ترفندهای هکری

افشاي هكرها
هدف ما اين است كه با افشاي "ترفندهاي هكر" استفاده كنندگان از اينترنت با دانش و ابزارهاي مورد نياز، آمادگي بهتري پيدا كنند تا فريب ترفندهاي هكر را نخورند.

پسوندهاي پنهان فايلهاي ويندوز
ممكن است از اين موضوع آگاهي نداشته باشيد، اما حتي اگر به ويندوز بگوييد كه تمام پسوندهاي فايل را نشان دهد، هنوز هم فايلهايي وجود دارند كه بطور پيش فرض مخفي شده‌اند. همچنين هر برنامه نصب شده‌ايي مي‌تواند پسوندها را پيكربندي كند تا پنهان شوند. در اينجا در مورد چگونگي انجام اين كار و همچنين دليل اينكه چرا برخي از پسوندهاي پنهان مي‌توانند براي تعدادي از كاربرهاي كامپيوتر خطرناك باشند، مثالهايي آورده شده است. به فرض اينكه شما قبلا ويندوز explorer را براي نشان دادن تمام پسوندهاي پيكربندي كرده‌ايد.

پسوندهاي SHS
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 desktop بكشيد. فايلي را كه ايجاد شده است (Scrap) به Readme.txt تغيير نام دهيد.

حالا يك 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. اگر اجازه نمايش اين پسوند داده مي شد شما فريب فايل Readme.txt.shs را نمي‌خورديد.

پسوندهاي PIF
اگر سعي كنيد تا notepad.exe را به anything.txt.pif تغيير نام دهيد، تنها فايلي با نام anything.txt روي desktop خود خواهيد ديد. و اين بدين دليل است كه PIF پسوند ديگري است كه ويندوز بطور پيش فرض پنهان مي‌كند. اگر شما فايل را اجرا كنيد برنامه اجرا خواهد شد، به خاطر اينكه ويندوز پسوندهاي PIF را اجرا خواهد كرد حتي اگر آنها فايلهاي اجرايي باشند.

پسوندهاي SCR
پسوند ديگري كه بايد مراقب آن بود SCR است. كپي notepad.exe خود را به notepad.scr تغيير نام دهيد و روي آن كليك كنيد. Notepad به عنوان يك فايل اجرايي اجرا خواهد شد. بسياري از افراد توسط هكرهايي فريب مي‌خورند كه account يك قرباني را بدست آورده‌اند. هكر email يا هر نوع پيغامي را به تمام دوستان قرباني مي‌فرستد كه "اين صفحه نمايش جديد و بامزه را ببينيد از خنده روده بر خواهيد شد!" از آنجايي كه اين پيغام از يك منبع مطمئن آمده، اكثر افراد فريب خورده و فايل SCR را اجرا مي‌كنند كه در نهايت به هكري ختم مي‌شود كه به كامپيوتر شما متصل شده است.

فرمانهاي خطرناكي كه مي‌توانند گنجانده شوند
پسوندهاي ميانبر PIF
برخي از پسوندهاي پنهان فايل قادرند به سادگي با فرمانهاي پنهان شده‌اي كه مي‌توانند براي سيستم شما مخرب باشند برنامه‌ريزي شوند. اين يك آزمايش ساده است:

دكمه راست ماوس خود را روي desktop كليك كنيد و New و سپس Shotcut را انتخاب نماييد. در Command line تايپ كنيد:

format a:/autotest

Next را كليك كنيد. در "Select a name for the shortcut" تايپ كنيد: readme.txt سپس Next را كليك كنيد. يك آيكن notepad را انتخاب كرده و Finish را كليك كنيد. حالا شما در desktop خود فايلي با نام readme.txt و با آيكن notepad داريد. مطمئن شويد كه در درايو شما ديسكي است كه از دست دادن آن براي شما اشكالي ندارد و روي آيكن كليك كنيد. فايلي كه شما روي آن كليك كرده‌ايد درايو A: را فرمت خواهد كرد. البته آيكن هكر درايو ديگري را مورد هدف قرار خواهد داد يا ممكن است نامي همچون 'game.exe' و فرماني براي حذف كردن دايركتوري ويندوز شما يا (deltree /y C:*.*) كل درايو C شما داشته باشد. اگر پسوند PIF پنهان نشود، قادر به فريب شما نخواهد بود.

پسوند SHS
فايلهاي Scrap نيز مي‌توانند فرمانهاي گنجانده شده را پنهان كند. اين يك آزمون ساده است: از notepad.exe يك كپي بگيريد و آن را روي desktop خود قرار دهيد. Wordpad را باز كنيد.Notepad.exe را كليك كنيد و آن را به سمت سند باز شده

wordpad بكشيد. روي Edit كليك كنيد و Package Object و سپس Edit package را انتخاب كنيد. روي Edit و سپس Command Line كليك كنيد.

در كادر، دستوري مانند format a:/autotest را تايپ كنيد و روي OK كليك كنيد. آيكن نيز مي‌تواند از اين پنجره تغيير يابد. از پنجره خارج شويد، اين كار سند را به روز خواهد كرد. روي notepad.exe كليك كنيد و آن را به عقيب به سمت Desktop بكشيد. فايلي را كه ايجاد شده (Scrap) به Readme.txt تغيير نام دهيد.

حالا شما آنچه را كه شبيه يك فايل متني است داريد. اگر اين فايل اجرا شود درايو A: را فرمت خواهد كرد. همانگونه كه در مثال بالا براي پسوندهاي ميانبر PIF ديده شد، هكر مي‌تواند از فرمانهاي خطرناكتري استفاده كند.

روشهاي Trojan در هنگام راه اندازي

روشهاي راه اندازي استاندارد

اكثر افراد از راههاي متفاوتي كه هكرها براي راه اندازي فايلهاي Trojan استفاده مي‌كنند آگاه نيستند. اگر هكري كامپيوتر شما را با يك Trojan آلوده كند، نياز به انتخاب يك روش راه‌اندازي خواهد داشت، بگونه‌اي كه در زمان راه‌اندازي مجدد كامپيوتر شما Trojan بارگذاري شود. روشهاي معمول راه‌اندازي شامل كليدهاي اجرايي registry، فولدر راه اندازي ويندوز، Windows Load= يا run=lines يافته شده در فايل win.ini و shell=line يافته شده در system.ini ويندوز مي‌باشند.

روشهاي راه اندازي خطرناك

از آنجايي كه فقط تعداد اندكي از اين روشهاي راه اندازي وجود دارند، هكرهاي زيادي را يافته‌ايم كه در پيدا كردن روشهاي جديد راه‌اندازي افراط مي‌كنند. اين شامل استفاده از تغييرات خطرناكي در سيستم registry مي‌باشد، كه در صورتي كه فايل Trojan يا فايل همراه آن از بين برود سيستم را بصورت بلااستفاده درخواهد آورد. اين يك دليل استفاده نكردن از نرم افزار ضد ويروس براي از بين بردن Trojanهاست. اگر يكي از اين روشها استفاده شود، و فايل بدون ثابت كردن registry سيستم از بين برود، سيستم شما قادر به اجراي هيچگونه برنامه‌اي پس از راه اندازي مجدد كامپيوترتان نخواهد بود.

قبل از آنكه سراغ registry برويم لازم به توضيح است كه يك فولدر به صورت C:\WINDOWS\StartMenu\Program\StartUp وجود دارد كه هر فايلي در اينجا باشد هنگام راه اندازي ويندوز اجرا خواهد شد.توجه داشته باشيد كه هرگونه تغييري مي‌تواند سيستم شما را به خطر بيندازد بنابراين، هرچه ما مي‌گوييم انجام دهيد. براي دستيابي به registry به منوي start>run> برويد و "regedit" را بدون علامت " " تايپ كنيد. در registry چندين مكان براي راه اندازي Startup وجود دارد كه ليستي از آنها را در اينجا مي آوريم.

```
[KEY_CLASSES_ROOT\exefile\shell\open\command] ="\"%1 "*% "\
[HKEY_CLASSES_ROOT\comfile\shell\open\command] ="\"%1 "*% "\
[KEY_CLASSES_ROOT\batfile\shell\open\command] ="\"%1 "*% "\
[KEY_CLASSES_ROOT\htafile\Shell\Open\Command]="\"%1 "*% "\
[KEY_CLASSES_ROOT\piffile\shell\open\command] ="\"%1 "*% "\
[KEY_LOCAL_MACHINE\Software\CLASSES\batfile\shell\open\command] ="\"%1 "*% "\
[KEY_LOCAL_MACHINE\Software\CLASSES\comfile\shell\open\command]="\"%1 "*% "\
[KEY_LOCAL_MACHINE\Software\CLASSES\exefile\shell\open\command]="\"%1 "*%"\
[KEY_LOCAL_MACHINE\Software\CLASSES\htafile\Shell\Open\Command]="\"%1 "*%"\
[KEY_LOCAL_MACHINE\Software\CLASSES\piffile\shell\open\command]="\"%1"\
```

اگر اين كليدها مقدار "\"%1\"*%" را نداشته باشند و به جاي اجراي فايل در هنگام راه اندازي به "\"%1 "\Server.exe %*" تغيير يابد به احتمال زياد يك Trojan است.

روش راه اندازي ICQ

روشي راه اندازي ديگري كه امروزه استفاده از آن معمول است شناسايي شبكه ICQ مي‌باشد. بسياري از كاربران ICQ نمي‌دانند كه هكر مي‌تواند يك خط پيكربندي را به ICQ اضافه نمايد تا با هر بار بارگذاري شدن برنامه Trojan نيز راه اندازي شود. به عنوان آزمايش مراحل زير را انجام دهيد:

ICQ را باز كنيد. روي آيكن ICQ كليك كنيد و preference را انتخاب نماييد. روي Edit launch List كليك كنيد. روي Add كليك كنيد. روي Browse كليك كنيد. فايلي را براي اضافه كردن به Windows\notepad.exe بيابيد كه به كار اين آزمايش بيايد. روي Open و سپس OK كليك كنيد. زماني كه شما ICQ را راه اندازي مجدد مي‌كنيد فايل اجرا خواهد شد.

منبع : http://www.rayanehmag.net