

Forum:[Hack Forums](#)

Thread: [How AV killers work.](#)

IcYSeptember - September 22, 2014, 8:22 am

Just thought I'd write up a quick paper on how AV killers work.

I'm not going into detail about how the file is deleted, or how any of the advanced stuff works...because that stuff is private, not a lot of people know that, I think.

Not a lot of people know the part I'm telling you, either.

This is not meant to bring on a new wave of skid malware that disables your AV, this is to bring common knowledge on how these things work so that they can be stopped.

Okay! On to the fun.

What is an AV killer?

Spoiler ([Click to View](#)) Really? It kills your Anti virus...you knew that.

How do they work?

Spoiler ([Click to View](#))

Before you learn how they work, let's take a peek at the registry really fast.

There's a registry key in HKLM (which means you need admin privileges to write there). It's called: Code Software\Microsoft\Windows NT\CurrentVersion\Image File Execution Options

What's so special about this?

This allows you to set a "debugger" for any program you want (that isn't protected against this, like Avast!).

What does this mean?

Watch this video, it'll explain it (disregard the title, I always forget to change it in the program I use to upload videos):

[Video: <https://www.youtube.com/watch?v=nK2XYqFwgmY>]

Thankfully some AntiViruses (like earlier, Avast!) guard against this. But if an AV killer is run before the AntiVirus is started, or installed, it's all over for the Anti Virus.

Now, for an AV killer, all it has to do is get administrator privileges, and write to that key.

Also, I've discovered a NEW way of killing antiviruses, that doesn't involve this registry key. And as far as I know, no antiviruses guard against this.

This method, however, I'll keep private for now.

I'll be releasing an AV killer tool in the Hacking Tools section in a few minutes, and I'll link to it here.

Edit: <https://hackforums.net/showthread.php?tid=4457573>

kannss - September 22, 2014, 8:30 am

thanks for proving good information sir

Waiting for tool to release

Austerity - September 22, 2014, 3:04 pm

Very interesting piece of work you have made here, keep it up!

TheExclusive - September 23, 2014, 5:50 am

Thanks for this very usefull information

Edge of Nowhere - September 23, 2014, 6:07 am

I was surprised that I actually learned something from HF.

Good work, we need to talk in private. Have an interesting proposition for you.

Meow - September 23, 2014, 6:12 am

Again,not sure what are you talking about but I'm sure it's some 1337 1-day Elite Sandboxie h4x0r shit!

Icy is very experienced 'hacker'.

Edge of Nowhere - September 23, 2014, 6:15 am

(Sep 23, 2014 06:12 AM)Meow. Wrote: [\[CITE\]](#) Again,not sure what are you talking about but I'm sure it's some 1337 1-day Elite Sandboxie h4x0r shit!

Icy is very experienced 'hacker'.

Bashing yet you didn't take 2 minutes to watch the video. It might not be a 0day, but it's equally as useful if used correctly.

Don't be mad he posted something useful and that you didn't.

Meow - September 23, 2014, 6:16 am

(Sep 23, 2014 06:15 AM)01000101 Wrote: [\[CITE\]](#) Bashing yet you didn't take 2 minutes to watch the video. It might not be a 0day, but it's equally as useful if used correctly.

Don't be mad he posted something useful and that you didn't.

HE IS MY CLOSE FRIEND AND I'M JOKING WITH HIM YOU DUMB..???

Edge of Nowhere - September 23, 2014, 6:17 am

(Sep 23, 2014 06:16 AM)Meow. Wrote: [\[CITE\]](#) HE IS MY CLOSE FRIEND AND I'M JOKING WITH HIM YOU DUMB..???

I'm supposed to know this? Next time, just don't post.

Just makes you look like an ignorant fool.

IcYSeptember - September 23, 2014, 7:54 am

(Sep 23, 2014 06:17 AM)01000101 Wrote: [\[CITE\]](#) I'm supposed to know this? Next time, just don't post.

Just makes you look like an ignorant fool.

Haha. It's fine, don't worry.

(Sep 23, 2014 06:07 AM)01000101 Wrote: [\[CITE\]](#) I was surprised that I actually learned something from HF.

Good work, we need to talk in private. Have an interesting proposition for you.

I'm glad I could teach you something.

If you want to talk, PM me with your Skype/Jabber. :)

Yoshikage Kira - September 23, 2014, 8:05 am

There are some other options, I forget how betabot does it, but I am pretty certain it does not do this. I also remember that Jack's channel(before it got removed) uninstalled a few av's if they had the silent uninstall option.

IcYSeptember - September 23, 2014, 8:16 am

(Sep 23, 2014 08:05 AM)Aletheia Wrote: [\[CITE\]](#) There are some other options, I forget how betabot does it, but I am pretty certain it does not do this. I also remember that Jack's channel(before it got removed) uninstalled a few av's if they had the silent uninstall option.

Like I said, I think I found a new (possibly not new, but new to me) method.

I'll analyse how BetaBot does it (I've got a bin) and update this thread.

tux1 - September 23, 2014, 9:16 am

Pretty interesting, thanks for sharing.