**اسفند ماه 1396**

# راه های مقابله با باج افزار Bad Rabbit

**تهیه شده توسط: امید عباسی**

**شرکت ارتباطات پرشیا**

## Bad Rabbit (خرگوش بد):

Bad Rabbit یکی از باج افزارهای جدیدی که در سال 2017 در فضای وب منتشر شد، که کاربران را تهدید به پاکسازی اطلاعاتشان در ازای عدم دریافت مبلغ مورد نظرشان می کند. Bad Rabbit بمانند WannCry و NotPetye بطور گسترده گسترش نیافته است.

بر اساس تحقیقات شرکت Kspersky، این یک حمله هدفمند علیه شبکه شرکتهای بزرگ است، که از روشی مشابه حمله ExPetr استفاده می کند، اما این شرکت نمی تواند تایید کند، که Bad Rabbit با ExPetr مرتبط است. شرکت Kaspersky اعلام کرده که وب سایت های خبری و رسانه ای بیشتر مورد حمله این باج افزار قرار گرفته اند. بیشتر قربانیان این حمله در روسیه قرار دارند و حملات مشابه، اما کمتر در اوکراین و سپس ترکیه و آلمان گزارش شده است.

محصولات Kaspersky تاکنون توانسته اند حملات این باج افزار را با مشخصات زیر شناسایی کنند:

- Trojan-Ransom.Win32.Gen.ftl
- Trojan-Ransom.Win32.BadRabbit
- DangerousObject.Multi.Generic
- PDM:Trojan.Win32.Generic
- Intrusion.Win.CVE-2017-0147.sa.leak

**برای جلوگیری از قربانی شدن توسط باج افزار Bad Rabbit اقدامات زیر را انجام دهید :**

- کاربرانی که از محصولات Kaspersky استفاده می کنند:

از فعال بودن امکانات (features)، System Watcher و Kaspersky Security Network اطمینان حاصل کنید. درصورت غیرفعال بودن، این امکانات را فعال کنید.

- دیگر کاربران:

فایل های زیر را بلاک (مسدود) کنند:

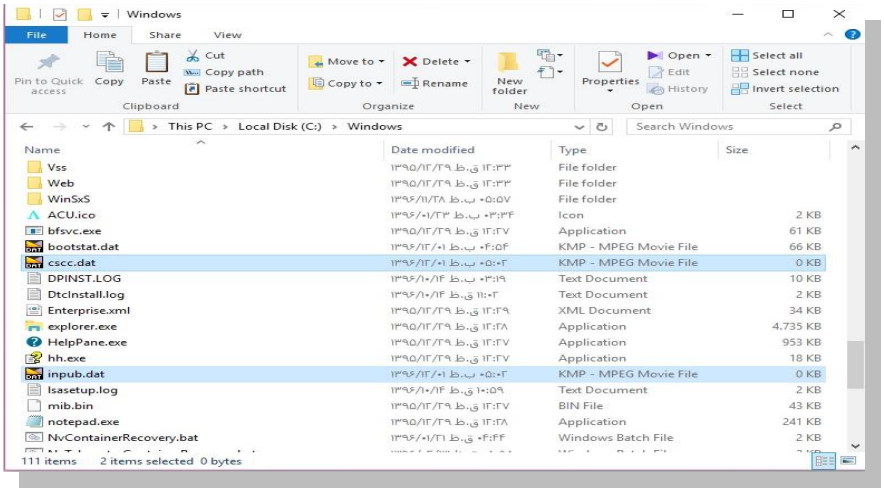
- C:\Windows\infpub.dat
- C:\Windows\cscc.dat
- C:\Windows\dispci.exe
- Flashutil.exe

- سرویس WMI غیرفعال (Disable) کنند ، برای جلوگیری از انتشار بدافزارها در شبکه.

نکته: باید توجه کرد که نرم افزارهای در شبکه وجود دارند که از سرویس WMI استفاده می کنند، و شاید امکان غیرفعال کردن این سرویس امکان پذیر نباشد.

- فایل های جعلی زیر را ایجاد کنید و طبق مراحل زیر سطح دسترسی برای آن تعیین کنید.
- C:\Windows\infpub.dat
- C:\Windows\ccsc.dat

فایل های فوق را ایجاد کرده و درمسیر بالا کپی کنید. (تصویر1)



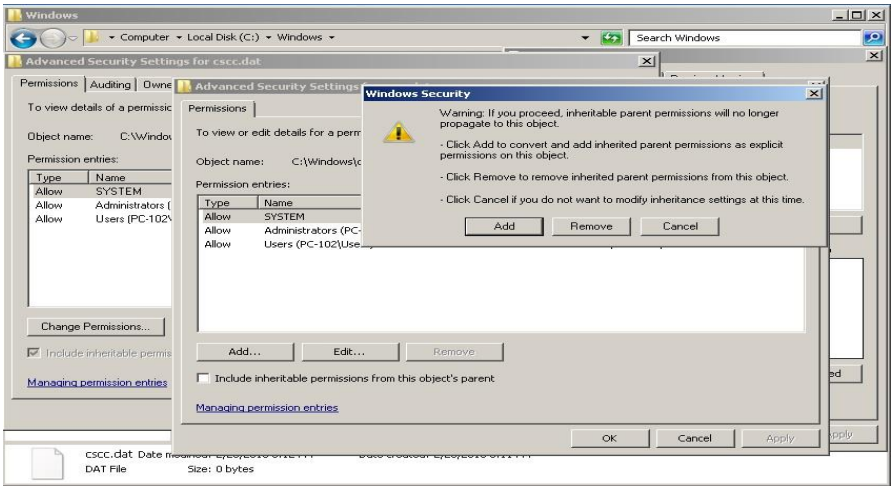

تصویر 1

طبق مراحل زیر سطح دسترسی را از تمامی کاربران و گروه ها بر روی این دو فایل مسدود کنید، این عمل باعث می شود که هیچ فایلی مشابه این دو فایل در این مسیر نتوان ایجاد و یا جایگزین شود.

ابتدا بر روی فایل مورد نظر کلیک راست کرده ومراحل زیر را ادامه می دهیم:

Properties ➡ Security Tab ➡ Advanced ➡ Change permissions

سپس Include inheritable permissions from this object's parent را از حالت انتخاب خارج کنید و بعد از آن بروی Remove کلیک کرده، درآخر دکمه OK را کلیک کنید و مراحل را تائید کنید.(تصویر۲)




تصویر 2

## توصیه ای برای همه:

- از داده های خود نسخه پشتیبان تهیه کنید.
- ویندوز و آنتی ویروس خود را بروز نگه دارید.
- پول درخواست شده (باج) را پرداخت نکنید.

در ادامه ما قصد داریم روش بلاک کردن فایل های اجرای مربوط به باج افزار Bad Rabbit را در کنسول Kaspersky Security Center، که این فایل ها شامل موارد زیر می باشند:

dispci.exe

flashutil.exe

برای این منظور از Hash code های مربوط به این فایل ها استفاده می کنیم، در ادامه توضیح مختصری در مورد Hash خواهیم داد و سپس به نحوهء بلاک کردن این فایل ها در Kaspersky Security Center می پردازیم.

## Hash:

Hash که به آن Digest یا Hash code نیز گفته می شود، فرآیندی است که بصورت ریاضی، حجم یک جریان داده را به یک طول ثابت کاهش می دهد. در واقع Hash code ها طبق یکسری الگوریتم هایی بر روی فایل ها، محاسبات انجام می دهند و برای آنها یک کد یکتا (Unique) تولید می کنند، توجه داشته باشید هیچ دو فایلی، Hash code مشابه هم ندارند مگر اینکه هر دو، یک فایل باشند ولی با نام های متفاوت ویا درمکان های متفاوت. بنابراین می توان Hash code را اثر انگشت فایل نامید.

انواع مختلفی از الگوریتم های قوی Hashing، برای استفاده در برنامه های کاربردی موجود هستند، که مهم ترین آنها MD5(Message-Digest) و الگوریتم SHA(Security Hash Algorithm) که این الگوریتم شامل (SHA-1,SHA256,SHA-384,SHA-512) می باشد.

### نحوه بلاک کردن فایل اجرای توسط Kaspersky Security Center:

همان طور که می دانیم Kaspersky Security Center، نسخه سرور می باشد. هرگونه تنظیمات و یا Policy بروی آن اعمال کنیم، بعد از بروزرسانی عملاً تمام کلاینت های که نسخه Kaspersky Endpoint Security دارا می باشند و تحت سرور هستند، این پیکربندی ها بر روی آنها اعمال می شود. یکی از قابلیت های مهم این نرم افزار امنیتی بلاک کردن فایل ها براساس Hash Code فایل می باشد.

برای بلاک کردن این فایل ها ابتدا باید Hash code مربوط به فایل را پیدا کنیم، برای این منظور شما می توانید از روش های زیر استفاده کنید:

1- وب سایت (سایت www.onlinemd5.com )
2- نرم افزار ( نرم افزار Hash Tab )

بنابراین در ادامه می خواهیم توسط Kaspersky Security Center، فایل های اجرای مربوط به باج افزار Bad Rabbit را بر اساس Hash code های بدست آمده از این فایل ها توسط شرکت های امنیتی را (طبق جدول۱) بلاک (مسدود) کنیم و از اجرای آن فایل ها جلوگیری کنیم.

| Dropper - Adobe_Flash_Player.exe (originally Flashutil.exe) | |
|---|---|
| **MD5** | 1d724f95c61f1055f0d02c2154bbccd3 |
| **SHA-256** | 630325cac09ac3fab908f903e3b00d0dadd5fdaa0875ed8496fcbb97a558d0da |
| **DiskCryptor Client – dropped as dispci.exe** | |
| **MD5** | b14d8faf7f0cbcfad051cefe5f39645f |
| **SHA-256** | 8ebc97e05c8e1073bda2efb6f4d00ad7e789260afa2c276f0c72740b838a0a93 |

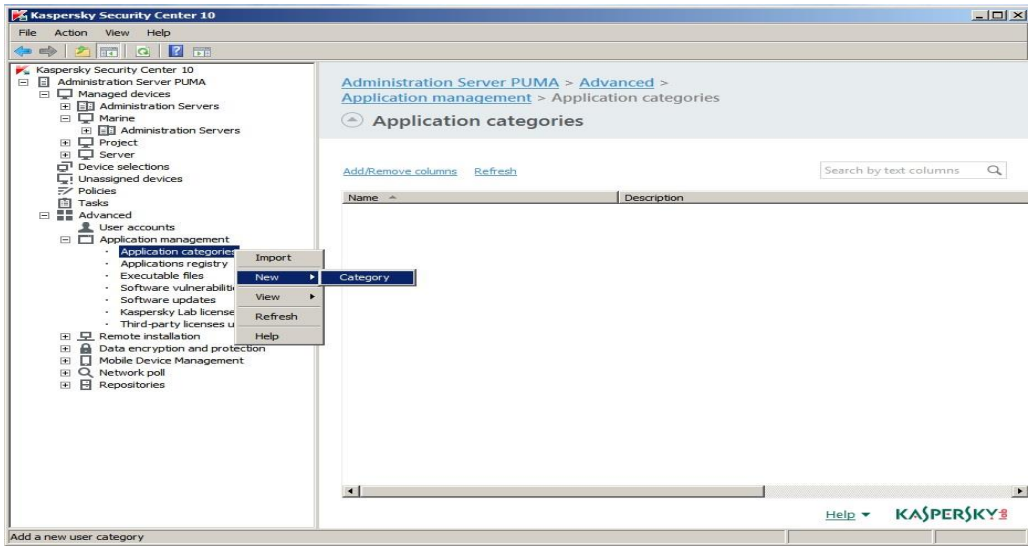
جدول ۱

**بلاک کردن فایل ها در Kaspersky Security Center:**

1. ابتدا از طریق سرور، وارد کنسول Kaspersky Security Center شده، از قاب سمت و مسیر زیر:

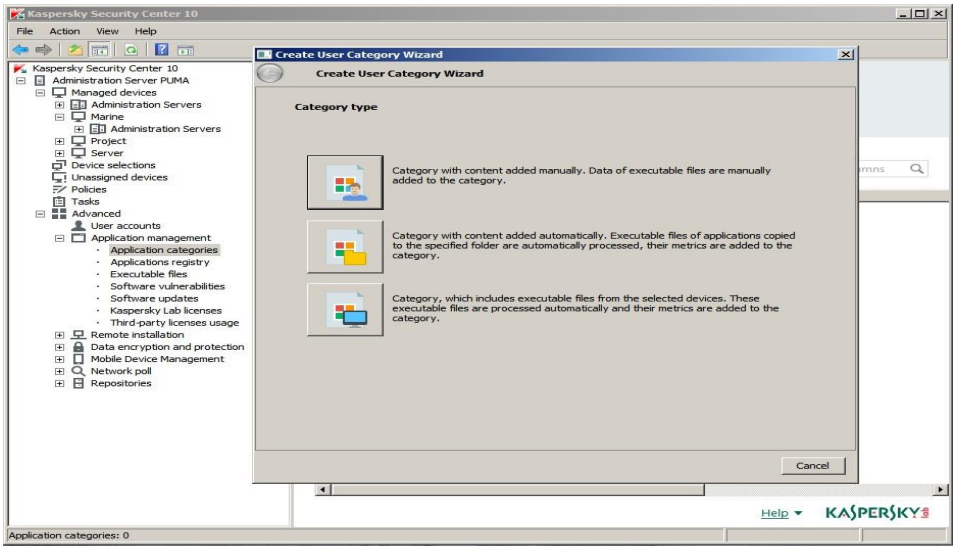
Administration Server ⇨ Advanced ⇨ Application management

گزینه Application Categories را انتخاب کرده و بروی آن کلیک راست کرده سپس New و در آخر Category را انتخاب می کنیم. (تصویر3)



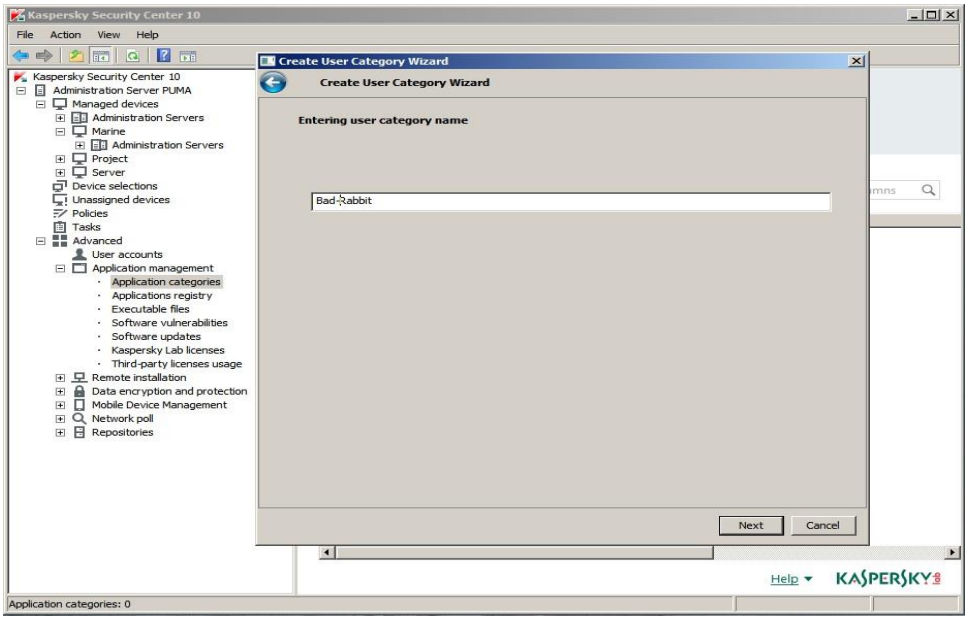

تصویر3

2. از پنجره Create User Category Wizard شده، گزینه ...Category with content added manually انتخاب می کنیم. (تصویر4)



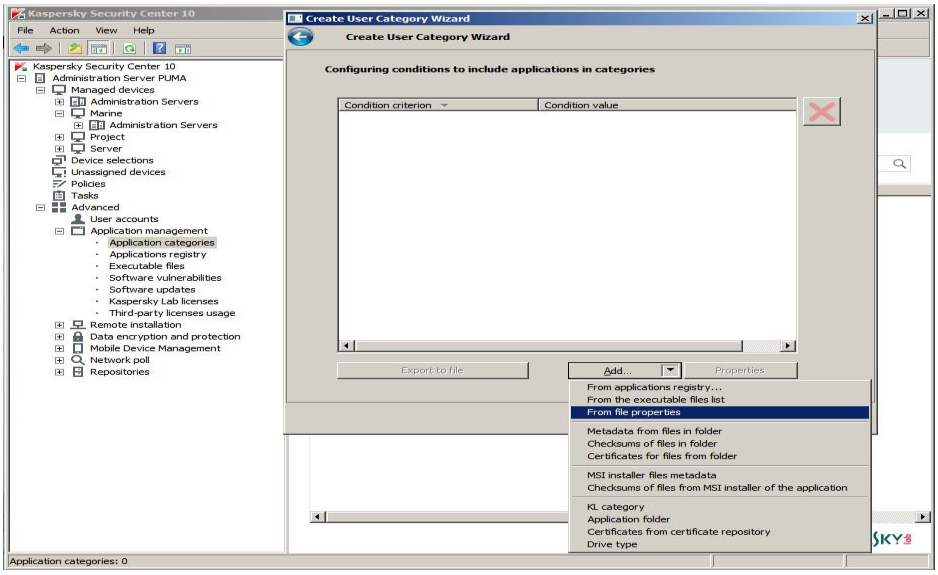

تصویر4

3. یک نام برای Category خود انتخاب کنید، سپس بر روی Next کلیک کنید. (تصویر5)



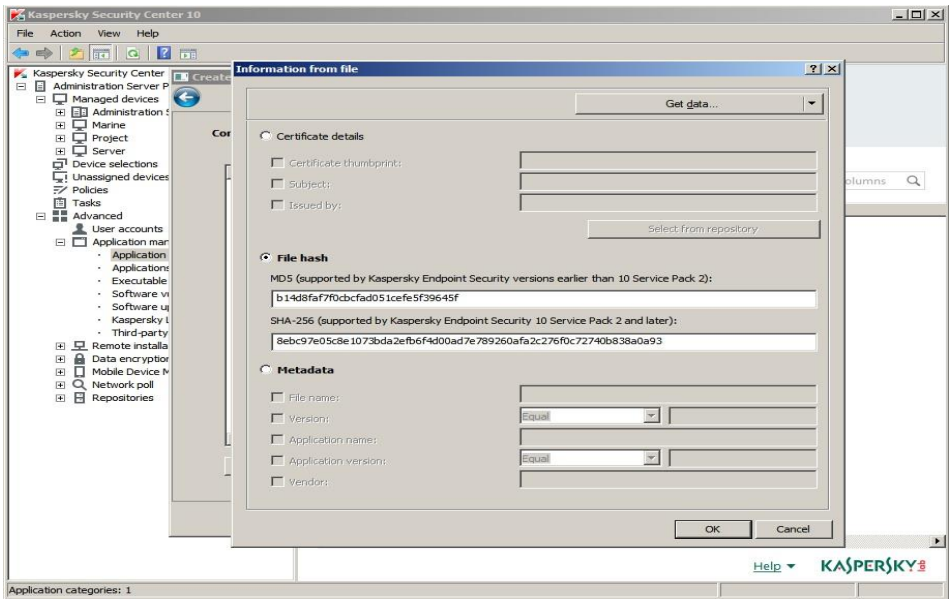

تصویر5

4. در این مرحله Condition یا شرطی را برای این Category تعیین می کنیم. برای این منظور بر روی فلش در کنار دکمه Add کلیک کرده و سپس گزینه From file properties را انتخاب می کنیم. (تصویر6)



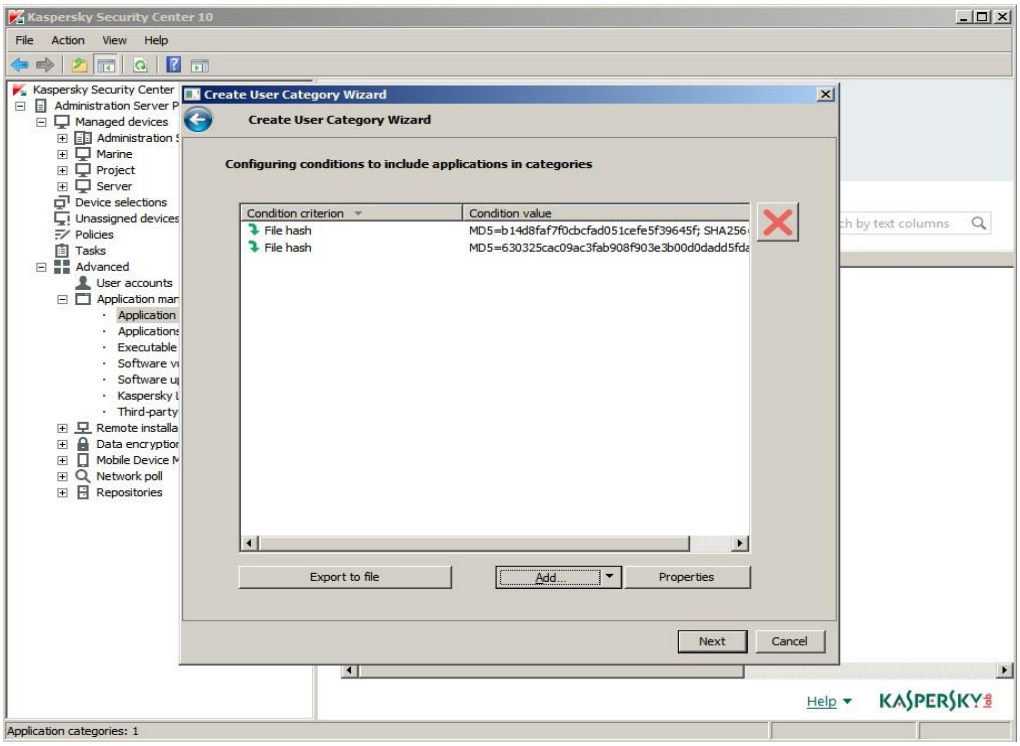

تصویر6

5. در پنجره Information from file گزینه File hash را انتخاب کرده و بر اساس جدول 1، Hash code ها را وارد کرده و سپس بر روی OK کلیک می کنیم. (تصویر7)




تصویر7

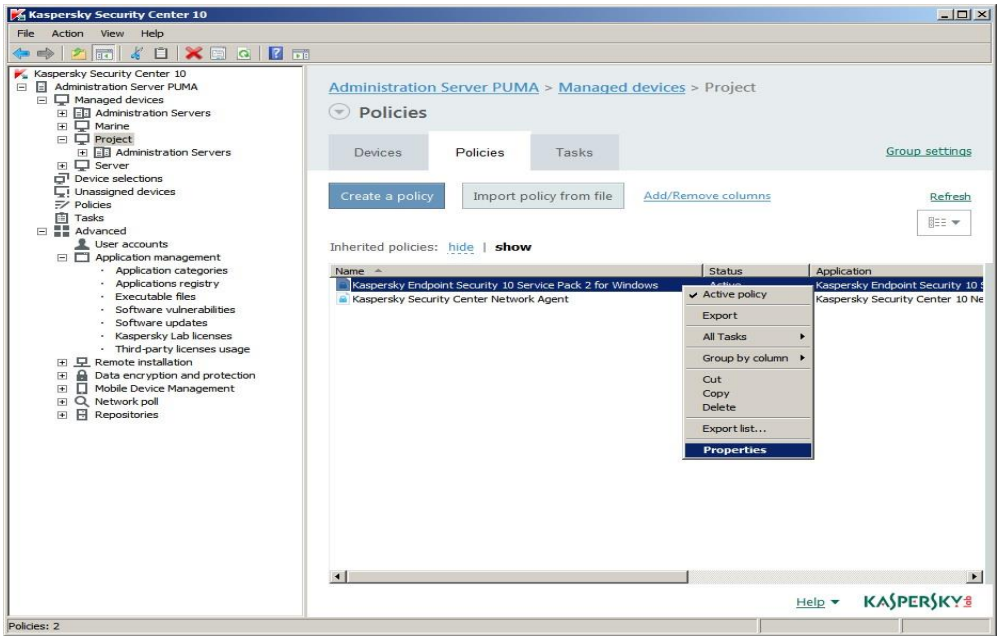
6. مرحله 4 و 5 را برای هر دو فایل تکرار کرده و بر روی Next کلیک می کنیم. (تصویر8)




تصویر 8

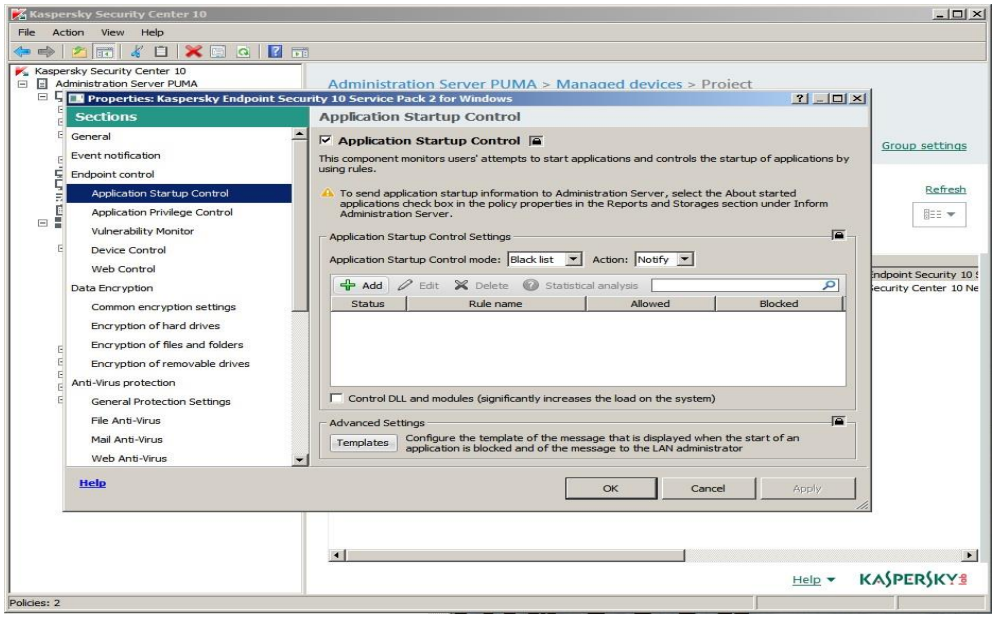
7. در مرحله بعد Exclusion ها تعیین می شود، که بر روی Next کلیک کرده و از مرحله عبور می کنیم و در مرحله آخر بر روی OK کلیک کرده و Category را ایجاد می کنیم، سپس می توانیم Category ایجاد شده را در پنجره Application Categories مشاهده کنیم.

8. در این مرحله می خواهیم فایل های موجود در Category Bad-Rabbit که ایجاد کردیم را بلاک یا مسدود کنیم، برای این منظور از کنسول Kaspersky Security Center و از مسیر Administration Server سپس زیر منوی Manage devices، بر روی گروه های ایجاد شده کلیک کرده و از قاب سمت راست، تب Policies را انتخاب کنید، سپس بر روی Policy تعریف شده کلیک راست کرده، Properties را انتخاب می کنیم.(تصویر 9)



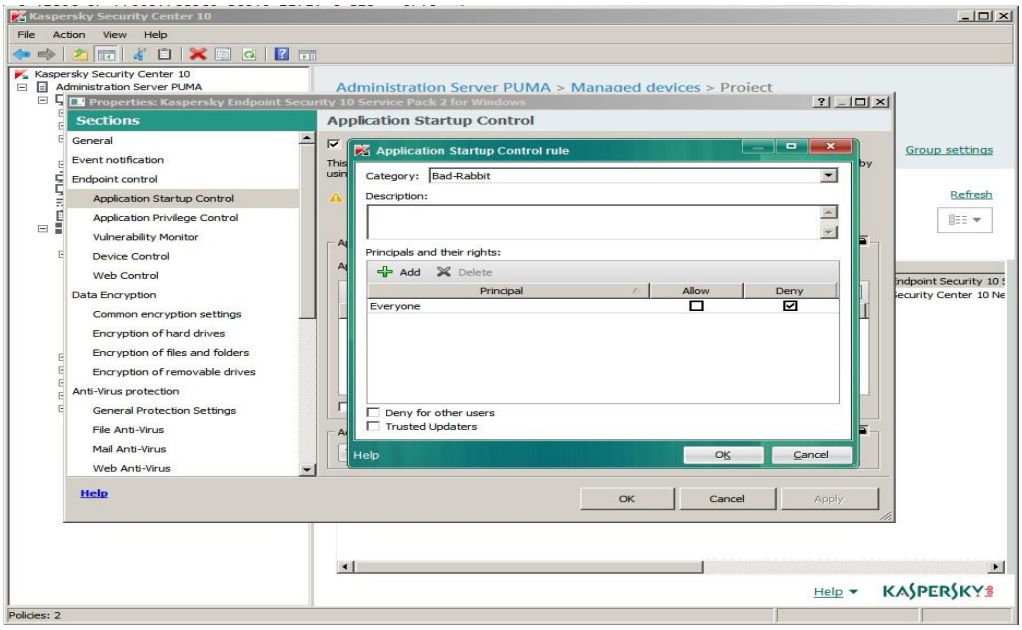

تصویر 9

9. در پنجره Properties از قاب سمت چپ، از منوی Endpoint control، زیر منوی Application Startup Control را انتخاب کرده و سپس در قاب سمت راست گزینه Add را انتخاب می کنیم و یک رول تعریف می کنیم. (تصویر 10)



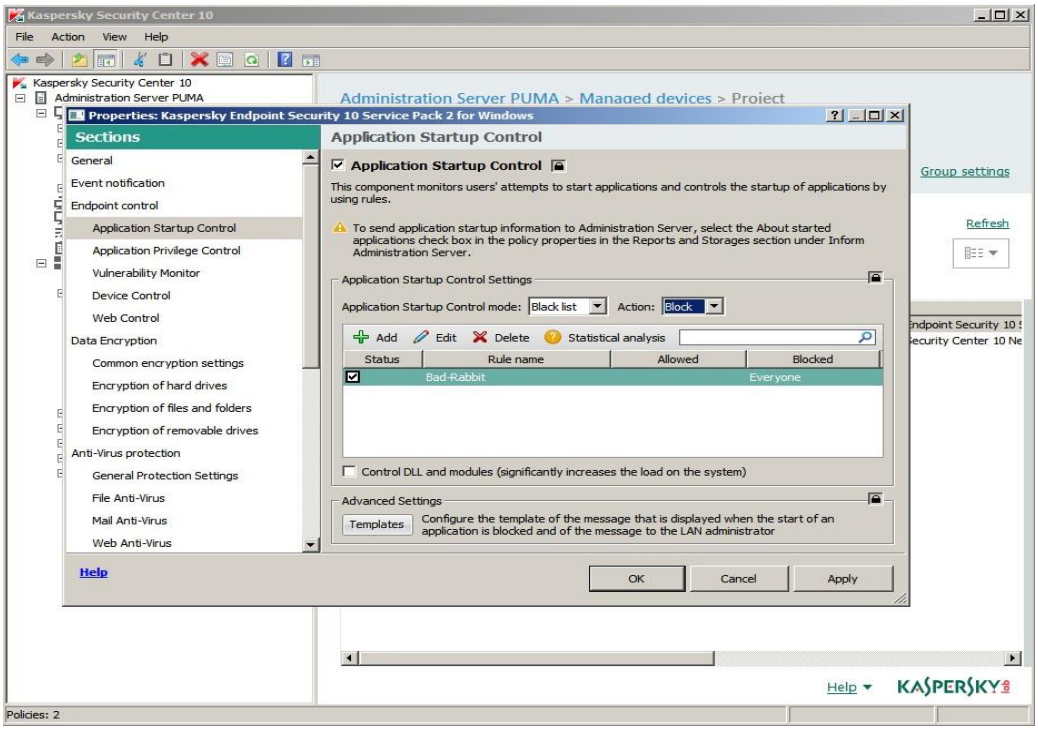

تصویر 10

10. در پنجره Application Startup Control rule، از قسمت Category، Category که ایجاد کرده ایم را انتخاب می کنیم. سپس از قسمت Principal and their rights بر روی Add کلیک می کنیم، از پنجره باز شده کاربر یا گروهی که می خواهیم این Rule بر روی آنها اعمال شود را انتخاب می کنیم (در این سناریو ما می خواهیم دسترسی را برای تمامی کاربران مسدود کنیم برای همین منظور Everyone انتخاب می کنیم.). درآخر Deny را انتخاب می کنیم و بر روی OK کلیک می کنیم. (تصویر11)




تصویر11

11. همان طور که مشاهده می کنیم Rule که در مراحل قبل ایجاد کردیم به لیست اضافه شده است. در نهایت می خواهیم Mode و Action را برای Rule تعریف شده انتخاب کنیم، از قسمت Application Startup Control Mode گزینه Black list را انتخاب می کنیم و همچنین در قسمت Action گزینه Block را انتخاب کرده و سپس OK می کنیم تا Rule ایجاد شده اعمال شود. (تصویر12)




تصویر 12

12. راحل 8 تا 11 را برای گروه های تعریف شده در قسمت Manage devices انجام دهید.

13- تمامی کلاینت ها را بروزرسانی کنید.

**Resources:**

www.kaspersky .com
blog.qualys.com
www.carbonblack.com