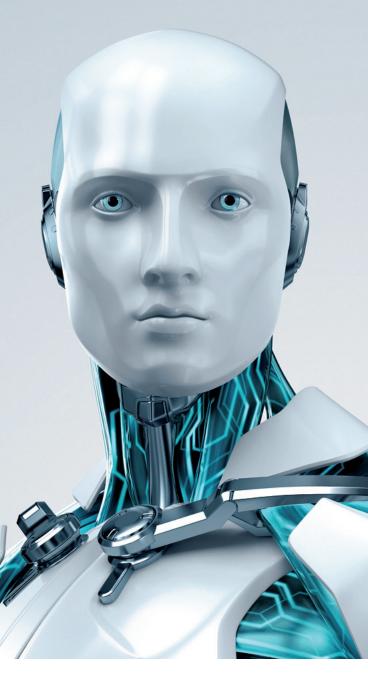
ESET Anti-Ransomware Setup

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





ENJOY SAFER TECHNOLOGY



CONTENT

Goal of this Tech Brief		. 3
Why these additional settings?		. 3
ESET Anti-Ransomware Setup for companies		. 4
Antispam rules for ESET Mail Security for MS Exchange		. 6
Firewall rules for Endpoint Security		. 7
HIPS rules for Endpoint Security & Endpoint Antivirus .		. 8
Test results ESET Anti-Ransomware Setup		. 9



ENJOY SAFER TECHNOLOGY™

esei

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.

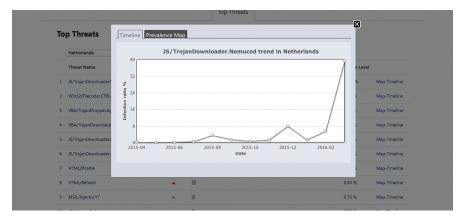


JS/TrojanDownloader.Nemucod [Threat Name] go to Threat

Last Day Last Week Last Month

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:

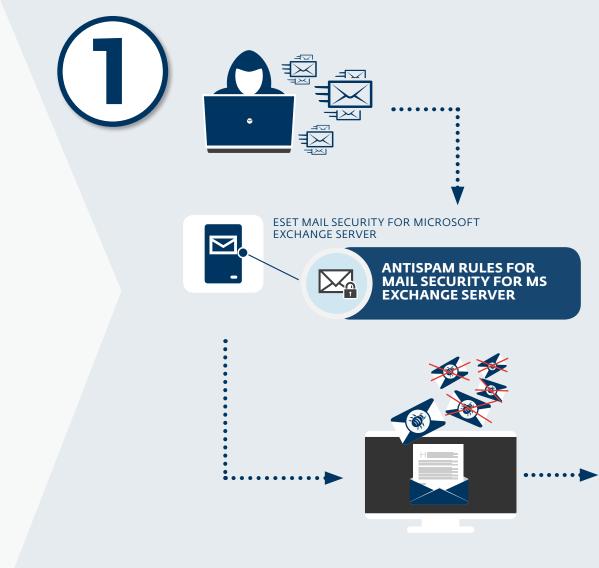
The ESET Anti-Ransomware Setup and policies are generically drawn and may vary by area We recommend to test the settings for each implementation in a customer area before fully implementing them.



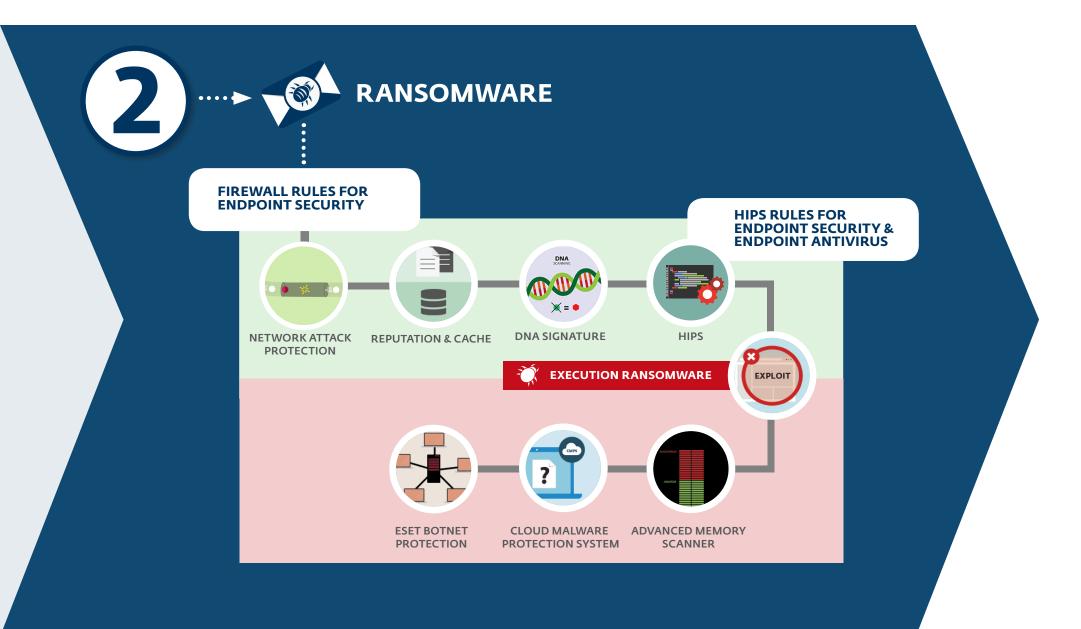
ESET ANTI-RANSOMWARE SETUP FOR BUSINESS

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









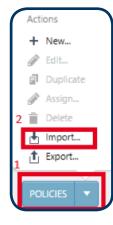


ANTISPAM RULES FOR ESET MAIL SECURITY FOR MS EXCHANGE SERVER

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

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.

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.

ESET REMOTE ADMINISTRATOR BACK Edit Policy - Settings Rules ? 🗆 🗙 Hits 🔍 + BASIC Active Name Level Dangerous system file attachments Attachment processing 0 - SETTINGS Dangerous executable file attachments Attachment processing 0 Forbidden archive file attachments Attachment processing 0 Common ransomware droppers Attachment processing 0 Password protected archive file attachments Result processing - RULES MAILBOX DATABASE PROTEC Rules MALL TRANSPORT PROTECTI Apply -Rules

Executable files

Windows Executable (*.exe;*.dll;*.sys;*.drv;*.ocx;*.scr)
 MS-DOS Executable (*.exe)
 ELF Executable and Linkable format (e.g. Linux) (*.elf)
 Adobe Flash (*.swf)
 Java Class Bytecode (*.class)
 Windows Installer Package (*.msi)
 Apple OS X Universal binary executable
 Apple OS X Mach-O binary executable
 Android executable (*.dex)

Common ransomware droppers which block the following extensions*:

*,js *.hta *.docm *.xlsm *.pptm *.vbs *.bat

* 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.



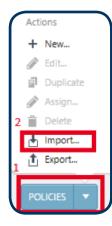
Should the dropper with malicious code be executed, ESET Endpoint Security still prevents the download of malware due to the integrated Firewall.

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 *<u>a group</u>* or <u>*client*</u>

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



	Application
	C:\Windows\System32\wscript.exe
	C:\Windows\SysWOW64\wscript.exe
? 🗆	C:\Windows\System32\cscript.exe
	C:\Windows\Syswow64\cscript.exe
	$\label{eq:c:Windows} C: Windows \ System 32 \ Windows \ Power \ Shell \ v1.0 \ power \ shell. exe$
	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
	C:\Windows\System32\ntvdm.exe
II.exe	

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.

Name	Enabled	Protocol	Profile	Action	Direction Local	Remote	Application
Deny network connections for wscript.exe (native)	~	Any	Any profile	Deny	Both		C:\Windows\System32\wscript.exe
Deny network connections for wscript.exe (SysWOW64)	\checkmark	Any	Any profile	Deny	Both		C:\Windows\SysWOW64\wscript.exe
Deny network connections for cscript.exe (native)	\checkmark	Any	Any profile	Deny	Both		C:\Windows\System32\cscript.exe
Deny network connections for cscript.exe (SysWOW64)	\checkmark	Any	Any profile	Deny	Both		C:\Windows\Syswow64\cscript.exe
Deny network connections for powershell.exe (native)	\checkmark	Any	Any profile	Deny	Both		C:\Windows\System32\WindowsPowerShell\v1.0\powershell
Deny network connections for powershell.exe (SysWOW64)	\checkmark	Any	Any profile	Deny	Both		C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powersh
Deny network connections for ntvdm.exe	\checkmark	Any	Any profile	Deny	Both		C:\Windows\System32\ntvdm.exe
Add Edit Remove							* * .





Edit Policy - Settings

IMPORTANT These rules block by legitimate appl you to test this be within your area.

HIPS RULES FOR ENDPOINT Ô **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 it applicable to servers. Plea legitimate scripts starting

How to import and apply the policies

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

Deny child process from dangerous executables.

e ESET File Security for Windows Server, making ase note that HIPS will not make a distinction ir in production areas.				Application C:\Windows\System32\wscript.exe C:\Windows\SysWOW64\wscript.exe C:\Windows\System32\cscript.exe C:\Windows\Syswow64\cscript.exe C:\Windows\Syswow64\cscript.exe C:\Windows\Syswow64\cscript.exe C:\Windows\Syswow64\cscript.exe C:\Windows\Syswow64\cscript.exe C:\Windows\Syswow64\cscript.exe C:\Windows\Syswow64\cscript.exe C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe		
HIPS rules				C:\Windows\System32\ntvdm.exe		
Rule	Fnabled	Action Sources	Targets Log	Deny script processes started by explorer		
Deny child processes from dangerous executables		Block	Applications V	C:\Windows\System32\wscript.exe		
Deny script processes started by explorer	~	Block	Applications 🗸	C:\Windows\SysWOW64\wscript.exe		
Deny dangerous child processes from Office 2013 processes	~	Block	Applications 🔽	C:\Windows\System32\cscript.exe		
Deny dangerous child processes from Office 2016 processes BASIC	v	Block	Application	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		
ecutables that may also be used						
ations. We therefore recommend				C:\Windows\System32\cscript.exe		
pre fully implementing the policy				C:\Windows\SysWOW64\cscript.exe		
ew application				C:\Windows\System32\ntvdm.exe		
				C:\Windows\System32\WindowsPowerShell\v1.0\powershell.ex		
✓ Rules				C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.		
Add Edit Remove						

eset enjoy safer technology™

TEST RESULTS ESET ANTI-RANSOMWARE SETUP

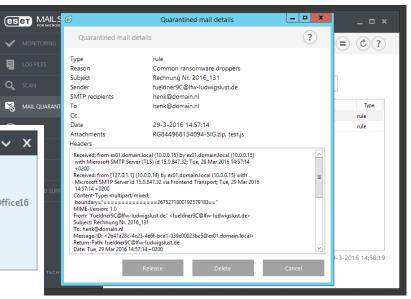
With a complete ESET Anti-Ransomware Setup from mailserver to endpoints and even servers the ransomware emails with droppers in the attachment are already filtered out before they are being detected as malicious code or ransomware. In addition on endpoints with these hardened settings, we have conducted 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.

🖬 7-Zip										
File	Edit	Viev	v Fa	vorites	Tools	Help				
"			\checkmark	•	-	×	ī			
Add	Extra	act	Test	Сору	Move	Delete	Info			
ø	🚹 C	\Use	rs\ing	rid\Desk	top\exc	luded\09	b16548	4f4ec6a4b032	42da56d980b6884e	3e52.zip\
Nam	ie					Size		Packed Size	Modified	Created
80	9b1654	84f4e	сба4t	0324		16 882	2	6 426	2016-03-24 16:33	



Rule: Deny network connections for wscript.exe (native)
Application: C:\Windows\System32\wscript.exe



Microsoft Visual Basic	
Run-time error '5':	
Invalid procedure call or argument	
Continue End	Debug Help

ENDPOINT SECURITY

Start new application

Application: C:\Program Files\Microsoft Office\root\Office16 \WINWORD.EXE Target: C:\Windows\System32\cmd.exe

Operation was blocked.