Pharming Attack Designs

Manish Gupta
State University of New York at Buffalo, USA

Raj Sharman
State University of New York at Buffalo, USA

INTRODUCTION

Pharming is emerging as a major new Internet security threat. Pharming has overtaken "phishing" as the most dangerous Internet scam tactic, according to the latest Internet Security Intelligence Briefing (VeriSign, 2005). Pharming attacks exploit the design and implementation flaws in DNS services and the way Internet addresses are resolved to Internet protocol (IP) addresses. There are an estimated 7.5 million external DNS servers on the public Internet (MF-Survey, 2006). Pharming attacks manipulate components of the domain and host naming systems to redirect Internet traffic from one Web site to a different, identical-looking site in order to trick users into entering personal and sensitive information on their fake site. Financial services' sites are often the targets of these attacks, in which criminals try to acquire personal information in order to access bank accounts, steal identities, or commit other kinds of fraud. The use of faked Web sites makes pharming sound similar to e-mail phishing scams, but pharming is more insidious, since users are redirected to a false site without any participation or knowledge on their part. Pharming is technically harder to accomplish than phishing, but also sneakier because it can be done without any active mistake on the part of the victim (Violino, 2005). The greatest security threat lies in the fact that a successful pharming attack leaves no information on the user's computer to indicate that anything is wrong.

The Etymology and Metaphor: "Pharming"

The coinage and usage of the word pharming has origins in metaphorical connection with "farming." The metaphor tunes with the characteristics and forms of the attack where attackers bring people onto a property they control, without having to "phish" for them. Pharming has also been called "phishing without a lure." "Pharming" also refers to manufacturing of pharmaceutical products via genetic engineering of farm crops and animals. Another form of pharming, known as gene pharming, is a biotechnological process in which the DNA of an animal, usually livestock, is altered so the animal produces human proteins for pharmaceutical use. The proteins appear in the blood, eggs, or milk of the animal.

Organization and Contribution of the Article

The article has a two-fold contribution. First, it presents classification of pharming attack designs in light of DNS components and characteristics. The second contribution is survey and synthesis of different modes and channels of pharming attacks based on design and implementation of DNS components and services.
The article is organized as follows. The Preliminaries section provides preliminaries on DNS that are extensively used in the explanation of attack designs in later sections. The section on Attacks and Designs presents, in detail, attack designs from DNS service and client perspectives, and classifies pharming attacks into three types based on location sensitivity of the DNS service. The next section on pharming incidents discusses successful pharming attacks and their methodologies to provide insights into the functioning of such attacks.

PRELIMINARIES

Social Engineering

Social engineering is a technique used by hackers or other attackers to gain unauthorized access to secure systems through obtaining the privileged information by manipulating human behavior. Mitnick (2004) iden-

tifies four distinct stages of the "Social Engineering Cycle": research, developing rapport and trust, exploiting trust, and utilizing information. Organizations and individuals alike must equip themselves with the knowledge on social engineering attacks such as what information can be used, how information divulged could precipitate attacks, how the attacker develops the attack, and in what forms the attack may appear.

Domain Name System: Concepts

The DNS is the method by which human-readable Internet addresses such as mgt.buffalo.edu, which are easy for people to understand and remember, are converted into the equivalent numeric IP address such as 128.205.202.194. This translation service is provided to the users and application processes either by the local host or from a remote host via the Internet. The DNS server (or address resolver) may communicate with other Internet DNS servers if it cannot translate the address itself. Following the example from above, the Web site that we referred to as mgt.buffalo.edu has the IP address 128.205.202.194. DNS implements a client server process architecture, where the client side is represented by a resolver, which submits queries to and receives responses from the DNS application itself.

Domain Name System: Components and Structure

DNS is a database that contains the mapping information in both distributed and hierarchical structure and can be represented as an inverted tree. All of the domain names that are registered with a naming authority are held within this database along with their associated IP addresses. The general structure of a domain name is hierarchical. For example, .edu is a top-level domain (TLD) in domain mgt.buffalo.edu. At least one root name server is associated with each TLD. The Internet today has a total of 13 root servers that are distributed geographically. Sub-domains can be created to an arbitrary level below each TLD. Domain registrars, within Internet context, can grant the authority over sub-domains to the organizations that manage those sub-domains. The boundary of authority that is granted within DNS is determined by means of the specification and implementation of zones. An example would be mgt.buffalo.edu, where there is:

- a TLD zone (.edu)
- a sub-domain (buffalo.edu) which is a zone,
- a sub-domain of buffalo.edu (mgt.buffalo.edu) which is a zone

Typical Transactional Flow for a DNS Query

Figure 1 (adapted from Stewart, 2004) shows a query and transaction path when the IP address of a domain name is requested. The flow of information and hierarchy of DNS servers is presented in the Figure 2 as: (1) Local-ns, (2) ISP-ns, (3) R-ns, and (4) A-ns. Explanation of each step from Figure 1 is presented below in the box.

The SP-ns is authorized to make queries on the user's behalf to as many nameservers as needed in order to find the answer. This is known as recursion. The root-level nameservers contain information about what nameservers hold the specific information about the hosts in each top-level domain. This information is known as the authority record for a domain, which contains pointers to the servers that are authoritative for a domain.

PHARMING ATTACK TYPES AND DESIGNS

Pharmers have a variety of motives and objectives, primarily malice and monetary gain. In several documented cases, pharming has caused disruption and malicious use of registrant's Internet services, discussed in detail in the section on pharming incidents. The pharming attacks are classified into three types as represented in Figure 2. The following subsections discuss pharming attack designs in these categories. Table 1 presents attack designs and their classifications. The second column of the table shows the section of the article in which that particular attack is discussed.

PHARMING ATTACK DESIGNS COMPONENT

This section presents pharming attack designs that fall under the category Internet name services (INS) as illustrated in Figure 2 and Table 1.