Anti-forensics techniques

Business

Discussion Topic 1: Describe a situation where malware may be used as an anti-forensic technique and at least one method that an investigator can work through the challenge presented Anti-forensic techniques have the primary objective of frustrating a digital forensic examination by making it extremely difficult or impossible to retrieve evidence during forensic analysis. Hartley (2007) defines anti-forensics as any tool, technique, software or hardware that is developed with the primary goal of hampering forensic investigation. A malware is one of the tools that malicious code developers can use to avoid forensic detection and obscure forensic analysis. Malware writers can use a number of subversive techniques in avoiding forensic detection and analysis; they include data destruction, data hiding and data contraception. Data destruction entails using the malware to delete the file residue such as data blocks, directory entries and inodes.

In addition, data destruction can also involve the deletion of file system activity using inode time stamps. Kissel et al. (2006) points out that the main goal of data destruction is to ensure nothing useful is left for the forensic investigators as well as removing the traces of evidence. With regard to the data hiding, malicious code writers can use malware to put data where it should not be placed; an example of this is storing data in blocks marked as bad, when they are not bad. The main objective of data hiding is to ensure that the evidence is hidden from the forensic investigator; this technique is only successful in instances where investigator is not knowledgeable on how to look for forensic evidence.

Data contraception entails using the malware to make sure that data storing does not take place on the disk. Data contracption involves using the

malware to ensure that data is not written to the disk; this limits the value of any digital evidence that the investigators are likely to find in the disk (Kissel et al., 2006). One method that a forensic investigator can use to overcome this challenge is through the use of automated malware detection and classification; however, this method is labor intensive and entails the use of both static and active analysis techniques. Depending on the abilities of the forensic investigator and the time constraints, there is the likelihood that the investigator can overlook critical evidence; therefore, it is still a work in progress. The investigators can also use memory analysis technique to access hidden data (Kissel et al.

2006). Discussion Topic 2: What anti-forensic techniques would you employ to throw off a digital forensic investigator? Why would you choose them? There are a number of anti-forensics techniques that can be used to throw away a forensic investigator. The most effective techniques are artifact wiping, data hiding, attacking the computer forensics tools and processes, and obfuscation of trail. Data hiding entails making digital evidence extremely difficult to find by the investigator while the malicious code writer can access it for future use. According to Householder, (Houle & Dougherty, 2002), encryption and obfuscation of data gives the malicious code writer to limit the collection and identification of digital evidence by forensic investigators while allowing themselves to access and use the data. Some of the data hiding techniques include steganography, wherein files are concealed within another file in order to hide data through leaving it in pplain sight, data encryption, program packers and compression bombs.

I would choose data hiding techniques because it would allow me to change the evidence frequently because I have access to the evidence while forensic investigators cannot access; such frequent changes can be used to question the integrity of the evidence, if in the long run, the forensic investigators find it. Artifact wiping, sometimes referred to as data erasure, have the main goal permanently eliminating specific or the entire system files; this can be achieved by using disk cleaning utilities, disk destruction techniques and file wiping techniques. The primary advantage of artifact wiping as an anti-forensic technique is that it is fast and it leaves a smaller signature. I would use artifact wiping techniques because it does not leave any evidence, which makes it extremely difficult to forensic evidence to the evidence. In addition, artifact wiping is faster when compared to other techniques.

With no evidence, a forensic investigator will lack the basis to initiate criminal charges. With regard to trail obfuscation, it has the primary object of confusing, disorienting or diverting the forensic analysis process. Some of the trail obfuscation tools include the Timestomp, which can make potential files to be gathered as evidence useless in a court of law by questioning the credibility of the evidence. Attacks against computer forensics can also be used to destroy, hide or alter data usage information (Kruse & Heiser, 2002). I would use trail obfuscation because it allows the malicious code writer more time by delaying the investigation process.

In addition, trail obfuscation raises a number of issues regarding the credibility of evidence, which is to the advantage of the malicious code writer.