Why doesn't the BitLocker wizard let me save the BitLocker key on an encrypted drive?

devblogs.microsoft.com/oldnewthing/20221220-00

December 20, 2022

Raymond Chen

When the BitLocker Drive Encryption wizard steps you through the process of applying BitLocker full volume encryption to a drive, one of the steps is backing up your recovery key. There are a number of options, one of which is to save the key to a file.

If you try to save that file to an encrypted drive, you are told, "Your recovery key cannot be saved to an encrypted drive." Why is that not allowed?

Saving your recovery key on an encrypted drive is the equivalent of locking your keys in the car. In order to get the recovery key, you would have to decrypt the drive, but decrypting the drive requires the recovery key!

The BitLocker wizard could in theory let you save the key to an encrypted drive that is unrelated to the drive being encrypted. For example, saving the system volume's recovery key on a data volume is a bad idea (because you need to boot the system volume before you can get to the data volume). But saving the recovery key for a data volume to the system volume could be allowed since you can boot the system volume first, and then use the recovery key to access the data volume.

But for simplicity, the BitLocker Drive Encryption wizard doesn't try to detect these scenarios. For your own safety, it simply refuses to save the recovery key to *any* encrypted volume.

Furthermore, the BitLocker Drive Encryption wizard won't save the recovery key to an unencrypted fixed drive. That would be the equivalent of leaving your keys on the hood of the car. If you computer is stolen, the bad guys can just look on the unencrypted drive and find your recovery key, and use that to access the encrypted volumes.

You can save your recovery key to a cloud service (such as your Active Directory account), to a removable drive, or to a network location. Somewhere that is *not* on the computer being encrypted.

A security vulnerability report came in that said that they could trick the BitLocker Drive Encryption wizard into saving the recovery key to a local drive by sharing a local drive over the network and then `net use` 'ing that network share via loopback. This tricks the BitLocker Drive Encryption wizard into thinking that it's saving the recovery key to another computer on the network, thereby circumventing the enforcement that the recovery key not be saved on an encrypted volume. The finder then requested a bounty payment.

First of all, the BitLocker Drive Encryption wizard requires administrator privileges, so this is an attack against the local machine coming from a user who already has administrator privileges, which is not interesting since there is no elevation of privilege.

Let's look at the usual questions when evaluating a security vulnerability report. Who is the attacker? The attacker is the person who bypasses the BitLocker Drive Encryption wizard's protections and saves the recovery key to an encrypted volume. Who is the victim? The victim is presumably the person who has now lost their recovery keys. But the attacker and the victim is the same person! The attacker has gained the ability to lock himself out of his own computer.

Now, you can circumvent the block in the BitLocker Drive Encryption wizard much more easily by just saving the recovery key to a removable drive, and then copying the file to an encrypted drive. *Ooh, the recovery key is on an encrypted drive!*

Or you can just use the `Enable-BitLocker` PowerShell cmdlet to enable BitLocker and tell it to put the recovery key on the encrypted volume. The PowerShell cmdlet doesn't care.

Returning to the "locking the keys in the car" analogy: Say you have a fancy car that detects that the key is inside the car when you try to lock the door, and it beeps at you to remind you that you left the key in the car. All of these mechanisms to circumvent the Bitlocker Drive Encryption wizard are like taking the key and wrapping it in tin foil so the car sensor can't see that the key is inside the car. "Using this trick, I am able to lock my keys inside my car. I have found a vulnerability in the don't-lock-your-keys-in-the-car feature!"

Congratulations, you locked your keys in your car.

Not allowing you to save the recovery key on an encrypted volume is not a security feature. It's a "Prevent you from making stupid mistakes" feature. When the wizard says "Your recovery key cannot be saved to an encrypted volume," it's not saying that saving the key to an encrypted volume is somehow illegal or invalid. It's saying "Saving the recovery key to an encrypted volume is such a bad idea that I'm going to stop you if I notice that you're trying to do it."

But if you want to wrap your key in tin foil and do lock your keys in your car, then you are welcome to do so. I hope you're happy now.

Raymond Chen

Follow