Understanding and Combating Man-in-the-Browser Attacks

22nd Annual FIRST Conference
16 June 2010
Jason Milletary
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
eCrime 2.0!

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

Continue
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
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
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: bbbbbbbbbblate
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
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
    - malware domainlist.com
    - malc0de.com
    - Zeus Tracker – zeustracker.abuse.ch
    - Trusted mailing lists
  - Paid services

- Automated analysis
  - FOSS and COTS tools

- 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