badWPAD
Maxim Goncharov
what is WPAD

1996 at Netscape Navigator 2.0
what is WPAD

- Browser issues DCHPINFORM query to DHCP server.
- DHCP server gives list of options and configurations.
- Computer Name: tomknopf
  Primary DNS suffix (search domain): infosec.mycompany.org
  Fully Qualified Domain Name: tomknopf.infosec.mycompany.org

- Browser requests wpad.file from WPAD servers until a server responds with the file.
  - It tries different URLs within domain of client:
    http://wpad.infosec.mycompany.org/wpad.dat
    http://wpad.mycompany.org/wpad.dat
    http://wpad.org/wpad.dat

- If option 252 is received, browser requests to download wpad.dat file.
- If successful, the browser will access the internet via proxy. If not, it will access the internet directly.
what is WPAD

Computer Name: tomkno pf
Primary DNS suffix (search domain): infosec.mycompany.org
Fully Qualified Domain Name: tomkno pf.infosec.mycompany.org

Browser requests wpad.dat file from WPAD servers until a server responds with the file.

It tries different URLs within domain of client:
- http://wpad.infosec.mycompany.org/wpad.dat
- http://wpad.mycompany.org/wpad.dat
- http://wpad.org/wpad.dat

If successful, the browser will access the internet via proxy. If not, it will access the Internet directly.
what is WPAD
WPAD experiment #1

3. Wpad.dat is automatically loaded

1. Hostname change from "tom knopf" to "WPAD"
2. wpad.dat is created in the Web server
4. System is configured to listen to port 1080

5. Network is instructed to use attacker's system as proxy
6. Attacker can now intercept ALL web traffic

Internet

Attacker's system

System using autoproxy

wpad.dat file
WPAD experiment #1

- Enigma (not unique): 21,894
- LH flight: 572
- LH flight return: 1,227
- PACSEC: 12
- Trend Micro Cupertino office: 6,378
## WPAD experiment #2

<table>
<thead>
<tr>
<th>Statistics for</th>
<th>Unique visitors</th>
<th>Number of visits</th>
<th>Pages</th>
<th>Hits</th>
<th>Bandwidth</th>
</tr>
</thead>
<tbody>
<tr>
<td>wpad.am</td>
<td>29 882</td>
<td>69 388</td>
<td>2 137 799</td>
<td>2 137 820</td>
<td>381.40 MB</td>
</tr>
<tr>
<td>direct</td>
<td>25 816</td>
<td>76 543</td>
<td>4 443 553</td>
<td>4 447 628</td>
<td>963.06 MB</td>
</tr>
<tr>
<td>wpad.cm</td>
<td>1 006</td>
<td>4 473</td>
<td>262 637</td>
<td>262 638</td>
<td>51.07 MB</td>
</tr>
<tr>
<td>wpad.media</td>
<td>667</td>
<td>4 962</td>
<td>1 492 337</td>
<td>1 492 394</td>
<td>297.21 MB</td>
</tr>
<tr>
<td>wpad.pub</td>
<td>633</td>
<td>1 929</td>
<td>52 064</td>
<td>52 154</td>
<td>9.84 MB</td>
</tr>
<tr>
<td>wpad.fm</td>
<td>483</td>
<td>1 885</td>
<td>260 274</td>
<td>260 320</td>
<td>50.59 MB</td>
</tr>
<tr>
<td>wpad.to</td>
<td>313</td>
<td>1 897</td>
<td>56 206</td>
<td>56 215</td>
<td>10.15 MB</td>
</tr>
<tr>
<td>wpad.video</td>
<td>268</td>
<td>1 615</td>
<td>2 159 710</td>
<td>2 159 799</td>
<td>451.23 MB</td>
</tr>
<tr>
<td>wpad.education</td>
<td>218</td>
<td>843</td>
<td>80 277</td>
<td>80 340</td>
<td>14.10 MB</td>
</tr>
<tr>
<td>wpad.technology</td>
<td>178</td>
<td>705</td>
<td>58 703</td>
<td>58 801</td>
<td>10.76 MB</td>
</tr>
<tr>
<td>wpad.today</td>
<td>162</td>
<td>639</td>
<td>49 311</td>
<td>49 392</td>
<td>8.26 MB</td>
</tr>
<tr>
<td>wpad.run</td>
<td>133</td>
<td>609</td>
<td>519 738</td>
<td>519 776</td>
<td>90.01 MB</td>
</tr>
<tr>
<td>wpad.limited</td>
<td>110</td>
<td>400</td>
<td>24 607</td>
<td>24 692</td>
<td>5.18 MB</td>
</tr>
<tr>
<td>wpad.news</td>
<td>60</td>
<td>427</td>
<td>23 522</td>
<td>23 559</td>
<td>4.66 MB</td>
</tr>
<tr>
<td>wpad.email</td>
<td>59</td>
<td>139</td>
<td>32 438</td>
<td>32 506</td>
<td>6.40 MB</td>
</tr>
<tr>
<td>wpad.university</td>
<td>57</td>
<td>202</td>
<td>22 529</td>
<td>22 617</td>
<td>4.35 MB</td>
</tr>
<tr>
<td><strong>Total</strong></td>
<td><strong>60 045</strong></td>
<td><strong>166 656</strong></td>
<td><strong>11 675 705</strong></td>
<td><strong>11 680 651</strong></td>
<td><strong>2.30 GB</strong></td>
</tr>
</tbody>
</table>
WPAD experiment #2
# WPAD experiment #2

<table>
<thead>
<tr>
<th>User Agent</th>
<th>Update client count</th>
</tr>
</thead>
<tbody>
<tr>
<td>WindowsUpdateAgent</td>
<td>29,171</td>
</tr>
<tr>
<td>AAM%20Updates%20Notifier/1.0.162.0 CFNetwork/720.5.7 Darwin/14.5.0 (x86_64)</td>
<td>59</td>
</tr>
<tr>
<td>AAM%20Updates%20Notifier/1.0.162.0 CFNetwork/720.5.7 Darwin/14.5.0 (x86_64)</td>
<td>57</td>
</tr>
<tr>
<td>AAM%20Updates%20Notifier/1.0.162.0 CFNetwork/720.5.7 Darwin/14.5.0 (x86_64)</td>
<td>42</td>
</tr>
<tr>
<td>avast! Emergency Update Agent</td>
<td>9</td>
</tr>
<tr>
<td>XProtectUpdater (unknown version) CFNetwork/596.6.4 Darwin/12.6.0 (x86_64) (MacBookAir5%2C2)</td>
<td>7</td>
</tr>
<tr>
<td>Software%20Update (unknown version) CFNetwork/596.6.4 Darwin/12.6.0 (x86_64) (MacBookAir5%2C2)</td>
<td>7</td>
</tr>
<tr>
<td>Microsoft%20AutoUpdate/2.3.6 CFNetwork/720.5.7 Darwin/14.5.0 (x86_64)</td>
<td>7</td>
</tr>
<tr>
<td>XProtectUpdater (unknown version) CFNetwork/454.12.4 Darwin/10.8.0 (i386) (MacBookPro2%2C2)</td>
<td>6</td>
</tr>
<tr>
<td>GoogleSoftwareUpdateAgent/1.2.2.428 CFNetwork/596.6.4 Darwin/12.6.0 (x86_64) (MacBookPro8%2C1)</td>
<td>3</td>
</tr>
<tr>
<td>GoogleSoftwareUpdateAgent/1.2.2.428 CFNetwork/596.6.4 Darwin/12.6.0 (x86_64) (MacBookPro8%2C1)</td>
<td>29,368</td>
</tr>
</tbody>
</table>
WPAD experiment #2

- Comcast, US: 6%
- Netia SA, PL: 4%
- IDOM Technologies, FR: 4%
- Shaw Communications, CA: 4%
- Telstra Europe, UK: 3%
- TW Telecom Holdings, US: 3%
- Liberty Global Operations, AT: 3%
- Bell Canada, CA: 3%
- National Internet Backbone, IN: 2%
- Cox Communications, US: 2%
- Emirates Telecommunications, AE: 2%
- Hughes Network Systems, US: 2%
- GIN Ipex, CZ: 2%
- T-Mobile USA, US: 2%
- Others: 58%
WPAD experiment #2

- United States: 27%
- Canada: 10%
- Poland: 6%
- India: 5%
- United Kingdom: 5%
- France: 5%
- Russia: 3%
- Australia: 2%
- Hungary: 2%
- Brazil: 2%
- Others: 33%

Total: 18M
WPAD experiment #2

- Specified: 57%
- Unidentified: 43%
WPAD experiment #3

know your target

register TLD

attack
WPAD experiment #3
tokyo area orgs
wpad.tokyo
attack
WPAD experiment #3

![Bar chart and table showing statistics]

<table>
<thead>
<tr>
<th>Month</th>
<th>Unique visitors</th>
<th>Number of visits</th>
<th>Pages</th>
<th>Hits</th>
<th>Bandwidth</th>
</tr>
</thead>
<tbody>
<tr>
<td>Jan 2016</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Feb 2016</td>
<td>230</td>
<td>1,565</td>
<td>8,069,757</td>
<td>8,070,202</td>
<td>1.65 GB</td>
</tr>
<tr>
<td>Mar 2016</td>
<td>361</td>
<td>2,822</td>
<td>12,719,884</td>
<td>12,720,009</td>
<td>1.52 GB</td>
</tr>
<tr>
<td>Apr 2016</td>
<td>399</td>
<td>2,408</td>
<td>12,900,202</td>
<td>12,900,470</td>
<td>2.22 GB</td>
</tr>
<tr>
<td>May 2016</td>
<td>319</td>
<td>2,365</td>
<td>14,118,936</td>
<td>14,119,056</td>
<td>2.46 GB</td>
</tr>
<tr>
<td>Jun 2016</td>
<td>359</td>
<td>2,576</td>
<td>9,772,524</td>
<td>9,772,565</td>
<td>1.35 GB</td>
</tr>
<tr>
<td>Jul 2016</td>
<td>246</td>
<td>2,071</td>
<td>2,997,977</td>
<td>2,998,018</td>
<td>132.68 MB</td>
</tr>
<tr>
<td>Aug 2016</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Sep 2016</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Oct 2016</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Nov 2016</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Dec 2016</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td><strong>Total</strong></td>
<td><strong>1,914</strong></td>
<td><strong>13,807</strong></td>
<td><strong>60,579,280</strong></td>
<td><strong>60,580,320</strong></td>
<td><strong>9.32 GB</strong></td>
</tr>
</tbody>
</table>
WPAD experiment #3

<table>
<thead>
<tr>
<th>Hosts (Top 10)</th>
<th>Full list</th>
<th>Last visit</th>
<th>Unresolved IP Address</th>
</tr>
</thead>
<tbody>
<tr>
<td>Hosts : 213 Known, 33 Unknown (unresolved ip)</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>246 Unique visitors</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>61.120.205.101</td>
<td>Pages</td>
<td>Hits</td>
<td>Bandwidth</td>
</tr>
<tr>
<td></td>
<td>2,784,827</td>
<td>2,784,827</td>
<td>80.85 MB</td>
</tr>
<tr>
<td></td>
<td>16,665</td>
<td>16,706</td>
<td>4.03 MB</td>
</tr>
</tbody>
</table>

61.120.205.101
WPAD experiment #3
WPAD and Hardware
WPAD and Hardware
WPAD and Hardware

AVM

register fritz.box

attack