available at www.sciencedirect.com

ScienceDirect

journal homepage: www.elsevier.com/locate/diin

Digital Investigation

Impersonator identification through dynamic fingerprinting

Chad M.S. Steel[*], *Chang-Tien Lu*

Computer Science Department, Virginia Polytechnic Institute, Haycock Road, Falls Church, VA 22043, USA

ARTICLE INFO

Article history:
Received 18 August 2006
Received in revised form
10 March 2008
Accepted 17 March 2008

Keywords:
Digital watermark
Phishing
Intellectual property
Forensics
Fingerprinting
Impersonation

ABSTRACT

Tracking the source of impersonation attacks is a difficult challenge for investigators. The attacks are frequently launched from botnets comprised of infected, innocent users and web servers compromised by malware. Current investigative techniques focus on tracking these components. In this paper, we propose the Automated Impersonator Image Identification System (AIIIS), which allows investigators to track images used in impersonation attacks back to the original download from the source. AIIIS accomplishes this by digitally encoding the IP address, server, and time of the image download into the image itself through a digital watermark. AIIIS differs from other image fingerprinting techniques in its combination of dynamic fingerprinting and spread spectrum data hiding. Additionally, the intended goal of AIIIS is tracking impersonation attacks, where the image is a tool used, whereas in most digital rights management techniques, the misuse of the content itself is the primary concern. Our experiments show that the AIIIS system permits recovery even after post-acquisition manipulation of the image, making it a significant addition to the fight against impersonators. The deployment of a pilot of AIIIS was successful in identifying the source of an impersonation attack, and further success is expected with full deployment.

Published by Elsevier Ltd.

1. Introduction

Phishing schemes and online trademark infringement are both on-the-rise crimes which rely on impersonation. Phishing attacks hit one in four Internet users each month (AOL/NCSA, 2005), and annual losses due to phishing are projected to be anywhere from US$100 Million to US$1 Billion (Goth, 2005), and are expected to continue to increase. Online trademark infringement is used to lure unsuspecting users to buy from less than reputable sources. An example trademark infringement incident may involve an attacker who uses Viagra branding and images to lure an individual into purchasing stolen or counterfeit pharmaceutical products.

A typical impersonation attack uses two components – an email message sent to a large number of users and a website those users are encouraged to visit. Through obfuscation of the URL and basic social engineering tactics, an unsuspecting user is enticed to click on a link in the email. The link takes the user to a look-alike site, where their username and password (or other personally identifiable information) are captured for malicious use or they are tricked into purchasing goods from a shady source. Typical targets include large financial institutions, pharmaceutical companies, and online merchants, e.g., Citibank, Bank of America, Pfizer, and eBay.

The value of the Automated Impersonator Image Identification System (AIIIS) is based on the methods used in many impersonation schemes. The emails sent are frequently transmitted from infected zombie machines, making tracking ineffective. Likewise, many schemes now use infected web servers not directly tied to the attackers as well. The construction of the emails and sites, however, involves the acquisition of the original site graphics and layout to be able to fool the unsuspecting victims. Frequently, the site is visited from the origin machine of the phishing attacks – since the visit is not

[*] *Corresponding author*. Tel.: +1 610 639 3884.
E-mail address: csteel13@vt.edu (C.M.S. Steel).

1742-2876/$ – see front matter Published by Elsevier Ltd.
doi:10.1016/j.diin.2008.03.001

malicious, server-based analysis isn't likely to pick up the first visit as suspicious (or later identify it as such) using existing techniques. A review of 148 phishing sites listed on millersmiles.co.uk revealed 42 sites active and viewable over the course of three weeks. Of the active phishing sites, 23 of the 42 (55%) used local copies of images that were verified to be exact matches to those on the corresponding real sites. The other 19 active phishing sites linked directly to images on the corresponding real sites (Millersmiles, 2006).

To-date, most impersonation defense mechanisms are provided through prevention and/or detection controls. Products like AntiPhish, which comprises a browser extension that warns users when visiting untrusted sites (Kirda and Kruegel, 2005), fall into the prevention category (as do anti-phishing toolbars (Netcraft Inc., 2006), image-based authentication (Topkara et al., 2005), and two-factor authentication (Geer, 2005)). Techniques like Dynamic Security Skins, a method of user image comparison for authentication (Dhamija and Tygar, 2005), fall primarily into the detection category (as do server-log analysis tools like Corillian and chat monitoring from MarkMonitor (Geer, 2005)). Limited work has been done in relation to response controls – those which allow after-the-fact investigation of activity.

To address the response gap, AIIIS provides a mechanism by which images can be tracked from the point of origin (the website being spoofed in an impersonation attack) through the insertion of unique watermarks for every download. By generating a string containing details from each image request, including server name, requesting IP address, and date/time of the initial request, a unique token is created which can be correlated with entries in the web server log. This unique token is dynamically embedded in each individual image download as a symmetrically encrypted and hidden watermark for later recovery from spoofed sites. In addition to the challenges that watermarking focuses on, AIIIS has a similar purpose to steganography in that both the image and the covert channel information need to be transmitted and reconstructable, and that the uncovering and altering of the covert channel information is an undesirable event (Wang and Wang, 2004).

AIIIS is novel in that it differs from prior art both in its execution and its intent. In its execution, AIIIS uses overinsertion, the practice of inserting multiple copies of the message, to provide further resilience to alteration over single-insertion techniques. Additionally, AIIIS applies transform-based insertion over the entirety of an image instead of on a block-basis. For intent, AIIIS is designed to investigate attacks after-the-fact and dynamically embed user data in the image at the time of request, instead of static strings identifying the copyright holder. Finally, to protect the string from disclosure or effective alteration, AIIIS uses simple symmetric encryption with Advanced Encryption Standard (AES) (National Institute of Standards and Technology, 2001) and/or the Data Encryption Standard (DES) (National Institute of Standards and Technology, 1993) and a server-specific key.

This paper details how AIIIS applies spread-spectrum techniques and dynamic fingerprinting to contribute a robust solution to track impersonators. In Section 2, a pilot implementation is used to illustrate the use of the system. In Section 3, the four major approaches to investigate impersonation schemes are outlined and the applications of prior art to the schemes are defined. Section 4 introduces the AIIIS system and details the processes for string extraction and insertion. An error rate analysis is also provided which mathematically quantifies the resiliency of the system against individual bit error probabilities. In Section 5, the experimental results of image recovery are provided for an array of image sizes and three key operations – scaling, compression, and cropping. Finally, a comparison of single-insertion, block-based spread spectrum recovery likelihood is compared with that of AIIIS. Section 6 discusses the results and applicability to other areas, and Section 7 provides concluding remarks.

2. In practice

AIIIS was used successfully by a major retailer to track down the source of a counterfeit operation. AIIIS was deployed by the retailer as a pilot project, and had success within the first two months in thwarting a sophisticated attack.

2.1. *Background*

The retailer in question was subject to frequent phishing attacks, with an additional problem of having counterfeit goods sold using their branding. As such, the retailer was looking for solutions to track down the counterfeiters and piloted AIIIS as one of the tools in their suite. As the impersonation attacks became more sophisticated, simple monitoring of brand misuse online was insufficient. Shutting down rogue websites as they appeared became a fruitless exercise, and the company decided it needed to pursue the individuals perpetrating the attacks. The details of one attack and its investigation are noted below.

2.2. *Attack methodology*

The attack in this case consisted of several different ‘‘companies’’ setup with the same basic website template, but slightly different company names and text. The websites were all hosted on what appeared to be hijacked machines, primarily in Southeast Asia. Similarly, the DNS entries for the company were numerous and appeared to be registered through a series of hacked accounts. The websites used the branding and logos of the original retailer to give the appearance of being authorized merchants, but in reality were counterfeiters using the brand recognition to push their product. Purchases had their credit cards charged from one of several China-based businesses, and received forgeries of the real product which looked similar but did not meet the quality standards of the originals.

2.3. *Investigation*

The impersonating sites began coming to the attention of the retailer after consumer complaints about substandard goods. The goods were purchased online, and the individuals who complained provided the names of the sites where the purchases occurred.