Automated Web Patrol with Strider HoneyMonkeys: Finding Web Sites That Exploit Browser Vulnerabilities

* four steps:
  1. code obfuscation
  2. URL redirection
  3. vulnerability exploitation
  4. malware installation.
* Report containing
  1. Exe files created/ files modified outside browser sandbox folders
  2. Processes created
  3. Windows registry entries created or modified
  4. Vulnerability exploited
  5. Redirect-URLs visited
* “traffic redirection can be tracked with a Browser Helper Object (BHO) running within each browser process or by intercepting and analyzing network packets”
  1. positively identify the web pages that actually perform the exploits by implementing an option in our redirection tracker to block all redirection traffic
  2. feed in the URLs that got visited back into the system

Cost-effective Detection of Drive-by-Download Attacks with Hybrid Client Honeypots

* Avoidances:
  + Obfuscation
  + Time bombs
    - Only do malicious stuff after a certain amount of time has passed, e.g. 25 seconds
  + IP tracking
    - Monitor where the website is being loaded from
    - Only serve malicious content once per IP

AMA: Static Code Analysis of Web Page For The Detection of Malicious Scripts

* Obfuscated
  + E.g. hexadecimal, unicode, base64, escaped characters and rarely with substitution ciphers like Vigenere, Caesar and Atbash
  + probable plaintext attack on the deobfuscated code
* iframe based web attacks