الفصل السادس

الفيروسات

Chapter six

virous

التعريف بالفيروسات

تعريف الفيروس

عبارة عن برنامج له أهداف تدميرية تهدف إلى إحداث أضرار جسيمة بنظام الحاسب سواء البرمجيات أو الأجزاء المادية مثل أي برنامج تطبيقي آخر يتم تصميمه وكتابته بإحدى لغات البرمجة من قبل أحد المخربين بهدف إحداث ضرر ممكن بنظام الحاسب، لتنفيذ ذلك يتم إعطاءه القدرة على ربط نفسه بالبرامج الأخرى، كذلك إعادة إنشاء نفسه حتى يبدو وكأنه يتكاثر ويتولد ذاتياً كما أن له القدرة على الانتشار بين برامج الحاسب المختلفة، في مواقع مختلفة في الذاكرة لتحقيق أهدافه التدميرية.

أعراض الإصابة بالفيروسات

هناك مشاكل قد تحصل في الحاسب يعود بعضها إلى علل برمجية أو حالات سوء في أداء الأجزاء المادية لوظائفها مما يتوجب فحص النظام بأحد البرامج المضادة للفيروس.

الأعراض التي تصاحب وجود الفيروس

1. تغير عدد الملفات إذ تقوم بعض أنواع الفيروسات بحذف الملفات عشوائياً أو وفق تعليمات محددة فإذا اختفى أحد الملفات من فهرس الملفات بدون سبب ظاهر عندها وجب الشك بوجود الفيروس، كذلك في حالة وجود ملفات لا مبرر لوجودها.
2. توقف النظام عن العمل.
3. عرض رسالة خطأ غير مألوفة، خاصة عند ظهور رسائل تشير إلى استخدام الأقراص أو البرامج بشكل متكرر دون أن يتم استعمالها من قبل المستخدم، فهذا يعني أن الفيروس يحاول الوصول إلى هذه الأقراص أو البرامج لتلويثها.
4. بطأ في تشغيل النظام وتنفيذ البرامج قد يستغرق وقت أكثر من المعتاد إذ يؤثر سلباً على وقت التنفيذ.
5. التعامل مع القرص بشكل غير طبيعي، يلاحظ أن مصابيح السواقات الخاصة بالقرص تضاء عدة مرات أكثر من المعدل الطبيعي بدون سبب ظاهر.
6. ظهور حروف غريبة عند الضغط على مفاتيح معينة في لوحة المفاتيح (Key Board) أو عدم ظهور حروف على الإطلاق.

7. انخفاض ذاكرة النظام إذ تنخفض ذاكرة النظام نظراً لأن الفيروس يحتل جزءاً من هذه الذاكرة فإذا ظهرت رسالة تدل على عدم وجود ذاكرة لتشغيل أحد البرامج الكبيرة فهذا يدل على وجود فيروس.
8. تغير مظهر الأيقونات.
9. عمليات الوصول إلى الأقراص تستغرق وقتاً طويلاً لا تحتاجه مثل هذه المهمات البسيطة مثلاً تخزين صفحة من نص قد يستغرق ثانيتان من الزمن، لكن في حالة عدم وجود فيروس لا يستغرق عادة أكثر من ثانية واحدة.
10. تغير في حجم البرامج التنفيذية، بعض الفيروسات تدخل إلى البرامج التنفيذية مما يؤدي إلى زيادة حجم البرامج. .

مكونات برنامج فيروس الكمبيوتر

إن أي فيروس كمبيوتر قابل للتطبيق وقابل للنمو يجب أن يمتلك على الأقل وحدتين برمجيتين (أو إجراءين) Two basic subroutines حتى يمكن أن يطلق عليه اسم فيروس هما:

أولاً: يجب أن يحتوي على روتين أو إجراء بحث Routine يقوم بتحديد الموقع الذي سيتم نسخ الفيروس إليه، كما يحدد كيفية النسخ (بسرعة أو ببطء)، إذا كان بإمكان الفيروس مهاجمة وحدات مختلفة داخل الكمبيوتر أو القرص الصلب فقط، إذا بإمكانه مهاجمة جزء من القرص أم أجزاء محددة فقط، يمكن أن يكون برنامج البحث أكثر تطوراً إلا أن ذلك يحتاج إلى استخدام ذاكرة أكبر بالرغم من أن طريقة البحث الأكثر كفاءة تساعد الفيروس على أداء عمله بشكل أفضل لكن ذلك يؤدي إلى زيادة حجم فيروس الكمبيوتر على روتين أو إجرائية copy Routine لإعادة نسخ الفيروس إلى منطقة حددها روتين البحث، يجب أن يكون روتين النسخ متطوراً ليؤدي عمله دون اكتشاف، كلما كان الروتين صغيراً كلما كان أداء الفيروس أفضل، يرتبط حجم الروتين بتعقيد النسخ فالفيروس المصمم لمهاجمة ملفات COM فقط يستخدم برنامجاً فرعياً (روتين أو إجرائية) للنسخ أصغر مما يستخدم فيروس مهاجمة الملفات التنفيذية EXE.
يمكن بواسطة هذين الجزأين (روتينات الفيروس) أن يحقق الفيروس أهدافه.

ثانياً: قد تضاف للفيروس أحياناً وظيفة حماية وإخفاء Antidelection Routine حتى لا يتمكن المستخدم أو تتمكن البرامج المضادة للفيروسات من اكتشافه، كما يمكن وضع هذه الوظيفة ضمن روتين البحث أو النسخ أيضاً يمكن تنفيذ هذه الوظيفة (وظيفة الحماية والاختفاء) بأن يجعل برنامج البحث يقوم بالبحث ضمن منطقة صغيرة محددة لذلك، إن ترك برنامج البحث يعمل دون قيود قد ينبه المستخدم إلى حدوث نشاط غير عادي في الكمبيوتر، أو يمكن إعداد وظيفة الاختفاء عن طريق ضبط نشاط عمل الفيروس في وقت وتاريخ محدد يظل الفيروس قبلها ساكناً أو ينطلق للهجوم عند توقف تحريك الفأرة أو عدم ضغط المفاتيح أو بعد فترة توقف عمل مما يعني أن المستخدم غائب عن مراقبة جهاز الكمبيوتر.

تشكل الأجزاء البرمجية الثلاثة (البرنامج الفرعي للبحث، والبرنامج الفرعي للنسخ، والبرنامج الفرعي للحماية والاختباء) Search, Copy, and Antidelection Routine المكونات الضرورية لعمل الفيروس، قد تتضمن بعض الفيروسات وحدات أخرى تهدف إلى تعطيل عمل الكمبيوتر أو تخريبه أو عرض رسائل أو غير ذلك من الأعمال التي يقوم الفيروس بتنفيذها، لا تعتبر الوحدات الإضافية أساسية بل قد تكون ضارة بالفيروس إذ تجذب انتباه المستخدم لوجود الفيروس.

أخطار الفيروسات

الفيروسات لا تظهر صدفة بل يكتبها مبرمجون ذوو مهارات عالية ثم يجدون طريقة لنشرها في أجهزة المستخدمين الغافلين عنها، كلما 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 تحدي والرغبة في إثبات تفوقهم بينما هو للبعض الآخر التلذذ بإثارة حيرة الآخرين وشكوكهم في الحاسب أو إزعاجهم أو حتى إيذائهم و هذا أمر سيء جداً إذ يمكنهم أن يجنوا أموالاً طائلة إذا وجهوا مواهبهم لمساعدة الشركات على حل مشاكلها بدلاً من هدرها في أعمال لا طائل منها مثل تطوير الفيروسات.

إن الفيروس يسبب أخطاراً شديدة تشمل:

1. الأخطار على البرمجيات Software.
2. الأخطار على المكونات المادية Hardware.

أخطار الفيروس على البرمجيات Software

إن البرامج هي وسيلة الانتقال الرئيسية للفيروسات، إن أكبر خطر للفيروس يتمثل في توقف البرامج أو تعديل وظائفها نتيجة أوامر الفيروس مكان جزء من أوامر البرامج ويظهر هجوم الفيروس على البرامج التي تعمل على نظام التشغيل Dos ويعمل الفيروس على الآتي:

أ. **إبطاء تشغيل الحاسوب**

قد يؤدي الفيروس في بعض الأحيان إلى إبطاء تشغيل الحاسوب، تستغرق العمليات التي يؤديها مدة أطول من المدة الافتراضية، قد يكون هذا التأخير غير ملحوظ عند تنفيذ عمليات منفصلة

يتم ملاحظته عندما يؤدي الحاسب مجموعة من العمليات كالبحث عن بيانات معينة أو طباعة تقارير وغيرها.

ب. تدمير قطاع التحميل Boot Sector

يقوم الفيروس بتدمير قطاع التحميل الذي يكون في مكان محدد وثابت في القرص ويقصد بقطاع التحميل جزء من القرص يحتوي على الأوامر والإشارات التي يستخدمها الحاسب لكي يبدأ في العمل، إن تحطيم هذا القطاع أو تغيير الأوامر المخزونة فيه يجعل القرص غير قادر على تشغيل النظام (Unbootable)، عندما نتعامل مع القرص المرن تكون هذه الحالة محتملة، في حالة التعامل مع القرص الصلب تحدث مشكلة كبيرة، يكون العلاج الوحيد لها هو إعادة تهيئة القرص Reformat مما يؤدي إلى فقدان جميع البرامج والبيانات المخزونة لهذا من الضروري الاحتفاظ بنسخ احتياطية من البرامج والبيانات.

ج. تدمير جدول توزيع الملفات File Allocation Table

إن جدول توزيع الملفات (File Allocation Table) هو منطقة على القرص يستخدمها نظام التشغيل لتتبع أماكن الملفات المخزنة على القرص والقطاعات الخالية التي يمكن تخزين الملفات الجديدة عليها، هذا الجدول يكون دائماً في مكان ثابت على القرص لذلك يسهل على الفيروس مهاجمته، في هذه الحالة يمكنه مسح هذا الجدول، بالتالي يصعب الوصول إلى أي ملف على القرص، كما يمكنه تغيير المعلومات الموجودة في هذا الجدول مثلاً تغيير المعلومات الخاصة بالمساحة التخزينية المتاحة على القرص بإنقاصها عن المساحة الفعلية المتاحة وبالتالي لا يستطيع المستخدم التعامل مع جزء صغير من المساحة التخزينية للقرص، مثال على ذلك فيروس Stoned الأكثر انتشاراً في الحاسبات الشخصية الذي يقدر كونه سبباً لـ 50% من الإصابات في الولايات المتحدة، انتقل هذا الفيروس إلى الولايات المتحدة من نيوزيلندا، صمم ليطبع عبارة تشجع ترويج الماريجوانا، يقوم بتكرار نفسه طوال فترة ستة أعوام، ما زال هذا الفيروس موجوداً ويتابع انتشاره يصيب جدول مواقع الملفات FAT: File Allocation Table أثناء تكراره نفسه مما يجعل القرص الصلب غير قابلاً للقراءة، بالتالي تضيع كافة المعلومات الموجودة على القرص الصلب على الرغم من أن مصمم هذا الفيروس لم ينوي أن يتسبب بهذا الأذى لأحد ولكن بعد الإصابة يصبح هذا الحاسب كأي حاسب قد تعرض لتخريب متعمد.

د. تحطيم الفهرس الرئيسي Root Directory

يقوم نظام التشغيل Dos بتنظيم الملفات المخزونة على القرص عن طريق الفهارس Directories والفهارس الفرعية Subdirectories، هذه الطريقة في تنظيم الملفات تجعل الوصول إلى أي ملف على القرص سهلاً حيث يصبح من السهل الوصول إلى الفهرس الفرعي المطلوب وعرض الملفات الموجودة به دون الحاجة إلى عرض جميع الملفات المخزونة على القرص، تظهر أهمية ذلك بوضوح عندما يزيد عدد الملفات لذلك فإن الفهرس الرئيسي **Root Directory** يمثل هدفاً استراتيجياً للفيروس حيث يمكن أن

يؤدي تغيير حرف واحد (Byte) في هذا الفهرس إلى عدم التمكن من الوصول إلى أي ملف على القرص رغم وجود الملفات فعلياً.

هـ. التجسس على النظم

في نظم شبكات الحاسب التي تستخدم أجهزة الاتصال (Modems) في الربط بين أجهزة الحاسوب في الأماكن المختلفة فإن الفيروس عند انتقاله إلى هذا النظام يقوم بالسماح للمخرب الذي يقوم بتصميمه بالدخول إلى النظام والحصول على أي بيانات سرية، ذلك بهدف تحقيق مكاسب شخصية سواء كانت مادية أو معنوية، حيث يقوم الفيروس في وقت محدد بالاتصال بالمخرب تلفونياً والسماح له بالدخول إلى النظام.

أخطار الفيروسات على المكونات Hardware

إن الفيروسات تسبب أخطاراً شديدة لمكونات الحاسوب المادية Hardware، قد تصل الخطورة إلى إجهاد الأجزاء الميكانيكية للحاسوب مما قد يسبب تدميرها، على سبيل المثال برنامج يعطي أمراً لجهاز التحكم في وحدة الأقراص Disc drive لتوجيه رأس القراءة والكتابة Read/Write head إلى مكان بعيد في اتجاه مركز القرص هذا يؤدي في بعض الحالات إلى تثبيت رأس القراءة والكتابة وعدم قدرته على الحركة وقراءة المسارات Tracks الموجودة على القرص، لكي يتم إعادته إلى الوضع الطبيعي يتطلب الأمر إصلاح العطل ميكانيكياً، إضافة إلى ذلك هناك برامج يمكنها التحكم في الطابعة بحيث يتم تغيير اتجاه الطابعة هذا يؤدي إلى تجمع الأوراق داخل الطابعة، ربما تعطيلها، كما أن هناك برنامج فيروسات تمسح مسار التحكم Control Track الخاص بالقرص الصلب، هذا يجعل القرص غير صالح.

هنالك برامج أخرى لا تسبب عطلاً مادياً بصورة مباشرة ولكنها تؤدي إلى تآكل أجزاء معينة في مكونات الحاسوب مما يقلل من عمرها الافتراضي، إن بعض الفيروسات الساكنة في الذاكرة يمكنها أن تقلل من حجم الذاكرة المؤقتة المتاح بدرجة كبيرة، يؤدي هذا إلى تعامل الذاكرة مع القرص عدداً من المرات حتى يستطيع تحميل البرامج المطلوبة، هذا يؤدي إلى استهلاك وحدة الأقراص بعد فترة وجيزة.

طرق انتقال الفيروسات

1. عن طريق الأقراص المرنة.
2. عن طريق شبكات الحواسيب.
3. عن طريق البريد الالكتروني.

طرق العلاج

عن طريق استخدام برامج مضادة للفيروسات (برامج مكافحة الفيروسات) يتم تنصيبها على الحاسوب وتثبيتها كما يجب تحديث البرامج المضادة بشكل دائم.

طرق الحماية

1. عن طريق برامج مكافحة الفيروسات.
2. إبقاء القرص للقراءة فقط (هناك جزء خاص بتأمين القرص يمكن فتحه أو إغلاقه وتسجيله للقراءة فقط ثم فتح هذا الجزء).
3. وضع كلمة مرور يتم إدخال كلمة المرور الصحيحة بهذا لا يمكن لأي شخص العبث بالحاسوب وإدخال فيروسات للإضرار.
4. حقوق النسخ الخاصة بالبرامج: هو ترخيص يسمح بنسخ البرنامج إذا لم يكن هذا الترخيص موجود تم نسخه، يعتبر هذا خرق للقانون يعرض الشخص الذي قام بنسخ الحقوق للإدانة والمسائلة القانونية ودفع التعويض المناسب .