

Forum:[Hack Forums](#)

Thread: [Where does malware hide on infected computers?](#)

Dex37 - March 8, 2025, 12:21 pm

Hi everyone,

Malware is just another file on a computer, and it needs a place to hide and store itself. Some common places are %appdata%, %temp%, Local, Roaming, etc.

But are there other, less commonly used locations that are also suitable for malware storage?

Actually, the path where the malware is stored on a system is important for its success, or it can be stored anywhere as long as it is somewhat hidden?

And is a good practice store the malware on shell:startup so it runs every time the user turns on the computer?

DramaKing - March 8, 2025, 12:46 pm

Technically, malware can hide pretty much anywhere, though the type of malware may matter, like DLLs. Just don't specify the path to the Startup folder as shell:startup.

Novo - March 8, 2025, 10:55 pm

Many places, DLLs, Scheduled Tasks, Registry Keys, Filesystem, the question is, where can it not hide?

Tha Sneak - March 9, 2025, 1:21 am

I feel like this question has more of a blackhat sense to it than a whitehat sense, but this is a HackForum. I'm not gonna tell you every single registry key malware can hide, but I'll give you some if you're more specific.

JosProud - March 14, 2025, 9:08 am

The answer to where malware can hide is in those locations where the user running it has write permissions.

You can get a quick view of these locations using AccessChk from Sysinternals.

Idea: What if we block execution in these directories with AppLocker?

SpiffyGraffiti - April 12, 2025, 3:39 pm

some malware like to hide in the startup folder. Always check for hidden folders. The startup folder will make the malware run when the computer is started.

Good luck removing the malware.

Viskow - May 14, 2025, 2:54 am

It can be hidden anywhere, but especially in files that you won't necessarily think to look at.

Phantom-Phreak - May 15, 2025, 6:53 pm

Whenever I am manually checking for malware I usually just look for places that would help with it's persistence. Some areas I would check: Auto Run Registry subkeys for both machine and user keys, and services set to automatic, task manager automatic tasks, etc.