



Using UEFI to inject executable files into BitLocker protected drives



Grzegorz Tworek · Follow

3 min read · Sep 9, 2019



To keep important things clear: BitLocker is a Windows-based full volume encryption solution. It encrypts every single sector of the volume, acting on the lowest possible layer — encrypting the data just before being written to the hardware and decrypting freshly it immediately after reading. BitLocker is considered relatively secure (including [FIPS certification](#)) and one of the main purposes is to protect data “at rest”, when the Operating System cannot guard it. In practice it means, BitLocker is totally transparent for computer users, but if you try to play the data offline (mounting the disk drive to another machine, booting from USB stick etc.) — you realize everything is encrypted. The beauty of the solution is highly related to a method how BitLocker manages encryption keys, but we will not cover it here as totally irrelevant to the main topic. Just to wrap it up: when the OS is running it protects unauthorized users from manipulating critical data, and when the OS is not working — the data is encrypted an you cannot manipulate it too.



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.

Sign up for free

★ 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

Try for 5 \$/month

- Initializing OS parameters such as safe boot etc.

- To make Medium work, we log user data. By using Medium, you agree to our [Privacy Policy](#), including cookie policy.

- Performing file operations postponed till reboot

- Logging drivers if enabled

- Initializing data related to Known Dlls

- Initializing pagefile(s)

Etc.

One of the steps to be performed relies on a NtQuerySystemInformation() function (deprecated 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 magic begins.

- Smss.exe stores the piece of UEFI memory within a file called *wpbbin.exe*.
- Smss.exe takes execution parameters (command line) from the same UEFI block.
- The wpbbin.exe is checked for integrity with IMAGE_DLLCHARACTERISTICS_FORCE_INTEGRITY.
- The wnbhin.exe is executed

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

Good luck!

To make Medium work, we log user data. By using Medium, you agree to our [Privacy Policy](#), including cookie policy.

Security

Uefi

Bitlocker

Hacking

Windows 10



Written by Grzegorz Tworek

Follow



64 Followers

More from Grzegorz Tworek



Grzegorz Tworek



Grzegorz Tworek

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

To make Medium work, we log user data. By using Medium, you agree to our [Privacy Policy](#), including cookie policy.

See all from Grzegorz Tworek


Recommended from Medium

 Alexander Nguyen in Level Up Coding

The resume that got a software engineer a \$300,000 job at Google.

1-page. Well-formatted.

 Jun 1  25K  483 

 Jonathan Mondaut

How ChatGPT Turned Me into a Hacker

Discover how ChatGPT helped me become a hacker, from gathering resources to tackling...

 Jun 18  1.6K  53 

Lists

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

To make Medium work, we log user data. By using Medium, you agree to our [Privacy Policy](#), including cookie policy.

 Austin Starks in DataDrivenInvestor

I used OpenAI’s o1 model to develop a trading strategy. It is...

It literally took one try. I was shocked.

★ Sep 15  5.3K  138



 kuldeep singh

10 Linux Commands Every Software Engineer Should Master...

Mastering Linux is like having a superpower. Whether you’re debugging, developing, or...

Oct 24  11



 Andrew Zuo

Async Await Is The Worst Thing To Happen To Programming

I recently saw this meme about async and await.

★ Jun 22  3.8K  216



 F. Perry Wilson, MD MSCE 

How Old Is Your Body? Stand On One Leg and Find Out

According to new research, the time you can stand on one leg is the best marker of...

★ Oct 23  6.4K  148



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