The Long Hack: How China Exploited a U.S. Tech Supplier

For years, U.S. investigators found tampering in products made by Super Micro Computer Inc. The company says it was never told. Neither was the public.

By Jordan Robertson and Michael Riley
February 12, 2021 at 5:00 AM

In 2010, the U.S. Department of Defense found thousands of its computer servers sending military network data to China—the result of code hidden in chips that handled the machines' startup process.

In 2014, Intel Corp. discovered that an elite Chinese hacking group breached its network through a single server that downloaded malware from a supplier's update site.

And in 2015, the Federal Bureau of Investigation warned multiple companies that Chinese operatives had concealed an extra chip loaded with backdoor code in one manufacturer's servers.

Each of these distinct attacks had two things in common: China and Super Micro Computer Inc., a computer hardware maker in San Jose, California. They shared one other trait; U.S. spymasters discovered the manipulations but kept them largely secret as they tried to counter each one and learn more about China's capabilities.

▲ Super Micro Computer Inc. headquarters in San Jose. Photographer: David Paul Morris/Bloomberg

China's exploitation of products made by Supermicro, as the U.S. company is known, has been under federal scrutiny for much of the past decade, according to 14 former law enforcement and intelligence officials familiar with the matter. That included an FBI counterintelligence investigation that began around 2012, when agents started monitoring the communications of a small group of Supermicro workers, using warrants obtained under the Foreign Intelligence Surveillance Act, or FISA, according to five of the

Whether that probe continues is unknown, as is a full account of its findings. But as recently as 2018, the FBI enlisted private-sector help in analyzing Supermicro equipment that contained added chips, according to an adviser to two security firms that did the work.

The Supermicro saga demonstrates a widespread risk in global supply chains, said Jay Tabb, a former senior FBI official who agreed to speak generally about China's interference with the company's products.

"Supermicro is the perfect illustration of how susceptible American companies are to potential nefarious tampering of any products they choose to have manufactured in China," said Tabb, who was the executive assistant director of the FBI's national security branch from 2018 until he retired in January 2020. "It's an example of the worst-case scenario if you don't have complete supervision over where your devices are manufactured."

▲ Jay Tabb Photographer: Chona Kasinger/Bloomberg

aware that China is doing this," he said. "And Silicon Valley in particular needs to quit pretending that this isn't happening."

Neither Supermicro nor any of its employees has been accused of wrongdoing, and former U.S. officials who provided information for this story emphasized that the company itself has not been the target of any counterintelligence investigation.

In response to detailed questions, Supermicro said it has "never been contacted by the U.S. government, or by any of our customers, about these alleged investigations." The company said Bloomberg had assembled "a mishmash of disparate and inaccurate allegations" that "draws farfetched conclusions." Federal agencies, including those described in this article as conducting investigations, still buy Supermicro products, the company said. And it noted that this account of a counterintelligence investigation lacks full details, including the probe's outcome or whether it's ongoing. The full response is published here.

"Supermicro is an American success story and the security and integrity of our products is a top priority," the company said.

A spokesperson for the Chinese Foreign Ministry called accounts of these attacks "attempts to discredit China and Chinese enterprises" and accused U.S. officials of "making things up to hype up the 'China threat.'"

"China has never and will never require enterprises or individuals to collect or provide data, information and intelligence from other countries for the Chinese government by installing 'back doors,'" the spokesperson said in a written statement.

This story is drawn from interviews with more than 50 people from law enforcement, the military, Congress, intelligence agencies and the private sector. Most asked not to be named in order to share sensitive information. Some details were confirmed in corporate documents Bloomberg News

Bloomberg Businessweek first reported on China's meddling with Supermicro products in October 2018, in an article that focused on accounts of added malicious chips found on server motherboards in 2015. That story said Apple Inc. and Amazon.com Inc. had discovered the chips on equipment they'd purchased. Supermicro, Apple and Amazon publicly called for a retraction. U.S. government officials also disputed the article.

With additional reporting, it's now clear that the *Businessweek* report captured only part of a larger chain of events in which U.S. officials first suspected, then investigated, monitored and tried to manage China's repeated manipulation of Supermicro's products.

Throughout, government officials kept their findings from the general public. Supermicro itself wasn't told about the FBI's counterintelligence investigation, according to three former U.S. officials.

The secrecy lifted occasionally, as the bureau and other government agencies warned a select group of companies and sought help from outside experts.

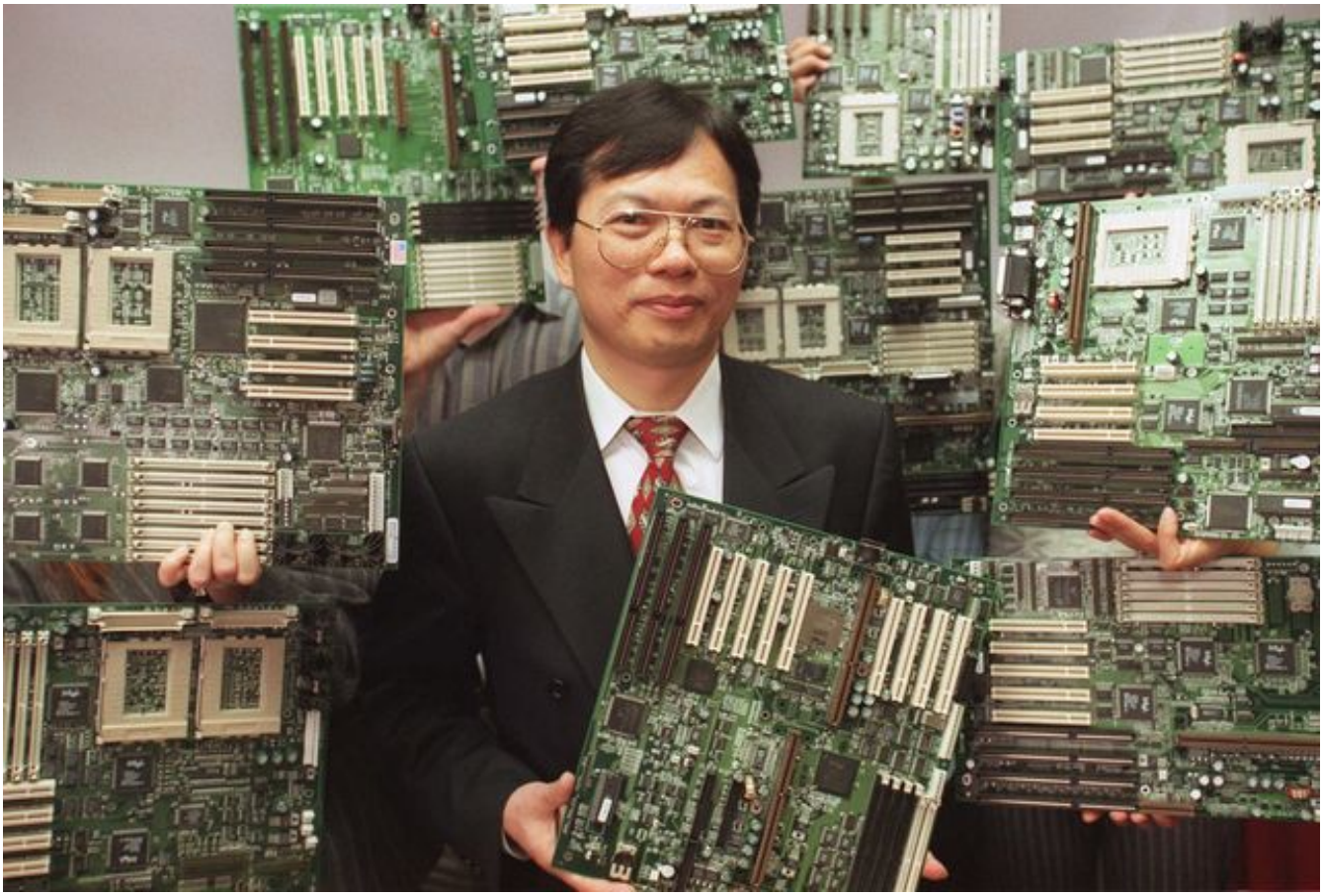
"In early 2018, two security companies that I advise were briefed by the FBI's counterintelligence division investigating this discovery of added malicious chips on Supermicro's motherboards," said Mike Janke, a former Navy SEAL who co-founded DataTribe, a venture capital firm. "These two companies were subsequently involved in the government investigation, where they used advanced hardware forensics on the actual tampered Supermicro boards to validate the existence of the added malicious chips."

Janke, whose firm has incubated startups with former members of the U.S. intelligence community, said the two companies are not allowed to speak publicly about that work but they did share details from their analysis with

“This is real,” Janke said, “and the government knows it.”

‘Unauthorized Intrusions’

Supermicro, founded in 1993 by Taiwanese immigrant Charles Liang, was built to take advantage of global supply chains. Many of its motherboards—the clusters of chips and circuitry that run modern electronics—were manufactured in China by contractors, then assembled into servers in the U.S. and elsewhere.



▲ Charles Liang in 1998. Photographer: Jim Gensheimer/The Mercury News/Getty Images

The company, which earned $3.3 billion in revenue last year, has seen its computer gear become pervasive in the cloud computing era. Its motherboards sit in products ranging from medical imaging scanners to cybersecurity devices. Supermicro declined to address questions about whether it relies on contract manufacturers in China today.

In an unusual disclosure for any public company, Supermicro told investors in May 2019 that its own computer networks had been breached over multiple years. “We experienced unauthorized intrusions into our network between 2011 and 2018,” the company wrote. “None of these intrusions, individually or in the aggregate, has had a material adverse effect on our business, operations, or products.” The company didn’t respond to requests for additional details about those intrusions.

Federal officials had concerns about China’s dominant role in global electronics manufacturing before Supermicro’s products drew sustained U.S. government scrutiny.

Another Pentagon supplier that received attention was China’s Lenovo Group Ltd. In 2008, U.S. investigators found that military units in Iraq were using Lenovo laptops in which the hardware had been altered. The discovery surfaced later in little-noticed testimony during a U.S. criminal case—a rare public description of a Chinese hardware hack.

“A large amount of Lenovo laptops were sold to the U.S. military that had a chip encrypted on the motherboard that would record all the data that was being inputted into that laptop and send it back to China,” Lee Chieffalo, who managed a Marine network operations center near Fallujah, Iraq, testified during that 2010 case. “That was a huge security breach. We don’t have any idea how much data they got, but we had to take all those systems off the network.”

Three former U.S. officials confirmed Chieffalo’s description of an added chip on Lenovo motherboards. The episode was a warning to the U.S. government about altered hardware, they said.

Lenovo was unaware of the testimony and the U.S. military hasn’t told the company of any security concerns about its products, spokeswoman Charlotte West said in an email. U.S. officials conducted “an extensive probe into Lenovo's background and trustworthiness” while reviewing its 2014

acquisitions of businesses from IBM and Google, West said. Both purchases were approved.

“As there have been no reports of any problems, we have no way to assess the allegations you cite or whether security concerns may have been triggered by third-party interference,” West said.

▲ Lenovo assembly line in Beijing in July 2008. Photographer: Tony Law/Redux

After the discovery in 2008, the Defense Department quietly blocked Lenovo hardware from some sensitive projects, the three U.S. officials said, but the company was not removed from a list of approved vendors to the Pentagon.

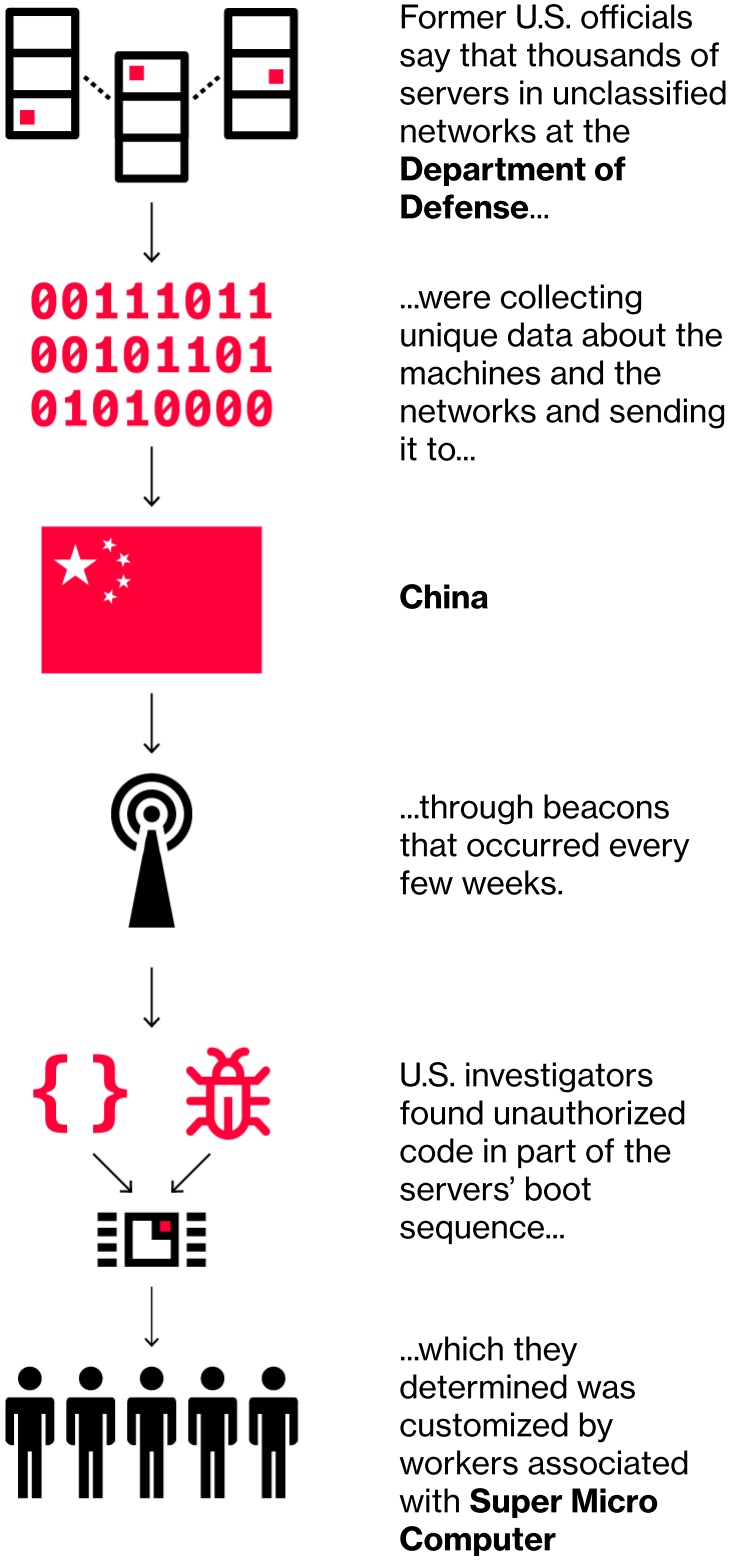
report that cited “known cybersecurity risks.”

The Defense Department needs a better process for evaluating technology purchases and imposing bans when necessary, according to the report.

Pentagon Attack

Around early 2010, a Pentagon security team noticed unusual behavior in Supermicro servers in its unclassified networks.

Implant in the Startup Process



The machines turned out to be loaded with unauthorized instructions directing each one to secretly copy data about itself and its network and send that information to China, according to six former senior officials who

implant in thousands of servers, one official said; another described it as "ubiquitous."

Investigators attributed the rogue code to China's intelligence agencies, the officials said. A former senior Pentagon official said there was "no ambiguity" in that attribution.

There was no evidence that the implant siphoned any details on military operations. But the attackers did get something of value: data that amounted to a partial map of the Defense Department's unclassified networks. Analysts were also concerned that the implant—which the attackers had taken pains to hide—might be a digital weapon that could shut down those systems during a conflict.

Without a fix on China's ultimate purpose, U.S. leaders decided in 2013 to keep the discovery secret and let the attack run, according to three officials who were informed of the plan. Keith Alexander, then-director of the National Security Agency, played a central role in the decision, the officials said. The Pentagon devised undetectable countermeasures to protect its networks, two of them said.

▲ Keith Alexander in 2013. Photographer: Andrew Harrer/Bloomberg

The moves allowed America's own spies to begin gathering intelligence on China's plans without alerting Beijing, the two officials said.

A spokesman for Alexander referred questions to the NSA. The agency declined to comment beyond a one-sentence statement: "NSA cannot confirm that this incident—or the subsequent response actions described—ever occurred."

A senior White House official declined to comment on a detailed description of the information in this story. "We will not have a comment on this specific issue," the official said in an emailed statement. "As a general matter, the President has made a commitment that his administration will conduct a wide-ranging supply chain review on a variety of goods and sectors to identify critical national security risks. We'll have more details on that review when we are ready to share."

Other federal agencies, including the Office of the Director of National Intelligence, the Department of Homeland Security and the FBI, declined to comment for this story.

A Defense Department spokeswoman said officials generally don't comment on investigations, intelligence matters or particular suppliers. In response to questions about the Pentagon's 2010 investigation, one official said the government has sought to safeguard its supply chain.

"When confronting adversarial effort, the Department takes many steps to continually work to exclude products or companies that pose a threat to our national security," said Ellen Lord, who served as the under secretary of defense for acquisition and sustainment before she stepped down on Jan. 20. She didn't name Supermicro or any other company.

▲ Ellen Lord, under secretary of defense for acquisition and sustainment, testifies during a Senate hearing on supply-chain integrity on Oct. 1. Photographer: Tom Williams/CQ-Roll Call/Getty Images

As they investigated the Pentagon's data centers, government officials took discreet steps to try to prevent the use of Supermicro products in sensitive

national-security networks—even though the company remained on public lists of approved suppliers.

Adrian Gardner, who was chief information officer for NASA's Goddard Space Flight Center in Greenbelt, Maryland, said he learned of the intelligence community's concerns about Supermicro products before he left NASA in 2013, during a review of Goddard's computer systems.

Gardner declined to discuss exactly what he was told or whether NASA removed any hardware. But he said the message was clear: "The U.S. government must use every control at its disposal to ensure that it does not deploy equipment from Supermicro within the system boundary of high-valued assets and sensitive networks," he said.

U.S. agencies continued to purchase Supermicro products. News releases from the company show that NASA's Goddard Center bought some for an unclassified network devoted to climate research in 2017. And last year, Lawrence Livermore National Laboratory, which does classified work on nuclear weapons, bought Supermicro equipment for unclassified research into Covid-19.

Customized Code

As military experts investigated the Pentagon breach, they determined that the malicious instructions guiding the Pentagon's servers were hidden in the machines' basic input-output system, or BIOS, part of any computer that tells it what to do at startup.

Two people with direct knowledge said the manipulation combined two pieces of code: The first was embedded in instructions that manage the order of the startup and can't be easily erased or updated. That code fetched additional instructions that were tucked into the BIOS chip's unused memory, where they were unlikely to be found even by security-conscious

Manufacturers like Supermicro typically license most of their BIOS code from third parties. But government experts determined that part of the implant resided in code customized by workers associated with Supermicro, according to six former U.S. officials briefed on the findings.

Investigators examined the BIOS code in Defense Department servers made by other vendors and found no similar issues. And they discovered the same unusual code in Supermicro servers made by different factories at different times, suggesting the implant was introduced in the design phase.

Overall, the findings pointed to infiltration of Supermicro's BIOS engineering by China's intelligence agencies, the six officials said.

By 2012, the FBI had opened a counterintelligence probe, and agents in the San Francisco field office used FISA warrants to monitor the communications of several people connected to Supermicro, according to five former U.S. officials.

Three of the officials said the FBI had evidence suggesting that the company had been infiltrated by people working—wittingly or unwittingly—for China. They declined to detail that evidence.

The FISA surveillance included individuals in a position to alter the company's technology, and didn't focus on senior executives, the officials said.

It's not clear how long that monitoring continued. The Justice Department hasn't acknowledged the probe or announced any charges linked to it. Counterintelligence investigations aim to monitor and disrupt foreign intelligence operations on U.S. soil and rarely result in criminal cases.

By 2014, investigators across the U.S. government were looking for any additional forms of manipulation—anything they might have missed, as one

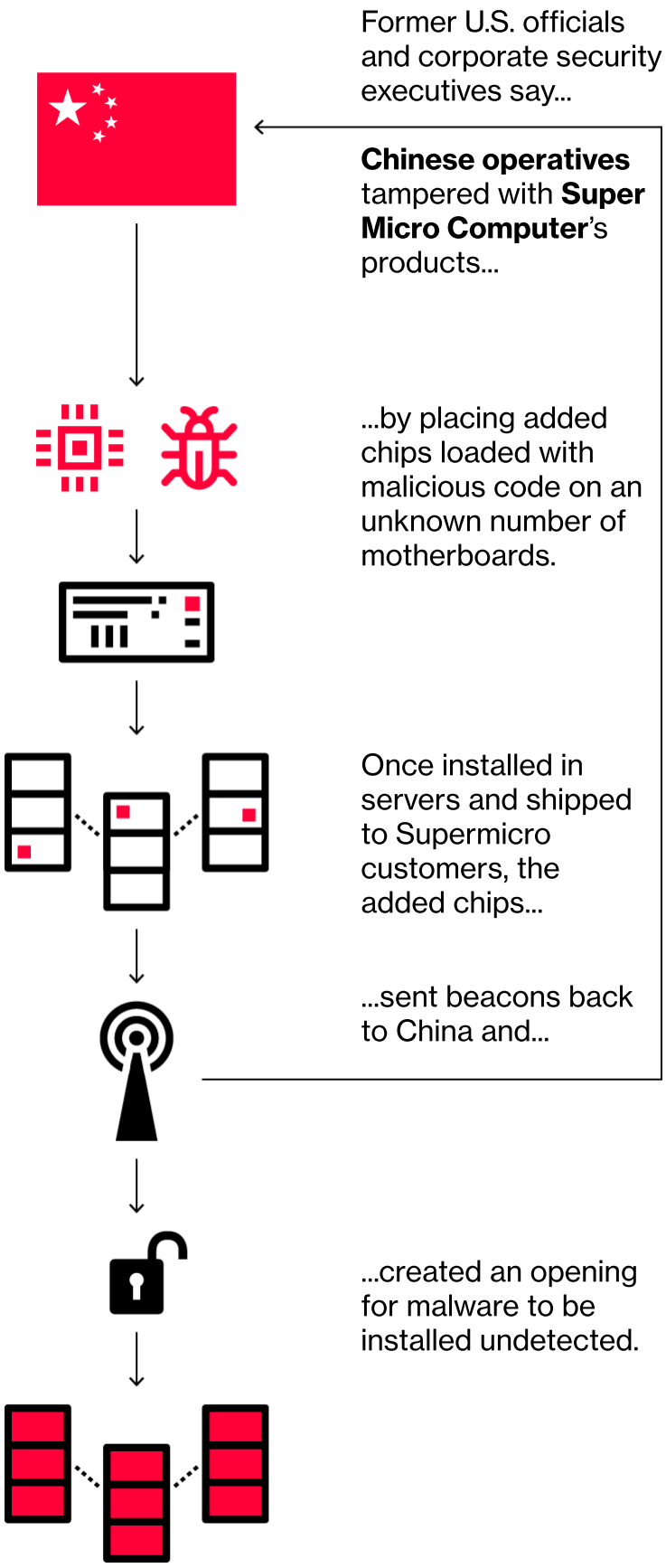
provided by American intelligence agencies, the FBI found another type of altered equipment: malicious chips added to Supermicro motherboards.

Warnings Delivered

Government experts regarded the use of these devices as a significant advance in China's hardware-hacking capabilities, according to seven former American officials who were briefed about them between 2014 and 2017. The chips injected only small amounts of code into the machines, opening a door for attackers, the officials said.

Small batches of motherboards with the added chips were detected over time, and many Supermicro products didn't include them, two of the officials said.

Added Chips With Malicious Code



Alarmed by the devices' sophistication, officials opted to warn a small number of potential targets in briefings that identified Supermicro by name. Executives from 10 companies and one large municipal utility told Bloomberg News that they'd received such warnings. While most executives asked not to be named to discuss sensitive cybersecurity matters, some agreed to go on the record.

"This was espionage on the board itself," said Mukul Kumar, who said he received one such warning during an unclassified briefing in 2015 when he was the chief security officer for Altera Corp., a chip designer in San Jose. "There was a chip on the board that was not supposed to be there that was calling home—not to Supermicro but to China."

Altera, which was purchased by Intel in December 2015, didn't use Supermicro products, Kumar said, so the company determined it wasn't at risk.

After his in-person briefing, Kumar said, he learned that peers at two other Silicon Valley semiconductor companies had already received the same FBI warning.

"The agents said it was not a one-off case; they said this was impacting thousands of servers," Kumar said of his own discussion with FBI agents.

It remains unclear how many companies were affected by the added-chip attack. Bloomberg's 2018 story cited one official who put the number at almost 30, but no customer has acknowledged finding malicious chips on Supermicro motherboards.

Several executives who received warnings said the information contained too few details about how to find any rogue chips. Two former senior officials said technical details were kept classified.

Supermicro motherboards by officials from the U.S. Air Force. Quinn was working for a company that was a potential bidder for Air Force contracts, and the officials wanted to ensure that any work would not include Supermicro equipment, he said. Bloomberg agreed not to specify when Quinn received the briefing or identify the company he was working for at the time.

"This wasn't a case of a guy stealing a board and soldering a chip on in his hotel room; it was architected onto the final device," Quinn said, recalling details provided by Air Force officials. The chip "was blended into the trace on a multilayered board," he said.

"The attackers knew how that board was designed so it would pass" quality assurance tests, Quinn said.

An Air Force spokesman said in an email that Supermicro equipment hasn't been excluded from USAF contracts under any public legal authority. In general, he said, the Defense Department has non-public options for managing supply-chain risks in contracts for national security systems.

In its written response to questions, Supermicro said that no customer or government agency has ever informed the company about the discovery of malicious chips in its equipment. It also said it has "never found any malicious chips, even after engaging a third-party security firm to conduct an independent investigation on our products." The company didn't respond to a question about who chose the samples that were investigated.

After Bloomberg reported on the added-chip threat in October 2018, officials for the U.S. Department of Homeland Security, the FBI, the Office of the Director of National Intelligence and the NSA made public statements either discounting the report's validity or saying they had no knowledge of

Bloomberg's report and was unable to corroborate it; the agency said last month that it stands by those comments.

Alerts about added chips weren't limited to the private sector. Former chief information officers at four U.S. agencies told Bloomberg they took part in briefings delivered by the Defense Department between 2015 and 2017 about added chips on Supermicro motherboards.

And the FBI was examining samples of manipulated Supermicro motherboards as recently as 2018, according to Janke, the adviser to two companies that assisted with the analysis.

Darren Mott, who oversaw counterintelligence investigations in the bureau's Huntsville, Alabama, satellite office, said a well-placed FBI colleague described key details about the added chips for him in October 2018.

"What I was told was there was an additional little component on the Supermicro motherboards that was not supposed to be there," said Mott, who has since retired. He emphasized that the information was shared in an unclassified setting. "The FBI knew the activity was being conducted by China, knew it was concerning, and alerted certain entities about it."

Mott said that at the time, he advised companies that had asked him about the chips to take the issue seriously.

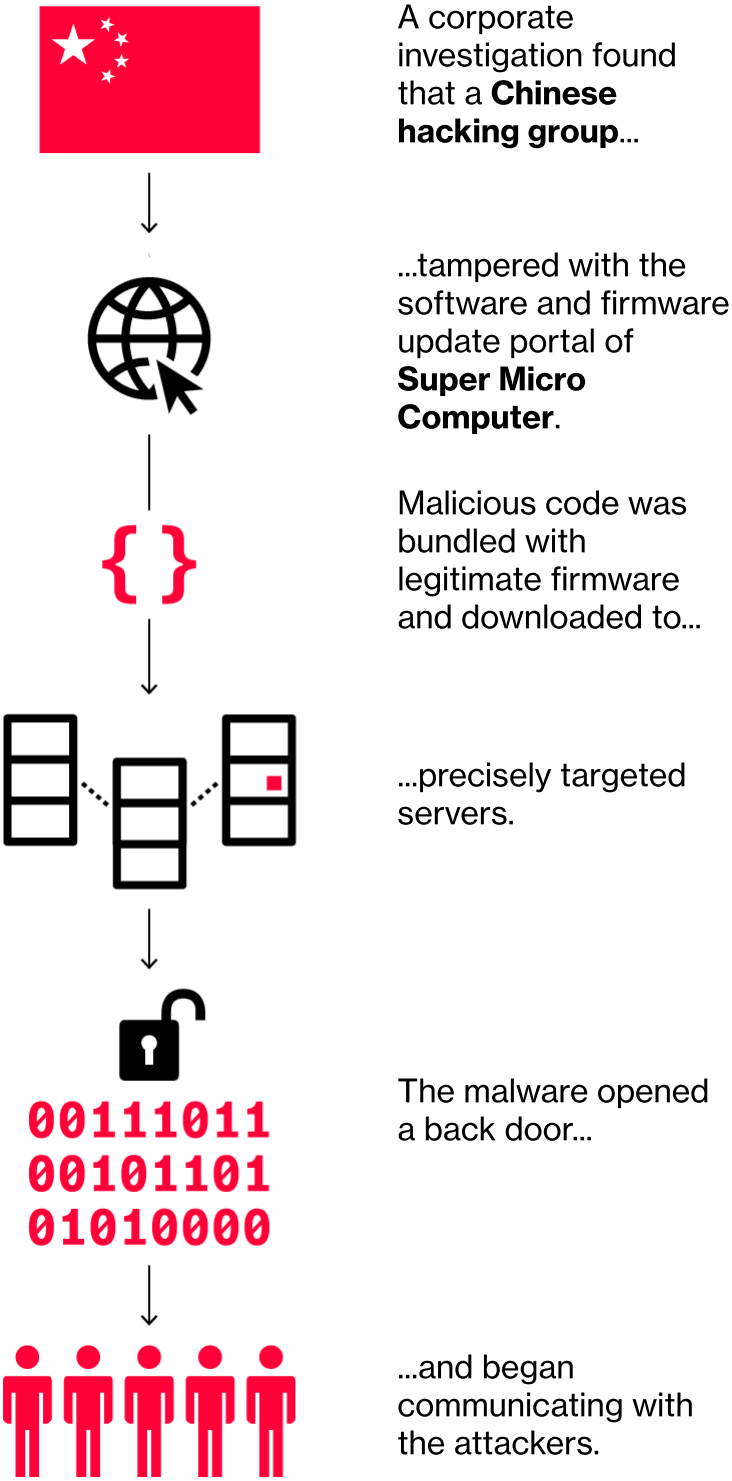
Altered Updates

Corporate investigators uncovered yet another way that Chinese hackers were exploiting Supermicro products. In 2014, executives at Intel traced a security breach in their network to a seemingly routine firmware update downloaded from Supermicro's website.

Intel security executives concluded that an elite Chinese hacking group

gathering of tech industry peers in 2015. Two participants agreed to share details of the presentation.

Malware Sent With an Update



In response to questions about the incident, an Intel spokeswoman said it was caught early and caused no data loss.

“In 2014, Intel IT identified and quickly addressed an issue found in non-Intel software on two systems in a contained part of our network,” spokeswoman Tara Smith said. “There was no impact to our network or data.” She declined to elaborate.

Intel’s presentation focused on the identity of the attackers and their use of a trusted supplier’s update site, according to people who saw the slideshow. A contact in the U.S. intelligence community alerted the company to the breach, according to a person familiar with the matter. The tip helped Intel investigators determine that the attackers were from a state-sponsored group known as APT 17.

APT 17 specializes in complex supply-chain attacks, and it often hits multiple targets to reach its intended victims, according to cybersecurity firms including Symantec and FireEye. In 2012, the group hacked the cybersecurity firm Bit9 in order to get to defense contractors protected by Bit9’s products.

Intel’s investigators found that a Supermicro server began communicating with APT 17 shortly after receiving a firmware patch from an update website that Supermicro had set up for customers. The firmware itself hadn’t been tampered with; the malware arrived as part of a ZIP file downloaded directly from the site, according to accounts of Intel’s presentation.

This delivery mechanism is similar to the one used in the recent SolarWinds hack, in which Russians allegedly targeted government agencies and private companies through software updates. But there was a key difference: In Intel’s case, the malware initially turned up in just one of the firm’s thousands of servers—and then in just one other a few months later. Intel’s investigators concluded that the attackers could target specific machines, making detection much less likely. By contrast, malicious code went to as

Intel executives told Supermicro about the attack shortly after it occurred, according to descriptions of the company's presentation.

Supermicro didn't respond to detailed questions about the incident, but said: "Intel raised a question we were not able to verify, but out of an abundance of caution, we promptly took steps to address." The two companies continue to do extensive amounts of business with each other.

Breaches involving Supermicro's update site continued after the Intel episode, according to two consultants who participated in corporate investigations and asked not to be named.

In incidents at two non-U.S. companies, one in 2015 and the other in 2018, attackers infected a single Supermicro server through the update site, according to a person who consulted on both cases. The companies were involved in the steel industry, according to the person, who declined to identify them, citing non-disclosure agreements. The chief suspect in the intrusions was China, the person said.

In 2018, a major U.S. contract manufacturer found malicious code in a BIOS update from the Supermicro site, according to a consultant who participated in that probe. The consultant declined to share the manufacturer's name. Bloomberg reviewed portions of a report on the investigation.

It's unclear whether the three companies informed Supermicro about their issues with the update site, and Supermicro didn't respond to questions about them.

Today, with the SolarWinds hack still under investigation, national-security concerns about the technology supply chain have erupted into U.S. politics.

▲ Frank Figliuzzi Photographer: Cheney Orr/Bloomberg

"Supermicro's tale of woe is a chilling wake-up call for the industry," said Frank Figliuzzi, who was the FBI's assistant director for counterintelligence until 2012. Figliuzzi declined to address specifics, but agreed to speak publicly about the implications of Supermicro's history with Chinese tampering.

"If you think this story has been about only one company, you're missing the point," he said. "This is a 'don't let this happen to you' moment for anyone in the tech sector supply chain."

–With assistance from Jennifer Jacobs

Editors: John Voskuhl, Robert Blau and Otis Bilodeau
Graphics: Christopher Cannon