Malware in BIOS stirs concern at Black Hat meet

August 2 2012, by Nancy Owano

(Phys.org) -- Security researcher Jonathan Brossard has drawn attention to a backdoor espionage problem that is in an ornery class by itself. Presenting his finds at the recent Defcon and Black Hat events, Brossard has shown that any snooper placing rogue firmware on your computer "basically owns you forever." Brossard's proof of concept is bracing news for security professionals in public and private sectors. The importance of his research is that this kind of back door allows secret remote access over the Internet, no matter what the attempt might be to switch the hard disk or reinstall the operating system; such moves will not help.

The backdoor that Brossard created, Rakshasa, is according to Brossard

“a generic proof of concept malware for the intel architecture.” This is also what he refers to as “permanent backdooring of hardware.”

Installed into the computer’s BIOS chip on a motherboard it can compromise the operating system at boot time without leaving any traces on the hard drive. A computer's BIOS chip contains the first code, or firmware, which a computer runs when it is powered on to start the process of booting up the operating system, as explained in *Technology Review*. Brossard tested his deliberate misdeed against 43 antivirus programs and he found that none flagged his move as dangerous. The malware can also affect other peripheral devices such as network cards or CD-ROMs.

Brossard built Rakshasa by drawing on open-source software packages for altering firmware. He used (nonmalicious) Coreboot, SeaBIOS, and iPXE. Coreboot was used to re-flash the BIOS with a SeaBIOS and iPXE bootkit.

Aside from relative permanence, the other concern deals with big-picture what-ifs for government to government spying. Computers manufactured overseas at the factory or warehouse stage can be injected with malware at the time of manufacture.

While there is no evidence of such attempted espionage by hiding surveillance tools inside new equipment, the question is raised whether something like Rakshasa, which refers in name to a demon from Hindu mythology, could be used to infect the BIOS before a computer is delivered to its overseas consumers.

The good news is that this fiendish takeover ploy has a remedy. The bad news is that the remedy would seem daunting for those with limited knowledge of computers. One could get rid of the malware by acting to reflash both the motherboard and all peripherals at the same time, The

x86 architecture, according to Brossard, “is plagued with legacy.”

He recommends that when you get a new laptop “to reflash all these dodgy firmware that you don't understand, and which you can't understand, because it is proprietary, with open-source stuff that you can actually understand."

Brossard also said he hoped his research will “raise awareness of the security community regarding the dangers associated with non open source firmwares shipped with any computer and question their integrity.”