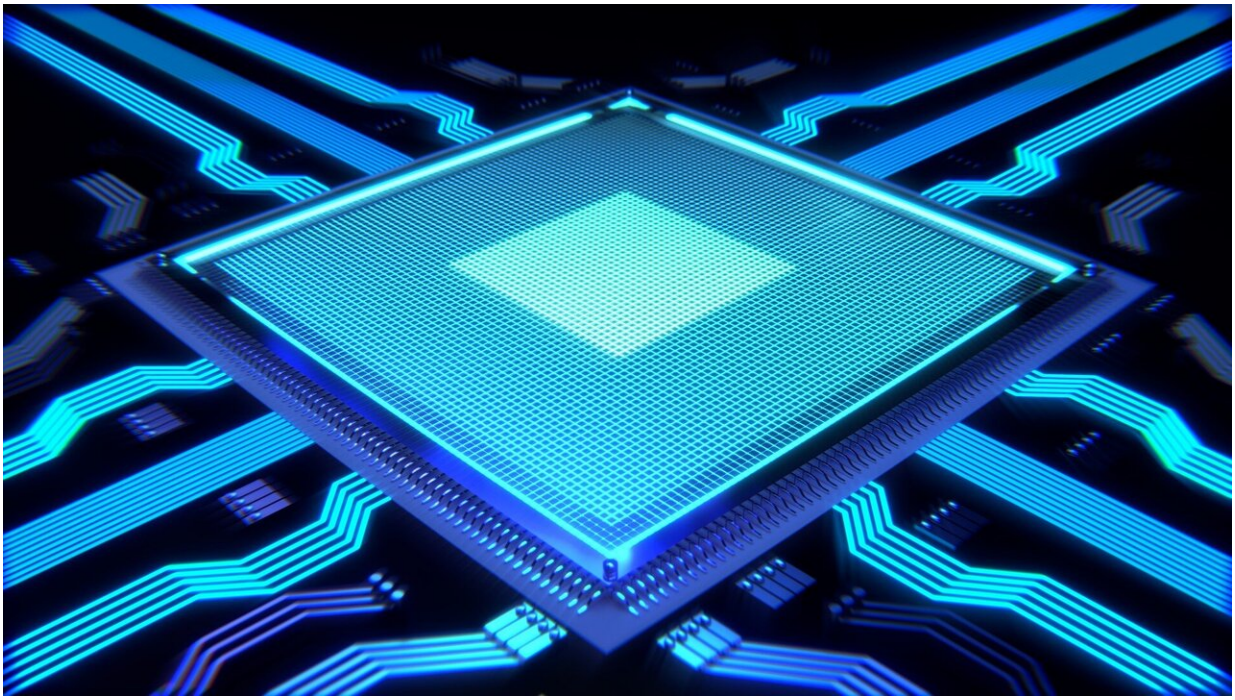
Spy chip planting said to be easy to do and tough to spot

October 15 2019, by Nancy Cohen



Credit: CC0 Public Domain

Much too easy: Planting a two-dollar spy chip on hardware with a technique that can be pulled off on a less than $200 budget? Yet that was the work of a proof in concept investigation by a security researcher and tech-watching sites were discussing the story on Monday.

Turns out you can slip a spy chip into any hardware for no more than

$198 to $200, said reports. The spotlight was on security researcher Monta Elkins, Hacker-in-Chief, FoxGuard Solutions. He has a proof-of-concept version of a hardware implant.

John Dunn, *Naked Security*, talked about the chip as bad news for security were it to happen. "In fact, this has already happened as part of a project by researcher Monta Elkins, designed to prove that this sort of high-end hardware hack is no longer the preserve of nation-states."

Elkins now intends to show organizations how easily cyberterrorists can plant one of these spy chips in company IT equipment for backdoor access to their systems, said *Tech Times*.

Elkins drove home the point that the hack was not magic, and not impossible to pull off. "I could do this in my basement," he said in *Wired*. "And there are lots of people smarter than me, and they can do it for almost nothing."

It's a tiny spy chip. Elkins used an ATtiny85 chip smaller than a pinky fingernail to write his code to that chip and ready it as a spy chip, said Ankush Das, *Ubergizmo*.

According to *Wired*, Elkins suggested he could have even used a smaller chip but ATtiny85 looked good because it was easier to program.

The chip was around 5mm squared found on an Arduino board. He soldered it to a motherboard of a firewall. (He de-soldered the chip from the board after reprogramming it, said *Computing*. The chip was then soldered on to the motherboard of firewall, giving the chip access to the serial port of the firewall.)

Andy Greenberg in *Wired* said, "He used an inconspicuous spot that required no extra wiring and would give the chip access to the firewall's

serial port."

According to the *Wired* report, none of the following would alert an administrator: Elkins said his attack could change firewall settings to offer remote access to the device, disable its security features, and give the hacker access to the device's log of connections it sees.

One might think about Dunn's other observation: "they're impossible to see let alone detect once they're installed inside equipment."

And getting rid of it? Dunn said, "the fact it depends on hardware might make it impossible to get rid of short of disabling the serial port or removing the chip itself."

The story in *Wired* drew particular attention. Andy Greenberg walked readers through the modest costs: A soldering tool, $150; a microscope, $40; and chips ordered online.

What's the message that Elkins would like to share through his work? Chip implants are relatively straightforward. "If I can do this, someone with hundreds of millions in their budget has been doing this for a while ."

Paul Lilly in *HotHardware* thought that "this is something companies need to be on the lookout for, particularly big ones that operate massive data centers and cloud computing infrastructures."

A substantial number of reader responses turned up in *Ars Technica*, reacting to the report there. Readers sent in pro and con arguments about whether or not such an exploit was easy to pull off. They asked if it was entirely plausible a person within the supply chain could alter the design.

One reader wrote, "Now, some may scuff at the notion of someone

breaking into a high security facility, Mission: Impossible style, and soldering the chip on—this is doable but not very likely. However, a factory operating on behalf of a state actor or someone else with a good bribe, could easily do this. In all likelihood they already are. And no, nobody checks their router or server down to the smallest black dot on the motherboard against the official blueprints (and where would you get them from)! As a rule—if something can be done, it is being done."

Also, a reader comment in *Ars Technica* pointed out that "this isn't about breaking into a datacenter to plant the chip. But about having access to the hardware before its even shipped to the datacenter and put something that can't be detected or prevented with normal methods."

What's next? Elkins will present his proof-of-concept attack at the CS3sthlm security conference later this month in Sweden. This is a summit on security in SCADA and industrial control systems. The event dates are October 21 to 24.