Threats and risks from malware on USB Flash

In addition to the undisputed benefits, USB flash drives sometimes contain risks that cannot be underestimated if not used properly.

USB is probably the oldest and most commonly used storage device in the world. In addition to the undisputed benefits, USB flash drives sometimes contain risks that cannot be underestimated if not used properly.

A USB flash drive, basically, is a type of data storage device that uses flash memory integrated with the USB interface. This type of hard drive can be infected with viruses and ransomware (accidentally or intentionally) and used for malicious purposes, causing damage to their users. There are even malicious software designed specifically for USB, which turns the USB device into an intermediary malware infection tool on the computer, thereby stealing login information and sensitive data.

Some use cases of USB flash drives spread malicious code

Malicious USB sticks are the number one choice for attackers when they have physical access to the target computer. The first incident was officially recorded in 2010 when some security researchers discovered the infamous 'poison' Stuxnet distributed via USB with the aim of launching malicious attacks against Network system of a facility in Iran.

Or the case of a malware called UsbFakeDrive in 2013 with a quite unique mechanism of infection. After successfully infecting the USB device, the malicious code will create another drive in that USB drive and force users to open the second drive to see the data. In essence, the second drive is a shortcut that contains the virus file. When a user opens the data, it is also when the computer is infected with malware from USB.

Previously, AutoRun virus has also been raging around the world with the mechanism of opening the drive is activating malicious code. This makes the spread of this virus on Windows systems uncontrollable.

How to use infected USB device to cause damage?

The ultimate and most dangerous purpose of the malware infection via USB drive is to gain control of the system and steal data. This can be done remotely by hackers with the help of malware, adware, spyware or gray software when they successfully infect the target computer.

In addition, with the emergence and outbreak of ransomware in the past two years, hackers could gain illicit profits by spreading this malicious code via USB, causing serious damage. masonry for organizations and individuals.

How to protect the system from malicious USB

1. Do not plug unspecified USB into important computers. Hitting people's curiosity is also an attack technique of malicious agents. This is especially true in case you picked up a USB flash drive somewhere.
2. Do not use the same USB flash drive for both home and work computers. This can reduce the risk of cross-contamination between computers.
3. Always enable security features like fingerprint authentication for USB connections. This will help protect the device from hackers' physical access.
4. Always update the software on your computer to the latest version for maximum protection against known types of malware and security holes.