A First Responder's Course in Drive By Downloads

Oliver Day (Akamai)

Agenda

- Propagation Methods
- Common Symptoms
- Diagnostic Tools
- Basic First Aid

Propagation Methods

- Browser Vulnerabilities
- Webmaster FTP credentials

Common Symptoms

- Inclusion in blacklists
- Browser warnings
- Webmasters all symptomatic

Diagnostic Tools

- Check Blacklists!
- Audit FTP logs
- Curl/wget/w3m
- Grep
- Vscan (shameless? Self promotion)

Basic First Aid

- Remove <iframe> and <script> tags that don't belong
- Rotate FTP passwords
- Better yet GET RID OF FTP
- Clean systems of all infected webmasters