Effect of Electronic Evidence Captured by Honeypots

Yi Wang
Department of Information Science and Technology, East China University of Political Science and Law, Shanghai, 201620, China

Abstract: Honeypot technique can be used as an active evidence capture method, which is effective in complex case investigation. However, it use temptation as the first step in evidence capture, much debate is emerging which compare it with entrapment. Through analyzes the honeypot technique, this paper suggests evidences principles when using honeypot as evidence capture method.
Keywords: Honeypot, Electronic evidence, Evidence effect

1. Introduction

Nowadays, many cases are related with information technology, electronic evidences become more and more important in evidence collection. Since easy hidden, easy modification and erase, etc., these features become obstacles in evidence collection, especially in complex case investigation. Traditional evidence collection is executed afterwards, which will omit many effective evidences. Honeypots as a new forensic method can overcome such shortage. It can collect evidences when attack is happening. On another hand, honeypot technique can also be used as a confronting anti-forensic method when more anti-forensic techniques are using.

With above advantages, some important online resources use honeypot technique as a detection and active forensic method. If attacking happens, honeypot can record details of intruder's action and preserve evidences, which can be used in court later. However, current laws are not clearly mentioned how to use such evidence. The core debate is focused on its procedural legality, and whether it is suitable by using temptation in evidence collection.

2. Comparing Honeypot with Entrapment

Honeypot is a security resource who's value lies in being probed, attacked or compromised[1]. From above definition, it is clear that if no attack happens to honeypot, it will not embody its value. From technical point of view, the vast majority of connections to honeypot belong to real attacks. Honeypot not like Intrusion Detection System (IDS), which needs to distinguish a real attack from huge network traffic and inevitably generates false negatives and false positives that haven't been solved yet. If there is no attack, connections to honeypot is zero. If there are, it is definitely attacks. Therefore, honeypot records the information which has high value, and it lightens the workload for finding out useful information.

Someone said honeypot using temptation which is similar with entrapment. So whether the evidence captured by honeypot is suitable is arguing. American legal definition of entrapment is: **A person is 'entrapped' when he is induced or persuaded by law enforcement officers or their agents to commit a crime that he had no previous intent to commit[2].**The criteria that judging one's behavior forms entrapment or not, the key point is whether it will let common people without criminal intent emerges criminal intent. If it will then it is not suitable, if not then

suitable. Chinese law doesn't exclude police encouragement, but it is strictly limited. Abusing police encouragement will result in entrapment. Therefore, many countries allow police encouragement but reject entrapment.

Let's look at the practical records captured by honeypot. Almost all records are referring to unauthorized access. Honeypot products are designed as when unauthorized access occurs, the connection is relocated into honeypot, or it will be treated as a legal and normal access. Therefore, honeypot catches those who have already had criminal intent and implemented. It doesn't belong to entrapment.

3. Other Legality Challenges

Although there are many benefits using honeypots to capture electronic evidences, several legal challenges it has to face: privacy and joint liability.

(1) Privacy

Since a honeypot is located in a machine or a network, information stored in these places is monitored by the honeypot, so it is convenience for the honeypot to access. On the other hand, if intruders break into the honeypot, they maybe use the honeypot as a platform to exchange information or as a relay station to personal chatting, which will be captured by the honeypot. Above cases will involve owners of stored information and intruders' privacy. In article [3], it suggests to use "Platform for Privacy Preferences" (abbreviated as P3P) to solve the latter case. Wherever you enter a website, it will clearly remind you that your private information will be used in this site, you can negotiate with the website how to do next. Today P3P is accepted by more and more people, but it is not mandatory.

(2) Joint liability

If a honeypot is broken and controlled by attackers, it is possible that attackers use honeypot as a springboard to break other systems. If the other system is successfully intruded, though operators of a honeypot don't break the system, what joint liability they should be taken? Or if operators of a honeypot aren't aware of their system is controlled by hackers, but the honeypot is used to store and forward prohibited information, what responsibility they should be taken?

In order to answer above questions, let's discuss the situation further. There are two kinds of cases to be considered: one is the honeypot is attacked by intruders with unknown technique or the flaws that don't set deliberately by operators of the honeypot. The other is the honeypot is attacked through the flaws set deliberately by the operators. In the first case, attacked honeypot likes a bot in a botnet, it is a victim. From technique point of view, attackers' skill is superior. Under this circumstance, operators of the honeypot should take the same joint liability as the owner of a bot.

In the second case, the intruder breaks the honeypot through the flaw it deliberately set. Although the intruder may delete his/her intrusion traces, from the angle of the management, the operators of the honeypot should discover or sense the abnormal things happens since those flaws are baits, who set the baits should monitor whether the baits are touched. Under this circumstance, the joint liability the operators should be taken is greater than the first case, since

it refers to lack of management. So using honeypots should be very careful, and as far as possible to reduce the risk of applying honeypots.

4. Evidences Effect Captured by Honeypots

Through above analysis, it is clear that the evidence captures by honeypots can be used in court, since it is satisfied three elements of evidences: objectivity, relationship and legality. Honeypot technique has been matured for years. There are several typical honeypot products are sold in market or open source, such as BackOfficer Friendly, Specter, Honeyd, Mantrap, Honeynet, etc. Their effect is examined by practice. From technical point of view, the objectivity can be guaranteed. Relationship also can be ensured by the mechanism designed by honeypot. Because honeypots only record intrusion information, therefore the evidence captured by honeypot is definitely associated with intrusion cases. Finally legality, in section 2 we analyzed honeypots and compared it with entrapment, then we draw the conclusion that honeypots are not entrapment. So the method it used is legal and can be accepted by law.

When admissibility is settled, we now focus on its evidence effect. Evidences captured by honeypots belong to electronic evidences. They are stored as files, like logging, packets, etc. Therefore, all principles applied on electronic evidences also can be used on evidences captured by honeypots. Here, we put our focus on their special aspects.

In section 3 joint liability, a case is mentioned that if a honeypot is intruded, it can be used as a springboard to attack other systems, or it can be as a transfer station to store contraband. The operator of the honeypot will take the joint liability. From the evidence effect's point of view, if the evidence is valid, it should maintain its integrity. Therefore improve the reliability of honeypots is very important. In order to reduce the risk of deploy honeypots and maintain their evidences' effect, following matters should be noted:

(1) According to practical requirements select suitable honeypot products.

There are two types of honeypots: production and research. On the basis of level of interaction, honeypots are classified as three categories: low, medium and high. Honeypots own lower the level of interaction less the risk it will sustain. On the other hand, lower the level of interaction it has fewer information it will get from attackers. Production honeypots often have low level of interaction. And research honeypots have high level of interaction. Most enterprises use honeypots to reduce threats their system facing and protect their resources, so production honeypots are preferred. Only academy and institute use research honeypots to study hacker's intrusion method and find out new attacking tools and ways.

(2) Clear the goal and strategy of your honeypot

In order to ensure the legality of your honeypot, the goal and strategy of your honeypot system should be taken into account. Then outlines the reasons why your honeypot is deployed, and what kind of information your honeypot collects. And Document all these details, and guarantee that no misconception will be made what your honeypot is for.

To clarify how to clear the goal and strategy of a honeypot, we give an example. In worm research

field, it is an effective way to deploy a distributed honeypot system to capture more information about the worm to be studied. In article [5], they set such a distributed honeypot to detect red code worm as their research object. Since the deployment is based on research background, the goal is to find out the relationship between the number of honeypot nodes and IP address numbers of a subnet. The strategy is to using high interactive distributed honeypot, which install Windows 2000 operating system without patches, and IIS web server, the object worm is red code with random scanning strategy. The strategy records how to deploy distributed honeypot nodes and the number it settled in every subnet. All research procedure has detailed records and clear topology map.

The advantages of clear the goal and strategy of a honeypot is when your honeypot is involved in attacks, it is easy to determine whether your system is under control, and your configuration can help you clarify how much liability you should take in the attacking event.

(3) Don't ignore your honeypot

When deploying a honeypot, you should pay close attention to your system, knowing its current status, finding out whether it is attacked. When an attack happens, as early as possible to collect evidences to determine when the attack happens, what kind of method it used, and most importantly ensure these evidences are not be damaged or polluted.

In practice, notice above points will reduce the risk of using honeypots. However, sometimes you do what you can do, dispute still exists. Especially, in court more questions about whether your system is losing control. In todays' level of technology, we can't answer all questions. Considering justice and efficiency principle, if there is no obvious evidence proving that honeypots is losing control, following guidelines can be applied.

Guildeline1: Evidences that qualified witnesses believe are true should be accepted.

The objectivity embodies the most effectiveness of electronic evidences. Qualified witnesses are normally technical staffs who are familiar with electronic records generated or stored by honeypots. In their daily life, they maintain or interact with honeypots, and understand the principle how these records are generated, or they observe, monitor and study the real procedure of electronic records created. Otherwise, to a certain extern they are close to the records and have ability to analyze, test and check the records. If honeypot system appears abnormal or error, they have the greatest chance to know and leave a record of relative matters. Even if there is nothing happens, a qualified staff should also leave relative records to illustrate the system's status.

Once these qualified witnesses are in court, their role may be located as compound witness. The author thinks that although these people are familiar with the honeypot, from technical point of view, they can be regarded as honeypot experts in their organizations or research field, but they also experience the whole procedure. They observe the honeypot's records, monitor the honeypot's status. From this aspect, they are witnesses of the running status of the honeypot. Therefore, author is more inclined to regard them as lay witnesses with experts' knowledge.

Guildeline2: Proving that a honeypot is normal in critical moment, the honeypot can be deduced that is in normal, evidences recorded by the honeypot should be accepted.

Electronic records have non-intuitive and vulnerable attributes, which make it difficult to be analyzed directly. Therefore, it is significant to use presumption method to prove the truth of the electronic records. In many cases, the status of the system decides the truth of electronic evidences. That is to say, to prove the truth of the electronic evidences can be transferred to prove the security of the system which generates the electronic evidences.

This deduction is made by the correct evaluation on a honeypot. Non-professionals are difficult to give valuable opinions. If a honeypot is in argument that whether it is under control, it is necessary to invite experts to evaluate the whole system, then draw their conclusions.

5. Conclusion

Through analyzing how honeypots record the intruders' information, and facing legal challenges, this paper gives suggestions on how to us evidences captured by honeypots, and maximize their probative force. Honeypots technique is very useful in information security. It is also an important method to collect valuable information from attackers. Although this technique is still in development, and legal problems are not settled down completely. But its prospect is bright.

Acknowledgement

This paper is supported by Humanities and Social Sciences project of Ministry of Education, project number: 11YJCZH175 .

References

[1] Lance Spitzner, Honeypots-Definitions and Value of Honeypots．http：//www .enteract.com ／lspitz／honeypot.html, 2001.

[2]Black, Henry Campbell, Black's Law Dictionary (7th Ed.), New York: Kluwer Law International.

[3] Wang Jianhong, He Xiaoxing, Research on the Technical and Legal Issues of Collecting Evidence by Honeypot, Computer Science, Vol.38, No.8,Augest,2011, pp121-124.

[4]Lance Spitzner, Honeypots: Tracking Hackers, Pearson Education Asia Limited and Tsinghua University Press, 2004.

[5] Wang qi, Wu bing, Yun Xiaochun, Research on The Deployment Strategy of Distributed Honeypot Based on Internet Worm Detection, Control & Automation, 2007, 23(3), PP65-67.

通信方式：
地址：上海市铜川路 1780 弄 7 号 503 室，邮编：200333
电话：13564998900
邮箱：wangyi@ecupl.edu.cn 或 tracy.wy@263.net