ESAT AV Remover

Threat: **AV Remover Tool**

Author: **Jeffrey Farnan**

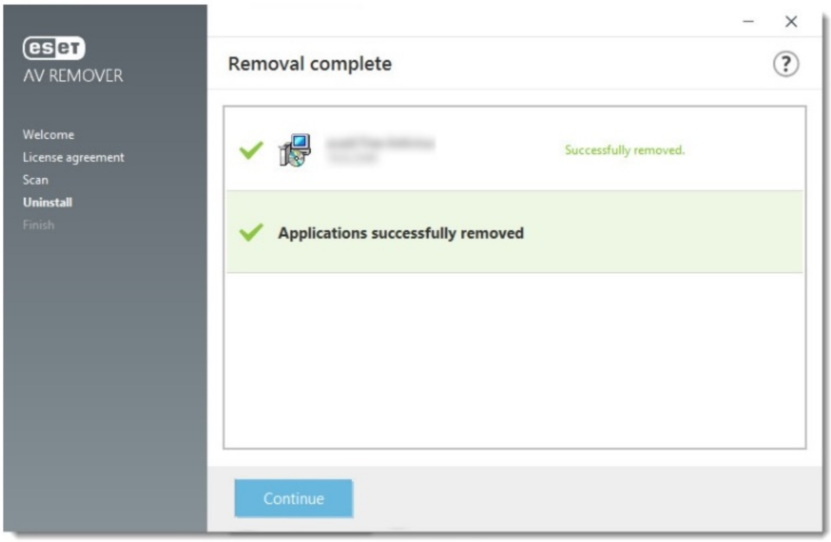
Date Originally Published: **July 26th, 2021**

1. SUMMARY

- The ESET AV Remover tool helps with the removal of any antivirus software previously installed on your system. This tool is useful for troubleshooting hard to remove products. It can also be used by hackers and bad actors to remove antivirus products before infecting a system.

2. THE PRODUCT INSTALLATION AND FUNCTIONALITY

- The installation of this product is fairly simple to download it and install it on your system. Go to the website: https://www.eset.com/int/support/av-remover/ choose the operating system and language and click download.
- This will download the executable avremover_nt_enu.exe onto your system, double click to run this application. Read the End-User Agreement and click accept.
- ESET AV Remover will now begin searching your system for antivirus products.



Removal complete

Successfully removed.

Applications successfully removed

- Once the scan is complete any security products it detects will show up in on screen. Click the selected item, and click uninstall, this should remove the product from your system. You will then be asked to restart your computer
- If you were unsuccessful in removing your antivirus software product, you will be prompted to restart your computer and rescan again.

3. MALWARE CHARATERISTICS

- **Suspected country of origin** = United States.
- **First seen date/period** = January 2013.
- **Still active** = Yes.
- **Last submitted sample as of writing this article** = October 20th, 2020.

4. APPLICATION HISTORY

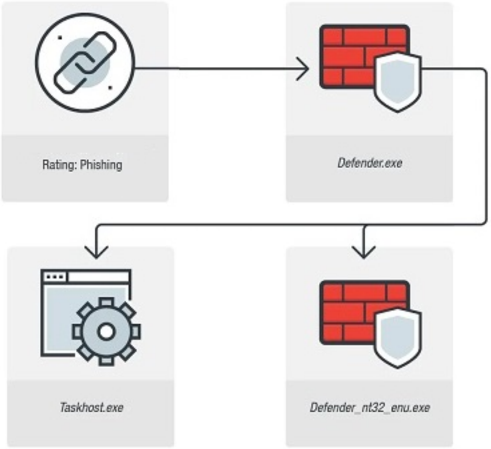
- ESET is an internet security company founded in 1987 and based in Bratislava, Slovakia. ESET is the Slovak name of the Egyptian goddess of health, marriage and love. ESET offers a range of high-performance, proactive endpoint security solutions.
- One of the products which ESET created is the Antivirus remover, users would complain off been unable to fully remove an Antivirus product, leaving files on their system and not completely erasing changes they have made. Sometimes traces of an old product interfere with the installation of new Antivirus being installed.

5. APPLICATION DESCRIPTION

- ESET AV Remover is a free portable application for the Windows operating system designed to uninstall antivirus products. Most anti-virus products offer uninstall programs to remove their products. From time to time you will find the uninstall process does not work or gets stuck and the product is left on your system. It is often complicated to remove all traces of the antivirus program from the operating system.
- ESET AV Remover is designed specifically to remove AV products. It has a selection process in which you select the programs that you want to remove.
- The remover supports the removal of antivirus and security products from companies such Avast, Avira, AVG, BitDefender, Kaspersky, Malwarebytes, Norton, Panda, Symantec and Trend Micro to name just a few.

6. POTENTIAL CUSTOMER DEFENCE

- Cybercriminals have a history of abusing authentic tools, this product is no exception, and it can be exploited. Hackers can use it to remove legitimate Antivirus products before infecting a system with other malware, or used to distract users while an infection is taking place.
- A recent campaign of Dharma Ransomware is using a legitimate installer such as ESET AV Remover to distract users while there machine is being encrypted in the background:
  - Trend Micro security experts found like other ransomware campaigns Dharma lures victims into downloading malicious files using phishing scams. Users get messages claiming to be from Microsoft alerting that their PC's are at risk and are corrupted and urging them to update and verify their antivirus product.



  - Once the users accepts, the files downloaded are a self-extracting archive name Defender.exe plus an old version of ESET Remover renamed as Defender_n32_enu.exe. This version of ESET AV Remover installer, to divert attention as it encrypts files on the victim's device. When the encryption is taking place in the background, users can see the ESET AV Remover installation being installed. Users will see the ESET GUI onscreen.

- **Good or Bad Verdict:** The product itself is deemed a good product, used in the right way. The tool itself is useful for Windows users who run into issues removing antivirus products from their systems. It can however can be used by Hackers to remove AV products when attempting to hack a system.

Research Sources:

- https://help.eset.com/ees/7/en-US/idh_bts_avremover.html
- https://help.eset.com/ees/7/en-US/idh_bts_avremover_error.html
- https://www.ghacks.net/2015/05/13/remove-antivirus-programs-with-eset-av-remover/
- https://www.spaceclick.com/blog/how-to-completely-remove-an-antivirus/

Disclaimer: All opinions expressed in this article are the opinions solely of the author.