كيف تنتشر الفيروسات

بمجرد تشغيل أي برنامج مصاب بالفيروس فإنه يقوم بمهاجمة نظام التشغيل Windows. (هذا لا يمنع أن يقوم أحدهم بتصميم برامج فيروسات لأنظمة التشغيل الأخرى – ولكن نظرا لشيوع استخدام الحاسبات الشخصية فكانت هي الأكثر استهدافاً لهذا الوباء). ونظرا لوجود نقاط ضعف لنظام التشغيل، فالآتي هو مسرح العمليات لبرامج الفيروسات لترتع فيها:

أ- الأول : لا توجد أي حماية لذاكرة التشغيل الرئيسة Main Memory. فبمجرد تحميل برنامج مصاب في ذاكرة التشغيل ، يقوم الفيروس بالاستيلاء على مجريات الأمور بجدول متجهات مقاطعة التشغيل Interrupt Vector Table ثم الذاكرة العادية Normal Memory وكذلك الذاكرة الفوقية High Memory وبناءا على ذلك يسيطر الفيروس علي الحاسب ويفعل ما يحلو له.

ب- الثاني : ضعف حماية الملفات : من المستحيل أن يتم تخبئة التعامل مع الملفات سواء من البرامج أو المستخدمين. وبالتالي فإنه لا يمكن حماية الملفات من تلاعبات الفيروس خاصة عندما يتداخل مع نظام التشغيل (وبناءً عليه فإن File Allocation Table ليس ببعيد عن التداول بواسطة الفيروس – لدرجة أن بعض الفيروسات تختبئ ضمن هذا الجدول ولا يمكن إزالتها بالطرق التقليدية مثل تمهيد الجهاز Formatting).

جـ الثالث : قطاعات بداية التشغيل Boot Sector وقطاع التقسيم Partition Sector (وهذه القطاعات هي أول قطاعات يتم وضعها على جميع الديسكات عند تهيئتها لأول مرة). وهذه القطاعات تحتوي علي برمجيات صغيرة: سجل بداية التشغيل ، سجل القطاعات وكلاهما يتم تشغيله في كل مرة يتم التعامل فيها مع الديسك خاصة في بداية توصيل التيار الكهربي للحاسب.

يظل الفيروس كامنا إلي أن يتم تشغيل برنامج مصاب بالفيروس أو إلي أن يتم قراءة سجل بدء التشغيل لديسك مصاب. ثم يتم تحميل الفيروس في ذاكرة الحاسب في المنطقة المخصصة لبرامج نظام التشغيل. وبعض الفيروسات تقوم بالمرور علي جميع الملفات الموجودة علي الديسك الصلب (Hard disk) والبعض الآخر يتعامل فقط مع البرامج والملفات التى يتم تحميلها في الذاكرة ، وفي الحالتين يقوم برنامج الفيروس بتغيير أوامر وعناوين البرامج الأخرى القابلة للتشغيل. والبرنامج المصاب الآن أصبح مصدر إصابة لباقي البرامج حيث أن الأوامر الأولي منه تقوم بنشر العدوى لباقي البرامج ، أما الأمر التالي لهذه الأوامر يكون السؤال عن شرط بدء تشغيل التأثير المدمر (مثلا: في تاريخ محدد ، أو عند تشغيل برنامج بعينه). وتعتبر شبكة الانترنيت من أنسب الوسائط لانتشار الفيروسات ، ويأتي بعدها استخدام ديسكات غير معلومة المصدر أو الهوية.

بعض أعراض الإصابة بالفيروسات:

- البطء الملحوظ على غير عادة الجهاز.
- البطء الملحوظ على غير العادة عند تشغيل البرامج.
- القرص الصلب يعمل بالدوام بالرغم من عدم تشغيل أي برنامج.
- تغيير في حجم البرامج وتاريخ ووقت إنشائها (في أحيان كثيرة).
- تقليل حجم الذاكرة وكذا الحيز المسموح بالتخزين عليه علي الديسك الصلب.
- تصرفات غير طبيعية للجهاز وظهور رسائل غير مألوفة سواء أثناء التشغيل أو عند بدء التشغيل.
- رسائل أخطاء Error messages غير متوقعة.
- كثرة البلوكات والقطاعات المعطوبة على الديسكات بصفة عامة.
- تصرفات غير طبيعية للشاشة.
- فشل تشغيل برامج كانت تعمل من قبل.
- الكتابة غير المتوقعة علي ديسكات يفترض القراءة منها فقط.
- فشل تشغيل الجهاز من أساسه.

طرق للتخلص من الفيروسات:

يقولون أن الوقاية خيرٌ من العلاج. نعم يجب أن تراعي جميع تعليمات تأمين الحاسب ضد الإصابة بالفيروس ، (ويجب أن يكون هناك حساباً شديداً لمن يخالف هذه التعليمات في حاسبات القاهرة) يمكن تلخيصها في الآتي:

١- عدم استخدام أي ديسكات مجهولة الهوية (المصدر).
٢- يجب أن يكون هناك حاسباً مخصصاً لاختبار أي ديسكات خارجية أو فلاشات.
٣- يجب استخدام برنامج حماية من الفيروسات أصلي ويتم تحديثه تباعا.
٤- فصل الحواسب المتصلة بشبكة الانترنيت عن بقية حواسب الشبكات المحلية.
٥- يجب الالتزام بتنفيذ خطة النسخ الاحتياطية وحفظها في خزائن خاصة ومنع تداول هذه النسخ الاحتياطية إلا تحت سيطرة رئاسة مركز الحاسب ، وكتابة الوثائق الخاصة بها والتفتيش عليها.

ولأي سبب من الأسباب يتم اكتشاف فيروس على الحاسب يجب الآتي:

١- فصل هذا الحاسب عن الشبكة المحلية فوراً.
٢- منع استخدام هذا الحاسب لحين معالجة الفيروس ، ووقف جميع الديسكات (غير المؤمنة ضد الكتابة) التي تم تداولها على هذا الجهاز.
٣- تشغيل برنامج اكتشاف وإزالة الفيروس علي هذا الحاسب (يجب التنويه والتحذير وحظر استخدام برنامج اكتشاف وإزالة الفيروس الوارد لنا مجانا من المؤسسة الإسرائيلية – فالحدأة لم ولن ترمي كتاكيت بأي حال من الأحوال). وقد أثبت برنامج نورتن الأصلي جدارته في اكتشاف وإزالة غالبية الفيروسات حتى الآن.
٤- تحديد حجم الخسائر على هذا الحاسب وإعادة تحميل البرامج والبيانات وتوثيق ما تم على هذا الجهاز في سجل يتم إعداده لذلك.

فيروسات الحاسب

إعداد
دكتور مهندس / هشام نبيه المهدي محمد
استاذ تكنولوجيا المعلومات المساعد
بكلية الحاسبات والمعلومات - جامعة القاهرة
رائد الجمعية العلمية بالكلية
http://www.h-elmahdy.net/

لم تعد فيروسات الحاسب قاصرة فقط على الهواة ، بل أصبحت سلاحا وصناعة. سلاحا تم استخدامه ضد الثورة الايرانية في مهدها وكذلك ضد أجهزة القيادة والسيطرة لنظام صدام حسين. أما في مجال الصناعة ، فإنها أصبحت صناعة مربحة فبعض الشركات تتيح نسخ مجانية من البرامج مضادات الفيروس وتوزع من خلالها أنواعا جديدة من الفيروسات (للضغط على المستهلك لشراء برامج مضادة للفيروس). هذا العدد من النشرة بمثابة تحذير وتوضيح لبعض الجوانب.

العدد الخامس - مايو ٢٠٠٨

فيروسات الحاسب

بادئ ذي بدء فإنه لا يوجد حاسب محصن ضد الإصابة بالفيروس ، وبالتالي فإن معركة الفيروسات لا ولن تنتهي بمجرد اختيار برنامج حماية ضد الفيروس وكفى!! ، ولكن هناك العديد من الاحتياطات التي يجب أن نلتزم بها كإجراء وقائي. بناءا علي البيانات الصادرة من شركة أي بي إم فإن المؤسسات التي بها ١٠٠٠ حاسب تتعرض لهجمات فيروس بمعدل مرة كل شهرين إلي ثلاثة شهور. وقد أعلن المركز القومي لجرائم بيانات الكمبيوتر بمدينة لوس أنجلوس The National Center for Computer Crime Data أن حجم خسائر السوق الأمريكية سنويا حوالي ٥٥٠ مليون دولار نتيجة للتصرفات غير المسئولة سواء من الفيروسات أو القرصنة علي شبكات الحاسب.

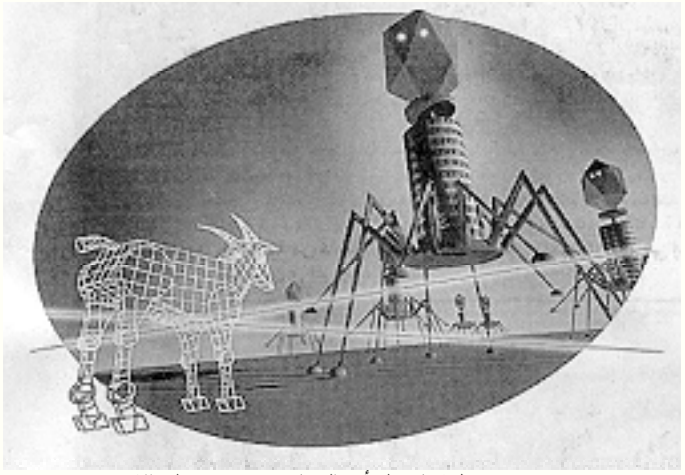
تعتبر فيروسات الحاسب تهديدا للأمن القومي ليس فقط المصري ولكنه أيضا تهديدا حقيقيا للأمن القومي العربي. وقد طالبنا في مناسبات عديدة ومن مسئولين ذوي مستوى رفيع بضرورة انشاء هيئة قومية لمقاومة فيروسات الحاسب لذلك يسعد الجمعية العلمية لكلية الحاسبات والمعلومات أن تلقي الضوء على هذا الموضوع الحيوي من خلال هذه النشرة لكي تعم الفائدة ونقلل الخسائر خاصة في جامعتنا الحبيبة.

منذ خلق الله سبحانه وتعالي سيدنا آدم عليه وعلى نبينا الصلاة والسلام فقد ابتلاه بشبهة الأكل من الشجرة على يد اللعين إبليس الرجيم ونحن بنو البشر نبتلي بالشبهات على مر الأجيال. واختلفت هذه الشبهات من قوم إلى قوم ومن عصر إلى عصر. وشبهة عصر المعلوماتية في رأينا تتمثل في فيروسات الحاسب. وللأسف الشديد فقد بدأ تأليف الفيروس في دولة باكستان الإسلامية. فقد قام بعض ضعاف النفوس في تلك الدولة (من المتأسلمين وليس المسلمين) بتأليف فيروس Brain والذي كان يصيب حاسبات الأجانب الذين يشترون برامج منسوخة بطرق غير قانونية –البرامج الأصلية باهظة الثمن ومحمية ضد النسخ بالطرق التقليدية– وقد عاني المسلمون بعد ذلك من جراء هذا التصرف الأهوج غير المسئول. فبمجرد أن زادت المشكلة لدي الأجانب أرسلوا للبنتاجون عينات من تلكم الديسكات لتحليلها .. وكذلك "جنت علي نفسها براقش". فهاهو صدام حسين يكون فريسة لفيروس على حاسبات أنظمة القيادة والسيطرة لديه مرتين في معركة تحرير الكويت وكذا في القرصنة الأمريكية البريطانية في ٢٠٠٣.

قد يستغرب الكثيرون من هذا الحديث ويدَّعون أن نظرية المؤامرة مسيطرة علينا. ولكن للأسف الأيام أثبتت صحة نظرية الفيروس الذي هاجم أنظمة القيادة والسيطرة للنظام العراقي. ولو تمحصنا في تاريخ الفيروس سنجد أن مؤسسة إسرائيلية قد أخذت بزمام المبادرة بانتاج مضادات للفيروسات الذي تنتجه وتنشر فيروسات جديدة تنتج لها مضادات جديدة لتستمر الصناعة. نبدأ أولاً بتعريف الفيروس.

تعريف الفيروس:

فيروس الحاسب هو برنامج صغير تم بناؤه ليتسلل إلي الحاسبات دون دراية مستخدميها ويختبئ في ذاكرة الحاسب لحين تحقق شرط معين (مثل : تاريخ معين كما حدث مع فيروس تشيرنوبل الشهير ، أو عند تشغيل برامج معينة). وفيروس الحاسب له بعض خواص الفيروس البيولوجي من حيث تكرار نفسه مع كل برنامج يتم تشغيله (كما يحدث لخلايا الجسم عندما يسيطر الفيروس عليها – فخلايا الجسم المصابة به تتوقف عن النشاط الطبيعي وتعمل كماكينة لإنتاج الفيروس). وينتقل فيروس الحاسب بطرق عدة منها: قراءة ديسكات مصابة بالفيروس ، أو عند زيارة أماكن موبوءة علي شبكة الانترنيت. (تحذير:بعض الديسكات التي توزع مجانا مع بعض المجلات تكون مصابة بالفيروس وكذلك بعض برامج إزالة الفيروس تقوم بوضع أنواع أخري من الفيروسات لذا وجب التحذير).



فيروس تشيرنوبل كما تخيله أحد الرسامين وتم نشره على الانترنت

ويجب أن ننتبه أن الفيروس لا يصيب المكونات المادية للحاسب (hardware) ولكن مع الإشاعات التي تطلق بواسطة وسائل الإعلام يمكن أن ييأس أحدهم ويقوم بتدمير الحاسب خاصته نتيجة لجهله بما يفعله الفيروس وما لا يستطيع أن يفعله الفيروس. فنتذكر جميعا فيروس حصان طروادة والذي سمعنا عنه من سنين فقد قالت الصحف عنه : أن كل من استقبل بريدا عاديا في ذلك اليوم قد أصيب حاسبه بفيروس. ذلك غير صحيح بالمرة فهناك فرق بين البريد العادي والبريد الإلكتروني ، فالبريد الإلكتروني يتم استقباله من خلال شبكات الحاسب أما البريد العادي فهو قصة أخري.

الفرق بين فيروس الحاسب Virus ودودة الحاسب Worm:

دودة الحاسب لا تنسخ نفسها مع البرامج التي يتم تشغيلها ولكن هذا البرنامج يكمن ويختبئ حتى يتم تحقيق شرط بداية تشغيل الأثر المدمر له.

المراجع: مجموعة من المقالات التي نشرها الدكتور هشام المهدي في دوريات ومؤتمرات
الشكر واجب لكل الزملاء المراجعين

نبذة عن تاريخ الفيروسات:

يعتبر يوم الاثنين الموافق ١٩٩٩/٤/٢٦ هو يوم الاثنين الأسود في تاريخ الحاسبات (مقارنة بيوم الاثنين الأسود لبورصة نيويورك) فقد بلغ عدد الحاسبات التي أصيبت بفيروس تشيرنوبل عشرات الملايين حول العالم. فلم يفرق ذلك الفيروس اللعين بين حاسب وحاسب ، فقد أصاب من كل الجنسيات ومن كل الديانات ، ولم يفرق بين حاسب يعمل عليه طالب علم أو حاسب يتم توجيه به صاروخ يقتل به البشر. وبدراسة تاريخ الفيروسات وجدنا الآتي :

اختلفت الروايات حول تاريخ بدء هذا الوباء المسمي بفيروس الحاسب. هناك حالة فردية حدثت في إحدى الشركات السعودية الكبري. ملخص هذه الحالة أن مديرا مركز تكنولوجيا المعلومات قد وضع برنامجا بسيطا يتم تشغيله اتوماتيكيا. وظيفة هذا البرنامج أنه يقوم باختبار قائمة المرتبات للشركة ، وحينما يكتشف البرنامج عدم وجود اسم ذلك الشخص (أي تم الاستغناء عن خدماته) ، يقوم البرنامج باتلاف بعض البيانات والبرامج ليوقف كل النظام حتى تضطر الشركة لإعادة توظيفه بشروطه.

أما أول الحالات علي المستوى العالمي كان الفيروس الذي تم تشغيله لتدمير قواعد بيانات صيانة الطائرات لإيران مع بداية ثورة الخوميني ، وقد نتج عن ذلك خسائر مالية فادحة.

ولكن كما ذكرنا من قبل أن الفيروسات بدأت بفيروس Brian في باكستان. هذا الفيروس يصيب قطاع بداية التشغيل للديسكات المرنة Floppy Disk وكذلك القطاعات التالية له ، ويقوم بنسخ قطاع بداية التشغيل الأصلي في مكان آخر كنوع من التمويه ، وبالتالي فإن خطر هذا الفيروس يعتبر محدوداً.

ثم انتقلت الدفة إلي الجامعة العبرية بإسرائيل فكان فيروس أورشليم Jerusalem المدمر في أواخر الثمانينات. وقد تفوقت إسرائيل على نفسها في هذا المجال حيث باتت مؤسسة إسرائيلية الأصل (أمريكية المكان الآن) مصدرا لكلاً من الفيروسات وبرامج معالجة الفيروسات. وقد كانت النسخ المجانية لبرنامج معالجة الفيروسات الإسرائيلي الأثر الكبير في انتشار أنواع جديدة من الفيروسات بالرغم من أن ظاهرها أنها تزيل بعض الفيروسات.

وقد شهد عام ٢٠٠٣ دودة Slammer والتي أصابت أكثر من ٨٠% من الحاسبات المتصلة بالانترنت خلال خمس دقائق (ولولا وجود خطأ في ذلك البرنامج لتم اصابة ١٠٠%). أما عام ٢٠٠٤ فقد شهد دودة Flash التي دمرت ٩٥% من الحاسبات المتصلة بالانترنت في ٥١ ثانية وصلت ٩٩% في ٧٢ ثانية وقد انهارت الانترنت فتم انقاذ ال ١% الباقي ...

ثم توالت الفيروسات.