

سلام عليكم ورحمة الله وبركاته

هذا الكتاب يتكلم عن اسهل طريقة لحذف ملف تجسس الهكر بسهولة تامه وعن الحيل وخدع هكر

نقاط مشروحه

١. متطلبات يستخدمها الهكر للاختراق
٢. حيل الهكر
٣. دمج ملف تجسس مع صفحه مزوره تعمل علي متصفح
٤. تحكم الهكر فيك اذا كنت مخترق
٥. حذف ملف التجسس بسهولة
٦. نقاش اسأله واجوبه عن طرق صحيحه ولماذا
٧. طريقه فاشله يقع فيها الكثير لمعرفة الجهاز مخترق او لا (system.ini)
٨. نصائح مهمه
٩. مسلتزمات تحميك من ملفات التجسس والفايروسات ومشاكل النت

هذي معلومات بسيطة عن هكر و تفيدك كمستخدم للنت و تحميك من ملفات تجسس بأذن الله
وتستطيع تنظيف جهازك بسهولة تامه من ملفات تجسس وتعرف الطرق صحيحة من الطرق الخاطئة والمنشره بالنت
وتعتمد علي طريقه واحد لكشف ملف تجسس وباقي طرق ليست قويه وسشرحها لك

يجب عليك معرفة معلومات لكي تستفيد ولا تتعرض للاختراق

مقدمة :

كثرة بالايام الاخيره (الاختراقات) وانتشار (ملفات التجسس) والمصيبة الكبرى انها من

مسلمين يخترقون اخوانهم والمعروف بديننا الحنيف بأن التجسس (حرام) وليس الهكر

لان الهكر هناك من ينصرون دينهم باختراق (المواقع المسيئه للاسلام)

١. متطلبات يستخدمها الهكر للاختراق

يعتمد الهكر علي برنامج لكي يتحكم في جهازك عن بعد ويستطيع مشاهدة كام واستخراج باسورداتك عن طريق ملفه تجسس موجود بجهاز

1. برنامج اختراق :

انواع برامج الاختراق كثيره وهذي صوره للبرنامج



برنامج الاختراق ينتج له ملف تجسس صغير حجمه بكواد خبيثه ترسل معلوماتك للهكر



يستطيع صنع اي ملف اسمه وشكله وتغير ايقونة ببرنامج الاختراق

وظيفة ملف تجسس :

ملف تجسس يكون مكشوف من الحماية ولكن الهكر نكي لديه طرق يستطيع بان يجعل الملف نظيف من جميع حمايات وتسمي تشفير

وهذا يدل علي ان لانتعمد علي برامج تنظيف ضد الهكر

اين يضع الهكر ملفه تجسس ولماذا ؟

يضع الهكر ملف تجسس ببدء تشغيل الجهاز لكي كل ماتتصل بالنت يعمل ملفه تجسس وتتصل عنده ببرنامج الاختراق

هنا في بدء تشغيل نحدد ملف ولانتعمد علي حمايات بالحدف لان كما ذكرت يستطيع تشفير من حمايات

٢. حيل الهكر

١. يستطيع الهكر تخطي كل شي سواء برنامج حمايه او موقع تحليل او ادوات كشف تلغيم

ولكن لايستطيع تخطي بدء تشغيل لماذا

لانه يحتاج ان نكون متصلين عنده كل مانشغل الجهاز

واذا وضع ملفه التجسس في مكان ثاني غير بدء تشغيل لان يراقبنا

٢. يستطيع دمج ملفه تجسس مع برنامج نظيف ومفيد للجميع ورفع علي مواقع رفع (فورشيرد او وميديافير.او أي مركز تحميل)

للحمايه من طريقه هذي :

قم بتحميل اي برنامج يعجبك من موقعه الرئيسي لكي يكون خالي من ملف تجسس

٣. دمج ملف تجسس مع صفحه مزوره تعمل علي متصفح

للحمايه من طريقه هذي :

استخدم متصفح فايرفوكس او قوقل قروم اكثر امان ويحميك من خدع وثغرات

٤. تحكم الهكر فيك اذا كنت مخترق

بعد قبولك ملف تجسس او كنت مخترق من قبل يتم اتصالك عند الهكر ببرنامج الاختراق

فوائد برنامج الاختراق :



يستطيع مشاهدة كامرتك مثل :



للحمایه من مشاهدة كام

ضع لازق او غطاء علي كام (اعتقد الكل يعرفها)

يستطيع سرقة باسورداتك وايميلاتك وحساباتك مصرفيه مثل :

Passwords type	Server Name	Users	Password
 http://www.alaw...	Server_HAMAD-PC^hama...	love yq8	love yq8
 Messenger	Server_HAMAD-PC^hama...	d@hotmail.com	loveyq8

الباسوردات محفوظه بجهازي التي استطاع
الهكر اخراجها وسرقتها

100%

[New Text Document.txt - Notepad] --- 12/08/2011 14:48:16

لأوف ياكويت [Right Alt]

لوف ياكويت

[Windows Live Messenger] --- 12/08/2011 14:49:13

d@hotmail.comloveyq8

[Google - ١٤:٤٩:٣٢ ٢٠١١/٠٨/١٢ --- موزيلا فَيْرُفُكس]

العوازم [Right Alt]

شبكة مجالس قبيلة العوازم الهوازنية - الموقع الرسمي لقبيلة العوازم - موزيلا فَيْرُفُكس] --- ٢٠١١/٠٨/١٢
14:49:49

لأوف ياكويتلوف ياكويت [Backspace][Right Alt][Backspace][Right Alt]

للحمية من سرقة باسورداتك

قم بمسح باسوردات محفوظة بجهازك ولا تحفظها

ويستطيع سماع صوتك عن طريق مايكروفون بجهازك

ويستطيع تحكم بالفارة ومراقبة شاشة ماذا تفعل

ويستطيع ارسال فايروسات لك لتجربتها عليك او مسح ملفات بجهازك

او نقل ملفات وخصوصيات بجهازك لدي دون ان تعلم

٥. حذف ملف التجسس بسهولة :

ملف تجسس يكون موجود ببدء تشغيل الجهاز كما ذكرت صوره لبرامج بدء تشغيل جهازي بعد فتح الملف

Starter (Windows 7)

File Edit Configuration Help

Exit New Edit Delete Refresh Launch Properties Options About

Startups Processes Services

Sections	Name	Value
All sections (4)	csrss	C:\Program Files\google\update.exe
Startup folders	KeyScrambler	C:\Program Files\KeyScrambler\keyscrambler.exe /a
Current user	rundll32	C:\Program Files\google\update.exe
All users	Shadow Defende...	C:\Program Files\Shadow Defender\DefenderDaemon.ex
Default user		
Registry (4)		
Current user (1)		
Run (1)		
RunOnce		
All users (3)		
Run (3)		
RunOnce		
RunOnceEx		
RunServices		
RunServices...		
Default user		
Run		
RunOnce		
INI files		

حيله حلوه لكي لانشك انه ملف تجسس
ايقونه ريل بريل واسم عمليه بجهاز ج
ومكان ملف بقوغل ابديت لخداعنا

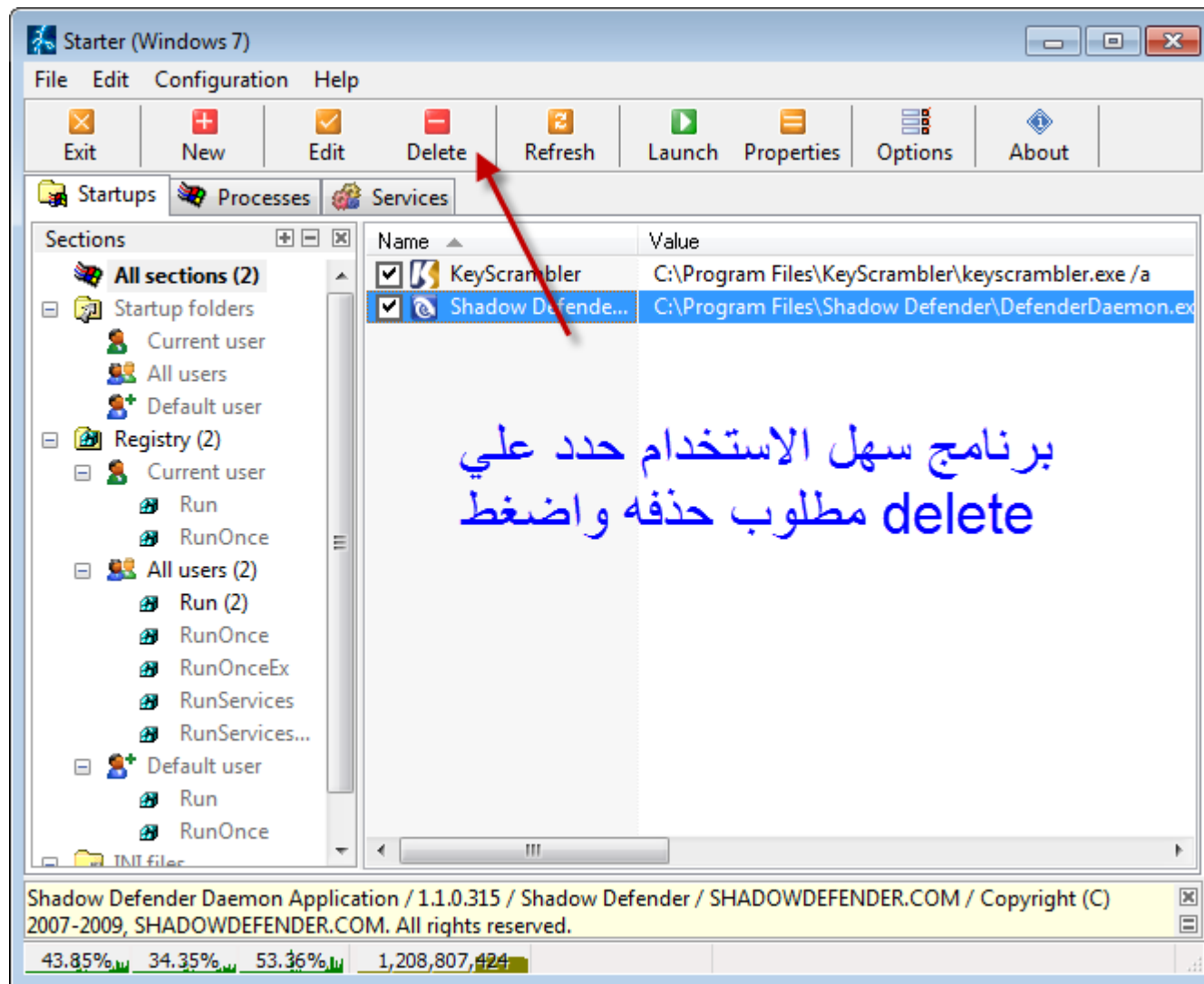
Shadow Defender Daemon Application / 1.1.0.315 / Shadow Defender / SHADOWDEFENDER.COM / Copyright (C)
2007-2009, SHADOWDEFENDER.COM. All rights reserved.

19.76% 18.22% 21.31% 1,127,364,992

للهمك خدع كثره لكي لانشك بملفه التجسس هناك اربع برامج برنامج تجميد الجهاز وبرنامج تشفير الكيبورد وبرنامج اساميهام مثل اسامي ملفات النظام ويايقونه ريل بلير

هذي طريقه وضعها الهكر لكي يخدعنا بان ملف هذا هو برنامج من برامج المثبته بجهازي او هي ملفات للنظام

الحل نحذف ملفين ونخلي برنامج تشفير الكيبورد وبرنامج تجميد النظام كما بالصوره



لو كان ملف التجسس مشفر من الحماية التي بجهازي وسويت فحص للجهاز ولم يكتشفها هل يعني ان جهازي ليس بمخترق

هذا غير صحيح الحل الافضل هو بدء تشغيل بدون الاعتماد علي برامج التنظيف

تحميل برنامج

<http://www.snapfiles.com/downloads/starter/dlstarter.html>

بعد تحميل اضغط كله (next) وثبيت برنامج

٦. نقاش اسأله واجوبه عن طرق صحيحه ولماذا

لماذا استخدم برنامج هذا وهناك طرق كثيرة منتشرة بالنسبة لمعرفة جهاز مخترق ؟

الطرق وبرامج منتشرة ليست قوية بالتأكد بان الجهاز مخترق او لا لان كما ذكرت يستطيع تلغيم وتشفير منها

لماذا ليست قوية ؟

لان الهكر مثل ما استطاع خداع حمايات بملفه تجسس يستطيع خداع برامج وطرق تاكد بان الجهاز مخترق

طيب ماهو الحل الاسهل والاقوي لتأكد بان الجهاز مخترق او لا ؟

الحل بسيط وهو اعتمادك علي معرفة برامج بدء تشغيل الجهاز كما بالصورة فوق حمل برنامج وحذف كل برامج بدء تشغيل مع الجهاز واترك الحماية (كما ذكرت بأن ملف تجسس يكون ببداية تشغيل الجهاز)

هل عند حذف برامج من بدء تشغيل تنحذف من جهازي او تضره ؟

لا لانها مثبتة بالجهاز كانت تعمل مع بدء تشغيل الجهاز والان لاتعمل الا اذا فتحت البرنامج الذي تريده بنفسك (فقط الذي ينحذف ملفات التجسس لانه ليس مثبت بالجهاز كبرنامج)

مثل ماذا برامج تعمل بدء تشغيل وبرامج التي لاتعمل ببداية تشغيل ؟

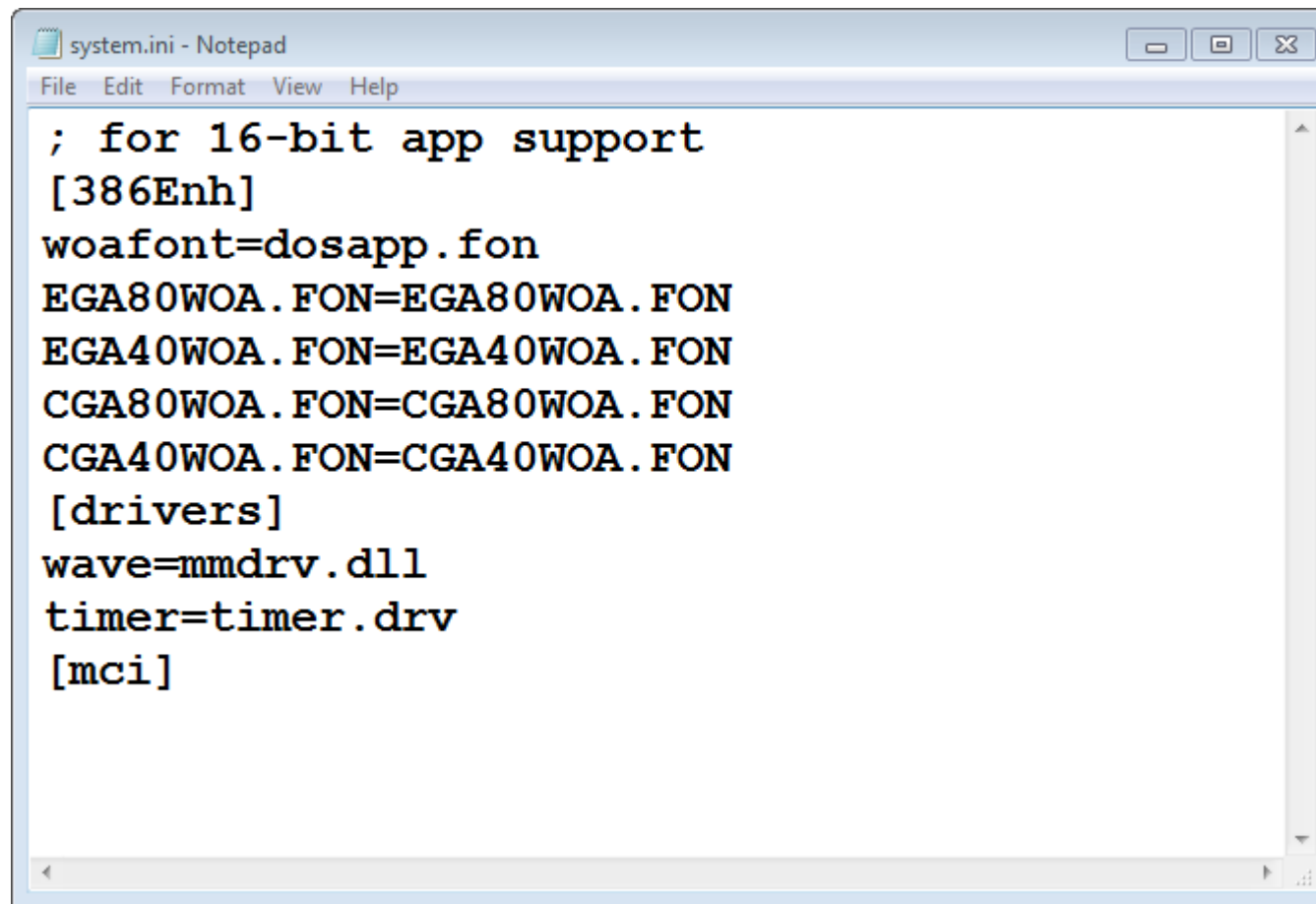
مثل فوتوشوب لايعمل مع بدء تشغيل الجهاز ولكن موجود بالجهاز متي ماردت العمل عليه فتحت فوتوشوب

ومثل الماسنجر تستطيع ان تجعله يعمل مع بدء تشغيل الجهاز كل ماتشغل الجهاز يشتغل الماسنجر امامك واذا حذفته من بدء تشغيل الجهاز لا يشتغل امامك الا اذا ضغط عليه

٧. طريقه فاشله يقع فيها الكثير لمعرفة الجهاز مخترق او لا (system.ini)

انتشرت بالنت طرق كثيره ليست لها اهميه كبيره بمعرفه جهاز مخترق او لا فكما ذكرناه الاختراق يكون بملف تجسس ويكون في بدء تشغيل الجهاز

الان جهازي مخترق نستخدم الطريقه منتشره وهي (system.ini)



```
system.ini - Notepad
File Edit Format View Help
; for 16-bit app support
[386Enh]
woafont=dosapp.fon
EGA80WOA.FON=EGA80WOA.FON
EGA40WOA.FON=EGA40WOA.FON
CGA80WOA.FON=CGA80WOA.FON
CGA40WOA.FON=CGA40WOA.FON
[drivers]
wave=mmdrv.dll
timer=timer.drv
[mci]
```

كما هو منشور **woa** تعني بان الجهاز سليم ! شلون هو سليم وانا فاتح ملف تجسس بجهازي

هل الاعتماد علي طريقه هذي تفيدني بتأكد من سلامة جهاز وهل ملف تجسس له اهميه بالملف هذا لكي يخبرني بان الجهاز مخترق ؟

الجواب لا لان ملف (system.ini) وظيفة معلومات عن نظام توزيعه ويندوز التي بالجهاز وليس لها اهميه بالاختراق

٨. نصائح مهمه :

ملف تجسس اسمه تروجان (trojan) واسمه بالعربي ببعض برامج حمايه معربه (حصان طرواده)

وهناك فرق بين ملف تجسس والفايروس

ملف تجسس مكانه الوحيد بدء تشغيل الجهاز والفايروس ليس له مكان محدد لانه يلتزم وينتشر بجميع ملفات

للحمايه من ملف تجسس كما ذكرت ببرنامج معرفة برامج بدء تشغيل وحذف ملف

للحمايه من الفايروس اسخدم برامج الحماية واعمل فحص لجهازك وينحذف الفايروس

٩. مسلتزمات تحميك من ملفات التجسس والفايروسات ومشاكل النت

1. يجب ان يكون في جهاز برنامج حمايه شغال بدون مشاكل وكل فتره اعمل فحص لجهازك

2. عدم حفظ ارقامك سريه بجهازك (مثل ماسنجر ويوزر نيم للمنتديات) وتركيب مشفر كيبورد keyscrambler

3. عدم حفظ خصوصياتك بالنسبة لضعها في فلاش او هارديسك خارجي ولا تضعها بالجهاز

4. مراقب برامج بدء تشغيل كل فتره

انتهى الشرح

اتمنى لكل الفائده من الكتاب ويكون مرجع لكل من يشك في جهازه

لا اريد منك الا الدعوات الطيبه لي ولوالديني علي عمل الخير والفائده لك

لوف ياكويت

m7nk@msn.com

(نحن قوم نصنع الابداع لكي نكسب من حولنا نعشق التحدي ولا نعرف الهزيمة وان طال بنا الزمان نصل للذي نريد)