

Forum:[Hack Forums](#)

Thread: [My Crypter, detected file in temp.](#)

autisticilab - December 27, 2017, 1:47 pm

First of all, I apologize for my bad English.

This is my problem:

I created my own Crypter and Stub in C #. The encrypted file is Timescan. When I start the Server file. It is not detected by Antivirus. but its counterpart created in Temp is detected. the file in Temp is removed and quarantined. instead the execution file is not touched by the antivirus. but by blocking the file in Temp, the Rat is not executed.

how can I solve this problem? Thank you

gigajew - December 27, 2017, 2:37 pm

The temporary folder is more than likely one of the #1 monitored folders by anti-virus solutions

autisticilab - December 27, 2017, 2:43 pm

how can I make the file created in Temp clean? through Runpe?

gigajew - December 27, 2017, 4:01 pm

(Dec 27, 2017 03:43 PM)autisticilab Wrote: [\[CITE\]](#) how can I make the file created in Temp clean? through Runpe?

Not necessarily, most anti-virus solutions are capable of scanning the detected file in memory

cicko - January 3, 2018, 2:10 am

try putting it in recycle bin

Electron - January 4, 2018, 8:59 am

(Dec 27, 2017 03:43 PM)autisticilab Wrote: [\[CITE\]](#) how can I make the file created in Temp clean? through Runpe?

I've seen only MalwareBytes detecting files put in directories by their names. Make sure the name doesn't look suspicious. If you are sure it's not that, it means that your file is detected or you could try Application Data.

(Jan 3, 2018 03:10 AM)cicko Wrote: [\[CITE\]](#) try putting it in recycle bin
? ? ?

gigajew - January 6, 2018, 6:32 am

I'm positive almost all of the antiviruses have a filewatch system with like high priority folders such as appdata and temp

kevy42 - January 6, 2018, 12:21 pm

(Jan 6, 2018 07:32 AM)gigajew Wrote: [\[CITE\]](#) I'm positive almost all of the antiviruses have a filewatch system with like high priority folders such as appdata and temp
i never had probs with Appdata, idk about temp though

Redrum - January 6, 2018, 11:38 pm

Sounds like it's only a scantime crypted TBH, you need a runtime one

Tsukiri - January 8, 2018, 8:11 am

OP's crypt probably just decrypts the malware and then writes it to a file in TEMP, resulting in a non-crypted file

being dropped. Ofcourse any AV will register this and directly remove them at runtime, even if its not flagged at scantime.

If you want to bypass runtime protection, you will have to find a way to load your code into the memory without dropping to disc. There are many ways to do it, including the RunPE like you mentioned (even though those standard ways get detected aswell nowadays so you will probably have to toy around with different techniques before you find something that will bypass most majors).

Basically, a RunPE allocates memory in an existing process (lets say svchost.exe for now). It will then copy the code to the allocated memory in the thread of the other process and afterwards start the thread, causing the code inside the thread to execute and thus running your (malicious) code from another process.

kirkkoz - January 10, 2018, 2:06 pm

(Jan 6, 2018 01:21 PM)WeedmasterOG Wrote: [\[CITE\]](#) i never had probs with Appdata, idk about temp though

AppData gets detected all the time in my experience. I use folders such as MyVideos or MyMusic all day ?

inyourmemory - January 11, 2018, 7:03 am

It's not recommended to drop files to disk, instead run them from memory

kevy42 - January 12, 2018, 7:34 am

(Jan 10, 2018 03:06 PM)kirkkoz Wrote: [\[CITE\]](#) AppData gets detected all the time in my experience. I use folders such as MyVideos or MyMusic all day ?
weird, i use random and it bypasses just fine

Ninja - January 12, 2018, 9:34 am

(Jan 11, 2018 08:03 AM)Win64Worm Wrote: [\[CITE\]](#) It's not recommended to drop files to disk, instead run them from memory
This.

Here is some more info:

<https://stackoverflow.com/questions/5797205/how-to-load-an-exe-as-a-net-assembly>