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-
Pharming Attack Designs

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.
Related Content

Employing Cost Effective Internet-Based Networking Technologies to Manage B2B Relationship: The Strategic Impact on IT Security Risk
[www.igi-global.com/article/employing-cost-effective-internet-based/65729?camid=4v1a](www.igi-global.com/article/employing-cost-effective-internet-based/65729?camid=4v1a)

A Methodology for Developing Trusted Information Systems: The Security Requirements Analysis Phase
[www.igi-global.com/chapter/methodology-developing-trusted-information-systems/23132?camid=4v1a](www.igi-global.com/chapter/methodology-developing-trusted-information-systems/23132?camid=4v1a)

Traditional Knowledge and Intellectual Property
[www.igi-global.com/chapter/traditional-knowledge-intellectual-property/13537?camid=4v1a](www.igi-global.com/chapter/traditional-knowledge-intellectual-property/13537?camid=4v1a)

[www.igi-global.com/article/six-view-perspective-framework-system/43057?camid=4v1a](www.igi-global.com/article/six-view-perspective-framework-system/43057?camid=4v1a)