

Malicious Proxies

The Web's Evil Twin

Introducing Doppelganger

Introduction

- Who am I?
- Security field since 1998
 - IDS
 - Pen testing
 - Malicious logic analysis
 - Incident response

Proxies

- Focusing on HTTP proxies
- Plenty of reasons to legitimately deploy a proxy

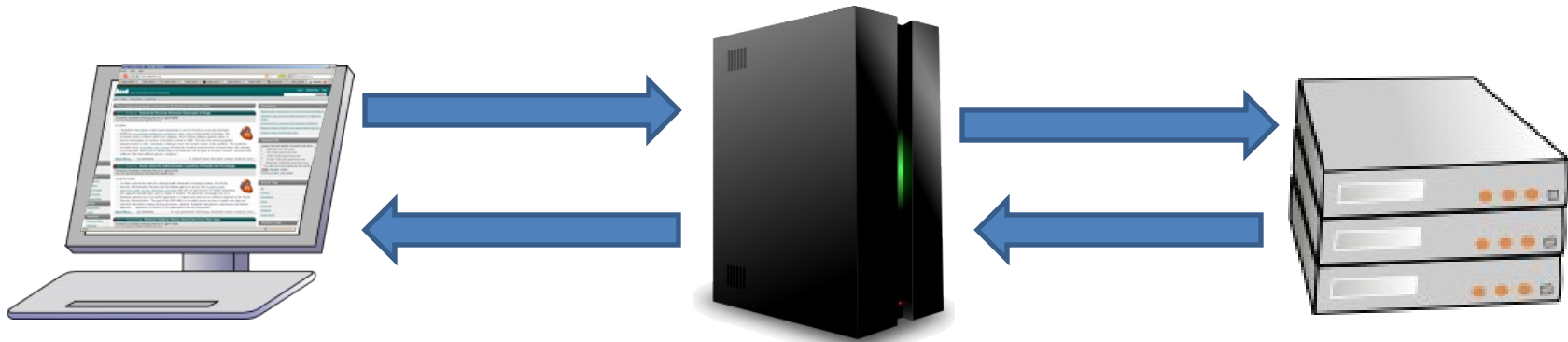
WHO CARES!?

Why a Malicious Proxy

- Come up with as many nefarious ways to distort a users interaction as I can
- Quickly & easily gather potentially useful information

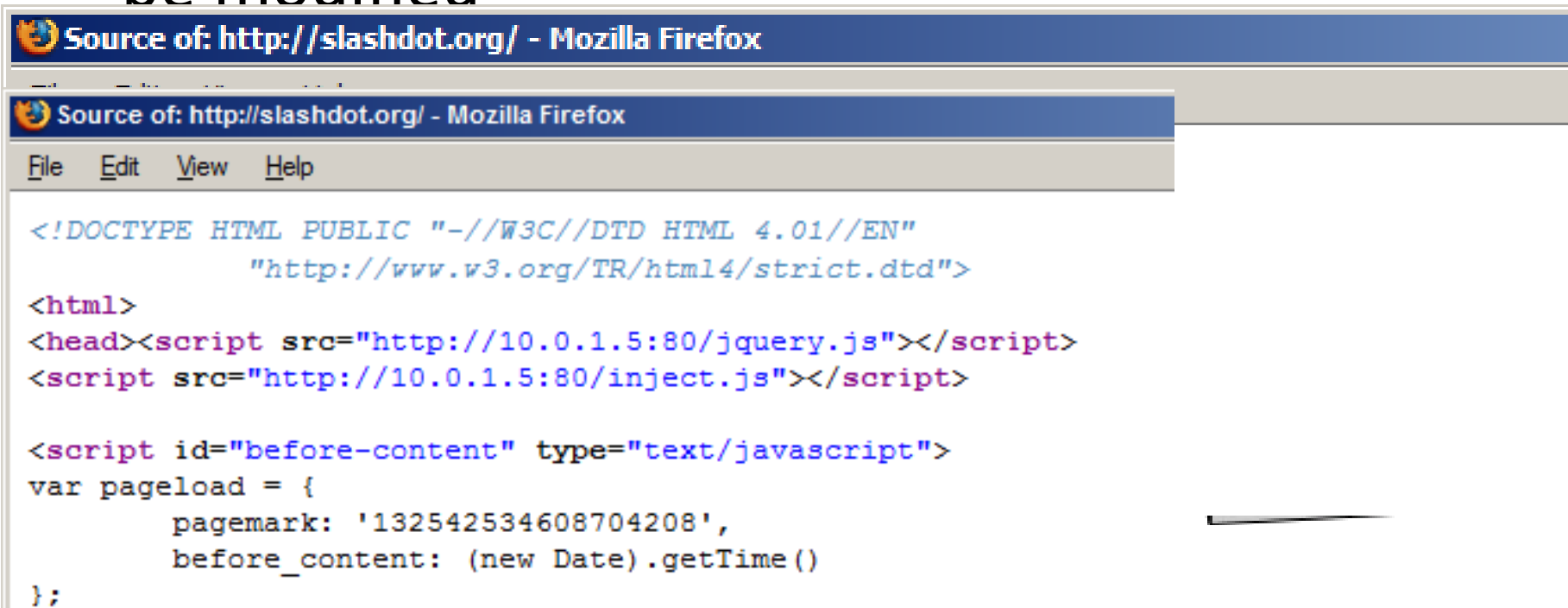
Proxies: Standard

- Client requests a page through proxy
- Proxy request the page from the server
- Server sends the response to the proxy
- Proxy serves the page to the client



Proxies: Malicious

- Similar to a standard proxy, but the data can be modified



```
Source of: http://slashdot.org/ - Mozilla Firefox
Source of: http://slashdot.org/ - Mozilla Firefox
File Edit View Help
<!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.01//EN"
    "http://www.w3.org/TR/html4/strict.dtd">
<html>
<head><script src="http://10.0.1.5:80/jquery.js"></script>
<script src="http://10.0.1.5:80/inject.js"></script>

<script id="before-content" type="text/javascript">
var pageload = {
    pagemark: '132542534608704208',
    before_content: (new Date).getTime()
};
```

Proxies: Malicious Cont.

- Not much different from a standard proxy
- Captures & modifies HTTP responses & requests
- Change the response adding HTML or JavaScript

Malicious Proxies: Modifying Content

- Modify static HTML
 - Cumbersome
 - Need a lot of customization
- Inject JavaScript
 - Considerably easier – find something all pages (should) have: a `<head>` tag
 - JavaScript can modify the DOM in a consistent way, alleviating major customization

Malicious Proxies: Potential Issues

- Inserted JavaScript may be blocked (NoScript)
- Some AJAX heavy sites don't play well
- Most sites use HTTP/1.1 compressed pages
 - Decompress & modify
 - Strip the compression header in the request
- Modifying the page slows down delivery
 - Use JavaScript to let the client make the changes, saving the proxy's CPU

Proxies: Assigning a proxy

- Statically
 - Tedious and not very feasible/easy
- Dynamically via DNS, or DHCP
 - DNS (WPAD Record)
 - DHCP Option 252
 - Only works with browsers set to use auto-proxy detection
- Others

Doppelganger: Goals

- Personal
 - Learning exercise in Ruby
 - code != pretty
 - documentation = sparse
 - proof of concept
- Tool
 - Semi-Plug & Pray
 - Easy to use
 - Target all sites out of the box

Doppelganger

- Can be used to update WPAD DNS record
- Greasemonkey for the Web, not just Firefox
- Can use Google APIs for hosted JavaScript libraries that are commonly used
 - (jquery, jqueryui), (prototype, scriptaculous), mootools, dojo, swfobject, yahooui, and/or extcore

Doppelganger: Requirements

- Ruby
 - webrick
- OpenSSL library for Ruby
- Ruby Gems
 - dnsruby
 - packr
 - windows-pr*
 - win32-process*

Doppelganger: Generic Capabilities

- Can operate on both the HTTP Request & Response
 - Add/Remove/Modify HTTP Headers
 - Inject/Remove HTML
 - Includes JavaScript

Doppelganger: Specific Capabilities

- Insert Calling Card
- Inject Flash Applets
- Scrape & Decode Basic Auth
- Steal submitted form data
- Other header data (cookies)

Doppelganger Calling Card

- Removes all child tags of <body>
- Adds a new tag prominently displaying calling card image in user's browser
- Malicious scale: 1

Doppelganger Header Capturing

- Captures Entire Header
 - Capture HTTP Basic Auth & decode
 - Cookies
 - Malicious Scale 5+

Doppelganger Flash Injection

- Adds the appropriate tags for a flash object at the body end
- Gather more information about hosts
- Potentially exploit flash vulnerabilities
- Malicious scale: 3+

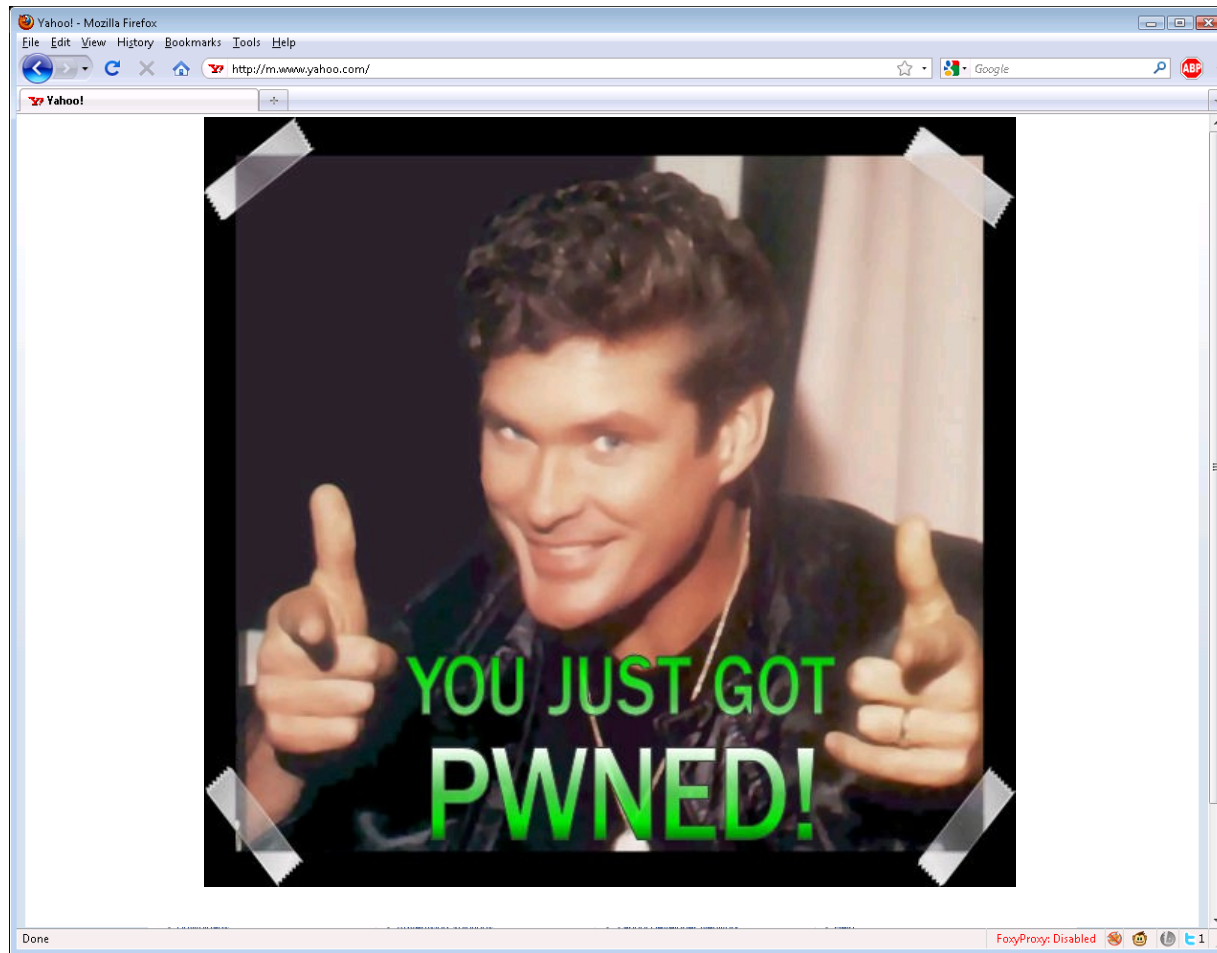
Doppelganger Form Data Capturing

- Finds all forms and binds to the “submit” event
- Form submission fires an Ajax request with serialized form data to a nonexistent URL, which in turn is logged by doppelganger
- Gets data from forms that are on a HTTP page even if GET/POST'd to an HTTPS page
- Malicious scale: 7+

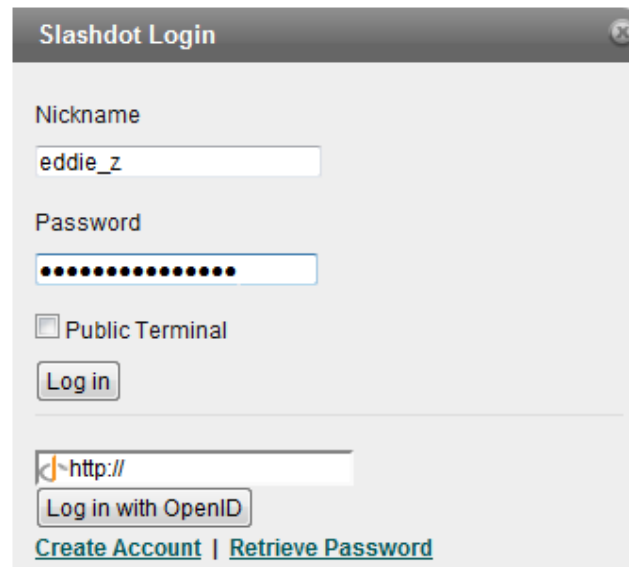
Doppelganger: Before



Doppelganger Calling Card: After



Doppelganger: Form Data



Slashdot Login

Nickname
eddie_z

Password
.....

Public Terminal

Log in

http://

Log in with OpenID

[Create Account](#) | [Retrieve Password](#)

```
192.168.176.43 - - [14/Jul/2009:18:01:36 EDT] "GET
http://slashdot.org/doppelganger-log?
formdata=aWYgdSByIHRoZSBmaXJzdCAyIGRlY29kZSB0aGlz
IGRlcmluZyBkZWZjb24xNywgaSBvd2UgdSBhIGRyaW5rIQ
HTTP/1.1" 404 0 "http://slashdot.org/" "Mozilla/5.0 (Windows; U;
Windows NT 6.1; en-US; rv:1.9.1) Gecko/20090624 Firefox/3.5.1
(.NET CLR 4.0.20506)"
```

Doppelganger: Other Uses

- Phishing
- CSRF Attacks
- Exploiting
 - (i.e., Firefox 0-days, Adobe 0-day)

Doppelganger: Future Additions

- Future Additions
 - More granular control over what pages to mimic
 - Interactivity (on-the-fly reconfiguration)
 - `sslstrip/sslstrip`

Curious Findings

- WPAD
 - One hour lead to for 320+ unique hosts grabbing my wpad.dat
 - Our environment pushes proxy setting via GPO; I'm sure GPO doesn't set the proxy to my laptop

Some Mitigations

- Serve the WPAD URL yourself
 - DHCP Option 252
 - DNS
- Ensure all browsers are configured to not automatically detect proxy
- This only protects against the WPAD-type of attack

Questions?

- or -

Script Ideas/Submissions

Edward J. Zaborowski

ed@thezees.net

<http://doppelganger.googlecode.com>



Dedication

- Dedicated to my wife Kristen, mother Joyce, my brother Dave and the memory of my Sister, Tina, my Brother Eugene JR (Jay), and my Father Gene, whom inspire me every day.