Microsoft's Really Hidden Files: A New Look At Forensics. (v2.5b)

By The Riddler

October 14, 2001 (v2.0 finished May 16, 2001; v1.0 finished June 11, 2000)

Written with Windows 9x in mind, but not limited to.

DISCLAIMER:

I will not be liable for any damage or lost information, whether due to reader's error, or any other reason.

SUMMARY:

There are folders on your computer that Microsoft has tried hard to keep secret. Within these folders you will find two major things: Microsoft Internet Explorer has been logging all of the sites you have ever visited -- even after you've cleared your history, and Microsoft's Outlook Express has been logging all of your e-mail correspondence -- even after you've erased them from your Deleted Items bin. (This also includes all incoming and outgoing file attachments.) And believe me, that's not even the half of it.

When I say these files are hidden well, I really mean it. If you don't have any knowledge of DOS then don't plan on finding these files on your own. I say this because these files/folders won't be displayed in Windows Explorer at all -- only DOS. (Even after you have enabled Windows Explorer to "view all files.") And to top it off, the only way to find them in DOS is if you knew the exact location of them. Basically, what I'm saying is if you didn't know the files existed then the chances of you running across them is slim to slimmer.

It's interesting to note that Microsoft does not explain this behavior adequately at all. Just try searching on microsoft.com.

FORWARD:

I know there are some people out there that are already aware of some of the things I mention. I also know that most people are not. The purpose of this tutorial is teach people what is really going on with Microsoft's products and how to take control of their privacy again. This tutorial was written by me, so if you see a mistake somewhere then it is my mistake, and I apologize.

Thanks for reading.

INDEX:

Coming Soon:

ù pstores.exe
ù Related Windows Tricks.
ù The NSA-Key.
ù Researching the [Microsoft Update] button.
ù Why the temp folders aren't intended to be temporary at all.
ù What's with Outlook Express's .dbx database files?
ù Win2k support.

1. DEFINITIONS AND ACRONYMS

Well, the best definition I have been able to come up with is the following:

I) A "really hidden" file/folder is one that cannot be seen in Windows Explorer after enabling it to "view all files," and cannot be seen in MS-DOS after receiving a proper directory listing from root.

  a) There is at least one loophole to enabling Windows Explorer to see them.
  B) There is at least one loophole to enabling MS-DOS to see them.

(Interesting to note that the "Find: Files or Folders" utility cannot even search through one of these folders. It doesn't even exist on the [Browse] menu.)

II) Distinguishes "really hidden" file/folders from just plain +h[idden] ones, such as your "MSDOS.SYS" or "Sysbckup" folder.

III) Distinguishes from certain "other" intended hidden files, such as a file with a name with high ascii characters (eg, "?ëï¨?").

DOS = Disk Operating System
MSIE = Microsoft Internet Explorer
TIF = Temporary Internet Files (folder)
HD = Hard Drive
OS = Operating System

2. WHY SHOULD I ERASE THESE FILES?

Just from one of these files I would be able to tell you which web sites you previously visited, what types of things you search for in search engines, and probably gather your ethnicity, religion, and sexual preference. Needless to

say, one can build quite a profile on you from these files. It has the potential to expose and humiliate -- putting your marriage, friendship, and corporation at risk. Here's one good example of the forensic capabilities...

"I've been reading your article as I have a problem with an employee of mine. He has been using the works pc for the internet and using it to chat and look at porn sites. He was then deleting the cookies and history in order to cover his tracks. A friend of mine pointed me in the direction of this site and your article. I have found it to be incredibly useful,..."

--Concerned Boss, 8/24/01

---

3. HOW TO ERASE THE FILES ASAP

Step by step information on how to erase these files as soon as possible. This section is recommended for the non-savvy. Further explanation can be found in Section 4.0. Please note that following these next steps will erase all your cache files and cookies files. If you use the offline content feature with MSIE, it will remove this as well. It will not erase your bookmarks.

3.1. IF YOU OWN A COPY OF MICROSOFT INTERNET EXPLORER

1) Shut your computer down, and turn it back on.
2) While your computer is booting keep pressing the [F8] key until you are given an option screen.
3) Choose "Command Prompt Only" This will take you to real DOS mode. ME users must use a bootdisk to get into real DOS mode.
4) When your computer is done booting, you will have a C:\> followed by a blinking cursor. Type in this hitting enter after each line (sans parenthesis):

C:\WINDOWS\SMARTDRV (Loads smartdrive to speed things up.)
CD\
DELTREE/Y TEMP (this line removes temporary files.)
CD WINDOWS
DELTREE/Y COOKIES (This line removes cookies.)
DELTREE/Y TEMP (This removes temporary files.)
DELTREE/Y HISTORY (This line removes your browsing history.)
DELTREE/Y TEMPOR~1

(If this last line doesn't work then type this:)

CD\WINDOWS\APPLIC~1
DELTREE/Y TEMPOR~1

(If this doesn't work then type this:)

CD\WINDOWS\LOCALS~1
DELTREE/Y TEMPOR~1

(If this still does not work, and you are sure you are using MSIE5.x, then please e-mail me. Finding the location of these may be difficult and I'd certainly like to know where else MSIE likes to hide its cache. I believe older versions of MSIE keep them under "\windows\content\".)

This last one will take a ridiculous amount of time to process. The reason it takes so incredibly long is because there is a ton of semi-useless cache stored on your HD.

3.2. CLEARING YOUR REGISTRY

It was once believed that the registry is the central database of Windows that stores and maintains the OS configuration information. Well, this is wrong. Apparently it also maintains a bunch of other doo-dah that has absolutely nothing to do with the configuration. I won't get into the other stuff, but for one, your Typed URLs are stored in the registry.

HKEY_USERS/Default/Software/Microsoft/Internet Explorer/TypedURLs/
HKEY_CURRENT_USER/Software/Microsoft/Internet Explorer/TypedURLs/

These "Typed URLs" come from MSIE's autocomplete feature. It records all URLs that you've typed in manually in order to save you some time filling out the address field. By typing "ama" the autocomplete feature might bring up "amazon.com" for you. Although, I find it annoying, some people prefer this feature. One thing is for sure, however -- it's an obvious privacy risk. You wouldn't want a guest to type "ama" and have it autocomplete "amateremudwrestlers.com" now would you?

You can clear your Typed URLs out of your registry by doing going to Tools > Internet Options > Content > [AutoComplete] > and finally [Clear Forms] under MSIE. If you do not like the AutoComplete feature then uncheck the appropriate boxes here.

3.3. IF YOU HAVE OUTLOOK OR OUTLOOK EXPRESS INSTALLED

Microsoft's e-mail clients DO NOT delete your messages until a) you really know how, and B) you go through the redundant process. And besides this, there's the glaring e-mail virus problems (in which virtually all other e-mail client's are immune to.) This, alone, should be enough to want to strangle Slick Willy -- as I like to call him.

My suggestion?

1) Install another e-mail program like Eudora or Pegasus Mail. Make sure everything is setup correctly. (www.eudora.com / www.pmail.com)
2) Backup any e-mail and address books that you wish to save by making use of the export/import features.
3) Uninstall Outlook.

Warning: Simply uninstalling Outlook does not erase any of your e-mail correspondence. The database files are still there on your hard drive. To find them open up a DOS window and type this:

dir *.mbx /s/p
The files you are looking for are:

INBOX.MBX
OUTBOX.MBX
SENTIT~1.MBX
DELETE~1.MBX
DRAFTS.MBX

If these files come up they should be listed in either of these folders:

C:\Windows\Application Data\Microsoft\Outlook Express\Mail\
C:\Program Files\internet mail and news\%USER%\mail\

Now type either of the following (depending on the location of your .mbx files...)

*Remember, this will erase all your e-mail correspondence so backup what you want to keep. By now you should have already imported your mail into Eudora, or Pegasus Mail.

CD\WINDOWS\APPLIC~1\MICROS~1\OUTLOO~1
DELTREE/Y MAIL

or

CD\PROGRA~1\INTERN~1\%USER%

(replace "%user%" with the proper name.)

DELTREE/Y MAIL

If you have newer versions of Outlook or Outlook Express the databases are *.dbx, or *.pst files. Five times as creepy as the *.mbx files. I recommend that you take a look at them yourself.)

3.4. SLACK FILES

As you may already know, deleting files only deletes the references to them. They are in fact still sitting there on your HD and can still be recovered by a very motivated person.

ù BCWipe is a nice program that will clear these files. (www.bcwipe.com).
ù For you DOS buffs, there's a freeware file wiper on simtel.net that I use. (www.simtel.net/pub/dl/45631.shtml).
ù If you are using PGP then there is a "Freespace Wipe" option under PGPtools.
ù The latest version of Norton Utilities has a nice filewiping utility.
ù You might want to check out Evidence Eliminator's 30 day trial. This is probably the best program as far as your privacy goes.

(www.evidence-eliminator.com)

3.5. KEEPING MICROSOFT'S PRODUCTS

If you insist on using Microsoft Internet Explorer then I strongly recommend that you check out at least one of these programs:

ù PurgeIE (www.aandrc.com/purgeie)
ù Cache and Cookie Cleaner for IE (www.webroot.com/washie.htm)
ù Anonymizer Window Washer (www.anonymizer.com/anonwash)

Other programs that claim to clear your history don't seem to work, although I haven't run any tests in a while.

And if you insist on using Outlook or Outlook Express then you should get in the habit of compacting your mailboxes.

You can do this by going to File > Folder > Compact All if you have Outlook Express.

or

Tools > Options > Other tab > [Auto Archive] if you have Outlook. Make sure to set things up here.

4. STEP-BY-STEP GUIDE THROUGH YOUR HIDDEN FILES

This next section is for those of you who are more interested in learning the ins and outs of your computer. This section is intended for the savvy user.

The most important files to be paying attention to are your "index.dat" files. These are database files that reference your history, cache and cookies. The first thing you should know is that the index.dat files is that they don't exist in less you know they do. They second thing you should know about them is that some will *not* get cleared after deleting your history and cache.

The result:

A log of your browsing history hidden away on your computer after you thought you cleared it.

To view these files, follow these steps:

In MSIE 5.x, you can skip this first step by opening MSIE and going to Tools > Internet Options > [Settings] > [View Files]. Now write down the names of your alphanumeric folders on a peice of paper. If you can't see any alphanumeric folder names then start with step 1 here:

1) First, drop to a DOS box and type this at prompt (in all lower-case) to bring up Windows Explorer under the correct directory...

c:\windows\explorer /e,c:\windows\tempor~1\content.ie5\

You see all those alphanumeric names listed under "content.ie5?" (left-hand side.) That's Microsoft's idea of making this project as hard as possible. Actually, these are your alphanumeric folders that was created to keep your cache. Write these names down on a peice of paper. (They should look something like this: 6YQ2GSWF, QRM7KL3F, U7YHQKI4, 7YMZ516U, etc...) If you click on any of the alphanumeric folders then nothing will be displayed. Not because there aren't any files here, but because Windows Explorer has lied to you. If you want to view the contents of these alphanumeric folders you will have to do so in DOS. (Actually, this is not always true. *Sometimes* Windows Explorer will display the contents of the alphanumeric folders -- but mostly it won't. I can't explain this.)

2) Then you must restart in MS-DOS mode. (Start > Shutdown > Restart in MS-DOS mode. ME users use a bootdisk.)

Note that you must restart to DOS because windows has locked down some of the files and they can only be accessed in real DOS mode.

3) Type this in at prompt:

CD\WINDOWS\TEMPOR~1\CONTENT.IE5
CD %alphanumeric%
(replace the "%alphanumeric%" with the first name that you just wrote down.)

DIR/P

The cache files you are now looking at are directly responsible for the mysterious erosion of HD space you may have been noticing. One thing particularly interesting is the ability to view some your old e-mail if you happen to have a hotmail account. (Oddly, I've only been able to retreive hotmail e-mail, and not e-mail from my other web-based e-mail accounts. Send me your experiences with this.) To see them for yourself you must first copy them into another directory and then open them with your browser. Don't ask me why this works.

A note about these files: These are your cache files that help speed up your internet browsing. It is quite normal to use this cache system, as every major browser does. On the other hand. It isn't normal for some cache files to be left behined after you have instructed your browser to erase it.

5) Type this in:

CD\WINDOWS\TEMPOR~1\CONTENT.IE5
EDIT /75 INDEX.DAT

You will be brought to a blue screen with a bunch of binary.

6) Press and hold the [Page Down] button until you start seeing lists of URLs. These are all the sites that you've ever visited as well as a brief description of each. You'll notice it records everything you've searched for in a search engine in plain text, in addition to the URL.

7) When you get done searching around you can go to File > Exit.

8) Next you'll probably want to erase these files by typing this:

C:\WINDOWS\SMARTDRV
CD\WINDOWS
DELTREE/Y TEMPOR~1

(replace "cd\windows" with the location of your TIF folder if different.)

This will take a seriously long time to process. Even with smartdrive loaded.

9) Then check out the contents of your History folder by typing this:

CD\WINDOWS\HISTORY\HISTORY.IE5
EDIT /75 INDEX.DAT

You will be brought to a blue screen with more binary.

10) Press and hold the [Page Down] button until you start seeing lists of URLS again.

This is another database of the sites you've visited.

11) And if you're still with me type this:

CD\WINDOWS\HISTORY

12) If you see any mmXXXX.dat files here, then check them out (and delete them.) Then...

CD\WINDOWS\HISTORY\HISTORY.IE5
CD MSHIST~1
EDIT /75 INDEX.DAT

More URLs from your internet history. Note, there are probably other mshist~x folders here.

3) You can repeat these steps for every occurrence of a mshist~x folder.

4) By now you'll probably want to type in this:

CD\WINDOWS
DELTREE/Y HISTORY

This is about it as far as I know. You may also want to take a look at your *.mbx files if you own Outlook. (dir *.mbx/s) All your e-mail correspondence and file attachments are located within these database files. More detailed information is covered in the next section.

5. A LOOK AT OUTLOOK EXPRESS

Would you think twice about what you said if you knew it was being recorded? E-mail correspondence leaves a permanent record of everything you've said --

even after you've told Outlook Express to erase it. You are given a false sense of security sense you've erased it twice, so surely it must be gone. The first time Outlook simply moves it to your "Deleted Items" folder. The second time you erase it Outlook simply "pretends" it is gone. The truth is your messages are still being retained in the database files on your hard drive. (Same with your e-mail attachments.)

For earlier versions of Outlook Express, they will be located in either of the following folder:

c:\program files\internet mail and news\%user%\mail*.mbx

(replace %user% with the name you use.)

or if your lucky, it will be located here:

c:\windows\application data\microsoft\outlook\mail*.mbx

At this point you have two choices.

a) Get in the habit of compacting your folders all the time.
B) Import the data into another e-mail client such as Pegasus Mail or Eudora and then delete the mbx files (and thus all your e-mail correspondence) by typing this:

```
cd\windows\intern~1\%user%\mail
deltree/y mail
```

or

```
cd\windows\applic~1\micros~1\outloo~1\
deltree/y mail
```

*Typing in the above commands will kill all your e-mail correspondence. Do not follow those steps in less you have already exported your e-mail and address book!

6. HOW MICROSOFT DOES IT

TIP: Study this section if you would like to learn how to obscure your files using Windows' own built-in mechanisms.

How does Microsoft make these folders/files invisible to DOS?

The only thing Microsoft had to do to make the folders/files invisible to a directory listing is to set them +s[ystem]. That's it. As soon as the dir/s command hits a system folder, it renders the command useless (unlike normal folders.) A more detailed explanation is given in Section 7.

So how does Microsoft make these folders/files invisible to Windows Explorer?

The "desktop.ini" is a standard text file that can be added to any folder to customize certain aspects of the folder's behavior. In these cases, Microsoft

utilized the desktop.ini file to make these files invisible. Invisible to Windows Explorer and even to the "Find: Files or Folders" utility (so you wouldn't be able to perform searches in these folders!) All that Microsoft had to do was create a desktop.ini file with certain CLSID tags and the folders would disappear like magic.

To show you exactly what's going on:

Found in the c:\windows\temporary internet files\desktop.ini and the c:\windows\temporary internet files\content.ie5\desktop.ini contains this text:

[.ShellClassInfo]
UICLSID={7BD29E00-76C1-11CF-9DD0-00A0C9034933}

Found in the c:\windows\history\desktop.ini and the c:\windows\history\history.ie5\desktop.ini contains this text:

[.ShellClassInfo]
UICLSID={7BD29E00-76C1-11CF-9DD0-00A0C9034933}
CLSID={FF393560-C2A7-11CF-BFF4-444553540000}

The UICLSID line cloaks the folder in Windows Explorer. The CLSID line disables the "Find" utility from searching through the folder. (Additionally, it gives a folder the appearance of the "History" folder.)

To see for yourself, you can simply erase the desktop.ini files. You'll see that it will instantly give Windows Explorer proper viewing functionality again, and the "Find" utility proper searching capabilities again. Problem solved right? Actually, no. As it turns out, the desktop.ini files get reconstructed every single time you restart your computer. Nice one, Slick.

Luckily there is a workaround which will keep Windows from hiding these folders. You can manually edit the desktop.ini's and remove everything except for the "[.ShellClassInfo]" line. This will trick windows into thinking they have still covered their tracks, and wininet won't think to reconstruct them.

I can't stress how rediculous it is that Windows actually makes sure the files are hidden and in place on every single boot. No other files or folders get this kind of special treatment. What's the agenda, here?

7. +S MEANS [S]ECRET NOT [S]YSTEM

Executing the "dir/a/s" command from root *should* be the correct command to display all files in all subdirectories in DOS. However, doing so will not display the index.dat files. This is because when DOS tries to get a list of the subdirectories of any +s[ystem] folder it hits a brick wall. No files or folders will be listed within any system folder. Not only does this defeat the whole purpose of the "/s" switch in the first place, but I'd say it looks like Microsoft took extra precautions to keep people from finding the files. Remember. The only thing you need to do to obscure a file in DOS is to mark the parent directory +s[ystem].

I was told by a few people that this was due to a very old DOS bug that dates back many years. Fine. I can accept that. A bug it is.

But, would you consider your Temporary Internet Files to be "system files?" It would seem that your TIF folder appears to be marked +s[ystem] for no good reason at all. Just because. Same with your history folder. Just because. You may not agree, but I tend to think that Microsoft marked the folders as +s[ystem] solely to hide any directory recursal from DOS.

In case you didn't understand, here's a small experiment that will show you what I mean...

Since the content.ie5 and history.ie5 subfolders are both located within a +s[ystem] folder, we will run the experiment with them. The proper command to locate them *should* be this:

```
CD\
DIR *.IE5 /as/s
```

The problem is that you will receive a "No files found" error message.

Since we already know there is a content.ie5 subfolder located here, why is it giving me the "no files found" message?

But there is a way to get around this brick wall. That is, once you are inside the system directory, then it no longer has an effect on the dir listings. For example, if you enter the system folder first, and THEN try to find any +s[ystem] directories you can see them just fine:

```
CD\WINDOWS\TEMPOR~1
DIR *.IE5 /as/s

1 folder(s) found.
```

Now you will get a "1 folder(s) found." message. (But only after you knew the exact location.)

In other words, if you didn't know the files existed then finding them would be almost impossible.

And, by the way. To see the "bug" in progress...

```
CD\
DIR *.IE5 /as/s
```

It will echo "no files found."

Now, just take away the system attributes from the parent directory...

```
CD\WINDOWS
ATTRIB -S TEMPOR~1
```

And retry the test...

CD\
DIR *.IE5 /as/s

It will echo "1 folder(s) found."

8. THE TRUTH ABOUT FIND FAST

Have you ever wondered what that "Find Fast" program was under your control panel? Here's a hint: It has NOTHING to do with the "Find: Files or Folders" utility located under the [Start] menu. Up until last month I honestly thought it was completely useless, but it was finally adequately explained to me...

"In any version of Word after 95, choose File Open and you'll get the Office App Open dialog. Instead of just a space for the file name, there are text boxes for file name, files of type, text or property & last modified. These are search criteria you can use to find one or more files. There is also an "Advanced" button that opens a dedicated search dialog with more options. When you use either of these dialogs to perform a search, that search process uses the indexes built by Find Fast."

--Oblivion

That sure answered a lot. Now instead of a "completely useless resource hog," I realize Find Fast actually does serve some purpose.

But what would you say if I told you that Find Fast was scanning every single file on your hard drive? Did you know that in Office 95, the Find Fast Indexer had an "exclusion list" comprised of .exe, .swp, .dll and other extensions, but the feature was eliminated? If you were a programmer would you program Find Fast to index every single file, or just the ones with Office extensions?

FYI: If you have ever had problems with scandisk or defrag restarting due to disk writes, it is because Find Fast was indexing your hard drive in the background. It loads every time you start your computer up.

Now here is a good example of the lengths Microsoft has gone through to keep people from finding out Find Fast is constantly scanning and indexing their hard drives. (Always good to have an alibi.) Here's a snippet taken from microsoft.com:

"When you specify the type of documents to index in the Create Index dialog box, Find Fast includes the document types that are listed in the following table.

Document type	File name extension

MS Office and Web Documents All the Microsoft Excel, Microsoft PowerPoint, Microsoft Project, and Microsoft Word document types listed in this table. Microsoft Binder (.odb, .obt) and Microsoft Access (.mdb) files. Note that in .mdb files, only document properties are indexed.

Word documents .doc (document), .dot (template), .ht* (Hypertext Markup Language document), .txt (text file), .rtf (Rich Text Format) files, Excel workbooks .xl* files

PowerPoint .ppt (presentation), .pot (template), .pps (auto-running presentation) files

Microsoft Project files .mpp, .mpw, .mpt, .mpx, .mpd files

All files *.* files"

Did you get that last part? "All files?" Find Fast indexes Office Documents, Web documents, Word Documents, Power Point files, Project files, and (oh I forgot) EVERY SINGLE other file on your computer.

Actually, the good news is that this isn't neccessarily true. In another statement, Microsoft claims that if Find Fast deems the file "unreadable" then the file will not be included in the index. For example, your command.com probably wouldn't get indexed because it doesn't have a lot of plain text -- mostly binary.

But, back to the bad news. Every single file that has legible text is going to be included in the Find Fast database. Do you understand the implication here? Well, if you don't, then maybe you should check out those Find Fast database files -- because acording to Microsoft, ALL TEXT SAVED TO YOUR HARD DRIVE IS INDEXED. Do you see the forensic capabilities now? And don't forget "all text" also means previously visited webpages from your cache. See for yourself...

1) Open up a DOS window and type...
2) CD\
3) DIR FF*.* /AH (This will bring up a list of the find fast databases.)
4) EDIT /75 %ff% (insert %ff% with any of the names that were listed.)

Notice the incredible amount of disk accesses to your cache and history folders? Why do we need two indexes?

8.1. REMOVING THE FIND FAST PROGRAM

You can remove Find Fast using your Office CD, but I recommend you do it manually...

1) Reboot your computer in MS-DOS Mode.
2) Delete the findfast.cpl file from c:\windows\system\
3) Delete the shortcut (.lnk) under c:\windows\start menu\programs\startup\
4) Delete the findfast.exe file from c:\progra~1\micros~1\office\
5) Delete the find fast databases in your root, by typing this:

cd\
deltree ff*.*

6) You can also safely delete FFNT.exe, FFSetup.dll, FFService.dll, and FFast_bb.dll if you have them.

Feel free to check out the ffastlog.txt (which is the Find Fast error log). It's a +h[idden] file under c:\windows\system\.

9. CONTACT INFO AND PGP BLOCKS

This tutorial is being updated all the time. If you have any useful input, or if you see a mistake somewhere, then please e-mail me so I can compile it into future versions. You will be able to find the most recent version of this tutorial at fuckmicrosoft.com

My e-mail address is located at the end of this note. Please let me know where you heard about this tutorial in your message. If you have something important to say to me, then please use encryption. My public key blocks are located below.

Thanks for reading,

-- The Riddler
Contact: theriddler@fuckmicrosoft.com

My PGP 2.6.2 Block:

-----BEGIN PGP PUBLIC KEY BLOCK-----
Version: 2.6.2

mQCNAzu4wRAAAAEEAJnvaDDA9PydmZnnAmo80XZL57OycoCndppYyMv6CBMh+U35
NYtOxFfQiH8JhUN8uF3FgGBxckG0vBJ+RsYBIBXaP/JdxLX4qQnTsByyPEkoIomW
QCDfWXBMbFXxEKc1mrVTRmXpANpIjsj557qzW7dXxuvd5/E/bhviYkNfEe49AAUR
tAt0aGUgcmlkZGxlcg==
=B7ib
-----END PGP PUBLIC KEY BLOCK-----

My GPG 1.0.6 Block:

-----BEGIN PGP PUBLIC KEY BLOCK-----
Version: GnuPG v1.0.6 (MingW32)

mQGhBDu3TSERBACO0Fx9pjMULe6qLQwOgfvdnQconLOMyftZdp9+ZX6t29ebJ/Z5
qQOJ9ce9Xr6Lj4u+M9VDx1FK5ueoD45bUAy0HAvYDV/HEu2vCRimpbreDky/U88a
XL59Pe8qwnmfUzYc/LnH86VCr4lPmpbz6/adXj44xE6EwkhFcq6BD4isCwCg8zZO
Hk9+KEKOyPHIFWq7TUA/JdUD/jWtNrGZ0tfSAS0WDiBifsBr1HW7n2IMDFX1anqC

DN0ToM5IFWGDkOh1NUvP0RvyrnNuBOP/oWxkPLR0nVvifETF0iG9o+kfitC9NmJn
QP/iw4WhCoHRCc5wqnAAXQC9j8JdodQ8E5VnfnNGkttgWz7mNzBongrIoTdfVdtf
o5NwA/d/lwMhGE0HNXnXOgRBcPjGD0LsR8pFoSP/HJ9Hu3zms2cbQqN2O/f99H2G
s9mXR7uvicu9SbKoTwFkptLVbOQIhvBnw0fTlZGrUsaiw4vzt99PffTKq1FPIpQe
K7HcnUK2+ZSVs5PxGiDckobJEjBssSw9Lg5RSNMy9H7s9jv3tAt0aGUgcmlkZGxl
cohXBBMRAgAXBQI7t00iBQsHCgMEAxUDAgMWAgECF4AACgkQ/bqXDRMV1MxyMgCc
CH2uO/f46JgQ0pspQxi7IBv0yNQAn11ebXHbZGuADwuBun1EnQCJb8VIuQINBDu3
UOAQCADKG2mf/FW3kuSAGoFmIMBm4l6m0O7denwUIpZP2jxeNTLmLW6ntGglHP++
wEQpHjKTJfXoSHZH0euuXVZ9hOVdf1+PuRNy0DzrDDiKX7fdQ6eSbw+heSWc0kOF
AB1j3pcovG4K2+bK66039kQLIT3kNUZgh9DdMZjIFzBg90aQnaEm5LLMkv1FNVZP
YehZm3RRIpLAX5vkJJbUA/VVh/FXDG5f21iAGDHgSdKsLW2JNDAWe6/rY0GV5dgx
C0gsqBn1rxNNDyG+z6nFCQtohL/x5zdTzedLQBjIlao91mSWhBsyxiX8mjhvGO97
o6zVUG5KHBKGmvWMqlyOsGY9VSbDAAMGCADIaFAcE+ADY3ku9Fy0NIlJhbj578YY
xpsE6KvZI1OqbHSoBnN06A3Mpxp4QRBXlr9eRRl+zMTQl1VcVWkahZYNapOqq6L3
wHBmf9psggCBxqQdI9n5zxnlkphb50J7G9UevB/IGzlW2fe7WMWjo2GegIvGHVWr
qeZgyaNf/CyMtihAX3O86rpqakq//nJvQ9MPcp/Brr9KT2NxBlpBm6xWY35IL5FG
dZ2hpHaO1TC6bdmWUPhvzmSVtD9f0AnnJEgVc03vBz7xJrc1IEa1DeRdfFNvkoch
+mNjc+fBAIQrVMCQ33u+yP/DWSdThrhxz1tAGWV7SlwxVyg6JPRQJ+moiEYEGBEC
AAYFAju3UOAACgkQ/bqXDRMV1MwVnACfaGrJRv2lgWHQbQWwv55t2cT+QWEAnA/n
ckswjlC9aNcBkcFl7X1SX8JX
=pFTK
-----END PGP PUBLIC KEY BLOCK-----

9.1. RECOMMENDED READING

And if you aren't already paranoid enough here's some sites/articles that I
definitely recommend:

[URL=http://www.theregister.co.uk/content/4/18002.html]http://www.theregister.co.uk/content/4/18002.html[/URL]
[URL=http://www.findarticles.com/m0CGN/3741/55695355/p1/article.jhtml]http://www.findarticles.com/m0CGN/3741/5
56...1/article.jhtml[/URL]
[URL=http://www.mobtown.org/news/archive/msg00492.html]http://www.mobtown.org/news/archive/msg00492.html[/URL]
[URL=http://194.159.40.109/05069801.htm]http://194.159.40.109/05069801.htm[/URL]
[URL=http://www.yarbles.demon.co.uk/mssniff.html]http://www.yarbles.demon.co.uk/mssniff.html[/URL]
[URL=http://www.macintouch.com/o98security.html]http://www.macintouch.com/o98security.html[/URL]
[URL=http://www.theregister.co.uk/content/archive/3079.html]http://www.theregister.co.uk/content/archive/3079.
html[/URL]
[URL=http://www.fsm.nl/ward/]http://www.fsm.nl/ward/[/URL]
[URL=http://slashdot.org]http://slashdot.org[/URL]
[URL=http://www.peacefire.org]http://www.peacefire.org[/URL]
[URL=http://stopcarnivore.org]http://stopcarnivore.org[/URL]
[URL=http://nomorefakenews.com]http://nomorefakenews.com[/URL]
[URL=http://grc.com/steve.htm#project-x]http://grc.com/steve.htm#project-x[/URL]

10. SPECIAL THANKS (and no thanks)

This version I want to give special thanks to Concerned Boss, Oblivion, and
the F-Prot virus scanner.

I also want to take this time to show my dissatisfaction to the New Zealand
Herald. Although partly flattering, it was more disgusting to see a
well-known newspaper try to take credit for my work.

11. REFERENCES

[URL=http://support.microsoft.com/support/kb/articles/Q137/1/13.asp]http://support.microsoft.com/support/kb/ar
...s/Q137/1/13.asp[/URL]
[URL=http://support.microsoft.com/support/kb/articles/Q136/3/86.asp]http://support.microsoft.com/support/kb/ar
...s/Q136/3/86.asp[/URL]
[URL=http://support.microsoft.com/support/kb/articles/Q169/5/31.ASP]http://support.microsoft.com/support/kb/ar
...s/Q169/5/31.ASP[/URL]
[URL=http://support.microsoft.com/support/kb/articles/Q141/0/12.asp]http://support.microsoft.com/support/kb/ar
...s/Q141/0/12.asp[/URL]
[URL=http://support.microsoft.com/support/kb/articles/Q205/2/89.ASP]http://support.microsoft.com/support/kb/ar
...s/Q205/2/89.ASP[/URL]
[URL=http://support.microsoft.com/support/kb/articles/Q166/3/02.ASP]http://support.microsoft.com/support/kb/ar
...s/Q166/3/02.ASP[/URL]
[URL=http://www.insecure.org/sploits/Internet.explorer.web.usage.logs.html]http://www.insecure.org/sploits/Int
ernet.e...usage.logs.html[/URL]
[URL=http://www.parascope.com/cgi-bin/psforum.pl/topic=matrix&disc=514&mmark=all]http://www.parascope.com/cgi-
bin/psforum.p...c=514&mmark=all[/URL]
[URL=http://www.hackers.com/bulletin/]http://www.hackers.com/bulletin/[/URL]
[URL=http://slashdot.org/articles/00/05/11/173257.shtml]http://slashdot.org/articles/00/05/11/173257.shtml[/UR
L]
[URL=http://peacefire.org]http://peacefire.org[/URL]

