روش های مقابله با باج افزارها (Ransomware)

- روش های انتشار باج افزار در شبکه:

۱- متداول ترین روش انتقال باج افزار از طریق ایمیل می باشد بدین صورت که ایمیلی حاوی لینک مخرب برای کاربران ارسال می گردد تا کاربران زود باور بر روی آن لینک کلیک کرده و سیستم خود را آلوده سازند.

۲- در روش دیگر باج گیرها از طریق حفره های امنیتی نرم افزارها اقدام به اجرا کردن باج افزارها می کنند.

۳- بازدید از وب سایت های نامعتبر نیز ریسک آلوده شدن به باج افزارها را در پی دارد.

۴- دانلود فایل های مشکوک نیز از دیگر موارد احتمال ابتلا به باج افزار می باشد.

۵- و . . .

نکته: برخی از باج افزارها به گونه ای طراحی شده اند که اگر وارد سیستم یک کاربر در محیط شبکه شوند، با اسکن نمودن شبکه و پیدا کردن دیگر کامپیوترها خود را منتشر می کنند.

- راه های مقابله با باج افزار در شبکه:

۱. همیشه از اطلاعات نسخه پشتیبان تهیه کنید.

۱,۱. توسط نرم افزارهایی مانند Veeam Backup ، Symantec Exec Backup ، Trilead و . . . از ماشین های مجازی[1] یک incremental Backup در طول هفته و یک Full Backup در پایان هفته تهیه کنید. یا اینکه یک نسخه Replicated به صورت روزانه بر روی همان سرور[2] یا سرور دیگر ایجاد نمایید.

۱,۲. از فایل ها و نرم افزارهای مورد استفاده در شبکه یک نسخه کپی به صورت incremental روزانه تهیه کرده و بر روی یک ذخیره ساز تحت شبکه[3] یا هارد دیسک مجزا[4] ذخیره نمایید.

۱,۳. همچنین می توانید برای اطمینان بیشتر در پایان هر ماه یک نسخه Clone از ماشین مجازی گرفته و در جای امنی نگه داری کنید.

[1] Virtual Machines
[2] Server or Host
[3] NAS Storage
[4] External HDD

۱,۴. شرکت های کوچک بهتر است یک نسخه از اطلاعات مهم خود را بر روی ذخیره سازهایی مانند Dropbox در خارج از سازمان نگهداری کنند یا از شرکت های ارایه دهنده سرویس های پردازش ابری بخواهند فضایی برای نگهداری اطلاعات در اختیارشان بگذارند.

نکته: نرم افزار پشتیبان گیری را طوری تنظیم کنید که حداقل تا ۴ نسخه از backup های گرفته شده را نگهداری کند زیرا ممکن است شما متوجه آلوده شدن سیستم نشده باشید و نرم افزار نیز از همان سیستم آلوده شده مجددا پشتیبان بگیرد.

۲. به روز رسانی و نصب وصله های امنیتی[5] بر روی سیستم عامل و نرم افزارها همیشه نقش به سزایی در حفاظت از شبکه دارد. نرم افزار هایپرویزور[6] و نیز سیستم عامل های سرور می بایست مرتبا به روز رسانی شوند.

۳. رمز عبور مدیر شبکه[7] می بایست پیچیده بوده و هر از گاهی عوض شود. همچنین بهتر است مدیر شبکه برای انجام کارهای روزمره از نام کاربری دیگری که محدودیت بیشتری نسبت به built-in administrator دارد استفاده نماید.

۴. بر روی مرورگرهایی[8] که استفاده می کنید تنظیمات امنیتی را ارتقا دهید و تا حد امکان بر روی آن پلاگین نصب نکنید.

۵. از آنتی ویروس های معتبر که دارای رتبه جهانی بالایی هستند استفاده کنید. حتما نحوه دسترسی بر روی فایل های مهم را بر روی آنتی ویروس تعریف کنید. (رجوع شود به پیوست۱)

۶. وجود آنتی ویروس و فایروال بر روی سیستم ها ضروری است. ترجیحا از UTM در لبه ی شبکه نیز استفاده شود.

۷. قابلیت show file extensions را بر روی ویندوز فعال کنید.

۸. فایل هایی که پسوند اجرایی مانند exe. دارند را بر روی ایمیل سرورها فیلتر کنید.

۹. سرویس های بدون استفاده در شبکه غیر فعال شوند و در صورت عدم نیاز به RDP آن را غیر فعال کنید.

۱۰. از باز کردن ایمیل های ناشناس یا دانلود فایل های مشکوک یا مشاهده وب سایت های نامعتبر خودداری کنید.

۱۱. از طریق Group Policy برای اجرای نرم افزارها محدودیت ایجاد کنید. (رجوع به پیوست شماره۲)

۱۲. پورت ۱۳۵ مربوط به سرویس WMI و پورت ۴۴۵ مربوط به SMB بر روی لبه خارجی شبکه (روتر یا فایروال) بسته شود.

---

[5] Security Patch
[6] Hypervisor
[7] Administrator
[8] Explorer

- روش های عمومی برای پاک کردن باج افزار از شبکه ی آلوده شده:

۱) یکی از فایل های آلوده شده را در وب سایت زیر آپلود کرده تا شاید نام آن را به شما بگوید.

id-ransomware.malwarehunterteam.com

۲) بهتر است سیستم آلوده شده را در حالت Safe Mode اجرا کنید.

۳) در task manager پروسس های نا آشنا را ببندید.

۴) توسط MSconfig اجرای خودکار[9] برنامه را غیر فعال کنید.

۵) در رجیستری نام باج افزار را جستجو کرده و آن را پاک کنید.

۶) از مسیر زیر فایل hots را ویرایش کرده و IP ناشناس را پاک کنید.

Windows\system32\drivers\etc\hosts

۷) تمام Temporary File ها در مسیرهای ذیل را پاک کنید:

%AppData%

%LocalAppData%

%ProgramData%

%WinDir%

%Temp%

۸) آخرین نسخه وصله های امنیتی را روی سیستم عامل نصب کنید.

۹) هرگونه پروسه backup یا replication متوقف شود.

۱۰) از طریق کنسول آنتی ویروس دسترسی write بر روی فایل های word و excel و . . . بسته شود.(رجوع به پیوست۱)

۱۱) ارتباطات شبکه و ترجیحا سرویس های file sharing موقتا غیر فعال شوند.

۱۲) فایل های آلوده شده را از روی سیستم پاک کنید.

۱۳) اگر باج افزار برای پرداخت باج برای شما مهلت زمانی[10] تعیین کرده بود، سعی کنید زمان سیستم را از طریق Bios به قبل برگردانید.

[9] Startup
[10] Clock

۱۴) تعدادی برنامه به نام free anti-ransomware tools و یا ransomware decryption tools در اینترنت وجود دارند که ادعا می کنند قادر به مقابله با برخی باج افزارها هستند.

نکته: روش مقابله با هر نوع باج افزار متفاوت است پس بهتر است با جستجو در اینترنت متد مقابله با آن را پیدا کنید. برای نمونه به مقاله روش مقابله با باج افزار bad rabbit در لینک زیر مراجعه نمایید.

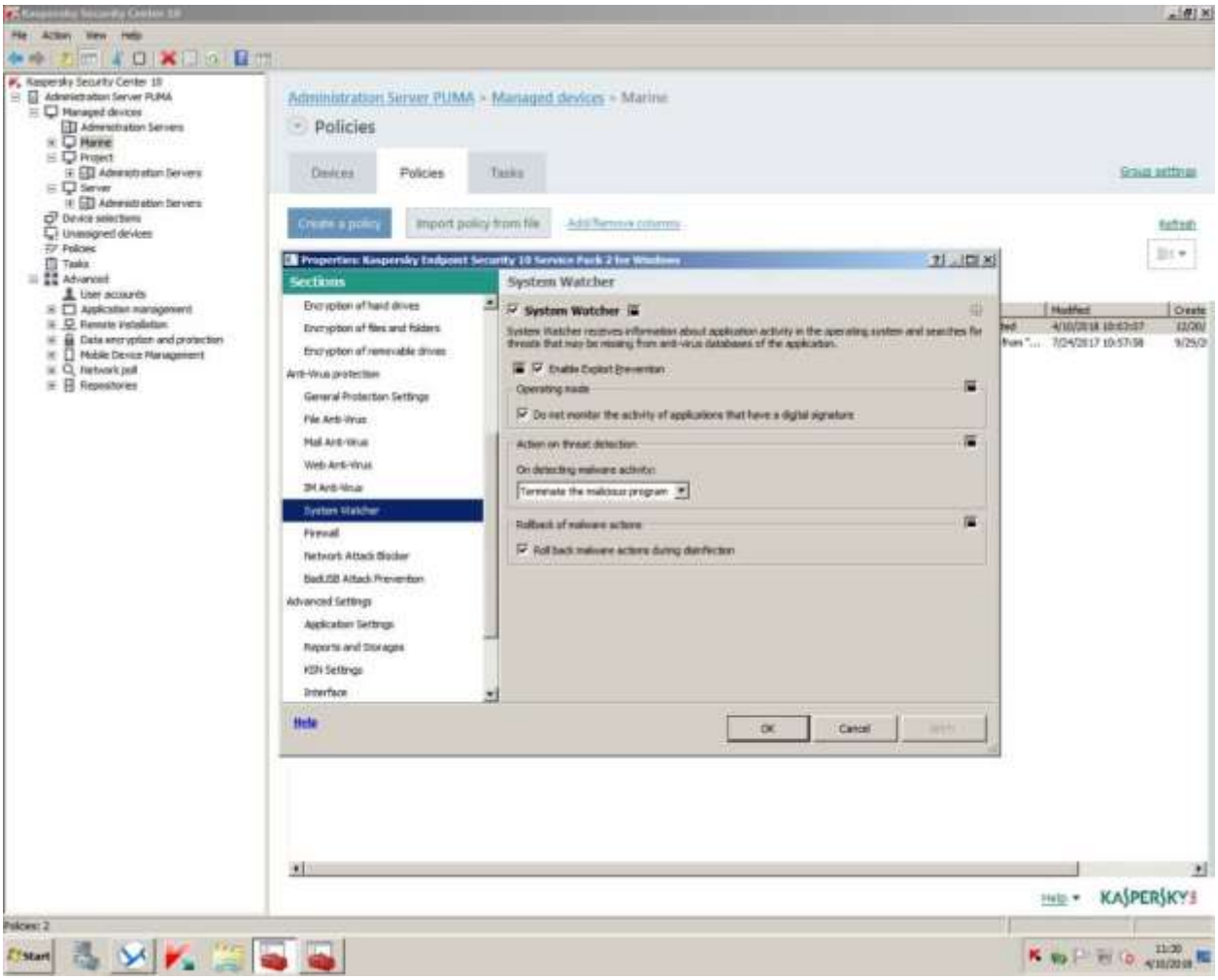
http://www.persiatc.com/Reading/BadRabbit

نکته: روش فوق یکی از شیوه های موثر برای حذف arrow. و جلوگیری از گسترش آن در شبکه می باشد.

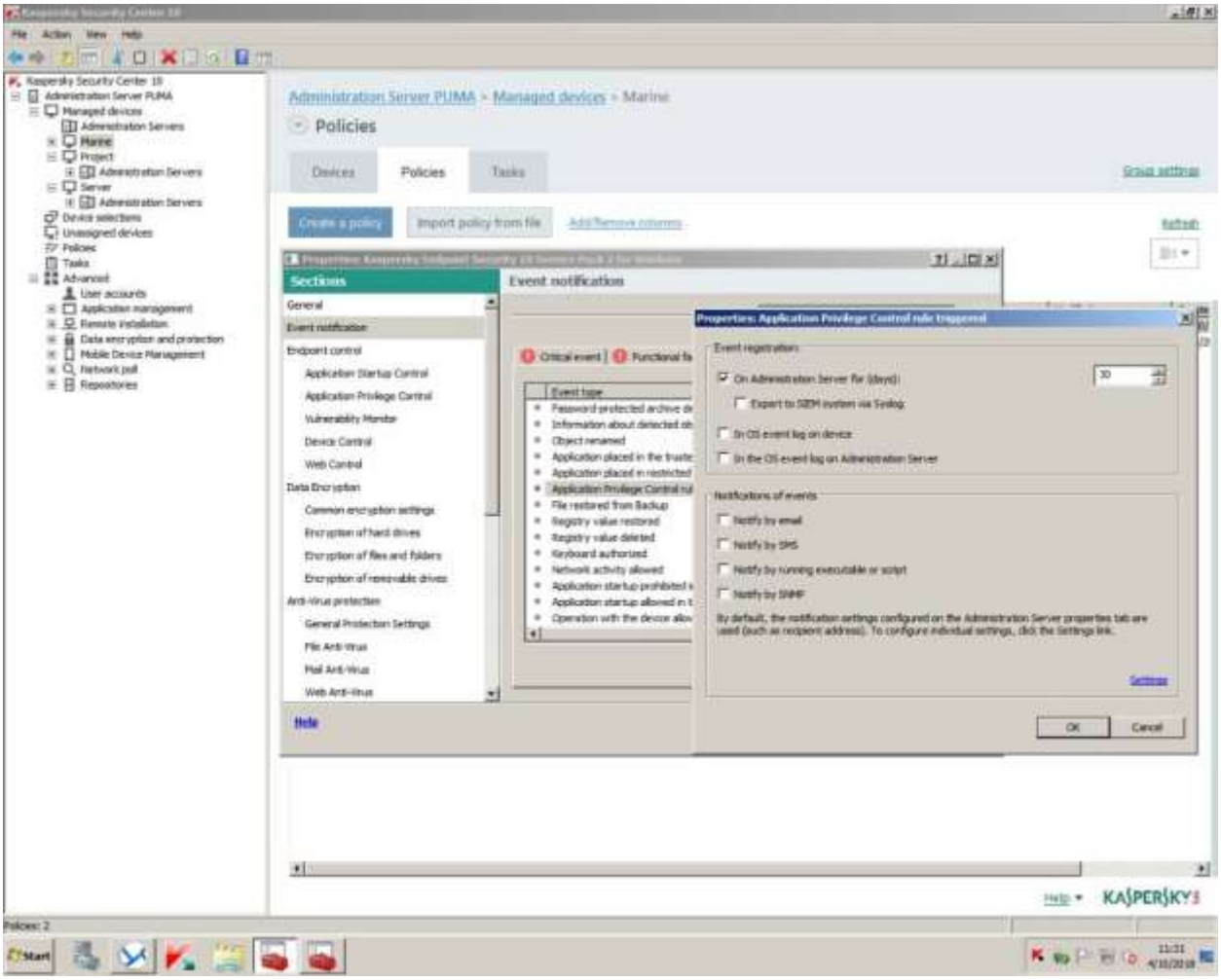
پیوست ۱

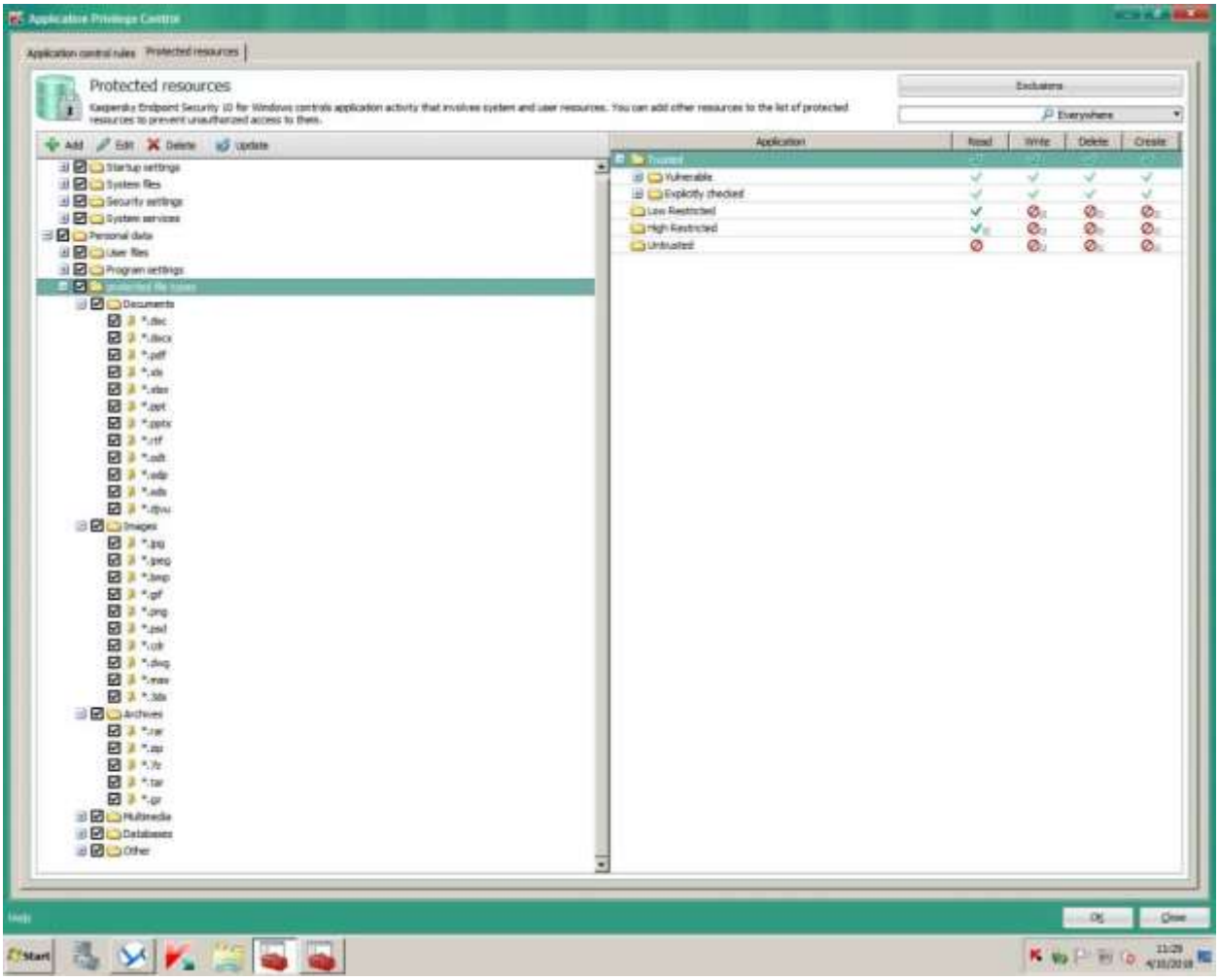
روش آنالیز دسترسی به فایل ها با کمک آنتی ویروس کسپرسکی:

۱. فعال کردن گزینه system watcher



۲. تعریف سطح دسترسی به فایل های مورد نظر





برای اطلاعات بیشتر از چگونگی تنظیمات می توانید به لینک ذیل رجوع نمایید:

https://support.kaspersky.co.uk/10905

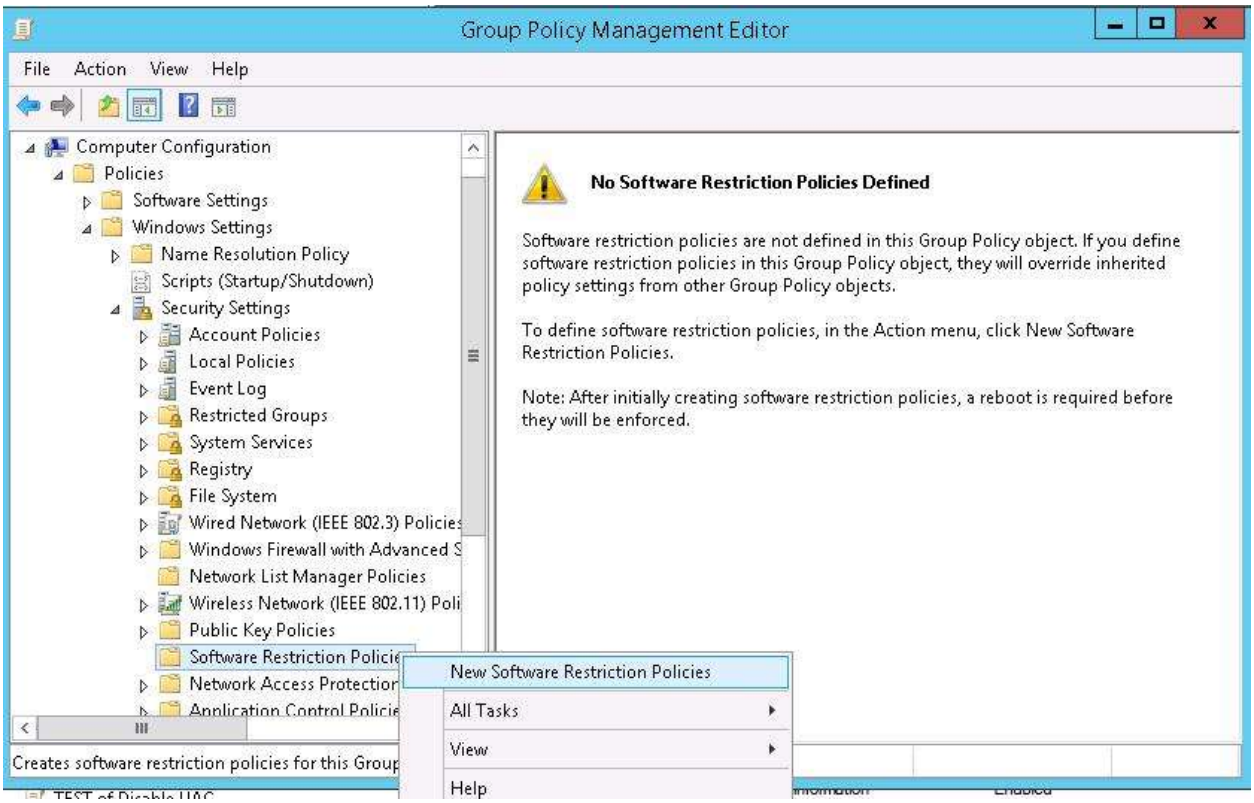
پیوست ۲

روش جلوگیری از اجرای نرم افزارها از مسیر %AppData%

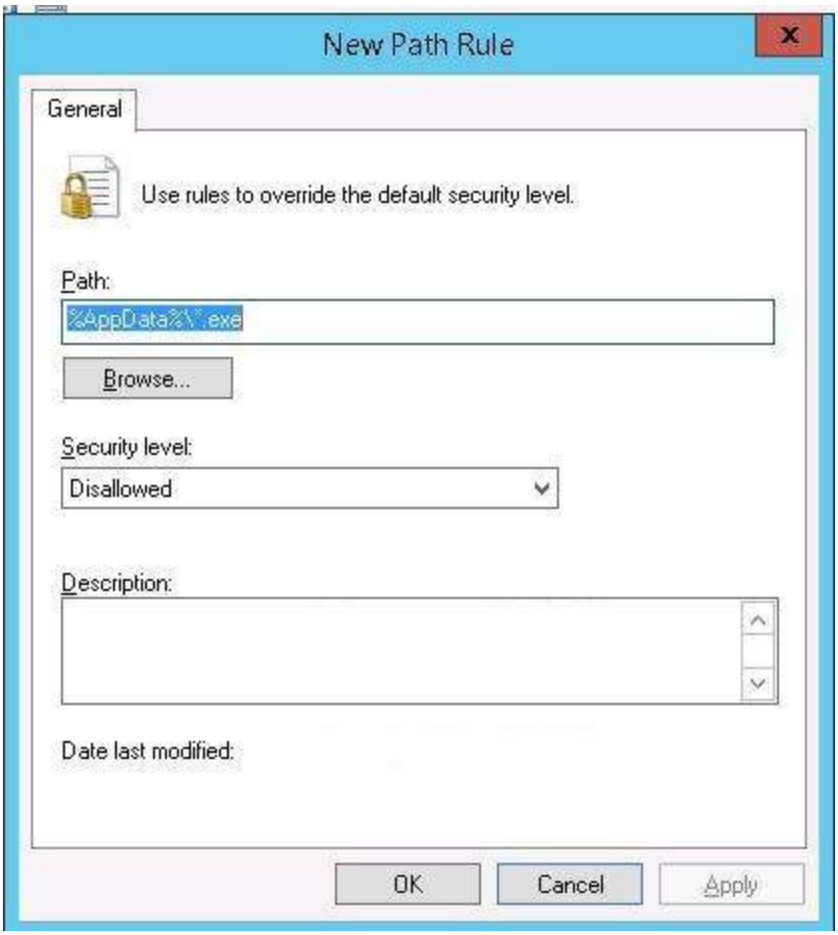
به روش زیر یک policy جدید ایجاد می کنیم:

Computer Configuration -> Windows Settings -> Security Settings.

Right-click Software Restriction Policies and select New Software Restriction Policies.



Select Additional Rules and create a new rule using New Path Rule.



نکته: برای اطلاعات بیشتر از چگونگی تنظیمات به لینک زیر مراجعه نمایید:

http://woshub.com/how-to-block-viruses-and-ransomware-using-software-restriction-policies

Persia Telecom Co.

Nicoukalam