Forums / General Discussion

Help Center

Here is an interesting case which boarders on being a hardware security issue

You are subscribed. Unsubscribe

No tags yet. + Add Tag

Chuck Gollnick · 13 minutes ago

http://www.bloomberg.com/news/articles/2015-02-17/spying-campaign-bearing-nsa-hallmark-found-infecti...

[quote]A sophisticated spying campaign infected tens of thousands of computers worldwide with surveillance software embedded in hard drives, according to a report from a cybersecurity company that points toward the U.S. National Security Agency.

The malware was found in 30 countries -- including Iran, Russia, China, Afghanistan and Pakistan -- and targeted governments and diplomatic institutions, military, Islamic activists and key industries such as telecommunications, aerospace, energy, financial institutions and oil and gas, Kaspersky Lab Inc., a Moscow-based cybersecurity company, said in a report released over the weekend.

....

The most sophisticated weapon in the group’s arsenal, however, is the ability to infect the hard drives. Kaspersky said the spy code was found in products made by Western Digital Technologies Inc., Samsung Electronics Co. and Seagate Technology Plc. [/quote]

This attack is clearly a firmware attack, a FIRMWARE TROJAN. Firmware is a broadly-defined and often abused jargon for embedded software.

In ancient days, hard disk drives were purely elector-mechanical devices. They consisted of the mechanical components of a motor and rotating magnetic disks, the electromagnetic read/write heads and the mechanical mechanism they are mounted and move on, and electronics to move the motors and write and read the data... but no processors and no firm/software. It wasn't long, though, before hard drive manufacturers began to incorporate processors to more-precisely control the motors and position the heads and then to use DSP techniques to improve reading and writing the magnetic media. Those processors needed embedded software, what is often called "firmware." That firmware is NOT part of the computer's operating system or application software. That firmware may very well not be field-accessible or updatable. That firmware is written into non-removable, non-volatile memory at the factory using some special access facility which is not generally available outside of the factory (JTAG, for example, accessed via test points on the drive's board).

Because it is not part of the computer's OS or application software, because it is not field-accessible, and because it has purely to do with the drive's internal operations, this "firmware" almost becomes part of the hardware. Many IT professionals would insist that because it comes with the hard drive and they never -- and can't -- touch it, it is just part of the hardware.

Now we see that someone apparently managed to inject a trojan into that firmware! Presumably, that would have to be done at the factory, Samsung, Seagate, and Western Digital.

As far as I know, there are only four companies left actually manufacturing hard drives: Western Digital, Seagate, Samsung, and Toshiba. So, apparently, whoever is responsible for this got into three of the four.

The big question: to what extent -- if any -- were Western Digital, Seagate, and/or Samsung cooperative in the insertion of this trojan into their products?

🡅 0 🡇 · flag

New post

To ensure a positive and productive discussion, please read our forum posting policies before posting.

☐ Make this post anonymous to other students

☑ Subscribe to this thread at the same time

Add post