Security researcher discovers badBIOS malware that jumps using microphone and speakers

November 1 2013, by Bob Yirka

(Phys.org) —Highly respected Canadian security expert Dragos Ruiu has been fighting, he claims, an unknown bit of malware that that appears to run on Windows, Mac OS X, BSD and Linux, for approximately three years. After much research and effort, which he has been documenting using several online venues (mainly Twitter), he says he believes the malware infects computers via memory sticks, and vice versa. He says also that he's found evidence that the malware is able to create mini-networks between infected machines using high frequency sound waves that are passed from a computer's microphone to another's speakers, and vice-versa. Unfortunately, at this time, Ruiu is the only person that appears to know about the malware, which he has dubbed badBIOS.

All of the things Ruiu has described have been seen before, just not all together. The Stuxnet virus, for example, was passed to infected machines from memory sticks, and high-frequency sound waves have been used to send network packets of information for years. What's troubling about badBIOS is that it's either infecting only Ruiu's machines, or it's infecting a lot of other machines but nobody knows about it because of its very sneaky nature. If it is infecting other computers, what is it doing, and why?

Ruiu contends that badBIOS is malware that infects a computer's BIOS, thus reformatting a hard drive won't kill it, nor will running any known commercial antivirus software suite. Ruiu says that despite cleaning every piece of hardware he owns, the infections return. He says it all started around three years ago after installing a fresh copy of Mac OS X on his MacBook Air—the firmware on it updated itself without him doing anything to cause it to do so. Afterwards, the machine refused to allow him to boot from a CD ROM. Over the next several months, he reports, his other computers began behaving strangely as well, modifying their own firmware, occasionally deleting data and undoing changes to configuration information. What really worried him though was that a computer not connected to a network, or the Internet became infected as well. That led him to discover that encrypted data packets were being sent between infected machines, even those not on a network. The only way to stop them, he found, was disconnecting the microphones and speakers.

Ruiu's tale is a strange one indeed, begging several questions. The first of which is why is he the only one infected? Also, because of the complexity of the malware, if it's real, it almost certainly has been created by an entity with a lot of money, most likely a government. If so, which one, and why? And if a group or a government went to so much trouble to create badBIOS, why use it to infect one security expert, unless perhaps, the purpose is to use him as a pawn to test how well it does whatever it's been designed to do?

Citation: Security researcher discovers badBIOS malware that jumps using microphone and speakers (2013, November 1) retrieved 11 July 2024 from https://phys.org/news/2013-11-badbios-malware-microphone-speakers.html