آموزش آنتی ویروس Kaspersky قسمت ۴۹ : جلوگیری از برنامه با KES (نسخه PDF)

نحوه ممانعت KES از یک برنامه

کسپراسکی بر اساس دو پارامتر عمده و اصلی مانع اجرای برنامه ها می شود :

- برنامه هایی که Trust آن ها در kaspersky security network شناسایی شده است

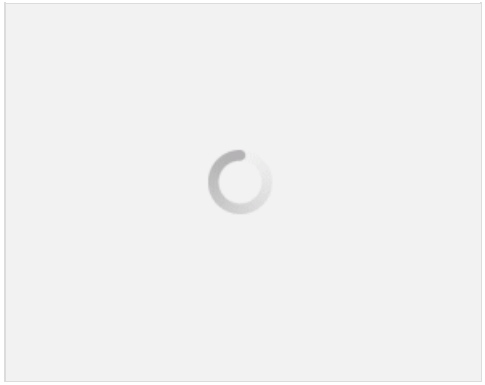
- بر اساس اعتبار برنامه هایی که Trust شده اند .

KSN اطلاعات تراست برنامه ها را بر اساس ابزار های زیر جمع اوری میکند :

- System Watcher

- Application Privilege Control

کسپراسکی Endpoint همیشه اعتبـار برنـامه هـا را بر اساس دیتابیس خود در محل هایی به نام Trusted Root و Certification Authorities بررسـی می کند این برنامه بروزرسانی منابع Certificate خود را با KSN بروزرسـانی می کنـد . اگر برنامه های دارای یک امضای دیجیتالی نبود شـما می توانید به صورت دستی ان را در گرو ه های Trust قرار دهیـد که در درس قبلی در مباحث Application control policy توضیح داده شد .



- نحوه تغییر در دسته بندی تراست

بعضـی از برنامه مثلاً آنهایی که متن باز هستند دارای ریسک کمتری هستند برای جلوگیری از کارکرد برنامه هایی که مدیر شبکه قصد دارد تا مانع اجرای انها شود از مراحل زیر استفاده می شود :

- باز کنید Application Privilege Control را در بخش پالیسی ها از Kaspersky Endpoint Security policy

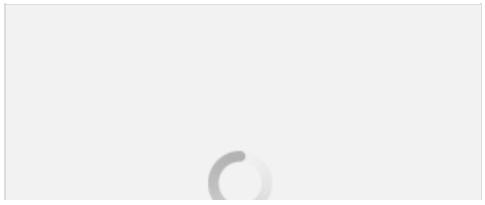
- بالاترین گزینه Settings به نام Application rules را بزنید

- کلیک کنید روی Add تا لیست دسته بندی ها باز شود

- حالا برنامه ای که EXE است را انتخاب و کلیک کنید روی Refresh

-حالا از لیست جستجو شده می توانید برنامه های اجرایی موردنظر را انتخاب کنید

- انتخاب برنامه هایی که اعتبار پایینی دارند و کلیک روی OK



نویسنده : سید احمد توسلی

منبع : جزیره امنیت اطلاعات و ارتباطات وب سایت توسینسو

مطلب اصلی