LiNz

التخلص من الفيروسات بواسطة الدوس

اجعل حاسوبك افضل

LiNz

2010

SAFIO9O AIN TOUTA

التخلص من الفيروسات بواسطة الدوس

معظم الفيروسات التي تصيب الحواسيب تمنع المستخدم من الوصول الى الريجستري و كذلك تمنع اظهار الملفات الخفية و ملفات النظام و قائمة البرامج الشغالة

Gestionnaire de taches

لنبدا

للتخلص من الفيروس يجب اولا معرفة اسمه

معظم الفيروسات تتوضع نسخ منها في الدريفر (ديسك لوكال)

c:\ ,d:\ ,e:\ ,f:\

لا ظهار اسم الفيروس نتبع الخطوات التالية

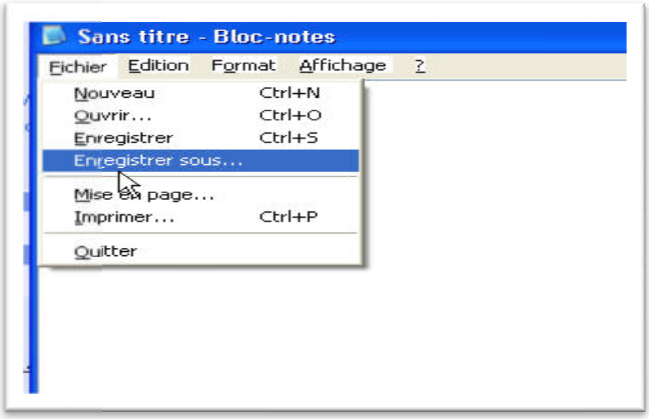
اذهب الى

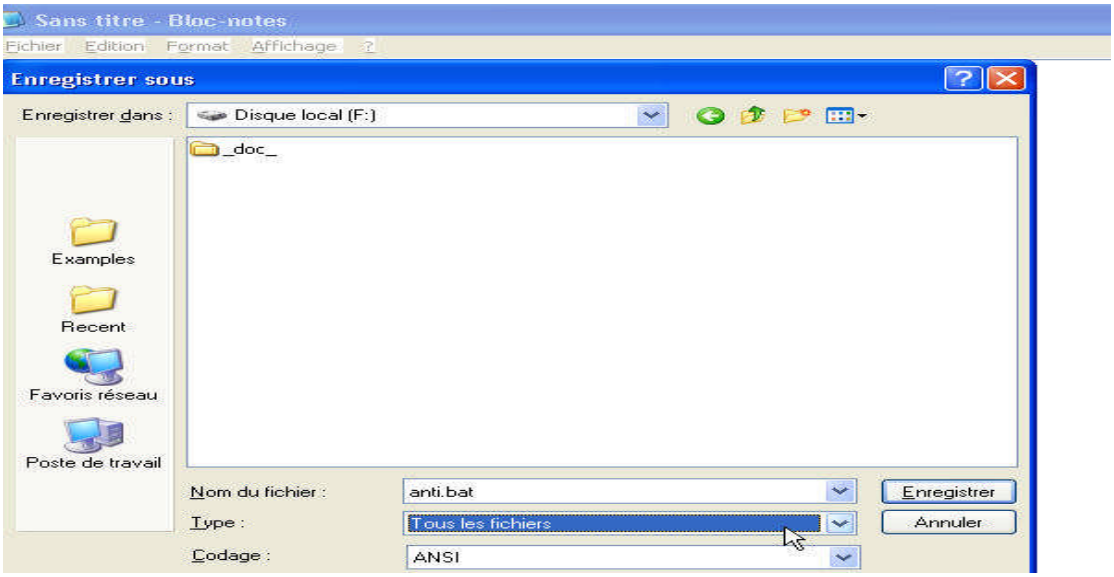
Demarer-→Tous les programmes-→Accessoires--→Bloc-Notes

و اكتب الاوامر التالية

```
:a

attrib -s -h *.*

goto a
```

قم بحفظ الملف باي اسم تريد لكن بامتداد
anti.BAT

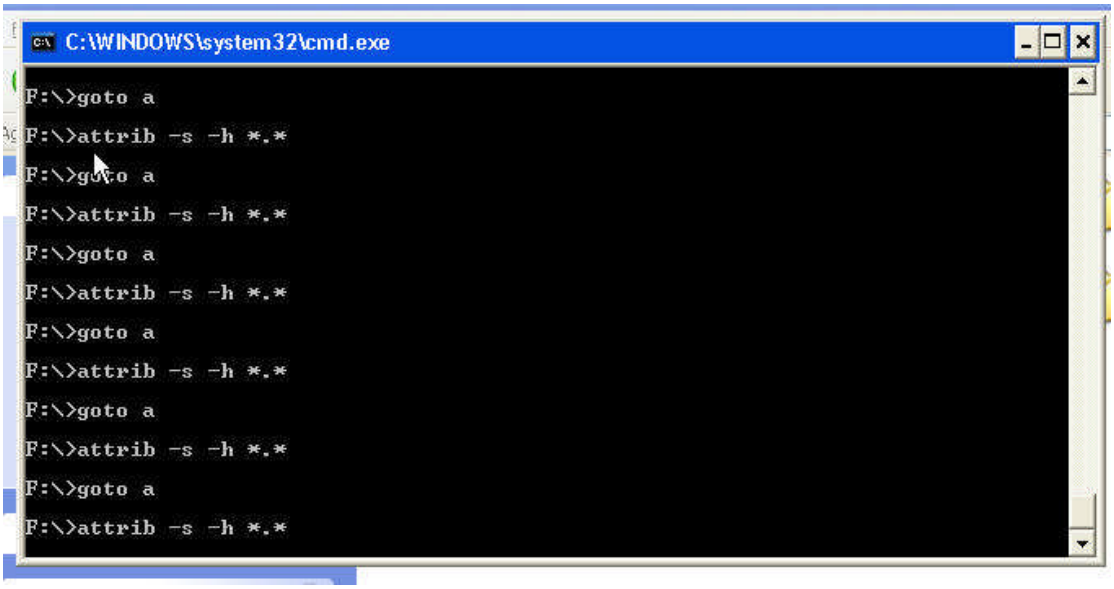




قم بحفظ الملف في

F:\

والان قم بالتنفيذ الملف (شغله) الان سوف يقوم الملف الذي صممناه بنزع خاصيه الاخفاء من اي ملف موجود معه في نفس المجلد



اذا كان هناك فيروس فسوف يظهر ويكون له اسم غريب مثل

Logonoui.exe + autorun.inf /akon.exe + autorun.inf / runVer.exe +autorun.inf

Winfile.jpg + autorun.inf/phiou...exe+autorun.inf/i love you.exe

...etc

تلاحظ ان لكل فيروس ملف "اوتو ران" .يعمل هذا الملف على تشغيل الفيروس 'اذا صح التعبير' عند دخولك الدريفر

F:\

لذلك انصح ببرنامج

USB Disk Security

يعمل هذا البرنامج على منع ملفات الوتو ران من التوضع داخل الدرايفرات

حمله

http://www.zbshareware.com/

CODE : BHHJD17793

NAME : nonokh

بعد ان يظهر لك ملف تنفيذي غير مالوف و كان مخفيا من قبل اوقف الملف الذي صممناه وانقر عليه بالزر الايمن واضغط على

واكتب داخله الامر التالي

قم بتعويض

Name of virus.exe

باسم الفيروس الذي وجدته

```
:a

attrib -s -h *.*

del /q name of virus.exe
```

معناه احذف الملف الذي اسمه

```
md NAME OF VIRUS.EXE
```

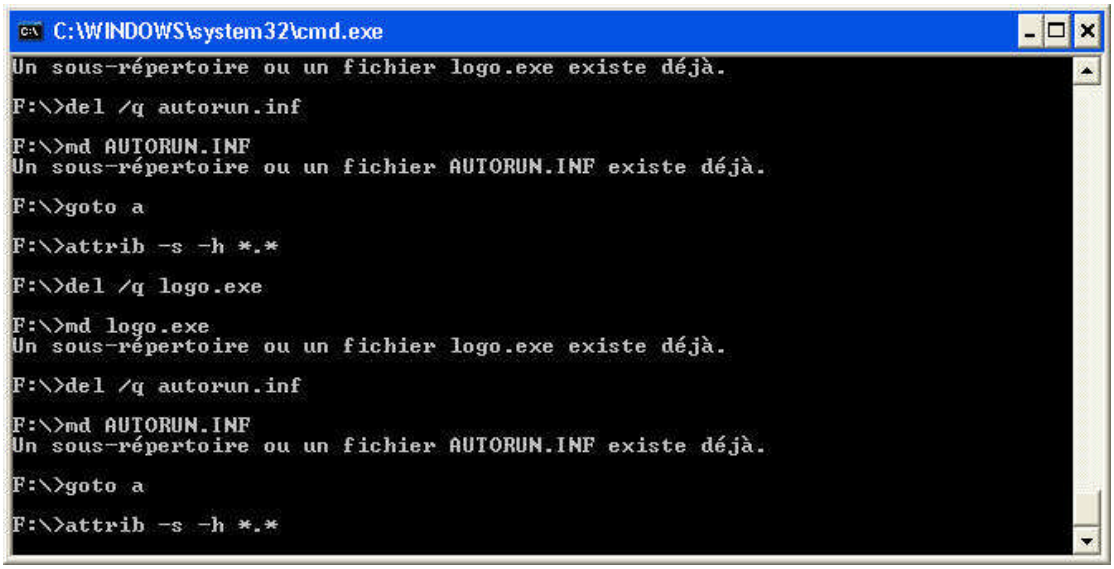
ضع في مكانه مجلد له نفس الاسم حتى لا يعاود الرجوع

```
del /q autorun.inf

md AUTORUN.INF

goto a
```

كتبت اسم المجاد الذي يحمل اسم الفيروس بحروف كبيرة حتى نميزه عن الفيروس الاصلي فيما بعد

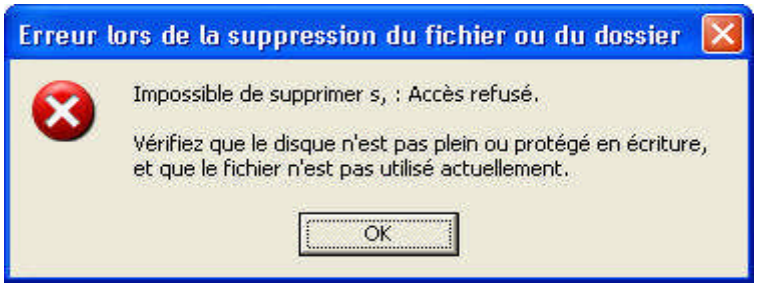
الان قم بحفظ التغييرات

و شغله



اذا لم يحذف الفيروس احذفه انت اثناء تشغيل ملفنا

لكن اذا ظهرت هذه الرسالة



!!!!!!معناه ان الفيروس يعمل الان

لا تقلق توجد طريقة لاظهار الملفات التي هي في طور العمل

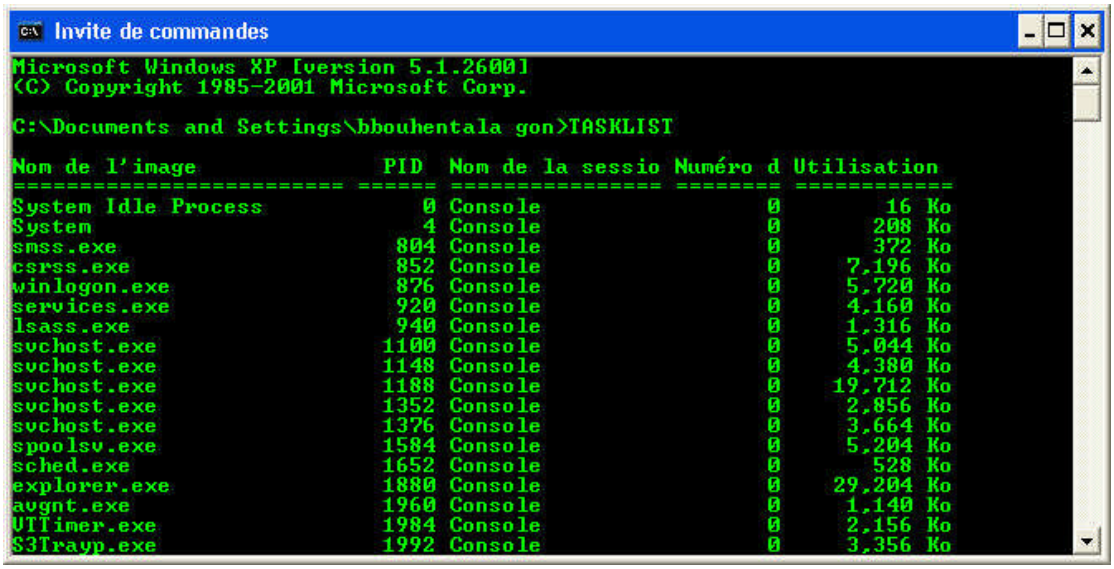
Demarer→Execute→

اكتب

CMD

اكتب داخل واجهة الدوس

TASKLIST



ابحث على اسم الفيروس في القائمة التي تظهر لك

اكتب الامر التالي في نفس الواجهة

Taskkill /f /im name of virus.EXE

هذ ا الامر شبيه ب

Terminer le processu

ثم عد الى الملف الذي صممناه وقم بتنفيذه

واحذف الفيروس بشكل عادي .سوف ترى ظهور مجلد يحمل اسم الفيروس بحروف كبيرة

والان ننقل الملف الذي صممناه الي باقي الدرافرات

ونشغله بنفس الطريقة

تنبيه

بالنسبة للدرايفر

C:\

عند تشغيل الملف الذي صممناه سوف تظهر لك ملفات النظام "" احذر من حذف ملفات النظام"" والا لن يعمل حاسوبك ابداااا وهي مثل

بعد حذف الفيروس من كل الدرافرات يبقى لنا ان نقضي على اللب

الفيروسات تختبا في مجلدات النظام مثل

Windows

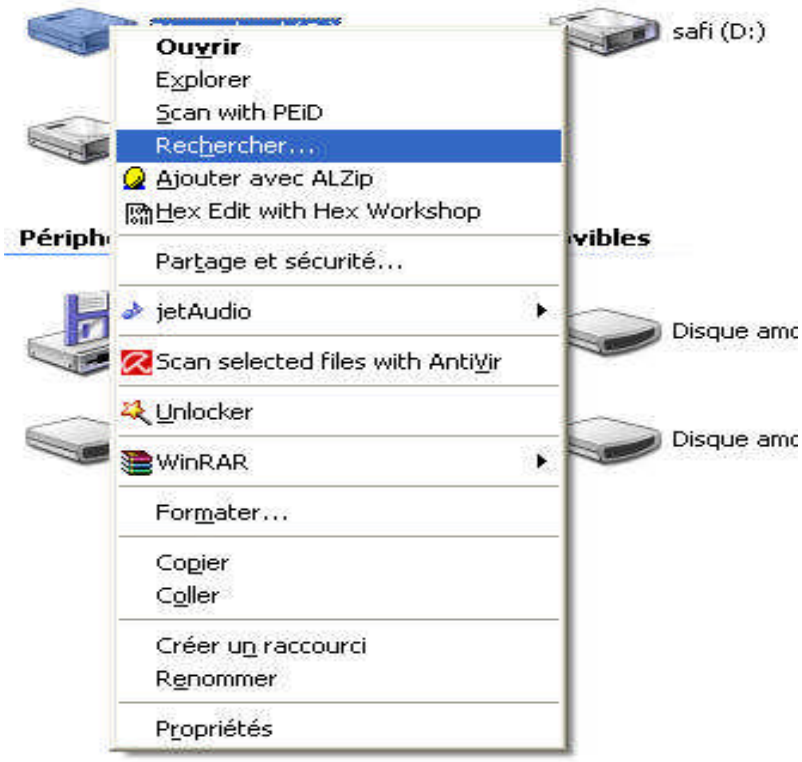
System

System32

C:\

بسهولة نقوم بالبحث عن الفيروس في الدرايفر

C:\


safi (D:)
Périph
vibles
Disque amc
Disque amc
Ouvrir
Explorer
Scan with PEiD
Rechercher...
Ajouter avec ALZip
Hex Edit with Hex Workshop
Partage et sécurité...
jetAudio
Scan selected files with AntiVir
Unlocker
WinRAR
Formater...
Copier
Coller
Créer un raccourci
Renommer
Propriétés


Résultats de la recherche
Fichier Edition Affichage Favoris Outils ?
Précédente
Rechercher
Dossier
Adresse
Résultats de la recherche
Assistant Recherche
Pour lancer une recherche, suivez
Rechercher en utilisant le(s) critère(s) ci-dessous.
Une partie ou l'ensemble du nom de fichier :
nom of virus.exe
Un mot ou une phrase dans le fichier :
Rechercher dans :
Disque local (C:)
Quand a eu lieu la dernière modification ?
Précédent
Rechercher

اذا لم يظهر ابحث في الملفات المخفية و النظام

بعد ان تجده

اضغط عليه بالزر الايمن كالتالي

بعدها انسخ الملف الذي صممناه الذي المكان الذي يظهر لك بعد النقر على

Ouvrir le dossier contenant

واكتب داخله

:a

attrib -s -h name of virus.exe

del /q name of virus.exe

md NAME OF VIRUS.exe

goto a

اذا ظهر لك المجلد فمبارك

بعد القضاء على الفيروس تبقى مشكلة اصلاح الخراب الذي صنعه الفيروس

لجعل ملف من ملفات النظام اذهب الى

Demarer→Execute→

اكتب

CMD

اكتب

عوض path

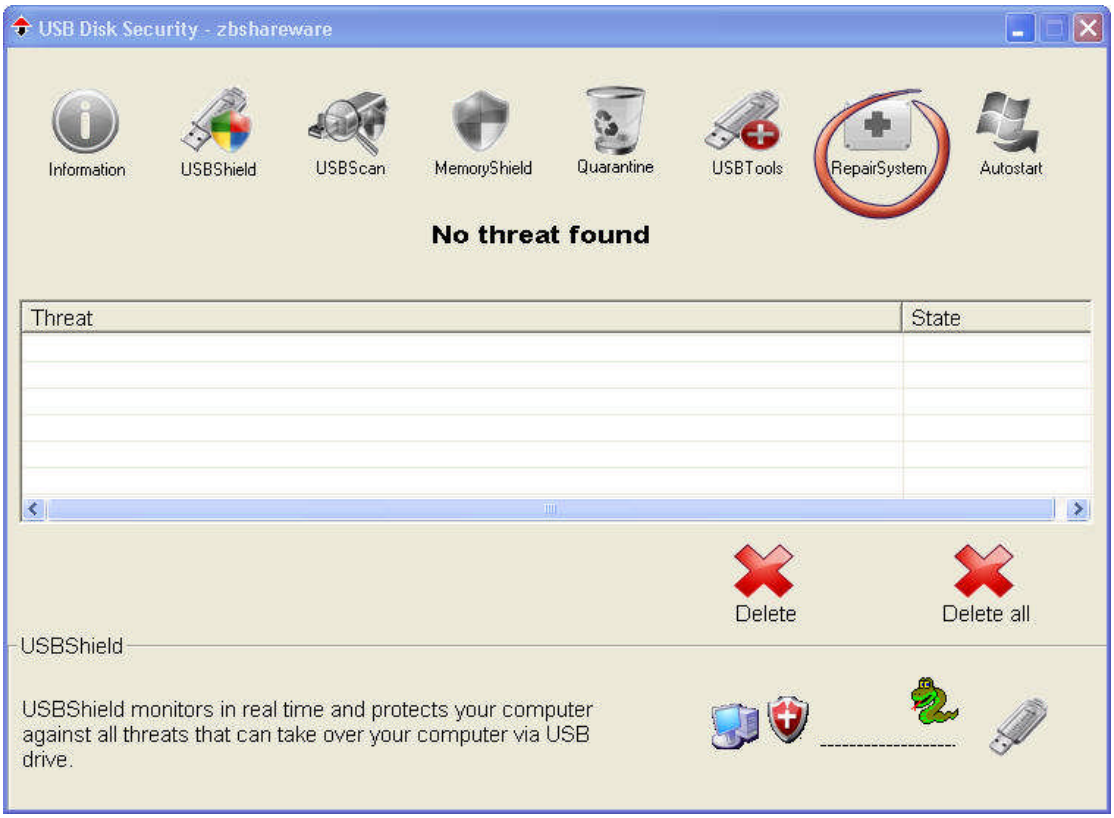
ب مسار الملف الذي تريد جعله من ملفات النظام

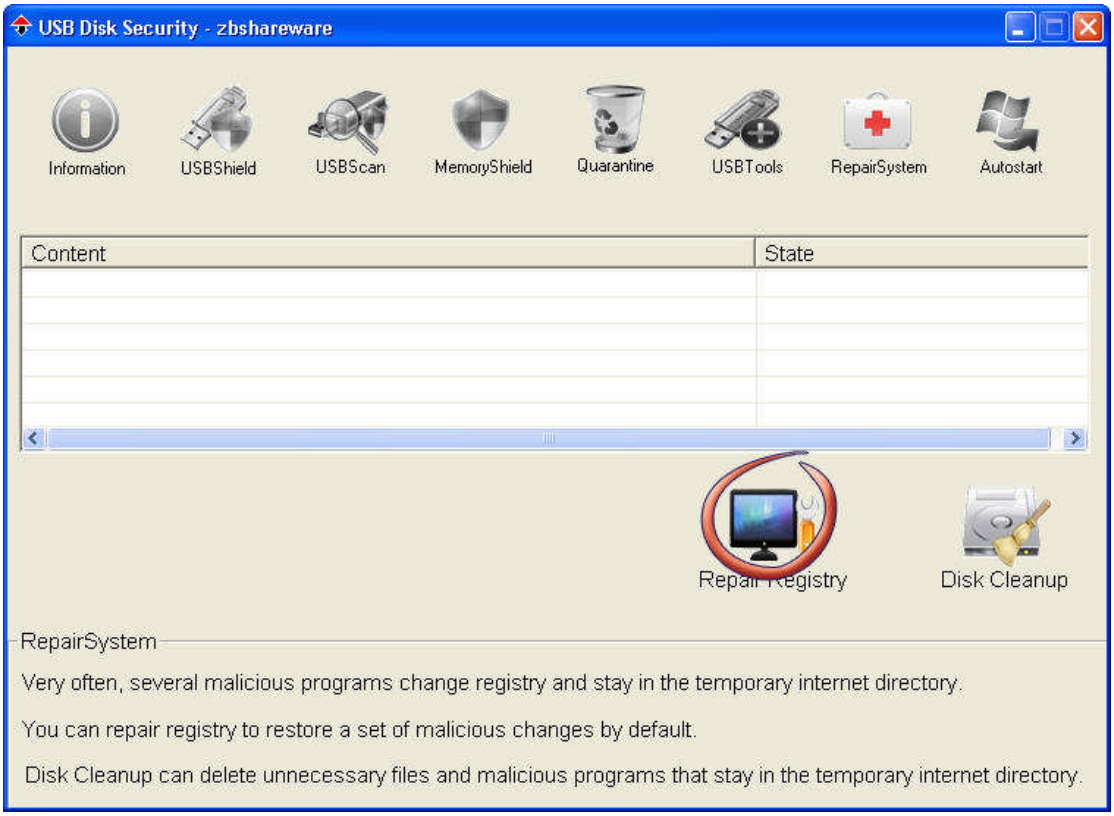
ATTRIB +S +H PATH

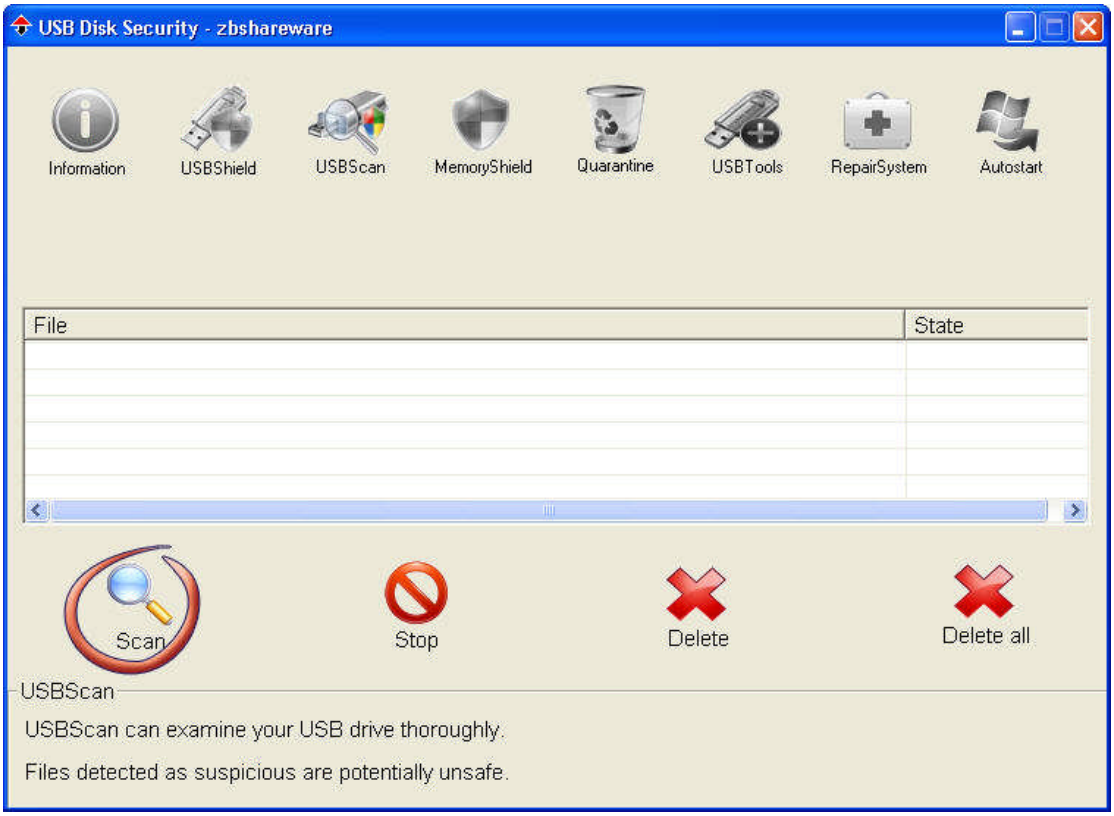
مثل

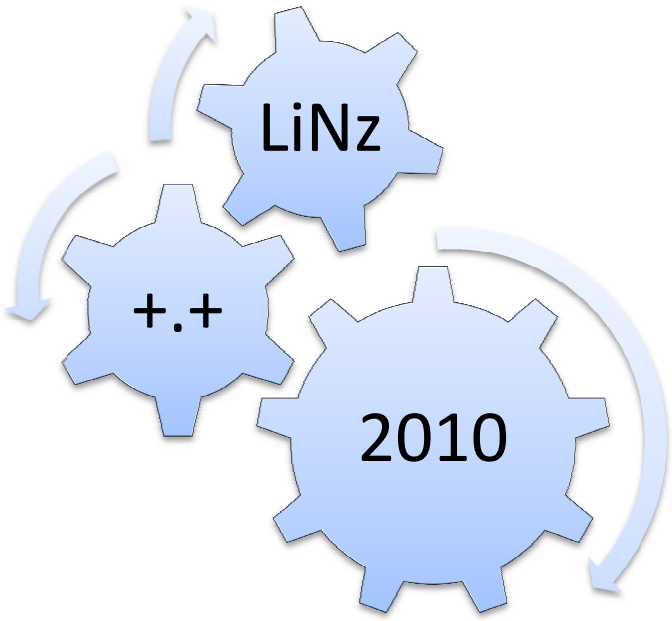
Attrib +s +h ‘’c:\myfile.txt ‘’

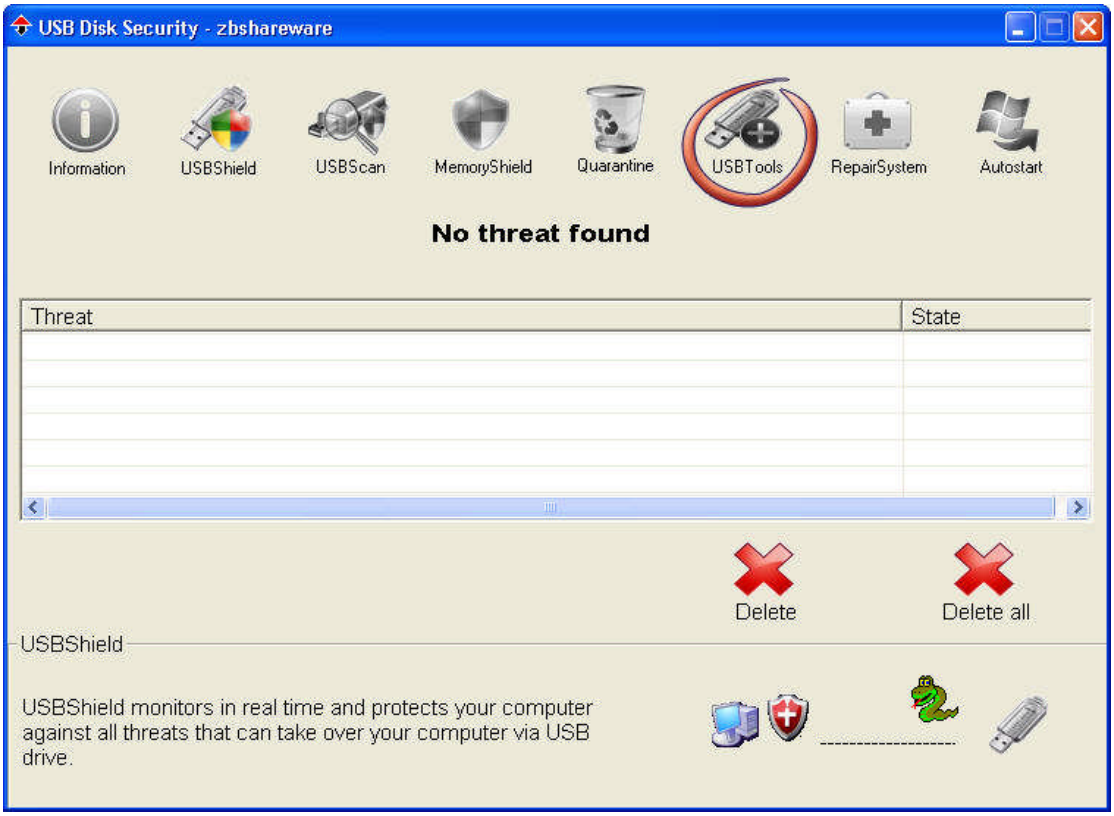
USB DISK SECURITY

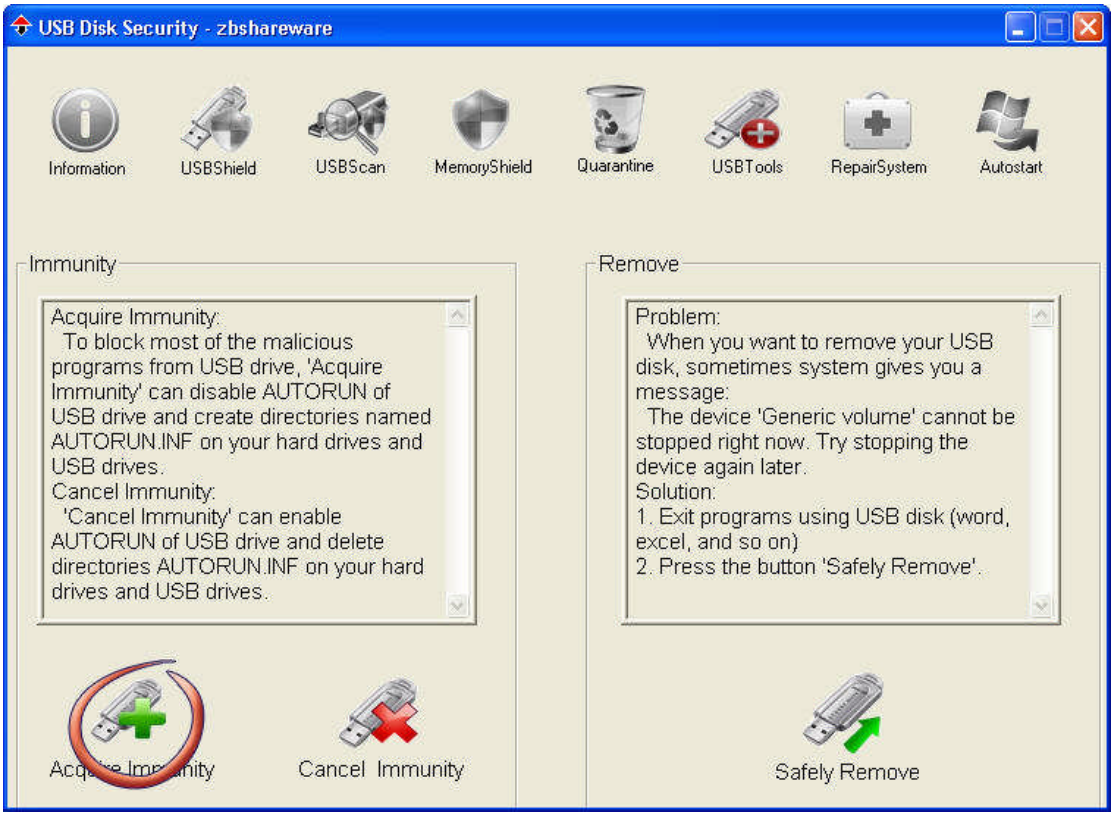



USB Disk Security - zbshareware
Information
USBShield
USBScan
MemoryShield
Quarantine
USBTools
RepairSystem
Autostart
Content
State
Repair Registry
Disk Cleanup
RepairSystem
Very often, several malicious programs change registry and stay in the temporary internet directory.
You can repair registry to restore a set of malicious changes by default.
Disk Cleanup can delete unnecessary files and malicious programs that stay in the temporary internet directory.


USB Disk Security - zbshareware
Information
USBShield
USBScan
MemoryShield
Quarantine
USBTools
RepairSystem
Autostart
File
State
Scan
Stop
Delete
Delete all
USBScan
USBScan can examine your USB drive thoroughly.
Files detected as suspicious are potentially unsafe.


LiNz
+.+
2010


USB Disk Security - zbshareware
Information
USBShield
USBScan
MemoryShield
Quarantine
USBTools
RepairSystem
Autostart
No threat found
Threat
State
Delete
Delete all
USBShield
USBShield monitors in real time and protects your computer against all threats that can take over your computer via USB drive.



digi4moon@gmail.com

او

safio9o@yahoo.fr

اتمنى ان اكون قد افدت

لا تنسوني من صالح دعائكم

Algeria /batna /Ain touta /

LiNz**