفيروس المحمول في طياتها.

وينتمي مفهوم **قنبلة (bomb)** الكمبيوتر إلى هذه الفئة، إذ تبني القنابل ضمن البرمجيات الماكرة كواسطة لتنشيطها. وتبرمج القنابل لتنشط عند حدوث حدث معين. تنشط بعض القنابل في وقت محدد، اعتماداً على ساعة الكمبيوتر. فيمكن برمجة قنبلة مثلاً، لمسح كافة الملفات ذات الامتداد .DOC من قرصك الصلب، عشية رأس السنة الميلادية، أو لعرض رسالة على الشاشة، في اليوم المصادف لعيد ميلاد شخصية مشهورة. وتعمل بعض القنابل تحت شروط أو أحداث أخرى، فيمكن أن تنتظر القنبلة إلى أن يتم تشغيل برنامج معين، عشرين مرة مثلاً، وعندها تمسح ملفات القوالب (templates) الخاصة بهذا البرنامج. ومن وجهة النظر هذه، تعتبر القنابل مجرد برامج جدولة زمنية مأكرة.

ويمكننا النظر إلى الفيروسات كحالات خاصة من البرمجيات الماكرة، إذ يمكن للفيروسات الانتشار بواسطة برامج الإنزال (ولا يشترط ذلك)، وهي تستخدم مفهوم **برامج الديدان** لإعادة إنتاج نفسها. ولا تعتبر الفيروسات مماثلة لأحصنة طروادة من الناحية التقنية، إلا أنها تشابهها في نقطتين: فهي تنفذ أعمالاً لا يريد المستخدم، وتحول البرنامج الذي تلتصق به إلى حصان طروادة عملياً (تختبئ داخله، وتعمل عندما يعمل البرنامج، وتنفذ أعمالاً غير مرغوبة).

كيف يعمل الفيروس؟

ويتكون برنامج الفيروس بشكل عام من أربعة أجزاء رئيسية وهي :

1 - آلية النسخ The Replication Mechanism

وهو الجزء الذي يسمح للفيروس أن ينسخ نفسه وبدونه لا يمكن للبرنامج أن يكرر ذاته وبالتالي فهو ليس فيروساً .

2 - آلية التخفي The Protection Mechanism

وهو الجزء الذي يخفي الفيروس عن الاكتشاف ويمكن أن يتضمن تشفير الفيروس لمنع البرامج الماسحة التي تبحث عن نموذج الفيروس من اكتشافه .

3 - آلية التثيظ The Trigger Mechanism

وهو الجزء الذي يسمح للفيروس بالانتشار قبل أن يعرف وجودة مثل:

- 1- استخدام توقيت الساعة في فيروس MICHELANGELO الذي ينشط في السادس من آذار من كل عام ،
- 2- فيروسات تنتظر حتى تنفيذ برنامج ما عدداً معيناً من المرات كما في فيروس ICELAND
- 3- DISK CRUNCHING الذي يستهدف ملفات EXE. ويصيب كل عاشر ملف يتم تنفيذه ،
- 4- بعد عدة مرات من إعادة إقلاع الكمبيوتر كما في فيروس TAIWAN الذي يسبب تهيئة القرص الصلب بعد (90) إقلاع للكمبيوتر .
- 5- عند تنفيذ تسلسل معين من الأوامر FUMANCHU الذي ينشط عند الضغط على CTRL+ ALT + DEL.

4- آلية التنفيذ The Payload Mechanism

وهو الجزء الذي ينفذه الفيروس عندما يتم تنشيطه وقد يكون مجرد رسالة على الشاشة أو مسح بعض الملفات أو تخريب كامل للقرص الصلب أو مسح تدريجي للبيانات.

أما كيف تعمل الفيروسات بالتفصيل

تعمل الفيروسات بطرق مختلفة، في البداية يظهر الفيروس على جهازك، ويكون قد دخل إليه مختبئاً في ملف برنامج ملوث (مثل ملفات COM أو EXE أو قطاع الإقلاع). وكانت الفيروسات في الماضي تنتشر بشكل أساسي عن طريق توزيع أقراص مرنة ملوثة. أما اليوم، فمعظمها يأتي مع البرامج المنقولة عبر الشبكات (ومن بينها الإنترنت)، كجزء من برنامج تركيب نسخة تجريبية من تطبيق معين، أو ماكرو لأحد التطبيقات الشهيرة، أو كملف مرفق (attachment) برسالة بريد إلكتروني.

ويجدر التنويه إلى أن رسالة البريد الإلكتروني نفسها لا يمكن أن تكون فيروساً، فالفيروس برنامج، ويجب تشغيله لكي يصبح نشطاً. إذا الفيروس المرفق برسالة بريد إلكتروني، لا حول له ولا قوة، إلى أن تشغله. ويتم تشغيل فيروسات المرفقات عادة، بالنقر عليها نقرة مزدوجة بالماوس. ويمكنك حماية جهازك من هذه الفيروسات، بالامتناع عن تشغيل أي ملف مرفق برسالة بريد إلكتروني، إذا كان امتداده COM أو EXE، أو إذا كان أحد ملفات بيانات التطبيقات التي تدعم الماكرو، مثل برامج أوفيس، إلى ما بعد فحصه والتأكد من خلوه من الفيروسات. أما ملفات الرسوميات والصوت، وأنواع ملفات البيانات الأخرى القادمة كمرفقات، فهي آمنة، ولا يمكن للفيروس أن ينشط من خلالها، ولذلك فهو لا يهاجمها.

إذا بدأ الفيروس دورة حياته على الجهاز بشكل مشابه لبرنامج حصان طروادة، فهو يختبئ في ثايليا برنامج أو ملف آخر، وينشط معه. في الملفات التنفيذية الملوثة، يكون الفيروس قد أضاف شيفرته إلى البرنامج الأصلي، وعدل تعليماته بحيث ينتقل التنفيذ إلى شيفرة الفيروس. وعند تشغيل الملف التنفيذي المصاب، يقفز البرنامج عادة إلى تعليمات الفيروس، فينفذها، ثم يعود ثانية لتنفيذ تعليمات البرنامج الأصلي. وعند هذه النقطة يكون الفيروس ناشطاً، وجهازك أصبح ملوثاً.

وقد ينفذ الفيروس مهمته فور تنشيطه (ويطلق عليه **فيروس العمل المباشر** direct-action)، أو يقبع منتظراً في الذاكرة، باستخدام وظيفة "الإنهاء والبقاء في الذاكرة" (terminate and stay resident, TSR)، التي تؤمنها نظم التشغيل عادة. وتنتمي غالبية الفيروسات لهذه الفئة، ويطلق عليها الفيروسات "**المقيمة**". ونظراً للإمكانيات الكبيرة المتاحة للبرامج المقيمة في الذاكرة، بدءاً من تشغيل التطبيقات والنسخ الاحتياطي للملفات إلى مراقبة ضغطات لوحة المفاتيح ونقرات الماوس (والكثير من الأعمال الأخرى)، فيمكن برمجة الفيروس المقيم، لتنفيذ أي عمل يمكن أن يقوم به نظام التشغيل، تقريباً. يمكن تشغيل الفيروس المقيم كقنبلة، فيبدأ مهمته على جهازك عند حدث معين. ومن الأمور التي تستطيع الفيروسات المقيمة عملها، مسح (scan) قرصك الصلب وأقراص الشبكة بحثاً عن الملفات التنفيذية، ثم نسخ نفسها إلى هذه الملفات وتلوئها.

أنواع الفيروسات

يبحث مطورو الفيروسات، بشكل دائم، عن طرق جديدة لتلويث كمبيوترك، لكن أنواع الفيروسات معدودة عملياً، وتصنف إلى: فيروسات قطاع الإقلاع (boot sector viruses). ملوثات الملفات (file infectors). فيروسات الماكرو (viruses macro). وتوجد أسماء أخرى لهذه الفئات، وبعض الفئات المتفرعة عنها، لكن مفهومها يبقى واحداً.

فيروسات قطاع الإقلاع (boot sector viruses). تقع فيروسات قطاع الإقلاع - أو بدأ التشغيل - في أماكن في القرص الصلب ولايتحتم أن يكون ذلك القرص هو قرص نظام System Disk ولأن المساحة التي يحتلها برنامج بدء التشغيل Boot Program صغيرة جداً فإن برنامج الفيروس يعتمد إلى نقلة إلى مكان آخر على القرص ويحل محله ليضمن لنفسه أولوية التنفيذ. كمثال فإن فيروس STONED يضع برنامج بدء التشغيل القديم في نهاية فهرس الملفات وبالتالي لا تمكن ملاحظته حتى يصل عدد الملفات على القرص العدد الأعظم المسموح، بينما يحتل فيروس YALE القطاعات الأخيرة من المسار الأخير على القرص ولا تمكن ملاحظته إلا عندما يمتلئ القرص بالكامل أما فيروس DEN ZUCK فإن يهيئ مساراً إضافياً يختبئ فيه خارج المنطقة المعتادة على القرص وبالتالي تتعذر ملاحظته بالطرق العادية، بينما تبحث بعض الفيروسات عن مكان فارغ على القرص وتحشر نفسها فيه ثم تسمه بعلامة عدم الصلاحية للتخزين BAD SECTORS، وهي الأماكن التي يقرأها الكمبيوتر وينفذ التعليمات المخزنة ضمنها عند الإقلاع.

تصيب فيروسات قطاع الإقلاع **الحقيقية** منطقة قطاع الإقلاع الخاصة بنظام دوس (DOS boot record)، بينما تصيب فيروسات قطاع الإقلاع **الفرعية** المسماة (MBR viruses)، قطاع الإقلاع الرئيسي للكمبيوتر (master boot record). يقرأ الكمبيوتر كلا المنطقتين السابقتين من القرص الصلب عند الإقلاع، مما يؤدي إلى تحميل الفيروس في الذاكرة. يمكن للفيروسات أن تصيب قطاع الإقلاع على الأقراص المرنة، لكن الأقراص المرنة النظيفة، والمحمية من الكتابة، تبقى أكثر الطرق أمناً لإقلاع النظام، في حالات الطوارئ. والمشكلة التي يواجهها المستخدم بالطبع، هي كيفية التأكد من نظافة القرص المرن، أي خلوه من الفيروسات، قبل استخدامه في الإقلاع، وهذا ما تحاول أن تفعله برامج مكافحة الفيروسات.

ملوثات الملفات (file infectors).

1 - الفيروسات الطفيلية (parasitic viruses)

تلتصق نفسها بالملفات التنفيذية، وهي أكثر أنواع الفيروسات شيوعاً. وعندما يعمل أحد البرامج الملوثة، فإن هذا الفيروس، عادة، ينتظر في الذاكرة إلى أن يشغل المستخدم برنامجاً آخر، فيسرع عندها إلى تلويثه. وهكذا، يعيد هذا النوع من الفيروس إنتاج نفسه، ببساطة، من خلال استخدام الكمبيوتر بفعالية، أي بتشغيل البرامج! وتوجد أنواع مختلفة من ملوثات الملفات، لكن مبدأ عملها واحد وطريقة التصاق أي أنها تلتصق نفسها بالملفات لكي تتكاثر وتبقى الملف نفسه بحالة سليمة في الغالب لأنها تضيف نفسها إما في بداية الملف Prepending Virus أو في نهايته Appending Virus والملفات من نوع COM يتم

تحميلها للذاكرة ويبدأ تنفيذها عند أول أمر في البرامج لذا فإن الفيروسات التي تستهدفها تقوم بوضع نفسها قبل بداية البرنامج وعندما يتم تشغيل البرنامج فإن الفيروس ينفذ أولاً . أما الملفات من نوع **EXE** ففيها جزء يسمى المقدمة Header في بداية الملف يحدد حجم البرنامج وعدد الأقسام المستخدمة وطريقة ربطها معاً والمكان الذي سيبدأ التنفيذ عنده ، لذا فإن الفيروسات التي تستهدفها تقوم بحفظ المحتوى الأصلي لهذه المقدمة وتنسخ نفسها في نهاية الملف وتعديل المقدمة لتضمن تحميل الفيروس كقسم من الملف وتنفيذه أولاً . وتوجد حالة نادرة هي للفيروس **COMMAND BOMBER** الذي يبحث عن مساحات فارغة ضمن الملف المستهدف ويخزن نفسه في عدة مناطق متفرقة من الملف .

2 - الفيروسات المرافقة (Companion Viruses).

تعتمد هذه الفيروسات على قاعدة الأسبقية في التنفيذ ، فعند وجود ملفين تنفيذيين من نوع **COM** . و **EXE** . لهما نفس الاسم فإن الملف **COM** . هو الذي سينفذ أولاً إذا لم يذكر امتداد الملف عند طلب تنفيذه ، وتتمكن من نقل العدوى بدون تغيير طول الملف عن خلق ملف جديد له نفس الاسم ولكن بامتداد **COM** . وعند تنفيذ الملف المصاب يقوم الفيروس بالبحث عن ملف **EXE** . جديد وإصابته ثم يحمل الملف المطلوب كما في فيروس **AIDS II** ، وكذلك يمكنها إصابة الملفات الدفعية **BAT** . بخلق ملفات مرافقة من نوع **EXE or .COM** .

3 - الفيروسات الرابطة (Linking Viruses).

تصيب هذه الفيروسات البرامج بتغيير المعلومات في جدول مواقع الملفات بحيث تبدأ كل البرامج المصابة من نفس الموقع وهو عادة وحدة التخزين الأخيرة Cluster في القرص والتي تتضمن نص الفيروس مما يضمن للفيروس انتشاراً سريعاً كما في فيروس **DIDII**

فيروسات الماكرو (macro viruses).

وهي من الأنواع الحديثة نسبياً. تصيب هذه الفيروسات الملفات والوثائق المكتوبة تطبيقات الكمبيوتر التي تتضمن لغات ماكرو مثل مايكروسوفت وورد وإكسيل . وقد صممت لغات البرمجة هذه -الماكرو- لمساعدة المستخدم على أتمتة العمليات المتكررة التي يجريها ضمن التطبيق، من خلال السماح له بإنشاء برامج صغيرة تدعى برامج الماكرو. تتضمن برامج طاقم أوفيس، مثلاً، لغة برمجة مبيتة، بالإضافة إلى العديد من برامج الماكرو المبيتة أيضاً، والجاهزة للاستخدام المباشر. **وفيروس الماكرو ببساطة**، هو برنامج ماكرو مصمم للعمل مع تطبيق معين، أو عدة تطبيقات تشترك بلغة برمجة واحدة. أصبحت فيروسات الماكرو شهيرة بفضل الفيروس المصمم لبرنامج مايكروسوفت وورد. فعندما تفتح وثيقة أو قالباً ملوثن، ينشط الفيروس ويؤدي مهمته التخريبية. وقد بُرمج هذا الفيروس لينسخ نفسه إلى ملفات الوثائق الأخرى، مما يؤدي إلى ازدياد انتشاره مع استمرار استخدام البرنامج. مثال : ففي معالج النصوص **WORD** . ينتقل الفيروس الماكرو من وثيقة مصابة عند فتحها ضمن البرنامج ويصيب قالب الرئيسي **DOT.NORMAL** . وبعدها ينتقل إلى جميع الوثائق التي يتم فتحها أو إنشاؤها . وأول فيروسات هذا النوع هو فيروس **CONCEPT** . أما في برنامج **Excel** فينتقل الفيروس من جدول مصاب عند فتحه ويصيب قالب الرئيسي للبرنامج **XLS.PERSONAL** وبعدها ينتقل ليصيب الملفات بنفس الطريقة ، وأول فيروسات هذا النوع هو فيروس **LAROUX** .

ويجمع نوع **رابع** يدعى **الفيروس "متعدد الأجزاء" (multipartite)** بين تلويث قطاع الإقلاع مع تلويث الملفات، في وقت واحد.

ذكاء الفيروسات في ازدياد

نجح مبدأ فيروس الماكرو، لأن لغات البرمجة أمنت إمكانية الوصول إلى الذاكرة والأقراص الصلبة. وهذا ما أمنتته التقنيات الحديثة أيضاً، بما فيها **عناصر تحكم ActiveX**، و**برمجيات جافا (Java applets)**. صحيح أن هذه التقنيات صُممت مع ضمان حماية القرص الصلب من برامج الفيروسات (تعد جافا أفضل من ActiveX في هذا المجال)، لكن الحقيقة أن هذه البرامج تستطيع تركيب نفسها على جهازك بمجرد زيارتك لموقع ويب. ومن الواضح أن أجهزتنا ستكون أكثر عرضة لمخاطر الفيروسات والبرمجيات الماكرو الأخرى، مع ازدياد تشبيك الكمبيوترات ببعضها، وبشبكة إنترنت، خصوصاً مع المزايا التي تعدنا بها إنترنت لإجراء ترقية نظم التشغيل عبرها (يؤمن نظاما ويندوز 98 وويندوز 2000 هذه الإمكانيات).

إن أقل ما يوصف به مطورو الفيروسات، هو مهارتهم وقدرتهم الفذة على الابتكار، فهم يخرجون إلينا دائماً بطرق جديدة لخداع برامج مكافحة الفيروسات. فمثلاً، تضلل **الفيروسات المتسللة (stealth viruses)** الجديدة، برامج مكافحة الفيروسات، بإيهامها أن الأمور تسير على ما يرام، ولا يوجد أي مؤشر على وجود فيروس. كيف؟

يعتمد مبدأ عمل **الفيروس المتسلل**، على الاحتفاظ بمعلومات عن الملفات التي لوثها، ثم الانتظار في الذاكرة، ومقاطعة عمل برامج مكافحة الفيروسات خلال بحثها عن الملفات المعدلة، وإعطائها المعلومات القديمة التي يحتفظ بها عن هذه الملفات، بدلاً من السماح لها بالحصول على المعلومات الحقيقية من نظام التشغيل!

أما **الفيروسات متغيرة الشكل (polymorphic viruses)**، فتعدل نفسها أثناء إعادة الإنتاج، مما يجعل من الصعب على برامج مكافحة الفيروسات التي تبحث عن نماذج معينة من مثل هذا الفيروس، اكتشاف كافة أشكاله الموجودة، وبالتالي تستطيع الفيروسات الناجية، الاستمرار وإعادة إنتاج أشكال جديدة.

تظهر أنواع جديدة من الفيروسات إلى حيز الوجود بشكل دائم، مع استمرار لعبة القط والفأر بين مطوري الفيروسات ومنتجي برامج مكافحتها. وأغلب الظن أن الفيروسات ظهرت لتبقى، إلى ما شاء الله.

بعض الفيروسات الشائعة

اسم الفيروس	نوعه	مجالات التلويث	مواصفاته
Aol4free.com	حصان طروادة	لا شيء! فهو يحذف الملفات من القرص الصلب، لكنه لا ينتقل إلى تطبيقات أخرى	يستخدم تعليمية Deltree (من دوس) عند تنشيطه، لحذف الملفات من القرص الصلب، وهو مختلف عن فيروس Aol4free السابق له
Form	مقيم، قطاع الإقلاع	قطاع الإقلاع على الأقراص المرنة	قديم نسبياً لكنه شائع، يصدر صوت نقرات عند الضغط على لوحة المفاتيح
Hare	مقيم، متغير الشكل، متعدد الأجزاء	ملفات COM و EXE، وقطاع الإقلاع الرئيسي، وقطاع الإقلاع على الأقراص المرنة	ينشط في الثاني والعشرين من أغسطس وسبتمبر، ويحاول مسح سواقات A: و B: و C:

ملوث ملفات، مباشر العمل	ملفات فئات جافا	أول فيروس يصيب برمجيات جافا، ويمكنه الانتشار عبر نظم تشغيل مختلفة، لكن لا تعرف له أضرار	Java.App Strange Brew
ماكرو	جداول إكسل الممتدة	يشكل الملف Spellck.xla في مجلد إقلاع إكسل، وهو غير مؤذ، لكنه يعرض رسائل يحذر فيها من فيروسات الماكرو	Microsoft.Excel.Spellcheck
ملوث ملفات، متسلل، مقيم	ملفات COM و EXE	يوقف عمل الكمبيوتر في الساعة السابعة وسبع دقائق، في اليوم السابع من شهر يوليو، أي 7/7-7:07، ويظهر كلمة Monica	(Monica (Hanko.4167
ملوث ملفات، مقيم	ملفات EXE لويندوز 95	ينشط في السادس والعشرين من كل شهر، ويحاول الكتابة فوق ذاكرة فلاش بيوس، وتخریب بيانات القرص الصلب	W95.CIH
ملوث ملفات، مباشر العمل	ملفات التطبيقات لنظم ويندوز 98/95 إن.تي	ينشط بعد ثلاثة أشهر من أول إصابة به، فعند تشغيل تطبيق ملوث، يغطي الشاشة بأيقونة الخطأ في ويندوز، ويحذف برامج مكافحة الفيروسات	W95.Marburg
ماكرو	وثائق (ملفات بيانات) وورد 97 وإكسل 97	أول فيروس من نوع الماكرو يصيب ملفات وورد وإكسل معاً، ويمنع تحميل الوثائق الملوثة	Shiver W97/X97M
ملوث ملفات، مقيم	ملفات EXE لنظم ويندوز	يرسل معلومات من عدة ملفات على القرص الصلب، إلى عناوين IP محددة، عبر إنترنت	Win32/Semisoft
ماكرو	وثائق وورد	يرسل رسالة إلى مجموعات نقاش محددة، بواسطة برنامج Free Agent، ويضع وثيقة وورد الراهنة كمرفق بالرسالة	WM.PolyPoster
ماكرو، متغير الشكل	جداول إكسل الممتدة	ينشط بعد تاريخ 31 أغسطس 1998 عند إغلاق جدول ملوث، فيختار مجموعة عشوائية من الخلايا العددية، ويغير قيمها بنسبة 5 %	XM.Compat

تمت بعونه تعالى . (انتظروا الإصدار الجديد).