Perverting WPAD For Passive Client Performance Evaluation and Weather Mapping

Alan Whinery

U. Hawaii

JT College Station 2/3/09

WPAD

- Expired Internet Draft
  - Web Proxy Auto-Discovery Protocol
  - Scheme for auto-configuring web browser proxy settings
  - See JoeTalk:
    - *http://darkwing.uoregon.edu/~joe/proxies/open-proxy-problem.pdf*
- Causes client to fetch a jscript file from a web server

WPAD

- Primarily used by WinHTTP service
- Used by Windows Update Agent
- Used by 52 other things
- If you disable it as a service, MSIE does it internally
- Good idea to define “wpad.xxx.edu”

The Idea

- I played with actual do-something wpad.dats for a while, using Squid
- Usually had something like 1000 to 1500 unwitting victims
- Discovered several interesting things, including the futility of caching.
- Shut down Squid, re-tasked the machine, put wpad.hawaii.edu on a sub-interface on my former NDT server, which, of course has a Web100 kernel.

The Idea

- Wrote a daemon that records web100 stats during iperf tests
- All the pieces were in place
- What if I recorded the web100 stats of each wpad.dat transfer?
  - Boring. Single segment, sometimes lost, but boring
- What if I put 10 segments of whitespace before the jscript code?
  - At this point, I laughed, in spite of myself.

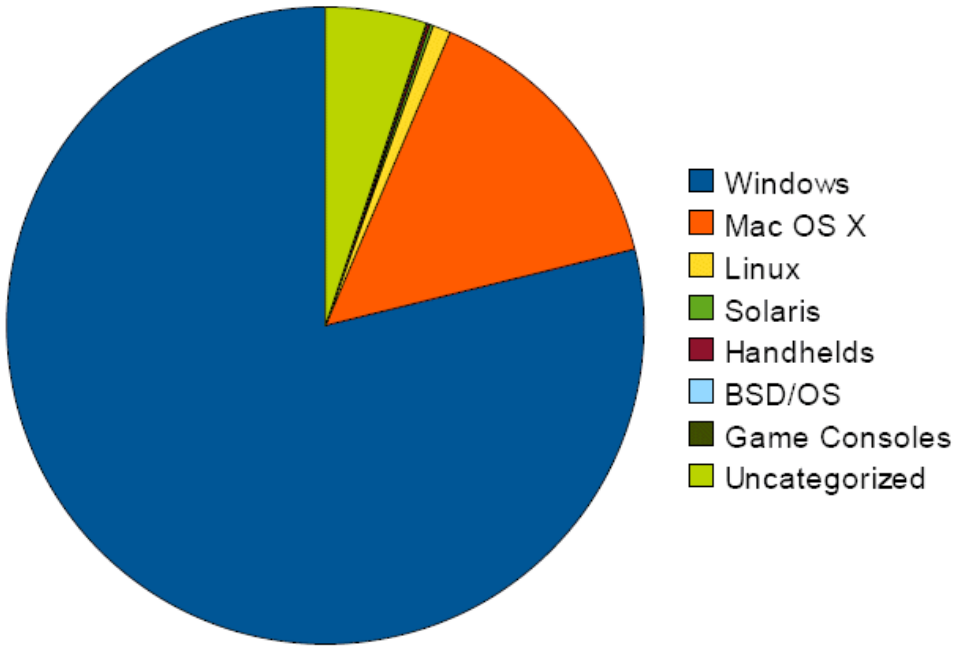
What you get

- Been doing this since July 2008
- Most recent run shows 5476 IP addrs on 254 /24 groups.
- Some hosts fetch wpad.dat often others seldom (power-on events?)
- Most bad performance is from individual addresses, the rest of local net is OK

To correllate

- Macs
- Uas
- Routing topology
- Like Malware notifiers in NPS/NAC

Everybody Hates Windows



OS Families	GETs	% all
Windows	32,998,321	78.858098%
Mac OS X	6,172,532	14.750876%
Linux	379,076	0.905901%
Solaris	73,381	0.175363%
Handhelds	59,939	0.143240%
BSD/OS	2,675	0.006393%
Game Consoles	14,693	0.035113%
Uncategorized	2,144,573	5.125017%