2010

Introduction to Malware
Arabic paper

- ASK PC "The Largest Arabic Technical Support Community Online" Supervision: Dr. Mohamed N. El-Guindy, PhD, MBCS CITP, AMBILD

Author :Mohamed Hesham Abd alakher
ASK PC Academy
8/27/2010

الشكر والإهداء

الشكر لله سبحانه وتعالى الذي علم الإنسان ما لم يعلم ...

ثم اشكر كل من ساعدني في إعداد هذا البحث ...

واشكر كل القائمين بالعمل على ASK PC Academy
وتحية خاصة إلى دكتور محمد الجندي وإتاحتهم الطيبة لي الفرصة في المشاركة في المسابقة الرائعة واهدي إليهم هذا العلم المتواضع وأتمنى من الله الإفادة لهم والنفع....

مقدمة

في البداية آخى القارئ نحن نتحدث بالفعل عن امن المعلومات وانه ليس مصطلح جديد لمن لا يعرفه ولكن تطور مفهومه الحقيقي عندما دخل ضيف جديد علينا وهو الانترنت فقد كانت عمليات التخريب والسرقة بما فيها سرقة الأموال أو المنقولات الثمينة والمعلومات المهمة من الآخرين وإيقاع الضرر بهم من أقدم الأخطار التي تعرض لها الإنسان وتختلف دوافع التخريب والسرقة من شخص لأخر ولكن في النهاية هناك طرف يقع عليه الخسارة والضرر ففي الماضي وخصوصا قبل ظهور الوسائط الالكترونية لتخزين المال والمعلومات لنقلها كان من اليسير اكتشاف السرقة بسرعة لان السارق لا بد إن يترك في معظم الأحوال أثرا لفعلته الشنعاء إلا انه مع ظهور ضيفنا الجديد وهو الانترنت واتساع نطاق استعمالاته قد يصعب اكتشاف اثر السرقة ولذلك لا يشعر المتضرر بفقد المعلومة أو المال إلا بعد فوات الأوان في بعض الحالات وسوف تتزايد هذه الأضرار مع سرعة تقدم في مجالات الاتصالات والحاسبات وهذه احد الإعراض التي يعانيها العالم بأسره عند استحداث تقنيات جديدة وكما هو مسلم به في كل مكان في العالم أن التقنيات لها محاسنها وعيوبها ولكن إذ يدو عقلك نتحدث عن امن المعلومات في وطننا العربي نجد أن الأمن لا يتعدى نسبة 1% ولان تضحك وتتبسم عندما توجد في دولة عربية بان يعتبر مجال امن المعلومات من المجالات التقنية التي لم تحظ باهتمام كبير في البلدان العربية حتى الآن نظرا للمفهوم السائد **Business first, security later!**

هكذا أطلق العرب شعارهم وفضلوا " السبوبة " هو ما يهيمن جميعا ألان وأيضا أن تجد أبحاث باللغة العربية في امن المعلومات من النادر فجرب وابحث في جوجل عن أى من المواضيع والأبحاث وغيرها ستضحك كثيرا عندما تصل إلى معلومة في الكثير من ساعات متعددة ولهذا يلجأ الطلبة والطالبات إلى اخذ دورات معتمدة من جهات عالمية في تخصص امن المعلومات على جميع المستويات للمساهمة في تطوير الوضع الراهن وأيضا إتاحة فرص جديدة للعمل في مجال تحتاجه المنطقة العربية

فانه اليوم وكل يوم منذ إن حل بديارنا الضيف الجديد "الانترنت " فتضرر الكثير من الحواسب جراء إصابتها بالبرامج الخبيثة "Malware" سواء من حيث فقدان المعلومات او من حيث الجهد والوقت المستغرق في إزالة تلك البرمجيات الخبيثة بنجاح من النظام

جدول المحتويات:

تعريف " أمن المعلومات "

يمكن تعريف أمن المعلومات بأنه العلم الذي يعمل على توفير الحماية للمعلومات من المخاطر التي تهددها أو الاعتداء عليها وذلك من خلال توفير الأدوات والوسائل اللازم توفيرها لحماية المعلومات من المخاطر الداخلية أو الخارجية. المعايير والإجراءات المتخذة لمنع وصول المعلومات إلى أيدي أشخاص غير مخولين عبر الاتصالات ولضمان أصالة وصحة هذه الاتصالات وان امن المعلومات هو أمر قديم ولكن بدا استخدامه بشكل فعلي منذ تطور التكنولوجيا..... فإننا نستطيع تغيير قواعد اللعب« مع المهاجمين بحيث يصبحون أقل اهتماما بمهاجمة حواسيبنا"""

تعريف البرمجيات الضارة او الخبيثة

البرمجيات الخبيثة (Malware)هي اختصار لكلمتين هما :("malicious software" وتعني البرمجية الماكرة أو الخبيثة، وهي برنامج مخصص للتسلل إلى نظام الحاسب أو تدميره بدون رضا المالك. وما إن تم تثبيت البرمجية الخبيثة فإنه من الصعب جداً إزالتها. وبحسب درجة البرمجية من الممكن أن يتراوح أذاها من إزعاج بسيط (بعض النوافذ الإعلانية الغير مرغوب بها خلال عمل المستخدم على الحاسب متصلاً أم غير متصلا بالشبكة) إلى أذىً غير قابل للإصلاح يتطلب إعادة تهيئة القرص الصلب على سبيل المثال. من الأمثلة على البرمجيات الخبيثة هي الفيروسات،وأحصنة طروادة وغيرها .يجب أن لا يتم الخلط بين البرامج الخبيثة والبرامج المعيبة، والتي هي برامج مكتوبة لأهداف مشروعة لكنها تحوي أخطاءً أو مشاكل.

وبالرغم من أهمية هذا الحقل من البرمجيات الخبيثة والفيروسات ودراستها والقضاء عليها إلا انه يندر وجود بحوث عربية في هذا المجال وذلك لسببين هامين :

الأول : لتنوع المجالات التي ينبغي الإلمام بها قبل الخوض في تقنيات المحاربة على هذه البرمجيات الضارة

والثاني : لندرة هذا الحقل وهو عدم وجود مراجع كافية تشرح كيفية عمل تلك البرامج او كيفية عملها بشكل مفصل فالشركات التي تصنع البرامج المضادة لا تفصح عن خوارزميات برامجها ولا عن كيفية بنائها حتى لا يتم سرقتها بواسطة أى منافس أخر .....

فتداخلت الأدوار وأصبح كاتب هذه البرمجيات الضارة يبحث عن الحماية وكاتب الحماية أصبح يبحث عن الكسر وهكذا تدور العجلة وينتصر من يملك المعلومات الأكثر Knowledge

فقديما كنا نسمع المثل " Knowledge is Power" ولكنه غير صحيح في مجال الحاسوب وبالأخص مجال البرمجيات الخبيثة والفيروسات والقضاء عليها حيث يجب تطبيق المعلومات والاستفادة منها بشكل حقيق وهذا ما نسعى إليه تفصيليا بإذن الله في هذا البحث البسيط:

" Knowledge's is not enough, we must apply it "

تعاريف أساسية Malware Definitions

هناك أربعة مخاطر رئيسية تصيب الأنظمة:

Spam

يشير المصطلح إلى استخدام عدة طرق لإغراق البريد Mailbox الخاص بالمستخدمين .الدراسات تشير إلى أن حوالي% 70 من حركه البريد Email traffic مصاب بالSpam Message ..

Bugs

يشير المصطلح إلى الأخطاء البرمجية الموجودة في الأنظمة، وفي حال وجدت هذه الأخطاء يمكن أن تسبب في أبسط الحالات تحطيم للبرنامج Crash أو حذف البيانات وتخريبها أو تؤدي لوجود ثغرة في النظام Security Weakness يمكن أن يستفاد منها لاحقًا في اختراق النظام بالكامل.

Denial of Services

يشير المصطلح إلى الهجوم على النظام من خلال إغراقه بالطلبات وذلك لاستهلاك المصادر Consume Resources حتى يتحطم النظام بالكامل أو على الأقل تبطئ الـــNetwork Traffic

Malicious Software

تعد البرامج الضارة (اختصارا بـــ Malware) من أخطر أنواع المخاطر السابقة حيث يمكن من خلال هذه البرمجيات أن تسبب في كل المخاطر السابقة، مثلا تقوم بإرسال رسائل Spam من جهاز أحد المستخدمين العاديين ، أو أن تكون مرفق مع أحد رسائل لـــــSpam أو أن تستغل وجود Bug في أحد الأنظمة لكي تخترقه ،أو تستخدم في القيام بهجوم من DoS لذلك سوف يكون الحديث في هذا الباب عن هذا النوع من المخاطر وتفصيل أنواعه..

تحليل البرمجيات الضارة ودراسة سلوكها وطريقة عملها

أهداف عمل البرمجيات الضارة

بأضرار بالغة.على كلٍ، فمنذ بداية انتشار حزم الوصول العريضة للإنترنت، أصبحت البرامج الخبيثة الجديدة متجهة لدافع ربحي. فعلى سبيل المثال، ومنذ عام 2003 ربما قام المبرمجون الصغار بكتابة البعض منها لإثبات ما يمكن أن يقوموا به ولأي مدى بإمكانهم كتابتها بالإنترنت أخرى من البرمجيات الخبيثة الربحية الهدف هي برامج التجسس spyware والتي صممت لتراقب تصفح المستخدم للانترنت وإظهار إعلانات غير مرغوب بها بهدف حصول داعم كتابتها لتكون عديمة الضرر ومزعجة نوعاً ما وليس من أجل التسب بالمنتشرة تم تصميمها للسيطرة على حواسب المستخدمين لاستغلالها لأغراض غير قانونية أو إجرامية. فالحواسب المصابة بفيروس zombie تم استخدامها لترسل بريداً يحوي مواد ممنوعة كاستغلال القاصرين، أو لتنظيم هجمات حجب الخدمة الموزعةdistributed denial-of-service attacks " كطريقة للابتزاز.

ظهرت صيغة أخرى من البرمجيات الخبيثة الربحية الهدف هي برامج التجسس spyware والتي صممت لتراقب تصفح المستخدم للانترنت وإظهار إعلانات غير مرغوب بها بهدف حصول داعم هذه الإعلانات (والذي هو منشئ البرنامج) على عائد إعلاني من جراء تكرار وصول المستخدمين الكبير إليها. برامج التجسس لا تنتشر عادةً بنفس الطريقة التي تنتشر ومن البرامج العدائية أكثر منها ما صمم لتخريب البيانات أو التسبب بضياعها. والعديد من فيروسات نظام MS-DOSصممت لتدمير الملفات على القرص الصلب أو لتخريب نظام الملفات وذلك بكتابة بيانات لا معنى لها. ويمكن أن نعطي ديدان الشبكات مثل دودة Code Red أو Ramenنفس التصنيف، فهي مصممة لتخريب المعلومات أيضاً ولكن لصفحات الويب.

والانتقام كان أيضاً دافعاً لكتابة برامج خبيثة. كأن يقوم مبرمج أو مدير على وشك أن يطرد من عمله بترك مداخل خلفية للنظام backdoor أو برامج "كقنبلة موقوتة" تسمح له بتدمير نظام صاحب العمل السابق أو تخريب عمله السابق.

ظهرت صيغة أ بها الفيروسات، إذ أنها تنصب عادةً باستغلال ثغرات أمنية في متصفح الإنترنت أو أنها تنصب كحصان طروادة Trojan Horse عند تنصيب برنامج آخر.

وأصبحت ألان البرامج الخبيثة بهدف الربح.....

spyware, botnets, loggers and dialers"

فخلال فترة الثمانينيات والتسعينيات كانت الفكرة عن البرامج الخبيثة أنها برمجيات تم إنشاؤها بهدف التخريب أو المزاح. ولكن وفي الآونة الأخيرة فإن معظم البرمجيات الخبيثة قد تمت كتابتها بدافع ربحي. برغبة من كاتبي هذه البرامج من السيطرة على الأنظمة المصابة وتحويل هذه السيطرة لتعود عليهم بعائد مادي. ومنذ حوالي عام 2003 أصبحت أكثر البرمجيات الخبيثة كلفة (من حيث المال والوقت اللازم لاستعادة الأنظمة) هي برامج التجسس .Spyware برامج التجسس هي برامج يتم إنشاؤها تجارياً بهدف *جمع المعلومات عن مستخدمي الكمبيوتر، *إظهار نوافذ إعلانية *وتعديل أداء متصفح الإنترنت ليفيد صانع البرمجية مادياً. وبعض برامج التجسس الأخرى التي شوهدت تعدل على شفرة داعمي الإعلانات بحيث يصبح الدخل العائد لهم موجهاً إلى منشئ البرنامج الماكر بدلاً من صاحب الموقع الحقيقي.

عادةً ما يتم تنصيب برامج التجسس بشكل أو بآخر من أحصنة طروادة: تختلف بمنشئها، تقدم نفسها بشكل مفتوح على أنها تجارية (على سبيل المثال بيعها مساحة إعلانية على النوافذ التي تظهر من البرنامج). ومعظم هذه البرامج تقدم للمستخدم اتفاقية ترخيص للاستخدام مغزاها حماية منشئ البرنامج من الملاحقة القانونية.

طريقة أخرى شجعت منشئي هذه البرامج على الاستفادة مادياً منها هي استخدام هذه الحواسب لتقوم بالعمل عنهم. ففيروسات السبام (أو الرسائل الغير مرغوبة) ومنها عائلة فيروسات So big و My doom تعمل لصالح عصابات سبام البريد الإلكتروني. فالكمبيوترات المصابة تستخدم كخدمات وكيلة لإرسال الرسائل الغير مرغوب بها. والفائدة التي يجنيها مرسل الرسائل باستخدامه الكمبيوترات المصابة هي توافرها بكميات كبيرة (كل الشكر للفيروسات!) كما أنها تؤمن لهم الخفاء، وتحميهم بذلك من الملاحقة. كما أن مرسلي هذه الرسائل قاموا باستخدام الكمبيوترات المصابة لتنظيم هجمات حجب خدمة موزعة تستهدف المؤسسات المضادة لهذا النوع من رسائل الـ.Spam

وحتى يتمكنوا من تنسيق نشاطات عدة كمبيوترات مصابة قام المهاجمون باستخدام أنظمة تنسيق معروفة باسم .botnets في هذه الأنظمة تقوم البرمجية الخبيثة بالدخول إلى قناة IRC (Internet Relay Chat) أو نظام دردشة آخر .ويستطيع المهاجم إعطاء تعليمات إلى جميع الأنظمة المصابة بنفس الوقت. ومن الممكن استخدام أنظمة BotNets لتحميل نسخة محدثة من البرمجية الخبيثة إلى النظام المصاب لتبقيهم عاصين على مضاد الفيروسات أو أي مقاييس أمنية أخرى.

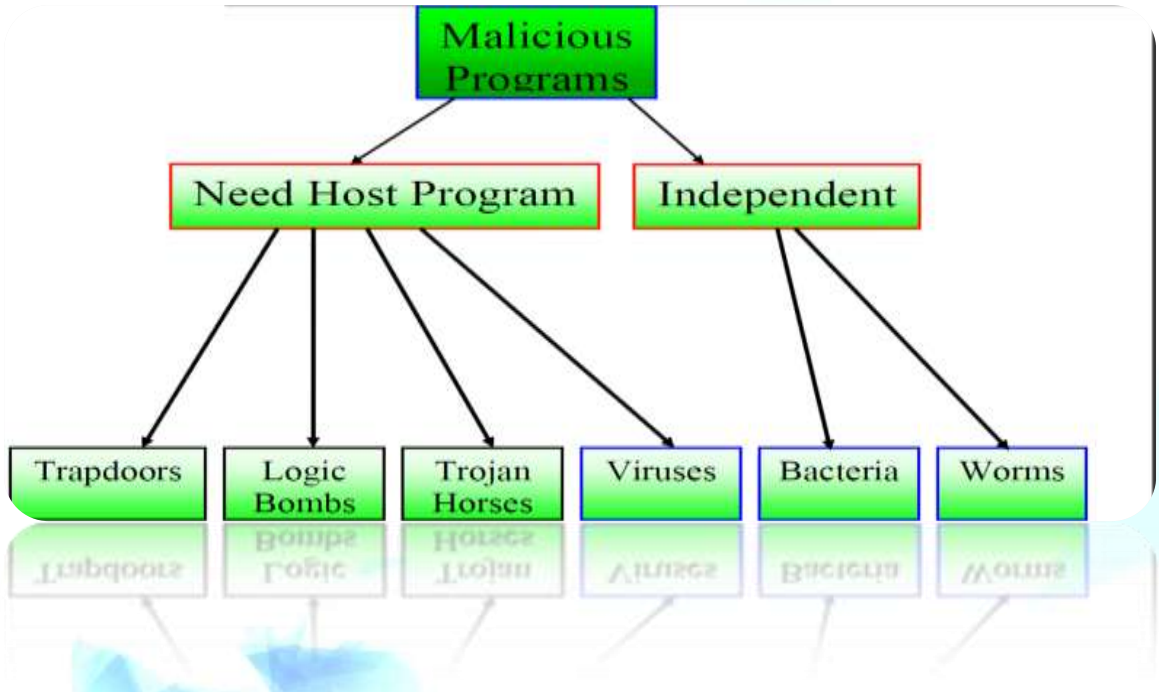
وأخيراً من الممكن لمنشئ البرمجية الاستفادة مادياً ببساطة بالسرقة من الشخص صاحب الكمبيوتر المصاب. بمعنى أنه من الممكن سرقة كلمات السر أو أي شيء مالي آخر. بعض البرامج تقوم بتنصيب برنامج key logger ليقوم بنسخ ضربات المستخدم على لوحة مفاتيح الحاسب عند إدخاله كلمة سر أو رقم بطاقة ائتمانية أو أية معلومة مفيدة أخرى. ومن ثم يتم إرسالها إلى منشئ البرنامج تلقائياً مما يمكنه من سرقة البطاقة الائتمانية وأي شكل آخر من السرقة .وبالطريقة نفسها يمكن للبرمجية نسخ مفتاح القرص الليزري أو كلمة سر للعبة على الإنترنت فتسمح له بسرقة حسابات أو أمور أخرى افتراضية.

وطريقة أخرى للسرقة من الحاسب المصاب هي التحكم بالمودم والقيام باتصالات مرتفع الثمن، ومن ثم ترك الخط مفتوحاً مما يكلف المستخدم فواتير هاتف بمبالغ مالية كبيرة

تصنيف البرامج الخبيثة

البرامج بطبيعة الحال مرنة وقابلة للإضافة والتعديل، لذلك أغلب الـ "Malware" هذه الأيام لا يمكن تصنيفها بسهوله، حيث أنها تحتوي على خصائص من أي صنف مما قد يجعلها مهجنة Hybrid

يقدم الشكل التالي تصنيفا كليا للتهديدات البرمجية (أو البرامج الخبيثة) وينمن تصنيفا كالتالي



برامج خبيثة تحتاج إلى مضيف (Malicious Programs need host program)

في الأساس تكون عبارة عن أجزاء لبرامج لا يمكن إن توجد بشكل مستقل عن بعض برامج التطبيق الحقيقية أو البرامج المساعدة و برامج النظام .

برامج خبيثة مستقلة (Independent malicious programs)

هي برامج ذات محتوى يمكن جدولتها وتشغيلها من قبل نظام التشغيل .

وهنالك تصنيف أخر لهذه التهديدات من حيث تكرارها لنفسها وعدم تكرارها :

برامج خبيثة لا تكرر نفسها (Non – replicate malicious programs)

وهى عبارة عن أجزاء من برامج يتم تنشيطها عندما يتم نداء البرنامج المضيف لانجاز عملية معينة .

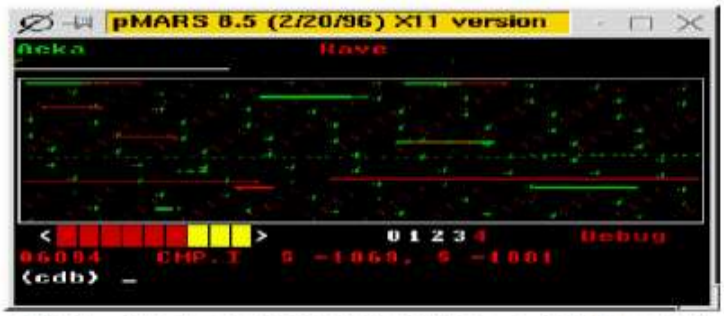
برامج خبيثة تكرر نفسها (Replicate malicious programs)

وهى تتكون من جزء من برنامج (Virus) أو قد تكون برنامجا مستقلا (Worm ,,bacteria) وعند تنفيذ هذه البرامج قد تنتج نسخة أو أكثر من نفسها بغرض تفعليها في نفس النظام أو في نظام أخر

تاريخ الفيروسات والديدان تفصيليا.

في معامل Bill قام الباحث الأول victor vyssotsky بعمل لعبة سميت بـــــ Darwin تقوم فيها برامج صغيرة بالتنافس مع بعضها البعض في بيئة تخيلية وساعده في ذلك زميله الأخر Douglas McElroy الذي برمج الكثير في اللعبة بالإضافة إلى كتابة المحاكي في اللعبة والباحث الثالث روبرت موريس Robert Morris Sir قام بمساعدتهم حيث أضاف بعض الإضافات على اللعبة واستخدمت اللعبة وقتها في جهاز IBM 7090 ولن تشتهر في ذلك الوقت مما أدى إلى نسيانها ....

بعد ذلك وبتطور الحاسبات طورت اللعبة من قبل الباحثين وأصبحت Core War والتي ما زال هناك العديد من المبرمجين والرياضيين يلعبون هذه اللعبة إلى وقتنا هذا حيث يستخدم اللاعب لغة أسمبلى تسمى " Red code " ويقوم بمهاجمة اللاعب الأخر ويخسر اللعب في حال كان مؤشرا التعليمات "Program Counter" يشير لتعليمة خاطئة ليست من ضمن تعليمات الـــــ" Red code ".. كانت البرامج فى Core War تعمل فى بيئة افتراضية "Virtual Machine" ولكن ليس جميع هذه الألعاب تتطلب ذلك فلعبة "Darwin" لم تتطلب ذلك



الشكل 1-1يبين صوره للعبة Core War تحت المحاكي PMars

وبعد بضعة أعوام شهد أول تطبيق لها في أوائل 1970 حيث قام Bob Thomas في شركة BBN بالتجربة في نظرية التكاثر الذاتي Self-Replicating Program " ونتج عن ذلك الفيروس "Creeper" الذي يعد أول وأسرع الفيروسات حيث أصاب أجهزة شركة DEC "من النوع PDP-10" والتي كانت تعمل على نسخة من نظام تشغيل " TENEX " فقد دخل هذا الفيروس عن طريق الشبكة "APANET" وقام بإصابة الأجهزة الأخرى على الشبكة . تأثير Payload ذلك الفيروس كان من خلال طباعة الجملة

."I'm the creeper, catch me if you can!"

وبعد إصابة الـــــ" Creeper"للعديد من الأجهزة قام Bob Thomas ببرمجة برنامج الـــــ "Reaper" لكى يتم القضاء على هذا الفيروس واستخدم نفس الية الإنتشار التي استخدمها الفيروس وبالتالي يعد الـــــ "Reaper" أول برنامج مضاد للفيروسات على الإطلاق

وبالتعريف الصحيح للفيروسات نجد إن ال" Creeper" لا يعد من الفيروسات ولكنه يصنف ضمن الديدان " Worms"وذلك لأنه

- يقوم بنشر نفسه عبر الشبكة Network Reproducing
- بالإضافة إلى عدم قدرته على إصابة الملفات التنفيذية

في هذه أللمحه التاريخية لن نفصل كثيرا في تصنيف ال Malware لذلك سوف نذكرهم جميعا بالفيروس "Virus" كما هو اللفظ الشائع للبرامج الخبيثة عامة " Software"Malicious

وبعدها وبمرور ثلاثة أعوام 1974 ظهر نوع جديد من الفيروسات يقوم بمحاولة استهلاك مصادر الجهاز " System Resources" بقدر الإمكان * وبداية مع الوابت "Wabbit" حيث يقوم هذا البرنامج بنسخ نفسه

مرات عديدة في النظام إلى أن تمتلئ الذاكرة ويقل أداء النظام إلى آن يحدث Crash للنظام .. ويعتبر هذا البرنامج من نوع الـــــFork Bomb وهو احد أنواع تصنيف شامل لهذا النوع من البرامج وهو الـــــRabbit .....

ولم تسلم البرامج العادية أيضا من الفيروسات فاللعبة "Animal" التي تعد من أشهر الألعاب على الأجهزة الضخمة Mainframe في فترة السبعينات 1970 تم التعديل عليها لكي تشكل ضررا للمستخدم وفى الأساس تقوم فكرة اللعبة على سؤال المستخدم 20 سؤال عن نوع الحيوان الذي يفكر به المستخدم ويبدأ المبرمجين بالتخمين حول هذا الحيوان . وقام جون واكر John Walker وهو مبرمج نظم لأجهزة الـــــ "UNIVAC " في ذلك الوقت بعمل تعديل بسيط على اللعبة حيث تحسنت بشكل جيد وبدأ كثير من المستخدمين بإرسال الأشرطة taps لبريد جون واكر حتى يرسل لهم النسخة المعدلة من اللعبة والذي كان بدوره لا يتردد في إرسال اللعبة لمن يريد . ولكن عملية التحميل والإرسال كانت مرهقة لدرجة الجنون لذا بدأ يفكر في كيفية إرسال اللعبة بدون أي تدخل من المستخدم ." Self-Reproducing "

ومن الألعاب الى الفيروسات حيث قام جون في 1975 بعمل نسخة جديدة من الـــــ "Animal"ولكن هذه المرة احتوت على برنامج فرعى يسمى بـــــ" Pervade "

يقوم هذا البرنامج الفرعي عندما تبدأ اللعبة بالعمل بفحص جميع مجلدات النظام ونسخ نفسه لأي مجلد واستبدال أي نسخة قديمة بالنسخة الجديدة للعبة

وبالرغم من قدم هذا الفيروس إلا انه شوهد بعد فترة في احد الأجهزة الصغيرة Unisys200 والى يعتبر احد أحفاد UNIVAC وهكذا يتم مرة أخرى إثبات إن الفيروسات لها طبيعة متقلبة unpredictable nature لا يمكن التكهن بها أو معرفتها حينها اعتبر Pervading Animal أول فيروس ينتشر in the Wild .

جون واكر بعدها بعدة سنوات في 1980 أسس شركة Autodesk وساهم كمبرمج في برنامج الاتوكاد AutoCAD الشهير .....

وبانتشار الأجهزة المكتبية Desktop Computer في ذلك الوقت لم يساعد ذلك فقط على ظهور العديد من الفيروسات بل ساعد على ظهور العديد من مبرمجين الفيروسات والذي تعلموا العديد من خفايا وأسرار عمل تلك الأجهزة .. واحد أبرز المبدعين هو الطالب ريتشارد سكرينتا Rich Skrenta البالغ من العمر 15 سنة حيث تعلم العديد من الأمور حول أجهزة APPLE II وقام بكتابه العديد من البرامج الطريفة يقوم بإعطائها لزملائه في الفصل .....

الشكل 1-2 يبين ريتشارد سكرينتا أول مبرمج فايرس لأجهزة أبل

إن جهاز APPLE II كان من الأجهزة التي تقلع من خلال نظام التشغيل يكون موجود على القرص المرن Floppy Disk وكان ريتشارد في بداية الأمر يأخذ أقراص أصدقائه لتوزيع الألعاب على حد قوله في تصريحه – ويقوم بإضافة برامجه الخاصة والتي كانت تقوم بإعادة تشغيل الجهاز أو طباعة رسالة على الشاشة بشكل يزعج الطلاب وحينما اكتشف الطلاب إن ريتشارد هو من يقوم بذلك فامتنعوا عن إعطائه أقراصهم الخاصة وعدم اخذ أي شيء منه مرة أخرى . فمن هنا فكر ريتشارد بطريقة تجعل البرنامج يقوم بتوزيع نفسه "self-propagating ويصيب أقراص APPLE II وقام بكتابة البرنامج في 1982 الذي سمي بـــــ Elk Cloner حيث يقوم الجهاز المصاب بإعادة تشغيل الجهاز كل 5 مرات تشغيل إضافة إلى طباعة قصيدة على الشاشة كل 50 إعادة لتشغيل الجهاز ...

الشكل 1-3 يبين الPayload للفايروس Elk-Cloner

في نفس العام ومن معامل Xerox PARC قام الباحثان John ShochوJon Hupp بعمل أول تجربة سموها فيما بعد بالاسم الدودة "Worm" نسبة إلى رواية الخيال العلمي The Shockwave Rider والتي تتحدث عن برنامج "tapeworm" انتشر حول شبكة تربط جميع إنحاء العالم ومن هذه الرواية أخذ الاسم الدودة worm كاسم للبرامج التي تنتشر عبر الشبكة

المحاولة التي قام بها الباحثان في معامل زيوركس كان الهدف منها هو عمل تحديث لبرنامج يقوم بقياس أداء الشبكة ولكن لم تمض تلك المحاولة كما تمنى الباحثان حيث أدى إلى وجود خطأ Bug في البرنامج إلى فشل التجربة بالكامل وتحطيم Crashed حوالي 100 جهاز كانوا من ضمن هذه التجربة..

وبمرور سنتين من تلك المحاولة في 1984 وبالدراسة الأكاديمية التي أجراها الطالب فريد كوهين Fred Cohen والتي اعتبرت أول دراسة حقيقة أكاديمية في مجال البرامج ذاتية الانتشار Self-Replicating Programs في جامعة Lehigh حينها وبمعاونة مشرفه أدلمان Adelman (وهو احد مخترعي شفرة RSA والحرف الأول من اسم الشفرة يعود إليه)

تم تسمية تلك البرامج بالاسم فيروسات "Viruses" والذي تم اقتباسه من إحدى روايات الخيال العلمي ومنذ تلك الوقت انتشر ذلك الاسم والى اليوم يعرف فريد كوهين بأنه الأب للمصطلح الفيروسات "Father of Computer Viruses"

الشكل 1-4 يبين فريد كوهين أول من أستخدم المصطلح Virus .

وبعد أربعة سنوات أخرى 1986 ومن قلب مدينة لاهور في باكستان قام الإخوة باسط فاروق 19 سنة وامجد فاروق بكتابة أول فيروس يصيب أجهزة IBM PCs وسمي ذلك الفيروس بـــ "Brain" نسبة إلى اسم الشركة التي أسسها الأخوان .حيث يصيب هذا الفيروس قطاع الإقلاع في الأقراص المهيأة بنظام ملفات FAT ويقوم بنقل الإقلاع إلى مكان أخر على القرص واستبداله بنسخة من الفيروس .

وكما ذكر الأخوان لمجلة TIME فيما بعد ان القصد لم يكن بغرض التخريب وإنما كان لحماية برامجهم الطبية التي يقوموا بصنعها من القرصنة وأن الرسالة سوف تظهر في حال قام من يريد انتهاك حقوق الملكية للبرنامج وربما كانوا صادقين في ذلك فالرسالة التي يخرجها الفيروس تحتوى على أسماء المبرمجين وأرقام هواتفهم واحتوى على رسالة تطلب الاتصال في حالة الإصابة ...

" Beware of this VIRUS.... Contact us for vaccination..."

الشكل 1-5يعرض صورة من قطاع الإقلاع لأحد الأقراص المصابة بفايروس الـــBrain .

وبعد مرور سنتين 1988 وبقيام الطالب الخريج روبرت موريس (يطلق عليه الابن بسبب تشابه الاسم مع روبرت موريس – الأب مبرمج اللعبة Darwin-) بكتابة دودة استغلت العديد من الثغرات في نظام "Unix " وأصابت حوالي 5% من الأجهزة المتصلة بالانترنت وسيتم توضيح عمل هذه الدودة بإذن الله عند الحديث حول الديدان بشكل عام.....

كل هذا كان مجرد البداية فقط عند بداية التسعينات كان عدد الفيروسات المعروفة يقدر ب 200 فيروس فقط ومن ذلك الوقت انتشرت فيروسات أكثر خطورة وتطور وأكثر ذكاء (وصلت عددها إلى 7000 فيروس في 2003) بدءا من فيروسات الماكرو" Macro Virus " (ظهرت في 1995) وفيروسات البريد Mass-Mailing والتي ترسل نفسها عبر البريد كمرفق " Attachment " (مثل فيروس ILOVEYOU الشهير والذي انتشر في 2000 ويقوم بإرسال رسالة بعنوان ILOVEYOU تحتوى على الفيروس كمرفق)

وانتهاء بالفيروسات أو الديدان والتي استغلت برامج معينة في النظام مثل SQL Slammer في عام 2003 والتي استغلت ثغرة Buffer Overflow في برنامج MS-SQL Server وأدت لتقليل حركة traffic العديد من مستضيفي المواقع Host

وأخيرا الدودة الأخيرة ظهرت أول نسخة منها في عام 2008 المسمى ب " Kido أوConficker " والتي استخدمت طرق متقدمة في الإصابة واستهدفت أنظمة لويندوز واستغلت ثغرة في "NetBIOS" في الويندوز الشكل التالي يبين مدى انتشار الدودة في الولايات المتحدة حيث انتشرت بمعد ل 6% من الأجهزة المتصلة بالإنترنت.

الشكل 1- 6 يبين انتشار الدودة Conficker في الولايات المتحده في April 2009

أنواع البرمجيات الضارة Malware Type:

تقسم البرامج الخبيثة "Malware " لعدة أقسام اعتمادا على طريقة عمل هذه البرامج ، وبغض النظر عن تسمية هذه البرامج وتصنيفها يستطيع مضاد الفيروسات القضاء عليها جميعا.

هناك عده أمور تشترك فيه هذه البرامج:

الانتشار الذاتي Self-Replication : وتشير هذه الخاصية إلى أن البرنامج لكي ينشر نفسه يقوم بإنشاء نسخ عديدة من نفسه "instance" بشكل متكرر .ويمكن أن ينتشر البرنامج عندما يقوم المستخدم بنقله بشكل يدوي إلى جهاز أخر ، ولكن هذا لا يعني أنه "Self-replicating".

قابلية التغيير Population growth: تشير هذه الخاصية إلى أن النسخة الجديدة من الفيروس يحصل بها تغيير وبالتالي تختلف عن الفيروس الأصلي ولو بشكل بسيط. فبعض الـــ "Malware " التى لا تعد "Self-Replicating " لها درجة الصفر في الـــ "population growth " والعكس غير صحيح حيث يمكن أن يكون الـــ"Malware " من الـــ"Self-Replicating " لكنه له Zero في معدل التغيير .

التطفل "Parasiti":: تشير هذه الخاصية إلى أن الـــ "Malware " يحتاج إلى أن يلتصق –يتطفل -بأي كود تنفيذي "executable code " حتى يعمل .الكود التنفيذي يمكن أن يكون الكود في قطاع الإقلاع "Boot block disk " أو أي "Binary code " أو "Interpreted code " وبعض الأحيان يكون الكود المصدر "Source Code " القابل لعملية الترجمة.

وفيما يلي نقوم بسرد أغلب أنواع هذه البرمجيات الضارة مع شرح مبسط لوظيفة والية عمل كل منهم.....

النوع الأول : Logic Bomb:

من حيث الخواص"

الإنتشار الذاتي Self-Replicate : لا يوجد

قابلية التغيير Population growth: صفر Zero

التطفل Parasitic : محتمل possibly .

الـــ"Logic Bomb " هو كود تنفيذي يتكون من جزأين ، الجزء الأول وهو الوظيفة "Payload " التي يقوم بها وهي غالبا ما تكون وظيفة لها طابع خبيث "Malicious Effect".أما الجزء الثاني وهو الـــ "Trigger " وهو شرط تنفيذ الـ"Payload " وقد يكون مرتبط ذلك الشرط بتاريخ معين متى تحقق يبدأ الـ"Payload " بالعمل، أو قد يكون الـــ "Trigger " مرتبط بتسجيل دخول مستخدم معين أو أي شرط ممكن.

من الممكن أن يتم إدخال ال"Logic Bomb " في برنامج ما– بين الأسطر البرمجية "Inserting to code " أو قد يكون برنامج مستقل بذاته "Standalone Application" الـــ"Pseudo-code " التالي يبين كيف يقوم "Logic Bomb " بتحطيم الجهاز عند اليوم ال13

```
//...
// other code
//....

if date == 13
    Crash_Computer() ;

//...
// other code
//....
```

الشكل 1- 9 يبين الPseudo-Code لل Logic Bomb

مثل هذا النوع صغير الحجم يكون عالي الخطورة في حال أدخل وسط عشرات الأكواد الأخرى حيث لا ي مكن اكتشافه بسهوله،وقد حدث أنه تم طرد أحد الموظفين فقام بكتابة "Logic Bomb" ووضعه في سيرفر الملفات الذي يستخدمه الموظفين وكان الـ"Trigger " بالضبط بعد أخر يوم له في العمل ، وبالفعل عند ذلك اليوم تم مسح جميع بيانات وملفات الموظفين في السيرفر، وتم بعد ذلك قبض الموظف الغاضب وحبس 41 شهر نتيجة لما قام به.

النوع الثاني Trojan horse:

من حيث الخواص :

الانتشار الذاتي Self-Replicate : لا يوجد

قابلية التغيير Population growth :صفر Zero

التطفل : "Parasitic " : نعم

يعود الاسم "Trojan Horse " لقصة حصان طروادة الشهيرة ، حيث تمكن اليونانيين من الاستيلاء على مدينة طروادة وذلك عندما بنوا حصان خشبي ضخم واختفى الجنود بداخل ذلك

التمثال الخشبي وقدم هذا التمثال كهدية لمدينة طروادة ، وعندما أدخل للمدينة وفي منتصف الليل خرج الجنود من التمثال واستولوا على المدينة. وهذا ما حدث بالطبع في الفيلم الشهير "Troy"

في عالم الحاسب لا يختلف طروادة كثيرا في المفهوم، حيث هو برنامج يعمل بشكل عادي ولكن يقوم ببعض المهام الضارة بشكل خفي، أحد الأمثلة على برامج الـ"Trojan Horse " هي برامج تسجيل الدخول المزيفة "fake login " حيث لها واجهة تشبه واجهة البرنامج تمامًا، تقوم هذه البرامج بحفظ الباسورد "Password-Grabbing " الذي يدخله المستخدم ثم تخرج له رسالة خطأ حتى يعيد إدخال الباسورد مره أخرى حينها تقوم بتشغيل البرنامج الأصلي وسيدخل المستخدم للبرنامج وهو لا يعلم أن باسورده قد سرق الآن.

النوع الثالث"Backdoor":

من حيث الخواص :

الانتشار الذاتي Self-Replicate : لا يوجد

قابلية التغيير Population growth :صفر Zero

التطفل Parasitic : محتمل possibly .

الـــ "Backdoor " هي أي وسيلة تمكننا من تجاوز الإجراءات الأمنية، وقد يقوم المبرمج بعمل "Backdoor " أحيانًا لتجاوز عمليات الفحص "password checking " والتي قد تأخذ زمنًا.

ال"Pseudo-code " التالي يبين لنا كيف يمكن للمبرمج أن يتجاوز الفحص والدخول مباشرة للنظام.

```
userName = getUserName() ;
password = getPassword() ;

//****** is this backdoor ******//
if ( userName == "Wajdy" )
    return ALLOW_LOGIN ;

// normal check from database
if ( checkUserPass(userName && password) )
    return ALLOW_LOGIN ;
else
    return DENY_LOGIN ;
```

الشكل 1-10 يبين الPseudo-Code للباكدور

هناك نوع من الباكدور وهو "Remote Administrator Tool " أو له الأسم الأخر "Remote Access Trojan " على حسب من يقوم باستعماله وفي أية غرض هذه البرامج RAT

تسمح للمستخدم الوصول البعيد لجهازه والتحكم به عن بعد .أيضا تسمح لفريق الدعم الفني اللازم .في حالة أصاب الجهاز أي نوع من الـــ "Malware " وقام بتنزيل RAT فسوف يعتبر هذا ألـــ RAT هو "Remote Access Trojan . "

النوع الرابع "Viruses":

من حيث الخواص :

الانتشار الذاتي Self-Replicate :نعم yes

قابلية التغيير Population growth : نعم positive.

التطفل Parasitic :نعمyes

الفيروس هو برنامج يقوم بنسخ نفسه في الملفات التنفيذية الأخرى، ويطلق على الملف الذي

نسخ الفيروس نفسه فيه ملف مصاب وعندما يعمل الملف المصاب يقوم مره "Infected ". وعندما يعمل الملف المصاب يقوم مرة أخرى بنسخ نفسه للملفات الأخرى وهكذا .وهذه الميزة "Self-Replicating" هي التي تميز الفيروس عن غيره من البرمجيات الضارة مثل الديدان Worms .

اللفظ فيروس Virus استخدم لأول مره في أحدى روايات الخيال العلمي وذلك في 1970 في رواية الرجل المجروح Scarred man لGregory Benford بنفورد. ولم تقتصر على ذلك ، فقد أستخدم مره أخرى بعد ذلك بسنتين في رواية لDavid Gerrold بعنوان When Harlie Was One وتحدثت الروايتين عن برنامج استخدم للقضاء على تلك الفيروس ولكن لم يتم ذكر أسم معين له .ولم يق تصر عمل جريجوري بنفورد على ذكر كلمة الفيروس في الرواية ، بل في عام 1969 قام بكتابة بضعة فيروسات– غير ضاره -في ما تسمى الآن ب " Lawrence Livermore National Laboratory " وكذلك في أول ظهور لـــ "ARPANET "

وكان أول فيروس يصيب الأجهزة العادية "Desktop Computer " Elk Cloner لريتش

أو فيروس "pervade " (لجون واكر) وهو أول فيروس بشكل عام

الفيروسات تقوم بنشر نفسها داخل الجهاز ، ويمكن أن تنتقل لجهاز أخر عن طريق وسيط نقل "Transported Media " مثل الأقراص الصلبة "Floppy Disk " أو الأقراص الممغنطة "CD/DVD ROM " أو الفلاش "USB/Flash Disk " ولا يقوم الفيروس بنقل نفسه عبر. الشبكة فهذه من مهام الديدان على أية حال الكلمة الشائعة" فيروس "كثيرا ما يقصد بها أي نوع من أنواع الـــ "Malware " يقوم بـــ "Self-Replicating " .

الفيروس بعد أن تصيب الجهاز يمكن أن نراها بأكثر من شكل، فالنسخة الأصلية من الفيروس يطلق عليها جرثومة Germ قبل أي عمليه (injection) والفيروس الذي لا يستطيع القيام بعملية النسخ (لوجود ثغره في الفيروس) أو أنه تعامل مع بيئة غير متوقعه يطلق عليه "Intended. " ويطلق علي الفيروس الموجود داخل النظام ولكنه لا يشكل ضررا للبيئة الحالية بـــ "Dormant " على سبيل المثال أغلب الفيروسات التي تصيب الملفات التنفيذية في نظام ويندوز WIN 32 في حال تم نقلها لنظام لينكس Linux أو أي نظام أخر غير عائله Win 32 فهي لن تعمل وستكون "Dormant " ولكنها بمجرد نقلها بواسطة المستخدم إلى نظام Win32 فلن تكون "Dormant " بعد ألان ....

النوع الخامس : الديدان "Worms" :

من حيث الخواص :

الانتشار الذاتي Self-Replicate :نعم yes

قابلية التغيير Population growth : نعم positive.

التطفل Parasitic : لا NO

تتشارك الديدان مع الفيروسات في الكثير من الخصائص وأهمها في أنها ذاتيه النسخ أو الانتشار "Self-Replicating " ولكن عملية النسخ في الديدان تختلف قليلا عن الفيروسات حيث أن الديدان هي برامج قائمه بذاتها "Standalone Application " ولا تحتاج للالتصاق في الملفات التنفيذية، إضافة إلى أنها تنشر نفسها من جهاز لأخر عبر الشبكة Network .

الظهور الأول للاسم الدودة " worm " ظهر أيضا في أحدى روايات الخيال العلمي "The Shockwave Rider " للمؤلف "John Brunner " في1975 (استخدم المؤلف أيضا " الفيروس في تلك الرواية) ومن التجارب الأولى في مجال الديدان هي " Creeper " حيث أستخدم في APRANETواستخدم الـ Reaper لإزالة الـــ " Creeper " كما ذكرنا من قبل

ومن الأحداث التاريخية في مجال الديدان في 1988 حيث قام طالب الـــ PHD روربت مورس (الابن) في جامعه كورنيل بعمل دودة وكان يريد أن تكون بطيئه الانتشار وغير مكتشفة حيث كان يريد– على حد قوله -أنه يريد قياس عمق الانترنت . ولكن لم تسر الأمور كما شاء روبرت مورس حيث انتشرت بسرعة رهيبة وعطلت الإنترنت بالكامل، وسميت تلك الدودة بـــ "Internet Worm " أو أحيانًا "Morris Worm " نسبه لصاحبها .قبض مورس أنذاك وحبس لمدة 3 سنوات على فعلته....

النوع السادس : Rabbit:

من حيث الخواص :

الانتشار الذاتي Self-Replicate :نعم yes

قابلية التغيير Population growth :صفر Zero

التطفل Parasitic : لا NO

يطلق الـــ "Rabbit " على أي برنامج يقوم بمهمة تتضاعف عددها بشكل سريع وأحيانًا تسمى "Bacteria. " وهناك نوعين من الـــ " Rabbit " الأول يقوم باستهلاك جميع مصادر الجهاز مثل الذاكرة والقرص الصلب ، أحد ألأمثله الشهيرة هو الـــ "Fork Bomb " وهو برنامج يقوم في حلقه لا نهائيه بإنشاء "Process " حتى يستهلك الذاكرة بشكل كامل .النوع الأخر من الـــ " Rabbit " يشبه الدودة ولكنه يحذف نفسه بعد عملية النسخ للجهاز التالي ، بهذا تكون هناك نسخه واحدة فقط على الشبكة من هذا الـــ " Rabbit " ويطلق عليه بـــ "Jumping Executable " لكن هذا النوع قليل الظهور.

النوع السابع : برامج التجسس Spyware:

من حيث الخواص:

الانتشار الذاتي Self-Replicate : لا NO

قابلية التغيير Population growth :صفر Zero

التطفل Parasitic : لا NO

هذه البرامج تقوم بجمع معلومات من الجهاز وتقوم بإرسالها لشخص أخر .أستخدم اللفظ "Spyware " لأول مره في 1995 في إحدى الطرف "Joke"ولكنه حاليا الاسم "Spyware " يشير لبرامج التجسس وهي من أحدى المخاطر "Threat "التي تشكل خطرا على الجهاز.

المعلومات التي تجلبها هذه البرامج تختلف من برنامج لأخر، فبعضها يهتم فقط بجلب كل مات المرور وأسماء المستخدمين "account & password " حيث يقوم بجلبها من أماكن تخزينها على الجهاز أو يقوم بتسجيلها عندما يكتبها المستخدم "Keylogger " يختلف الـــ "Keylogger " عن الـــ "Trojan Horse " في أنها تقوم فقط بمهمة تسجيل ما يكتبه المستخدم "keystroke " وليس لديه أي مهمة أخرى .بعض برامج الـــ " Spyware " يهتم بجلب وسرقة المعلومات البنكية أو سرقه مفاتيح تسجيل البرامج "Serial Key " وبعضها يقوم بسرقة عناوين البريد "Emails " ويقوم بإرسالها للـــ "Spammers".

قد نرى أن هناك فيروسات أو ديدان تقوم ببعض أو كل وظائف الـــ "Spyware " ولكنها لن تعتبر "Spyware " لأنها ليست "Self-Replicating " أخيرا يمكن أن تدخل الـــ "Spyware " للجهاز بعده طرق منها وقت تحميل البرامج من موقع مشكوك أو استغلال ثغرة في متصفح الويب وهنا سوف يدخل الـــ "Spyware " بمجرد زيارتك للموقع الذي يحتوي على Spyware.

النوع الثامن : "Adware" :

من حيث الخواص :

الانتشار الذاتي Self-Replicate : لا NO

قابلية التغيير Population growth :صفر Zero

التطفل Parasitic : لا NO

تشابه هذه البرامج الـــ "Spyware " من حيث جمع المعلومات ولكن هذه البرامج تجمع المعلومات لغرض التسويق ومعرفة المنتجات والمواقع التي يزورها المستخدم باستمرار .بعض هذه البرامج قد تزعج المستخدمين من خلال رسائل الـــ "Popup " تحتوي على إعلانات تسويقية

وبعضها أكثر شراسة يقوم بتحويل الصفحة الرئيسية للمستخدم "Home Page " الى الموقع التجاري .على أي حال الهدف منها ليس التجسس وسرقة المعلومات بل لأغراض تسويقية بحتة "Marketing Purpose . "

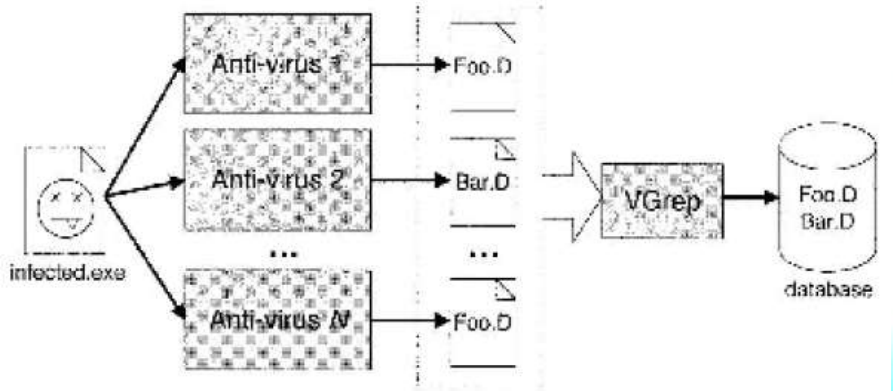
تسمية الفيروسات Naming of Viruses:

عندما تصيب أحد الـــ "Malware " الجديدة الأجهزة وتبدأ بالانتشار، تكون الأولوية لشركات ألأنتي فيروس هو إيجاد المضاد لهذا الفيروس، وموضوع التسمية يأتي في المرحلة الثانية مباشره .يتم اختيار اسم الفيروس من قبل محللي الفيروسات وباحثي ألأنتي فيروس، وعاده يتم اختيار الاسم من خلال وظيفة الفيروس، أو من خلال المخرج الذي يظهر أ و الذي يقوم بطباعته الفيروس (كما في فيروس Stoned حيث كان يخرج رسالة

Your Pc is now Stoned!

مبرمجي الفيروسات عندما لاحظوا ذلك بدءا بإدخال أسمائهم ووضع عبارات واضحة في الفيروس على أمل أن يتم تسمية الفيروس بهذا الاسم ، لكن بالمقابل تجاهل محللي الفيروسات ذلك لكي لا يكونوا لعبة في أيدي كاتبي الفيروسات.

لسوء الحظ لا توجد طريقة موحدة يتم فيها تسمية الفيروس، لذلك قد تجد فيروس واحد بعشرات الأسماء والألقاب، فلكل محلل وباحث طريقته في التحليل والتسمية .ألمشكله سوف تقع على كاهل المستخدم النهائي الذي يسمع الأخبار المتداولة بين الناس عن ظهور فيروس معين، ويبدأ بالشك في المضاد الذي يستخدم في حال لم يظهر الاسم الذي يتوقعه المستخدم وكان يستخدم أسم أخر. أوضح بعض الباحثين صعوبة وجود تسمية موحدة للفيروسات وحتى في المستقبل القريب، والسبب هو الانتشار السريع للفيروسات بشكل شبه يومي يجعل عملية انتظار الاسم الذي يجب أن يوافق عليه أغلب المحليين أمر بطئ، السبب الأخر وهو عدم وجود معيار معين في عملية التسمية حيث لا يتضح ما الذي يجب النظر إليه لكي يتم تسمية الفيروس ، ومن هنا سنجد أنه يمكن أن نسمى الفيروس بأسماء لا تنتهي كل اسم منها قد يكون نتيجة لوجهه نظر معينة.
هناك نصائح وإرشادات في عملية التسمية لكن لا يوجد من يتبع مثل هذه مقاييس ولكل شركه
أنتي فيروس طريقتها الخاصة في التسمي ة .لذلك الحل الأفضل هو عند ظهور فيروس محدد
القيام بأخذ جميع الأسماء من محللي الفيروس لهذه الفيروسات ومن ثم تخزينها كأسماء لهذا الفيروس
هناك أداة تقوم بشكل أوتوماتيكي بهذا العملية تسمى. "VGreb " قام بها Ian Whaley مبدأ عملها هو أخذ جميع الأسماء التي تخرجها برامج ألأنتي فيروس للفيروس المحدد وتقوم بتخزينها للبحث عنهم لاحقًا . الشكل التالي يبين طريقة عمل الـ "VGreb "



الشكل 1-11 يبين طريقة عمل أداه VGreb

الأسماء التالية هي للدودة الأخيرة "Conficker " ويظهر أن لكل مضاد أسم مختلف عن الأخر:

Common name: Conficker
Aliases:
***Win32/Conficker.A (CA)**
***W32.Downadup (Symantec)**
***W32/Downadup.A (F-Secure)**
***Conficker.A (Panda)**
***Net-Worm.Win32.Kido.bt (Kaspersky)**
***W32/Conficker.worm (McAfee)**
***Win32.Worm.Downadup.Gen (BitDefender)**
***Win32:Confi (avast!)**
***WORM_DOWNAD (Trend Micro)**
***Worm.Downadup (ClamAV)**

بشكل عام يمكن أن تكون التسمية بإتباع الأقسام التالية:
Malware Type: وهنا يتم تحديد نوع الـــ "Threat " مثلا دودة "Worm "
Platform Specifier: وهنا يتم تحديد البيئة التي يعمل عليها الفيروس ، مثلا Win32 أو w32 وهذا يعني أنها تحتاج لنظام تشغيل ويندوز 32 بت وبشكل أعم يمكن أن تكون الـــ "Platform Specifier " هي بيئة التنفيذ مثلا VBS لبرامج "Visual Basic Script "
Family Name: هنا يتم تحديد اسم مقروء وواضح لأسم الفيروس.

Variant: الكثير من الفيروسات الجديدة يتم فيها تعديل نسخة سابقة من فيروس قديم ، هذه الفيروسات تسمى "**Variant** " وعاده يتم إسناد حروف هجائية للإشارة للنسخة الجديدة (فمثلا الحرف C) للتفريق من ألنسخه السابقة (مثلا B) وفي حال انتهت الأحرف (وصلت الأحرف لـZ) يمكن البدء بـــ AA وهكذا.

Modifier: هنا يتم إعطاء معلومات إضافية عن الفيروس، مثلا طريقة الانتشار مثل MM وهي اختصار Mass Milling.

هناك مواقع تقدم خدمة اختبار الملف في العديد من البرامج المضادة للفيروسات ، فقط تقوم برفع الملف وتخرج النتيجة كما يبين الشكل التالي للموقع VirusTotal.com .

Antivirus	Version	Last Update	Result
a-squared	4.0.0.101	2009.05.15	Leapfrog.516!IK
AhnLab-V3	5.0.0.2	2009.05.15	Leapfrog.516
AntiVir	7.9.0.168	2009.05.15	Leapfrog
Antiy-AVL	2.0.3.1	2009.05.15	Virus/DOS.V
Authentium	5.1.2.4	2009.05.15	Leapfrog.516.A
Avast	4.8.1335.0	2009.05.15	UNSS-516
AVG	8.5.0.336	2009.05.15	LeapFrog
BitDefender	7.2	2009.05.15	Leapfrog.516.A
CAT-QuickHeal	10.00	2009.05.15	Leapfrog.516.A
ClamAV	0.94.1	2009.05.15	UNSN-516.B
Comodo	1157	2009.05.08	Virus.DOS.V.516.a
DrWeb	5.0.0.12182	2009.05.15	LeapFrog
eSafe	7.0.17.0	2009.05.14	DOS.V.516.a
eTrust-Vet	31.6.6507	2009.05.15	Leapfrog
F-Prot	4.4.4.56	2009.05.15	Leapfrog.516.A
F-Secure	8.0.14470.0	2009.05.15	Virus.DOS.V.516.a
Fortinet	3.117.0.0	2009.05.15	LeapFrog.516
GData	19	2009.05.15	Leapfrog.516.A
Ikarus	T3.1.1.49.0	2009.05.15	Leapfrog.516
K7AntiVirus	7.10.735	2009.05.14	Virus.DOS.USSR 516
Kaspersky	7.0.0.125	2009.05.15	Virus.DOS.V.516.a
McAfee	5616	2009.05.15	Leapfrog

الشكل 1-12 يبين نتيجة فحص فايروس من خلال الموقع VirusTotal.com

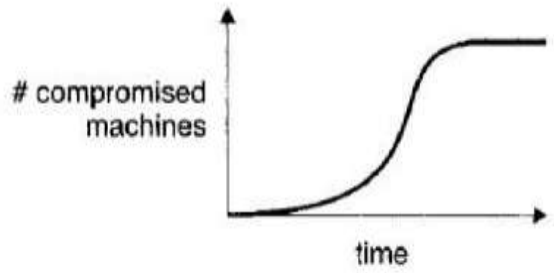
عدد المخاطر للبرمجيات الضارة The Number of Threats:

بالرغم من تزايد عدد الفيروسات في كل يوم إلا أنه لا يمكن تحديد نوعية هذه الـــ"**Threats** " أو تحديد عددها بالضبط، فقد تجد أن بعض البرامج المضادة للفيروسات تتعرف على عدد معين من الفيروسات يختلف من برنامج لأخر ومن شركه لأخرى .ذلك الاختلاف يرجع لعده عوامل منها حصول المضاد الأول على نوعية من الفيروسات لم يحصل عليها المضاد الأخر، أو قد تصنف أحدى المضادات برنامج ما على أنه فيروس "**Threat** " في حين يراه المضاد الأخر برنامج طبيعي. حتى طريقة حساب الفيروسات قد تختلف من مضاد لأخرى فمثلا الفيروسات التي تقوم بتوليدها برامج توليد الفيروسات بضغطه زر "**Virus Generated Tools** " هل يمكن اعتبارها فيروس واحد أم كل منها فيروس منفصل؟ حيث حدث في 1998 عندما تم توليد حوالي 15000 فيروس في ليلة وضحاها بواسطة أحد تلك البرامج.

اعتبار أخر وهو الفيروسات غير المعروفة وغير المنتشرة، وبشكل عام يجب أن تتعامل البرامج المضادة مع الفيروسات المعروفة وغير المعروفة، ولكن القبض على جميع الفيروسات المستقبلية أمر يستحيل القيام ب ه كما وضح فريد كوهين ذلك .أيضا الفيروسات التي لا تعمل إلا في ظل وجود نظام معين ، ففي حال لم تجد تلك البيئة فلن تعمل وتكون خامدة "**Dormant**" ولكن بمجرد نقلها ولو بطريق الخطأ إلى البيئة المخصصة لعمل الفيروس سوف يبدأ بالعمل، لذلك قد نجد مضاد يتعامل معها ومضاد أخري يتجاهلها باعتبار أنها ملفات غير مضره للنظام الحالي.

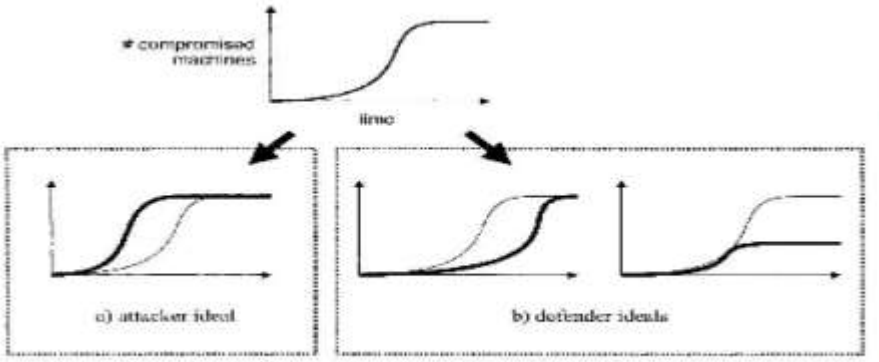
سرعة انتشار الفيروسات Speed of Propagation:

سرعة انتشار الـ "**Malware** " قد يختلف باختلاف طريقة التصميم أو الطريقة التي ينتشر بها، وبتخصيص الحديث حول الديدان"**Worms** " نجد أن السرعة القصوى-بشكل نظري -لانتشار دودة قوية تكون ما بين510 ميلي ثانية –عند استخدام " **UDP** " إلى 1.3 ثانية– عند استخدام" **TCP**" لإصابة جميع الأجهزة والتي تحتوي على الثغرة التي تستغلها الدودة. الشكل التالي"" **Worm propagation curve**"" يبين المنحنى العام لكيفية انتشار دودة مع تقدم الزمن وازدياد عدد الأجهزة المصابة.



الشكل 1- 7 يبين المنحنى لكيفية انتشار الدودة مع الزمن

صاحب الدودة "Worm Author" سوف يريد أن تنتشر الدودة بأسرع وقت ممكن ، وبالتالي من جهته يكون شكل فإن منحنى الوقت يرجع قليلا لجهة اليسار، أما صاحب المضاد "Defender" سوف يريد أن تبطئ سرعة الانتشار حتى يقوم بوضع المضاد اللازم " Fix " أو أن يكون معدل انتشار الدودة صغير جدا.



الشكل 1- 8 يبين المنحى من وجهه نظر المخترق والمدافع

مقدمة في الفيروسات وتقنياتها :

مقدمة في الفيروسات وتقنياتها :

تتكون الفيروسات من ثلاث خصائص:

1 - طريقة الإصابة :Infection Mechanism: وهذا الجزء متعلق بكيفية انتشار الفيروس وكيف يعدل البرامج الأخرى للالتصاق بها يطلق على هذه الطريقة أحيانا "Infection Vector " هذا لا يعني أن هناك طريقة واحدة للإصابة فهناك فيروسات مصممة لكي تصيب بأكثر من طريقة يطلق عليها الفيروسات متعددة الأهداف "Multipartite"

2 - الـTrigger: وهذا الجزء هو الذي يحدد متى تبدأ عمليه الإصابة أو بدء وظيفة الفيروس "Payload." "

3 - الـ "Payload " وهو الذي يحدد وظيفة الفيروس وما الذي يفعله سواء طباعة رسالة طريفة إلى إصابة جميع الملفات في الجهاز .يمكن أن يكون الضرر أحيانًا بالمصادفة –غير مقصود -وذلك لوجود خطأ في الفيروس Bug أو تعامله مع بيئة تختلف عن البيئة التي يتوقع أن يعمل الفيروس فيها، أو أحيانًا بسبب وجود فيروس سابق بالجهاز يقوم بالتضارب مع الفيروس الجديد.

الخاصية الأولى– طريقة الإصابة -تعتبر الأهم بالنسبة للفيروس وحتى في حال غياب الـــTrigger اوالـــ Payload فإن طريقة الإصابة هي أهم ما يميز الفيروس عن غيره من البرمجيات الضارة فمثلا في غيابها قد يعتبر الفيروس Logic Bomb وليس فيروس..

```
void Virus () {
    infect() ;  // call to infect function

    if ( Trigger() == true )
        PayLoad() ; // call to payload when Trigger accure
}
```

الشكل 2-1 يقدم Pseudo-code لوصف آلية عمل الفايروس .

طريقة الإصابة تكون عن طريق اختيار أي من الـــ "Target Code " ثم يتم أصابته .تبدأ المشاكل في حال تم اختيار ملف مصاب مسبقًا بنفس الفيروس لأن عملية الإصابة مره أخرى سوف يستغرق زمنًا لا يفيد بشي ء .حل هذه المشكلة هو عن طريق أن يختبر الفيروس الملف هل هو مصاب مسبقًا بهذا الفيروس أم لا، فإذا كان مصاب فيتجاهل الإصابة ويكمل عملية البحث عن الملفات الأخرى .بوجود مثل هذا الاختبار عن وجود الفيروس في الفيروس نفسه يستطيع مبرمج ألأنتي فيروس بأن يبحث عن الفيروس بنفس الطريقة التي يستخدمها الفيروس لكي يتم الكشف عن وجوده .لذلك من جهة المخترق أو صاحب الفيروس يجب التحايل بطريقة أو أخرى.

```
void Infect () {
    do {
        target = SelectTarget();

        if ( isInfect ( target ) )
            continue ;
        else
            Infect_Code(target) ;

    } while ( N Time) ;
}
```

الشكل 2-2 يبين كود Pseudo-Code لطريقة الإصابة

أقسام الفيروسات Virus Classification :

تقسم الفيروسات للعديد من الأقسام، الفقرة التالية سوف تتناول طريقة التقسيم بالاعتماد على :

1 - حسب نوع الملفات التي يصيبها الفيروس

2 - على حسب الطريقة التي يستخدمها الفيروس للاختفاء عن برامج ألأنتي فيروس.

Classification by Target:

الفيروسات التي تصيب قطاع الإقلاع Boot Sector Infector:

عند تشغيل الحاسب يقوم الجهاز بعدة خطوات لك ي يبدأ العمل، أولا يقوم المعالج بتنفيذ الأوامر الموجودة في الـــ "ROM " حيث يقوم بعمل اختبار لجميع المكونات " Self-Testing " وبعدها يقوم بالبحث عن جهاز الإقلاع لكي يقوم بالإقلاع منه .بعد أن يجد ذلك الجهاز "Boot Device " يقوم بالقراءة من قطاع الإقلاع"Boot Block " وتحميلها إلى الذاكرة حتى يقوم بتنفيذ تلك الأوامر (هذا يعرف بقطاع الإقلاع الأول Primary Boot Block) تلك الأوامر التي سوف يبدأ الحاسب بتنفيذها تقوم هي الأخرى بتحميل برامج لكي تتعرف على نظام ملفات الجهاز الذي تم الإقلاع منه ومن ثم ينتقل التنفيذ إلى ذلك الكود (هذا يعرف بـــ Secondary Boot) وفي مرحلة الإقلاع الثانية يقوم بتحميل وتشغيل نواة النظام ومن ثم يبدأ النظام بالعمل.

الفيروسات التي تصيب قطاع الإقلاع Boot Sector Infector (واختصاراًBSI) تصيب بطريقتين ، الأول أن تقوم بإصابة الجهاز عن طريق نسخ نفسها إلى ذلك القطاع.والثانية وهي أن تقوم بتحويل كود قطاع الإقلاع لمنطقة أخرى على القرص وتقوم بنسخ نفسها إلى تلك المنطقة. وعندما تنتهي من عملها وقت الإقلاع تقوم بتنفيذ كود تحميل النظام.

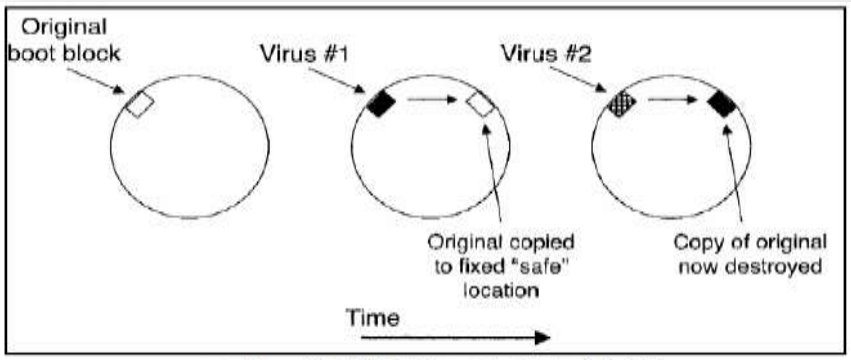
الطريقة الأولى

في الإصابة طريقة صعبة ومعقدة لأن ذلك يتطلب كتابة برنامج متكامل للإقلاع، حيث ي جب أن يقوم صاحب الفيروس بإزالة كود تحميل ملفات الإقلاع بالكامل ووضع الفيروس الذي يجب أن يقوم بهذه المهمة بالضبط كما هي والا لن يعمل الفيروس. لذلك تتطلب هذه الطريقة الكثير من الكود بالإضافة إلى عدم ضمان عملها على جميع الأجهزة، حيث هي لا تعمل مع جميع الأقراص فلكل قرص طريقته في الإقلاع. ا

الطريقة الثانية

وهي الأفضل، حيث يتم نسخ كود تحميل ملفات الإقلاع إلى مكان جديد على القرص الصلب، ويتم وضع الفيروس في المكان الأصلي ويتم وضع إشارة في الأخير إلى موقع كود التحميل الأصلي لكي تكمل عملية الإقلاع ولكن بعد أن يكون الفيروس محملا في الذاكرة.

لكن هذه الطريقة قد لا تخلو من المشاكل هي الأخرى حيث يمكن أن يتعطل الجهاز بسببها بشكل غير مقصود، وذلك حينما يصيب فيروس "BSI " جهاز مصاب بفيروس "BSI " أخر ويقوم بنقل الكود الموجود في قطاع الإقلاع (كود الفيروس القديم) ونسخه لموقع أخر المشكلة سوف تكون في حال تم وضع الكود القديم (كود الفيروس القديم) في نفس المكان الذي قام الفيروس القديم بنقل كود تحميل ملفات النظام الأصلي، وبالتالي ستضيع كود التحميل ولن يقلع الجهاز بتاتًا.



الشكل 2-3 يبين عندما يصيب قطاع الإقلاع أكثر من فايروس

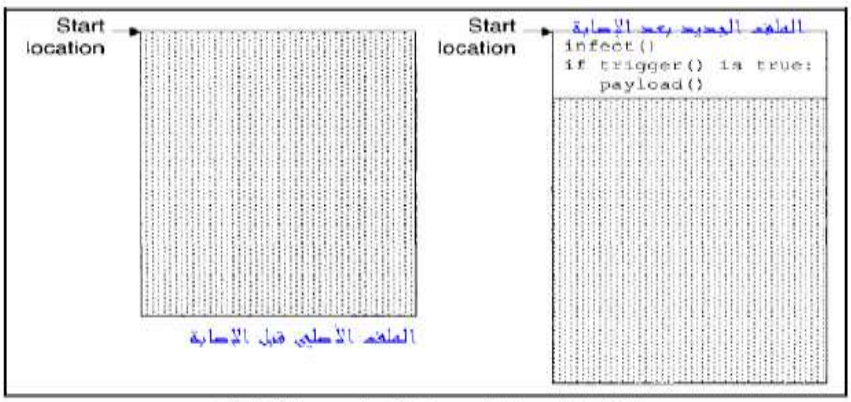
على أية حال ، فيروسات الـــ "BSI" لم تعد فعالة كما في السابق ، والسبب أن أغلب أنظمه التشغيل تمنع من الكتابة المباشرة في قطاع الإقلاع من غير توفر صلاحيات لازمة .أيضا يمكن حماية قطاع الإقلاع من خلال الإعدادات في لوحة الـــ "BIOS"

الفيروس التي تصيب الملفات File Infector:

ويقصد بها الفيروسات التي تصيب الملفات التنفيذية والتي تعمل مباشرة بالضغط عليها "Double-Click" أو من خلال سطر الأوامر "Command Line" وهناك نقطتان مهمتان في موضوع إصابة الملفات ، الأولى هي أن يمكن أن يضع الفيروس نفسه في الملف، والثانية هي كيف يمكن أن يعمل الفيروس "get-control" عندما يبدأ الملف المصاب بالعمل.
قبل الحديث عن النقطة الأولى نجد أن في فيروسات الـ"BSI" كانت مسألة أين يضع الفيروس نفسه مسألة بسيطة، حيث يقوم الفيروس بنسخ نفسه لقطاع الإقلاع ثم يبدأ بالعمل عندما تصل مرحله ال "BOOT" إلى القراءة من القطاع المصاب . أما بالنسبة لإصابة الملفات فذلك يكون عن طريق أما وضع الفيروس نفسه في بداية الملف أو في نهاية الملف ، كما سيتبين الآن.

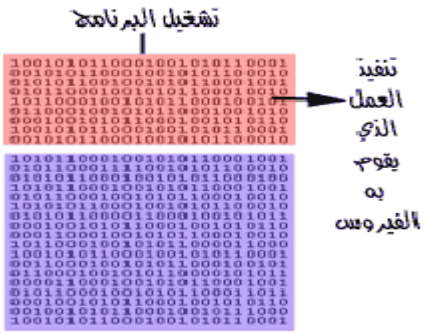
بداية الملف *Beginning of File*:

قديمًا كانت ملفات الـــ "COM" من أبسط الملفات التنفيذية وأصغرها حجمًا أيضًا، حيث يتم تحميلها إلى الذاكرة ويبدأ المعالج بالتنفيذ بدءًا من التعليمة الأولى في أول الملف "COM"
ولكي تتم إصابة هذا النوع من الملفات يتم وضع الفيروس في بداية الملف قبل الكود الأصلي، وهذا يتطلب عملية نسخ الأكواد القديمة في الملف إلى مواقع جديدة. الشكل التالي يبين كيفية الإصابة بهذه الطريقة بالرغم من أنها ليست بالصعوبة من ناحية التطبيق خصوصا أيام ملفات "COM" الآن أنها لا تعتبر من أسهل طرق الإصابة .ويطلق على الفيروس التي تصيب بهذه الطريقة بالاسم "Prepending Viruses"



الشكل 2-4 يبين الفايروسات التي تصيب بداية الملف

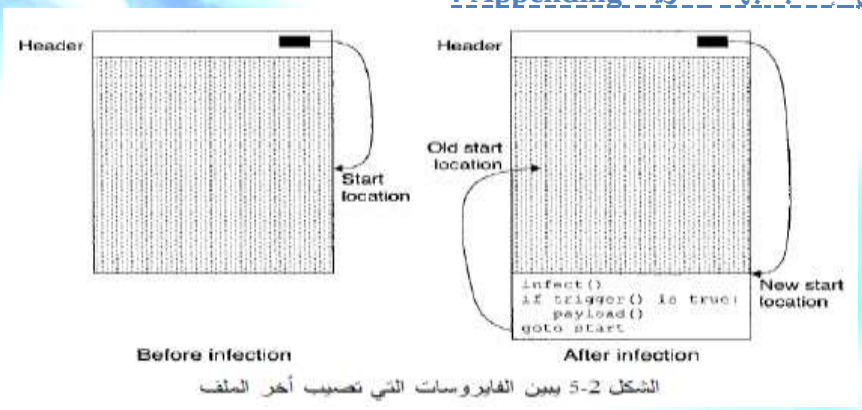
صورة أخرى للتوضيح



نهاية الملف *End of File*:

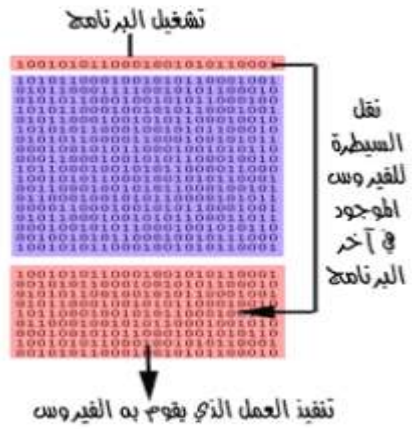
طريقة الإصابة هذه تعتبر من أسهل طرق الإصابة على الإطلاق حيث تقوم بنقل الفيروس إلى أخر الملف، وهذا ما يعرف بـــ " Appending Virus "
لكن كيف يبدأ الفيروس بالعمل فور تشغيل الفيروس وهو في أخر الملف؟ الحل هو بأن الملفات التنفيذية تحدد موقع التعليمة الأولى من البرنامج وذلك في ملف الرأس "Header " للملف التنفيذي، ومن هنا يقوم الفيروس بتعديل ذلك العنوان إلى عنوان مكان الفيروس في أخر الملف، وعندما ينتهي من العمل يقوم الفيروس بالقفز إلى العنوان الأصلي لبدء التنفيذ.

الشكل التالي يوضح الإصابة بهذه الطريقة Appending :



الشكل 2-5 يبين الفايروسات التي تصيب أخر الملف

صورة أخرى للتوضيح



الكتابة فوق الملف *Overwrite into File*:

فيروسات الكتابة " Overwrite " تقوم بمسح جزء معين من الملف وتقوم بوضع الفيروس في ذلك المكان ، وهكذا سيتم تجنب زيادة الحجم الواضح الذي يكون عند استخدام طريقتي الإصابة Prependingأو Appending ويتم وضع

الفيروس في مكان ما يمكن الوصول إليه فيما بعد .وعملية ألكتابه في جميع أجزا ء الملف "overwrite all content" بالتأكيد ستحذف محتويات الملف الأصلي وبالتالي يجعل كشف الفيروس أسهل وأسرع، لحل ذلك توجد عده حلول كل منها تختلف من حيث صعوبة التطبيق والمخاطر المحتملة.

الحل الأول هو أن يقوم الفيروس بالبحث عن الأجزاء المتكررة في الكود تكون في جزء "Data Section " ويقوم بكتابة نفسه مكانها ، وبالتالي عند بدء العمل سوف يبدأ الفيروس بالعمل "get control " ويمكن للفيروس أن يسترجع تلك المعلومات المتكررة عندما ينتهي من العمل .

الحل الثاني هو أن يقوم الفيروس بكتابة نفسه في أي موقع في الملف ويقوم بنخرين تلك البيانات التي سيتم الكتابة فوقها في مكان أخر مثل طريقة عمل الـــ "BSI " وقت ما ينتهي الفيروس من العمل..

الحل الثالث هو أن يقوم الفيروس بضغط جزء من الكود لكي تكون هناك مساحة لوضع نسخه من الفيروس ويتم فك ضغط الكود المضغوط عندما ينتهي الفيروس من العمل على أية حال يجب أن تكون هناك مساحة للفيروس ولكود فك الضغط أيضًا.

وفي كل الحالات أعلاه ، لن نجد طريقة يمكن أن توفر لنا كميه كبيره من المساحة لذلك فيروسات الـــ "Overwriting " يجب أن تكون صغيره جدا.

بدون إصابة الملف *Not in File*:

الفيروسات الـــ "Companion " تقوم بتشغيل نفسها قبل أن يعمل الملف وبدون أي تغيير على الملف، وذلك من خلال الاستفادة من الأسبقية في تنفيذ الملفات في نظم التشغيل حيث يقوم النظام– على سبيل المثال "MS-DOS- " عند سؤاله عن البحث عن الملف "file " بالبحث عن الملف "file.COM " فإذا لم يجده بدأ البحث عن الملف file.BAT ثم file.BAT وهكذا فإذا كان قصد المستخدم أن الملف file هو "file.EXE " فإن الفيروس يمكن أن يكون بالاسم "file.COM " وبالتالي يعمل قبل أن يعمل الملف "file.EXE " لأنه له أولوية أعلى.

بعض الفيروسات من هذا النوع تقوم بتغيير اسم الملف الأصلي، ويأخذ الفيروس اسم ذلك الملف .طريقة أخرى للإصابة وهي تغيير البرنامج المسئول عن فتح نوع معين من الملفات مثلا في نظام التشغيل ويندوز نجد أن هناك قيمه في مسجل النظام "Registry " تحدد البرنامج الذي يشغل الامتداد المعين ، فإذا تم تغيير تلك ألقيمه إلى الفيروس مباشرة، فهذا يعني أنه يتم إصابة جميع الملفات التي لها ذلك الامتداد.

الفيروسات الـــ "Companion " ممكن أن تكون في بيئة "Gul " حيث يتم استخدام أيقونه البرنامج العادي ووضعها في الفيروس وبالتالي يفكر المستخدم بأن هذا هو البرنامج الصحيح ويقوم بتشغيل ه .وبالتالي فيروسات الـــ "Companion " خطيرة ، فهي تحمل كل صفات الفيروس ما عدا أنها لا تلتصق بملف معين وبالتالي يجعلها غير مكتشفه بالنسبة للمستخدم.

Classification by Concealment:

الطريقة الثانية لتصنيف الفيروسات وهي عن طريق تقنيات الإخفاء التي تستخدمها الفيروسات لكي تخفى نفسها عن المستخدمين وعن برامج ألأنتي فيروس، سوف نتناول الطرق التالية:

No concealment, Encryption, Stealth, Oligomorphism, Polymorphism, Metamorphism, Strong Encryption

وسوف نشرح كل منهم تفصيليا بإذن الله في هذا البحث المتواضع

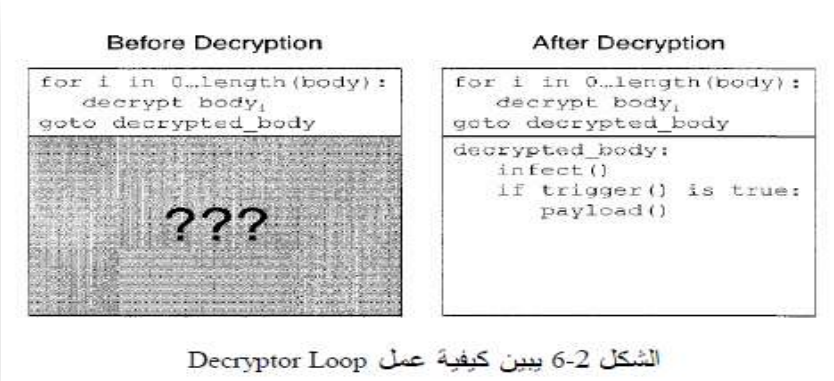
بدون إخفاء *No Concealment*:

أحد أسهل أنوع الفيروسات للتطبيق وهي التي لا تستخدم أي طرق للاختفاء على الإطلاق،وبالمقابل اكتشاف عمل هذه الفيروسات يعتبر الأسهل على الإطلاق.

التشفير *Encryption*:

يمكن استخدام التشفير في الفيروسات وذلك لإخفاء جسم الفيروس "Virus Body " (طريقة الإصابة والـــ"trigger " والـــ "payload ") وجعله أصعب للاكتشاف .وعندما يكون جسم الفيروس مشفر فهو يحتاج لفك التشفير حتى يعمل، بالتالي يجب أن يكون هناك جزء مسئول عن فك تشفير جسم الفيروس ويطلق عليه حلقه الفك "Decryptor Loop " ومهمتها هي فك تشفير جسم الفيروس ثم الانتقال إلى ذلك الجسم لبدء التنفيذ.

الشكل التالي بين "Pseudo-Code " للفيروس المشفر ويوضح ه ذا الكود كيف تعمل الـــ"Decryptor Loop " لفك الفيروس المشفر، ويضع الناتج من فك التشفير في مكان الجسم المشفر "In Place Decryption. "



الشكل 2-6 يبين كيفية عمل Decryptor Loop

سوف نستعرض الآن الطرق التي يمكن أن يستخدمها الفيروس في التشفير ، وهي:

Simple Encryption, Static Encryption Key, Variable Encryption Key,
Substitution Cipher, Strong Encryption

التشفير البسيط Simple Encryption:

وهنا سوف يتم التشفير بدون استخدام مفتاح وذلك بالاعتماد على عمليات الجمع والطرح أو عمليات تدوير البتات "Bitwise Rotations" أو معامل النفي " Not Operator "

التشفير	الفك
inc variable	dec variable
rol variable	ror variable
neg variable	neg variable

الشكل 2-7 يبين طرق التشفير البسيط

التشفير باستخدام مفتاح ثابت Static Encryption Key:

وهنا سوف يتم استخدام مفتاح ثابت لا يتغير أبدًا من إصابة لأخرى، ويتم ذلك باستخدام العمليات التي بها مقابل "مقابل" inverse " وهذا النوع شائع في الكثير من الفيروسات التي تستخدم نوع بسيط من التشفير.

التشفير	الفك
variable + 123	variable - 123
variable xor 30	variable xor 30

الشكل 2-8 يبين طرق التشفير بمفتاح ثابت

التشفير باستخدام مفتاح متغير Variable Encryption Key:

وهنا سوف يتم اختيار متغير يتغير في كل مره يتم فيها فك جزء من جسم الفيروس.

```
key = 123 ;

for (i=0 ; i<length(VirusBody) ; i++) {
    VirusBody[i] = VirusBody[i] xor key ;
    key = key + VirusBody[i] ;
}
```

الشكل 2-9 يبين التشفير بمفتاح متغير

التشفير باستخدام طرق الإحلال "Substitution Cipher" يمكن استخدام أي طريقة من طرق التشفير بالإحلال ، مثلا يمكن اختيار جدول " Lookup Table" من خلاله يتم إدخال النص الأصلي للحصول على النص المشفر ، والعكس أيضا فيمكن أن ندخل النص المشفر لكي نحصل على النص الأصلي.

```
// Encryption
VirusBody[i]=encrypt(VirusBody[i]) ;

// Decryption
VirusBody[i]=decrypt(VirusBody[i]) ;
```

الشكل 2-10 يبين التشفير بطرق الإحلال

هذا النوع من التشفير يعتبر one-to-one mapping ويمكن استخدام نوع one-to-many مثل استخدام الـــ " Homophonic Substitution Cipher".

التشفير باستخدام الشفرات الحديثة Strong Encryption:

قديما كان استخدام الشفرات الحديثة لتشفير جسم الفيروس يجعل حجم الفيروس كبير وبالتالي قد يشك به المستخدم لذلك لم تكن هناك فيروسات تستخدم مثل هذا النوع من الشفرات .أما الآن فأغلب أنظمة التشغيل تحتوي على مكتبات للتشفير يمكن أن يقوم باستخدامها مباشره بدلا من كتابة الشفرة بالكامل داخل الفيروس. الفيروسات التي تستخدم التشفير كوسيلة للاختفاء تحتوي على ضعف واضح وهو أن جسم الفيروس المشفر يكون كما هو من إصابة لأخرى، هذا الجزء الثابت يجعل الفيروس سهل القبض كما لو أنه لم يستخدم أي وسيلة للاختفاء. يمكن تجاوز العيب السابق وذلك باستخدام مفتاح للتشفير يتم توليده عشوائيا في كل مرة يتم فيها الإصابة ويجب ضمان أن جزء فك التشفير يحتوي على المفتاح الصحيح والذي تم توليده في المرة السابقة.

تقنيات التسلل *Stealth*:

الفيروسات التي تستخدم هذه الطرق تحاول أن تخفى الإصابة من نفسها، بحيث لا يشعر المستخدم أنه أصيب بأحد الفيروسات، من هذه الطرق التي تستخدمها الفيروسات للإخفاء: يقوم الفيروس بعد إصابة أحد الملفات بإرجاع تاريخ التعديل الذي يتم تغيير مباشره وقت الإصابة إلى الوقت الأصلي ما قبل الإصابة، وبالتالي يبدوا أن الملف لم يحدث له أي تغيير.

يمكن أن يقوم الفيروس قبل إصابة الملف بحفظ كل المعلومات التي تتعلق بالملف مثل الـ "Timestamp " وحجم الملف "Size" ومحتويات الملف، وعندما تجري أي عملية I/O على الملف يقوم الفيروس بمقاطعة هذه العملية وإرجاع

المعلومات الأصلية للملف وبالتالي يظهر الملف كما هو بدون تغيير .الطريقة التي يستخدمها الفيروس لمقاطعة الـــI/O تعتمد على نظام التشغيل نفس ه .مثلا في نظام "MS-DOS " طلبات القراءة والكتابة تكون على شكل مقاطعات تؤشر لمناطق معينة موجود في الذاكرة "Interrupt Vector " وبالتالي يحتاج الفيروس أن يعدل هذه الـــ "Interrupt Vector " لكي يكون جزء من تنفيذ المقاطعة وبالتالي يمكن أن يقطع عملية القراءة الكتابة لتنفيذ ما يريد.
نوع أخر وهو الـــ "Reverse Stealth "والذي يجعل كل الملفات كأنها مصابة والإصابة تتم من قبل برامج الإنتي فيروس والتي تحاول أن تصلح تلك الملفات ولكن بشكل خاطئ .أخيرًا تستخدم تقنيات الـ "Stealth " من قبل الـــ "Rootkit " وهي برامج يضعها المخترقين على الأجهزة المخترقة وتستخدم الـ "Stealth " حتى يصعب تعقب المخترقين واكتشاف الاختراق حتى بعض البرمجيات الضارة بدأت تستخدم الـــ"Rootkit " على سبيل المثال الـــ "Trojan Horse" المسمى بـــ "Ryknos " يستخدم الـــ"Rootkit " مصمم من الأساس لحفظ الحقوق " Digital Right."

الفيروسات الـــ*Oligomorphism* :

يستخدم هذا النوع من الفيروسات مجموعة من حلقات فك التشفير "Decryptor Loop " ويقوم الفيروس باختيار دالة واحدة من هذه الدوال في كل مرة إصابة .على سبيل المثال الفيروس "Whale " استخدام 30 حلقة فك تشفير مختلفة والفيروس "Memorial " أستخدم 96 حلقة فك تشفير.
من ناحية القبض على تلك الفيروسات فإن استخدام الـــ "Oligomorphism " يجعل الفيروس أصعب للقبض حيث على البرنامج المضاد أن يبحث عن أي وجود لحلقات فك التشفير في الفيروس .ويطلق على هذا النوع أحيانا "Semi-Polymorphism "

الفيروسات الـــ " *Polymorphism* "

الفيروسات الـــ "Polymorphism " تشابه الفيروسات الـــ "Oligomorphism " حيث كلاهما يستخدمان حلقة فك تشفير جديدة في كل مرة إصابة، ولكن الاختلاف في أن فيروسات الـ "Polymorphism " هو في أنها تحتوي على عدد لا نهائي من حلقات فك التشفير .!على سبيل المثال الفيروس "Termor" أستخدم حوالي 6 بليون حلقة فك تشفير !
وبشكل واضح جدا لا يمكن القبض على هذه الفيروسات من خلال البحث على حلقات الفك لأنها غير منتهية.
فإذن هذا النوع الصعب من الفيروسات قد وضعنا أمام قضيتان مهتمان في هذا النوع من الفيروسات ،
الأولى هو كيف يمكن للفيروس أن يعرف هذا الملف مصاب أم لا،؟
والثانية هو كيف يمكن للفيروس أن يغير حلقة فك التشفير من إصابة لأخرى؟؟
نقوم الآن بالحديث عن كل منهم بشيء من التفصيل.

القضية الأولى : كيف يمكن للفيروس أن يعرف هل الملف مصاب أم لا

بما أن للفيروس عدد غير معروف من دوال فك التشفير بالتالي لا يمكن أن يعرف الفيروس هل الملف مصاب أم لا من خلال البحث عن كود حلقة فك التشفير، إذا يجب أن يبحث الفيروس عن (شيء أخر يكون بعيد غير متعلق بالكود.)

File Stamping:

عن طريق تغيير الـــ "File Stamping " في الملف المصاب بحيث يكون مجموع الزمن والتاريخ يساوي عدد ثابت K في كل الإصابات ، وبالتالي عندما يرى الفيروس هذا العدد K يعرف أنه ملف مصاب مسبقًا .بعض البرامج تعرض أخير رقمين للسنة عند عرض معلومات الملف وتتجاهل عرض التاريخ بالكامل، يمكن أن يغير الفيروس السنة ويزيد 100 عام ولن يكون هناك أي تغيير ملحوظ.

File Size:

الملفات المصابة يمكن أن يجعلها الفيروس بحجم واحد ، أو يجعلها من مضاعفات عدد معين مثل 1234 ويقوم بالحشو في الملف متى تطلب ذلك.

Data Hiding:

في بعض بنى الملفات التنفيذية كـــ "ELF " (المستخدمة في أنظمة Unix/Linux) نجد أن النظام لا يستخدم جميع المعلومات المتعلقة بالملف، بالتالي يمكن أن يضع الفيروس اشاره "Flag " تبين وجوده في أحد المناطق غير المستخدمة .

على سبيل المثال الفيروس "Zperm " يبحث عن الحرف "Z " في الخانة "Minor Linker Version " في بنية الملف التنفيذي في ويندوز.

File System Feature:

بعض أنظمه الملفات يمكن أن تستخدم خصائص أضافية لا يمكن عرضها بالطرق العادية وبالتالي يمكن أن يستخدمها الفيروس لكي يضع إشارة تدل على أن الملف مصاب .مثل الـــ "Alternate Data Stream " والذي يستخدم في أنظمه الملفات NTFS لإضافة "Flags" (ملفات أخرى) للملف وهذه الإشارات لا يمكن عرضها بالطرق العادية سواء من نافذة الويندوز "explorer " أو من خلال أمر العرض العادي "Dir "

External Storage:

يمكن أن يضع الفيروس اشاره على أن الملف مصاب في موقع أخر بخلاف الملف نفسه، مثلا أن يقوم الفيروس بحساب الـــ "Checksum " للاسم الملف ويخزن الناتج في مفتاح بمسجل النظام "Registry " وعندما يريد إصابة ملف ما يقوم بأخذ الهاش ويبدأ بالبحث عن وجود هاش مشابه لكي يعرف هل الملف مصاب مسبقًا أم لا.

جميع هذه الطرق قد لا تعمل بشكل كامل وقد يحصل "False Positive " ويقوم الفيروس بعدم إصابة ملف غير مصاب من الأساس، لذلك كانت هناك بعضا من النصائح حول تغيير الإعدادات للملف حتى يجعل الملف كأنه مصاب وبالتالي لن يصيب ذلك الفيروس المعين الجهاز، لكن لسوء الحظ هناك الآلاف من الفيروسات ولن تنفع هذه الطريقة مع جميع الفيروسات .الطرق السابقة يمكن أن تستخدم الفيروسات العادية أيضا لكي تكشف هل قامت بإصابة الملف أم لا ، وتوجد طرق أسهل تستخدمها الفيروسات الضعيفة وهي بفحص عده بايتات في البداية لكي يتأكد من وجود الإصابة.

القضية الثانية كيف يقوم الفيروس بتغيير حلقة فك التشفير من إصابة لأخرى "Changing :Decryptor Loop " ::

الكود الموجود داخل الفيروس الـــ "Polymorphism " يتغير في كل مره إصابة جديدة بواسطة الـــ "Mutation Engine " هذا المحرك يأخذ مجموعه من الأكواد كمدخل ويخرج مجموعة أخرى من الأكواد لها نفس الوظيفة ولكن بشكل أخر أو بتعليمات أخر ى .نستعرض الآن بعضًا من الطرق التي يستخدمها الـــ"Mutation Engine " لكي يقوم بعملية التحويل:

1 - التبديل بواسطة تعليمات مشابهه Instruction Equivalence:

في أغلب معماريات الحواسيب نجد أن هناك الكثير من التعليمات تكون لها نفس الوظيفة ، في المعمارية "CISC " على سبيل المثال (مثل معالجات أنتل Intel x86) نجد أن التعليمات التالية جميعها لها نفس التأثير حيث تضع ألقيمه 0في المسجل R1

```
; all this instruction put
; 0 in r1 Register

clear   r1
xor     r1,r1
and     r1,0
mov     r1,0
```

الشكل 2-11 يبين عدة تعليمات لنفس الوظيفة

2 - التبديل بواسطة مجموعة من التعليمات Instruction Sequence Equivalence:

يمكن أن تبدل تعليمة واحدة بمجموعه من التعليمات المكافئة لها المثال التالي يبين ذلك :

```
// one method to put
// 1 in x
x =1 ;

// other Method
y = 21 ;
x = y - 20 ;
```

الشكل 2-12 يبين عملية التبديل بواسطة عده تعليمات مكافئة

3 - تبديل مواقع الكلمات Instruction Reordering :

يمكن تبديل ترتيب العمليات بدون اختلاف النتيجة النهائية ، المثال التالي يوضح أن المتغير r4 يعتمد على r2 و r1 وكل من هذين المتغيرين لا يعتمدوا على أي متغير أخر لذا يمكن تبديل مواقعهم، غير ذلك يمكن الاستفادة من الخوارزميات المستخدمة في تحسين المترجمات "Optimization Compilers. "

```
// Instruction Reordering
r1 = 12 ;
r2 = r3 + r2 ;
r4 = r1 + r2 ;

// after reordering
r2 = r3 + r2 ;
r1 = 12 ;
r4 = r1 + r2 ;
```

الشكل 2-13 يبين التبديل باعاده ترتيب مواقع التعليمات

4 - تغيير المتغيرات والمسجلات Register Renaming:

يتم هنا تغيير أسماء المتغيرات أو المسجلات ، وقد لا يكون هناك أثر عند قرائه الكود عند تغيير أسماء المتغيرات بالنسبة للمبرمج ولكنه بالتأكيد يجعل المسألة أصعب بالنسبة لبرامج المكافحة والتي تبحث عن تعليمات معينة .المثال التالي يوضح ذلك:

```
// Variable renaming
r1 = 12 ;
r2 = 34 ;
r3 = r1 + r2 ;

// after renaming
r3 = 12 ;
r1 = 34 ;
r2 = r3 + r1 ;
```

الشكل 2-14 يبين التبديل بتغيرات المسجلات و المتغيرات

5 - ترتيب البيانات Data reordering :

وهنا يتم تغيير مواقع البيانات في الذاكرة ويكون له نفس تأثير تغيير أسماء المسجلات والمتغيرات حيث تغير طريقة الوصول لهذه البيانات.

6 - جعل الكود أكثر تداخلا Making Spaghetti :

بالرغم من أن بعض المبرمجين يكتبوا برامج "Spaghetti" بالفطرة إلا أن الكثير من المبرمجين ليس كذلك . المثال التالي يوضح كيف يمكن تعقيد عملية جمع متغيرين مع بعضها البعض.

```
// simple code
r1 = 12 ;
r2 = 34 ;
r3 = r1 + r2 ;

//after making spaghetti
L1:
     r2 = 34 ;
     goto L2

Start:
     r1 = 12 ;
     goto L1

L2:
     r3 = r1 + r2 ;
```

الشكل 2-15 يبين عمل تداخل للأكواد

7 - إدخال كود غير مفيد Junk Code

الـ "Junk Code" هو كود لا يغير في العمليات الحالية فقط لزيادة عدد التعليمات وذلك لتشويش ألأنتي فيروس ، المثال التالي يبين مثالين على ذلك:

```
// simple code
r1 = 12 ;
r2 = 34 ;
r3 = r1 + r2 ;

// first method for inserting Junk code
r1 = 12 ;
r1 = r1 + 1 ;    // r1 = 13
r1 = r1 + 1 ;    // r1 = 14
r1 = r1 - 2 ;    // r1 = 12
r2 = 34 ;
r3 = r1 + r2 ;

// second method for inserting Junk code
// (Junk Loop)
r5 = 42 ;
r1 = 12 ;

x:
     r2 = 34 ;          // not change
     r5 = r5 - 1 ;

     if ( r5 != 0 )
          goto x

r3 = r1 + r2 ;
```

الشكل 2-16 يبين ادخال أكواد غيره نافعه Junk Code

8 - توليد الكود وقت التشغيل Run-Time Code Generation:

أحدى طرق تحويل الكود هي أن لا يكون هناك كود موجود على الإطلاق ويتم توليده وقت التنفيذ سواء بتوليد كود جديد أو بالتعديل على كود موجود:

```
// simple code
r1 = 12 ;
r2 = 34 ;
r3 = r1 + r2 ;

// Generate new code
r1 = 12 ;
ptrToFunction = generate(r3=r1+r2);
call ptrToFunction ;
```

الشكل 2-17 يبين كيفية عمل توليد للكود وقت التشغيل at Run-Time

9 - استخدام أكثر من مسار في التنفيذ Concurrency :

يمكن فصل الكود الى أكثر من "Thread " وهكذا سيجعل عملية التحليل أكثر تعقيدًا . المثال التالي يوضح ذلك:

```
// simple code
r1 = 12 ;
r2 = 34 ;
r3 = r1 + r2 ;

// After Threading
start Thread T ;
r1 = 12 ;
wait for Singal ;
r3 = r1 + r2 ;

T:
    r2 = 34 ;
    Start Singal ;
    exit Thread T ;
```

الشكل 2-18 يبين استخدام أكثر من Thread لجعل البرنامج أكثر تعقيداً

10 استخدام الـــ "Inlining " والـــ "Outlining " :

الـــ "Inlining " هي عملية تستخدم في تبديل استدعاء الدوال بكود الدالة بالكامل ، ويستخدمها المترجمات عاده لتسريع البرنامج المثال التالي يوضح ذلك:

```
// simple code
call S1() ;
call S2() ;

void S1 () {
    r1 = 12 ;
    r3 = r3 + r2 ;
    r4 = r1 + r3 ;
}

void S2 () {
    r1 = 12 ;
    r2 = 34 ;
    r3 = r1 + r2 ;
}

// After Inlining
r1 = 12 ;
r3 = r3 + r2 ;
r4 = r1 + r3 ;

r1 = 12 ;
r2 = 34 ;
r3 = r1 + r2 ;
```

الشكل 2-19 يبين كيفية عمل الـInlining

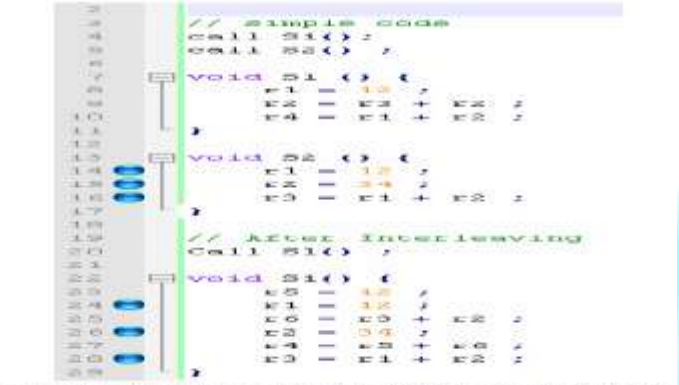
أما الـــ "Outlining " هو عكس العملية السابقة:

```
// simple code
r1 = 12 ;
r2 = r3 + r2 ;
r4 = r1 + r2 ;

r1 = 12 ;
r2 = 34 ;
r3 = r1 + r2 ;

// After Outlining
//it need not preserve any logical code grouping
r1 = 12 ;
r2 = r3 + r2 ;
call S1();
r3 = r1 + r2 ;

void S1 () {
     r4 = r1 + r2 ;
     r1 = 12 ;
     r2 = 34 ;
}
```

الشكل 2-20 يبين كيفية عمل الOutlining

11 تداخل الدوال Function Interleaving:

يمكن أن نجمع دالتين مع بعض مع تغيير المتغيرات بما يلزم ، المثال التالي يوضح ذلك:



الشكل 2-21 يبين طريقة عمل الFunction Interleaving

هناك العديد من هذه التحويلات وغيرها تستخدم في مجال تشويش الكود "Code Obfuscating " والذي يهدف لمنع عمليات الهندسة العكسية للبرامج "Reverse Code Engineering " وهناك الكثير من طرق التحويل تستخدم في مجال الـــ "Compilers Optimization " ولكن لم تستخدم الفيروسات جميع طرق هذا الفرع من العلوم بعد.
بدلا من تقديم التحويلات للـــ "Mutation Engine " كي يختار منها منها، قد تستخدم الفيروسات محرك يقوم بشكل تلقائي بتوليد المقابل لحلقة فك التشفير، يسمى هذا الفرع في علم المترجمات بالبحث التلقائي عن مجموعه من الأكواد " Super optimization " ويمكن أن يكون البحث بعدة طرق منها البحث الشامل "Brute-Force " أو من خلال الاستفادة من الـــ "Automated Theorem Proving " أو من خلال أي تقنية تساعد في البحث في مساحات البحث الكبيرة "for searching a large search space. "
الفيروس " Zellome " على سبيل المثال أستخدم الخوارزمية الجينية "Genetic Algorithms " فى الـــ " Mutation Engine " وبشكل عام قد تحتاج عمليات البحث هذه لعمليات معقدة لذلك الاتجاه الأفضل هو اختيار خوارزمية ذكية بحيث تتجاوز الكثير من الكود الخاطئ وبالتالي تحسن زمن البحث بشكل كبير.

الفيروسات Metamorphism :

الفيروسات من هذا النوع تكون غير مشفرة وبالتالي لا تحتاج لحلقة لك تشفير ، وتقوم بالاختفاء عن طريق توليد نسخة جديدة من جسم الفيروس في كل مرة إصابة .طريقة التوليد في هذا النوع من الفيروسات يستخدم الـــ " Mutation Engine " هو الأخر . وفيروسات هذا النوع تكون عادة كبيرة فمثلا الفيروس "Simile " الذي أطلق في2002 يتكون

الـــ "Mutation Engine " من حوالي 12000 سطر مكتوبة بلغة الاسمبلي. ويقوم بتحويل كود لغة الآلة الناتج إلى كود وسيط يقوم ال "Mutation Engine " بقراءته وتوليد كود آلة جديد.

الفرق بين فيروسات الـــ "Metamorphism " وفيروسات "Polymorphism "

هو أن الـــ " Polymorphism " لا يغير من الـــ " Metamorphism " في كل مرة إصابة لأنه يكون في الجانب المشفر في الفيروس .لكن فيروسات الـ "Metamorphism " تقوم بعمل نسخة جديدة من نفسه "morph itself" " في كل مرة إصابة.

يسهل تطبيق الـــ "Metamorphism " مع الفيروسات التي تنتشر مع الكود "Source Code مثل فيروسات الماكرو "Macro Virus " حيث يستخدم الفيروس أدوات النظام لتوليد نسخه "Metamorphism ": مثلا الفيروس "Apparition " المكتوب بباسكال يقوم بعد الإصابة بإدخال "Junk Code " ويقوم بعمل إعادة ترجمه لنفسه.

بالرغم إن فيروسات الـــ "Metamorphism " وفيروسات "Polymorphism " ليست بالسهولة في القبض بالنسبة لبرامج الحماية إلا أنها أيضا يصعب كتابتها بشكل صحيح ، وبالتالي عدد فيروسات هذه الأنواع قليل مقارنة مع غيره من الأنواع الأخرى.

Strong Encryption:

باستخدام طرق التشفير السابقة وحدث أن شك المستخدم أو محلل الفيروسات بوجود فيروس مشفر ، فهذا يعني أنه عرضة للفك في أي لحظة والسبب ليس في طريقة التشفير نفسها بل لأن الفيروس يحمل طريقة فك التشفير معه (المفاتيح) وبدون وجود هذا المفتاح فيعني أن الفيروس لن يستطيع فك جسم الفيروس وبالتالي لن يعمل . على أية حال هناك طريقتين لحل هذه المشكلة

الأولى : هو أن يأتي المفتاح من جهة خارج النظام المصاب

والثانية: هي أن يأتي المفتاح من جهة داخل النظام المصاب

نستعرض الآن هذه الطرق ونرى كيف يمكن تطبيقها:

يأتي المفتاح من خارج النظام المصاب :يمكن أن يقوم الفيروس بطلب المفتاح من موقع معين، ولكن هذا يعني وجود العنوان داخل الفيروس والذي يمكن أن يعرضه للكشف ثم يقوم المستخدم بمنع الوصول لهذا الموقع من خلال خيارات المتصفح. طريقة أخرى للدخول للموقع والوصول للمفتاح وهو أن يقوم الفيروس باستخدام محرك البحث للوصول لذلك المفتاح وكتجاوز لهذه المشكلة.وهكذا يستطيع الفيروس جلب المفتاح من أي جهة لا يحتمل أن تكون مغلقة "Blocked " مثل IRC وSharing Network -File و Email-Message وغيرهم ...

حل أخر وهو باستخدام مفهوم الفيروسات الثنائية "Binary Viruses " حيث هي فيروسات تتكون من قسمين ولا يمكن أن يصاب نظام إلا بوجود هذين القسمين معا. الفيروسات من هذا النوع قليلة مثل "RMNS " و "Dichotomy " يمكن أن تعمل هذه الفيروسات بأن يحتوي القسم الأول V1 على الكود المشفر والجزء الثاني V2 على المفتاح ولكن احتمال عمل هذه الطريقة قليل للغاية والسبب أنه في حال أنتشر الجزء الأول والثاني في نفس اللحظة سوف يعرضهم للتحليل وبالتالي يتم كشف المفتاح، أما في حال أنتشر الجزء الأول V1 وبعد مده أنتشر الجزء الثاني (شهر مثلا) فقد يكون المستخدم قد قام بحذف الجزء الأول وبالتالي لن تتم الإصابة . إذا احتمال اجتماع الملفين وإصابة الجهاز فيما بعد سوف تكون صغيره للغاية.

يأتي المفتاح من داخل النظام المصاب :وهنا يتم توليده من خلال أسم الدومين "Host Name " للجهاز أو من خلال التاريخ والوقت أو بعض البيانات في النظام ، أو أسم المستخدم الحالي واللغة المستخدمة في النظام .ولكن هذا يجعل الفيروس محدد لشخص واحد أو مجموعه من الأشخاص لهم نفس الخصائص.

غير ذلك باستخدام كلا الطريقتين فإن الفيروس لن يعلم أن عملية فك التشفير صحيحة وتمت بنجاح ، للتأكد من ذلك يمكن أن يحمل الفيروس "Checksum " معه لكي يتحقق من عملية الفك أو استخدام جمله " Try and Catch" للـــ " exception " الناتج من تنفيذ الكود الخاطئ.

ديناميكية عمل الملفات التنفيذية خلال النظام:

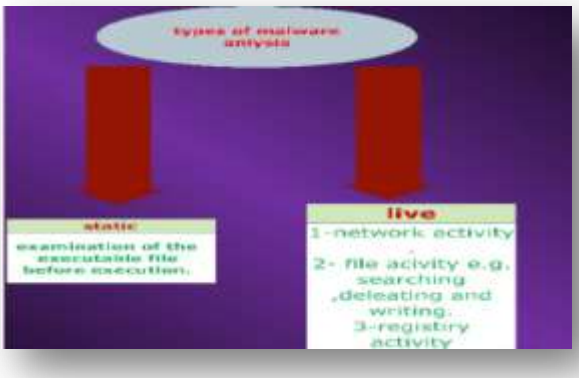
هذا رسم بياني بسيط يوضح طريقة عمل الملفات التنفيذية داخل النظام فكما نرى عند تنفيذ احد البرامج والتي في حالتنا هنا البرمجيات الضارة فان النظام يقوم بتحميل ال "process" والإجراءات الخاصة بالبرنامج إلى الذاكرة وعلى هذا فإن كل برنامج يعمل في نظامنا تكون له"process " مقابلة له في الذاكرة ويكون لكل process رقم يميزها يسمى ب(PID) "process identifier " إلى هنا الكلام جيد لكن ماذا يحدث بعد اكتمال تنفيذ البرنامج على النظام ما هي التأثيرات والنشاطات الحيوية الذي يحدثها بالنظام وهذا ما نحن بصدد دراسته

للمعلومية فقط:

عند تحميل ال "process"لأي برنامج إلى الذاكرة تتجزأ إلى عدة مقاطع مثل مقطع text. ومقطعdata. ومقطع bss.

عموما هذا فقط لإثراء المعلومات

انواع تحليل البرمجيات الضارة:

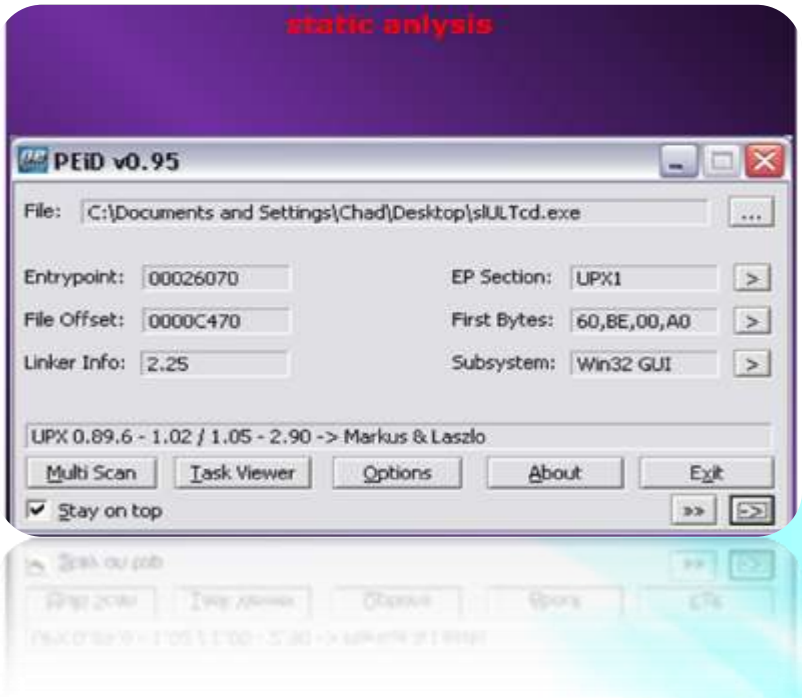


كما نرى في الرسم البياني الموضح بالأعلى هناك نوعان رئيسيين لتحليل البرمجيات الضارة STATICو. LIVE

أولا :Static Analysis:

وهو تحليل الملف التنفيذي بشكل مبدأي قبل تنفيذه على النظام وجمع معلومات عنه مثل اسم البرنامج المستخدم لعمل packingللملف إذا كان الملف مشفر ومعمول له packing أيضا معرفة اللغة البرمجية المكتوب بها البرنامج ونقطة الدخول وكثير من المعلومات الأخرى.
هناك أداوت

ثانيا Live Analysis:



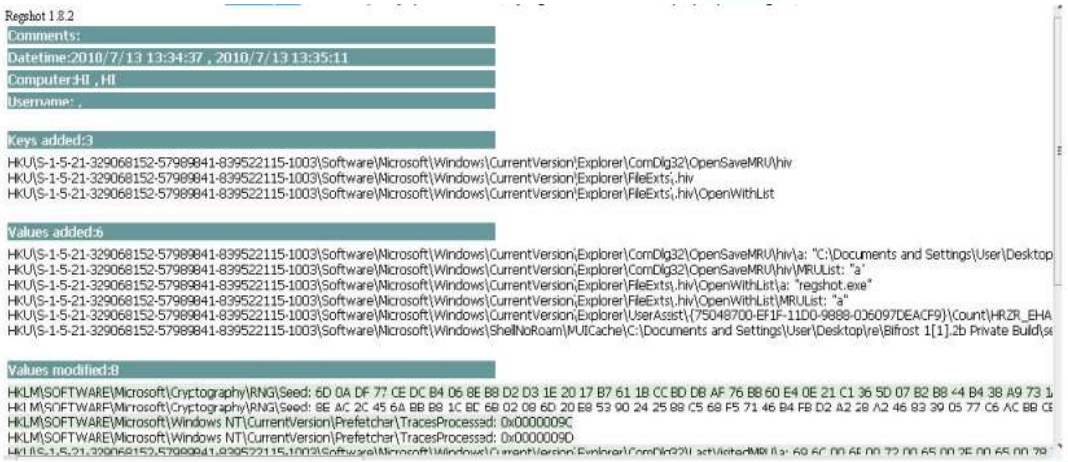
ويقصد به تحليل الملف التنفيذي إثناء تشغيله على النظام"Run Time " ويساعدنا هذا التحليل على معرفة التأثيرات والنشطات الخاصة بهذا الملف على النظام مثل معرفة تأثيرات تنفيذ الملف على ال " registry“ ونشاطات الملف عبر الشبكة وغيرها من الأمور التي سنتعرف عليها لاحقا.

Registry Activity

من المعلوم لدى الجميع أن ال ”malware تحدث تغيرات في ال" registry" وان هذه التغيرات التي تحدثها هي طريقة للتأكد من تثبيت الmalwareعلى النظام وذلك لان جميع الإعدادات التي في ال" registry" تعمل مع عمل” reboot " t للنظام.
والاداة التي سنستخدمها هنا لرصد التغيرات في ال"Registry" هي أداة" regshot "

فكرة عمل الأداة:

بساطة من خلال هذه الأداة سنقوم بعمل "snapshot " للريجستري قبل تنفيذ الملف المراد تحليله ومن ثم سنقوم بأخذ صورة أخرى "2nd snapshot " الرجيستري بعد تنفيذ الملف المراد اختباره ومن ثم سنقوم بالضغط على الزر " compare " ليقوم البرنامج بعمل مقارنة بين الصورتين وتقديم مفاتيح الرجستري الذي لذي حدث لها تغير وأيضا المفاتيح التي تم إضافتها للريجستري في "text report " أو "html report " كما تريد .



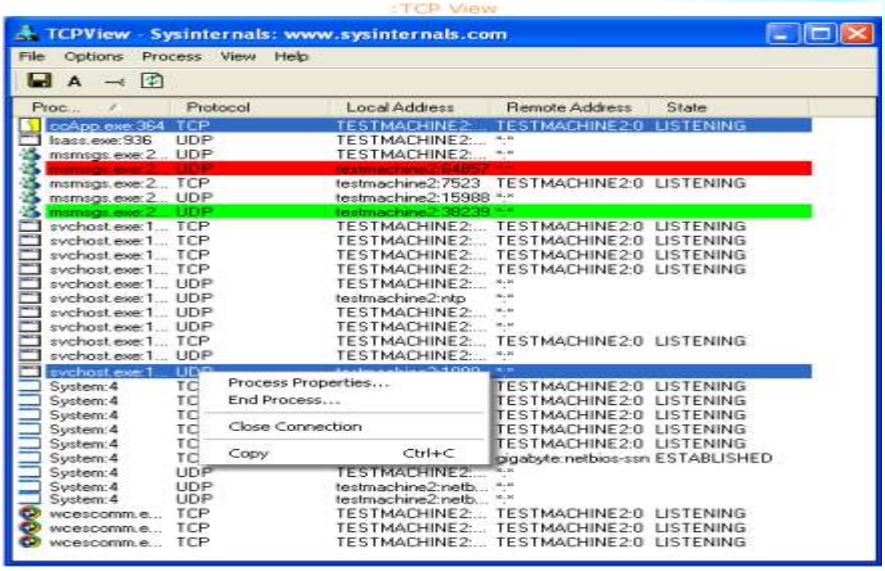
Network Activity

هنا سنقوم بتحليل جميع النشاطات التي يقوم بها البرنامج عبر الشبكة وهناك أداوت كثيرة منها من يقوم بمراقبة الشبكة بشكل عام وتحليل الحز مثل "sniffer " منها منا يقوم بتحليل النشاطات التي تحدث عبر الشبكة بالاعتماد على مراقبة الـــ "process " الخاصة البرنامج ومن الأدوات التي تقوم بعمل ذلك:

TCP View :

فكرة عمل هذه الأداة

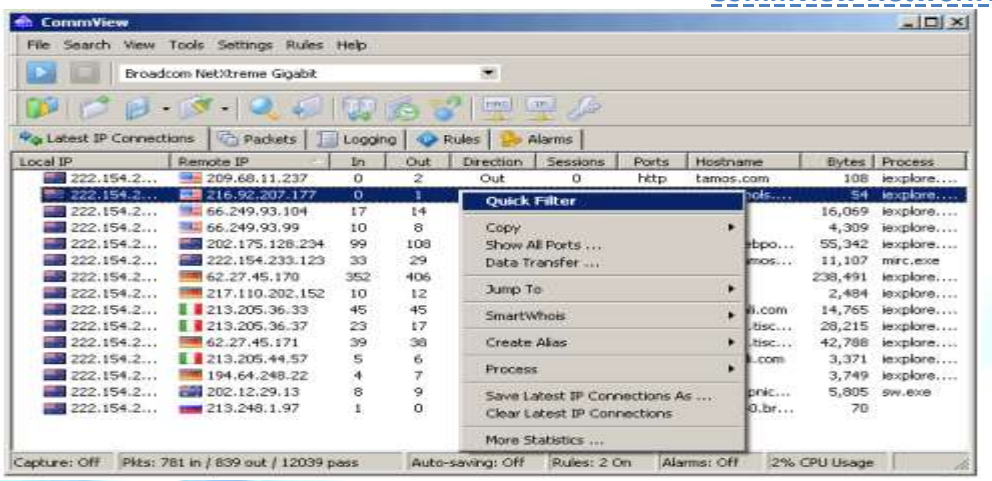
من الجيد في استخدام مثل هذه الأدوات انك ربما تستطيع كشف الديدان او البوت نت فمثلا ولنفرض أن هناك " bot botnet " على نظامك وكان البوت نت يحتوي على طريقة للانتشار عبر ثغرة ما عبر الشبكة كيف تستطيع اكتشافه؟؟ بما أن البوت نت سوف يقوم بفحص الأنظمة التي تعمل على الشبكة هذا يعني ان البوتنت سوف يقوم بعمل اتصال مع هذه الأنظمة من داخل نظامك إذا عن طريق هذه الأداة إذا وجدنا "process " معينة تعمل على النظام تقوم بالاتصال بالأنظمة الأخرى على الشبكة الداخلية فهذا يعني أن هذه الـــ "process " هي عبارة عن "botnet " أو الدودة طبعا من خلال المنفذ التابع للدودة تستطيع عمل بحث بسيط عبر محركات البحث لمعرفة الخدمة الخاصة بهذا المنفذ ومعرفة اسم البرنامج الضار والخبيث ايضا تستطيع بما انك عرفت الـــ "process " الخاصة بالدودة أو البوت نت تستطيع عمل "dump " لهذه الـــ "process " للحصول على نسخة من هذ الملف الخبيث وتحليله ودراسته وعموما سوف نشرح هذه الطريقة لاحقا في الفقرات القادمة.



Sniffers

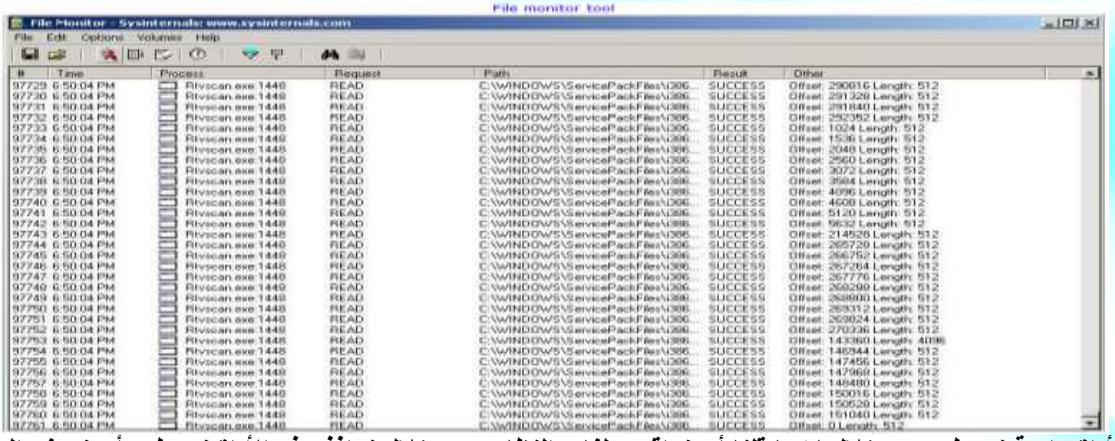
وهى بشكل عام لها استخدامات كثيرة لكن وظيفتها بشكل عام مراقبة إي اتصال يخرج أو يدخل إلى النظام أو الشبكة وتحليل حزم هذا الاتصال ومن اشره برمجياتها هى برنامج "wireshark " الشهير وبرنامج و:"commview" هو الذي سنتكلم عنه

Commview Network Analyzer:

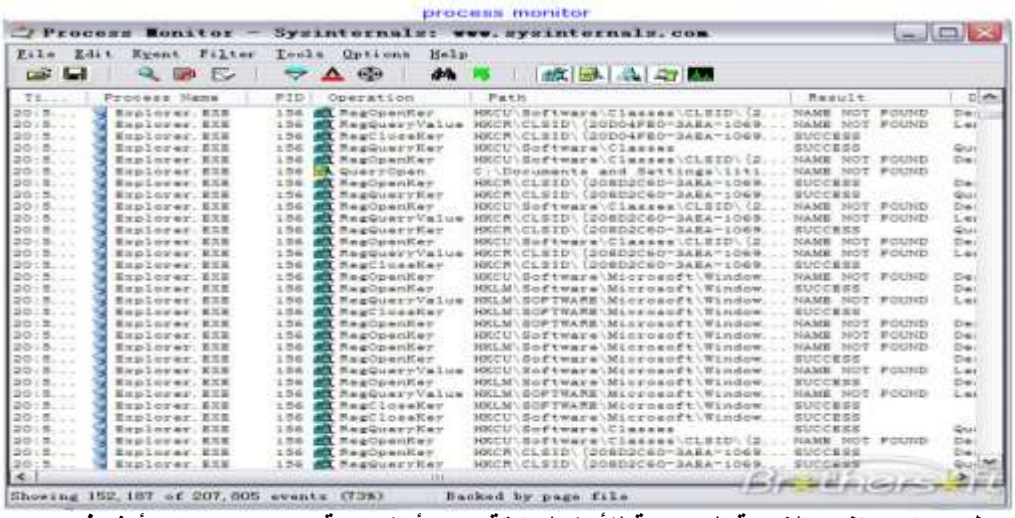


File Activity

هنا سنقوم بمراقبة وتحليل نشاطات وحركات الملف داخل النظام هل يقوم بعمل مسح لملفات معينة مثلا أو يقوم بوضع ملفات في مسارات معينة من الأدوات البسيطة والشهيرة لهذا العمل أداة " file monitor"



هذه الأداة رائعة نستطيع من خلالها كما قلنا أن نراقب ملفات النظام ومن خلال نوافذ هذه الأداة نستطيع أن نعرف المسارات التي تقوم كل "process " بعمل "access " عليها وما نوع هذا إل "access " مثلا هل هو write كان تقوم الـــ " process " بالكتابة على ملف معين أو وضع ملف جديد بمسار معين.



هذه الأداة تم تطويرها من نفس الشركة المبرمجة للأداة السابقة وهي أداة رائعة وتحوي مميزات أكثر فهي تستطيع مراقبة ملفات النظام والريجستري وتقوم بعرض أسماء ال "process" " التي تقوم بعمل "access" " على كلا من الريجستري أو ملفات معينة في النظام.

Packer basics

عملية الضغط والتشفير اوالـ "Packing" " هي عبارة عن خوارزمية "algorithm" " يقوم المبرمج ببرمجتها واستخدامها لحماية البرنامج من التحليل أو ما نسميه أيضا بال "Reverse Engineering" "

ما الذي يحدث للملف التنفيذي عند ضغطه وتشفيره بالpacker؟؟

بكل بساطة الملف التنفيذي سوف يتغير حجمه بما انه أصبح مشفر أيضا عنوان نقطة الدخول القديمة للملف الأصلي سوف تتغير إلى نقطة الدخول الجديدة والتي سيقوم النظام بقراءتها إثناء تنفيذ الملف التنفيذي المشفو ليقوم بتنفيذ كود فك الضغط.

IS This Malware Packed ؟

هناك برمجيات كثيرة لإجابة هذا السؤال وتقوم بإخبارك هل هذا الملف التنفيذي مشفر أم لا وما اسم هذه التشفيرة مثل برنامج "peid" " أو "file inspector" " عموما سبق لنا أن تكلمنا عن هذه النقطة في ال"Static analysis" " ..

طبعا هذه البرمجيات تستطيع التعرف على أنواع التشفير بالاعتماد على مقارنتها بمجموعة من "signature" " ن ثم التعرف على نوع التشفير مثل طريقة الإنتي فيروس تماما في التعرف على الملفات الضارة.

Unpacking Binaries

إذا استطعنا التعرف على نوع التشفير من خلال البرمجيات السابق ذكرها تستطيع عمل بحث بسيط عبر محركات البحث وتحميل الأدوات اللازمة لفك الضغط عن الملف التنفيذي.

ولكن!! ماذا لو لم تستطع الأدوات التعرف على التشفيرة ماذا سوف نفعل في هذه الحالة؟

بالتأكيد سوف نلجأ فيما يسمى بـــ "manual unpacking" "

Manual Unpacking

هناك أكثر من طريقة لفك الضغط والتشفير عن الملفات التنفيذية يدويا
بالطبع الطرق تعتمد على مهاراتك الخاصة في الهندسة العكسية أن صح القول فأي شخص له خلفية عن هندسة العكسية وطرق عمل كراك ينج على البرامج المشفرة والمضغوطة سوف يفهم إنا كل ما سوف نقوم به الآن ما هو إلا هندسة عكسية للملف التنفيذي.(: عموما سوف نشرح الطريقة الأكثر شهرة فك ضغط البرمجيات المشفرة لكن لا تعتقد أن أي ملف تنفيذي سوف يكون فك تشفيره بهذه السهولة فهناك طرق كثيرة للمناورة!(:

Run and Dump Unpacking

حتى نفهم هذه الطريقة وديناميكية عملها تعالوا نسترجع بعض المعلومات الأساسية لآلية عمل الملفات التنفيذية: إن أي ملف تنفيذي نقوم بتنفيذه على النظام يقوم النظام بتحميل ال "process" " الخاصة به في الذاكرة هذه "process" " تحتوي على أي صورة طبق الأصل من ملفات البرنامج.

لكن ماذا عن الملفات التنفيذية المشفرة ؟

أن الملفات التنفيذية المشفرة قلنا عنوان نقطة الدخول "entry point" " لها تتغير لنقطة دخول جديدة لكي يستطيع النظام البدء من عند كود فك الضغط الذي أضيف للملف التنفيذي إثناء تشفير وما سيحدث انه عندما نقوم بالضغط على الملف التنفيذي المشفر سوف يقوم النظام بقراءة نقطة الدخول الجديدة والذي اشرنا إليها سابقا ومن ثم يبدأ فك الملف التنفيذي وتحميل الملفات اللازمة لل"process" " الخاصة به في الذاكرة في هذه الإثناء سوف يكون عندنا صورة طبق الأصل من الملف التنفيذي لكن غير مشفرة أي الملف الأصلي.
كل ما سوف نقوم بفعله هو قراء الذاكرة واستخراج "Dump" " هذه الصورة من الملف التنفيذي أثناء عمله على النظام والبرمجيات التي تستطيع عمل ذلك كثير مثل "task manger" " والذي يكون موجود مع نظام الوندوز

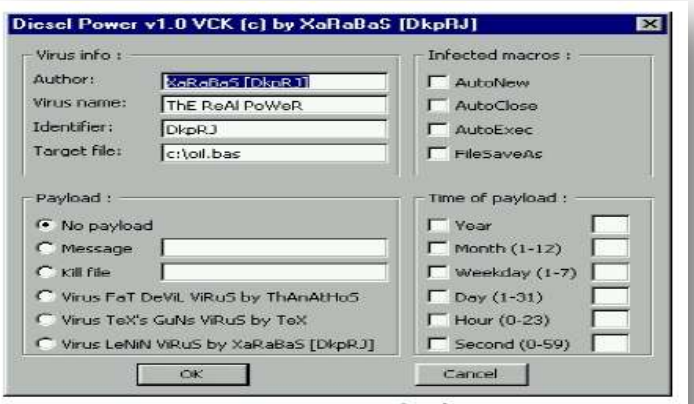
ايضا برنامج lordpe المعروف.

كما ترى في الصورة تستطيع اختيار الprocess التي تريدها وعمل full dump لها.

هناك طرق أخرى أيضا كما قلنا كاستخدام المنقحات كبرنامج"olly" " وكما قلت تذكر هناك طرق كثيرة للمناورة هنا فلا تعتقد أن الأمر دائما سيكون بهذه السهولة كل ما ذكر هنا هو مجرد بداية لتأخذ فكرة جيدة عن تحليل الملفات التنفيذية بشكل عام والملفات الضارة بشكل خاص.

مولدات الفيروسات Virus Kit:

هناك العديد من الأدوات التي تستخدم في كتابة الفيروسات وتسمى "Virus-Kit " وهي تقوم بتوليد كود الفيروس بشكل تلقائي أو تقوم بتوليد جزء معين من الكود .هذه البرامج لها أشكال وأنواع مختلفة ، فمنها ما يعمل من خلال سطر الأوامر ، ومنها ما يستخدم الواجهة الرسومية GUI والشكل التالي يوضح أحد أنواع هذه البرامج.



الشكل 2-22 يبين أحد أدوات توليد الفايروسات بضغطة زر

أيضا هناك العديد من المكتبات البرمجية والتي تستخدم لتحويل الفيروس العادي إلى "Polymorphism " أو الى " Metamorphism " وكلما ازدادت شعبية هذه الأدوات كلما قام محللي الفيروسات بتحليلها ودراستها لاكتشاف كل السلالات التي تنتجها هذه البرامج.

مضادات مقاومة الفيروس Anti-Anti Virus:

كل الفيروسات ذاتية الانتشار "Self-Replicate " ولكن ليس جميعها موجه للهجوم على برامج مقاومات الفيروس وتسمى هذه الفيروسات الموجهة لبرامج ألأنتي فيروس" المضادة لمضاد الفيروسات "Anti-Anti Viruses وتستفيد من ذلك في القضاء على برنامج مقاوم الفيروس في الجهاز ، وجعل عملية تحليل الفيروس أصعب بالنسبة لمحلل الفيروسات ، وجعل الفيروس غير قابل للكشف من قبل برنامج الأنتي فيروس وذلك من خلال معرفة إلية عمل الأنتي فيروس ، وباستخدام طرق التشفير التي تم التعرض لها سابقًا نجد أننا نستطيع تحقيق أهداف الـ "Retroviruses " ما عدا الهجوم على برنامج الأنتي فيروس والتي سنستعرضها في هذه الفقرة

قد تستخدم برامج الأنتي فيروس نفس طرق الفيروسات وتقوم بعمل فيروس يهاجم الأجهزة للقضاء على الفيروسات ويطلق على هذه الفيروسات المفيدة "Anti-Virus Virus " وهي تختلف عن الـ "Anti-Anti Viruses " والتي يستخدمها كاتبي الفيروسات للهجوم على الفيروسات . هناك العديد من التقنيات التي تستخدمها الفيروسات لتطبيق هذه الخاصية "Anti-Anti Viruses " وهم

Retroviruses, Entry Point Obfuscation, Anti-Emulation, Armoring, Tunneling, Integrity Checker Attack, Avoidance.

خدع الفيروسات *Virus Hoax*:

هي رسائل تأتي للبريد للتحذير من أحد الفيروسات ، وهذه الرسائل غير ضاره بحد ذاتها ولكنها مستهلكه للمصادر ، وبعض الرسائل تجعل المستخدم يضر نفسه بنفسه عن طريق عمل بعض التعديلات في الجهاز حتى يحذف الفيروس" المزعوم. " أحد أشهر الخدع التي انتشرت في 2002 هي خدعه برنامج "jdbgmgr.exe " والذي كانت تطلب من المستخدم حذف هذا الملف لأنه فيروس خطير ، وهذا الملف في الحقيقة ليس إلا عبارة عن منقح للتطبيقات الجاف وهو يكون موجود مع أي نسخه ويندوز.

I found the little bear in my machine because of that I am sending this message in order for you to find it in your machine. The procedure is very simple:

The objective of this e-mail is to warn all Hotmail users about a new virus that is spreading by MSN Messenger. The name of this virus is jdbgmgr.exe and it is sent automatically by the Messenger and by the address book too. The virus is not detected by McAfee or Norton and it stays quiet for 14 days before damaging the system.

The virus can be cleaned before it deletes the files from your system. In order to eliminate it, it is just necessary to do the following steps:
1 - Go to Start, click "Search"
2 - In the "Files or Folders option" write the name jdbgmgr.exe
3 - Be sure that you are searching in the drive "C"
4 - Click "find now"
5 - If the virus is there (it has a little bear-like icon with the name of jdbgmgr.exe DO NOT OPEN IT FOR ANY REASON
6 - Right click and delete it (it will go to the Recycle bin)
7 - Go to the recycle bin and delete it or empty the recycle bin.

IF YOU FIND THE VIRUS IN ALL OF YOUR SYSTEMS SEND THIS MESSAGE TO ALL OF YOUR CONTACTS LOCATED IN YOUR ADDRESS BOOK BEFORE IT CAN CAUSE ANY DAMAGE

الشكل 2-23 يبين الرسالة الخادعه التي تطالب بحذف البرنامج jdbgmgr

تقنيات مقاوم الفيروسات

تقنيات الانتي فيروس

تقوم برامج الأنتي فيروس بثلاث مهام ، هي:

1 - الكشف عن وجود الفيروس "Detecting " :

حيث تكشف هل البرنامج الحالي هو مصاب أم لا .والنتيجة النهائية قد لا تكون صحيحة تمامًا . فلطالما تمكن صانعي الفيروسات من كتابة فيروسات لا تستطيع برامج مقاومة الفيروس كشفه ا .وبالتالي يجب أن يقوم المستخدم بعمل تحديث للبرنامج حتى يتمكن من كشف الفيروس الجديد وفي المقابل يبدأ صانع الفيروس بكتابة فيروس جديد وهكذا تستمر دورة الحياة.

على برامج مقاوم الفيروس كشف جميع الفيروسات بما فيها الفيروسات الخاملة "Dormant " والتي لا تعمل في النظام الحالي ولكنها يمكن أن تنتقل للنظام الأخر عن طريق النسخ بواسطة المستخدم فيجب على تلك البرامج كشف هذه الفيروسات .أيضا يجب أن تكشف عن الـــ "Intended " وهي التي لا تعمل على أي نظام نظرًا لوجود خلل "Bug " في الفيروس ووجود هذه الفيروسات في النظام وحتى ان لم تعمل يدل على وجود ضعف في النظام وبالتالي يجب كشفها أيضًا.

2 - التعرف على الفيروس "Identification"

بعد الكشف عن وجود الفيروس حيث يجب التعرف على ماهيته .ويمكن أن تكون هذه المرحلة منفصلة عن مرحلة الكشف أو أن تكون ضمن خطوات الكشف.

3 - إزالة الفيروس "Disinfection "

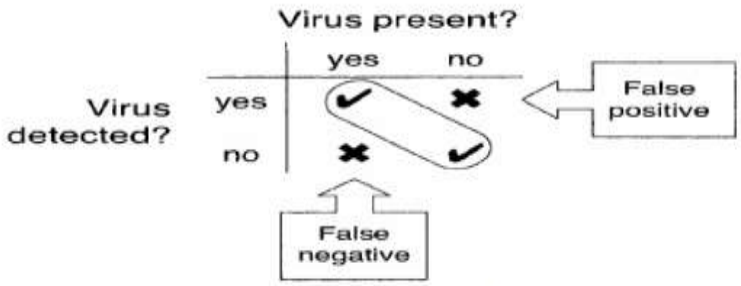
وهنا يقوم البرنامج بإزالة الفيروس المعين ويطلق عليها أحيانًا "Cleaning " هذه المرحلة تأتي بعد التعرف على الفيروس حيث أن لكل فيروس طريقة للتخلص منه

شرح مرحلة الكشف والإزالة والتعرف :

مرحلة التعرف والإزالة يمكن أن تقوم بها من خلال الطرق العامة "Generic Method " والتي تتعامل مع الفيروسات المعروفة وغير المعروفة أو من خلال طرق مخصصه لنوع "Virus Specific " ولكنها سوف تتعامل مع نوع معين من الفيروسات (بالرغم من أنها قد تقوم بكشف الفيروسات الـــ "Variant " من أحد الفيروسات المعروفة)

وأهم مرحلة في هذه المراحل مرحلة الكشف "Detecting "

لأن المرحلتين الأخريات (التعرف والإزالة) تتطلب الكشف قبل أن تبدأ تلك المراحل بالعمل، إضافة إلى أن الكشف المبكر قبل حدوث الإصابة يلغي الحاجة للمرحلتين التعرف والإزالة. بعد إجراء عملية الكشف قد تحصل على النتائج التي توضحها ألصوره التالية:



الشكل 1-3 يوضح الناتج من عملية الكشف

الحالة الأفضل " Perfect " وهي عندما يتم الكشف عن فيروس موجود ولا يتم الكشف عن وجود فيروس عندما لا يكون هناك فيروس. لكن لسوء الحظ عملية التعرف ليست " Perfect " دائما فقد يحصل أن يتم التبليغ حول ملف لا يحتوي على فيروس وبالتالي هذا يعتبر إنذار خاطئ "False Positive " أو قد لا يستطيع المضاد كشف الفيروس وهو موجود وبالتالي يكون "False Negative " أو يطلق عليه " Miss " وكلا الحالتين الخاطئتين أمر غير مرغوب به إطلاقا وقد يجعل مستخدم المضاد يفقد الثقة بالبرنامج ويتجه لاستخدام أخر.

وعملية الكشف على الفيروس قد تكون "static " أو "dynamic " وذلك بالاعتماد على هل الفيروس يعمل عندما حصل الكشف.

الحماية والوقاية من البرمجيات الضارة:

ونحن اليوم لدينا استخدام أجهزة الكمبيوتر للقيام بأمور كثيرة .نذهب على الانترنت للبحث عن المعلومات ، والمتاجر والبنوك ، لا الواجبات المنزلية ، والألعاب ، والبقاء على اتصال مع العائلة والأصدقاء .ونتيجة لذلك ، لدينا أجهزة الكمبيوتر تحتوي على ثروة من المعلومات الشخصية عنا .وقد يشمل ذلك الخدمات المصرفية والسجلات المالية الأخرى ، والمعلومات الطبية -- المعلومات التي نريد حمايتها .إذا لم يتم حماية الكمبيوتر ، قد هوية اللصوص والمحتالين أخرى تكون قادرة على الوصول وسرقة معلوماتك الشخصية .أطول يمكن استخدام جهاز الكمبيوتر الخاص بك وطائرة بلا طيار غيبوبة "" لإرسال البريد المزعج التي يبدو أنها جاءت من أنت .يمكن أن الفيروسات أو برامج التجسس تودع على الكمبيوتر الخاص بك لذا يجب توخى الحذر واتبع تلك النصائح والإرشادات :

1 - التواصل مع دعم تكنولوجيا المعلومات :

الاستفسار منهم عن ما تريد لحماية جهازك واستدعائهم إذا كان لديك مشكلة دخول برنامج ضار إلى جهازك أو اختراق إليك ولكن أن يكون دعم فني معروف وموثوق فيه لأناس كثيرون مثل الدعم الفني لميكروسوفت

/http://www.microsoft.com/security/portal

2 - عليك دائما بأخذ نسخة احتياطية من ملفات الهامة :

هو فكرة جيدة لتأخذ من الوقت لإجراء نسخ احتياطي للملفات الخاصة بك .وإذا كان ممكنا ، ترجمة جميع الصور الخاصة بك ، وثائق ، الإنترنت المفضلة ، الخ ، ونسخها على قرص مضغوط أو دي في دي أو حفظها على جهاز تخزين بعض الخارجية الأخرى

3 - تثبت جدار الحماية "Fire Wal"

4 - ∞استخدام البرامج المضادة للفيروسات

ويحمي الكمبيوتر من الفيروسات التي يمكن أن تدمر البيانات الخاصة بك ، وإبطاء أو تعطل جهاز الكمبيوتر الخاص بك مكافحة الفيروسات الحماية بتفحص الكمبيوتر والبريد الالكتروني الخاص بك للبحث عن الفيروسات واردة ، ومن ثم يحذف عليها .يجب عليك ابق على برنامج مكافحة الفيروسات المحدثة لمواجهة الخلل "آخر" تعميم الإنترنت .معظم برامج مكافحة الفيروسات يتضمن ميزة لتحميل التحديثات تلقائيا عندما كنت على الانترنت .وبالإضافة إلى ذلك ، تأكد من أن البرنامج يعمل بشكل مستمر وفحص النظام الخاص بك للبحث عن الفيروسات ، وخاصة إذا كنت تحميل الملفات من الويب أو فحص البريد الإلكتروني الخاص بك . اول منعطف على جهاز الكمبيوتر الخاص بك .يجب عليك أيضا إعطاء النظام الخاص بك مسح شامل على الأقل مرتين في الشهر .

5- استخدام برامج مكافحة برامج التجسس .

برامج التجسس والبرامج المثبتة دون علمك أو الموافقة التي يمكن رصد الأنشطة الخاصة بك على الانترنت وجمع المعلومات الشخصية أثناء تصفح الويب .بعض أنواع برامج التجسس ، ، بما في ذلك كلمات المرور والمعلومات المالية .العلامات التي قد تكون إصابة الكمبيوتر مع برامج التجسس وتشمل موجة مفاجئة من الإعلانات المنبثقة ، التي يجري اتخاذها لمواقع ويب التي لا تريد الذهاب إلى وتباطأ عموما الأداء .
يتم تضمين برامج التجسس الحماية في بعض البرامج المضادة للفيروسات .تحقق من وثائق برنامج مكافحة الفيروسات للحصول على تعليمات حول كيفية تنشيط ميزات الحماية من برامج التجسس .يمكنك شراء منفصلة البرامج المضادة للبرامج التجسس .إبقاء البرنامج الخاص لمكافحة برامج التجسس المحدثة وتشغيله بشكل منتظم .
لتجنب برامج التجسس في المقام الأول ، وتحميل البرنامج فقط من مواقع تعرفه وتثق به .

6- إدارة النظام الخاص بك والمتصفح لحماية خصوصيتك.

قراصنة يحاولون باستمرار لإيجاد عيوب أو ثغرات في أنظمة التشغيل والمتصفحات .لحماية الكمبيوتر والمعلومات على ذلك ، وضعت إعدادات الأمان في النظام الخاص بك والمتصفح في متوسطة أو أعلى من ذلك .الاختيار "أداة" أو "الخيارات" القوائم لكيفية القيام بذلك .تحديث النظام الخاص بك والمتصفح بشكل منتظم ، والاستفادة من التحديث التلقائي عندما يكون متوفرا .تحديث ويندوز هو الخدمة التي تقدمها مايكروسوفت .وسوف تنزيل وتثبيت تحديثات البرامج لنظام التشغيل مايكروسوفت ويندوز ، وإنترنت إكسبلورر ،

7- استخدم كلمة مرور قوية -- وتحتفظ بها لنفسك ..

حماية الكمبيوتر من المتسللين عن طريق اختيار كلمات السر التي يصعب تخمينها .استخدم كلمات مرور قوية مع ما لا يقل عن ثمانية أحرف ، مزيج من الحروف والأرقام والحروف الخاصة .لا تستخدم الكلمة التي يمكن بسهولة العثور عليها في القاموس .بعض الهاكرز استخدام البرامج التي يمكن أن تحاول كل كلمة في القاموس .حاول استخدام عبارة لمساعدتك على تذكر كلمة السر الخاصة بك ، وذلك باستخدام الحرف الأول من كل كلمة في الجملة .على سبيل المثال ، - HmWc @ wC2 -كيف يمكن لكثير الخشب تشوك الفأر الجبلي .حماية كلمة السر الخاصة بك بنفس الطريقة التي كنت المفتاح إلى منزلك . بعد كل شيء ، بل هو "مفتاح" على المعلومات الشخصية الخاصة بك.

التأكد والحظر والتطهير Verification, Quarantine and Disinfection :

القليل من الناس من يرغب بأن يحتفظ بالفيروس في جهازه بعد أن يتم اكتشافه في الجهاز وكثيرون يريدون التخلص منه نهائيا ومهمة برامج ألأنتي فيروس لا تقتصر فقط على الكشف بل على التأكد والحجر الصحي والتطهير . وبالمقارنة مع الكشف هذه المهام قد تعمل نادرًا حيث يمكن أن تكون بطيئة ومستهلكة للمصادر أكثر من الكشف.

التأكد *Verification*:

كشف الفيروس قد لا يعطي الكلمة الأخيرة بأن هل الملف مصاب أم لا، لذلك تستخدم برامج الأنتي فيروس عملية تأكد " Verification " بعد أن يتم الكشف الأولى، هذه العملية مهمة لسببين
الأول هو تقليل الإنذارات الخاطئة"False Positive" والذي قد يحصل بالمصادفة أو باستخدام تواقيع قصيرة
والثاني هو لان عملية التأكد تستخدم للتعرف على الفيروس "identification " التعرف على الفيروس ضروري لكي يتم التطهير من الفيروس وقد يقوم الأنتي فيروس بتطهير ملف فيروس ولكن بطريقة أخرى مما يسبب الضرر غير المتعمد للملف .وتبدأ عملية التأكد بأخذ معلومات أكثر عن الملف وفي حال كان الملف مشفر يقوم الأنتي فيروس بمحاولة فك التشفير وذلك بإظهار تواقيع أكبر هذه العملية تسمى "X-Raying " وهي تستخدم في طريقة " Emulation " ولكن الـــ "X-Raying " هنا أبسط من ما هو في الـــ "Emulation " فمثلا في الفيروسات المشفر بتفسير بسيط بدون مفتاح أو من خلال مفتاح ثابت تكون هناك حروف مكررة في الشفرة وبالتالي يمكن الاستفادة من طرق التحليل الإحصائي والـ "Cryptanalysis " ومعرفة الحروف الأصلية.
مثلا في حال كانت القيمة 99 هي القيمة الأكثر ظهورا في النص الأصلي ووجد أن القيمة 27 هي القيمة الأكثر ظهورا في الشفرة فم ن خلال التشفير بالاعتماد على "XOR " يكون المفتاح هو 120 (من خلال عمل 27 XOR 99) وبعد أخذ جميع المعلومات من الملف تكون عملية البحث بأكثر من طريقة:

1. **مقارنة الفيروس الذي تم كشفه مع مجموعه من الفيروسات ولكن عملية تقديم مجموعه من الفيروسات مع مقاوم الفيروسات عملية مضرة لذلك فإن هذه الخيار يكون مفيد فقط لمحللي الفيروسات.**
2. **في حال تم الكشف باستخدام طرق غير السكان فيمكن أن يتم عمل سكان باستخدام مجموعه من التواقيع أما في حال كان الكشف باستخدام السكان يمكن أن يتم فحص التواقيع الأكبر "Longer " لكي يتم التأكد ..**
3. **أخذ الـــ "Checksumming " لجزء أو جميع أجزاء الفيروس ثم تتم مقارنه هذا الـــ " Hash " بجميع الهاش للفيروسات المعروفة.**
4. **استخدام كود مخصص لنوع معين من الفيروسات يتم استدعائه ليتحقق من الفيروس.**

الطرق أعلاه (ماعدا الأخير) غير مفيدة عند التعامل مع فيروسات الـــ "Metamorphism " لأنها تعتمد على أن جسم الفيروس (بعد فك التشفير) يكون ثابت في كل مره إصابة.

الحظر *Quarantine*:

عندما يتم كشف الفيروس قد تحتاج برامج مقاوم الفيروسات إلى عزل الفيروس عن النظام فقط لفترة مؤقتة حتى يقرر المستخدم ماذا يفعل بالملف (تطهير أو حذف) في حالات أخرى قد لا تكون لدى برامج مقاوم الفيروسات أي فكرة حول كيف يمكن تطهير الملف بالتالي تضع الملف في الحجر الصحي حتى يقوم محللي الفيروسات بوضع حلول للتطهير ويتم تقديم ذلك الحل مع التحديث التالي لقاعدة البيانات. تتم عملية الحجر وذلك بنسخ الملفات المصابة إلى مجلد الحجر ويتم حذف الملف الأصلي وتحذف جميع صلاحيات الوصول للملف، لكن قد يستطيع المستخدم تغيير الصلاحيات أو نسخ الملفات خارج الحجر الصحي لذلك يمكن تشفير الملفات في الحجر الصحي مثلا باستخدام أي طريقة بسيطة مثل "XOR " مع

ثابت وهكذا سيصبح الفيروس خامد "Inert " ولن يتأذى المستخدم لو نقله لخارج مجلد الحجر الصحي لأن الملف لن يعمل من الأساس. طريقة أخرى وهي باخفاء الملف في الحجر الصحي وذلك باستعمال نفس أساليب الـــ " stealth Virus " و الـــ "rootkit " على أي حال قد لا تكون هذه فكرة جيدة لأن الفيروس يمكن أن يستغل ذلك ويخبئ نفسه في مجلد الحجر الصحيح بالإضافة إلى أن استخدام أساليب الإخفاء قد تجعل برامج مقاوم الفيروسات الأخرى تشك بأن البرنامج (مقاوم الفيروسات) هو فيروس.

التطهير Disinfection:

التطهير لا يعني بأن النظام سيعود لحالته الأصلية وحتى لو تمت عملية التطهير بشكل صحيح، فبعض الحالات لا يمكن فيها التطهير مثل الفيروسات الـــ "overwritten " والتي تقوم بحذف جميع محتويات الملف .وهناك عدة طرق مختلفة لكي تتم عملية التطهير منها:

استرجاع الملفات المصابة من الـــ "Backup " وهنا سوف يتم استبدال الملفات المصابة بالملفات النظيفة الموجودة في مجلد "Backup " ولكن قد تضيع بعض البيا نات خصوصا في حال كان أخر "Backup " قديم . مسألة أخرى وهي في حال وجود فيروس في الـــ "Backup "ومثلا فهناك نوع من الفيروسات يسمى "Data Diddlers " يقوم بالتغيير في الملفات ببطء فاذا وجد في الـــ "Backup " فهذا يعني أن البيانات الأصلية قد تمت تغييرها.

قاعدة بيانات الأنتي فيروسVirus Database ولغة وصف الفيروسات Virus Description Language:

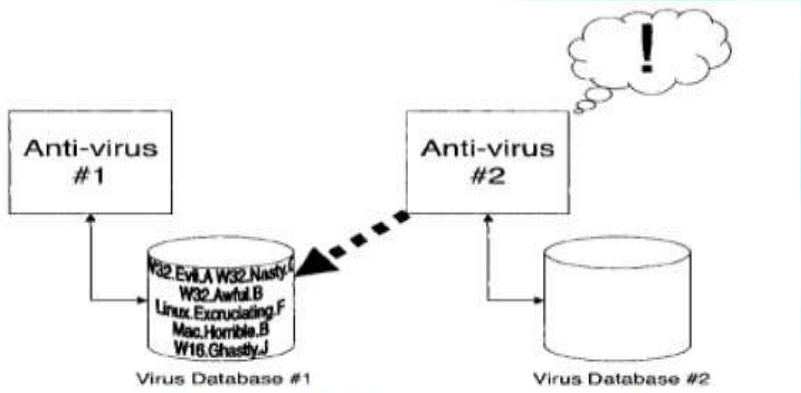
قاعدة بيانات الفيروسات تحتوي على سجلات كل فيروس وكل سجل يحتوي على جميع المعلومات المتعلقة بالفيروس والتي يطلبها مقاوم الفيروسات لكي يتعامل مع الفيروس منها أسم الفيروس حتى يطبعه ل لمستخدم ومنها معلومات التحقق من الفيروس (من غير وضع نسخة من الفيروس) ومنها معلومات التطهير.

والتواقيع الموجودة داخل قاعدة البيانات يجب أن تعامل بشكل خاص حيث يمكن أن تحدث مشكلة في حال كانت التواقيع موجودة بشكل واضح "ClearText " واحتوى الجهاز على أكثر من برنامج أنتي فيروس هنا سيعتبر أحد المضادات بأن قاعدة مقاوم الفيروسات الأخر عبارة عن ملف مصاب لأنه وجد تواقيع فيروسات.

مثال من الحياة توضيحي لو انك مرضت وأمرك الدكتور أن تأخذ مضاد (دواء) وقمت أنت بإغفال كلامه وأخذت مضادين كل منهما يقوم بنفس العمل فسيقوم كل منهم بإتلاف عمل الأخر ويرهقك جسمانيا وصحيا

==========

الطريقة الأفضل هي تشفير التواقيع وعدم فكها مطلقا وعند مقارنه المدخل يتم تشفيره أولا ومن ثم تتم عملية المقارنة بصوره مشفره



الشكل 2-3 يبين في حال أحتوي النظام على أكثر من قاعده بيانات للفايروسات بدون أن يتم تشفيرها

عندما يكتشف فيروس جديد تقوم شركات برامج مقاومة الفيروسات بتحديث قاعدة بيانات الفيروسات بالإضافة إلى أن جميع مستخدمي هذا البرنامج يجب أن يقوموا بعمل التحديث اللازم للحماية من الفيروس الجديد، وهذا يظهر لنا بعضًا من الأمور التي تخطر بالبال والأذهان مثل :

كيف يعلم المستخدم بظهور تحديثات جديدة ؟

الطريقة التي تستخدمها برامج مقاومة الفيروسات هي "Polling " وتتم تلقائيا بواسطة برنامج مقاومة الفيروسات ويستطيع المستخدم بشكل يدوي عمل التحديث.

طريقة أخرى وهي الـــ "Push Model" وذلك بأن يقوم مصنعي برامج مقاومة الفيروسات برفع "Push out" التحديثات فور صدورها . أغلب برامج مقاومة الفيروسات تستخدم الـــ "Pulling" وتقوم بإعلام المستخدمين بضرورة عمل التحديث نظرا لوجود فيروس جديد.

هل التحديث يكون تلقائي أو يدوي؟

التحديثات التلقائية تزود المستخدم بالحماية بأسرع ما يمكن لكن في حال كانت هناك مشكلة أو "Bug" فقد تحدث مشاكل كثيرة في الجهاز .كما حدثت في شبكة أحد شبكات السكة الحديد في اليابان (2005) وتسببت في توقف العمل لعدة ساعات.

متى تحصل عملية التحديث؟

قديما كانت عمليات التحديث تتم مره كل ش هر وكان هذا كافي .أما اليوم فعمليات التحديث الأسبوعية وحتى اليومية لا تكفي أحيانا وأفضل حل هو التحديث فور ما يتوفر توقيع جديد لأحد الفيروسات.

كيف توزع هذه التحديثات؟

التحديثات الالكترونية خاصة عن طريق الانترنت هي أفضل طريقة للتحديثات المستمرة.

عملية التحديث قد تكون هدف جيد للمخترقين حيث في حالة استولى المخترق على عملية التحديث بالتالي يمكن أن يخترق جميع أجهزه المستخدمين لهذا البرنامج، ويمكن أن يتم الاستيلاء بعدة طرق مثلا أن يقوم باختراق جهاز الـــ "vendor" والذي يقوم بتوزيع التحديثات أو حتى الاستيلاء على التحديث قبل أن يصل للجهاز المسئول عن توزيع التحديث .أو يمكن عمل "Spoofed" لجهاز المستخدم وبالتالي يتصل بجهاز المخترق بدلا من جهاز الـــ "vendor"

أو يمكن عمل هجوم رجل في الوسط "Man-in-the-Middle" حيث يقطع المخترق الاتصال بين المستخدم "vendor" ويقوم المخترق بتعديل التحديثات القادمة أو إضافة تحديثات خاصة به على قناة الاتصال.

وعملية التحديث ليست مقتصرة على التواقيع بل حتى للـــ "Antivirus Engine" وهذا ضروري لإصلاح الـــ "Bugs" أو إضافة تقنيات أخرى للقضاء على الفيروسات .ويستخدم مصنعي الأنتي فيروس عادة لغة خاصة لوصف الفيروسات وهي لغة تمكنهم من وصف الفيروس وكيف يمكن القبض عليه والتحقق منه وتطهيره ويقوموا بعمل مترجم بسيط "Compiler" اللغة إلى صيغه "Format" التواقيع في قاعدة البيانات . الشكل التالي يبين ذلك.

VERV description

```
VIRUS example                    ; short alias for virus
NAME  An example virus           ; full virus name
LOAD  S-EXE 0000 0500            ; load bytes 0-500 from .EXE entry point
DEXOR1   0100 0500 0035 0000     ; XOR bytes 100-500 with key at byte 35
ZERO     0035 0001               ; set key at byte 35 to zero
CODE     0000 0500 4a4f484e      ; is checksum of bytes 0-500 = 4a4f484e?
```

CVDL description

```
; looks for two words in virus' data
:example,"painfully" AND "contrived",#
```

الشكل 3-3 يبين طريقة لوصف الفايروسات

مستقبل أمن المعلومات خلال عام 2010

مستقبل أمن المعلومات خلال عام 2010

"أمن المعلومات" مصطلح أصبح متصدراً للمناقشات والحوارات التي تدور في العديد من المجالات بدءاً من المجالات العسكرية ومروراً بالمعاملات المالية وحتى في المواقع الالكترونية والمجلات. وقد أجرى موقع WWW.NETWORKWORL.COM سلسلة من الحوارات حول موضوع "امن المعلومات" مع عدد من خبراء الأمن طلباً لإلقاء نظرة فاحصة على مستقبل تقنية المعلومات و البنية التحتية لشبكة الانترنت خلال عام 2010. هاورد شميدت – مسئول أمن المعلومات السابق في موقع السداد الإلكتروني المشهور eBay ونائب الرئيس الأمريكي لشئون حماية البنية التحتية ورئيس مؤسسة ICSA المسئولة عن اختبار واعتماد المئات من شركات أمن المعلومات – ألقى نظرة على حالة التعاملات عبر شبكة الانترنت خلال تلك السنة. تتضمن الموضوعات التي ناقشها ما يلي:

1) غزو البرمجيات الضارة للأجهزة المحمولة

سوف يشتد الخطر الذي تمثله البرمجيات الضارة على الأجهزة المحمولة والهواتف الذكية نتيجة لزيادة التطبيقات الموجهة لذلك النوع من الأجهزة بغرض تسهيل قدرة المستخدمين على القيام بأشياء أكثر ترتبط بالتجارة الالكترونية والسفر والمعاملات المالية. ومع الأخذ في الاعتبار شعور المستخدمين النهائيين بانخفاض درجة تعرض معاملتهم على الأجهزة المحمولة للخطر فلن يكن من السهل إقناعهم بالحاجة لاتخاذ تدابير حماية لأجهزتهم المحمولة كتلك الموجودة في الحاسبات المكتبية.

2) تدعيم بنية الانترنت (السحابة) كأحد عوامل التمكين الأمني

شهدت الأعوام السابقة بعض أشكال حوسبة البنية الخاصة بالانترنت لكن عام 2010 سوف يشهد تبني المزيد من أشكال تلك الحوسبة في كل القطاعات. سوف يكون لبنية الشبكة دوراً مؤثراً في توفير فرص أفضل لتطوير أمن بنية الانترنت من خلال استخدام أفضل لإدارة وتقليل الثغرات بالإضافة إلى أساليب التوثيق والتشفير القوية وزيادة التركيز على الحقوق القانونية.

3) اختبار البرامج

سوف تتطلب إجراءات الشراء المزيد من الاختبارات القوية للتطبيقات وبرامج التشغيل المثبتة في الذاكرة لضمان التقليل الشديد للثغرات الموجودة حالياً. بل قد يرتقى الأمر ليصل إلى مستوى بعض برامج الاعتماد لإظهار الوحدة بين أفضل الممارسات.

4) الالتزام بالتوثيق ثنائي العناصر

سوف يشهد عام 2010 زيادة في استخدام التوثيق ثنائي العناصر من قبل المستخدمين النهائيين بمعنى أن تبني العديد من وسائل التوثيق ثنائي العناصر الموجودة سوف ينتهي بالتوثيق القوي ليصبح القاعدة وليس الاستثناء.

أما معامل الاختبار و الاعتماد في مؤسسة" ICSA" التي يرأسها شميدت فقد أصدرت توقعاتها لمستقبل أمن المعلومات خلال عام 2010 على النحو التالي:

1) استمرار استخدام جدران الحماية المتوافقة مع مقبس التوصيل PCI

لا تزال سوق جدران الحماية الخاصة بتطبيقات الويب سوقاً صاعدة حيث تشهد بنية الانترنت إضافة المزيد منها على سبيل المثال تسعى شركة Gartner إلى انتهاء جهودها في مشروع Magic Quadrant الخاص بتحليل البيانات .

2) نمو التهديدات الموجهة للأجهزة الطرفية المرتبطة بالشبكة

مع ازدياد عدد الأجهزة المتصلة بالشبكة تتزايد فرص إحداث الأضرار. وقد زاد الاقتصاد المضطرب هذا العام أعداد فسخ عقود الموظفين والمخاطر المترتبة على ذلك من

3) زيادة التهديدات الموجهة للشبكات الاجتماعية

مع تزايد اتجاه حركة الأعمال نحو مواقع الشبكات الاجتماعية لتصل إلى العملاء ولتنشر الوعي بمنتجاتها فقد أصبحت البيانات الحساسة متوفرة ومعرضة للضرر بدرجة أكبر. وقد شهد العام الماضي 2009 انتشار واسع النطاق للدودة الإلكترونية المعروفة باسم KoobFace من خلال العديد من الشبكات الاجتماعية مثل Facebook و MySpace و Friendster و Twitter. مثال أخر هو الهجوم الذي حدث في شهر أكتوبر 2009 بواسطة أحد البرامج الخبيثة المعروف باسم Bredolab حيث أصاب ما يقرب من ثلاثة أرباع مليون من مستخدمي Facebook عن طريق إرسال رسائل كاذبة حول إعادة تهيئة كلمة المرور. لذلك يجب على أصحاب مواقع الشبكات الاجتماعية ومموليها لعب دور أكثر فاعلية في تثقيف المستخدمين بما يواجهونه من تهديدات مثل Bredolab.

4) الكشف عن عيوب نظام التشغيل Windows 7

إن الانتشار الواسع لاستخدام نظام التشغيل ويندوز يجعله الهدف الرئيسي للتهديدات الخبيثة مثل الفيروسات والديدان الالكترونية وغيرها. والدليل على ذلك هو ما حدث في شهر ديسمبر 2009 عندما أصدرت شركة مايكروسوف Microsoft رقع تحديث لثلاثة عيوب برمجية خطيرة اكتُشفت في متصفح الانترنت Internet Explorer 8.

5) اتجاه هجمات الاصطياد الالكتروني والرسائل غير المرغوبة نحو الأجهزة المحمولة

تصدر رسائل البريد غير المرغوبة من جميع أنحاء العالم إلا أن عام 2010 سوف يشهد تزايداً ملحوظاً في كمياتها الصادرة من قارة آسيا طبقاً لما لدى مؤسسة ICSA من تقارير أسبوعية حول مكافحة البريد غير المرغوب.

6) برامج مجانية لمكافحة الفيروسات وظهور برامج الاحتيال عن طريق مكافحة الفيروسات

تمثل برامج مكافحة الفيروسات المجانية قيمة عظيمة في خفض العدد المتزايد لتهديدات البرمجيات الضارة لكن على المستخدمين توخي الحذر من الاحتيال باستخدام برامج مكافحة البرمجيات الضارة أو ما يعرف باسم Scareware التي سوف تستخدمها دوائر الجريمة المنظمة لاستغلال المستخدمين النهائيين وتعطيل حواسيبهم. وقد ظهر هذا النوع من برامج الاحتيال هذا العام على موقع جريدة New York Times الإلكتروني من خلال إعلانات مزيفة عن مكافحات فيروسات.

أسطورة الأمن المطلق: The Myth of Absolute Security.

قد تكون الحماية الكاملة هي الرغبة لأي مستخدم أو مبرمج أي نظام، ولسوء الحظ لا توجد حماية" مطلقة "Absolute والتي تعني الإجابة بنعم أو لا، إذ مهما بلغت استخدام التقنيات والوسائل القوية في الحماية إلا أنها لن تصمد كثيرا في وجه مخترق يعرف تفاصيل هذه الحماية .وأحيانا يمكن أن يشكل المخترق العادي بوسائل التقليدية (السرقة،التسلل،إجبار المستخدمين على الحديث) ضررا كبيرا على النظام.

من هنا تكون الحماية نسبية دائمًا، ويمكن تقدير تلك النسبة اعتمادًا على النقاط التالية:

- أهمية المعلومات أو البيانات التي تقوم بحمايتها.
- نوعية المخترق الذي يريد الحصول على هذه المعلومات.
- نوعية المهارات والمصادر التي يجب أن تتوفر لهذا المخترق.
- القيود المفروض لاستخدام النظام بشكل صحيح Legitimate.
- .المصادر المتاحة لتطبيق الحمايةSecurity

بتقسيم مسألة الحماية بهذه الطريقة سوف تتحول المسألة من إجابة قاطعه(نعم\لا) إلى إدارة كاملة للمخاطر " Risk Management" وبالتالي تطبيق الحماية سوف يكون اعتمادا على درجة الحماية المطلوبة، ومدى أستخدامية النظام " Usability " وتكلفة تطبيق الحماية .

التكلفة الناتجة من الإصابة بالفيروسات The Cost of Malware:

للبرامج الضارة تأثير كبير من الناحية المالية" Financial" سواء كان ذلك بالنسبة للمؤسسات والشركات" Business" أو بالنسبة للمستخدمين العاديين .وبما أن الحماية كما ذكرنا هي عبارة عن إدارة للمخاطر فيجب أن تكون الخسائر الناتجة من الإصابة بهذه البرمجيات الخبيثة واضحة ومقدرة بشكل جيد. لكن عملية تقدير هذه المخاطر عملية معقدة وصعبة في أن واحد ولا يتفق عليها اثنان، فهناك خسائر واضحة " Real Cost" يمكن تقديرها كإصابة الأجهزة في أحدى الشركات بفيروس يؤدي لتعطيل العمل لعدة ساعات، في هذه الحالة يمكن تقدير الخسائر وذلك بتقدير الوقت المستهلك من غير عمل بالإضافة لحساب الوقت الذي يقوم به الفريق التقني " Support Stuff" للقضاء على الفيروس .أما في حالة أصاب الفيروس بنك أو مؤسسة تجارية فعملية التقدير لن تكون دقيقة إطلاقًا حيث هناك " Hidden Cost" لا يمكن معرفتها ولا تقديره، فسمعة ذلك البنك على سبيل المثال سوف تنخفض ويقل عدد عملاء البنك ومثل هذه الأضرار لا يمكن تقديرها بشكل واضح.

من جانب المستخدم العادي Users فيمكن أن تتسبب له الـــــ Malware بفقدان معلوماته الشخصية ككلمات المرور ورقم الحساب البنكي ومثل هذه المعلومات التي قد يخسر المستخدم من كشفها.

استراليا : استخدم الحماية وإلا سنقطع الانترنت :

أصبحت برامج الحماية من الفيروسات ضرورة لا بد منها خصوصا مع ازدياد اعتمادنا على الإنترنت في إدارة العديد من الأمور من فواتيرنا إلى حساباتنا البنكية ، ولأن النصب على الإنترنت يعتبر من أكثر النشاطات الإجرامية انتشارا على الإنترنت فإن الحكومة الأسترالية تنصح بقطع الإنترنت عن المستخدم الذي لاستخدم برامج حماية.فقد جاء في تقرير أمني حكومي متعلق بالاختراق والحماية بأن عبئ حماية البيانات يجب أن لا يكون مهمة شركات الإنترنت فقط فالمستخدم مسئول أيضا عن حماية بياناته الشخصية ويجب أن يتم تثقيف المستخدم حول كيفية حماية بياناته من الاختراق.

ومن ضمن الأمور التي ذكرت في هذا التقرير هو أنه في حالة اكتشاف مستخدم مصاب بفيروس ما فمن المفضل أن يتم فصل الإنترنت عنه لحين تنظيف النظام، وهي خطوة تهدف إلى حماية المستخدم نفسه وفي نفس الوقت الشبكة نفسها.هذه القواعد التي شملها تقرير الحماية المقدم للحكومة مازالت قيد الدراسة وستخضع للتحسين من أجل جعل الإنترنت أكثر أمناً (في أستراليا بالطبع)

ثغرة في جميع برامج مكافحة الفيروسات:

قامت مجموعة من الباحثتين الأمنيين بنشر دراسة تشير إلى وجود مشكلة في برامج الحماية من الفيروسات قد تسمح للمخترقين بتخطي أنظمة الحماية بسهولة والمثير في الأمر أن هذه المشكلة ليست محصورة ببرنامج معين بل هي تطال جميع برامج حماية الفيروسات.

المشكلة هي في الطريقة المتبعة من قبل برامج الحماية (أو أغلبها) فبرامج الحماية تقوم بوضع ما يشبه نقاط التفتيش أو إضافات بين البرامج وبين نواة ويندوز بحيث تقوم بالتحقق من أي شفرة يتم تنفيذها على مستوى النواة قبل أن تسمح لها بالتنفيذ الفعلي، ولكن ما قام به الباحثون هو أمر يشبه أفلام الخيال العلمي.

فقد قام الباحثون بعمل برنامج يقوم بإرسال شفرة نظيفة إلى أدوات التحقق التي تقوم بحماية نواة النظام وهذا الأمر سيؤدي إلى تجاوز أنظمة الحماية والسماح لها بالتنفيذ، وقبل أن يتم التنفيذ الفعلي للشفرة فسيقوم البرنامج باستبدال الشفرة النظيفة بآخري ضارة ولن يكون بإمكان برنامج الحماية عمل أي شيء وقتها لحماية نظامك.

هذه الطريقة لاحتاج إلى حساب المدير أيضا فبالإمكان تنفيذها عبر حساب مستخدم عادي وسيكون لها نفس الأثر وقد أوضح الباحثون أنه بالإمكان استغلال هذه المشكلة من أجل إن يقوم البرنامج بالاستيلاء على النواة وإزالة برامج الحماية من الفيروسات أو استبدال ملفاتها.

لكن أحد العيوب التي تعاني منه هذه الطريقة (في الوقت الحالي) هو انها تحتاج إلى أن يتم تشغيل ملف تنفيذي على الجهاز من أجل إتمام العملية وهي تحتاج إلى كمية شفرة كبيرة لكنها مسألة وقت قبل أن نرى نسخاً محسنة من هذه الثغرة وبحجم أقل وفعالية كبيرة.

هذه الدراسة شملت حوالي 34 منتج حماية من نورتن وكالسبو وغيرها وكل هذه البرامج لم تستطع الحماية من هذه المشكلة وهي تطال نسخ ويندوز كلها مما يعني آن على مصنعي برامج الفيروسات أن يعيد التفكير في كيفية حماية النظام.

.

أبحاث وتقارير شركة سيمانتك للأعوام الأخيرة

في تقرير سيمانتك في عام 2009

أوضحت وقتها انه بمقارنة عام 2008 فقد زادت نسبة البرمجيات الضارة بمعدل 71 % هذا يعني عمليا أن 51 ٪ من جميع قضايا الأمن تتبع أي وقت مضى من قبل الشركة وردت في هذا العام وحده .ويعقد هذا ليكون ناجما عن زيادة توافر الأدوات التي تسمح للأفراد لتقديم واستخدام البرمجيات الخبيثة الخاصة بهم.
واحد من اللاعبين الرئيسيين في هذا المجال في العام الماضي كان مبرمج للبرمجيات الخبيثة "زيوس." ويتم تسويق هذه البرامج وبيعها للاسيبرانية المجرمين وكثيرا ما تستخدم لخلق برمجيات الخبيثة "« بوت نت »" أو شبكات من أجهزة الكمبيوتر التي تقوم إصابة ثم استخدم لأغراض غير المرغوبة أو سرقة البيانات.
وللمزيد
http://news.suite101.com/article.cfm/symantecs-2009-security-report-shows-a-71-increase-in-malware-a227776

وفي تقرير عام 2010

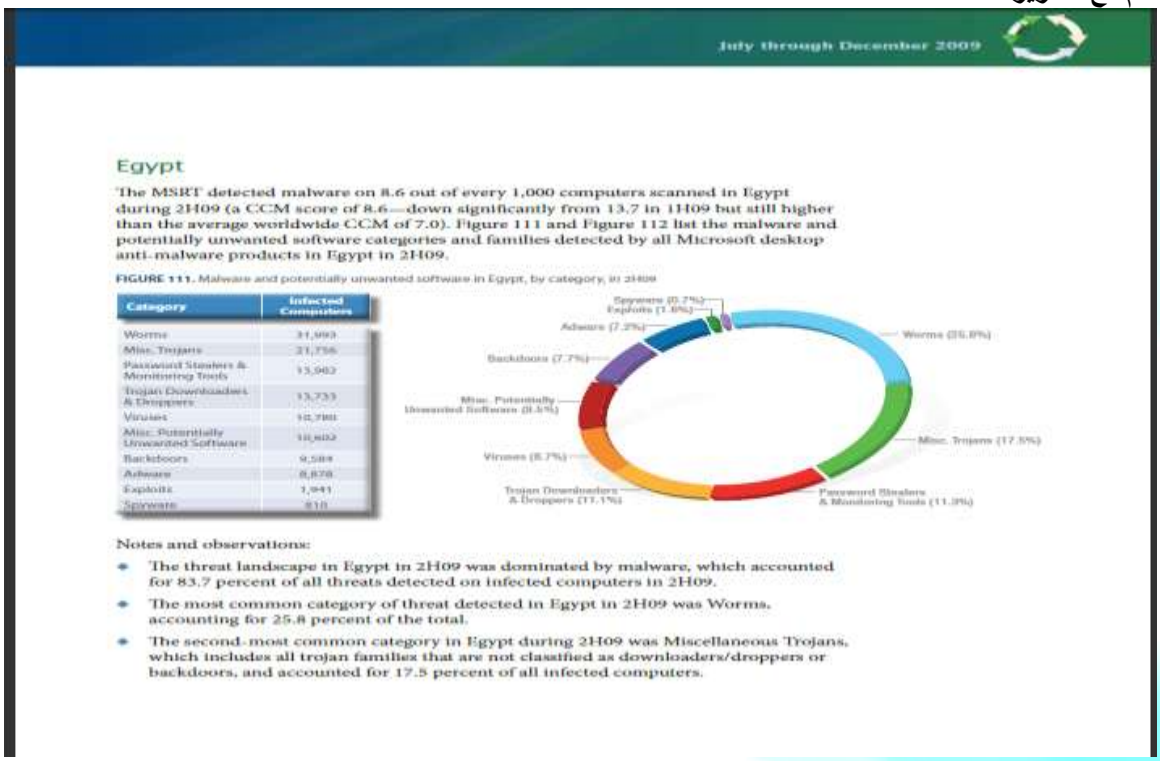
أوضحت انه كانت الولايات المتحدة أول دولة للنشاط ضار في هذا الربع ، وهو ما يمثل 30 في المائة من المجموع.
النشاط الخبيثة حسب البلد
هذا وسوف متري تقييم البلدان التي أكبر قدر من النشاط الخبيثة وقعت أو نشأت .الترتيب
وتتحدد عن طريق حساب متوسط نسبة النشاط الخبيثة التي نشأت في كل بلد.
الولايات المتحدة هي البلد الذي يحتل أعلى مرتبة لنشاط ضار هذا الربع ، وهو ما يمثل 30 في المائة من المجموع
)الجدول 1 .(ضمن قياسات فئة معينة ، في المرتبة الأولى في الولايات المتحدة في جميع الفئات.

Rank	Country	Percentage	Malicious Code Rank	Spam Zombies Rank	Phishing Website Hosts Rank	Bots Rank	Attack Origin Rank
1	United States	30%	1	1	1	1	1
2	China	6%	3	7	7	5	2
3	Germany	6%	16	2	2	2	3
4	Italy	4%	14	10	12	4	7
5	Brazil	4%	6	11	9	6	6
6	India	4%	2	17	13	20	12
7	United Kingdom	3%	5	5	5	13	5
8	Taiwan	3%	23	16	17	3	9
9	Russia	3%	18	6	6	10	10
10	France	3%	18	6	6	10	10

ميكروسوفت في امن المعلومات (أبحاث)

وعند قراء بحث ميكروسوفت الأخير July through December 2009 وقد ركزت التفكير على دولتنا الحبيبة مصر لرؤية النسب والمؤشرات للبرمجيات الضارة

فوجدت انه جاء تقريرها جاءت النسب كبيرة جدا في الديدان التي تصيب الأجهزة بمصر وكان اغلبها من النوع win32 وأترككم مع التقرير



وجاءت عائلات الفيروسات والديدان وكانت 25 عائلة ذكرتها ميكروسوفت كما في الصورة التالية :

وقد عرضت ميكروسوفت ملاحظتها واهم ما انتشر بمصر من برمجيات ضارة في الصورة التالية

Notes and observations:

- **The two most prevalent threats in Egypt during 2H09 both target players of online games and attempt to steal passwords and other player credentials. Win32/Taterf, the number one threat in Egypt and worldwide, is a family of worms that spread via mapped drives to steal login and account details for popular online games. Win32/Frethog, the second-most prevalent threat in Egypt and the sixth worldwide, is a large family of password-stealing trojans that target confidential data, such as account information, from massively multiplayer online games, like World of Warcraft.**
- **Three of the eight most prevalent threats in Egypt during 2H09 (Win32/Hamweq, Win32/Conficker and Win32/Autorun) spread via mapped drives with weak or missing passwords, removable media (such as USB drives), or a combination of both.**
- **Win32/Sality was the seventh-most prevalent family in Egypt in 2H09, but it was not present in the top 25 threats worldwide. Win32/Sality is a family of polymorphic file infectors that target Windows executable files with the extensions .src or .exe. The family may also execute a damaging payload that deletes files with certain extensions and terminates security-related processes and services.**

Encyclopedia

Win32/Hamweq: A worm that spreads through removable drives, such as USB memory sticks. It may contain an IRC-based backdoor enabling the computer to be controlled remotely by an attacker.

Win32/Conficker: A worm that spreads by exploiting a vulnerability addressed by Security Bulletin MS08-067. Some variants also spread via removable drives and by exploiting weak passwords. It disables several important system services and security products, and downloads arbitrary files.

Win32/Autorun: A worm that attempts to spread by being copied into all removable drives.

http://www.microsoft.com/av

الخاتمة

وهكذا نكون قد وصلنا إلى نهاية هذا البحث المتواضع الكمال لله وحده ، وهذا البحث ومهما طال عدد صفحاته فما هو إلا مجرد بداية في حقل كبير ويحتاج للمزيد من الإسهام في البحوث والدراسة ، لذلك على الباحث الذي يريد الخوض في هذا المجال أن يكمل من حيث توقف هذا البحث ويدرس الأمور التي يجب أن توضح وتفسر بشكل أكبر و أوضح.
وما كان في هذا البحث من صواب أو جزالة خطأ فهو من فضل الله والشكر عائد له
أما ما فيه من خطأ وتقصير فهو من نفسي وعائد إلى
ويجب إن يستغل المجتمع العربي أفكاره في الاختراع وليس لاستهلاك واستخدام خامات الغرب دون وعى بها وإذا سئلنا العرب عن السبب الذي يمنعنا من اللحاق بهم ماذا سوف نقول لهم ؟ إذا كان لأي شخص عربي إجابة إنا بانتظار رده !!!

References المراجع

مواقع الانترنت

http://www.microsoft.com/protect/fraud/phishing/reduce.aspx
http://onecare.live.com/site/en-US/center/howsafe.htm
- http://3asfh.net
- http://elnimrelmasry.blogspot.com

www.amoaly.com
ar.wikipedia.org
/http://coeia.edu.sa
http://www.sh1m.com/vb/showthread.php?t=14955
http://www.moheet.com/show_files.aspx?fid=369933
http://www.microsoft.com/athome/security/bank/RecognizeVirus.mspx#top
http://www.teedoz.com
http://news.suite101.com/article.cfm/symantecs-2009-security-report-shows-a-71-increase-in-malware-a227776
http://threatpost.com/en_us/blogs/introduction-malware-analysis-042810
http://win32assembly.online.fr
http://sudancs.com
http://at4re.com
http://arabteam2000.com

المراجع المتعلقة بالفيروسات والانتى فيروس

Sushil Jajodia, Computer Viruses and Malware, Springer, Canada, 2006.
Peter Szor, the Art of Computer Virus Research and Defense, Addison Wesley Professional, 2005.
Ed Skoudis and Lenny Zeltser, Malware: Fighting Malicious Code, Prentice Hall PTR, 2003.
Eric Filiol, Computer viruses: from theory to applications, Springer, France, 2005
.

مراجع لبعض الخوارزميات والبيانات

Jeffrey Richter and Christophe Nasarre, Windows via C/C++, Microsoft Press, 2008.
Johnson M. Hart, Windows System Programming, Addison Wesley Professional, 2004.

المراجع الخاصة بالابحاث

Microsoft Security Intelligence Report Volume 8
Microsoft Security Intelligence Report Volume7
Symantec IntelligenceQuarterly January - March 2010
Understanding Anti-Malware Research and Response at Microsoft
Understanding Anti-Malware Technologies
Malware Research Group Rogue Software Execution prevention test January 2010

كتاب عرب

Wajdyessam
Egyptian tiger