GlobalResearch
Center for Research on Globalization

Is the Government Spying On You Through Your Own Computer's Webcam Or Microphone?

By Washington's Blog
Global Research, June 24, 2013
Washington's Blog

Region: USA
Theme: Intelligence, Police State & Civil Rights

Government – Or Private Individuals – May Be Watching and Listening

We documented earlier today that – if you are near your smart phone – the NSA or private parties could remotely activate your microphone and camera and spy on you.
This post shows that the same is true for our computer.

Initially, the NSA built backdoors into the world's most popular software program – Microsoft Windows – by 1999.

And a government expert told the Washington Post that the government "quite literally can watch your ideas form as you type" (confirmed).

Reuters documented last year that the U.S. and Israeli governments can remotely turn on a computer's microphone:

> Evidence suggest that the virus, dubbed Flame, may have been **built on behalf of the same nation or nations that commissioned the Stuxnet worm that attacked Iran's nuclear program in 2010** [i.e. the U.S. and Israel], according to Kaspersky Lab, the Russian cyber security software maker that took credit for discovering the infections.
>
> Kaspersky researchers said they have yet to determine whether Flame had a specific mission like Stuxnet, and declined to say who they think built it.
>
> Cyber security experts said the discovery publicly demonstrates what experts privy to classified information have long known: that nations have been using pieces of malicious computer code as weapons to promote their security interests for several years.
>
> ***
>
> The virus contains about 20 times as much code as Stuxnet, which caused centrifuges to fail at the Iranian enrichment facility it attacked. It has about 100 times as much code as a typical virus designed to steal financial information, said Kaspersky Lab senior researcher Roel Schouwenberg.
>
> **Flame can** gather data files, remotely change settings on computers, **turn on PC microphones to record conversations, take screen shots** and log instant messaging chats**.**
>
> Kaspersky Lab said Flame and Stuxnet appear to infect machines by exploiting the same flaw in the Windows operating system and that both viruses employ a similar way of spreading.

***

> "The scary thing for me is: **if this is what they were capable of five years ago, I can only think what they are developing now**," Mohan Koo, managing director of British-based Dtex Systems cyber security company.

PC Magazine tech columnist John Dvorak writes:

> From what we know the NSA has back door access into Apple, Microsoft [background], and Google. What kind of access we don't know, but let us assume it is similar to what they did about 7 years ago to AT&T. They had a secret room at Fulsom St. in San Francisco and the AT&T engineers had no control and no access to a room full of NSA equipment that had direct access to everything AT&T could do.
>
> Microsoft is the source of the operating system for Windows and Windows cell phones. Apple controls the OS for Macs, iPhones, and iPads. Google controls the Chrome OS, Chrome Browser, and Android cell phones. The companies regularly push operating system upgrades and security updates to users on a regular basis.
>
> Imagine however that the NSA has access to these updates at the source and has the ability to alter these update in order to install some sort of spyware on your phone, tablet, or computer. **The software could turn on your camera or microphone remotely**, read all your private data, or erase everything and brick your phone or computer.

Moreover – as documented by Microsoft, Ars Technica, cnet, the Register, Sydney Morning Herald, and many other sources – ***private*** *parties* can turn on your computer's microphone and camera as well.

Cracked noted in 2010:

> All sorts of programs are available to let you remotely commandeer a webcam, and many of them are free. Simple versions will just take photos or videos when they detect movement, but more complex software will send you an e-mail when the computer you've installed the program on is in use, so you can immediately login and control the webcam without the hassle of having to stare at an empty room until the person you're stalking shows up.

The bottom line is that – as with your phone, OnStar type system or other car microphone, Xbox, and other digital recording devices – you shouldn't say or do anything near your computer that you don't want shared with the world.

Postscript: You could obviously try to cover your webcam and microphone when you don't want to use them.

But if you really want privacy, take a lesson from spy movies: Go swimming with the person you want to speak with ... since electronics can't operate in water.

Comment on Global Research Articles on our Facebook page

Become a Member of Global Research

Articles by: **Washington's Blog**