SILICON VALLEY MESSAGE FOR THE DIGITAL WORLD: YOU ARE F*CKED!

- NEVER USE A SILICON VALLEY HARDWARE ITEM!

Chinese spy chips said to be found in hardware used by APPLE, AMAZON...

Feds warn of new hacking spree...

FACEBOOKGOOGLE Join Forces on AI Tech...

Russian Military Officers Indicted for Cyber Attacks...

Explosive Report Details Chinese Infiltration Of Apple, Amazon And The CIA

Profile picture for user Tyler Durden

by Tyler Durden
Thu, 10/04/2018 - 08:14

0
SHARES

One week ago, President Trump stood up at a meeting of the United Nations Security Council and accused China of attempting to tamper with US elections - mimicking some of the same allegations that had first been levied against Russia nearly two years prior. In his speech, Trump claimed that China was working to undermine Republicans, and even the president himself, warning that "it's not just Russia, it's China and Russia." While the media largely shrugged off this proclamation as more presidential bombast probably inspired by the burgeoning US-China trade beef, the administration continued to insist that it was taking a harder line against Chinese efforts to subvert American companies to aide the Communist Party's sprawling intelligence apparatus. As if to underline Trump's point, the FBI had arrested a Taiwanese national in Chicago the day before Trump's speech, accusing the 27-year-old suspect of trying to help China flip eight defense contractors who could have provided crucial intelligence on sensitive defense-related technology.

But in a game-changing report published Thursday morning, Bloomberg Businessweek exposed a sprawling multi-year investigation into China's infiltration of US corporate and defense infrastructure. **Most notably, it confirmed that, in addition to efforts designed to sway US elections, China's intelligence community orchestrated a pervasive infiltration of servers used to power everything from MRI machines to the drones used by the CIA and army.** They accomplished this using a tiny microchip no bigger than a grain of rice.

BBG published the report just hours before Vice President Mike Pence was expected to "string together a narrative of Chinese aggression" during a speech at the Hudson Institute in Washington. According to excerpts leaked to the New York Times, his speech was expected to focus on examples of China's "aggressive moves against American warships, of predatory behavior against their neighbors, and of a sophisticated influence campaign to tilt the midterms and 2020 elections against President Trump". **His speech is also expected to focus on how China leverages debt and its capital markets to force foreign governments to submit to its will (something that has happened in Bangladesh and the Czech Republic.**

China

But while those narratives are certainly important, they pale in comparison to Bloomberg's revelations, which reported on an ongoing government investigation into China's use of a "tiny microchip" that found its way into servers that were widely used throughout the US military and intelligence infrastructure, from Navy warships to DoD server farms. The probe began three years ago after the US intelligence agencies were tipped off by Amazon. And three years later, it remains ongoing.

> ***Nested on the servers’ motherboards, the testers found a tiny microchip, not much bigger than a grain of rice, that wasn’t part of the boards’ original design. Amazon reported the discovery to U.S. authorities, sending a shudder through the intelligence community. Elemental’s servers could be found in Department of Defense data centers, the CIA’s drone operations, and the onboard networks of Navy warships. And Elemental was just one of hundreds of Supermicro customers.***
>
> *During the ensuing top-secret probe, which remains open more than three years later,* ***investigators determined that the chips allowed the attackers to create a stealth doorway into any network that included the altered machines.*** *Multiple people familiar with the matter say investigators found that the chips had been*

> *inserted at factories run by manufacturing subcontractors in China.*

With those two paragraphs, Bloomberg has succeeded in shifting the prevailing narrative away from Russia and toward China. Or, as Pence is expected to state in Thursday's speech (via NYT) **"as a senior career member of our intelligence community recently told me, what the Russians are doing pales in comparison to what China is doing across this country."**

The story begins with a Silicon Valley startup called Elemental. Founded in 2006 by three engineers who brilliantly anticipated that broadcasters would soon be searching for a way to adapt their programming for streaming over the Internet, and on mobile devices like smartphones, Elemental went about building a "dream team" of coders who designed software to adapt the super-fast graphics chips being designed for video gaming to stream video instead. The company then loaded this software on to special, custom-built servers emblazoned with its logo. These servers then sold for as much as $100,000 a pop - a markup of roughly 70%. In 2009, the company received its first contract with US defense and intelligence contractors, and even received an investment from a CIA-backed venture fund.

- **Elemental also started working with American spy agencies. In 2009 the company announced a development partnership with In-Q-Tel Inc., the CIA’s investment arm, a deal that paved the way for Elemental servers to be used in national security missions across the U.S. government.** Public documents, including the company’s own promotional materials, show that the

> servers have been used inside Department of Defense data centers to process drone and surveillance-camera footage, on Navy warships to transmit feeds of airborne missions, and inside government buildings to enable secure videoconferencing. NASA, both houses of Congress, and the Department of Homeland Security have also been customers. This portfolio made Elemental a target for foreign adversaries.

Like many other companies, Elementals' servers utilized motherboards built by Supermicro, which dominates the market for motherboards used in special-purpose computers. It was here, at Supermicro, where the government believes - according to Bloomberg's sources - that the infiltration began. Before it came to dominate the global market for computer motherboards, Supermicro had humble beginnings. A Taiwanese engineer and his wife founded the company in 1993, at a time when Silicon Valley was embracing outsourcing. It attracted clients early on with the promise of infinite customization, employing a massive team of engineers to make sure it could accommodate its clients' every need. Customers also appreciated that, while Supermicro's motherboards were assembled in China or Taiwan, its engineers were based in Silicon Valley. But the company's workforce featured one characteristic that made it uniquely attractive to China: **A sizable portion of its engineers were native Mandarin speakers. One of Bloomberg's sources said the government is still investigating whether spies were embedded within Supermicro or other US companies).**

But however it was done, these tiny microchips somehow found their way into Supermicro's products. Bloomberg provided a step-by-step guide detailing how it believes that happened.

- A Chinese military unit designed and manufactured microchips as small as a sharpened pencil tip. Some of the chips were built to look like signal conditioning couplers, and they incorporated memory, networking capability, and sufficient processing power for an attack.
- The microchips were inserted at Chinese factories that supplied Supermicro, one of the world’s biggest sellers of server motherboards.
- The compromised motherboards were built into servers assembled by Supermicro.
- The sabotaged servers made their way inside data centers operated by dozens of companies.
- When a server was installed and switched on, the microchip altered the operating system’s core so it could accept modifications. The chip could also contact computers controlled by the attackers in search of further instructions and code.

In espionage circles, infiltrating computer hardware - especially to the degree that the Chinese did - is extremely difficult to pull off. And doing it at the nation-state level would be akin to "a unicorn jumping over a rainbow," as one of BBG's anonymous sources put it. But China's dominance of the market for PCs and mobile phones allows it a massive advantage.

> *One country in particular has an advantage executing this kind of attack: China, which by some estimates makes 75 percent of the world’s mobile phones and 90 percent of its PCs. Still, to actually accomplish a seeding attack would mean developing a deep understanding of a product’s design, manipulating components at the factory, and*

> *ensuring that the doctored devices made it through the global logistics chain to the desired loc*__*ation - a feat akin to throwing a stick in the Yangtze River upstream from Shanghai and ensuring that it washes ashore in Seattle. "Having a well-done, nation-state-level hardware implant surface would be like witnessing a unicorn jumping over a rainbow,"*__ *says Joe Grand, a hardware hacker and the founder of Grand Idea Studio Inc.* ***"Hardware is just so far off the radar, it’s almost treated like black magic."***
>
> *But that’s just what U.S. investigators found: The chips had been inserted during the manufacturing process, two officials say, by operatives from a unit of the People’s Liberation Army. In Supermicro, China’s spies appear to have found a perfect conduit for what U.S. officials now describe as the most significant supply chain attack known to have been carried out against American companies.*

Some more details from the report are summarized below:

The government found that the infiltration extended to nearly 30 companies, including Amazon and Apple.

- One official says investigators found that it eventually affected almost 30 companies, including a major bank, government contractors, and the world’s most valuable company, Apple Inc. **Apple was an important Supermicro customer and had planned to order more than 30,000 of its servers in two years for a new global network of data centers. Three senior insiders at Apple say that in the summer of 2015, it, too, found malicious chips on Supermicro motherboards.** Apple severed ties with Supermicro the following year, for what it described as unrelated reasons.

Both Amazon and Apple denied having knowledge of the infiltration (Amazon eventually acquired Elemental and integrated it into its Amazon Prime Video service). Meanwhile, the Chinese government issued a conspicuous non-denial denial.

- In emailed statements, Amazon (which announced its acquisition of Elemental in September 2015), Apple, and Supermicro disputed summaries of Bloomberg Businessweek’s reporting. "It’s untrue that AWS knew about a supply chain compromise, an issue with malicious chips, or hardware modifications when acquiring Elemental," Amazon wrote. "On this we can be very clear: Apple has never found malicious chips, 'hardware manipulations’ or vulnerabilities purposely planted in any server," Apple wrote. **"We remain unaware of any such investigation," wrote a spokesman for Supermicro, Perry Hayes. The Chinese government didn’t directly address questions about manipulation of Supermicro servers, issuing a statement that read, in part, "Supply chain safety in cyberspace is an issue of common concern, and China is also a victim."** The FBI and the Office of the Director of National

Intelligence, representing the CIA and NSA, declined to comment.

Bloomberg based its story on interviews with 17 anonymous sources, including 6 former government intelligence officials. One official told BBG that China's long-term goal was "long-term access" to sensitive government secrets.

- In all, 17 people confirmed the manipulation of Supermicro’s hardware and other elements of the attacks. The sources were granted anonymity because of the sensitive, and in some cases classified, nature of the information.
- **The companies’ denials are countered by six current and former senior national security officials, who - in conversations that began during the Obama administration and continued under the Trump administration - detailed the discovery of the chips and the government’s investigation.** One of those officials and two people inside AWS provided extensive information on how the attack played out at Elemental and Amazon; the official and one of the insiders also described Amazon’s cooperation with the government investigation. In addition to the three Apple insiders, four of the six U.S. officials confirmed that Apple was a victim. In all, 17 people confirmed the manipulation of Supermicro’s hardware and other elements of the attacks. The sources were granted anonymity because of the sensitive, and in some cases classified, nature of the information.

One government official says China’s goal was long-term access to high-value corporate secrets and sensitive government networks. No consumer data is known to have been stolen.

Notably, this revelation provides even more support to the Trump administration's insistence that the trade war with China was based on national security concerns. The hope is that more US companies will shift production of sensitive components back to the US.

- **The ramifications of the attack continue to play out.** The Trump administration has made computer and networking hardware, including motherboards, a focus of its latest round of trade sanctions against China, and White House officials have made it clear they think companies will begin shifting their supply chains to other countries as a result. Such a shift might assuage officials who have been warning for years about the security of the supply chain—even though they’ve never disclosed a major reason for their concerns.

As one government official reminds us, ***the extent of this attack cannot be understated.***

- With more than 900 customers in 100 countries by 2015, Supermicro offered inroads to a bountiful collection of sensitive targets. "Think of Supermicro as the Microsoft of the hardware world," says a former U.S. intelligence official who’s studied Supermicro and its business model. **"Attacking Supermicro motherboards is like attacking Windows. It’s like attacking the whole world."**

But perhaps the most galling aspect of this whole scandal is that ***the Obama Administration should have seen it coming.***

- Well before evidence of the attack surfaced inside the networks of U.S. companies, American intelligence sources were reporting that China’s spies had plans to introduce malicious microchips into the supply chain. **The sources weren’t specific, according to a person familiar with the information they provided, and millions of motherboards are shipped into the U.S. annually. But in the first half of 2014, a different person briefed on high-level discussions says, intelligence officials went to the White House with something more concrete: China’s military was preparing to insert the chips into Supermicro motherboards bound for U.S. companies.**

And thanks to Obama having dropped the ball, China managed to pull off the most expansive infiltration of the global supply chain ever discovered by US intelligence.

- But that’s just what U.S. investigators found: **The chips had been inserted during the manufacturing process, two officials say, by operatives from a unit of the People’s Liberation Army. In Supermicro, China’s spies appear to have found a perfect conduit for what U.S. officials now describe as the most significant supply chain attack known to have been carried out against American companies.**

The inconspicuous-looking chips were disguised to look like regular components but they helped China open doors that "other hackers could go through" meaning China could potentially manipulate the systems being infiltrated (as a reminder, these chips were found in servers used in the US drone program).

- The chips on Elemental servers were designed to be as inconspicuous as possible, according to one person who saw a detailed report prepared for Amazon by its third-party security contractor, as well as a second person who saw digital photos and X-ray images of the chips incorporated into a later report prepared by Amazon's security team. Gray or off-white in color, they looked more like signal conditioning couplers, another common motherboard component, than microchips, and so they were unlikely to be detectable without specialized equipment. Depending on the board model, the chips varied slightly in size, suggesting that the attackers had supplied different factories with different batches.

- Officials familiar with the investigation say the primary role of implants such as these is to open doors that other attackers can go through. "Hardware attacks are about access," as one former senior official puts it. **In simplified terms, the implants on Supermicro hardware manipulated the core operating instructions that tell the server what to do as data move across a motherboard, two people familiar with the chips' operation say. 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.**
- Since the implants were small, the amount of code they contained was small as well. But they were capable of doing two very important things: telling the device to communicate with one of several anonymous computers elsewhere on the internet that were loaded with more complex code; and preparing the device's operating system to accept this new code. <strong>The illicit chips could do all this because they were connected to the baseboard management controller, a kind of

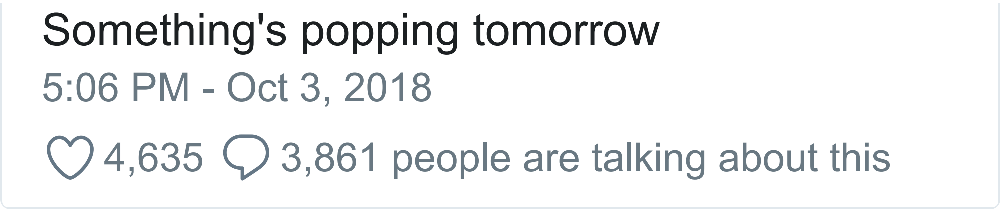
superchip that administrators use to remotely log in to problematic servers, giving them access to the most sensitive code even on machines that have crashed or are turned off.

- This system could let the attackers alter how the device functioned, line by line, however they wanted, leaving no one the wiser. To understand the power that would give them, take this hypothetical example: Somewhere in the Linux operating system, which runs in many servers, is code that authorizes a user by verifying a typed password against a stored encrypted one. **An implanted chip can alter part of that code so the server won’t check for a password—and presto! A secure machine is open to any and all users.**

Shortly after the report was published, the US Department of Defense has scheduled a national-security related press conference for 9:30 am ET on Thursday. It didn't reveal the subject of the briefing, but the timing is certainly suspicious...

View image on Twitter

Chuck Ross
@ChuckRossDC



Something's popping tomorrow

5:06 PM - Oct 3, 2018

♡ 4,635 🗨 3,861 people are talking about this

But regardless of what is said on Thursday, one thing probably won't change: Expect to hear a lot less about Russia, and a lot more about China as the deep state's interference myopic focus on the former shifts to the latter. As Kevin Warsh framed the question during a Thursday interview with CNBC where he asked "are we at the beginning of a 20-year Cold War?" **in response to a question about curbing China's influence - both economically and defensively. We imagine we'll be hearing a lot more about the breach from senior US officials, including both the vice president and the president himself, in the very near future.**