Forum:Hack Forums

Thread: disable client AVs?

THC - *November 26, 2016, 9:40 pm*
I'm currently using njrat and I was wondering if there is any way to disable client AVs, especially windows defender. I can execute scripts and such.

yotoprules - *November 27, 2016, 5:32 am*
If you had a paid RAT you could use a UAC exploit to gain privilages to setup hidden RDP and uninstall it from the second account. A lot of work I know. Otherwise, sorry I don't think you can disable your clients AV.

Viikinki - *November 27, 2016, 5:34 am*
Dunno know about njrat. But for metasploit there's killav.

CichyCichoCiemny - *November 27, 2016, 12:30 pm*
Get the list of AVs from the Metasploit kill avs module list and re-write them into a batch file.
You also could just compile the ruby script.
?

SIM-2053312 - *November 27, 2016, 3:20 pm*
If you have admin you can disable them

Armada - *November 27, 2016, 3:23 pm*
Prob want a AV nuker/filter run on Admin rights to properly circumvent the hooks, or add the filtration required.

VirtualMon3y - *November 27, 2016, 4:16 pm*
(Nov 26, 2016 10:40 PM)M.D. Wrote: *[CITE]* I'm currently using njrat and I was wondering if there is any way to disable client AVs, especially windows defender. I can execute scripts and such.
I know you are skint bro but:

https://hackforums.net/showthread.php?tid=5398632

LanMan - *November 28, 2016, 4:10 am*
Get the product ID of the AV installed and then "msiexec /x PRODUCTID" to uninstall it silently.
You need to have Admin right and that's all.

Armada - *November 28, 2016, 8:05 am*
(Nov 28, 2016 05:10 AM)LanMan Wrote: *[CITE]* Get the product ID of the AV installed and then "msiexec /x PRODUCTID" to uninstall it silently.
You need to have Admin right and that's all.
That is actually pretty tricky lol
GG

warpje - *November 28, 2016, 8:43 am*
(Nov 28, 2016 05:10 AM)LanMan Wrote: *[CITE]* Get the product ID of the AV installed and then "msiexec /x PRODUCTID" to uninstall it silently.
You need to have Admin right and that's all.

Gone test this out! Would be pretty Nice and Easy to do!

LanMan - *November 28, 2016, 8:56 am*

(Nov 28, 2016 09:05 AM)Armada Wrote: [CITE] That is actually pretty tricky lol
GGYes it is haha, using the installation manager to "officialy" uninstall AV.

(Nov 28, 2016 09:43 AM)warpje Wrote: [CITE] Gone test this out! Would be pretty Nice and Easy to do!
If i remember correctly you can list all programs (with their product id) with "wmic.exe product list brief"

QU?CKSILVER - *November 28, 2016, 12:02 pm*

(Nov 28, 2016 09:56 AM)LanMan Wrote: [CITE] Yes it is haha, using the installation manager to "officialy" uninstall AV.

If i remember correctly you can list all programs (with their product id) with "wmic.exe product list brief"
Hmm, you forgot a little something at the end of it ?

"/quiet" for silent uninstallation ?

LanMan - *November 28, 2016, 12:18 pm*

(Nov 28, 2016 01:02 PM)QU?CKSILVER Wrote: [CITE] Hmm, you forgot a little something at the end of it ?

"/quiet" for silent uninstallation ?
Oops maybe, i wrote it off the top of my head

Armada - *November 28, 2016, 1:46 pm*

(Nov 28, 2016 01:02 PM)QU?CKSILVER Wrote: [CITE] Hmm, you forgot a little something at the end of it ?

"/quiet" for silent uninstallation ?
(Nov 28, 2016 01:18 PM)LanMan Wrote: [CITE] Oops maybe, i wrote it off the top of my head
Think he meant the /q or /s command line....

Regardless interesting and efficient approach.