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

Sort replies by: Oldest first Newest first Most popular

Chuck Gollnick · 4 days 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?

If we accept that the manufacturers were not complacent in this matter, then we have to conclude that someone managed to infiltrate these factories and gain access to the master copy of the firmware image and alter it. Presumably, the attack probably started at the engineering offices by first stealing the source code since inserting a very-difficult-to-detect trojan would be very difficult to do without the source. Then, the perpetrator managed to substitute their modified image at the factory such that it would pass all manufacturing tests and also all periodic engineering quality assurance tests. And there's a risk here: what if the manufacturer's engineers found a bug in their code (hey, a bug in code? It could happen.). They'd fix the bug and send the factory a new image, one without the trojan. So, two things come up: first, if the covert programmer found the bug in the code while weaving in the trojan, they might just fix it for the manufacturer as a courtesy... and to prevent the bug from motivating a change to the firmware which would require the covert crew to go through their whole process again. And, second, the covert operation would have to keep the engineering and manufacturing facilities under constant surveillance to detect such an update in-the-works, intercept it, weave the trojan into it, and then inject back the trojanified object code. This is suddenly becoming very sophisticated. But here's how it ties to this class on hardware security. If we are to believe that a firmware trojan could thusly be injected into a hard drive's firmware, it's not at all difficult to believe that a hardware trojan could be injected into a chip's hardware.

If, on the other had, we choose to believe that such a violation of security would not be possible on an ongoing basis and, therefore, the manufacturers must have secretly cooperated in the insertion of this firmware trojan, we now face a similar question: if hard drive manufacturers can be persuaded to cooperate with the addition of such a trojan into their products, is it not possible that semiconductor manufacturers could similarly be persuaded to cooperate with the addition of hardware trojans into their products?... especially Samsung which makes both known-to-harbor-firware-trojans hard drives and also microchips?

Either way, this is a PR problem for Samsung. Either their design/IP security and manufacturing secuirty is lax or they deliberately cooperated with the introduction of spyware into their hard drive products. Do you want to buy a hard drive... or a microchip... or, really, even a TV set from them?

"if the covert programmer found the bug in the code while weaving in the trojan, they might just fix it for the manufacturer as a courtesy... and to prevent the bug from motivating a change to the firmware which would require the covert crew to go through their whole process again. " This raises a really interesting problem for the covert crew. If they don't fix the bug, they risk it causing field problems for the manufacturer which would tank sales of the drives in question thus reducing the bounty they might reap with their trojan. They also risk the manufacturer either finding the bug as part of routine engineering testing or in responding to customer complaints and, either way, fixing the bug and issuing a new -- now trojan-free -- firmware image But, if the covert programmer fixes the bug, this could also draw attention. If the bug is found in the manufacturer's own engineering offices where the engineers use trojan-free firware they compile themselves, they might ask, "Why aren't we getting customer complaints about this?" and start to investigate. They might pull some trojan-infected drives from finished goods, for example, and find that they don't exhibit the bug behavior (because the covert programmers fixed the bug while inserting their trojan) and go investigating. So, this is a bit of a conundrum for the covert crew, eh? Dammed if you do, and dammed if you don't. Of course, someone trying to inject a hardware trojan into a chip design could face the same conundrum too.

🡅 0 🡇 · flag

Dan Cogan Signature Track · 2 days ago

Someone mentioned to me the other day about the idea that a compiler could inject extra code into your binary than you intended. When was the last time you checked your binary to make sure extra code isn't in there!? I'm not saying that's the case here, although seems like a nice way to get around the problem of engineers updating their firmware. Instead, make sure when engineers update their compiler, that they get a version which as the code injector built in. Also wouldn't be noticed by CRC checks.

And as you proposed, a synthesis tool (or other back-end tools) for hardware could inject trojan logic as well.

You mentioned TV - There's an article that discusses Samsung's use of microphones in their smartTVs. They warn that conversations near the microphone used for voice recognition may be picked up. No one knows if these conversations are kept or not, but we can imagine. Not sure how long this link will be around, but for what its worth :http://www.cnbc.com/id/102407345

↑ 0 ↓ · flag

+ Comment

Gang Qu INSTRUCTOR · 19 hours ago 🔗

It is more than compilers. Even with clean binary (no maliciously injected code), it is possible to attack the system. If you google the phrase "code reuse attack", you probably will find hundreds of thousands links. I guess that this is more of a topic in Mike's software security course. But researchers are also looking at solutions with the help from hardware.

↑ 0 ↓ · flag

+ Comment

Georgescu Adrian Signature Track · 17 hours ago 🔗

It was a hell of a week for security..it started with the announcement of a major bank theft, continued with the HDD firmware trojan, then the ad-ware use mainly by Lenovo witch could be used to steal data, and ended with the Edward Snowden presenting leaked documents showing that NSA and GCHQ hacked into the world's largest SIM card manufacturer, stealing encryption information (encryption keys).

↑ 0 ↓ · flag

+ Comment

Dan Cogan Signature Track · 17 hours ago 🔗

Yes, security (and lack of) is becoming an important public topic. Just understanding the terms from this course helps to follow the dialog when these cases of security breach occur. I have a feeling that these security breaches will become increasingly more common (whether we know it or not), as large corporations without the expertise, struggle to protect themselves. And with the oncoming "Internet of Things" people will open themselves up to so many possibilities for attack. People who can provide good security will be in high demand.

↑ 0 ↓ · flag

+ Comment

Chuck Gollnick · 17 hours ago

Certainly, to Prof. Qu's credit, this course has made this last week or two a lot more interesting, as Mr. Cogan says.

The problem with trying to tamper with compilers -- or FPGA/Gate Array place-and-route tools -- is that the makers of those tools are also constantly issuing updates. If we assume that the tool manufacturer goes back to uncorrupted source code to make their updates, then a covert actor wanting to somehow tamper with that tool so as to affect soft/firmware or gateware produced by that tool will contain some trojan has to keep tampering with each new version of the tool.

It all seems just too unreasonable to me... until this hard drive thing came along. HDD firmware is generally not field accessible. There just isn't a physical port to go through. This had to be put on the drives at the factory. Furthermore, this trojan code does not run on the computer's x86 main processor as part of the well-defined PC architecture. No. This code runs on the HDD's own embedded processor which is probably an ARM core -- possibly customized -- and is embedded in an ASIC surrounded by custom peripherals. To write code of any significant complexity to run on that processor, a programmer has to know the confidential and proprietary details of that ASIC... which is different on all three brands of HDDs affects.

As I see it, one of two options exist: A) the HDD manufacturers were complicit in this. B) whoever did it had penetrated three engineering offices and their captive factories very deeply.

Either way, if the spooks could manage to get this HDD firmware trojan into the products of three companies -- either by method A or by method B -- then it's just not hard to believe that the spooks could get a hardware trojan into a chip too.

↑ 0 ↓ · flag

+ Comment

Georgescu Adrian Signature Track · 16 hours ago

News flash: in the last 5 years the HDD manufactures reduced from 3 (Samsung in South Coreea, Hitachi and Toshiba in Japan, and Seagete and Western Digital in USA) to 1 (or 2 if you want) ..through acquisitions and partnerships Seagate/WD became the only one "developers/manufactures" on the market.

↑ 0 ↓ · flag

+ Comment

New post

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

B | I | Link | <code> | Pic | Math | Edit: Rich ▾ | Preview

☐ Make this post anonymous to other students

☑ Subscribe to this thread at the same time

Add post