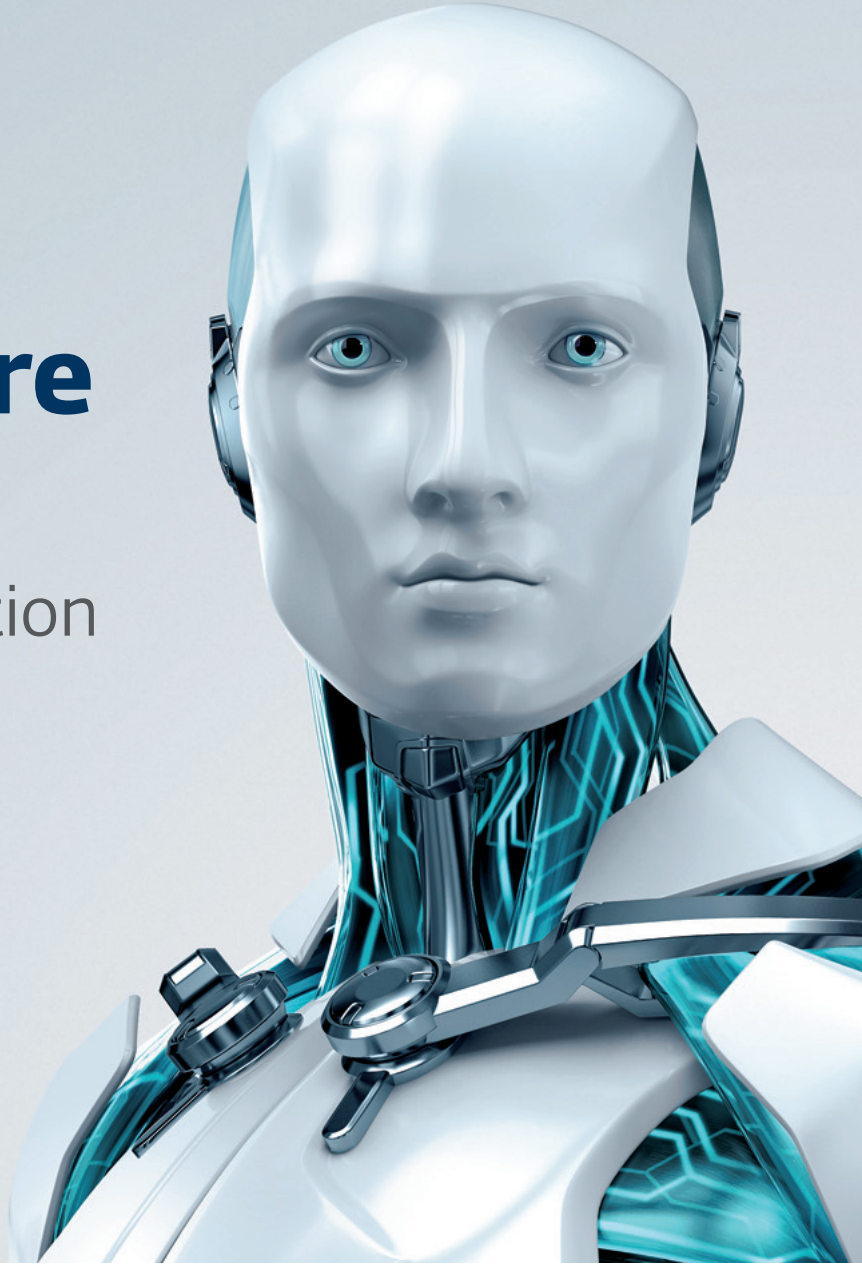
ESET Anti-Ransomware Setup

Multi-layered security against encryption



Document version:
1.1

Authors:
Michael van der Vaart, Chief Technology Officer | ESET Netherlands
Donny Maasland, Head of Cybersecurity Services and Research | ESET Netherlands

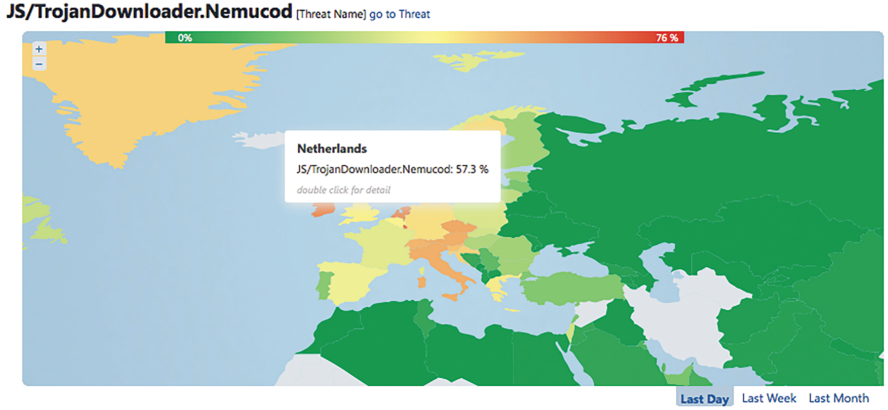
CONTENT

GOAL OF THIS TECH BRIEF

In this Tech Brief we describe the optimal settings of our ESET security solutions against the current form of ransomware and the most common infection scenarios. The goal is to protect our customers even better against a ransomware outbreak where valued data can be encrypted and/or held hostage, only to be released after a ransom is paid.

WHY THESE ADDITIONAL SETTINGS?

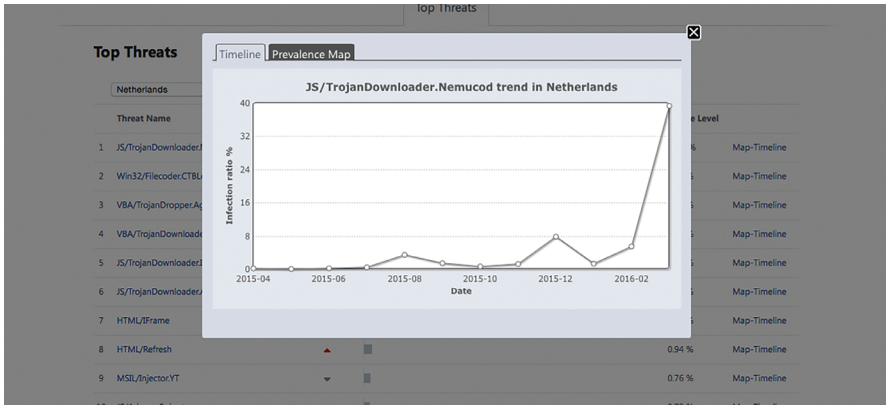
Close to 60% of all malware we detect in the Netherlands can lead to a ransomware infection.



Current ransomware attacks use advanced infection techniques allowing malicious malware to infect your device. They persuade people to execute a so-called dropper which in turn will download the malicious malware payload to start the encryption process. By attaching the dropper to an email, cybercriminals try to prevent detection at entry. In most cases a properly constituted phishing mail is used with a ZIP file as attachment. This ZIP file most commonly contains a JavaScript file of the type .JS.

Because JavaScript is used by numerous websites, it is impossible to block in the browser. Besides that, Windows also executes JavaScript directly.

Meanwhile the JavaScript code in the dropper is heavily obfuscated, defaced and continuously modified in order to prevent detection. This gives us the opportunity to influence the execution of potentially malicious code through standard processes, by using various security modules.

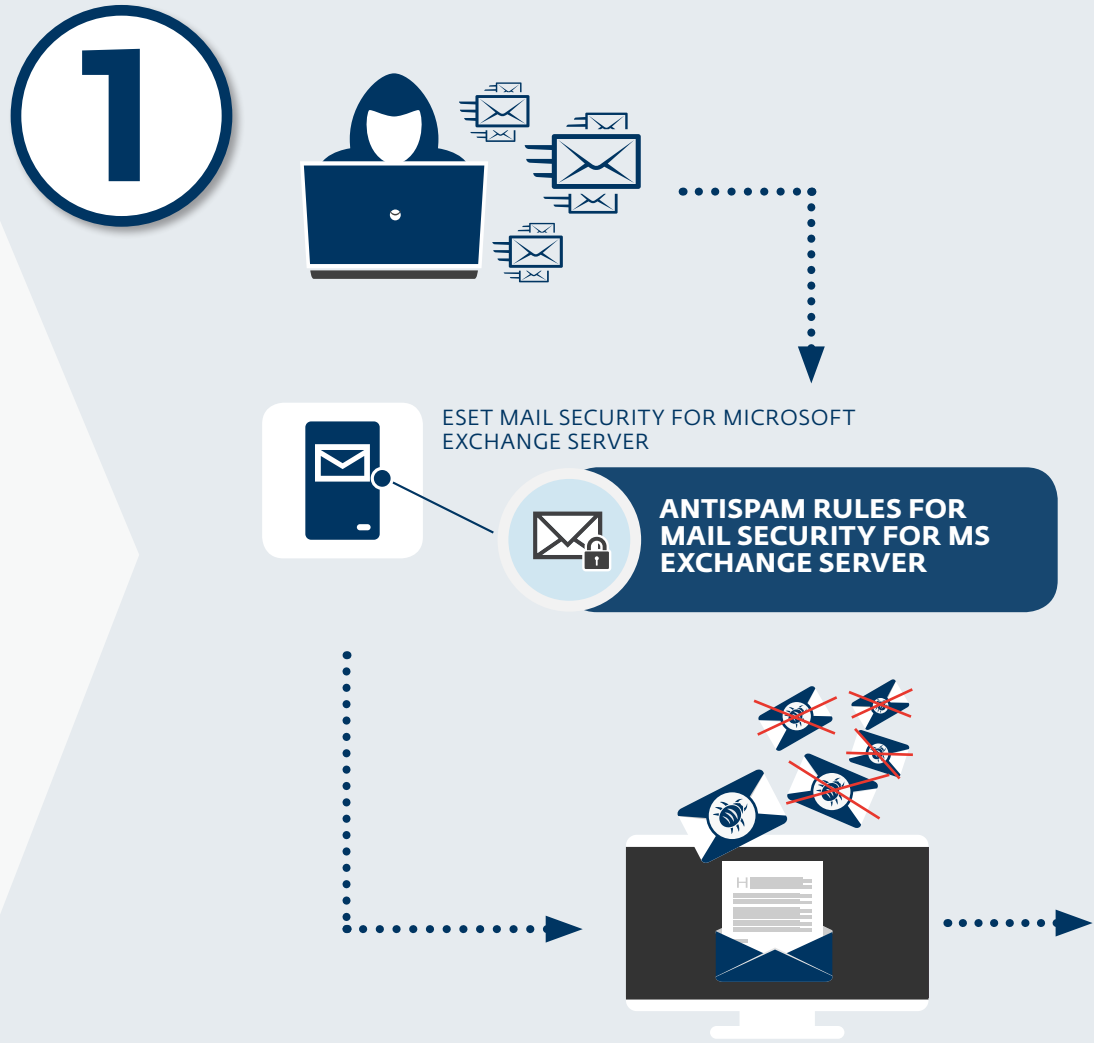


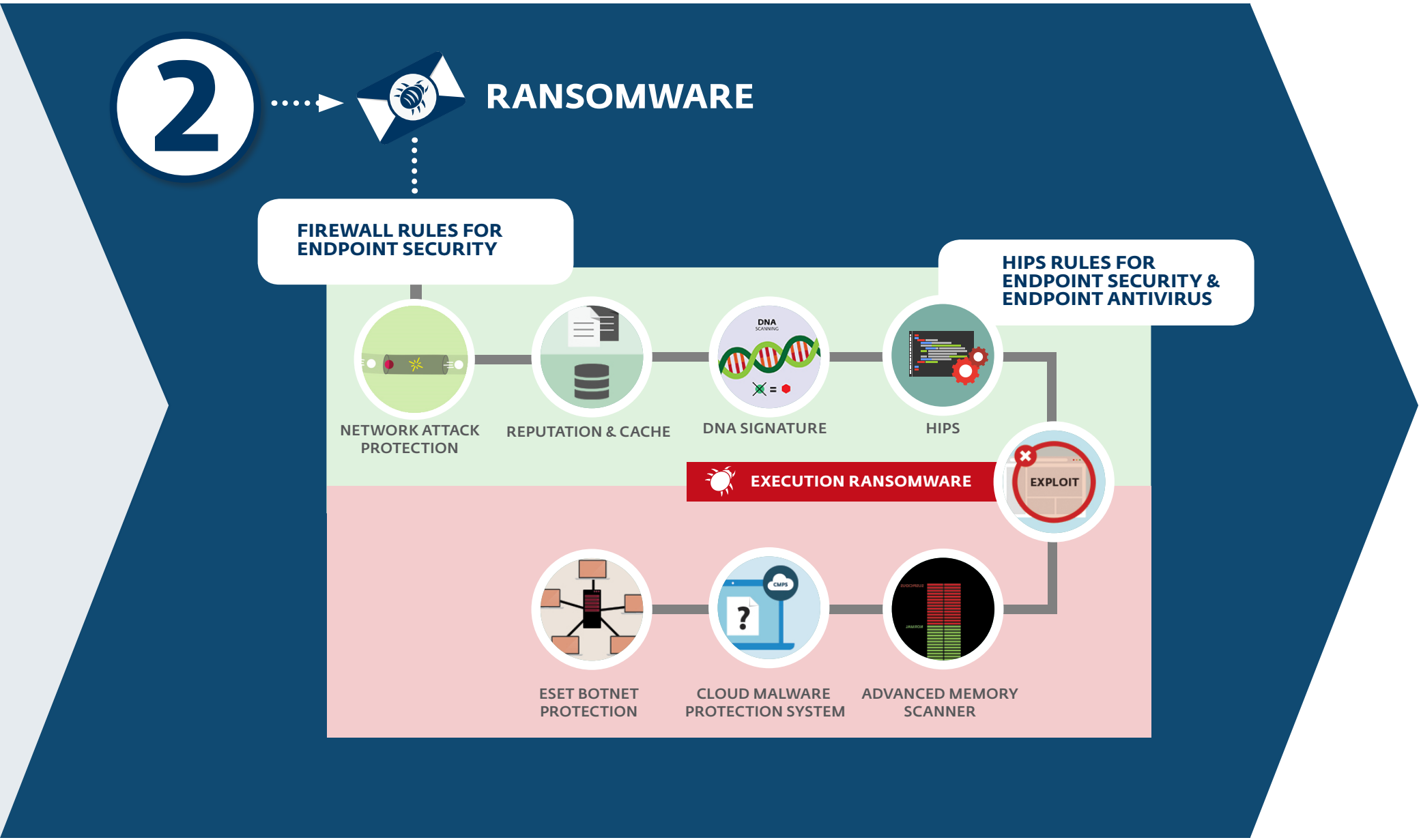
Disclaimer:
The ESET Anti-Ransomware Setup and policies are generically drawn and may vary by area We recommend to test the settings for each implementation in a customer area before fully implementing them.

ESET ANTI-RANSOMWARE SETUP FOR BUSINESS

By blocking the ransomware infection method (using a Javascript dropper), the additional settings of our ESET Anti-Ransomware Setup prevent malicious malware to start downloading. Because this approach shows to be very efficient, we decided to explain the additional settings in detail in this Tech Brief and offer it as a policy configuration which you are able to download and implement using our ESET Remote Administrator.

DOWNLOAD YOUR SETTINGS HERE




2
RANSOMWARE
FIREWALL RULES FOR ENDPOINT SECURITY
HIPS RULES FOR ENDPOINT SECURITY & ENDPOINT ANTIVIRUS
NETWORK ATTACK PROTECTION
REPUTATION & CACHE
DNA SIGNATURE
HIPS
DNA
SCANNING
EXECUTION RANSOMWARE
EXPLOIT
ESET BOTNET PROTECTION
CLOUD MALWARE PROTECTION SYSTEM
ADVANCED MEMORY SCANNER
CMPS

ANTISPAM RULES FOR ESET MAIL SECURITY FOR MS EXCHANGE SERVER

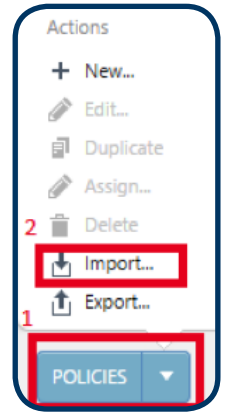
Using the right antispam rules, incoming emails are already being filtered on the mail server itself. This ensures that the attachment containing the malicious dropper will not be delivered in the mailbox of the end user and the ransomware is not given the chance to execute

Important:

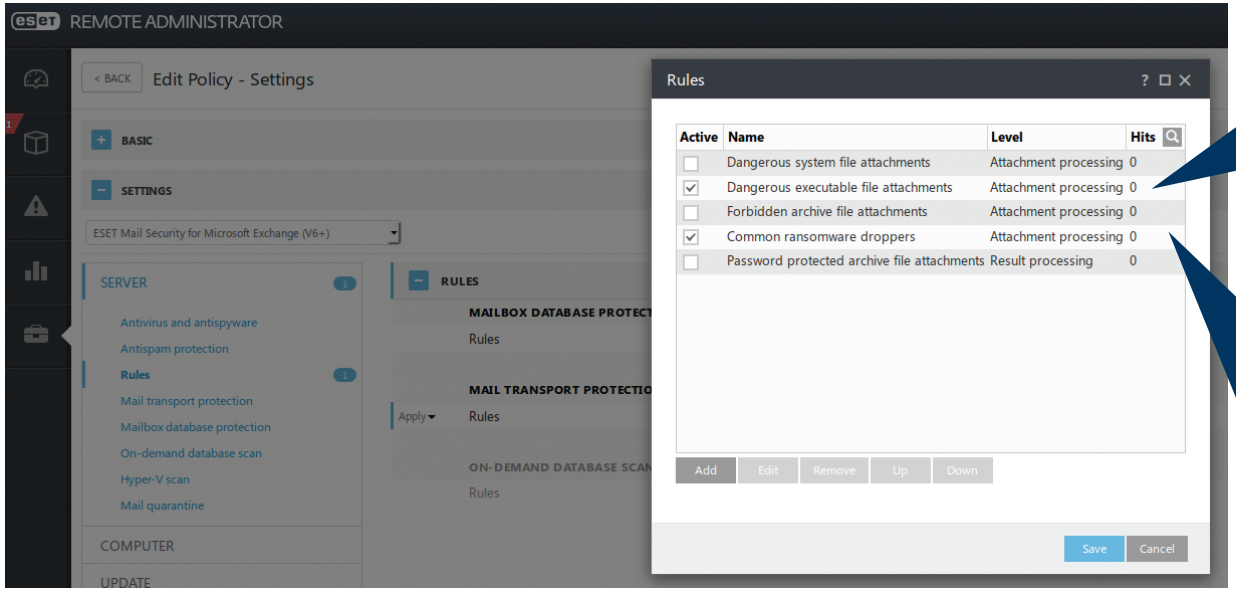
Upgrade ESET Mail Security for Microsoft Exchange Server to the latest available build 6.3.x or higher to ensure the working of the filtering rules.

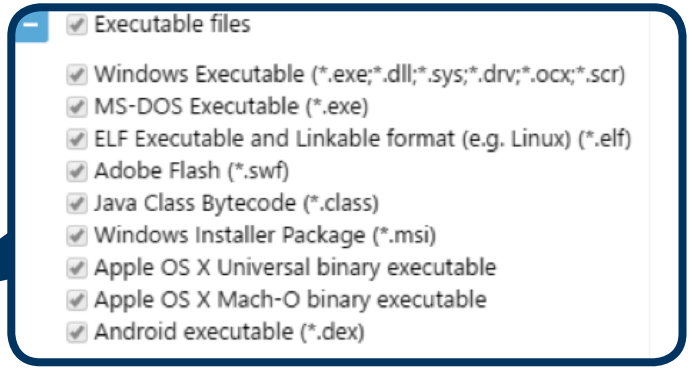
How to import and apply the policies*

1. Log in to ERA 6 Webconsole
2. Navigate to ADMIN > Policies
3. Then choose "Policies" and after that "Import"
4. Import the policies one at a time
5. Adjust the policies to a *a group* or *client*



*** Repetition is not necessary with other settings.**





Common ransomware droppers which block the following extensions*:

* In this case **Microsof Office files with Macro's will also be blocked (docm, xlsm and pptm)**. When such files are used within your area, this rule has to be adjusted or disabled.

FIREWALL RULES FOR ENDPOINT SECURITY

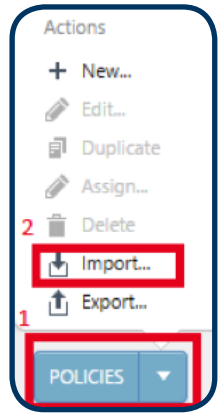
Should the dropper with malicious code be executed, ESET Endpoint Security still prevents the download of malware due to the integrated Firewall.

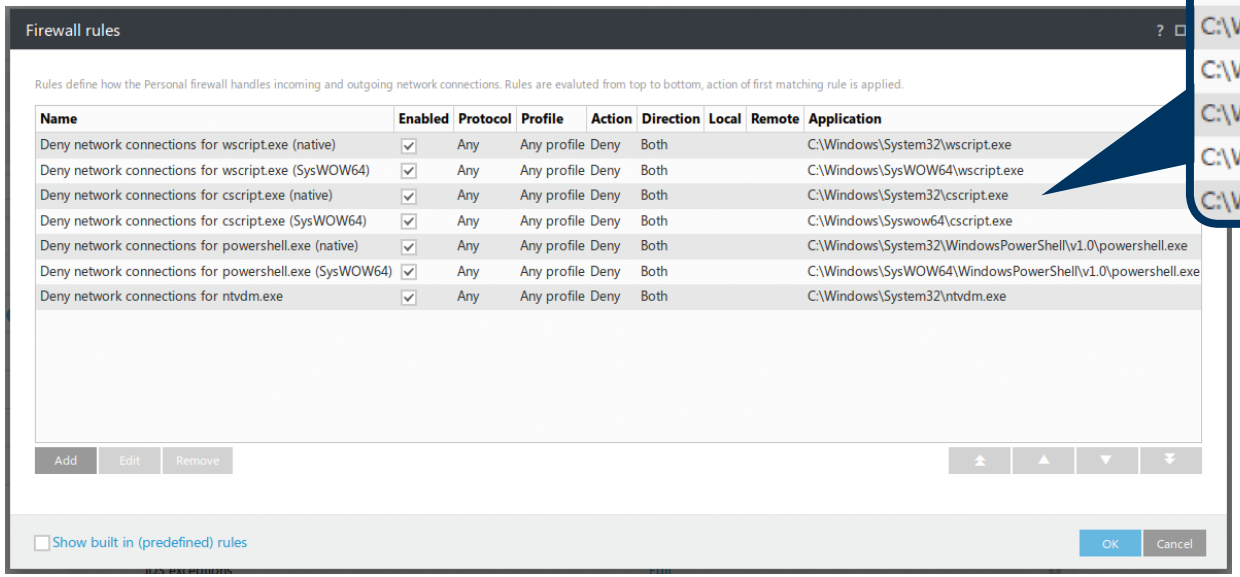
By applying these firewall rules ESET Endpoint Security will block the download of malicious payloads and deny other scripting access to the Internet.

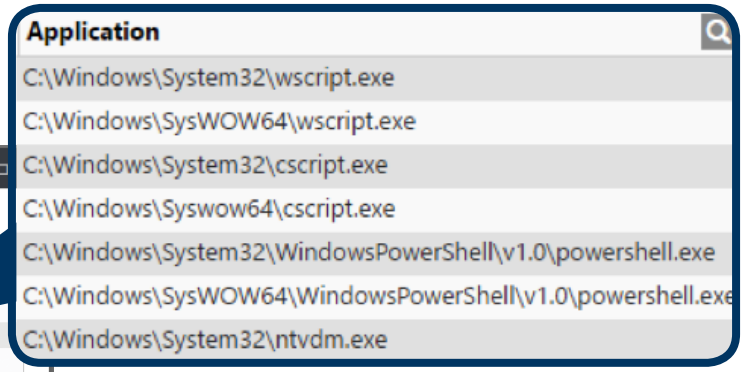
How to import and apply the policies

1. Log in to ERA 6 Webconsole
2. Navigate to ADMIN > Policies
3. Then choose "Policies" and after that "Import"
4. Import the policies one at a time
5. Adjust the policies to a *a group* or *client*

Please note that when importing the Firewall rules other rules may be overwritten.







IMPORTANT

- This policy only works in combination with ESET Endpoint Security because of the integrated firewall module.
- For these rules it also applies that legitimate applications can use the executables. We therefore recommend you to test this before fully implementing the policy within your area.

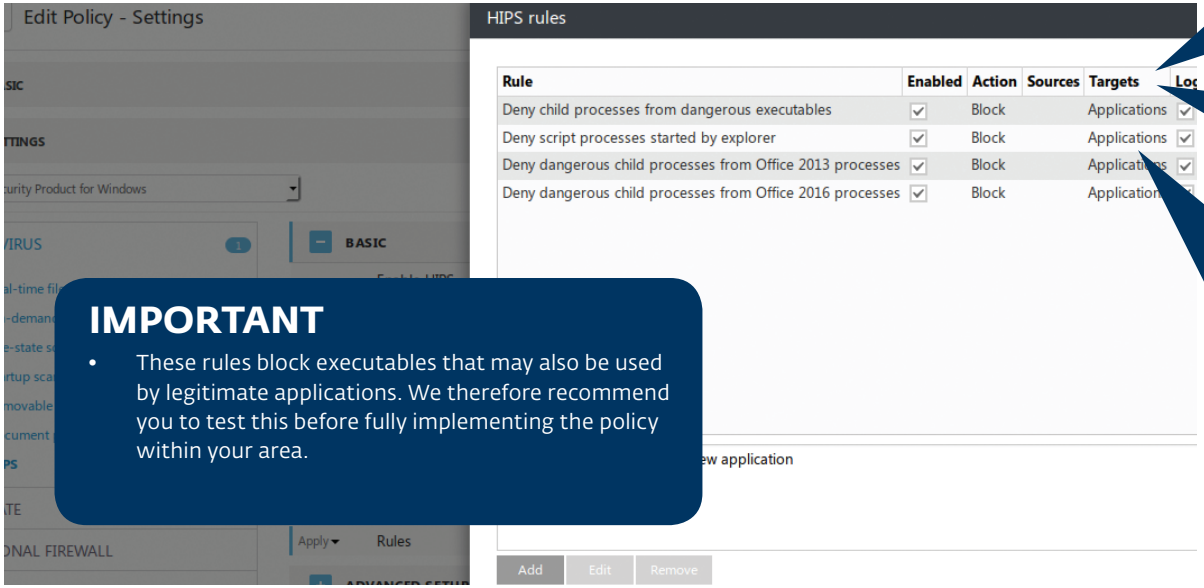
HIPS RULES FOR ENDPOINT SECURITY & ENDPOINT ANTIVIRUS

Host-based Intrusion Prevention System (HIPS) defends the system from within and is able to interrupt unauthorized actions from processes before they are being executed. By prohibiting the standard execution of JavaScript and other scripts, ransomware is not given the chance to execute malware, let alone download it.

Our HIPS is also part of the ESET File Security for Windows Server, making it applicable to servers. Please note that HIPS will not make a distinction in legitimate scripts starting in production areas.

How to import and apply the policies

1. Log in to ERA 6 Webconsole
2. Navigate to ADMIN > Policies
3. Then choose "Policies" and after that "Import"
4. Import the policies one at a time
5. Adjust the policies to a *a group* or *client*



IMPORTANT

- These rules block executables that may also be used by legitimate applications. We therefore recommend you to test this before fully implementing the policy within your area.

Deny child process from dangerous executables.

Application
C:\Windows\System32\wscript.exe
C:\Windows\SysWOW64\wscript.exe
C:\Windows\System32\cscript.exe
C:\Windows\Syswow64\cscript.exe
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
C:\Windows\System32\ntvdm.exe

Deny script processes started by explorer

C:\Windows\System32\wscript.exe
C:\Windows\SysWOW64\wscript.exe
C:\Windows\System32\cscript.exe
C:\Windows\SysWOW64\cscript.exe

Deny Dangerous child processes from Office 201x

C:\Windows\System32\cmd.exe
C:\Windows\SysWOW64\cmd.exe
C:\Windows\System32\wscript.exe
C:\Windows\SysWOW64\wscript.exe
C:\Windows\System32\cscript.exe
C:\Windows\SysWOW64\cscript.exe
C:\Windows\System32\ntvdm.exe
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe

TEST RESULTS ESET ANTI-RANSOMWARE SETUP

With a complete ESET Anti-Ransomware Setup from mailserver to endpoints and even servers the ransomware emails with droppers in the attachment are already filtered out before they are being detected as malicious code or ransomware. In addition on endpoints with these hardened settings, we have conducted several tests where we disabled all detection layers of our ESET Security solutions, showing that these types of ransomware do not have any chance to encrypt the system and network.

Concluding that the ESET Anti-Ransomware Setup as hardening of the ESET Security solutions minimizes the chance of infection with ransomware and the encryption of valued corporate data.