ELCOMSOFT
PROACTIVE SOFTWARE

A case of an accidentally encrypted photo library

Sometimes the prospect of loosing valuable data makes inexperienced users hasty about the necessity of taking precautionary measures. Loosing data access can also happen because of awkward data handling or accidental data encryption, and this is the case of our attention.

Problem

Nick Buick, a Web developer from Refreshweb, is a real creative mind whose clients cannot but thank him and recommend his services to others. He produces and stores collections of artworks not only at work, but also at home. Not so long ago he got into trouble, to be precise, he and his partner, who almost lost all photo archives they collected during their life together. *"My partner's Windows corrupted a few days ago, It wasn't until after I'd slaved her HDD, deleted both the System and Windows folders and done a fresh windows install that I discovered she'd somehow managed to encrypt her entire photo library before the crash with no record of the keys in sight... I thought we'd lost EVERYTHING! The last 3 years of our lives, engagement photos, our trip around the world, etc..."*

A seemingly sad situation was worsened by the lack of any backups of the data. *"Wedding photos, trips around the world, buying our first home, thousands of images of our life over the last decade with no other backups,"* - reproached Nick himself. Yet again, we have a situation which demonstrates it's really worth making backups in time, especially if you do not store your photo-, video- or whatever- archives on a separate hard drive.

Not knowing all tricks of encrypting using EFS, originally meant and designed to help rather than trouble, often ends up in big problems with data decrypting after system upgrade or reinstallation. *"In reinstalling Windows, the encryption key was lost and the drive was no longer readable..."* The situation has already become a commonplace experience for all users previously living in a computer security vacuum; it's like a good old school of trial and error.

Solution

Good news is that after reinstalling Windows or even disk formatting the EFS certificates are still there in your computer and can be retrieved with help of either computer security experts or special tools, like Advanced EFS Data Recovery.

Nick scanned several forums but they all unanimously recommended Best practices for the Encrypting File System article in Microsoft Knowledge Base. In its turn it recommends, first, creating recovery agent for the encrypted files (an additional certificate for recovery "in case of necessity"), and, second, making certificate backups. Naturally, both recommendations should be implemented in advance, when everything works, otherwise they are useless as in Nick's case.

"*…After a series of panic attacks we came across your [ElcomSoft] software, the trial indicated we could retrieve the data, and we were more than happy to pay the small license fee for the software which then recovered all the data in a matter of hours."* Nick realized there wasn't anything to be done without expert skills or dedicated software. So, he searched the Web and decided to resort to Advanced EFS Data Recovery. He purchased a product license, got a registration key and executed a couple of operations with the software. "*I just ran your program and within a couple of hours it had restored EVERY single file. I have no idea how it did this, but it worked.*"

Actually, AEFSDR works very simply and efficiently. If the encryption certificates has been deleted (e.g. the disk has been reformatted, and/or operating system has been reinstalled), there is a good chance that they're still there - of course, if they have not been overwritten by other data. An unique AESDR approach is: it scans the whole hard disk at the low level, sector-by sector (including ones marked as 'free'), and try to locate the keys by 'patterns'. That way, the keys can be found even in the most hard situations - and so it becomes possible to decrypt the files. And yes, AEFSDR can also find deleted EFS-encrypted files, so there is no need to use any 3rd party undelete software.

Conclusion

Unwise or unconscious data encryption can eat your time and money and the moral is that making timely backups (or at least storing valuable data on a separate storage device) is vital for your nerves and good mood. However, sometimes overcoming troubles gives you a second wind: *"Thank goodness Microsoft make such lousy encryption software, and you make such good unencryption software"*, said Nick after all his worries about encrypted family photo library had vanished.

These are all quirks of fate, still ElcomSoft team is always happy to hear *"You guys have an incredible product!"*