

Forum:[Hack Forums](#)

Thread: [Virus that remains after format](#)

Account of the Gods - August 5, 2016, 6:24 am

What you think about it? Is it possible? By format i mean hard one from boot level

Ive once had a virus that remained after system upgrade, but thats other story
would it be possible for a virus to hide somewhere else as we remove all partitions?

something like, invisible partition (maybe possibly with unusable file format of partition for windows?) or other way?

Wafflemonger - August 5, 2016, 6:36 am

It would technically be possible, but the odds of you encountering something like that just in the wild is slim to none. Those types of attacks are generally only used in targeted attacks, since they're usually using zero-day exploits. If those exploits were to become common place, they'd more than likely be patched quite quickly (think Java ...).

However, the UEFI BIOS' generally have a pretty big handle on these sorts of attacks. They cannot be written to from within the OS and can barely be written to outside of the OS. Upgrading the BIOS (flashing it, whatever) is very difficult to do if you don't have the manufacturer's verified coding signature.

EDIT: Added in "flashing" BIOS xD.

Tawts - August 5, 2016, 8:26 am

Heard a couple months ago of people placing viruses in hard drive firmware, so technically it is possible but unless you're a very high priority target it would be unlikely.

Zach_Farlow - August 5, 2016, 8:33 am

if that's possible then i think its time to trash my pc and buy a new one every 2-3 months.

Tawts - August 5, 2016, 8:44 am

(Aug 5, 2016 08:33 AM)Zach_Farlow Wrote: [\[CITE\]](#) if that's possible then i think its time to trash my pc and buy a new one every 2-3 months.

Kaspersky released a report on the Equation group early last year where they talked about it, I'd post the link but I can't since I'm fairly new to this website. I can PM it if you'd like but its easily searchable in google.

Batidas - August 5, 2016, 8:45 am

it is true, can be done but at the moment it is not a reason to be worried about.

<https://blog.kaspersky.com/equation-hdd-malware/7623/>

Code So, the practical outcome of the story is – HDD-infecting malware is not a legend anymore, but the average individual isn't at risk. Don't slam your drives with a hammer, unless you work in Iran's nuclear industry. Pay more attention to less exciting, but more probable, risks like being hacked because of bad passwords or an outdated antivirus.

