Understanding Internet Censorship Policy: The Case of Greece

Vasilis Ververis [1] [2] George Kargiotakis Arturo Filasto [2]
Benjamin Fabian [1] Alexandros Afentoulis

[1]Information Systems Humboldt University Berlin

[2]The Tor Project

August 10, 2015

A new censorship "trend"

- Governments started blocking gambling/betting resources
- Austria, Belgium, Denmark, Finland, France, **Greece**, Hungary, Netherlands, Norway, Italy, Portugal, Slovakia, Slovenia, Spain, Sweden, UK, ...[1]
- "Mistaken blocking" (overblocking/underblocking)

[1] http://ec.europa.eu/internal_market/gambling/docs/study5_en.pdf

Blocked Landing Page

ΜΗ ΕΠΙΤΡΕΠΤΗ ΠΡΟΣΒΑΣΗ

Η πρόσβαση στον δικτυακό τόπο που θέλετε να επισκεφθείτε έχει απαγορευτεί με βάση το Νόμο 4002/2011 (Άρθρο 51 Παράγραφος 5), ο οποίος απαγορεύει στους παρόχους υπηρεσιών διαδικτύου (ISPs) με καταστατική έδρα ή έδρα πραγματικής διοίκησης ή μόνιμη εγκατάσταση στην Ελλάδα σύμφωνα με τις γενικές διατάξεις του ν. 2238/1994, να επιτρέπουν την πρόσβαση σε ιστοχώρους που προσφέρουν υπηρεσίες τυχερών παιγνίων και στοιχημάτων χωρίς άδεια.

Για περισσότερες πληροφορίες παρακαλώ επισκεφτείτε την ιστοσελίδα της Επιτροπής Εποπτείας και Ελέγχου Παιγνίων (Ε.Ε.Ε.Π.): http://www.gamingcommission.gov.gr

The access to this website is forbidden in accordance with Greek Law 4002/2011 (Article 51, Paragraph 5). For more information please visit the webpage of the Hellenic Gambling Commision: http://www.gamingcommission.gov.gr

Hellenic Gaming Commission (EEEP)

- Independent Administrative Authority
- Acts as public body responsible for the supervision of gambling services in Greece
- Jurisdiction to publish and enforce blacklists
- Law: Serious criminal offense[2] for users/companies/ISPs

[2] https://web.archive.org/web/20140829223000/http://nomoi.info/%CE%A6%CE%95%CE%9A-%CE%91-180-2011-%CF%83%CE%B5%CE%BB-44.html

EEEP Blacklist

- 1st release: July 2013[3]
- 401-438 websites blacklisted
- Distribution of blacklist remains unclear

[3] http://www.gamingcommission.gov.gr/images/deltia_tipou/dt2.pdf

EEEP Blacklist: Publication Timeline

31/07/2013 · · · · · version 1: 401 entries.

22/11/2013 · · · · · version 2: 423 entries.

22/02/2014 · · · · · version 3: 438 entries.

11/07/2014 · · · · · version 4: 437 entries.

EEEP Blacklist: Analysis

- Blacklist version 4: one entry was removed
  - Most of the ISPs still block this entry

EEEP Blacklist: Analysis

- Blacklist version 4: one entry was removed
  - Most of the ISPs still block this entry
- 28 entries are duplicate domains (different URLs)
- 17 entries refer to malformed pages or subdomains
- 3 entries host no gambling content (empty A record, expired/parked domain names)

Collection of Network Measurements

- Collection Period: June - August 2014
- 8 major ISP (5 landline, 3 mobile)
  - Landline: Cyta, Hol, Forthnet, Ote, Wind
  - Mobile: Cosmote, Vodafone, Wind

Collection of Network Measurements

- OONI (ooniprobe)
- Lepidopter

OONI: Open Observatory of Network Interference

- A set of principles and test specifications for conducting network measurements
- Measuring **network irregularities** that can be a symptom of **internet censorship** and **surveilance** since 2012
- Peer reviewed methodology, implemented using free software and publishing the data

---

`https://ooni.torproject.org`

Lepidopter: Raspberry Pi image

- Concept: Easily contribute by running an RPi probe.
- Distribution Image ready to boot and run tests.
- FLOSS Project

`https://github.com/TheTorProject/lepidopter`

Analysis of Network Measurements

- OONI tools

Analysis of Network Measurements

- OONI tools
- Python parser
- Common FLOSS tools

```
Reports Parser Output
Certain censorship: 300
Certain censorship (single requests): 57
Possible censor mistakes (404): 72
Total Censored (Certain + Single + Mistakes): 429
----
Total Single responses: 65
Single responses over Tor (exclude from stats): 0
Control failure: 18
```

Responsible Disclosure

- Contacted (2 Aug 2014) ISP representatives/support
  - Clarification on filtering
  - How they review/renew the rules
  - Use of another blacklist?
  - Comments on the blocking process

Responsible Disclosure

- Contacted (2 Aug 2014) ISP representatives/support
  - Clarification on filtering
  - How they review/renew the rules
  - Use of another blacklist?
  - Comments on the blocking process
- Only 1 (Cyta) replied with a link to the EEEP website
- No further communication as of today :(

Blocking Methods

- DNS Hijacking
- Erroneous HTTP 404 errors
- DPI

Blocking Methods: DNS Hijacking

ooniprobe http_requests -u http://www.pokerstarsblog.com

```
[..]
body_length_match: false
body_proportion: 0.0
control_failure: null
experiment_failure: null
factor: 0.8
headers_diff: !!set {Accept-Ranges: null, Content-Length: null, Content-Type: null,
  Date: null, Location: null, Transfer-Encoding: null, Vary: null}
headers_match: false
input: null
requests:
- request:
    body: null
    headers:
    - - User-Agent
      - ['Mozilla/5.0 (Windows; U; Windows NT 5.1; en-US; rv:1.9.2) Gecko/20100115
          Firefox/3.6']
    method: GET
    tor: {is_tor: false}
    url: http://www.pokerstarsblog.com/
  response:
    body: ''
    code: 302
    headers:
    - - Connection
      - [close]
    - - Location
      - ['http://eeep.forthnetgroup.gr/']
    - - Content-Length
      - ['0']
    - - Server
      - [BigIP]
[..]
```

Blocking Methods: HTTP 404

ooniprobe http_requests -u http://betting.stanjames.com/Blog

```
[..]
- request:
    body: null
    headers:
    - - User-Agent
      - ['Mozilla/5.0 (Windows; U; Windows NT 5.1; en-US; rv:1.9.2) Gecko/20100115
          Firefox/3.6']
    method: GET
    tor: {is_tor: false}
    url: http://betting.stanjames.com/Blog
  response:
    body: '<!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN">
      <html><head>
      <title>404 Not Found</title>
      </head><body>
      <h1>Not Found</h1>
      <p>The requested URL /Blog was not found on this server.</p>
      </body></html>
      '
    code: 404
    headers:
    - - Date
      - ['Tue, 03 Jun 2014 21:54:22 GMT']
    - - Content-Length
      - ['202']
    - - Content-Type
      - [text/html; charset=iso-8859-1]
    - - Connection
      - [close]
    - - Server
      - [Apache]
[..]
```

Blocking Methods: DPI

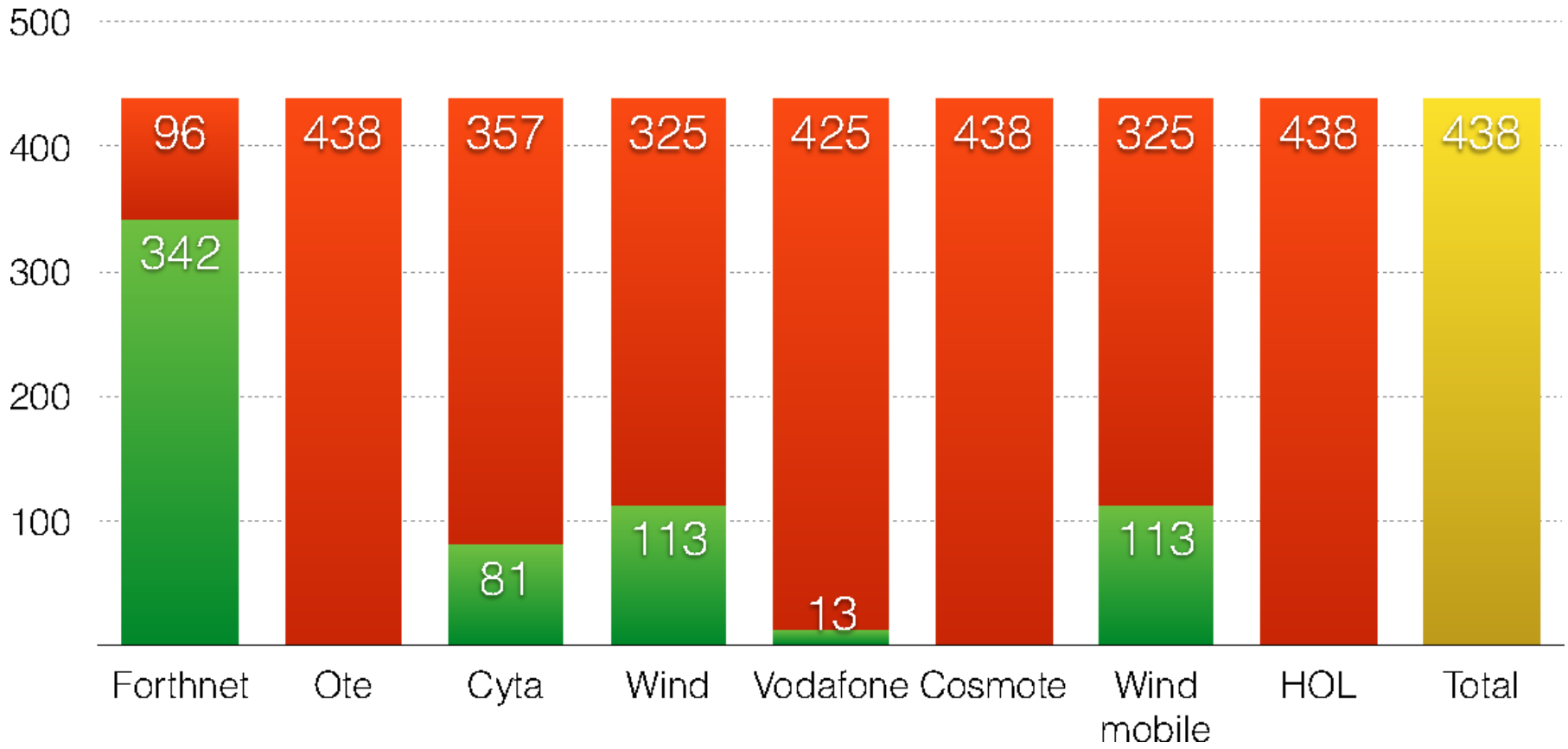
```
——— curl -I http://www.rivernilecasino.net ———
HTTP/1.1 302 Moved Temporarily
Date: Sun, 31 Aug 2014 12:38:28 GMT
Server: Microsoft-IIS/6.0
X-Powered-By: ASP.NET
X-AspNet-Version: 4.0.30319
Location: http://www.vegaspartnerlounge.com/
generic/informer.asp [..]
Set-Cookie: RiverNileCasino [..]
Cache-Control: private
Content-Type: text/html; charset=utf-8
Content-Length: 283
Connection: keep-alive
————————————————————————————————————————
```

Blocking Methods: DPI

```
——— curl -I http://www.rivernilecasino.net ———
HTTP/1.1 302 Moved Temporarily
Date: Sun, 31 Aug 2014 12:38:28 GMT
Server: Microsoft-IIS/6.0
X-Powered-By: ASP.NET
X-AspNet-Version: 4.0.30319
Location: http://www.vegaspartnerlounge.com/
generic/informer.asp [..]
Set-Cookie: RiverNileCasino [..]
Cache-Control: private
Content-Type: text/html; charset=utf-8
Content-Length: 283
Connection: keep-alive
```

```
curl -I http://www.rivernilecasino.net/index.asp
HTTP/1.1 301 Moved Permanently
Server: WebProxy/6.0
Date: Sun, 31 Aug 2014 12:39:01 GMT
Content-Length: 0
Location: http://1.2.3.50/[..]
ups/no_access_gambling.htm
-
-
-
-
-
-
Connection: keep-alive
```

EEEP blacklist: Per ISP blocking



Red: Blocked / Green: Unblocked / Yellow: Total entries in blacklist

Collateral Damage

- ISPs block URLs but not email communication?

Collateral Damage

- ISPs block URLs but not email communication?
- DNS Hijacking: Non legitimate A records
- No MX records
- Email delivery failure

dig MX bingocafe.com

```
; <<>> DiG 9.9.5-4-Debian <<>> bingocafe.com
;; Got answer:
;; ->>HEADER<<- opcode: QUERY,
;; status: SERVFAIL, id: 22828
;; flags: qr rd ra; QUERY: 1, ANSWER: 0,
;; AUTHORITY: 0, ADDITIONAL: 1
;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 4096
;; QUESTION SECTION:
;bingocafe.com.                  IN      MX
;; Query time: 49 msec
;; SERVER: 213.249.17.11#53(213.249.17.11)
;; WHEN: Thu Jul 03 11:45:05 EEST 2014
;; MSG SIZE  rcvd: 42
```

Conclusions

- ISPs lack of transparency:
  - How frequent ISPs evaluate their filtering rules
  - Outdated/poorly implemented blacklists
  - Block arbitrary web resources according to their needs

Conclusions

- ISPs lack of transparency:
  - How frequent ISPs evaluate their filtering rules
  - Outdated/poorly implemented blacklists
  - Block arbitrary web resources according to their needs
- DNS Hijacking can be easily circumvented
- 404 HTTP errors: users assumed a technical issue

Thank you for your attention!

Questions?