روشهای اجرای خودکار برنامه‌ها
و
جلوگیری از برنامه‌های جاسوسی

در سیستم عاملهای ویندوز

Auto Startup Methods in Microsoft Windows

تهیه و تنظیم:

Little Hacker

July 2004

به نام ایزد یکتا

تفاهم نامه : اطلاعات موجود در این مقاله می‌تواند در راستای خیر یا شر مورد استفاده قرار گیرد. نگارنده این مقاله جز به اهداف خیرخواهانه نمی‌اندیشد و طبیعی است که مسئولیت نحوه استفاده از این اطلاعات بر عهده خواننده می باشد. نگارنده هیچگونه مسئولیتی در رابطه با صدمه های احتمالی ناشی از اشتباه و یا مقاصد شوم خواننده را نمی‌پذیرد و مسئولیت آن تماما بر عهده خواننده می‌باشد.

هدف : در این مقاله سعی شده تا روشهای اجرای اتوماتیک برنامه‌ها را در سیستم عامل ویندوز بطور کامل تشریح نموده تا خوانندگان عزیز حتی‌الامکان خود قادر بررسی وجود و از کار انداختن تروجانها و کرمهای اینترنتی باشند.

نکته : علی رغم تعداد زیاد مقالات مشابه از این سری، لیکن اکثر آنها ناقص بوده و ضعفهای موجود نگارنده را به تهیه این مقاله واداشت.

یادآوری : است که قبل از اعمال هر تنظیمی از فایلهای سیستمی خود نسخه پشتیبان تهیه نمایید تا در صورت اشتباه یا بروز مشکلات با جایگزینی آنها مساله مرتفع گردد.

طبقه بندی روشها:

به طور کلی روشهای اجرای خودکار برنامه‌ها در سیستم عامل ویندوز را می‌توان به شکل زیر طبقه بندی نمود.

I. اجرا در محیط *Dos* و قبل از بالا آمدن کامل *Windows*: در این شکل از روشهای اجرای خودکار، برنامه معمولا توسط یک فایل دستوری[1] فراخوانی می‌شود و بیشتر مرتبط با *Windows* های قدیمی است. در این روش برنامه باید در کنسول قابل اجرا باشد و دارای هیچ پنجره‌ای نباشد.

II. اجرا از طریق فایلهای سیستمی آغاز کننده: بعضی از این فایلها که معمولا با پسوند *ini*. شناخته می‌شوند توانایی اجرای برنامه‌ها با شروع *Windows* را دارند. این روش نیز بیشتر در ویندوزهای قدیمی‌تر رایج است.

III. اجرا از طریق پوشه[2] *Startup* : این روش بیشتر مورد استفاده نرم‌افزارهای مجاز می‌باشد.

IV. اجرا از طریق محضرخانه ویندوز[3]: که خود به قسمتهای مختلفی تقسیم شده و از روشهای جدید محسوب می‌شود و بیشتر از هر روش دیگر مورد استفاده تروجانها و کرمهای اینترنتی قرار می‌گیرد.

V. سایر روشها : روشهایی که برنامه به طور مستقیم توسط *Windows* فراخوانی نمی‌شود.

اکنون که با یک طبقه‌بندی نسبی در این زمینه آشنا شدیم به توضیح تک تک آنها می‌پردازیم:

I. اجرا از طریق فایلهای دستوری ویندوز:

تعدادی از فایلهای دستوری هستند که با بالا آمدن ویندوز به طور اتوماتیک اجرا می‌شوند و بنابراین میتوانند فایلهای دیگر را نیز به اجرا در آورند. البته این دسته از فایلها بیشتر برای کپی یا حذف قایلهای دیگر بکار می‌روند. همانطور که ذکر شد برنامه‌هایی که با این روش اجرا می‌شوند، معمولا فاقد پنجره ارتباطی با کاربر هستند و خود به صورت اتوماتیک تمام کارهای مورد نیاز خود را انجام می‌دهند (تروجانها و کرمها نیز می‌توانند در این گروه قرار بگیرند).

الف) *AutoExec.bat*: از جمله معروفترین فایلهای دستوری از این دسته می‌باشد که قبل از بالا آمدن کامل ویندوز اجرا می‌شود. این فایل در شاخه اصلی در پارتیشن بوت قرار دارد. (معمولا *C:\Autoexec.bat*)

ب) *WinStart.Bat*: این فایل که در شاخه نصب ویندوز *(%Windir%\winstart.bat)* قرار گرفته مثل هر فایل دستوری دیگر عمل می‌کند.

[1] *Batch File*
[2] *Folder*
[3] *Registry*

II. اجرا از طریق فایلهای سیستمی آغازکننده:

در این روش با استفاده از یکی ار سه فایل *ini*. زیر می‌توان برنامه‌ای را با شروع ویندوز به طور اتوماتیک ارا کرد :

الف) *Win.ini* : در این فایل که در شاخه نصب ویندوز(*%Windir%\win.ini*) قرار دارد، دو محل برای فراخوانی وجود دارد که به صورت ریرمی‌توان به آنها دست یافت:

```
[Windows]
Load = نام و مسیر فایل
Run = نام و مسیر فایل
```

اگر نام فایلی در یکی از دو قسمت بالا قرار بگیرد با شروع ویندوز اجرا خواهد شد.

ب) *System.ini* : این فایل نیز در شاخه نصب ویندوز(*%Windir%\System.ini*) قرار گرفته و به صورت ریرمی‌توان به فراخوانی آن دست یافت:

```
[Boot]
Shell = نام و مسیر فایل
```

فایل مشخص شده در واقع پوسته ویندوز را به آن معرفی می‌کند که اگر به *Explorer.exe* یا *%Windir%\Explorer.exe* تنظیم شده باشد مشکلی وجود ندارد. در صورتی که به فایل دیگری اشاره کند ممکن است فایل مذکور یک تروجان یا کرم باشد (در صورتی که از نرم‌افزار Talisman یا نرم‌افزارهای مشابه استفاده می‌کنید نگران نباشید) اما در صورتی که مقدار شل به صورت زیر تنظیم شده باشد آنگاه File.exe حتما یک تروجان یا کرم است و باید آنرا پاک کنید (در Safe Mode):

Shell = Explorer.exe File.exe

ج) *Wininit.ini*: همانند دو مورد قبلی این فایل نیز در شاخه نصب ویندوز (*%Windir%\System.ini*) قرار داشته و بیشتر مورد استفاده برنامه‌های نصب[1] قرار می‌گیرد. اگر نام فایلی در آن قرار گرفته باشد فقط برای یکبار توسط *Wininit.exe* اجرا شده سپس توسط ویندوز پاک می‌شود. در مثال زیر فایل ذکر شده تهی می‌شود که نتیجه

```
[Rename]
Null = نام و مسیر فایل
```

[1] *Setup*

آن حذف فایل مذکور است. فرایند فوق بدون هیچ‌گونه ارتباطی با کاربر و به طور کاملا محفیانه انجام می‌شود.

III. اجرا از طریق پوشه ***Startup*** :

به این پوشه می‌توانید به راحتی از منوی استارت و دسترسی داشته باشید.

StartMenu > Programs > Startup

تمام فایلهای اجرایی موجود در این پوشه بلافاصله پس از بالا آمدن ویندوز اجرا خواهند شد. معمولا دو پوشه وجود دارد که یکی مخصوص کاربر فعلی و دیگری برای تمامی کاربران است. با وجود مشخص بودن محل آنها، می‌توان از محضرخانه ویندوز محل دقیق این پوشه‌ها را به صورت زیر استخراج کرد.

```
[HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\Shell Folders]
Startup="C:\windows\start menu\programs\startup"

[HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\User Shell Folders]
Startup="C:\windows\start menu\programs\startup"

[HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\explorer\User Shell Folders]
"Common Startup"="C:\windows\start menu\programs\startup"

[HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\explorer\Shell Folders]
"Common Startup"="C:\windows\start menu\programs\startup"
```

اگر مسیرهای مشخص شده به پوشه دیگری اشاره کنند تمام فایلهای اجرایی آن پوشه بطور خودکار اجرا می‌شوند.

IV. اجرا از طریق محضرخانه ویندوز:

این روش خود به چند گروه کاملا مجزا تقسیم می‌شود:

الف: ***Registry/Run*** :

فایلهای که نام آنها در کلیدهای زیر ذکر شده باشند به طور اتوماتیک با بالا آمدن ویندوز اجرا خواهند شد.

```
[HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run]                    <all>
" نام و مسیر فایل اجرا شونده"= هر نام دلخواه
[HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\RunOnce]
" نام و مسیر فایل اجرا شونده"= هر نام دلخواه
[HKEY_LOCAL_MACHINE\ Software\Microsoft\Windows\CurrentVersion\RunServices]          <98>
" نام و مسیر فایل اجرا شونده"= هر نام دلخواه
[HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Run]                   <all>
" نام و مسیر فایل اجرا شونده"= هر نام دلخواه
 [HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\RunServices]         <98>
" نام و مسیر فایل اجرا شونده"= هر نام دلخواه
[HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\RunServicesOnce]      <98>
" نام و مسیر فایل اجرا شونده"= هر نام دلخواه
 [HKEY_LOCAL_MACHINE\System\ CurrentControlSet\Services]                            <NT>
" نام و مسیر فایل اجرا شونده"= هر نام دلخواه
```

در این روش می‌توان حتی پسوند فایل اجرایی را به پسوند دلخواه هم تغییر داد و فایل اجرایی کماکان اجرا خواهد شد.

ب: *Registry /Shell Open* :

پسوند فایلها ویندوز را در نحوه رفتار با آنها یاری می‌کند. مثلا با کلیک روی یک فایل متنی (با پسوند *.txt*) ویندوز ابتدا پسوند آنرا تشخیص می‌دهد و سپس با مراجعه به بانک اطلاعاتی خود در می‌یابد که بایستی ابتدا برنامه *Notepad.exe* را اجرا کند و فایل مذکور را به عنوان ورودی به آن معرفی کند. یک تروجان یا کرم می‌تواند با تنظیم چنین مشخصاتی باعث اجرای خود شوند. هر چند چنین تنظیماتی برای هر پسوندی می‌توانند اعمال شوند ولی از آنجا که بیشتر تروجانها و کرمها به کامپیوترهای سرور[1] اهمیت زیادی می‌دهند و پشت چنین کامپیوترهایی ممکن است تا ساعتها کسی ننشیند و یا با فایلهایی مثل *.txt* یا *.bmp*. یا غیره کار نکند برای بالابردن ضریب اطمینان از پسوند فایلهایی استفاده می‌کنند که خود ویندوز آنها را به دفعات اجرا کند ! بدین ترتیب با هر بار اجرای آن فایلها توسط ویندوز شانسی دوباره در اختیار تروجان قرار می‌گیرد !!!

برای کسب اطمینان از اینکه این تنظیمات برای چنین فایلهایی صحیح می‌باشند باید مسیرهای ذکر شده زیر در ویرایشگر رجیستری به صورت ذیل باشد:

```
[HKEY_CLASSES_ROOT\ exefile\Shell\open\Command]
Default = “”%1” %*”
 [HKEY_CLASSES_ROOT\comfile\Shell\open\Command]
Default = “”%1” %*”
[HKEY_CLASSES_ROOT\batfile\Shell\open\Command]
Default = “”%1” %*”
[HKEY_CLASSES_ROOT\piffile\Shell\open\Command]
Default = “”%1” %*”
[HKEY_CLASSES_ROOT\htafile\Shell\open\Command]
Default = “”%1” %*”
[HKEY_LOCAL_MACHINE\Software\Classes\exefile\Shell\open\Command]
Default = “”%1” %*”
[HKEY_LOCAL_MACHINE\Software\Classes\comfile\Shell\open\Command]
Default = “”%1” %*”
[HKEY_LOCAL_MACHINE\Software\Classes\batfile\Shell\open\Command]
Default = “”%1” %*”
[HKEY_LOCAL_MACHINE\Software\Classes\piffile\Shell\open\Command]
Default = “”%1” %*”
[HKEY_LOCAL_MACHINE\Software\Classes\htafile\Shell\open\Command]
Default = “”%1” %*”
```

در صورتی که با *Export* یک فایل *.reg* تهیه کرده‌اید در محتویات آن باید به جای Default=“”%1” %*” مقدار @="\"%1\" %*" باشد.در صورتی که شامل نام فایل اجرایی باشد، آن فایل اجرایی را یک تروجان یا کرم بشمارید.

[1] *Server*

مثلا اگر تنظیمات به صورت *Default = "File.exe %1 %* "* باشد *File.exe* را تروجان فرض کنید. جالب است بدانید این یکی از روشهایی بود که تروجان معروف *Sub7* از آن استفاده می‌کرد.

ج. *Registry /ActiveX*

این هم یکی دیگر از روشهای اجرای اتوماتیک تروجانها و کرمهاست. بازیابی در این مورد کمی وقت‌گیرتر می‌باشد. در این روش تروجان/کرم یک زیرکلید با نام دلخواه در مسیر زیر از رجیستری ایجاد می‌کند و نام و مسیر فایل اجرایی خود را در مقداری با نام *Stubpath* ذخیره می‌کند. ممکن است مقادیر دیگری هم در این زیرکلید ایجاد کند که یا تنظیمات داخلی آن است یا برای رد گم کردن از آن استفاده می‌نماید.

```
[HKEY_LOCAL_MACHINE\Software\Microsoft\Active Setup\Installed Components\نام دلخواه ]
StubPath = نام و مسیر فایل اجرایی
```

V. سایر روشها :

در میان سایر روشها فقط به روش آلوده کردن فایلهای اجرایی ویندوز و *ICQ* و سواستفاده از ویندوز بسنده می‌کنیم:

الف: آلوده‌کردن فایلهای اجرایی ویندوز:

اگر با تروجانها کار کرده باشید حتما با نامهایی چون *Binder* یا *Wrapper* و ... آشنا هستید. این فایلها تروجان را به یک یا چند فایل اجرایی پیوند می‌زنند و یک فایل جدید (با ظاهری ریبنده) ایجاد می‌کنند که با اجرای آن تمامی فایلهای پیوند شده اجرا خواهند شد. چنین روشی می‌تواند برای آلوده‌سازی فایلهای اجرایی ویندوز مورد استفاده قرار گیرد. مثلا آلوده سازی *Explorer.exe* باعث خواهد شد بدون نیاز به اعمال تنظیم خاص برای اجرای اتوماتیک، تروجان یا کرم به طور حتمی اجرا شود. با وجود اینکه نگارنده تا کنون با چنین موردی در عمل برخورد نکرده‌است ولی چنین امکانی از لحاظ نظری وجود داشته و ممکن است مورد استفاده تروجانهای خصوصی که بین عموم توزیع نشده‌اند مورد استفاده قرار گیرند. بهترین و سریعترین راه بررسی آن اطلاع دقیق از حجم فایل *Explorer* مربوط به نسخه ویندوز شماست. البته خوشبختانه در ویندوزهای جدید فکری به حال این موضوع شده و سیستم محافظ فایل ویندوز این بررسی را د رمورد تمامی فایلهای سیستمی ویندوز برای شما انجام می‌دهد. کافی است در حالیکه لوح فشرده نصب ویندوز در *CD-Rom* قرار دارد، تایپ کنید *sfp /scannow* و عملیات به صورت خودکار شروع می‌شود.

ب: سوء استفاده از نرم‌افزار *ICQ*:

این روش فقط بعلت کاربرد زیاد آن در تروجانهای مختلف تشریح می‌شود، زیرا که در ایران (برخلاف بقیه جاهای دنیا) *ICQ* کاربران زیادی ندارد و فقط آندسته از خوانندگانی که برنامه‌هایی نظیر *ICQ Lite* در کامپیوتر خود نصب کرده‌اند باید نگران این قسمت باشند زیرا که دارای این قابلیت هستند که با ایجاد اتصال به اینترنت هر فایل دلخواهی را اجرا کند. برای بررسی اینکه چه فایلهایی به اجرا در می‌آیند باید نظری به مسیر زیر از رجیستری بیاندازید. تمامی فایلهای ذکر شده در مسیر زیر به محض ارتباط با اینترنت اجرا خواهند شد:

```
[HKEY_CURRENT_USER\Software\Mirabilis\ICQ\Agent\Apps\نام دلخواه ]
“Path” = ″نام و مسیر فایل اجرایی″
```

ج. سوء استفاده از ضعف ویندوز در فراخوانی و اجرای *Explorer*:

همانطور که ذکر شد در ویندوزهای *95* ، *98* و *ME* فایل *Explorer* که پوسته ویندوز را تشکیل می‌دهد توسط فایل *System.ini* فراخوانی می‌شود و در ویندوزهای سری *NT* به جای پوسته از مسیر زیر در رجیستری هنگام بالا آمدن ویندوز فراخوانی می‌شود:

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\WindowsNT\CurrentVersion\Winlogon\Shell

این فراخوانی بدون هیچ مسیری است و فقط نام فایل را ذکر می‌کند. مشکل از اینجا ناشی می‌شود که ویندوز باید هنگام بالا آمدن به دنبال *Explorer* بگردد. جستجو ابتدا در مسیر جاری انجام می‌گردد. اگر فایل مورد نظر پیدا نشد آنگاه در مسیرهای تعریف شده جستجو ادامه می‌یابد. این مسیرها در ویندوز *95*، *98* و *ME* در فایل *Autoexec.bat* بصورت زیر تعریف می‌شوند SET PATH = مسیر

در ویندوزهای سری NT در مسیر زیر از رجیستری می‌باشد

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SessionManager\Environment\Path

چون جستجو به صورت پی در پی و یکی پس از دیگری است لذا اگر تروجان یا کرمی خود را بصورت *C:\Explorer.exe* کپی کند به جای *Explorer* اصلی در *%windir%\explorer.exe* بدون هیچ اشکالی اجرا می‌شود. تجربه شخصی نگارنده ثابت می‌کند که این روش برخلاف تمامی روشهای قبلی حتی در حالت *Safe Mode* هم کارآیی دارد و نیز تروجان در ظاهر هیچ ردی هم از خود به جای نمی‌گذارد !

نکات:

در پایان ذکر نکات ذیل خالی از لطف نیست:

1- روشهای ذکر شده فقط به وشهای اجرای خودکار برنامه‌های اجرایی[1] پرداخته و از بررسی بالا آمدن سایر فایلهای سیستمی[2] صرف نظر نموده‌است.

2- یک تروجان یا کرم ممکن است از ترکیب چند روش با هم استفاده کند.

3- با استفاده از *Sysedit.exe* و *MsConfig.exe* (وحتی *DrWatson* در ویندوزهای *95*، *98* و *ME*) می‌توانید برخی از (و نه همه) روشهای ذکر شده را به راحتی بررسی کنید. اما روشهایی که در تروجانها به عنوان *Unknown* یا *Invisible* و مشابه آن لقب گرفته‌اند در واقع همانهایی هستند که با برنامه‌های فوق قابل شناسایی نیستند و هیچ چیز جای بررسی دستی شما را نخواهد گرفت.

4- در صورت یافتن آثاری از تروجان یا کرم همیشه قبل از پاک نمودن تنظیمات اجرای خودکار آن مطمئن شوید که پروسه آن در حال اجرا نیست. زیرا تقریبا تمامی تروجانها قبل از بسته شدن حداقل یکبار تنظیمات خود را برای اطمینان از اجرای مجدد چک می‌کنند. در صورت پیش آمدن مورد آخر باید با دیسکت *Boot* بالا آمده و فایل *C:\Explorer.exe* را حذف نمود. در بقیه موارد بالا آمدن در حالت *Safe Mode* برای انجام کارهای بعدی کافی است.

5- تروجانهایی دیده شده‌اند که از روشهای مختلف *RunOnce* استفاده می‌کردند و یا پس از بالا آمدن اثرات خود را برای اجرای اتوماتیک پاک می‌نمودند. بدین ترتیب هنگام بررسی در استتار کامل به سر می‌بردند و درست قبل از خاموش شدن ویندوز مجددا تنظیمات لازم را اعمال می‌نمودند. در این موارد اگر کامپیوتر به طور فیزیکی *reboot* شده بطوریکه ویندوز *Shutdown* نکرده باشد این شانس وجود دارد که تروجان با بالا آمدن مجدد ویندوز دیگر اجرا نشود. از آنجا بعضی از تروجانها و کرمها تقریبا هوشمند عمل کرده و فعالیت سایر برنامه‌ها را زیر نظر می‌گیرند لذا باز بودن برنامه *regedit* هنگام *reboot* فیزیکی توصیه می‌شود. هر چند در این موارد معمولا بالا آمدن در حالت *Safe Mode* هم برای بررسی کارساز خواهد بود.

6- در پایان بر نصب و به روز نگهداری آنتی- ویروس و دیوارآتشین تاکید می‌گردد.

در پناه حق

[1] exe, bat, com, vbs, js & …
[2] dll, sys, vxd & …