Forging What's Next
Preserving Nature
By Trading It
Learn More
Sponsored by Bloomberg

Businessweek / Features

The Big Hack: How China Used a Tiny Chip to Infiltrate U.S. Companies

The attack by Chinese spies reached almost 30 U.S. companies, including Amazon and Apple, by compromising America's technology supply chain, according to extensive interviews with government and corporate sources.

Jordan Robertson and Michael Riley
October 4, 2018, 3:00 AM MDT

Illustration: Sarah Grillo for Bloomberg Businessweek

Read in this story
Hardware Hack
Spy Chips
Supermicro
Apple
Amazon
Aftermath

Illustration: Alexandra Mazzarella for; Z. Edel Bulawan; Bloomberg Businessweek; Photo: Tuan Tran for Bloomberg Businessweek

In 2015, Amazon.com Inc. began quietly evaluating a startup called Elemental Technologies Inc. about a month before it was ready for acquisition of its streaming video service, known today as Amazon Prime Video. Based in Portland, Ore., Elemental made software for compressing massive video files and formatting them for different devices. Its technology had helped stream the Olympic Games and presidential inaugurations, and it was being used by the U.S. Special Ops Group on the Central Intelligence Agency. Elemental's national security contracts weren't the main reason for the proposed acquisition. Its work with Amazon's government businesses, such as the highly secure cloud that Amazon Web Services (AWS) was building for the U.S.

To help with due diligence, AWS, which was overseeing the acquisition, hired a U.S. cybersecurity firm to examine Elemental Elemental's security, including its use pieces familiar with the process. The firm pass uncovered troubling issues, prompting AWS to ask for more time to investigate. The firm discovered security servers that customers installed in their networks to handle the video compression. These servers were assembled for Elemental by Super Micro Computer Inc., a San Jose-based company (commonly known as Supermicro) that's also one of the world's biggest suppliers of motherboards. The firm's hardware teardowns found tiny chips and components that are not the manufacturer's doing. Some chips and small. In late spring of 2015, Elemental's staff boosted up several servers and sent them to Ontario, Canada, for the third-party security company to test, the process was

Second-tier servers' motherboards, the sensors that control power, were much bigger than a grain of rice, that wasn't part of the boards' original design. Amazon reported the discovery to U.S. officials, sending a shudder through the intelligence community. Investigators soon found the Elemental of Defense data centers, the CIA's drone operations, and the unbiased networks of Navy warships. Supermicro was at fault, just one of hundreds of Supermicro customers.

During the ensuing top-secret probe, which remains open more than three years later, investigators determined that China's People's Liberation Army had contracted a month discovery 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.

This attack was something greater than the software-based incidents the world has grown accustomed to seeing. Hardware hacks are rarer, harder to pull off, and more dangerous. Intelligence officials say the kind of long-term, stealth access that spy agencies are willing to invest millions of dollars and many years to get.

There are two ways for spies to alter the guts of computer equipment. One, known as interdiction, consists of manipulating devices as they in in transit from manufacturer to customer. This tactic, dubbed Tailored Access Operations, is a specialty of elite hacking unit inside the National Security Agency known as Tailored Operations. The other method involves sending changes from the very beginning.

One country in particular has an advantage executing this kind of attack. China, which has overtaken Indian TV processor of the world's mobile phones and 90 percent of its PCs, 5G, or actually anything else. Supermicro's Taiwan-based factory, for understanding of a product's design, manipulating components at the factory, and ensuring that the doctored devices made it through the production process and into the hands of U.S. buyers. Doing so, throwing a rock in the Yangtze River upstream from Shanghai and ensuring that it washes ashore in Seattle. "Having a well-done custom-made hardware implant surface would be the winnowing a unicorn jumping over a stadium," says Joe Grand, a hardware hacker who has helped the National Security Agency. "Hardware is just so far off the radar, it's almost treated like black magic."

Illustration: Alexandra Mazzarella for Bloomberg Businessweek

But that's just what U.S. investigators found. The chips had been inserted during the manufacturing process, two officials say, by operatives of the People's Liberation Army. According to investigators, 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 carried out against American companies.

One officials now investigators found that it eventually affected almost 30 companies, including a major bank, government contractors, and two of the most iconic U.S. technology firms. 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. These servers totaled at Apple site in the summer of 2015, it, too, found malicious chips on Supermicro motherboards. Apple's security team discovered the following year, for what is described as unrelated reasons.

Illustration: Alexandra Mazzarella for Bloomberg Businessweek

But that's just what U.S. investigators found. The chips had been inserted during the manufacturing process, two officials say, by operatives of the People's Liberation Army. According to investigators, 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 carried out against American companies.

One officials now investigators found that it eventually affected almost 30 companies, including a major bank, government contractors, and two of the most iconic U.S. technology firms. 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. These servers totaled at Apple site in the summer of 2015, it, too, found malicious chips on Supermicro motherboards. Apple's security team discovered the following year, for what is described as unrelated reasons.

Illustration: Alexandra Mazzarella for Bloomberg Businessweek

It entailed numerous, tenacious hitchcock announced in acquisition of Elemental Technologies Inc. Amazon Web Services Inc. Elemental summarizes of Elemental Business Intelligence's reporting. "It's unusual that AWS knew about a supply-chain compromise, an issue with malicious chips, or hardware implants on its underlying equipment." Elemental." Amazon wrote. "On this we can be very clear. Apple has stated that it has found no such malicious chips or other vulnerabilities purposely planted in any server." Apple wrote. "We remain assurance of any such investigation," wrote a spokesman for Supermicro, Perry Hayes. The Chinese government didn't directly address questions about manipulation of Supermicro's servers, saying in a statement that it "has never, ever, ever, ever

to the factories.

The investigators concluded that this intricate scheme was the work of a People's Liberation Army unit specializing in hardware attacks, according to two people briefed on its activities. The existence of this group has never been revealed before, but one official says, "We've been tracking these guys for longer than we'd like to admit." The unit is believed to focus on high-priority targets, including advanced commercial technology and the computers of rival militaries. In past attacks, it targeted the designs for high-performance computer chips and computing systems of large U.S. internet providers.

advertisement

Provided details of *Businessweek*'s reporting, China's Ministry of Foreign Affairs sent a statement that said "China is a resolute defender of cybersecurity." The ministry added that in 2011, China proposed international guarantees on hardware security along with other members of the Shanghai Cooperation Organization, a regional security body. The statement concluded, "We hope parties make less gratuitous accusations and suspicions but conduct more constructive talk and collaboration so that we can work together in building a peaceful, safe, open, cooperative and orderly cyberspace."

The Supermicro attack was on another order entirely from earlier episodes attributed to the PLA. It threatened to have reached a dizzying array of end users, with some vital ones in the mix. Apple, for its part, has used Supermicro hardware in its data centers sporadically for years, but the relationship intensified after 2013, when Apple acquired a startup called Topsy Labs, which created superfast technology for indexing and searching vast troves of internet content. By 2014, the startup was put to work building small data centers in or near major global cities. This project, known internally as Ledbelly, was designed to make the search function for Apple's voice assistant, Siri, faster, according to the three senior Apple insiders.

Documents seen by *Businessweek* show that in 2014, Apple planned to order more than 6,000 Supermicro servers for installation in 17 locations, including Amsterdam, Chicago, Hong Kong, Los Angeles, New York, San Jose, Singapore, and Tokyo, plus 4,000 servers for its existing North Carolina and Oregon data centers. Those orders were supposed to double, to 20,000, by 2015. Ledbelly made Apple an important Supermicro customer at the exact same time the PLA was found to be manipulating the vendor's hardware.

Project delays and early performance problems meant that around 7,000 Supermicro servers were humming in Apple's network by the time the company's security team found the added chips. Because Apple didn't, according to a U.S. official, provide government investigators with access to its facilities or the tampered hardware, the extent of the attack there remained outside their view.

American investigators eventually figured out who else had been hit. Since the implanted chips were designed to ping anonymous computers on the internet for further instructions, operatives could hack those computers to identify others who'd been affected. Although the investigators couldn't be sure they'd found every victim, a person familiar with the U.S. probe says they ultimately concluded that the number was almost 30 companies.

That left the question of whom to notify and how. U.S. officials had been warning for years that hardware made by two Chinese telecommunications giants, Huawei Corp. and ZTE Corp., was subject to Chinese government manipulation. (Both Huawei and ZTE have said no such tampering has occurred.) But a similar public alert regarding a U.S. company was out of the question. Instead, officials reached out to a small number of important Supermicro customers. One executive of a large web-hosting company says the message he took away from the exchange was clear: Supermicro's hardware couldn't be trusted. "That's been the nudge to everyone—get that crap out," the person says.

Amazon, for its part, began acquisition talks with an Elemental competitor, but according to one person familiar with Amazon's deliberations, it reversed course in the summer of 2015 after learning that Elemental's board was nearing a deal with another buyer. Amazon announced its acquisition of Elemental in September 2015, in a transaction whose value one person familiar with the deal places at $350 million. Multiple sources say that Amazon intended to move Elemental's software to AWS's cloud, whose chips, motherboards, and servers are typically designed in-house and built by factories that Amazon contracts from directly.

A notable exception was AWS's data centers inside China, which were filled with Supermicro-built servers, according to two people with knowledge of AWS's operations there. Mindful of the Elemental findings, Amazon's security team conducted its own investigation into AWS's Beijing facilities and found altered motherboards there as well, including more sophisticated designs than they'd previously encountered. In one case, the malicious chips were thin enough that they'd been embedded between the layers of fiberglass onto which the other components were attached, according to one person who saw pictures of the chips. That generation of chips was smaller than a sharpened pencil tip, the person says. (Amazon denies that AWS knew of servers found in China containing malicious chips.)

China has long been known to monitor banks, manufacturers, and ordinary citizens on its own soil, and the main customers of AWS's China cloud were domestic companies or foreign entities with operations there. Still, the fact that the country appeared to be conducting those operations inside Amazon's cloud presented the company with a Gordian knot. Its security team determined that it would be difficult to quietly remove the equipment and that, even if they could devise a way, doing so would alert the attackers that the chips had been found, according to a person familiar with the company's probe. Instead, the team developed a method of monitoring the chips. In the ensuing months, they detected brief check-in communications between the attackers and the sabotaged servers but didn't see any attempts to remove data. That likely meant either that the attackers were saving the chips for a later operation or that they'd infiltrated other parts of the network before the monitoring began. Neither possibility was reassuring.

When in 2016 the Chinese government was about to pass a new cybersecurity law—seen by many outside the country as a pretext to give authorities wider access to sensitive data—Amazon decided to act, the person familiar with the company's probe says. In August it transferred operational control of its Beijing data center to its local partner, Beijing Sinnet, a move the companies said was needed to comply with the incoming law. The following November, Amazon sold the entire infrastructure to Beijing Sinnet for about $300 million. The person familiar with Amazon's probe casts the sale as a choice to "hack off the diseased limb."

As for Apple, one of the three senior insiders says that in the summer of 2015, a few weeks after it identified the malicious chips, the company started removing all Supermicro servers from its data centers, a process Apple referred to internally as "going to zero." Every Supermicro server, all 7,000 or so, was replaced in a matter of weeks, the senior insider says. (Apple denies that any servers were removed.) In 2016, Apple informed Supermicro that it was severing their relationship entirely—a decision a spokesman for Apple ascribed in response to *Businessweek*'s questions to an unrelated and relatively minor security incident.

That August, Supermicro's CEO, Liang, revealed that the company had lost two major customers. Although he didn't name them, one was later identified in news reports as Apple. He blamed competition, but his explanation was vague. "When customers asked for lower price, our people did not respond quickly enough," he said on a conference call with analysts. Hayes, the Supermicro spokesman, says the company has never been notified of the existence of malicious chips on its motherboards by either customers or U.S. law enforcement.

Concurrent with the illicit chips' discovery in 2015 and the unfolding investigation, Supermicro has been plagued by an accounting problem, which the company characterizes as an issue related to the timing of certain revenue recognition. After missing two deadlines to file quarterly and annual reports required by regulators, Supermicro was delisted from the Nasdaq on Aug. 23 of this year. It marked an extraordinary stumble for a company whose annual revenue had risen sharply in the previous four years, from a reported $1.5 billion in 2014 to a projected $3.2 billion this year.

One Friday in late September 2015, President Barack Obama and Chinese President Xi Jinping appeared together at the White House for an hourlong press conference headlined by a landmark deal on cybersecurity. After months of negotiations, the U.S. had extracted from China a grand promise: It would no longer support the theft by hackers of U.S. intellectual property to benefit Chinese companies. Left out of those pronouncements, according to a person familiar with discussions among senior officials across the U.S. government, was the White House's deep concern that China was willing to offer this concession because it was already developing far more advanced and surreptitious forms of hacking founded on its near monopoly of the technology supply chain.

In the weeks after the agreement was announced, the U.S. government quietly raised the alarm with several dozen tech executives and investors at a small, invite-only meeting in McLean, Va., organized by the Pentagon. According to someone who was present, Defense Department officials briefed the technologies on a recent attack and asked them to think about creating commercial products that could detect hardware implants. Attendees weren't told the name of the hardware maker involved, but it was clear to at least some in the room that it was Supermicro, the person says.

The problem under discussion wasn't just technological. It spoke to decisions made decades ago to send advanced production work to Southeast Asia. In the intervening years, low-cost Chinese manufacturing had come to underpin the business models of many of America's largest technology companies. Early on, Apple, for instance, made many of its most sophisticated electronics domestically. Then in 1992, it closed a state-of-the-art plant for motherboard and computer assembly in Fremont, Calif., and sent much of that work overseas.

Over the decades, the security of the supply chain became an article of faith despite repeated warnings by Western officials. A belief formed that China was unlikely to jeopardize its position as workshop to the world by letting its spies meddle in its factories. That left the decision about where to build commercial systems resting largely on where capacity was greatest and cheapest. "You end up with a classic Satan's bargain," one former U.S. official says. "You can have less supply than you want and guarantee it's secure, or you can have the supply you need, but there will be risk. Every organization has accepted the second proposition."

In the three years since the briefing in McLean, no commercially viable way to detect attacks like the one on Supermicro's motherboards has emerged—or has looked likely to emerge. Few companies have the resources of Apple and Amazon, and it took some luck even for them to spot the problem. "This stuff is at the cutting edge of the cutting edge, and there is no easy technological solution," one of the people present in McLean says. "You have to invest in things that the world wants. You cannot invest in things that the world is not ready to accept yet."

Bloomberg LP has been a Supermicro customer. According to a Bloomberg LP spokesperson, the company has found no evidence to suggest that it has been affected by the hardware issues raised in the article.

advertisement

Ad

In this article

AAPL	AMZN	GBSN:SGD	MSFT
APPLE INC	AMAZON.COM INC	BLOOMBERG BUSINESSWEEK	MICROSOFT CC
145.42 USD	153.67 USD	Private Company	229.25 USD
▲ +0.33 +0.24%	▼ -0.89 -0.58%		▼ -4.88 -2.13%

Have a confidential tip for our reporters? Get in touch.

Before it's here, it's on the Bloomberg Terminal

©2022 Bloomberg L.P. All Rights Reserved