راهنمای راه اندازی

ESET Anti-Ransomware

امنیت چند لایه در مقابل باج افزارها

با استفاده از کنسول ERA6

لابراتوآر ویروس شناسی کامیران

نمایندگی رسمی محصولات تحت شبکه ESET در ایران

www.KAMIRAN.Asia

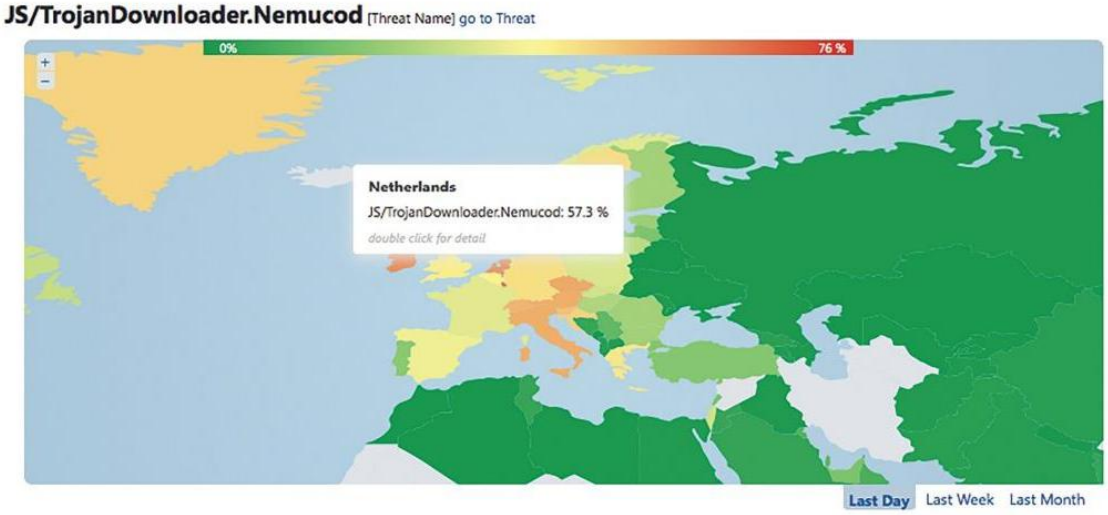
نگارش 11-2016

هدف از این آموزش

در این مقاله تنظیمات بهینه راه حل های امنیتی *ESET* در مقابل *Ransomware* و رایج ترین سناریو های آلودگی آن را بررسی می کنیم.هدف ما محافظت بهتر از مشتریان خود در برابر حملات *Ransomware* است.هنگامی که داده های ارزشمند رمزنگاری شده،گروگان گرفته شده و فقط هنگامی که پول درخواستی پرداخت شود داده ها تحویل داده می شوند.

چرا این تنظیمات بیشتر مورد نیاز است؟

نزدیک به % 66 از تمام بد افزارهایی که در هلند تشخیص داده شده اند از خانواده *ransomware* بوده اند.



در حال حاضر حملات *ransomware* از تکنیک های پیشرفته استفاده می کنند تا دستگاه شما را آلوده کنند .این بدافزارها مردم را متقاعد به اجرای اصطلاحا برنامه ای به نام*dropper* می کنند که این برنامه خود را به یک ایمیل متصل کرده و اقدام به دانلود تروجان های مخرب می کند تا فرآیند رمزنگاری را آغاز کند . مجرمان اینترنتی در بیشتر مواقع برای جلوگیری از تشخیص ورودشان به سیستم از یک ایمیل فیشینگ به همراه یک فایل *zip* استفاده می کنند.

این فایل *zip* معمولا یک فایل *JavaScrip* از نوع *JS* درون خود دارد.

به دلیل اینکه *JavaScript* در بیشتر سایت ها مورد استفاده قرار می گیرد، امکان مسدود کردن آن درون مرورگر غیر ممکن بوده و همچنین ویندوز خود نیز مستقیما فایل های *JavaSript* را اجرا می کند.

در همین حال کدهای فایل *JavaSript* که درون *dropper* قرار دارد بسیار مبهم بوده و به منظور جلوگیری از تشخیص به طور مداوم خود را اصلاح می کنند .این به ما این فرصت را می دهد تا از طریق فرآیندهای استاندارد و با استفاده از ماژول های مختلف امنیتی اجرای کد های مخرب را تحت تاثیر قرار داده و آن ها را مختل کنیم.

هشدار:

راه حل ها و سیاست های *ESET* در برابر *Ransomware* به صورت کلی بوده و در مناطق مختلف متفاوت می باشد.ما توصیه می کنیم قبل از پیاده سازی نهایی برای مشتری تنظیمات را آزمایش نمائید.

تنظیمات ESET برای شرکت ها در برابر Ransomware :

تنظیمات اضافی *ESET* در برابر *ransomware* از شروع فرآیند دانلود تروجان های مخرب جلوگیری می کند .به دلیل اینکه این رویکرد بسیار کارآمد می باشد، تصمیم گرفتیم تا در ادامه این مقاله این تنظیمات را با جزئیات توضیح داده و آن ها را به عنوان یک سیاست پیکربندی ارائه دهیم .شما می توانید این تنظیمات را دانلود کرده و با استفاده از *ESET Remote Administrator* آن ها را پیاده سازی نمائید.

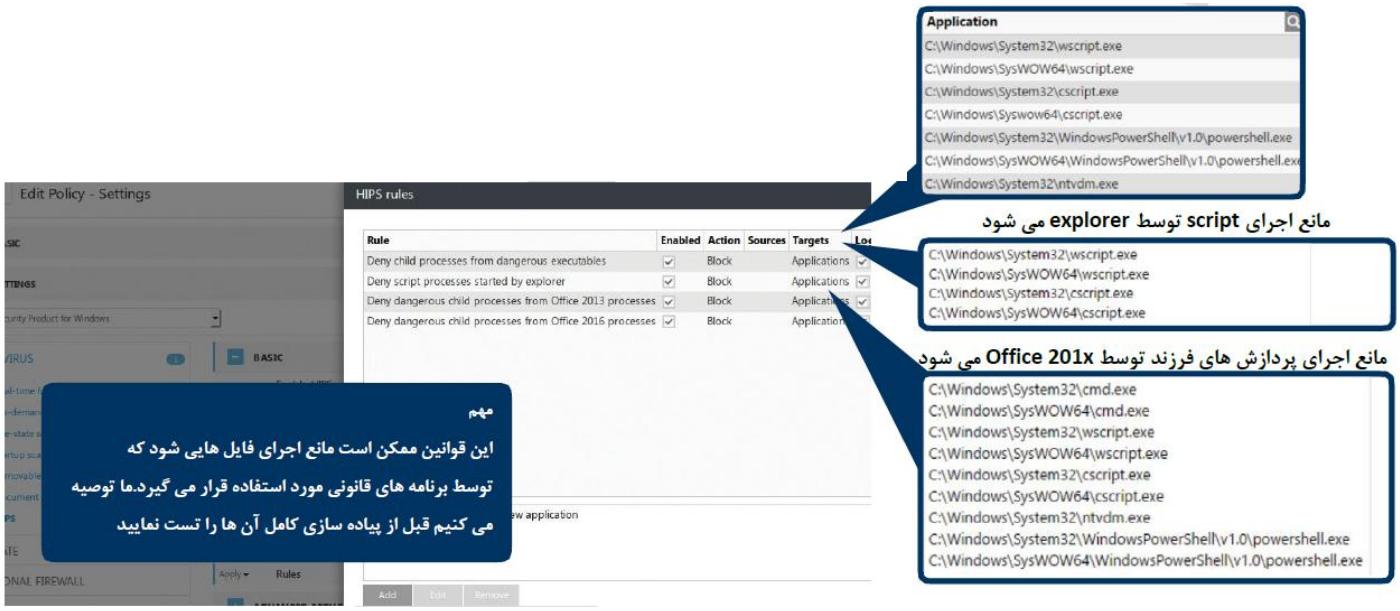
فایل تنظیمات Policy ها به همراه این راهنما در یک فایل ZIP در شاخه Policy برای شما ارسال شده است.

قوانینHIPS برایENDPOINT SECURITY وENDPOINT ANTIVIRUS

سیستم پیشگیری از نفوذ مبتنی بر میزبان *HIPS* سیستم را از داخل مورد محافظت قرار میدهد .این سیستم قادر است تا اقدامات غیر مجاز فرآیندها را قبل از اجرا قطع نماید .این کار با منع اجرای *Javascrip* و *script* های دیگر انجام می پذیرد.
همچنین *HIPS* قسمتی از *ESET File Security* برای *Windows Server* نیز می باشد و روی سرورها نیر قابل اجرا است .لطفا توجه داشته باشید که *HIPS* تمایزی میان *script* های قانونی و غیر قانونی انجام نمی دهد.

چگونه سیاست ها را وارد برنامه کرده و آن ها را اعمال کنیم
1.وارد کنسول وب *ERA 6* شوید : https://ipserver/era
2.به قسمت *ADMIN > Policies* بروید.
3.در پایین کنسول با استفاده از دکمه *"Policies"* گزینه *"Import"* را انتخاب کنید.
4.سپس سیاست های HIPS را از داخل شاخه Policy در فایل ZIP همراه این راهنما ، Import کنید.
5.در نهایت سیاست ها را با دکمه Assign Group به یک گروه یا یک کلاینت خاص اختصاص دهید.

تذکر : سیاست های HIPS برای ESET Endpoint و ESET File Security در دوفایل مجزا در شاخه Policy قرار دارند. سیاست HIPS Policy for FileSecurity for Servers.dat برای ویندوز های سرور با آنتی ویروس ESET File Security For Microsoft Server قابل اعمال میباشد.



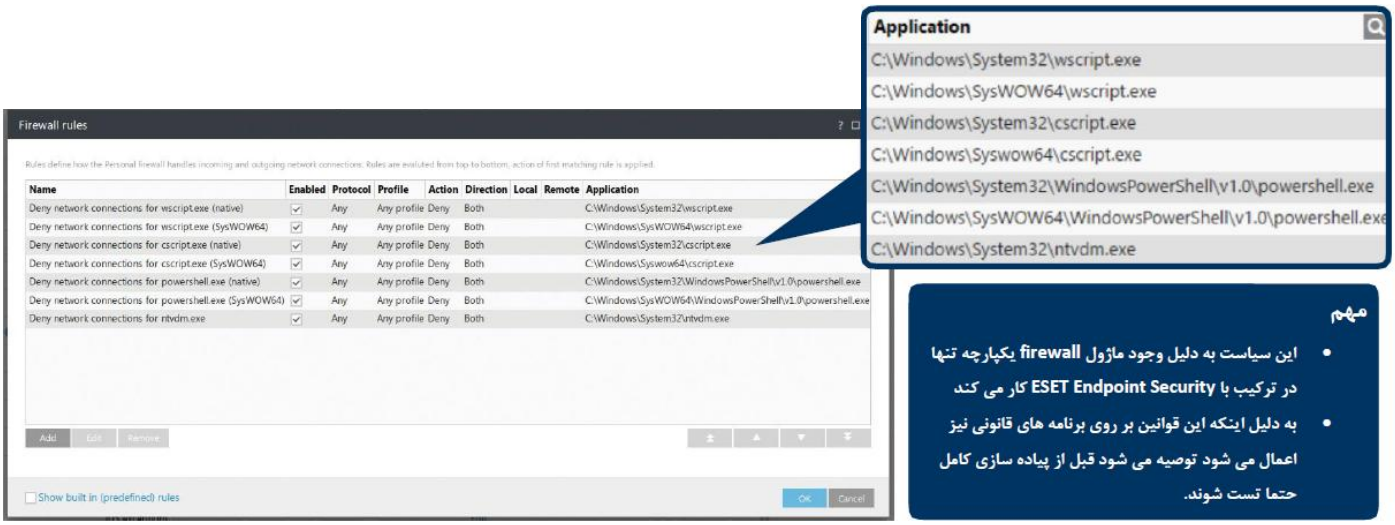
قوانین FIREWALL برای ENDPOINT SECURITY :

با استفاده از این سیایت ها *ESET Endpoint Security* به دلیل وجود *firewall* یکپارچه از دانلود تروجان جلوگیری می نماید.
با اعمال این قوانین *firewall* ، *ESET Endpoint Security* از دانلود موارد مخرب جلوگیری می نماید و مانع اتصال *scrip* های دیگر به اینترنت می شود.

چگونه سیاست ها را وارد برنامه کرده و آن ها را اعمال کنیم
1.وارد کنسول وب *ERA 6* شوید : https://ipserver/era
2.به قسمت *ADMIN > Policies* بروید.
3.در پایین کنسول با استفاده از دکمه *"Policies"* گزینه *"Import"* را انتخاب کنید.
4.سپس سیاست Firewall را از داخل شاخه Policy در فایل ZIP همراه این راهنما ، Import کنید.
5.در نهایت سیاست ها را با دکمه Assign Group به یک گروه یا یک کلاینت خاص اختصاص دهید.

!!! لطفا توجه داشته باشید که با وارد کردن قوانین *firewall* ممکن است این قوانین جایگزین قوانین دیگر شوند.

*** این سیاست به دلیل وجود ماژول firewall یکپارچه تنها در ترکیب با ESET Endpoint Security کار می کند.**
*** به دلیل اینکه این قوانین بر روی برنامه های قانونی نیز اعمال می شود توصیه می شود قبل از پیاده سازی کامل حتما تست شوند.**



قوانین ANTISPAM برای ESET Mail Server برای سرور MS EXCHANGE

با استفاده از قوانین درست *antispam* ، ایمیل های دریافتی به صورت خودکار فیلتر می شوند. این تنظیمات تضمین می کنند که فایل پیوست مخرب *dropper* درون صندوق ایمیل کاربر نهایی قرار نگیرد و *ransomware* فرصت اجرا بر روی سیستم را پیدا نکند.

چگونه سیاست ها را وارد برنامه کرده و آن ها را اعمال کنیم :

1.وارد کنسول وب *ERA 6* شوید : https://ipserver/era

2.به قسمت *ADMIN > Policies* بروید.

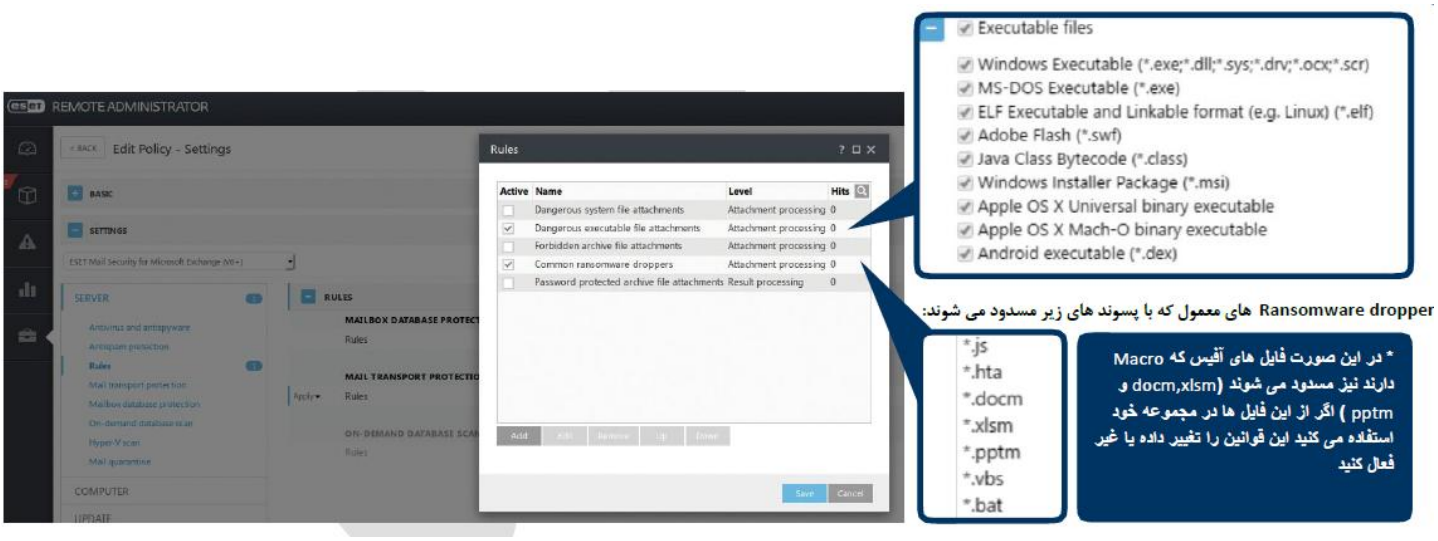
3.در پایین کنسول با استفاده از دکمه *"Policies"* گزینه *"Import"* را انتخاب کنید.

4.سپس سیاست Antispam را از داخل شاخه Policy در فایل ZIP همراه این راهنما ، Import کنید.

5.در نهایت سیاست ها را با دکمه Assign Group به یک گروه یا یک کلاینت خاص اختصاص دهید.

مهم:

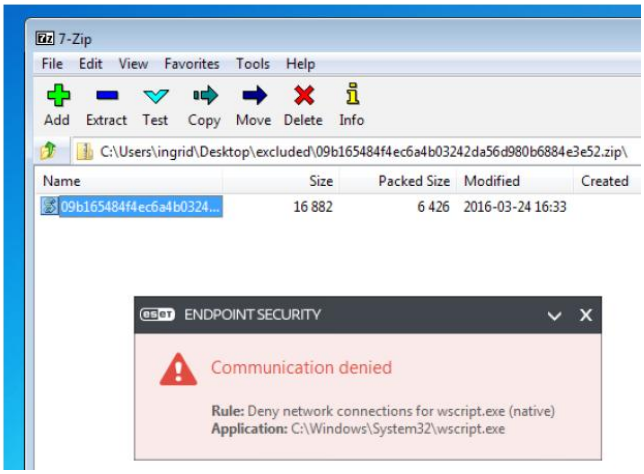
ESET Mail Security برای *Microsoft Exchange Server* را به جدیدترین نسخه *6.3.x* یا بالاتر به روز رسانی کنید تا قوانین فیلترینگ به درستی اجرا شوند.

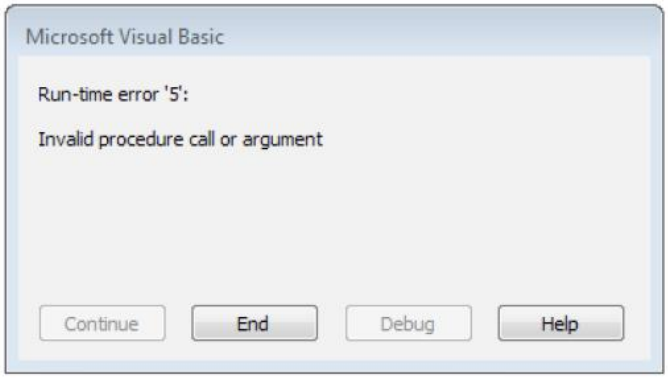


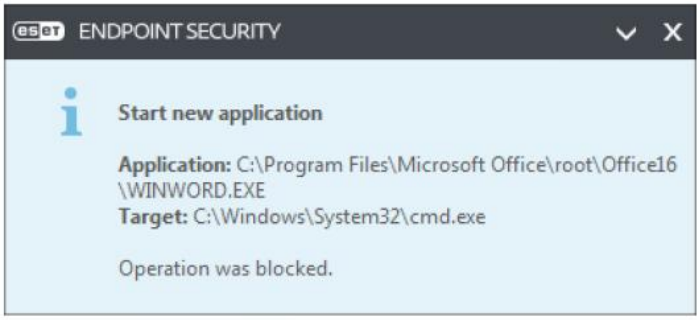
نتیجه راه اندازی ESET ANTI-RANSOMWARE :

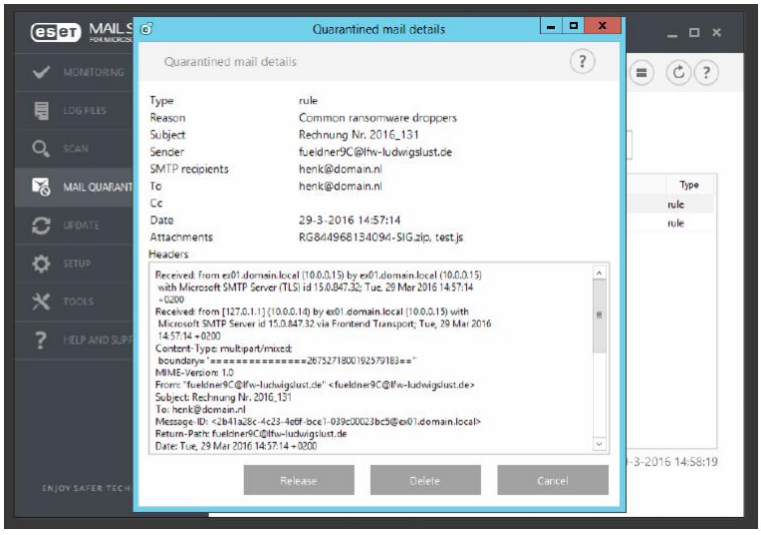
با راه اندازی کامل *ESET Anti-RansomWare* به علاوه تنظیمات سخت گیرانه بر روی کلاینت ها ، Ransomware به همراه Dropperها و فایل های پیوست آن قبل از تشخیص به عنوان کد های مخرب فیلتر می شوند . ما آزمون هایی انجام داده ایم و در تمامی موارد *ransomware* هیچ شانسی برای رمزگذاری اطلاعات و یا شبکه پیدا نکرده است .

در آخر به این نتیجه می رسیم که با پیاده سازی و اعمال *ESET Anti-RansomWare* و *سیاست های* سختگیرانه تر بر روی راه حل های امنیتی ESET امکان آلوده شدن و رمزنگاری اطلاعات مهم سازمان به حداقل می رسد.









پس از اعمال سیاست های فوق میتوانید شبکه خود را با استفاده از اسکریپت های تست موجود در شاخه SampleScripts تست نمائید. این اسکریپت ها کاملا بی خطر می باشند و نمونه های شبیه سازی شده فایل های دانلود کننده باج افزار هستند.

برای اطلاعات بیشتر و اجرای سیاست های ضد باج افزار میتوانید با واحد پشتیبانی شرکت کامیران تماس حاصل نمائید.

تذکر : شبکه هایی که از ERA5 یا از آنتی ویروس های خانگی یا بدون کنسول مدیریت استفاده میکنند میتوانند به جای استفاده از این راهنما از ابزار رایگان ضد باج افزار شرکت کامیران بر روی سیستم های شبکه خود استفاده نمایند. این ابزار در سایت شرکت برای دانلود در دسترس شما میباشد. پس از اعمال ابزار ضد باج افزار حتما با استفاده از اسکریپت های تست ، امنیتی سیستم های خود را چک نمائید.
توصیه اکید ما استفاده از کلیه راه کارها و سیاست های ضد باج افزاری کامیران میباشد.

خواهشمند است برای دریافت آخرین اخبار امنیتی مقابله با ویروس ها و باج افزار های جدید در کانال امنیتی تلگرام شرکت عضو شوید : @KAMIRANChannel : https://telegram.me/kamiranchannel

با تشکر از توجه شما

KAMIRAN

لابراتوآر ویروس شناسی شرکت مهندسی کامیران
نمایندگی رسمی ESET و Kaspersky در ایران

www.KAMIRAN.Asia

02147251