ESET Anti-Ransomware Setup

Meerlaagse beveiliging tegen versleuteling

Document version:
1.1

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

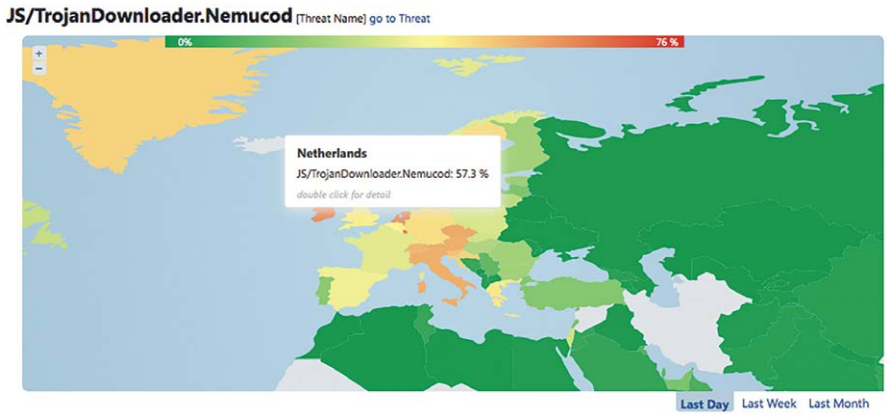
INHOUD

DOEL VAN DEZE TECH BRIEF

In deze Tech Brief beschrijven wij de optimale instellingen van onze ESET beveiligingsoplossingen tegen de huidige vorm van ransomware en de meest populaire infectiescenario's. Doel is om onze ESET klanten nog beter te beschermen tegen een ransomware uitbraak waarin kostbare data versleuteld en/of gegijzeld kan worden tegen betaling.

WAAROM DEZE ADDITIONELE INSTELLINGEN?

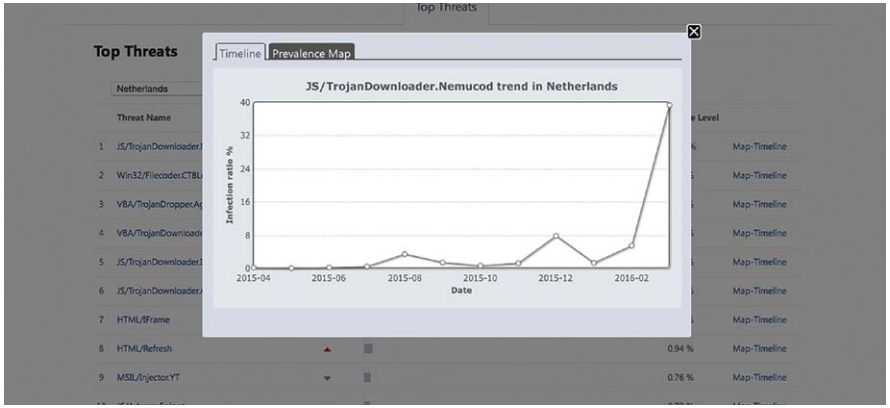
Bijna 60% van alle malware die wij in Nederland detecteren kan een ransomware-infectie tot gevolg hebben.



Daarnaast zijn de huidige ransomware aanvallen zo geavanceerd dat kwaadwillende malware pas wordt binnengehaald na het uitvoeren van een zogenoemde dropper. Door de dropper als bijlage met de e-mail mee te sturen, proberen cybercriminelen een detectie bij binnenkomst te voorkomen. Vaak betreft dit een correct opgestelde phishingmail met als bijlage een ZIP bestand. In het ZIP bestand bevindt zich een Javascript bestand van het type .JS.

Javascript wordt door talloze websites gebruikt, waardoor het simpelweg onmogelijk is om dit te blokkeren in de browser. Daarnaast voert Windows ook rechtstreeks Javascript uit.

Ondertussen wordt deze Javascript code zwaar gemaskeerd, onleesbaar gemaakt en continu gewijzigd om detectie te voorkomen. Dit geeft ons de mogelijkheid om met verschillende ESET beveiligingsmodules in de software invloed uit te oefenen bij het uitvoeren van mogelijk schadelijke code via deze standaardprocessen.



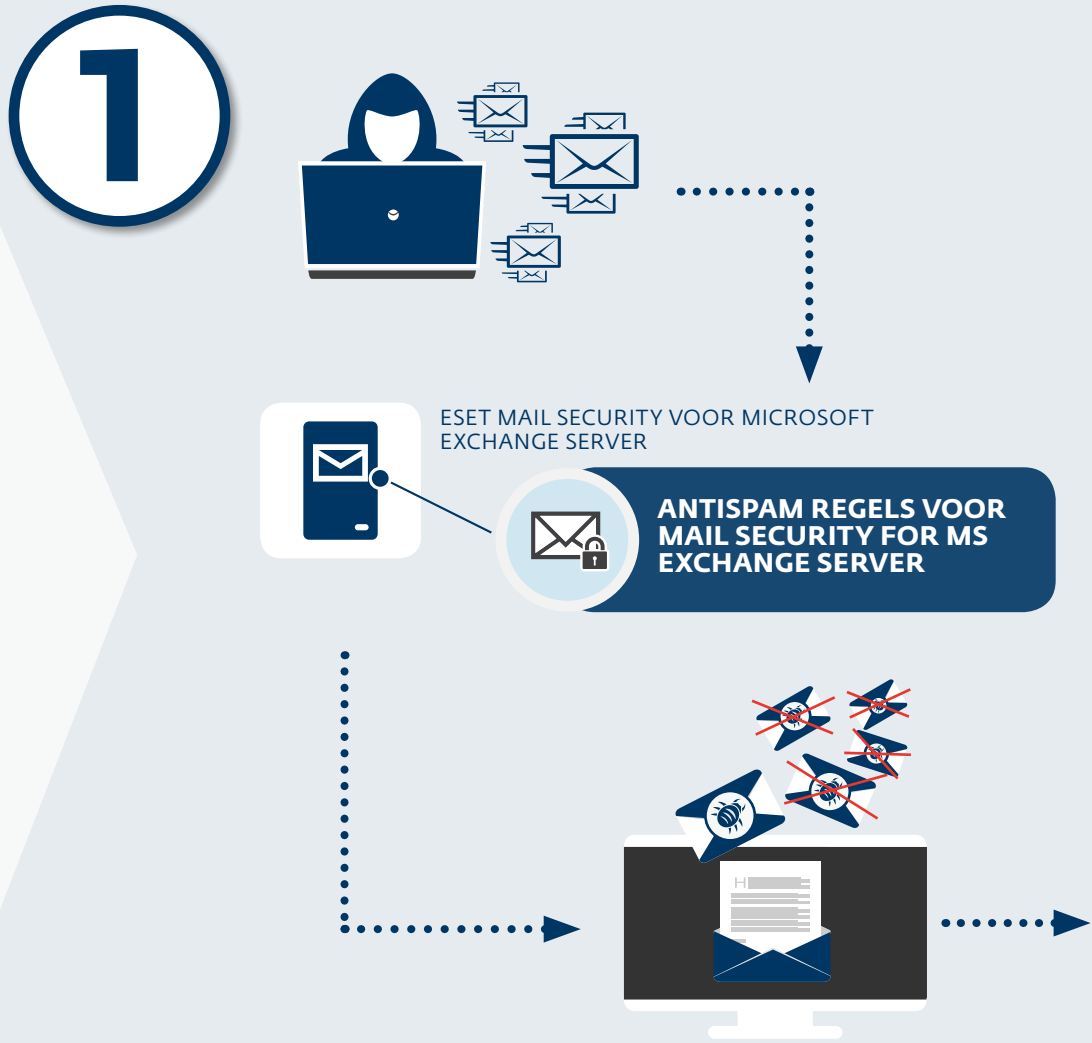
Disclaimer:

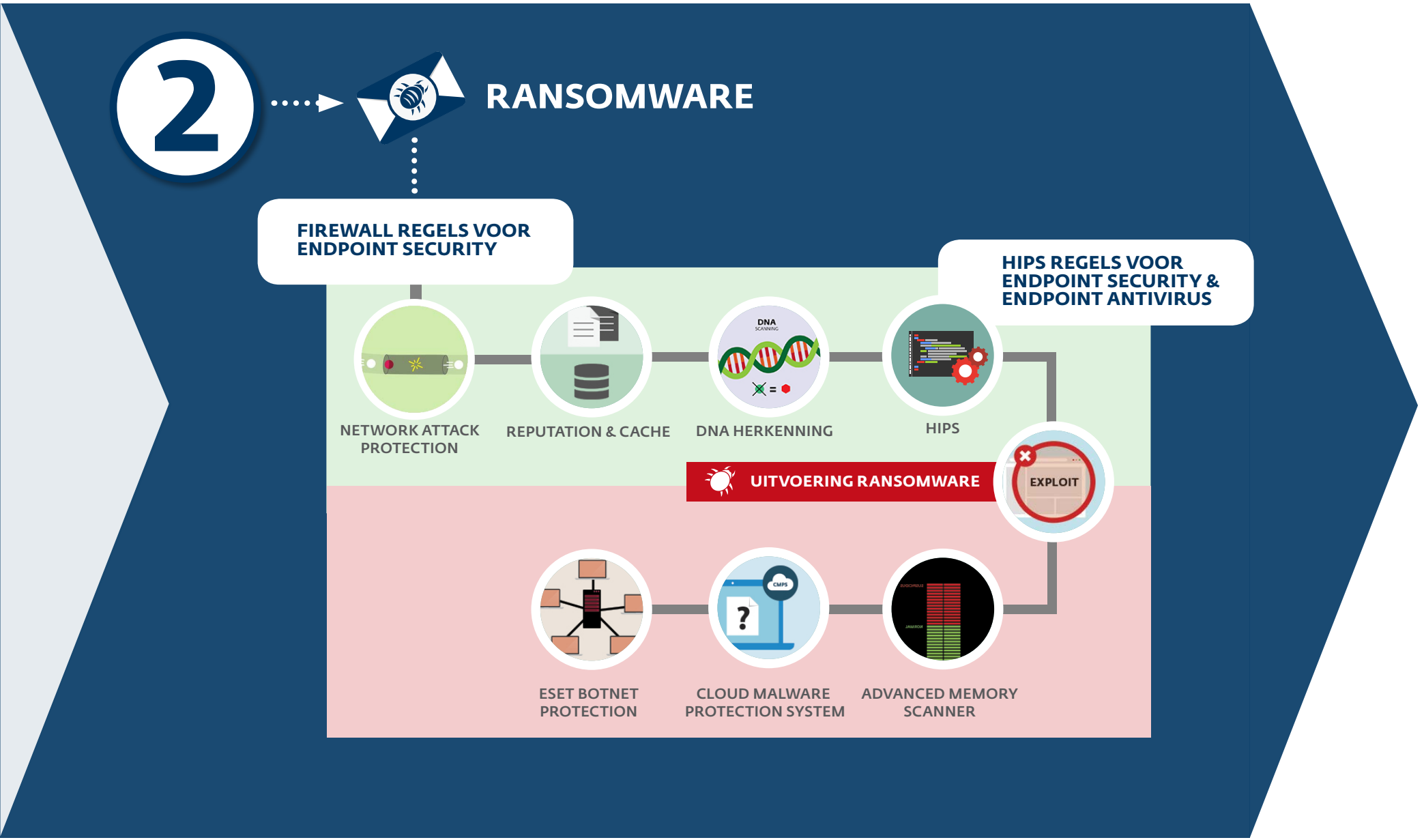
De ESET Anti-Ransomware Setup en policies zijn generiek opgesteld en kunnen verschillen per omgeving. Wij raden aan de instellingen per implementatie in een klant omgeving eerst te testen alvorens deze volledig door te voeren. Bij vragen kunt u terecht bij ESET Support.

ESET ANTI-RANSOMWARE SETUP VOOR BEDRIJVEN

De additionele instellingen van onze ESET Anti-Ransomware Setup blokkeren de ransomware-infectie methode (middels een Javascript dropper) waardoor de kwaadwillende malware simpelweg geen kans krijgt om gedownload te worden. Deze aanpak blijkt zo efficiënt dat wij vanuit ESET Nederland de instellingen uitgebreid in deze tech brief toelichten en aanbieden als policy configuratie die pasklaar gedownload en geïmplementeerd kan worden via onze ESET Remote Administrator.

DOWNLOAD HIER UW INSTELLINGEN




2
RANSOMWARE
FIREWALL REGELS VOOR ENDPOINT SECURITY
HIPS REGELS VOOR ENDPOINT SECURITY & ENDPOINT ANTIVIRUS
NETWORK ATTACK PROTECTION
REPUTATION & CACHE
DNA HERKENNING
HIPS
UITVOERING RANSOMWARE
EXPLOIT
ESET BOTNET PROTECTION
CLOUD MALWARE PROTECTION SYSTEM
ADVANCED MEMORY SCANNER

ANTISPAM REGELS VOOR ESET MAIL SECURITY FOR MS EXCHANGE SERVER

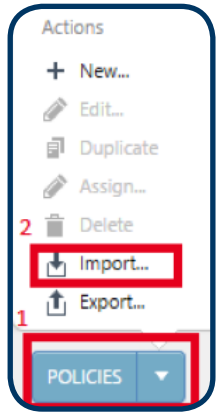
Met de juiste antispam regels worden de binnenkomende e-mails op basis van het type bijlage al uitgefilterd op de mailserver zelf. Op deze manier wordt de bijlage met schadelijke dropper niet afgeleverd in de mailbox van de eindgebruiker en krijgt de ransomware geen kans zich uit te voeren.

Belangrijk:

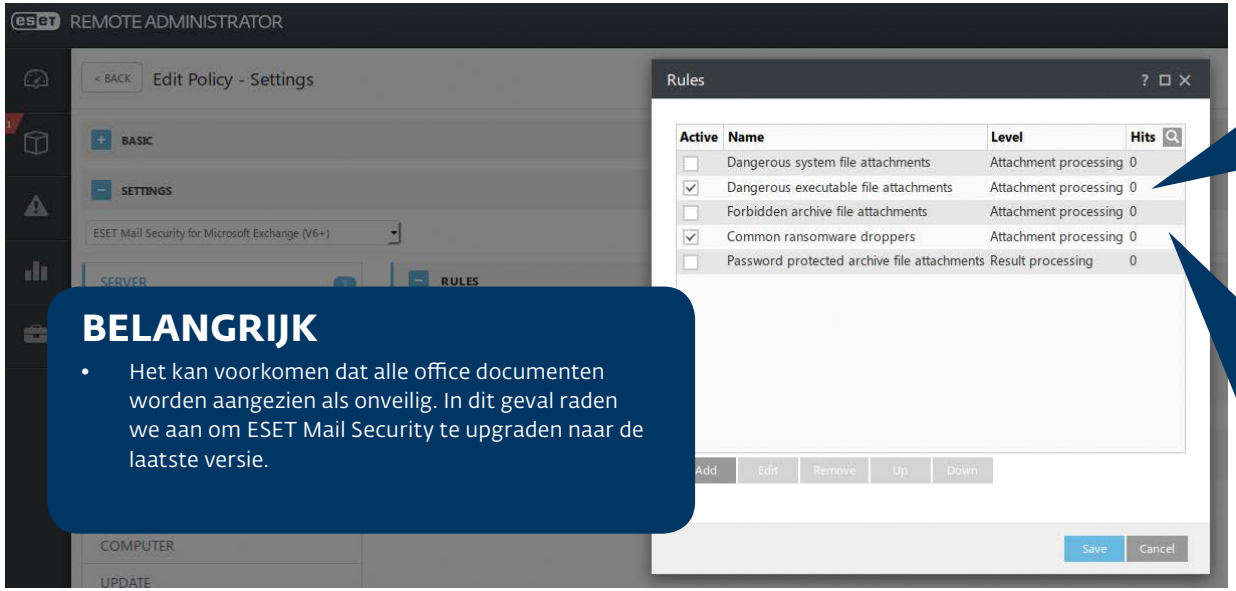
Upgrade ESET Mail Security for Microsoft Exchange Server naar de laatst beschikbare build 6.3.x of hoger voor een juiste werking van de filter regels.

Importeren en toepassen van de policies*

1. Log in op de ERA 6 Webconsole
2. Navigeer naar ADMIN > Policies
3. Klik vervolgens onderaan op "Policies" en hierna op "Import"
4. Importeer vervolgens een voor een de policies.
5. Pas de policies toe op *een groep* of *client*

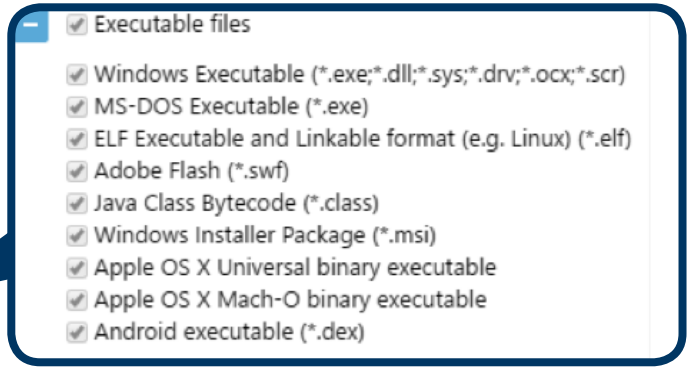


*** Deze handeling hoeft niet te worden herhaald bij de overige instellingen.**



BELANGRIJK

- Het kan voorkomen dat alle office documenten worden aangezien als onveilig. In dit geval raden we aan om ESET Mail Security te upgraden naar de laatste versie.



Common ransomware droppers, deze blokkeert de volgende extensies*:

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

*In dit geval worden dus ook **Microsoft Office bestanden met Macro's geblokkeerd (docm, xlsm en pptm)** Mocht u binnen uw omgeving gebruikmaken van dergelijke bestanden dan zult u deze regel moeten aanpassen of uitschakelen.

FIREWALL REGELS VOOR ENDPOINT SECURITY

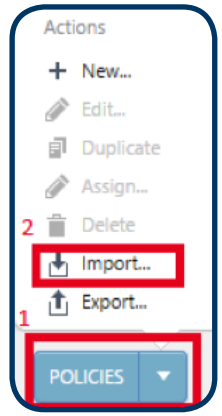
Mocht de dropper met schadelijke code worden uitgevoerd, dan voorkomt ESET Endpoint Security de download van malware alsnog dankzij de ingebouwde firewall.

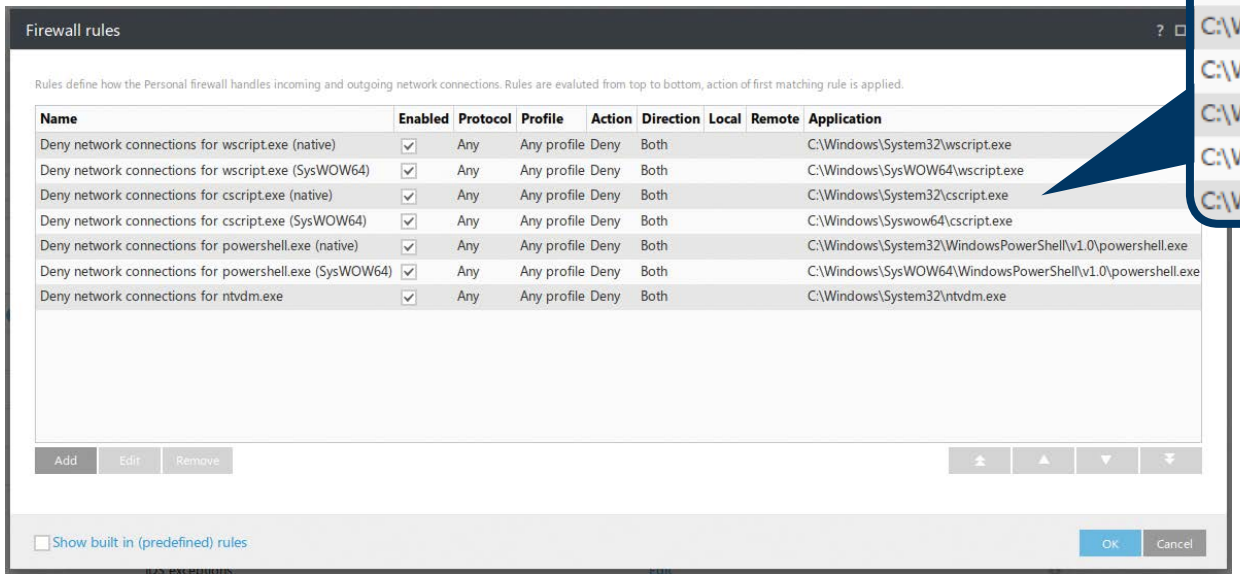
Door het toepassen van de juiste firewall regels blokkeert ESET Endpoint Security standaardprocessen en andere scripting de toegang tot het internet en voorkomt hiermee de download van schadelijke code (payload) en het starten van de ransomware.

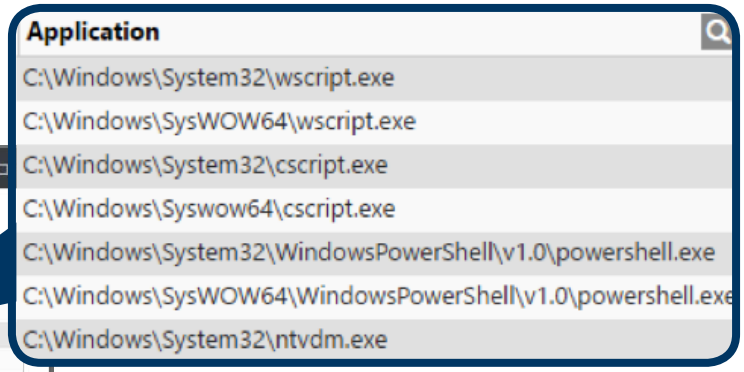
Importeren en toepassen van de policies

1. Log in op de ERA 6 Webconsole
2. Navigeer naar ADMIN > Policies
3. Klik vervolgens onderaan op "Policies" en hierna op "Import"
4. Importeer vervolgens een voor een de policies.
5. Pas de policies toe op *een groep* of *client*

Let op: bij het importeren van Firewall regels kunnen bestaande regels overschreven worden.







BELANGRIJK

- Deze Policy werkt alleen in combinatie met ESET Endpoint Security i.v.m. de aanwezigheid van de firewall module
- Ook voor deze regel(s) geldt dat legitieme applicaties gebruik kunnen maken van deze executables. Wij adviseren u dan ook deze te testen alvorens u de Policy binnen uw gehele omgeving uitrolt.

HIPS REGELS VOOR ENDPOINT SECURITY & ENDPOINT ANTIVIRUS

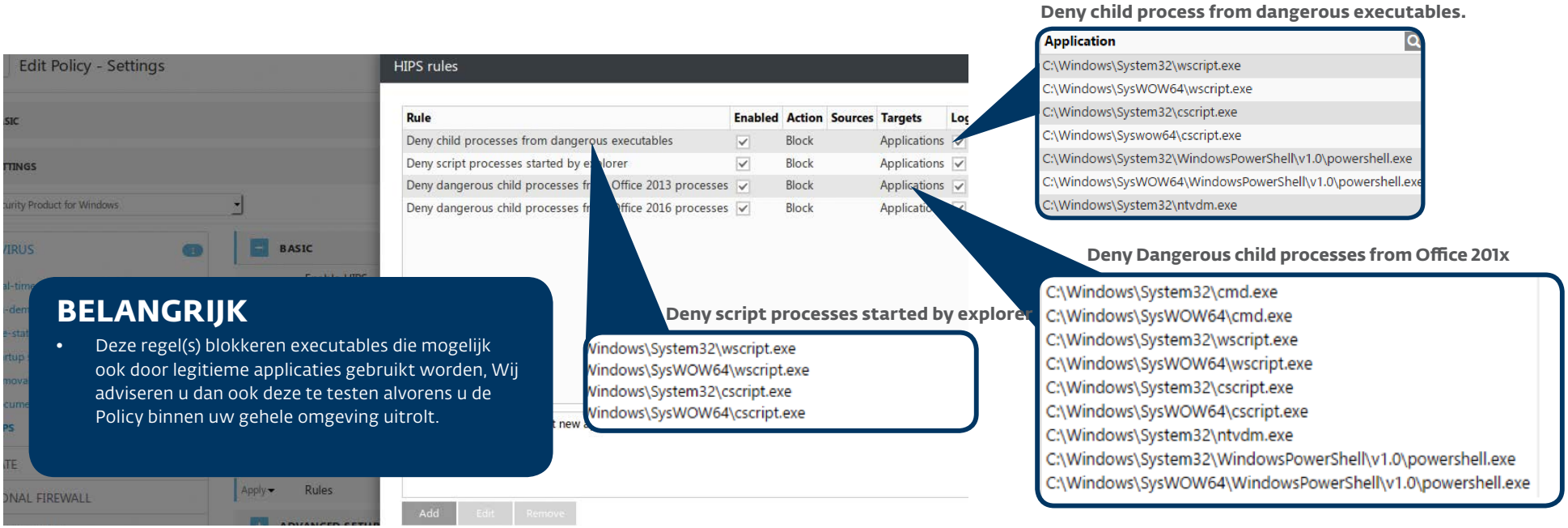
Host-based Intrusion Prevention System (HIPS) verdedigt het systeem van binnenuit en kan ongeoorloofde acties van processen onderbreken voordat deze worden uitgevoerd. Door het standaard uitvoeren van Javascript en andere scripts te verbieden, krijgt ransomware geen kans de malware uit te voeren, laat staan te downloaden.

Onze HIPS is tevens onderdeel van ESET File Security voor Windows Server waardoor deze ook toepasbaar is op servers. Let op dat HIPS geen onderscheid zal maken in legitieme scripts die starten in productieomgevingen.

Importeren en toepassen van de policies

1. Log in op de ERA 6 Webconsole
2. Navigeer naar ADMIN > Policies
3. Klik vervolgens onderaan op "Policies" en hierna op "Import"
4. Importeer vervolgens een voor een de policies.
5. Pas de policies toe op *een groep* of *client*

Let op dat machines welke lid zijn van een domein op een SBS server vaak voorzien zijn van een Log On script (ClientAgent.vbs) welke tracht sbslogon.exe te starten. Dit wordt geblokkeerd door de HIPS regel "Deny child processes from script executables". (Specifiek het starten van een applicatie middels wscript) Hierdoor kan het inlogproces van verbonden endpoints (erg) lang duren. We raden dan ook aan om deze regel in een SBS omgeving **niet** te gebruiken.



RESULTATEN ESET ANTI-RANSOMWARE SETUP

Met een volledige ESET Anti-Ransomware Setup vanaf de (mail)server tot aan de endpoints, worden ransomware e-mails met droppers in de bijlage al gefilterd op basis van de filterregels voordat deze worden gedetecteerd als schadelijke code en/of ransomware en krijgen droppers op de endpoints geen kans zich uit te voeren. Daarnaast hebben wij verschillende tests met deze hardened instellingen uitgevoerd op endpoints waarbij, ondanks het uitschakelen van alle detectielagen in onze ESET Security oplossingen, deze typen ransomware geen kans krijgen om het systeem en het netwerk te versleutelen.

Kortom, de ESET Anti-Ransomware Setup als hardening van de ESET beveiligingsoplossingen verkleinen de kans op ransomware en versleuteling van gevoelige bedrijfsgegevens.