

# Re: %temp% Mystery

---

*Source:*

<http://www.tech-archive.net/Archive/WinXP/microsoft.public.windowsxp.general/2006-09/msg03235.html>

---

- *From:* "Wesley Vogel" <[123WVogel955@xxxxxxxxxxxx](mailto:123WVogel955@xxxxxxxxxxxx)>
  - *Date:* Sat, 9 Sep 2006 19:55:12 -0600
- 

I understand some of it, not all of it. ;-)

I forgot to mention in my previous post that malware likes to hide crap in  
%systemroot%\system32\config\systemprofile

Make sure that you're malware free.

ZoneAlarm has a file, always in C:\WINDOWS\Temp\ called ZLT07742.TMP

I do not pay attention to it, so the file name may change, it always startw  
with ZL though.

—

Hope this helps. Let us know.

Wes  
MS-MVP Windows Shell/User

In [news:ui19IxFIGHA.2196@xxxxxxxxxxxxxxxxxxxxxxxxxxxx](mailto:news:ui19IxFIGHA.2196@xxxxxxxxxxxxxxxxxxxxxxxxxxxx),  
antioch <[antioch@xxxxxxxx](mailto:antioch@xxxxxxxx)> hunted and pecked:

Reply intertwined/spliced

"Wesley Vogel" <[123WVogel955@xxxxxxxxxxxx](mailto:123WVogel955@xxxxxxxxxxxx)> wrote in message  
[news:On0Va6E1GHA.4108@xxxxxxxxxxxxxxxxxxxxxxxxxxxx](mailto:news:On0Va6E1GHA.4108@xxxxxxxxxxxxxxxxxxxxxxxxxxxx)

Hi Antioch,

some info in the below link that I have found & still find  
confusing.  
<http://windowsxp.mvps.org/cleantemp.htm>

Go to that page and click on Send your feedback, at the top, in the blue  
box, type your questions in the Comments box. Maybe Ramesh will get back  
to

Re: %temp% Mystery

you.

Yes – thanks for that – I will see if I can leave a message for him.  
I will have to think very clearly about what I will say – I take note of what he says in the groups so I must be careful that anything I say does not offend.  
Wesley – what are you trying to do to me – have you forgotten 'You cant educate pork'  
Are you thinking 'out loud' – perhaps you wish to absolutely kill my poor brain with all this tech stuff – and kill this thread as well :-> :->  
Be fair – if YOU don't get it how will I?  
It took me six months or a bit more, to realise there are 2 main temp folders into which stuff is placed on a daily basis.  
There are those who have posted that I did not know what I was talking about – and there more switched–on than me with a far better knowledge of Windows than me. Well they don't post against me anymore when temp comes up in a thread.  
One pompous ass said they delete automatically every seven days.  
I wish I had not mentioned these others now – there are a couple more but my mouth is sealed :->  
Believe me I am most grateful for your attention in this thread.  
Please forgive my lack of knowledge – I hate to admit that it is wasted on me though – but I can tell it has caused you a degree of interest, judging by all the work you have put into the below.  
No doubt there will be others who will find your work of interest as well – hope so.  
I have just switched on – 1 file in %temp% – but I am not being smug about it or complacent – Windows can kick you in the ass with no warning.  
Please, I beg you, no more – I promise not to do another thread like this again – honest ;->  
Rgds  
Antioch

I do not understand all of this.

%systemroot%\system32\config\systemprofile is used by the system, the Local System account.

All the profiles on a machine are listed in...  
HKEY\_LOCAL\_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\ProfileList

%systemroot%\system32\config\systemprofile is SID S-1-5-18.

Security identifiers (SIDs) are numeric values that identify a user or group.

Re: %temp% Mystery

S-1-5-18 is an identity that is used locally by the operating system and by services configured to log on as LocalSystem. A service account that is used by the operating system.

SID: S-1-5-18

Name: Local System

LocalSystem account

Description: A service account that is used by the operating system.

HKEY\_LOCAL\_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\ProfileList\S-1-5-18

Value Name: ProfileImagePath

Data Type: REG\_EXPAND\_SZ

Value Data: %systemroot%\system32\config\systemprofile

<quote>

System Profile

In Windows 2000, when an application or service used the LoadUserProfile API

to load a user profile for a process running as the local system, Windows created a profile named %computename%\$, where %computename% is the

name of the local computer. This could cause problems for some applications and services, because depending on whether the system profile was loaded, HKEY\_CURRENT\_USER could in fact resolve to different

registries either HKEY\_USERS\S-1-5-18 or HKEY\_USERS\DEFAULT depending

on whether another component has loaded the SYSTEM profile.

To avoid this, Windows XP creates a new profile for the system, located in %systemroot%\System32\Config\SystemProfile. This profile is always loaded, and is a link to HKEY\_USERS\DEFAULT. This ensures that system components always have a consistent profile and registry.

<quote>

from...

User Data and Settings Management

<http://www.microsoft.com/technet/prodtechnol/winxpro/maintain/xpusrdat.mspx>

<quote>

Local File System When a certificate or CRL is retrieved via LDAP or HTTP by a Windows 2000 client with MS04-11, Windows XP SP2 client, or Windows Server 2003 client, it is cached by CAPI in the Application Data folder. The per-user cache location is C:\Documents and Settings\{user name}\Application Data\Microsoft\CryptnetUrlCache and the per-machine cache

location is %WINDIR%\System32\config\SystemProfile\Application

Re: %temp% Mystery

Data\Microsoft\CryptnetUrlCache .  
<quote>

<http://www.microsoft.com/technet/prodtechnol/winxpro/support/tshtcr1.mspx>

S-1-5-21-some long number is probably Your SID.

S-1-5-21-some long number that ends with -500 is the built in Administrator account.

\* SID: S-1-5-18  
Name: Local System  
LocalSystem account  
Description: A service account that is used by the operating system.  
%systemroot%\system32\config\systemprofile

\* SID: S-1-5-19  
Name: NT Authority  
LocalService account  
Description: Local Service  
It is used to run local services that do not require LocalSystem account.  
%SystemDrive%\Documents and Settings\LocalService

\* SID: S-1-5-20  
Name: NT Authority  
NetworkService account  
Description: Network Service  
S-1-5-20 refers to NetworkService account. It is used to run network services that do not require LocalSystem account.  
%SystemDrive%\Documents and Settings\NetworkService

\* SID: S-1-5-domain-500  
Name: Administrator  
Description: A user account for the system administrator. By default, it is the only user account that is given full control over the system.  
%SystemDrive%\Documents and Settings\Administrator

—  
Hope this helps. Let us know.

Wes  
MS-MVP Windows Shell/User

In [news:%23niPrqA1GHA.4228@xxxxxxxxxxxxxxxxxxxxxxxxxxxx](mailto:news:%23niPrqA1GHA.4228@xxxxxxxxxxxxxxxxxxxxxxxxxxxx),  
antioch <antioch@xxxxxxx> hunted and pecked:

Re: %temp% Mystery

Re: %temp% Mystery

Hi Wesley

Thank you for your reply, but I still have the first advice(similar to

the

below)which you gave to be nearly two years ago. :-) :-)

I know, thanks to you and Malke, all the ins and outs re temp folder/files

etc.

I decided long ago to do a manual delete rather than have yet another

prog

on the system.

My main reason for the thread was that the norm for the last two years

of having to do a manual delete, has for no apparent reason, decided to

go auto.

The other temp in Windows still behaves as it always has.

There are two other temps which never seem to get anything in them.

They are also Windows – phealth\helpctr & system32\config.

I just thought it worth a mention and wondered if you 'switched-on' guys

and girls could come up with an explanation.

Last night, before switching off, there were 8 entries.

This morning there are two, dated and timed at switch-on.

I was hoping that Ramesh might have spotted this thread because there is

some info in the below link that I have found & still find confusing.

<http://windowsxp.mvps.org/cleantemp.htm>

Rgds

Antioch

"Wesley Vogel" <123WVogel955@xxxxxxxxxxxx> wrote in message

[news:ejzXfC80GHA.772@xxxxxxxxxxxxxxxxxxxxxxxxxxxx](mailto:news:ejzXfC80GHA.772@xxxxxxxxxxxxxxxxxxxxxxxxxxxx)

All kinds of applications leave tmp files. If you use MS Word it leaves all kinds. So does about every program you open.

I just now opened one Word doc, copied one line and it left two folders in %tmp%.

## Re: %temp% Mystery

Description of how Word creates temporary files

<http://support.microsoft.com/default.aspx?scid=kb:en-us:211632>

temp typed into the Run command should open C:\WINDOWS\Temp

%tmp% or %temp% typed into the Run command should open %userprofile%\Local Settings\Temp

Check 'em once in while and clean them out manually, some apps do not clean up after themselves.

Disk Cleanup (cleanmgr.exe) leaves file younger than 7 days old.

\* Temporary files  
[[ Programs sometimes store temporary information in a Temp folder. Before a program quits, the program usually deletes this information. You can safely delete temporary files that have not been modified in over a week.]]

Safely delete access time stored here (7 is days):

HKEY\_LOCAL\_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\Volume Caches \Temporary Files

Value Name: LastAccess

Data Type: REG\_DWORD

Value Data: 7

You can change the value to 1 (day) instead of 7 (days).

Or use...

Disk Cleaner

<http://www.robortenfemke.nl/~diskclean/>

EasyCleaner

<http://personal.inet.fi/business/toniarts/ecleaner.htm>

Empty Temp Folders



Re: %temp% Mystery

accessed via Start/Run etc.

<http://windowsxp.mvps.org/cleantemp.htm>

Most who found they had this full folder, had assumed that Disk

Cleanup deleted them when it was run but found that it was a

different Temp that Disk Cleanup cleaned, that is C:\Windows\temp.

Last weekend, I went to do the deletion only to find that there were

just 2 items there instead of the normal 200 or 300 I

would have expected.

I have monitored this %temp% now for the past 5 days and there has as

yet never been more than 2 items each time I have switched on the

computer. Good news – yes – but when one sees that what was the norm

is no longer so, it does make one think – what happened – how did this

come to pass? I have added no software or other prog in the last 5–6

weeks.

So what has caused this – have others found the same to be happening?

Was there something in the last Black Tuesday updates/security/critical

patches/fixes that I didn't spot.

They are the only additions to my computer in the time frame.

If anyone has a solution/cause I would like to hear it.

Rgds

Re: %temp% Mystery

Antioch