هشدار مهم ویروس ! مراقب و آماده برای ویروس احتمالی Wipe باشید

بر اساس گزارشات دریافتی از برخی از مشتریان شرکت مهندسی شبکه گستر، اخیراً نامه ای از حراست وزارت خانه ها و سازمان های کشور درباره ویروس جدیدی که اطلاعات دستگاه ها را بصورت دائمی و غیرقابل برگشت، حذف (Wipe) می کند، ارسال گردیده است. با توجه به اینکه در این نامه هیچگونه اطلاعات فنی دقیقی برای پیگیری موضوع وجود ندارد، در حال حاضر تنها می توان توصیه های زیر را به مدیران شبکه ای که نگران آلوگی به این ویروس و یا قرار گرفتن در معرض تهدیدهای مشابه هستند، ارائه کرد.

۱- از به روز بودن ضد ویروس بر روی دستگاه های شبکه اطمینان حاصل کنید.

۲- از اطلاعات موجود بر روی سرویس دهنده های خود یک نسخه پشتیبان (Backup) بطور کامل تهیه کرده و در محل دیگری، جدا از سرویس دهنده ها- مثلاً بر روی دیسک های قابل حمل و یا DVD- کپی کنید.

۳- آخرین بسته های بروز رسانی (Service Pack) و اصلاحیه (Patch) های سیستم عامل و نرم افزارهای کاربردی مورد استفاده را بر روی تمام دستگاه ها و به ویژه سرویس دهنده ها نصب کنید. برای اینکار می توان از نرم افزار WSUS استفاده کرد. همچنین شرکت شبکه گستر نیز تمام اصلاحیه های سیستم عامل Windows و سایر نرم افزارهای کاربردی را بر روی DVD گردآوری کرده است که از آنها هم می توان بهره برد.

۴- دسترسی کاربران به درگاه های فیزیکی مانند درگاه USB برای استفاده از دیسک های قابل حمل را محدود کنید. برای اینکار می توان از محصولی مانند McAfee Device Control یا مشابه آن استفاده کرد.

۵- در صورتیکه از سخت افزارهای امنیتی (UTM) یا نرم افزارهای دیواره آتش بر روی ورودی شبکه (Gateway) استفاده می کنید، دسترسی کاربران به اینترنت را محدود به سرویس ها و درگاه های (Port) لازم نمایید تا از ویروسی شدن احتمالی کاربران پیشگیری شود.

۶- در صورت دیدن فایل های مشکوک و به ویژه مرتبط با ویروس احتمالی Wipe، نسخه ای از آنها را از طریق ایمیل support@shabakeh.net یا سایت http://help.shabakeh.net برای گروه پشتیبانی شرکت شبکه گستر بفرستید.

۷- برای اطلاعات بیشتر می توانید از طریق سایت پشتیبان شبکه گستر به نشانی help.shabakeh.net یا پست الکترونیک help@shabakeh.net و یا بصورت تلفنی با کارشناسان پشتیبانی شرکت تماس حاصل فرمایید.

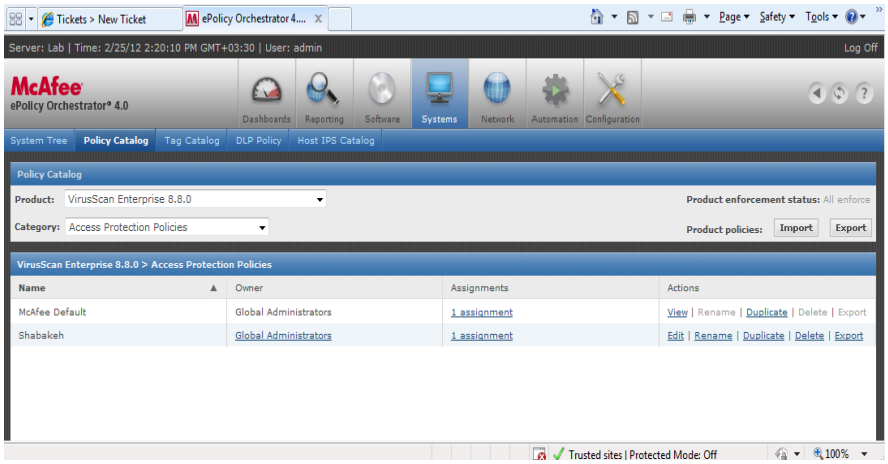
همچنین برخی منابع کارشناسی و تحقیقاتی درباره روش مقابله با ویروس احتمالی Wipe راهکارهایی را پیشنهاد داده اند. بر این اساس، باید دسترسی و فعالیت فایلی با نام diskpart محدود گردد. بدین منظور می توانید به روش زیر، با استفاده از امکانات Access Protection ضد ویروس McAfee جلوی فعالیت این فایل را بگیرید.

- ابزار مدیریتی McAfee ePolicy Orchestrator 4

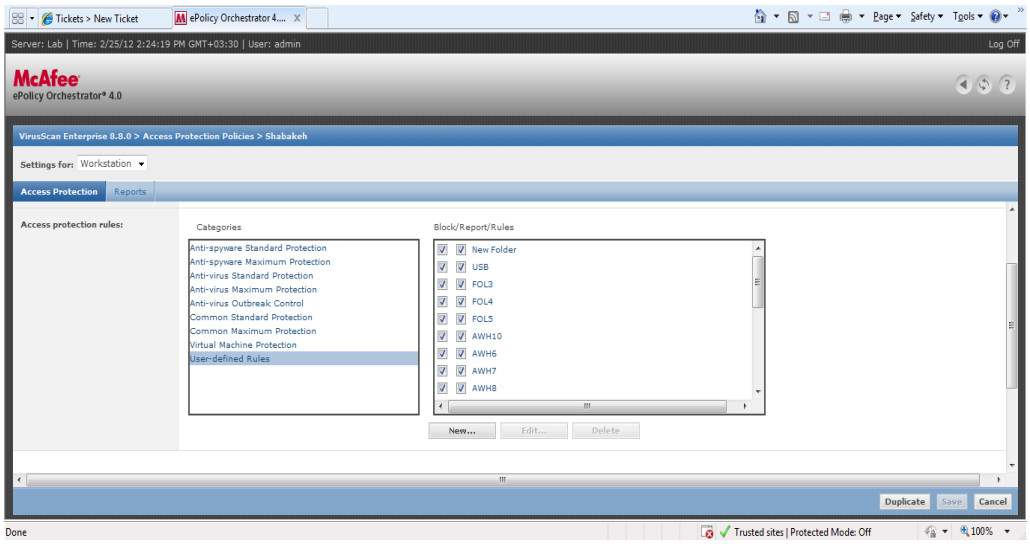
۱- در نسخه ePolicy 4.0، زبانه Systems را انتخاب و بر روی Policy Catalog کلیک کنید.
در نسخه ePolicy 4.5، بر روی Menu کلیک و در بخش Policies بر روی Policy Catalog کلیک کنید.

۲- در بخش Product ابتدا گزینه VirusScan Enterprise 8.8.0 را انتخاب و سپس در قسمت Category بر روی Access Protection Policies کلیک نمایید.

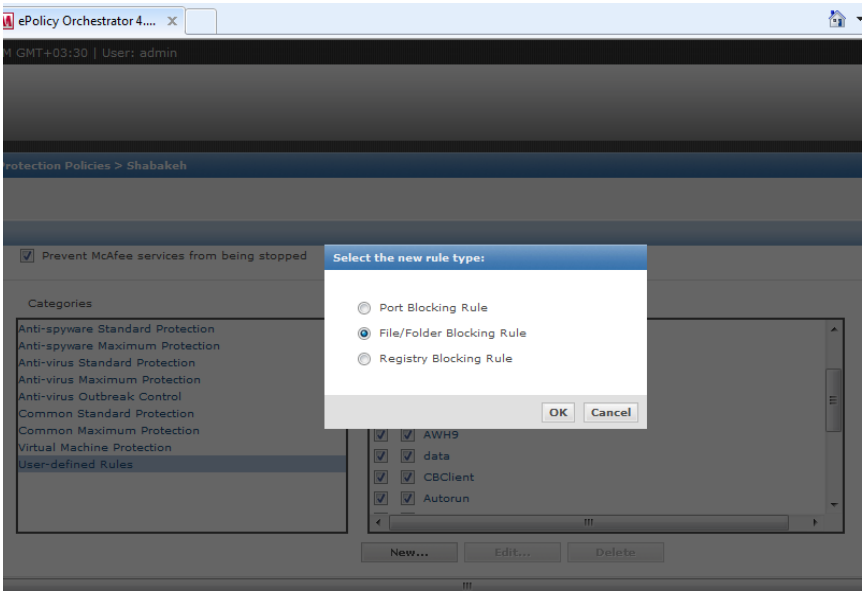
۳- در اینجا سیاست نامه (Policies) مورد استفاده در شبکه (برای مثال Shabakeh) را Edit نمایید.



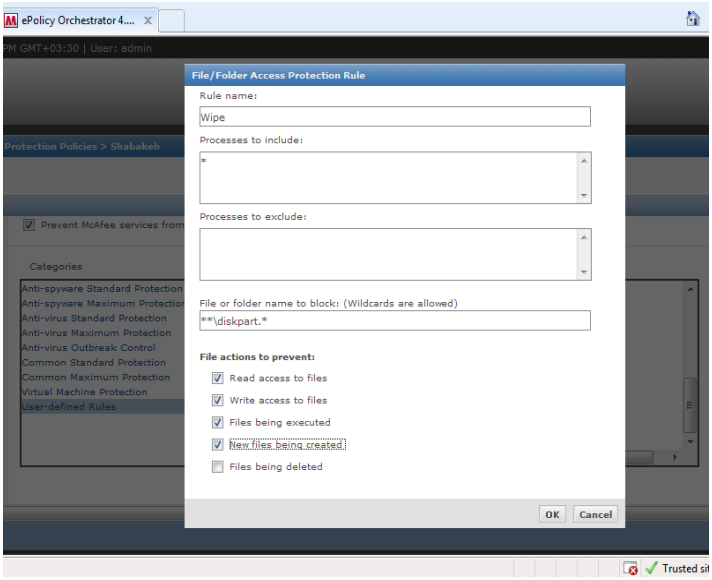
۴- در پنجره ظاهر شده و در قسمت Categories، گزینه User-defined Rules را انتخاب و در بخش سمت راست بر روی دگمه New... کلیک کنید.



۵- در ادامه File/Folder Blocking Rule را انتخاب نمایید.



۶- در پنجره ای که به نمایش در می آید، مطابق شکل زیر Wipe را در قسمت Rule name، * را در قسمت Processes to include و *.diskpart** را در قسمت File or folder name to block وارد کنید. در بخش File actions to prevent نیز تمامی گزینه ها به غیر Files being deleted را فعال نمایید.



۷- چنانچه می خواهید این قاعده بر روی سرورها نیز اعمال گردد در قسمت Settings for گزینه Server را انتخاب کرده و مراحل ۴ تا ۶ را انجام دهید.

۸- پایان کار. بدین ترتیب هرگونه سعی برای دسترسی و اجرای غیرمجاز از فایل diskpart مسدود و متوقف خواهد شد.