How to Remove Autorun Worm???

آموزش حذف کرم اتوران

نویسنده: محمود زیوری

Just Relax!!!!

مقدمه

سلام دوست گرامی که داری این کتاب رو مطالعه میکنی.
ابتدا میریم سراغ بحث کلی در مورد بدافزار ها.مهم ترین بدافزارها به شرح زیر هست:
1)ویروس(Virus):قطعه نرم افزار کوچکی هست که خودش رو به یک نرم افزار دیگه می چسبونه و اعمال خرابکارانه ای رو انجام میده.برای اینکه ویروس بتونه انتشار پیدا کنه باید به یک فایل دیگر(فایل میزبان)وصل بشه

2)کرم(Worm):قطعه نرم افزار کوچکی شبیه ویروس با این تفاوت که برای خرابکاری و انتشار،نیازی به فایل میزبان نداره و خودش قادر هست که از خودش نسخه هایی رو ایجاد و شروع به خرابکاری کنه.

3)تروجان(Trojan):قطعه نرم افزار کوچکی که ظاهرا یک نرم افزار کاربردی یا هر چیز سودمند دیگه هست اما در باطن اعمال خرابکارانه انجام میده.پس قادر به انتشار نیست.اسم تروجان از داستان تسخیر شهر تروا توسط یونان گرفته شده که در اون داستان،یونان یک اسب چوبی بزرگ حاوی سرباز رو به ظاهر یک هدیه به کشور تروا پیشکش میکنه ولی در باطن قصد حمله به کشور تروا رو داشتنه.پس تروجان مثل اسب و کامپیوتر میزبان مثل شهر تروا میمونه.

اصل مطلب

خوب..دیگه بریم سراغ اصل مطلب.شما یه فلش رو که حاوی کرم هست به سیستم میزنید ولی بعد از مدتی میبینید که ویندوزتون یه جوری شده یا اینکه هر اطلاعاتی که وارد فلشتون میکنید،اطلاعاتتون مخفی میشه و به جاش یه سری فایل اجرایی یا شورتکات همنام با اطلاعاتتون میبینید(که این حالت به کرم آتوران معروفه).میخوایم که این مشکل رو حل کنیم که مشکل دوم رایجتره و با

روش من روی اکثر کرم ها جواب میده ولی مشخصه که ممکنه روی تعداد کمی از کرم های حالت اول جواب بده.وقتی شما با این مشکلات روبرو میشید دو واکنش نشون میدید:اول اینکه مثل خانم زیر با چکش بیفتید به جون سیستم و سیستم رو داغون کنید!

یا اینکه مثل آقای زیر یک روش صلح آمیز رو انتخاب کنید(که انتهای انتهاش این هست که ویندوز رو باید عوض کرد) و تعطیلات آخر هفته رو کنار ساحل بگذرونید و حالشو ببرید!

البته این رو بگم که دو تصویر بالا که مشاهده کردین کاملا اتفاقیه و یه وقت خانم ها دلخور نشن که چرا این تصویر رو گذاشتم!پس اگه مشکلی نیست بریم رو روش دوم کار کنیم.روش اول که نیاز به یادگیری نداره.فقط یه چکش میخواد و یه ذره پول واسه خرید سیستم جدید!کافیه که چکش رو با زاویه حدود 150 درجه

به سیستم بکوبید و سیستم رو داغون کنید!حالا روش دوم رو روی ویندوز 8 پیاده سازی میکنیم که تفاوت زیادی با ویندوز 7 نداره و هرجا لازم شد مرحله رو از طریق ویندوز 7 هم میگم

بریم که شروع کنیم

مرحله 1)حفظ خونسردی کامل

مرحله 2)اگه گفتین!خوب معلومه؛باید سیستم رو روشن کنید دیگه!با سیستم خاموش که نمشیه کاری کرد!

مرحله 3)رفتن به محیط Safe Mode:این محیط،شبیه محیط ویندوز کنونی با پس زمینه مشکی رنگ،با ضریب امنیتی بالا هستش.

ویندوز 8:کلید ترکیبی win+I رو بفشارید سپس مسیر زیر رو طی کنید:

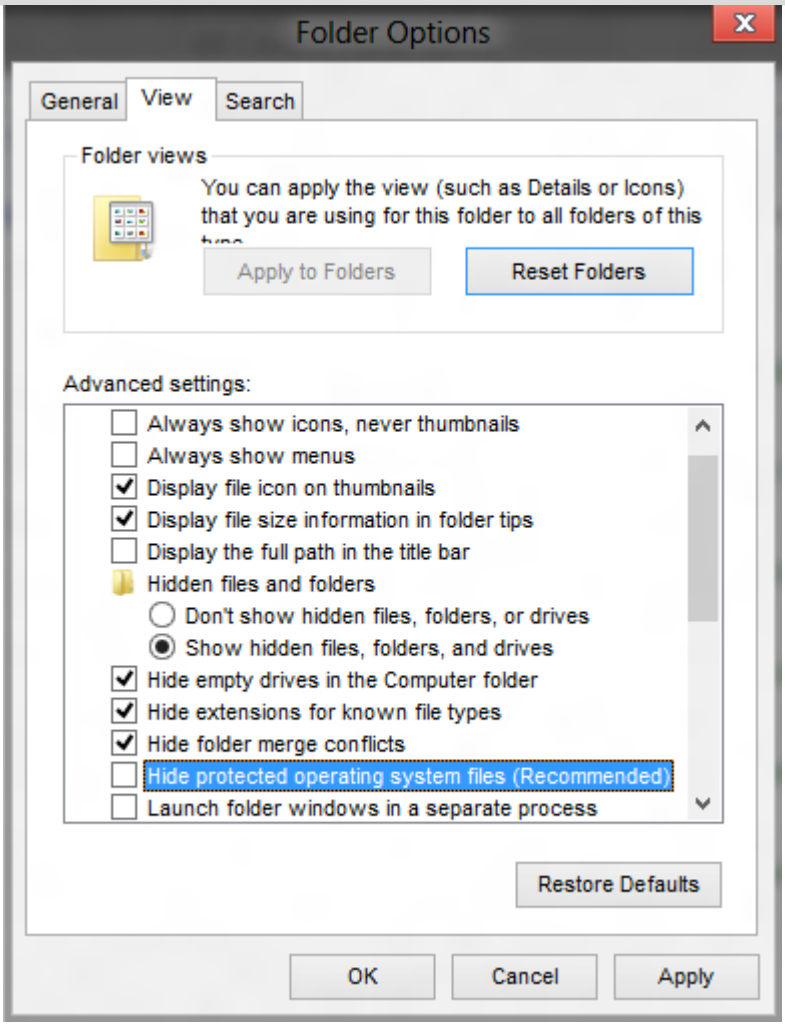
Settings\change PC settings\General\Advanced Startup

روی Restart now کلیک کنید تا پنجره choose option باز شود سپس Troubleshoot و پس از آن Advanced option رو انتخاب کنید و پس از آن Startup Settings و پس از آن روی Restart کلیک کنید.پس از راه اندازی مجدد سیستم یک صفه آبی رنگ ظاهر میشه که با فشردن کلید 4 وارد محیط Safe Mode میشوید.

ویندوز 7:موقع روشن شدن سیستم؛قبل اینکه لوگوی ویندوز ظاهر بشه،کلید F8 رو بفشارید و پس از آن گزینه Safe Mode رو انتخاب کنید.

مرحله 4)ظاهر کردن فایل ها و پوشه های مخفی:

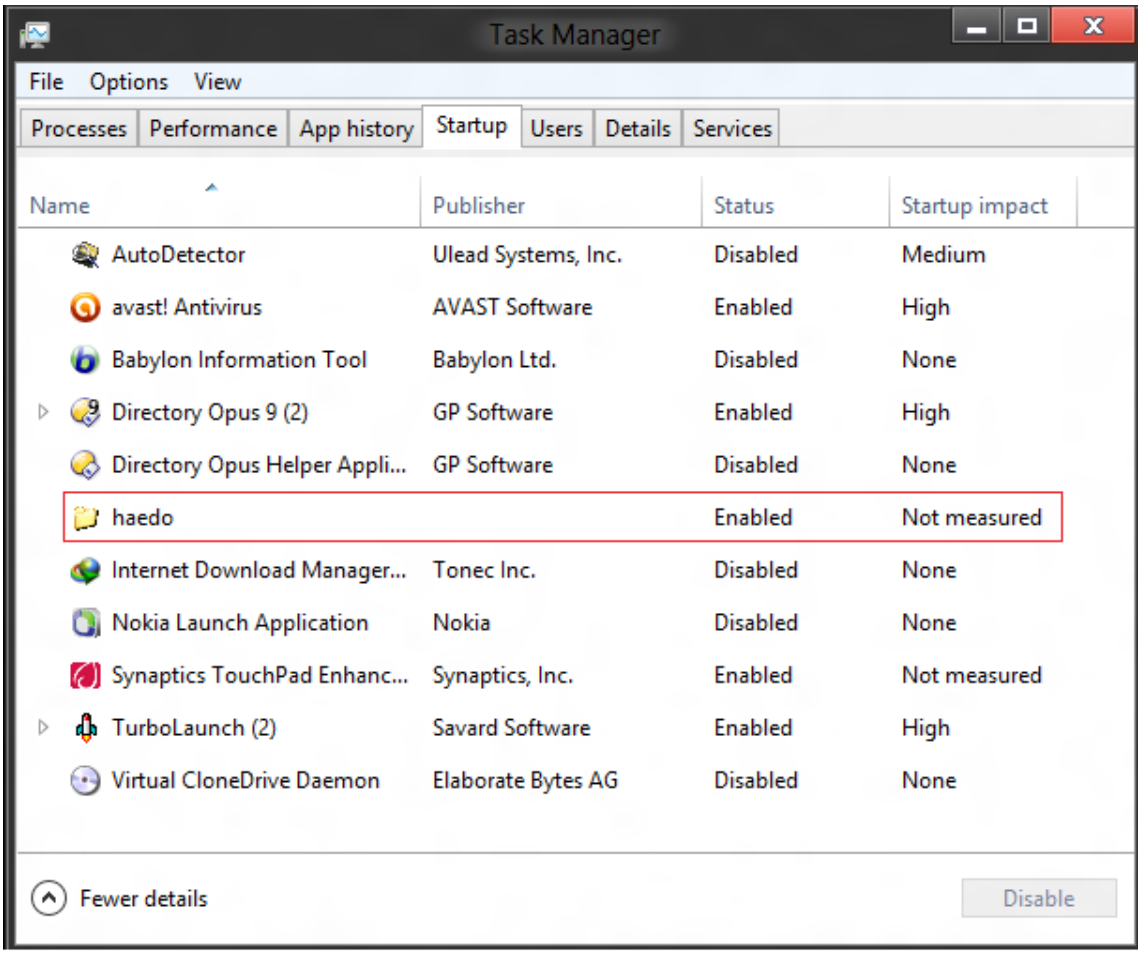
به control panel رفته و folder option رو انتخاب کنید.سپس روی تب View کلیک کنید و قسمت ...show hidden files رو انتخاب کنید و پس از آن تیک ...Hide protected رو بردارید و در پنجره ظاهر شده روی yes کلیک کنید.



مرحله 5)شناسایی فایل کرم و پیدا کردن آدرس آن:

بالاخره یک کرم باید در حافظه Ram باشه که کار خودش رو بکنه.بنابرین باید اون رو در قسمت Startup جستجو کنیم.پس بریم که داشته باشیم...

ویندوز 8: Task Manger رو اجرا کنید.سپس به قسمت Startup برید.در اینجا باید فایل مشکوک رو جستجو کنید که معمولا یک نام نامفهوم، شرکت بی نام و یک آیکون مشکوک داره که در این آموزش فایل مشکوک haedo با شرکت بی نام و با یک آیکون مشکوک هست.تصویر رو در صفحه بعد سیاحت کنید.البته ممکنه در مواردی چندین فایل مشکوک به کرم وجود داشته باشه که شما باید همه اونها رو شناسایی کنید.



ویندوز 7:کلید ترکیبی win+R را بفشارید و عبارت msconfig را تایپ و ok کنید.سپس به قسمت startup رفته و فایل مشکوک به کرم را آنجا جستجو کنید.

مرحله 6)حذف فایل کرم:

ویندوز 8:روی فایل مشکوک راست کلیک؛سپس enable رو انتخاب کنید.پس از آن مجددا روی فایل راست کلیک و پس از آن open file location رو انتخاب کنید.در پنجره ی باز شده،فایل کرم رو پیدا کنید و اون را انتخاب و پس از آن کلید ترکیبی shift+delete را بفشارید تا فایل کرم از صحنه روزگار محو شود!

ویندوز 7:آدرس فایل کرم رو از قسمت startup پیدا کنید و پس از آن به پوشه مربوطه رفته و فایل کرم رو پاک کنید.

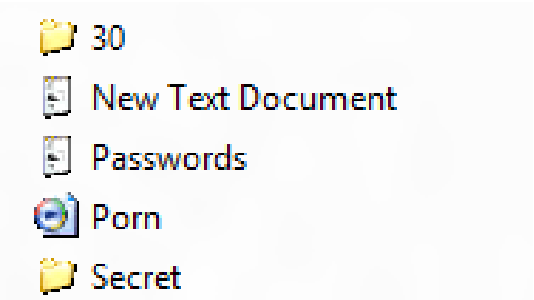
خوب...دیدید که این روش خیلی بهتر از چکش کاری سیستم هست!حالا بریم به قسمت دوم این بحث که جبران خرابکاری کرم هست.درسته که شما فایل کرم رو پاک کردین اما خساراتی که به اطلاعات فلش شما وارد کرده همچنان وجود داره.پس بریم...

مرحله 1)اطمینان داشته باشید که مرحله 4 قسمت قبلی همچنان سر جاشه(ظاهر کردن فایل ها و پوشه های مخفی).البته مرحله 1 رو هم باید داشته باشید(حفظ خونسردی!)

مرحله 2)وارد شدن به درایو فلش:یه وقت با دابل کلیک روی درایو فلش این کار رو انجام ندید وگرنه فایل کرم دوباره وارد سیستم میشه پس از طریق نوار درختی سمت چپ وارد درایو فلش بشید.

مرحله 3)حذف فایل کرم: فایل Autorun را بدون هیچ معطلی پاک کنید.بعد از اون ببینید کدوم فایل متعلق به شما نیست.اونها رو شناسایی و پاک کنید.اگه یه شبه پوشه دیدید که یک فایل اجرایی هست اون رو هم بدون هیچ معطلی پاک کنید.برای این که بفهمید فایل مربوطه از نوع اجرایی هست کافیه که ببینید در قسمت Type پنجره باید Application نوشته شده باشه.وقتی که تعداد فایل ها زیاد باشه،

شناسایی فایل ممکنه یکم مشکل باشه.برای این کار در قسمت خالی پنجره فلش راست کلیک کرده سپس در قسمت Sort by گزینه Size رو انتخاب کنید.حالا میتونید فایل های مشکوک رو بهتر شناسایی کنید.



مرحله 4)از حالت مخفی در آوردن:برای اینکه بتونید فایل و پوشه های مخفی را به حالت اول برگردانید این کار رو انجام بدید:یک Notepad باز کنید و دستور زیر رو در آن قرار بدید:

```
attrib -h -s /s /d
```

سپس اون رو ذخیره کنید فقط موقع انتهای اسمی که براش انتخاب میکنید عبارت ".bat" رو اضافه کنید مثلا "show hidden.bat" . اگه کرم اتوران طوریه که یک شورتکات رو از پوشه هاتون درست میکنه دستور زیر رو هم اضافه کنید:

```
Del *.lnk
```

پس دستورات به شکل زیر در میاد:

```
attrib -h -s /s /d
Del *.lnk
```

این فایل رو تو فلش بریزید و اون رو اجرا کنید.اگه تعداد پوشه ها زیاد باشه ممکنه یکم طول بکشه.بعد اینکه پنجره فایل show hidden بسته شد دیگه کار تمومه و شما تونستید یک راه صلح آمیز رو طی کنید.پس میتونید تعطیلات آخر هفته خوبی رو داشته باشید.

چکار کنیم؟؟؟

آنتی ویروس که نصبه ولی بعضی موقع ها عین یه بت رفتار میکنه!در این صورت کاربر باید خودش دست به کار بشه.اما چه بکنیم؟؟؟

خیلی راحت...از قسمت folder optionفایل ها و پوشه های مخفی رو ظاهر کنید.بعد از اون از طریق نوار درختی سمت چپ وارد درایو فلش بشید.فایل های مشکوک رو طبق آموزش های قبل شناسایی و پاک کنید.محض احتیاط یه بار فلش رو بیرون بیارید و دوباره فلش رو به سیستم بزنید و مطمئن بشید که هیچ فایل مشکوکی وجود نداشته باشه.

اما مسئله اینه که شما که حوصله ندارید هر دفعه برید folder option و تنظیمات رو بهم بزنید و بعدش دوباره درست کنید!!!پس باید به فکر یه نرم افزاری باشید که این کار رو براتون انجام بده.نرم افزار های زیادی تو این زمینه هست ولی من نرم افزار Directory Opus رو بیشتر ترجیح میدم.با این نرم افزار راحت میتونید فایل ها و پوشه ها حتی اونایی که مخفی هستن رو ببینید.پس هر وقت خواستید کرم آتوران رو از فلش پاک کنید از طریق این نرم افزار اقدام کنید.این نرم افزار،فایل ها و پوشه های مخفی رو با رنگ قرمز نشون میده.

این نرم افزار دو نسخه 32 و 64 بیتی رو داره و شما باید متناسب با سیستم تون این نرم افزار رو تهیه کنید.

سخن آخر

برای اینکه شما بتونید کرم آتوران رو پاک کنید باید تجربه زیادی در این زمینه کسب کنید و با خوندن این کتاب مشکلتون به خوبی حل نمیشه پس باید یه ذره جرات به خرج بدید فقط مواظب باشید زیادی شلوغش نکنید.من خودم چند تا کرم آتوران رو تو سیستمم دارم.اگه میخواین که این آموزش رو بهتر درک کنید کافیه یه ایمیل به من بزنید تا فایل ها رو براتون ارسال کنم.

این کتاب الکترونیکی اولین تجربه من تو نوشتنه.پس نمیتونه خالی از اشکال باشه.با ارسال نظرات و پیشنهاداتتون منو دلگرم کنید.امیدوارم که مطالب رو به خوبی انتقال داده باشم.

موفق باشید...

محمود زیوری

ZIVARI_TS@YMAIL.COM