Understanding and Combating Man-in-the-Browser Attacks

22nd Annual FIRST Conference
16 June 2010
Jason Milletary

SecureWorks®
secureworks.com

Topics

- What is a Man-in-the-Browser Attack?
- How are they used?
- How can I identify and mitigate when they are used against our users?

What Is It?

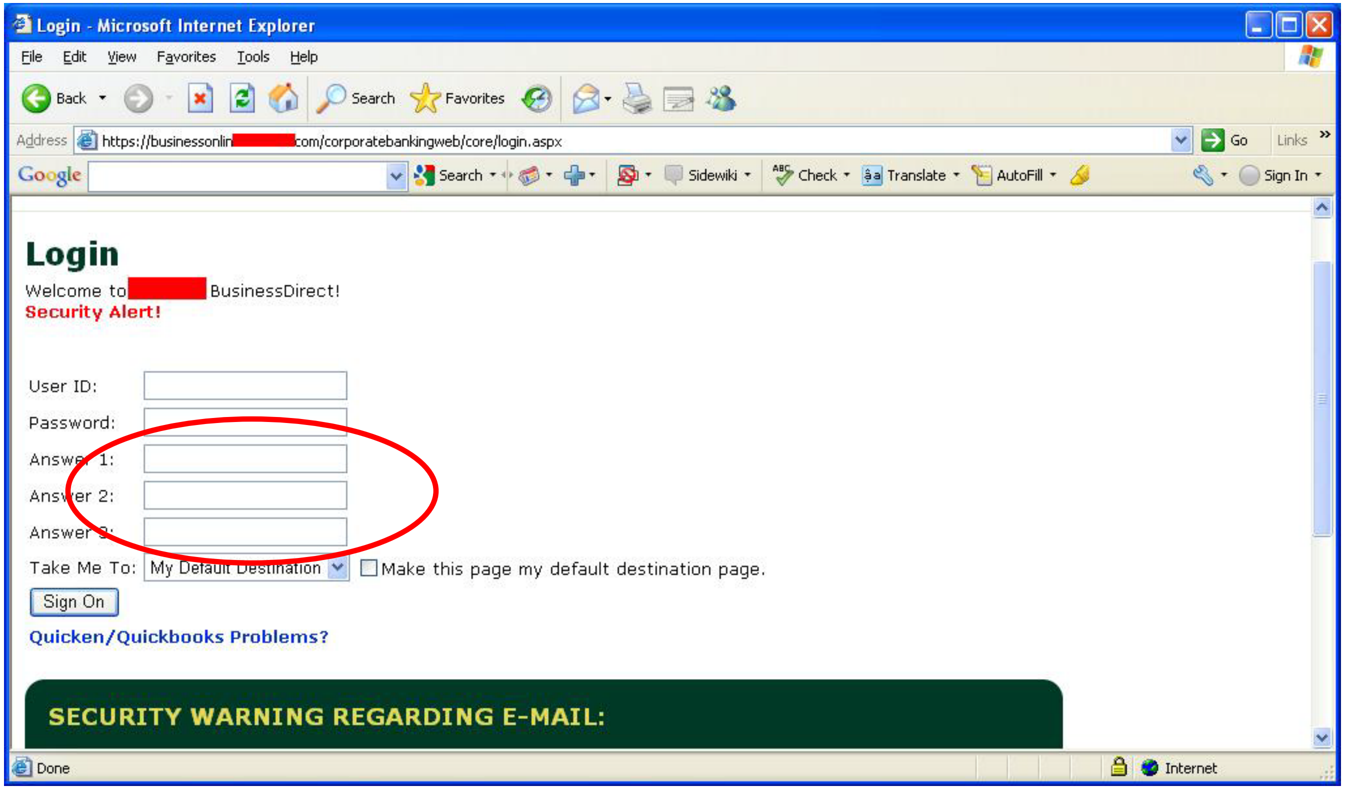
- Man-in-the-Browser (MITB) attacks refer to the use of malicious code to perform advanced information stealing attacks
- Attacks involve an active component beyond simple data theft
- Previously the scope of many of these attacks were thought only to be possible with true Man-in-the-Middle (MITM) attacks
- Typically used for facilitating online financial fraud against banking, trading, or e-commerce institutions
  - Techniques are generic enough to apply elsewhere
- Most commonly observed attacks is the modification of legitimate HTML
  - Also see HTML grabbing and MITM style transaction alteration

How It Works

- Malware is installed on machine through various mechanisms
- Malware inserts functionality into the memory of a running web browser process (Internet Explorer, Firefox, Opera, et c.)
- Extension techniques
  - IE Browser Helper Objects (BHOs)
  - Firefox extensions
- Viral techniques
  - Inline API function hooking
  - Import Address Table (IAT) hooking
- Malicious code now sits inline with normal browser functionality
  - Access to view and manipulate data
  - Above SSL in the stack

HTML Injection Example

- Modify the HTML of a targeted site. Commonly used to add additional input fields to phish additional information from a victim
- Address bar and SSL lock icon and information are intact



https://businessonlin[redacted]com/corporatebankingweb/core/login.aspx

Login

Welcome to [redacted] BusinessDirect!

Security Alert!

User ID:

Password:

Answer 1:

Answer 2:

Answer 3:

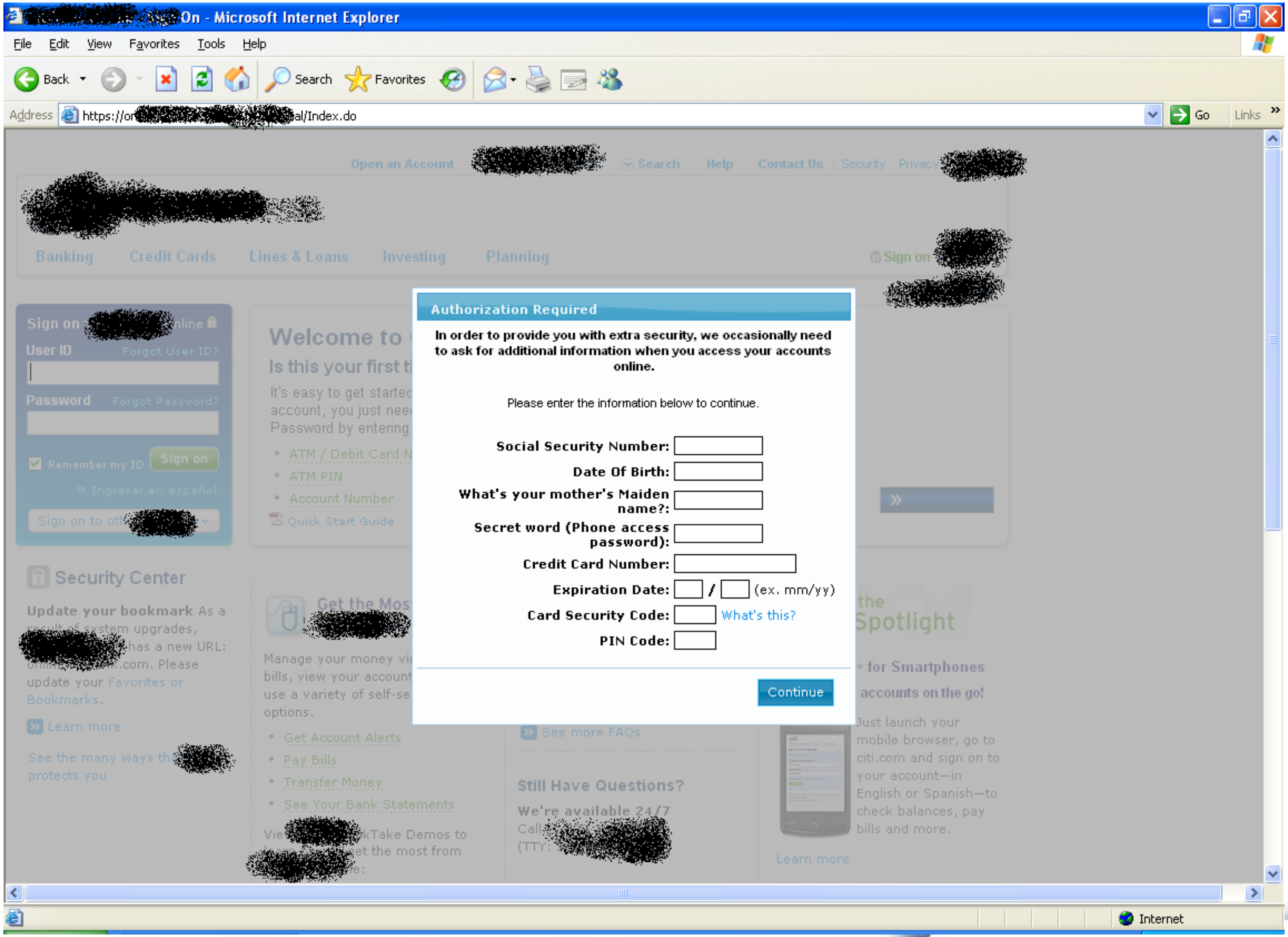
Take Me To: My Default Destination □ Make this page my default destination page.

Sign On

Quicken/Quickbooks Problems?

SECURITY WARNING REGARDING E-MAIL:

eCrime 2.0!



[redacted] On - Microsoft Internet Explorer

https://or[redacted]al/Index.do

Open an Account [redacted] Search Help Contact Us | Security Privacy [redacted]

[redacted]

Banking Credit Cards Lines & Loans Investing Planning Sign on [redacted]

[redacted]

Sign on [redacted] nline

User ID Forgot User ID?

Password Forgot Password?

☑ Remember my ID Sign on

» Ingresar en español

Sign on to ot[redacted]

Welcome to

Is this your first ti

It's easy to get startec account, you just nee Password by entering

- ATM / Debit Card N
- ATM PIN
- Account Number

Quick Start Guide

Security Center

Update your bookmark As a result of system upgrades, [redacted] has a new URL: [redacted].com. Please update your Favorites or Bookmarks.

» Learn more

See the many ways th[redacted] protects you

Get the Mos[redacted]

Manage your money vi bills, view your account use a variety of self-se options.

- Get Account Alerts
- Pay Bills
- Transfer Money
- See Your Bank Statements

Vie[redacted]kTake Demos to [redacted]et the most from [redacted]e:

» See more FAQs

Still Have Questions?

We're available 24/7

Call[redacted] (TTY:

the Spotlight

for Smartphones

accounts on the go!

Just launch your mobile browser, go to citi.com and sign on to your account—in English or Spanish—to check balances, pay bills and more.

Learn more

Authorization Required

In order to provide you with extra security, we occasionally need to ask for additional information when you access your accounts online.

Please enter the information below to continue.

Social Security Number:	
Date Of Birth:	
What's your mother's Maiden name?:	
Secret word (Phone access password):	
Credit Card Number:	
Expiration Date:	/ (ex. mm/yy)
Card Security Code:	What's this?
PIN Code:	

Continue

Internet

SecureWorks®

HTML Injection/Modification

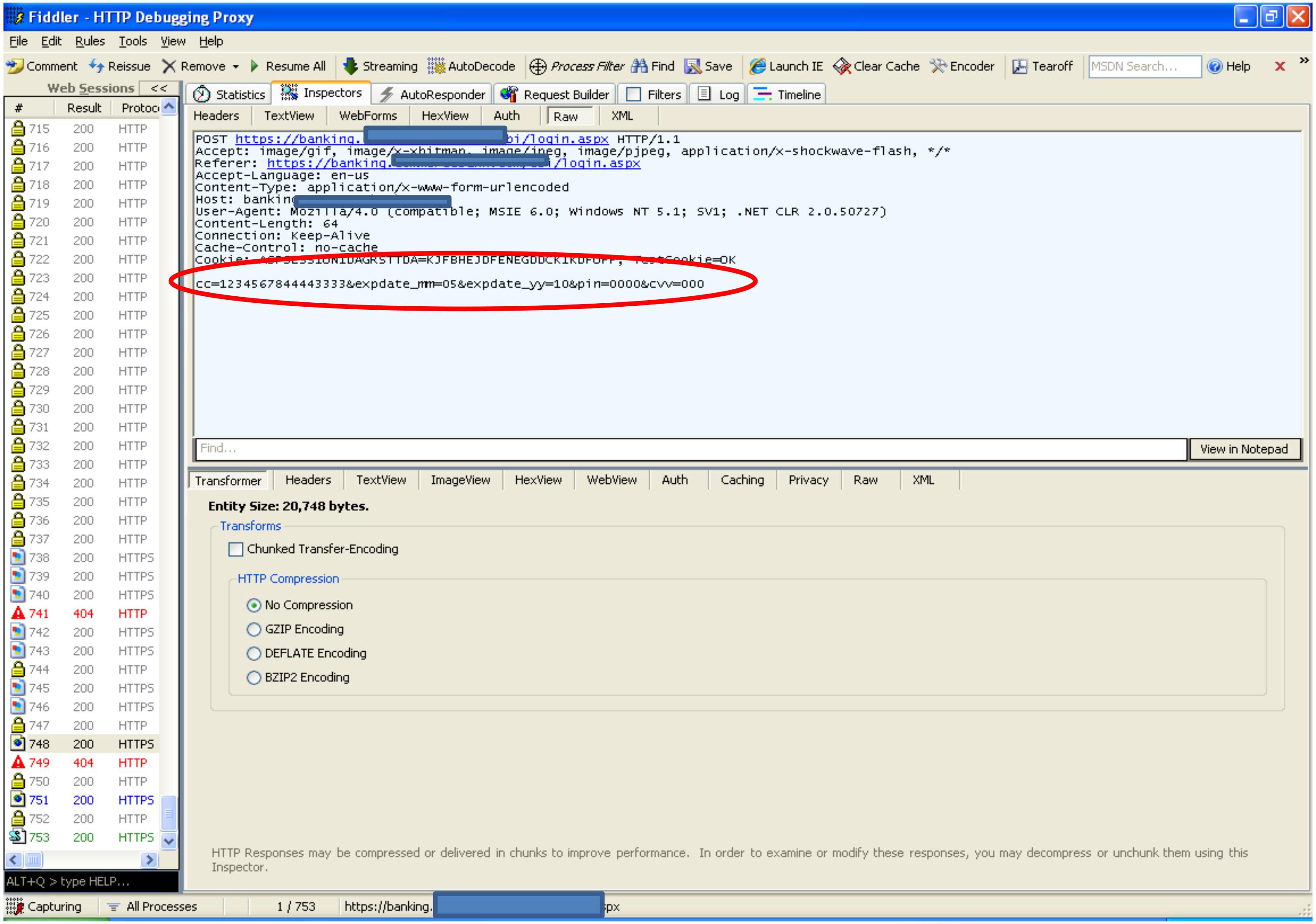
- Often URL-targeted
  - By site
  - By keyword
- Examines the HTML code returned by a targeted link and adds, modifies, or remove content
- Can be used to inject static content (HTML) or dynamic content (JavaScript)
- Used to trick victims into divulging information needed to commit fraud that may not normally be attainable by passive monitoring
- Can also be used to modify content presented to users
  - Remove warnings
  - Present fake “site down for maintenance” screens
  - Modify transaction records

Detection

- Modification of the user experience will often leave artifacts that can be detected in web/application logs
- Idea designed around the goal of detecting infected users whose accounts are at risk at being taken over
  - Not necessarily for detecting miscreants accessing the account to commit fraud, but some of the techniques may help there as well
- The ability to log, review, and mine HTTP headers, access logs, and application data (e.g. HTTP POST data) can be a valuable weapon in fraud detection

Extraneous POST data

- Common HTML injection attack involves phishing extra information from victims
  - ATM PINs
  - Date of Birth/Mother Maiden Name/Social Security Number/Tax ID
  - Memorable questions and answers
- The victim enters in additional information into the web form
- The default form action of submitting data to the legitimate server page is typically kept intact
- Malware uses existing form grabbing capability to grab injected content
- Using a tool like Fiddler lets us examine HTTP traffic, even over SSL
  - www.fiddler2.com



#	Result	Protocol
715	200	HTTP
716	200	HTTP
717	200	HTTP
718	200	HTTP
719	200	HTTP
720	200	HTTP
721	200	HTTP
722	200	HTTP
723	200	HTTP
724	200	HTTP
725	200	HTTP
726	200	HTTP
727	200	HTTP
728	200	HTTP
729	200	HTTP
730	200	HTTP
731	200	HTTP
732	200	HTTP
733	200	HTTP
734	200	HTTP
735	200	HTTP
736	200	HTTP
737	200	HTTP
738	200	HTTPS
739	200	HTTPS
740	200	HTTPS
741	404	HTTP
742	200	HTTPS
743	200	HTTPS
744	200	HTTP
745	200	HTTPS
746	200	HTTPS
747	200	HTTP
748	200	HTTPS
749	404	HTTP
750	200	HTTP
751	200	HTTPS
752	200	HTTP
753	200	HTTPS

```
POST https://banking.[redacted]bi/login.aspx HTTP/1.1
Accept: image/gif, image/x-xbitmap, image/jpeg, image/pjpeg, application/x-shockwave-flash, */*
Referer: https://banking.[redacted]/login.aspx
Accept-Language: en-us
Content-Type: application/x-www-form-urlencoded
Host: bankin[redacted]
User-Agent: Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; SV1; .NET CLR 2.0.50727)
Content-Length: 64
Connection: Keep-Alive
Cache-Control: no-cache
Cookie: ASPSESSIONIDAGRSTTDA=KJFBHEJDFENEGDDCKIKDFOFF; TestCookie=OK

cc=1234567844443333&expdate_mm=05&expdate_yy=10&pin=0000&cvv=000
```

Entity Size: 20,748 bytes.

Transforms

□ Chunked Transfer-Encoding

HTTP Compression

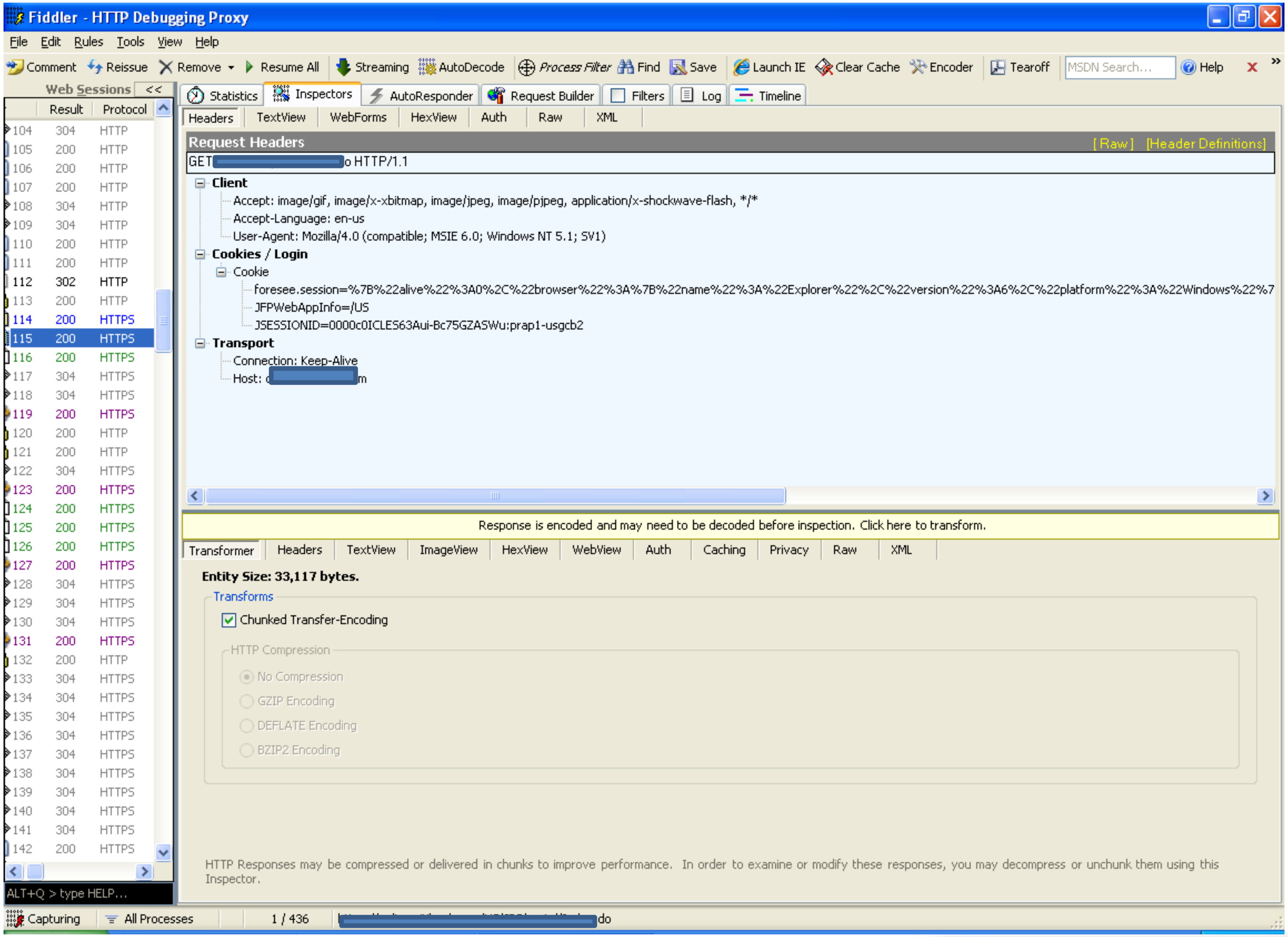
● No Compression
○ GZIP Encoding
○ DEFLATE Encoding
○ BZIP2 Encoding

HTTP Responses may be compressed or delivered in chunks to improve performance. In order to examine or modify these responses, you may decompress or unchunk them using this Inspector.

https://banking.[redacted]px

HTTP Header Anomalies

- Malware may often need to modify HTTP headers in order to utilize MITB techniques
- “Accept-Encoding”
  - Used to tell a web server which alternate encoding methods that the browser can handle
  - E.g. “Accept-Encoding: gzip, deflate”
- Malware does not want to have to deal with compressed HTML data from the server
- Modify/remove header to force default behavior
  - “Identity” encoding, i.e. plain text



Fiddler - HTTP Debugging Proxy
File Edit Rules Tools View Help
Comment Reissue Remove Resume All Streaming AutoDecode Process Filter Find Save Launch IE Clear Cache Encoder Tearoff MSDN Search... Help
Web Sessions <<
Statistics Inspectors AutoResponder Request Builder Filters Log Timeline
Headers TextView WebForms HexView Auth Raw XML
[Raw] [Header Definitions]
Transformer Headers TextView ImageView HexView WebView Auth Caching Privacy Raw XML
ALT+Q > type HELP...
Capturing All Processes 1 / 436

	Result	Protocol
104	304	HTTP
105	200	HTTP
106	200	HTTP
107	200	HTTP
108	304	HTTP
109	304	HTTP
110	200	HTTP
111	200	HTTP
112	302	HTTP
113	200	HTTP
114	200	HTTPS
115	200	HTTPS
116	200	HTTPS
117	304	HTTPS
118	304	HTTPS
119	200	HTTPS
120	200	HTTP
121	200	HTTP
122	304	HTTPS
123	200	HTTPS
124	200	HTTPS
125	200	HTTPS
126	200	HTTPS
127	200	HTTPS
128	304	HTTPS
129	304	HTTPS
130	304	HTTPS
131	200	HTTPS
132	200	HTTP
133	304	HTTPS
134	304	HTTPS
135	304	HTTPS
136	304	HTTPS
137	304	HTTPS
138	304	HTTPS
139	304	HTTPS
140	304	HTTPS
141	304	HTTPS
142	200	HTTPS

Request Headers

```
GET [redacted]o HTTP/1.1
⊟ Client
   Accept: image/gif, image/x-xbitmap, image/jpeg, image/pjpeg, application/x-shockwave-flash, */*
   Accept-Language: en-us
   User-Agent: Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; SV1)
⊟ Cookies / Login
   ⊟ Cookie
      foresee.session=%7B%22alive%22%3A0%2C%22browser%22%3A%7B%22name%22%3A%22Explorer%22%2C%22version%22%3A6%2C%22platform%22%3A%22Windows%22%7
      JFPWebAppInfo=/US
      JSESSIONID=0000c0ICLES63Aui-Bc75GZASWu:prap1-usgcb2
⊟ Transport
   Connection: Keep-Alive
   Host: [redacted]m
```

Response is encoded and may need to be decoded before inspection. Click here to transform.

Entity Size: 33,117 bytes.

Transforms

☑ Chunked Transfer-Encoding

HTTP Compression

● No Compression
○ GZIP Encoding
○ DEFLATE Encoding
○ BZIP2 Encoding

HTTP Responses may be compressed or delivered in chunks to improve performance. In order to examine or modify these responses, you may decompress or unchunk them using this Inspector.

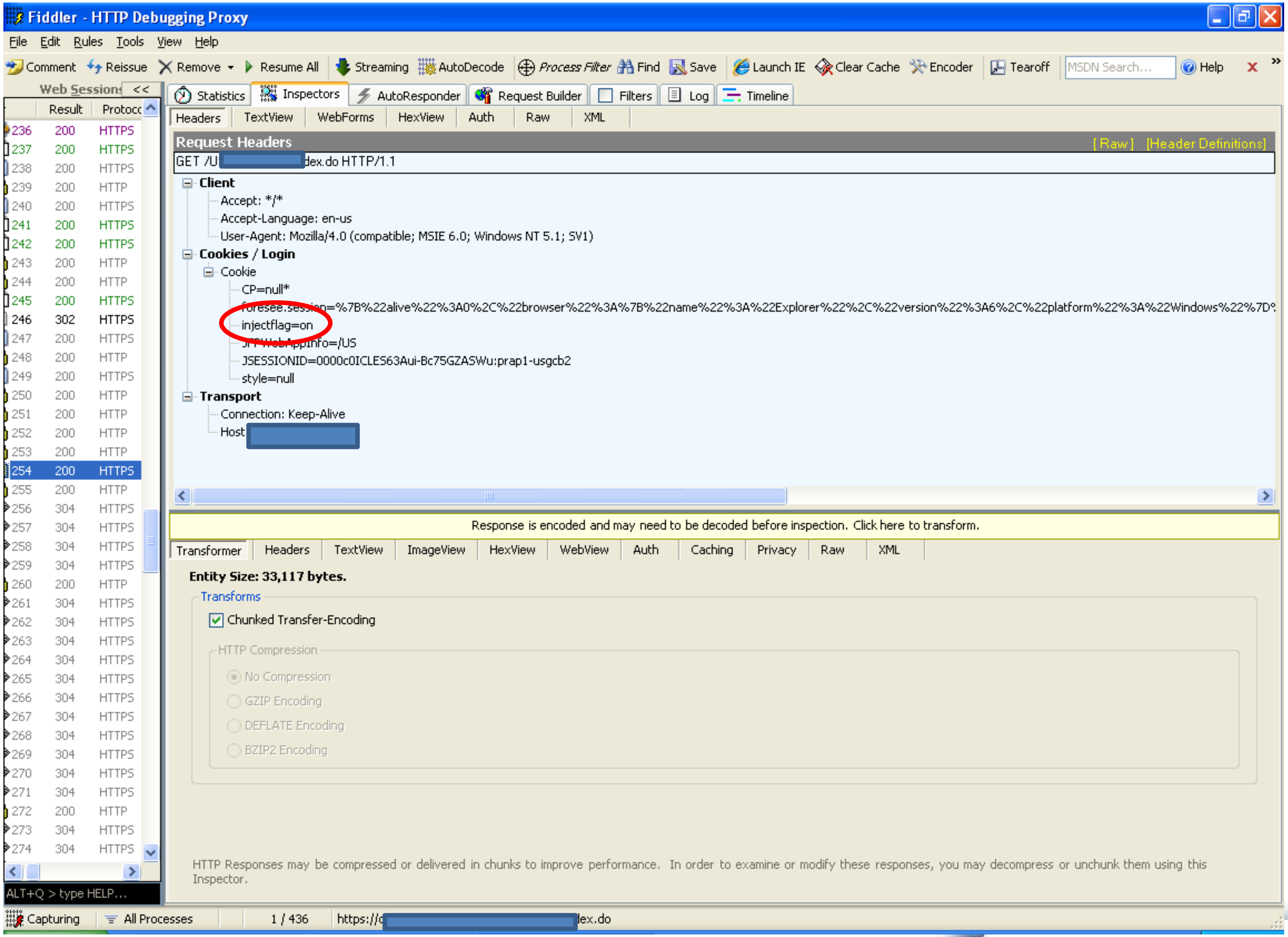
[redacted]do

Examples

- Zeus Trojan
  - Removes Accept-Encoding header altogether for targeted sites
- SpyEye Trojan
  - May remove Accept-Encoding header for Internet Explorer versions 6 or lower
- Bugat Trojan
  - Replaces header content with 14 spaces
  - Accept-Encoding:
- Tigger Trojan
  - Changes header name to “Accepl-Encoding”
  - Lower case “l” instead of “t”
- Opachki Search Hijack Trojan
  - Overwrites first several characters with the letter “b” or “n”
  - Accept-Encoding: bbbbbbbblate

Cookies

- MITB attacks may add or delete HTTP Cookies
- Deleting cookies
  - May force user to have to log in again
- Adding cookies
  - Store state
  - Timing flag to keep from repeatedly doing an injection attack


Fiddler - HTTP Debugging Proxy
File Edit Rules Tools View Help
Comment Reissue Remove Resume All Streaming AutoDecode Process Filter Find Save Launch IE Clear Cache Encoder Tearoff MSDN Search... Help
Web Sessions <<
Statistics Inspectors AutoResponder Request Builder Filters Log Timeline
Headers TextView WebForms HexView Auth Raw XML
[Raw] [Header Definitions]
Transformer Headers TextView ImageView HexView WebView Auth Caching Privacy Raw XML
ALT+Q > type HELP...

#	Result	Protocol
236	200	HTTPS
237	200	HTTPS
238	200	HTTPS
239	200	HTTP
240	200	HTTPS
241	200	HTTPS
242	200	HTTPS
243	200	HTTP
244	200	HTTP
245	200	HTTPS
246	302	HTTPS
247	200	HTTPS
248	200	HTTP
249	200	HTTPS
250	200	HTTP
251	200	HTTP
252	200	HTTP
253	200	HTTP
254	200	HTTPS
255	200	HTTP
256	304	HTTPS
257	304	HTTPS
258	304	HTTPS
259	304	HTTPS
260	200	HTTP
261	304	HTTPS
262	304	HTTPS
263	304	HTTPS
264	304	HTTPS
265	304	HTTPS
266	304	HTTPS
267	304	HTTPS
268	304	HTTPS
269	304	HTTPS
270	304	HTTPS
271	304	HTTPS
272	200	HTTP
273	304	HTTPS
274	304	HTTPS

Request Headers

```
GET /U[redacted]dex.do HTTP/1.1
Client
    Accept: */*
    Accept-Language: en-us
    User-Agent: Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; SV1)
Cookies / Login
    Cookie
        CP=null*
        foresee.session=%7B%22alive%22%3A0%2C%22browser%22%3A%7B%22name%22%3A%22Explorer%22%2C%22version%22%3A6%2C%22platform%22%3A%22Windows%22%7D%
        injectflag=on
        JFPWebAppInfo=/US
        JSESSIONID=0000c0ICLES63Aui-Bc75GZASWu:prap1-usgcb2
        style=null
Transport
    Connection: Keep-Alive
    Host [redacted]
```

Response is encoded and may need to be decoded before inspection. Click here to transform.

Entity Size: 33,117 bytes.

Transforms

☑ Chunked Transfer-Encoding

HTTP Compression

● No Compression

○ GZIP Encoding

○ DEFLATE Encoding

○ BZIP2 Encoding

HTTP Responses may be compressed or delivered in chunks to improve performance. In order to examine or modify these responses, you may decompress or unchunk them using this Inspector.

Capturing | All Processes | 1 / 436 | https://[redacted]dex.do

Intelligence Gathering

- In addition to understanding how current attacks may be affecting your users, it is important to keep aware of new and emerging threats
- A malware analysis capability can be used to gather actionable intelligence
- Runtime analysis in specialized environments can produce indicators of anomalous behavior
- Collection of samples and associated files can be used to build a larger picture
  - Assess threat against your organization
  - Linking of criminal groups for damage aggregation and prosecution purposes

Intelligence Tools

- Sample Acquisition
  - Free resources
    - malwaredomainlist.com
    - malc0de.com
    - Zeus Tracker – zeustracker.abuse.ch
    - Trusted mailing lists
  - Paid services
- Automated analysis
  - FOSS and COTS tools
  - Truman – http://www.secureworks.com/research/tools/truman.html
- Reverse engineering
  - Provides insight into malware capabilities
  - Recovery of cryptographic key material
- Configuration analysis
  - May require reverse engineering to understand crypto and format
  - Automation is your friend, so is Python (or Perl, or Ruby…)
  - Relational databases and/or full-text search engines

Thank You

Questions/Comments?

Your Speaker:

Jason Milletary jmilletary@secureworks.com