فيروس الحاسوب

هذه هي النسخة المستقرة، المفحوصة في 3 أبريل 2011. ش {{PLURAL:1|يوجد تغيير واحد موقوف ينتظر|يوجد [تغييران موقوفان ينتظران|توجد [1 تغييرات تنتظر|يوجد [1 تغييرًا ينتظر|يوجد [1 تغيير ينتظر}} المراجعة.

الدقة منظورة

فيروس الحاسوب هو برنامج خارجي صنع عمداً بغرض تغيير خصائص الملفات التي يصيبها لتقوم بتنفيذ بعض الأوامر إما بالإزالة أو التعديل أو التخريب وما شابهها من عمليات. اي ان فيروسات الكومبيوتر هي برامج تتم كتابتها بواسطة مبرمجين محترفين بغرض إلحاق الضرر بكومبيوتر آخر، أو السيطرة عليه أو سرقة بيانات مهمة، وتتم كتابتها بطريقة معينة.

يتصف فيروس الحاسب بأنه :

برنامج قادر على التناسخ Replication والانتشار.

الفيروس يربط نفسه ببرنامج أخر يسمى الحاضن host.

لا يمكن أن تنشأ الفيروسات من ذاتها.

يمكن أن تنتقل من حاسوب مصاب لآخر سليم.

محتويات [أخف]

مكونات الفيروس

يتكون برنامج الفيروس بشكل عام من أربعة أجزاء رئيسية وهي

آلية التناسخ The Replication Mechanism

وهو الجزء الذي يسمح للفيروس أن ينسخ نفسه.

آلية التخفي The Protection Mechanism

وهو الجزء الذي يخفي الفيروس عن الاكتشاف.

آلية التنشيط The trigger Mechanism

وهو الجزء الذي يسمح للفيروس بالانتشار قبل أن يعرف وجوده كاستخدام توقيت الساعة في الحاسوب كما في فيروس (Michelangelo) الذي ينشط في السادس من آذار من كل عام.

آلية التنفيذ The Payload Mechanism

وهو الجزء الذي ينفذ الفيروس عندما يتم تنشيطه.

[اللغات التي يكتب بها الفيروس

من أهم اللغات التي يكتب بها كود الفيروس هي لغة التجميع اسمبلي لسهولة الوصول لعتاد الحاسوب وهنا أيضاً اللغات الراقية مثل لغة سي ولغة سي ++ وفيجوال سي وفيجوال بيسك.

] طرق انتقال الفيروسات (العدوى)

يمكن أن نميز فئتين من فيروسات الحاسوب تبعاً لآلية العدوى وانتشار الفيروس :

فيروس العدوى المباشر Direct Infector

عندما يتم تنفيذ برنامج مصاب بفيروس من هذا النوع, فإن ذلك الفيروس يبحث بنشاط عن ملف أو أكثر لينقل العدوى إليه, وعندما يصاب أحد الملفات بالعدوى فإنه يقوم بتحميله إلى الذاكرة وتشغيله ,وهذا النوع قليل الانتشار.

فيروس العدوى غير المباشر Indirect Infector

عندما يتم تنفيذ برنامج مصاب بفيروس من هذا النوع, فإن ذلك الفيروس سينتقل إلى ذاكرة الحاسوب ويستقر فيها, ويتم تنفيذ البرنامج الأصلي ثم يصيب الفيروس بالعدوى كل برنامج يتم تحميله إلى الذاكرة بعد ذلك, إلى أن يتم قطع التغذية الكهربائية عن الحاسوب أو إعادة تشغيله.

أسباب التسمية

سمي الفيروس (Virus) بهذا الاسم لأنها تشبه تلك الكائنات المتطفلة في صفتين رئيسيتين:

اولا : فالفيروسات دائماً تتستر خلف ملف آخر، ولكنها تأخذ زمام السيطرة على البرنامج

المصاب. بحيث أنه حين يتم تشغيل البرنامج المصاب، يتم تشغيل الفيروس أيضا ثانيا :
تتواجد الفيروسات في مكان أساسي في الحاسب كالذاكره رام مثلا وتصيب اي ملف يشغل في أثناء وجودها بالذاكره مما يزيد عدد الملفات المصابه كلما طال وقت اكتشاف الفايروس
تستخدم عادة لغة التجميع (الاسمبلي) لكتابة كود تنفيذ الفيروس
أنواع الملفات التي يمكن ان يصيبها الفيروس
بشكل عام الفيروس تصيب الملفات التنفيذية أو الملفات المشفرة غير النصية مثل التالية
الملفات ذاتية التنفيذ مثل ملفات ذات امتداد (.COM., .EXE)ضمن أنظمة التشغيل دوس وميكروسوفت ويندوز ,أو (ELF) في أنظمة لينكس
سجلات الملفات والبيانات(VOLUME BOOT RECORD) في الاقراص المرنة والصلبة والسجل رقم (0) في القرص الصلبMASTER BOOT
ملفات الأغراض العامة مثل ملفات الباتش والسكريبت في ويندوز وملفات الشل في يونيكس
ملفات الاستخدام المكتبي في النوافذ WINDOWS التي تحتوي ماكرو مثل الوورد والاكسل واكسس
قواعد البيانات وملفات الاوتولوك لها دور كبير في الاصابة ونشر الاصابة لغيرها لما تحويه من عناوين البريد الالكتروني
ملفات الاكروبات (PDF) وبعض النصوص المهجنة HTML احتمال احتوائها على كود خبيث
الملفات المضغوطة مثل ZIP,RAR

[طرق الانتقال

أهم طرق الانتقال الآن هي الشبكة العنكبوتية الإنترنت تكون وسيلة سهلة لانتقال الفيروسات من جهاز لاخر ما لم تستخدم أنظمة الحماية مثل الجدران النارية وبرامج الحماية من الفيروسات ياتي ثانيا وسائط التخزين مثل ذواكر الفلاش والاقراص الضوئية والمرنة سابقا وياتي أيضا ضمن رسائل البريد الإلكتروني وأيضا تنتقل الفيروسات إلى نظامك عند استلامه ملفات اي كانت الملفات مخزنة على(اقراص مرنة أو اقراص مضغوطة أو اقراص zip,)

[أعراض الإصابة

تكرار رسائل الخطأ في أكثر من برنامج.
ظهور رسالة تعذر الحفظ لعدم كفاية المساحة.
تكرار اختفاء بعض الملفات التنفيذية.

حدوث بطء شديد في إقلاع[نظام التشغيل]أو تنفيذ بعض التطبيقات. رفض بعض التطبيقات للتنفيذ.

فعند تشغيل البرنامج المصاب فإنه قد يصيب باقي الملفات الموجودة معه في قرص صلب أو المرن, لذا يحتاج الفيروس إلى تدخل من جانب المستخدم كي ينتشر, بطبيعة الحال التدخل عبارة عن تشغيله بعد أن تم جلبه من الايميل أوإنترنت أو تبادل الاقراص المرنة.

تعمل الفيروسات بطبيعتها على تعطيل عمل الحاسوب أو تدمير ملفاته وبرامجة هناك فيروسات تعمل على خلق رسائل مزعجة وأنواع تعمل على تشغيل برامج غير مطلوبة وأنواع تعمل على اشغال المعالج بحيث تبطئ سرعة الحاسوب أو سرقة بيانات من حاسوب المستخدم مثل ارقام حسابات وكلمات السر أو ارقام بطاقات الائتمان وبيانات مهمة أخرى وهذه أهم اهداف الفيروسات الحديثة وبرامج التجسس التي يتم تطويرها يوما بعد يوم

[أنواع الفيروسات من حيث الانتشار

[من حيث النوع

أنواع الفيروسات ثلاثة :(الفيروس والدودة وحصان طروادة) ما الفرق بين الفيروس والدودة وحصان طروادة؟

•الفيروس: يمكن القول بأنه برنامج تنفيذي(ذات نوع .com ,.exe,.bat,.pif,.scr) يعمل بشكل منفصل ويهدف إلى أحداث خلل في نظام الحاسوب وتتروا خ خطورتة حسب مهمته فمنه الخطير ومنه الخفيف وكلاهما خبيث.وينتقل بواسطة نسخ الملفات من جهاز به ملفات مصابة إلى جهاز اخر عن طريق الاقراص المدمجة سي دي وذواكر الفلاش.

•الدودةديدان الحواسيب: فيروس ينتشر فقط عبر الشبكات والإنترنت ويعمل على الانتشار على الشبكات عن طريق دفتر عناوين البريد الإلكتروني مثلا فعند اصابة الجهاز يبحث البرنامج الخبيث عن عناوين الاشخاص المسجلين في دفتر العناوين على سبيل المثال ويرسل نفسه إلى كل شخص وهكذا... مما يؤدي إلى انتشاره بسرعه عبر الشبكه وقد اختلف الخبراء فمنهم اعتبره فايروس ومنهم من اعتبره برنامج خبيث وذلك كون الدوده لاتنفذ اي عمل مؤذي انما تنتشر فقط مما يؤدي إلى اشغال موارد الشبكه بشكل كبير ومع التطور الحاصل في ميدان الحوسبه أصبح بإمكان المبرمجين الخبيثين إضافة سطر برمجي لملف الدوده بحيث تؤدي عمل معين بعد انتشارها (مثلا بعد الانتشار إلى عدد 50000 جهاز يتم تخريب الأنظمة في هذه الأجهزة) أو اي شيء اخر (مثلا في يوم معين أو ساعة أو تاريخ...الخ) وأصبحت الديدان من أشهر الفيروسات على الشبكه العالميه واشهر عملياتها التخريبيه واخطرها تلك التي يكون هدفها حجب الخدمه تسمى (هجمات حجب الخدمه) حيث تنتشر الدوده على عدد

كبير من الأجهزة ثم توجه طلبات وهميه لجاهز خادم معين (يكون المبرمج قد حدد الخادم المستهدف من خلال برمجته للدوده) فيغرق الخادم بكثرة الطلبات الوهميه ولا يستطيع معالجتها جميعا مما يسبب توقفه عن العمل وهذه الديدان استهدفت مواقع لكثير من الشركات العالميه اشهرها مايكروسوفت وغيرها الكثير.

•حصان طروادة Trojan Horse: سمي هذا الفيروس بحصان طروادة لانه يذكر بالقصة الشهيرة لحصان طروادة حيث اختبأ الجنود اليونان داخله واستطاعوا اقتحام مدينة طرواده والتغلب على جيشها وهكذا تكون الية عمل هذا الفيروس حيث يكون مرفقا مع أحد البرامج أي يكون جزء من برنامج دون أن يعلم المستخدم. فعندما يبدأ البرنامج تنفيذ عمله ويصل إلى مرحلة ما حيث تم توزيع قرص مجاني على المشافي به برنامج حول مرض الايدز (أسبابه - طرق انتشاره - طرق العلاج.. الخ) وبعد مدة شهر من تشغيل البرنامج تم تشفير المعلومات على الحواسب الحاضنه للفايروس وظهرت رساله مفادها ان الحاسب مصاب بالايدز (المقصود هنا انه تم تشفير ملفات الحاسب وايقافها عن العمل بطريقه نظاميه) ارسل مبلغ كذا إلى الحساب كذا ليتم إرسال رقم فك الشيفره مما اجبر المختصين بالرضوخ للطلب كونهم لم يستطيعو فك التشفير.

توجد عدة تقسيمات للفيروسات، فمثلاً من حيث سرعة الانتشار هناك فيروسات سريعة الانتشار وفيروسات بطيئة الانتشار ومن حيث توقيت النشاط فهناك فيروسات تنشط في أوقات محددة وفيروسات دائمة النشاط ومن حيث مكان الإصابة فيروسات مقطع التشغيل boot sector على الأقراص وهي الأكثر شيوعاً، وفيروسات الماكرو macro التي تختص بإصابة الوثائق والبيانات الناتجة عن حزمة مايكروسوفت أوفيس، أما من حيث حجم الضرر فهناك الفيروسات المدمرة للأجهزة طبعا لايوجد فايروسات خارقه بحيث انها تدمر الأجهزة كما نسمع أحيانا (احترق المعالج بسبب الفايروس تعطلت وحدة التغذيه بسبب الفايروس أو تلفت الشاشة بسبب الفايروس ،... الخ) ولكن يمكن للفايروس ان يؤذي الذاكره روم في الحاسب كما في فايروس تشرنوبل أو ان يمحي معلومات ال MBR (Main Boot Sector) على القرص الصلب فتعود الاقراص الصلبه كما اتت من المصنع وفي الحالتين السابقتين لا يتم اقلاع الجهاز مما يوحي للبعض ان الفايروس (حرق) الحاسب طبعا هذه الفيروسات تعتبر خطيره جدا لانها تتسبب في اتلاف البيانات المخزنه والتي قد تكون (البيانات) نتاج عشرات السنين مما يؤديي إلى خسائر جسيمة أو إلى توقف الحاسبات عن العمل كما في تشرنوبل مما يؤدي إلى توقف الخدمات المقدمه، وهنالك أيضا الفيروسات المدمرة للبرامج وتاثيرها محدود طالما ان البيانات لم تتاثر حيث يمكن تخزين البيانات واعادة تهئية الحاسب واعادة البرامج المتضرره من اقراصها الاصليه، والفيروسات عديمة الضرر وهي التي لاتقوم باي عمل

مؤذي وانما تم برمجتها لاثبات الذات والقدره على البرمجه من بعض المراهقين فمنها ما يرسم كرة أو اي شكل على الشاشه طوال فترة عمل الكمبيوتر ومنها ما يغير بعض الاحرف (كتغير حرف بحرف اينما وجد) أو تغيير مؤشر الماوس.. الخ.

[عدل] امثلة على بعض الفيروسات

فيروس Brontok أو الفيروس الذي يخفي خيارات المجلداو يفقدك التحكم في الرجستري فتصبح غير قادر على التحكم في الحاسوب: هذا الفيروس من أبرز مهامه أنه يقوم بإخفاء خيارات المجلد من قائمة أدوات الموجودة في نظام الويندوز وأيضا يقوم بتكرار جميع المجلدات التي يصيبها حتى أنك لاتعرف الأصل من النسخة وقد تحذف الأصل ظنا منك أنه الفيروس، وهو أيضا يقوم بفتح شاشة الإنترنت اكسبلورر ويقوم بفتح شاشة خضراء اللون بشكل مستمر ممايسبب بطء في النظام ومما يؤدي ألى زيادة انتشار هذا الفيروس في الكمبيوتر

فيروس xcopy والذي يصيب الـــ Partion القسم للقرص الصلب ويجعله لايفتح مباشرة وذلك بزرع ملف autorun وحينما تحاول فتح القسم يعطيك قائمة فتح باستخدام ولا تستطيع الدخول إلى القسم الذي تريده إلا بطرق ملتوية مثل (استكشاف وتشغيل) للمحترفين فقط ويقوم أيضا بجعل الفلوبي دسك القرص المرن يصيح باستمرار مطالبا بإدخال قرص مرن للكمبيوتر تصنيف الفيروسات حسب خطورتها :

العادي Trivial :

لا يفعل الفيروس العادي شيئا سوى التكاثرreplication ولا يسبب أي ضرر أو تخريب للمعلومات مثل فيروس stupid

الثانوي Minor :

يصيب الملفات التنفيذية فقط executable file ولا يؤثر على البيانات

المعتدل Moderate :

يقوم بتدمير جميع الملفات الموجودة على القرص إما باستبدال المعلومات بمعلومات لا معنى لها أو عن طريق إعادة التهيئة Reformatting مثل فيروس Disk killer الذي يقوم بإعادة تهيئة القرص. ويمكن حل مشكلة هذه الفيروسات عن طريق استخدام النسخ الاحتياطي

الرئيسي Major :

يؤدي الفيروس إلى تخريب المعلومات بإجراء تغيرات ذكية وبارعة للبيانات دون أن يترك أثرا يشير إلى التغيير الحاصل كأن يقوم بتبديل كتل المعلومات المتساوية في الطول بين

الملفات كما أن تأثيره يكون على المدى الطويل ولن يكون من الممكن اكتشاف الإصابة إلا بعد بضعة أيام وبذالك لا يمكن الوثوق بالنسخة الاحتياطية أيضا.

اللامحدود Unlimited :

يستهدف الشبكات والملفات المشتركة وتمضي أكثر الوقت في محاولة معرفة كلمة السر للمستخدمين الأكثر فاعلية وعند معرفتها يقوم بتمريرها إلى أحد أو أكثر من مستخدمي الشبكة على أمل أنهم سيستخدمونها لأغراض سيئة. ترينا الفيروسات كم نحن معرضين للهجوم ولكن بالمقابل ترينا مدى التعقيد والترابط الذي وصل إليه الإنسان. على سبيل المثال

My doom : قدر الخبراء الحواسيب المتضررة من هذه الدودة بحوالي ربع مليون حاسوب خلال يوم واحد والذي كان في كانون الثاني 2004

Melissa: أعطى هذا الفيروس فاعلية كبيرة جدا حيث أجبر شركة Microsoft والعديد من كبرى الشركات الأخرى على إطفاء مخدمات البريد بشكل كامل حتى تمكنوا من القضاء عليه وذلك في آذار 1999

وفي الشهر الأول من عام 2007 ظهرت دودة اسمها Storm وبحلول الشهر التاسع كان أكثر من 50 مليون حاسوب مصاب. كلنا تصور أن كل هذا التأثير ينتج عن برامج بسيطة جدا.

فيروس Melissa :

أنشاء الفيروس على شكل مستند Word ووضع في موقع للأخبار عندما يقوم أي شخص بتحميل الملف وفتحه فإن الفيروس يتفعل ويقوم بإرسال المستند إلى أول 50 شخص في الAddress book والمستند يحوي على ملاحظة لطيفة واسم الشخص المرسل إليه وعندما يقوم المرسل إليه بفتح المستند يتم إرساله إلى 50 شخص أخر وبهذه الطريقة أصبح فيروس Melissa أسرع فيروس في الانتشار

الفيروس I love you الطريق نفسها لكن عوضا عن نسخ نفسه تلقائيا فأنه كان يربط كوده برابط معين ضمن الرسالة وعند النقر عليه كان يرسل نفسه إلى جميع العناوين الموجودة في الAddress book

استخدم الفيروس ميزة الVBA (visual basic for application) وهي لغة برمجة كاملة وتستطيع من خلالها أن تبرمج أي شيء مثل تعديل ملف أو إرسال الرسائل الإلكترونية أي يمكنك كتابة أي برنامج وعند فتح المستند يتم تنفيذه طبعا هي ميزة مفيدة ولكنها في نفس الوقت ميزة تنفيذ تلقائية خيرة

[عدل] لماذا يعمل الناس فيروسات الحاسوب ?

فيروسات الحاسوب لا تتشابه في وجودها بالفيروسات الحيوية. إن فيروس الحاسوب لا ينشأ من لا شيء ولا ياتي من مصدر مجهول ولا ينشأ بسبب خلل بسيط حدث في الحاسوب.

فيروس الحاسوب يتم برمجته من قبل المبرمجين أو الشركات ويتم صنعه بشكل متعمد ويتم تصميمة بشكل متقن. يعمل المبرمجون على برمجة الفيروسات وذلك لاهداف عديدة تتنوع من اقتصادية وسياسية وتجارية وعسكرية. فبعض المبرمجين الهواة يعتبرون أن عمل الفيروس نوع من الفن والهواية التي يمارسونها. ومن أهم الأهداف لعمل فيروس الحاسوب هو الهدف التجاري. ذلك عن طريق عمل وصنع الفيروسات من أجل بيع برامج مضادات الفيروسات لانة بعمل الفيروس يصبح المستخدمون بحاجة إلى برامج مضادة للفيروسات ويضطرون للشراء. يذكر أن المبرمج الذي يعمل الفيروس يعتبر حسب القانون مجرما وصناعة الفيروس جريمة يحاسب عليها حسب قانون الدولة الموجود بها.

معظم شركات مضادات الفيروسات تقوم بصناعة الفيروسات من قبل المبرمجين وتقوم بعمل مضادات لها وذلك لتسويق منتجاتها وبرامجها لدى مستخدمي الكمبيوتر. اما الاهداف العسكرية فهي محاولة الدخول لأنظمة الطرف الاخر لكشف اسرار واخذ بيانات عن طريق برامج التجسس. الاهداف الإجرامية فأهمها سرقة بيانات وارقام حسابات أو ارقام بطاقات الائتمان وكلمات السر لمحاولة الدخول