

السلام عليكم ورحمة الله
اليوم ان شاء الله سنحاول دراسة أداة قوية نعم اخوانى أداة قوية
لأنها أزالة أقوى الأدوات من طريقها
دور هذه الأداة هو اعطاء تقرير شامل للجهاز من كل الجوانب
من تعريفات للجهاز وبرامج بداية التشغيل والتغييرات التي طرأت على الجهاز
نتيجة الاصابة بأحد الفيروسات و نتيجة الاستعما الخاطى لأحد التطبيقات
أعتقد أنكم عرفتم هذه الأداة??

نعم اخوانى الأداة هي **Runscanner**
قبل وضع محاور لدرس
سنطرح عليكم سؤال ماذا تعرفون عل هذه الأداة??

اخوانى نريد من جميع الأخوة تحميل الأداة أولا

من هنا

[Download Runscanner](#) 

موقع الأداة

<http://www.runscanner.net/>

هذه أهم المحاور التي سنتناولها ان شاء الله

بخصوص هذه الأداة

1* تعريف أداة Runscanner

2* تبين الخصائص الجديدة التي أتت بها والتي امتازة بها على hijackthis

3* توضيح لماذا لم نعتمدها لحد الآن بالقسم وتشبنتنا ب hijackthis

4* شرح لكيفية التعامل مع هذه الاداة أولا كيفية اسخراج التقرير بصيغتين

و كيفية الفحص المباشر من الموقع وكل هذا يوجد فى الخاصية الاولى وهي **Beginner mode**

5* شرح خاصية Expert mode فى هذه الخاصية يوجد الكثير لتوضيح

6* التركيز على التقرير التنفيذي run لشرح كيفية رفع التقرير الى خبير ليتم تحليله

ثم اعادة ارساله للعضو ليقوم بحذف الأسطر التي حددها الخبير

7* شرح كيفية تعلم تحليل أسطر هذه الاداة

[تعريف شامل للأداة من موقعها الرسمي](#)

اداة مجانية تقوم بفحص شامل للنظام والبرامج العاملة به وبرامج بدء التشغيل والتعريفات والخدمات ونقاط الاختطاف.

ويمكن استعمالها لاكتشاف التغييرات التي طرأت على النظام نتيجة الاصابة بملفات تجسس او فايروسات او اخطاء بشرية من قبل المستخدمين انفسهم.

هذه الاداة العجيبة بها مزايا خرافية بمعنى الكلمة حسب موقع الشركة الرسمي

وعن تجارب معها بكل صراحة وسنعرضها لكم الان.

- عدد الاسطر بها غير محدود ويزيد مع كل تحديث للمنتج.

- تحليل مباشر للمالوير على المواقع المتخصصة.

- تتمتع بقاتل بروسييس قوي جدا.

- حفظ التقارير بصيغتين مختلفتين على هيئة مفكرة او ملف تشغيلي.

- فلتر قوية للملفات.

- محرر لملفات الهوست.

- استعادة الاسطر والقيم المحذوفة بكل بساطة.

- اصلاح وتنشيط متصفح الاكسبلورر.

- تحليل شهادة ومصادقية البرامج المثبتة على انظمتنا.

- يوجد بها وضعين للاستخدام وضع للمبتدئين ووضع للخبراء.

- تحليل للقيم الخوارزمية الرقمية والتشفيرات على موقع FILE ADVISOR.

- تحليل التقارير على موقع www.systemlookup.com.

- رفع التقارير وتحليلها على موقع www.VirusTotal.com.

- تحليل الوحدات المحملة.

- فحص التقارير بموقع المنتج الرسمي.

- اصلاح قيم الريجستري.

ولا ننسى اخواني تحدير بخصوص هذه الأداة

يجب عدم استعمال الاداة بشكل فردي لان ذلك سيؤدى الى نتائج سلبية على نظامك

وانا اخلى مسنوليتي عن اي اجتهاد فردي دون استشارة فريق الخبراء.

من هنا الموقع الرسمي للاداة لمزيد من المعلومات

<http://www.runscanner.net/>

اخوانى الاداة بها 3 خاصيات للفحص

1الفحص عبر الموقع

2الفحص عبر الاداة

3الفحص من طرف الخبراء

ودائما نجد تحديثات لها

والجميل ان التغييرات التى تطرء عليها نجدها بالموقع

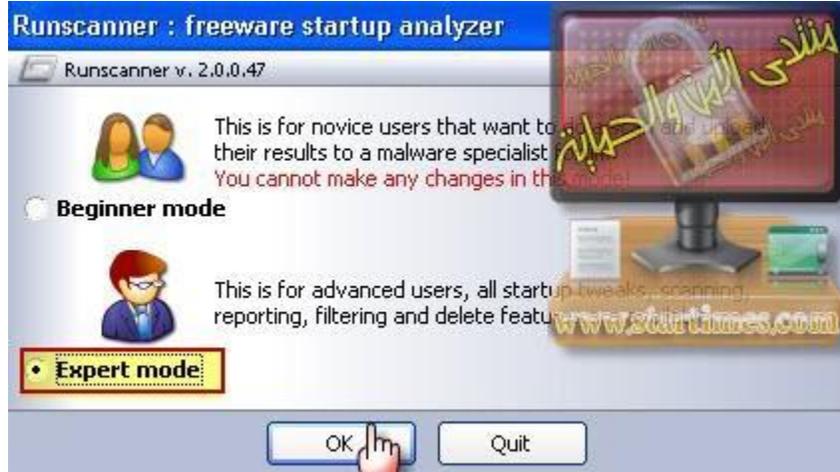
من هنا

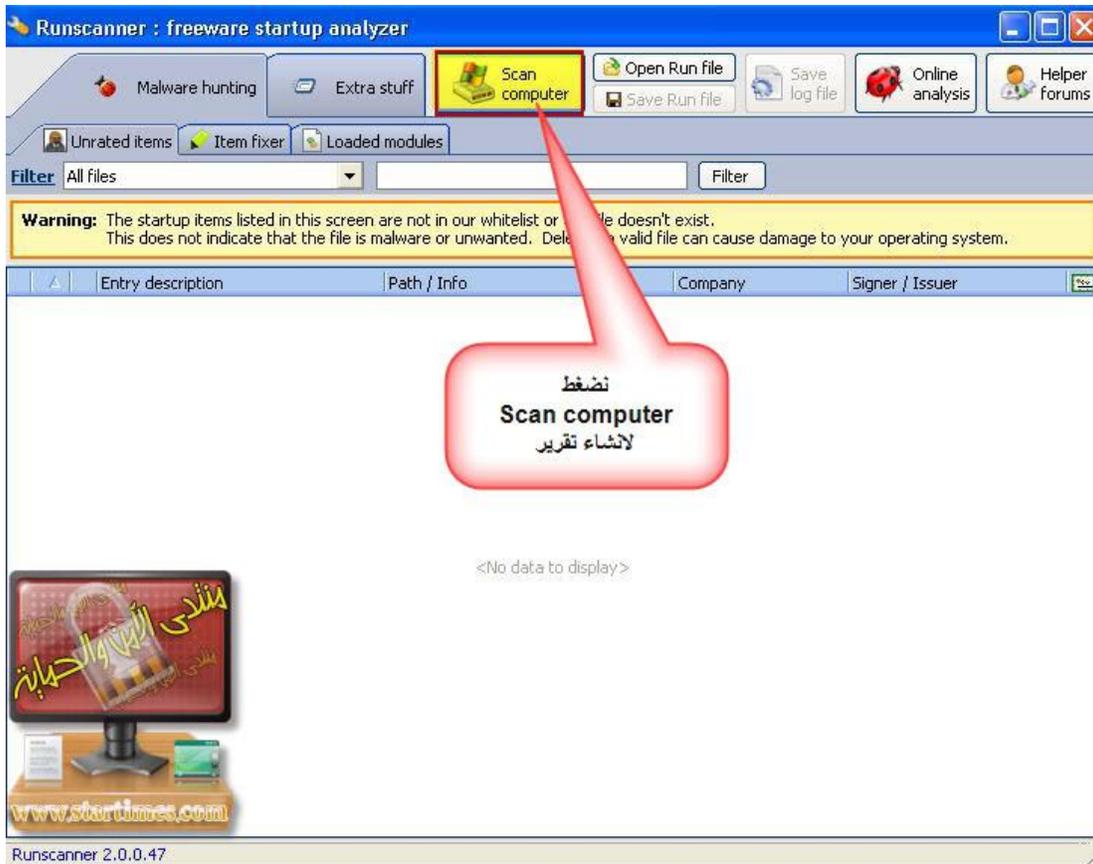
<http://www.runscanner.net/changelog.aspx>

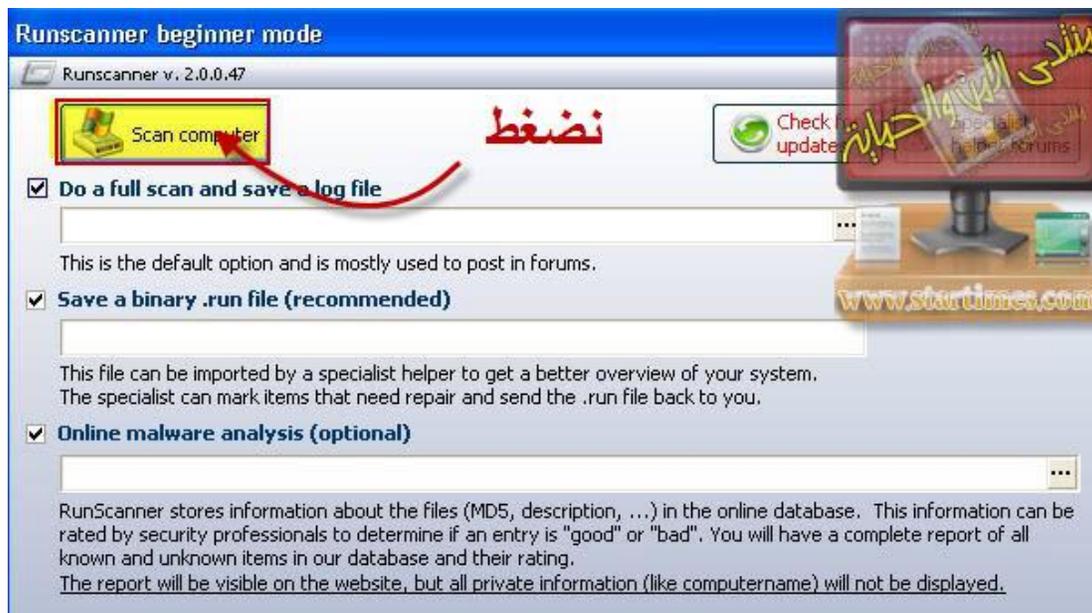
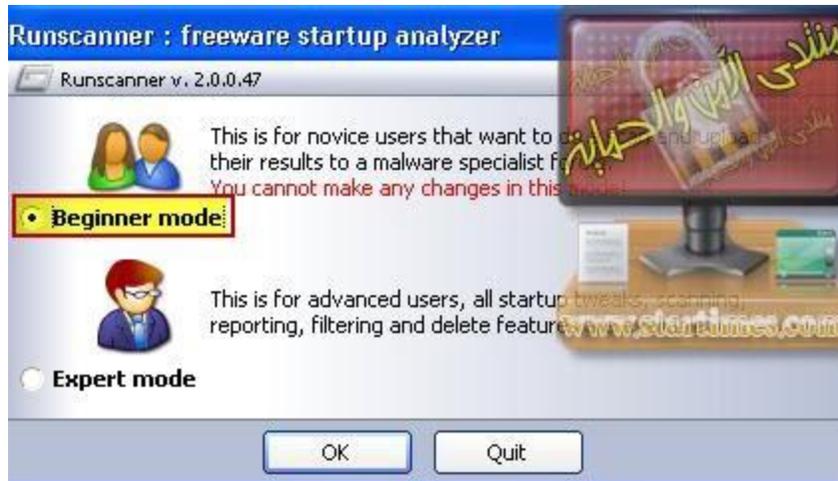
كيفية انشاء التقرير اذا كنت تريد ارسله لحد الخبراء لتحليله

بعد الضغط على دويل كليك على أيقونة Runscanner

نتقوم بتالى



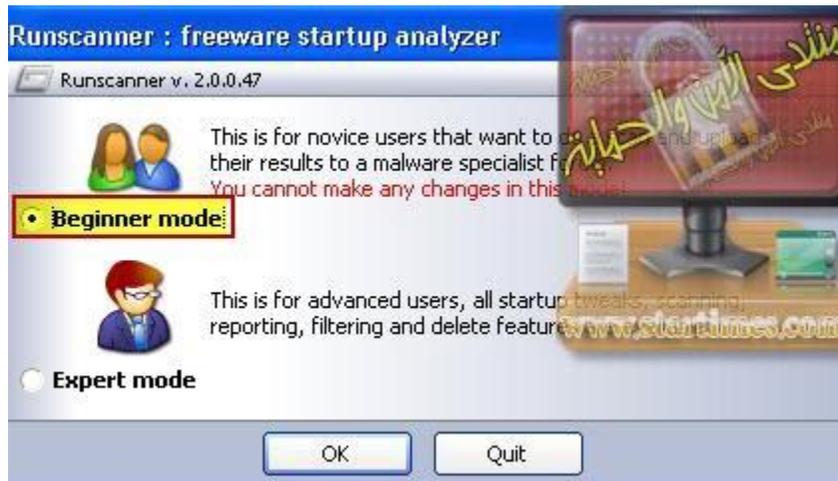


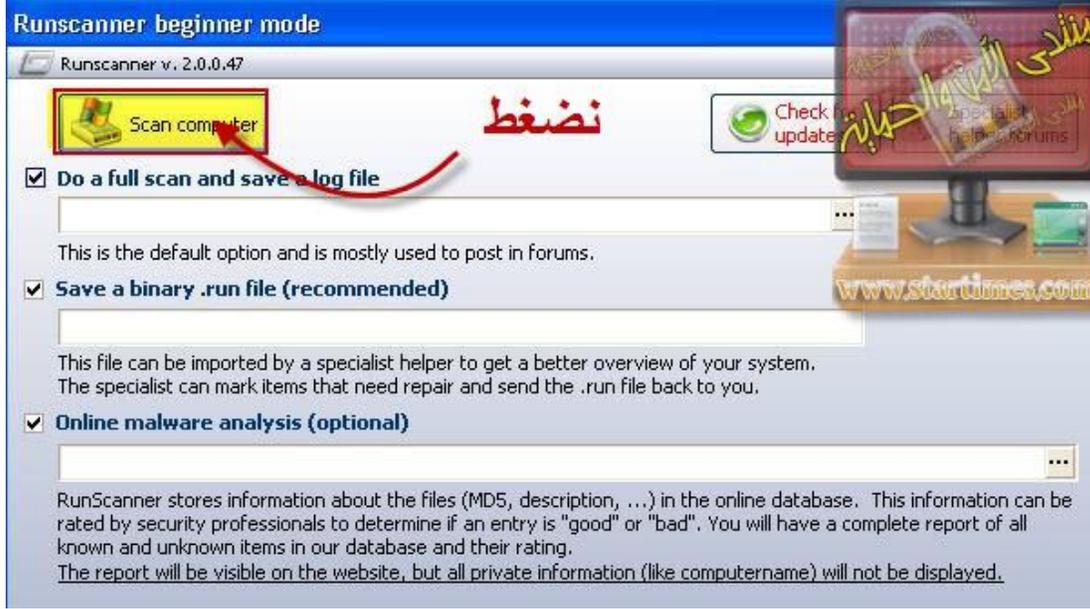




هذا شرح

لكيفية تحليل التقرير عبر موقع الأداة





تم انشاء التقرير بجميع الخصائص

هدفنا هو الفحص عبر الموقع لدى يجب ان

نضغط كما هو موضح فى الخاصية 3 Online malware analysis

ليتم تحويلنا مباشرة الى موقع الفحص



هذا هو موقع الفحص الآن يجب ان نبدأ بالفحص

وذلك بالاعتماد على الألوان

يوجد عندنا 3 ألوان

الأخضر وهو سليم

الأزرق لا توجد له معلومات في هذا الرابط لهذا يجب المزيد من الفحص عبر عدة خصائص

سنتعرف عليها فيما بعد

أما اللون الأحمر فهذا يعني ان السطر ضار مباشرة للحذف

Analysis report

Report is not yet complete.
You are relying on an online report.

Security.

?report=ae49f051-a37b-47e6-adf4-6df614add22b

Compact report

fixing items on your system!

كيفية معرفة الأسطر السليمة من الضار

- ① اللون الأخضر يعني سطر سليم
- ② اللون الأزرق لا توجد له معلومات في هذا الموقع غالبا يكون سليم
- ③ اللون الأحمر يعني سطر ضار وهو للحذف

-

2.0.0.47
08/09/2010 15.53.16
Administrator
Microsoft Windows XP
2600
Service Pack 2
Arabe (Maroc)
8.0.6001.18702
C:\WINDOWS
%SystemRoot%\System32\drivers\etc
0

نضغط

Switch to the compact report

ليظهر التقرير كاملا

C:\WINDOWS\system32\smss.exe - Microsoft Corporation
C:\WINDOWS\system32\csrss.exe - Microsoft Corporation
C:\WINDOWS\system32\winlogon.exe - Microsoft Corporation
C:\WINDOWS\system32\services.exe - Microsoft Corporation
C:\WINDOWS\system32\lsass.exe - Microsoft Corporation
C:\WINDOWS\system32\svchost.exe - Microsoft Corporation
C:\WINDOWS\system32\svchost.exe - Microsoft Corporation
C:\WINDOWS\system32\svchost.exe - Microsoft Corporation

Internet Download Manager agent for click monitoring in IE-b...	C:\Program Files\Internet Download Manager\IEMonitor.exe - Tonec Inc.
Runscanner freeware startup analyzer	C:\Documents and Settings\Administrateur\POSTE\Bureau\runscann... - Runsc...
Paint	C:\WINDOWS\system32\mspaint.exe - Microsoft Corporation
002 Autorun registry entries local machine	
avgnt	C:\Program Files\Avira\AntiVir PersonalEdition Premium\avgnt.e... - Avira Gm...
003 Autorun registry entries Current User	
IDMan	C:\Program Files\Internet Download Manager\IDMan.exe - Tonec Inc.
ctfmon.exe	C:\WINDOWS\system32\ctfmon.exe - Microsoft Corporation
008 Autorun registry entries Default user	
CTFMON.EXE	C:\WINDOWS\system32\CTFMON.EXE - Microsoft Corporation
010 Installed services	
Avertissement	C:\WINDOWS\system32\svchost.exe - Microsoft Corporation
Service de la passerelle de la couche Application	C:\WINDOWS\System32\alg.exe - Microsoft Corporation
Avira AntiVir Premium MailGuard	C:\Program Files\Avira\AntiVir PersonalEdition Premium\avmailc... - Avira GmbH
Planificateur Avira AntiVir Premium	C:\Program Files\Avira\AntiVir PersonalEdition Premium\svched.e... - Avira GmbH
Avira AntiVir Premium Guard	C:\Program Files\Avira\AntiVir PersonalEdition Premium\avguard... - Avira GmbH
Avira AntiVir Premium WebGuard	C:\Program Files\Avira\AntiVir PersonalEdition Premium\AVWEBGR... - Avira GmbH
Apple Mobile Device	C:\Program Files\Fichiers communs\Apple\Mobile Device Support... - Apple Inc.
Gestion d'applications	C:\WINDOWS\system32\svchost.exe - Microsoft Corporation
ASP.NET State Service	C:\WINDOWS\Microsoft.NET\Framework\v2.0.50727\aspnet_state.e... - Microsoft Corporation
AST Service	C:\WINDOWS\system32\ASTSRV.EXE - Nalpeiron Ltd.
Audio Windows	C:\WINDOWS\System32\svchost.exe - Microsoft Corporation
Service d'assistance Avira AntiVir Premium MailGuard	C:\Program Files\Avira\AntiVir PersonalEdition Premium\avesvc... - Avira GmbH
Service de transfert intelligent en arrière-plan	C:\WINDOWS\system32\svchost.exe - Microsoft Corporation
Service Bonjour	C:\Program Files\Bonjour\mDNSResponder.exe - Apple Inc.
Explorateur d'ordinateur	C:\WINDOWS\system32\svchost.exe - Microsoft Corporation
Capture Device Service	C:\Program Files\Fichiers communs\InterVideo\DeviceService\Dev... - InterVideo Inc.
Gestionnaire de l'Album	C:\WINDOWS\system32\clipsrv.exe - Microsoft Corporation
.NET Runtime Optimization Service v2.0.50727_X86	C:\WINDOWS\Microsoft.NET\Framework\v2.0.50727\mscorsvw.exe - Microsoft Corporation
Application système COM+	C:\WINDOWS\system32\dllhost.exe - Microsoft Corporation
CryptSvc	C:\WINDOWS\system32\svchost.exe - Microsoft Corporation
Lanceur de processus serveur DCOM	C:\WINDOWS\system32\svchost.exe - Microsoft Corporation
Client DHCP	C:\WINDOWS\system32\svchost.exe - Microsoft Corporation
Service d'administration du Gestionnaire de disque logique	C:\WINDOWS\System32\dmadmin.exe - Microsoft Corp., Veritas Software
Gestionnaire de disque logique	C:\WINDOWS\System32\svchost.exe - Microsoft Corporation
Client DNS	C:\WINDOWS\system32\svchost.exe - Microsoft Corporation
Service de rapport d'erreurs	C:\WINDOWS\System32\svchost.exe - Microsoft Corporation

تم تحليل جميع الأسطر

أخواني فقط لتوضيح بعض الأشياء
إذا وجدنا في المستطيل الملون بالأصفر

فقط لون أزرق ولون أحمر

فهذا يعني أن الأزرق سليم والأحمر ضار

sis report

e is not yet complete.
an relying on an online report.

ety.

?report=ae49f051-a37b-47e6-adf4-8df614add22b

compact report

fixing items on your system!

كيفية معرفة الأسطر السليمة من الضار

- ① اللون الأخضر يعني سطر سليم
- ② اللون الأزرق لا توجد له معلومات في هذا الموقع غالبا يكون سليم
- ③ اللون الأحمر يعني سطر ضار وهو للهدف

2.0.0.47
08/09/2010 15.53.16
Administrator
Microsoft Windows XP
2600
Service Pack 2
Arabe (Maroc)
8.0.6001.18702
C:\WINDOWS
%SystemRoot%\System32\drivers\etc
0

نضغط

Switch to the compact report

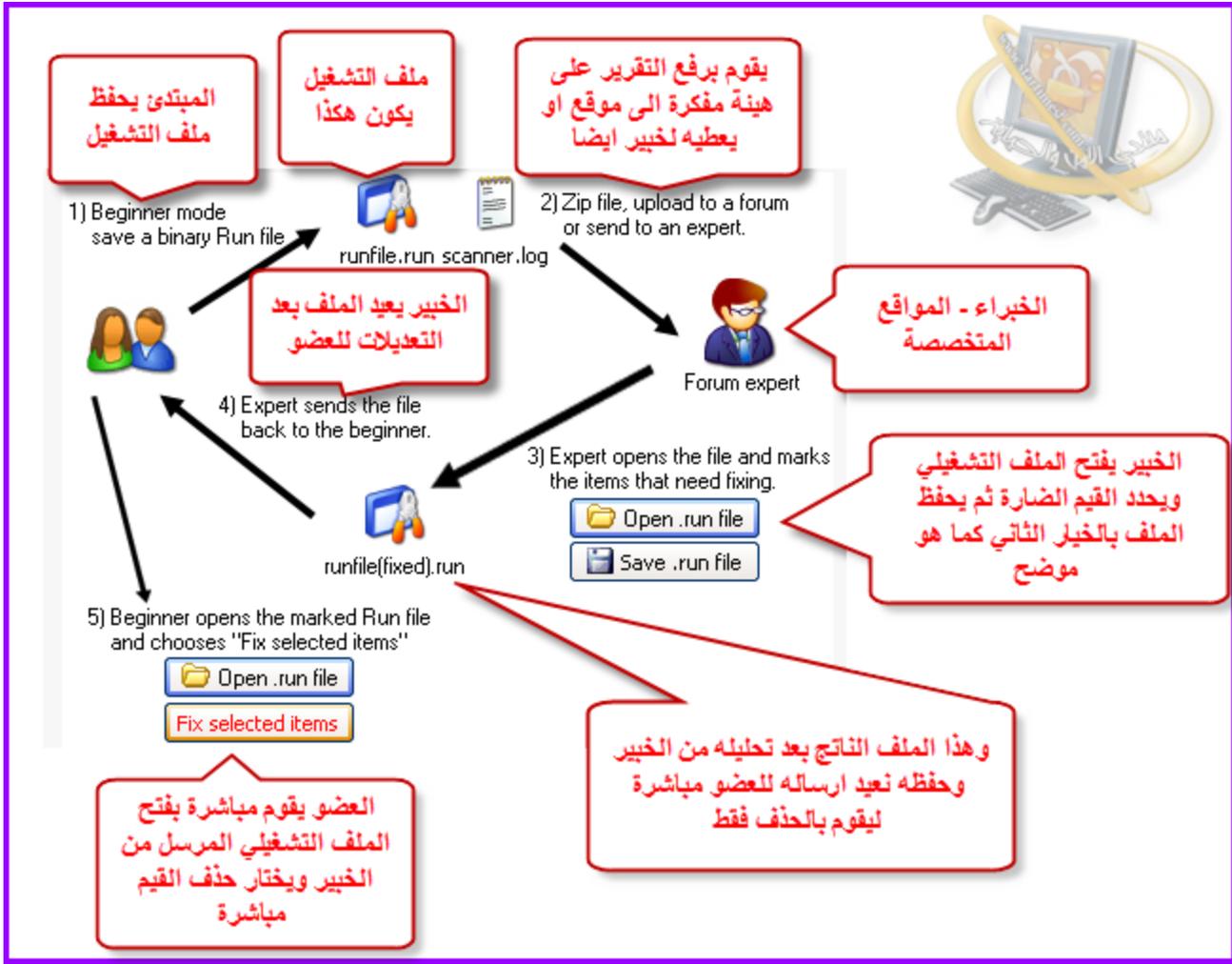
ليظهر التقرير كاملا

C: \ WINDOWS \ system32 \ smss.exe - Microsoft Corporation
C: \ WINDOWS \ system32 \ csrss.exe - Microsoft Corporation
C: \ WINDOWS \ system32 \ winlogon.exe - Microsoft Corporation
C: \ WINDOWS \ system32 \ services.exe - Microsoft Corporation
C: \ WINDOWS \ system32 \ lsass.exe - Microsoft Corporation
C: \ WINDOWS \ system32 \ svchost.exe - Microsoft Corporation
C: \ WINDOWS \ system32 \ svchost.exe - Microsoft Corporation
C: \ WINDOWS \ system32 \ svchost.exe - Microsoft Corporation

في انتظار التحاق الاخوة

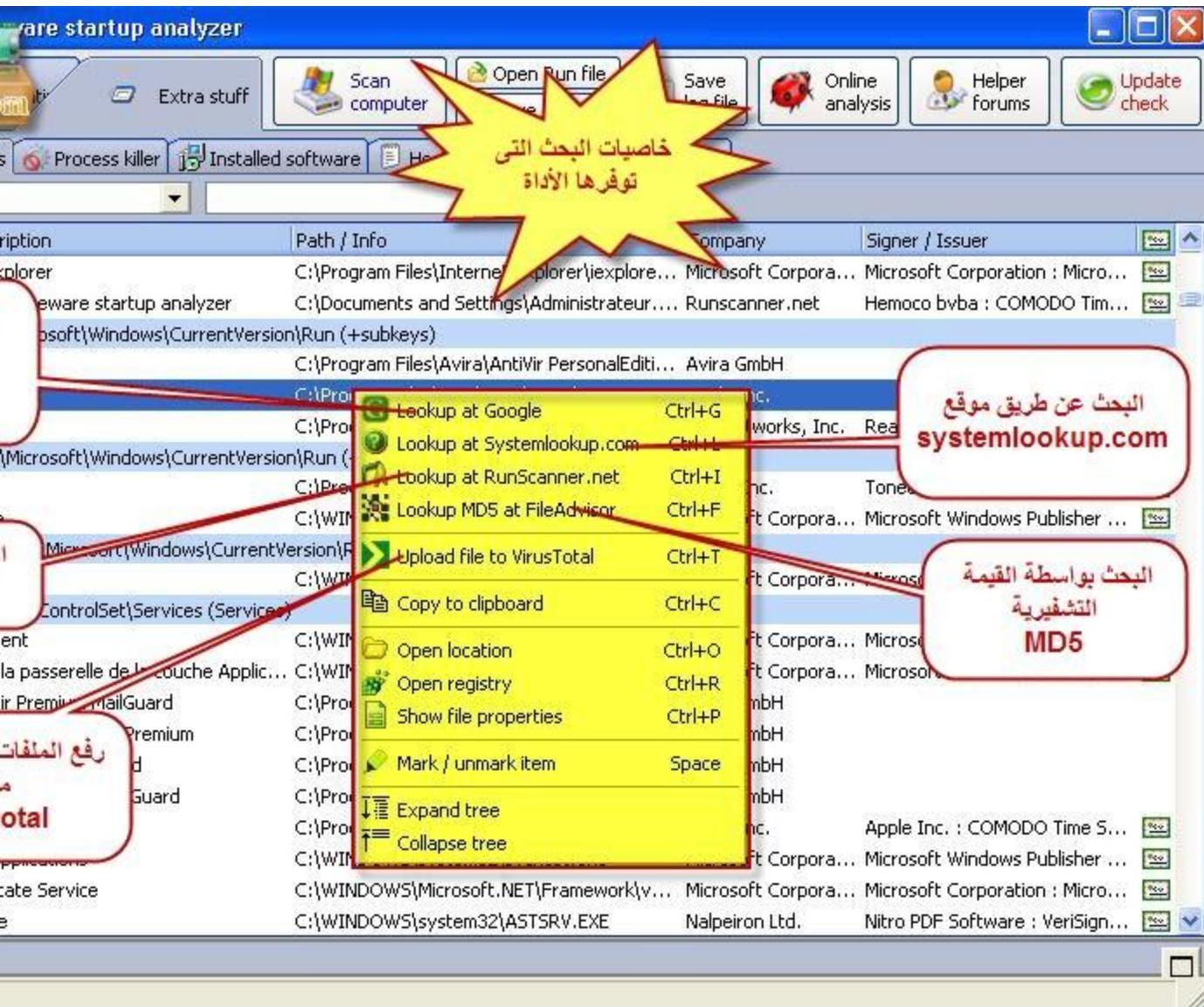
يمكنكم مراجعة هذا الرسم الذى يوضح

كيفية العمل بالاداة



كيفية تحليل أسطر هذه الاداة سهل وأفضل من Hijackthis

المشكلة فقط هو في كثرة الأسطر أي تأخذ منك الوقت الكثير رغم عمل فيلتر للأسطر
للتأكد من سلامة الاسطر فقط يجب الضغط بيمين الفأرة لكي يظهر لك كما في الصورة



أي يظهر لك

Lookup at google

Lookup at systemlookup.com

Lookup at Run scanner.net

Lookup MD5 at FileAdvisor

هذه العناصر الثلاثة هي الخاصيات التي تقوم بفحص أسطر

الأول هو محرك البحث google وهو الافضل أي عندما تضغط عليه يتم تحويلك مباشرة اليه

وبتالى يعطيك مجموعة من النتائج لكي تتأكد هل السطر سليم ام ضار كما نقوم في Hijackthis
نقوم بنسخ الجزء الأخير دات الامتداد exe أو... dll

ونضعه بمحرك البحث للحصول على نتائج وهو كذلك مع runscanner لا يوجد أي اختلاف لكن
runscanner توفر عليك نسخ لصق

وتقوم بتحويلك مباشرة الى الموقع....

ونفس الشيء بنسبة لى المواقع الأخرى هي الأخرى بمجرد الضغط عليها تقوم بتحويلك مباشرة الى
موقع الفحص للحصول على نتائج

التصنيف حسب الأكثر فعالية فى اعطاء نتائج صحيحة بين هذه العناصر هو

1

google

2

الفحص بواسطة القيمة التشفيرية MD5

3

Runscanner.net

4

systemlookup.com

أما اذا لم تجد اجابة فى هذه المواقع يمكنك رفع الملف المتمثل فى السطر
تقوم برفعه على موقع virustotal لكي يتم فحصه واعطائك النتائج
وهذه الخاصية هي

Upload file to virus total

بنسبة للفحص بواسطة محرك البحث

أعتقد أنها مفهومة لا تستدعى الى شرح

سننتقل مباشرة الى الفحص بواسطة

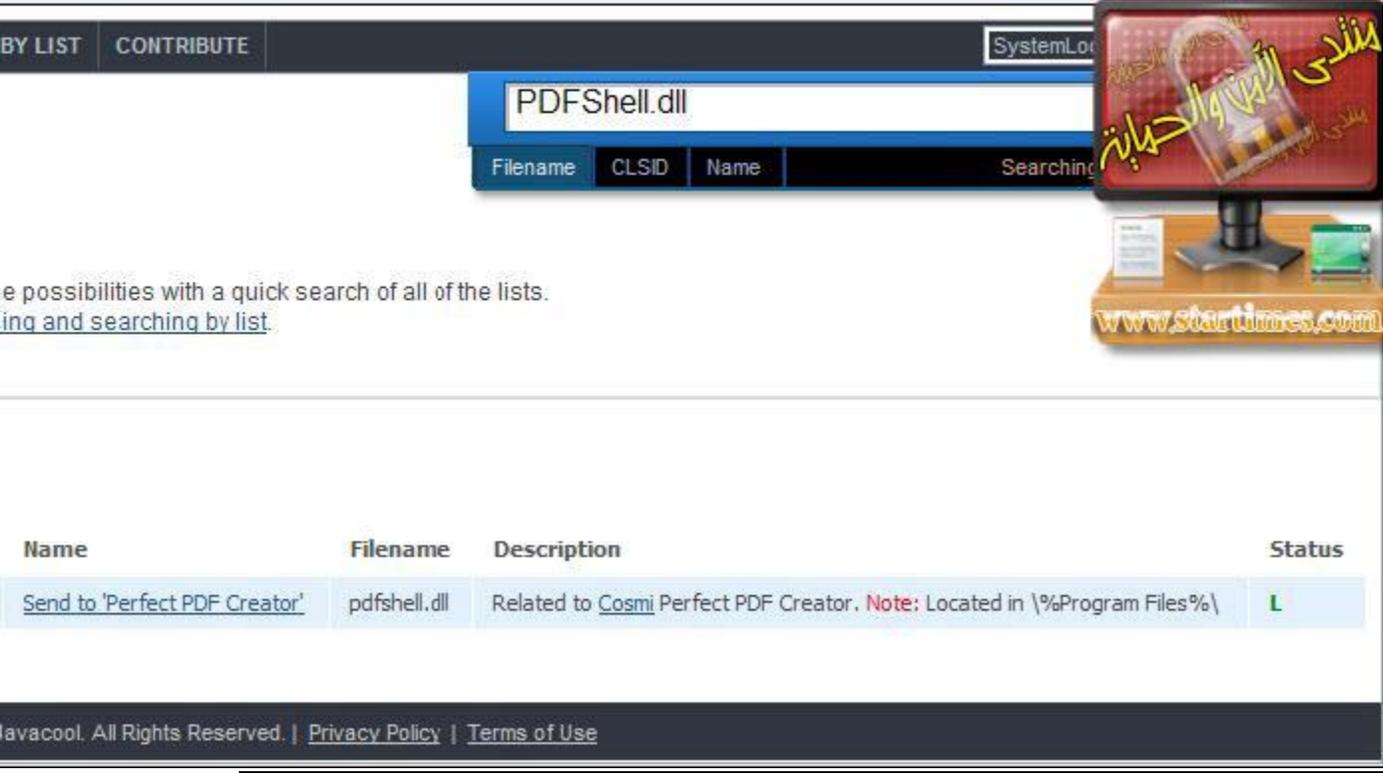
Lookup at systemlookup.com

عندما نضغط عليه يتم تحويلنا مباشرة الى الموقع

وهذه صورة للموقع كيفية معرفة الأسطر السليمة من الضار

انظرو الى الحرف الأخير الملون بالأخضر الموجود بـ**Status**

هذه الوضعية هي التي تحدد الاسطر السليمة من الضارة



SystemLo

PDFShell.dll

Filename CLSID Name Searching

www.startimes.com

possibilities with a quick search of all of the lists.
ing and searching by list.

Name	Filename	Description	Status
Send to 'Perfect PDF Creator'	pdfshell.dll	Related to Cosmi Perfect PDF Creator . Note: Located in \%Program Files%\	L

lavacool. All Rights Reserved. | [Privacy Policy](#) | [Terms of Use](#)

عندما نريد فحص عبر هذا الموقع

سنجد هذه الأحرف

الصف الأول وهو خاص بالبرامج التي تقلع مع تشغيل الوندوز

وهي

Y

N

U

X

?

الصف التنى من الأسطر وهي خاصة بباقى التطبيقات

وهي

X

L

O

?

شرح الأحرف

Xمباشرة للحدف

Lسطر سليم

Oلك الاختيار فى حدفه او تركه هنا وجب المزيد من التأكد

? غير معروف هو الآخر يجب ان نتأكد منه عبر باقى المواقع

الآن ننتقل الى الخاصية 3

وهي موقع الأداة وهو

Lookup at Run scanner.net

عندما نضغط عليه يتم تحويلنا مباشرة الى الموقع

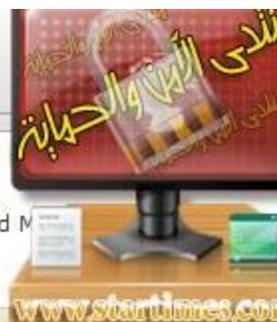
وهذا فحص للأحد الأسطر

هنا نجد جميع المعلومات المتعلقة بالسطر الذى أردنا فحصه



Search filename

Search



Atiacmxx.dll

AMD Desktop Control Panel - AMD Desktop Component - Advanced M

Run a Free Scan for ATIACMXX.DLL related errors

Atiacmxx.dll file description

Atiacmxx.dll with description AMD Desktop Control Panel is a process file from company Advanced Micro Devices, Inc. belonging to product AMD Desktop Component. In total there are 8 launchpoints for this file . There are 12 different variations of the file in our database and the file is not digitally signed.

Automatic startup locations



- 061 Shell Approved Extensions
- 173 ContextMenuHandlers
- 221 HKLM *\ShellEx\ContextMenuHandlers
- 223 HKLM AllFileSystemObjects\ShellEx\ContextMenuHandlers
- 225 HKCU Folder\ShellEx\ContextMenuHandlers
- 227 HKLM Directory\ShellEx\ContextMenuHandlers
- 229 HKLM Directory\Background\ShellEx\ContextMenuHandlers

File versions in our database

Company	Version	Size
Advanced Micro Devices, Inc.	6 14.10.2001	708608
Advanced Micro Devices, Inc.	6 14.10.2001	704512
Advanced Micro Devices, Inc.	6 14.10.2001	700416
Advanced Micro Devices, Inc.	6 14.10.2001	696320
Advanced Micro Devices, Inc.	6 14.10.2001	692224
n/a	2 0, 0, 0	688128
n/a	1 0, 0, 1	73728
n/a	2 0, 0, 0	73728

بنسبة للفحص بواسطة القيمة التشفيرية MD5

Lookup MD5 at FileAdvisor

لقد سبق وشرحتها بهذا الموضوع

شرح القيمة التشفيرية MD5 على Runscanner

وتعتبر هذه القيمة هي أكثر استعمالا في العديد من الأمور الأمنية خاصة كلمات المرور

وقواعد البيانات الى أخره ...اسمها العلمى هو Data integrity

هي عبارة عن أرقام وحروف مشفرة طول مخرجات التشفير ب MD5 هو Bits128

لكن طول الرسالة الأصلية هو Bits 521 وادا زادت يتم تقسيمها الى حزمات هذا هو الذى يعطي لهذه القيمة مصداقية.

كان هذا فقط نظرة عن هذه القيمة

الآن نعود الى موضوعنا وهو كيفية استخراج هذه القيمة بRunscanner

ثم فحصها على أحد المواقع الخاصة بالفحص

بعد عمل فحص للجهاز بواسطة Runscanner

يعطينا الكثير من الأسطر وادا شككنا فى أحد الأسطر على انها فيروسات

نقوم بالضغط عليها بيمين الفأرة ثم نختار Lookup Md5 at FileAdvisor

freeware startup analyzer

Extra stuff

Scan computer

Open Run file

Save log file

Save Run file

Online analysis

Process killer

Installed software

Host file editor

History / backups

Temara_M2

Filter

Description	Path / Info	Company	Signer / Issuer
...	C:\DOCUME~1\morad\LOCAL5~1\Temp\wi...		
Update	C:\WINDOWS\system32\wuauclt.exe	Microsoft Corpora...	Microsoft Windows Compone...
...	C:\DOCUME~1\morad\LOCAL5~1\Temp\wi...		
Update	C:\WINDOWS\system32\wuauclt.exe	Microsoft Corpora...	Microsoft Windows Compone...
er freeware startup analyzer	C:\Documents and Settings\morad\Mes doc...	Runscanner.net	Hemoco byba : COMODO Tim...
C:\Microsoft\Windows\CurrentVersion\Run (+subkeys)			
ader Speed Launcher	C:\Program Files\Adobe\Reader 9.0\Reade...	Adobe Syst	
	C:\WI	Lookup at Google	Ctrl+G
	C:\WI	Lookup at Systemlookup.com	Ctrl+L
	C:\WI	Lookup at RunScanner.net	Ctrl+I
	C:\WI	Lookup MD5 at FileAdvisor	Ctrl+F
	C:\WI	Copy to clipboard	Ctrl+C
	C:\WI	Mark / unmark item	Space
	Expand tree		
	Collapse tree		

www.starttimes.com

نضغظ بيممين الفأرة على
على أحد الأسطر المراد حذفها ثم
نختار
**Lookup MD5 at
FileAdvisor**

بعد الضغظ يتم تحويلنا مباشرة الى الموقع الذي يكشف لنا عن القيمة



Search Results

are in your
rise?

Click here

You searched for

MD5: 4B10675852FE8862521024778E264D5F

Your hash has been found in **27 Package(s)**.

Click here to **Login** or **Register** to view more information.

ثم نقوم بنسخ هذه القيمة
وهي قيمة السطر الذي تريد أن
تفحصه

بعدما حصلنا عن القيمة ندخل على أحد مواقع الفحص

سأختار موقع **virustotal**

<http://www.virustotal.com>

بعد الدخول على الموقع نقوم بتألي

1 - بعد الدخول على الموقع
نضغط

Search



Virustotal is a **service that analyzes files and URLs** and facilitates the quick detection of viruses, worms, trojans, and all kinds of malware detected by antivirus engines. [More](#)



[Analysis](#) **[Search](#)** [Statistics](#) [Advanced](#) [VT Community](#) [About VT](#)

2 - نضع القيمة
هنا

Search for file reports (hash), url reports, VT Community users and VT community comment tags. [Find out more.](#)

59DC5BB82E4C8E0B3EADCFDBC44BA6E4

search

3 - نضغط على

هذه هي نتيجة الفحص لسطر سليم

0 VT Community user(s) with a total of 0 reputation credit(s) say(s) this sample is goodware. 0 VT Community user(s) with a total of 0 reputation credit(s) say(s) this sample is malware.

File name: **ctfmon.exe**
Submission date: **2010-09-07 00:31:28 (UTC)**
Current status: **finished**
Result: **0 /43 (0.0%)**

نتيجة الفحص هي

43/0

وهذا يعني ان سطر سليم
و اذا قرأنا اسم الملف ستجد اسمه

ctfmon.exe

وهذا يعني ان سطر اللغة



Compact

Antivirus	Version	Last Update	Result
ahnLab-V3	2010.09.07.00	2010.09.07	-
antiVir	8.2.4.50	2010.09.06	-
antiv-AVL	2.0.3.7	2010.09.03	-
Authentium	5.2.0.5	2010.09.06	-
avast	4.8.1851.0	2010.09.06	-
avast5	5.0.594.0	2010.09.06	-
AVG	9.0.0.851	2010.09.06	-
BitDefender	7.2.1010.0	2010.09.07	-
CAT-QuickHeal	10.0.0.10	2010.09.06	-
ClamAV	0.10.2	2010.09.07	-
Comodo	2.12.10.10	2010.09.07	-
DrWeb	4.4.1.10	2010.09.07	-
Emsisoft	12.0.1010.0	2010.09.07	-
ESafe	1.0.0.10	2010.09.05	-
Trust-Vet	1.0.0.10	2010.09.06	-
F-Prot	4.5.1.10	2010.09.01	-
F-Secure	9.0.15370.0	2010.09.07	-
Fortinet	4.1.143.0	2010.09.05	-
SafeData	21	2010.09.07	-

هنا نجد أسماء برامج الحماية التي قامت بفحص القيمة ونجد كذلك اصدار البرنامج وآخر تحديث له ثم نجد نتيجة كل برنامج

وهذه النتيجة مثال لسطر مصاب

خاصية فحص الملفات والبروسيس عبر المواقع التي توتال وغيرها خاصية جد قوية ورهيبة تقوم بالفحص اكثر



نختار اي ملف نريد مثلاً هذا

نضله بزر الفارة الايمن ثم نلاحظ الخصائص الرهيبة المتوفرة ونشرحها الان

هذا ما بهمنا

Icon	Action	Shortcut
	Lookup at Google	Ctrl+G
	Lookup at Systemlookup.com	Ctrl+L
	Lookup at RunScanner.net	Ctrl+I
	Lookup MD5 at FileAdvisor	Ctrl+F
	Upload file to VirusTotal	Ctrl+T
	Copy to clipboard	Ctrl+C
	Open location	Ctrl+O
	Open registry	Ctrl+R
	Show file properties	Ctrl+P
	Mark / unmark item	Space

فحص الملف عبر قوقل
فحص الملف عبر الموقع المحدد
فحص الملف عبر موقع البرنامج
فحص الخوارزميات بالموقع المحدد
رفع الملف الى موقع فايروس توتال
نسخ الملف الى الحافظة
فتح المكان او المسار الخاص به
فتح الريجستري
عرض خصائص الملفات
تحديد-الغاء تحديد الملف

File not found



Virustotal is a **service that analyzes suspicious files and URLs** and facilitates the quick detection of viruses, worms, trojans, and all kinds of malware detected by antivirus engines. [More information...](#)



0 VT Community user(s) with a total of 0 reputation credit(s) say(s) this sample is goodware. 0 VT Community user(s) with a total of 0 reputation credit(s) say(s) this sample is malware.

VT Community



not reviewed
Safety score: -

File name: **BRSERVICE.exe**
Submission date: **2010-08-26 01:52:36 (UTC)**
Current status: **analysing**

جاري فحص الملف عبر الموقع واظهار النتائج

المضاد Antivirus	Version	النسخة	Last Update	آخر تحديث	النتيجة Result
Avast5	5.0.594.0		2010.08.25		-
AVG	9.0.0.851		2010.08.25		-
Fortinet	4.1.143.0		2010.08.25		-

Additional information **معلومات اضافية**

اظهار الكل Show all

MD5 : f432922812d4bad5d80f5b15315d9cf2

وهذه الخوارزميات التي نتكلم عنها وقيم



Virustotal is a **service that analyzes suspicious files and URLs** and facilitates the quick detection of viruses, worms, trojans, and all kinds of malware detected by antivirus engines. [More information...](#)

0 VT Community user(s) with a total of 0 reputation credit(s) say(s) this sample is goodware. 0 VT Community user(s) with a total of 0 reputation credit(s) say(s) this sample is malware.

VT Community



not reviewed
Safety score: -

File name: **BRService.exe** اسم الملف
Submission date: **2010-08-26 01:52:36 (UTC)** تاريخ الفحص
Current status: **finished** انتهت العملية
Result: **0/42 (0.0%) مضاد** النتيجة الملف سليم وتم فحصه بـ ٤٢ مضاد

Compact

Print results

Antivirus	Version	Last Update	Result
AhnLab-V3	2010.08.26.00	2010.08.25	-
AntiVir	8.2.4.38	2010.08.25	-
Antiy-AVL	2.0.3.7	2010.08.23	-
Authentium	5.2.0.5	2010.08.26	-
Avast	4.8.1351.0	2010.08.25	-
Avast5	5.0.594.0	2010.08.25	-
AVG	9.0.0.851	2010.08.25	-
BitDefender	7.2	2010.08.26	-
CAT-QuickHeal	11.00	2010.08.24	-
ClamAV	0.96.2.0-git	2010.08.26	-

وكذلك يمكننا الفحص عبر محرك البحث Google

ودلك على الشكل التالي

بعد الدخول على محرك
البحث
نضع القيمة هنا

Google
France



59DC5BB82E4C8E0B3EADCFDBC44BA6E4

Recherche avancée
Outils linguistiques

Recherche Google

J'ai de la chance

aire de Google ma page d'accueil

ثم نضغط على

Programmes de publicité

Propos de Google

Google.com in English

© 2010 - Confidentialité

اخواني هذا العمل دائما نقوم به في الخاصية

Extra stuff

بمجرد تحديد الأسطر في هذه الخاصية مباشرة يتم تحديدها حتى في الخاصية Malware hunting

1 Extra stuff

3

Temara_M2

Path / Info

Extra stuff خاصية هي التي سنشتغل عليها ثم نقوم بفلتر لتقرير لتظهر لنا فقط الأسطر المشكوك فيها كما هو موضح



Temara_M2

2.0.0.50

08/09/2010 00:43:43

Administrator

Windows 7 Ultimate

7600

Arabe (Maroc)

181

C:\Windows

%SystemRoot%\System32\drivers\etc

0

هذا هو الجزء الأول من التقرير و توجد به معلومات حول الجهاز

re de sessions Windows	C:\Windows\System32\lsass.exe	Microsoft Corpora...	Microsoft Windows : Microsof...	[Close]
d'exécution client-serveur		Microsoft Corpora...	Microsoft Windows : Microsof...	[Close]
de démarrage de Windows		Microsoft Corpora...	Microsoft Windows : Microsof...	[Close]
d'exécution client-serveur		Microsoft Corpora...	Microsoft Windows : Microsof...	[Close]
s Services et Contrôleur		Microsoft Corpora...	Microsoft Windows : Microsof...	[Close]
ity Authority Process		Microsoft Corpora...	Microsoft Windows : Microsof...	[Close]
gestionnaire de session locale		Microsoft Corpora...	Microsoft Windows : Microsof...	[Close]
d'ouverture de session Windows	C:\Windows\System32\lsass.exe	Microsoft Corpora...	Microsoft Windows : Microsof...	[Close]

الجزء الثاني من التقرير وهو خاص بالبروسيسات ويجب فحصها

كيفية حذف الأسطر الضارة التي وجدنا بتقرير

Software startup analyzer

1 Extra stuff

3

Temara_M2

Path / Info

Extra stuff

خاصية هي التي سنشتغل عليها

ثم

نقوم بفلتر لتقرير لتظهر لنا فقط الأسطر

المشكوك فيها

كما هو موضح



Temara_M2

2.0.0.50
08/09/2010 00:43:43
Administrator
Windows 7 Ultimate
7600

Arabe (Maroc)

181

C:\Windows

%SystemRoot%\System32\drivers\etc

0

هذا هو الجزء الأول من

التقرير

و توجد به معلومات حول

الجهاز

الجزء الثاني من التقرير
وهو خاص بالبروسيسات
ويجب فحصها

re de sessions Windows	C:\Windows\System32\lsass.exe	Microsoft Corpora...	Microsoft Windows : Microsof...	...
d'exécution client-serveur		Microsoft Corpora...	Microsoft Windows : Microsof...	...
de démarrage de Windows		Microsoft Corpora...	Microsoft Windows : Microsof...	...
d'exécution client-serveur		Microsoft Corpora...	Microsoft Windows : Microsof...	...
s Services et Contrôleur		Microsoft Corpora...	Microsoft Windows : Microsof...	...
ity Authority Process		Microsoft Corpora...	Microsoft Windows : Microsof...	...
gestionnaire de session locale		Microsoft Corpora...	Microsoft Windows : Microsof...	...
d'ouverture de session Windows	C:\Windows\System32\lsass.exe	Microsoft Corpora...	Microsoft Windows : Microsof...	...

Software startup analyzer

Extra stuff

Scan computer Open Run file Save log file Online analysis

Save Run file

Process killer Installed software Host file editor History / backups

Temara M2 Filter

Description	Path / Info	Company	Signer / Issuer
withoutlogon	1		
withoutlogon	1		
RegistryTools	0		
ContextMenuHandlers			
Extension for Malware scanning	C:\Program Files\Avira\AntiVir Desktop\avguard.exe	Avira GmbH	
Extension	GUID / CLSID not found		
	C:\Program Files\Avira\AntiVir Desktop\avguard.exe		
C:\Microsoft\Windows NT\CurrentVersion\Winlogon\Shell32,Control_RunDLL "sysdm.cpl"	rundll32 sysdm.cpl, /s		
SSES_ROOT batfile	"%1" %*		
SSES_ROOT cmdfile	"%1" %*		
SSES_ROOT comfile	"%1" %*		
SSES_ROOT exefile	"%1" %*		
SSES_ROOT htfile	C:\WINDOWS\system32\cmd.exe		
SSES_ROOT piffile	"%1" %*		
SSES_ROOT scrfile	"%1" /S		
classes*\ShellEx\ContextMenuHandlers			
Extension for Malware scanning	C:\Program Files\Avira\AntiVir PersonalEdition\avguard.exe	Avira GmbH	
Extension	GUID / CLSID not found		
	C:\Program Files\WinRAR\rrarext.dll		
classes\Folder\ShellEx\ContextMenuHandlers			

www.starttimes.com

الآن نقوم بتحديد الأسطر المراد حذفها
 وذلك بالضغط دويل كليك على السطر
 أو نضغط فراغ من لوحة Espace
 المفاتيح

نتأكد من الأسطر التي أردنا حذفها وذلك

eware startup analyzer

hunting Extra stuff Scan computer Open Run file Save Run file Save log file Online analysis

Item fixer Loaded modules

d files can cause damage to your operating system.

Item	Path / Info	Company	Signer / Issuer
	C:\DOCUME~1\ADMINI~1\POS\LOCALS~1\...		File not found
on	GUID / CLSID not found		
on	GUID / CLSID not found		

الآن نقوم بالضغط على
Fix selected item
لكي يتم الحذف

نضغط OK

Fix selected items

Warning!

RunScanner is an advanced tool, and requires advanced Windows and operating systems in general. If you delete something without knowing what it is, it can lead to major problems such as Windows no longer working or problems with running Windows itself.

Are you sure you want to fix all selected items?

OK Cancel

ثم OK لتأكيد



الآن مع

شرح لكيفية استرجاع الأسطر التي تم حذفها بالخطأ

A screenshot of the "malware startup analyzer" software interface. The interface includes a toolbar with buttons for "Extra stuff", "Scan computer", "Open Run file", "Save Run file", "Save log file", "Online analysis", and "Help". Below the toolbar is a list of registry keys that have been deleted, such as "DK011 Deleted registry key HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\catchme". A red cloud-shaped callout box contains four numbered steps: 1- اضغط على Extra stuff, 2- ثم من History/backups, 3- نختار السطر الذي نريد استرجاعه, 4- نضغط على Restore to original setting. Red arrows point from the callout box to the corresponding buttons and registry entries in the software interface.

ثم نضغط على

Yes

لتأكيد



العملية تمت بنجاح



أخواني أعتقد يجب علينا الوقوف هنا
حتى لا نبتعد كثيرا على الأعضاء اللذين لم يحضروا الدرس
+المحور القادم فهو يريد التركيز
لأنه سنقوم فيه بمقارنة أسطر hijackthis مع أسطر Runscanner
وكيفية معرفة بعض الأسطر التي تظهر بشكل واضح على هيجاكديس
وبشكل معقد على Runscanner

فقط لدي إضافة أو تعقيب اعتقد ان اكبر شيء يجب على اداة ال **RUNSCANNER** تجاوزه هي قضية **MD5** فيفضل ان نجد النتيجة مباشرة من احد المواقع دون المرور على الفيروس تونال او غوغل لانو الموقع المستعمل حاليا يحتاج للتسجيل به اي لا اهمية له سوى معرفة **MD5** للملفات وهذه العملية يمكن ان تقوم بها الاداة بدون مواقع مثل ما تقوم به اداة الهيجاك...

نعم أخي فكرة جيدة

بنسبة للأمتداد مثلا هذه الأسطر الملونة بالأصفر فهي لا تحتاج الى فحص

فهي مباشرة للحذف

<input type="checkbox"/>	120	NameServer {02AA66E9-5F94-4404-8205-189862D84973}	192.168.50.58 192.168.60.55
<input type="checkbox"/>	160	DisableTaskMgr	1
<input type="checkbox"/>	160	DisableRegistryTools	1
<input type="checkbox"/>	170	{3580a4f7-a5a2-11df-b735-806d6172696f}	D:\lahlrx.exe
<input type="checkbox"/>	170	{3580a4f8-a5a2-11df-b735-806d6172696f}	E:\qlji.exe
<input type="checkbox"/>	170	{3580a4fa-a5a2-11df-b735-806d6172696f}	C:\eupfjw.exe
<input type="checkbox"/>	170	{a33e2bd1-a595-11df-a12b-f9371f4aec27}	G:\Setup.exe

جيد اخواني الآن بعد فتح الأداة وعمل تقرير

سنضغط على Extra stuff

وبتالي سنواجه أولا فقرة وهي المثلثة في هذه الصورة

والتي تعطينا معلومات على الجهاز

Path / Info	Company	Signer
Temara_M2		
2.0.0.50		
05/10/2010 17:11:47		
Administrator		
Microsoft Windows XP		
2600		
Service Pack 3		
Arabe (Maroc)		
8.0.6001.18702		
C:\WINDOWS		
%SystemRoot%\System32\drivers\etc		
0		



الآن سنتعرف من خلال Runscanner كيفية معرفة وجود الهوست بالجهاز

أي أسطر 01 التي نجدها في hijackthis

مثل هذه الأسطر

O1 - Hosts: 74.125.45.100 target=_new>www secure-plus-paymenom

O1 - Hosts: 74.125.45.100 target=_new>www getavplusnow com

O1 - Hosts: 74.125.45.100 safebrowsing-cache.google.com

O1 - Hosts: 74.125.45.100 urs.microsoft.com

Runscanner أداة بخصوص

الأمر سهل والصورة تبين ذلك

yzzer

stuff

Scan computer

Open Run file

Save Run file

Save log file

Online analysis

Helper forums

Update check

Installed software

Host file editor

History / backups

Temara_M2

Filter

Path / Info

Company

Signer / Issuer

Temara_M2
2.0.0.50
11/09/2010 07:21:27 PM
Administrator
Microsoft Windows XP
2600
Service Pack 2

181
C:\WINDOWS
%SystemRoot%\System32\drivers\etc

55

C:\WINDOWS\system32\smss.exe Microsoft Corpora... Microsoft Windows Publisher
C:\WINDOWS\system32\csrss.exe Microsoft Corpora... Microsoft Windows Publisher
C:\WINDOWS\system32\winlogon.exe Microsoft Corpora... Microsoft Windows Publisher
C:\WINDOWS\system32\services.exe Microsoft Corpora... Microsoft Windows Publisher
C:\WINDOWS\system32\lsass.exe Microsoft Corpora... Microsoft Windows Publisher
rvice C:\WINDOWS\system32\svchost.exe Microsoft Corpora... Microsoft Windows Publisher
rvice C:\WINDOWS\system32\svchost.exe Microsoft Corpora... Microsoft Windows Publisher
rvice C:\WINDOWS\system32\svchost.exe Microsoft Corpora... Microsoft Windows Publisher

منتدى التوعية الحياتية

www.startupmea.com

الجميل هو ان الأداة يمكنها ان تتخلص من الهوست

الصور توضح كيفية التخلص منه



لكي نقضي على
o default



الأداة تأكد اصلاح
اللون الأصفر

ervers\etc
: names.
em to "wrong" IP addresses.
127.0.0.1 localhost"

%SystemRoot%\System32\drivers\etc
0

نعود الى الهوست سنجد ان القيمة أصبحت 0 وهذا يدل على انه تم اصلاحه

تفضل أخي لتتعرف على الهوست أكثر

★ درس حول التعديلات على HOSTS © تعديل على

الفقرة الثانية وهي خاصة ب

البروسيسات الشغالة بالجهاز وهي الأخرى يجب فحصها جيداً

Malware startup analyzer

Process killer | Installed software | Host file editor | History / backups

Reboot computer | Start "explorer.exe"

Path	Domain\Username	Description	Version	CompanyName
C:\WINDOWS\system32\csrss.exe	AUTORITE NT\SYSTEM	Client Server Runti...	5.1.2600.218...	Microsoft Corporation
C:\WINDOWS\system32\ctfmon...	KHALID\Administrateur	CTF Loa...	5.1.2600.218...	Microsoft Corporation
C:\WINDOWS\explorer.exe	KHALID\Administrateur		5.2900.21...	Microsoft Corporation
C:\Program Files\Windows Live\F...	AUTORITE NT\SYSTEM		118.0427	Microsoft Corporation
C:\Program Files\Internet Explor...	KHALID\...		1.18...	Microsoft Corporation
C:\Program Files\Internet Explor...	KHALID\...		1.18...	Microsoft Corporation
C:\Program Files\Internet Explor...	KHALID\...		01.18...	Microsoft Corporation
C:\WINDOWS\system32\lsass.exe	AUTORITE NT\SYSTEM		5.1.2600.218...	Microsoft Corporation
C:\Program Files\Bonjour\mDNSR...	AUTORITE NT\SYSTEM		2.0.2.0	Apple Inc.
C:\Program Files\Windows Live\M...	KHALID\Administrateur	Windows Live mes...	14.0.8117.0416	Microsoft Corporation
C:\Program Files\Fichiers commu...	KHALID\Administrateur	RealNetworks Sch...	0.1.1.790	RealNetworks, Inc.
C:\Program Files\Avira\AntiVir Pe...	AUTORITE NT\SYSTEM	Antivirus Scheduler	8.00.00.17	Avira GmbH
C:\WINDOWS\system32\services...	AUTORITE NT\SYSTEM	Applications Servic...	5.1.2600.352...	Microsoft Corporation
C:\WINDOWS\system32\smss.exe	AUTORITE NT\SYSTEM	Gestionnaire de se...	5.1.2600.218...	Microsoft Corporation
C:\WINDOWS\system32\spoolsv...	AUTORITE NT\SYSTEM	Spooler SubSyste...	5.1.2600.218...	Microsoft Corporation
C:\WINDOWS\system32\svchost...	AUTORITE NT\SYSTEM	Generic Host Proce...	5.1.2600.218...	Microsoft Corporation
C:\WINDOWS\system32\svchost...	AUTORITE NT\SYSTEM	Generic Host Proce...	5.1.2600.218...	Microsoft Corporation
C:\WINDOWS\system32\svchost...	AUTORITE NT\SYSTEM	Generic Host Proce...	5.1.2600.218...	Microsoft Corporation
C:\WINDOWS\system32\svchost...	AUTORITE NT\SYSTEM	Generic Host Proce...	5.1.2600.218...	Microsoft Corporation
C:\WINDOWS\system32\svchost...	AUTORITE NT\SYSTEM	Generic Host Proce...	5.1.2600.218...	Microsoft Corporation
C:\WINDOWS\system32\svchost...	AUTORITE NT\SYSTEM	Generic Host Proce...	5.1.2600.218...	Microsoft Corporation
C:\WINDOWS\system32\svchost...	AUTORITE NT\SYSTEM	Generic Host Proce...	5.1.2600.218...	Microsoft Corporation
C:\WINDOWS\system32\svchost...	AUTORITE NT\SYSTEM	Generic Host Proce...	5.1.2600.218...	Microsoft Corporation
C:\WINDOWS\system32\wdfmgr...	AUTORITE NT\SYSTEM	Windows User Mod...	5.2.3790.123...	Microsoft Corporation

نقوم بتحديد البروسيس المراد حذفه ثم نضغط على kill selected

www.startimes.com

المرحلة التي تأتي بعد البروسيسات الشغالة

وهي البرامج التي تقلع مع تشغيل الوندوز

بنسبة للأسطر التي تقلع مع تشغيل الوندوز في هيجاك ديس تأخذ الرقم 04

لكن في runscanner الأمر مختلف وتوجد عدة طرق لمعرفة

أولا بنسبة للخاصية Malware hunting تبدأ أرقام الاسطر التي تقلع مع بدأ تشغيل الوندوز من

002

مثلا في هذه النسخة تبدأ من 002 الى 008 لكن هذا قد يختلف

فهذه الصورة يتبين لنا أن الأسطر التي تعلق مع الجهاز هي 002 و 003 و 004

Entry description	Path / Info	Company	Signer / Issuer
002 Adobe Reader Speed Launcher	C:\Program Files\Adobe\Reader 9.0\Rea...	Adobe Systems Inco...	
003 Z810PNP	C:\Program Files\Modem Samsung SCH-U...		
003 Z810SysStart	C:\Program Files\Modem Samsung SCH-U...		
003 AdobeUpdater	C:\Program Files\Fichiers communs\Adob...	Adobe Systems Inco...	
004 Notification de cadeaux MSN	C:\Documents and Settings\morad\Appl...	Microsoft Corporation	

لكن أنا أنصح بأن الطريقة الجيدة في معرفة الأسطر التي تعلق مع تشغيل الوندوز هي موجودة في
خاصية Extra Stuff

لأنها تعطينا جميع البرامج والملفات التي تبدأ مع تشغيل الوندوز وسهل معرفتها

الصورة توضح سهولة هذه الخاصية فقط يمكن معرفتها من خلال كلمة Run أو Démarrage
وبتالي نتجاهل الأرقام

Entry description	Path / Info	Company	Signer / Issuer
002 HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Run (+subkeys)			
igfxtray	C:\WINDOWS\system32\igfxtray.exe		
igfxhkcmd	C:\WINDOWS\system32\hkcmd		
igfxpers	C:\WINDOWS\system32\igfxp...		
IMJPMIG8.1	C:\WINDOWS\IME\imjp8_1\I...		
MSPY2002	C:\WINDOWS\system32\IME\...		
PHIME2002ASync	C:\WINDOWS\system32\IME\...		
PHIME2002A	C:\WINDOWS\system32\IME\...		
003 HKCU\SOFTWARE\Microsoft\Windows\CurrentVersion\Run (+subkeys)			
CTFMON.EXE	C:\WINDOWS\system32\ctfmo...		
IDMan	C:\Program Files\Internet Downl...		
msnmsgr	C:\Program Files\Windows Live\Messenger\...		
008 Default user \Software\Microsoft\Windows\CurrentVersion\Run (+subkeys)			
CTFMON.EXE	C:\WINDOWS\system32\CTFMON.EXE	Micro...	Windows Compone...

عندما نجد كلمة
Run
أو
Démarrage
فهذا يعني ان البرامج الموجودة تعلق مع تشغيل
الوندوز

بنسبة لبرامج التي تعلق مع تشغيل الوندوز
دائما نتجنب أسطر الويفي وبرنامج الحماية وجدار الناري
وأسطر موديم واللغة وأسطر النت وكذلك نترك البرامج التي نريدها ان تعلق
مع تشغيل الجهاز
أما الاسطر التي نراها ملونة بالأحمر فهي مباشرة للحذف

هذا مثال للفيروس kubernesis.vbe

ونلاحظ بأن الاداة قامت بتوضيحه باللون الأحمر وهذه ميزة جيدة للأداة

Entry description	Path / Info	Company	Signer / Issuer
(+subkeys)			
C:\Program Files\Winamp\winampa.exe		Nullsoft	
C:\Documents and Settings\All Users\Menu Démarrer\Programme...			File not found
C:\WINDOWS\kubernesis.dll.vbe			File not found
C:\Program Files\VIA\VIAudio\SBADeck\ADeck.exe		VIA Technologies, Inc.	
(+subkeys)			
C:\Program Files\Software Informer\softinfo.exe			File not found
C:\Program Files\BlazeVideo\BlazeDVD4 Professional\MediaDetec...		BlazeVideo Company	

أخواني ادا كان كل شئى واضح
سننتقل الى توضيح بعض أسطر hijackthis
على أداة Runscanner
لأننى سبق وقرأة فى أحد النقاشات بالمنتدى
أن runscanner لا تحتوي على ما يوجد ب hijackthis
أي من خلال بعض الأسطر في hijackthis
نعرف أنا الجهاز مصاب
سأقول نعم حتى أداة runscanner تكتشف جميع أسطر hijackthis
فقط يجب البحث جيدا
وسأضع بعض الأمثلة

سنبدأ بأسطر R0 و R1

هذه الأسطر خاصة ب hijackthis

R1 - HKCU\Software\Microsoft\Internet Explorer\Main,Search Page =
<http://www.google.fr/>
R0 - HKCU\Software\Microsoft\Internet Explorer\Main,Start Page =
<http://go.microsoft.com/fwlink/?LinkId=69157>
R1 - HKLM\Software\Microsoft\Internet Explorer\Main,Default_Page_URL =
<http://go.microsoft.com/fwlink/?LinkId=69157>
R1 - HKLM\Software\Microsoft\Internet Explorer\Main,Default_Search_URL
= <http://go.microsoft.com/fwlink/?LinkId=54896>
R1 - HKLM\Software\Microsoft\Internet Explorer\Main,Search Page =
<http://go.microsoft.com/fwlink/?LinkId=54896>
R0 - HKLM\Software\Microsoft\Internet Explorer\Main,Start Page =
<http://go.microsoft.com/fwlink/?LinkId=69157>

وعلى أداة runscanner نجدها على هذا الشكل دائما نتبع المسار

<http://www.google.ma/>
<http://go.microsoft.com/fwlink/?LinkId=69157>
<http://www.microsoft.com/isapi/redir.dll?prd=ie&ar=iesearch>
<http://go.microsoft.com/fwlink/?LinkId=54896>
<http://go.microsoft.com/fwlink/?LinkId=69157>
<http://go.microsoft.com/fwlink/?LinkId=69157>
<http://go.microsoft.com/fwlink/?LinkId=54896>
http://ie.search.msn.com/{SUB_RFC1766}/srchasst/srchasst.htm
http://ie.search.msn.com/{SUB_RFC1766}/srchasst/srchcust.htm



أما بخصوص أسطر 01 أي المتعلقة بالهوست لقد سبق وتطرقتنا إليها

الآن سنري أسطر 07 في hijackthis وكيف تظهر على runscanner

عندما نجد العدد 1 فهذا يعنى أن Task manger مصاب أو بالفرنسية gestionnaire des taches

are\Microsoft\Windows\CurrentVersion\Policies\System	
oleTaskMgr	1
oleRegistryTools	1



أما

أسطر 06 في hijackthis

تظهر على هذا الشكل في runscanner

ft\Internet Explorer	
	1
	1



بنسبة لبرامج التي تقلع مع تشغيل الوندوز
دائما نتجنب أسطر الويفي وبرنامج الحماية وجدار الناري

وأسطر موديم واللغة وأسطر النت وكذلك نترك البرامج التي نريدها ان تقلع
مع تشغيل الجهاز
أما الاسطر التي نراها ملونة بالأحمر فهي مباشرة للحذف

بخصوص هذه الأسطر اعتمد على

systemlookup.com

لقد قمت بشرحه بالدرس 2

بخصوص هذه الاسطر عندما نجد القيمة 1 نقوم بحذفها

urrentVersion\Policies\System	
	1
	1



أما

عندما نجدها بتقريرنا مباشر للحذف

ft\Internet Explorer	
	1
	1



اخي لم تفهم قصدي جدا ومازلت تقول ان سطر الاحمر دائما للحذف سأقوم بتجربة على جهازي بحذف
ملف explorer.exe موجود في مجلد نظام windows وساقوم

بوضع تقرير

يعني هذا ما جري من تغيرات عند حذف ملف **explorer.exe** من نظام لنفترض اننا حذفنا هذا سطر من روجيستري وارادنا ان نحل مشكلة بنسخ ملف احتاطي للملف

explorer.exe ونسخناه في مجلد نظام مع العلم اننا حذفنا هذا السطر من روجيستري فهل سيشتغل ملف **explorer.exe** مرة اخي مع اشتغال النظام!؟

أسطر **hijackthis** التي سبق وتوضيحتها في الدرس السابق وهي

01 , R0 , R1 , 07 , 06 ,

والآن مع أسطر 08

هذه أمثلة لأسطر 08 في **hijackthis** أما على **runscanner** نجدها

في الخاصيتين أي **Malware hunting** و **Extra stuff**

هذه الصور على الخاصية **Malware hunting**

```
res://C:\PROGRA~1\MICROS~2\Office12\EXCEL.EXE/3000
res://C:\Program Files\Google\Google Toolbar\Component\Go...
C:\Program Files\Internet Download Manager\IEExt.htm
C:\Program Files\Internet Download Manager\IEGetVL.htm
C:\Program Files\Internet Download Manager\IEGetAll.htm
```



وهذه على الخاصية **Extra stuff**

```
res://C:\PROGRA~1\MICROS~2\Office12\EXCEL.EXE/3000
res://C:\Program Files\Google\Google Toolbar\Component\Googl...
C:\Program Files\Internet Download Manager\IEExt.htm
C:\Program Files\Internet Download Manager\IEGetVL.htm
C:\Program Files\Internet Download Manager\IEGetAll.htm
```



بنسبة لهذه الأسطر يجب فحصها

أو النظر فيها اذا عرفنا البرامج التي تعود فلا بأس بتركها وادا لم نعرف ذلك يجب فحصها

أسطر 10 على hijckathis أما على Runscanner نجدها على هذا الشكل

trolSet\Services\WinSock2\Parameters\NameSpace_Catalog5		www.startimes.com
{system32\nlasvc.dll,-1000	C:\Windows\system32\NLAapi.dll	
{system32\wshtcpip.dll,-60103	C:\Windows\System32\mswsock.dll	
	C:\Windows\System32\winrnr.dll	
{system32\napinsp.dll,-1000	C:\Windows\system32\napinsp.dll	
{system32\pnrpnp.dll,-1000	C:\Windows\system32\pnrpnp.dll	
{system32\pnrpnp.dll,-1001	C:\Windows\system32\pnrpnp.dll	
	C:\Program Files\Common Files\Microsoft Shared\Windows Live\WLIDNSP.DLL	
NSP	C:\Program Files\Common Files\Microsoft Shared\Windows Live\WLIDNSP.DLL	

الأسطر المهمة التي لا يجب حذفها هي التي تنتهي ب

mswsock.dd

winrnr.dl

pnrpnp.dll

وهنا يجب حذف السطرين الأخيرين وهما

WLIDNSP.DLL

وكذلك يمكن الاعتماد على هذا الموضوع في اصلاح هذا الخلل والذي يتعلق بالاتصال

<http://www.startimes.com/f.aspx?t=25076006>

أسطر 015 في hijackthis نجدها على الشكل التالي بنسبة ل Runscanner

هذه بنسبة للخاصية Malware hunting

<http://www.flvdirect.com>

<http://www.flvdirect.com>



وهذه لخاصية Extra stuff

http://www.flvdirect.com

http://www.flvdirect.com



أسطر 016 في hijackthis

أما على Runscanner نجدها في خاصية Extra Stuff هذه الخاصة نجد فيها كل شيئ وهذا جيد

الصورة توضح ذلك

Path / Info	Compar
C:\windows\system32\OGACheckContr...	
C:\windows\system32\LegitCheckContr... Microsoft	
C:\Program Files\ma-config.com\MCATL... Cybel50	
C:\windows\system32\Macromed\Fash... Adobe S	

يجب أولاً ان نقوم بوضع الفأرة هنا اي قر ونقوم بتحريكها الى الأمام لكي يظهر المس كما هو موضح هنا
هذه الاسطر مثل أسطر 016 في his

هذا مثال لسطر 017 الموجد في hijackthis

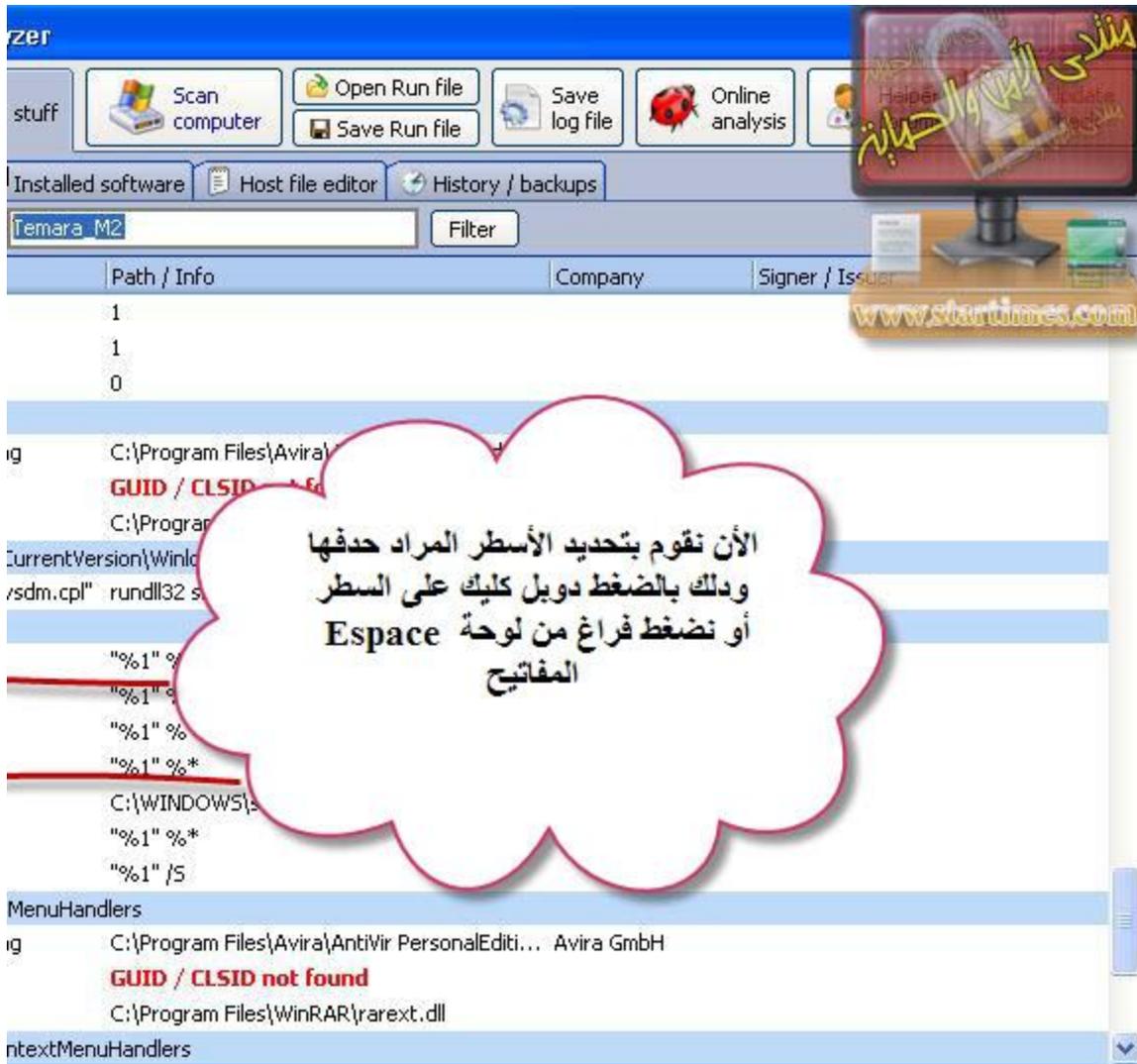
في هيجاك ديس يكون على هذا الشكل

O17 - HKLM\System\CCS\Services\Tcpip\..\{02AA66E9-5F94-4404-8205-189862D84973}: NameServer = 192.168.50.58 192.168.60.55

أما في Runscanner هو السطر الملون بالأخضر

<input type="checkbox"/>	120	NameServer {02AA66E9-5F94-4404-8205-189862D84973}	192.168.50.58 192.168.60.55
<input type="checkbox"/>	160	DisableTaskMgr	1
<input type="checkbox"/>	160	DisableRegistryTools	1
<input type="checkbox"/>	170	{3580a4f7-a5a2-11df-b735-806d6172696f}	D:\lahlrx.exe
<input type="checkbox"/>	170	{3580a4f8-a5a2-11df-b735-806d6172696f}	E:\qlji.exe
<input type="checkbox"/>	170	{3580a4fa-a5a2-11df-b735-806d6172696f}	C:\eupfjw.exe
<input type="checkbox"/>	170	{a33e2bd1-a595-11df-a12b-f9371f4aec27}	G:\Setup.exe

كيفية حذف الأسطر بعد تحديدها



1

ثم نضغط على Malware hunting

ثم

item fixer

ثم

eware startup analyzer

hunting Extra stuff Scan computer Open Run file Save Run file Save log file Online analysis

Item fixer Loaded modules

Files can cause damage to your operating system.

Item	Path / Info	Company	Signer / Issuer
	C:\DOCUME~1\ADMINI~1\POS\LOCALS~1\...		File not found
	GUID / CLSID not found		
	GUID / CLSID not found		

الآن نقوم بالضغط على
Fix selected item
لكي يتم الحذف

نضغط Ok

Fix selected items

Warning!

RunScanner is an advanced tool, and requires advanced Windows and operating systems in general. If you delete something not knowing what it is, it can lead to major problems such as Windows no longer working or problems with running Windows itself.

Are you sure you want to fix all selected items?

OK Cancel

ثم Ok لتأكيد



ليست للحذف فقط ولحد الآن يوجد فيروس واحد يتضح من خلال هذه الأسطر وهو للحذف

وهو

NameServer = 85.255.115.2,85.255.112.7

عندما نجد مثل هذه الأرقام المهم ان تكون تبدأ ب 85.225

فهذا مباشرة للحذف

كيفية فحص تقرير وتحديد أسطره

ادا أرسله لنا أحد الأعضاء

والتقرير الذي نعتد عليه يجب ان يكون بصيغة **run** وليس **log**

نتابع الشرح بالصور



هذا هو التقرير الذي سنعتد عليه
في حذف الأسطر وهو بصيغة **run**

Software startup analyzer

hunting Extra stuff Scan computer Open Run file Save Run file Save log file Online analysis

Item fixer Loaded modules

Temara_M2 Filter

Items listed in this screen are not in our whitelist or the file doesn't exist. This indicates that the file is malware or unwanted. Deleting a valid file can cause damage to your operating system. www.startimes.com

Item Name	Path / Info	Company	Signer / Issuer
Taskbar Control	C:\Program Files\IVT Corporation\BlueSol...	Proland Software	PROLAND SOFTWARES PRIVA...
InstaUpdate	...	Proland Software	PROLAND SOFTWARES PRIVA...
...	...	LG Electronics	LG Electronics : VeriSign Time ...
...	...	Proland Software Pvt Ltd.	Proland Softwares Private Limi...
...	...	Proland Software	PROLAND SOFTWARES PRIVA...
64/x86 Hybrid Driver	...	Protect Software GmbH	Protect Software GmbH : Veri...
...	C:\Program Files\A...rojan Elite\ATEPM...		File not found
Network Filter Driver	C:\Program Files\IVT Corporation\BlueSol...	IVT Corporation.	IVT SOFTWARE TECHNOLOGY...
...	C:\Users\YassinE\AppData\Local\Temp\c...		File not found
h Definition Audio Function ...	C:\Windows\system32\drivers\RTKVHDA....	Realtek Semiconductor ...	
s Antivirus for Windows Ker...	C:\Protector Plus\PPDrv.sys	Proland Software	PROLAND SOFTWARES PRIVA...
s Antivirus Email Scan Driver	C:\Protector Plus\PEMSCAN.sys	Proland Software	PROLAND SOFTWARES PRIVA...
FC8B962-9B40-4DFF-9458...	C:\Windows\system32\skype4com.dll	Skype Technologies	Skype Technologies SA : VeriSi...
neNote {2670000A-7350-4f...	GUID / CLSID not found		

هذه هي واجهة التقرير
عندما نضغط دويل كليك على التقرير
مباشرة تظهر لنا هذه الواجهة



Software startup analyzer

1 Extra stuff

3

Temara_M2

Path / Info

Extra stuff

خاصية هي التي سنشتغل عليها

ثم

نقوم بفلتر لتقرير لتظهر لنا فقط الأسطر
المشكوك فيها
كما هو موضح



Temara_M2

2.0.0.50
08/09/2010 00:43:43
Administrator
Windows 7 Ultimate
7600

Arabe (Maroc)

181

C:\Windows

%SystemRoot%\System32\drivers\etc

0

هذا هو الجزء الأول من

التقرير

و توجد به معلومات حول
الجهاز

الجزء الثاني من التقرير
وهو خاص بالبروسيسات
ويجب فحصها

re de sessions Windows	C:\Windows\System32\lsass.exe	Microsoft Corpora...	Microsoft Windows : Microsof...	...
d'exécution client-serveur		Microsoft Corpora...	Microsoft Windows : Microsof...	...
de démarrage de Windows		Microsoft Corpora...	Microsoft Windows : Microsof...	...
d'exécution client-serveur		Microsoft Corpora...	Microsoft Windows : Microsof...	...
s Services et Contrôleur		Microsoft Corpora...	Microsoft Windows : Microsof...	...
ity Authority Process		Microsoft Corpora...	Microsoft Windows : Microsof...	...
gestionnaire de session locale		Microsoft Corpora...	Microsoft Windows : Microsof...	...
d'ouverture de session Windows	C:\Windows\System32\lsass.exe	Microsoft Corpora...	Microsoft Windows : Microsof...	...

Software startup analyzer

Extra stuff

Scan computer | Open Run file | Save log file | Online analysis

Save Run file

Process killer | Installed software | Host file editor | History / backups

Temara_M2 | Filter

Description	Path / Info	Company	Signer / Issuer
MS Module	C:\Program Files\IVT Corporation\BlueSoleil...		
MS Module	C:\Program Files\IVT Corporation\BlueSoleil...		
MS Module	C:\Program Files\IVT Corporation\BlueSoleil...		
System Tray	C:\Program Files\IVT Corporation\BlueSoleil...		
Task Manager	C:\Program Files\IVT Corporation\BlueSoleil...		
Taskbar.exe	C:\Program Files\IVT Corporation\BlueSoleil...		
Taskbar\Microsoft\Windows\...	C:\Program Files\IVT Corporation\BlueSoleil...		
Taskbar\AppData\Roaming\...	C:\Program Files\IVT Corporation\BlueSoleil...		
Taskbar\AppData\Roaming\...	C:\Program Files\IVT Corporation\BlueSoleil...		
Taskbar\CurrentControlSet\Services (Services)	C:\Program Files\IVT Corporation\BlueSoleil...		
Taskbar\MS Module	C:\Program Files\IVT Corporation\BlueSoleil...		
Taskbar\MS Module	C:\Program Files\IVT Corporation\BlueSoleil...		
Taskbar\CurrentControlSet\Services (drivers)	C:\Program Files\IVT Corporation\BlueSoleil...		
Taskbar\...	C:\Program Files\AIDA32 - Personal System...		
Taskbar\...	C:\Program Files\Anti Trojan Elite\ATEPMon...		File not found
Taskbar\...	C:\Users\YassinE\AppData\Local\Temp\cat...		File not found
Taskbar\High Definition Audio Function D...	C:\Windows\system32\drivers\RTKVHDA.sys	Realtek Semicond...	
Taskbar\Microsoft\Internet Explorer\Extensions			

- Lookup at Google (Ctrl+G)
- Lookup at Systemlookup.com (Ctrl+L)
- Lookup at RunScanner.net (Ctrl+I)
- Lookup MD5 at FileAdvisor (Ctrl+F)
- Copy to clipboard (Ctrl+C)
- Expand tree
- Collapse tree

نقوم بضغط يمين الفأرة
على السطر المراد فحصه
ونختار أحد مواقع الفحص
أنا اخترت محرك البحث google
ثم
نفحص جميع الأسطر بهذه الطريقة



Software startup analyzer

Extra stuff

Scan computer Open Run file Save Run file Save log file Online analysis

Process killer Installed software Host file editor History / backups

Temara M2 Filter

Description	Path / Info	Company	Signer / Issuer
withoutlogon	1		
withoutlogon	1		
RegistryTools	0		
ContextMenuHandlers			
Extension for Malware scanning	C:\Program Files\Avira\AntiVir Desktop\avguard.exe	Avira GmbH	
Extension	GUID / CLSID not found		
	C:\Program Files\Avira\AntiVir Desktop\avguard.exe		
C:\Microsoft\Windows NT\CurrentVersion\Winlogon\Shell32,Control_RunDLL "sysdm.cpl"	rundll32 sysdm.cpl,Control_RunDLL "sysdm.cpl"		
SSES_ROOT batfile	"%1" %*		
SSES_ROOT cmdfile	"%1" %*		
SSES_ROOT comfile	"%1" %*		
SSES_ROOT exefile	"%1" %*		
SSES_ROOT htfile	C:\WINDOWS\system32\cmd.exe		
SSES_ROOT piffile	"%1" %*		
SSES_ROOT scrfile	"%1" /S		
Classes*\ShellEx\ContextMenuHandlers			
Extension for Malware scanning	C:\Program Files\Avira\AntiVir PersonalEdition\avguard.exe	Avira GmbH	
Extension	GUID / CLSID not found		
	C:\Program Files\WinRAR\rrarext.dll		
Classes\Folder\ShellEx\ContextMenuHandlers			



الآن نقوم بتحديد الأسطر المراد حذفها
 وذلك بالضغط دويل كليك على السطر
 أو نضغط فراغ من لوحة Espace
 المفاتيح

Malware startup analyzer

1 Malware hunting

2 Item fixer

3 Save Run file

Extra stuff

Scan computer

Open Run file

Save Run file

Save log file

Online analysis

Help

Update

www.starttimes.com

Files can cause damage to your operating system.

Option	Path / Info	Company	Signer / Issuer
	C:\DOCUME~1\ADMINI~1\POS\LOCALS~1\...		File not found
on	GUID / CLSID not found		
on	GUID / CLSID not found		

تتأكد من الأسطر التي قمنا بتحديدتها
وذلك بالضغط على **Malware hunting**
ثم
Item fixer
عندما نتأكد منها
نقوم بحفظ التقرير بصيغة **run**
وذلك بضغط على
Save run file



runscanner
Fichier RUN
170 Ko

هذا هو التقرير الذي تم تحليله من طرف الخبير
فقط يجب ارسال التقرير للعضو لكي يقوم
بحذف الأسطر
التي تم تحديدها بالتقرير

ملاحظة: الخبير لا يستطيع حذف الأسطر فقط يقوم بتحديد ما ويحفظ التقرير

ويرسله لصاحبه لكي يقوم بالحذف لأنه هو الذي يمتلك خاصية الحذف

و عملية الحذف التي يجب على صاحب التقرير القيام بها

هي على الشكل التالي



eware startup analyzer

hunting Extra stuff Scan computer Open Run file Save Run file Save log file Online analysis

Item fixer Loaded modules

d files can cause damage to your operating system.

Option	Path / Info	Company	Signer / Issuer
	C:\DOCUME~1\ADMINI~1\POS\LOCALS~1\...		File not found
on	GUID / CLSID not found		
on	GUID / CLSID not found		

الآن نقوم بالضغط على
Fix selected item
لكي يتم الحذف

نضغط Ok

Fix selected items

Warning!

RunScanner is an advanced tool, and requires advanced Windows and operating systems in general. If you delete something not knowing what it is, it can lead to major problems such as Windows no longer working or problems with running Windows itself.

Are you sure you want to fix all selected items?

OK Cancel

ثم Ok لتأكيد



هذا البرنامج للأخوة اللذين لا يعرفون كيفية رفع التقارير

برنامج خفيف للرفع التقارير

وهو **Shup**

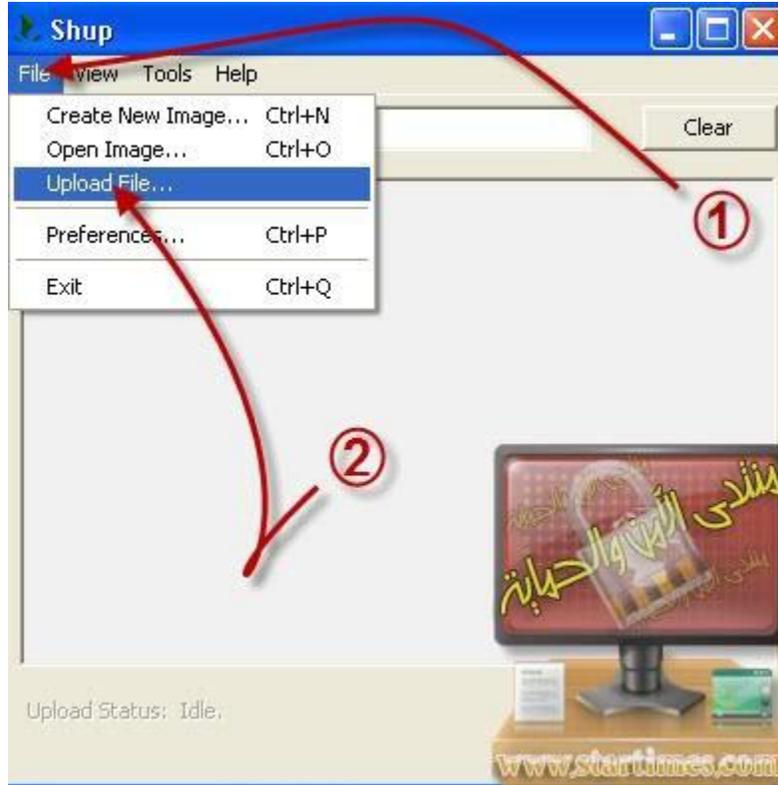
هذا موقع البرنامج

<http://shup.com/>

من هنا تحميل البرنامج

↓ **Shup v0.27 (692kb)**

لرفع نقوم بتالى





ثم نقوم بلصقه للخبير الذي سيقوم بفحص التقرير

ايوب "محب العطاء"

اتمنى ان تدعوا لي بالنجاح في دراستي