

Forum: [Hack Forums](#)

Thread: [Process Persistence like AntiVirus Process](#)

aerohacker - November 18, 2019, 10:28 am

What Crypter has a Process Persistence feature same as those used by AntiVirus, making the AV process "impossible" to kill/terminate and/or suspend a RAT's process using any Process Manager Tool like Windows Task Manager, Process System, Process Monitor and/or Process Hacker (Even with Administrator privileges) or any BotKill.

"Unable to terminate process.exe (PID XXX). Access is denied."

Some Process Persistence that hooks in Kernel Mode Driver.

If a AntiVirus can use this technique so a Crypter can or could use too, right?!

realsunjester - November 18, 2019, 10:39 am

"Unable to terminate process.exe (PID XXX). Access is denied."

usually mean you don't have high enough privileges to kill the process (not admin). have you tried killing it from the command line using the force switch? I bet it works. If not you could more than likely boot into safe mode and remove reg entries and startup options for the app and kill it then.

Maybe you want something like API hooking? <https://github.com/nybble04/Shady-Hook>

start checking open source a/v's,
<https://github.com/clamwin/clamav-win32/blob/0.101/src/dllmain/dllmain.c>

Cyber Coder - November 18, 2019, 3:07 pm

is funny how you make the same threads every few months but never get a satisfying answer
insanity : doing the same thing over and over again expecting s.hit to change

SIM-3132187 - November 18, 2019, 3:15 pm

Make a privilege escalation exploit to run your payload at NT-AUTHORITY/system. And you will be able to have a good persistence lol.

Dotexe - November 18, 2019, 3:23 pm

(Nov 18, 2019 04:07 PM)Cyber Coder Wrote: [\[CITE\]](#) is funny how you make the same threads every few months but never get a satisfying answer
insanity : doing the same thing over and over again expecting s.hit to change
Exactly my thoughts

Xamarin - November 18, 2019, 3:35 pm

(Nov 18, 2019 11:28 AM)aerohacker Wrote: [\[CITE\]](#) What Crypter has a Process Persistence feature same as those used by AntiVirus, making the AV process "impossible" to kill/terminate and/or suspend a RAT's process using any Process Manager Tool like Windows Task Manager, Process System, Process Monitor and/or Process Hacker (Even with Administrator privileges) or any BotKill.

"Unable to terminate process.exe (PID XXX). Access is denied."

Some Process Persistence that hooks in Kernel Mode Driver.

If a AntiVirus can use this technique so a Crypter can or could uses too, right?!

Yes you could. Anti-viruses use kernel mode drivers to hook all terminate process requests (and many more), and they deny/modify all of them that have to do with the antivirus processes and come from the user.

Now, of course you can buy a signature for your driver (which is mandatory to spread it), but the problem is that it costs a lot of \$\$ and it will be flagged in a few days at best - not to mention that you need to make it through Microsoft's approval process.

Of course, there is the option of using a driver exploit in order to map your driver that way, but many of these vulnerable drivers work up to a specific Windows version, and many of these exploits due to their instability tend to end up on a nice BSOD quite a few times.

In short: It isn't worth it, because the problems from such a technique heavily out-weight the benefits.

(Nov 18, 2019 04:07 PM)Cyber Coder Wrote: [\[CITE\]](#) is funny how you make the same threads every few months but never get a satisfying answer

insanity : doing the same thing over and over again expecting s.hit to change

This is one way to see it. Another one is that he is persistent enough to get an answer, which depending on the case it's not a bad skill to have ?

raghavsood999 - November 20, 2019, 2:53 pm

Hey does your crypter - able to hide the process, hide msconfig keys, tray icon, install file - path, folder and file?

aidan liang - November 21, 2019, 2:33 pm

Hello anyone has time here? Can lead me througth this website super confusing

lo0sr - November 26, 2019, 10:47 am

I think what you are looking for is a Rootkit. Those have features like making your files undeletable, hiding files and processes, etc. Crypters normally are for not being detected, rootkits offer the persistance.