

Forum:[Hack Forums](#)

Thread: [When resetting Windows to remove malware, do not use the built-in tool.](#)

Novo - January 28, 2025, 2:45 pm

PLEASE READ THIS FOR YOUR OWN SECURITY!

The Windows Reset Wizard is a tool that can be modified by malware, making it unsafe to rely on for removing malware.

Instead, follow these steps to ensure a clean and secure recovery:

1. Download a verified ISO file directly from the official Microsoft website.
2. Flash the ISO onto a USB drive using a trusted tool like Rufus.
3. Boot from the USB and use it to begin the Windows installation process.
4. During installation, fully remove the old system by deleting all existing partitions. This ensures no traces of malware or compromised files remain.

^^^

STEPS 1-2 ARE DONE ON A SEPERATE MACHINE!!!

Hackers - January 28, 2025, 2:47 pm

This is good information that is probably either overlooked, forgotten, or disregarded by many.

Nice post

Secrets - January 28, 2025, 4:40 pm

Easy to do, and one would think difficult to forget but happens. Thanks for the refreshing reminder. Will help those in need.

Tha Sneak - January 28, 2025, 6:09 pm

I'm actually working on a solution to this in the form of a tool used in malware removal for scanning and fixes. I've done an extensive amount of research and have located key locations malware persists through resets, booting, and full formats. A majority of it is malware modifying registry entries relating to the boot process, reset process, and etc. adding or changing the executable with the malicious one in order to persist.

However, there is a very small percentage of malware that can and will exploit these so the likelihood of losing all of your files because of malware is very slim since 99% of all infections can be cleaned and those that cannot are named infections and well known to the malware removal community. One of said infections that is nearly impossible to clean is a file replication virus named Virut. It adds its malicious payload onto files including system files and causes some to be corrupted.

ttbr0 - January 28, 2025, 9:37 pm

do you have any evidence to suggest that malware tampers with removal software? i would be very interested to know if any exist and their history. if you are going to this extent to clean your infected machine, perhaps you may as well remove the disk that hosts the infected os and reformat it on the other machine because you can make the argument that malware can execute during the boot sequence, then hope that it hasnt infected the firmware in your drive. but all of this is incredibly

unlikely since 99% of malware arent made by developers who have this level of skill or care. personally i think reformatting disks to clean malware is overkill.

Novo - January 28, 2025, 10:57 pm

(Jan 28, 2025 10:37 PM)ttbr0 Wrote: [CITE](#) do you have any evidence to suggest that malware tampers with removal software? i would be very interested to know if any exist and their history. if you are going to this extent to clean your infected machine, perhaps you may as well remove the disk that hosts the infected os and reformat it on the other machine because you can make the argument that malware can execute during the boot sequence, then hope that it hasnt infected the firmware in your drive. but all of this is incredibly unlikely since 99% of malware arent made by developers who have this level of skill or care. personally i think reformatting disks to clean malware is overkill.

You don't need 'evidence' to justify taking security precautions when threats like LoJax, a known UEFI rootkit, already exist.

LoJax proves that malware can persist beyond a simple disk format by infecting the firmware itself, requiring a BIOS reflash to remove.

Yes, I know that the method I gave won't remove LoJax, but the fact that malware as advanced as a UEFI rootkit exists is proof that less sophisticated malware that can tamper with removal tools or survive reinstalls in other ways-also exist.

Dismissing this as 'unlikely' and an excuse to lower security is bad practice.