STILL RATTLED: FALLOUT AND PUSHBACK

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

The tech industry and technology journalism outlets remain rattled by Bloomberg Businessweek's The Big Hack article.

Bloomberg Businessweek's Jordan Robertson and Michael Riley published a second article last Tuesday in which a security expert went on the record about compromised servers with Supermicro motherboards in an unnamed telecommunications provider. Do read the article; the timing of the discovery of the unexpected network communications and the off-spec covert chip fit within the timeline of Apple and Amazon problems with Supermicro motherboards.

The FBI's and DHS' responses are also interesting — the first refused to comment and the second offered a tepid endorsement of Apple's and Amazon's denials.

The second article hasn't assuaged industry members or journalists, though, in spite of a source on the record about a third affected entity.

The main criticisms of Bloomberg piece are:

- No affected equipment or firmware has been produced for review;
- Too much of Bloomberg's sourcing remains anonymous;
- The claims cannot be validated by other journalists, technology companies, persons at Apple and Amazon who have been contacted and interviewed by non-Bloomberg journalists;
- Contacts inside the companies in question continue to deny knowledge if they don't

express confusion about the alleged hack;

– Apple and Amazon have published firm denials, including Apple's preemptive letter to Congress.

However,

– Something drove both Apple and Amazon to change their relationship with Supermicro within a fairly tight time frame;

– The uniformity of their early denials in which they avoid mentioning hardware and lean toward web application as a point of conflict is odd;

– Neither of these enormous firms nor Supermicro have filed a lawsuit against Bloomberg for libel that the public can see, preventing questioning of Bloomberg's journalists and sources under subpoena;

– Securities and Exchange Commission doesn't appear to have been engaged to investigate the claims (although it's possible the SEC is on this and may simply not have disclosed this publicly);

– None of the other unnamed companies alleged to have received compromised motherboards have uttered a peep to defend (or rebut) Apple or Amazon.

I have not seen in any reporting I've read to date – from either Bloomberg Businessweek in The Big Hack or subsequent articles examining the claims or rebutting them – that any journalist, tech industry member or infosecurity community member has asked whether Apple, Amazon, or the other affected companies ordered customized motherboards or servers with customized motherboards made to their company's specifications. Supermicro has also said nothing about any possible differentiation between motherboards for different companies which would affect the scenario. The silence on this point is confounding.

This piece in Ars Technica captures many of the

concerns other tech news outlets have with the Bloomberg reports. Complaints that software – meaning firmware – is easier to hack than adding off-spec hardware miss two key points.

> The complexity, sophistication, and surgical precision needed to pull off such attacks as reported are breathtaking, particularly at the reported scale. First, there's the considerable logistics capability required to seed supply chains starting in China in a way that ensures backdoored equipment ships to specific US targets but not so widely to become discovered. Bloomberg acknowledged the skill and sheer luck of success by comparing the feat to "throwing a stick in the Yangtze River upstream from Shanghai and ensuring that it washes ashore in Seattle." The news service also quotes hardware hacking expert Joe Grand comparing it to "witnessing a unicorn jumping over a rainbow."

Made-to-order components or assemblies in Just-In-Time lean manufacturing enterprises make it easier to ensure that adulterated products reach their intended mark because each order represents an identified, traceable batch. Adherence to ISO standards in manufacturing processes may even make traceability easier.

We know Supermicro uses lean manufacturing techniques because it's in job postings online (lousy pay, by the way, which may also say something).

Does Supermicro use the same lean manufacturing approach overseas? Do any of its suppliers also use lean manufacturing?

In contrast, release of firmware (without corresponding adulterated hardware) to a single target is more difficult to control than hardware – the example given is Stuxnet (excerpt here from Ars Technica).

> The articles don't explain how attackers ensured the altered equipment shipped broadly enough to reach intended targets in a distant country without also going to other unintended companies. Nation-state hackers almost always endeavor to distribute their custom spyware as narrowly as possible to only chosen high-value targets, lest the spy tools spread widely and become discovered the way the Stuxnet worm that targeted Iran's nuclear program became public when its creators lost control of it.

Why wouldn't a determined nation-state ensure there was a failover, a Plan B method for accessing specific intelligence from a narrow

range of sources instead of betting the farm on one method alone? Given the means to deploy both malicious firmware and adulterated hardware, why wouldn't they try both?

~ | ~ | ~

In spite of tech industry and journalists' criticisms of Bloomberg's reporting, these facts remain:

1 – Technology supply chain has been compromised;

2 – U.S. government has known about it (pdf);

3 – U.S. government has not been forthcoming about it or the blacklists it has implemented;

4 – U.S. government has tried to investigate the compromise but with insufficient success;

5 – Some companies are also aware of the compromised supply chain.

We're no closer to resolving this question: has the compromise of the supply chain remained limited to counterfeiting, or does the compromise now include altered products?

At what point will the tech industry and infosecurity community begin to take supply chain hacks more seriously?

_____

[*AN: I still have to analyze both Apple's letter to Congress and its second response posted on their website along with Amazon's published response. More to come./~Rayne*]