راهنمای بازیابی فایل ها و فولدرهای پنهان شده توسط بدافزارهای پنهان گر:

مقدمه:

به تازگی بدافزاری شیوع پیدا کرده است که باعث پنهان شدن برخی از فایل ها و پوشه های حافظه های قابل حمل (از قبیل فلش ها، هارد اکسترنال و ...) می گردد. این تروجان که BackDoor-FHI نام دارد (بدافزارهایی با عملکرد مشابه نیز در گذشته شناسایی شده اند)، همچنین قادر به آلوده سازی منابع مشترک شبکه می باشد. آلودگی هنگامی رخ می دهد که فایل اصلی بدافزار اجرا شود که معمولاً shortcut جعلی از فایل ها و پوشه های موجود در حافظه است. این بدافزار از روش های متفاوتی برای انتشار خود استفاده می کند که از آن جمله می توان به انتشار از طریق e-mail، صفحات وب آلوده و هک شده، شبکه های peer-to-peer و IRC ها اشاره کرد.

نحوه عملکرد:

به محض اجرای فایل اصلی بدافزار، این تروجان خود را در مسیر زیر قرار می دهد.

- %UserProfile%\Application Data\[random]\[random].exe

سپس چند کپی از خود را در محل های مختلف قرار می دهد.

- $ReChCLE.BIN[malware data file]
- readme.tat[malware data file[
- reYdme.tat[malware data file[

·thLmbs.db

·desktopfini[malware data file[

·vagefile.sys[malware data file[

همچنین فایل های lnk که نامشان را از فایل های موجود در حافظه سیستم گرفته است، ایجاد می شوند. این کار پس از پنهان نمودن فایل های اصلی صورت می گیرد.

پسوندهای مورد توجه این بدافزار که اقدام به ایجاد shortcut از آنها و سپس پنهان نمودن فایل اصلی می کند عبارتند از:

·xls

·doc

·mp3

·ppt

·dll

·db

تروجان سپس کد خود را در چند پروسس تصادفی inject کرده، سعی در برقراری ارتباط با host های آلوده زیر می نماید. (URL های ذکر شده می تواند بر حسب نقاط جغرافیایی مختلف تغییر کند).

·www.guard.su

·www.protection.su

·www.e-statics.cc

·somesytems.cc

·www-protection.su

·estore-main.su

·strong-services.su

·wprotections.su

·wguards.su

علائم آلودگی به بدافزار BackDoor-FHL

موارد زیر نشان دهنده نشان دهنده آلودگی به این بدافزار است:

· اگر یک فایل یا پوشه با نام یکسان، در همان مکان ایجاد و فایل اصلی hidden شده باشد.

· اگر فایل یا پوشه هم نام با فایل shortcut موجود باشد و hidden نشده باشد. به نظر می رسد که این فایل های shortcut به منظور هدایت کاربر به سمت بدافزار ایجاد شده اند.

· اگر فایل یا پوشه ای با نامی غیر از فایل shortcut باشد، امکان آن وجود دارد که shortcut آلوده باشد.

· اگر کلید رجیستری زیر وجود داشته باشد، احتمال آلودگی وجود دارد

HKEY_CURRENT_USER\Software\Microsoft\\Windows\CurrentVersion\Run"{8DF9EE17-84FF-E9C9-901F-18FC59A5DB1E}" =%UserProfile%\Application Data \ [Random] \[random].exe /r

روش های جلوگیری از آلوده شدن به این بدافزار:

· احتیاط در باز کردن ایمیل های ناشناس و لینک های ناشناخته

· بروزرسانی ویندوز و وصله های برنامه های کاربردی و آنتی ویروس ها و اعمال قوانین فیلترینگ مناسب

· مسدود کردن دسترسی شبکه به URL های ذکر شده

· فعال کردن Access Protection و تنظیم قوانین به نحوی که از تغییر ناخواسته attributes فایل ها و فولدرها جلوگیری شود.

راهکار نمایش فایل های پنهان

در صورت آلودگی به این بدافزار، با آنکه خود بدافزار توسط تمامی آنتی ویروس های معتبر شناخته و پاک می شود ولی نشانه های آن باقی می ماند، یعنی بسیاری از فایلهای شما پنهان می مانند و استفاده از لبه view منوی folder option نیز کار زمان بری می باشد. لذا می توانید برای اصلاح فایل های خود، از دستور ذیل استفاده کنید.

1. ابتدا برنامه command prompt را از بخش Accesories منوی استارت اجرا نمایید.
2. سپس عبارت روبرو را تایپ نمایید: attrib -s -h -r "c:*" /s /d
3. توجه داشته باشید که می بایست به جای عبارت c:\ مسیری که قصد غیرفعال نمودن فایلهای پنهان آن را دارید، وارد نمایید. مثلا اگر قصد دارید فایلهای پوشه test که در درایو d قرار دارند را از حالت پنهان خارج سازید، می بایست دستور زیر را وارد کنید.

attrib -s -h -r "d:\test*" /s /d

*****

منبع : مرکز ماهر

لینک مطلب در وبلا گ صفر و یک امن: http://01amn.rozblog.com/post/115