بسم الله الرحمن الرحيم

CEN 448

McAfee VirusScan

Done by:

Mishari mohammed al-rashed

423102016

مقدمه 1

يحتوي هذا التقرير على عرض لبرنامج McAfee VirusScan والذي يقوم بمكافحة الفيروسات وملفات التجسس وقبل ان نبدا لابد ان نوضح ماالمقصود بالتجسس وملفات التجسس والاختراق؟

تسمى هذه العملية HAKING وتسمى باللغة العربية عملية التجسس أوالاختراق . حيث يقوم أحد الأشخاص الغير مصرح لهم بالدخول إلى نظام التشغيل في جهازك بطريقة غير شرعية ولأغراض غير سوية مثل التجسس أو السرقة أو التخريب حيث يتاح للشخص المتجسس (الهاكر) أن ينقل أو يمسح او يضيف ملفات أو برامج كما أنه بإمكانه أن يتحكم في نظام التشغيل فيقوم بإصدار أوامر مثل إعطاء أمر الطباعة أو التصوير أو التخزين ....
من هم الهاكرز؟ هم الأشخاص الذين يخترقون جهازك فيستطيعون مشاهدة مابه من ملفات أو سرقتها أو تدمير جهازك أو التلصص ومشاهدة ما تفعله على شبكة الإنترنت ..ولكن ما هي الأشياء التي تساعدهم على اختراق جهازك ؟لا يستطيع الهاكر الدخول إلى جهازك إلا مع وجود ملف يسمى (Trojan أو Patch) في جهازك وهذه الملفات هي التي يستطيع الهاكر بواسطتها الدخول إلى جهازك الشخصي حيث يستخدم الهاكر أحد برامج التجسس التي ترتبط مع ملف الباتش والذي يستطيع أن يضع له الهاكر إسم مستخدم و رمز سري تخوله أن يكون هو الشخص الوحيد الذي يستطيع الدخول إلى جهازك وكذلك يستطيع أن يجعل جهازك مفتوحاً فيستطيع أي هاكر أن يدخل إلى جهازك !!
ولا يستطيع الهاكر أن يدخل إلى جهازك إلا إذا كنت متصلاً بشبكة الإنترنت أما إذا كان جهازك غير متصل بشبكة الإنترنت أو أي شبكة أخرى فمن المستحيل أن يدخل أحد إلى جهازك سواك !! ولذللك إذا أحسست بوجود هاكر في جهازك فسارع إلى قطع الاتصال بخط الإنترنت بسرعة حتى تمنع الهاكر من مواصلة العبث والتلصص في جهازك ..ولكي يتمكن الهاكر من اختراق جهازك لابد أن يتوافر معه برنامج يساعده على الاختراق ولكن كيف يتمكن الهاكر من الدخول إلى جهازك؟ عندما يتعرض جهاز الكمبيوتر للإصابة بملف التجسس وهو (الباتش أو التروجان) فإنه على الفور يقوم بفتح منفذ PORT أو منفذ داخل جهازك فيستطيع كل من لديه برنامج تجسس أن يقتحم جهازك من خلال هذا الملف الذي يقوم بفتح منطقة أشبه بالنافذة السرية التي يدخل منها اللصوص وهم الهاكرز !!
كيف يتمكن الهاكر من الدخول إلى جهاز كمبيوتر بعينه ؟ لا يستطيع الهاكر أن يخترق جهاز كمبيوتر بعينه إلا إذا توافرت عدة شروط أساسية وهي:
1- : ذا كان هذا الكمبيوتر يحوي ملف التجسس (الباتش) .
2- إذا كان الهاكر يعرف رقم IP الخاص بجهاز الكمبيوتر
ولابد من وجود الشروط الأخرى وهي اتصال الضحية بالإنترنت ومعرفة الهاكر بكيفية استخدام برنامج التجسس والاختراق من خلاله ! بمعنى آخر إذا كان جهاز الكمبيوتر سليماً ولا يحوي أي ملفات باتش فمن المستحيل أن يدخل عليه أي هاكر عادي حتى لو كان يعرف رقم الآي بي أدرس ما عدا المحترفين فقط وهم قادرون على الدخول بأية طريقة وتحت أي مانع ولديهم طرقهم السرية في الولوج إلى مختلف الأنظمة !! وإذا كان الهاكر لا يعرف رقم IP الخاص بك فإنه لن يستطيع الدخول إلى جهازك حتى لو كان جهازك يحوي ملف الباتش والمقصود ب IP العنوان الخاص بكل مستخدم لشبكة الإنترنت أي أنه الرقم الذي يُعَّرف مكان الكمبيوتر أثناء تصفح شبكة الإنترنت وهو رقم متغير وغير ثابت فهو يتغير مع كل دخول إلى الإنترنت .
بعد ان القينا الضوء على مفهوم التجسس وكيفية حدوثة نبدا الان في عرض البرنامج الذي نحن بصدده وهو من انتاج شركة McAfee وهذاالبرنامج متخصص في مكافحة الفيروسات وملفات التجسس spyware.
ومن اشهر برامج التجسس :-

Netbus1.70

وهو الأكثر شيوعا بين مستخدمي المايكروسوفت شات SERVER من أقدم البرامج في ساحة الاختراق بالخادم وهو برنامج به العديد من الإمكانيات التي تمكن الهاكر من التحكم بجهاز الضحية وتوجد نسخ مختلفة أكثر حداثة من النت باس وكل نسخى منها أكثر تطوراً من الأخرى..

Hackers utility

برنامج مفيد ورهيب للهاكرز وخاصة المبتدئين والمحترفين حيث أنه يمتلك أغلب وأفضل إمكانيات مختلف برامج الهاكرز ويمكن من خلاله كسر الكلمات السرية للملفات المضغوطة وفك تشفير الملفات السرية المشفرة وكذلك تحويل عناوين المواقع الى عناوين والعكس كما به العديد من الإمكانيات والمميزات التي يبحث عنها الكثير من الهاكرز ..

2 برنامج McAfee VirusScan

يقدم هذا البرنامج حماية شاملة ضد الفيروسات وملفات التجسس مثل Trojan Horses وHybrid Attack والعديد من التهديدات التي يتعرض لها جهاز الحاسب .

مميزات البرنامج :-

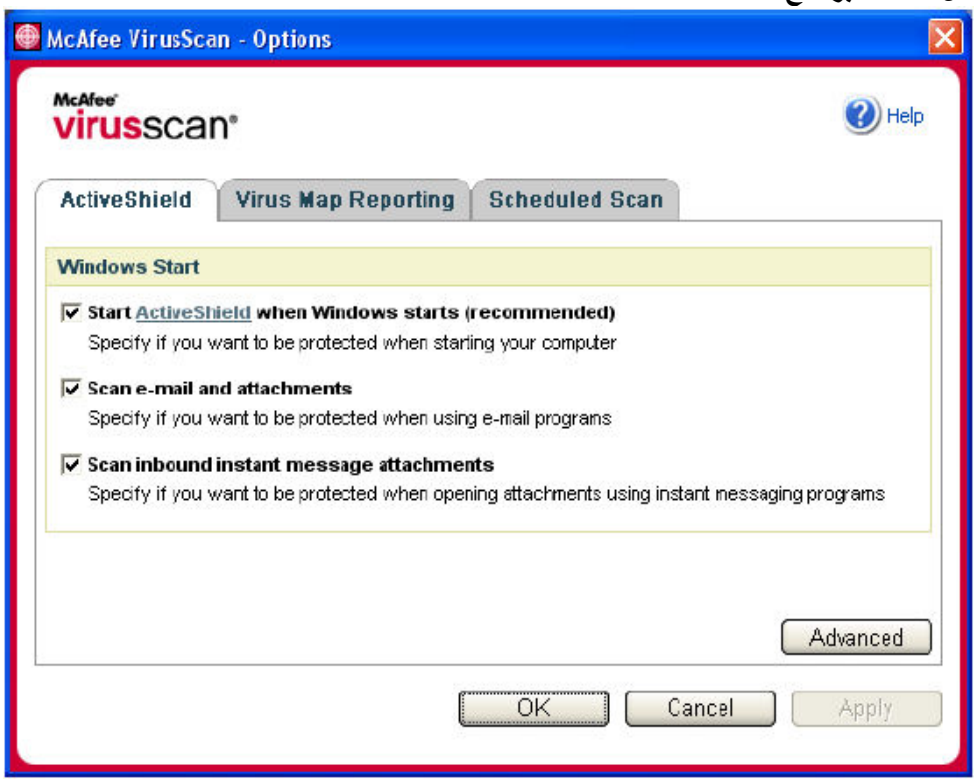
هذا البرنامج يتضمن العديد من المميزات الجديدة منها:

- تحديد ملفات التجسس spyware و ملفات الدعاية adware وازالتها.
- تجديد يومي up to date للتعامل والتخلص من الانواع الجديدة من الفيروسات.
- عمل مسح شامل غير مرئي background scanning للتعرف على الفيروسات وتدميرها.
- اصدار انذارات alerts ضد الفيروسات الطارئة وتهديدات الامان security threats واعطاء الخيار لإزالتها او تثبيطها ومعرفة معلومات اكثر عنها.
- مراقبة البريد الالكتروني والرسائل وعمليات التحميل downloads.
- ارسال رسائل الكترونية لقسم الدعم الفني بالشركة المنتجة للحصول على الدعم في حالة الحاجة اليه.

متطلبات النظام :

- جهاز كمبيوتر مع معالج PII او اعلى.
- نظام تشغيل ويندوز 98 أو 2000 أو XP
- ذاكرة 128 أو أعلى
- قرص صلب يحتوي على 40 ميجا
- انترنت اكسبلورر 5.5 او اعلى

ويوضح شكل 1 نافذ البرنامج



شكل -1

استخدام ActiveShield

يحتوي البرنامج علي ActiveShield وهو درع الحماية حيث يتم تحميله تلقائيا في الذاكرة ويتم تفعيله تلقائيا بعد تنصيب installation البرنامج واعادة تحميل الجهاز. وعند عمل تحديث تلقائي من خلال update wizard يتم اخلاء الذاكرة من ActiveShield مؤقتا حتى ينتهي update wizard ثم يتم تفعيله مرة اخرى.
اذا حاول المستخدم تعطيل ActiveShield فهذا معناه ان جهاز الكمبيوتر خارج نطاق الحماية وعدم امكانية التحديث ولابد من التأكد من عدم الاتصال بالانترنت في هذه الحالة.
فحص البريد الاكتروني والملفات المرفقة
ان خاصية فحص البريد والتخلص من الفيروسات التي قدتكون ملتصقة بها يتم تفعيلها عن طريق Scan e-mail and attachments كما يظهر في شكل -1. وعند تفعيل هذا الخيار يقوم ActiveShield بالفحص تلقائيا لل inbound POP3 و outbound SMTP والمرفقات attachments ومسح الفيروسات العالقة بها.

فحص الدودة Scanning Worms

من المميزات الكبيرة الموجودة في البرنامج انه يستطيع مراقبة الانشطة المشبوهة suspect activity التي ربما تشير الي تعرض الجهاز للخطر.فعندما يقوم البرنامج بعمل فحص وتنظيف scan and clean فان WormStopper ™ يمنع الفيروسات الدود worms من الاختراق. ويعرف worm بأنه فيروس مقيم في الذاكرة ذاتيا self replicating virus وربما يرسل نسخ من نفسه خلال البريد الاكتروني. وفي حالة عدم وجود WormStopper فان هذا الفيروس يؤدي الي انخفاض اداء الجهاز وابطاء سرعته وقد نصل الي توقف النظام halt system .
ويقوم WormStopper بتعيين الانشطة المشبوهة وارسال انذارات وعمل حجز blocking لهذة الانشطة والتي قد تضم:-

- محاولة ارسال بريد الكتروني لاكبر مجموعة من الناوين الموجودة في address book .
- محاولة ارسال رسائل متعددة multiple message بطريقة سريعة.

لذا يفضل تفعيل هذة الخاصية Enable WormStopper.

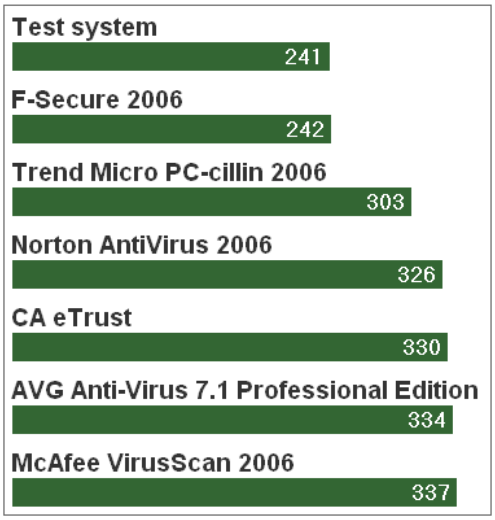
فحص كل الملفات

من المستحسن تفعيل خاصية all files في ActiveShield حيث يقوم البرنامج بفحص جميع الملفات زانواعها المختلفة وهذا يؤدي الي الحصول علي اعلى درجات الفحص والحماية. كما يعطي البرنامج خيارا آخر بفحص ملفات البرامج والمستندات فقط مما يعطي سرع افضل على حساب الحماية الكاملة.

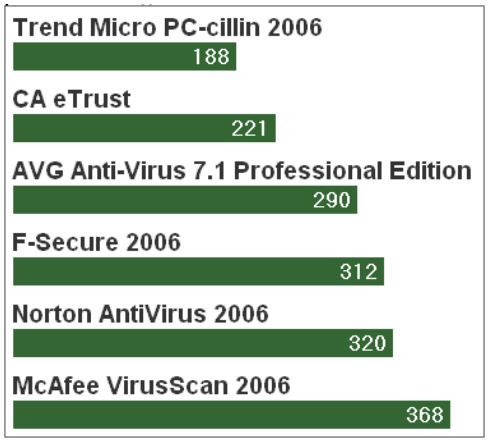
مما سبق نتبين ان هذا البرنامج ومثيلاته من البرامج لا غنى عنة في ظل التهديدات الاتي يواجها مستخدمو الحاسب والمخاطر التي قد يتعرضون لها في حالة وجود مثل هذه البرامج التي توفر حماية كبيرة للبيانات والمعلومات كما توفر الحماية ضد المتلصصين.

تقييم الآداء 3

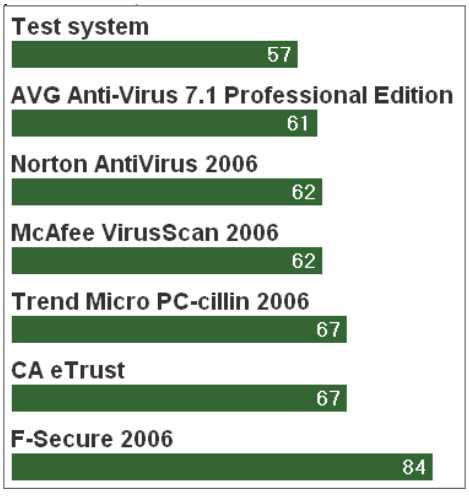
ونظرا لوجود العديد من البرامج التي تقوم بمهمة الحماية ومكافحة الفيروسات كان لابد من عمل مقارنة بين هذه البرامج ومن الجير بالذكر ان هذه البرامج تستهلك جزء كبير من ذاكرة الحاسب والقرص الصلب كما تؤدي الى انخفاض في سرعة اداء الجهاز مما يؤدي الى ضيق المستخدمين بهذه البرامج ولكن اذا تفحصنا الدور الهام التي تقوم به هذه البرامج لوجدناها في غاية الاهمية بحيث يمكن ان نقبل عيوبها بصدر رحب في ظل الخدمات التي توفرها لنا. والشك التالي يوضح مقارنة بين اشهر هذه البرامج من هيث الاداء حيث تدل الاعمدة الاقصر طولا على معدل اداء اسرع ويعتبر البرنامج الذي يتحدث التريز عنه ليس الافضل .
واعتمدت عملية التقييم على DEEP SCANNING و SCAN SPEED و BOOT SPEED



DEEP SCANING (SEC)



SCAN SPEED (SEC)



BOOT SPEED (SEC)