روش تشخیص سیستم های آلوده به ویروس و پاک کردن آن ها

حالا از کجاها بفهمیم که کامپیوتر ما ویروس گرفته است

موقعی که شما وارد *My Computer* می شوید و روی درایو های آن راست کلیک می کنید و در این هنگام یک گزینه با یک زبان نامفهوم را می بینید.یا اینکه وقتی روی درایو هایتان دو بار کلیک می کنید محتوای درایو های شما در یک صفحه جدید باز می شود .یا موقع دابل کلیک کردن روی درایو هایتان پنجره *Open With* باز می شود و به شما می گوید *Choose the you want to use to open this file program* یا هنگام کلیک بر روی درایو هایتان *error* به شما داده می شود .

گاهی اوقات هم زمانیکه روی درایوهایتان راست کلیک میکنید گزینه ی *Auto Run* دیده میشود.

این موارد نشان میدهد که یعنی سیستم شما ویروسی شده است. این ویروس، ویروس *autorun.inf* میباشد

همچنین این ویروس باعث از بین رفتن و پاک شدن *Folder Options* خواهد شد.

و اگر شما گزینه های *Show hidden files and folders* و *protected operating system files (Recommended Hide*) را مارک دار کنید با *ok* کردن پنجره این گزینه کار نخواهند کرد . و دوباره به حالت اولیه باز خواهند گشت.همچنین این ویروس باعث غیر فعال شدن *Task Manage*و *Registry Editor* خواهد شد .

اگر شما روی گزینه *command prompt* یا *cmd* نیز کلیک کنید یا باز نخواهد شد و پیغام زیر را خواهد داد یا اینکه به سرعت باز و بسته خواهد شد .

the command prompt has been disabled by your administrator

راههای ورود این ویروس از طریق قطعاتی خواهد بود که از طریق *USB* با سیستم شما ارتباط دارند . قطعاتی مانند فلش مموری ها (کولدیسک) ، موبایل ها ، رم ریدر ها و ...

نحوه از ببن بردن ویروس *autorun.inf*

روش اول :

ابتدا وارد *My Computer* شوید.بعد از مشاهده لیست درایوها از نوار بالا بروی گزینه *Tools* کلیک کرده سپس گزینه *Folder Options* را انتخاب کنیددر پنجره جدید باز شده گزینه *View* را انتخاب کنید و بروی گزینه *Show hidden files and folders* کلیک کنید تا دایره آن توپر شود .کمی پایینتر تیک گزینه *Hide Protected Operating System Files* را بر دارید.حالا *ok* کنیدسپس با راست کلیک کردن و زدن *open* وارد درایو هایتان شوید

سپس دنبال یک فایل به نام *autorun.inf* بگرید و ان را پاک کنید برای همه درایو ها این کار را انجام بدید .

بعد از این کار بلافاصله بدون هیچ معطلی سیستم خودتون را ریستارت کنید . یادتون نره حتما حتما بدون انجام هیچ کاری سیستم را ریستارت کنید .

روش دوم :

ابتدا با زدن کلید *F* سیستم را در حالت *safe mode* راه اندازی کنید و سپس از منوی استارت گزینه *run* را بزنید و سپس داخل ان *cmd* را تایپ کنید و *ok* بزنید .عبارات زیر را یکی یکی نوشته و *enter* بزنید . این کار را برای تمامی درایو ها انجام دهید .

del x:/autorun.inf \a:h

del x:/autorun.inf \a:r

del x:/autorun.inf \a:s

به جای *x* باید نام درایوها را بنویسید .

روش سوم :

***copy.exe* تروجانی است که گاهی اوقات در تمامی درایو های شما قرار میگیره و با هر بار کلیک بر روی درایو ها فایل *autorun.inf* فایل این فایل را اجرا می کند.یکی از روشهای پاک کردن این ویروس این است که ابتدا شما باید پروسه های *temp .exe* و *temp .exe* رو از بین ببرید . برای این کار ابتدا باید سیستم را به صورت *safe mode* راه اندازی کنید .**

شما نباید روی درایو ها یتان دابل کلیک کنید چون با این کار ویروس *autorun.inf* که در درایو هایتان قرار دارد باعث فعال شدن پروسه های *temp .exe* و *temp .exe* می شود.

بعد از راه اندازی سیستم به صورت *safe mode* شما باید با راست کلیک کردن و زدن گزینه *open* وارد درایو *c* ویندوز شده و به پوشه *windows* و بعد هم پوشه *system* رفته و دو فایل *temp .exe* و *temp .exe* را حذف کنید.

البته در بعضی از نسخه های ویروس *copy.exe* ویروس *autorun.inf* حتی درون پوشه %*win*% هم وجود داره بنابراین حتما حتما برای ورود به درایوها پوشه ها را با راست کلیک باز کنید.

نکته: قبل از اینکار باید ابتدا این پروسه ها را از *Manager Task* پاک کنید. برای این کار با زدن کلید های ترکیبی *ctrl + alt + delete* وارد *Task Manager* بشید و پروسه های *temp .exe* و *temp .exe* را از لیست *processes* با کلیک بر روی انها و زدن *end process* حذف کنید.

ویروس *autorun.inf* با هر بار فعال شدن موجب میشود که دو فایل *xcopy.exe* و *host.exe* درون همان درایو فعال بشوند و دوباره دو فایل *temp .exe* و *temp .exe* را بسازند.

شما نباید فایل های *xcopy.exe* را با فایل های خود *windows* که درون پوشه ی *system* هستند اشتباه بگیرید.

برای تشخیص ویروس *xcopy.exe* و فایل *xcopy.exe* که در پوشه *system* است باید از حجم انها این دو را شناسایی کرد اگر فایل *xcopy.exe* حجمی معادل 32 کیلو بایت داشت مربوط به خود ویندوز می باشد در غیر این صورت ویروس خواهد

بود.حالا فایلهای سیستمی را مانند روش اول از حالت هایدن خارج کنید و ویروس ***autorun.inf*** را پاک کنید و بعد هم به درایوهای خودتون نگاه کنید اگر فایلهایی با عنوان ***xcopy.exe*** و***host.exe*** بودند با خیال راحت پاک کنید.

نحوه پاک کردن ویروس *Copy.exe*

اسامی دیگر این ویروس *host.exe, xcopy.exe, temp .exe, temp .exe and svchost.exe,Salga-A worm*

این ویروس یکی از خطرناک ترین ویروس ها هست که به عنوان یک پروسه در سیستم شروع به فعالیت و انتشار خودش می کنه و با توجه به اینکه بعضی از انتی ویروسها به صورت نامناسب این ویروس را پاک می کنند باعث نمایش یک پیغام در زمان دابل کلیک کردن روی درایو و یا فولدر در محیط ویندوز می شوند.

برای پاک کردن دستی این کرم شما باید ابتدا همه پروسه هایی که با نام های *host.exe, xcopy.exe, temp .exe, svchost.exe,Salga-A worm temp .exe and* هستند را پیدا کنید و آنها را پاک کنید .

تذکر: مواظب باشید این فایلها را با فایلهای اساسی سیستم عامل اشتباه نگیرید .

مهم :یکی از دلایل اصلی به وجود امدن این مشکل ویروس *Autorun.inf* هست که شما باید طبق روش هایی که در اموزش گفته ام ان را پاک کنید . این کار را حتما انجام دهید . یعنی حتما باید ابتدا ویروس *Autorun.inf* را طبق اموزش باید از بین ببرید.سپس به این آدرس در رجیستری رفته و اگر کلیدی به اسم *Copy.exe* در زیر منوی *MountPoints* وجود داشت آن را پاک کنید.

HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\MountPoints

با این برنامه به طور کامل می توانید این ویروس را از بین ببرید .

http://www.securitystronghold.com/download/solutions/TrueSword .exe

راههای دستی برای از بین بردن ویروسی که *Show Hidden Files* را غیر فعال می کند .

وقتی صفحه ی رجیستری باز شد ، از سمت چپ وارد این مسیر بشید :

HKEY_CURRENT_USER\Software\Microsoft\Windows\Curre ntVersion\Explorer\Advanced

در این قسمت ، در لیست متغیر هایی که سمت راست وجود دارند ، متغیر آبی رنگی (*DWORD Value*) رو به نام *Hidden* پیدا کنید و روی ان دابل کلیک کنید . اگر مقدارش (*Value data*) به 0 تغییر کرده ، ان را به 1 یا 2 تغییر دهید و *OK* کنید. حالا رجیستری را ببندید و ریستارت کنید.مسیر زیر را دنبال کنید:

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft

=>*Windows\CurrentVersion\Explorer\Advanced\Folder\Hidden*

اکنون در سمت راست پنجره ی *Regedit* روی *Type* دو بار کلیک کرده و مقدار آن رو برابر با *group* قرار دهید

با این کار تونستید *Show Hidden Files* از دست رفته را که دیده نمی شد برگردونید .

مسیر زیر رو دنبال کنید :

HK LocalMachine\Software\Microsoft\Windows\CurrentVersion\Explorer\Advanced\Folder\Hidden\SHOWALL

در سمت راست پنجره ی *Regedit* مقدار *CheckedValue* رو برابر با 1 قرار بدید.

راههای دستی برای برگرداندن قسمتهای حذف شده از سیستم شما

فعال ساختن (*Registry (Regedit* :

روش اول:

ابتدا وارد منوی *start* شده و روی گزینه *run* کلیک کنید و کلمه *gpedit.msc* را تایپ کنید .

در صفحه *Group Policy* به مسیر پایین بروید:

System <Administrative Templates <User Configuration

بعد از کلیک نمودن بروی *System* در سمت راست پنجره *Group Policy* بالای

***Prevent access to registry editing tools* دابل کلیک نموده و در تب *Setting* گزینه *Disable* را علامت دار نموده و بالای کلید *OK* کلیک نمایید اما پنجره *Group Policy* را نبندید!**

روش دوم :

مسیر زیر را داخل *note pad* کپی کرده و سپس با نام *Regedit.reg* ذخیره کنید و بعد ان را اجرا کنید .

Windows Registry Editor Version .

REG add HKCU\Software\Microsoft\Windows\CurrentVersion\Pol icies\System /v DisableRegistryTools /t REG_DWORD /d /f

برگرداندن *Run* :

در صفحه *Group Policy* به مسیر پایین بروید:

Start Menu and Taskbar <Administrative Templates <User Configuration

بعد از کلیک نمودن بروی *Start Menu and Taskbar*، در سمت راست پنجره *Group Policy* بروی گزینه *Remove Run menu from Start Menu* دابل کلیک نموده و در تب *Setting* گزینه *Disable* را علامت دار نمایید.

برگرداندن *Folder Option* :

برای برگرداندن *Folder Option* به مسیر زیر در پنجره *Group Policy* بروید:

Windows Explorer <Windows Components <Administrative Templates <User Configuration

بعد از کلیک نمودن بروی *Windows Explorer*، در سمت راست پنجره *Group Policy* بروی *Removes the Folder menu Options menu item from the Tools* دابل کلیک نموده و از تب *Setting* گزینه *Disable* را علامت دار نمایید و بروی کلید *OK* کلیک نمایید .

فعال کردن *task manager*

در *System < Administrative Templates < group policy: User Configuration*

حالا در زیر شاخه *System* بروی *Ctr + Alt + Del* کلیک کن و سپس در سمت راست صفحه *Group Policy* بروی *Remove Task Manager* دابل کلیک نموده و در تب *Setting* گزینه *Disable* را علامت دار کن. بعد از آن بروی کلید *OK* کلیک نموده و پنجره *Group Policy* را ببند.

روش دوم :

مسیر زیر را داخل *note pad* کپی کرده و سپس با نام *task manager.reg* ذخیره کنید و بعد ان را اجرا کنید .

Windows Registry Editor Version .

REG add HKCU\Software\Microsoft\Windows\CurrentVersion\Pol icies\System /v DisableTaskMgr /t REG_DWORD /d /f

استفاده از برنامه ای که در زیر برای شما معرفی کرده ام.این برنامه قادر به انجام کارهای زیر می باشد .

از بین بردن ویروس های *ravmon.exe* و *mdm.exe* و *SCVHOST.exe* و *SVCHOST.ini*

فعال کردن قسمتهای زیر

NoFolderOptions, NoControlPanel, DisableTaskMgr, DisableRegistryTools, DisableCMD

و به حالت پیش فرض برگرداندن قسمتهای زیر

\HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows]

[***CurrentVersion\Explorer\Advanced\Folder\Hidden\NOH IDDEN***

CheckedValue”=dword: “

\HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows]

[***CurrentVersion\Explorer\Advanced\Folder\Hidden\NOH IDDEN***

DefaultValue”=dword: “

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\C]

[***urrentVersion\Explorer\Advanced\Folder\Hidden\SHOW ALL***

CheckedValue”=dword: “

\HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows]

[***CurrentVersion\Explorer\Advanced\Folder\Hidden\SHO WALL***

DefaultValue”=dword: “

http://javedkhalil.com/techBlog/wp-content/uploads/ / /ravmon-removal.rar

بعد از اجرا کردن برنامه سیستم خود را ریستارت کنید .

پاک کردن برنامه ی مخربی که پوشه ها را مخفی (*Super Hidden*) می کند.

نام دقیق این برنامه ی مخرب *Trojan.Win .Delf.aam* است.با زبان برنامه نویسی *Borland Delphi* نوشته شده.

این برنامه ی مخرب تمام پوشه های *Open* شده توسط قربانی را *Super Hidden* می کند و یک نسخه از خودش را با همان نام در همان مسیر کپی می کند که اگر طرف آن را اجرا کند هم *Malware* اجرا می شود و هم محتوی پوشه ی *Super Hidden* نمایش داده می شود !!

همانطور که می دانید برای آشکار کردن فایل ها و پوشه های *Super Hidden* باید ابتدا در *Folder Options\View* روی گزینه ی *Show hidden files and folders* کلیک کنید و پس از آن تیک گزینه ی (*Hide protected operating system files (Recommended* را بردارید و به پیغام امنیتی پاسخ مثبت و شستی *OK* را فشار دهید .این *Malware* به کاربر اجازه ی آشکار کردن پوشه ها و فایل های *Super Hidden* را نمی دهد !

ضمنا ***Registry Tools***، ***Windows Task Manager*** و ***Folder Options*** را ***Disable*** نمی کند .

پر واضح است که این برنامه ی مخرب از آشکار کردن پسوند فایل ها هم جلوگیری می کنه !برای پاک کردن این ویروس می توانید از برنامه ای که نوشتم استفاده کنید.

http://feng .persiangig.com/Programs/Anti% T.Delf.aam. z

نحوه پاک کردن ویروس ***Saldost/ W***

این بد افزار اینترنتی پس از اجرای فایل آن بر روی سیستم کاربر، ابتدا خودش را بر روی سیستم کپی می‌کند و سپس با تغییر دادن کلیدهایی در رجیستری باعث بروز مشکلاتی از جمله باز نشدن ? ***Option Folder***?و مخفی نگه داشتن فایل‌های مخفی می‌شوداز جمله کارهای دیگر این ویروس این است که خودش را در ریشه همه درایوها با نام ? ***autoply.exe***?کپی کرده و در کنار آن فایلی با نام ? ***Autorun.inf***?ایجاد می‌کند.این عمل باعث می‌شود که هر گاه کاربر بخواهد به هر شکلی وارد هر درایوی شود، فایل مربوط به کرم اجرا گردد.نوع ? ***Autorun***?ایجاد شده به گونه‌ای است که اگر فایل ? ***autoply.exe***?که خود کرم است از روی سیستم پاک شده ولی فایل ? ***Autorun.inf***?باقی بماند، با دوبار کلیک کردن بر روی نام درایو پنجره ? ***Open with***?نمایش داده می‌شود و کاربر نمی‌تواند وارد درایو شود. در این حالت با کلیک راست نمودن بر روی نام درایو و انتخاب گزینه ***open***? نیز نمی‌توان وارد درایو شد.

این کرم اینترنتی ایرانی بوده که توسط ضدویروس ایمن شناسایی و پاکسازی می شود و پس از اجرای فایل آن بر روی سیستم کاربر، ابتدا خودش را به صورت زیر بر روی سیستم کپی می نماید:

TEMP%\svchost.exe%

PROGRAMFILES%\Sound Utility\Soundmax.exe%

PROGRAMFILES%\Common Files\Microsoft Shared\MSshare.exe%

WINDIR%\Web\OfficeUpdate.exe%

سپس فایل خود با نام ***svchost.exe*** در مسیر ***TEMP***% را اجرا کرده و برای این که با هر بار راه اندازی سیستم آلوده به طور خود کار اجرا گردد، خود را به شکل زیر در رجیستری ثبت می نماید:

HKLM\SOFTWARE\Microsoft\Windows\CurrentVe rsion\Run

SoundMax = %PROGRAMFILES%\Sound Utility\Soundmax.exe

سپس کلیدهای در رجیستری را به شکل زیر تغییر می دهد:

HKCU\Software\Microsoft\Windows\Curr entVersion\Explorer\Advanced

Hidden = HideFileExt = ShowSuperHidd n =

HKCU\Software\Microsoft\Windows\CurrentVersion\Pol icies\Explorer

Nof olderoptions =

HKLM\Software\Microsoft\Windows\CurrentVersion\Pol icies\E xplorer

Nofolderoptions =

HKLM\SOFTWARE\Policies\Microsoft\Windows NT\ SystemRestore

DisableConfig = ***DisableSR =***

تغییرات فوق باعث بروز مشکلاتی از جمله باز نشدن *FolderOption* و مخفی نگه داشتن فایلهای مخفی می گردد که برای برطرف کردن این مشکلات می توانید برنامه زیر را از سایت ایمن دانلود کرده و ر جیستری خود را پاکسازی نمایید:

http://www.imenantivirus.com/RegRepair.zip

همچنین کلید *IsShortCut* را از مسیرهای زیر در رجیستری پاک می کند:

HKEY_CLASSES_ROOT\lnkfile

HKEY_CLASSES_ROOT\piffile

HKEY_CLASSES_ROOT\InternetShortcut

و کلیدی با نام *Wintek* در مسیر زیر ایجاد می کند:

\ HKEY_CURRENT_USER\Software

و کلید زیر را در آن ایجاد می نماید:

(Install = b?ed? (Dword - Value i s in hex

بعد از انجام کارهای فوق تمام برنامه های موجود در زمانبند ویندوز (دستور *at*) را پا ک کرده و با استفاده از زمانبند ویندوز فایل خود را که با نام *OfficeUpdate.exe* در مسیر *%WINDIR%\Web* وجود دارد هر روز در ساعات 11,30 و 20,30 اجرا می نماید.

یکی دیگر از کارهای این کرم این است که خود را در مسیرهای زیر با نام های فریبنده کپی می کند و از آنجایی که برخی از این مسیرها مخصوص برنامه ها ی شبکه های اشتراک گذاری فایل (یا *P P*) هستند، با این کار امکان انتشار آن در سراسر دنیا از طریق اینگونه برنامه ها فراهم می گردد:

%PROGRAMFILES\Kazaa Lite \My Shared Folder

\PROGRAMFILES%\Kazaa\My Shared Folder%

\PROGRAMFILES%\I cq\Shared Files%

\PROGRAMFILES%\emule\incoming%

\PROGRAMFILES%\Gnucleus\Do wnloads\Incoming%

\PROGRAMFILES%\KMD\My Shared Folder%

\PROGRAMFILES%\Lime wire\Shared%

\PROGRAMFILES%\XPCode%

\C:\Inetpub\ftproot

به علاوه در مسیرهایی که در آنها فایل های از نوع *MP*، *JPG* یا *EXE* وجود داشته باشد، خود را با نام *zfile.exe* کپی می کند. همچنین خود را با نام *setup.exe* و *setlib.exe* در مسیرهای زیر کپی می کند:

\WINDOWS\system??\config\systemprofile\My Documents

\WINDOWS\system??\config\systemprofile\Start Menu\Programs

\WINDOWS\system??\config\systemprofile\Start Menu\Programs\Accessories

\WINDOWS\system??\ config\systemprofile\Start Menu\Programs\Accessories\Entertainment

...\WINDOWS\system??\config\systemprofile\Start Menu\Programs\Startup

WINDOWS\system??\drivers

\WINDOWS\system??\spool\drivers

\?\??×??WINDOWS\system??\spool\drivers\w

این کرم برای اینکه بتواند خود را درون شبکه تکثیر کند، کامپیوترهای موجود در آن را جستجو کرده و با استفاده از درایوهای به اشتراک گذاشته شده، سعی می‌کند خودش را به شکل زیر بر روی آن سیستم‌ها کپی کند:

C$\Documents and Settings\All Users\Start Menu\Programs\Startup\AdobeUpdate.exe

این کار باعث می‌شود که پس از راه‌اندازی آن سیستم‌ها، ویروس به طور خودکار اجرا شده و عملیات تکثیری خود را بر روی آنها انجام دهد.

از جمله کارهای جالب این ویروس این است که خودش را در ریشه همه درایوها با نام *autoply.exe* کپی کرده و در کنار آن فایلی با نام *Autorun.inf* ایجاد می‌کند.

این عمل باعث می‌شود که هر گاه کاربر بخواهد به هر شکلی وارد هر درایوی شود، فایل مربوط به کرم اجرا گردد.

نوع *Autorun* ایجاد شده به گونه‌ایست که اگر فایل *autoply.exe* که خود کرم است از روی سیستم پاک شده ولی فایل *Autorun.inf* باقی بماند، با دوبار کلیک کردن بر روی نام درایو پنجره *Open with* نمایش داده می‌شود و کاربر نمی‌تواند وارد درایو شود. در این حالت با کلیک راست نمودن بر روی نام درایو و انتخاب گزینه *Open* نیز نمی‌توان وارد درایو شد. برای برطرف نمودن این مشکل بایستی فایل زیر را از روی سایت ایمن دانلود نموده و آن را بر روی سیستم خود اجرا نمایید:

http://www.imenantivirus.com/NoAutorun.zip

این کرم فایلی با نام *Important.htm* را در مسیرهای زیر بر روی سیستم کاربر کپی می‌نماید که حاوی جملاتی به زبان فارسی است:

%USERPROFILE%\Desktop

%USERPROFILE%\My Documents

یکی از نشانه‌های ویروس به نمایش درآوردن نواری زرد رنگ در بالای صفحه همراه با جملاتی فارسی با رنگ قرمز است

معرفی برنامه *SmitFraudFix*

***SmitFraudFix* ابزاری است برای از بین بردن ویروسهای مانند *adware* و *malware* و تروجان و پاکسازی رجیستری**

ابتدا برنامه را از لینک زیر دانلود کنید . و ان را روی دسکتاپ قرار بدید .

http://siri.urz.free.fr/Fix/SmitfraudFix.exe.

از صفحه باز شده گزینه *safe mode* را انتخاب کنید . و سپس وارد یوزر خودتان شوید .

برنامه *Smitfraudfix.exe* را اجرا کنید . منتظر بمانید تا صفحه ای آبی ظاهر شود.

سپس یکی از کلید های روی صفحه کلید را فشار دهید.

عدد 2 را انتخاب کنید یعنی *Clean (SafeMode Recommended)* و سپس کلید اینتر را بزنید

با این کار اسکن کردن و *clean* کردن سیستم اغاز می شود .

بعد از انجام این مراحل ابزار *Disk Cleanup tool* اجرا می شود و فایلهای بی مصرف را از روی سیستم پاک می کند .

بعد از *Disc Cleanup* پنجره زیر نشان داده می شود .

Do you want to clean the registry **؟**

ایا شما می خواهید پاکسازی کنید رجیستری را : کلید *Y* را فشار دهید تا رجیستری بازسازی شود .

Replace infected file **؟**

ایا جایگزین کند فایلهای الوده را که شما کید *Y* را فشار می دهید .

در این هنگام سیستم احتیاج به یکبار راه اندازی دارد . که سیستم به طور اتوماتیک راه اندازی می شود .

اگر این اتفاق نیفتاد شما خودتان به صورت دستی این کار را انجام دهید .

در این هنگام فایلی به نام *rapport.txt* در درایو *c* ایجاد می شود که گزارشاتی از کارهای انجام گرفته را به شما می دهد .

همچنین این ابزار فایل های *wininet.dll* را نیز چک میکند مبادا الوده باشند .

نحوه از بین بردن تروجان *Win /Agent.AEC* یا ویروس *Soundmix.exe*

همون طور که می دونید اخیرا ویروسی به نام *Soundmix.exe* انتشار یافته و باعث الوده شدن بسیاری از سیستم های خانگی و اداره ها شده است . قصد دارم در این قسمت نحوه پاک کردن این تروجان را اموزش دهم .

شایع ترین راه انتقال این ویروس حافظه های فلش می باشد. هرچند که باز کردن برخی سایت های آلوده نیز می تواند این ویروس را در سیستم مستقر سازد

این ویروس با دستکاری رجیستری ، هر بار که ویندوز راه اندازی می شود خود را اجرا می کند. با اجرای هر فایل اجرایی در ویندوز نیز این فایل اجرا خواهد شد و پس از اجرا *Processes* آن را به هیچ عنوان نمی توان خاتمه داد.

این ویروس اجازه دیدن فایل های پنهان را به کاربر نمی دهد و فایل هایی که مخفی شوند دیگر قادر به مشاهده نخواهند بود. دسترسی به برخی سایت ها ممکن نمی باشد و این ویروس با اجرای خود منجر به ایجاد سربار روی سیستم ، کندی دستگاه ، بسته شدن ناخواسته برخی برنامه ها و احیانا بوت شدن خود بخود کامپیوتر می گردد.

همچنین با آلوده کردن حافظه های فلشی که به دستگاه متصل می گردند ، سعی به انتشار خود می کند.

راههای شناخت این تروجان

برای این که متوجه شوید که ایا سیستم شما الوده به این تروجان است یا نه از طریق فشرن همزمان سه کلید

Alt + Ctrl + Delete **وارد** ***Task Manager*** **شوید و سپس به تب** ***Processes*** **رفته و در صورتی که فایل اجرایی** ***Soundmix.exe*** **در حال اجرا باشد سیستم شما به این تروجان آلوده شده است.**

راه دیگر شناسایی این تروجان عدم نمایش پسوند فایلهاست

از طریق منوی ***Folder Option*** **و فعال کردن گزینه** ***files and folder Show Hidden*** **و تایید آن در صورتی که پسوند فایلها نمایش داده نشوند سیستم شما به این تروجان الوده شده است.**

این تروجان در درایو ویندوز و در مسیر زیر قرار میگیرد .

C:\WINDOWS\system \soundmix.exe

فایل کتابخانه ای ان نیز در مسیر زیر قرار میگیرد

C:\WINDOWS\system \dllcachezipexr.dll

این تروجان علاوه بر کاهش سرعت سیستم باعث عدم نمایش پسوند فایلها و جلوگیری از دسترسی شما به رجستری ویندوزتان می شود و باعث دزدیده شدن اطلاعات سیستم شما خواهد شد.

این ویروس خودش را در ***system*** **با نام** ***soundmix.exe*** **و به صورت یک فایل سیستمی قرار می دهد .**

یک کپی در ***dllcache*** **با نام** ***zipexr.dll*** **نگه می دارد و اگر شما این فایل را پاک کنید بعد از این که سیستم بالا می اید هیچ فایل** ***exe*** **رو اجرا نمی کند .**

سه قسمت را در رجیستری دستکاری می کند

Software\Microsoft\Windows\CurrentVersion\Run

exefile\shell\open\command

SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer \Advanced\Folder\Hidden\SHOWALL

بعد از اتصال حافظه فلش خود به سیستم روی آیکون حافظه که ایجاد شده است کلیک راست کنید. در حالت عادی گزینه های زیر بایستی نمایان گردد :

Open **و** ***Explore*** **و** ***Search*** **و** ***Autoplay***

در غیر این صورت اگر نوشته هایی عجیب و غریب مشاهده گردد بیان گر وجود ویروس می باشد

راه پاکسازی ***Soundmix.exe*** **یا تروجان** ***Win /Agent.AEC***

در حال حاضر انتی ویروسهایی که توانایی شناسایی این ویروس را دارند آنتی ویروس *NOD* و کسپر اسکای و بیدیفندر می باشند شایان ذکر است این انتی ویروس ها نیز فقط در صورتی که به روز باشد توانایی پاکسازی *Soundmix.exe* را خواهد داشت .

در ضمن می توانید از برنامه ای که برای پاک کردن این ویروس درست شده است استفاده کنید .

http://mahdi .parsaspace.com/ANTI% SOUNDMIX.rar

حل مشکل *open with*

اگر بر روی هر درایو کلیک می کنید پنجره *open with* باز می شود به دلیل پاک شدن فایلی می باشد که مسئول باز کردن درایو می باشد .

شما می توانید از برنامه زیر برای حل این مشکل استفاده کنید . البته قبل از ان باید ویروس *autoran* را از درایو های خودتون پاک کرده باشید . بعد از اجرا کردن برنامه باید چند دقیقه منتظر باشید تا برنامه کار خود را انجام دهد . بعد از اینکه کارش به اتمام رسید به شما پیغام می دهد . پس صبور باشید .

http://www.techsupportforum.com/sectools/sUBs/Flash_Disinfector.exe

نحوه پاک کردن ویروس *Jeefo/ Virus Win* یا *SVCHOST.EXE*

بعلت وجود ویروسی مخرب به اسم *Jeefo* که با نام *SVCHOST.EXE* البته در شاخه دیگری غیر از فایل اصلی ساکن می شود و اقدام به خرابکاری تمام فایلهای اجرایی *exe* می کند .

اکثر انتی ویروس ها *SVCHOST.EXE* را به عنوان ویروس می شناسند . در حالی که *SVCHOST.EXE* ویروس نیست بلکه ویروس فایل دیگری می باشد که خود را به این نام در اورده است.

این ویروس باعث می شود که برنامه ها درست اجرا نشوند . و طولانی بودن زمان الودگی سیستم باعث از کار افتادن سیستم عامل می شود.

نحوه پاک کردن ویروس

ابتدا سعی کنید *System Restore* را غیر فعال کنید .

برای این کار ابتدا روی *my computer* راست کلیک کنید و سپس *properties* را بزنید از پنجره باز شده به تب

***System Restore* رفته و تیک گزینه *all drives Turn off System Restore on* را بزنید و بعد پنجره را *ok* کرده و به سوال پرسیده شده جواب مثبت دهید .**

حال ابتدا با زدن سه کلید ترکیبی *ctrl + alt + delete* وارد *Task Manager* شوید و به تب *Processes* رفته و از اوجا فایل *SVCHOST.EXE* در حال اجرا توی ویندوز را پاک می کنیم .

البته در تب *Processes* شما حداقل 4 تا یا بیشتر *SVCHOST.EXE* در حال اجرا می بینید که باید با برنامه های مدیریت پروسه های *Task Manager* بتونید این فایل را تشخیص دهید . زیرا این برنامه ها مسیر پروسه های اجرایی را در *Task Manager* نشان می دهند . این فایل بیشتر خود را با نام یوزر که در ان هستید (*Log On*) اجرا می کند .

حال به مسیر *C:\WINDOWS* رفته و فایل *SVCHOST.EXE* را پاک می کنیم .

البته شما نباید فایل اصلی *SVCHOST.EXE* را که در مسیر *C:\WINDOWS\System* قرار دارد را پاک کنید .

بعد از این کار سیستم را ریستارت کنید .

سپس سیستم را در حالت *safe mode* راه اندازی کرده و انتی ویروس *jeefogui* را اجرا کنید .

ممکن است بعد از این عملیات بعضی از فایلهای *exe* شما از کار بیفتند که شما باید دوباره برنامه انها را نصب کنید .

انتی ویروس *jeefogui*

http://mahdi .parsaspace.com/jeefogui.rar

پاک کردن ویروسی که از طریق باهو مسنجر منتشر می شود

عملکرد این ویروس

1- در ابتدا ویروس صفحه شخصی اینترنت اکسپلورر (*Page Default IE*) را به یک سایت تغییر می دهد. در این صورت به هیچ طریق امکان عوض کردن آن وجود نخواهد داشت. بعد از هر باز باز کردن یک صفحه وب جدید، ویروس مجددآ خود را در سیستم شما کپی می کند.

غیر فعال کردن *Task Manager* و رجیستری

ایجاد فایلهایی با نام های *svhost.exe , svhost .exe , internat.exe*

نحوه از بین بردن این ویروس و مشکل

ابتدا با استفاده از روشهای گفته شده در بالا *Task Manager* و رجیستری را فعال کنید .

اتصال خود به اینترنت را قطع کنید .

حال برای برگرداندن صفحه نخست مروگر خود به حالت قبل وارد رجیستری شوید .

ابتدا وارد منوی استارت شوید و روی گزینه *run* کلیک کنید و عبارت *regedit* را نوشته تا وارد رجیستری شوید .

میسر های زیر را با دقت پیدا نموده و در آنها وارد شوید حال اسم سایت مورد نظر را که در *home page* شما قرار گرفته است را پاک کرده و اسم سایت خودتان را بنویسید مثلا [*/URL="http://www.forum.p world.com*]

سپس به *internet option* رفته و این کار را هم انجام دهید *se current- use default -use blank*

HKEY_CURRENT_USER\SOFTWARE\Microsoft\Internet Explorer\Main

HKEY_ LOCAL_MACHINE\SOFTWARE\Microsoft\Internet Explorer\Main

HKEY_USERS\Default\Software\Microsoft\Internet Explorer\Main

انتی ویروس *Y.V.Remover*

http://mahdi .parsaspace.com/Y.V.Remover.zip

رفع مشکل غیر فعال شدن *Home Page* اینترنت اکسپلورر

1 . در کادر محاوره ای *Run* عبارت *Regedit* را تایپ کنید و از روی کیبرد کلید *Enter* را فشار دهید تا محیط ویرایش رجیستری ظاهر شود .

2 . به مسیر زیر بروید و 2 متغییر *DWORD* با نام های *RunOnceComplete* و *RunOnceHasShown* به ارزش 1 بسازید .

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Internet Explorer\Main

3 . محیط ویرایش رجیستری را ببندید و مجددا در کادر محاوره ای ***Run*** عبارت ***inetcpl.cpl*** را تایپ کنید و شستی ***OK*** را فشار دهید تا کادری با عنوان ***Internet Properties*** ظاهر شود .

4 . در قسمت ***Home Page*** آدرس مورد علاقه ی خود را تایپ کنید و شستی ***OK*** را فشار دهید تا تنظیمات دلخواه ذخیره شود .

5 . اکنون ***Internet Explorer*** را اجرا کنید و لذت ببرید .

کسانی که این مشکل را از راه اصولی حل کرده اند و اکنون دوست دارند روش فوق را تست کنند ، مراحل زیر را دنبال نمایید ...

1 . در کادر محاوره ای ***Run*** عبارت ***inetcpl.cpl*** , تایپ کنید و شستی ***OK*** را فشار دهید تا کادری با عنوان ***Internet Properties*** ظاهر شود .

2 . در زبانه ی ***Advanced*** دکمه ی ***Reset*** را فشار دهید تا کادر دیگری با عنوان ***Reset Internet Explorer Settings*** خودنمایی کند .

3 . مجددا روی دکمه ی ***Reset*** کلیک کنید تا تمام تنظیمات ***IE*** به حالت پیش فرض بر گردد .

4 . اکنون روش دوم را جهت تغییر ***Home Page*** تست کنید.

اموزش از ***MB_Danger***

نحوه از بین بردن ویروس ***services.exe***

متاسفانه اکثر ویروسهایی که جدیدا به وجود می ایند همنام پروسه های مربوط به سیستم عامل می باشند به همین دلیل تشخیص انها هم برای کاربران و هم برای انتی ویروس ها نسبتا مشکل شده است .

و از کار انداختن انها نیز قدری سخت شده است .

و همین عامل می تواند یکی از نقاط ضعف سیستم عامل های ماکروسافت محسوب شود .

فعالیت های ویروس *services.exe*

اولین کاری که این ویروس انجام می دهد خودش را با نام فایلهایی که در یک فولدر است در می اورد و فایلهای فولدر را مخفی می کند و یک فایل با نام همان فولدر می سازد که دارای پسوند *exe* می باشد .

و به فولدر هایی که مخفی می کند علاوه بر خصلت *hidden* خصلت سیستمی هم می دهد .

سپس به وسیله *windows policy* برنامه های *regedit* و *cmd* و *msconfig* و *taskmanager* رو از کار می اندازد(گاهی اوقات هنگام استفاده از دستور *cmd* کامپیوتر را ریستارت هم میکند) در بعضی مواقع از قسمت *option folder* گزینه *view* رو مخفی میکند.

و اجازه دسترسی به بعضی از گزینه های مدیریتی رو بطور کامل از بین میبرد .

و حتی با تعویض ویندوز هم فایلها از حالت مخفی خارج نخواهند شد . به خاطر این که با تعویض ویندوز هنوز اثرات این ویروس در دیگر درایو ها وجود دارد و تنها با کلیک کردن روی یکی از انها ویروس فعال شده و دوباره همه جا را الوده می کند .

نحوه از بین بردن ویروس *services.exe*

برای از بین بردن این ویروس ابتدا کدهای زیر را داخل *note pad* کپی کرده و با نام و پسوند *rescue.bat* در مسیر در مسیر *c:* ذخیره نمایید.

@echo off

try:

del c:\windows\services.exe

if exist c:\windows\services.exe goto try

حالا به منوی *start* رفته و روی گزینه *run* کلیک کنید و عبارت*regedit* را تایپ کرده و *ok* را بزنید. تا وارد محیط رجیستری شوید .

حال به مسیر زیر بروید.

HKEY_LOCAL_MACHINE\system\currentcontrolset\servic es\eventlog

روی فایل *image path* دوبار کلیک کرده و در این پنجره به جای *%systemroot%\system \services.exe* عبارت *c:\rescue.bat* را تایپ کنید.

ویندوز را *restart* کنید.

دوباره به منوی *start* رفته و برنامه *run* را اجرا کرده و *regedit* را تایپ کرده و *ok* را بزنید.

حال به مسیر زیر بروید.

HKEY_LOCAL_MACHINE\system\current control set\services\eventlog

روی فایل *image path* دوبار کلیک کرده و در این پنجره به جای *c:\rescue.bat* عبارت *%systemroot%\system \services.exe* را تایپ کنید.

فایلهای مسیرهای زیر را پاک کنید .

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\serenta

و

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\Curr entVersion\Run

و

"***services.exe"="%windir%\services.exe***"

حال تغییرات زیر را انجام دهید.

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon\shell

shell **را از مسیر بالا باز کنید.حال به جای** ***explorer.exe*** %***windir%\services.exe*** **عبارت** ***explorer.exe*** **را تایپ کنید یعنی به عبارت ساده ته اون را پاک کنید.**

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon\userinit

userinit **را از مسیر بالا باز کرده و به جای عبارت** ***C:\WINDOWS\system \userinit.exe,,%windir%\service s.exe***

عبارت ,,%***windir%\services.exe*** **را حذف نمایید یعنی مسیر به صورت زیر در می آید.**

C:\WINDOWS\system \userinit.exe

به پوشه ***temp*** **رفته و در صورت وجود فایل** ***Service.exe*** **ان را پاک کنید .**

حالا آنتی ویروس های ***kaspersky*** **و** ***nod*** **را** ***update*** **نمایید و سیستم را به طور کامل در حالت** ***safe mode*** **ویروس یابی کنید .**

ضمناً بهتر است بعد از ***update*** **و ویروس یابی ویندوز خود را عوض کنید.**

anti spyware **برای از بین بردن ویروس** ***services.exe***

این انتی ***spyware*** **یکی از بهترین ها برای از بین بردن ویروس** ***services.exe*** **می باشد .**

http://www.spywareremove.com/download/Free-SpyHunter-Scanner_p_s_.exe

فقط توجه داشته باشید که این *anti spyware* ویروس *services.exe* را پیدا می کند و برای از بین بردن انها حتما باید این برنامه کرک شده باشد .

این برنامه کرک شده نیست . اگه کسی کرک اونا پیدا کرد لطف کنه بده بزارمش اینجا تا دوستان دیگه هم استفاده کنند .

مهم : نحوه برگردوندن فایلهایی که به صورت سیستمی مخفی شده اند.

همون طور که می دونید ویروس *services.exe* فایلهای شما را به صورت سیستمی مخفی می کند و شما قادر به دیدن اونها نیستید . شما می توانید از روش زیر به فایلهای خودتون دسترسی داشته باشد .

کافی است نام درایو و مسیر فایل خود را در مسیر زیر وارد کرده و سپس این مسیر را در *run* کپی کرده و سپس *ok* را بزنید تا فایلهای شما نمایان شوند.

attrib -r -a -s -h drive:\file path

(به جای *drive* نام درایو حاوی فایل مخفی را بنویسید و به جای *file path* مسیر فایل را به طور کامل بنویید .)

روشی برای تشخیص این که فایلهای درون فولدر حذف شده اند یا اینکه به حالت سیستمی در امده اند

گاهی اوقات وقتی به داخل یکی از فولدرهایی که تعداد زیادی فایل درون ان داریم رجوع می کنیم با کمال تعجب متوجه می شویم که فولدر ما خالی است و هیچ یک از فایلهایی که قبلا وجود داشتند دیگر وجود ندارند .

در این قسمت روشی را به شما اموزش می دهم که با این روش می توانید متوجه شوید که ایا فایلهای شما واقعا حذف شده اند یا این که به حالت سیستمی مخفی شده اند .

برای اینکه بتونید فایلها را ببینید از منوی *Start* روی گزینه *run* کلیک کرده و سپس عبارت *cmd* را تایپ کنید و سپس *ok* را بزنید

بعد از باز شدن محیط *cmd* در ان تایپ کنید *name_of_the_folder dir /A* با این کار تمامی فایلهایی که به حالت سیستمی در امده اند قابل روئت خواهند بود . و شما متوجه خواهید شد که فایلها حذف نشده اند . و با استفاده از روش بالا می توانید انها را از حالت سیستمی خارج کنید .

نکته : *name_of_the_folder* نام فولدری می باشد که اطلاعات شما در ان مخفی شده است .

با این برنامه هم می تونید تا حدودی فایلهای *Hidden* شده خودتون را *UnHidden* کنید .

http://tetra.persiangig.com/Prog/Delphi/UnHiden.rar

بازگردانی سریع فایلهای مخفی شده

این هم روشی برای کسانی که می خواهند به سرعت به فایلهای مخفی خودشون دسترسی پیدا کنند .

برای این کار کافی است دستورات زیر را داخل *Notepad* کپی کنید و بعد ان را با نام و پسوند *mahdi.bat* ذخیره کنید و بعد ان را اجرا کنید . چند لحظه منتظر بمانید تا فایلهای مخفی نمایان شوند .

تذکر : با این روش فایلهای سوپر هایدن نیز قابل روئیت خواهند بود .

attrib -s -h C:*.* /s /d

attrib -s -h d:*.* /s /d

attrib -s -h E:*.* /s /d

attrib -s -h f:*.* /s /d

attrib -s -h g:*.* /s /d

attrib -s -h h:*.* /s /d

ویروس ***Win /PSW.Agent.NDP***

این ویروس باعث غیرفعال شدن گزینه ***folders show hidden files and*** در ***folder option*** می شود و باعث عدم نمایش فایلهای مخفی می شود و اجازه نمی دهد کاربرها فایلهای مخفی را از حالت مخفی بیرون بیاورند .

این ویروس با دستکاری رجیستری ویندوز باعث می شد که شما نتونید تنظیمات ***hidden file and folder*** را تغییر دهید .

به محض تغییر دادن این قسمت و خارج شدن از ان تنظیمات به حالت پیش فرض خود برمیگردند .

البته این ویروس خرابکاریهای دیگری هم انجام می دهد اول اینکه داخل تمام درایوهای شما یه فایل ***autorun.inf*** می سازد که درایوهای هارد شما را ***autorun*** می کند .

دوم اینکه دوباره داخل تمام درایوها یک فایل به نام ***ntde ect*** می سازد که شما به محض اینکه فلاپی وارد سیستم کنید یا فلش یا ***mp pleyer*** را به کامپیوتر متصل کنید یک کپی از خودش به صورت ***hidden*** وارد دستگاه شما یا فلاپی شما می کند که شما متوجه ان نمی شوید .

البته فایل ***ntde ect*** خیلی شبیه فایل ***ntdetect*** هست که داخل درایو ***C*** وجود دارد و برای بالا امدن ویندوز ضروری می باشد .

مواظب باشید این دو فایل را اشتباه نگیرید .

سوم اینکه با اجرای فایل ***avpo.exe*** به شما اجازه نمیدهد که فلش یا ***mp pleyer*** یا هر چیز دیگه رو از پورت ***USB***، ***safe remove*** کنید .

نحوه پاک کردن ویروس ***Win /PSW.Agent.NDP***

در حالت ***safe mode*** وارد ویندوز شوید . (با زدن دکمه ***F*** قبل از بالا آمدن ویندوز حالت ***safe mode*** را انتخاب کنید)

پنجره ***Task Manager*** را باز کنید (***Ctrl-Alt-Delete***) و برنامه های زیر را در صورت اجرا ببندید .

wscript.exe : اگر در حال اجرا بود آن را ببندید (***End process***)

avpo.exe : اگر در حال اجرا بود آن را ببندید (***End process***)

از قسمت ***start*** برنامه ***Run*** را اجرا کنید و در عبارت ***cmd*** را در آن تایپ کنید و ***enter*** را بزنید .

در این قسمت در خط فرمان برنامه ، دستور زیر زیر را تایپ کنید و ***enter*** را بزنید .

del c:\autorun.* /f /a /s /q

این دستور را برای درایوهای دیگر اجرا کنید . با این دستور تمام فایلهای***autorun*** موجود ***delete*** می شود .

در این مرحله در خط فرمان ***c:*** دستور زیر را تایپ کنید تا وارد پوشه ***system*** شوید :

C:\cd windows\system

C:\windows\system

در ادامه دستور زیر را تایپ کنید و آنرا اجرا کنید .

dir /a avp*.*

در این قسمت هر فایلی به نامهای ***avp .dll*** و ***avpo.exe*** و ***avp .exe*** دیده شد آنرا پاک کنید .

attrib -r -s -h avpo.exe

del avpo.exe

بعد از این مراحل تمام پنجره ها رو ببندید و برنامه ***registry*** را اجرا کنید :

(***Run \regedit***)

مسیر زیر را دنبال کنید :

HKEY_CURRENT_USER \ SOFTWARE \ Microsoft \ Windows \ CurrentVersion \ Run

در این قسمت هر کلیدی که به نام *avpo.exe* بود را *delete* کنید .

در برنامه *registry* قسمت *edit* گزینه *Find*را کلیک کنید و عبارت *ntde ect* را جستجو کنید. تمام کلیدهای پیدا شده را *delete* کنید .

این کار را برای فایل *avpo.exe* نیز انجام دهید و تمام کلیدهای پیدا شده را*delete* کنید .

در آخر کار سراغ کلید زیر بروید و مقدار *CheckedValue* را برابر 1 قرار دهید .

HKEY_LOCAL_MACHINE/SOFTWARE/Microsoft/Windows/CurrentVersion

Explorer/Advanced/Folder/Hidden/SHOWALL

ویروس *kernel.exe*

***kernel* ویروسی است که هر چند دقیقه یکبار با *error* ی که در زیر تصویر ان را قرار داده ام ظاهر می شود .اکثر کاربران به این ویروس گرفتار شده اند .**

در واقع این یک ویروس نیست زیرا کار مخربی روی سیستم انجام نمی دهد . در واقع یک برنامه می باشد که شباهتی به ویروس دارد و به همین دلیل هیچ یک از انتی ویروس ها قادر به شناسایی و پاک کردن ان نیستند . حتی قوی ترین و به روز ترین انتی ویروس ها .

این ویروس از طریق صفحات *html* که از اینترنت ذخیره می کنید به وجود می اید .

این ویروس سه فایل با نام های *kernal.vbs* و *kernal.exe* و *systems.exe* دارد که هر سه فایل در پوشه *C:\WINDOWS\system* ذخیره می شوند .

در واقع این ویروس خود را جزء پروسه های سیستم عامل نیز می داند و در *task manager* در تب *processes* با نام *kernel.exe* در حال فعالیت می باشد .

این ویروس همه ی فایل های *HTML* و *Htm* رو آلوده میکند و به آخر فایل ها کدهای مخرب *Vbscript* رو که چند تا فایل با نام ها *kernel.exe* و *kernel.vbs* است را ایجاد میکند .

این ویروس حتی با تعویض سیستم عامل هم از بین نخواهد رفت .

از اثرات این فایل آلوده:

1- ارورهای پشت سر هم

2- باعث پایین آمدن سرعت کامپیوتر

3- باعث پایین آمدن سرعت اینترنت

4- دادن اطلاعات مثل یوزر و پسورد اینترنتتان به شخص هکر

5- آلوده کردن فایلهای *HTML*

نحوه پاک کردن ویروس *kernel.exe*

برای پاک کردن این ویروس شما باید ابتدا با زدن کلید های ترکیبی *ctrl + alt + delete* وارد *task manager* شوید و به تب *processes* رفته و فایلی با نام *kernel.exe* را پاک کنید .

سپس به مسیر زیر رفته *C:\WINDOWS\system* رفته و دو فایل با نام *kernel* و یک فایل با نام *Systems* را پیدا کرده و پاک کنید .

توجه داشته باشید شما در صورتی می توانید این فایلها را پاک کنید که پروسه *kernel.exe* را از *task manager* پاک کرده باشید . در غیر این صورت اجازه پاک شدن را به شما نخواهد داد.

سپس به منوی استارت رفته و عبارت *msconfig* را در *run* تایپ کنید و در قسمت *startup* اگر فایلهای بالا وجود دارند تیک انها را بردارید و سپس کامپیوتر را ریستارت کنید دوباره چک کنید که ویروس در حافظه بار نشده باشد .

بعد به ***internet temporary*** از طریق مسیر زیر رفته و تمام محتویات ان را خالی کنید .

Documents and Settings\\Local Settings\Temporary Internet Files:

برنامه برای از بین بردن این ویروس

http://rapidshare.com/files/ /Setup.exe.html

www.radsoftwareteam.com/Downloads/Files/rad-kk.exe

http://softestan.persiangig.com/ya n/Setup.exe

نحوه پاک کردن ویروس ***BronTok.A*** :

در زیر به برخی از ویژگی های این ویروس اشاره می کنیم :

1 . ***Folder Options*** را حذف می کند !

2 . ***Registry Tools*** را قفل می کند !

3 . ***Task Manager*** نمی تواند فایل های مربوط به این ویروس را ***End*** کند !

4 . پس از اجرا شدن ، محتویات ***My Documents*** را نمایش می دهد !

5 . اگر در کادر محاوره ای ***Run*** عبارت ***CMD***، ***Regedit***، ***msconfig***، ***Regedt*** را تایپ کنید ، سیستم بلافاصله ***Restart*** می شود !

6 . اگر روی گزینه ی ***Log Off*** یا ***Turn Off Computer*** کلیک کنید ، سیستم ***Restart*** می شود !

7 . آیکون این ویروس شبیه آیکون یه پوشه است !

همانطور که می دانید فایل های ***lsass.exe***، ***winlogon.exe*** و ***services.exe*** از فایل های سیستمی بوده و همیشه در حال اجرا هستند ...

اگر شما برنامه ی ***Process Master*** را اجرا کنید ، می بینید که این فایل ها در پوشه ی ***System*** قرار دارند .

اما اگر ویروس ***BronTok.A*** روی سیستم شما نصب باشد ، خواهید دید که سه تا فایل دیگر با همین نام ها در

حال اجرا هستند !!

یعنی دو تا *winlogon.exe* ، دو تا *lsass.exe* و دو تا *services.exe* !

اما به راحتی میشود فهمید که کدام ویروسند و کدام فایل اصلی ویندوز ...

آن سه تا فایلی که مربوط به ویروس میشوند ، در پوشه ای غیر از *System* قرار دارند .<