DIGITAL FORENSICS
EMPLOYEE MISCONDUCT

Kristopher Bleich, CISSP, EnCE, C|EH

Organizations spend a significant amount of money on hardware and software to secure the corporate network, prevent unauthorized access by outside entities, or fight the ongoing battle against malware. All too often, management overlooks the threat to corporate intellectual property which exists "within the walls": the employee. A study titled Data Loss Risks During Downsizing, conducted by the Ponemon Institute, found that only 15% of organizations took any steps to review or audit departing employees' access to sensitive company information.

This study also found that 59% of employees leaving former employers are taking sensitive intellectual property. Employees leaving on "bad terms" were found to be more likely to take company information. According to the study, the top reasons for the theft of intellectual property were:

"Others have done it"
"I might be able to use it"
"I created this"
"The company doesn't deserve the data"

The Ponemon Study found that the types of data being taken were numerous, including email lists, employee records, financial information, trade secrets, and customer lists.

YOUR DATA HAS BEEN STOLEN

Employee misconduct is a real danger faced by companies, both while the employee works at the company, as well as during the period of time just prior to the employee's departure. Whether they are losing their jobs due to company contraction, misconduct, or simply the individual finding new work, the possibility that the employee is leaving with sensitive company information is a very real threat to organizational data security.

HOW DID YOUR DATA LEAVE?

With modern day technical advancements, several avenues exist which an employee may use to steal data. The avenue used by the employee will often turn on the relative technical expertise or job duties of that employee. Departing employees may use one or more methods from the two "categories" below to steal intellectual property.

Hardware: The use of hardware such as USB devices, CDs/DVDs and printers, remains a popular method of stealing an organization's intellectual property. The employee often believes that the data will not be missed or that the use of these devices cannot be detected.

Network: The Internet presents many other avenues for employees to steal data prior to their departure from the company. Attaching documents to personal emails, sending data via instant messenger applications, or uploading sensitive documents to file sharing websites, such as *YouSendIt* or *Dropbox*, has become an increasingly popular method to steal data.

Several recent SpearTip cases have involved the copying of data to portable USB devices prior to the employee's departure from a company. Analysis of the registry of the employee's work system can detect the connection of USB devices that were previously connected to the system. The registry is a centralized database utilized by Windows-based operating systems to track software installations, hardware configurations, and other specific operating system settings.

Below is an example of the information that may be retrieved from the registry of the work system identifying the connection of a USB device.

*Disk&Ven_Initio&Prod_INI-T640&Rev_1.43 [Tue Jun 22 15:45:22 2010] S/N:**00901016406E7ABEW**&0 [Tue Jul 19 18:26:19 2011]*
FriendlyName : Initio INI-T640 USB Device

The information in bold above is the hardware serial number identifying the connected USB device. This serial number is usually specific to the device and cannot be changed or altered by the user.

In addition, an analysis of link files on the work system can be conducted to examine the access of documents from external devices. Link files are "shortcut" files which contain information useful to a forensic analyst. This analysis may also identify sequential access of link files on the system, which may indicate an automated file copy operation on the system.

Other sources of information exist, such as antivirus logs, which may contain information identifying the copying of company data. A recent analysis conducted in connection with an organization's litigation identified the connection of a USB device and the copying of company data to the device by the employee. This information was located in a log associated with Sophos antivirus software.

*<notification xmlns="http://www.sophos.com/xml/msys/genericEventMessage.xsd" description="**Use of controlled device type 'Removable drives'detected:**REV_1.43**00901016406E7ABEW**&0
"type="sophos.management.notification.event"*
*Username: SOI********
 Rule names: 'SOItransfer2USB', 'drawings or images'
User action: File copy
Data Control action: Allow
*
*File type: Document (Microsoft Word-OLE)
*

*Source path: C:\Documents and Settings******\My Documents**********.doc
*

*Destination path: D:\aa*******2011**********.doc
*
*Destination type: Removable storage
"*

The serial number of the device and the action (file copy) identified by the software are shown above in bold. Sensitive information has been redacted. The information above, located during this analysis, shows the connection of a USB device and the copying of data from a source file path to a destination file path on the external device. The copying of company client lists occurred days before the employee resigned from the company. These findings quickly resulted in a favorable settlement for the organization.

Other avenues associated with personal email or the internet, which can be used by employees wishing to steal data, also exist. Employees may send emails to their personal email with sensitive documents attached, which they then retrieve from their personal computer at home.

Previous casework confirms that employees leverage access to their personal web-based email accounts from their offices. To circumvent monitoring of their company email account, they may send sensitive documents attached to emails from their personal email account to that same account. Forensic analysis of unallocated space on the work system's hard drive may detect these emails weeks or months after they were sent by the employee.

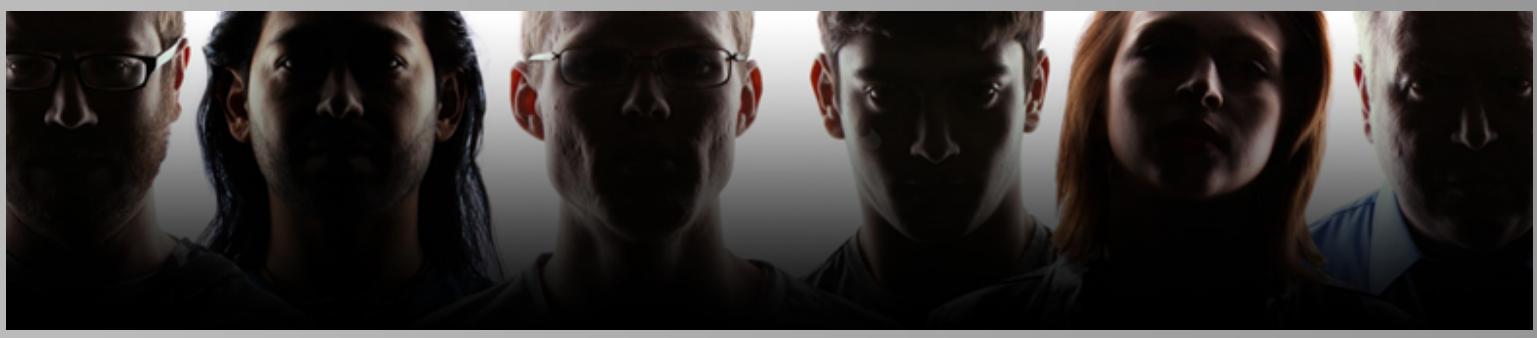
In a recent SpearTip case, analysis of unallocated space on the work system hard drive of an employee located evidence of the use of the file sharing website *YouSendIt (see below)*.

http://rcpt.yousendit.com/961721929/030994823749174503abb579354013a5

https://rcpt.yousendit.com/905389857/e24f3734b95e1a3d77b31dbc9d456544

https://rcpt.yousendit.com/919037139/12eab6784cfad0942e87524a3d3ac154

https://rcpt.yousendit.com/948480935/841a703089301e1fdd3dc09fcb9d8fc6

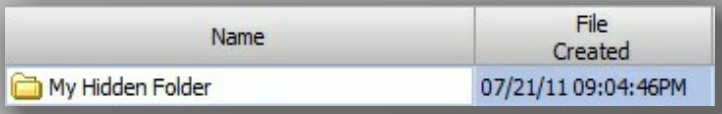


During an analysis of a separate SpearTip case, the use of the *DropBox* service to send sensitive company information was located during an analysis of link files (file name, below, redacted).

These examples demonstrate how, through a detailed forensic analysis, information may be located piecing together events showing the theft of data by an employee.

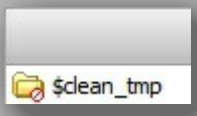
COVERING THEIR TRACKS

In some cases, employees take steps to conceal their actions, or destroy information that may incriminate them during a forensic analysis. These actions may include the creation of “hidden folders” (below) using third party software.



While the use of this type of software will hide files and folders from IT managers or other typical users, a forensic analysis will detect the presence of these directories.

An employee may also attempt to selectively wipe or “shred” specific files on their system that they don’t want located. In many cases, this activity is detectable during a forensic analysis. A deleted temporary folder may be located indicating that an employee has made use of this type of software (see below).



Another avenue of data destruction, considered by employees who wish to hide their activities, is the reformat of the file system and reinstallation of the operating system on the system. An analysis of the file system and registry on the system can identify this activity, including the date and time of the reformat of the file system, as well as the date and time of the reinstallation of the operating system. In addition, data residing in unallocated space on the hard drive may still be located after an employee takes these steps.

WHAT CAN BE DONE?

When board members or executive officers are presented with an acute situation involving theft of sensitive intellectual property or some other employee malfeasance – the threat and repercussions to your Brand can be devastating. An in-depth analysis of the individual's electronic devices can reveal a significant amount of information. In many cases, employees do not believe that their activities will be investigated or that they will be held accountable. These beliefs often increase the likelyhood that an employee will take company data with them when they leave.

Organizations can take proactive steps to protect themselves against data theft and increase the effectiveness of a forensic analysis on employee computer systems. Corporations should identify their key employees who have access to sensitive information and implement policies such as removing and retaining their hard drives upon their departure from the company.

In the event that management believes that an employee may have taken data from an organization, the preservation of the original devices by the organization coupled with a detailed forensic analysis can often determine if an employee stole or inappropriately retained company information. Proper vigilance and accountability is the key in deterring employee malfeasance and thwarting any actions that could threaten the integrity of your Brand and confidentiality of your intellectual property.