

Open in app ↗

Sign up

Sign in

Medium

Search

Write



LOLBINed — Using Kaspersky Endpoint Security “KES” Installer to Execute Arbitrary Commands



Medium

Sign up to discover human stories that deepen your understanding of the world.

Free

- ✓ Distraction-free reading. No ads.
- ✓ Organize your knowledge with lists and highlights.
- ✓ Tell your story. Find your audience.

Sign up for free

✦ Membership

- ✓ Read member-only stories
- ✓ Support writers you read most
- ✓ Earn money for your writing
- ✓ Listen to audio narrations
- ✓ Read offline with the Medium app

Try for 5 \$/month

One AV uninstaller, in particular, we’ll be focusing on today is Kaspersky's **kavremover**. We’ll talk about how this uninstaller led to another issue in the Kaspersky Endpoint Security (KES) installer.

. . .

kavremover

Here is a quick description of the tool from the Kaspersky doc

Medium

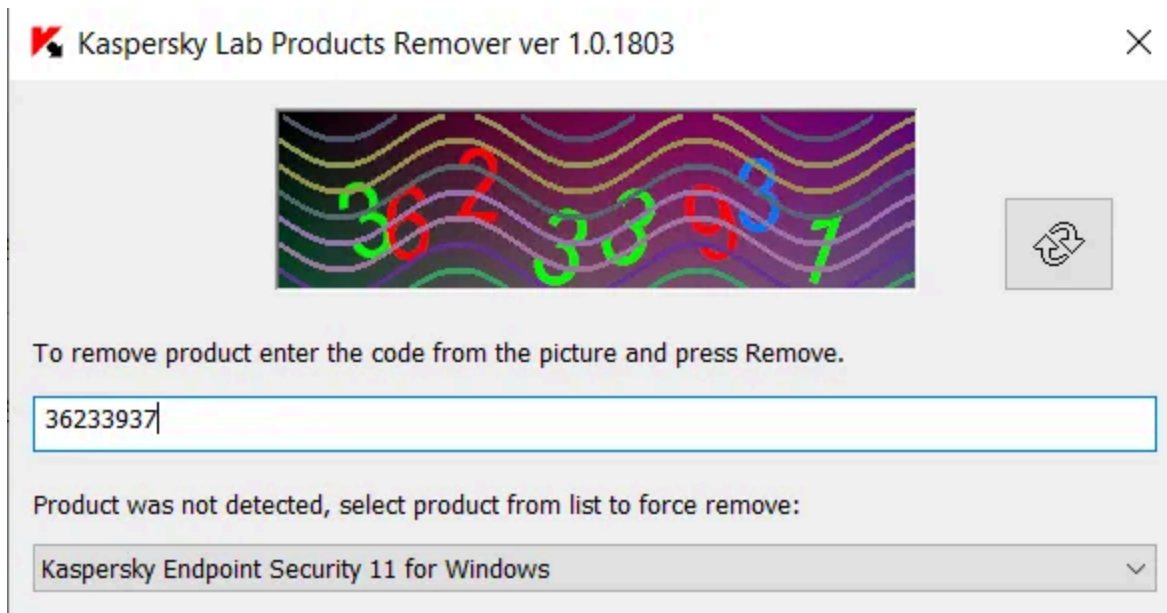
Sign up to discover human stories that deepen your understanding of the world.

Free

- ✓ Distraction-free reading. No ads.
- ✓ Organize your knowledge with lists and highlights.
- ✓ Tell your story. Find your audience.

✦ Membership

- ✓ Read member-only stories
- ✓ Support writers you read most
- ✓ Earn money for your writing
- ✓ Listen to audio narrations
- ✓ Read offline with the Medium app



Medium












Sign up to discover human stories that deepen your understanding of the world.

Free

- ✓ Distraction-free reading. No ads.
- ✓ Organize your knowledge with lists and highlights.
- ✓ Tell your story. Find your audience.

✦ Membership

- ✓ Read member-only stories
- ✓ Support writers you read most
- ✓ Earn money for your writing
- ✓ Listen to audio narrations
- ✓ Read offline with the Medium app

Process	Image Path
 kavremover.exe (15776)	C:\Users\lab\AppData\Local\Temp\{36CC7965-F668-481...
 regsvr32.exe (16068)	C:\Windows\SysWOW64\regsvr32.exe
 regsvr32.exe (16088)	C:\Windows\SysWOW64\regsvr32.exe
  actA7A1.tmp (16112)	C:\Users\lab\AppData\Local\Temp\actA7A1.tmp
 regsvr32.exe (16216)	C:\Windows\SysWOW64\regsvr32.exe
 regsvr32.exe (16236)	C:\Windows\SysWOW64\regsvr32.exe
  actA7A1.tmp (16276)	C:\Users\lab\AppData\Local\Temp\actA7A1.tmp
 regsvr32.exe (16376)	C:\Windows\SysWOW64\regsvr32.exe
 regsvr32.exe (12556)	C:\Windows\SysWOW64\regsvr32.exe
  actA7A1.tmp (14804)	C:\Users\lab\AppData\Local\Temp\actA7A1.tmp
 msixexec.exe (11768)	C:\Windows\SysWOW64\msixexec.exe
  actA7A1.tmp (15940)	C:\Users\lab\AppData\Local\Temp\actA7A1.tmp

Medium

Sign up to discover human stories that deepen your understanding of the world.

Free

- ✓ Distraction-free reading. No ads.
- ✓ Organize your knowledge with lists and highlights.
- ✓ Tell your story. Find your audience.

✦ Membership

- ✓ Read member-only stories
- ✓ Support writers you read most
- ✓ Earn money for your writing
- ✓ Listen to audio narrations
- ✓ Read offline with the Medium app

Medium

Sign up to discover human stories that deepen your understanding of the world.

Free

- ✓ Distraction-free reading. No ads.
 - ✓ Organize your knowledge with lists and highlights.
 - ✓ Tell your story. Find your audience.
-

✦ Membership

- ✓ Read member-only stories
 - ✓ Support writers you read most
 - ✓ Earn money for your writing
 - ✓ Listen to audio narrations
 - ✓ Read offline with the Medium app
-

Now with the executable in hand, let's follow the same structure and replace the “regsvr32” call with a random command:

```
RT_RCDATA503.exe run run-cmd "cmd /c whoami > whoami.txt"
```

Medium

Sign up to discover human stories that deepen your understanding of the world.

Free

- ✓ Distraction-free reading. No ads.
- ✓ Organize your knowledge with lists and highlights.
- ✓ Tell your story. Find your audience.

✦ Membership

- ✓ Read member-only stories
- ✓ Support writers you read most
- ✓ Earn money for your writing
- ✓ Listen to audio narrations
- ✓ Read offline with the Medium app

Now this is an interesting LOLBIN and if the story ended here I would've been happy but it didn't, so let us continue.

Kaspersky Endpoint Security (KES) Installer

While doing this research and in order to test these different uninstallers, I was also installing the AV product in question and while playing with KES installer I got the following prompt from KES

Medium

Sign up to discover human stories that deepen your understanding of the world.

Free

- ✓ Distraction-free reading. No ads.
- ✓ Organize your knowledge with lists and highlights.
- ✓ Tell your story. Find your audience.

✦ Membership

- ✓ Read member-only stories
- ✓ Support writers you read most
- ✓ Earn money for your writing
- ✓ Listen to audio narrations
- ✓ Read offline with the Medium app

The “act3CB2.tmp” has the same arguments as the previous binary we looked at with “kavremover” which leads us to the theory that the KES installer is using the same method to remove other AVs. Now the thing that got me super interested in this, is how was KES able to detect that I had AVG 2015 installed.

Medium

Sign up to discover human stories that deepen your understanding of the world.

Free

- ✓ Distraction-free reading. No ads.
- ✓ Organize your knowledge with lists and highlights.
- ✓ Tell your story. Find your audience.

✦ Membership

- ✓ Read member-only stories
- ✓ Support writers you read most
- ✓ Earn money for your writing
- ✓ Listen to audio narrations
- ✓ Read offline with the Medium app

The contents of “incompatible.txt” are a long list of security products (AV, EDR, VPN, Firewalls...) that from the name of the file we guess that KES may be incompatible with (ie can cause issues if both software are installed).

Medium

Sign up to discover human stories that deepen your understanding of the world.

Free

- ✓ Distraction-free reading. No ads.
- ✓ Organize your knowledge with lists and highlights.
- ✓ Tell your story. Find your audience.

✦ Membership

- ✓ Read member-only stories
- ✓ Support writers you read most
- ✓ Earn money for your writing
- ✓ Listen to audio narrations
- ✓ Read offline with the Medium app

Medium

Sign up to discover human stories that deepen your understanding of the world.

Free

- ✓ Distraction-free reading. No ads.
- ✓ Organize your knowledge with lists and highlights.
- ✓ Tell your story. Find your audience.

✦ Membership

- ✓ Read member-only stories
- ✓ Support writers you read most
- ✓ Earn money for your writing
- ✓ Listen to audio narrations
- ✓ Read offline with the Medium app

To view the content of the “cleaner.cab” file we first need to unzip it using a tool like 7zip.

Medium

Sign up to discover human stories that deepen your understanding of the world.

Free

- ✓ Distraction-free reading. No ads.
- ✓ Organize your knowledge with lists and highlights.
- ✓ Tell your story. Find your audience.

✦ Membership

- ✓ Read member-only stories
- ✓ Support writers you read most
- ✓ Earn money for your writing
- ✓ Listen to audio narrations
- ✓ Read offline with the Medium app

go back to the “.ini” files in a moment.

Scrolling down a little we find the binary we’re looking for, “cleanapi.exe”.

Hey, I Don’t Like Your AV...Can I Remove It

Back to the original question, how was KES able to determine that I had AVG 2015 installed? Well, looking inside the cleaner folder I’ve found the following “.ini” files

Medium

Sign up to discover human stories that deepen your understanding of the world.

Free

- ✓ Distraction-free reading. No ads.
- ✓ Organize your knowledge with lists and highlights.
- ✓ Tell your story. Find your audience.

✦ Membership

- ✓ Read member-only stories
- ✓ Support writers you read most
- ✓ Earn money for your writing
- ✓ Listen to audio narrations
- ✓ Read offline with the Medium app

```
....
```

```
type=uninstall
```

```
....
```

```
env-
```

```
registry=HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\AVG\UninstallString->UninstallString
```

Sparing you the boring details because this is getting long already. Basically, the check for “AVG” is done by checking the registry for the key specified in the “**detect-registry**” variable. If it’s found then the value pointed at by the

Medium

Sign up to discover human stories that deepen your understanding of the world.

Free

- ✓ Distraction-free reading. No ads.
- ✓ Organize your knowledge with lists and highlights.
- ✓ Tell your story. Find your audience.

✦ Membership

- ✓ Read member-only stories
- ✓ Support writers you read most
- ✓ Earn money for your writing
- ✓ Listen to audio narrations
- ✓ Read offline with the Medium app

Notepad executed

We now are able to execute arbitrary commands and processes from the context of the signed Kaspersky process as long as we simulate an AV that is “unsupported” by KES in order to trigger the uninstallation process.

Note that this command requires administrative privileges to execute.

Medium

Sign up to discover human stories that deepen your understanding of the world.

Free

- ✓ Distraction-free reading. No ads.
- ✓ Organize your knowledge with lists and highlights.
- ✓ Tell your story. Find your audience.

✦ Membership

- ✓ Read member-only stories
- ✓ Support writers you read most
- ✓ Earn money for your writing
- ✓ Listen to audio narrations
- ✓ Read offline with the Medium app

I created a simple script that parsed all those “.ini” files and compiled the results in a CSV file that will be available in the repository mentioned at the start of this blog.

Here is an example of how it looks.

Medium

Sign up to discover human stories that deepen your understanding of the world.

Free

- ✓ Distraction-free reading. No ads.
- ✓ Organize your knowledge with lists and highlights.
- ✓ Tell your story. Find your audience.

✦ Membership

- ✓ Read member-only stories
- ✓ Support writers you read most
- ✓ Earn money for your writing
- ✓ Listen to audio narrations
- ✓ Read offline with the Medium app

Medium

Sign up to discover human stories that deepen your understanding of the world.

Free

- ✓ Distraction-free reading. No ads.
- ✓ Organize your knowledge with lists and highlights.
- ✓ Tell your story. Find your audience.

✦ Membership

- ✓ Read member-only stories
- ✓ Support writers you read most
- ✓ Earn money for your writing
- ✓ Listen to audio narrations
- ✓ Read offline with the Medium app

One last thing before I wrap this up. If you noticed when we looked at the process tree, the “cleanapi.exe” had a bunch of command-line arguments.

```
"C:\Users\lab\AppData\Local\Temp\282527F5EDA44439AD3CC23FD270EE91\
clr\flt\cleanapi.exe" -r -t 1 -n cleanapi.dll -d
C:\Users\lab\AppData\Local\Temp\282527F5EDA44439AD3CC23FD270EE91\c
lr\flt\
```

One interesting argument out of the bunch is the “-n” where we’re passing it

Medium

Sign up to discover human stories that deepen your understanding of the world.

Free

- ✓ Distraction-free reading. No ads.
- ✓ Organize your knowledge with lists and highlights.
- ✓ Tell your story. Find your audience.

✦ Membership

- ✓ Read member-only stories
- ✓ Support writers you read most
- ✓ Earn money for your writing
- ✓ Listen to audio narrations
- ✓ Read offline with the Medium app

Medium

Sign up to discover human stories that deepen your understanding of the world.

Free

- ✓ Distraction-free reading. No ads.
- ✓ Organize your knowledge with lists and highlights.
- ✓ Tell your story. Find your audience.

✦ Membership

- ✓ Read member-only stories
- ✓ Support writers you read most
- ✓ Earn money for your writing
- ✓ Listen to audio narrations
- ✓ Read offline with the Medium app

- We can execute arbitrary commands from the context of the KES installer using the registry (or any installation method described in the INI files in theory) as described above.
- You can “remove”/“detect” more than “2400” security products using Kaspersky Endpoint Security “KES” installer.
- We can call arbitrary DLLs using the “cleanapi.exe” binary using the following command.

Medium

Sign up to discover human stories that deepen your understanding of the world.

Free

- ✓ Distraction-free reading. No ads.
- ✓ Organize your knowledge with lists and highlights.
- ✓ Tell your story. Find your audience.

✦ Membership

- ✓ Read member-only stories
- ✓ Support writers you read most
- ✓ Earn money for your writing
- ✓ Listen to audio narrations
- ✓ Read offline with the Medium app



-- 1



Written by **Nasreddine Bencherchali**

Follow

Medium

Sign up to discover human stories that deepen your understanding of the world.

Free

- ✓ Distraction-free reading. No ads.
- ✓ Organize your knowledge with lists and highlights.
- ✓ Tell your story. Find your audience.

✦ Membership

- ✓ Read member-only stories
- ✓ Support writers you read most
- ✓ Earn money for your writing
- ✓ Listen to audio narrations
- ✓ Read offline with the Medium app