ELCOMSOFT
PROACTIVE SOFTWARE

Don't let EFS trick you: Tips on recovering EFS-encrypted data when it gets lost.

The Encrypting File System (EFS) was first introduced in Windows 2000 and, as Microsoft claims, is an excellent encryption system with no back door.

However, the most secure encryption can be ambiguous. It would efficiently prevent hackers and other illegal intruders from breaking into your system and getting access to your well-encrypted data. The other side of the coin is that both a regular user and a seasoned administrator can lose important data due to unforeseen circumstances. It is also the case with EFS.

Problem

Neil Strom from Oklahoma, US, encountered the loss of EFS-encrypted data. "My original situation was that I had some problems with Windows consistently crashing all of the sudden. So, I tried several things to fix it, and none of them seemed to work. I decided that I should probably reformat the entire computer and then reinstall Windows," explains Neil. Before reinstalling the system he went through the process of trying to backup files, including documents, pictures, schoolwork files (such as PDFs, programming files, etc.), resumes, Microsoft Outlook email and calendar backups (.pst files), etc., and put them on an external hard drive. Neil goes on explaining his situation: "Many of the files were unencrypted, but many of them were encrypted with the Microsoft Encrypting File System (where files turn green when they are encrypted). Unfortunately, I failed to remember to decrypt them before I reformatted, which denied me access to them because of the nature of the encryption system and the loss of a user profile. After backing up the files, I went through the process of reformatting and trying to re-install Windows. However, after I did that, when I tried to open, or even move, the encrypted files, it told me that access was denied. I realized that I needed to figure out a way to gain back access."

Loss of EFS-encrypted data is a common problem with regular users. The EFS documentation issued by Microsoft is often difficult for them to understand. It is also true that only a few read full instructions before starting to work.

Following the complex descriptions of the algorithm, that can be misleading or even incomprehensible for a regular user, Microsoft states on its website "If the private key is damaged or missing, even the user that encrypted the file *cannot decrypt* it. If a recovery agent exists, then the file *may be* recoverable. If key archival has been implemented, then the key may be recovered, and the file decrypted. If not, the file *may be lost*. EFS is an excellent file encryption system—there is no "back door." Overloaded with such kind of information, a regular user can, figuratively saying, get brain freeze easily.

Moreover, EFS-encrypted files can pose a problem even for seasoned administrators. The trick here is that the system itself is stored on one disk, whereas encrypted files on another. After having reinstalled the operating system, the administrator to his surprise receives "Access Denied" message. A backup of just the disk with the data was made, but the encryption keys are gone for good, together with the disk not backed-up, on which the system was stored.

Neil Strom says: "As far as I know, Microsoft does not provide a way to gain back the files, and really little warning was given about the danger of this encryption process when I first used it (although Microsoft provides warnings about reformatting). It had crossed my mind to try to change my username and password back to my original username and password. However, this did not seem to work."

System reinstallation, as in Neil's case, is only one of the scenarios of losing access to EFS-encrypted data. Imagine you have deleted the user profile. Although the files and the encryption keys are still on the disk, the system is not able to see them any longer. Creating a profile with the same user name would not solve the problem. The system assigns a different ID to the account and this newly-created ID is used in the encryption process. The EFS-encrypted data can be lost if the user password was reset or the user migrated to a different domain, as well as due to damaged boot sector, corrupted system files or another operating system failure.

Besides trying to reset his username and password to the original ones, Mr. Strom attempted to get his data back in several other ways. "I also tried several other things, including trying to change the system administrator's

password, searching the computer for exported Microsoft certificates, using the Microsoft Virtual PC profiles that I had used previously to access the files, searching online on Microsoft's support website to find a solution, and calling Dell (the manufacturer of my computer). However, nothing seemed to work," explains Neil.

Solution

Neil browsed the Internet for software capable of recovering EFS-encrypted data. After trying some recovery programs that yielded no results, he finally came across Advanced EFS Data Recovery.

Advanced EFS Data Recovery allows one to decrypt files even if the user database is protected with SYSKEY. First, AEFSDR searches for all EFS keys, scanning the hard drive sector by sector. After the user has entered the user password into the program, the software decrypts the keys, or at least one key, needed for decryption of user's encrypted data. On the second stage AEFSDR looks for EFS-encrypted files in the file system and attempts to recover them. The recovery rate is usually very high, 99% or more.

Neil explains how he managed to save his data: "I finally stumbled upon the Elcomsoft software, and when I installed it and searched for the files using its searching feature, it seemed to find most all the files I needed. Also, when I searched for the decryption keys, it actually found many keys on the hard drive that were thankfully not written over by the reformatting process (since it gradually writes over the hard drive as it needs to, but leaves whatever it doesn't need there, although not accessible except with certain software such as Elcomsoft provides)."

Results

Some of the files still did not work. According to Mr. Strom, their rate was less than 1%, "perhaps a hundred out of approximately 20,000 or so [files]". The encrypted files that could be decrypted turned green in the software window. Neil concludes, "I was then able to choose where to move the files, and the program automatically decrypted them and moved them to that folder."