EVERY PHONE AND WEB SERVICE IS NOW HACKE

New Evidence of Hacked Supermicro Hardware Found U.S. Telecom

Discovery shows China continues to sabotage critical technology compone bound for America

By Jordan Robertson and Michael Riley

What Is Known So Far About China's Cyber Attack on the U.S.

SHARE THIS ARTICLE

Share

Tweet

Post

Email

In this article

700
TENCENT
293.80 HKD
-5.20 -1.74%

SMCI
SUPER MICRO COMP
12.94 USD
-1.81 -12.27%

AMZN
AMAZON.COM INC
1,877.86 USD
+13.44 +0.72%

AAPL

A major U.S. telecommunications company discovered manipulated hardware from Super Micro Computer Inc. in its network and removed it in August, fresh evidence of tampering in China of critical technology components bound for the U.S., according to a security expert working for the telecom company.

The security expert, Yossi Appleboum, provided documents, analysis and other evidence of the discovery following the publication of an investigative report in Bloomberg Businessweek that detailed how China's intelligence services had ordered subcontractors to plant malicious chips in Supermicro server motherboards over a two-year period ending in 2015.

APPLE INC
225.22 USD
+1.45 +0.65%

T
AT&T INC
33.57 USD
-0.04 -0.13%

Yossi Appleboum
Source: Yossi Appleboum

Appleboum previously worked in the technology unit of the Israeli Army Intelligence Corps and is now co-chief executive officer of Sepio Systems in Gaithersburg, Maryland. His firm specializes in hardware security and was hired to scan several large data centers belonging to the telecommunications company. Bloomberg is not identifying the company due to Appleboum's nondisclosure agreement with the client. Unusual communications from a Supermicro server and a subsequent physical inspection revealed an implant built into the server's Ethernet connector, a component that's used to attach network cables to the computer, Appleboum said.

The executive said he has seen similar manipulations of different vendors' computer hardware made by contractors in China, not just products from Supermicro. "Supermicro is a victim -- so is everyone else," he said. Appleboum said his concern is that there are countless points in the supply chain in China where manipulations can be introduced, and deducing them can in many cases be impossible. "That's the problem with the Chinese supply chain," he said.

Supermicro, based in San Jose, California, gave this statement: "The security of our customers and the integrity of our products are core to our business and our company values. We take care to secure the integrity of our products throughout the manufacturing process, and supply chain security is an important topic of discussion for our industry. We still have no knowledge of any unauthorized components and have not been informed by any customer that such components have been found. We are dismayed that Bloomberg would give us only limited information, no documentation, and half a day to respond to these new allegations."

Bloomberg News first contacted Supermicro for comment on this story on Monday at 9:23 a.m. Eastern time and gave the company 24 hours to respond.

Supermicro said after the earlier story that it “strongly refutes” reports that servers it sold to customers contained malicious microchips. China's embassy in Washington did not return a request for comment Monday. In response to the earlier Bloomberg Businessweek investigation, China’s Ministry of Foreign Affairs didn’t directly address questions about the manipulation of Supermicro servers but said supply chain security is “an issue of common concern, and China is also a victim.”

Supermicro shares plunged 41 percent last Thursday, the most since it became a public company in 2007, following the Bloomberg Businessweek revelations about the hacked servers. They fell as much as 27 percent on Tuesday after the latest story.

The more recent manipulation is different from the one described in the Bloomberg Businessweek report last week, but it shares key characteristics: They’re both designed to give attackers invisible access to data on a computer network in which the server is installed; and the alterations were found to have been made at the factory as the motherboard was being produced by a Supermicro subcontractor in China.

Based on his inspection of the device, Appleboum determined that the telecom company's server was modified at the factory where it was manufactured. He said that he was told by Western intelligence contacts that the device was made at a Supermicro subcontractor factory in Guangzhou, a port city in southeastern China. Guangzhou is 90 miles upstream from Shenzhen, dubbed the `Silicon Valley of Hardware,’ and home to giants such as Tencent Holdings Ltd. and Huawei Technologies Co. Ltd.

The tampered hardware was found in a facility that had large numbers of Supermicro servers, and the telecommunication company's technicians couldn’t answer what kind of data was pulsing through the

infected one, said Appleboum, who accompanied them for a visual inspection of the machine. It's not clear if the telecommunications company contacted the FBI about the discovery. An FBI spokeswoman declined to comment on whether it was aware of the finding.

AT&T Inc. spokesman Fletcher Cook said, “These devices are not part of our network, and we are not affected.” Verizon Communications Inc. had no immediate comment on whether the malicious component was found in one of its servers. T-Mobile U.S. Inc. and Sprint Corp.didn’t respond to requests for comment.

Sepio Systems’ board includes Chairman Tamir Pardo, former director of the Israeli Mossad, the national defense agency of Israel, and its advisory board includes Robert Bigman, former chief information security officer of the U.S. Central Intelligence Agency.

U.S. communications networks are an important target of foreign intelligence agencies, because data from millions of mobile phones, computers, and other devices pass through their systems. Hardware implants are key tools used to create covert openings into those networks, perform reconnaissance and hunt for corporate intellectual property or government secrets.

The manipulation of the Ethernet connector appeared to be similar to a method also used by the U.S. National Security Agency, details of which were leaked in 2013. In e-mails, Appleboum and his team refer to the implant as their “old friend,” because he said they had previously seen several variations in investigations of hardware made by other companies manufacturing in China.

In Bloomberg Businessweek’s report, one official said investigators found that the Chinese infiltration through Supermicro reached almost 30 companies, including Amazon.com Inc. and Apple Inc. Both

Amazon and Apple also disputed the findings. The U.S. Department of Homeland Security said it has “no reason to doubt” the companies’ denials of Bloomberg Businessweek’s reporting.

People familiar with the federal investigation into the 2014-2015 attacks say that it is being led by the FBI's cyber and counterintelligence teams, and that DHS may not have been involved. Counterintelligence investigations are among the FBI's most closely held and few officials and agencies outside of those units are briefed on the existence of those investigations.

Appleboum said that he's consulted with intelligence agencies outside the U.S. that have told him they've been tracking the manipulation of Supermicro hardware, and the hardware of other companies, for some time.

In response to the Bloomberg Businessweek story, the Norwegian National Security Authority said last week that it had been "aware of an issue" connected to Supermicro products since June. It couldn’t confirm the details of Bloomberg's reporting, a statement from the authority said, but it has recently been in dialogue with partners over the issue.

Hardware manipulation is extremely difficult to detect, which is why intelligence agencies invest billions of dollars in such sabotage. The U.S. is known to have extensive programs to seed technology heading to foreign countries with spy implants, based on revelations from former CIA employee Edward Snowden. But China appears to be aggressively deploying its own versions, which take advantage of the grip the country has over global technology manufacturing.

Three security experts who have analyzed foreign hardware implants for the U.S. Department of Defense confirmed that the way Sepio's software detected the

implant is sound. One of the few ways to identify suspicious hardware is by looking at the lowest levels of network traffic. Those include not only normal network transmissions, but also analog signals -- such as power consumption -- that can indicate the presence of a covert piece of hardware.

In the case of the telecommunications company, Sepio's technology detected that the tampered Supermicro server actually appeared on the network as two devices in one. The legitimate server was communicating one way, and the implant another, but all the traffic appeared to be coming from the same trusted server, which allowed it to pass through security filters.

Appleboum said one key sign of the implant is that the manipulated Ethernet connector has metal sides instead of the usual plastic ones. The metal is necessary to diffuse heat from the chip hidden inside, which acts like a mini computer. "The module looks really innocent, high quality and 'original' but it was added as part of a supply chain attack," he said.

The goal of hardware implants is to establish a covert staging area within sensitive networks, and that's what Appleboum and his team concluded in this case. They decided it represented a serious security breach, along with multiple rogue electronics also detected on the network, and alerted the client's security team in August, which then removed them for analysis. Once the implant was identified and the server removed, Sepio's team was not able to perform further analysis on the chip.

The threat from hardware implants “is very real,” said Sean Kanuck, who until 2016 was the top cyber official inside the Office of the Director of National Intelligence. He's now director of future conflict and cyber security for the International Institute for Strategic Studies in Washington. Hardware implants

can give attackers power that software attacks don't.

"Manufacturers that overlook this concern are ignoring a potentially serious problem," Kanuck said. "Capable cyber actors -- like the Chinese intelligence and security services -- can access the IT supply chain at multiple points to create advanced and persistent subversions."

One of the keys to any successful hardware attack is altering components that have an ample power supply to them, a daunting challenge the deeper into a motherboard you go. That's why peripherals such as keyboards and mice are also perennial favorites for intelligence agencies to target, Appleboum said.

In the wake of Bloomberg's reporting on the attack against Supermicro products, security experts say that teams around the world, from large banks and cloud computing providers to small research labs and startups, are analyzing their servers and other hardware for modifications, a stark change from normal practices. Their findings won't necessarily be made public, since hardware manipulation is typically designed to access government and corporate secrets, rather than consumer data.

National security experts say a key problem is that, in a cybersecurity industry approaching $100 billion in revenue annually, very little of that has been spent on inspecting hardware for tampering. That's allowed intelligence agencies around the world to work relatively unimpeded, with China holding a key advantage.

"For China, these efforts are all-encompassing," said Tony Lawrence, CEO of VOR Technology, a Columbia, Maryland-based contractor to the intelligence community. "There is no way for us to identify the gravity or the size of these exploits -- we don't know until we find some. It could be all over the place -- it

could be anything coming out of China. The unknown is what gets you and that's where we are now. We don't know the level of exploits within our own systems."