Publication: The Times Of India Delhi;Date: Jun 27, 2010;Section: Tech Talk;Page: 10

Every move you make, I'll be watching you

The army major suspected to have leaked information to Pakistan using his computer might agree with the words of that 'Police' song. They are apt for cyber space, where digital records are easily retrieved, by criminals or sleuths

Javed Anwer | TNN

In a world of devices, digital records are ubiquitous. The computer is handy for so much – writing a report for the office, friendly banter with friends or listing monthly expenses. But most people don't realize that all the information stored on a computer is available to those who know how – and where – to look for it. That could be cyber criminals in search of a victim or sleuths in search of an offender.

Every digital move you make is recorded. This treasure trove of clues is what investigators look for when they seize computers belonging to suspects. The most recent case is that of an army major, Shantanu Dey, who is suspected of espionage.

"Many computer users falsely believe that when they delete a file, it is gone for good. For example, in Microsoft FAT file systems, when a file is deleted, the operating system simply replaces the first character of the filename with the lowercase sigma character (). This tells the operating system that the file is no longer available and the disk space can receive new data. However, until that file space receives new data and overwrites the old file, the deleted file remains exactly as it is. This can be retrieved by cyber forensic experts," says Santosh Raut, cofounder of Pune-based Intense Forensic Services.

Experts can retrieve an overwritten file. "The exact file recovery may be difficult, but partial file and file history details, including when the file was created, last accessed, modified, deleted and content can be retrieved," says Raut.

Retracing digital footprints on the web and rebuilding entire web sessions days after the computer was disconnected may not be as easy as retrieving deleted files, but it too is possible.

Satheesh Kumar, senior scientist at Trivandrum's Resource Centre for Cyber Forensics in Trivandrum says, "We can definitely find out what sites someone was visiting or what he was doing on the web from the information recorded on the computer's hard disk. Internet history is available within a browser until it is overwritten."

Whenever someone goes online, he leaves behind a log, IP addresses, email ids, user names, passwords and the names of websites he visited. Kumar says this can be collected using investigation and analysis tools.

The problem with the indelible digital footprint is that investigators regard them as a valuable clue and feel entitled to use them when trying to crack a case.

But those who advocate privacy have long said that internet surfers and computer users should be made aware of the way computers store data. The result so far is a number of tools and devices that allow computer users "safely" to delete a file and hide a visit to a website.

Examples abound. The first and most basic tool is a web-based email service such as Gmail. "Without the help of the email service provider (eg Google or Yahoo), it's difficult to retrieve information from these accounts if the emails have been deleted from the inbox,'' says Kumar.

Raut says, "Of course, we can always approach the mail service provider but that takes time and even then, these companies allow permission only in very important cases. This is probably why China banned Google Services in the country."

Users can also rely on proxy servers, says Kumar and encrypt their connection to hide their online trail. "For safely deleting data, they can use wipers (see box). Around three to four passes are enough to make sure the file isn't retrieved. But a good forensic expert can still find information related to the deleted file,'' says Raut.

Perhaps, everyone should pay heed to the words of the song by '70s band 'Police': "Every move you make, I'll be watching you".

HOW TO HIDE THE NET TRAIL

DARIK'S BOOT & NUKE | Excellent open-source (free) tool that can boot from a CD and "completely delete the contents of any hard disk." A wipe with DBAN is highly recommended if you are selling or discarding your old PC or hard drive

CCLEANER | Also known as Crap Cleaner, this too is free. Handy for keeping PC clean and securely deleting temp files, cookies, and similar logs

FIREFOX | When paired with add-ons like NoScript and ForcedHTTPS (secure connection wherever possible), Firefox gives you a lot of privacy on the web

PROXY | Accessing through web-based proxies helps hide many digital footprints. Experts can still track you but not novices. Whistleblowers who want anonymity can use proxy tools such as Tor. Proxies often slow down internet speed