[redacted]

Dr. Waleed

COSC 316

9/27/15

Difficulties of Malware in Computer Forensics

Abstract

As the use of internet technologies continue to grow in our industrialized society, the ability to use it on unsuspecting victims for criminal conduct increased. Malware plays an integral part in how these victims are being targeted. This same malware also complicates the work done in investigating the crime. Malware is able to tamper with the evidence in cybercrime, and can lead to false conclusions by forensics analysts.

Background

Computer forensics have come a long way from where it started. Originally, anyone in the field of Computer Forensics had to dissect machine code to be able to discover the truth. With this being a painstaking process, new tools have been developed to make dealing with digital investigations easier. While the tools have become more advanced, the interference from malware has become more troublesome in these investigations. Malware is malicious code that sets out to steal, edit, or delete data and other criminal activities on your computer. Malware has the capability of producing false clues that an analyst must distinguish from the real ones.

Description

Malware has the ability to manipulate code in a way that can make it difficult for someone in Computer Forensics to even notice that it was changed. Theses manipulations can be done to edit

existing data, or to cover the tracks showing what has done the manipulating. After such an attack occurs, it is the forensics team's responsibility to determine the source of the attack. One of the problems with assigning blame to an incident is because of malware botting techniques. Also known as zombie computing, botting allows a hacker to gain access to another person's hardware and use it for their needs. These needs can be anything from using your processing power to commit a denial of service attack to storing files on your computer. Even with computer forensics tools used to track down the true culprit, malware can be sophisticated enough to throw the investigators off the trail. Detailed knowledge of how to use these tools is the key to finding out the truth. A forensics team without the proper knowledge to use the tools may only find what the malware wants them to find. Although these tools do help with tracking down who is truly responsible, it sometimes may not be enough.

One of the biggest problems with Computer Forensics is the use of the Trogon Horse Defense. The deceptive nature of the damage that malware can cause may lead to innocent people being blamed for the criminal activities. This defense has been used many times in the past, with mixed results. In the past it was mostly dismissed early on, but has gained more credibility over the years. Jazmine discusses in her article about how much this defense is actually used and verified as true. In the case of child pornography, this defense is used, but with no success. She states that in an interview with a computer forensics specialist, that in over 300 cases of child pornography he has dealt with, none of their proposed guilt was caused by a malware infection. With this sort of crime, much of the evidence is found off the computer in forms of DVD's and camera, rather than just on a computer where malware may have put it there.

Malware can also be deceptive to a forensics team because of how well some can go unnoticed. It can take from days to months for a specific piece of malware to get added to an anti-virus directory. If the malware used is not in the directory, it will take a keen eye by the investigator to find that it even exists. Due to this fact, whether or not anti-virus finds a suspicious program or not is not a definitive answer as to the innocence or guilt of the investigated party.

Conclusion

Malware makes finding the truth in cybercrimes more of a hassle. The first reason is it can mistakenly incriminate someone that had nothing to do with the crime. The editing of system files may lead a may lead a perfect trail to the innocent party. It also may hide itself very well, and its deeds may never be discovered. These factors mean that any forensics done on a computer must be done methodically and with the proper knowledge. With the proper use of machine code dissecting and forensics tools, the true cause of the crime can be uncovered.

References

Ulloa, Jazmine. "Viruses can lead to child porn on your computer." The Brownsville Herald (Texas). (November 15, 2009 Sunday): 918 words. LexisNexis Academic. Web. Date Accessed: 2015/09/27.

"Computer forensics has taken on increasing importance in a complex world.." The Minnesota Lawyer (Minneapolis, MN). (June 15, 2009): 1270 words. LexisNexis Academic. Web. Date Accessed: 2015/09/29.