Open in app ↗

Sign up   Sign in

Medium   Search   ✎ Write   👤

Using UEFI to inject executable files into BitLocker protected drives

Grzegorz Tworek · Follow

✕

Medium

Sign up to discover human stories that deepen your understanding of the world.

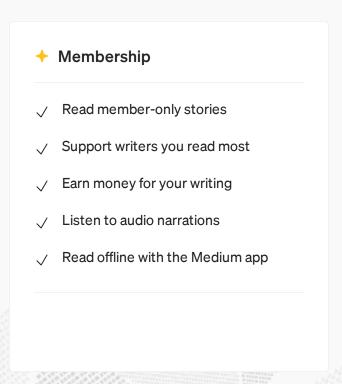| Free	Membership
✓ Distraction-free reading. No ads.	✓ Read member-only stories
✓ Organize your knowledge with lists and highlights.	✓ Support writers you read most
✓ Tell your story. Find your audience.	✓ Earn money for your writing
	✓ Listen to audio narrations
	✓ Read offline with the Medium app
Sign up for free	**Try for 5 $/month**

Having the landscape described, we can quickly realize that injecting a file into encrypted partition looks like the bad guys Holy Grail. After we launch it with high privileges (a challenge on its own), we can disarm some protections, create new admins, transfer the disk content over Internet etc. Of course, it should be not allowed if we want to keep the computer protected. Injecting a file into disk is impossible before booting due to encryption and after the boot, when encryption is transparent, the OS does not allow us to drop the file into sensitive locations allowing an execution with high privileges. Problem solved.

Medium

Sign up to discover human stories that deepen your understanding of the world.

Free

✓ Distraction-free reading. No ads.

✓ Organize your knowledge with lists and highlights.

✓ Tell your story. Find your audience.

✦ Membership

✓ Read member-only stories

✓ Support writers you read most

✓ Earn money for your writing

✓ Listen to audio narrations

✓ Read offline with the Medium app

Etc.

One of the steps to be performed relies on a NtQuerySystemInformation() function (depreciated by Microsoft) with a 0x85 as a parameter. This parameter is not documented but according to the information provided within PDB symbol files, it may be interpreted as SystemPlatformBinaryInformation. NtQuerySystemInformation() scans UEFI tables stored within hardware memory looking for a piece of data with properly constructed headers. If such pattern ("WPBT", length, revision and a checksum) is found, the structure is passed to the smss.exe. And here the

Medium

Sign up to discover human stories that deepen your understanding of the world.

can do, but at the same time, it means that the bar keeping bad guys off the encrypted drive is hung significantly lower than we used to think.

I'd suggest that it is the high time check if %systemroot%\system32\wpbbin.exe exists in your system.

And a second later you can create your own file (empty one is good enough) and mark it read only. Smss.exe can overwrite an existing file, but does not check or reset such simple thing as the R attribute.

Medium

Sign up to discover human stories that deepen your understanding of the world.

Free

✓ Distraction-free reading. No ads.

✓ Organize your knowledge with lists and highlights.

✓ Tell your story. Find your audience.

✦ Membership

✓ Read member-only stories

✓ Support writers you read most

✓ Earn money for your writing

✓ Listen to audio narrations

✓ Read offline with the Medium app