

Re: a forensic question

Source: <http://www.derkeiler.com/Newsgroups/comp.security.misc/2003-02/0388.html>

From: Peter L (peter.m.lynch.SpamWedge@blueyonder.co.uk)

Date: 02/22/03

From: "Peter L" <peter.m.lynch.SpamWedge@blueyonder.co.uk>

Date: Sat, 22 Feb 2003 17:51:21 -0000

Why not undelete the files (with freeware or commercial tools) then start keeping files on a fileserver, with proper security!

Peter

"Karl Levinson [x y] mvp" <levinson_k@despammed.com> wrote in message news:esSrjgn2CHA.2296@TK2MSFTNGP10.phx.gbl...

> Also, you have to ask yourself whether it is likely that someone deleted
> those files. Are they important? Would anyone gain anything by deleting
> them? Would someone with malicious intent be more likely to copy the
files

> or do something else to cause more damage? IMHO, usually file deletions
> like this turn out to be user error, though without auditing logs all
you've

> got is guesses [and the information to make changes to prevent this from
> happening next time].

>

> "Steven L Umbach" <n9rou@attbi.com> wrote in message

> news:sQC5a.196004\$tq4.5077@sccrnsc01...

>> Hi Doug. If the computer had file and print sharing enabled on it then

>> someone who had administrator privileges could have deleted files

> remotely,

>> but if auditing was not enabled it will be impossible to find out who it

>> was. Did the computer have a floppy drive and if so was it bootable from

> it

>> or perhaps the cmos was not password protected? The files may have been

>> deleted from a bootable floppy and that would leave no trace. -- Steve

>>

>> "Doug Fox" <dfox168@hotmail.com> wrote in message

>> news:xUB5a.36937\$UXa.28377@news02.bloor.is.net.cable.rogers.com...

>>> A user swore that she had powered down her NT 4.0 workstation before

> going

>>> home. But she discovered that some important files on her workstation

>> were

>>> deleted this morning.

>>>

>>> Checked:

comp.security.misc: Re: a forensic question

> > >
> > > *The Event Viewer / Security Log, there was no entry as auditing was not enabled.*
> > > *The Event Viewer / System Log, the PC was powered down at 5:15 pm yesterday and a DHCP request this morning. There was no activity in between these two entries.*
> > > *The Recycle Bin was empty.*
> > >
> > > *Also checked file://winnt/profiles directory. There was no unrecognizable username.*
> > >
> > > *Where else I can check for un-authorized access to this workstation? Could it be "remote control" by a user with administrative privilege? For instance, net use file://computername/c\$. How can I find it out?*
From
> *the security log of the PDC?*
> > >
> > > *Are there tools which help in-depth investigations?*
> > >
> > > *Any pointers are appreciated.*
> > >
> > > *Thanks,*
> > >
> > >
> > >
> >
> >
>
>
> ----
> *Outgoing mail is certified Virus Free.*
> *Checked by AVG anti-virus system (<http://www.grisoft.com>).*
> *Version: 6.0.449 / Virus Database: 251 – Release Date: 1/27/2003*
>
>