Survey on Behaviors of Captive Portals

Mariko Kobayashi
ao@sfc.wide.ad.jp

IETF98, Chicago
March 2017
Abstract

- In capport BoF in IETF 97
  - “We needs a volunteer for survey about capport.”

- I implemented a survey tool kit to automate the survey (on Raspberry Pi) and use it for this time.

- This survey shows an actual situation of Captive Portals in Japan.
Survey Overview

Survey on behaviors of 40 Captive Portals in Central area of Tokyo, Japan.

Survey Items:
1. False Negatives (iOS/macOS, Windows, Android)
2. HTTP Status Code
3. DNS poisoning
# Basic capport Detection Strategy

<table>
<thead>
<tr>
<th>Detection Strategy (Well-Known Web Pages)</th>
<th>Full Internet Access (not capport )</th>
<th>Captive Portal</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>iOS/macOS (Apple)</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>✓ Access captive.apple.com to check the Internet connectivity</td>
<td>• txt ”Success”</td>
<td>• Cannot get txt ”Success”</td>
</tr>
<tr>
<td><strong>Windows (Microsoft)</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>✓ Request DNS lookup for dns.msftnncsi.com (to judge whether Captive Portal or bad internet connectivity)</td>
<td>• IP address 「133.107.2 55.255」</td>
<td>• IP Address 「133.107.25 5.255」</td>
</tr>
<tr>
<td>✓ request <a href="http://www.msftnncsi.com/ncsi.txt">http://www.msftnncsi.com/ncsi.txt</a></td>
<td>• txt ”Microsoft NCSI”</td>
<td>• Cannot get txt ”Microsoft NCSI”</td>
</tr>
<tr>
<td><strong>Android (Google)</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>• Access <a href="http://google.com/gen_204">http://google.com/gen_204</a> (for HTTP probe)</td>
<td>• 204 &amp; No Content</td>
<td>• Cannot get both “204” and “No Content”</td>
</tr>
<tr>
<td>• <a href="https://google.com/generate_204">https://google.com/generate_204</a> (for HTTPS probe)</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

References => P.16
1.1 False Negatives (macOS/iOS)

- Less than 10% of capport defeat the detection strategy and some of them had been implemented by the same NSP.
- They defeat detection for some reason…?
1.2 False Negatives (Windows)

- 11% of capport defeat Window’s detection strategy, but I cannot find remarkable characteristics.
One-third of capport defeat the detection strategy, and they replies 204 & No Content to Android’s well-known Web page(it means “not capport”)

Most of the HTTPS probe does not success on capport.
2 Status Code

- Current Proposal: **511** (by mnot)
- Actual status code when the terminal accesses Well-Known Web Pages (of iOS/macOS or Windows): 302, 200, 307
3 DNS Poisoning

Can be detected DNS Poisoning?

- Most of the capport do not do DNS poisoning for its redirection.
- Most of the probes failed when I set Public DNS(8.8.8.8) for my survey tool kit.
Expected behavior of cappport:

- Replies with either 302 or 307 with a redirection url.

- Most of OS can detect this type of cappport.
Undesirable Behavior

- Some of capport which response 200 defeats the detection.

- Some of them also reply “204 & No Content” to Android’s Well-Known Web Page (defeat the detection strategy)

=> All of this model of capport are deployed and operated by the same NSP (in JP).
Why Network Service Provider (NSP) try to defeat capport detection?

• Because of complaint for detection from users?
  - Incognito windows have some troubles with login process (e.g. Google login) or API.

• For marketing (business) reason?
  - They want to get the information from browser’s cookie?

• Only Japanese NSP defeat for some conservative reason? How about other countries?
Why are Captive Portals deployed?

- For Authentication, Payment, Information, Advertisement, Notification.

What do NSPs want to get from capport?
- E-mail address – for tracking, marketing.
- Open ID – for tracking, marketing.
- Credit card Info. – to take credit, for payment.
- Browser’s cookie – for marketing.
- UA(user agent) – for judging whether the traffic is users’ true traffic or not.
My Proposal

- Writing “capport survey I-D” will be valuable output for WG.

- Conduct a further survey in other main cities or countries.
  - Singapore, San Francisco, London, Australia, Seoul, Beijing, Prague, Chicago etc.

- Implement capport survey app
  - Android app?
  - Or adding this contents on IETF app?
Discussion

- capport detection does not work correctly in Japan. => NSPs cannot provide their service.

We need to cooperate with NSPs not only OS vendors. It is important to meet their demand for our capport solution.

- Any opinion or ideas for my survey proposal? Any ideal survey items which have to be included for the further survey?
References

- Basic Strategies by Tanaza

- Basic Strategies by socifi
  https://socifi-doc.atlassian.net/wiki/display/SC/Operating+System+and+Browser+Capabilities+and+Behaviours

- Windows’ strategy
  https://msdn.microsoft.com/windows/hardware/drivers/mobilebroadband/captive-portals

- Android’s strategy
  https://android.googlesource.com/platform/frameworks/base/+master/services/core/java/com/android/server/connectivity/NetworkMonitor.java