Configure HIPS rules for ESET business products to protect against ransomware

Ondersteuning | ESET Nederland - 2017-11-06 - 0 Comments - in KB

https://support.eset.com/kb6119

Issue

Configure additional ESET Remote Administrator (6.3 and later) HIPS rules in the following ESET products to protect against Filecoder (ransomware) malware

- ESET Endpoint Security
- ESET Endpoint Antivirus
- ESET Mail Security for Microsoft Exchange
- ESET File Security for Microsoft Windows Server

Click each image to open a new window for additional anti-ransomware best practices and additional policy configurations:

Details

Solution

To further help prevent ransomware malware on your Windows systems, create the following policy rules in ESET Remote Administrator version 6.3 or later:

Do not adjust policies on production systems

The following policy settings are additional configurations and

the specific settings needed for your security environment may vary. We recommend that you test the settings for each implementation in a test environment before using them in a production environment.

1. Open ESET Remote Administrator Web Console (ERA Web Console) in your web browser and log in. How do I open ERA Web Console?
2. Click **Admin** → **Policies**, select the Agent policy being applied to your server(s) (your default parent policy) and then click **Policies** → **Edit**.

   Alternatively, you can create a new policy in ESET Remote Administrator (6.x).

3. Expand **Settings** → **Antivirus**, click **HIPS** and then click **Edit** next to **Rules**.

Figure 1

Click the + to expand each section below to create the HIPS rules for the suggested processes.

I. Deny processes from script exe

cut abl es

II. De ny scri pt pro ces ses star ted by exp lore r

III. De ny chil d pro ces ses fro m Offi ce 20 13/ 20 16 pro ces ses

IV. De ny chil d

processes for regsrv32.exe

V. Deny child processes for mshta.exe

VI. Deny child processes for rundll32.exe

VII. De

Tags

Ransomware