Exclude PUAs by their hash value in ESET Security Management Center

Anish | ESET Nederland - 2018-09-14 - Reacties (0) - ESET Security Management Center

Issue

- Create a policy to exclude PUAs by their hash value in ESET Security Management Center

Solution

1. Click **Tools → Quarantine** on the client machine that has already detected the PUA, and verify that the PUA is listed in the Quarantine list.

Figure 1-1
Click the image to view larger in new window

1. Open ESET Security Management Web Console (ESMC Web Console) in your web browser and log in. Click **More → Quarantine**. Verify that the PUA found on the client machine is listed in the Quarantine list.

Figure 1-2
Click the image to view larger in new window

1. Click **Client Tasks → Quarantine management → New**. Enter the necessary information in the **Basic** section.
2. Click the **Settings** section and select **Restore object(s) and Exclude in Future** from the **Action** drop-down menu. Select **Hash items** from the **Filter Type** drop-down menu.
3. Click **Add** in the **Hash Item(s)** section under **Filter Settings**, select the check box next to the PUA that was detected on the client machine and click **OK**.
4. Click **Finish** to complete the task and create a Trigger for this Client Task.

Figure 1-3
Click the image to view larger in new window

1. On the client machine, navigate to **Exclusions** (**Setup → Advanced Setup → Detection Engine → Files and folders to be excluded from scanning → Edit**). The PUA is now listed as an exclusion in the Exclusions list.

Figure 1-4
Click the image to view larger in new window

1. In ESET Security Management Center Web Console, click **Computers**, select the client computer and click **Show details → Configuration → Request Configuration**.

2. Select **Security product** and click **Open Configuration** and then click **Convert to Policy**. The policy with this excluded PUA is now available to use for any client computer.

Figure 1-5
Click the image to view larger in new window

1. Open the policy you just created and enter the necessary information in the **Basic** section. Click the **Settings**section, click **Detection Engine → Exclusions → Edit** and you can see the excluded PUA.

   

   Figure 1-6
   Click the image to view larger in new window

2. Click **Assign** and assign the policy with the PUA exclusion to other computers and click **Finish**.

KB Solution ID: KB6832 |Document ID: 25738|Last Revised: August 17, 2018