Supermicro Hack – Truth or Fiction?

- Bloomberg Businessweek article – October 4, 2018
  - https://www.bloomberg.com/news/features/2018-10-04/the-big-hack-how-china-used-a-tiny-chip-to-infiltrate-america-s-top-companies

Supermicro Hack (2)

- Allegation: Chinese spies planted surveillance chips on motherboards of Supermicro servers
- Found by Amazon in 2015 as part of due diligence in acquisition of Elemental Technologies
  - Video compression software, running on Supermicro servers
  - Key customers include U.S. Dept. of Defense, CIA, NASA, DHS, others
- U.S. investigators determined that chips were inserted during manufacturing process in China, by operatives of People's Liberation Army
- Objective – steal Corporate and U.S. Government secret info.

Supermicro Hack (3)

- Apple also discovered suspicious chips, removed 7,000 Supermicro servers and canceled additional 30,000 server order
- AWS found altered motherboards in data center in China
- Supermicro is based in San Jose, CA
  - Assembly facilities in California, Netherlands & Taiwan
  - Almost all Motherboards are manufactured by contractors in China
  - 900 customers in 100 countries
- Suspect chip functions:
  - Communicate with servers elsewhere on the Internet
  - Alteration of server functions (e.g., bypass passwords, steal encryption keys)

Supermicro Hack (4)

- Not so fast, my friend?
- Fortune website headline October 14, 2008:
- **Cyber Saturday—Doubts Swirl Around Bloomberg's China Chip Hack Report**
  - Fortune notes lack of substantiation since Bloomberg article published
  - Quotes skepticism among security experts
- Developing story – “watch this space”