RATTLED: CHINA'S HARDWARE HACK

[*NB: Note the byline. Portions of my analysis may be speculative. / ~Rayne*]

As I noted in my last Three Things post, information security folks are rattled by the October 4 Bloomberg Businessweek report that extremely tiny microchips may have been covertly embedded in motherboards used by U.S. businesses.

Their cognitive dissonance runs in two general directions – the feasibility of implanting a chip at scale, and the ability of such a chip to provide a viable backdoor to a device.

Hardware security researchers and professionals have been debating manufacturing feasibility and chip ability across Twitter. Joe Fitz' recent tweet threads suggest implantation of a rogue chip is entirely doable on a mechanical basis though what happens once a chip has been embedded must be assessed from a software perspective. Fitz is not alone in his assessment; other professionals and academics believe it's possible to insert a 'malicious' chip. Computer security academic Nicholas Weaver pointed to small devices which could do exactly what the Bloomberg report suggested if these tiny objects were embedded into motherboards during manufacturing.

The feasibility also requires the right opportunity – a confluence of personnel, manufacturing capability and capacity, timing and traceability. Let's say a rogue or compromised employee manages to slip chips into a batch of motherboards; which ones? To whom will they ship? How could a rogue/compromised employee ensure the motherboards left the facility undetected?

The Bloomberg report paints the U.S.-based Supermicro plant as a perfect environment in which such hardware infiltration could happen

easily. With employees divided by two very different languages – English-speakers far less likely to understand Mandarin-speakers – discussions between multiple rogue/compromised employees could be very easy as would be sharing of written instructions. Supermicro's ISO certifications for standards 9001, 13485, 14001, and 27001 may shed some light on how the company expected to manage two different languages in the same workplace.

One could argue a bilingual workplace shouldn't pose a challenge given how many companies already use English/Spanish, English/French, or English/German. Compare, however, these words:

English: *hardware*

German: either *hardware* or *computerhardware*

French: either *hardware* or *le matériel*

Spanish: either *hardware* or *los equipos*

Mandarin: □□ (yìng jiàn)

With enough exposure the average English-as-primary-language worker could readily understand the most common western language words for equipment they were manufacturing. It would take considerably more investment in education to recognize and understand a pictographic language making casual quality control difficult.

The environment is even more challenging for mixed language staff in manufacturing plants located in China.

~ | ~ | ~

Let's look at a timeline of events leading up to the Bloomberg report this week. Note how often the word 'firmware' is used in this timeline and in the responses from Apple and Amazon to the Bloomberg story:

1993 – Charles Liang launched Supermicro.

2007 – Social search analytics company Topsy founded.

2005 – Defence Science Board warned “trojan horse” chips bought overseas could negatively affective military systems.

2008 – BusinessWeek reported that fake Chinese-made microchips had entered the military’s supply chain causing system crashes.

2010 – Defence Department bought 59,000 chips, unaware they were counterfeit.

2Q2011 – China denied entry visas to senators Levin and McCain staff for congressional probe in Guangdong province.

October 2011 – Apple releases Siri.

December 2013 – Apple acquired Topsy.

December 2013 – Supermicro publicly disclosed vulnerability/ies in a web application related to management of motherboards (Amazon response, email Oct 2018)

December 2013 – CBS’ 60 Minutes program aired a story about the NSA in which a plot involving a rogue BIOS had been identified.

First half 2014 (date TBD) – Intelligence officials tell White House that PRC’s military would infiltrate Supermicro’s motherboard production with microchips intended for the U.S. market.

January 2014 – Elemental communicated to existing customers that a new version of the web app was available for download; equipment shipped after this date had updated versions of the web app. (Amazon response, email Oct 2018)

Early 2015 – Amazon launched pre-acquistion evaluation of startup Elemental Technologies which used Supermicro motherboards in servers it made.

Late spring 2015 – Elemental sent several servers to Ontario CAN for testing by third-party security firm. It found non-spec chips on server motherboards. (Bloomberg report)

May 2015 – Apple detected unusual network

activity and experienced firmware problems.

Summer 2015 – Apple found non-spec chips on Supermicro motherboards Apple bought from Supermicro. (Bloomberg report)

September 2015 – Amazon announced its acquisition of Elemental.

December 2015 – Apple shut down Topsy.

Mid-2016 – Apple broke off its relationship with Supermicro.

June 2018 – Researchers publicized vulnerabilties found in Supermicro firmware. AWS notified customers and recommended a firmware upgrade. (Amazon response, email Oct 2018)

October 2018 – Amazon, Apple, Supermicro, and PRC submitted responses denying Bloomberg's report. (Published by Bloomberg)

~ | ~ | ~

Follow up reporting by other news outlets increase the layers of denial that cloud companies Amazon and Apple were affected by a possible breach of the hardware supply chain.

Some have asked if Bloomberg's report is merely an attempt to undermine Amazon and Apple, which are the two most valuable companies in the U.S. and in Apple's case, the world.

It is their value and their place in the stock market along with the customers they serve which may drive some of the denial.

Remember that Amazon's AWS has provided hosting to U.S. government agencies. Government employees also use Apple iPhones and by extension, Apple's cloud services. Is it at all possible that in providing services to government agencies these corporations and/or their subsidiaries have been read into programs obligating a degree of secrecy which includes denial of vulnerabilities and breaches which do not affect directly the average non-governmental user of Amazon and Apple products and services?

~ | ~ | ~

There are additional events which appear to have happened independently of the alleged hardware supply chain infiltration. They may be extremely important and highly relevant if looked at from an industry and intelligence perspective.

March 2014 – Freescale Semiconductor lost 20 employees in apparent crash of Malaysia Air flight MH370 en route to Beijing. The employees were supposed to begin work on a new chip manufacturing facility in China. While Freescale's chips were not those one might ordinarily associate with server motherboards, it's worth asking if Freescale at that time had any chips which might have served as server chips, or if they could work as illicit hardware hacks when embedded in a motherboard. Freescale has since been acquired by NXP.

Late 2010 – Beginning in late 2010, China identified and executed a network of U.S. agents within its borders over a two-year period, resulting in the deaths of at least 30 persons and the prosecution of former CIA agent Jerry Chung Shin Lee who worked as an informant for PRC. The exposure of these spies was blamed in part on a compromised communications system which had been previously used in the middle east. Due to compartmentalization of the project, it's reported Lee could not have identified the agents, placing more emphasis on the communications system.

Mid-2011 – China refused visas to staff for senators Carl Levin and John McCain for the purposes of investigating electronic components manufacturing in city of Shenzhen in Guangdong province. The congressional probe sought the source of counterfeit parts which had entered the U.S. military's supply chain; U.S. Commerce Department reported in January 2010 that 400 companies surveyed "overwhelmingly cited China" as the point of origin for counterfeit parts.

These events spawn more questions when looking at technology supply chain hacking and

communications systems which rely on this supply chain.

Did Freescale's plans to expand production in China pose a risk to the hardware supply chain hack? Or was it simply a fluke that a substantive portion of the company's manufacturing engineers disappeared on that flight? Though Freescale originated in Austin, Texas, it had a presence in China since 1992 with at least eight design labs and manufacturing facilities in China as of 2014.

Was the communications system used by doomed U.S. assets in China affected not by tradecraft or betrayal, or even by counterfeit parts, but by the hardware supply chain hack – and at an even earlier date than the timeline of events shown above related to Supermicro's compromised motherboard production?

Did China refuse admittance to Guangdong province in 2011 related not to counterfeit parts but to the possibility that supply chain hacks beyond counterfeiting alone might be revealed?

Is the supply chain hack reported by Bloomberg part of a much larger security threat which has been slowly revealed but not widely acknowledged because the threat has been viewed through narrow military, or intelligence, or tech industry lenses?

The tech industry may be rattled by allegations that the computer hardware supply chain has been hacked. But the possibility this hack has gone on much longer and with massive potential collateral damage may truly shake them up.

~ | ~ | ~

There is a third train of cognitive dissonance, not limited to information security professionals. Persons outside the tech industry have indulged in denialism, taking comfort in the aggressive pushback by Apple and Amazon which each claim in their own way that the Bloomberg report is inaccurate. (I have an

analysis of the early responses by Apple and Amazon; I will also examine later expanded responses as well as Supermicro's and PRC's responses as soon as time permits.)

But there have been reports for years about counterfeit electronic components, obstruction of investigations into these components, system failures which could be attributed to hardware or software which do not meet specifications. Cognitive dissonance also resists Bloomberg's report that as many as 30 U.S. companies were affected, not just Apple and Amazon which have offered up high-profile rebuttals.

And there have been reports in industries outside of cloud services and the military where off specification or counterfeit electronic components have made it into production. One such anecdote appears in a thread at Hacker News YCombinator, discussing credit card payment systems and development of screening systems requiring application of tests using angular momentum to determine if a board has been altered without breaking the board's tamper-proof seal.

In addition to his early tweets assessing feasibility of malicious or covert off-spec chips added to motherboards, Nicholas Weaver wrote a post for Lawfare about the Bloomberg report.

> The Bloomberg story also explains a previous mystery: in 2016, Apple quietly removed all SuperMicro servers from their products due to an unspecified "Security Incident." At the time the rumor was that SuperMicro provided a sabotaged BIOS—that is, the bootstrap program used to start the computer, another "god mode" target for compromise. Apple denied then that there was any security incident—just as they are denying one now.
>
> This incident once again illustrates the "Coventry problem," referring to Winston

> Churchill's apocryphal decision not to prevent the bombing of Coventry in order to keep secret that British intelligence had decrypted the Enigma machine. Robertson and Riley describe a U.S. intelligence apparatus that knew of these ongoing attacks, but could not effectively notify the affected companies nor provide useful recommendations. If the intelligence community had warned these companies, it would probably have revealed to the Chinese that the U.S. was aware of these activities, as well as potentially compromise an ongoing FBI investigation described in the article.

Weaver called the suspect Supermicro firmware a 'BIOS' – the first use of this term across multiple reports covering the Bloomberg report and its aftermath. This change in nomenclature is critical, particularly so given the point he makes about the "Coventry problem." The term 'BIOS' does not appear in the early responses from Apple, Amazon, or Supermicro.

In December 2013, CBS' 60 Minutes aired a report about the NSA; it appeared at the time to puff up the agency after the publication of Edward Snowden's leaked documents about the government's domestic spying using PRISM. Within the story was a claim about a thwarted cyberattack:

> Debora Plunkett: One of our analysts actually saw that the nation state had the intention to develop and to deliver, to actually use this capability– to destroy computers.
>
> John Miller: To destroy computers.
>
> Debora Plunkett: To destroy computers. So the BIOS is a basic input, output system. It's, like, the foundational component firmware of a computer. You start your computer up. The BIOS kicks

> in. It activates hardware. It activates the operating system. It turns on the computer.
>
> This is the BIOS system which starts most computers. The attack would have been disguised as a request for a software update. If the user agreed, the virus would've infected the computer.
>
> John Miller: So, this basically would have gone into the system that starts up the computer, runs the systems, tells it what to do.
>
> Debora Plunkett: That's right.
>
> John Miller: —and basically turned it into a cinderblock.
>
> Debora Plunkett: A brick.
>
> John Miller: And after that, there wouldn't be much you could do with that computer.

The description sounds remarkably like the rogue firmware update in concert with a malicious/covert chip.

The manner in which this report was handled by the NSA, however, made it appear like disinformation. The assessment that such firmware would be used solely brick a device heightened the FUD around this report, deterring questions about applications other than bricking a device — like taking control of the computer, or collecting all its transaction and data. Was the FUD-enhanced release via 60 Minutes the intelligence community's approach to the "Coventry problem"?

~ | ~ | ~

The problem Bloomberg's Jordan Robertson and Michael Riley reported is probably much bigger than they described. It is bigger than Supermicro motherboards and firmware, and it's not a problem of the near-term future but

ongoing over the last decade.

At what point will U.S. industries organize a collective response to both counterfeit and off-specification manufacturing of electronic components overseas? They can’t count on a calm and rational response from the Trump administration given the unnecessary trade war it launched against China.

———

Disclosure: I have positions in AAPL and AMZN in my investment portfolio.