Faceless crimes

Law, Crime

Part I. Computer crimes or cybercrimes have been on the rise since the introduction of the Internet. More so with the onset of mobility and the launch of wireless networking, the increase in mischievous computer activities was exponentially high. Since cybercrimes are considered " faceless crimes" where a criminal hacker can do their misdeeds miles or continents away, or set-up a logic bomb a few hours later, it has been more difficult to trace these malicious acts.

In determining specific categories or types of IT-related attacks, it is noteworthy to examine the lists prepared by Mandia et al. (2001) in the book " Incident Response: investigating Computer Crime:

1. Denial-of-service attacks are some of the easiest incidents to respond to, because they do not involve actual intrusions.

2. Unauthorized uses of resources are typically insiders using their computers in an inappropriate manner. These investigations are often more oriented around personnel rather than technical issues.

3. Theft of information attacks involves unauthorized read-only access to information. While these are typically solved easily through configuration, it is very difficult to tell through an initial investigation if the attacker's access is read-only or actually involved a full-blown computer intrusion.

4. Vandalism is really a subset of computer intrusion, because it is not possible without access to the victim system.

5. Computer intrusions are the " mother of all incidents," in that they require the most involved response.

The best way to determine unauthorized computer access, downloading, copying and transferring of classified or confidential materials is by examining and evaluating the log files and access control lists. Unless the intruder or attacker is a sophisticated or high-caliber criminal hacker, this is the quickest and simplest method available, otherwise hiring trained professionals who will do computer forensics investigation is necessary to establish criminal liability and culpability.

Part II. Depending upon the forensics investigator, there are various techniques or methodologies in investigating cybercrimes. But in general, there are four major steps namely; " evidence identification, evidence preservation, evidence analysis and evidence presentation (Solomon et al., 2005).

There are two major tools required in forensics investigation, the first are the disk imaging and validating tools and the second are the forensics tools. Disk imaging and validating tools basically check the integrity of the hard disks and creates a mirror copy of the hard disk involved in the investigation. Forensics tools are the hardcore equipment that does data analysis, recovery and rebuilding, for deleted files and data.

Numerous tools are available commercially on the market. One important note for an aspiring computer forensics investigator is that all tools to be utilized in the course of their trade should be properly licensed and the used is authorized by the vendor otherwise the case might be thrown out of court for using pirated or illegally purchased software.

Some of the common disk imaging and validation tools as listed by Solomon et al. (2005) are: ByteBack by Tesch Assist, inc. and used for data recovery; EnCase from Guidance Software is one of the best drive duplicators; and Norton Ghost by Symantec provides the ability to create disk copies that are almost exact copies of the original. Solomon et al. (2005) also listed SMART by ASR Data Acquisition as a suite of forensics examination tool and WinHex ftom X-Ways is a universal hexadecimal editor and disk management utility.