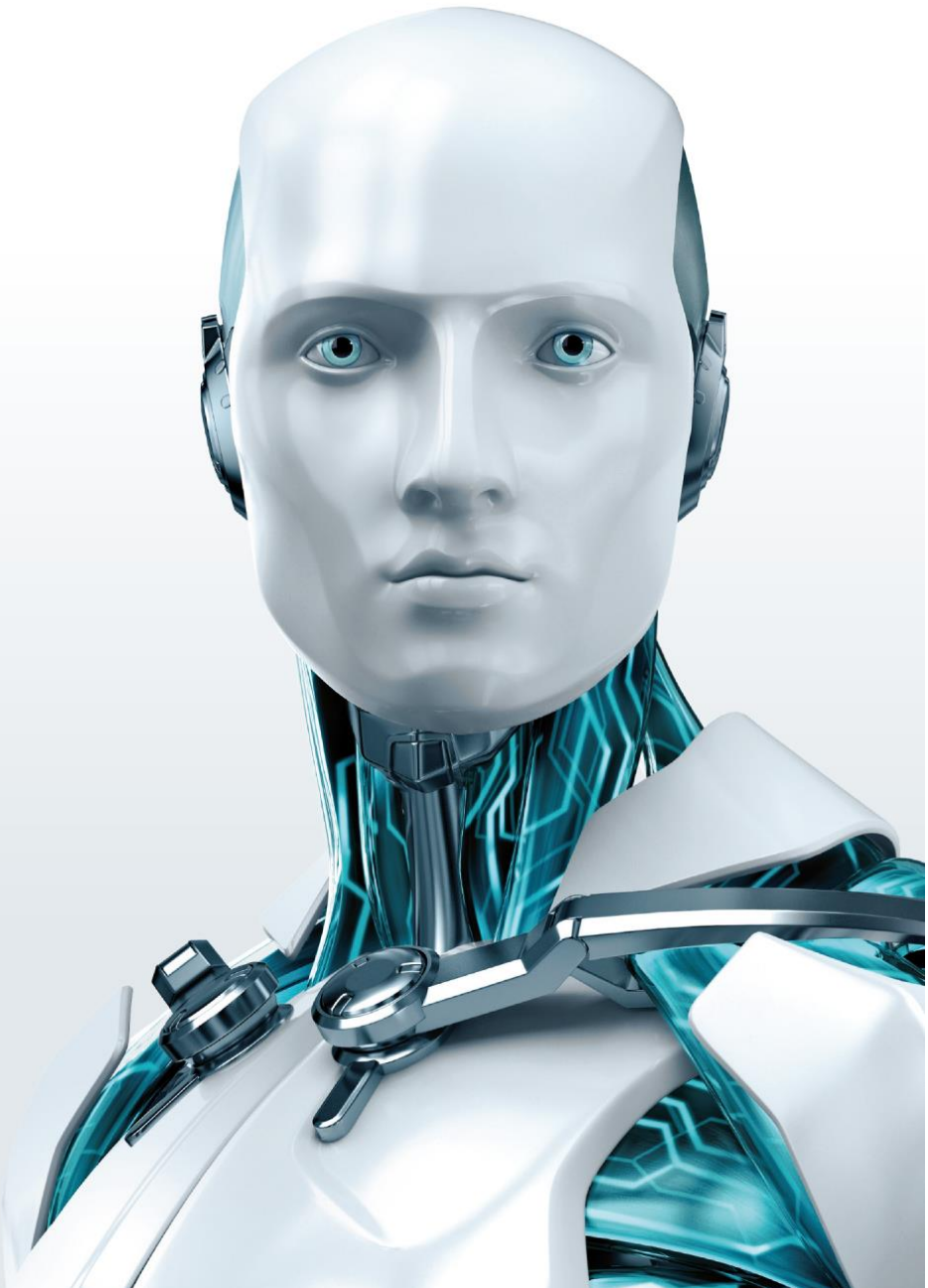
Рекомендації спеціалістів ESET для протидії атакам програми-шифратора Win32/Diskcoder.C trojan

Версія 1.0
27.06.2017



НАСОЛОДЖУЙСЯ БЕЗПЕКОЮ

УВАГА! У разі виявлення ознак здійснення атаки, будь ласка, зверніться за допомогою до технічних спеціалістів ESET в Україні, надіславши запит на електронну адресу support@eset.ua.

Інструкція спеціалістів ESET

1. Якщо інфікований комп'ютер увімкнений, не перезавантажуйте та не вимикайте його!

a) Виконайте створення логу за допомогою програми ESET Log Collector:

- Завантажте утиліту ESET Log Collector: http://eset.ua/ua/download/utility?name=logcollector
- Переконайтеся в тому, що встановлені всі галочки у вікні «Артефакти для збору».
- У вкладці «Режим збору журналів ESET» встановіть: «Вихідний двійковий код із диска».
- Натисніть на кнопку: «Зібрати».
- Надішліть архів з журналами на електронну адресу support@eset.ua.

b) У продуктах ESET увімкніть сервіс ESET Live Grid, а також виявлення потенційно небажаних та небезпечних додатків. Дочекайтеся оновлення сигнатур до версії 15653 та проскануйте ПК.

2. Якщо комп'ютер вимкнений, не вмикайте його!

Для збору інформації, яка допоможе написати декодер, перейдіть до виконання пункту 3, для сканування системи перейдіть до пункту 4.

3. З уже інфікованого комп'ютера (який не завантажується) потрібно зібрати MBR для подальшого аналізу. Зібрати його можна за допомогою цієї інструкції:

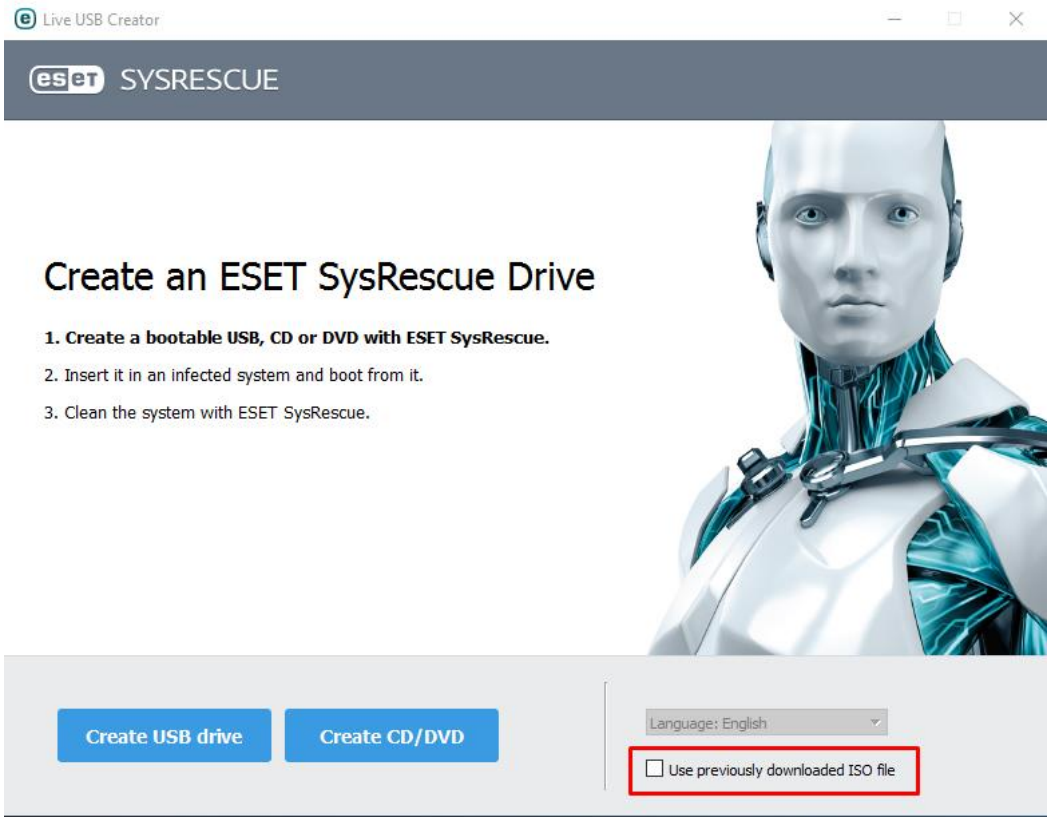
- Завантажте ПК з ESET SysRescue Live CD або USB (створення описано в Додатку 1).
- Надайте згоду з умовами ліцензії використання.
- Натисніть CTRL+ALT+T (відкриється термінал).
- Напишіть команду "parted -l" без лапок, параметром є маленька буква "L" та натисніть <enter>.
- Перегляньте список дисків та ідентифікуйте заражений (повинен бути один з /dev/sda).
- Введіть команду "dd if=/dev/sda of=/home/eset/petya.img bs=4096 count=256" без лапок, замість "/dev/sda" використовуйте диск, який визначили в попередньому кроці, та натисніть <enter> (файл /home/eset/petya.img буде створений).
- Підключіть USB-флешку і скопіюйте файл /home/eset/petya.img.
- Комп'ютер можна вимкнути.
- Надішліть файл petya.img на електронну адресу support@eset.ua.

4. Для сканування комп'ютера дотримуйтесь інструкцій, які подано у Додатку 3.

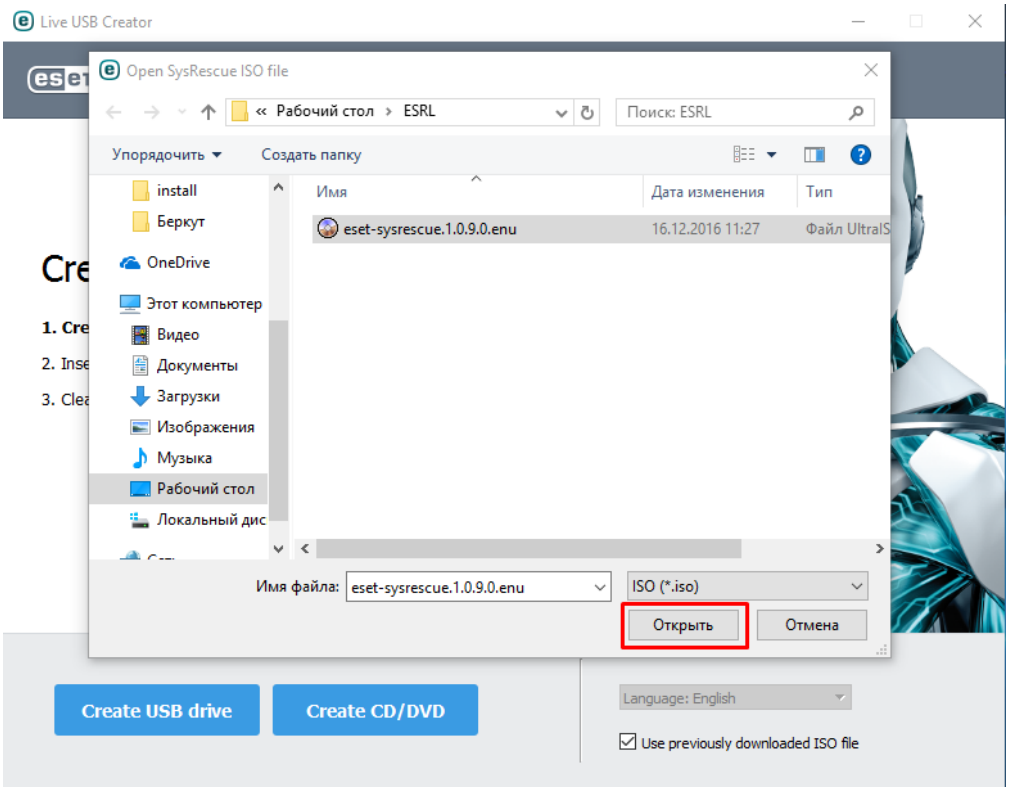
Додаток 1. Створення ESET SysResqueLive

ПРИМІТКА! Цей завантажувальний диск може працювати з RAID масивами та використовуватись для їх лікування.

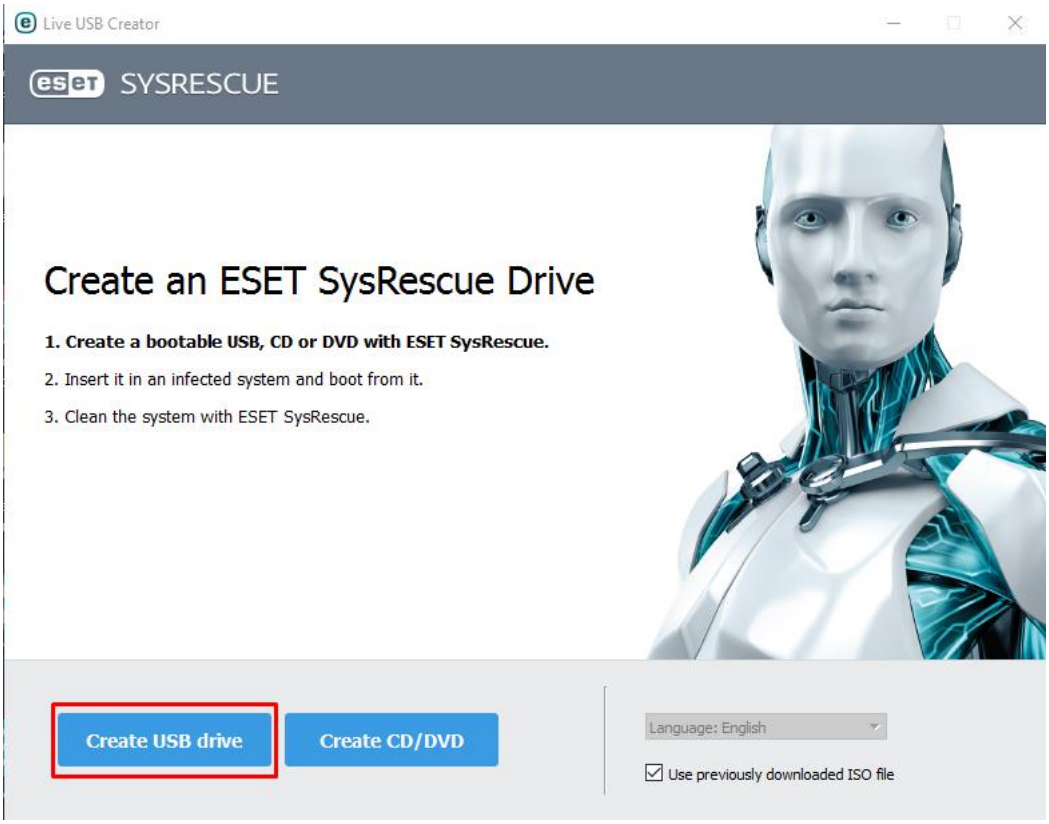
1. Завантажити eset-sysrescue.1.0.9.0.enu за посиланням http://download.eset.com/special/sysrescue-iso/eset-sysrescue.1.0.9.0.enu.iso
2. Завантажити eset_sysrescue_live_creator_enu за посиланням http://download.eset.com/special/sysrescue-creator/eset_sysrescue_live_creator_enu.exe
3. Запустити eset_sysrescue_live_creator_enu.exe
4. Відмітьте «Use previously downloaded ISO file»



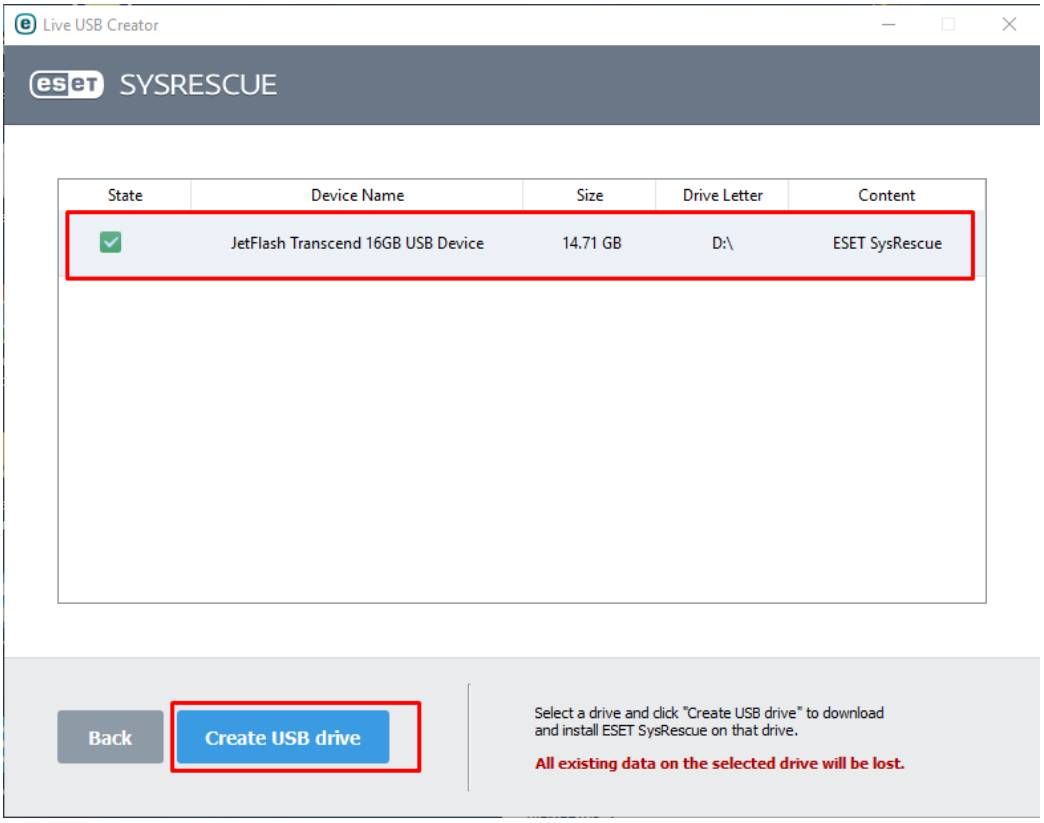
5. Вкажіть шлях до образу eset-sysrescue.1.0.9.0.enu.iso та натисніть кнопку Открыть



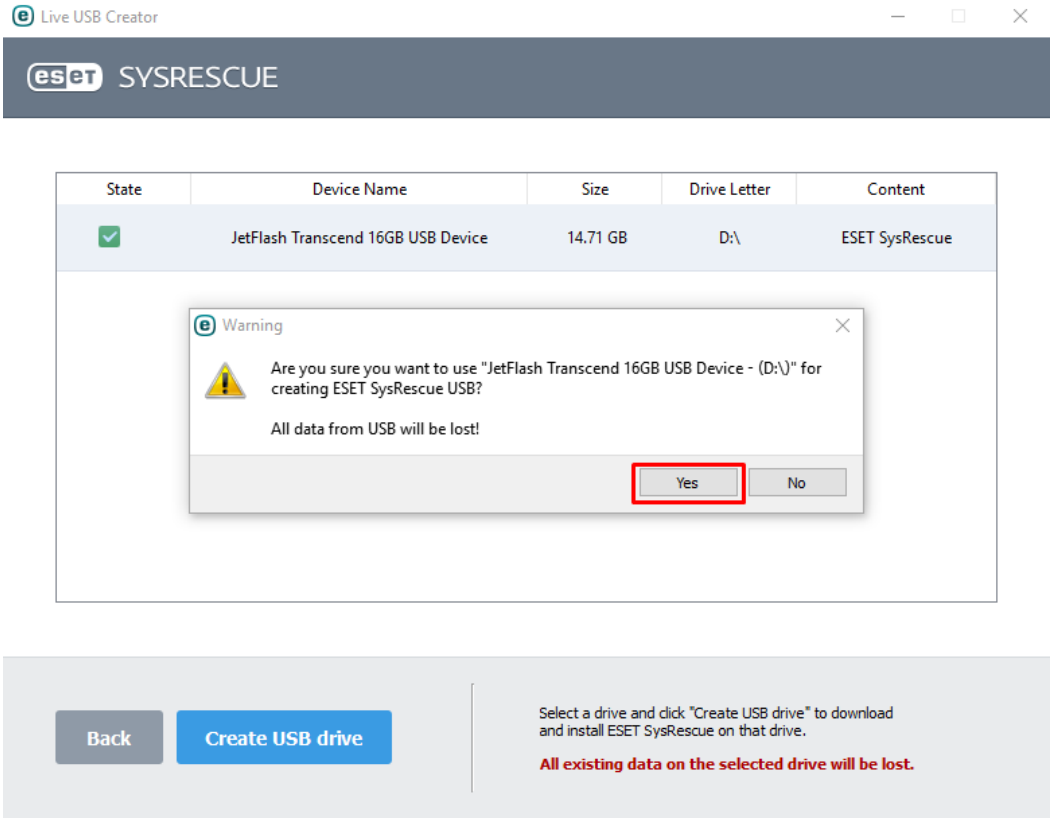
6. Підключіть usb-накопичувач до ПК.
7. Натисніть кнопку Create USB drive (якщо Ви бажаєте записати образ на usb-накопичувач, якщо на диск – Create CD/DVD)



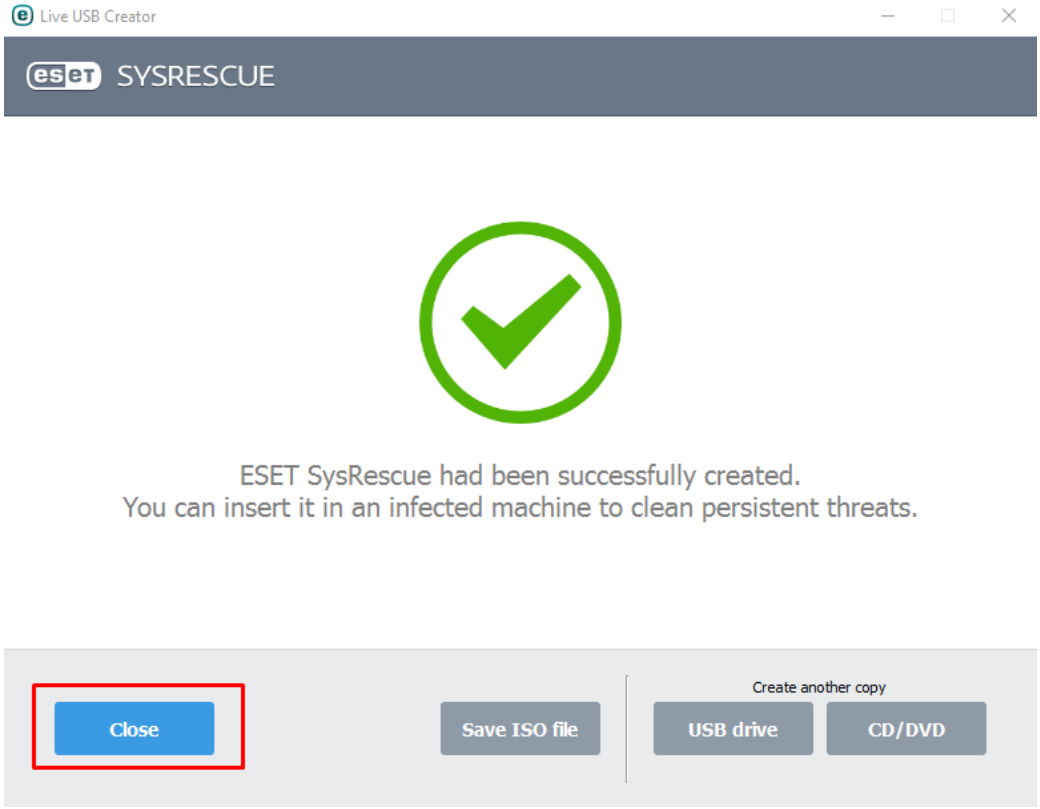
8. Оберіть необхідний накопичувач в списку (якщо їх кілька) та натисніть кнопку Create USB drive



9. Натисніть кнопку Yes



10. Коли образ буде успішно записаний, натисніть кнопку Close



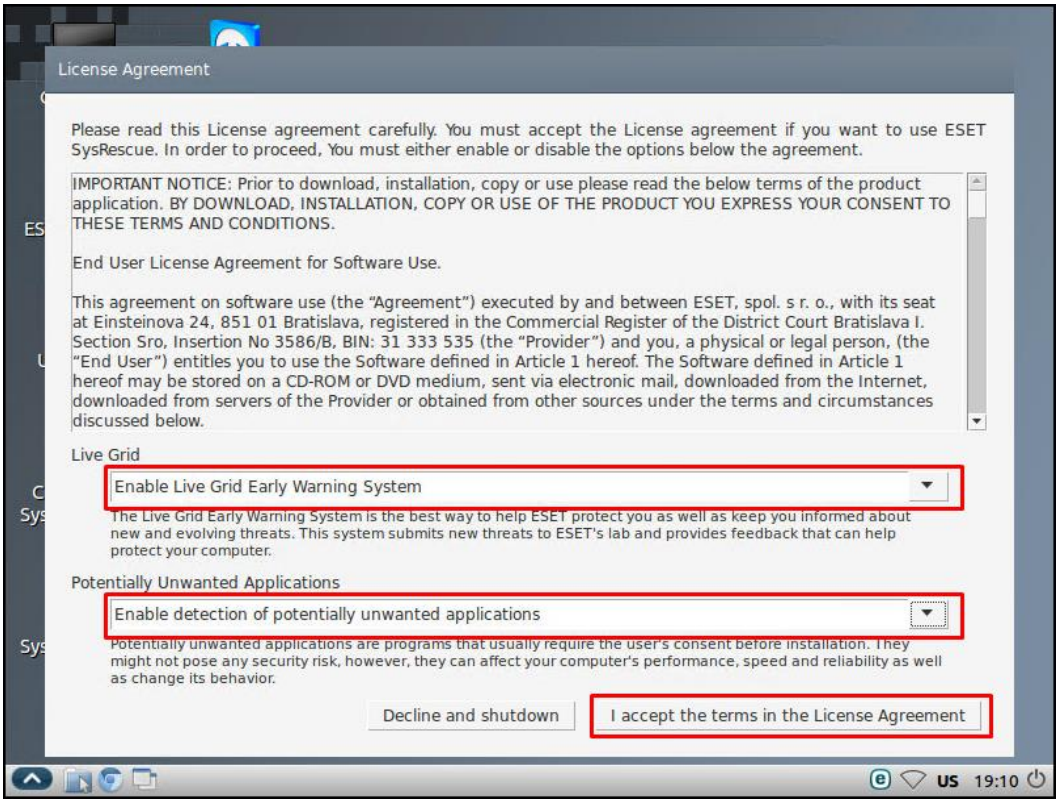
Додаток 2. Оновлення баз сигнатур ESRL

ПРИМІТКА!

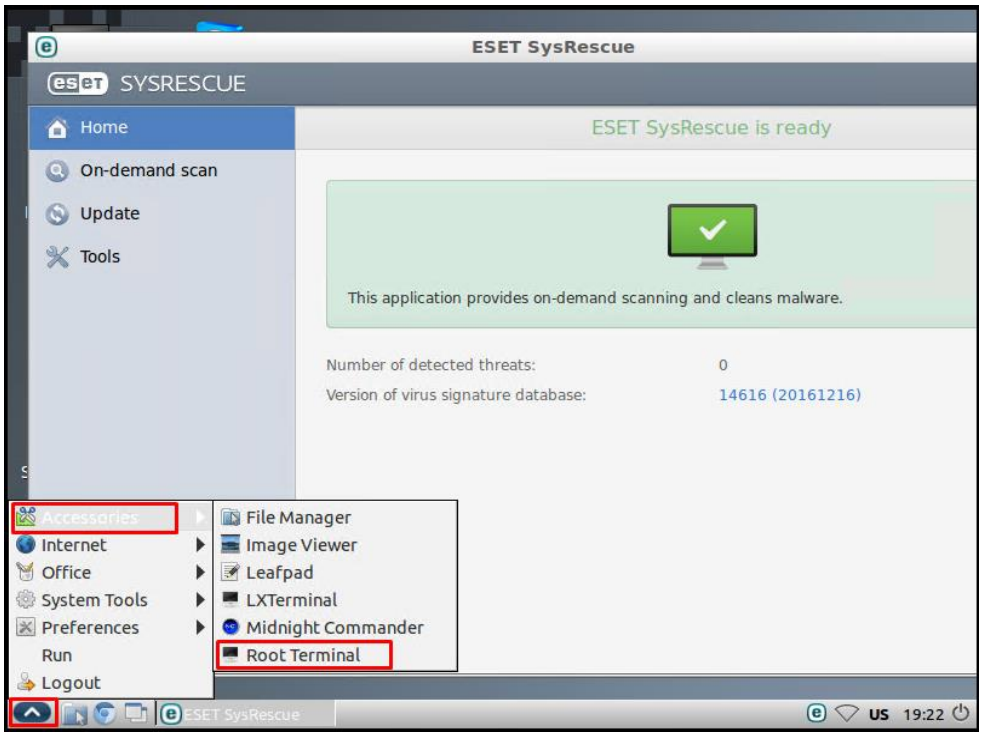
1. **Цей завантажувальний диск може працювати з RAID масивами.**
2. **Для того, щоб можна було лікувати компь'тери, що не мають підключення до інтернету, потрібно спочатку оновити бази на компь'тері, який підключений до інтернету.**

Завантажте ПК із usb-накопичувача (ESRL)

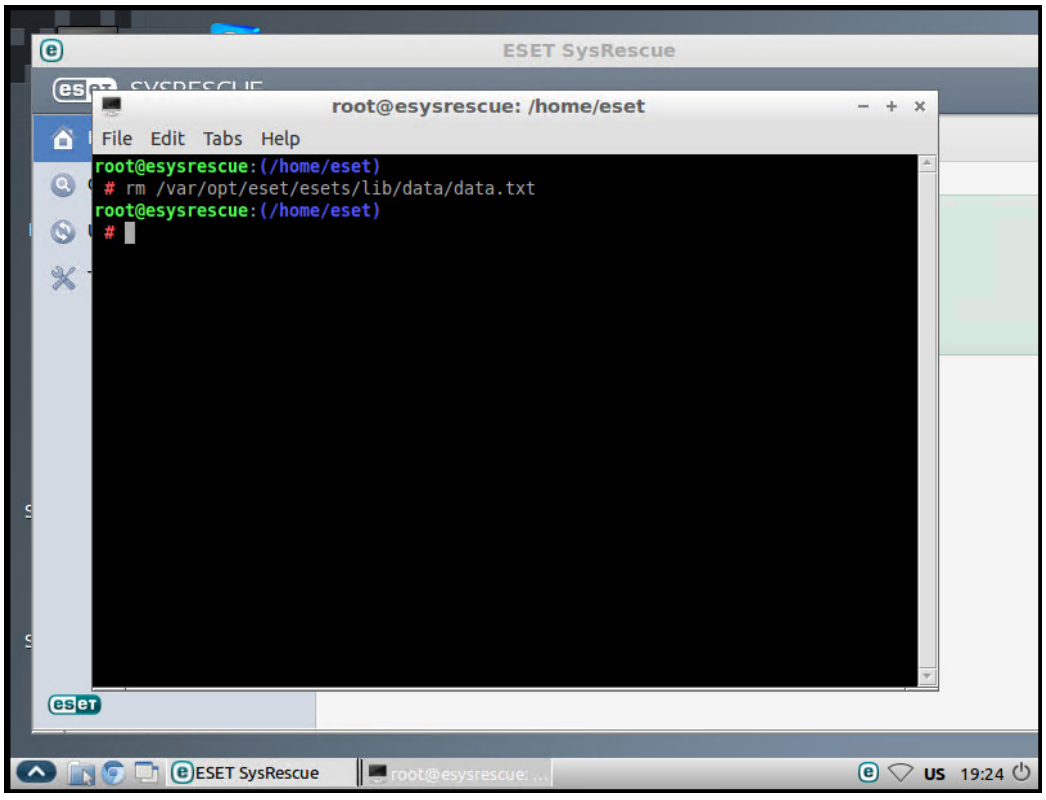
1. Оберіть із випадаючого меню показані на скріншоті пункти та натисніть кнопку "I accept …"



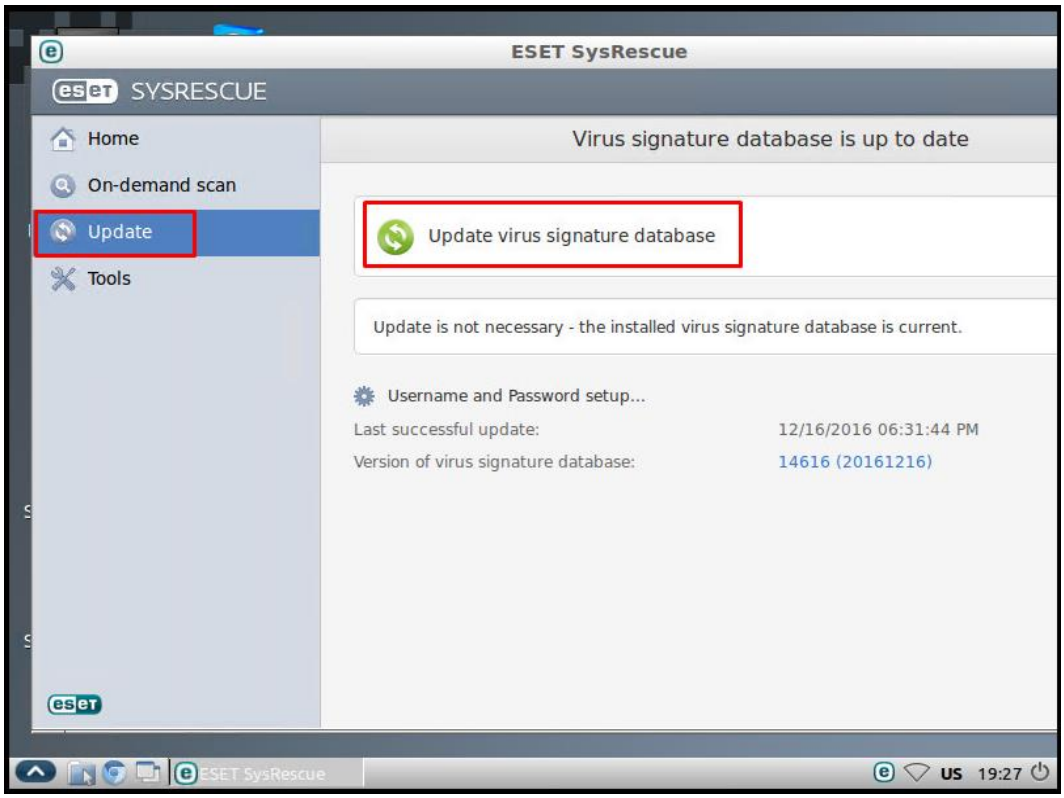
2. Відкрийте термінал



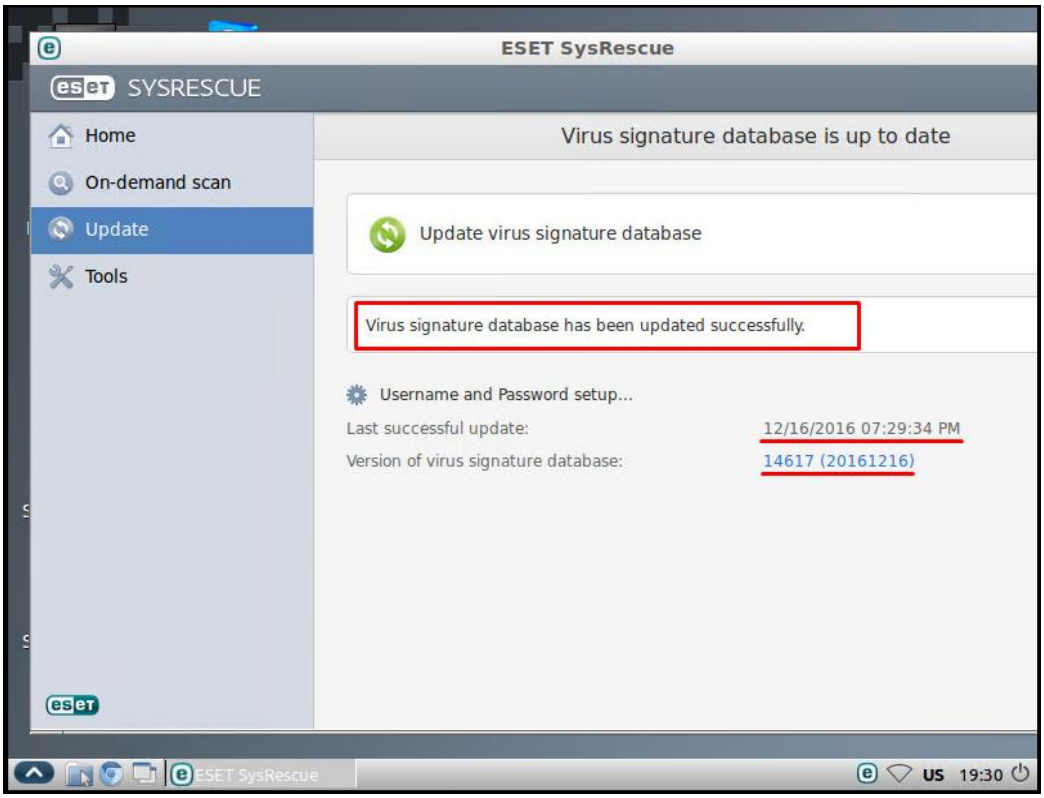
3. Введіть команду “rm /var/opt/eset/esets/lib/data/data.txt” та натисніть Enter на клавіатурі



4. Закрийте вікно терміналу.
5. У вікні сканера перейдіть до меню Update та натисніть “Update virus signature database”.



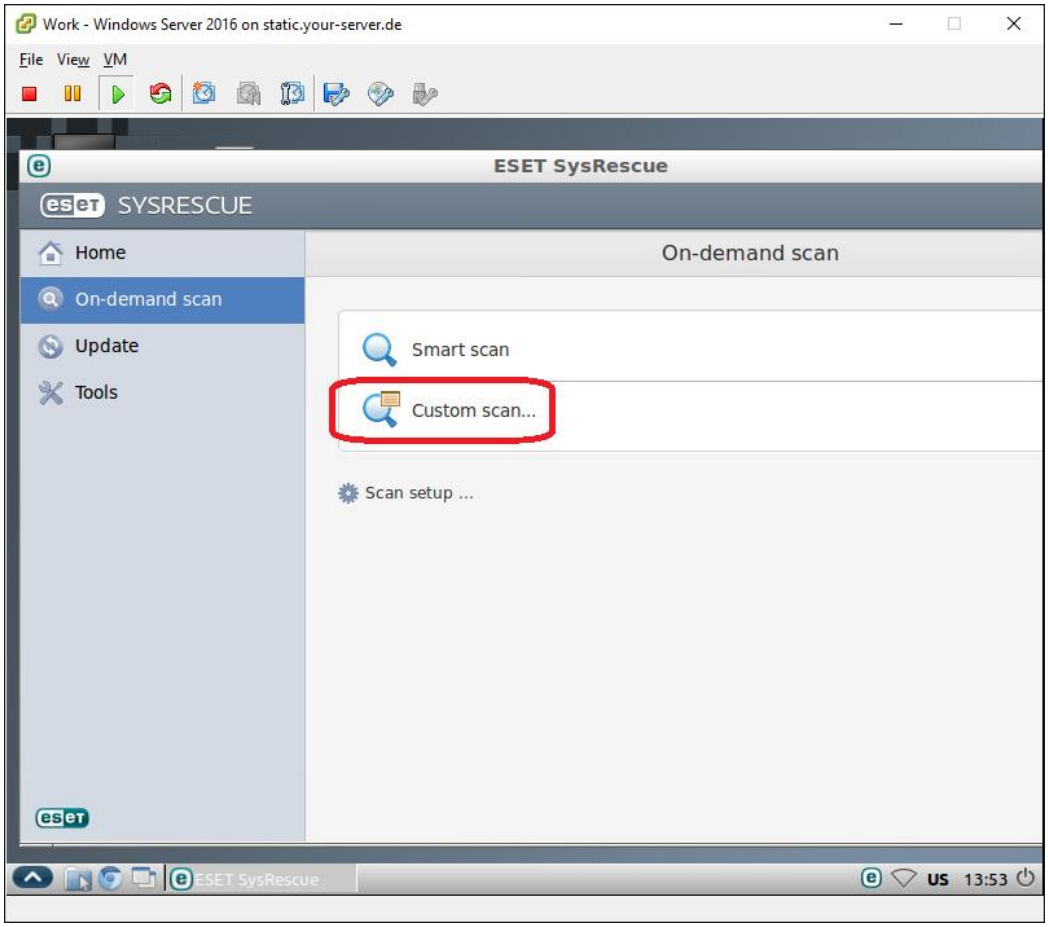
6. По завершенню процесу Ви побачите наступне



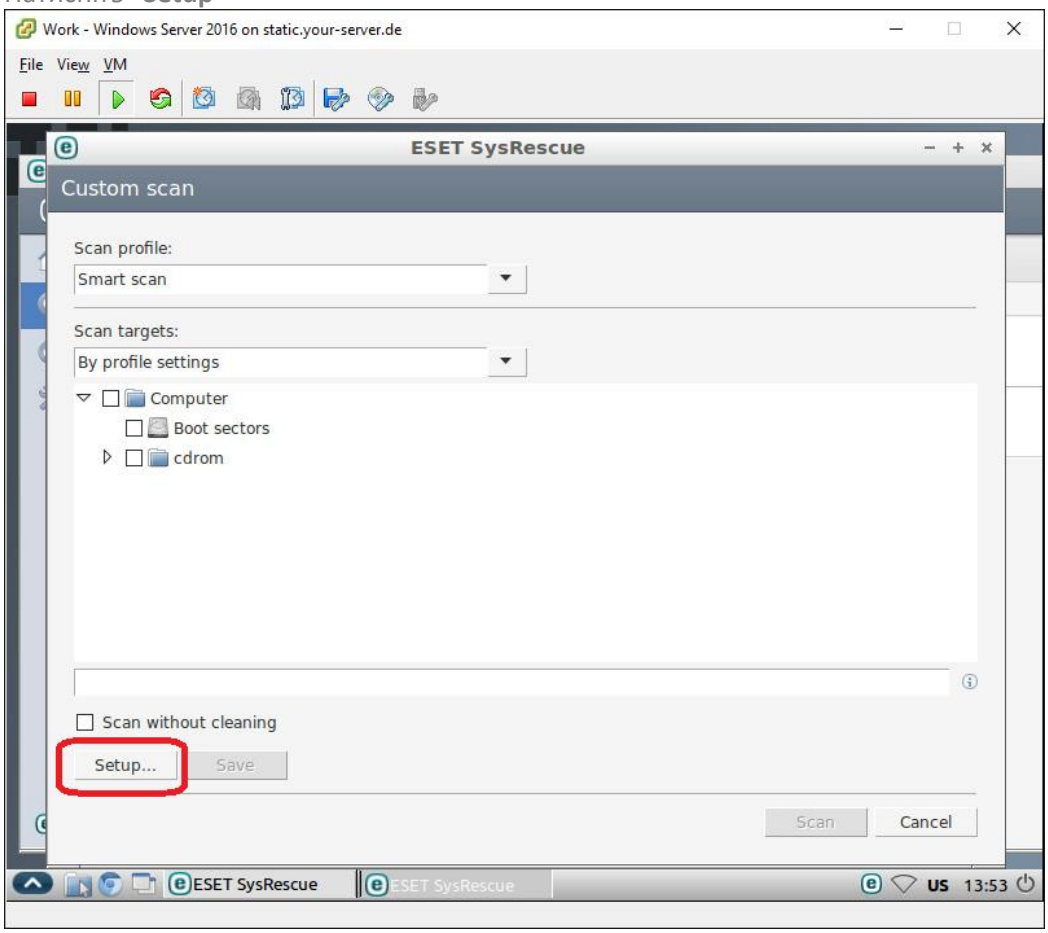
Додаток 3. Інструкція з лікування

ПРИМІТКА! Перед тим, як почати сканування? необхідно встановити ОПТИМАЛЬНІ параметри.

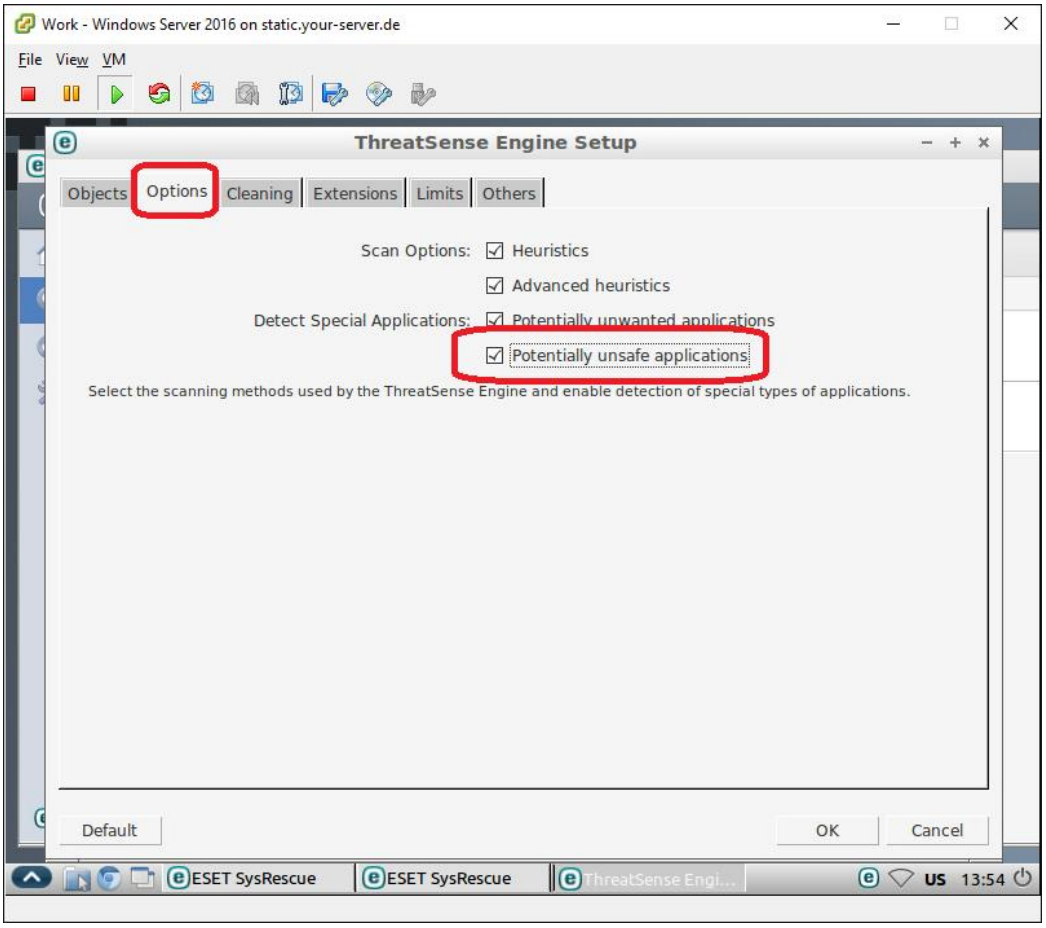
1. Оберіть **“Custom scan”**



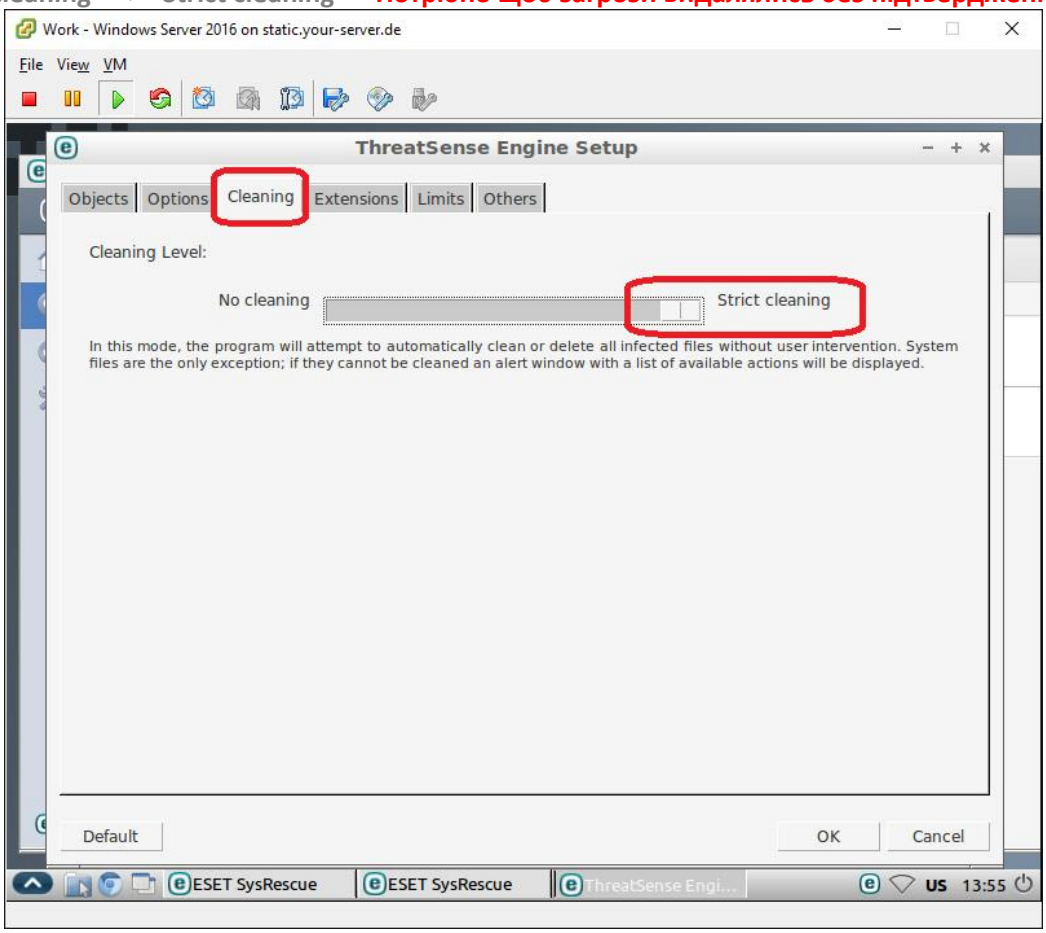
2. Натисніть **“Setup”**



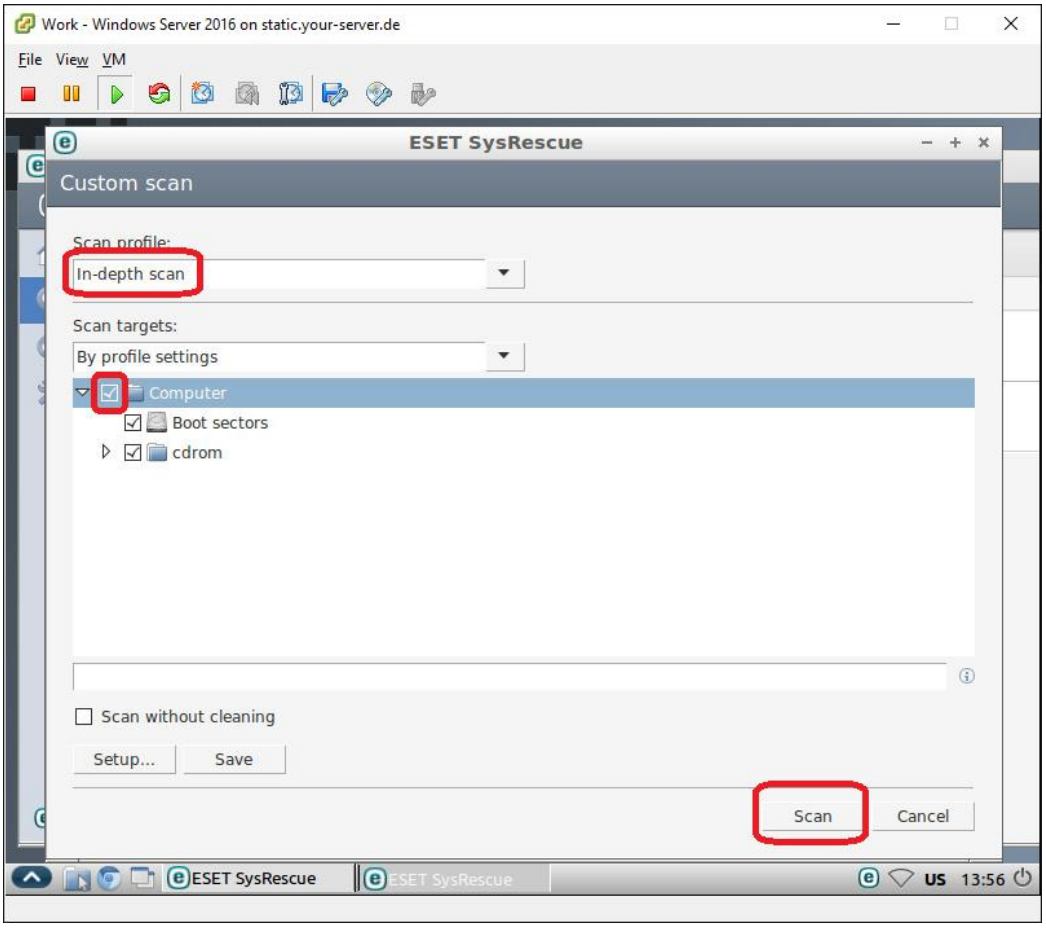
3. **“Options” --> “Potentially unsafe applications” – ЦЕ ДУЖЕ ВАЖЛИВО!!!!**



4. **“Cleaning” --> “Strict cleaning”** – **Потрібно щоб загрози видалялись без підтвердження.**



5. Режим – **“In-depth”**, можна обирати весь **“Computer”.**



6. По завершенню процесу Ви побачите наступне