

microsoft.public.windowsxp.security_admin: Re: Encrypted files -- would this work to get them back?

Re: Encrypted files -- would this work to get them back?

Source:

http://www.derkeiler.com/Newsgroups/microsoft.public.windowsxp.security_admin/2002-11/18900.html

From: Karl Levinson [x y] mvp (levinson_k@excite.com)

Date: 11/21/02

From: "Karl Levinson [x y] mvp" <levinson_k@excite.com>

Date: Wed, 20 Nov 2002 23:02:53 -0500

I'm guessing it's there because you use the public key to encrypt your files. It's called Public, but that doesn't mean it's necessarily for the public. It does however mean that it's not sensitive information, and that its "capture" by someone wanting to crack the file is not a worry, because it is not very useful in cracking the encryption.

I'm not aware of any way to retrieve the private keys once Windows will not boot up. Believe me, many before you have asked and asked and asked this, and no one here has ever given a positive response that resulted in the files being cracked.

You could read <http://securityadmin.info/faq.htm#efs> in case you haven't already, and in case there's something there you haven't already thought of. [I'm thinking of the section about trying to use forensic tools to retrieve unencrypted copies of the files from the unused space on your hard drive.]

<lostfiles@screwed.com> wrote in message

news:k9cotu88csmj6ib5hb642ieed4ngdn781t@4ax.com...

> *If it were a Public Key, then why would it only appear in MY Keys*

> *folder within Application Data?*

>

> *In the MMC, look at the "Local Computer" certificates. If any given*

> *certificate were public, shouldn't it appear there instead of in the*

> *"User Account"? If it's in the User Account, to me, that sounds like*

> *a private key. Just as you thought, I'm not 100% sure.*

>

> *Can anyone tell me where exactly the "Private Key" is located on the*

> *hard drive? I still might be able to recover it if it's still there.*

>

> *thanks*

>

>

>

> *On Wed, 20 Nov 2002 16:14:46 -0500, "Karl Levinson [x y] mvp"*

Re: Encrypted files -- would this work to get them back?

microsoft.public.windowsxp.security_admin: Re: Encrypted files -- would this work to get them back?

> <levinson_k@excite.com> wrote:

>

> >Sorry, I don't think so. I'm not 100% sure, but that message sounds like

> >that is a public key. You need the private key to decrypt, which it seems

> >is stored elsewhere. In Public Key encryption, the public key is available

> >to everyone and can only be used to encrypt a file, not decrypt it. If you

> >could easily use a public key to decrypt a file or get the private key, just

> >about all the internet banking web sites and other public key encryption in

> >use today wouldn't protect a thing.

> >

> >

> ><lostfiles@screwed.com> wrote in message

> >news:k0nntus1ogegat1he8snkl8tuk4a0a6r94@4ax.com...

> >> Windows version: XP Pro SP1

> >>

> >> Ok, call me an idiot because like so many other people in here I had

> >> to reformat and forgot about my encrypted folder until it was too

> >> late. I was able to restore my old certificate and key but I'm stuck

> >> and not sure what else to do.

> >>

> >> After the format and new install of XP, I ran a recovery utility on my

> >> C drive and was able to recover ALL the files and folders in the

> >> following directory:

> >>

> >> "C:\Documents and Settings\<username>\Application Data\Microsoft"

> >>

> >> If you notice, there is a Crypto folder and a "System Certificates"

> >> folder in there and the files contained within them were recovered

> >> without errors. Including the system certificate and the key.

> >>

> >> Note: I only had ONE certificate and key before the format. This was

> >> my first reload of XP pro since it's release date, so those are the

> >> correct files. The new Crypto and certificates folders/subfolders

> >> were blank.

> >>

> >> I checked the Certificates snap-in with the MMC on my new install of

> >> XP Pro and there were none listed. The Crypto, Certificates and Keys

> >> folders on my hard drive were empty, so I copied all the files within

> >> the recovered folders to the appropriate places. Now when I open the

> >> Certificates Snap-in, the certificate is listed. It has the

> >> following properties:

> >>

> >> "Enable all purposes for this certificate"

> >> "Encrypting file system" box is checked

> >>

> >> Before copying the recovered files, when I would try to get the

Re: Encrypted files -- would this work to get them back?

microsoft.public.windowsxp.security_admin: Re: Encrypted files -- would this work to get them back?

> > > *encryption details on one of my encrypted files, the user list was*
> > > *blank. Now when I right-click on one of my encrypted files and go to*
> > > *Properties, Advanced, Details, it shows my user name and a certificate*
> > > *thumbprint. If I click the Add button, the "Select User" box pops up*
> > > *and I am able to view the certificate. It has the following*
> > > *properties:*
> > >
> > > **GENERAL TAB**
> > > *"This certificate is intended for the following purposes"*
> > > *Allows data on disk to be encrypted.*
> > > *All issuance policies.*
> > >
> > > *Issued to: username*
> > > *Issued by: username*
> > >
> > > *Valid from: 11/19/2002*
> > > *Valid to: 10/26/2102*
> > >
> > > *"You have a prIvate key that corresponds to this certificate"*
> > >
> > > **DETAILS TAB:**
> > > *Too much info to type.*
> > >
> > > **CERTIFICATION PATH TAB**
> > > *Certification Path: It shows the certificate name*
> > > *Certification status: "This certificate is OK"*
> > >
> > >
> > > *So since I have the old certificate/key and they are in the right*
> > > *places, why can't I open one of the encrypted files? My user name,*
> > > *login password and computer name are all the same as they were before*
> > > *the reload.*
> > >
> > > *The permissions for the encrypted folder are set to "Full Controll*
> > > *(this folder, subfolders and files)". I was able to take ownership of*
> > > *the folders/files and I do have administrator rights.*
> > >
> > > *Is there anything else I can do with the recovered certficate/key that*
> > > *might work? Any other ideas?*
> >
>

Re: Encrypted files -- would this work to get them back?