ESET Tech Center

You receive an ESET UEFI detection

Anish | ESET Nederland - 2021-01-20 - Reacties (0) - Endpoint Solutions

Issue

- Your ESET product notifies you of a UEFI detection (for example, EFI/CompuTrace, Win32/CompuTrace, EFI/Lenovo, Win32/Lenovo)
- What is UEFI malware and how to prevent them
- How to resolve detections of applications in UEFI

Details

> UEFI Detections
> Since UEFI detections are specific to the hardware firmware that they are on, ESET cannot remove a UEFI detection. See the **Solution** section for possible remediation steps you can take.

The UEFI firmware loads into the memory at the beginning of the boot process. It is stored in a flash memory chip soldered onto the mainboard. If attackers infect the firmware, they can deploy malware that survives system reinstallations, reboots and even new hard drive installations. The malware can also remain unnoticed by antimalware solutions since most of them do not scan the firmware layer.

The ESET UEFI Scanner adds an industry-first protection layer against UEFI bootkits by scanning for malware in the firmware layer.

The following ESET products contain the UEFI scanner:

- ESET Mail Security for Microsoft Exchange Server (version 7)
- ESET File Security for Microsoft Windows Server (version 7)
- ESET Security for Microsoft SharePoint Server (version 7)
- ESET Mail Security for IBM Domino (version 7)
- ESET File Security for Azure
- ESET Smart Security Premium (version 11 and later)
- ESET Internet Security (version 11 and later)
- ESET NOD32 Antivirus (version 11 and later)
- ESET Endpoint Security/Antivirus (version 7 and later)

Solution

How to resolve ESET UEFI detections

> If you are not familiar with UEFI
> If you are not familiar with UEFI settings or the updating/flashing process, we recommend that you contact an experienced professional to help with this procedure.

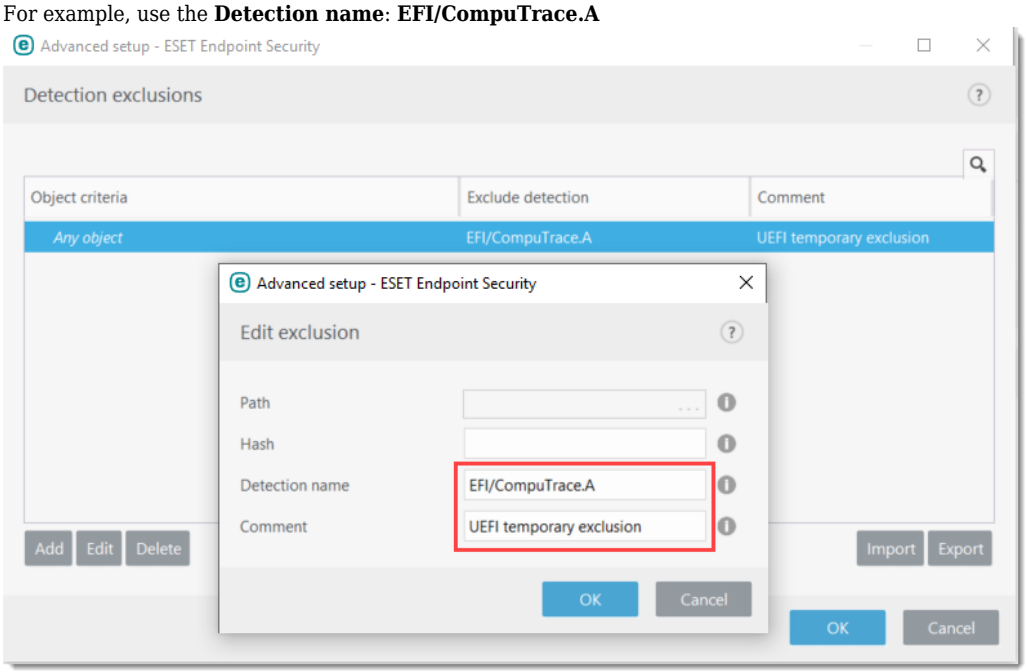
- Upgrade the firmware from your computer vendor and rescan with ESET UEFI scanner. If the UEFI detection remains, you can ask your computer vendor to update their firmware to remove the problematic detection.
- Exclude the detection in your ESET product. If you have enabled the detection of potentially unsafe applications and your computer vendor does not remove the application from its firmware, you can exclude the detection from future scans.

Home users: Exclude an application by name from scanning in ESET Windows home products.

Business users version 8: Add or Edit detection exclusions (8.x)

Business users version 7: Add or Edit detection exclusions (7.x)

For example, use the **Detection name**: **EFI/CompuTrace.A**



- Disable the "detection of potentially unsafe applications" option in your ESET product.

  Home users: Configure ESET products to detect or ignore unwanted, unsafe and suspicious applications.

  Business users: Enable or disable endpoint detection of potentially unwanted/unsafe applications using ESET Security Management Center (7.x).

- Reflash the SPI Flash Memory where the UEFI lives. This is a delicate and complex procedure and is different for every motherboard. Your computer manufacturer will be able to tell you if this is possible.

- For detailed information about UEFI malware including prevention and remediation, see the following WeLiveSecurity.com post: Lojax: First UEFI rootkit found in the wild, courtesy of the Sednit group.

- If you think that the detection is incorrect, submit the detection to the ESET malware lab for analysis.

- **How to protect your computer from UEFI malware**

  - **Use a computer with a newer chipset**
    Verify all of your systems have modern chipsets with Platform Controller Hub (starting from Intel Series 5 chipsets onwards).

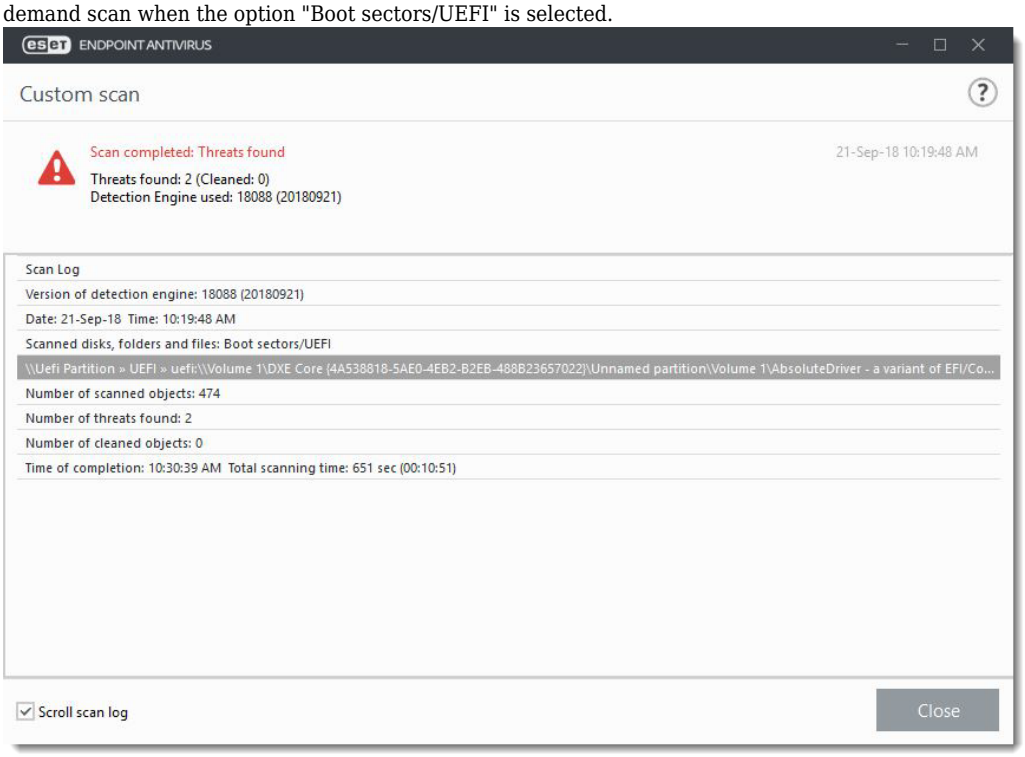
  - **Ensure that your computer has Secure Boot enabled**
    Typically, UEFI malware is not properly signed and having Secure Boot enabled will keep it from loading and infecting your computer.

  - **Upgrade your UEFI firmware on your computer**
    We recommend that you perform a UEFI firmware update even if your computer does not notify you of a detection. As a preventive measure, it may help minimize the chances of this type of infection.

ESET detects UEFI malware or applications

UEFI scanning is available in the latest versions of ESET products. See the Details section above for a list of ESET products that contain the UEFI scanner.

By default, the detection of potentially unsafe or unwanted applications is disabled in ESET products. Because UEFI infections are very specific to the hardware firmware that they infect, ESET can only detect and notify you of a UEFI infection. UEFI is only scanned during startup scan or during On-demand scan when the option "Boot sectors/UEFI" is selected.



If you are still unable to resolve your issue, email ESET Technical Support.

-