Available online at www.sciencedirect.com

ScienceDirect

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

Computers & Security

# Design and evaluation of the highly insidious extreme phishing attacks

*Rui Zhao* [a], *Samantha John* [b], *Stacy Karas* [c], *Cara Bussell* [c], *Jennifer Roberts* [c], *Daniel Six* [c], *Brandon Gavett* [c], *Chuan Yue* [a,*]

[a] *Colorado School of Mines, Golden, CO 80401*
[b] *Emory University, Atlanta, GA 30322*
[c] *University of Colorado Colorado Springs, Colorado Springs, CO 80918*

ARTICLE INFO

*Article history:*
Received 26 February 2017
Received in revised form 29 July 2017
Accepted 16 August 2017
Available online 24 August 2017

*Keywords:*
Web
Phishing
Susceptibility
Single Sign-On
Toolkit

ABSTRACT

One of the most severe and challenging threats to Internet security is phishing, which uses spoofed websites to steal users' passwords and online identities. Phishers mainly use spoofed emails or instant messages to lure users to the phishing websites. A spoofed email or instant message provides the first-layer context to entice users to click on a phishing URL, and the phishing website further provides the second-layer context with the look and feel similar to a targeted legitimate website to lure users to submit their login credentials. In this paper, we focus on the second-layer context to explore the extreme of phishing attacks; we explore the feasibility of creating extreme phishing attacks that have the almost identical look and feel as those of the targeted legitimate websites, and evaluate the effectiveness of such phishing attacks. We design and implement a phishing toolkit that can support both the traditional phishing and the newly emergent Web Single Sign-On (SSO) phishing; our toolkit can automatically construct unlimited levels of phishing webpages in real time based on user interactions. We design and perform a user study with 194 participants to evaluate the effectiveness of the phishing attacks constructed from this toolkit. The results demonstrate that extreme phishing attacks are indeed highly effective and insidious as over 90% of the participants became the "victims". It is reasonable to assume that extreme phishing attacks will be widely adopted and deployed in the future, and we call for a collective effort to effectively defend against them.

© 2017 Elsevier Ltd. All rights reserved.

## 1. Introduction

One of the most severe and challenging threats to Internet security is phishing, which uses spoofed websites to steal users' passwords and online identities. Anti-Phishing Working Group (APWG) reported that 364,424 unique phishing attacks occurred during the third quarter in 2016. Phishing attacks have been continuously causing serious damage to users and organizations. For example, phishers stole a victim's life savings of 1.6 million (Phishing gang steals victim's life savings of $1.6M, 2012), caused a massive data breach at the South Carolina Department of Revenue (Spear Phishing Attack Cause of Massive South Carolina Data Breach, 2012), and stole university employees' passwords for changing the direct deposit (UC Berkeley iNews: Impact of Phishing Scams on Direct Deposits).

To defend against phishing attacks, researchers have proposed various blacklist-based, heuristics-based, and whitelist-based solutions (Section 6), organizations and communities such as APWG (Anti-Phishing Working Group (APWG)) and PhishTank

* *Corresponding author.*
*E-mail address:* chuan.yue@gmail.com (C. Yue).

http://dx.doi.org/10.1016/j.cose.2017.08.008
0167-4048/© 2017 Elsevier Ltd. All rights reserved.

(PhishTank) have provided phishing reporting and verification services; many vendors have also provided secure browsing systems such as Google Safe Browsing, Microsoft SmartScreen Filter, McAfee SiteAdvisor, and Norton Safe Web. However, phishing attacks have also been quickly evolving to evade the detection and defense (Yue and Wang, 2010), and the battle between phishers and defenders will be long-standing.

Phishers mainly use spoofed emails or instant messages to lure users to the phishing websites. A spoofed email or instant message provides the ***first-layer context*** (e.g., asking for account verification or update) to entice users to click on a phishing URL, and the phishing website further provides the ***second-layer context*** with the ***look and feel*** similar to a targeted legitimate website to lure users to submit their login credentials (Yue, 2013). In terms of the first-layer context, the success of phishing is mainly limited by two constraints (Yue, 2013). One is that if phishing emails or instant messages are suspicious, users would not click on phishing URLs and visit the phishing websites (Downs et al., 2006; Jakobsson and Ratkiewicz, 2006). The other is that phishing emails captured by spam filters (Whittaker et al., 2010) cannot even reach users in the first place. In terms of the second-layer context, the success of phishing is mainly limited by two other constraints (Yue, 2013). One is that phishing websites will trigger warnings if they are detected by browsers, thus security-conscious users would not visit them and submit credentials (Akhawe and Felt, 2013). The other is that if the look and feel of the undetected phishing websites are suspicious, security-conscious users would not submit their credentials (Dhamija et al., 2006; Downs et al., 2006; Hong, 2012; Jackson et al., 2007; Sheng et al., 2010).

In this paper, we focus on the second-layer context to explore the extreme of phishing attacks. In other words, we explore the feasibility of creating extreme phishing attacks that have the almost identical look and feel as those of the targeted legitimate websites, and evaluate the effectiveness of such phishing attacks.

In particular, we design and implement a phishing toolkit that can support both the traditional phishing and the newly emergent Web Single Sign-On (SSO) phishing (Yue, 2013). In terms of the traditional phishing, our toolkit can automatically construct unlimited levels of phishing webpages in real time based on user interactions; in terms of the Web SSO phishing, our toolkit can allow attackers to easily construct spoofed Web SSO login "windows" for Gmail, Facebook, and Yahoo. The constructed phishing webpages and Web SSO login "windows" are almost identical to their legitimate counterparts, potentially making it very difficult for users to identify if they are interacting with real or spoofed websites.

The toolkit can be used by attackers to easily construct and deploy extreme phishing attacks; it can also be used by researchers to easily construct testbeds for performing phishing related user studies and exploring new phishing defense mechanisms. In particular, we design and perform a user study to evaluate the effectiveness of the phishing attacks constructed from this toolkit. The user study results based on 194 participants demonstrate that extreme phishing attacks constructed by our toolkit are indeed highly effective, i.e., insidious. The questionnaire results show that **178 (91.8%)** of the 194 participants were actually not suspicious about the extreme phishing websites that they visited, and the observation results show that **182 (93.8%)** of the 194 participants submitted their credentials to the extreme phishing websites; meanwhile, most of those "victims" were aware of phishing before participating in this study or had been susceptible to some phishing attacks in the past. Therefore, it is reasonable to assume that extreme phishing attacks will be widely adopted and deployed in the future, and we call for a collective effort to effectively defend against them.

The main contributions of our paper include the following: (1) we define and explore extreme phishing attacks and investigate the techniques for constructing them, (2) we design and implement a concrete toolkit that can be feasibly and easily used by attackers to construct and deploy such attacks, (3) we design and perform a user study with 194 participants to demonstrate the effectiveness of such attacks, and (4) we discuss the impacts of extreme phishing on existing phishing defense mechanisms and provide suggestions to users and researchers for them to better defend against such attacks. This journal paper significantly extends our conference paper Zhao et al., 2016.

The rest of the paper is organized as follows. Section 2 reviews the related work on phishing toolkits and testbeds. Section 3 defines extreme phishing attacks and our goal in this paper. Section 4 presents the design and implementation of our toolkit for such attacks. Section 5 presents a user study for evaluating the effectiveness of such attacks. Section 6 provides a discussion. Section 7 makes a conclusion.

## 2. Related work

We review the related work on phishing toolkits and testbeds in this section, and defer the discussion of the related phishing detection and defense techniques to Section 6.

Attackers often use phishing toolkits to construct their phishing websites (Hong, 2012). Cova et al. analyzed a large collection of free underground phishing toolkits (Cova et al., 2008), and found that those toolkits target not only users but also inexperienced phishers (through backdoors) as victims. They also found that most of those toolkits target only one organization, and include the related resources (e.g., HTML, JavaScript, CSS, image, and PHP files) with a limited page depth for replicating a portion of a targeted legitimate website; meanwhile, the links in the replicated webpages are often unchanged and still point to the targeted website, thus the phishing website may easily lose the control of visitors and fail to collect their login credentials. In contrast, our toolkit can replicate many targeted organizations by automatically constructing unlimited levels of phishing webpages in real time based on user interactions; meanwhile, all the links in the replicated webpages are modified to keep holding visitors on the corresponding phishing website and maximize the chances of collecting their login credentials. In addition, Cova et al. (2008) did not report the existence of Web Single Sign-On (SSO) phishing (Yue, 2013) in those toolkits; while our toolkit supports Web SSO phishing as well as the traditional phishing.

Existing phishing susceptibility studies (Dhamija et al., 2006; Downs et al., 2006; Egelman et al., 2008; Jackson et al., 2007; Jagatic et al., 2007; Schechter et al., 2007; Sheng et al., 2010) often use some specific, not very realistic, and non-sharable

Download English Version:

https://daneshyari.com/en/article/4955441

Download Persian Version:

https://daneshyari.com/article/4955441

Daneshyari.com