PhishFarm: A Scalable Framework for Measuring the Effectiveness of Evasion Techniques Against Browser Phishing Blacklists

Reference (recently-published work)

Adam Oest, Yeganeh Safaei, Adam Doupé, Gail-Joon Ahn, Brad Wardman and Kvein Tyers, "PhishFarm: A Scalable Framework for Measuring the Effectiveness of Evasion Techniques against Browser Phishing Blacklists," 2019 IEEE Symposium on Security and Privacy (SP), San Francisco, CA, US, pp. 764-781. doi:10.1109/SP.2019.00049

Full text available:
https://www.computer.org/csdl/proceedings/sp/2019/6660/00/666000a764.pdf

Abstract

Phishing attacks have reached record volumes in recent years. Simultaneously, modern phishing websites are growing in sophistication by employing diverse cloaking techniques to avoid detection by security infrastructure. In this paper, we present PhishFarm: a scalable framework for methodically testing the resilience of anti-phishing entities and browser blacklists to attackers' evasion efforts. We use PhishFarm to deploy 2,380 live phishing sites (on new, unique, and previously-unseen .com domains) each using one of six different HTTP request filters based on real phishing kits. We reported subsets of these sites to 10 distinct anti-phishing entities and measured both the occurrence and timeliness of native blacklisting in major web browsers to gauge the effectiveness of protection ultimately extended to victim users and organizations. Our experiments revealed shortcomings in current infrastructure, which allows some phishing sites to go unnoticed by the security community while remaining accessible to victims. We found that simple cloaking techniques representative of real-world attacks— including those based on geolocation, device type, or JavaScript— were effective in reducing the likelihood of blacklisting by over 55% on average. We also discovered that blacklisting did not function as intended in popular mobile browsers (Chrome, Safari, and Firefox), which left users of these browsers particularly vulnerable to phishing attacks. Following disclosure of our findings, anti-phishing entities are now better able to detect and mitigate several cloaking techniques (including those that target mobile users), and blacklisting has also become more consistent between desktop and mobile platforms— but work remains to be done by anti-phishing entities to ensure users are adequately protected. Our PhishFarm framework is designed for continuous monitoring of the ecosystem and can be extended to test future state-of-the-art evasion techniques used by malicious websites.

PhishFarm: A Scalable Framework for Measuring the Effectiveness of Evasion Techniques Against Browser Phishing Blacklists

IRA A. FULTON SCHOOLS OF engineering
ARIZONA STATE UNIVERSITY

Adam Oest, Yeganeh Safaei, Adam Doupé, Gail-Joon Ahn, Brad Wardman, and Kevin Tyers
{aoest, ysafaeis, doupe, gahn}@asu.edu, {bwardman, ktyers}@paypal.com

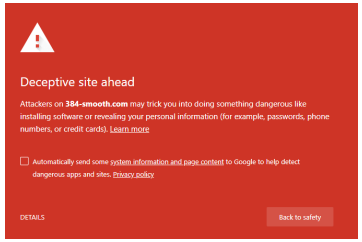
CENTER FOR CYBERSECURITY & DIGITAL FORENSICS

Problem

- Phishing web sites make use of **cloaking** to **evade** security crawlers while displaying content to victims
- Cloaking can defeat modern anti-phishing **blacklists**
- Phishing attacks are growing in volume, compromise users' online security, and incur high mitigation costs

Background: Browser Blacklists

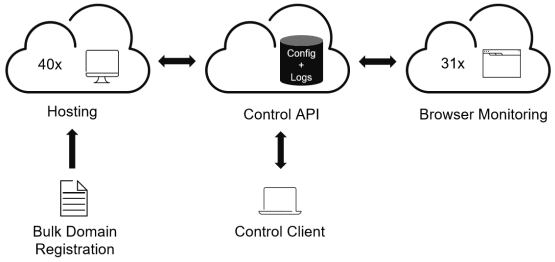
- Widespread "always on" defense against phishing
  - Used in 99% of desktop, ~75% of mobile browsers by worldwide market share
- Effective mitigation for users, but **not proactive**
- Uses extensive detection infrastructure



Motivation

- First controlled study of the **impact of cloaking** on the **anti-phishing ecosystem**
- Identify (and fix) gaps in blacklist coverage
- Improve security of users, stay ahead of attackers
- Develop a robust, re-usable testbed framework

PhishFarm Framework



- **Automated**, scalable framework for testing the effectiveness of cloaking against browser blacklists
  1. **Deploy** large sets of phishing websites (innocuous)
  2. **Report** them to anti-phishing entities
  3. **Monitor** blacklisting status across browsers

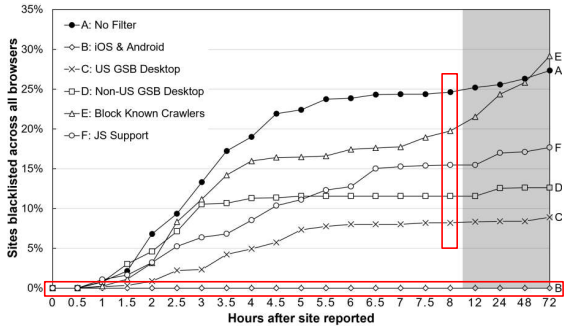
Experiment

- Launched **2,380** phishing sites, unique *.com* domains
- **Cloaking types:**
  - Mobile / desktop user agents
  - Geolocation
  - Javascript
  - Phishing kit *.htaccess*
- Tested **all major browsers**

- Reported to *Google Safe Browsing*, *SmartScreen*, *APWG*, *PhishTank*, and *PayPal*
- Initial tests → responsible disclosure → full tests

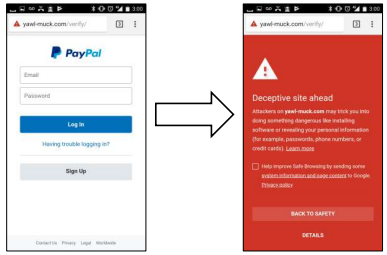
Key Finding: Cloaking Works

- Cloaking slowed blacklisting by ~2 hours & reduced site blacklisting likelihood by 55% in our experiments
- No blacklisting in mobile Firefox/Chrome/Safari (GSB)



Outcomes

- Mobile GSB blacklisting greatly improved
- Industry collaboration, security recommendations
- Framework to be shared and extended



Complete work to appear in the Proceedings of the IEEE Symposium on Security & Privacy, May 2019