TECHNICAL FEATURE 3

eXPect the uneXPected

Andreas Marx, AV-Test.org, Germany and
Costin Raiu, Kaspersky Labs, Romania

Long gone are the days when *Windows 3.11* was the latest and the greatest OS version from *Microsoft*, or when *Microsoft*'s flagship servers were running *Linux*. Nowadays, if you care to 'fingerprint' them with a tool such as 'Queso' or 'nmap', you'll see that most will be running some flavour of *Windows*, probably *2000*.

I say probably, because it's hard to determine exactly which *Windows* version a system is running based only on the replies of its TCP/IP stack. However, I have no doubt that a lot of them may be running the newly released *XP* version as well, as there's no doubt that some servers carrying *Microsoft*'s name might still be running some version of *Linux*.

New Kid on the Block

But it is obvious that, as time passes, more and more systems connected to the Internet will be running *Windows XP*, especially after the 'traditional' six-month transition period is over.

The fact is that, as for any new operating system which brings a host of new features and connectivity options, it is highly likely that *Windows XP* also carries a certain number of bugs, some already known, and some unknown.

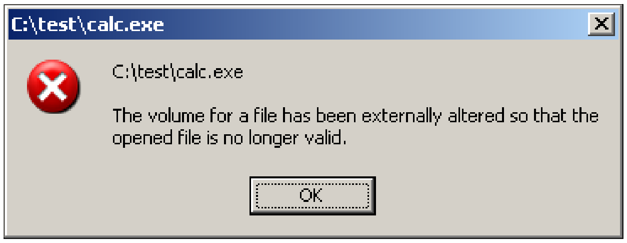
Since the release of *Windows XP*, we have come by a set of problems of which the most important are described in this article. Some of these have been fixed by *Microsoft* already, while others remain unfixed since they are more or less regarded as 'features' of the OS version, or that they work this way 'by design'.

We intend this article to be a useful reference for IT staff or system administrators who have to deal with *XP* systems in their networks, or for the casual *XP* user whose computer is running, according to a *Microsoft* quote, 'the most secure *Windows* version ever'.

1. Manifest Files

The phenomenon of the '.manifest' extension may not be widely known amongst new users of *XP*.

If you create an empty file named with the same name as an existing executable on your disk followed by the '.manifest' extension (for example, 'notepad.exe.manifest') and then save the file in the same directory as the respective program, then *Windows XP* will steadfastly refuse to execute the program anymore.



C:\test\calc.exe

C:\test\calc.exe

The volume for a file has been externally altered so that the opened file is no longer valid.

As can be seen above, on attempting to execute the file, a more than cryptic message appears: 'The volume for a file has been externally altered so that the opened file is no longer vaild.'

If you attempt to start the respective program from the command prompt, a more or less generic message of the same form appears, which says: 'The system cannot execute the specified program.'

Curious things, '.manifest' files are new additions to *Windows XP* – their main purpose is to allow developers to specify the so-called 'shared assemblies' between modules and applications.

Unfortunately, the problem is that in order to render a system unusable, one does not need to have the right to change important system files – the permission to add an innocent empty '.manifest' file into the right place is more than enough.

Moreover, '.manifest' files are supposed to be located in a special sub-folder of the *Windows XP* installation directory. So, for example, there should be no legitimate reason for one to exist in the 'system32' directory.

Such a problem is likely to be very hard to diagnose, especially given that no existing file has been modified, and no change has been made to the registry. That's why you may want to look for zero-byte-sized '.manifest' files if you ever happen to encounter one of the messages listed above.

2. Universal Plug'n'Play

By default, on the TCP port 5000 and UDP port 1900 of *Windows XP* systems there is a service listening for connections called the 'SSDP Discovery Service'.

Basically, this service provides an interface between the network and the 'Universal Plug and Play Device Host', the service taking care of Plug'n'Play devices. The main purpose here is, of course, to allow your computer to discover and use automatically any Plug'n'Play devices connected to the network (such as 'smart' printers, or remotely controllable microwave ovens).

On 20 December 2001, *eEye Digital Security* released an advisory which covers three major bugs in the Universal

Plug'n'Play (UPnP) implementation included in *Windows XP*. These three bugs allow a remote attacker to launch a DoS attack against the respective system, to use the system to make connections to other arbitrary addresses on the Internet and, worst of all, to execute code on the system with higher privileges.

Microsoft's response can be found in the MS01-059 Security Bulletin (see http://www.microsoft.com/security/bulletin/MS01-059.asp), in the form of a 585 KB executable that replaces a number of system files, amongst them 'ssdpapi.dll' and 'ssdpsrv.dll'. This package takes care of the vulnerability and protects the affected systems against the three types of attack.

Given that it took the author of CodeRed about one month to write the worm after a public exploit for the respective vulnerability was released, we wonder how long will it be before we see a similar thing exploiting the *XP* UPnP hole.

And unfortunately, not only will such a thing have a much larger target base than CodeRed (we expect the number of *Windows XP* systems on the Internet to outrank the number of *Windows 2000* systems running IIS), but also it should be more compatible than CodeRed and, technically, be able to spread much faster.

3. Outlook Express 6.0 and the German Version

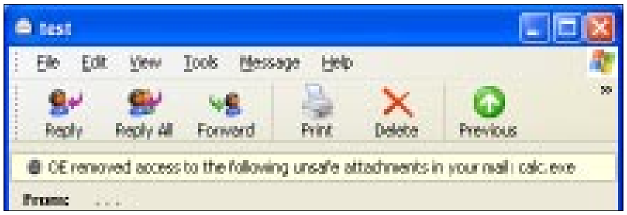
Installed and configured by default into *Windows XP*, *Outlook Express 6.0* and *Internet Explorer 6.0* have the task of acting as 'email', 'news', 'Web' and 'ftp' access clients.

Of these, it is interesting to note that *Outlook Express 6.0* includes some basic 'virus-protection' options which can prevent the user from accessing attachments with a certain set of extensions belonging to executable or script files, such as .VBS, .EXE or .BAT.

This is intended as some form of simple protection against email viruses, and despite the fact that it greatly reduces the usability of the product, it might actually prove useful in some cases.

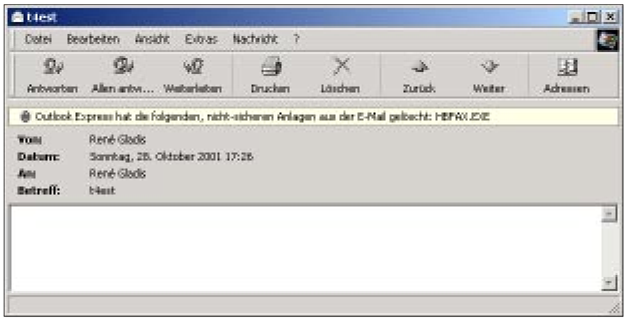
Whenever the user receives an attachment in the form of a file with one of these extensions, *Outlook* will display the 'status' message: 'OE removed access to the following unsafe attachments in your mail: filename.extension'

However, it seems that the team that translated *OE6.0* into German, made a little mistake, so instead of 'removed access' the German version of *OE6.0* says it has 'deleted' the attachments.



OE removed access to the following unsafe attachments in your mail: calc.exe

From: ...



Outlook Express hat die folgenden, nicht-sicheren Anlagen aus der E-Mail gelöscht: HBFAX.EXE

Von: René Gladis
Datum: Sonntag, 28. Oktober 2001 17:26
An: René Gladis
Betreff: t4est

So, quite understandably, an unsuspecting user might imagine that the attachment had actually been deleted from the message. Thus a false sense of security is created.

First of all, the problem is that the attachment has not been deleted. If the *OE6.0* security option is disabled, the attachment can be accessed again without problems.

Secondly, the attachment could very well have been something useful to the receiver – a legitimate file that the user was expecting and wanted to receive. This way he/she may be tricked into believing that the attached file has been lost.

And finally, if the attachment was indeed infected with a virus, imagine the surprise of the user who is certain that the attachment has been 'deleted' from his mails, while an anti-virus product able to scan the *OE6* mailbox reports the virus still to be present in the message.

Of course, a proper fix would be required in this case, which translates to the right meaning in the German *Outlook Express 6.0*, but until then, users should be aware of this fact.

4. The Windows XP Personal Firewall

Of the many security features *Windows XP* can provide, of great interest, especially to home users who connect their systems to the Internet through a dial-up, cable or DSL link, is *XP*'s embedded Personal Firewall (PF).

Once activated, the *Windows XP* Personal Firewall does a very simple, yet very effective thing – it will prevent remote machines from initiating connections towards the protected system on a large array of TCP/IP ports, thus greatly reducing the possibility of external attacks.

Of course, the Personal Firewall can be explicitly permitted to allow certain ports to pass the lock, which is very useful if someone wants, for example, to run an ftp server.

The only problem with the Personal Firewall is that, under various circumstances, it will open a server port automatically for connections from the outside. In doing so this allows remote access to the machine virtually from anywhere on the Internet, without even notifying the user.

This problem occurs when someone has the Personal Firewall running, and tries to activate the *XP* Remote

Desktop Server. During this process, *XP* will add the Remote Desktop port to the 'allowed' server ports automatically, and silently give remote parties the ability to initiate a Remote Desktop session with the machine.

Of course, to initiate the Remote Desktop session, one would also require a valid username and passport. However the fact remains that the first step has been made, and along with it, a door has been opened into the security defences of the machine, without any warning at all to the unsuspecting user.

Microsoft was notified of this problem in November 2001, and the issue was said to be under investigation, maybe scheduled for fixing in the future.

One other thing we should mention is that this effect could not be reproduced on all of our test configurations. It did not occur on an English test installation of *XP*, but initially it was found and reproduced on the German MSDN *Windows XP Home* and *Pro* versions.

Some Conclusions

The recommendations to practise caution with *Windows XP* are posted virtually everywhere on the Internet. That's why we are not going to add any fuel to the topic.

On the contrary, all of the problems we have mentioned in this article can be avoided through very simple means, and an informed user should have no problems (provided the translation issues in the German *Outlook Express 6.0* are dealt with).

So, if you want to take advantage of all the new features in *Windows XP*, just go ahead.

But wait! When you install *Windows XP* don't forget at least to take care of the UPnP problem by installing the patch or disabling the SSDP service.

If you have a firewall, we recommend that you close the TCP port 5000 and the UDP port 1900 – there's absolutely no reason why someone from the Internet should connect a Plug'n'Play device into your network.

Also, especially if you use an isolated computer, it would be better to install a separate, more configurable personal firewall with more features than *XP*'s built-in implementation which is designed to provide only a very basic line of security. There are many very good personal firewall applications available on the Internet, many of which are free, and most of which are reported to work without any problems on *XP*, even if *XP*'s built-in personal firewall is running as well.

And finally, if you notice any of the strange error messages indicated in the '.manifest' section of this article, you may want to take a look for any such files in the system or *Windows* directories since, most likely, they have no legitimate reason to be in there.