Security related to the use of USB

Although USB has become an indispensable thing in anyone's life, these devices also pose a significant challenge to network security.

In this article we will show you some files that are generated by USB storage devices on the system, besides how to collect and clarify those files and determine whether USB Is it related to the distribution of malicious code on Windows computers .

Although USB has become an indispensable thing in anyone's life, these devices also pose a significant challenge to network security. Nothing is as clear as what happened in 2008, when the Conficker virus spread with a tremendous speed on the Internet and infected millions of home and business computers, even finding its way. to infiltrate tightly secured networks of the US Department of Defense. At that time, people began to pay attention to the behavior of users' USB in protected networks. Not only effective in self-replicating malware, these devices can also be used to remove sensitive, proprietary or confidential information from an unauthorized network. For the above reasons, going to check the files left after plugging in the USB has become a hot topic in the last few years.

Files are generated on the computer when plugging in USB

When investigating something, we often tend to what remains. When browsing the web in Internet Explorer, we often leave some traces in the browser deposit. When logging into a system, you will also leave an entry in the system security log. By examining a system in detail, this information will help us a lot in determining what happened. There are many things you do on the system that can leave this type of information. The same with USB. The question is, what do USB devices leave behind when we plug them into a computer.

What USB left in the computer will be useful for research. It can help you determine which computer is the cause of the infection. It can also help you determine when someone plugs into the system and copies the data illegally. Whatever your purpose is, we will go looking for a place to store this type of information inside the Windows operating system.

Manual extraction

The most basic way to find out what happens when plugging the USB into the system is to browse to the location of this information. In this article, we will focus on such locations in Windows 7 operating system.

The first and most easily extracted information is the list of USB devices that are plugged into the system. You can quickly find this information by the path: **HKLMSYSTEMCurrentControlSetEnumUSBSTOR** . Here you will find the USB devices that are plugged into the system, along with other information such as company name, product number, version number and Serial number.

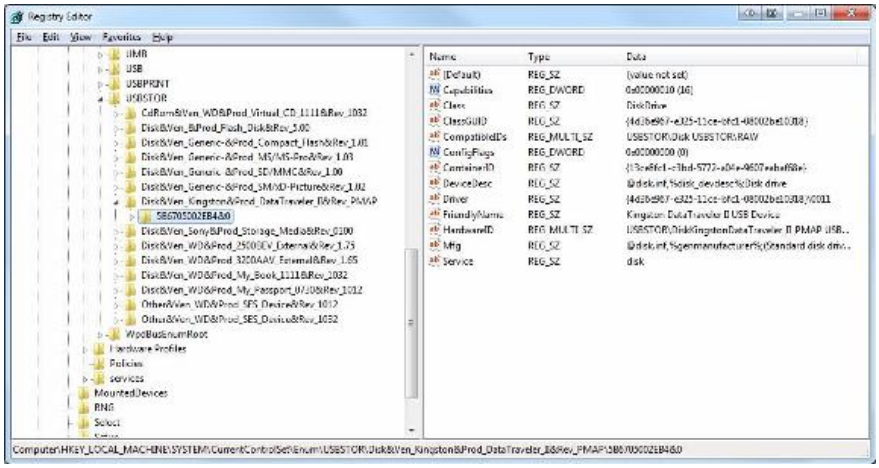

Figure 1: List of some USB devices plugged into a recent Windows 7 computer

After obtaining a list of used devices, you need to determine whose devices they are. This can be done but there must be some additional steps. In the registry, first visit **HKLMSYSTEMMountedDevices** . Within this area, you can search for the serial number of the device in question. After finding the serial number, this key will give you the GUID associated with the device.

After obtaining the device GUID, you need to focus on personal profile on the computer. Inside each users profile folder (C: Users) there will be an NTUSER.DAT file. This file can be opened with the system registry editor with administrator privileges. To bind certain users to any device, you need to browse to the directory below inside NTUSER.DAT hive: **SoftwareMicrosoftWindowsCurrentVersionExplorerMountPoints2** . Here you can search the GUID of the device in question. If it is found, the user is logged in when the USB device is plugged into the system. Note that this search must be done for all users on the system when trying this type of correlation.

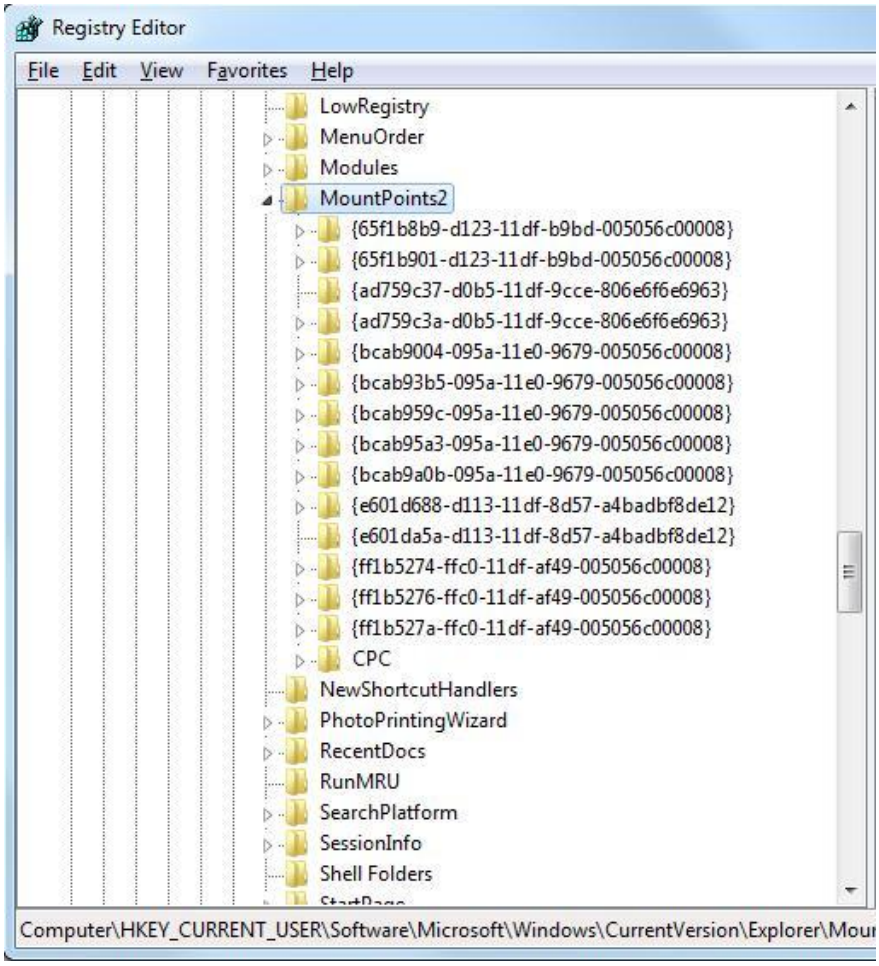

Figure 2: Searching in the NTUSER.DAT file to determine the USB GUID

One of the most important aspects of research is finding the timing of events around the thing being investigated. The important thing to know here is when the suspect USB is connected or disconnected from the system.

Determining when the device is first connected to the system is quite easy in case you already have its serial number (how we did it in the previous steps). With that information, go to file **C: Windowsinfsetupapi.dev.log** and perform a search for that serial number, when you will know when it was first plugged into the system.

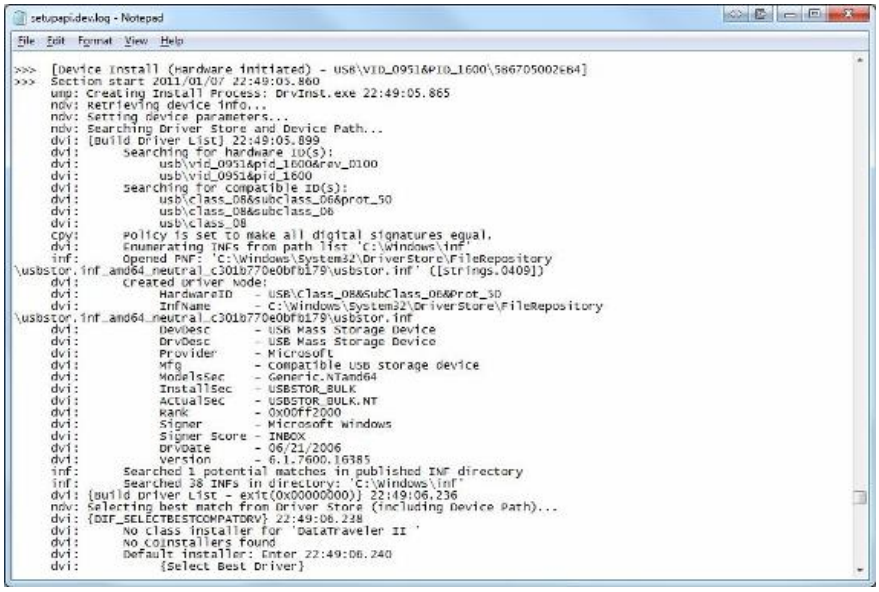

Figure 3: Search in the setupapi.dev.log log file to determine when the USB device was first plugged into the system

On the other hand, we also need to determine when the device is most recently connected to the system. To access this information, we just need to look in the registry at **HKLM / System / CurrentControlSetEnumUSBVID_12345 & PID_12345** , replacing '12345' here with the company name and the product ID we have obtained from the previous step. Here, you can export the registry key as a text file to see when the latest key was written. This is done by clicking File, then Export from within regedit, when the key is selected.

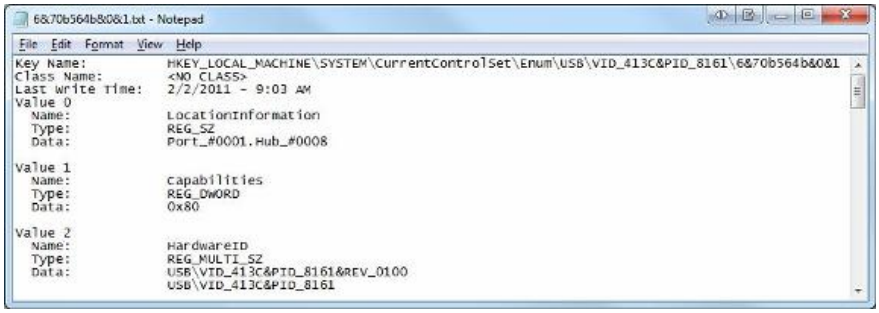

Figure 4: Determining the last time the USB was connected from the registry

Automatically extract

In addition to finding the information above, there are many tools that can help you do this.

The two tools we introduced here are USBDeview and Windows USB Storage (USBSTOR) Parser. The first tool, USBDeview has a GUI interface, can extract and display the information we can find by manual method above. This is a free utility and you can download it here. The second tool we mentioned has similar functionality and can run on both Windows and Linux. You can download that tool here.

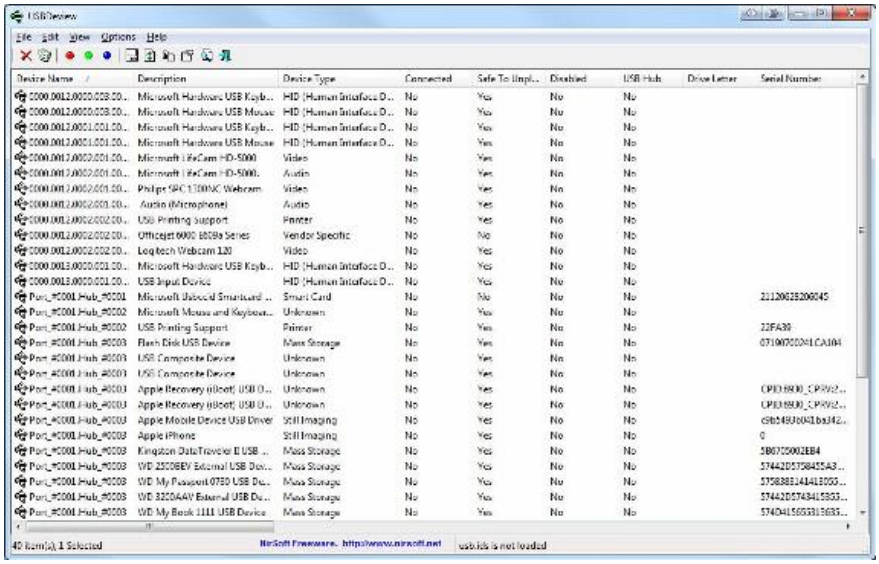

Figure 5 :: Use USBDeview to view files generated by USB plugging

Conclude

Unless in a complete environment with no USB devices, we may not have to pay attention to how these devices relate to system security. It is almost impossible, so we think this article has a lot of useful knowledge that can help you find the cause of things.

You finished reading the article "**Security related to the use of USB**" edited by the **TipsMake** team. We hope this article has provided you with many useful tech tips and tricks. You can search for similar articles on tips and guides. Thank you for reading and for following us regularly.