نویسنده : GodVB

تاریخ : ۱۳۸۷/۳/۲۳

منابع : خودم و Help ویندوز ☺ و تشکر فراوان از دوست عزیز Lord-viper

امیدوارم که تونسته باشم به معلوماتتون اضافه کنم در صورت هرگونه مشکل منو مطلع کنین .

ID : ahax92

www.godvb.blogfa.com

www.forum.iranled.com

شاید به نظر شما وقتی که از طریق Folder Option تیک Hide Extensions را بر میدارید ویندوز پسوند تمام فایل ها را نشان میدهد ولی کاملا در اشتباه هستید و غافل از اینکه پسوند هایی خاصی هستند که به هیچ وجه دیده نمیشوند .

«« PIF FILE :
فایل های میانبری برای اجرای دستورات DOS با آیکن های خاص .
مثلا شما پسوند یک فایل اجرایی را به pif تغییر دهید . به راحتی خواهید دید که پسوند آن ازبین میرود و به هیچ وجه دیده نمی شود . و حتی آیکن آنهم تغییر میکند و از همه جالب تر اینکه برنامه تان هم کار میکند . حالا اگر این فایل یک کیلاگر ، تروجان و یا یک ویروس باشد . . . ؟!!!
در ادامه به پسوند هایی که این امکان (اجرا شدن برنامه و از بین نرفتن اصل آن) را میتوانند به فایل مان بدهند و طرز Hide کردن پسوند فایل میپردازم .البته پسوندهای زیادی وجود دارند که قابلیت Hide شدن دارند اما نمیتوانند اصل فایل اجرایی مان را حفظ کنند .این چند پسوند پایین از این مدل پسوندها هستند :

۱. Url
۲. Lnk
۳. و . . . . .

«« Scrap File :
پسوند آنها shs هست که قابلیت Hide شدن رو دارند .
يك كپي از notepad.exe بگيريد و آن را روي desktop خود قرار دهيد .
WordPad را باز كنيد. روي notepad.exe كليك كنيد و آن را به سمت سند باز شده WordPad بكشيد. روي notepad.exe كليك كنيد و آن را به عقب به سمت desktopبكشيد. فايلي را كه ايجاد شده است (Scrap) به Readme.txt تغيير نام دهيد.

حالايك آيكن كه نشان دهنده سند متني است و فايلي با نام مشخص readme.txt بر روي desktop شما وجود دارد كليك كردن بر روي فايل فوق باعث مي‌شود notepad باز شود. اگر اين فايل يك Trojan باشد، شما فريب خورده‌ايد و توسط آنچه كه يك فايل متني بي‌خطر بنظر مي‌رسيد آلوده شده‌ايد.

«« COM File :
این پسوند هم مربوط به MS DOS هست . اصل فایل مان را حفظ می کند ، آیکن آن را هم تغییر میدهد ولی قابلیت Hide شدن پسوندش را ندارد .

»» SCR File :
این پسوند مخصوص اسکرین سیورها است . این پسوند قابلیت Hide شدن را ندارد ولی میتواند اصل فایل اجرایی را حفظ کند و آیکن آن هم به هیچ وجه تغییر نمیکند ، یعنی آیکن فایل SCR مان آیکن همان فایل EXE مان است و هیچ تغییری نمیکند .

»» BATCH File :
که شامل دستورات سیستم است . بازهم میتوانیم از طریق تبدیل پسوند فایل مان به این پسوند ، اصل فایل را حفظ کرده . این پسوند آیکن فایل مان را هم تغییر میدهد .

»» CMD File :
مربوط به Command Script است .این پسوند مانند بقیه هم اصل فایل مان را حفظ و آیکن آن را هم عوض می کند .

در فایل های CMD , BATCH , PIF آیکن ها براساس خود ویندوز تغییر میکند ، بهترین چیزی که برای هر ویروس لازم است، و با باز شدنش هم یک error تقلبی میدیم و میگیم فایل خرابه . وقتی روی سیستم من یک پک ویستا نصب باشد حتما همه آیکن ها هم تغییر میکنند، حالا سرور یاکوزا با آیکن فایل های JPG اورجینال هم که باشه از دو کیلومتری مشکوک میزنه . منم دنبال راهی بودم که بشه آیکن فایل مون رو براساس خود ویندوز بدیم و یا حداقل واسه پسوندش یک کاری بکنم مثلا اینطوری دیگه نشه lopez.jpg.exe . تا به نتایج بالا و پایین رسیدم .
بهرحال ، من این روش رو توضیح میدم براساس SCR مثال ها رو میزنم .
من فایل سرورمو با پسوند CMD و یا . . . درست میکنم که اول کار خیلی سه نباشه . بعد از اینکه اجرا شد میخوام سرورمو با ایکن فایل های DLL بندازم تو سیستم Victim . که دیگه اصلا نفهمه . حالا طرز کار :
پسوند سرور رو که CMD میدم . دلیل : چون BATCH , PIF مال اجرا کردن دستورات هستن و آیکن شون هم تابلویه ، کسی که به کامپیوتره وارد باشه سریع بهشون مشکوک میشه ، ولی CMD نه تازه طرف ذوق میکنه و اجراش میکنه که چیه ؟
واسه اینکه بخوام ایکون سرور افتاده تو سیستم طرف تغییر بدم ، پسوند SCR رو انتخاب کردم .
وقتی سرور اجرا شد منم باید توی رجیستری سیخ کاری هایی رو انجام بدم .

۱. پسوند فایل های SCR رو باید Hide کنم تا طرف با اسم gmtel.dll گمراه بشه .
۲. آیکن فایل ها رو براساس ویندوز تعیین کنم .

شرح مراحل :

۱. به این مسیر در رجیستری میرم
HKEY_CLASSES_ROOT\scrfile .
یک مقدار از نوع string value توی همون کلید SCR FILE میسازیم به اسم NeverShowExt . واسه Hide پسوند .

۲. یک کلید به اسم DefaultIcon میسازم و
مقدارشو %SystemRoot%\System32\shell32.dll,-154 (درصد بعد از ۱۵۴- رو باید اول بزارین)میذارم و هی کپی ازش میگیرم تو system32 .
دیگه عمرا بفهمه .

خوب اگه به چیزهایی که گفتم عمل کرده باشین تمومه .
همیشه حواستونو جمع کنین!! ، کجا تمومه؟ ؛ یک فایل با ایکن فایل های DLL که وقتی روش کلیک راست میکنی می بینی نوشته Install . خوب باید همه جوانب رو در نظر گرفت .
حالا واسه اینکه کپ خود Dll بشه و بیل گیتس هم نتونه تشخیص بده ☺ باید این کار ها رو انجام بدین :

۱. در این مسیر HKEY_CLASSES_ROOT\scrfile در کلید scrfile یک مقدار از نوع string value با نام NoOpen میسازیم ، از اسمش هم معلومه چیکار میکنه البته روی بیشتر ویندوز ها اصلا تاثیری نداره .
۲. یک مقدار از نوع string value با نام InfoTip میسازیم ، وقتی ماوس رفت روی فایلمون چیزایی رو که باید تو تول تیپش نشون بده توی این مقدار نگهداری میشه . این مقدار رو درونش قرار بدین :
prop:FileDescription;Company;FileVersion;Create;Size

البته این متن هایی رو که نشون میده بستگی به خودتون داره که موقعه کامپایل چی براش بنویسین .

۳. یک مقدار دیگه بازهم از نوع string value با نام TileInfo بسازین موقعه ای که برنامه تون در حالت Tiles باشه زیر اسم فایلتون با رنگ خاکستری دیده میشه رو مشخص میکنه . بهش این مقدار رو بدین :
prop:FileVersion;FileDescription

۴. از زیر کلیدهای scrfile ، کلید shell را انتخاب بکنید ، اگه توش هر کلیدی غیر open بود پاکش کنید . در کلید open کلیدی دیگر به نام command وجود دارد که مقدار آن را %۱ بدهید (توی تایپ شاید جای درصد و عدد یک جابجا شده باشه، دقت کنید ) بخاطر اینکه برنامه خودش باز بشه و با برنامه دیگه ای باز نشه .

خداییش ویندوز چیزه باحالیه ☺