ESET Tech Center

[KB6119] Configure HIPS rules for ESET business products to protect against ransomware

Ondersteuning | ESET Nederland - 2020-08-11 - Comments (0) - FAQ's

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 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

ESET's Host-based Intrusion Prevention System (HIPS) is included in ESET Endpoint Security, ESET Endpoint Antivirus, ESET Mail Security for Microsoft Exchange, and ESET File Security for Microsoft Windows Server. HIPS monitors system activity and uses a pre-defined set of rules to recognize suspicious system behavior. When this type of activity is identified, the HIPS self-defense mechanism stops the offending program or process from carrying out potentially harmful activity. Changes to the Enable HIPS and Enable Self-defense settings take effect after the Windows operating system is restarted.

By prohibiting the standard execution of JavaScript and other scripts, ransomware is not able to download or execute.

Solution

End of support for version 6.5 and 6.5 of ESET Remote Administrator / MDM

ESET Remote Administrator version 6.5 is currently in Limited Support status and will soon be in Basic Support status. It is expected to reach End of Life status in December 2020.

ESET Remote Administrator version 6.4 is currently in End of Life status and no longer available for download.
The MDM functionality in ESET Remote Administrator version 6 is currently in End of Life status and no longer available for download

- To see the list of products and dates for ESET end-of-life, visit the ESET End of Life policy (Business products)
- See our instructions for migrating ESET Remote Administrator to version 7 (ESMC).

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**.

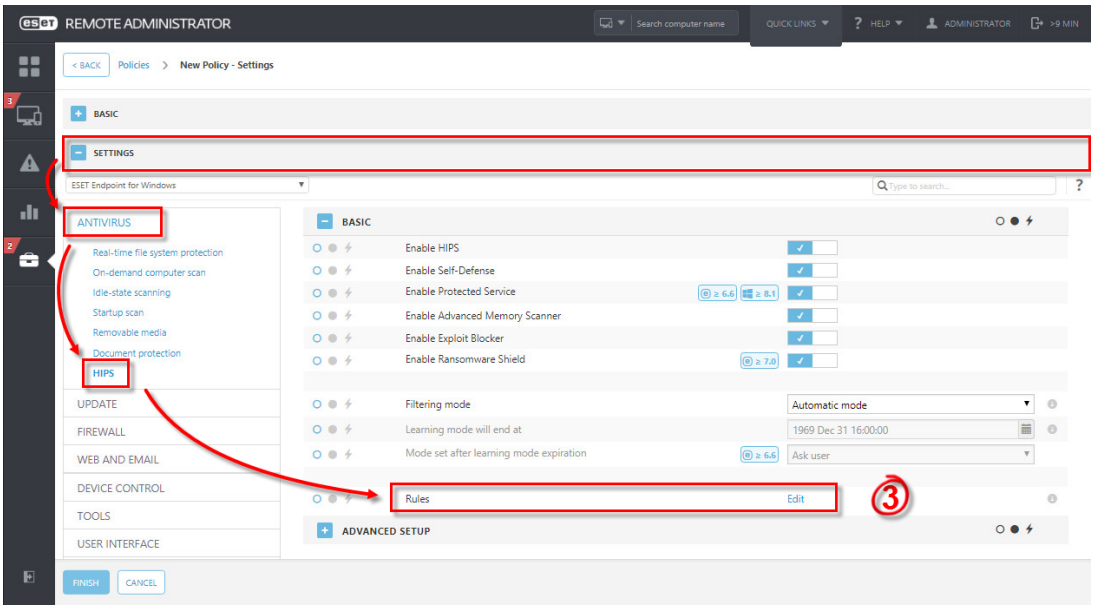

Figure 1

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

I. Deny processes from script executabl

es

II. Deny script processes started by explorer

III. Deny child processes from Office 2013/2016 processes

IV. Deny child proces

sesforregsrv32.exe

V. Denychildprocessesformshta.exe

VI. Denychildprocessesforrundll32.exe

VII. Denychi

ld
pr
oc
es
se
s
for
po
we
rs
he
ll.e
xe

Tags

Ransomware