Detecting In-Flight Page Changes with Web Tripwires

Charlie Reis
Steve Gribble, Yoshi Kohno, Nick Weaver

Industrial Affiliates 2007
ISP-Injected Ads

- Surprising reports of web page modifications
- How often does this occur?
Detecting Page Changes

- Can detect with JavaScript
- Built a Web Tripwire:
  - Runs in client’s browser
  - Finds most changes to HTML
  - Reports to user & server

http://vancouver.cs.washington.edu
Attracting Visitors

- Wanted view of many clients on many networks
- Posted to Slashdot, Digg, etc.
- Visits from over 50,000 unique IP addresses

http://vancouver.cs.washington.edu
Outline

- Detecting In-Flight Changes
- Measurement Results
- Web Tripwires for Publishers
Many Users Affected

- 650+ clients saw changes (1.3%)
  - Many were client software
  - Some occurred in network
- Diverse incentives
- Often concerning for publishers

http://vancouver.cs.washington.edu
Changes by ISPs

- **Injected Advertisements (2.4%)**
  - NebuAd, MetroFi, LokBox, ...

  Revenue for ISP; annoy users
Changes by Enterprises

- Security Checking Scripts (2.3%)
- BlueCoat Web Filter

Safer for clients; reduce risk

http://vancouver.cs.washington.edu
Changes by Client Proxies

- Popup & Ad Blockers (71%)
- Zone Alarm, Ad Muncher, ...

Less annoying; impact revenue

http://vancouver.cs.washington.edu
Changes by Malware

- **Adware** (1 client)
- **Worms** (2 clients)

Helps malware author; risk to user

[http://vancouver.cs.washington.edu]
Unanticipated Impact

- Some changes inadvertently broke pages
- JavaScript errors
- Interfered with MySpace / forum posts
XSS Vulnerabilities

✦ Some changes made pages vulnerable to attack
  ✦ Like root exploit: almost all pages affected
✦ Ad Muncher, Proxomitron:
  ✦ Inserted URL into page
  ✦ Allowed script injection

http://vancouver.cs.washington.edu
Example Exploit

✦ Redirect user to Google
✦ Inject script code into search form
✦ Append exploit code to all outgoing links
✦ Reported vulnerabilities, now fixed

http://vancouver.cs.washington.edu
Outline

- Detecting In-Flight Changes
- Measurement Results
- Web Tripwires for Publishers
How to React?

- HTTPS is costly and rigid
- Publishers can deploy web tripwires
  - Detect and understand page changes
  - Low cost, works in current browsers
- We offer a configurable toolkit

http://vancouver.cs.washington.edu
Conclusion

- HTTP web pages are being **changed in flight**
  - Real negative impact for publishers & users
  - Page rewriters have dangerous power
- **Web tripwires** can help publishers react

http://vancouver.cs.washington.edu