Warning of the risk of businesses being attacked through micro-chips attached to servers

According to SecurityBox, a network security company in Vietnam, it is possible to penetrate important information systems of businesses, organized through micro chips.

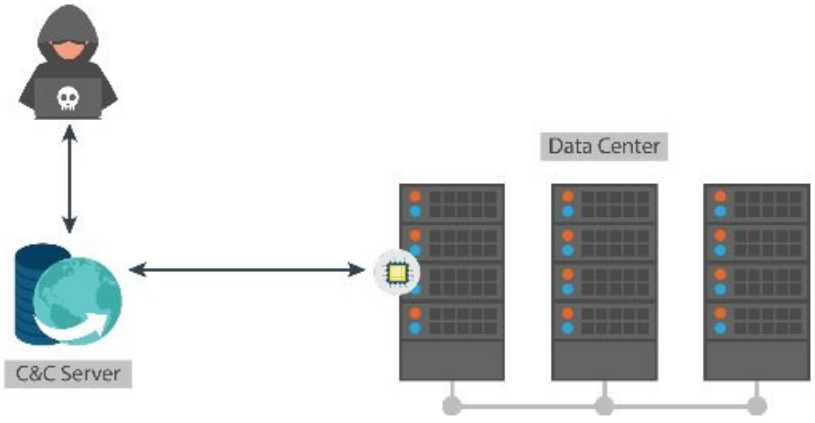
Information that China implanted spy chips into servers of large US corporations in recent days has made many businesses unable to panic. Although it is still not possible to determine whether this information is real or not, according to SecurityBox, a network security company in Vietnam, the penetration of important information systems of businesses and organizations through Micro chips are absolutely possible.

According to the security experts' analysis of the SecurityBox, the process of building the board is very complicated, including the steps of design, experience and finally machining.

In order to secure the technology, firms often use two separate suppliers for circuit making and circuit welding in the process of board machining. The board machining units only get the printed board file, the information about the overall design of the board is very small. Therefore, mounting the chip on the board is difficult to implement.

To do this, before machining the board machining lines must reach the motherboard design or the design of the modified boards to be able to decompile the printed board and adjust Edit and add new design with microchip. Although this is very difficult, theoretically, if the area of ??intervention and on-board impact is not too large, it can still be done.

Microchip mounting is a form of attack that is difficult to detect, stable and highly effective by easily penetrating important information systems of large corporations or government organizations.



The SecurityBox offers two microchip microchip attack scenarios.

The first scenario: Microchip attacks organizations and businesses thanks to the ability to open back ports.

Microchip with extremely large script can perform memory control, network connection or firmware loading operations on the server which can provide functional support code for microchip. This microchip can insert malicious code into the operating system kernel because it can interact or replace BMC - Baseboard Management Controller. BMC is an embedded microcontroller in the motherboard to manage the interface between the system management software and the hardware platform.

If the Firewall and security systems do not prevent, microchip can download and execute malware.

This option requires very high technical requirements.

Second scenario: Microchip creates vulnerabilities that can exploit remote systems to take control.

Microchip has the ability to interact or replace BMC so it can handle data streams. Microchip with a special data structure format will trigger a designed feature that has a vulnerability that allows remote exploitation in it. Meanwhile, hackers only need to rely on specially structured data to be able to detect servers that contain microchips and exploit.

SecurityBox adds that it is not too complicated to detect whether the boards are microchip-mounted but need to cooperate with hardware manufacturers. Then, only the difference between the design of the motherboard and the finished machined board can be found.

See more:

1. The malware detection is extremely dangerous, unable to destroy even if the operating system is reinstalled and the hard drive is replaced
2. Cold boot, an attack technique 10 years ago can crack the encryption of most PCs today
3. Facebook was attacked, more than 50 million user accounts are at risk of being leaked