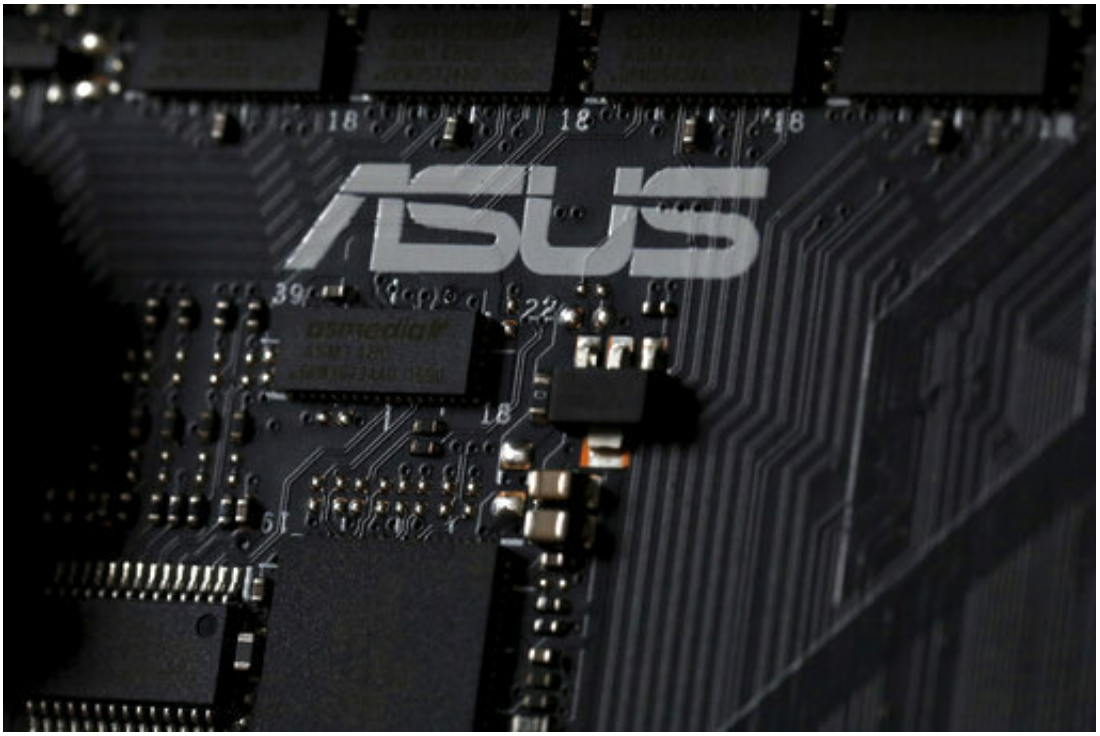
Researchers: ASUS computers infected by auto-update virus

March 26 2019



This Feb 23, 2019, photo shows the inside of a computer with the ASUS logo in Jersey City, N.J. Security researchers say hackers infected tens of thousands of computers from the Taiwanese vendor ASUS with malicious software for months last year through the company's online automatic update service. Kaspersky Labs said Monday, March 25, that the exploit likely affected more than 1 million computers from the world's No. 5 computer company, though it was designed to surgically install a backdoor in a much smaller number of PCs. (AP Photo/Jenny Kane)

In a sophisticated targeted espionage operation, hackers infected tens of thousands of computers from the Taiwanese vendor ASUS with malicious software using the company's online automatic update service, security researchers reported Monday.

Kaspersky Lab said it detected 57,000 infections among customers of its antivirus software. It estimates that the exploit likely affected more than 1 million computers from the world's No. 5 computer company .

UPDATE: ASUS acknowledges computers infected by auto-update virus

The malware was designed to open a "backdoor" for intruders in the infected machines, researchers said.

About 50 percent of the affected Kaspersky anti-virus software customers were in Russia, Germany and France, the company said . The U.S. accounted for less than 5 percent.

A Symantec spokeswoman said about 13,000 of its antivirus customers received the malicious updates.

The so-called supply-chain attack was first reported by the online news site Motherboard.

Kaspersky said the infected software was on ASUS's Live Update servers from June to November and was signed with legitimate certificates. It did not detect the malware until January, when new capabilities were added to its anti-virus software, the company said.

Kaspersky said its researchers determined that the malware was programmed for surgical espionage when they saw that it was designed to accept a second malware payload for specific computers based on

unique identifiers of their network connections. It identified more than 600 computers programmed to receive the payload.

In a blog post and answers to emailed questions, the company said the nature of the second malware payload was unknown because the server that delivered it was no longer active.

Kaspersky said that while is too early to know who was behind the operation, it is consistent with a 2017 incident blamed by Microsoft on a Chinese state-backed group the company calls BARIUM.

ASUS did not immediately respond to two emailed requests seeking comment.