АНТИВИРУСНАЯ ЗАЩИТА
БИЗНЕС-КЛАССА

# НАСТРОЙКИ ESET ПРОТИВ ШИФРАТОРОВ

# СОДЕРЖАНИЕ

# ВВЕДЕНИЕ

Предлагаем описание оптимальных настроек решений безопасности ESET для противодействия современным версиям шифраторов и распространенным сценариям заражения. Цель документа – помочь нашим клиентам построить надежную защиту от вредоносных программ, которые блокируют доступ к ситеме, шифруют данные и требуют выкуп за расшифровку.

# ЗАЧЕМ НУЖНЫ ДОПОЛНИТЕЛЬНЫЕ НАСТРОЙКИ?

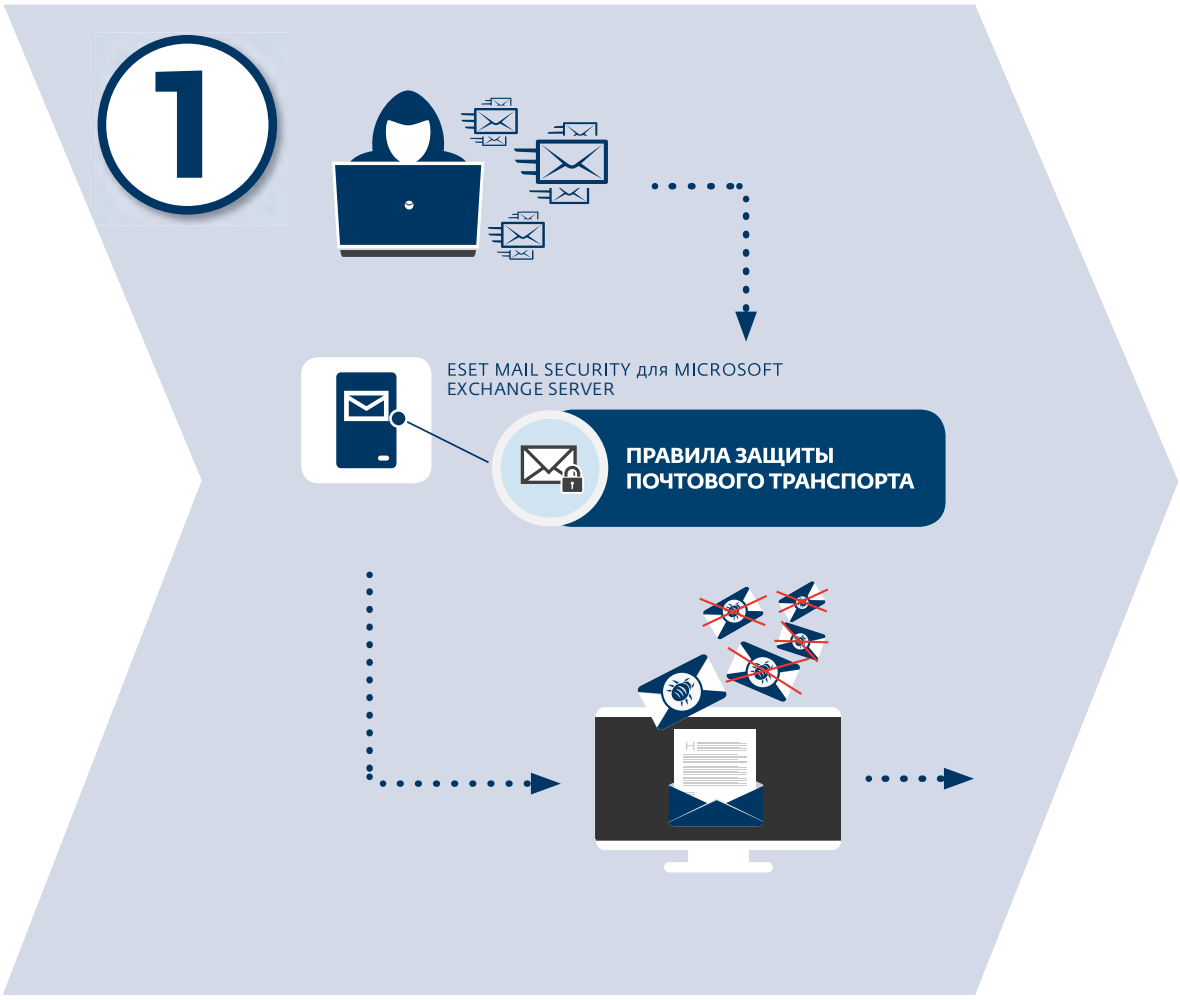
Современные шифраторы и программы-вымогатели используют продвинутые технологии заражения. Они убеждают пользователя запустить исполняемый файл – дроппер, – который в свою очередь скачивает из интернета на компьютер сам шифратор. Киберпреступники стремятся предотвратить обнаружение дроппера при первом попадании на компьютер. В большинстве случаев они используют убедительное фишинговое письмо с ZIP-архивом во вложении, который содержит JavaScript-файл с расширением .JS.
Код JavaScript используется многими сайтами, JavaScript-файлы выполняет операционная система Microsoft Windows, поэтому заблокировать его достаточно сложно. В дроппере код JavaScript сильно искажен для маскировки. Но мы можем предотвратить его исполнение через стандартные процессы, используя различные модули безопасности.

**Примечание:** *Настройки ESET против шифраторов являются типовыми и могут варьироваться в зависимости от области применения. Мы рекомендуем тестировать настройки для каждого внедрения в инфраструктуре клиента до финального развертывания.*

# НАСТРОЙКИ ESET ПРОТИВ ШИФРАТОРОВ ДЛЯ БИЗНЕСА

Дополнительные настройки ESET позволяют обнаружить возможность заражения вымогателем через дроппер JavaScript и не допустить скачивания вредоносной программы. В этом документе мы рассказываем о дополнительных настройках и предлагаем готовые политики конфигурации, которые вы можете скачивать и применять в ESET Remote Administrator.

**СКАЧАТЬ НАСТРОЙКИ**

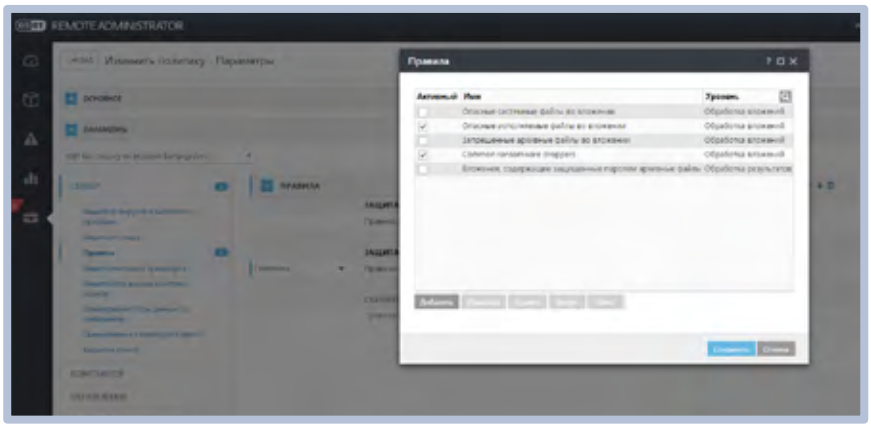



2
ПРОГРАММА-ВЫМОГАТЕЛЬ
ПРАВИЛА ФАЙЕРВОЛА
ПРАВИЛА HIPS
ЗАЩИТА ОТ СЕТЕВЫХ АТАК
РЕПУТАЦИОННЫЙ КЭШ
СЕТЕВЫЕ СИГНАТУРЫ
HIPS
ИСПОЛНЕНИЕ ПРОГРАММЫ-ВЫМОГАТЕЛЯ
ЭКСПЛОЙТ
ЗАЩИТА ОТ БОТНЕТОВ
ОБЛАЧНАЯ СИСТЕМА ЗАЩИТЫ
РАСШИРЕННОЕ СКАНИРОВАНИЕ ПАМЯТИ

# ПРАВИЛА ДЛЯ ESET MAIL SECURITY ДЛЯ MICROSOFT EXCHANGE SERVER

Настройте модуль «Защиты почтового транспорта» так, чтобы автоматически фильтровать входящие письма на почтовом сервере. Вложения с дроппером не попадут в почту конечного пользователя, поэтому у шифратора не будет шанса заразить систему.

**ВАЖНО:** *Для полноценной работы правил фильтрации обновите ESET Mail Security для Microsoft Exchange Server до последней версии (6.3 или выше).*



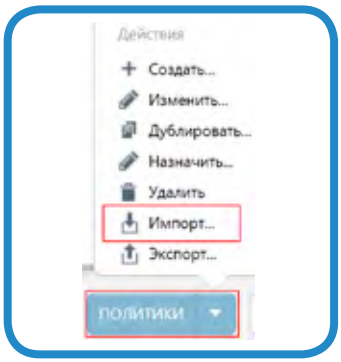
*Блокируемые расширения файлов распространённых дропперов шифраторов*:*

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


** В этом случае также будут заблокированы файлы Microsoft Office с макросами (docm, xlsm and pptm). Если вы используете файлы с такими расширениями, тогда это правило должно быть отрегулировано или отключено.*

## Как импортировать и применить политики**

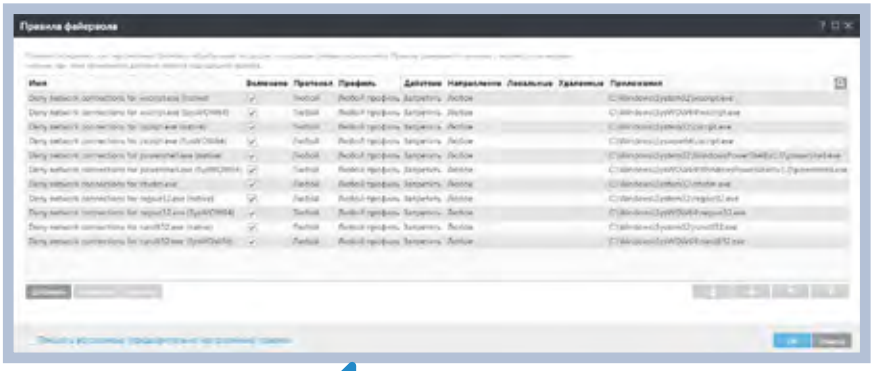
1. Войдите в веб-консоль ERA 6
2. Перейдите к АДМИН > Политики
3. Далее выберите «Политики» и после «Импорт»
4. Импортируйте политики
5. Настройте политики для группы или клиента




*** Повторение с другими настройками не требуется*

# ПРАВИЛА ФАЙЕРВОЛА ДЛЯ ESET ENDPOINT SECURITY

Когда дроппер с вредоносным кодом уже выполняется, ESET Endpoint Security все еще может предотвратить загрузку вредоносной программы. При применении указанных правил файервола ESET Endpoint Security заблокирует скачивание вредоносных элементов и запретит другим скриптам доступ к интернету.

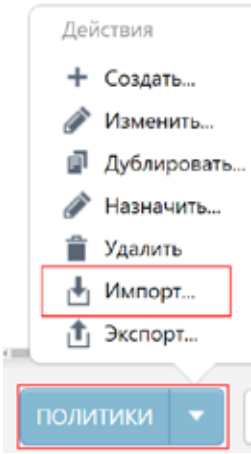



**Важно**

- *Политика работает исключительно в сочетании с ESET Endpoint Security из-за встроенного модуля файервола.*
- *Под эти правила также попадают исполняемые файлы легитимных приложений. Перед полноценным внедрением политики в компании рекомендуется заранее ее протестировать.*

## Как импортировать и применить политики*

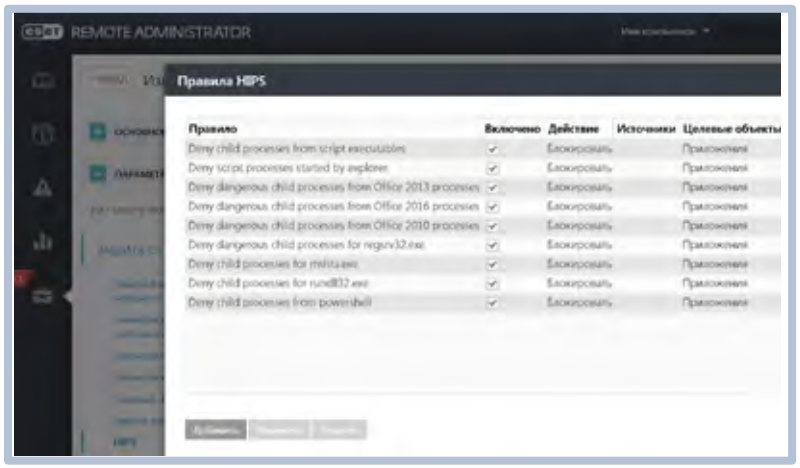
1. Войдите в веб-консоль ERA 6
2. Перейдите к АДМИН > Политики
3. Далее выберите «Политики» и после «Импорт»
4. Импортируйте политики
5. Настройте политики для группы или клиента




** Обратите внимание, что при импорте правил файервола другие правила могут быть перезаписаны*

# ПРАВИЛА HIPS ДЛЯ ESET ENDPOINT SECURITY, ESET ENDPOINT ANTIVIRUS И ESET FILE SECURITY ДЛЯ WINDOWS SERVER

Система предотвращения вторжений HIPS защищает систему от внешних угроз и может прервать несанкционированные действия процессов до их исполнения. Благодаря запрету стандартного выполнения JavaScript и других скриптов шифратор не сможет загрузить на компьютер вредоносное ПО или запустить его. Обратите внимание, что HIPS не будет различать легитимные скрипты.




**Важно**

*Эти правила блокируют исполняемые файлы, которые могут использоваться легитимными приложениями. Поэтому рекомендуется перед полноценным внедрением политики в компании заранее ее протестировать.*

*Запретите дочерние процессы опасных исполняемых файлов*

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

*Запретите скриптовые процессы, запущенные проводником*

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

*Запретите опасные дочерние процессы MS 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

## Как импортировать и применить политики

1. Войдите в вебконсоль ERA 6
2. Перейдите к АДМИН > Политики
3. Далее выберите «Политики» и после «Импорт»
4. Импортируйте политики
5. Настройте политики для группы или клиента

# РЕЗУЛЬТАТЫ ИСПЫТАНИЙ НАСТРОЕК ESET ПРОТИВ ШИФРАТОРОВ

Если применить настройки ESET против шифраторов на почтовых серверах, конечных точках и серверах, письма с вложенными дропперами будут отфильтрованы до обнаружения вредоносного кода или программы-вымогателя. Тесты на рабочих станциях с усиленными настройками и полностью отключенными уровнями защиты ESET доказали беспомощность таких шифраторов в системе и сети.
Настройки ESET против шифраторов повышают эффективность защиты решений ESET и минимизируют риск заражения вымогателем и шифрования корпоративных данных.