دراسة عن البرمجيات الضارة وتقنيات التطهير

Study about malicious software and disinfection techniques

إعداد:
أحمد البرواري

بسم الله الرحمن الرحيم

﴿ إِنَّمَا يَخْشَى اللَّهَ مِنْ عِبَادِهِ الْعُلَمَاء إِنَّ اللَّهَ عَزِيزٌ غَفُورٌ ﴾ .

صدق الله العظيم
سورة فاطر / الآية: ٢٨

المبحث الأول
مدخل إلى علم البرمجيات الضارة

مصطلح البرنامج الضار (الفيروس) Malware term (the virus):

إن أول من أطلق مصطلح الفيروس على فيروسات الكمبيوتر هو الباحث فريد كوهين Fred Cohen من جامعة Lehigh سنة ١٩٨٤ ، من خلال دراسة أكاديمية قام بها بمساعدة مشرفه ادلمان Adelman. وقد قام فريد باقتباس هذه التسمية من أحدى روايات الخيال العلمي .
فالباحث فريد كوين هو الأب لمصطلح فيروس الكمبيوتر Father of Computer Virus

تاريخ البرمجيات الضارة Malware history:

يحتوي الجدول الآتي على أسماء أهم واشهر البرمجيات الضارة وللفترة الزمنية بين سنة ١٩٧٠ إلى سنة ٢٠٠٨.

اسم البرنامج الضار	السنة
١- Creeper	١٩٧٠
٢- Elk Cloner	١٩٨٢
٣- Brain	١٩٨٦
٤- Aids Trojan	١٩٨٩
٥- Concept	١٩٩٥
٦- CIH - Back Orifice	١٩٩٨
٧- Melissa	١٩٩٩
٨- I love you	٢٠٠٠
٩- Code red – Nimda	٢٠٠١
١٠- Klez	٢٠٠٢
١١- Slammer	٢٠٠٣
١٢- My Doom	٢٠٠٤
١٣- Conficker	٢٠٠٨
١٤- Stuxnet	٢٠١٠

وفيما يلي نبذة مختصرة عن كل برنامج ضار ذُكر في الجدول.
١- Creeper: يعتبر هذا الفيروس هو أول فيروس في تاريخ الحواسيب ، وتمت برمجته من قبل شاب يدعى بوب توماس والذي يعمل لشركة تدعى BBN .
فقد قام الفيروس بإصابة أجهزة شركة (DEC) والتي تعمل على نظام Tenex.
٢- Elk Cloner: تمت برمجة هذا الفيروس من قبل الطالب ريتش سكرينتا ، حيث يقوم الفيروس بإصابة أجهزة وأقراص Apple II.
٣- Brain: قام مبرمجان من باكستان ببرمجة هذا الفيروس لحماية برامجهم الطيبة من القرصنة
٤- Aids Trojan: يقوم هذا التروجان بإخفاء المجلدات وتشفير أسماء جميع الملفات في الدليل "C" بعد كل عملية إقلاع للنظام ، مما يجعل نظام التشغيل غير قابل للاستعمال .
٥- Concept: يعتبر هذا الفيروس من أول فيروسات المايكرو التي تصيب ملفات برنامج مايكروسوفت وورد.

٦- CIH: يعرف هذا الفيروس بالفيروس شيرنوبل نسبة إلى الكارثة التي أصابت المفاعل الاوكراني . مبرمج هذا الفيروس هو تايواني الأصل ، ويعتبر هذا الفيروس من اخطر الفيروسات على الإطلاق وذلك بسبب خروج الفيروس من عملية الأضرار بالمكونات البرمجية للحاسب (كما هو الحال في الفيروسات الأخرى) إلى الإضرار بالمكونات المادية . حيث يقوم الفيروس بإصابة نظام ألـ BIOS وجعل الحاسوب غير قابل للإقلاع أبداً.

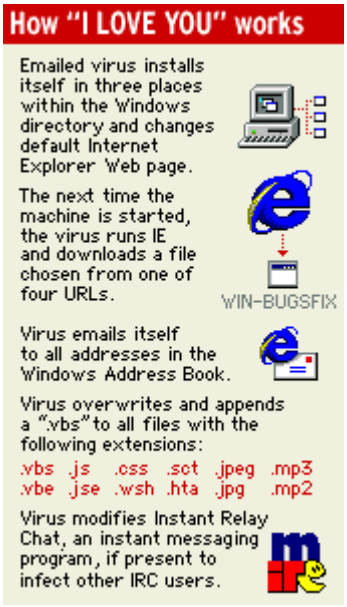
٧- Back orifice: هو عبارة عن أداة اختراق للتحكم بالأجهزة عن بعد باستخدام معمارية (عميل+خادم) . تم تصنيف هذا الأداة على أنها برنامج ضار عند باحثين الفيروسات . تمت برمجة الأداة من قبل مجموعة من القراصنة والذين اطلقو على أنفسهم (جماعة البقرة الميتة the cult of - dead cow).

٨- Melissa: تسبب هذا الفيروس بخسائر مالية تقدر بـ 80 مليون دولا . حيث يقوم الفيروس بإصابة ملفات برنامج مايكروسوفت وورد . بالإضافة إلى الانتشار عن طريق قيام الفيروس بإرسال نفسه إلى أول خمسين شخص موجودين في قائمة برنامج Outlook express . وفي نفس العام تم القبض على مبرمج الفيروس وتم سجنه في سجن فيدرالي لمدة عشرين شهر.

شكل رقم (١) - طريقة عمل فيروس melissa

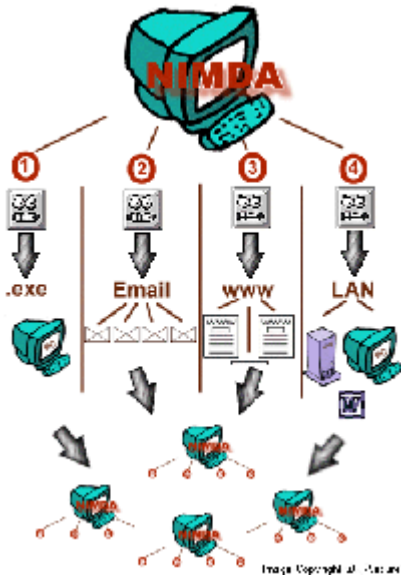
٩- I love you: يستخدم هذا الفيروس الطريقة ذاتها التي يستخدمها فيروس ميليسا . حيث تسببت هذا الفيروس بإصابة حوالي مليون جهاز كمبيوتر خلال ليلة واحدة. كما يقوم الفيروس بجمع أسماء المستخدمين وكلمات المرور الموجودة في الحاسوب المصاب ، وإرسالها إلى مبرمج الفيروس.

وقد تبين فيما بعد بأن مبرمج الفيروس هو شاب فلبيني الأصل .



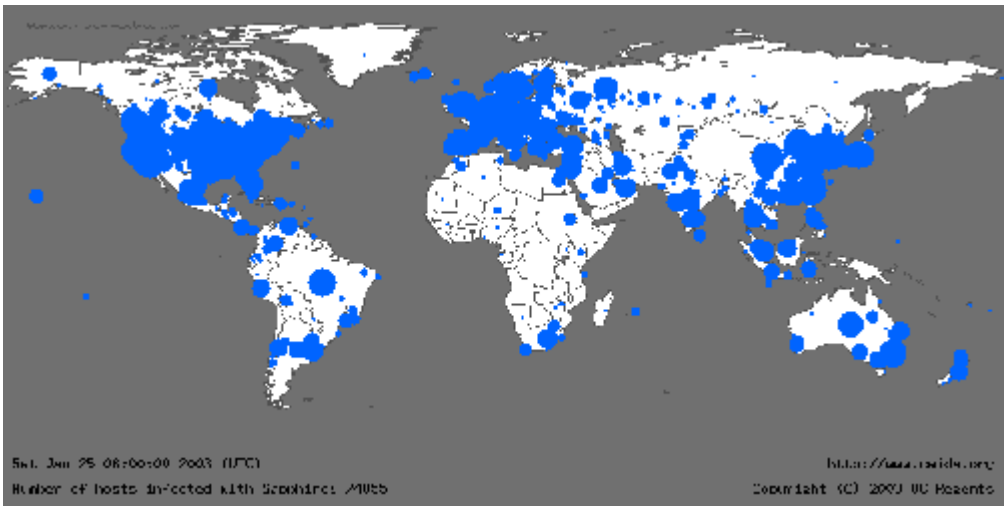
شكل رقم (٢) - طريقة عمل فيروس i love you

١٠- Code Red: تمت برمجة هذه الدودة من قبل مبرمجين صينيين .ردا على هبوط طائرة تجسس أمريكية على الأراضي الصينية . حيث أصابت هذه الدودة ألاف الأجهزة التي تعمل بنظام window nt 2000، واستخدمت كل هذه الأجهزة من قبل الدودة لتنفيذ هجوم نكران الخدمة DoS ضد أجهزة البيت الأبيض .
وقدرت الخسائر التي سببتها الدودة بحوالي ٢ بليون دولار.
١١- Nimda: ظهرت هذه الدودة بعد أيام من أحداث ١١ سبتمبر ، وقُدر عدد الأجهزة التي أصيبت بالدودة بمئات الأجهزة ، حيث تستخدم الدودة خمسة طرق للانتشار والتكاثر في نفس الوقت.



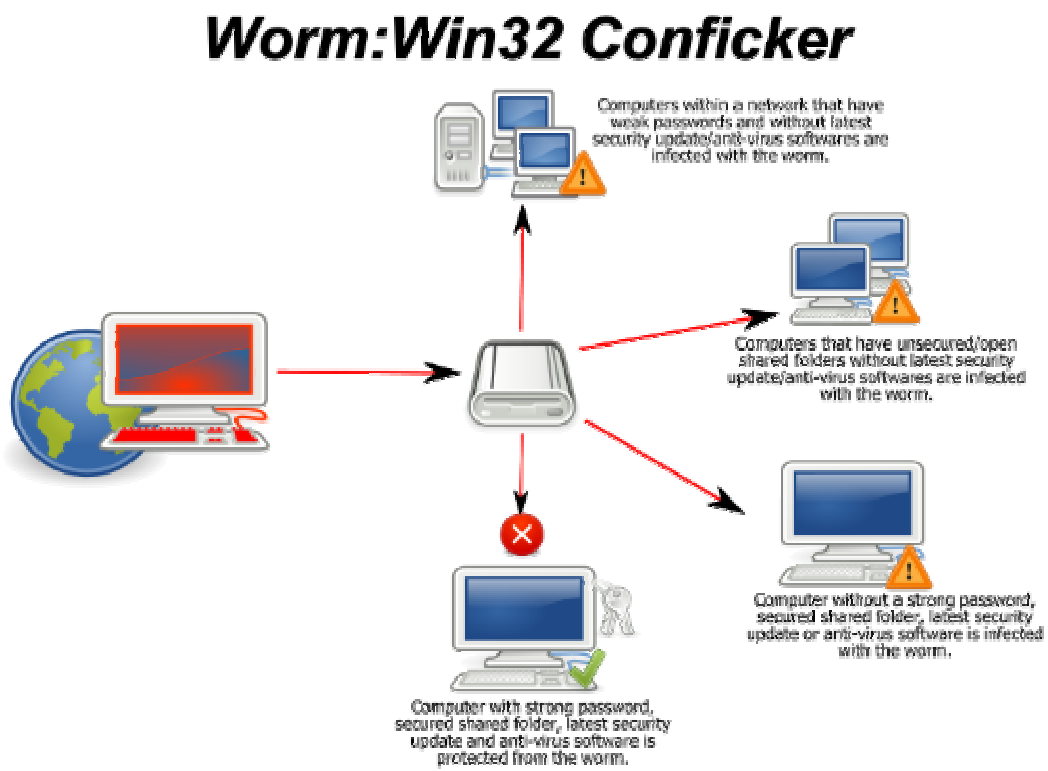
شكل رقم (٣) - طريقة عمل دودة nimda

١٢- Klez: تقوم هذه الدودة بالإضافة إلى الانتشار عبر البريد الالكتروني بعدة وظائف ، منها مسح محتويات الملفات وملئها بالاصفار . بالإضافة إلى تعطيل برامج الحماية الموجودة في الجهاز المصاب.
١٣- Salmmer: تعتبر هذه الدودة أسرع دودة عرفها التاريخ . حيث قامت بإصابة مئات الأجهزة في ظرف ثلاث ساعات . بالإضافة إلى تخريب شبكات وأجهزة الأعمال والتجارة وأجهزة الصرف الآلي ATM.



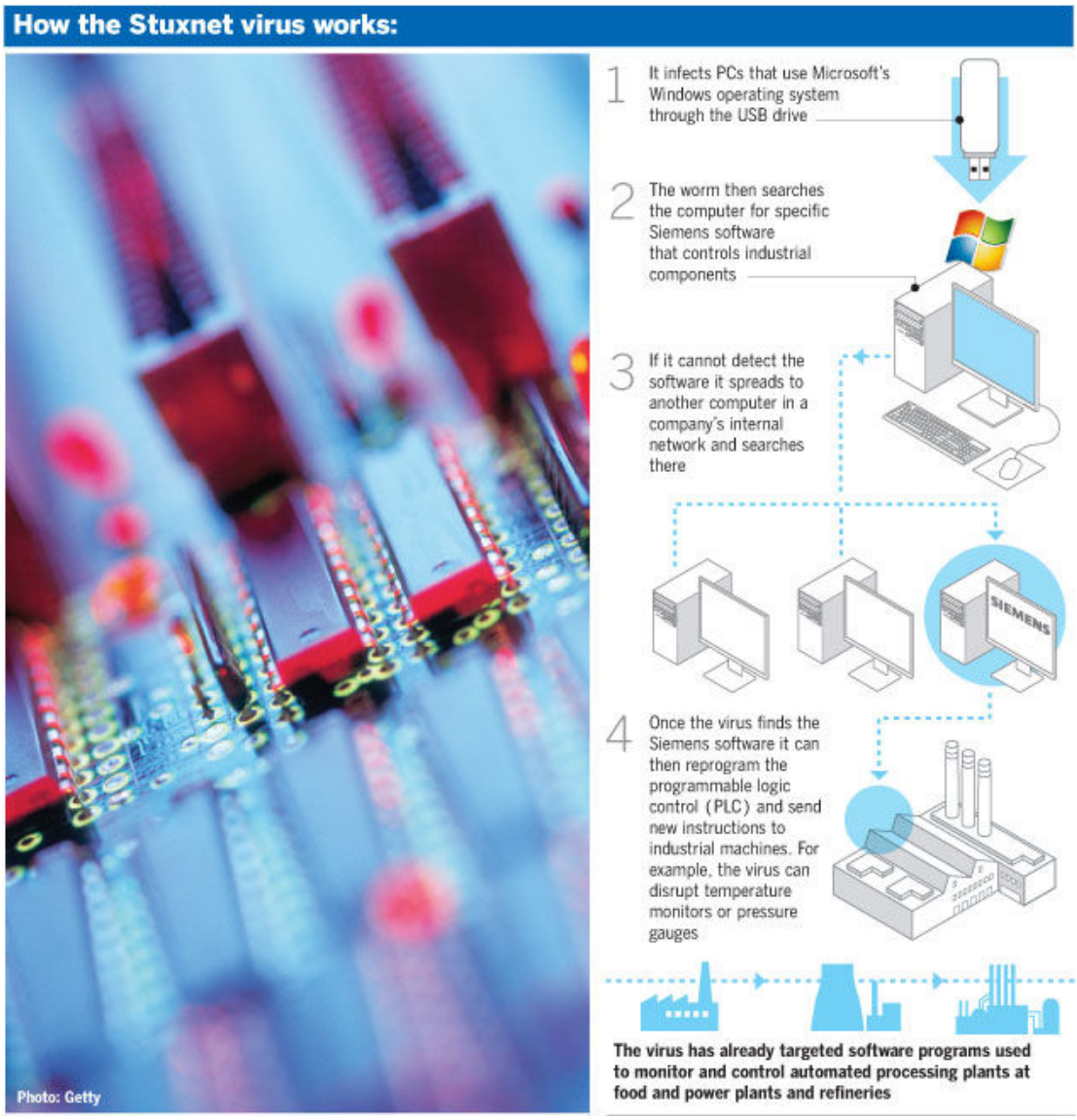
شكل رقم (٤) – انتشار دودة slammer

١٤- My Doom: تستخدم هذه الدودة أسلوب الهندسة الاجتماعية والخدع النفسية لدفع المستخدمين إلى فتح الملف المرفق المصاب بالدودة. والذي أدى بدوره إلى الانتشار الكبير للدودة.
١٥- Conficker: تستخدم هذه الدودة طرق متطورة للانتشار عن طريق استغلال الثغرات الموجودة في برنامج ألـ NetBIOS الذي يعمل على نظام ويندوز.



شكل رقم (٥) - طريقة عمل دودة conficker

١٦- Stuxnet: تم اكتشاف هذه الدودة في منتصف شهر حزيران سنة ٢٠١٠ ، وتعمد هذه الدودة إلى استهداف أنظمة السيطرة الصناعية كأنظمة التحكم بأنابيب الغاز ومحطات الطاقة في المؤسسات النووية . حيث استهدفت الدودة أنظمة التحكم بالطاقة في المؤسسات النووية في عدد كبير من الدول بغرض إعاقة عمليات تخصيب اليورانيوم عن طريق تعطيل أجهزة الطرد المركزي.



شكل رقم (٦) - طريقة عمل دودة stuxnet

تعريف البرنامج الضار Malware definition:

البرنامج الضار: هو عبارة عن برنامج اعتيادي ولكنه مصمم لغرض إلحاق الضرر بأجهزة الحاسوب .

وللبرنامج الضار القدرة على الانتشار وإصابة حواسيب أخرى إما عن طريق إصابة الملفات أو عن طريق إصابة وسائط الخزن القابلة للإزالة كالأقراص الليزرية والمرنة ووسائط الذاكرة الضوئية (Flash Memory).

الدوافع التي تقف وراء تصميم البرامج الضارة Impetuses behind malware design:

لابد من وجود دوافع لكل عمل يقوم به الإنسان . وما دامت البرامج الضارة من صنع البشر فلا بد من وجود دوافع تقف وراء برمجة وتصميم هذا النوع من البرامج..

ويمكن تلخيص هذه الدوافع بما يأتي:
- الهواية والمرح.
- جني و سرقة الأموال.
- الفضول والتجسس على خصوصيات الآخرين.
- الابتزاز والانتقام.
- الشهرة وإبراز القدرات الفكرية.
- تحدي ألذات كما أثبتت بعض الدراسات النفسية
- تسويق البرامج المضادة للفيروسات، كما في بعض الشركات التي تقوم بتصميم الفيروسات بهدف لفت الأنظار نحو برامجها.
- لأغراض التجارب والبحث العلمي
- إشهار أو تخليد شخص أو شي معين كما حصل مع الفيروس الذي سمي باسم راقصة (ميليسا) ، بالإضافة إلى الفيروس الذي سمي باسم الرسام المشهور مايكل أنجلو.
- حماية الحقوق الفكرية . كفيروس brain الذي صممه مبرمجان من باكستان لحماية برامجهما من القرصنة.
- إرسال رسائل سياسية.

أعراض الإصابة بالبرامج الضارة Malware infection symptoms:

- بطء في أداء الذاكرة بالإضافة إلى أن البرامج أو العمليات تأخذ وقتا طويلا عن المعتاد عند تشغيلها.
- حدوث نقص في ذاكرة القرص الصلب دون سبب معين.
- ظهور رسائل أو رسائل خطأ غريبة.
- زيادة في حجم الملفات التنفيذية.
- ظهور ملفات غريبة ليست معروفة للمستخدم.
- البرامج تعمل بشكل شاذ أي تعمل من تلقاء نفسها دون تدخل مسبق من المستخدم.
- الجدار الناري يظهر رسالة بان برنامج معين يحاول الاتصال بالانترنيت (وهذا البرنامج لم يتم فتحه من قبل المستخدم).
- نظام التشغيل لا يتم تحمليه مع بداية تشغيل الحاسوب.
- حذف ملفات أو مجلدات لم يتم حذفها من قبل المستخدم.
- متصفح الانترنيت يتصرف بغرابة (على سبيل المثال عدم تمكن المستخدم من غلق مصتفح الانترنيت).
- مصباح القرص الصلب يضيء بشكل مستمر من دون تشغيل أي برنامج أي في حالة سكون نظام التشغيل.
- إخبار المستخدم من قبل اصداقاءه عن استلامهم رسائل الكترونية ، ولكنه لم يرسل شيأ.

وسائط انتقال البرمجيات الضارة Malware transport media:

تنتقل وتنتشر البرمجيات الضارة من حاسوب لأخر عن طريق الوسائط الآتية:
- وسائط الخزن المؤقتة كالفلاش ميموري أو الأقراص المرنة.
- مواقع الانترنيت.Internet websites
- البريد الالكتروني E-Mail
- برامج الدردشة IM.
- عبر الشبكات

دورة حياة البرنامج الضار Malware life cycle:

١- تصميم البرنامج الضار: مرحلة تصميم البرنامج الضار أو برمجته تعد المرحلة الأولى في دورة حياته . إذ تبدأ بقيام احد المبرمجين أو القراصنة بتصميم برنامج ضار وإطلاق اسم معين له. ففي السابق كان تصميم البرامج الضارة مقتصراً على المبرمجين المتقدمين . أما الآن فأي شخص يمتلك معرفة ولو قليلة بالبرمجة ، يستطيع تصميم برمجيات ضارة أو فيروسات ، وذلك بسبب ظهور اللغات العالية المستوى (High level languahes - HLL) والتي سهلت علمية البرمجة كثيراً.

٢- التكاثر أو الانتشار (Reproduction): تتضاعف وتنتشر البرمجيات الضارة ، وأي برنامج ضار مصمم بشكل جيد سيستمر فترة طويلة بالانتشار والتضاعف قبل التنشيط .

٣- التنشيط (Activation): تنشط البرامج الضارة التي لديها وظائف تخريبية بتحقق شرط معين . على سبيل المثال تنشيط البرنامج الضار في تاريخ أو وقت معين ، ففي هذه الحالة يطلق على البرمجيات الضارة من هذا النوع باسم القنبلة المؤقتة Timer Bomb.

أو التنشيط عند حدوث إجراء معين من قبل المستخدم ، ويطلق عليها حينئذ باسم القنبلة المنطقية Logic Bomb.

٣- الاكتشاف Discovery: هذه المرحلة . لا تأتي بعد مرحلة التنشيط دائما ، وتبدأ هذه المرحلة باكتشاف البرنامج الضار من قبل شركات مضادات الفيروسات . وتستمر هذه المرحلة مدة سنة على الأقل قبل تصنيف البرنامج الضار كتهديد لمجتمع الحواسيب.

٤- الاستيعاب (Assimilation): يقوم مطوري البرامج المضادة في هذه المرحلة بإضافة التحديثات اللازمة لبرامجهم لكي تتمكن من اكتشاف البرنامج الضار الجديد . وتستغرق هذه المرحلة مدة من يوم إلى ستة اشهر اعتمادا على المطور ونوع البرنامج الضار.

٥- الاستئصال (Eradication): إذا قام عدد كافي من المستخدمين بتحديث برامجهم المضادة ، سيتم في هذه الحالة ابادة البرنامج الضار.

لحد الآن لم يختفي برنامج ضار بشكل كامل . فهناك برامج ضارة تتوقف لمدة طويلة دون أن تصنف كتهديد رئيسي ولكنها لم تختفي بشكل كامل.

بيئات البرمجيات الضارة Malware environments:

للبرمجيات الضارة منصات وبيئات مختلفة . فمنها ما هو مصمم ليعمل على أنظمة ويندوز ومنها ما هو مصمم للعمل ضمن بيئات أخرى كأنظمة لينكس أو ماكنتوش .

وفيما يلي سرد لأشهر البيئات التي يمكن للبرمجيات الضارة أن تعمل ضمنها:

أسم البيئة	الوصف
W16	بيئة نظام تشغيل Windows 16-bit
W32	بيئة نظام تشغيل Windows 32-bit
W64	بيئة نظام تشغيل Windows 64-bit
Linux	بيئة نظام تشغيل لينكس
Unix	بيئة نظام تشغيل يونكس
DOS	بيئة نظام الدوس
Boot	بيئة قطاع الإقلاع
SymbOS	بيئة نظام تشغيل سمبيان لأجهزة الجوال
AndroidOS	بيئة نظام تشغيل اندرويد لأجهزة الجوال
PalmOS	بيئة نظام تشغيل بالم لأجهزة الجوال

WinCE	بيئة نظام تشغيل ويندوز سي اي لأجهزة الجوال
MSIL	بيئة Microsoft Intermediate Language runtime
INF	بيئة سكربتات الـ INF
VBS	بيئة سكربتات الـ VBS
Bat	بيئة سكربتات الـ Bat
PHP	بيئة سكربتات لغة PHP
HTML	بيئة سكربتات لغة HTML
Perl	بيئة سكربتات لغة Perl
JS	بيئة سكربتات لغة Java
SH	بيئة سكربتات لغة الـ Shell Code
MacOS	بيئة نظام ماكنتوش
Solaris	بيئة نظام سولاريس

أنواع البرمجيات الضارة Malware types:

١- الفيروس: عبارة عن برنامج يقوم بحقن نفسه في الملفات التنفيذية كوسيلة للتكاثر والانتشار ، فهذا النوع لا يستطيع العمل بشكل مستقل إلا أن يلصق نفسه بالملف التنفيذي . ففي هذه الحالة سيتم تشغيل الفيروس مع كل عملية تشغيل لملف مصاب .
وهناك أنواع وتقسيمات كثيرة للفيروسات . سيتم شرحها والتفصيل فيها لاحقا.
ولكن يجب الإشارة الى أن النسخة الأولى من الفيروس التي يتم نشرها في بداية الأمر من قبل كاتب الفيروس والتي لم تصيب أي ملف بعد ، يطلق عليها اسم الجرثومة (Germ).
٢- الديدان: وهي برامج ضارة تعمل بشكل مستقل ولها القدرة على التضاعف والتكاثر عبر الويب ، ويندرج تحت هذا النوع عدة أنواع اخرى ، منها:
- دودة الايميل: وهي دودة لها القدرة على الانتقال والانتشار عبر ايميلات المستخدمين وذلك من خلال إرسال نفسها عبر رسائل البريد الالكتروني كملف مرفق أو رابط مصاب بالدودة.
- دودة IM: وهي تسمية لكل دودة تنتشر عبر رسائل برامج المحادثة (Internet Messengers).
- دودة الشبكات: وهي دودة لها القدرة على الانتشار من شبكة لأخرى . وتستخدم الدودة تقنيات مختلفة للانتشار منها استغلال ثغرات معينة كثغرة Buffer Overflow التي استُغلت من قبل دودة Slammer . ويمكن للدودة أن تستغل ثغرة للهجوم على الأجهزة المحتوية على كلمات مرور ضعيفة أو افتراضية . وهناك ديدان تستخدم مشاركة الملفات للانتشار عبر أجهزة شبكة معينة.
- دودة الـ (IRC): وهي الدودة التي تستخدم شبكات الـ (Internet Relay Chat) للانتشار ونسخ نفسها إلى أجهزة المستخدمين.
٣- أحصنة طروادة: هي برامج غالبا ماتبدو أنها برامج شرعية ولكن بعد تشغيلها تقوم بتنفيذ أوامر دون علم المستخدم ، وهناك أنواع فرعية أخرى يمكن حصرها ضمن خانة أحصنة طروادة وهي:
- الباب الخلفي (Backdoor): كل برنامج يقوم بمساعدة المخترق في الولوج واختراق نظام معين يعتبر بابا خلفيا سوءا بتخطي برامج الحماية أو بفتح منفذ معين .
- مُسجل لوحة المفاتيح (Keylogger): يقوم هذا النوع من البرامج الضارة بتسجيل عنوان كل زر يتم الضغط عليه من قبل المستخدم ثم يقوم بإرسال تقرير إلى المخترق يحتوي على معلومات كاملة حول ما تم ضغطه من أزرار في جهاز الضحية ... وفي هذه الحالة سيتمكن المخترق من سرقة كلمات المرور التي يستخدمها الضحية .

- مختلس كلمات المرور (PWS): وهي اختصار لـ (Password Stealer). حيث يقوم هذا النوع بمهمة سرقة أي كلمات مرور محفوظة في جهاز الضحية.
- المغرق (Spammer): هو برنامج يقوم بإرسال مجموعة هائلة من الرسائل إلى بريد الكتروني معين إما لغرض تدميري أو لغرض دعائي.
وهناك نوع خاص لهذا النوع من البرامج الضارة ويسمى (SMS-Spammer) حيث يقوم بتنفيذ هجوم من نوع Spam على أجهزة الجوال وذلك بإرسال مجموعة كبيرة من الرسائل القصيرة إلى رقم معين . لغرض الإزعاج أو تعطيل أجهزة جوال المستخدمين.
- برمجيات التجسس Spyware : يقوم هذا النوع بسرقة وجمع معلومات عن جهاز الضحية لغرض التجسس.
- برمجيات الـ (Bot): وهي برامج ضارة يقوم المهاجم أو المخترق بزرعها في أجهزة الضحايا وذلك للتحكم بها عن بعد ، ويطلق على شبكة ألأجهزة المصابة بهذا النوع من البرامج الضارة تسمية (BotNet) وكل جهاز في هذه الشبكة يسمى (Zombie) ، حيث يستفيد المخترق من هذه الشبكة المصابة بالتحكم بها عن بعد واستخدامها لشن هجمات من نوع (Spam) أو هجمات من نوع (DDoS).
- مضاد الفيروس المزيف (Fake AV): هو كل برنامج حماية مزيف يقوم بأعمال ضارة لجهاز الكمبيوتر.
- ملف الاستغلال Exploit: عبارة عن ملف يستخدم من قبل المخترقين للحصول على صلاحيات مرتفعة في المواقع المستهدفة بالاختراق. ويستغل هذا الملف ثغرة معينة موجودة في برنامج الخادم الخاص بالمواقع والشبكات أو في البرامج المنصبة عليه ، بهدف الوصول إلى ملفات الجذر واختراق الموقع المستهدف.
- المُنزل Dropper: هو كل برنامج ضار يهدف إلى تنزيل وتنصيب برامج ضارة أخرى في جهاز الضحية ، ومبدأ عمله نفس عمل الـ Multi-Dropper ولكنه يختلف عنه من ناحية أن ألـ Multi-Dopper يكون مدموجا بأكثر من برنامج ضار حيث يقوم بتنزيلهم أو زرعهم في جهاز الضحية ، أما ألـ Dropper فيكون مدموج ببرنامج ضار واحد فقط حيث يقوم بتنزيله أو زرعه في جهاز الضحية.
هناك نوع أخر يندرج تحت خانة المُنزل ولكنه لا يقوم بتنزيل أي ملف ولكنه يقوم بدلا من ذلك بحقن كود ملف خبيث في الذاكرة من خلال حقن الكود الخبيث في عملية من عمليات النظام (OS Process) ، ويسمى هذا النوع من البرامج الخبيثة بـالـ (Injectors).
- المُحمل (Downloader): وهو برنامج ضار صغير الحجم عادة ، وظيفته إنزال برنامج ضار أخر ولكن هذا الملف غير مدموج به . ولكن يقوم بإنزاله من الانترنيت بدون علم الضحية وزرعه وتشغيله في الجهاز.
- المُفيض (Flooder): هو كل برنامج يقوم باستخدام هجوم نكران الخدمة Denial of Service Attack ومن الاسم نستطيع فهم وظيفة هذا النوع من البرامج الضارة ، فوظيفته تتجلى في الهجوم على عنوان معين وتفيضيه بعدد كبير من الـ Packets وبالتالي لن يستطيع الخادم معالجة هذا الكم الهائل من البيانات فيتوقف أو يفصل عن الخدمة.
- عدة الجذر(Rootkit): هي برامج معقدة البرمجة ، تقوم بالعمل في مستويات منخفضة من نظام التشغيل أي في لب النظام وذلك للحصول على صلاحيات مرتفعة كإخفاء البرامج الضارة أو أثارها عن برامج الحماية آو عن المستخدمين بهدف البقاء مدة أطول في جهاز الصحية.
- برمجيات الفدية (Ransom): وهي برمجيات ضارة صممت لغرض ابتزاز المستخدمين ، حيث تقوم بتشفير المستندات الموجودة على جهاز الحاسوب وطلب مبلغ من المال مقابل برنامج فك التشفير.
- برمجيات الطلب (Dialer): وهي برامج خبيثة تقوم بعمل اتصال هاتفي بين جهاز الحاسوب الخاص بالضحية بدون علمه في حالة احتواء جهازه على مودم ، وبين أجهزة كمبيوتر أخرى.

ومن الأمثلة على هذا النوع ... البرمجيات التي تقوم بعمل اتصال بين جهاز الضحية وبين مواقع إباحية لغرض نشر الدعارة أو لغرض سرقة الأموال ، ويطلق عليها تسمية برمجيات الطلب الإباحي (Porn-Dialer).

٤- برمجيات الإعلان Adware : يقوم هذا النوع بجمع معلومات عن جهاز الضحية لغرض تجاري . على سبيل المثال جمع معلومات لمعرفة ما هي المواقع التي يرتادها الضحية وتوجيهه نحو مواقع معينة لغرض الإعلان والترويج لهذه المواقع.

٥- أدوات الاختراق (Hacking-Tool): ويدخل في هذا النوع كل أدوات الاختراق كبرامج الاختراق والتحكم عن بعد ، برامج كسر كلمات المرور .....الخ

٦- مولدات الفيروسات (Virus-Generators): وهي برامج تقوم بتوليد وإنتاج فيروسات جديدة حسب رغبة المستخدم . ويستفيد من هذه البرامج الأشخاص الذين يرغبون في إنتاج وصنع فيروسات بدون خبرة في لغات البرمجة .

ويطلق على هذا النوع من الفيروسات أحيانا اسم أدوات الفيروسات (VirusTool).

٧- برامج السخرية (Joke): هي برامج لا تعتبر ضارة ولكنها تكون غالبا مصدر ذعر وسخرية للمستخدمين ، ومن الأمثلة على هذه النوع ؛ البرامج التي توهم المستخدم بان جميع ملفاته قد تم حذفها أو على سبيل المثال إخافة المستخدم بإظهار رسالة تفيد بان احد أقسام القرص الصلب قد تمت إعادة تهيئته والى أخره من الأمثلة على هذا النوع من البرمجيات.

٨- برامج الخداع (Hoax): وهي برمجيات تقوم بنشر معلومات خاطئة عن وجود إصابة بأحد الفيروسات عن طريق إرسال رسائل بريدية إلى المستخدم ثم الطلب منه بإرسال الرسالة ونشر الخبر الكاذب إلى جميع المستخدمين الذين يعرفهم ، مما يؤدي إلى نشر الاشاعات الغير صحيحة.

٩- برمجيات الـ (Phishing): يعمد هذا النوع من البرمجيات الخبيثة إلى محاولة سرقة كلمات المرور الخاصة بالمستخدمين عن طريق استخدام صفحات مزورة بدلا من صفحات الدخول الأصلية الخاصة بالحساب الالكتروني للمستخدم.

١٠- فيروسات الاختبار (Zoo Viruses): وهي فيروسات أو برمجيات خبيثة يتم جمعها من قبل باحثين الفيروسات في أجهزتهم ومختبراتهم لغرض دراستها وتطوير البرامج المضادة.

أنواع البرمجيات الضارة من حيث فاعليتها وعدم فاعليتها

Malware types according to its activity and inactivity:

يمكن تصنيف البرمجيات الضارة من حيث فاعليتها وعدم فاعليتها إلى نوعين :

- برمجيات ضارة نشطة Active malware: وهي البرمجيات الضارة التي لا تحتوي على أخطاء برمجية بالإضافة لكونها موجودة وتعمل في بيئتها المخصصة والمصممة لها . ففي هذه الحالة سيقوم البرنامج الضار سواء كان فيروس أو دودة بكامل الوظائف والأوامر التي صمم من اجلها .

- برمجيات ضارة سابتة أو خاملة Dormant malware: وهي البرمجيات الضارة التي توجد في بيئة آو نظام تشغيل غير متوافق معها ، ففي هذه الحالة لن تعمل هذه البرامج وستصبح خاملة dormant . على سبيل المثال : عندما يوجد فيروس أو دودة تعمل ضمن بيئة نظام لينكس . ويتم انتقالها عمدا أو خطأ إلى بيئة أخرى كنظام ويندوز مثلا ، طبيعي أن الدودة لن تعمل لأنها غير متوافقة مع هذا النظام.

ويدخل ضمن هذا النوع أيضا البرمجيات الضارة التي لا تعمل لوجود خلل في برمجتها ، وقد يودي هذا الخلل أحيانا إلى مشكلات في نظام التشغيل أو الانهيار الكامل للنظام.

أنواع الفيروسات Viruses types:

أولا: أنواعها من حيث هدف الإصابة Viruses types according to infection target:

١- فيروسات الملفات (Files viruses): عبارة عن برنامج يقوم بحقن نفسه في الملفات التنفيذية كوسيلة للتكاثر والانتشار.
فهذا النوع لا يستطيع العمل بشكل مستقل إلا أن يلصق نفسه بملف تنفيذي (ملف مضيف). ففي هذه الحالة سيتم تشغيل الفيروس مع كل عملية تشغيل لملف مصاب .
٢- فيروسات قطاع الإقلاع (Boot Sector viruses) : يقوم هذا النوع من الفيروسات بإصابة القطاع المسئول عن الإقلاع في القرص الصلب أو في الأقراص المرنة . ويتم تشغيل الفيروس مع كل عملية إقلاع من قرص مصاب.
٣- فيروسات الماكرو (Macro viruses): يصيب هذا النوع من الفيروسات ملفات برامج الأوفيس التابعة لشركة مايكروسوفت .
٤- فيروسات الـ (Companion): بعض الفيروسات لا تغير أي شي في الملفات . ولكنها تستخدم خاصية الأولوية في تشغيل الملفات . فعلى سبيل المثال ، الملفات ذات الامتداد com في نظام التشغيل يتم تشغيلها قبل الملفات من نوع exe و bat ، فيقوم الفيروس بتكوين نسخة من نفسه في نفس المجلد الذي يوجد فيه الملف ولكن امتداد الفيروس هو com وليس exe ، فمع كل عملية استدعاء للملف الأصلي سيتم تشغيل الفيروس أولا لان الأولوية في التنفيذ هي للامتداد com وهو امتداد الفيروس.

ثانيا: أنواعها من حيث طريقة التخفى Viruses types according to stealth method:

١- فيروسات التسلل (Stealth virus): يحاول هذا النوع من الفيروسات إخفاء الإصابة بحيث لا يشعر المستخدم انه أصيب بأحد الفيروسات .
ومن الطرق التي تستخدمها الفيروسات للتخفي ، إن تقوم بإرجاع تاريخ التعديل إلى وقت ما قبل الإصابة ، وبالتالي يبدو الملف كما هو بدون تغيير.
٢- الفيروسات متعددة الأشكال (Polymorphism viruses): يقوم الفيروس من هذا النوع في كل مرة يصيب بها ملف جديد بتغيير توقيعه (كالنمط الثنائي Binary Pattern على سبيل المثال) وذلك لضمان عدم الكشف من قبل البرامج المضادة للفيروسات.
وتعمد هذه الفيروسات إلى تشفير الشفرة البرمجية لجسم الفيروس ، ثم استخدام نمط فك تشفير متغير من إصابة إلى أخرى ، ويستخدم الفيروس آلية تغيير (Mutation Engine) وذلك لغرض تغيير نمط فك التشفير من إصابة إلى أخرى وبالتالي تصعيب عملية الكشف من قبل البرنامج المضاد.
٣- الفيروسات المتحولة (Metamorphic viruses): هي الفيروسات التي تقوم بإعادة ترجمة شفرتها البرمجية (Recompiling code) من إصابة لأخرى . بحيث يظهر الفيروس مختلفا في كل إصابة مع بقاء وظيفة الفيروس .
٤- الفيروسات الانقلابية Retroviruses: من الاسم تعرف الوظيفة ، فهذا النوع من الفيروسات يقوم بالبحث عن أي برنامج مضاد فيروسات منصب في الجهاز ثم الهجوم عليه . إما بإصابته أو بإيقاف عمله. وذلك لضمان بقاء الفيروس في النظام مدة أطول دون الكشف.
ويطلق أحيانا على هذا النوع من الفيروسات اسم مضادات مضادات الفيروسات Anti-Anti-Virus أو قاتل مضاد الفيروس Anti-Virus Killer.
٥- الفيروسات المدرعة (Armored viruses): وهي الفيروسات التي تعمد إلى تصعيب عملية التحليل بوجه باحثي مضادات الفيروسات . ويستخدم الفيروس عدة تقنيات لهذا الغرض . منها تقنية (Anti-Debugging) وتقنية (Anti-Disassembly) . بالإضافة إلى تقنية (Anti-

Emulation) والتي يعمد الفيروس من خلالها إلى عدم تشغيل نفسه عن طريق الكشف المبكر عن الأجهزة التخيلية (Virtual Machines) وذلك للحيلولة دون تحليل الفيروس من قبل محللين الفيروسات أو من قبل مضاد الفيروسات نفسه.

ثالثا: أنواعها من حيث مكان الحقن Viruses types according to injection place:

١- فيروسات البداية (Prepending viruses): وهي الفيروسات التي تقوم بحقن شفرتها البرمجية في بداية الملف.
٢- فيروسات النهاية (Appending viruses): تقوم الفيروسات من هذا النوع بحقن شفرتها في نهاية الملف.
٣- فيروسات الكتابة (Overwriting virus): وهي الفيروسات التي تقوم بإخلاء جزء من الملف و إدراج نفسها في هذا المكان الخالي وذلك لتجنب أي زيادة في حجم الملف جراء الإصابة ولكن هذا النوع من الفيروسات يكتشف بسرعة لان الملف الأصلي لن يعمل بعد الإصابة فيُلاحظ الفيروس ويكتشف بشكل أسرع.

أوجه الشبه والاختلاف بين الفيروس الحيوي والفيروس الرقمي:

الفيروسات الحيوية تسيطر على الوظائف الخلوية الحيوية . وتمتلك هذهِ الفيروسات مجموعتان من الايعازات : مجموعة ايعازات DNA ومجموعة ايعازات RNA والتي تكون محاطة بغلاف بروتيني. بعد أن تدخل هذهِ الايعازات إلى الخلية ، يقوم الفيروس باكتساب كل وظائف الخلية وذلك لأداء الواجبات التي يريد الفيروس عملها.
أما فيروسات الكمبيوتر فتسيطر على الوظائف الرقمية للحاسوب . ففيروس الحاسوب يمتلك سلسلة من (0 , 1) لتمثيل مجموعة الايعازات والتعليمات . بعد أن تدخل هذهِ الايعازات إلى الحاسوب ، يقوم الفيروس باكتساب كل وظائف الحاسوب لأداء الواجبات التي عليه تأديتها.

تصنيف البرمجيات الضارة Malware Classification:

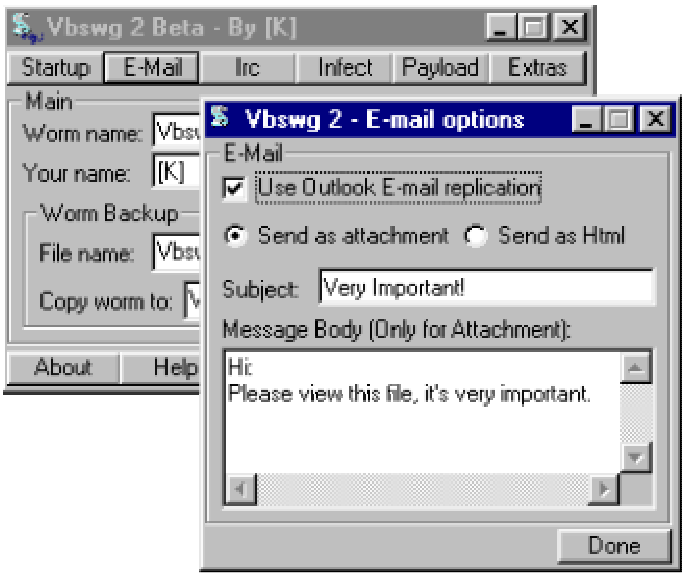
لكل فيروس أو برنامج ضار تسمية أو تصنيف خاص به . حيث يوضح التصنيف غالبا اسم الفيروس والبيئة التي يعمل عليها والنوع أو العائلة التي ينتمي له كعائلة الديدان مثلا ، بالإضافة إلى معلومات أخرى.
لسوء الحظ إن تسمية البرمجيات الضارة غير ثابتة ، وتختلف من شركة مضاد فيروسات إلى أخرى ومن باحث لأخر. ويلاحظ ذلك عند القيام باستخدام أكثر من مضاد ثم القيام بفحص ملف مصاب ، سيلاحظ أن كل برنامج يعطي تسمية مختلفة.
على أية حال التسمية المثلى للبرمجيات الضارة هي بالصيغة الآتية:
(Malware type.Enveronment\malwrae name.Varients@additional Info)
وسنأخذ مثال على تسمية البرمجيات الضارة لكي نتمكن من فهم الطريقة:
(Worm.W32/klez.a@MM) ، نأخذ أول معلومة في التسمية وهي كلمة (Worm) والتي تدل على نوع البرنامج الضار وتبين انه من عائلة الديدان.
المعلومة الثانية توضح بيئة البرنامج الضار حيث أنه يعمل على منصة (W32) .
المعلومة الثالثة تدل على اسم البرنامج الضار (klez) .
المعلومة الرابعة تشير إلى وجود أكثر من نسخة للبرنامج الضار . واقصد بالنسخ هنا أن مبرمجين الفيروسات يقومون بإطلاق نسخ أخرى (Variants) من نفس الفيروس بين الحين والأخر . فيتم تصنيف كل نسخة تصدر على أنها نسخة من نفس الفيروس القديم وتعطى النسخ تسلسل من الحروف . (a , b , c ..... ect) . فحرف a في المثال يشير إلى تسلسل نسخة البرنامج الضار. ومن المهم الإشارة إلى أن تسلسل النسخ لا يظهر في كل البرامج الضارة . فهناك برامج ضارة تظهر مرة واحدة ولايتم إطلاق أي نسخ ثانية عنها . وفي هذه الحالة يتم

تجاهل هذه المعلومة كما في البرنامج الضار (Trojan.W32/Hoon) الذي ظهر منه نسخة واحدة فقط.
أما المعلومة الخامسة والأخيرة فتذكر عندما نريد توضيح تفاصيل إضافية عن البرنامج الضار .
في المثال السابق توضح المعلومة الإضافية (@MM) أن البرنامج الضار هو من نوع الديدان التي لها القدرة على الانتشار عبر البريد الالكتروني وهي اختصار لكلمتي Mass-mailer.

شكل رقم (٧) – مثال على تصنيف الفيروس في برنامج kaspersky

مولدات البرامج الضارة Malware generators:

عبارة عن برامج تمكن أي شخص من إنتاج البرمجيات الضارة سوءا كانت فيروسات ، ديدان أو أحصنة طروادة ، حتى ولو لم يكن لدى هذا الشخص أي خبرة أو معرفة بلغات البرمجة .
وعادة ما تكون هذه البرامج ذات واجهات رسومية ، وذلك لكي يتسنى للمستخدم اختيار وتغيير الأوامر والخيارات الخاصة بإنتاج البرامج الضارة بكل سهولة وحسب الرغبة.
فمثلا لو أراد المستخدم إنتاج دودة أيميل ، فيمكن له اختيار اسم للدودة وأيضا يمكنه إضافة اسمه كمصمم أو كاتب للدوة بالإضافة إلى إمكانية إضافة متى ستنفذ الدودة أمر الانتشار واختيار رسالة تظهر للضحية أو حتى اختيار امتداد الدودة وأين ستستقر بعد الإصابة ، والى أخره من الأوامر المتاحة للمستخدم.



شكل رقم (٨) - برنامج لتوليد ديدان البريد الالكتروني

المبحث الثاني

جمع وتحليل البرمجيات الضارة Malware collecting and analysing

تعد عملية جمع وتحليل الفيروسات من العمليات المهمة لباحثي مضادات الفيروسات . حيث أن الفيروسات والبرمجيات الضارة تظهر باستمرار . فكل ساعة تقريبا يتم إطلاق نوع جديد من البرمجيات الضارة لكي تبدأ بالتخريب حسب الهدف الذي صنعت من اجله، فمن الضروري الحصول على عينة من الفيروسات الجديدة ثم الشروع بالعملية المكملة لها ، ألا وهي تحليل البرمجيات الضارة الجديدة ، وذلك بغرض دراستها ووضع التقنيات المناسبة لكشفها والقضاء عليها.

أولا: عملية جمع البرمجيات الضارة Malware collecting:

وهي العملية التي تتم بالحصول على عينات من البرمجيات الضارة وذلك (كما ذكرنا سابقا) لتحليلها ودراستها . كما يفعل علماء الفيروسات البيولوجية الذين يجمعون عينات من البكتريا والفيروسات بغرض دراستها ووضع المضاد المناسب لها ، اعتمادا على سلوكها . ونفس الأمر هو مع الفيروسات الرقمية.

وتطلق تسمية (Zoo Viruses) على الفيروسات الموجودة لدى الباحثين لغرض الدراسة.

طرق الحصول على البرمجيات الضارة Methods of collecting malwares:

١- عن طريق بعض المواقع التي تتيح لك تحميل عينات من الفيروسات مثل موقع (http://www.offensivecomputing.net/) . فبعد التسجيل في الموقع ، يمكنك البحث عن البرمجيات الضارة وتحميلها.

٢- عن طريق البحث في الانترنيت عن برمجيات ضارة كالاستعانة بمحركات البحث. وذلك بالبحث عن عبارات تدل على جمع البرمجيات الضارة مثلا (Malware Collection) أو (Virus Collection)

٣- صنع ايملات وهمية ومراقبتها بشكل دائم . ففي هذه الحالة سيتم الحصول على رسائل دعائية (Spam) مصابة بالبرمجيات الضارة.

٤- برامج ألـ Honeypots: وهي برامج صممت لجمع البرمجيات الضارة ، حيث تقوم هذه البرامج بمحاكاة نظام مليء بالثغرات وبالتالي فالديدان والبرمجيات الضارة ستتوقع أن هذا النظام هو هدف للهجوم ولكنه في الحقيقية بمثابة فخ.

٥- من مواقع الهكر والاختراق . حيث يمكنك الدخول إلى هذه المواقع وتحميل أخر الفيروسات والبرمجيات الضارة.

٦- مبادلة البرمجيات الضارة (Malware Exchange). حيث يمكنك بعد الحصول على مجموعة كبيرة من الفيروسات من مبادلتها مع أشخاص آخرين لديهم نفس الولع في مجال البرمجيات الضارة.

تحليل البرمجيات الضارة Malware analysing:

هي عملية فهم واكتشاف آلية عمل البرنامج الضار وطريقة إصابته للجهاز بالإضافة إلى التقنيات التي يستخدمها في التخفي والانتشار.

فوائد تحليل البرمجيات الضارة Benefits of malware analysing:

١- الكل منا يعلم أن البرامج المضادة للفيروسات لا تكتشف جميع الفيروسات ، فكل شخص لديه خبرة في تحليل البرامج الضارة ، يمكنه تحليل أي ملف مشبوه لم يكتشف من قبل المضاد ، ومن ثم صنع مضاد شخصي للقضاء عليه اعتمادا على السلوك الخبيث للملف الضار.

وبذلك نستنتج حكمة ذهبية وهي "عدم الاعتماد الكلي على البرامج المضادة للفيروسات والاعتماد على النفس أحياناً".
٢- بالنسبة لمطوري البرامج المضادة فعملية التحليل في غاية الأهمية وذلك لاستخراج توقيع الفيروس وتطوير أو تزويد قاعدة بيانات المضاد بتعاريف الفيروسات الجديدة. ثم توزيع التحديث على المستخدمين بشكل فوري وذلك لكشف الفيروس.
٣- عند إطلاق برامج ضارة جديدة ، يعمد كاتبيها إلى استخدام تقنيات جديدة منها خداع البرامج المضادة ، فعملية التحليل مهمة في كشف هذه التقنيات والعمل على إيجاد تقنيات جديدة مضادة لها.
٤- تطوير قاعدة بيانات تطهير الملفات ، لان برامج مضادات الفيروسات تحتفظ بمعلومات التطهير لكل فيروس في قاعدة بيانات . فعند اكتشاف أي فيروس طفيلي ، يجب معرفة طرق إصابته للملفات واستنتاج طريقة لتطهير الملفات من هذا الفيروس.
٥- إعداد تقارير كاملة عن كل برنامج ضار وجمعها في موسوعة يمكن الرجوع إليها وقت الحاجة.

خطوات تحليل البرمجيات الضارة Malware analysing steps:

١- تجهيز بيئة التحليل Preparing analysing environment:

قبل الشروع في تحليل البرامج الضارة ، يجب إعداد بيئة للتحليل وذلك لان تحليل البرنامج الضار في الحاسوب الشخصي هي عملية في غاية الخطورة ، ومن الممكن أن ينتج عن ذلك انهيار نظام التشغيل أو فقدان ملفات مهمة .
فيجب استخدام بيئة معزولة لتكون بمثابة مختبر لتحليل البرمجيات الضارة. وهنا يحب الإشارة إلى نوعان من البيئات يمكننا استخدامها في التحليل:
- بيئة فيزياوية: وذلك بتجهيز حاسوب فارغ من الملفات مخصص لتحليل البرمجيات الضارة.
- بيئة وهمية: وذلك باستخدام برامج الأجهزة الوهمية ، حيث يمكن تنصيبها في جهازنا الشخصي واستخدامها في التحليل بكل أمان ، حيث يتم نقل العينات المراد تحليلها من الحاسوب الشخصي إلى الجهاز الوهمي عن طريق الفلاش ميموري.

٢- جمع المعلومات حول البرنامج الضار Collecting information about the malware:

في الوقت الحالي نحن نملك عينة من البرنامج الضار ونملك بيئة للتحليل ، علينا الآن تجهيز ورقة وقلم لجمع وتدوين بعض المعلومات المهمة حول البرنامج الضار والتي يمكن الرجوع إليها ، والمعلومات الواجب جمعها هي كالآتي:
- تاريخ الاكتشاف: أي التاريخ الذي حصلت فيه على العينة.
- حجم الملف: أي حجم البرنامج الضار مثلا 10 KB
- البيئة: يجب تدوين البيئة أو النظام الذي صمم البرنامج الضار للعمل فيه ، مثلا: ويندوز ، لينكس الخ ...
- لغة البرمجة: هناك برامج تمكننا من معرفة لغة البرمجة ، ومن أفضل هذه البرامج وأسهلها برنامج Detect it easy.
- حالة ضغط الملف: يمكنك استخدام نفس البرنامج السابق في معرفة حالة ضغط الملف. وفي حالة كان الملف مضغوط فيجب علينا فك الضغط عنه وذلك لكي نحصل على نسخة نقية من البرنامج الضار لاستخدامها في التحليل . وبالنسبة لعملية فك الضغط فسوف نتناولها لاحقا بشي من التفصيل.
- MD5Checksum : يمكن الحصول على بصمة الفيروس باستخدام برنامج (MD5Win32) ، وتستخدم هذه البصمة في تمييز أو تصنيف الفيروس واكتشافه.

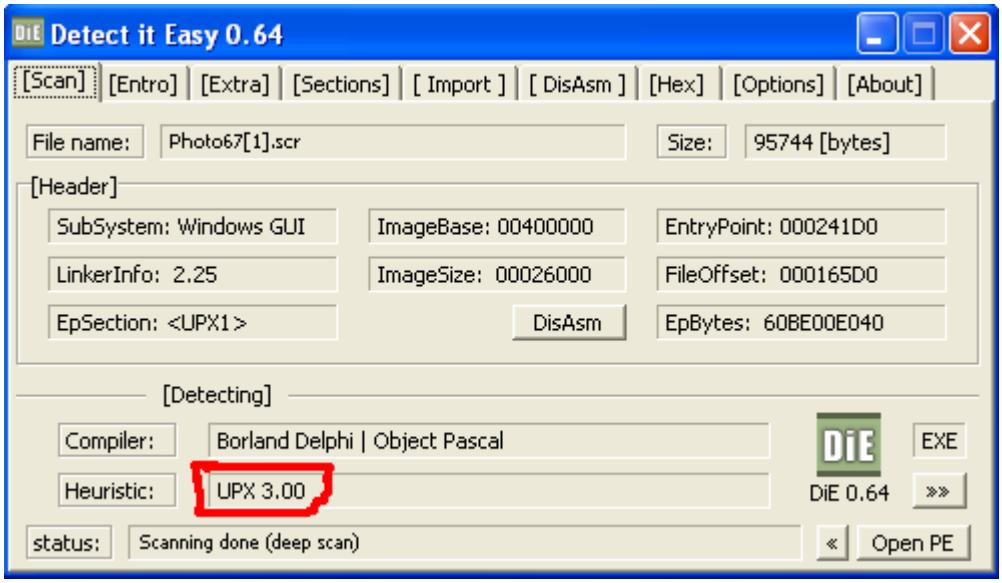
بعد جمع المعلومات أعلاه ، نقوم بفحص الفيروس بكل برامج مضادات الفيروسات الموجودة ، فهناك مواقع تقدم هذه الخدمة ، مثلا:

http://scanner.novirusthanks.org
http://www.virustotal.com/ar
http://virscan.org
http://virusscan.jotti.org/en

فكل ما عليك هو فتح واحد من هذه المواقع ثم رفع عينتك ، وبعد لحظات ستحصل على نتائج الفحص ، وبالتي يمكنك معرفة ما هي مضادات الفيروسات التي تمكنت من كشف البرنامج الضار ، وما هي مضادات الفيروسات التي لم تتمكن من اكتشافه.

٣- فك الضغط Unpacking:

تعد عملية فك الضغط من العمليات المهمة في التحليل ، ففي حالة كان البرنامج الضار مضغوط فمعنى ذلك أننا سنواجه صعوبات في عملية التحليل وذلك لان محتويات البرنامج الضار المضغوط كالسطور البرمجية تكون مشفرة ويصعب قراءتها وتحليلها. فيجب فك الضغط لكي تجري عملية التحليل بشفافية ومرونة.
في الحقيقة إن ضغط البرنامج الضار هو تقنية من تقنيات تشويش البرامج المضادة للفيروسات أو تشويش تحليل البرنامج الضار وبالتالي إطالة مدة بقاءه وانتشاره في أجهزة المستخدمين.
هناك أدوات كثيرة تستخدم في ضغط البرامج الضارة واشهرها:
(UPX – ASPack – FSG – Themida).
ولكي نفك الضغط عن البرنامج الضار فيجب معرفة ما هي الأداة المستخدمة في ضغط البرنامج الضار ، وهناك عدة برامج لعمل ذلك كبرنامج (Detect it Easy) كما في الشكل التالي:



شكل رقم (٩) يبين الشكل أن البرنامج الضار مضغوط باستخدام برنامج (UPX 3.00).

فبعد معرفة نوع الضغط نبحث في الويب عن البرنامج الذي يعكس العلمية أو الذي يقوم بفك الضغط مثلا البرامج المضغوطة ببرنامج (UPX) يمكن فكها باستخدام نفس البرنامج أو

باستخدام برنامج UnUPX ، واستخدام البرنامج UnFSG لفك الضغط عن البرامج الضارة المضغوطة ببرنامج FSG وهكذا مع باقي أداوت الضغط.
إما إذا كان البرنامج الضار مضغوط ببرنامج ضغط مجهول أو أننا لم نستطع فك الضغط بأي برنامج ، ففي هذه الحالة يمكننا اللجوء إلى برامج خاصة تستخدم تقنيات عامة في فك الضغط (Generic Unpacking) ، ومن هذه البرامج برنامج AllUnpack . وهنا يحب الملاحظة إلى أن عملية فك الضغط بالطرق العامة يجب أن تتم في بيئة معزولة أو جهاز وهمي وذلك لان أكثر البرامج من هذا النوع تعمد إلى تشغيل البرنامج الضار قبل فك الضغط.

٤- بدء عملية التحليل Start analysing:

هناك مرحلتان للتحليل: التحليل الاستاتيكي والتحليل الديناميكي.
١- التحليل الاستاتيكي: ويقصد به تحليل البرنامج الضار من دون تشغيله ، حيث يتم معرفة آلية عمله ومعرفة الدوال التي يستخدمها.
ويمكننا عمل التحليل الاستاتيكي للبرنامج الضار باستخدام الأدوات الآتية:
- برنامج Bin Text: ويستخدم هذا البرنامج في عرض جميع النصوص التي يحتويها البرنامج الضار . حيث نقوم بقراءة هذه النصوص واخذ المفيد منها ، ومثال على ذلك عناوين الانترنيت التي يقوم البرنامج الضار بالاتصال عليها ، أو أسماء بعض الدوال المستخدمة في البرنامج الضار وغيرها من المعلومات التي يمكن الاستفادة منها في فهم بعض جزئيات البرنامج الضار.
- برنامج OllyDBG: وهو احد برامج التنقيح المستخدمة في الهندسة العكسية ، حيث يمكن استخدام هذه الأداة في الكشف عن شفرة البرنامج الضار البرمجية وعرضها بلغة الاسمبلي ، حيث تمكنك هذه الأداة من تتبع تنفيذ الأوامر في البرنامج الضار وفهم طريقة عمله ولكن يجب أن تكون لديك خبرة ولو متوسطة في لغة التجميع (الاسمبلي).

٢- التحليل الديناميكي: وهو تحليل البرامج الضارة وقت التشغيل أي أننا في هذه المرحلة نعمد إلى تنفيذ البرنامج الضار ونرى ما هي النشاطات والتغييرات التي يقوم بها.
وبالنسبة للأدوات التي سنستخدمها في هذه المرحلة من التحليل فهي كالآتي:
- **RegShot:** يعتبر هذا البرنامج من أهم البرامج في التحليل الديناميكي ، حيث يقوم البرنامج بالتقاط صورة لمسجل النظام ثم التقاط صورة أخرى بعد تشغيل البرنامج الضار وذلك لملاحظة التغييرات التي أحدثها في مسجل النظام .
ويحتوي البرنامج على وظيفة أخرى وهي مراقبة التغيرات على ملفات القرص الصلب. لمراقبة الملفات التي يقوم الفيروس بإضافتها.
- Process Explorer: يستخدم هذا البرنامج لمراقبة عمليات النظام التي قام البرنامج الضار بإنشائها.
- Active Ports: وهو برنامج يعطيك المنافذ المفتوحة في الجهاز بالإضافة إلى حالة الاتصالات المتوفرة على النظام مع إعطاء معلومات تخص الاتصال كرقم الايبي المحلي والبعيد بالإضافة إلى رقم المنفذ والبروتوكول المستخدم مثلا (TCP - UDP) بالإضافة إلى مسار البرنامج الذي أنشئ الاتصال.
وبالتالي فتستطيع استخدام هذا البرنامج للحصول على تفاصيل حول الاتصالات المشبوهة التي تجريها التروجونات (كبرمجيات الأبواب الخلفية) على الجهاز.
- Process Monitor: هذا البرنامج عبارة عن أداة تراقب النظام وتعطيك معلومات كثيرة حول العمليات التي تحدث في النظام مثل:
- عمليات الملف كتكوين وقراءة الملفات
- عمليات مسجل النظام.
- التغييرات في عمليات النظام OS Processes.

- عمليات الاتصال بالشبكة.
- الخ ...

ويمكنك عمل ترشيح (Filter) للمراقبة بحيث يراقب البرنامج العمليات التي تحددها أنت بالإضافة إلى جعل المراقبة موجهة نحو مراقبة العمليات التي ينشئها ملف معين تحدده أنت وذلك بتحديد اسم الملف التنفيذي في نفس النافذة.

المبحث الثالث
تقنيات المعالجة والتطهير Treating and disinfection techniques

تاريخ البرامج المضادة للفيروسات Anti-virus software history:

1986	Avira
1989	Symantec Norton
1989	McAfee
1990	ESET Node32
1997	Kaspersky

طرق الوقاية (مرحلة ما قبل الإصابة)
Protection methods (stage before infection):

انطلاقا من مبدأ الوقاية خير من العلاج ، فمن الواجب علينا إذا ما أردنا جعل حواسيبنا سليمة دائما من الفيروسات والبرمجيات الضارة ، أن نعمد إلى وقايتها في حالتها السلمية قبل أن نجبر إلى اللجوء إلى العلاج بعد الإصابة.

وتتمثل الوقاية من البرمجيات الضارة وتجنب الإصابة بالنقاط الآتية:

١- تنصيب برنامج مضاد فيروسات قوي . بالإضافة إلى التحديث المستمر وبشكل دوري لقاعدة بيانات كشف الفيروسات وذلك لكي يتم القضاء على أخر الفيروسات والبرمجيات الضارة . واحرص على تفعيل خاصية الفحص الذاتي للفيروسات (Real-time protection).

٢- التحديث الدوري لنظام التشغيل.

٣- فحص الكمبيوتر بشكل كامل بين فترة وأخرى باستخدام مكافح الفيروسات الموجود لديك.

٤- فحص أي ملف يتم تحميله من الويب قبل فتحه.

٥- فحص الوسائط القابلة للإزالة كالفلاش ميموري قبل فتحها أو استعراض محتوياتها.

٥- قم بإغلاق منافذ نظام الويندوز كمنفذ مشاركة الملفات NetBIOS مثلا . وذلك باستخدام برنامج اسمه Windows worms doors cleaner : وطريقة سد المنافذ باستخدام البرنامج سهلة جدا . فقط قم بعمل disable لكل المنافذ عن طريق أزرار البرنامج ثم اعد تشغيل الكمبيوتر ثم شغل البرنامج مرة أخرى لتجد أن البرنامج يخبرك بأن نظامك أصبح أمنا. فهذه البرنامج مفيد كدرع بوجه الديدان التي تستخدم منافذ النظام للانتشار .

٦- تنصيب جدار ناري للوقاية من هجمات الفيروسات التي تأتي جراء الدخول الغير شرعي إلى الجهاز.

٦- استخدم متصفح انترنيت قوي وأنا أفضل متصفح الـ Mozila Firefox وذلك لأنه متصفح يعطيك أمنية عالية ضد الثغرات والمخاطر الأمنية .

٧- لأتفتح أي ملف مرفق آو رابط سواء كان في الدردشة أو البريد الالكتروني أو المواقع إلا إذا كان من مصدر موثوق واتبع الحكمة القائلة Think before click .

٨- عدم الدخول إلى المواقع الإباحية لان هذه المواقع عبارة عن مستعمرات للبرمجيات الضارة وخاصة ملفات التجسس.

٩- الحذر من البرامج المجانية والكركات أو الكيجين لاحتوائها في الغالب على برامج ضارة.

تقنيات البرامج المضادة للفيروسات Anti-virus techniques:

تستخدم هذه البرامج العديد من التقنيات التي تساعد في التشخيص والكشف المبكر عن أي إصابة ببرنامج ضار ومنعه من الإضرار بجهاز الكمبيوتر.
وتنقسم هذه التقنيات إلى عدة أقسام:

- معرفة حالة الضغط والتشفير X-Raying:

قبل الشروع بعملية فحص الملف ، يجب معرفة هل الملف مضغوط أو مشفر وذلك لمحاولة فك الضغط أو فك التشفير ، لان الضغط والتشفير هي من الطرق المستخدمة لتشويش تقنيات الفحص التي تستخدمها مضادات الفيروسات ، فتعتبر هذه العملية في غاية الأهمية وذلك لأنها تهيئ صورة واضحة وجاهزة للملف ليتم الاعتماد عليها في الفحص.

- الفحص Scan :

وهي عملية تحليل أي عنصر من عناصر النظام كالملفات ومعرفة هل هو مصاب أم لا.
ويقصد بعناصر النظام : الملفات ، رسائل البريد ، قطاع الإقلاع ، الذاكرة النشطة ، حزم الشبكة . فكل هذه العناصر تدخل ضمن عملية الفحص للتأكد من خلوها من أي إصابة.
وينقسم الفحص إلى نوعين:

فحص حسب الطلب On-demand scan:

وهو الفحص الذي يتم حسب رغبة المستخدم ، فالمستخدم يعمد إلى إجراء الفحص متى ما أراد.

الفحص التلقائي On-Access scan:

وهو الفحص الذي يتم دون تدخل المستخدم ، حيث يقوم البرنامج المضاد بمراقبة النظام وعندما يلاحظ أي عملية نشطة (كقراءة ملف أو نقل ملف مثلا) فانه يقوم تلقائيا بتعليق العلمية مؤقتا ريثما يتم فحص العنصر الذي جرت عليه العملية ، فإن كانت النتيجة إصابة العنصر فيتم تحذير المستخدم وتنفيذ الإجراء اللازم.

طرق واليات الفحص Scan mechanisms:

١- فحص الـ MD5:

ويتم هذا الفحص بحساب الـ Md5 Checksum للملف ومطابقته مع الـ MD5 checksums الموجودة في قاعدة البيانات الفيروسات. حيث يعتبر MD5 بمثابة بصمة فريدة تميز البرنامج الضار عن غيره من الملفات السليمة.
ولكن من مساوئ هذه الطريقة أنها لا تكشف عن البرامج الضارة المتحولة Metamorphic Viruses ، إذ أنها تغير بصمتها من إصابة إلى أخرى. ولكن هذا لا يعني أن يتم ترك هذه الطريقة ، ولكن يمكن استخدامها مع باقي الطرق لتحقيق حماية متكاملة.

٢- الفحص باستخدام التوقيع Signature-based scan:

وهي من الطرق الشائعة في الكشف عن الفيروسات والبرمجيات الضارة ، عن طريق مقارنة محتويات الملف المفحوص (هيكس الملف) بمجموعة من التواقيع الفيروسية الموجودة في قاعدة بيانات المضاد والبحث عن أي تطابق ، ويتم استخلاص التوقيع للبرنامج الضار باستخدام أي محرر Hex بشرط أن يكون التوقيع ثابت ويظهر في كل العينات المصابة بنفس البرنامج الضار. مثلا التوقيع الثابت للبرنامج الضار Backdoor/GhostDial هو:

E8003CFEFFE881DEFEFF89442408DB44240883EC10DD5C2408DD0
548034700DD1C24E84E02000033C0DD5C24088BCFE8

وتتكون قاعدة البيانات من تواقيع متسلسلة للبرامج الضارة ويتم مقارنتها واحدة تلو الأخرى والبحث عنها داخل الملف المفحوص للبحث عن أي تطابق.
ومن محاسن هذه الطريقة أنها تكشف عن البرمجيات الضارة المتحولة بالإضافة إلى أنها قد تكشف عدة أنواع من البرمجيات الضارة من نفس العائلة.

٣- تدقيق النزاهة Intgrity checker: وهي من الطرق التي تستخدم في الكشف عن الفيروسيات الطفيلية ، حيث تتم هذه الطريقة بجمع MD5 checksum لجميع الملفات التنفيذية الموجودة في القرص الصلب ، وإثناء عملية الفحص يتم مقارنة checksum الملف القديم مع ألـ checkcum الجديد ، فإذا وجد أي اختلاف فيدل على تغير الملف وبالتالي احتمال كبير لإصابته بفيروس طفيلي لان الفيروس عندما يصيب ملف فان الـ checksum سيتغير . وهذه الطريقة فعالة وتكشف عن الفيروسات الطفيلية ولو كانت مشفرة .
ومن مساؤوى هذه الطريق أنها تحدث إنذارات خاطئة false positive في حالة كان تغيير الملف من قبل المستخدم أو من قبل النظام.
٤- الفحص التجريبي الاستاتيكي Static heuristic scan:
منذ فترة ويحاول باحثي الفيروسات إيجاد طريقة للكشف عن البرمجيات الضارة الغير معروفة من قبل مضاد الفيروسات وبعبارة أخرى البرمجيات الضارة الجديدة والتي لم يتم إضافة تواقيعها إلى قاعدة البيانات ، فهناك برمجيات ضارة تنتشر بشكل كبير وتلحق أضرار كبيرة قبل أن تحصل شركات الحماية على نسخة وتضيف قيم التحديث إلى قاعدة البيانات.
فعملية الكشف ألاستباقي عن البرمجيات الضارة الغير معروفة أمر في غاية الأهمية ، فالفحص التجريبي وجد لتأدية هذه المهمة .
يتكون الفحص التجريبي من مكونين:
- مُجمع المعلومات : حيث يقوم بجمع وتهيئة قائمة بجميع الدوال Functions التي يستخدمها الملف المفحوص.
- المحلل: يقوم المحلل بتصنيف الدوال الضارة والدوال السليمة . ثم عمل مقارنة بين المجموعتين ، فإذا كانت الدوال الضارة أكثر من الدوال السليمة فيتم تحذير المستخدم بوجود ملف مشبوه Suspicious file . والسبب في تصنيف الملفات المكتشفة بهذه الطريقة على أنها ملفات مشبوهة لان البرنامج المضاد غير متأكدا ١٠٠% من أن الملف هو برنامج ضار.
وفي هذه الحالة يتم عزل الملف في الحجر ، وينصح المستخدم بإرسال الملف المشبوه إلى الشركة المصنعة للمضاد لإضافة التحديث والإجراء اللازم.
وهنا يجب الإشارة إلى شكل أخر من أشكال المحلل ، وهو باستخدام الشبكات العصبية ، حيث يتم عمل شبكة عصبية مدربة على مجموعة كبيرة من البرمجيات الضارة ، ويكون التدريب على الدوال السليمة والضارة وبالتالي ستتمكن الشبكة العصبية من تمييز هذه الدوال والعمل كمحلل للفحص التجريبي لتحقيق نسبة جيدة في الكشف عن البرمجيات الضارة الغير معروفة.
٥- الفحص التجريبي الديناميكي Dynamic heuristic:
يحمل هذا النوع من الفحص نفس فكرة الفحص التجريبي الاستاتيكي ولكن يختلف عنه في إن الفحص التجريبي الديناميكي يفحص الملف في حالة تشغيله ، أما الأول فيفحص الملف بدون تشغيله.
ولكن عملية تشغيل البرنامج المفحوص في جهاز الحاسوب أمر خطير جدا ، لذلك يكون تشغيل البرنامج المفحوص في بيئة تخيلية (Emulator) ينشئها المضاد ، ثم بعد ذلك يتم مراقبة الدوال التي تم استدعائها من قبل البرنامج وعمل مقارنة (كما في الفحص الاستاتيكي) بين الدوال الضارة والسليمة باستخدام الشبكات العصبية أو المقارنة الحسابية النسبية لتحديد هل الملف هو ملف ضار أم ملف عادي وذلك بإعطاء النتائج لبرنامج الفحص ليعرضها للمستخدم.
ويستفاد من هذا النوع من الفحص في الكشف عن البرمجيات الضارة المشفرة وذلك لان البرنامج الذي سيتم تشغيله في البيئة التخيلية تظهر شفرته البرمجية واضحة (Plain text code) ، حيث يقوم البرنامج الضار بفك التشفير عن شفرته البرمجية وقت التشغيل (Runtime) وبالتالي يمكن للبرنامج المضاد الاستفادة من هذه الميزة في الكشف عن البرمجيات الضارة المشفرة والمضغوطة.

التطهير Disinfection:

وهي عملية تنظيف الملف التنفيذي المصاب بفيروس طفيلي ، وذلك بطرح شفرة الفيروس وإبقاء شفرة الملف السليمة .

وعملية التطهير تنقسم إلى قسمين:

- التطهير القياسي: حيث يقوم باحثي الفيروسات بتحليل الفيروسات وذلك بحقنها في عدد من الملفات وعمل مقارنة بين هذه الملفات ورؤية المكان الذي يقوم الفيروس بإصابته. بعد ذلك يقوم الباحثون باستخلاص المعلومات التي تم استخراجها من سلوك الفيروس ووضعها في قاعدة بيانات تسمى قاعدة بينات التطهيرDisinfection database لكي يستخدمها المضاد في تطهير الملفات المصابة بالفيروس.

- التطهير بالطرق العامة Generic disinfectio: تتلخص هذه الطريقة في إنتاج تقنية أو خوارزمية موحدة تقوم بتطهير حتى الفيروسات الغير معروفة (أي الفيروسات التي تم اكتشافها بالفحص التجريبي) حيث يقوم المضاد بفتح الملف المصاب بالفيروس في بيئة تخيلية ومن ثم مراقبة سلوكه والتقنية التي يستخدمها في الإصابة بالإضافة إلى مكان التلويث ، ثم يقوم المضاد بتطهير الملف اعتمادا على المعلومات التي تم جمعها.

أنظمة المناعة (Immune Systems):

تعمد الفكرة من وراء استحداث أنظمة المناعة إلى التحصين والحماية الاستباقية ضد أي إصابة محتملة ، وتتلخص الفكرة في وضع قيود على عمليات النظام وعلى التطبيقات التي تستخدم من قبل البرامج الضارة ، ويعني ذلك وضع قيود على العناصر الآتية:

- استدعاء الدوال Function calls: وذلك بمراقبة استدعاء الدوال ، ومنع أي دالة قد تستخدم من قبل البرامج الضارة.

- السكربتات Scripts: ويتم ذلك بإيقاف عمل بعض السكربتات في النظام والتي قد تكون كأداة بيد البرنامج الضار كسكربتات الجافا والفجوال و سكربتات ألـ INF والتي يمكن استخدامها لتشغيل البرنامج الضار عند الدخول إلى القرص الثابت أو القرص القابل للإزالة.

تقنيات أخرى Other techniques:

تحتوي مضادات البرامج الضارة الحديثة على تقنيات أخرى مثل:

١- الجدران النارية Firewalls:

وهي أنظمة تستخدم للسيطرة على سير الاتصالات الواردة والصادرة بالإضافة إلى المنافذ في جهاز أو شبكة معينة ، وتقوم هذه الأنظمة بوضع قوانين للاتصالات المسموح بها والاتصالات الغير مسموح بها ، ويتم ذلك حسب رغبة المستخدم وبالتالي سيكون الجهاز آمناً وبعيدا عن الاتصالات المشبوهة والغير الشرعية التي تتم دون علم المستخدم.

٢- Anti-Phishing:

تستخدم هذه التقنية في برامج مضادات الفيروسات المدعمة بحماية الانترنيت Internt security ، حيث تتلخص هذه التقنية بالكشف عن الصفحات المزورة التي تستخدم من قبل المخترقين للحيلولة دون حصول أي عملية سرقة لكلمات المرور الخاصة بحسابات المستخدمين.

٣- Anti-Spam:

وهي تقنية تعمد إلى حماية صناديق البريد الخاصة بالمستخدمين من الرسائل الدعائية المزعجة والعمل على حجبها ومنعها من إزعاج المستخدم.

٤- مضادات عدة الجذر Anti-Rootkit:

اغلب البرامج المضادة تبحث عن البرمجيات الضارة من هذه النوع وكما قلنا سابقا فهذه البرامج تعمل في مستويات منخفضة من النظام (in kernal level) بهدف التلاعب بوظائف النظام لإخفاء الفيروسات وجعل عملية الكشف عنها أمر مستحيل ، فمضاد الفيروسات يجب أن يعمل في مستويات منخفضة أيضا من النظام وذلك للكشف عن هذا النوع الخطير من البرمجيات الضارة.

٥- حارس الويب Web-Guard:

وهي تقنية تعمل على مراقبة عناوين الانترنيت في متصفحات الويب وتحذير المستخدم عند الدخول إلى مواقع خطرة أو مواقع تحتوي على برمجيات ضارة.
فهناك برمجيات ضارة تستغل ثغرات المتصفح لإنزال فيروسات إلى الجهاز فحارس الويب يأخذ مهمة محاربة فيروسات الويب.

٦- قرص الإنقاذ Rescue Disk:

وهو عمل نسخة من البرنامج المضاد على قرص إقلاع bootable disk أو على فلاش ميموري وذلك لاستخدامها في فحص الحاسوب مع بدء الإقلاع ، وذلك لتطهير النظام المصاب قبل الدخول إليه.

٧- فاحص البريد الالكتروني Email Scanner:

تقوم بعض البرامج المضادة بفحص البريد الوراد والصادر للحيلولة دون استقبال أو إرسال رسائل مصابة بالبرمجيات الضارة.
ففحص البريد الالكتروني من الضروريات في حماية الحواسيب ، فالكثير من ديدان الكمبيوتر تستغل البريد الالكتروني للانتشار وإصابة اكبر عدد من الأجهزة. بالإضافة إلى أن بعض الديدان تستخدم الجهاز المصاب لإرسال ديدان وبرمجيات ضارة إلى المضافين في حساب البريد الالكتروني ، فلهذا وجد الباحثون هذا النوع من الفحص لزيادة نسبة الحماية ضد البرمجيات الضارة.

٨- نظام الغيمة Cloud system:

الكثير من المستخدمين يعانون من مشكلة التحديث لبرامج الحماية وذلك بسبب سرعة انتشار البرمجيات الضارة . فيتوجب على كل مستخدم أن يقوم بتحديث برنامج الحماية الخاص به باستمرار . لذلك أوجد الباحثون نظام يهدف إلى حل هذه المشكلة . فنظام الغيمة يتمثل بوضع قاعدة بيانات الفيروسات على خادم بعيد تابع للشركة المصنعة للمضاد بدلا من وضعها في جهاز المستخدم ، وتكون جميع أجهزة المستخدمين متصلة بهذه القاعدة والتي تكون محدثة بشكل تلقائي ، فعند إطلاق فيروس جديد تقوم الشركة مباشرة بإضافة توقيع الفيروس الجديد إلى قاعدة البيانات .
ومن فوائد هذا النظام السرعة في اكتشاف الفيروسات ومخاطر الانترنيت الجديدة بشكل فوري مما يوفر مستويات عالية من الحماية بالإضافة إلى التخلص من عناء عملية التحديث.

المصادر والمراجع:

- Introduction to Malware and Countermeasures - Tan Han Chiang
- A Short History of Computer Viruses and Attacks - Brian Krebs
- The art of computer virus research and defense - By Peter Szor
- Certified ethical hacking – the career academy of south flodida community college
- http://en.wikipedia.org
- http://www.bleepingcomputer.com
- http://www.kaspersky.com/
- http://www.f-secure.com
- http://www.virusbtn.com
- http://www.pandasecurity.com
- http://www.webopedia.com
- http://wiki.answers.com
- http://www.at4re.com/f/
- http://www.ullapool.co.uk
- http://www.advpc.net
- دراسة في علم الفيروسات وطرق القضاء عليها – وجدي عصام عبد الرحيم
- الفيروسات - هند كاظم و علا طحطوح
- مجلة البوابة الالكترونية – الإصدار الثالث

تم بحمد الله

The_researcher_1986@yahoo.com