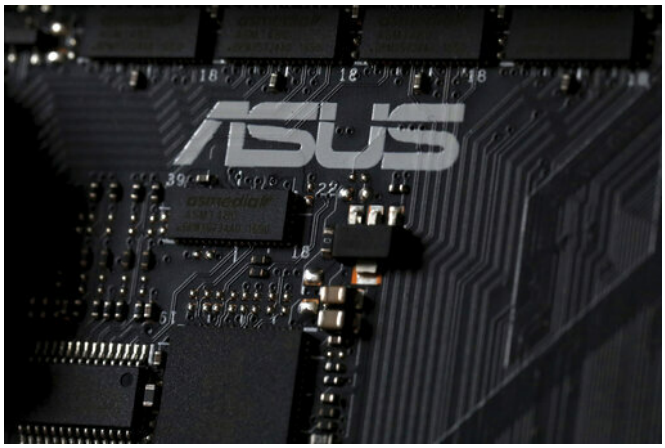
ASUS acknowledges computers infected by auto-update virus

26 March 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)

The Taiwanese computer company ASUS is acknowledging that suspected nation-state hackers planted malware on its online automatic update service in a sophisticated and targeted espionage operation.

Security researchers at Kaspersky Lab disclosed Monday that hackers infected tens of thousands of ASUS computers last year in the scheme. Kaspersky said it detected 57,000 infections among customers of its antivirus software. It estimated the exploit likely affected more than 1 million computers.

The malware was designed to open a "backdoor" for intruders in infected machines.

ASUS said in a prepared statement that the malware infected a small number of devices in an attempt to target a very small, specific user group. It did not specify how many or who.

The world's No. 5 computer company said it fixed the compromised updating software, which automatically sends drivers and firmware to ASUS laptops when authorized by users.

ASUS did not respond to emailed questions. Nor did it acknowledge that Kaspersky notified it of the so-called supply-chain attack, which was first reported by the online news site Motherboard. Cybersecurity experts say such attacks are likely far more common than is known.

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 infected software was on ASUS's Live Update servers from June to November and was signed with legitimate certificates, according to Kaspersky. 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 address which state-backed hacking group may have been responsible but noted that their targets are not average consumers.