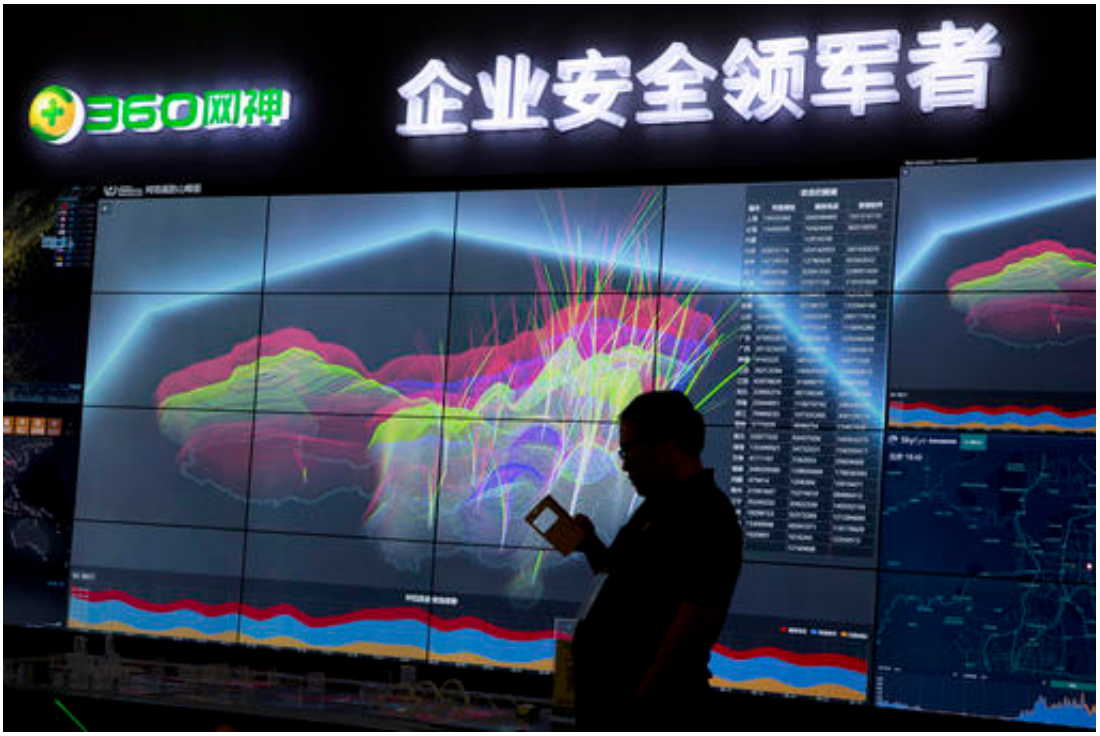
Chinese firm says it did all it could ahead of cyberattack

October 25 2016, by Gerry Shih



In this Aug. 16, 2016 file photo, a worker is silhouetted against a computer display showing a live visualization of the online phishing and fraudulent phone calls across China during the 4th China Internet Security Conference (ISC) in Beijing. Chinese electronics maker Hangzhou Xiongmai Technology has issued a recall on Monday, Oct. 24, 2016, for millions of products sold in the U.S. following a devastating cyberattack, but has lashed out at critics who say its devices were at fault. (AP Photo/Ng Han Guan, File)

A Chinese electronics maker that has recalled millions of products sold

in the U.S. said Tuesday it did all it could to prevent a massive cyberattack that briefly blocked access to websites including Twitter and Netflix.

Hangzhou Xiongmai Technology has said millions of web-connected cameras and digital recorders became compromised because customers failed to change their default passwords.

Liu Yuexin, Xiongmai's marketing director, told The Associated Press that Xiongmai and other companies across the home surveillance equipment industry were made aware of the vulnerability in April 2015. Liu said Xiongmai moved quickly to plug the gaps and should not be singled out for criticism.

"We don't know why there is a spear squarely pointed at our chest," Liu said.

The hack has heightened long-standing fears among security experts that the rising number of interconnected home gadgets, appliances and even automobiles represent a cybersecurity nightmare. The convenience of being able to control home electronics via the web also leaves them more vulnerable to malicious intruders, experts say.

Unidentified hackers seized control of gadgets including Xiongmai's on Friday and directed them to launch an attack that temporarily disrupted access to a host of sites, ranging from Twitter and Netflix to Amazon and Spotify, according to U.S. web security researchers.

The "distributed denial-of-service" attack targeted servers run by Dyn Inc., an internet company located in Manchester, New Hampshire. These types of attacks work by overwhelming targeted computers with junk data so that legitimate traffic can't get through.

"The issue with the consumer-connected device is that there is nearly no firewall between devices and the public internet," said Tracy Tsai, an analyst at Gartner, adding that many consumers leave the default setting on devices for ease of use without knowing the dangers.

Researchers at the New York-based cybersecurity firm Flashpoint said most of the junk traffic heaped on Dyn came from internet-connected cameras and video-recording devices that had components made by Xiongmai. Those components had little security protection, so devices they went into became easy to exploit.

In this April 29, 2016, file photo, a woman sits near a display showing the dangers of hackers breaking into mobile devices during the Global Mobile Internet Conference in Beijing. Chinese electronics maker Hangzhou Xiongmai Technology has issued a recall on Monday, Oct 24, 2016, for millions of products sold in the U.S. following a devastating cyberattack, but has lashed out at critics who say its devices were at fault. (AP Photo/Ng Han Guan, File)

In an acknowledgement of its products' role in the hack, Xiongmai said in a statement Monday that it would recall products sold in the U.S. before April 2015 to demonstrate "social responsibility." It said products sold after that date had been patched and no longer constitute a danger.

The company, which also makes dashboard cameras and computer chips, said it would recall more than 4 million web-connected cameras and has offered customers a software security fix. The recall will apply only to devices sold under Xiongmai's name. As an original equipment manufacturer, close to 95 percent of the company's products are sold by other firms that repackage its devices under their own brand names, said Liu, the marketing director.

Xiongmai and Dahua, a video surveillance manufacturer also based in the eastern Chinese tech hub of Hangzhou, first came under scrutiny several weeks ago after Flashpoint assessed that hackers had controlled their devices to attack the website of cybersecurity writer Brian Krebs, among other targets. Dahua has responded by saying it is dedicated to testing vulnerabilities, and has offered discounts for replacement equipment.

Xiongmai has adopted a less conciliatory stance. It downplayed its culpability this week, saying that as even the world's largest technology companies experience security lapses, "we are not afraid to also experience it once."

Xiongmai also slammed as "completely untrue, malicious and defamatory" reports about its products and appended to its statement a letter from its lawyers threatening litigation.

Mark James, an expert with Slovakia-based security company ESET, said that he doubted Xiongmai could be held liable for an attack such as Friday's, but that the company's officials "obviously recognize a concern

here."

"Hopefully other manufacturers will follow suit and take a look at what they can do to increase security of their own products," he said.