RATTLED: CHINA'S HARDWARE HACK – APPLE'S RESPONSE

[*NB: Note the byline. Portions of my content are speculative. / ~Rayne*]

The following analysis includes a copy of an initial response received from Apple by Bloomberg Businessweek in response to its story, The Big Hack. In tandem with the Bloomberg story this was published on October 4 at this link. Apple's response is offset in blockquote format. No signer was indicated in the published response. Additional responses from Apple to Bloomberg's story will be assessed separately in a future post.

This analysis is a work in progress and subject to change.

———————

Apple

> Over the course of the past year, Bloomberg has contacted us multiple times with claims, sometimes vague and sometimes elaborate, of an alleged security incident at Apple.[1] Each time, we have conducted rigorous internal investigations based on their inquiries and each time we have found absolutely no evidence to support any of them.[2] We have repeatedly and consistently offered factual responses, on the record, refuting virtually every aspect of Bloomberg's story relating to Apple.[3]

[1] Phrasing avoids who made the allegation(s).

[2] "rigorous internal investigations" doesn't describe what they actually investigated; "each time" refers to investigations AFTER Bloomberg contacted Apple, AFTER 2016 when Apple had broken off relations with Supermicro.

[3] “refuting virtually aspect” does not mean “every and all.”

> On this we can be very clear: Apple has never found malicious chips, “hardware manipulations” or vulnerabilities purposely planted in any server.[4] Apple never had any contact with the FBI or any other agency about such an incident.[5] We are not aware of any investigation by the FBI, nor are our contacts in law enforcement.

[4] (a) What about problems with firmware updates, including malicious firmware, firmware not issued by Supermicro, or hijacking to firmware upgrade sites not created by Supermicro?

(b) “purposely planted in any server” refers not to Supermicro’s motherboards but Elemental or other server assemblies.

[5] What about contact with any government agency regarding firmware? What about contact with a third-party entity regarding firmware problems, including security researchers?

[6] This phrasing focuses on law enforcement but not on other possibilities like intelligence entities or non-law enforcement functions like Commerce or Treasury Departments.

> In response to Bloomberg’s latest version of the narrative, we present the following facts: Siri and Topsy never shared servers;[7] Siri has never been deployed on servers sold to us by Super Micro; and Topsy data was limited to approximately 2,000 Super Micro servers, not 7,000. None of those servers has ever been found to hold malicious chips.[9]

[7] (a) What about earlier versions of Bloomberg’s narrative the public hasn’t seen?

(b) Did Siri and Topsy ever share a data farm

facility?

[8] (a) Was Siri ever deployed on Elemental brand servers?

(b) Was Topsy ever deployed on Elemental brand servers?

[9] Did any of the servers on which Siri and Topsy were deployed experience firmware problems including malicious firmware, firmware not issued by Supermicro, or hijacking to firmware upgrade sites not created by Supermicro?

> As a matter of practice, before servers are put into production at Apple they are inspected for security vulnerabilities and we update all firmware and software with the latest protections. We did not uncover any unusual vulnerabilities in the servers we purchased from Super Micro when we updated the firmware and software according to our standard procedures.[10]

[10] Is this a statement of current practices or practices during the period of time about which Bloomberg reported? Why did Apple end its relationship with Supermicro?

> We are deeply disappointed that in their dealings with us, Bloomberg's reporters have not been open to the possibility that they or their sources might be wrong or misinformed. Our best guess is that they are confusing their story with a previously-reported 2016 incident in which we discovered an infected driver on a single Super Micro server in one of our labs.[11] That one-time event was determined to be accidental and not a targeted attack against Apple.[12]

[11] Gaslighting about the journalists' credibility. Have there ever been any servers from Elemental or other server manufacturer with

“infected drivers,” including the “single Super Micro server in one of our labs”? Were any servers of any make with “infected drivers” in production environments, whether they faced customers or not?

[12] How is an “infected driver” an accident?

> While there has been no claim that customer data was involved, we take these allegations seriously and we want users to know that we do everything possible to safeguard the personal information they entrust to us.[13] We also want them to know that what Bloomberg is reporting about Apple is inaccurate.[14]

[13] This is not the same as saying “customer data was not exposed.”

[14] “inaccurate” but not “wrong,” “erroneous,” “false,” or “untrue”?

> Apple has always believed in being transparent about the ways we handle and protect data.[15] If there were ever such an event as Bloomberg News has claimed, we would be forthcoming about it and we would work closely with law enforcement.[16] Apple engineers conduct regular and rigorous security screenings to ensure that our systems are safe. We know that security is an endless race and that’s why we constantly fortify our systems against increasingly sophisticated hackers and cybercriminals who want to steal our data.[17]

[15] Tell us about iPhone encryption.

[16] “an event” is not “events”. “Forthcoming” may not mean “public disclosure” or “reveal that we are under non-disclosure agreements.” “Would work closely with law enforcement” is not the same as “working with intelligence community,” or “working with Commerce/Treasury Departments.”

[17] No specific mention of nation-state actors.