Malware

البرمجيات الخبيثة

جميل حسين طويله

دليل عملي لاستخدام البرمجيات الخبيثة وبرمجيات التجسس
وإجراءات الوقاية والحماية منها

- أحصنة طروادة
- مسجلات ضربات المفاتيح
- الفيروسات
- برمجيات التجسس

البرمجيات الخبيثة

Malware

دليل عملي لاستخدام البرمجيات الخبيثة
وبرمجيات التجسس
وطرق الوقاية والحماية منها

حول هذا الكتاب

شرح مفصل لأنواع البرمجيات الخبيثة والطرق التي يستخدمها الهاكرز في صناعة هذه البرمجيات ونشرها من أجل عدوى وإصابة أجهزة الضحايا وطرق تجاوز الحماية المطبقة من قبل مضادات الفيروسات وبرامج الحماية، بالإضافة لطرق وإجراءات الوقاية والحماية من هذه البرمجيات.

وقد يتسأل البعض أعم محتوى هذا الكتاب

أليس شرح لطرق الاختراق والتجسس؟

أليست هذه البرمجيات والتقنيات مخالفة للقوانين؟

الإجابة على كلا السؤالين هي لا

العلم ليس مخالف للقوانين ولكن طريقة استخدام هذا العلم يمكن أن تكون بشكل سيء أو مخالف للقوانين.

الغاية من شرح هذه التقنيات ليست تعليم الناس طرق الاختراق والتجسس بل توعية الناس ليتمكنوا من النظر إلى أجهزتهم من عيون الهاكرز ليصبحوا قادرين على حماية أنفسهم من الاختراق والتجسس.

معظم البرمجيات الخبيثة المستخدمة في هذا الكتاب هي برمجيات بسيطة ويتم اكتشافها من معظم برامج الحماية ومضادات الفيروسات.

الهاكرز الحقيقيون يستخدمون برمجيات أكثر تعقيداً ولكن طرق الحماية هي نفسها.

حاولت عدم التعمق بالمواضيع التقنية لتكون مواضيع هذا الكتاب مفهومة لأشخاص الذين لا يملكون معلومات تقنية سابقة.

إخلاء المسؤولية

الهدف من هذا الكتاب هو التوعية الرقمية.

رجاءً لا تستخدم أي من البرمجيات أو الطرق المشروحة في هذا الكتاب بشكل مؤذي أو مخالف للقوانين.

الكاتب يخلي مسؤوليته عن أي استخدام للبرمجيات أو الطرق المشروحة في هذا الكتاب بشكل مؤذي أو مخالف للقوانين.

رخصة الكتاب

هذا الكتاب نشر تحت رخصة المشاع الإبداعي Creative Commons license وهو كتاب مجاني

عن الكاتب

جميل حسين طويله

مهندس اتصالات سوري

مختص في الشبكات اللاسلكية وأمن المعلومات واختبار الاختراق

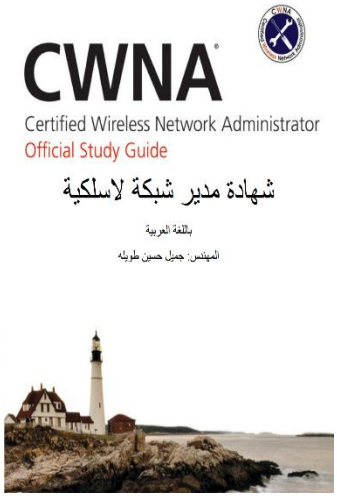
dolphin-syria@hotmail.com

الإهداء

إلى روح أبي وأمي رحمهما الله

إلى أرواح شهداء وطني سوريا

منشورات سابقة



مدير شبكة لاسلكية

(3 أجزاء)

http://www.kutub.info/library/book/13857

http://www.kutub.info/library/book/13890

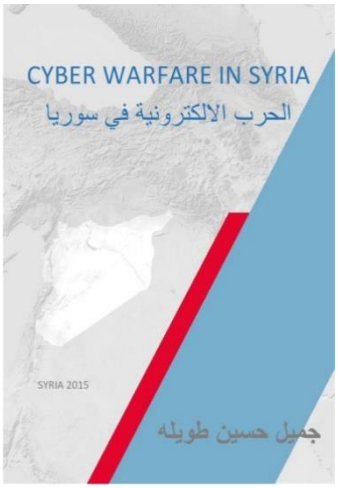
http://www.kutub.info/library/book/14144

اختراق الشبكات اللاسلكية

http://www.kutub.info/library/book/15987

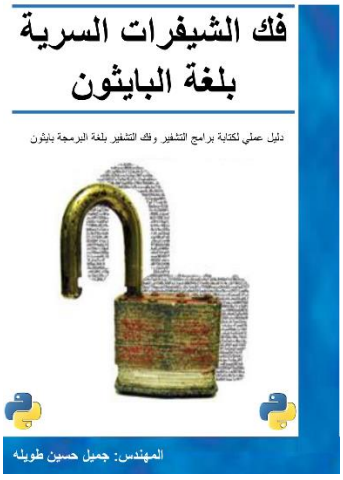
الحرب الالكترونية الأميركية في العراق

https://arabcyberwarrior.files.wordpress.com/2015/01/american-cyber-war-in-iraq.pdf



الحرب الالكترونية في سوريا

https://arabcyberwarrior.files.wordpress.com/2015/02/cyber-warfare-in-syria.pdf



فك الشيفرات السرية بلغة البايثون

https://arabcyberwarrior.files.wordpress.com/2015/03/arabic-hacking-secret-ciphers-with-python.pdf

الفهرس

البرمجيات الخبيثة

Malware هي اختصار ل malicious software وتعني "برمجية خبيثة"

البرمجيات الخبيثة: هي برامج تهدف إلى إلحاق الضرر بالحاسوب أو تعطيله وجمع المعلومات والتجسس وعرقلة العمليات، وتتمكن بطريقة غير شرعية من عدوى نظام الحاسب بدون معرفة أو علم المستخدم من أجل اختراق جهازه والتجسس عليه

أنواع البرمجيات الخبيثة:

١- Keylogger مسجل ضربات لوحة المفاتيح:

وهو عبارة عن جهاز hardware أو برنامج software يقوم بمراقبة وتسجيل كل حرف يتم كتابته بواسطة لوحة المفاتيح كما يمكن أن يقوم أيضاً بالتقاط وتسجيل لقطات للشاشة.

٢- Trojan Horse حصان طروادة (تروجان):

وهو أكثر أنواع البرمجيات الخبيثة انتشاراً وأكثرها خطورة.

للوهلة الأولى يبدو أنه برنامج شرعي وسليم ولكنه في الحقيقة يمنح المهاجم قدرة كاملة على الوصول والتحكم بجهاز الضحية.

يعود سبب التسمية إلى الأسطورة اليونانية لحصار الإغريق لمدينة طروادة حيث قام الإغريقيون باستخدام حيلة من خلال صناعة حصان خشبي كبير وملئه بالمحاربين وتقديمه كهدية لطرواديين على أنه هدية سلام.

قبل الطروايون الهدية واحتفلوا بفك الحصار عن مدينتهم وعندها خرج المحاربون الاغريق من داخل الحصان وكان سكان طروادة في حالة سكر

فقام المحاربون بفتح بوابات المدينة للسماح لبقية الجيش بدخولها وسقطت طروادة وحرقت وقتل رجالها.

وبشكل مشابه تطلق هذه التسمية على البرامج التي تبدو للوهلة الأولى أنها برامج سليمة ولكن في الحقيقة هي برامج خبيثة تسمح للمهاجم التحكم بجهاز الضحية واختراقه.

٣- RAT أداة الإدارة عن بعد:

وهي اختصار ل Remote Administration Tool وتعتبر من البرمجيات الخبيثة ذات الخطورة الشديدة فعندما يتم تنصيب هذه الأداة على جهاز الضحية فإن المهاجم يستطيع أن يقوم بكل شيء عن بعد، كتنصيب مسجل ضربات المفاتيح Keylogger أو إيقاف تشغيل الجهاز أو حذف الملفات.

٤- Viruses الفيروسات:

وهي عبارة عن برامج يتم كتابتها وتطويرها من أجل إصابة أجهزة الحاسب وعندما تقوم بإصابة جهاز ما فهي تقوم بنسخ أو تكررا نفسها لتقوم بعدوى وإصابة أجهزة أخرى وهي تتكاثر وتنتشر بالاعتماد على ملفات أخرى.

٥- Worms الديدان:

وهي تشبه الفيروسات والفرق الوحيد بينهما هو أن الديدان تعتمد على نفسها للتكاثر وعدوى الأجهزة الأخرى وتتميز بسرعة الانتقال.

عندما تقوم الدودة worm بعدوى أو إصابة جهاز فهي تقوم بنسخ وتكرار نفسها وهي تنتقل بسرعة وتنتشر داخل الشبكة وتستهلك موارد الشبكة أثناء انتشارها.

الديدان تعتبر الخطر الرئيسي الذي يهدد الشبكات الكبيرة.

٦- Adware برمجيات الإعلانات والتجسس:

وهي اختصار ل Advertisement software

وتسمى أيضاً Spyware "برمجيات التجسس"

وهي مصممة لتقوم بجمع المعلومات وعرض الإعلانات على الجهاز المصاب بها.

بعض هذه البرمجيات تحوي على فيروسات مؤذية وبرامج تجسس.

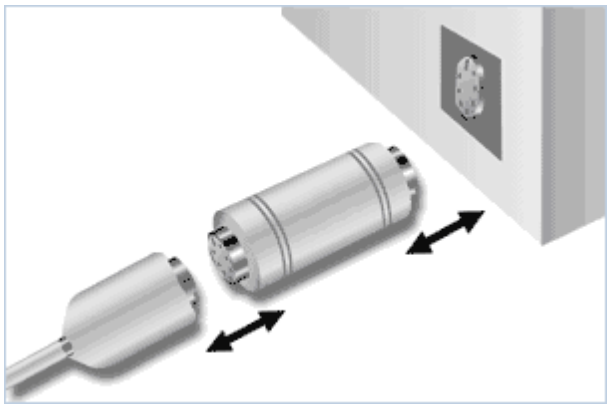
مسجل ضربات المفاتيح keylogger

يمكن تصنيفها في نوعين رئيسيين:

١. Hardware Keylogger
٢. Software Keylogger

Hardware Keylogger

عبارة عن جهاز صغير يتم وصلة بين لوحة المفاتيح ومنفذ USB or PS/2 في جهاز الحاسب ويقوم بتسجيل كل حرف يتم كتابته بواسطة لوحة المفاتيح.



وهو عبارة عن قطعة صغيرة لا تلفت انتباه الضحية وتحوي على ذاكرة داخلية تقوم بتخزين كل حرف تم كتابته من خلال لوحة المفاتيح

Keycobra

أفضل جهاز مسجل لضربات المفاتيح

يوجد العديد من hardware keylogger ولكن انا أنصحك باستخدام Keycobra لأنه يسجل كمية كبيرة من ضربات المفاتيح ويمكن أن يسجل 2 بليون حرف (أكثر من مليون صفحة) ويقوم بحفظها وتنظيمها داخل ملف نظام من نوع flash FAT

كما أنه يدعم عملية استرداد سريعة للبيانات وهو لا يحتاج لأي برامج تعريف ويمكن أن يعمل مع أنظمة التشغيل ويندوز و لينكس وماك ولا يمكن اكتشافه من قبل مضادات الفيروسات أو برامج كشف البرمجيات الخبيثة

ومتوفر بنوعين USB and PS2

ميزات Keycobra

- يقوم بتسجيل كل الأحرف (حتى كلمة سر الفيس بوك)
- مساحة ذاكريه كبيرة
- قائمة نصية متقدمة من أجل مشاهدة البيانات المسجلة تحوي على إمكانية البحث عن الكلمات أو العبارات

Keysnatch

متوفر بعدة أنواع PS2 , USB or WiFi

ويدعم عدة أنظمة تشغيل ويحوي على مساحة ذاكريه كافية لتسجيل وحفظ ٢ بليون حرف ويدعم سرعة تحميل تصل إلى 125 KB/S ولا يحتاج لأي برامج تعريف ولا يمكن كشفه من قبل مضادات الفيروسات وبرامج كشف برمجيات التجسس.

WiFi Keylogger

يحوي في داخله على مرسل ومستقبل خاص بالشبكات اللاسلكية كما أنه مُبرمج ليتعامل مع TCP/IP stack وهذا يعطيه القدرة على الاتصال بالإنترنت بشكل لاسلكي من خلال الاتصال بجهاز الاكسس بوينت Access point

كيف يعمل:

عندما يتصل مع الأكسس بوينت فإن Keysnatch wifi keylogger سوف يقوم بإرسال كل حرف يقوم الضحية بكتابته إلى عنوان الايميل الذي يقوم المهاجم باختياره ولا تستطيع مضادات الفيروسات كشفه.

يتم استخدام hardware keylogger في الحالات التي يستطيع المهاجم بها الوصول بشكل فيزيائي إلى جهاز الضحية.

أما في الحالات التي لا يتمكن المهاجم من الوصول الفيزيائي إلى جهاز الضحية فعندها يتم استخدام software keylogger

Software Keylogger

يمكن تصنيف software keyloggerإلى نوعيين:

١- محلي Local Keylogger

٢- بعيد Remote Keylogger

مسجل ضربات المفاتيح المحلي

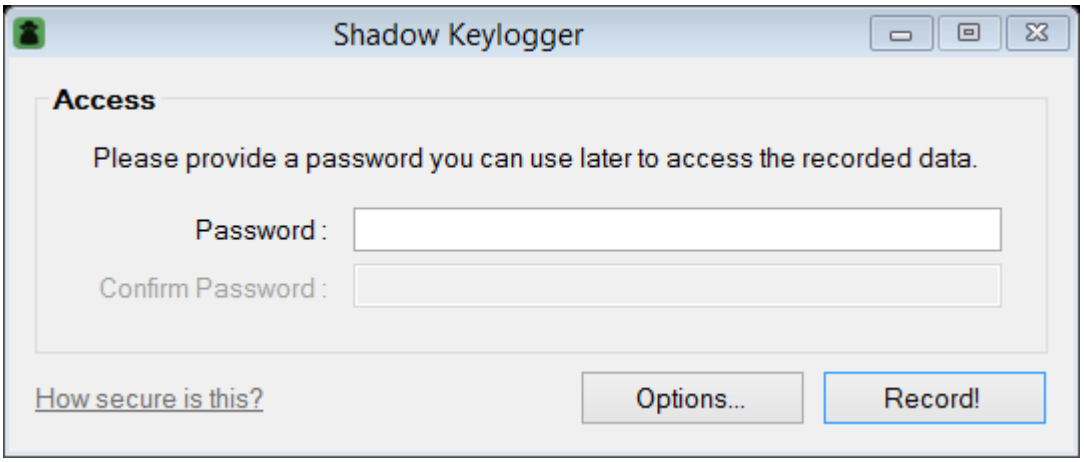
Local Keylogger

يستخدم من أجل مراقبة أجهزة كمبيوتر محلية وهو سهل التنصيب ومن الصعب اكتشافه لأنه يخفي نفسه من شريط المهام وسجلات الويندوز.

وعندما تريد رؤية السجلات التي قام بتسجيلها (الأحرف ولقطات الشاشة) تقوم بالضغط على مفاتيح معينة أو كلمة سر معينة أنت تختارها عند القيام بعملية التنصيب.

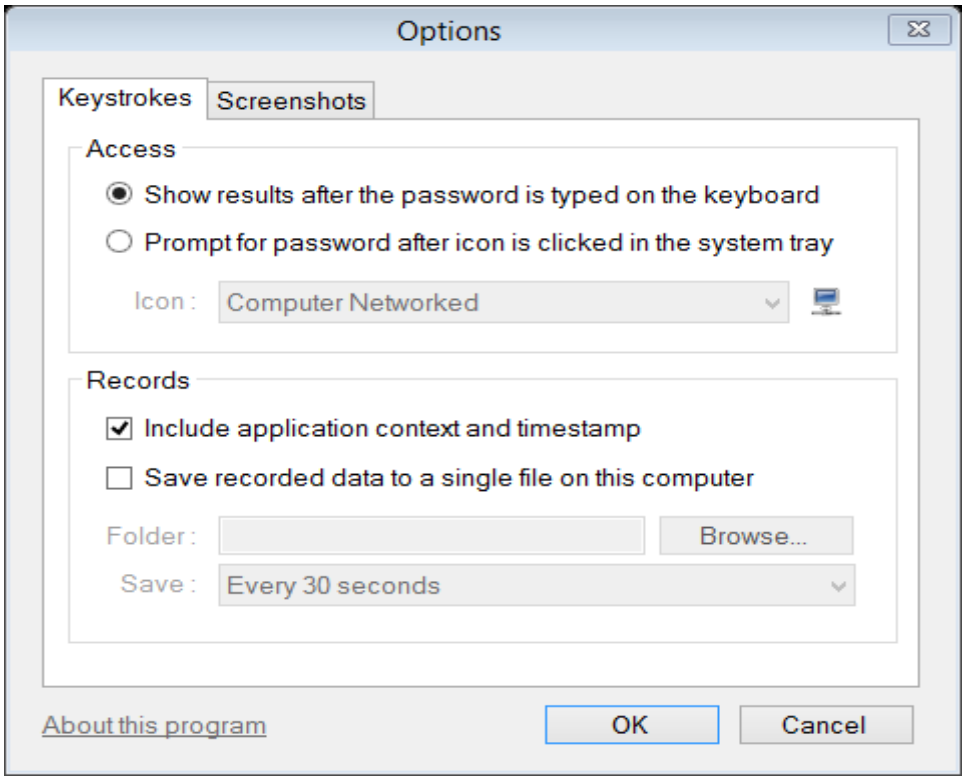
Shadow Keylogger

قم بتحميل Shadow ثم قم بفتحه وستظهر الشاشة التالية التي تطلب منك إدخال كلمة سر وتأكيدها.

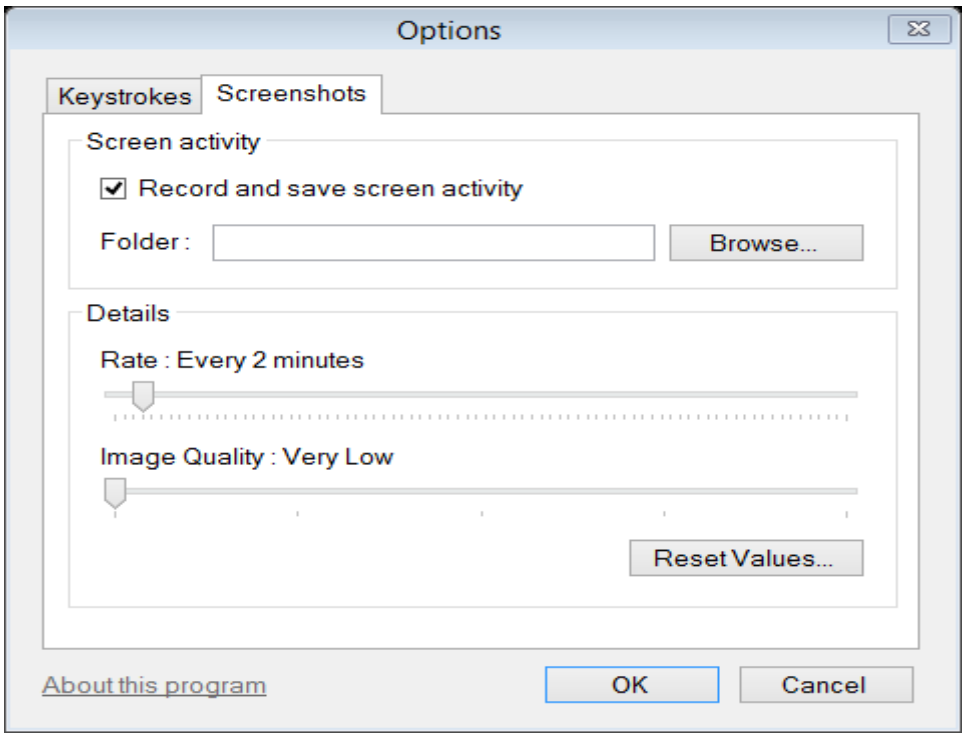


قم بإدخال كلمة سر تختارها أنت، كما يمكنك الضغط على الخيارات Options لتظهر الشاشة التالية والتي يمكن من خلالها اختيار طريقة إظهار النتيجة إما من خلال كتابة كلمة السر التي قمت بإدخالها على لوحة المفاتيح أو إظهار نافذة منبثة بعد الضغط على أيقونة معينة تقوم أنت باختيارها و يطلب منك إدخال كلمة السر لتظهر السجلات التي تم تسجيلها.

كما يمكن اختيار حفظ السجلات التي تم تسجيلها في ملف معين تقوم أنت بتحديد مساره.

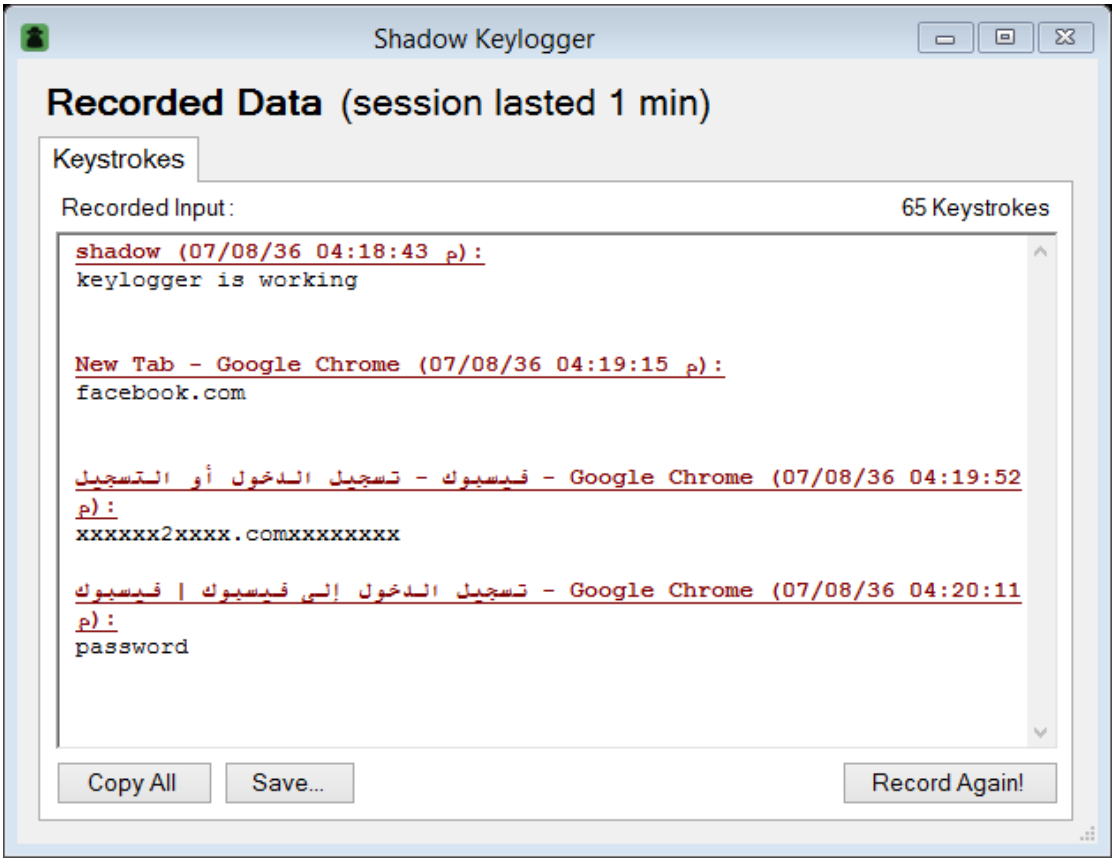


كما يمكن التقاط صور لسطح المكتب وحفظها في المسار الذي تقوم أنت باختياره ويمكنك تحديد الفترة الزمنية بين كل صورة يتم التقاطها كما يمكنك اختيار مستوى دقة الصورة.



عند الانتهاء من تحديد الخيارات المطلوبة قم بالضغط على Record

الآن كل حرف يتم كتابته سيتم تسجيله ولإظهار النتيجة قم بكتابة كلمة السر التي قمت بإدخالها لتظهر النتيجة كما في الشكل التالي



SpyAgent

يمكن أن يستخدم لمراقبة جهاز محلي أو جهاز بعيد وهو يعمل بسرية تامة ولا يمكن كشفه من قبل الضحية.

دليل تنصيب Spyagent

الخطوة ١:

قم بتحميل Spyagent ثم قم بفتح ملف التنصيب

وبعد الانتهاء من عملية التنصيب يمكنك حذف ملف التنصيب من أجل عدم لفت انتباه الضحية.

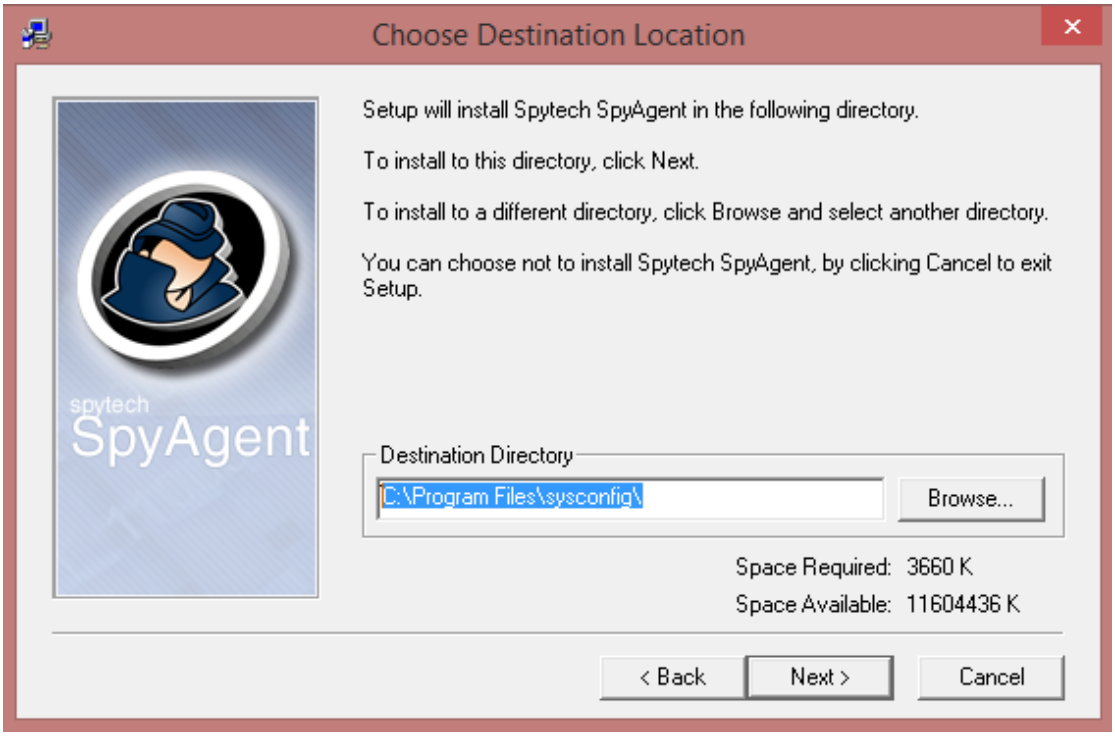
الخطوة ٢:

استمر في عملية التنصيب إلى أن تصل إلى الشاشة التالية التي يمكن من خلالها اختيار مسار المجلد المراد تنصيب Syyagent فيه

أنا أنصحك بتغير المسار الافتراضي

(c:\program files\spytech software……)

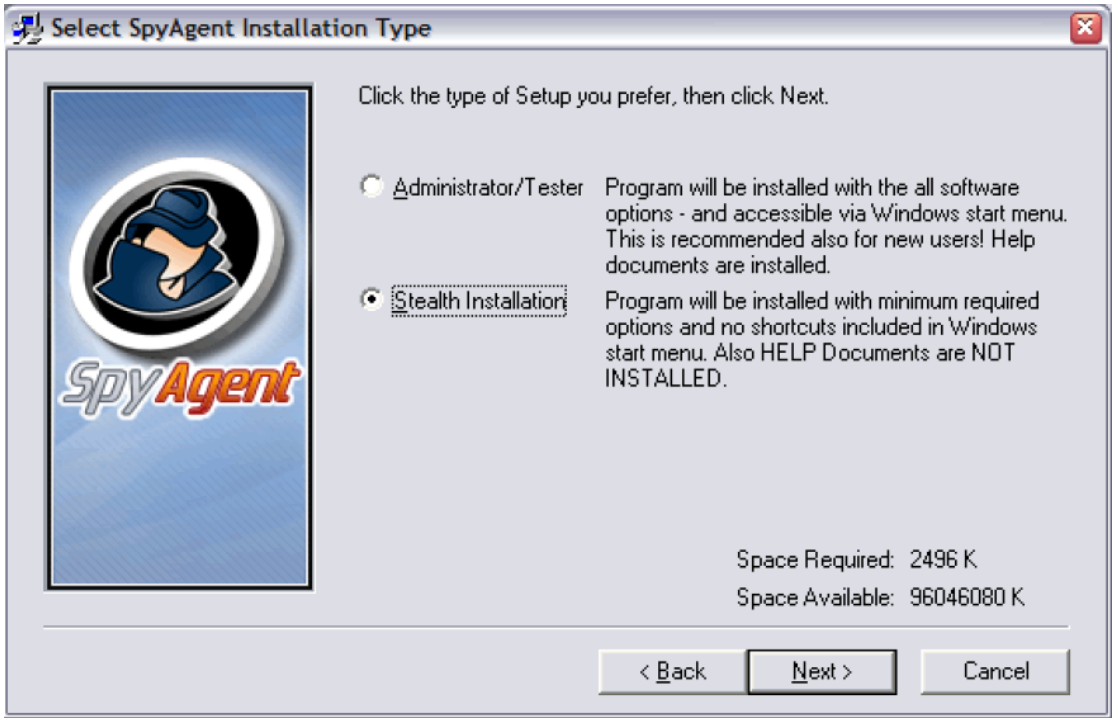
إلى المسار الذي يظهر بالشكل التالي وتذكر هذا المسار من أجل الوصول إلى هذا البرنامج



الخطوة ٣:

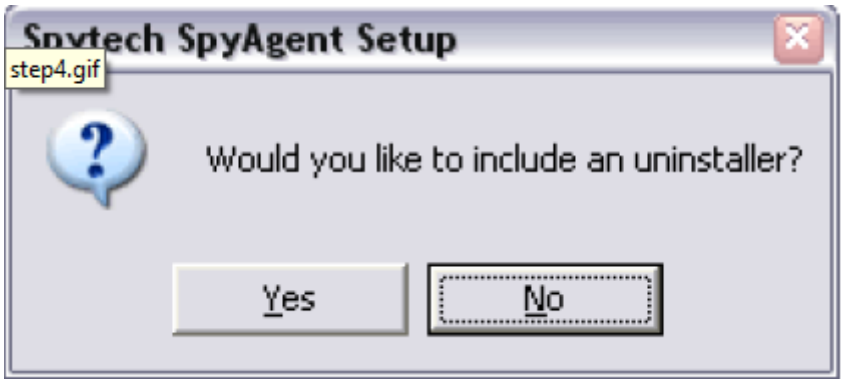
استمر بعملية التنصيب إلى أن تصل إلى الشاشة التالية والتي يمكن من خلالها اختيار نوع البرمجية المراد تنصيبها

إذا كنت تريد عدم ظهور SpyAgent في قائمة ابدأ وعدم إظهار أي ملفات فقم باختيار التنصيب السري Stealth installation كما في الشكل التالي



الخطوة ٤:

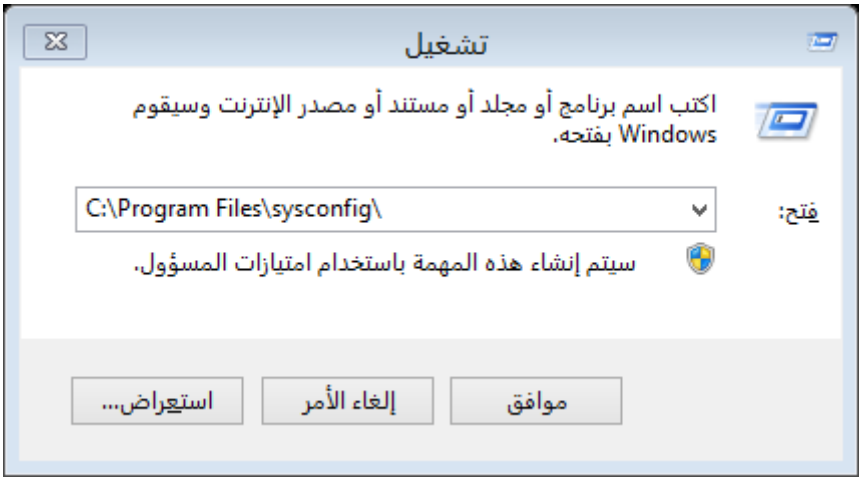
عند انتهاء عملية التنصيب سوف تظهر شاشة تسألك فيما إذا كنت تريد تضمين إلغاء التنصيب، من أجل السرية التامة قم باختيار NO

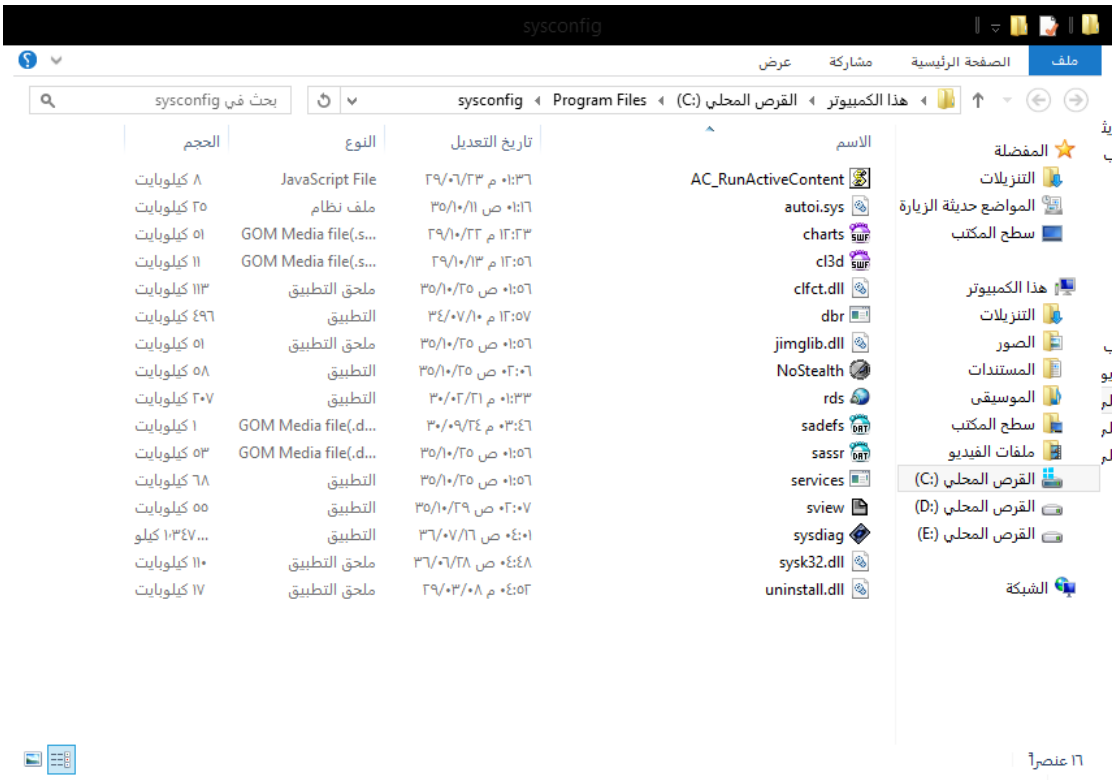


الخطوة ٥:

بعد الانتهاء من عملية التنصيب يمكنك إعداد SpyAgent

قم بالضغط على زر الويندوز + R وقم بكتابة المسار الذي قمت بتنصيب الملف فيه





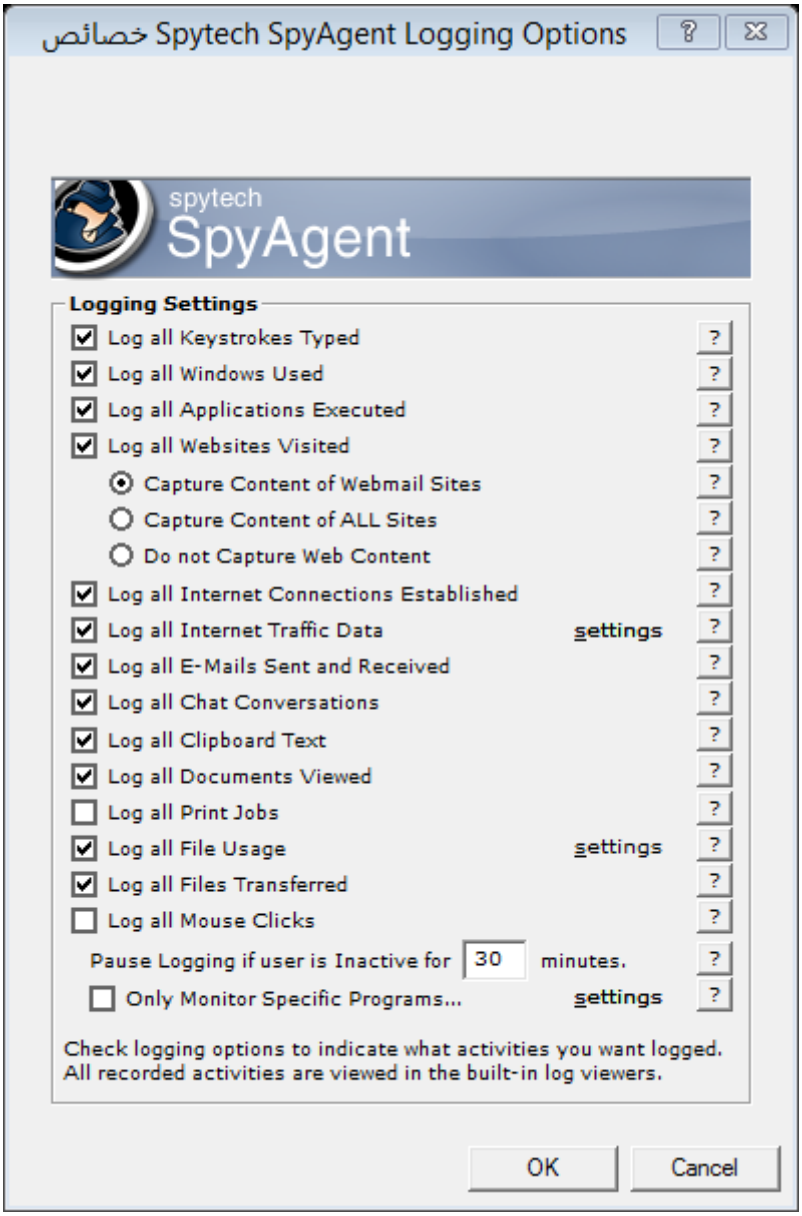
الخطوة ٦:

قم بفتح الملف NoStealth ثم قم بإدخال كلمة السر التي قمت بإدخالها بعد عملية التنصيب لتظهر نافذة البرنامج التالية

قم باختيار General من القائمة اليمنية من أجل إعداد الخيارات الأساسية


خصائص Spytech SpyAgent Options
AutoArchive
AutoClear
AutoRemove
General
Alert Notifications
Instant Log Retrieval
spytech
SpyAgent
When the Computer is Started...
Load SpyAgent for all users of this machine.
Load SpyAgent for this username only.
Do not load SpyAgent
When SpyAgent is Started...
Load SpyAgent in ACTIVE Monitoring Mode
Run SpyAgent in Stealth-Mode
For optimal STEALTH performance, make sure you check the above options to load SpyAgent on Windows startup in Active and Stealth mode.
Display Splash Warning on SpyAgent Startup
General Options
Show Password Prompt when Keyword is Typed
Show Summary Report when Monitoring is Stopped
Set/Change Your SpyAgent Password
OK
Cancel

ثم قم بالضغط على Logging من أجل إعداد خيارات التسجيل



الخطوة ٧:

قم بالضغط على Start Monitoring

سوف تظهر نافذة منبثقة تطلب منك إدخال كلمة السر وعندها سوف تبدأ عملية المراقبة والتسجيل.

الآن تعمل هذه البرمجية بشكل سري وعندما تقوم بإعادة تشغيل الجهاز سوف تعود هذه البرمجية للعمل وبشكل غير مرئي للضحية.

من أجل إيقاف العمل بالنمط السري stealth mode قم بفتح الملف NoStealth ثم قم بكتابة كلمة السر.

يمكنك رؤية السجلات التي تم تسجيلها وهي كل حرف تم كتابته بالإضافة للقطات الشاشة والمواقع التي تم زيارتها والبرامج التي تم استخدامها والملفات التي تم فتحها.

مسجل ضربات المفاتيح عن بعد

Remote Keylogger

تستخدم من أجل مراقبة الأجهزة عن بعد حيث يقوم المهاجم بتنصيب هذه البرمجية في جهاز الضحية من على بعد ويتم إرسال سجل ضربات المفاتيح ولقطات للشاشة وسجلات المحادثات إلى عنوان الايميل الذي يقوم المهاجم باستخدامه.

يوجد العديد من برمجيات التجسس البعيدة ولكن القليل منها مازال غير مكتشف من قبل مضادات الفيروسات.

معظم برمجيات التجسس المجانية يتم اكتشافها من قبل مضادات الفيروسات، يوجد أنواع من البرمجيات الخبيثة غير مجانية تستخدم طرق تشفير معينة لا تسمح لمضادات الفيروسات باكتشافها.

WinSpy

عبارة عن برمجية مراقبة تعمل بشكل سري ويمكنها مراقبة جهاز محلي أو جهاز بعيد وهي تقوم بمراقبة وتسجيل كل حرف يقوم الضحية بكتابته ويوجد العديد من الطرق التي يستخدمها الهاكرز من أجل تنصيب هذه البرمجية في جهاز الضحية عن بعد.

خطوات إعداد WinSpy:

الخطوة ١:

قم بتحميل WinSpy

الخطوة ٢:

بعد التحميل قم بتشغيل البرمجية ثم قم بخلق حساب جديد من خلال كتابة الاسم وكلمة السر كما في الشكل التالي

الخطوة ٣:

قم بالضغط على ctrl + shift + F12 وقم بتسجيل الدخول

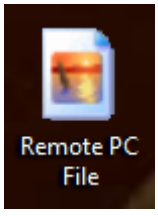
الخطوة ٤:

من القائمة العلوية اختر Remote ثم اختر Remote install

قم بتحديد مسار الصورة التي تريد استخدامها كطعم لخداع الضحية ثم قم بإدخال عنوان ايميل Gmail

هذه البرمجية تعمل فقط مع Gmail ولا تعمل مع Hotmail

الخطوة ٥:



قم بالضغط على Create remote file سوف يظهر الملف الناتج كالتالي

الآن يجب أن تقوم بإرسال هذه الملف إلى الضحية وخداع الضحية ليقوم بفتح هذا الملف ويمكنك القيام بذلك من خلال إرسال الملف عبر الايميل أو عبر البلوتوث أو رفع الملف في أحد المواقع وخداع الضحية ليقوم بتحميله من خلال إرسال رابط التحميل له وعندما يقوم الضحية بفتح هذا الملف سوف تصلك سجلات ضربات المفاتيح التي يقوم الضحية بكاتبتها إلى ايميل Gmail الذي قمت باستخدامه.

حصان طروادة Trojan

برمجية خبيثة نبدو للوهلة الأولى أنها برنامج أو ملف سليم (صورة أو ملف صوتي أو مقطع فيديو) وعند فتحه يقوم بتنصيب سيرفر server (خادم) على جهاز الضحية والذي يمنح المهاجم سيطرة كاملة على الجهاز وبدون علم الضحية.

ويصبح المهاجم قادراً على سرقة أو حذف ملفات الضحية وتثبيت برامج أخرى مثل برنامج مسجل ضربات المفاتيح keylogger وسرقة المعلومات السرية كمعلومات تسجيل الدخول ومعلومات بطاقات الائتمان وتعطيل الجدران النارية ومضادات الفيروسات والاتصال مع جهاز الضحية بشكل عكسي والتحكم به بشكل كامل كما يصبح قادر على استخدام جهاز الضحية في أعمال غير شرعية كالقيام بهجوم منع الخدمة Denial Of Service

النظام المخترق يمكن أن يستخدم لأغراض غير شرعية ومخالفة للقوانين وبالتالي سوف يتحمل الضحية كامل المسؤولية القانونية.

أعراض الإصابة بحصان طروادة

- إعادة توجيهك إلى صفحات انترنت غير مرغوبة ولم تقم بطلبها
- حركة مؤشر الماوس بشكل عشوائي على الشاشة
- ظهور رسائل غريبة على الشاشة
- اختراق حسابات التواصل الاجتماعي الخاصة بك وتغير كلمات السر لها
- فتح باب السواقة من تلقاء ذاته
- تعطيل الجدران النارية وتوقف مضاد الفيروسات عن العمل
- إيقاف تشغيل الجهاز أو إعادة تشغيله بشكل تلقائي

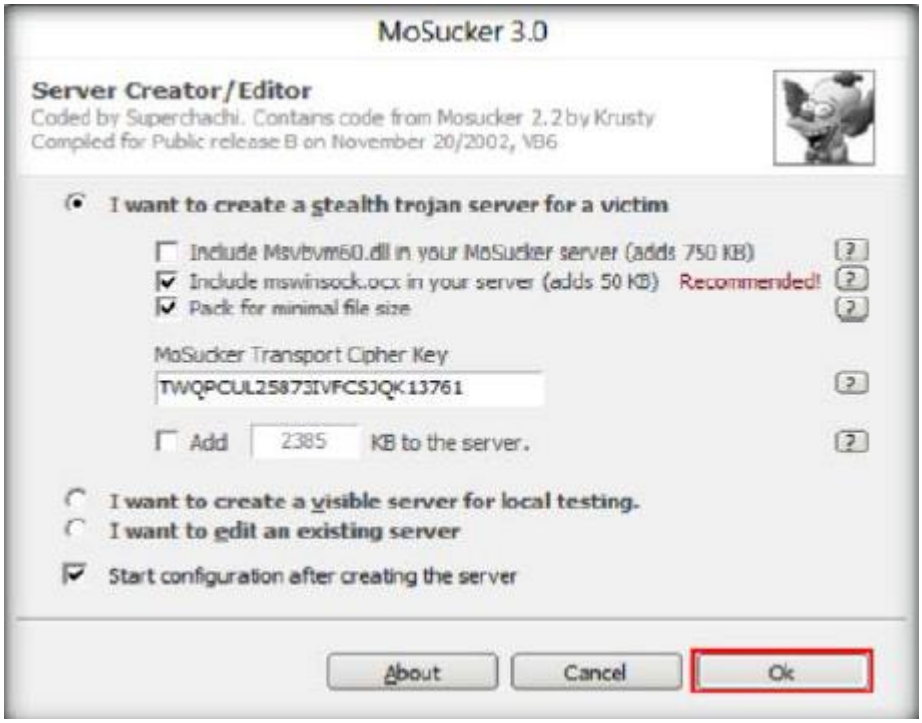
MoSuker Trojan

عبارة عن تروجان ذو واجهة رسومية يتيح للمهاجم الدردشة مع الضحية و إلتقاط صور لسطح المكتب والتحكم بالماوس والوصول إلى الملفات وسرقة كلمات السر والمعلومات السرية بالإضافة إلى فتح وإغلاق باب السواقة.

خطوات إعداد سيرفر تروجان باستخدام MoSuker

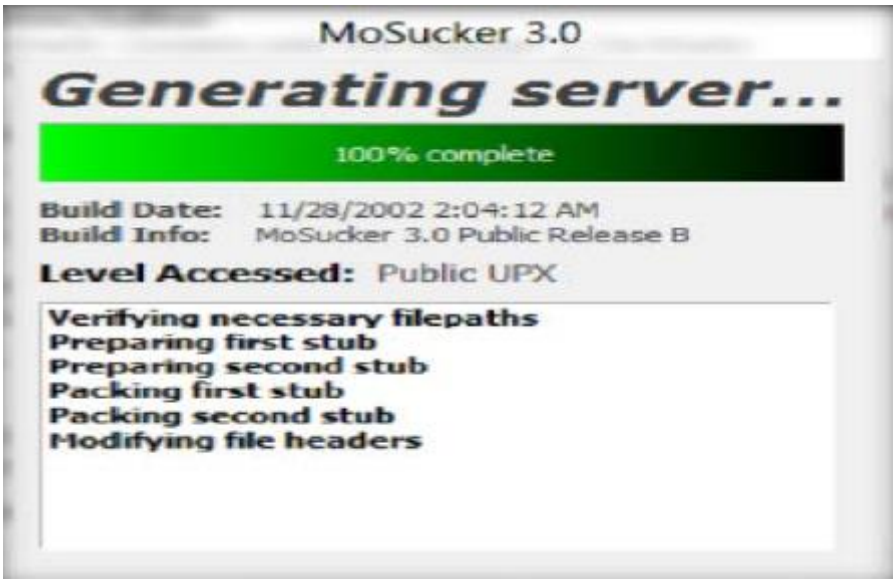
الخطوة ١:

بعد تحميل هذه الأداة قم بفتح CreateServer.exe لتظهر الشاشة التالية ثم قم بالضغط على OK مع ترك الإعدادات الافتراضية كما هي.



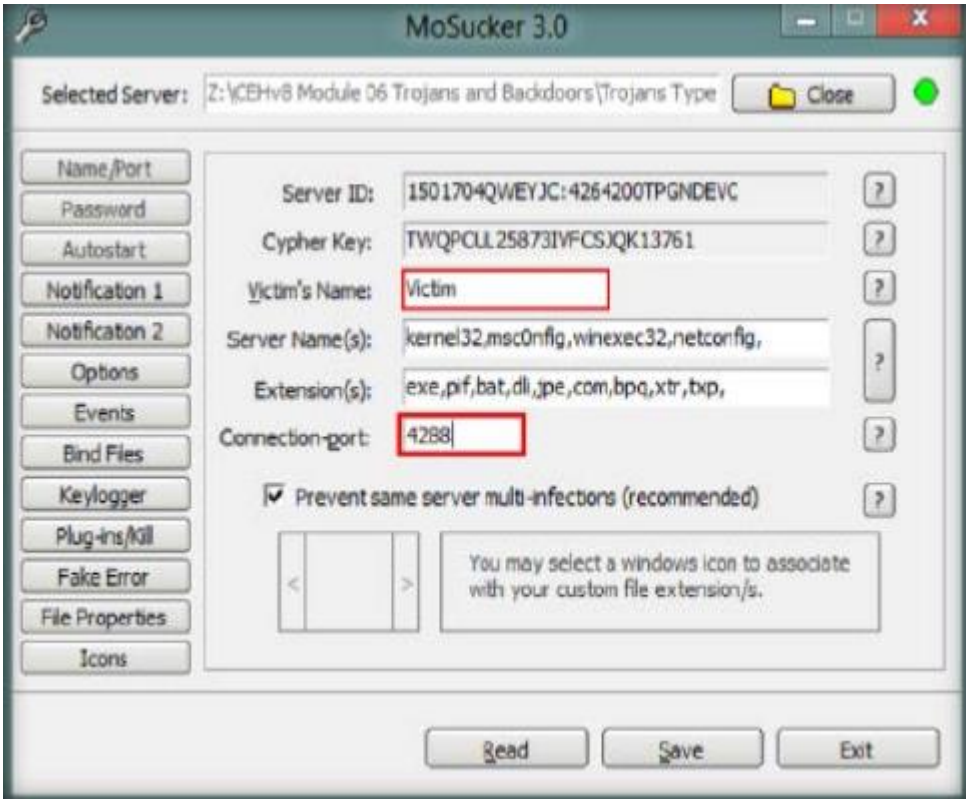
الخطوة ٢:

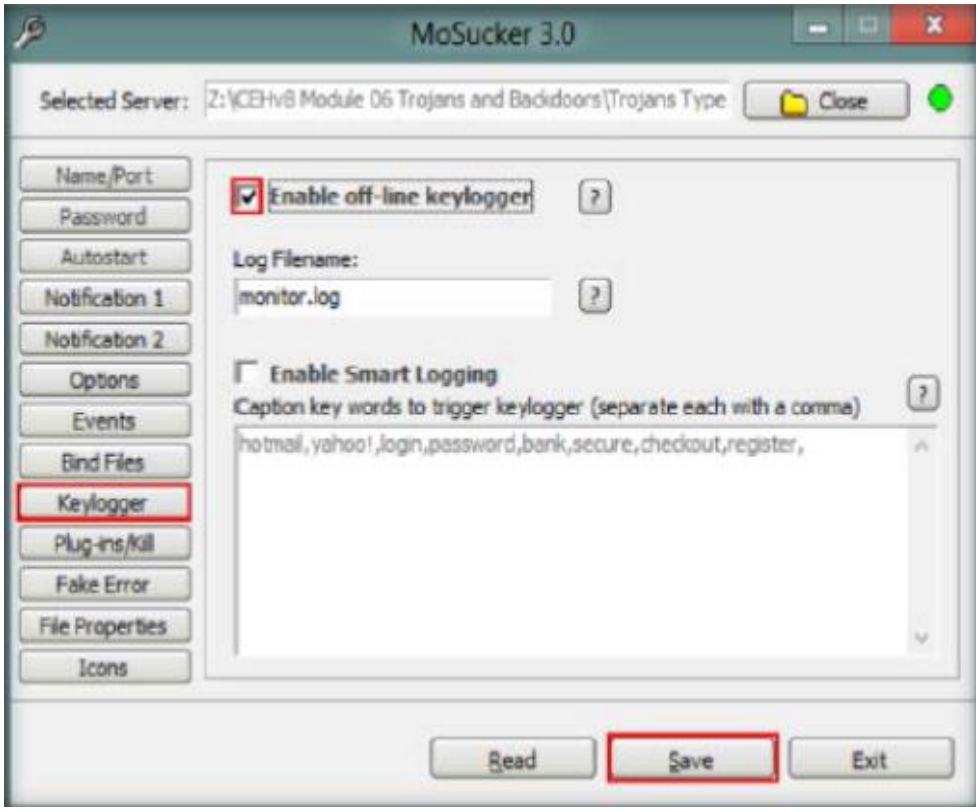
بعد إدخال اسم ومكان حفظ السيرفر تظهر الشاشة التالية



الخطوة ٣:

بعد الانتهاء من الخطوة السابقة تظهر الشاشة التالية والتي يمكن من خلالها ضبط الإعدادات والمهام التي سوف يقوم بها التروجان


MoSucker 3.0
Selected Server:
Z:\CEHv8 Module 06 Trojans and Backdoors\Trojans Type
Close
Name/Port
Password
Autostart
Notificaton 1
Notificaton 2
Options
Events
Bind Files
Keylogger
Plug-ins/Kill
Fake Error
File Properties
Icons
Server ID:
1501704QWEYJC:4264200TPGNDEVC
Cypher Key:
TWQPCLL25873IVFCSJQK13761
Victim's Name:
Victim
Server Name(s):
kernel32,msc0nfig,winexec32,netconfig,
Extension(s):
exe,pif,bat,dli,jpe,com,bpq,xtr,txp,
Connection-port:
4288
Prevent same server multi-infections (recommended)
You may select a windows icon to associate with your custom file extension/s.
Read
Save
Exit


MoSucker 3.0
Selected Server:
Z:\CEHv8 Module 06 Trojans and Backdoors\Trojans Type
Close
Name/Port
Password
Autostart
Notification 1
Notification 2
Options
Events
Bind Files
Keylogger
Plug-ins/Kill
Fake Error
File Properties
Icons
Enable off-line keylogger
Log Filename:
monitor.log
Enable Smart Logging
Caption key words to trigger keylogger (separate each with a comma)
hotmail,yahoo!,login,password,bank,secure,checkout,register,
Read
Save
Exit

الخطوة ٤:

الآن وبعد الانتهاء من إعداد السيرفر قم بإرساله إلى الضحية بعد دمجه مع ملف أخر وتغير شكل الأيقونة من أجل خداع الضحية وبمجرد أن يقوم الضحية بفتح هذا الملف يتم تفعيل التروجان.

الخطوة ٥:

قم بفتح MoSuker.exe لتظهر الشاشة التالية

والتي يمكن من خلالها الاتصال بالضحية والتحكم بجهازه.

ProRat

عبارة عن تروجان و أداة تحكم عن بعد RAT تقوم بفتح منفذ port في جهاز الضحية وتسمح للمهاجم الاتصال والتحكم بجهاز الضحية بشكل كامل.

عندما يتم تنصيب سيرفر هذه الأداة على جهاز الضحية يصبح من الصعب جداً إزالتها بدون استخدام مضاد فيروسات قوي وله قاعدة بيانات محدثة.

التالي هي خطوات إعداد سيرفر ProRat من أجل التحكم بجهاز الضحية

الخطوة ١:

قم بتحميل ProRat

كلمة سر فك الضغط هي "Pro"

يجب أن تقوم بإيقاف مضاد الفيروسات قبل أن تتمكن من استخدام ProRat

الخطوة ٢:

قم بالضغط على زر Create من أجل القيام بخلق ملف خبيث من نوع حصان طروادة Trojan file ثم قم باختيار Create prorate server

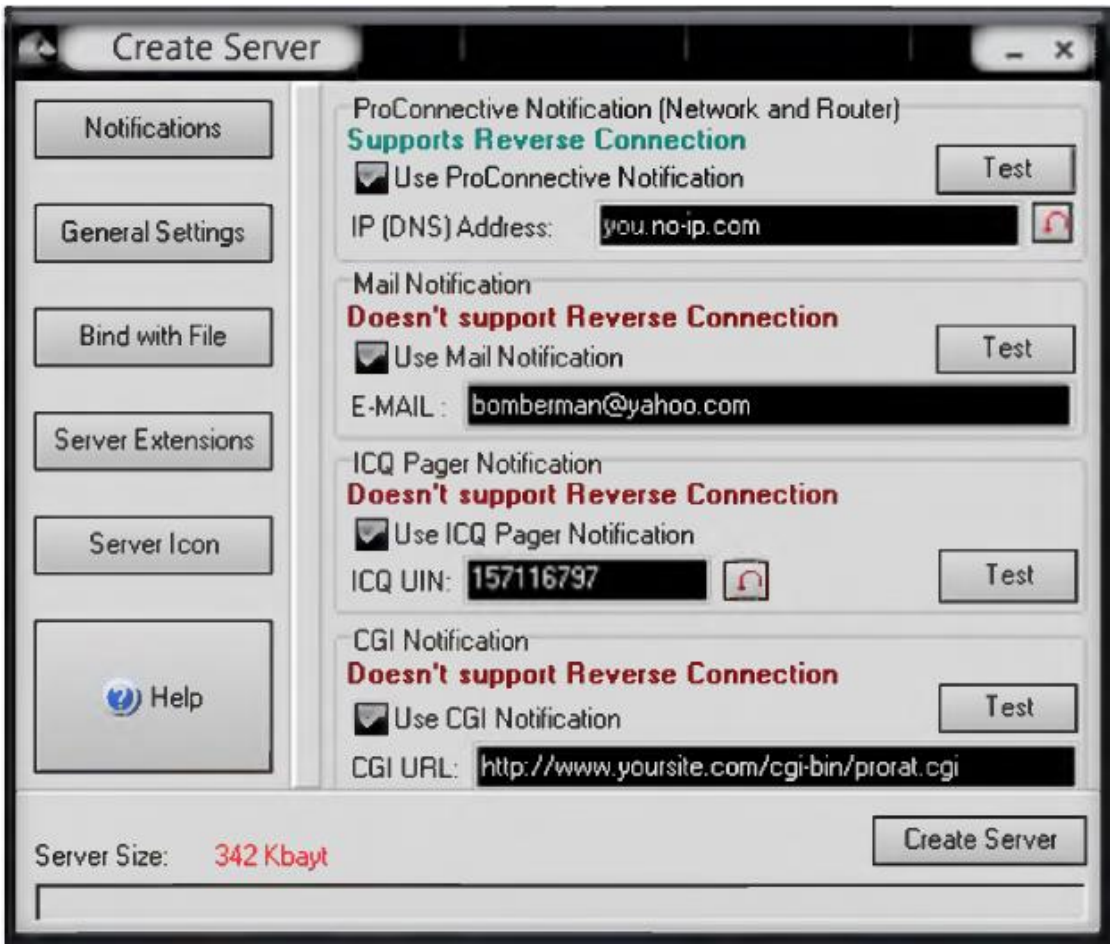
الخطوة ٣:

قم بإدخال عنوان IP الخاص بك ليتمكن السيرفر (البرمجية الخبيثة) من الاتصال بك.

إذا كنت لا تعرف ما هو عنوان IP الخاص بك قم بالضغط على الزر الأحمر وسوف يتم كتابة عنوان IP بشكل أتوماتيكي

الخطوة ٤:

نافذة خلق سيرفر التروجان كما في الشكل التالي:

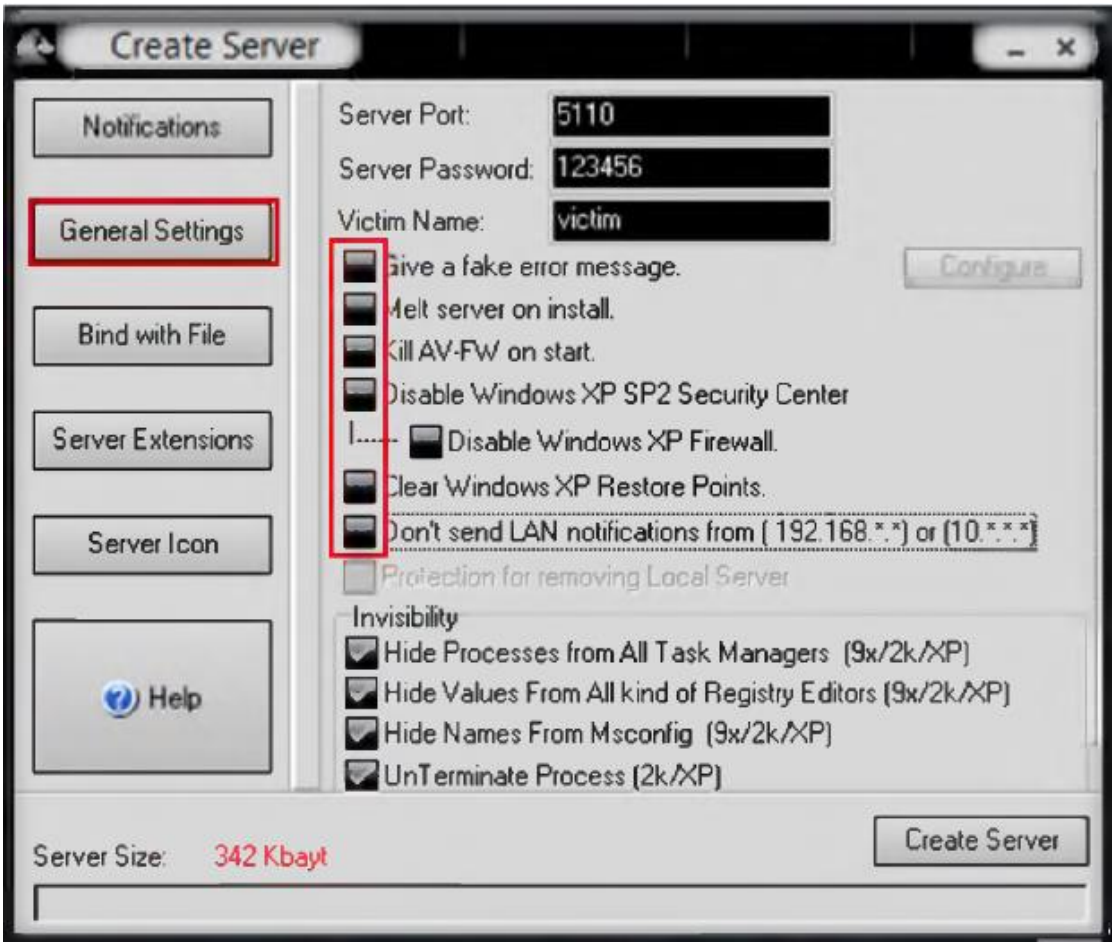


الخطوة ٥:

اضغط على General Setting من أجل تغير الخصائص مثل كلمة السر ورقم البورت

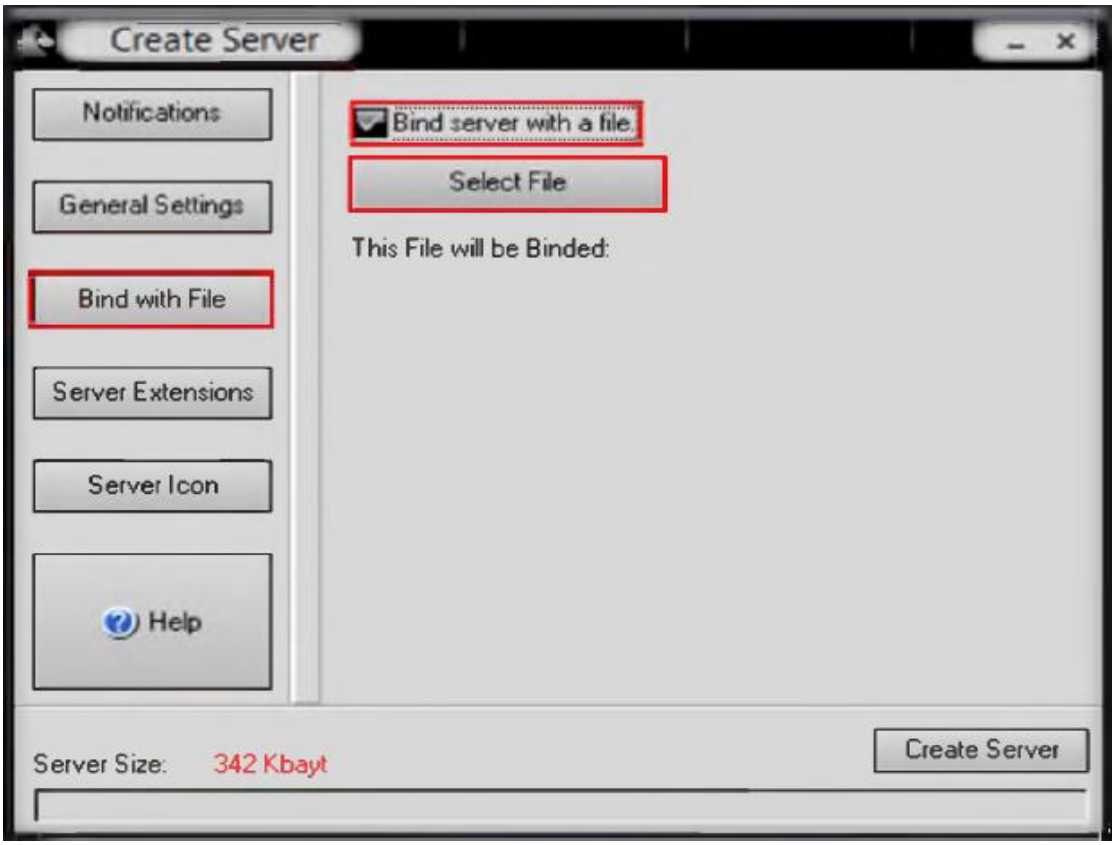
الخطوة ٦:

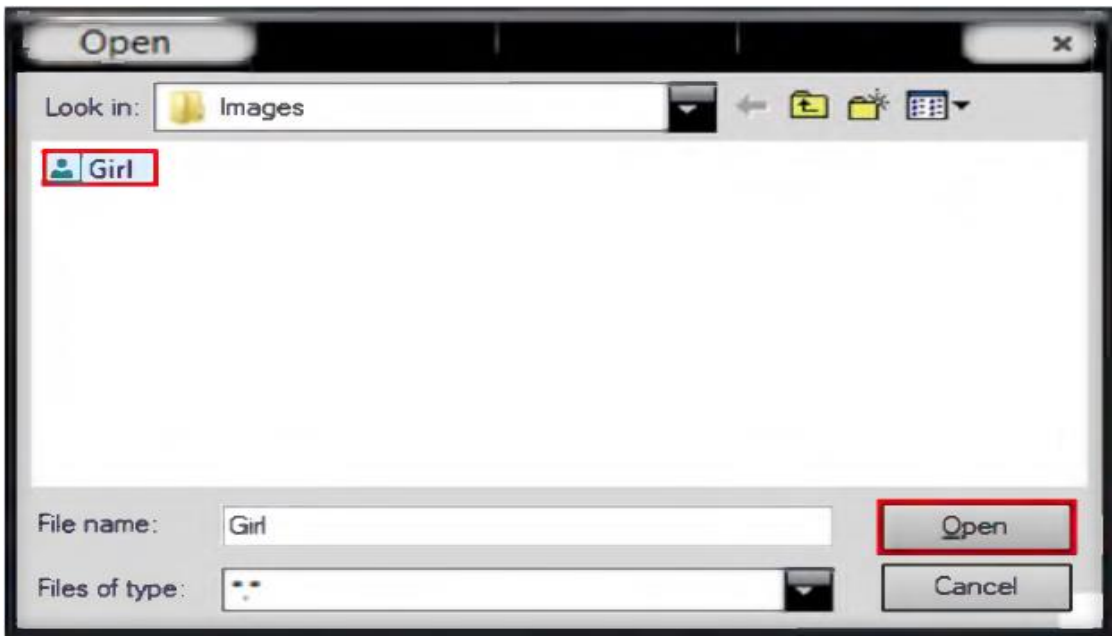
قم بإلغاء تفعيل الخيارات التي تظهر بالشكل التالي



الخطوة ٧:

اضغط على Bind with File من أجل دمج السيرفر مع ملف أنت تختاره من أجل خداع الضحية

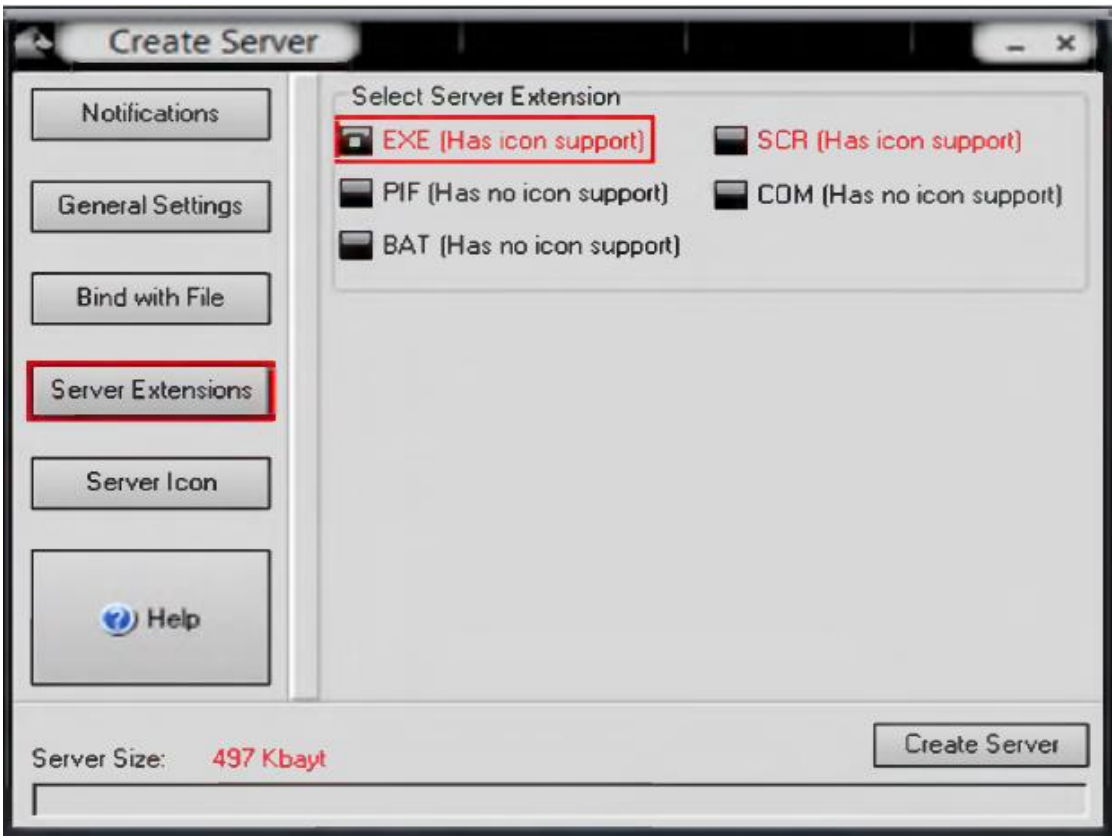




الخطوة ٨:

من اعدادات Server Extensions

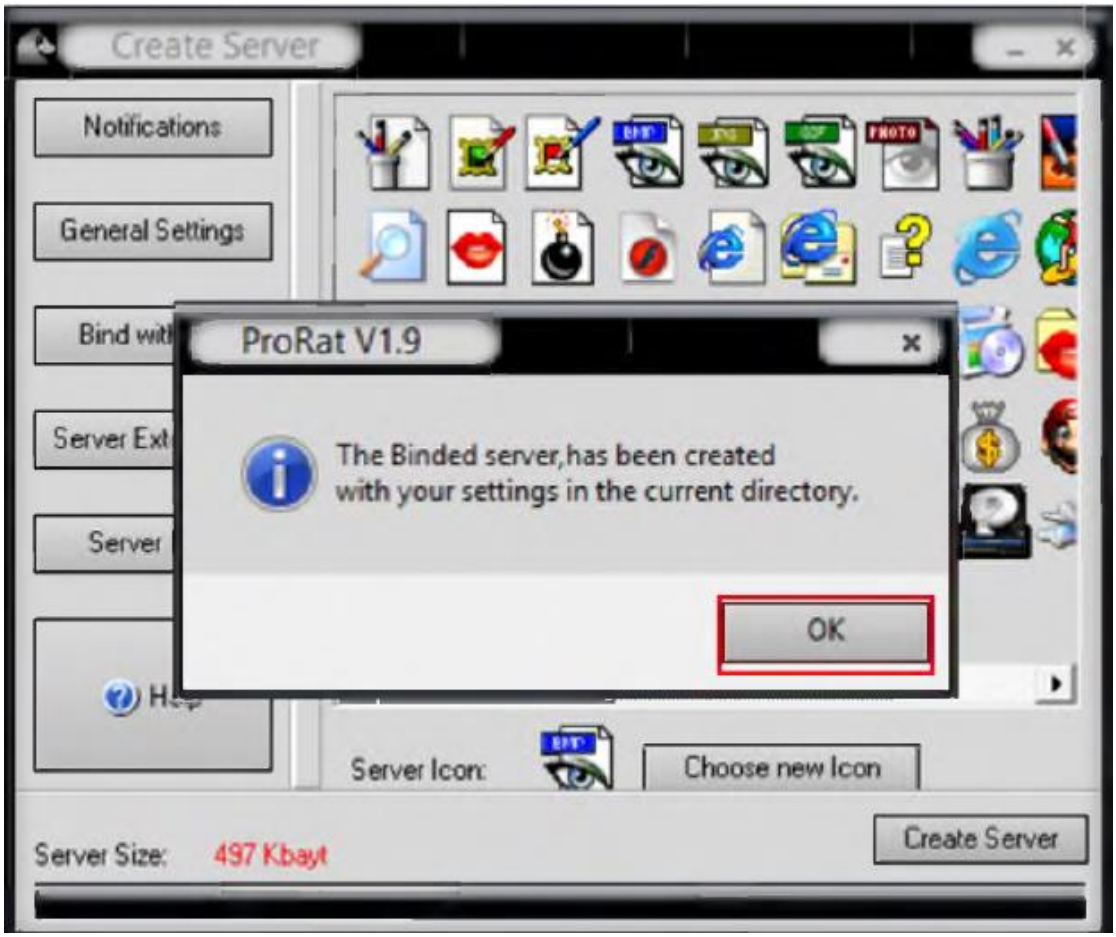
قم باختيار EXE (has icon support) من الخيار Select Server Extension



الخطوة ٩:

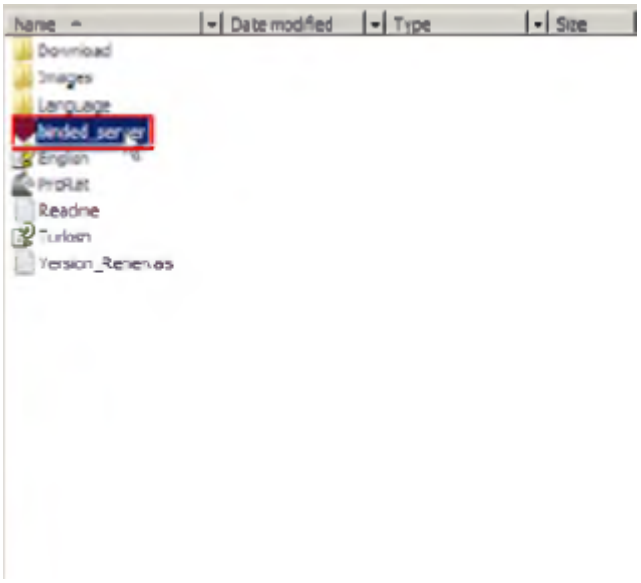
من Server Icon قم باختيار شكل الأيقونة التي تريدها

ثم قم بالضغط على Create Server


Create Server
Notifications
General Settings
Bind wit
Server Ext
Server
ProRat V1.9
The Binded server,has been created
with your settings in the current directory.
OK
Server Icon:
Choose new Icon
Server Size:
497 Kbayt
Create Server

الخطوة ١٠:

الآن يمكنك إرسال ملف السيرفر (البرمجية الخبيثة من نوع حصان طروادة) عبر الايميل أو عبر وسائل التواصل الاجتماعي وعندما يصل ملف السيرفر للضحية سوف يبدو كما في الشكل التالي

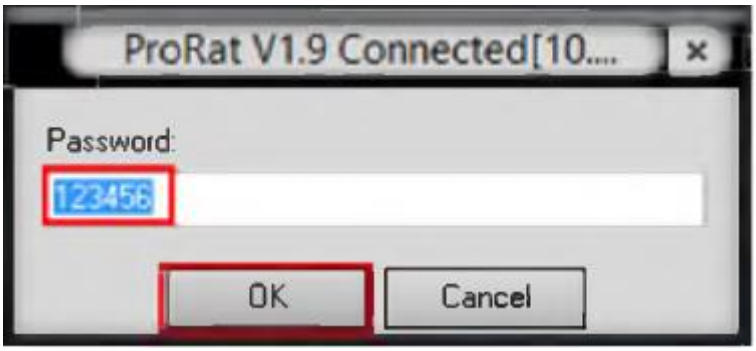


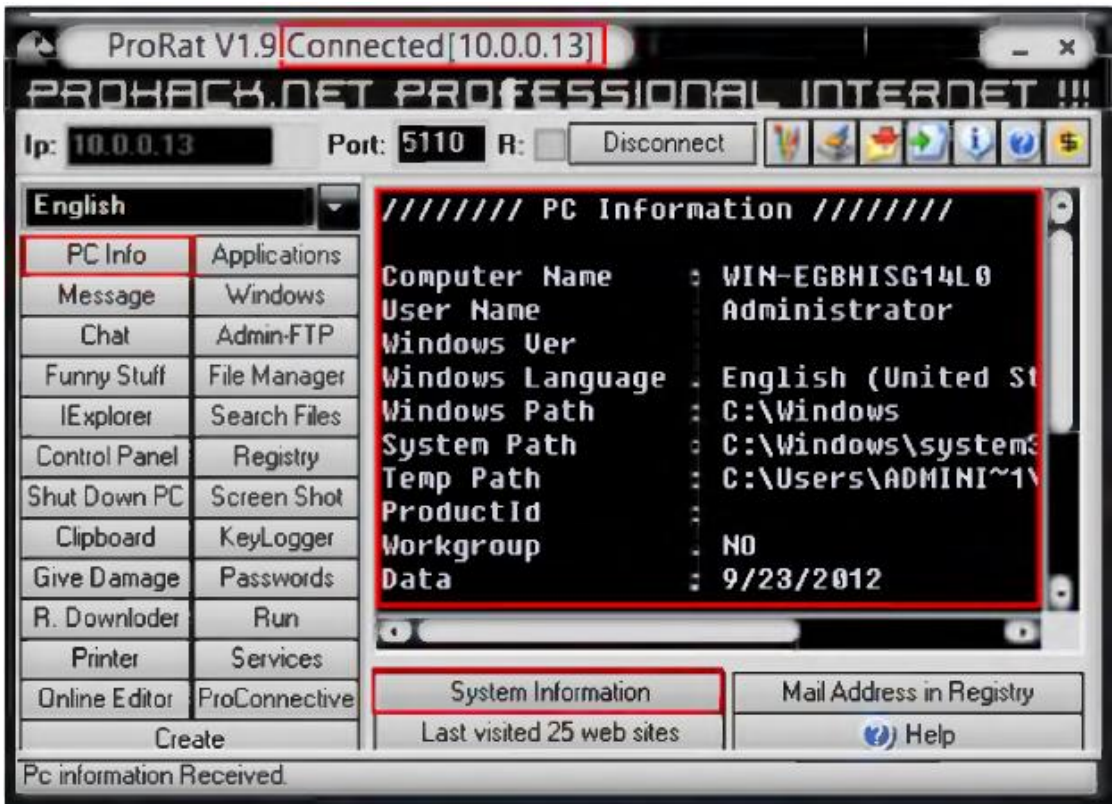
الخطوة ١١:

في هذا المثال عنوان IP المستخدم هو 10.0.0.13 ورقم البورت المستخدم 5110

الخطوة ١٢:

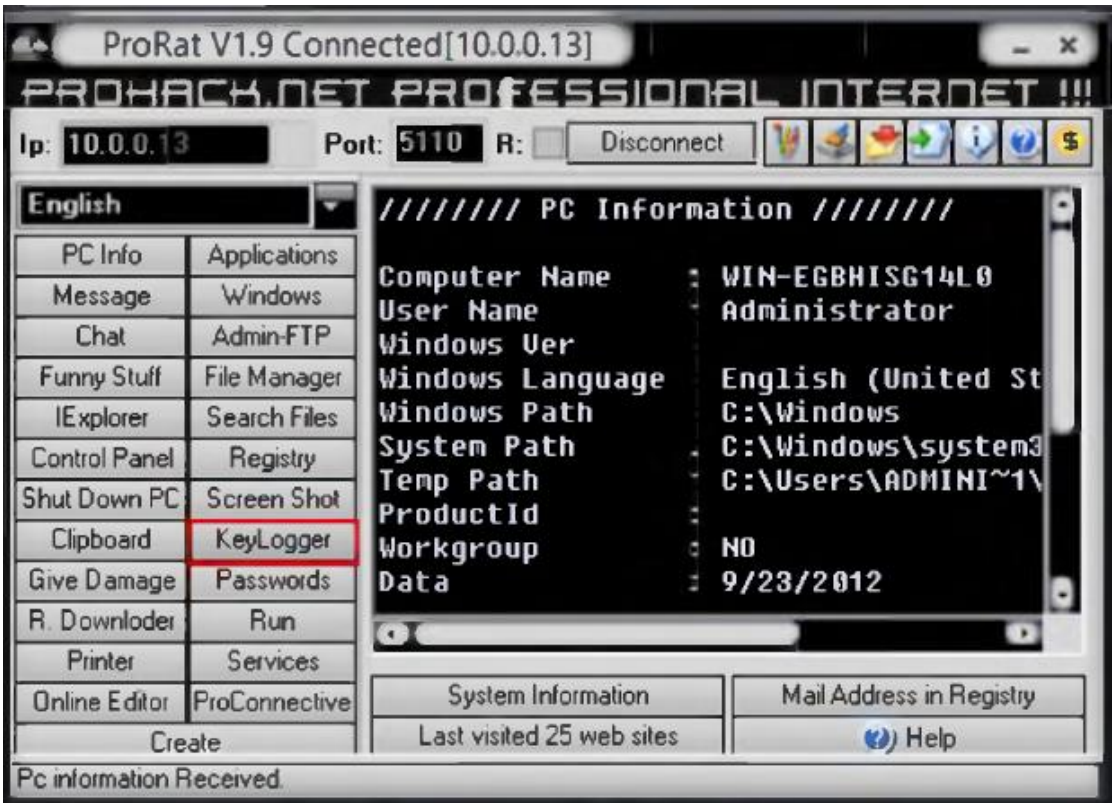
قم بإدخال كلمة السر من أجل الاتصال بجهاز الضحية، لاختبار الاتصال اضغط على PC Info واختر معلومات النظام system information كما في الشكل التالي

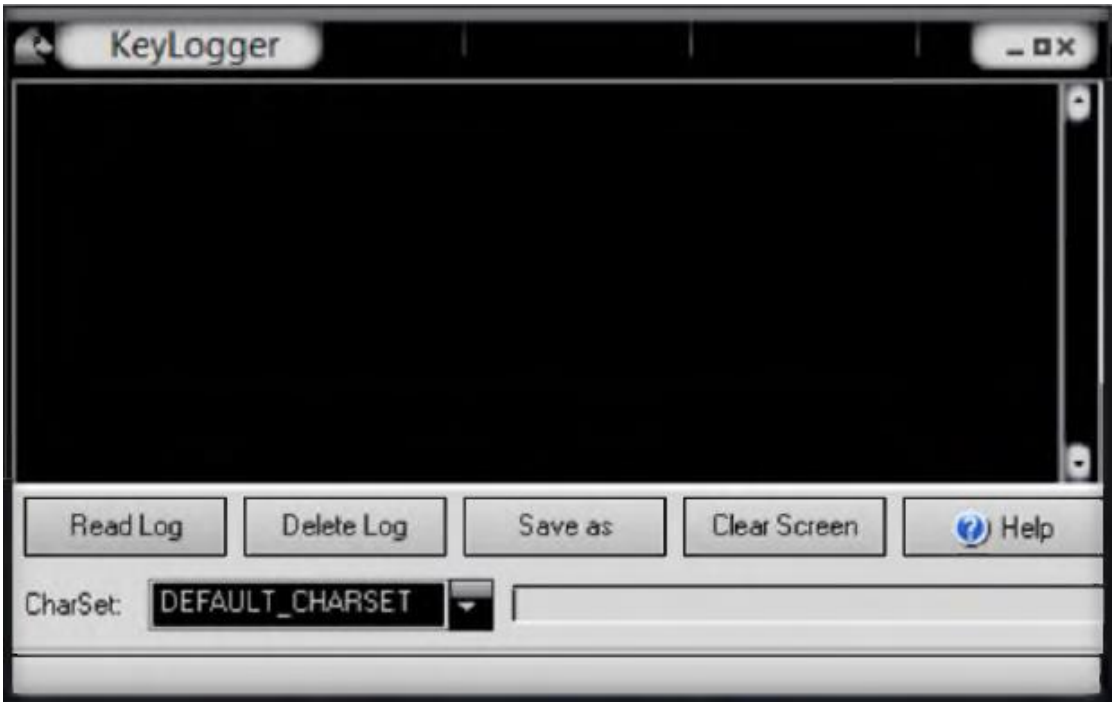


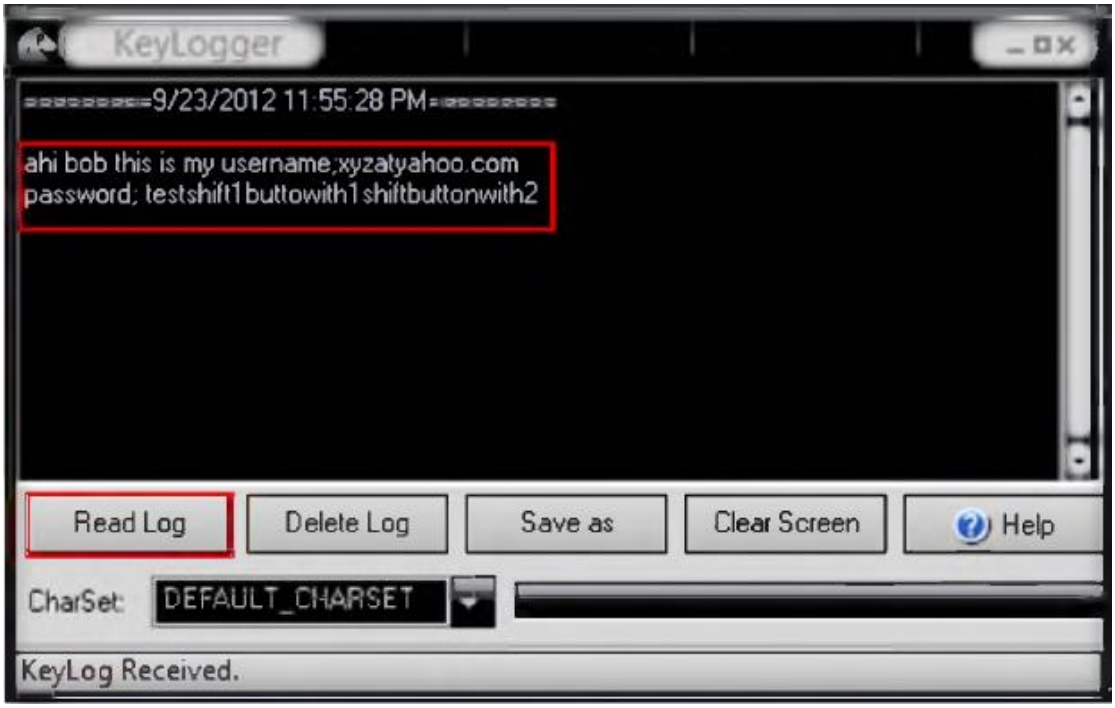


الخطوة ١٣:

اضغط على KeyLogger من أجل سرقة كلمات سر الضحية




KeyLogger
Read Log
Delete Log
Save as
Clear Screen
Help
CharSet:
DEFAULT_CHARSET


KeyLogger
========9/23/2012 11:55:28 PM========
ahi bob this is my username;xyzatyahoo.com
password; testshift1buttowith1shiftbuttonwith2
Read Log
Delete Log
Save as
Clear Screen
Help
CharSet:
DEFAULT_CHARSET
KeyLog Received.

دمج الملفات وتغير الامتداد

لخداع الضحية يقوم الهاكرز بدمج ملف البرمجية الخبيثة مع ملف له امتداد مختلف لا يثير شك الضحية كملف صوتي أو مقطع فيديو أو صورة ويتم ذلك باستخدام برنامج binder (مجمع)

المجمع Binder

عبارة عن برنامج صغير يستخدم لدمج أكثر من ملف ضمن ملف واحد له اسم وامتداد أنت تختاره.

معظم البرمجيات الخبيثة تكون بامتداد exe. وهذا يمكن أن يثير شك الضحية ويقلل من احتمال فتح الضحية لهذا الملف لذلك يقوم الهاكرز باستخدام binder من أجل دمج ملف البرمجية الخبيثة مع ملف أخر يمكن أن يكون له امتداد mp3 , jpg

بعض برامج الدمج المشهورة هي:

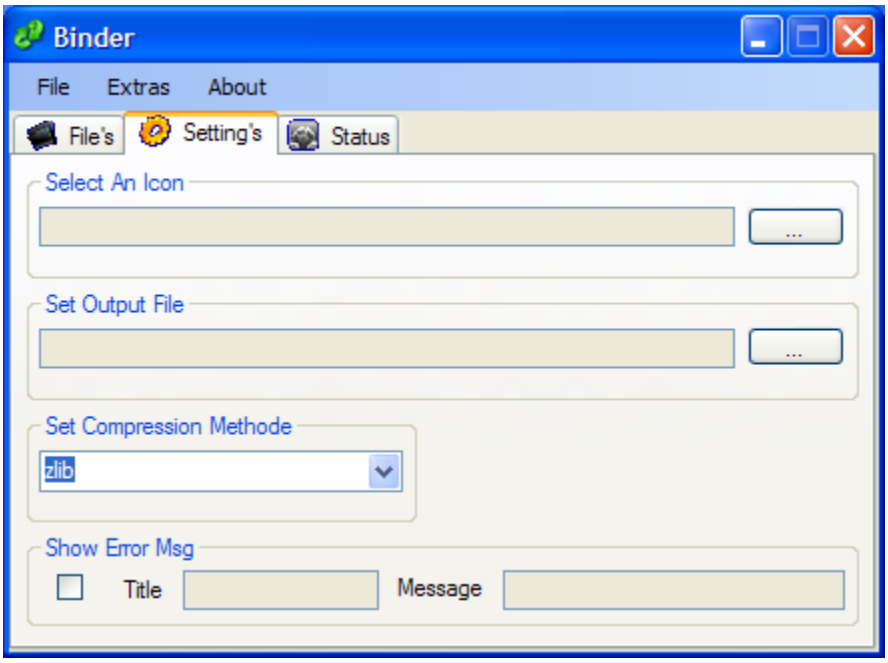
Simple Binder

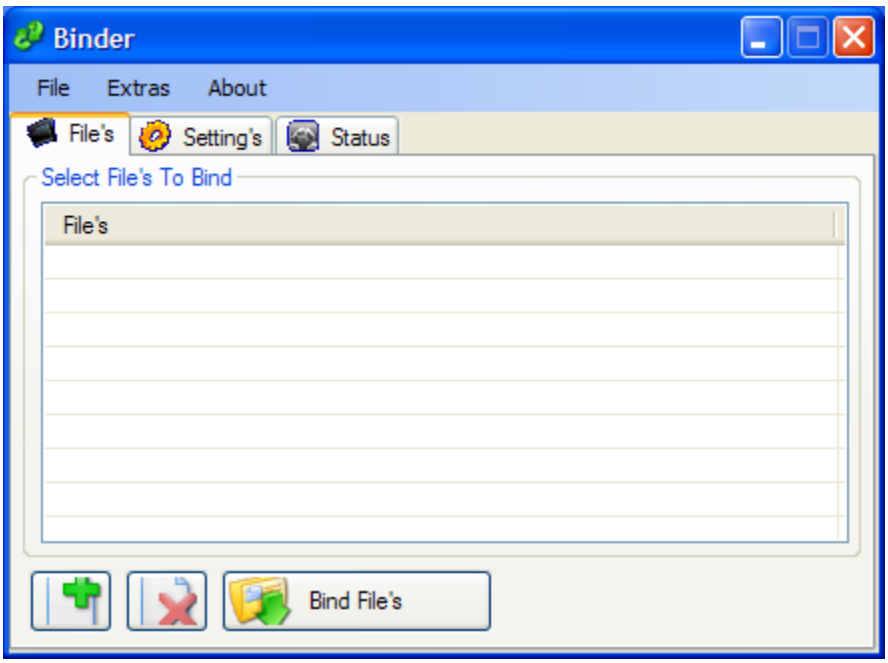
برنامج بسيط يقوم بدمج ملفين ضمن ملف واحد ويستخدم بشكل واسع من قبل الهاكرز من أجل دمج ملف البرمجية الخبيثة مع ملف لا يثير شك الضحية.

Weekend Binder

Easy Binders

برنامج سهل الاستخدام وله قدرة على دمج عدد غير محدود من الملفات كما له القدرة على تغير شكل ايقونة الملف المدمج.

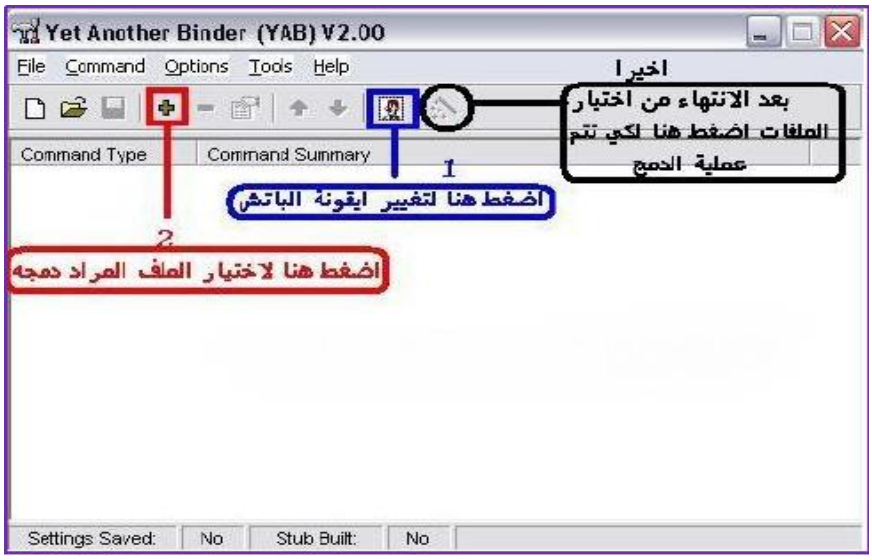




Yet Another Builder (YAB)

برنامج صغير الحجم وهو من أفضل برامج التشفير والدمج وتغيير الامتداد

و يمكنه حذف الملف أو المجلد بعد فتحه ويمكنه إخفاء البرمجية الخبيثة في مجلدات النظام التي تختارها أنت كما يمكنه أن يظهر رسالة خطأ عند التشغيل من أجل تشويش وخداع الضحية.



كيف يعمل مضاد الفيروسات

قبل التحدث عن الطرق التي يقوم الهاكرز باستخدامها من أجل تجاوز أو تخطي الحماية المطبقة من قبل مضادات الفيروسات من أجل تنصيب البرمجية الخبيثة على جهاز الضحية يجب أن تفهم كيف تعمل مضادات الفيروسات.

مضادات الفيروسات تستخدم استراتيجيات مختلفة من أجل كشف البرمجيات الخبيثة وأكثر هذه الطرق شيوعاً هي كشف البرمجيات عن طريق التوقيع الرقمي signature

مضاد الفيروسات يحوي على قاعدة بيانات فيها التوقيعات الرقمية الخاصة بالبرمجيات الخبيثة وهي عبارة عن أكود رقمية مميزة.

عندما يتم فحص البرمجية من قبل مضاد الفيروسات فإن مضاد الفيروسات يقوم بمقارنة الأكواد الخبيثة ضمن قاعدة البيانات الخاصة به مع الكود الخاص بالبرمجية التي يقوم بفحصها ومن ثم يظهر نتيجة الفحص فيما إذا كانت هذه البرمجية التي تم فحصها سليمة أو أنها عبارة عن برمجية خبيثة.

لذلك يجب عليك دائماً تحديث مضاد الفيروسات بشكل دوري لكي تحصل على الأكواد الرقمية (التوقيع) الخاص بالبرمجيات الخبيثة الحديثة.

طريقة أخرى تستخدمها مضادات الفيروسات تعتمد على التجريب المساعد على الكشف Heuristic-based method حيث يتم التعرف على البرمجية الخبيثة من خلال سلوكها المشبوه والمثير للشك.

هذه الطريقة فعالة ومفيدة ضد الأنواع الجديدة من البرمجيات الخبيثة.

تخطي مضادات الفيروسات

الآن وبعد أن أخذت فكرة عن كيفية عمل مضادات الفيروسات سوف نتعرف على بعض الطرق التي يستخدمها الهاكرز من أجل تجاوز أو تخطي مضاد الفيروسات في جهاز الضحية لكي لا يتم كشف البرمجية الخبيثة المراد تنصيبها في جهاز الضحية.

التشفير Crypter

عبارة عن طريقة يتم استخدمها بشكل شائع لتجاوز وتخطي الحماية المطبقة من قبل مضادات الفيروسات وهي طريقة بسيطة وليست بحاجة لأي معرفة سابقة بلغات البرمجة

كيف تعمل هذه الطريقة:

Crypter هو عبارة عن برنامج صغير يسمح للهاكرز بإخفاء الكود المصدري source code للبرمجية الخبيثة وتتم هذه العملية من خلال مزج أو خلط أو تشفير الكود البرمجي للبرمجية الخبيثة لجعلها غير مكتشفة من قبل مضاد الفيروسات.

ما هو FUD

يمكن أنك قد سمعت عن فيروس FUD Virus أو حصان طروادة FUD Trojan ولكنك لا تعرف معنى FUD والتي هي اختصار لعبارة Fully Undetectable "غير قابل للاكتشاف بشكل كامل" حيث يكون الفيروس أو حصان طروادة لا يمكن كشفه من قبل مضاد الفيروسات.

إنشاء برمجية خبيثة من نوع FUD لا يمكن كشفها من قبل أي مضاد فيروسات هو ليس بالأمر السهل وهو بحاجة لهاكرز محترفين من أجل القيام بهذه المهمة.

البرامج المجانية التي تقوم بتشفير البرمجية الخبيثة من أجل عدم اكتشافها من قبل مضاد الفيروسات هي غير فعالة دائماً أما البرامج الغير مجانية فهي قادرة على تشفير البرمجية الخبيثة بشكل لا يمكن اكتشافه من قبل مضاد الفيروسات.

التالي هو بعض البرامج المستخدمة في عملية تشفير البرمجيات الخبيثة:

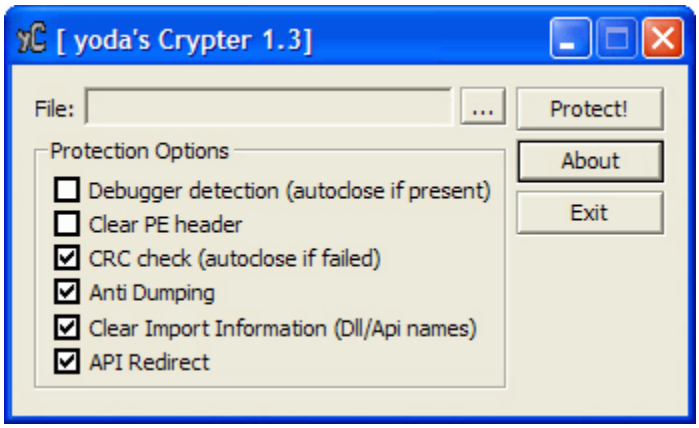
Ultimate Crypter

وهو غير قادر على إنشاء برمجية خبيثة غير قابلة للاكتشاف بشكل كامل ولكنه قادر على تقليل احتمال اكتشاف البرمجة الخبيثة.

يوجد نسخة غير مجانية من هذا البرنامج وهي قادرة على جعل البرمجيات الخبيثة غير مكتشفه بشكل كامل.

Yoda,s Crypter

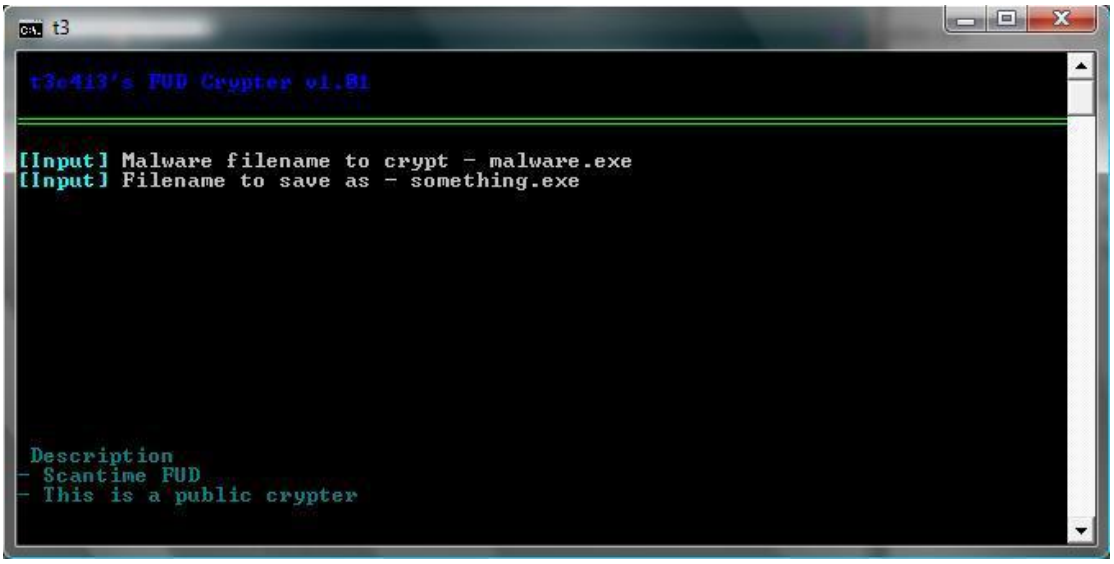
يقلل من احتمال اكتشاف البرمجية الخبيثة من قبل مضاد الفيروسات وهو سهل الاستخدام وله واجه رسمية بسيطة كما يظهر بالشكل التالي:



T3c4i3 Crypter

يستخدم من أجل الحصول على برمجية خبيثة غير قابلة للاكتشاف بشكل كامل ولكن هناك بعض مضادات الفيروسات قامت حديثاً بالوصول إلى التوقيعات الرقيمة الخاصة بهذا البرنامج.

طريقة عمل هذا البرنامج تتم من خلال إخفاء الكود البرمجي للبرمجية الخبيثة بداخل كود برمجي لبرنامج آخر وهذا يجعل مضاد الفيروسات غير قادر على اكتشاف البرمجية الخبيثة.



يوجد العديد من المواقع التي تقوم بإخفاء البرمجيات الخبيثة وتعمل بشكل أون لاين قم بالبحث عبر Google وستجد العديد من الأدوات والمواقع المجانية.

تغيير شكل الايقونة

وهي طريقة يعتمد عليها الهاكرز من أجل إنشاء برمجية خبيثة لا يمكن اكتشافها

يوجد الكثير من الفيروسات وأحصنة طروادة التي يتم اكتشافها من قبل مضادات الفيروسات بسبب أن الايقونة الخاصة بها تحوي على توقيع رقمي مكتشف من قبل مضادات الفيروسات لذلك فإن استخدام شكل الايقونة الافتراضي ليس بالخيار الجيد بالنسبة للهاكرز.

من أجل الوصول إلى برمجية خبيثة غير مكتشفة بشكل كامل يجب أن تكون هذه البرمجية غير مثيرة لشك الضحية ويوجد العديد من البرامج التي تؤمن خدمة تغير شكل الأيقونة مثل برنامج Icon changer والذي يسمح بتغير أيقونا الملفات المدمجة التي نحصل عليها من دمج البرمجية الخبيثة مع ملف آخر سليم باستخدام binder

Hexing

وهي طريقة أخرى من أجل الحصول على برمجية خبيثة غير مكتشفة وهذه الطريقة لها احتمال نجاح كبير جداً.

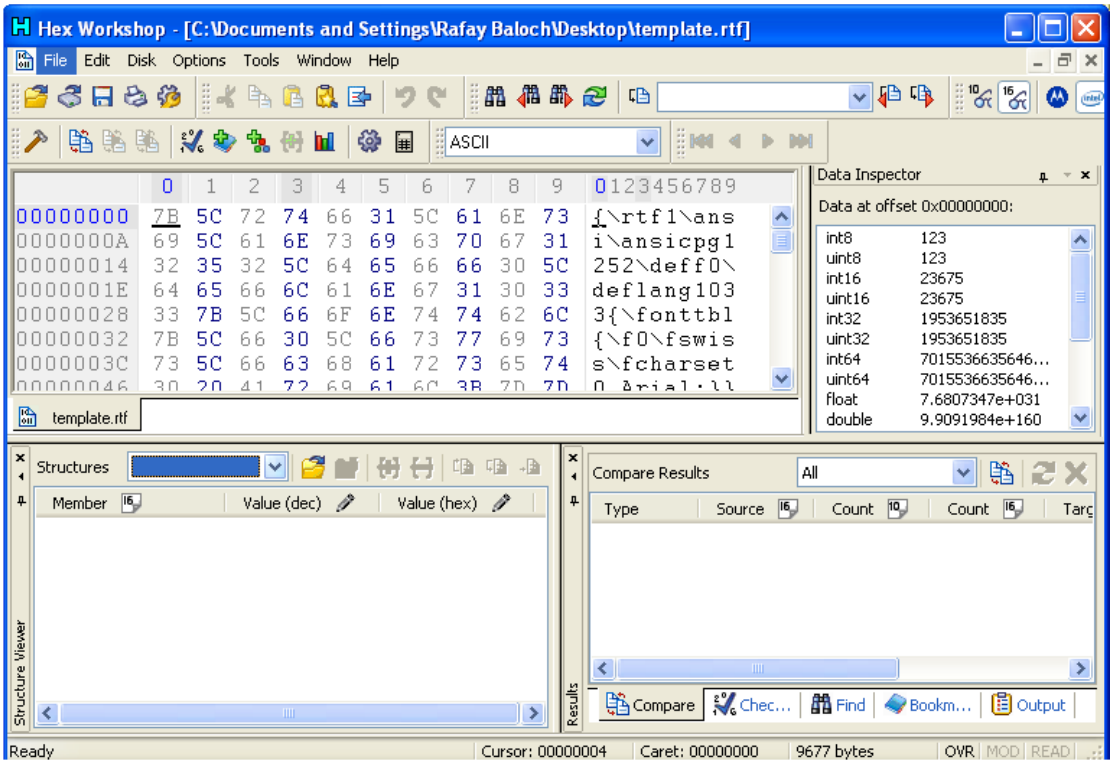
وهذه الطريقة غير منتشراً بشكل واسع وهي طريقة معقدة ويتم استخدامها من قبل الهاكرز المحترفين.

كيف تعمل هذه الطريقة

كما تحدثنا سابقاُ فإن مضاد الفيروسات يستخدم التوقيع الرقمي كطريقة لاكتشاف البرمجيات الخبيثة.

في هذه الطريقة يتم البحث عن علامة التوقيع ويتم تغييره وبالتالي لن يتمكن مضاد الفيروسات من اكتشاف هذه البرمجية الخبيثة.

وتتم هذه العملية باستخدام برنامج يسمى hex editor والذي يسمح بتغير الكود الثنائي لملف البرمجية الخبيثة.



إجراءات الوقاية والحماية من مسجلات ضربات المفاتيح وأحصنة طروادة

في بعض الأحيان يكون من الصعب اكتشاف البرمجيات الخبيثة لأن الهاكرز يستخدمون طرق وحيل مخادعة في إخفاء هذه البرمجيات لعدم كشفها من قبل مضاد الفيروسات.

التالي بعض الاجراءات التي يجب عليك القيام بها من أجل حماية جهازك من مسجلات ضربات المفاتيح وأحصنة طروادة

- لا تقم بفتح أي مرفقات تصلك عبر الايميل من مصادر غير معروفة أو غير موثوقة.
- لا تقم بتحميل البرامج المجانية من المواقع الغير معروفة.
- انتبه عند استخدام أجهزة الذاكرة المحمولة (USB) أو الأقراص الليزرية (CD or DVD) وتأكد من تعطيل خاصيه الفتح التلقائي و قم بعملية فحص هذه الوسائط باستخدام مضاد الفيروسات قبل أن تقوم بفتحها.
- انتبه من الوصول المادي لجهازك لأنه يمكن وبكل بساطه أن يقوم المهاجم بتنصيب برمجية خبيثة بجهازك وبدون علمك وتأكد من وضع كلمة سر لجهازك عند تشغيله قبل أن يسمح لك بالوصول إلى البيانات وقم بقفل جهازك في حاول نويت الابتعاد عنه لفترة زمنية قصيرة.
- انتبه عند استقبال ملفات عبر البلوتوث أو عبر الانترنت وبرامج المحادثة لأنها يمكن أن تكون ملفات لبرمجيات خبيثة وقم بفحصها بمضاد الفيروسات قبل أن تفتحها.

- لا تستخدم نسخة قديمة من متصفح الانترنت إكسبلورر لأنه يحوي على ثغرات تسمح بإصابة جهازك بالبرمجيات الخبيثة بمجرد زيارة موقع خبيث وبدون أن تقوم بتحميل أو فتح أي برامج وتأكد من استخدامك لأحدث نسخة من برامج تصفح الانترنت وبرامج البريد الالكتروني.
- استخدم مضاد فيروسات قوي وقم بتحديثه بشكل دوري

أنصحك باستخدام مضاد الفيروسات المجاني "أفيرا"

- استخدم مضاد للبرمجيات الخبيثة وقم بتحديثه بشكل دوري

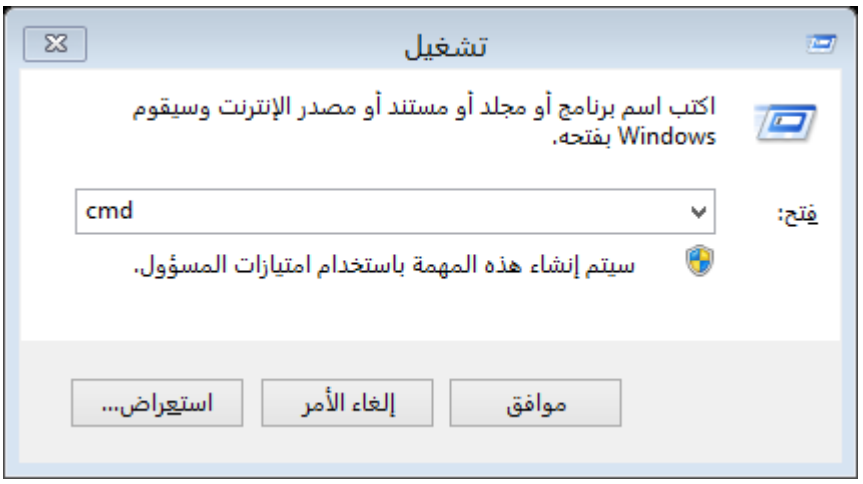
مثل Spybot أو Zemana.AntiMalware

- استخدم جدار ناري Firewall (وهو عبارة عن برنامج يمنع عمليات الاتصال غير المسموح بها عبر الشبكة) ويساعد على الحماية من البرمجيات الخبيثة

أنصحك باستخدام الجدار الناري المجاني "كومودو"

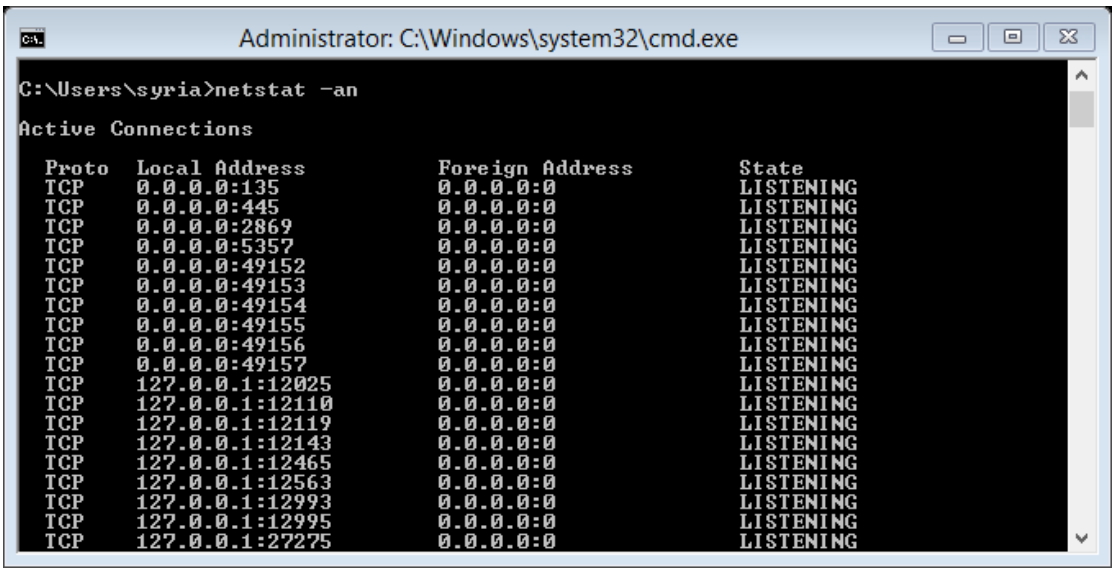
- فحص البورتات المفتوحة والمشبوهة والبحث عن اتصال مع عناوين IP غير معروفة من خلال الضغط على زر الويندوز + R

ثم كتابة cmd

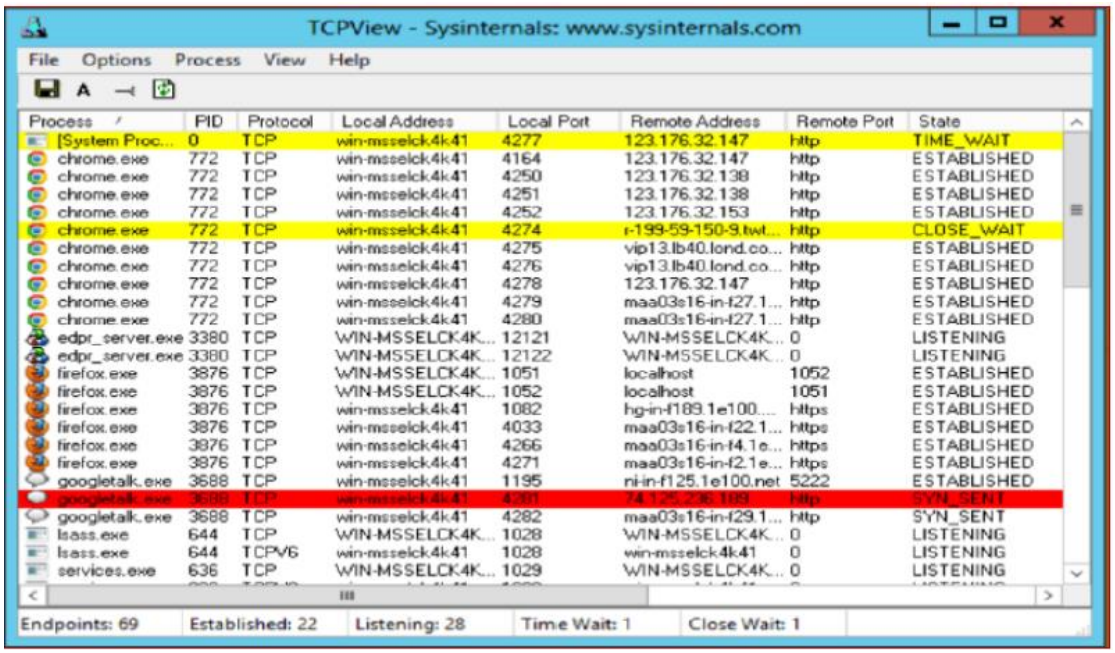


ثم كتابة التعليمة التالية

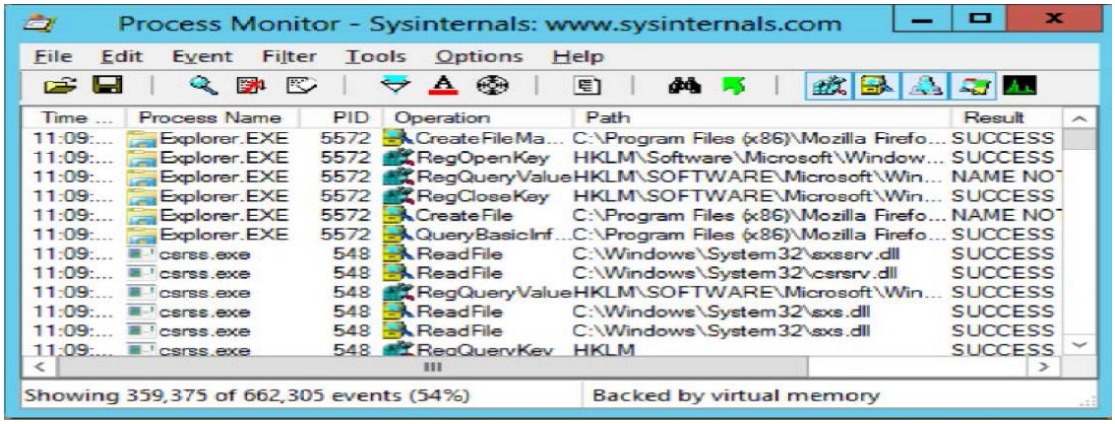
netstat -an



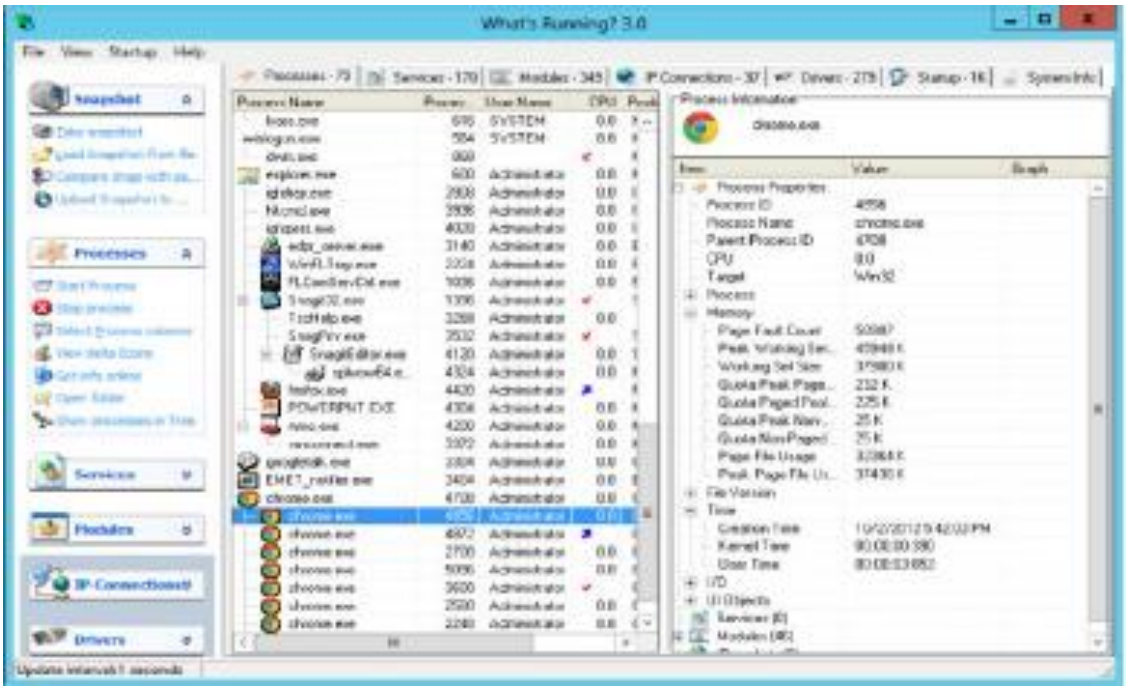
- مراقبة الاتصالات باستخدام برنامج مثل TCPView وهو برنامج يتيح لك رؤية جميع اتصالات بروتوكولات TCP and UDB ويعطي تقرير عن حالة الاتصال واسم العملية المرتبطة بها مع إمكانية انهاء اتصال أي عملية تشك في طبيعة عملها.



- فحص العمليات المشبوهة باستخدام أداة مثل Process Monitor وهي عبارة عن أداة تظهر العمليات التي تعمل في الوقت الحالي وتفيد في كشف وتحليل سلوك البرمجيات الخبيثة وبرمجيات التجسس.



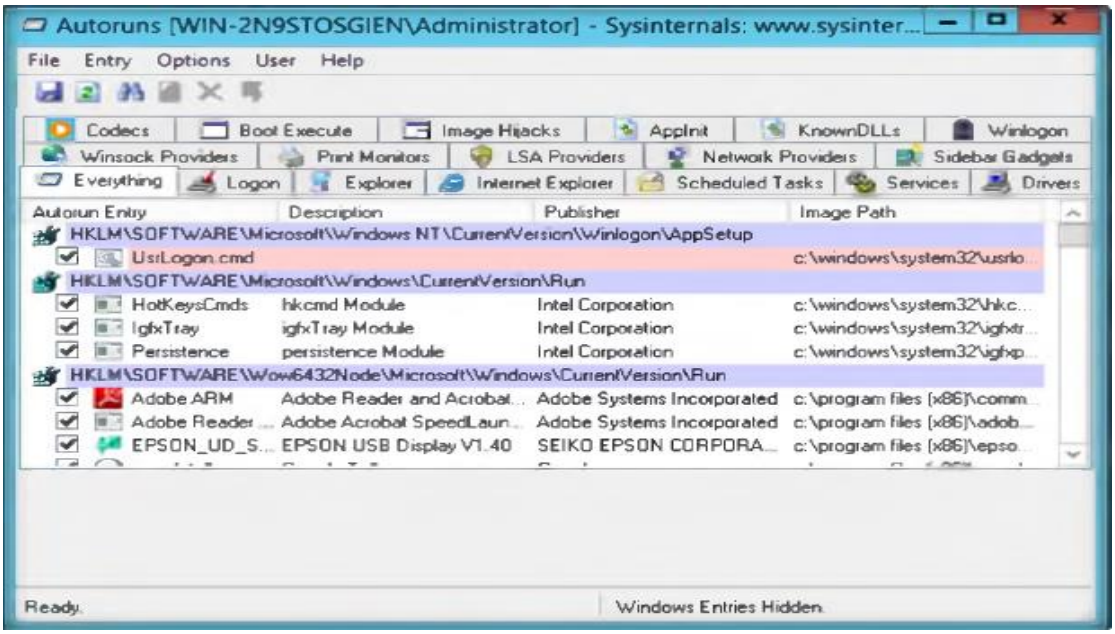
أو باستخدام برنامج What's Running

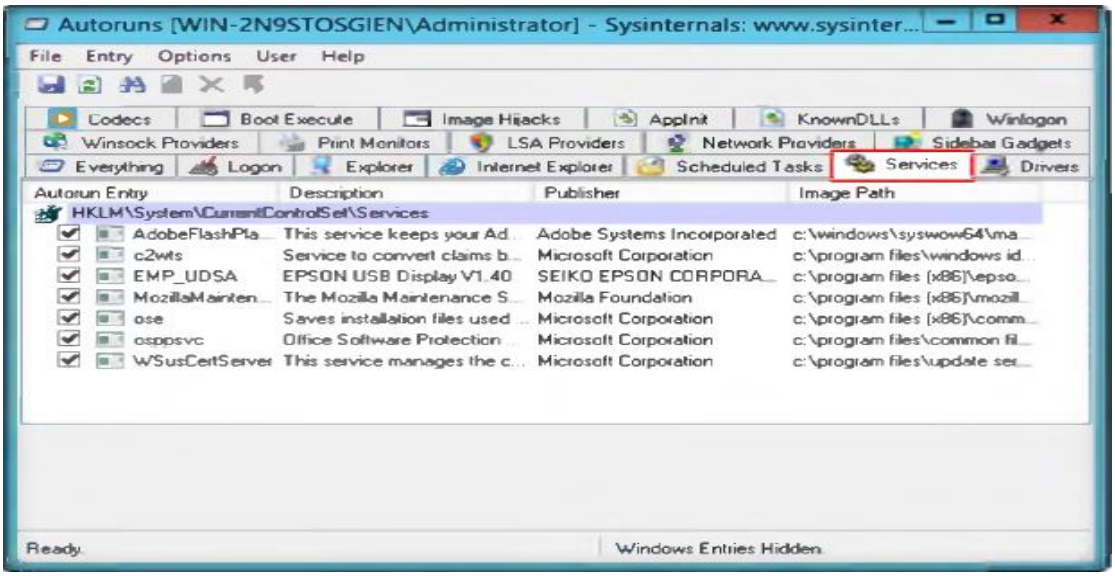


- مراقبة البرامج التي تبدأ العمل تلقائياً عند بدء تشغيل النظام من خلال فحص مجلد startup الموجود في المسار التالي:

C:\ProgramData\Microsoft\Windows\Start Menu\Program

أو باستخدام برنامج AutoRun



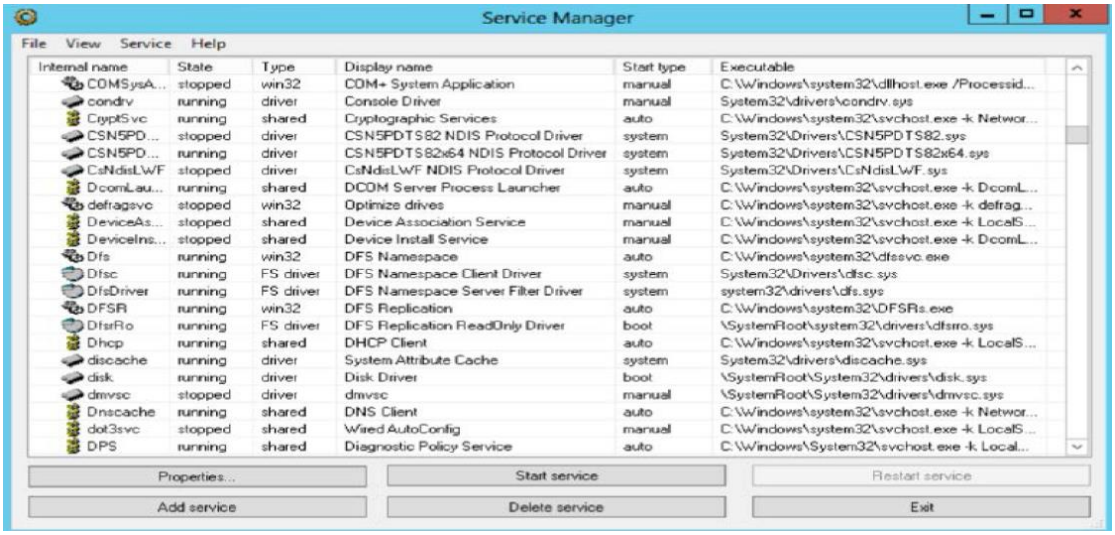


- إصلاح أخطاء السجلات registry والكشف عن إدخالات السجلات التي تم إنشاؤها بواسطة البرمجيات الخبيثة باستخدام أداة

Jv16 Power Tool 2014 – Registry Cleaner

- مراقبة خدمات وعمليات نظام الويندوز باستخدام أداة

Windows Service Manager (SrvMan)



برمجيات الإعلانات والتجسس

Spyware or Adware

وهي البرمجيات التي يتم تنصيبها في جهاز الحاسب بدون علم أو أذن المستخدم وتقوم بجمع معلومات عن المستخدمين ومراقبة تصرفاتهم على الشبكة من أجل خلق الإعلانات.

وهي تقوم بخلق النوافذ المنبثقة المزعجة أثناء تصفح الانترنت وتقلل من سرعة تصفح الانترنت وتقلل من أداء وسرعة الجهاز وسرعة الانترنت لأنها تستهل موارد الشبكة وفي بعض الأحيان تجعل الجهاز المصاب بها أكثر عرضة للاختراق

ولأن هذا النوع من البرمجيات يتم تنصيبه في جهاز الضحية بدون علمه فمن الممكن أن تبقى في جهازه لفترة زمنية قبل أن يلاحظها أو يتمكن من اكتشافها و إزالتها.

كيف يمكنك اكتشاف برمجيات الإعلانات والتجسس

إذا كان جهازك مصاب ببرمجية من هذا النوع فإنك سوف تعاني من إحدى الأمور التالية:

- ظهور الكثير من النوافذ المنبثقة الغير مرغوب بها أثناء تصفح الانترنت.
- فتح صفحات انترنت لم تقم بطلبها.
- إعادة توجيهك إلى صفحات انترنت غير مرغوب بها.
- تحرك مؤشر الماوس بشكل عشوائي.
- تغير الصفحة الرئيسية في متصفح الانترنت وظهور صفحات غير مألوفة.

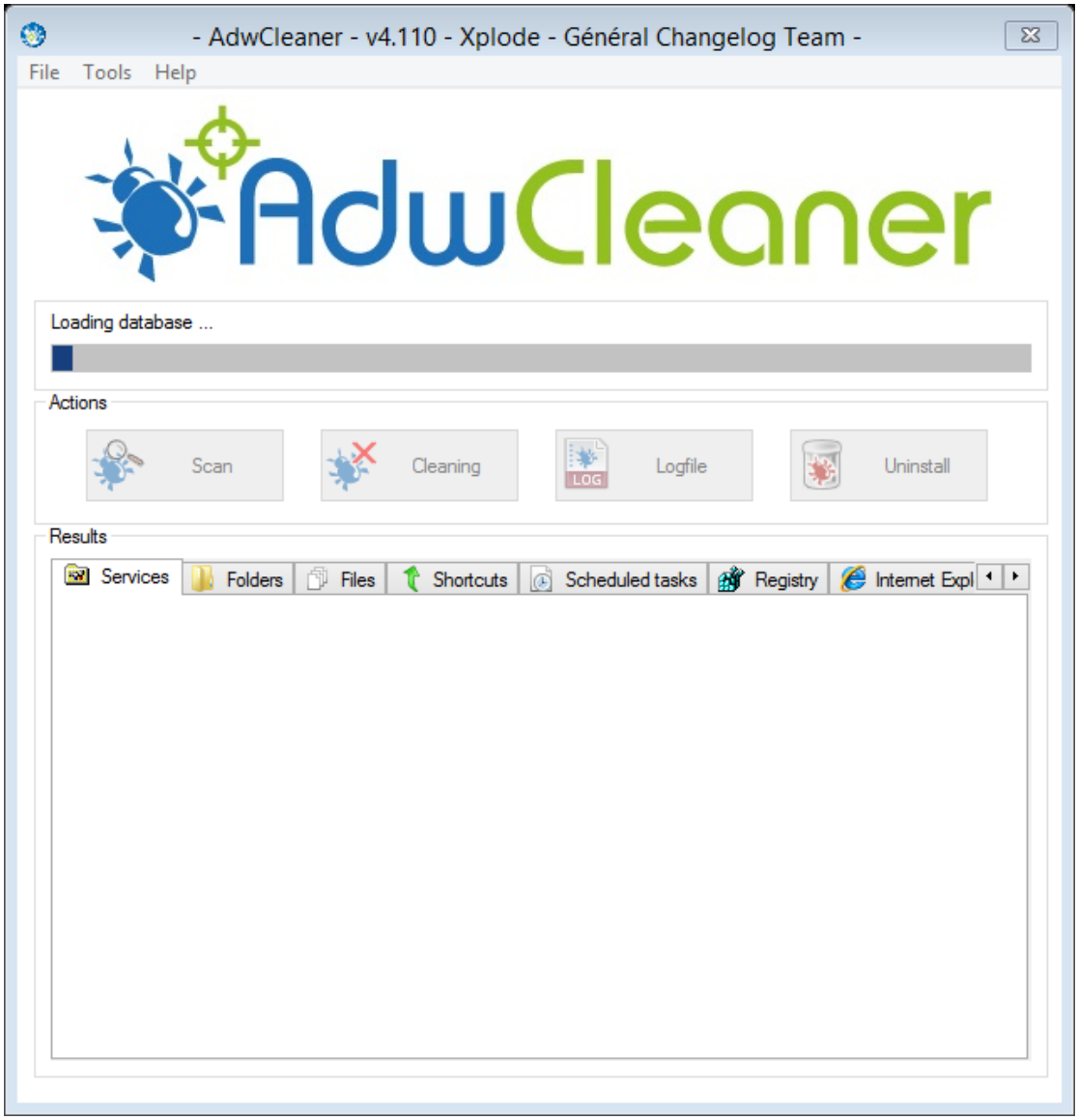
- ظهور أيقونات جديدة في شريط المهام.

إجراءات الوقاية من برمجيات الإعلانات والتجسس

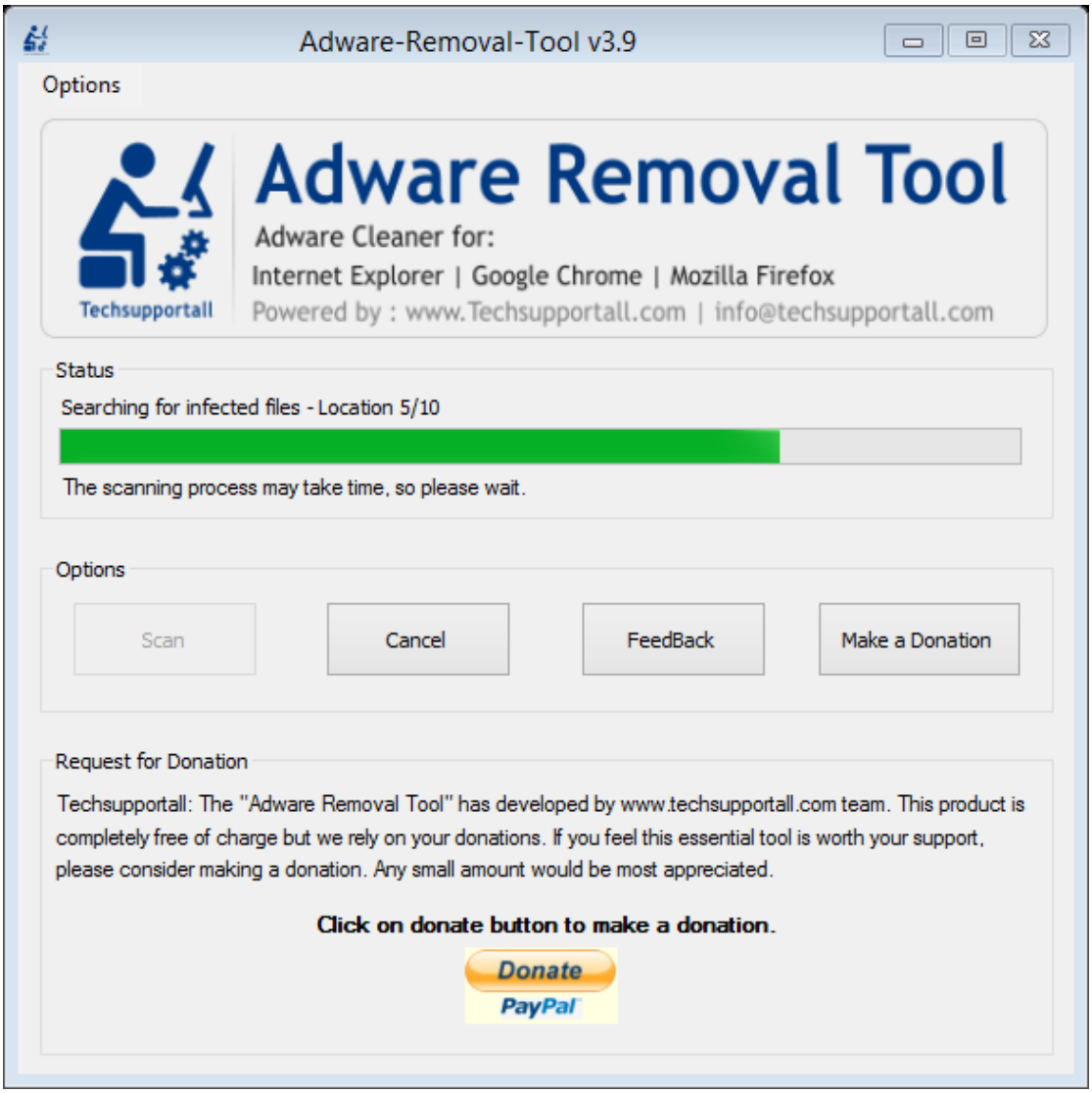
- لا تقم بتحميل برامج مجانية من مواقع غير معروفة.
- لا تقم بتحميل أي برامج تصلك من خلال روابط عبر الايميل دون أن تعرف مصدر هذا الايميل (في بعض الأحيان تصلك رسائل عبر الايميل تحوي على روابط وتخبرك بضرورة تحميل وتنصيب مضاد فيروسات أو مضاد للبرمجيات الخبيثة في جهازك ولكن في حقيقة الأمر هي رسائل مضللة وتحوي على برمجيات خبيثة وبرمجيات تجسس)
- لا تقم بالضغط على أي روابط تظهر من خلال النوافذ المنبثقة لأنها ستقوم بتنصيب برمجيات تجسس في جهازك.
- عند ظهور نافذة منبثقة مزعجة قم بالضغط على إشارة X بدلاً من الضغط على زر "close" من أجل أغلاقها.
- استخدم جدار ناري قوي.
- قم بفحص البرامج الجديدة باستخدام مضاد فيروسات قوي ومحدث.
- استخدم مضاد للبرمجيات الخبيثة وقم بتحديثه بشكل دوري.

كيف تتخلص من برمجيات الإعلانات والتجسس

إذا كنت تعتقد أن جهازك مصاب ببرمجية من هذا النوع يجب أن تقوم باستخدام برنامج مثل ADwCleaner



أو Adware Removal Tool



كما أن بعض مضادات الفيروسات لها القدرة على اكتشاف وحذف برمجيات الاعلانات والتجسس.

الفيروسات

الفيروس عبارة عن برنامج يقوم بالتكاثر وتكرير نفسه بشكل ذاتي ويقوم بنسخ وربط كوده البرمجي مع أكواد برامج أخرى وهو يعمل بدون علم المستخدم ويلحق نفسه مع برامج أخرى أو ملفات أخرى أو مع ملفات إقلاع النظام.

الفيروسات تنتقل عادتاً من خلال تحميل الملفات

أو من خلال وسائط نقل البيانات (ذواكر USB أو الأقراص الليزرية) أو عبر مرفقات الايميل.

كيف تعمل الفيروسات

الفيروسات تقوم بمهاجمة النظام الهدف من خلال عدة طرق مختلفة حيث تقوم بإلحاق نفسها مع البرامج أو الملفات وتنتقل معها إلى برامج أخرى أو إلى أجهزة أخرى وذلك من خلال الاستفادة من بعض الأحداث.

الفيروسات تمر بمرحلتين:

- مرحلة العدوى infection phase
- مرحلة الهجوم attack phase

في مرحلة العدوى:

فإن الفيروسات تتكاثر بشكل ذاتي وتلحق نفسها بملفات تنفيذية ذات امتداد exe.

البرامج المصابة بالفيروس تقوم بتمكين الفيروس من العمل على النظام ويصبح الفيروس جاهزاً للعمل بمجرد تشغيل البرنامج أو فتح الملف المصاب بها.

في مرحلة الهجوم:

عندما تنتشر الفيروسات في النظام الهدف فإنها تبدأ بتخريب الملفات والبرامج أو حذفها وتدميرها.

أسباب كتابة برامج الفيروسات

- إلحاق الضرر بالشركات المنافسة.
- مشاريع بحثية.
- المزح مع الأصدقاء.
- تخريب وتدمير الملفات والأنظمة.
- مهاجمات منتجات شركة معينة.
- توجيه رسائل لأغراض سياسية.
- تحقيق ربح مادي.
- الابتزاز.

أعراض الإصابة بالفيروسات

- البرامج تأخذ وقت طويل لتبدأ العمل.
- القرص الصلب يبدو دائماً ممتلئ.
- السواقة تعمل بدون أن تستخدمها.
- ظهور ملفات غير معروفة.
- إصدار أصوات غريبة أو أصوات تصفير من الجهاز.
- تغيير أسماء الملفات.
- تغير حجم البرامج باستمرار.
- بطئ في أداء النظام.
- استهلاك موارد النظام.

طرق الوقاية والحماية من الفيروسات

- الانتباه عند استقبال وتحميل ملفات من مصادر غير موثوقة.
- عدم فتح الايميلات القادمة من مصادر غير موثوقة لأن الهاكرز عادتاً يقومون بإرسال الملفات المصابة بالفيروسات كمرفقات للبريد الالكتروني وعندما يقوم الضحية بفتح الايميل يتم عدوى جهازه بالفيروس.
- تحديث البرامج وتحديث نظام التشغيل بشكل دوري.
- عدم الضغط على أي روابط أو أيقونات تظهر من خلال النوافذ المنبثقة أثناء تصفح مواقع الانترنت.
- عدم فتح أو تصديق أي رسائل او ايميلات تدعي أن جهازك مصاب بفيروسات وتطلب منك الضغط على روابط معينة من أجل تحميل مضاد فيروسات وبالحقيقة هي عبارة عن روابط خبيثة تقوم بتحميل فيروسات.

- فحص وسائط نقل البيانات (فلاشات USB والأقراص الليزرية) قبل فتحها.
- استخدام مضاد فيروسات قوي وتحديث قاعدة البيانات الخاصة به بشكل دوري.