

Forum:[Hack Forums](#)

Thread: [What kind of malware can survive a full clean install of windows?](#)

SIM-5022267 - October 3, 2023, 11:04 am

A full clean install of windows and PC should remove all malwares? Not to mention reformatting the drives completely.

In the case where someone who has done this multiple times, and yet continues to get infected. What are possibilities?

There were no downloading of anything malicious, no clicking on strange links, no response to suspicious emails or texts.

Also in the case of a bios virus, it's been flashed and updated many times.

BiNBo - October 3, 2023, 11:17 am

Could be a number of things, the malware could be embedded into the firmware. When embedded into the firmware of hardware components, even BIOS flashing and updates might not completely remove the malware. It's also possible that it's being reinfected from external sources such as network or other external devices that are infected. It's also slim but possible chance that the installation media has been compromised. More advanced malware can exploit vulnerabilities or leave backdoors that allow persistence even after a clean install.

SIM-5022267 - October 3, 2023, 11:26 am

(Oct 3, 2023 11:17 AM)BiNBo Wrote: [\[CITE\]](#) Could be a number of things, the malware could be embedded into the firmware. When embedded into the firmware of hardware components, even BIOS flashing and updates might not completely remove the malware. It's also possible that it's being reinfected from external sources such as network or other external devices that are infected. It's also slim but possible chance that the installation media has been compromised. More advanced malware can exploit vulnerabilities or leave backdoors that allow persistence even after a clean install.

In this case, is it best to just get a brand new system and network?

webdev77 - October 3, 2023, 11:32 am

(Oct 3, 2023 11:26 AM)randomness528432 Wrote: [\[CITE\]](#) In this case, is it best to just get a brand new system and network?

What other option do you have at that point besides living with questionable hardware?

aerohacker - October 4, 2023, 9:21 pm

(Oct 3, 2023 11:04 AM)randomness528432 Wrote: [\[CITE\]](#) A full clean install of windows and PC should remove all malwares? Not to mention reformatting the drives completely.

In the case where someone who has done this multiple times, and yet continues to get infected. What are possibilities?

There were no downloading of anything malicious, no clicking on strange links, no response to suspicious emails or texts.

Also in the case of a bios virus, it's been flashed and updated many times.

There are a number of possibilities for this...

1 - What kind of strange behavior the computer is doing to make you think that you are infected?

2 - If even after formatting the HD/SSD, the Operating System still infected with some Malware, then it can be installed through:

- BIOS/UEFI
- HD/SSD (Some Malware that install in a "secret area", survive and reinstall)
- Modem/Router
- CD/DVD/BD or USB Stick with infected or modified ISO

3 - Are you using some crack or keygen to activate Windows, Office and/or another paid software?!

DramaKing - *October 6, 2023, 8:50 am*

It's not impossible to have a rootkit in hard drive firmware (the secret area), which wouldn't be affected by a reformat and clean install. Ignore the modem/router possibility above. Do you know what the malware is?