


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

 Nasreddine Bencherchali · Follow
8 min read · Nov 1, 2022



17



1



Kaspersky Logo

Introduction

At the start of the year, I was doing some research into AV uninstaller tools, understanding how they work, and trying to find misconfigurations and other ways they can be abused I’ve compiled my findings in the repository that I’ll make public soon.

One AV uninstaller, in particular, we’ll be focusing on today is Kaspersky's

Medium

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

Free

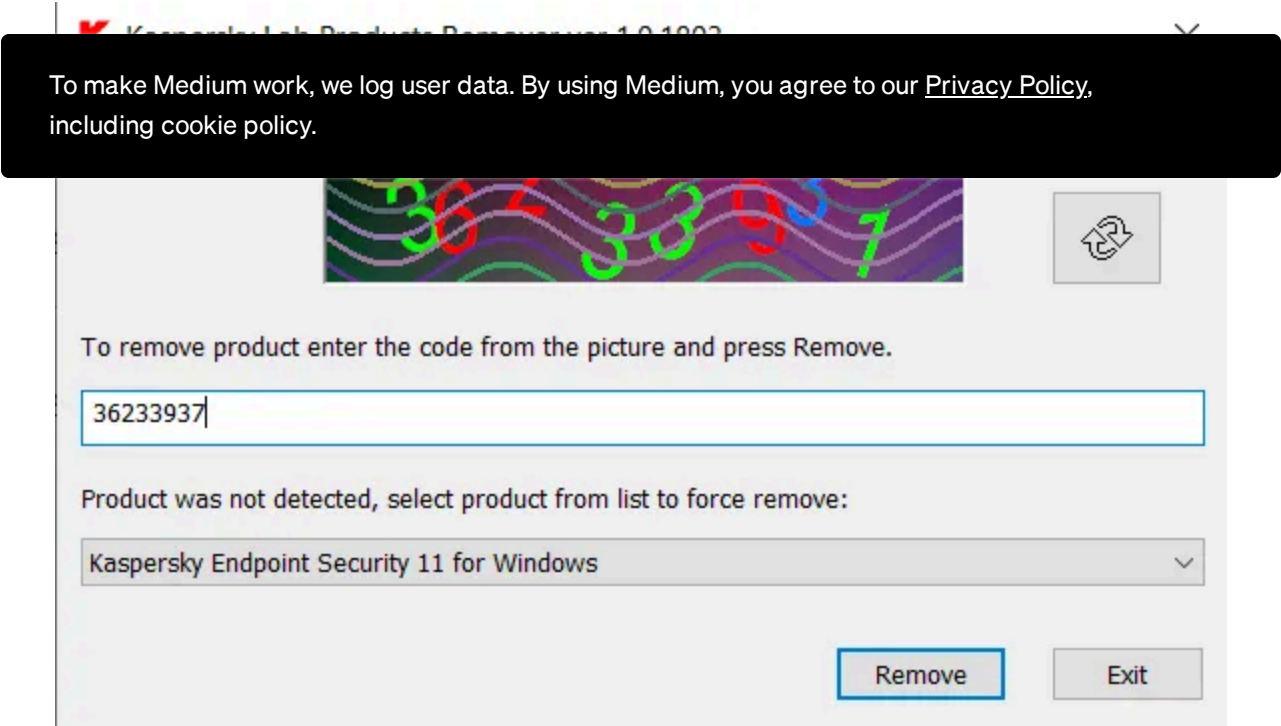
- ✓ Distraction-free reading. No ads.
- ✓ Organize your knowledge with lists and highlights.
- ✓ Tell your story. Find your audience.

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



Once we click “Remove” the removal process starts with no additional prompts until it finishes. (Note that this tool requires administrator privileges to be executed)

Now, let’s take a look at this from “Process Monitor” to see what the process is actually doing behind the scene.

| 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 |

Medium

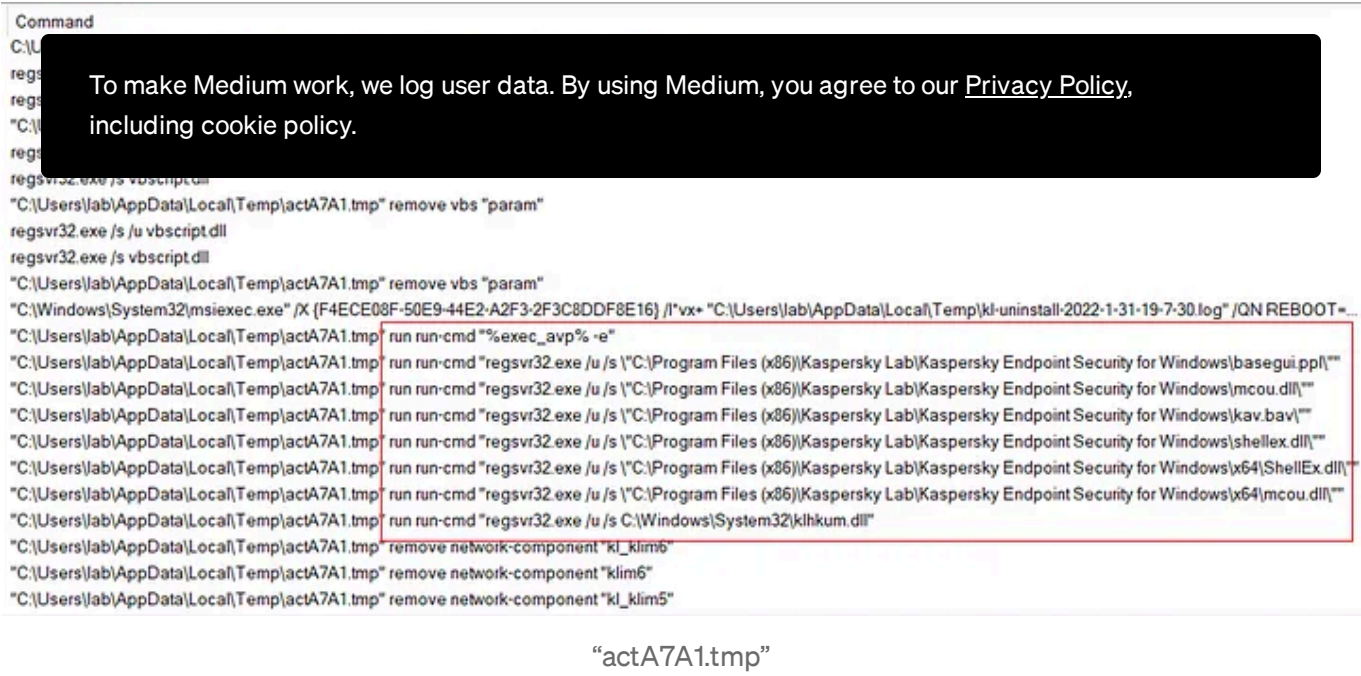
Sign up to discover human stories that deepen your understanding of the world.

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 “run-cmd” keyword got me intrigued, especially since it’s running an instance of “regsvr32”

```

"C:\Users\lab\AppData\Local\Temp\actA7A1.tmp" run run-cmd
"regsvr32.exe /u /s \"C:\Program Files (x86)\Kaspersky
Lab\Kaspersky Endpoint Security for Windows\mcou.dll\""
```

This command line seemed like it would allow arbitrary binaries to execute just like a LOLBIN, so I decided to take a look at this dropped file.

To get it I simply re-run the “kavremover” process and used a SYSTEM command prompt to copy it while it was running.

Note that we can extract this binary by extracting it from the resource section of the original “kavremover” using a tool like “[Resource Hacker](#)”.

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 make Medium work, we log user data. By using Medium, you agree to our [Privacy Policy](#), including cookie policy.

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. This time, however, the arguments are not the same. This got me super interested in this, is how was KES able to detect that I had AVG 2015 installed.

By looking at the process tree we can see that the “act3CB2.tmp” has a parent process called “cleanapi.exe” which sounds very interesting, so I started looking for this “cleanapi.exe” inside the KES installer

By double-clicking on the installer it first “decompresses” itself into a specified location. If we look at the directory structure of the uncompressed data we see two interesting files that are maybe related to the “cleaning” functionality.

- cleaner.cab
- incompatible.txt

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

Page 5 of 14

To make Medium work, we log user data. By using Medium, you agree to our [Privacy Policy](#), including cookie policy.

incomptabile.txt

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

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 make Medium work, we log user data. By using Medium, you agree to our [Privacy Policy](#), including cookie policy.

cleaner.cab

At first glance, we can see that the names of the “.ini” files correspond with a one-to-one mapping with the names inside the “**incompatible.txt**” file. We’ll go back to the “.ini” files in a moment.

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

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 make Medium work, we log user data. By using Medium, you agree to our [Privacy Policy](#), including cookie policy.

Content of “avg_free_av_2015_x64.ini”

Three things pop up right out of the gate:

```

detect-registry=HKEY_LOCAL_MACHINE\SOFTWARE\Avg\Avg2015

....

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 “env-registry” is run.

To test this out I did the following steps:

- Remove AVG from the system

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

To make Medium work, we log user data. By using Medium, you agree to our [Privacy Policy](#), including cookie policy.

We can execute arbitrary commands in 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 of course requires admin privileges in order to modify the necessary registry keys (HKLM) and run the KES installer.

On the other hand, this could offer an interesting setup for attackers who might stumble upon organizations that are already running Kaspersky, as this could be used to execute commands coming from a Kaspersky process which could be already whitelisted by the security team or it could be used as some kind of backdoor/persistence where each time the KES installation occurs this behaviour will occur.

Do You Have This AV Installed?

One interesting side effect of this research is the discovery of those “.ini” files that I mentioned above. There are 2450 “.ini” files in the “cleaner.cab” file which means we have a method and in some cases “multiple” methods to detect around “2450” different security products (AV, EDR, VPN, Firewalls...).

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

“Resource Hacker” we find that the binary in question is located inside the resource file.

To make Medium work, we log user data. By using Medium, you agree to our [Privacy Policy](#), including cookie policy.

By dumping it, we get a similar signed binary (different hash though) as 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

To make Medium work, we log user data. By using Medium, you agree to our [Privacy Policy](#), including cookie policy.

We can clearly see via “Process Monitor” that the process in question is looking for our random DLL

cleanapi.exe looking for malware.dll

We can quickly create a “calc” POC to test if it’s loading arbitrary DLLs. And indeed once the POC is run we get a calc popping up. (Of course, the “cleanapi.exe” binary is signed.)

Signed “cleanapi.exe”

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

To make Medium work, we log user data. By using Medium, you agree to our [Privacy Policy](#), including cookie policy.
- 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.


```
cleanapi.exe -n [MaliciousDLL]
```

Kaspersky has published a security advisory on these findings that you can find below.

List of Advisories

List of disclosed vulnerabilities in Kaspersky products and researchers that reported them to us.

support.kaspersky.com



Thanks for reading and I hope you found the post useful. If you want to chat about anything related to infosec I’m on Twitter [@nas_bench](#)

- Lolbin

Windows

Kaspersky

Vulnerability

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

Page 12 of 14

To make Medium work, we log user data. By using Medium, you agree to our [Privacy Policy](#), including cookie policy.



Nasreddine Bencherchali

Demystifying the “SVCHOST.EXE” Process and Its Command Line...

Understanding the “svchost.exe” process and its command line options

Sep 26, 2020



366



1



Nasreddine Bencherchali

What is the “DLLHOST.EXE” Process Actually Running

A Deep Dive Into “DLLHOST.EXE”

Oct 17, 2020



122



Nasreddine Bencherchali

Windows System Processes—An Overview For Blue Teams

An overview into windows system process and their parent child relationship.

Oct 24, 2020



77



3



Nasreddine Bencherchali

A Deep Dive Into Windows Scheduled Tasks and The...

Understanding the task scheduler service, “taskhostw.exe” and its command line...

Nov 1, 2020



18



1



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

