Internet Explorer keeps a record of every page you've visit since it was installed!

Summary

Description:	*.DAT files in the Win95/NT "Temporary Internet Files" directory store every move you make on the web.
Author:	From something called "technet"
Compromise:	Huge potential privacy violation if you can get physical access to a computer running IE. Also some URLs have access information encoded in them.
Vulnerable Systems:	Those running M$ Internet Explorer 4.0 or earlier. Mostly W95/NT boxes.
Date:	5 August 1997
Notes:	Apparently %SystemRoot%\History also contains .DAT files with the same information. Asking IE to clear the cache doesn't eliminate this, see the post in the addendum.

Details

Date: Tue, 5 Aug 1997 00:41:13 -0400 From: Mohamad Azlan <IMCEAMS-HADEED_MDDNT_XMS20853@HADEED.MIDLEAST.NET> To: NTBUGTRAQ@RC.ON.CA Subject: Re: Strange behavior regarding directory Gretings, I tried to duplicate this situation on the NT 4.0 setup I have and did face the same problem. Perhaps even more interesting, when I went to a command prompt and performed a directory list of my local "SystemRoot%\Temporary Internet File", it was empty. Opening the directory and selecting a "details" view also give information which seems to be quite different from a standard detail view of any other directory. Right clicking an item in the Temporary Internet Files directory also give a different pop-up, with an option to delete a local copy, which does seem to indicate that the file is stored both locally and at the internet address location shown in detail view. technet has this to say about the directory: 9. Warn Users About the Dangers of Snooping It isn't much fun to think about, but somebody snooping around on your system could learn a great deal about what you've been up to. Suppose, for example, you've gone off to lunch, and left your door open and your computer running. Anyone who walks in could learn a lot about where you've been online, just by looking in the folder where Internet Explorer caches the pages you've downloaded. Users can delete these files, but that's not a bulletproof solution. Unbeknownst to most Internet Explorer users, the program keeps an exact byte-by-byte record of where they've been online. This record is stored in .DAT files located in the Temporary Internet Files folder. Amazingly enough, these files also include an exact byte transcription of everything you've uploaded and everything you've downloaded, right back to the time you installed the program. Here's the rub. Unlike files stored in Internet Explorer's cache, you can't delete these .DAT files. (Try it-you'll be denied access.) By copying these files and inspecting them with a binary decoder, a knowledgeable intruder could reconstruct your users' every move going back months, even years. If you're worried about snooping, the best defense is to install a bulletproof, password-based authentication program on your users' computers. -----Original Message----- From: Richard Burgett [SMTP:burgett@moe.psislidell.com] Sent: Friday, August 01, 1997 2:30 PM To: NTBUGTRAQ@RC.ON.CA Subject: Strange behavior regarding directory Greetings, I was wondering if anyone could tell me why the "Temporary Internet Files" directory (under \windows in 95 and %SystemRoot% in NT 4.0) behave differently. If you are using explorer and try to access this file on a remote machine, the directory that is displayed is actually the local directory, even though the path displayed in the title bar of the window says "\\<remote machine>\Windows\Temporary Internet Files" If you try this from a Windows NT 3.51 machine, the directory is empty. Regards, Richard

```
Date: Wed, 6 Aug 1997 11:36:30 +0200
From: Kouti Sakari
To: NTBUGTRAQ@RC.ON.CA
Subject: Re: Strange behavior regarding directory

Mohamad wrote:
>I went to "SystemRoot%\Temporary Internet File"...
>>Internet Explorer keeps an exact byte-by-byte record of where they've
>>been online. This record is stored in .DAT files located in the Temporary
>>Internet Files folder.

%SystemRoot%\History too has MM2048.DAT and MM256.DAT. These two files
also contain every url you visited and every query you made in search
sites.

You can choose in IE 3 View/Options/Navigation/Clear History. After this
NT Explorer shows you have (almost) empty history. But when you open
these files with whichever binary editor (or just TYPE command), ALL THE
URLS ARE STILL THERE.

Yours, Sakari Kouti, MCSE, MCT
```

More Exploits!

The master index of all exploits is available here (Very large file)
Or you can pick your favorite operating system:

All OS's	Linux	Solaris/SunOS	Micro$oft
*BSD	Macintosh	AIX	IRIX
ULTRIX/Digital UNIX	HP/UX	SCO	Remote exploits

This page is part of Fyodor's exploit world. For a free program to automate scanning your network for vulnerable hosts and services, check out my network mapping tool, nmap. Or try these Insecure.Org resouces:

[Nmap | Sec Tools | Mailing Lists | Site News | About/Contact | Advertising | Privacy]