بسم الله الرحمن الرحیم

آشنایی با مسیرهای Start up که ویروس ها و تروجان ها در آن ها مخفی می شوند

همان طور که می دانید ، ویروس ها و تروجان ها در هنگام بالا آمدن سیستم عامل ویندوز ، خود را به صورت خودکار راه می اندازند.آن ها خود را با کپی کردن در پوشه ها و مسیرهایی که ویندوز در هنگام شروع خود تمام محتویات آن ها را اجرا می کند ، در هنگام بالا آمدن ویندوز همراه با آن اجرا می شوند.در این مقاله در مورد این مسیرها توضیح داده شده است و تقریبا اکثر مسیرهای مهم گفته شده است.

1) پوشه Start up ویندوز:
ویندوز تمامی مواردی را که در پوشه Start up ویندوز هستند را ، باز می کند.این پوشه در مسیر Start-All Programs-Start up واقع شده است.یاد آور می شوم که ویندوز به طور کامل همه ی محتویات این پوشه را اجرا نمی کند ودر اکثر موارد آن ها را باز می کند.بین اجرا شدن و باز شدن تفاوت بسیار زیادی است.به عنوان مثال اگر شما یک سند Word را در این پوشه بگذارید ، در هنگام بالا آمدن ویندوز برنامه ی Word اجرا شده و سند مورد نظر را باز می کند ، یا اگر شما یک صفحه ی اینترنتی یا مثلا صفحه ی علاقه مندی ها را در این جا بگذارید ، بعد از بالا آمدن ویندوز ابتدا Internet Explorer یا مرورگر مورد استفاده ی شما ، اجرا شده و صفحه مورد نظر را باز می کند.

2) رجیستری ویندوز:
در رجیستری ویندوز قسمت های زیادی وجود دارند که در هنگام بالا آمدن ویندوز ، فایل هایی را که مسیر شان در آن مشخص شده است ، اجرا می شوند.در ادامه هر یک از این مسیرها توضیح داده خواهند شد.یکی از این قسمت ها ، قسمت Run است. ویندوز تمام دستورالعمل هایی را که در قسمت Run رجیستری است را اجرا می کند.مواردی که در قسمت Run و سایر قسمت هایی که در ادامه آمده اند می توانند ، فایل های اجرایی باشند و یا برنامه های خاصی آن ها را به عنوان یک سند یا فایل خود آن ها را باز کنند(مانند یک سند Word).

آدرس Run:
HKEY_Current_User-Sotfware-Microsoft-Windows-CurrentVersion-Run

و

HKEY_Local_Machine-Sotfware-Microsoft-Windows-CurrentVersion-Run

است.

3) رجیستری ویندوز:
در قسمت RunServices که یکی از قسمت های دخیل در اجرای فایل ها در هنگام بالا آمدن ویندوز در رجیستری است ، تمام فایل هایی که مسیرشان در آن مشخص شده است اجرا می شوند.
4) رجیستری ویندوز:
قسمتی دیگر از رجیستری ویندوز که تمام محتویات آن در هنگام بالا آمدن ویندوز اجرا می شوند ، قسمت RunOnce است.
5) رجیستری ویندوز :
قسمت دیگری از رجیستری در هنگام بالا آمدن ویندوز ،که محتویات آن اجرا می شود ، قسمت RunServicesOnce است.(نکته ی مهم که باید به آن توجه کنید این است که ویندوز از دو قسمت RunOnce استفاده می کند که یکی از آن ها تنها برای یک بار اجرای شد یک برنامه است ، که معمولا بعد از نصب هر نرم افزار اجرا می شود)
6) رجیستری ویندوز:
ویندوز تمام دستور العمل هایی را که در مسیر
HKEY_CLASSES_ROOT\exefile\shell\open\command "%1" %*
آمده اند را اجرا می کند.همه ی دستورات و فایل ها در این قسمت ، باز یا اجرا می شوند.
آدرس های دیگری از رجیستری که در هنگام بالا آمدن ویندوز ، تمام دستورالعمل ها و فایل های موجود در آن ها اجرا یا باز می شوند در زیر آمده اند:

```
[HKEY_CLASSES_ROOT\exefile\shell\open\command] ="\"%1\" %*"
[HKEY_CLASSES_ROOT\comfile\shell\open\command] ="\"%1\" %*"
[HKEY_CLASSES_ROOT\batfile\shell\open\command] ="\"%1\" %*"
[HKEY_CLASSES_ROOT\htafile\Shell\Open\Command] ="\"%1\" %*"
[HKEY_CLASSES_ROOT\piffile\shell\open\command] ="\"%1\" %*"
[HKEY_LOCAL_MACHINE\Software\CLASSES\batfile\shell\open\comm
and] ="\"%1\"
%*"
[HKEY_LOCAL_MACHINE\Software\CLASSES\comfile\shell\open\com
mand] ="\"%1\"
%*"
[HKEY_LOCAL_MACHINE\Software\CLASSES\exefile\shell\open\comm
and] ="\"%1\"
%*"
[HKEY_LOCAL_MACHINE\Software\CLASSES\htafile\Shell\Open\Com
mand] ="\"%1\"
%*"
[HKEY_LOCAL_MACHINE\Software\CLASSES\piffile\shell\open\comm
and] ="\"%1\"
%*"
```

اگر Key های گفته شده دارای مقدار "*% "\1%"\" نشان داده شده نباشند ، و به "*% "\1% somefilename.exe"\" این صورت تغییر داده شده اند ، آن ها به صورت خودکار مسیر فایل را از شما می خواهند.

7) Batch File:

ویندوز تمام دستورالعمل هایی را که در دسته فایل Winstart (Winstart Batch File) هستند را اجرا می کند.(شاید این فایل برای شما کمی نا آشنا به نظر برسد.شما می توانید خودتان آن را ایجاد کنید.نکته ضروری دیگر ،نام پوشه ی ویندوز است که در بعضی از نسخه های ویندوز ، با نام WinNT یاد می شود)نام کامل این فایل WINSTART.BAT است.

8) فایل های سری بندی شده یا Initialization :

در پوشه ی ویندوز ، فایلی به نام WIN.INI قرار دارد که در خط =Run موجود در این فایل ، می توان دستورالعمل هایی را قرارداد تا ویندوز در هنگام بالا آمدن آن ها را اجرا کند.

9) فایل های سری بنده شده یا Initialization:

در فایل WIN.INI در خط =LOAD آن ، می تواند دستورالعمل هایی را قرارداد تا ویندوز در هنگام بالا آمدن ، آن ها را اجرا کند.

همچنین دستوراتی را که در خط =shell در System.ini در پوشه ی ویندوز آمده اند نیز اجرا می شوند

```
[boot]
Shell=explorer.exe C:\windows\<filename>
```

فایل مشخص شده همراه با explorer.exe در هنگام بالا آمدن ویندوز اجرا خواهد شد.

10) دوباره راه اندازی یا Re-lunching:

اگر برنامه هایی مانند Internet Explorer در هنگام خاموش شدن ویندوز در حال اجرا باشند ، ویندوز دوباره در هنگام Start up بعدی آن ها را اجرا خواهد کرد.البته ویندوز کمتر می تواند این کار را برای برنامه های ساخته شده شرکت های دیگر به غیر از شرکت مایکروسافت اجرا کند ، اما به راحتی با برنامه هایی مانند Internet Explorer و یا Windows Explorer و یا برنامه هایی که مدیریت فایل ها و پوشه را انجام می دهند کار می کند.اگر شما مرورگر اینترنت اکسپلورر را باز کنید و سپس ویندوز را خاموش کنید ، در Start up بعدی به طور خودکار این مرورگر برای شما باز خواهد شد.(اگر همچین اتفاقی برای شما روی نداد ، ممکن است که این قابلیت بر روی سیستم شما خاموش شده باشد ، برای راه اندازی این قابلیت توصیه می شود از نرم افزار Tweak UI شرکت مایکروسافت که رایگان نیز می باشد استفاده کرده و قابلیت Remember Explorer Settings را روشن کنید.البته اسم این قابلیت در نسخه های مختلف ویندوز ، متفاوت است)

11) زمان بندی کارها یا Task Scheduler:

ویندوز تمام دستورات autorun هایی را که در Task Scheduler مشخص شده اند را اجرا می کند(یا تمامی برنامه Task Scheduler که جایگزین Task Scheduler هستند). Task Scheduler یکی از قسمت های ویندوز است که امکان اجرا شدن کارها و یا برنامه ها را در زمانی مشخص بر عهده دارد.

12) دستورالعمل های دومی:
برنامه هایی را که ویندوز در هنگام بالا آمدن اجرا می کند ، برنامه های آزاد و جداگانه برای اجرا شدن هستند.از دید فنی ، این برنامه ها آن برنامه هایی نیستند که ویندوز خود به صورت اولیه آن را اجرا می کند ، اما گاهی کاملا غیر قابل تشخیص از برنامه هایی که به صورت خودکار اجرا می شوند ، هستند.مانند برنامه های آنتی ویروس که در هنگام بالا آمدن ویندوز همراه با پروسه ای مانند winlogon.exe اجرا می شود.winlogon.exe جزو برنامه های از پیش تعیین شده ویندوز است که اجرا می شود اما آنتی ویروس یک برنامه ی اضافه شده توسط کاربر است اما به نظر می آید که ویندوز خود آن ها اضافه کرده است.

13) روش Explorer.exe:
ویندوز در هنگام بالا آمدن ، explorer.exe را اجرا می کند که در پوشه ویندوز یا System32 قرار دارد.حال اگر فایلی با همین نام و در مسیر C:\explorer.exe ایجاد کنیم که یک تروجان یا ویروس باشد ، ویندوز گاهی ممکن است آن را به جای explorer.exe اصلی اجرا کند.اگر این فایل خراب شده باشد ، در بالا آمدن ویندوز در زمانی دیگر اختلال ایجاد خواهد شد.
همان طور که گفته شد اگر این فایل explorer.exe یک تروجان یا ویروس باشد ، در این صورت ما بدون دستکاری هیچ گونه فایل یا مقداری در رجیستری توانستیم در بالا آمدن ویندوز دخالت کنیم.

14) دیگر روش های اضافه کردن:
HKEY_LOCAL_MACHINE\Software\Microsoft\Active Setup\Installed Components
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\Currentversion\explorer\Usershell folders
دو آدرس اول توسط تروجان ها بیشتر مورد استفاده قرار می گیرند.

Icq Inet
[HKEY_CURRENT_USER\Software\Mirabilis\ICQ\Agent\Apps\test]
"Path"="test.exe"
"Startup"="c:\\test"
"Parameters"=""
"Enable"="Yes"

[HKEY_CURRENT_USER\Software\Mirabilis\ICQ\Agent\Apps\]
This key specifies that all applications will be executed if ICQNET Detects an Internet Connection.

[HKEY_LOCAL_MACHINE\Software\CLASSES\ShellScrap] ="Scrap object"
"NeverShowExt"=""
همان طور که دیدید شما می توانید به راحتی با دستکاری مقادیر بالا و گذاشتن مقادیر دلخواه خود به جای آن ها ، برنامه های مورد نظر خود را در هنگام بالا آمدن ویندوز اجرا کنید.

در این مقاله حدود 14 مسیر که بیشترین نقش را در اجرای فایل ها در هنگام بالا آمدن ویندوز دارند ، توضیح داده شدند که عمدترین آن ها مربوط به آدرس هایی در رجیستری می باشند که بیشتر مورد استفاده قرار می گیرند.

در آخر از مدیر سایت

نیز تشکر می کنم.

Copyright© by Siahacker
2005-2006 All Rights Reserved
Email:Siahacker@gmail.com