Learn about the safe anti-virus mechanism on the Vietnamese military

A new USB capable of preventing and controlling virus infection and malware from computer to computer was created by the Research Institute of Electronics Institute of Military Science and Technology. This Vietnamese military's safe USB is called VS-key and has been officially sold to the market.

A new USB capable of preventing and controlling virus infection and malicious code from computer to computer was received by Colonel, Dr. Tran Xuan Kien and colleagues from the Institute of Electronics and Science and Technology Institute. Military - Ministry of Defense has been officially sold to the market. This Vietnamese military's safe USB is called VS-key.

1. 20 ways to create the best USB boot
2. Instructions on how to create USB install Windows 10
3. How to connect printer 2.0 USB port to USB 3.0 port on Windows 10

Let's learn a bit about the anti-virus mechanism that the USB VS - use this Key offline.

First, we need to know about **the mechanism of virus spread via regular USB** .

USB is a storage device capable of reading and writing data, can communicate with the computer thanks to a standard data format for device memory specified by the operating system.

For example, in macOS, read the standard HFS, APFS, and Windows devices, and receive the common standards like NTFS, FAT32, FAT .

In order for a virus to spread from a computer to a USB, it is required that the type of data used on the USB must be supported by the computer's operating system (except in some special cases). That means that the computer must read and write data to USB. Then, the virus can easily 'move' from computer to USB. And when USB has been infected with malicious code, it is plugged into another computer, it will copy the malicious code from the USB to the new computer and start the destructive process.

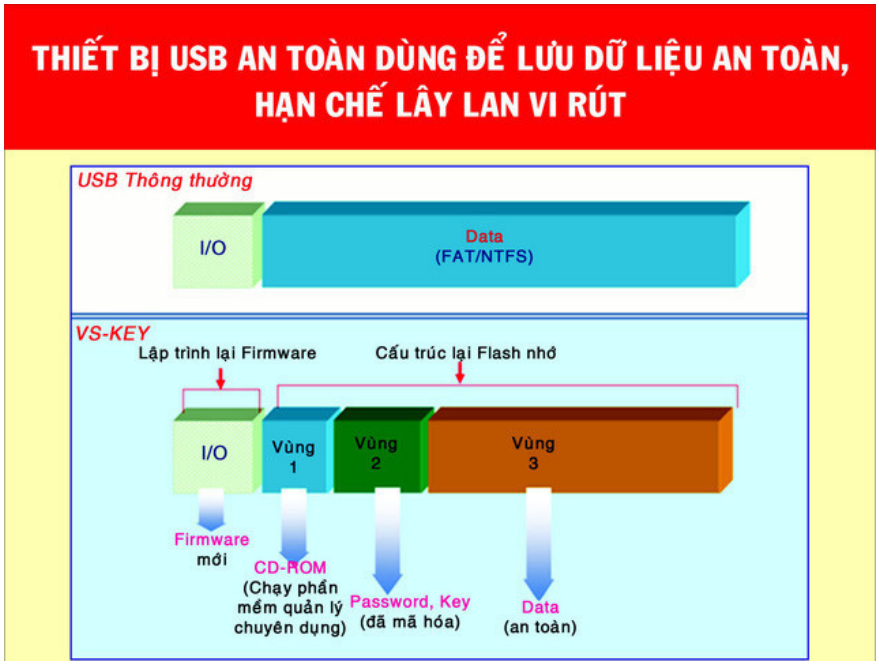
So, how does VS-Key secure USB have data processing mechanism?

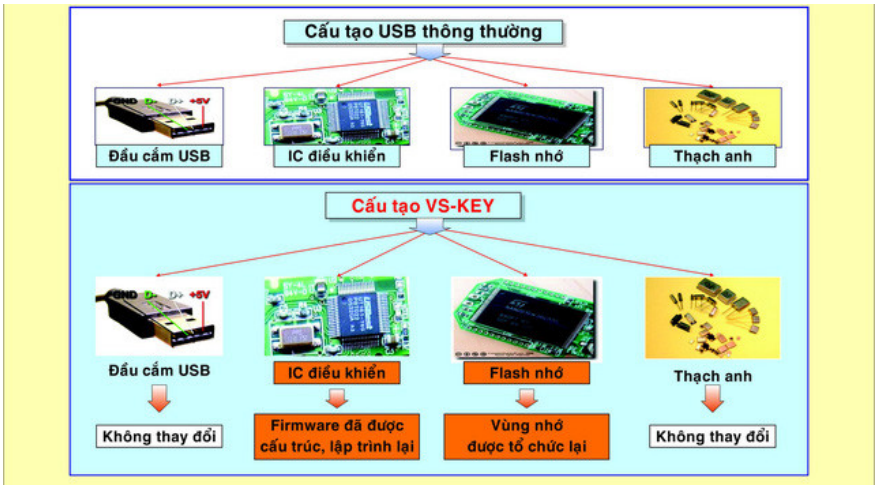
The authors have divided USB memory into 3 independent zones including:

Partition 1: Contains own writing software of VS-Key. This area is formatted as a CDFS partition (emulating a CD drive) containing software built by Viettel and using common data standards with Windows such as NTFS or FAT32 but locked up like a CD does not allow overwriting. .

Partition 2: Contains the password to decode the data from the 3 partition into readable data on the computer.

Partition 3: Contains encrypted data. Partition 3 and partition 1 communicate with each other through a separate data standard developed by the author (non-standard). Data will be encrypted with software in partition 1, then stored in partition 3. The operating system cannot access data in this partition.





With regular USB, when copying data, you need to go through software such as Windows File Explorer to copy over and over. But when using VS-KEY, we have to copy data through separate software located on partition 1.

Before using to read and write data, we must enter the user password. If you enter the correct software, you will access to the second area containing the security password to get the access key and identify the file system stored in the third partition with non-standard format. If the password is entered incorrectly 10 times, the device will be locked.

This helps prevent infection with viruses, spyware, worms, trojans . preventing unauthorized access to information theft. In particular, the data is automatically encrypted when saved from the computer to the drive. User passwords are encrypted and stored on USB.

But VS-KEY is only capable of preventing acts of copying underground data caused by viruses in order to put malicious data on USB but not capable of scanning or destroying Viruses are inserted into USB.

Therefore, if the virus is maliciously embedded in data files such as Ransomware embedded in a word file, when the infected document file is inserted into the USB, the software will encrypt and store as a document file. normal clean. And when plugging the USB into another computer, pop the document file and read it, it will still stick with ransomware.

Therefore, secure USB must still work in tandem with Antivirus software to detect when encountering the infected document file.

See also: Instructions for restoring lost USB storage