ICIT | Institute for Critical Infrastructure Technology

The Cybersecurity Think Tank

What we Learned from the Bloomberg-SuperMicro Debate

Industry's Inability to Definitively Prove Supply Chain Security Highlights a Need for Radical Change

December 2018

Authored by:

Parham Eftekhari, Executive Director, Institute for Critical Infrastructure Technology

Drew Spaniel, Lead Researcher, Institute for Critical Infrastructure Technology

What we Learned from the Bloomberg-SuperMicro Debate

Industry's Inability to Definitively Prove Supply Chain Security Highlights a Need for Radical Change

December 2018

The authors would like to thank the following ICIT Fellows for their advisement and expertise around supply chain security. The views expressed in this paper is that of the authors, not that of the Fellows listed below.

- Michael Aisenberg, ICIT Fellow & Principal, Cyber Policy Analyst / Counsel, Center for National Security, MITRE
- Jerry Davis, ICIT Fellow & Vice President and Global Chief Security Officer, Lam Research

Contents

Introduction: Supply Chain Risk is Not New

Supply chain security was a pressing problem long before Bloomberg Businessweek published its article alleging that Chinese threat actors compromised SuperMicro's supply chain. Why are American firms, the media, and the public only now beginning to take notice of the importance of supply chain security when defense, intelligence and other communities have been sounding the alarm for over a decade?

Bloomberg's October assertion that SuperMicro's supply chain might be vulnerable should not have been a bombshell viral report. Supply chains in every commercial sector have been vulnerable for over a decade, and not enough has been done by stakeholders to mitigate the risk of compromise. In order to achieve any measure of progress towards supply chain security, government agencies, private companies, the media, the public, and other stakeholders need to demonstrate through meaningful action that the security of the products employed in our critical infrastructure sectors, businesses, and everyday lives is a top priority.

A History of Ignoring Calls to Action

Since at least 2007 (and most certainly going back even further, had ICIT chosen to focus on the history of supply chain security for this paper), major cybersecurity institutions have been discussing the need for improvements to the security and trust of our critical infrastructure supply chains.

- In June 2007, the U.S. Department of the Navy, Naval Air Systems Command (NAVAIR) asked the Bureau of Industry and Security's (BIS) Office of Technology Evaluation (OTE) to conduct a defense industrial base assessment of counterfeit electronics. A total of 387 companies and organizations, representing all five segments of the U.S. supply chain – original component manufacturers (OCMs), distributors and brokers, circuit board assemblers, prime contractors and subcontractors, and Department of Defense (DOD) agencies – were surveyed about the 2005 to 2008 period. OTE found that 39 percent of the organizations had received electronic components that differed from what was supposed to be included in their systems. Worse, the rate more than doubled from 3,868 incidents in 2005 to 9,356 incidents by 2008. All elements of the supply chain were impacted by counterfeit components [1].
- In 2008, under President Obama, the Comprehensive National Cybersecurity Initiative listed "Develop a multi-pronged approach for global supply chain risk management" as its eleventh initiative. It acknowledged that "Managing this risk will require a greater awareness of the threats, vulnerabilities, and consequences associated with acquisition decisions; the development and employment of tools and resources to technically and operationally mitigate risk across the lifecycle of products (from design through

retirement); the development of new acquisition policies and practices that reflect the complex global marketplace; and partnership with industry to develop and adopt supply chain and risk management standards and best practices. This initiative will enhance Federal Government skills, policies, and processes to provide departments and agencies with a robust toolset to better manage and mitigate supply chain risk at levels commensurate with the criticality of, and risks to, their systems and networks" [2].

- The Armed Forces Communication and Electronics Association Cyber Committee published a 2012 report entitled "Supply Chain Risk Management Awareness" that was intended to "raise awareness of the risks, highlight current issues surrounding supply chain risks, list current initiatives that may further mitigate supply chain risk, and put forth continuing challenges to promote actionable results" [3].

The findings of these (and other) initiatives should have spurred action from congress, and public and private sector organizations to prioritize supply chain security to address the systemic issues identified. As we will discuss in this paper, the community no longer has an excuse to ignore the urgency at which we must address supply chain security.

Two Perspectives to the Bloomberg Supermicro Story

Months after the initial Bloomberg story was published, there are two camps which exist; those who believe Bloomberg reporting at face-value, and those who refute its findings. In the next two sections, we will present short, objective summaries of both perspectives. ICIT is not giving credence to one storyline over the other and is not endorsing any of the information in this section. Our intention is to outline each perspective for the purposes of supporting thoughts and ideas discussed in the remainder of the paper.

Bloomberg Alleges that Miniscule Microchips Could Have Global Impacts

The US-based SuperMicro Computer, Inc. manufactures hardware used in systems belonging to government organizations such as the Department of Defense and CIA as well as private companies such as Amazon and Apple. On October 4, 2018, Bloomberg Business reported that Chinese threat actors had compromised SuperMicro's supply chain and thereby laterally infected nearly 30 US companies, including servers that support government agencies and the cloud [4].

Bloomberg Businessweek asserts that it conducted its investigation over the course of a year and it relied on information from 17 different anonymous sources including "one from a Chinese foreign ministry," and it drew upon research spanning more than three years of investigations. It alleges that China engaged in the systematic, technically sophisticated, resource intensive (compared to malware infections), and precision-targeted campaign that compromised the supply chain of one of the world's largest motherboard and custom hardware

manufacturers in order to engage in clandestine espionage operations against foreign governments and to exfiltrate sensitive data and intellectual property from leading technology firms. It contends that People's Liberation Army agents coerced the Chinese-based subcontractors responsible for the hardware circuitry, to embed advanced surveillance chips, which are about the size of a pencil tip (i.e. thin enough to be embedded between the layers of fiberglass onto which the other components were attached), into the motherboards and components of systems designated for high-value targets.

The access and intelligence gathered from this attack would enable the Chinese government to conduct nearly undetectable precision espionage campaigns against high-value targets in government, finance, technology, healthcare, and other critical sectors across the globe. While the specific capabilities of the embedded chip remain undefined, Bloomberg suggests that the unit is capable of pushing code to the device operating system and communicating with remote adversarial systems [4]. In their words,

> "The implants on SuperMicro hardware manipulated the core operating instructions that tell the server what to do as data move across a motherboard. This happened at a crucial moment, as small bits of the operating system were being stored in the board's temporary memory en route to the server's central processor, the CPU. The implant was placed on the board in a way that allowed it to effectively edit this information queue, injecting its own code or altering the order of the instructions the CPU was meant to follow. Deviously small changes could create disastrous effects" [4].

In layman's terms, the microchips would function as the hardware equivalent to malware; except that the chip would not be detectable to anti-malware or other software defenses. While hardware implanted spyware would be much more difficult to detect and would remain on the victim system longer (potentially indefinitely), it is significantly more expensive and more difficult to deploy [6]. Outside of examining the motherboard and identifying one alien microchip, no larger than a pencil tip, the intrusion would be overwhelmingly difficult to detect. Like sophisticated malware, the devices could allow for code to be injected, facilitate data alteration, act as a backdoor into networked devices, or modify the instructions between the CPU and the operating system [5].

Embattled Tech Giants and the Security Community Dispute Bloomberg's Narrative

Bloomberg Business's story was met with derision and incredulity by the alleged victims, the security community, and many government entities.

- SuperMicro denied all aspects of the publication, stating that said the design complexity makes it practically impossible to insert a functional, unauthorized component onto a

motherboard without it being caught by the checks in its manufacturing and assembly process.

- Amazon refuted Bloomberg's claims that systems were infected and it rebuked sources claiming that it was working with the FBI to investigate hardware infected with the microchips.
- Apple reported that they had repeatedly and consistently contested every aspect of Bloomberg's story during pre-publication verification efforts and that they continue to contest virtually every aspect of the article now [7].
- The United States Department of Homeland Security said it "had no reason to question denials by US technology companies." For its part, the Chinese Ministry of Foreign Affairs stated that any government intrusion into a product supply chain would violate China's commitment to the proposal of the 2011 International Code of Conduct for Information Security.
- Two technology experts named in the piece have publicly withdrawn contributions attributed to them. Joe Grand, the founder of Grand Idea Studio, Inc., claimed in a Twitter post that his quote was given over a year ago and referred to a broad, purely hypothetical attack scenario. In an email read aloud on a podcast on Risky.biz, Hardware Security Resources founder Joe Fitzpatrick commented, "The whole setup doesn't really make sense," the email is quoted as saying. "It just doesn't make sense to spend the time and money to do what you are describing. Are you sure that the person who did the analysis had actual hardware knowledge and understanding?" Fitzpatrick concludes, "I'm incredibly skeptical" [5].

This Debate is Bigger than Bloomberg and SuperMicro

The crux of the debate is that no one can seem to prove or disprove the allegations in the story to the satisfaction of the opposing faction. Most organizations are not keen on hiring researchers to dissect extremely valuable, mission-critical, and sometimes custom systems based on reports attributed to anonymous sources; especially considering that in order to find and remove the hypothetical microchip, researchers would have to test and remove minute elements from the circuit board. Metaphorically, this is akin to manually tearing apart the roof of your house because the rumor on the street is that a stranger believed that houses in the neighborhood had leaks in their roofs. Conversely, if adversaries are precision-targeting firms, then Apple or Amazon investigating a sample of the overall systems may not reveal the alleged espionage campaign if the percentage of systems actually infected is small relative to the overall number of systems.

However, despite the inability to prove or disprove the allegations, Bloomberg's story may have contributed to a forty-one percent drop in SuperMicro's stock in the following week [8]. The

financial impact demonstrates the power that the market can have when confidence in a firm's ability to deliver secure products falters. Apple may have lost as much as $18 billion in market share as a result of the publication of the story; although, given Apple's market share, the loss only amounts to about a 2% loss in stock value [9]. Additionally, the firms named in the piece, SuperMicro, Amazon, Apple, etc. suffered reputational harm as the story went viral. Meanwhile, Bloomberg experienced challenges to its credibility and potential reputational harm as the alleged victims and the security community critically scrutinized its story and its decision to publish cybersecurity information based on anonymous sources [8].

At the time of this writing, Bloomberg Business has not retracted its story despite vocal calls from Apple, Amazon, SuperMicro, and other firms [7] [10]. As an objective, non-partisan cybersecurity think-tank, ICIT is not taking a side in the debate. Instead, ICIT urges critical infrastructure communities to take an objective step back and learn invaluable lessons from the uproar and impact caused by the publication of a single article. The significant underlying problem is not whether a supply chain, providing sensitive, mission-critical components, was compromised by foreign adversaries. The real problem is that no mechanisms are in place to confirm beyond a doubt that vital components were not compromised.

Our inability to trust or verify the integrity and security of the hardware, software, and firmware components of vital systems is a glaring weakness in national security in the broad sense and more specifically it is a failing on the part of the Information Security community. Sensationalism aside, supply chain verification and integrity mechanisms are severely lacking. The widespread problem is not limited to advanced persistent threats, sophisticated malware, or technologically advanced microchips. It is not limited to components manufactured in a specific nation or threat actors originating from a specific region. Hardware faults, counterfeit components, and other supply chain compromises are not unheard of in the critical infrastructure sectors; however, they should be. Incidents, where IoT botnets seize control of millions of devices due to credentials embedded in the firmware, should not happen. Incidents in which systems' hardware or software are infected during the manufacturing process at the behest of governments or insider threats should not happen. Incidents, where an update from a trusted source can be poisoned with malware and disseminated to millions of consumers, should not happen. Multiple instances of each of the aforementioned scenarios have occurred within the past few years. Supply chain insecurity is an epidemic that can no longer go unaddressed..

We are All at Fault. We All Must Do More.

Manufacturers have failed to develop and implement adequate security-by-design throughout the development lifecycle of their devices in part because buyers have not exerted market

pressures to prioritize such action and in part, because regulatory bodies have not required the application of demonstrative security controls throughout supply chain processes.

Supply chain security is not easy for B2B consumers either. Due to constraints such as profit margins, deadlines, and similar factors, many either ignore security concerns or knowingly settle for inferior products in order to progress their business.

Few security professionals possess the skillsets necessary to detect, understand, or reverse engineer malicious hardware components that were tailored to masquerade as legitimate elements within custom systems. Expecting a rapid shift in the education of the security community to be able to do so is unrealistic and would ultimately prove unfruitful because the specialist would have to be intimately familiar with the design of each subsystem and they would have to inspect each manufactured element. Instead, compensating controls should be implemented to allow for the confirmation that the integrity of the product was not compromised at any stage of the supply chain and verification measures should ensure that the received components are exactly those purchased by the consumer.

In their article, Bloomberg states that the alleged espionage microchips are so dangerous because “This stuff is at the cutting edge of the cutting edge, and there is no easy technological solution.” Nevertheless, by Bloomberg’s account, the attacks required people posing as representatives of SuperMicro or the Chinese government to approach the managers of at least four subcontractor factories that built SuperMicro motherboards. The representatives would offer bribes in exchange for the managers making changes to the boards’ official designs. If bribes didn’t work, the representatives threatened managers with inspections that could shut down the factories. Eventually, the factory managers allegedly agreed to modify the board designs to add the minuscule malicious hardware [6].

Regardless of whether or not Bloomberg’s account is factually accurate, ICIT contends that attempting to mitigate emerging hyper-evolving threats using existing technologies alone is inadequate. Even after extensive audits, penetration testing, and research, B2B consumers can never be certain that a device or equipment is secure. In addition to deploying layered security strategies to detect and prevent exploitation of vulnerabilities on networks and devices, buyers should also be leveraging their buying power to pressure manufacturers into transparently and comprehensively ensuring that equipment & devices cannot become compromised during production. Compensating controls can be used to ensure the holistic security of devices throughout development and manufacture by preventing malicious insiders, by verifying the integrity of manufacturers, contractors, and subcontractors, and by implementing layered security solutions.

What Can We Do?

Prioritize Security

Financial losses, reputational harm, and angry diatribes on both sides of the Bloomberg-SuperMicro debate occurred because the organizations involved at large did not have mechanisms in place to immediately confirm or dismiss the allegations presented in the publication with empirical evidence. As per MITRE's Deliver Uncompromised proposal and NIST's SP 800-160, transparent and verifiable mechanisms to verify the security and integrity of the allegedly infected devices could have immediately resolved the debate prior to denationalization, global panic, and the realization of cascading impacts. Manufacturers can prevent future incidents by including layered security at each stage of product development. For their part, consumers should ensure that their networks adhere to sector-specific best practices, such as NIST SP 800-53.

When it Comes to Suppliers, Trust, but Verify

Governments and other stakeholders can ensure that purchased devices are more secure by evaluating purchase decisions based on security, by auditing purchased products to ensure their integrity, and by leveraging market forces against firms that refuse to secure their supply chain. Consumers have the power to incite meaningful change, if only they chose to use it. Researching the firms designing their products to understand their processes, demanding the inclusion of security, and verifying that the manufacturer will protect the privacy of the client should be the foundation of decisions to purchase and deploy technologies.

Firms should calculate their risk appetite and the risk tolerance of the device, and they should be cognizant that by relying on a service or product, they are staking their sensitive information and intellectual property on its inherent security. Newly acquired equipment should be tested and audited in isolation prior to introduction to the network. IT departments should regularly patch and update systems as well as monitor for emerging threats specific to their sector and systems. Nascent technologies should be implemented only after extensive review by the widespread security community [5].

Conclusion: Supply Chain Risk is a Developing Epidemic, But We Can Mitigate It

Though the viral story publicized and sensationalized the issue, Supply chain security is a developing epidemic that is not limited to the debate between Bloomberg Businessweek and SuperMicro, Apple, and Amazon. Security-by-design as expressed in NIST's SP 800-160 and integrity verification models such as MITRE's Deliver Uncompromised can help to course-correct the technology communities to begin to mitigate exploitable supply chain

vulnerabilities. Information security depends on market pressures, public-private collaborations (such as between government, the media, and tech firms), and on transparency in the security and integrity compensating controls employed during production.

Supply chain security is complex. It will not be solved overnight, let alone within the next decade. It will not be solved through the release of exposes or heated press releases. Progress will require the unification of researchers, manufacturers, engineers, governments, and the public against the immeasurable collective of digital adversaries. Prioritizing security, verifying the integrity of products and being judicial with trust, and practicing holistic cyber-hygiene are good first steps to securing supply chains in the future; however, to achieve any lasting positive impact, stakeholders need to care about more than fear or anger. They need to care about the layered security of their products.

Sources:

[1] "DEFENSE INDUSTRIAL BASE ASSESSMENT: COUNTERFEIT ELECTRONICS", 2010. [Online]. Available: https://www.bis.doc.gov/index.php/forms-documents/technology-evaluation/37-defense-industrial-base-assessment-of-counterfeit-electronics-2010/file. [Accessed: 16- Nov- 2018].

[2] "The Comprehensive National Cybersecurity Initiative", White House, 2008. [Online]. Available: https://fas.org/irp/eprint/cnci.pdf. [Accessed: 16- Nov- 2018].

[3] J. Filsinger, B. Fast, D. Wolf, J. Payne and M. Anderson, "Supply Chain Risk Management Awareness", Afcea.org, 2012. [Online]. Available: https://www.afcea.org/committees/cyber/documents/Supplychain.pdf. [Accessed: 16- Nov- 2018].

[4] "The Big Hack: How China Used a Tiny Chip to Infiltrate U.S. Companies", Bloomberg.com, 2018. [Online]. Available: https://www.bloomberg.com/news/features/2018-10-04/the-big-hack-how-china-used-a-tiny-chip-to-infiltrate-america-s-top-companies. [Accessed: 16- Nov- 2018].

[5] A. McNeil, "Bloomberg blunder highlights supply chain risks - Malwarebytes Labs", Malwarebytes Labs, 2018. [Online]. Available: https://blog.malwarebytes.com/cybercrime/2018/10/bloomberg-blunder-supply-chain-risks/. [Accessed: 16- Nov- 2018].

[6] D. Goodin, "If Supermicro boards were so bug-ridden, why would hackers ever need implants?", ArsTechnica.com, 2018. [Online]. Available: https://arstechnica.com/information-technology/2018/10/SuperMicro-boards-were-so-bug-ridden-why-would-hackers-ever-need-implants/. [Accessed: 16- Nov- 2018].

[7] J. Paczkowski and J. Bernstein, "Apple CEO Tim Cook Is Calling For Bloomberg To Retract Its Chinese Spy Chip Story", Buzzfeednews.com, 2018. [Online]. Available: https://www.buzzfeednews.com/article/johnpaczkowski/apple-tim-cook-bloomberg-retraction. [Accessed: 16- Nov- 2018].

[8] T. Poletti, "New cloud over Super Micro adds to its dark relationship with Wall Street", MarketWatch, 2018. [Online]. Available: https://www.marketwatch.com/story/new-cloud-over-super-micro-adds-to-its-dark-relationship-with-wall-street-2018-10-04. [Accessed: 16- Nov- 2018].

[9] A. Root, "Apple Suppliers Took an $18 Billion Stock Hit After the China Hacking Report", Barrons.com, 2018. [Online]. Available: https://www.barrons.com/articles/apple-suppliers-

take-17-billion-stock-hit-after-china-hacking-allegations-1538676503?mod=mktw. [Accessed: 16- Nov- 2018].

[10] S. Rai, "Super Micro to review hardware for malicious chips", U.S., 2018. [Online]. Available: https://www.reuters.com/article/us-china-cyber-super-micro-comp/super-micro-to-review-hardware-for-malicious-chips-idUSKCN1MW1GK. [Accessed: 16- Nov- 2018].

ICIT Contact Information

Phone: 202-600-7250

E-mail: http://icitech.org/contactus/

ICIT Websites & Social Media

www.icitech.org

https://twitter.com/ICITorg

https://www.linkedin.com/company/institute-for-critical-infrastructure-technology-icit-