Chapter XLV
Bouncing Techniques

Stéphane Coulondre
University of Lyon, France

ABSTRACT

Police investigation methods and tools are very efficient today in tracking down a cyber-attack. As a consequence, skilled cyber-terrorists now use some particular techniques in order to hide their real electronic identity. They can even mislead the investigators by showing another identity. Unfortunately, these techniques increasingly become widespread. We present several of these techniques and show how they can either help or betray attackers. An important conclusion of this paper is that unfortunately nowadays anonymity is practically attainable. The solution can not only rely on technology. International collaboration and information sharing is a key to this problem.

INTRODUCTION

In order to make it difficult to track them down, cyber terrorists do not directly use their own computer to attack a target, especially if the target is in the same country as they are. Indeed, it is very often technically possible nowadays to gather enough information on the attacker to know where the attack has come from. For these reasons, they commonly use bouncing techniques. These techniques aim at hiding their real identity or, more precisely, at using another real cyber identity. In this case, the police are first confronted with a wrong suspect, thus they have to find the previous computer in the attack chain, and so on. This can be a very difficult task, legally and technically.

We present basic types of bouncing techniques, their pros and cons, and discuss their efficiency and anonymity. We explain how and why these bounces are made possible. We also illustrate why international collaboration is essential. We finally show that it is very hard, if at all possible, to reconstruct the attack chain in order to find its origin.

BACKGROUND

Every computer on the Internet has an address that is either public or private. This address can reveal the identity of the owner, either by means of the *whois* protocol, which is a protocol widely used for querying the addresses and domain name registration databases, or with the help of Internet service providers (ISPs). When an attacker is using the Internet, every visited Web site and every attacked computer can virtually know where he or she is. This is indeed a huge drawback for cyber terrorists, who aim at keeping this information secret.

However, not every activity on the Internet is logged, because it would represent, if ever possible, a huge amount of information. Therefore, some techniques, namely forensic techniques (Jones, Bejtlich, & RoseReal, 2005), which have been greatly developed in these last years, aim at gathering traces whenever an attack has been performed. These techniques generally give some good results and the origin of the attack can often be traced back. Therefore, skilled cyber terrorists now rely on new sophisticated techniques to cover their tracks, based on bouncing techniques. These bouncing techniques aim at replacing the final origin of the attack with another address.

Bouncing techniques can be divided in two types:

- Those using the Internet identity of someone who is unaware of it
- Those using the Internet identity of someone who is aware of it (Notice that it does not mean that this person is aware of the corresponding kind of activity.)

BOUNCING TECHNIQUES

There are essentially two popular ways of getting access to the Internet using someone else's name. The first one relies on the poor security design of the first Wi-Fi networks, particularly those conforming to the 802.11b norm (Edney & Arbaugh, 2003). The second one relies on public proxies that can be found in the Internet. Each of them has advantages and drawbacks for a cyber terrorist.

The 802.11b access points have a well-known design flaw. In no more than five minutes, it is possible for a skilled hacker to break the cryptographic shared key (Fluhrer, Mantin, & Shamir, 2001), allowing a connection to this access point, thus to the Internet. This connection, including attacks, is realized in the name of the access point owner, who is not aware of it (unless using a specific intrusion detection system, which is very rare for individuals). One the favorite games of some hackers is to drive in an urban area with a laptop that can automatically detect 802.11b waves, which often overlap the streets, and construct a geographical map of encrypted (and unencrypted) 802.11b networks. Whenever an encrypted key has been detected, the hacker can break it from his or her car without being detected. Databases of broken keys and geographical 802.11b network positions are then published on the Internet.

Proxies are computers that agree to act in their name for a client (Luotonen, 1997). There are different types of proxies; the most used being *http* and *socks* proxies. Http proxies allow for Internet browsing, and socks proxies allow for almost all major Internet protocols. Public proxies can be roughly divided into three types:

- Misconfigured proxies, which allow everybody to use it without the owner being aware of it
- Free proxies, working with some organizations, which are then aware of it, but that could be used to gather personal information
- Nonfree commercial proxies, which aim at providing anonymous services, but nobody can truly verify this
- Hacked proxies, which are, by definition, made anonymous by the attackers

At the present time, very few public proxies can guarantee to be really anonymous, because there is no general way of knowing if the proxy is really free, misconfigured, or hacked, or if it keeps logs of activ-