

Re: Can't delete folders in ftproot

Source:

<http://www.tech-archive.net/Archive/Internet-Server/microsoft.public.inetserver.iis.ftp/2004-05/0203.html>

From: Bernard (qbernard_at_hotmail.com.discuss)

Date: 05/20/04

Date: Thu, 20 May 2004 12:28:29 +0800

I like this part –

- > *While those are great suggestions, remember that these files were uploaded*
- > *and created using FTP – it should always be possible to delete them the*
- > *same*
- > *way. Log on using your favourite FTP client, and then delete the files*

Now, from this log

```
01:43:53 XX.XXX.24.186 [31]MKD /+/L?x/ftp3++++/+ 257
```

```
01:43:54 XX.XXX.24.186 [31]MKD /+/L?x/ftp3++++/nul1++++/+ 257
```

```
01:43:54 XX.XXX.24.186 [31]MKD /+/L?x/ftp3++++/nul1++++/ftp1++++++/+
```

So we know that the 'bad' folders are created.
what will the remove command looks like ?

--

Regards,

Bernard Cheah

<http://www.tryiis.com/>

<http://support.microsoft.com/>

<http://www.msmvps.com/bernard/>

"Alun Jones [MS MVP - Security]" <alun@taxis.invalid> wrote in message
news:I5Kqc.1973\$Fz1.1050@newssvr23.news.prodigy.com...

> In article <uB58WKXPEHA.1160@TK2MSFTNGP09.phx.gbl>, "Bernard"

> <qbernard@hotmail.com.discuss> wrote:

> >You have been tagged!

>

> While it's a cute term for what's being done, it is a nasty thing for
> someone to do to your system. It's usually done to prevent you from
> deleting the files, so that the hacker can carry on exchanging files -
> usually stolen software, pirated movies, and pornography - with his
> associates.

>

> This is a natural result of allowing anonymous users the right to upload
> _and_ download from the same area. I recommend creating a separate
account

> for your users to upload data to the server, and prevent downloads from
the

> upload directory; move files from the upload area to the download area
> manually, rather than through FTP.

>

> >a) disable anonymous access

>

> Not strictly necessary to completely disable it - but if you don't need

microsoft.public.inetserver.iis.ftp: Re: Can't delete folders in ftproot

it,
> absolutely, disable it.
>
> >b) configure strong NTFS permissions
>
> This is a must - anonymous users must not have upload and download
rights
> to the same space.
>
> >c) read <http://securityadmin.info/faq.htm#ftpfolder>
> >d) use the following kb(s) to remove files
>
> While those are great suggestions, remember that these files were uploaded
> and created using FTP - it should always be possible to delete them the
same
> way. Log on using your favourite FTP client, and then delete the files.
>
> >e) do a virus scan to see if any backdoor program installed
> >f) last resort, format partition or rebuilt entire machine.
>
> If you can afford to, make your public-facing servers "ephemeral" - so
that
> you can easily wipe them and restore them with whatever data you need to
> provide.
>
> A 'tagging' incident doesn't generally mean that you've allowed a hacker
to
> install software, or make any code run, so it's significantly less likely
> that you'll need to reformat and rebuild - but your server storage and
your
> bandwidth are no longer yours to control. Definitely do a virus check.
> Also, see if you can track down the hacker's IP address, and make a report
> to his ISP. Include IP address and time information.
>
> Strictly speaking, the hacker probably hasn't even broken any laws, since
> you did provide guest access. If you haven't included a message to the
> effect that the guest access is limited to certain purposes, there's
> probably no criminal action you could take - and even then, too many FTP
> clients don't display the greeting message to users, so a hacker could
even
> make the defence that you don't adequately publish policies. But it's
worth
> reporting them to the ISP, because that may be all the ISP needs to
> terminate their Internet access (or at the very least, start keeping
better
> tabs on this user, considering that future legal action might come).
>
> Alun.
> ~~~~
>
> [Please don't email posters, if a Usenet response is appropriate.]
> --
> Texas Imperial Software | Find us at <http://www.wftpd.com> or email
> 1602 Harvest Moon Place | alun@taxis.com.
> Cedar Park TX 78613-1419 | WFTPD, WFTPD Pro are Windows FTP servers.
> Fax/Voice +1(512)258-9858 | Try our NEW client software, WFTPD Explorer.