آموزش از بین بردن ویروس Shortcut و بازیابی اطلاعات مخفی شده

ویروس های shortcut یکی از شایع ترین ویروس های مربوط به فلش مموری ها می باشند . نحوه کار این ویروس ها به صورتی است به محض اینکه فلش مموری خود را به یک سیستم آلوده به ویروس متصل می کنید، فلش مموری شما آلوده می گردد که با فعال شدن ویروس روی فلش مموری، فایل های موجود را پنهان کرده و Shortcut آنها را می سازد.

روش کار این دسته از ویروسها به این شکل می باشد که ابتدا یک فولدر در فلش مموری شما ایجاد کرده و تمامی اطلاعات فلش مموری را به این پوشه انتقال می دهد. پس از انتقال فایلها پوشه مورد نظر را مخفی کرده و اقدام به ایجاد یک فایل Shortcut در ریشه فلش با آیکونی مشابه فلش مموری می کند . پس شما عملا در حالت عادی درون فلش جز یک Shortcut که به شکل درایو هم هست چیز دیگری نمیبینید . شما با اجرای فایل Shortcut به سمت فولدر مخفی که حاوی تمام اطلاعات فلش می باشد، هدایت می شوید پس به هدف خود میرسید اما در کنار انجام چنین کاری فایل ویروس هم یک بار بطور نامحسوس بر روی سیستم اجرا شده و شروع به نفوذ به سیستم می کند.

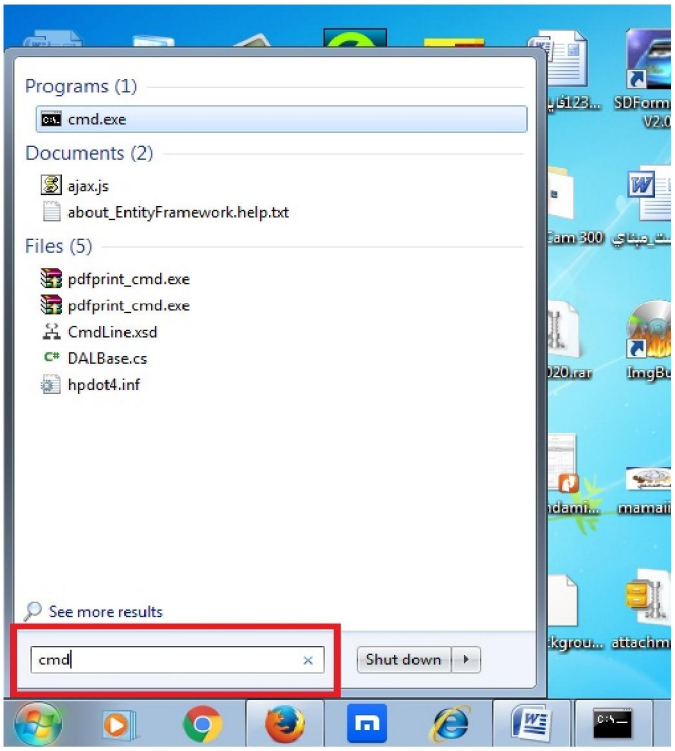
با اتصال یک فلش آلوده به سیستم جدید و باز کردن فلش (در صورتی که سیستم دارای آنتی ویروس نباشد) سیستم مورد نظر نیز به ویروس آلوده می شود. در صورتی که سیستم جدید دارای آنتی ویروس باشد (به شرط آنکه آنتی ویروس بروزرسانی شده باشد) آنتی ویروس اقدام به از بین بردن ویروس میکند. با این کار فایل Shortcut از روی فلش شما پاک میشود ولی اطلاعات شما همچنان در فولدر ایجاد شده توسط ویروس روی فلش پنهان می باشد که در حالت عادی غیر قابل مشاهده است و امکان دسترسی به اطلاعات وجود ندارد.

برای بازیابی اطلاعات مخفی شده توسط ویروس مراحل زیر را انجام دهید:

۱- ابتدا از نصب آنتی ویروس بر روی سیستم خود و به روز بودن آن مطمئن شوید .

۲- فلش آلوده را به سیستم متصل کنید و توسط آنتی ویروس آنرا اسکن کنید .

۳- در قسمت Search programs and files ویندوز کلمه cmd را تایپ کنید و کلید Enter را بزنید.



۴- سپس در خط فرمان دستور زیر را تایپ و کلید Enter را بزنید .

Attrib –h –r –s /s /d نام درایو مربوط به فلش یا هارد دیسک :*.*

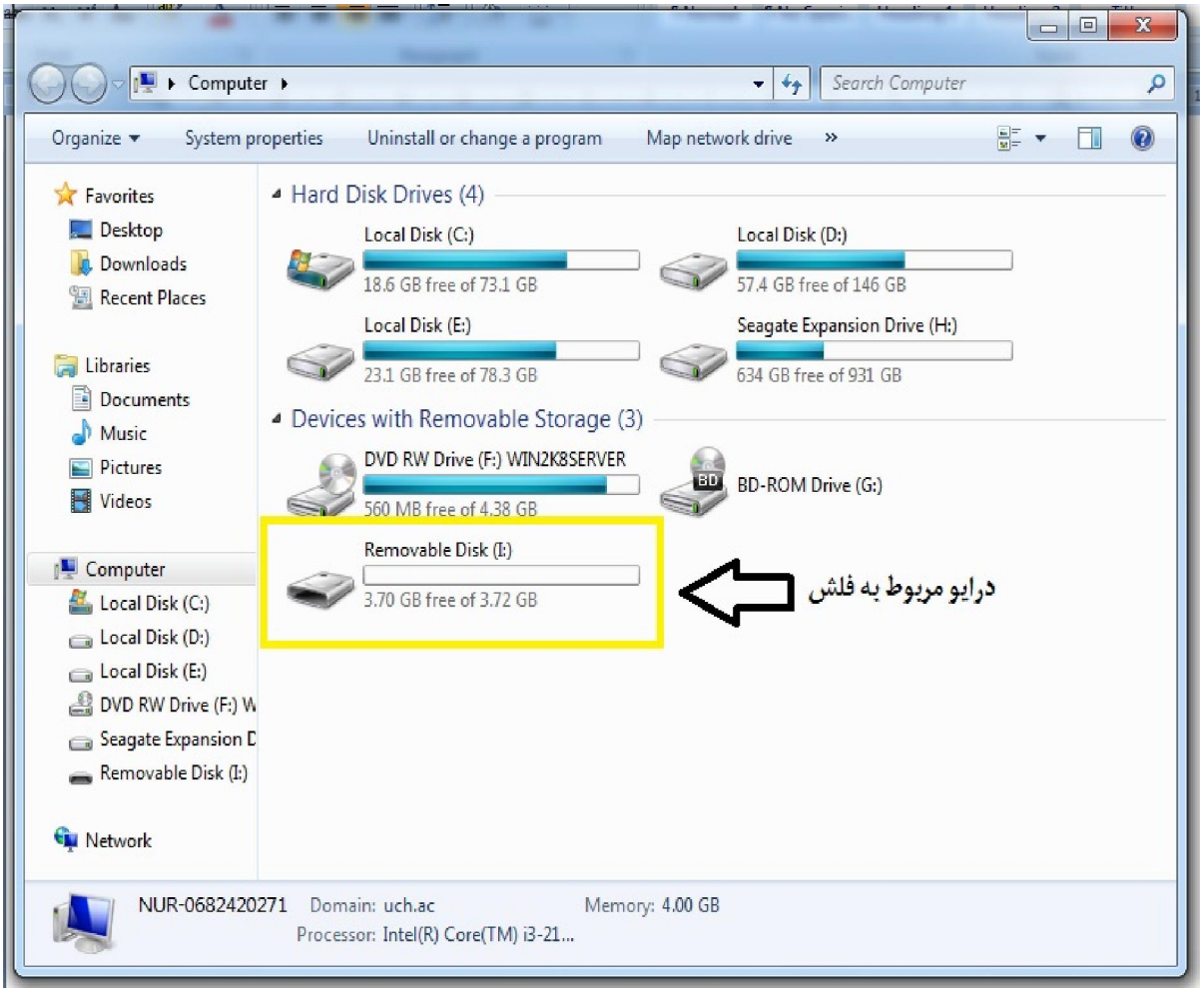
توجه کنید که متن دستور را دقیقا مشابه بالا تایپ کنید.

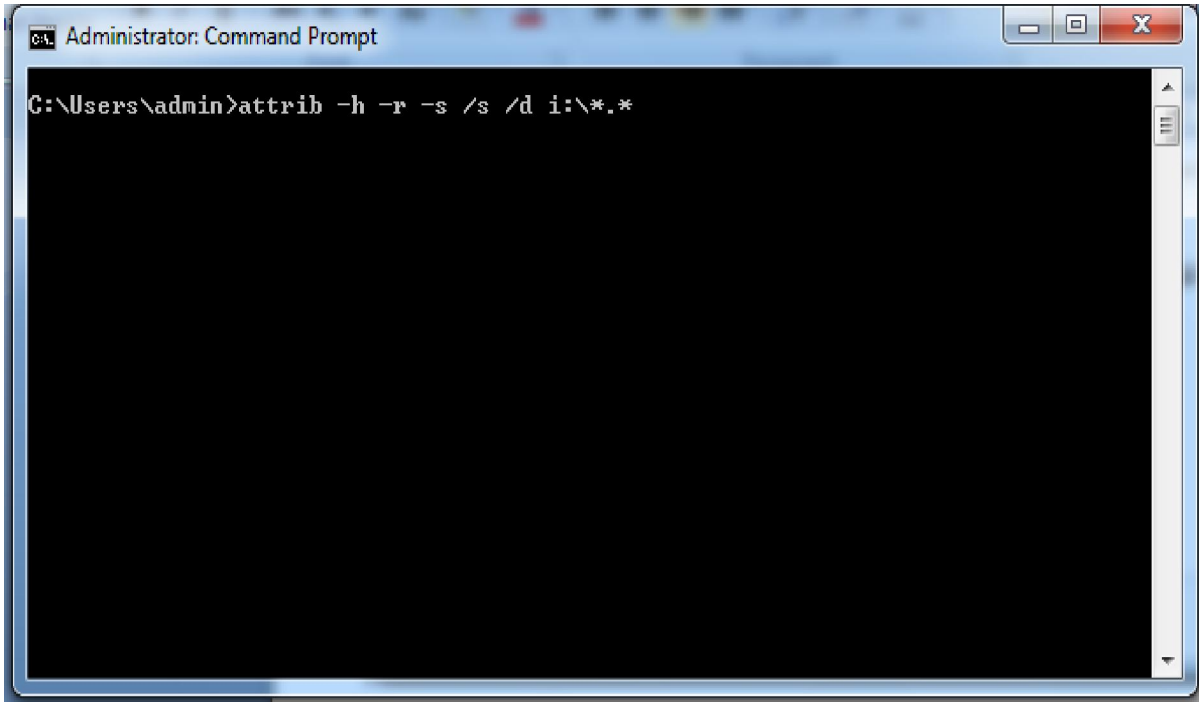
کمی منتظر بمانید تا دستور صادره کار خود را انجام داده و دوباره خط فرمان به نمایش در آید.

حال اگر فلش یا هارد دیسک خود را باز کنید، می بینید که پوشه ایجاد شده توسط ویروس از حالت مخفی خارج شده و به صورت یک فولدر بدون نام قابل مشاهده است . فولدر مورد نظر را باز کنید و اطلاعات خود را مشاهده نمایید.

- نام درایو مربوط به فلش مموری را می توان از My computer مشاهده نمود. برای مثال در شکل روبرو نام درایو مربوط به فلش i می باشد (حرف لاتین نوشته شده درون پرانتز در عبارت Removable Disk ((i:)) و دستور را باید به شکل زیر نوشت

Attrib –h –r –s /s /d i:*.*





تصویر اجرای دستور در cmd