International Journal of Science and Research (IJSR)
ISSN (Online): 2319-7064
Index Copernicus Value (2013): 6.14 | Impact Factor (2015): 6.391

USB Detection in Industrial Espionage Cases

Aparna Chandran[1], Harsha V[2]

[1]Cochin University, College of Engineering Kallooppara, Kerala, India

Abstract: ***Industrial Espionage is the covert and illegal practice of investigating competitors to gain a business advantage. The target of industrial espionage might be a trade secret such as a proprietary product specification or formula, or information about business plans. Nowadays USB plays a leading role in Industrial espionage. Employees can easily access systems and there is a chance of thefting confidential data and that may cause problem. Here I introduce a new concept which provides a way to store USB details in central server system and the method runs in client systems without the knowledge of employees. The method will retrieve every information about the USB drive whenever it is mounted in any of the system which is useful to verify the data theft team.***

Keywords: USB, Registry, Backup, Data Transfer, Industrial Espionage

1. Introduction

Industrial espionage is an illegal practice of leaking confidential information of a company by an insider or outsider to a competitor. This can be devastating to the company and can ruin the company‟s image and reputation in the market along with brand distrust that comes from insiders itself who steal company‟s trade secrets. The two key words in Industrial Espionage are Collection and Profit. Collection means obtaining the desired information or data. Profit means fee provided for the collected information or data. The methods of industrial espionage [1] mainly classified into technical and non- technical methods. They are cyber-attacks, electronic surveillance, reverse engineering, dumpster diving, corrupt practices, etc.

Large and highly successful companies in the world have to deal with the problem of industrial espionage at several times. Industrial espionage is a reaction to the efforts of much business to keep secret about their product designs, formulas, manufacturing methods, research and future plans in order to protect or expand their shares of the market.ie, companies spy on other companies to obtain information related to trade secrets and intellectual property that can bring financial information, market leadership, and economic growth. The industrial espionage is a process [4] not a single act. The process of industrial espionage can be divided into four phases. They are Definition of Requirements, Collection, Analysis, and Evaluation.

Insiders believe that they could remain anonymous while conducting industrial espionage. What we need is an application that will be able to catch these insiders without their knowledge. i.e., the proposed scheme is an application to detect the USB devices in the industrial espionage cases. The proposed solution is a method runs in client systems without the knowledge of employees which is used as an evidence in court.

2. Literature Survey

In literatures of industrial espionage, most of researches were focused on how industrial espionage takes place and methods of industrial espionage. But the study seldom concentrates on how to prevent or identify the industrial espionage.

Author defines the technical and non-technical methods of conducting Industrial Espionage [1]. The methods include cyber-attacks, electronic surveillance, reverse engineering, request for information, dumpster diving, conferences, conventions, and trade shows, corrupt practices, exploitation of joint research and business, etc. Among them USB drives are best way to transfer data which are available in various sizes and shapes. „Understanding Industrial Espionage for Greater Technological and Economic Security „written by Shared Sinha.

The paper „In the company of spies: The ethics of industrial espionage‟, focus on recent cases of industrial espionage [2]. For example, „Ericsson involved in spy scandal'. In this case, Ericsson, the Swedish telecommunications company was best known for its mobile phones. Here Industrial Espionage was conducted by the employees. They were leaking the company information to a foreign intelligence service. Two Ericsson employees, and one employee, were taken into custody suspected of passing on secret documents, and two other employees were suspended on suspicion of breaking the company security rules. „In the company of spies: The ethics of industrial espionage‟ written by Andrew Crane.

William Alvin Wallace addresses the process of Industrial Espionage that can be broken down into four phases [4]: Collectors perform first phase ie, Definition of Requirements. Collection phase involves obtaining the desired information or data with the value of the fee that they will be paid. In Analysis phase, huge amount of data and information accumulated by the collector must be analyzed. Once the data has been analyzed the Collector refers the original Requirement to see if he has met his goals ie, Evaluation phase. „Industrial Espionage Experts‟ written by William Alvin Wallace.

Author focus on five measures to mitigate the Industrial Espionage [5]: firstly, employs multilayer security; Secondly, employs the principle of „need to know'; Thirdly, email communication; Fourthly, protect mobile devices' data; And lastly, recruit quality and skilled employees. Education

makes employees more alert to security problems. „Dealing with industrial espionage „by Seth Mukwevho.

Ira focuses on the legal and illegal methods of Industrial Espionage [3]. Several forms of industrial espionage that is legal. This method includes the purchase of companies or products, and has the net result of transferring technology to the previous competitor Illegal method involves stealing information. Espionage could involve breaking into buildings and offices to steal the required information. Industrial spies can go through locked and unlocked office spaces, search file cabinets, examine computer systems which is not protected, etc. „Case study of Industrial Espionage through Social Engineering" written by Ira S.

3. Proposed Method

Insiders believe that they could remain anonymous while conducting industrial espionage. What we need is an application that will be able to catch these insiders without their knowledge. i.e., the proposed scheme is an application to detect the USB devices in the industrial espionage cases.
The proposed solution is a method runs in client systems without the knowledge of employees which is used as an evidence in court. The method will retrieve every information about the USB device whenever it is mounted in any of the system.ie; identify the information like USB serial number, mounting time, date, etc and get stored in the client system itself. A copy of this data is then stored into a central server system.i.e, when a USB connected to the client system the USB details stored into the client system that means USB details in windows registry. The Windows Registry is a database that stores low-level settings for the Microsoft Windows operating system and for applications. In windows registry keys and sub keys are available. The USB details stored in the USBSTOR sub key. From this sub key collect the USB details such as serial number, date, mounting time, etc. And create backup copy of these details and stored in the specific location. After creating the backup file which is transfer into the central server system. Finally view the USB details used by the client system in central server system.

3.1 Collect the USB Details

Any time a new USB Device is connected to the system, it will leave information about this USB device within the Registry. This information can uniquely identify USB devices connected to the system. The Windows Operating system stores vendor ID, product ID and Serial Number for each connected USB device. So that collects the necessary USB details information from the Registry key.

Figure 1: USB details in the Windows Registry

3.2 Backup the Collected USB Details

After collecting necessary USB details such as USB serial number, mounting time, date, etc from windows registry create a backup file with these details to a specific location. Before make changes to a registry key or sub key, export, or make a backup copy, of the key or sub key. Save the backup copy to a location specify, such as a folder on your hard disk or a removable storage device.

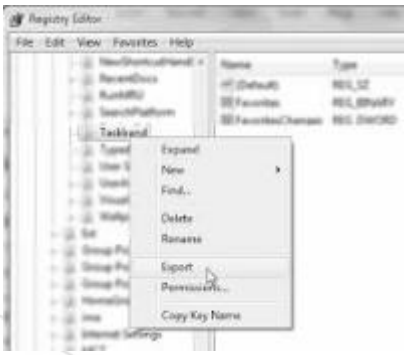

Figure 2: Backup the Windows Registry

3.3 Transfer the Backup File

Connecting PCs using a LAN cable is the safest and easiest way of transferring files, pictures, videos and music. Connecting PCs using a LAN cable is simple and secure. Change both computer names and in the network connection properties, select the ip properties and add values to the IP address and Subnet Mask and save the changes. All internet connections are made and restart the PCs and view the LAN of the two computers in the network connections. Created backup file transfer into the central server system.ie view the details of USB used by the client system in central server system. Finally, view the USB details used by the client system in central server system.

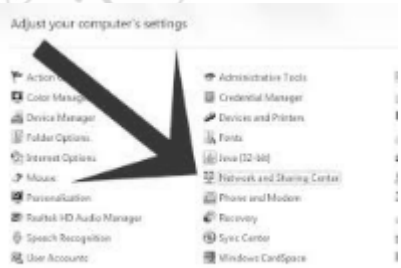

Figure 3: Enable Sharing Option

4. Result

Many cases of industrial espionages are unsolved due to lack of proper evidence. The proposed work helps in solving industrial espionage cases which involve the use of USB drives for retrieving confidential information. The data about USB drive stored in the central server while connecting to the company"s system while conducting industrial espionage can be used as evidence and is reliable to submit before court.

5. Conclusions

Industrial Espionage is one of the major threats to a company which is very difficult to get completely avoided. This paper is used to develop a method that deals with leaking of data through USB devices. Usually, the USB details stored in the registry when the USB connected to the system. The Windows Registry is a database that stores low-level settings for the Microsoft Windows operating system and for applications. In windows registry keys and sub keys are available. The USB details stored in the USBSTOR sub key. From this sub key collect the USB details such as serial number, date, mounting time, etc. And create backup copy of these detailed and stored in the specific location. After creating the backup file which is transfer into the central server system. Finally view the USB details used by the client system in central server system.

This method runs as a service in a client system i.e. without the knowledge of client and storing the USB details such as the mounting time, date, USB serial number, etc in the client system as a backup file and store a copy of it in the central server system. Also we can view the USB details of USB used by the client, in central server system which can be used as evidence in Industrial cases.

References

[1] Sharad Sinha (2012)" Understanding Industrial Espionage for Greater Technological and Economic Security" Nanyang Technological University, Singapore, vol. 51, pp. 37–41.
[2] Andrew Crane (2003)" In the company of spies: The ethics of industrial espionage" International Centre for Corporate Social Responsibility Nottingham University Business School Nottingham University, United Kingdom, No: 15, pp.1-22.
[3] Ira S (2002)" Case study of industrial espionage through social engineering" National Computer Security Association, Pennsylvania, No: 7, pp.27-32.
[4] William Alvin Wallace "Industrial Espionage Experts"downloaded8/11/2015,www,newheaven.edu/California/CJ625/p6.html.
[5] Seth Mukweho (Feb 2015),"Dealing with Industrial Espionage", https://google.com/Industrialespionage (08/11/15).

Author Profile

Aparna Chandran obtained the Degree of Bachelor of Technology in Computer Science and Engineering from VKCET in 2014. She is now pursuing her master degree in Computer Science with specialization in Cyber Forensics and Information Security at College of Engineering, Kallooppara under Cochin University of Science and Technology.

Harsha V obtained B.Tech in Computer Science and Engineering from SHM College of Engineering and M.Tech in Computer and Information Science from Cochin University. She is currently working as Assistant Professor in College of Engineering, Kallooppara.