Content blocking systems in Cyprus

OWASP Chapter Limassol
whoami

• Dmitrii Stepul
• I am a student of Neapolis University Pafos (final year)
• transferred from SpBU
• My first talk, so don’t judge me strictly)
How this topic occurred

• result of my research work at the university
• provided by Ivan Agarkov
Why this topic important

• Blocking and Internet censorship can affect everyone (Telegram blocking in Russia, Great Firewall in China)
Why this topic important

- Blocking and Internet censorship can affect everyone (Telegram blocking in Russia, Great Firewall in China)
- Council Regulation (EU) 350/2022 and with EU and National Laws
Why this topic important

• Blocking and Internet censorship can affect everyone (Telegram blocking in Russia, Great Firewall in China)
• Council Regulation (EU) 350/2022 and with EU and National Laws
• Cyprus is placed in the second place in terms of the number of blocked gambling websites in EU

^1Website blocking in the European Union: Network interference from the perspective of Open Internet, DOI: 10.1002/poi3.367
Disclaimer 1

- OWASP does not encourage the violation of any laws; and cannot be responsible for any violations of such laws. The purpose of the research is purely educational.
- The tools described here are absolutely legal. It’s like a knife: someone cuts cabbage into a salad, and someone uses it for attacks.
Disclaimer 2

- There is a small amount of research in Cyprus on this topic
- Russia is often mentioned because it is well-researched
- It all can also be applied to Cyprus

---

2Internet Censorship Capabilities in Cyprus: An Investigation of Online Gambling Blocklisting 2017
This site can’t be reached due to compliance with the Council Regulation (EU) 350/2022 and with EU and National Laws, only for as long as necessary.

Figure 1: Standard Cypriot ISP’s payload
Deep Packet Inspection

How can DPI behave in general after receiving a "bad request":

- Freeze
- Redirect (only HTTP requests)
- Certificate substitution

³https://github.com/bol-van/zapret
Bypass DPI using RFC standards

GET / HTTP/1.1
Host: vk.com
Accept-Encoding: gzip, deflate, br
Connection: keep-alive

4https://habr.com/ru/articles/335436/
Bypass DPI using RFC standards

GET / HTTP/1.1
Host: vk.com
Accept-Encoding: gzip, deflate, br
Connection: keep-alive

3.2. Header Fields Each header field consists of a case-insensitive field name followed by a colon (":"), optional leading whitespace, the field value, and optional trailing whitespace.

5Source: RFC 7230
6https://habr.com/ru/articles/335436/
Bypass DPI using RFC standards

GET / HTTP/1.1
Host: vk.com
Accept-Encoding: gzip, deflate, br
Connection: keep-alive

- Host -> hOst or hOST
- Add spaces and tabulation
- Split one packet into two and send it fragmented
- Add paddings

7https://habr.com/ru/articles/335436/
DNS leaks

- DNS translates domain names, like "example.com" \rightarrow 192.0.2.123.
DNS manipulation

- DNS translates domain names, like "example.com" -> 192.0.2.123.
- ISP can intercept our DNS queries.
DNS manipulation

- DNS translates domain names, like "example.com" -> 192.0.2.123.
- ISP can intercept our DNS queries.
- How to bypass it?
DNS manipulation

We can:

- Use public Google, Cloudflare, Adguard DNS (UDP port 53)
- Use DNS over HTTPS - DoH (TCP port 443)
- Use DNS over TLS - DoT (TCP port 853)
DoH Example

DNS over HTTPS example workflow
SNI-blocking

Figure 2: TLS scheme

9Service-Level Monitoring of HTTPS Traffic, DOI: 10.13140/RG.2.2.32296.67849
SNI and Encrypted Client Hello

Figure 3: Client-hello

Figure 4: Encrypted Client Hello

---

\(^a\)https://support.mozilla.org/en/kb/understand-encrypted-client-hello
ECH underhood

1. User visits example.com
2. Intermediaries see example.com
3. Intermediaries see cloudflare-ech.com
4. Cloudflare

10https://developers.cloudflare.com/ssl/edge-certificates/ech/
DoT and DoH blocking

• It is hard to block DoH and DoT as it hurts the Internet in a country
• If some ISP decides to block CloudFlare, there will be some working issues with the Internet
• ESNI and TLSv1.3 traffic has been blocked in China since August 2020. 

11 www.zdnet.com/article/china-is-now-blocking-all-encrypted-https-traffic-using-tls-1-3-and-esni/
DoH / DoT possible blocking
DoT and DoH support

Since:

- Android 9, iOS 14 support DoT
- Linux with systemd-resolved from systemd 239: DoT through the DNSOverTLS option.
- Firefox 62, Opera 65, Chrome 78 support DoH
- BIND 9.17, Unbound
The Citizen Lab is an interdisciplinary laboratory based at the Munk School of Global Affairs Public Policy, University of Toronto, focusing on research and development at the intersection of information and communication technologies, human rights, and global security.
DNS bypassing comparing results in Cyprus

<table>
<thead>
<tr>
<th>DNS type</th>
<th>ISP plain resolver</th>
<th>Google DoH</th>
<th>1.1.1.1 UDP DNS</th>
<th>Google DoT</th>
<th>Cloudflare DoH</th>
</tr>
</thead>
<tbody>
<tr>
<td>Successful requests</td>
<td>54%</td>
<td>86%</td>
<td>86%</td>
<td>86%</td>
<td>86%</td>
</tr>
</tbody>
</table>

12 [github.com/citizenlab/test-lists](https://github.com/citizenlab/test-lists)
GEO-ip blocking

Сайт может не работать с VPN

Рекомендуем отключить VPN для стабильной работы сайта.

Figure 5: Blocking non-Russian IP addresses on the Russian side
Russian Trusted Root CA ¹³

- `curl -Lk admburla.ru`

```html
<div>
  <strong>403: Access Forbidden</strong>
  <p>Malware detected</p>
</div>
```

¹³certizdat.org/
Russian Trusted Root CA

```bash
#!/bin/bash
openssl s_client -showcerts -connect admburla.ru:443
| openssl x509 -noout -issuer -subject
| head -n 1

issuer = RU
O = The Ministry of Digital Development and Communications
CN = Russian Trusted Sub CA
```

\[14\] certizdat.org/
Russian Trusted Root CA

- Certificates signed with Russian cryptography methods
- AES -> Kuznechik (GOST P 34.12-2015)
- 3DES -> Magma (GOST 28147-89)
- SHA2-256 -> STREEBOG (GOST P 34.11-2012)
- ECDSA -> GOST P 34.10-2012
- ECDH -> VKO GOST P 34.10-2012

15www.gost.cypherpunks.ru/Russian.html
certizdat.org (open-source)

Some of the strange detected self-signed certificates issuer by Russia

SberCA, St. Petersburg, VTB Group, Bank GPR, Администрация Партизанского городского
округа, Kaliningrad, Siga-NEZERV, Moscow, Stavropol, Saint Petersburg, Petrozavodsk,
Bryansk, skif, SAMARA, Samara, SPb, Vladimir, s-t-DRY, Donetsk, Karelia, fav:ru,
Plesk, Stavropol, Yaroslavl, 77 Moskva, tatarstan, Internet Widsits Pty Ltd, 77 r.
Moskva, KRSK, kb-CA, ddos-guard, jarekt-DCEADS-CA, voronezh, GVN-SMV-CA, TULA, rostobr-
SMV-GHCP-PLAN-CA, Kostov-on-Don, Pskov, SBER.CA.GOVBR.RU, B-Navigosta, RU, sovet-mso.ru,
xk.all.culture.ru, CAP root CA, Certum Certification Authority, Khanty-Mansiysk,
mall.khbor.meteorf.ru, Sarian, #T, SomeCity, krs, UserGate, XX, Finance Dept,
Oldstatehotel, AxelHame LLC, IT-Group Certificate Authority, Nu-Shi, Yekaterinburg,
ca-3841m0344856380674.
VPN usage

With VPNs like Cloudflare WARP\textsuperscript{16}, and NordVPN\textsuperscript{17} everything works fine. but:

- added delay
- ISPs can block VPNs
- under the hood they used WireGuard

\textsuperscript{16}github.com/cloudflare/boringtun
\textsuperscript{17}support.nordvpn.com/hc/en-us/articles/19564565879441-What-is-NordLynx
VPN usage

WireGuard

- The goal was to create a simple alternative to OpenVPN, not a super secure utility
- It is secure and uses newly created cryptography protocols and algorithms but it isn’t private
VPN usage

WireGuard

- Wireguard is blocked in Egypt if it isn’t obfuscated
VPN usage

WireGuard

• Wireguard is blocked in Egypt if it isn’t obfuscated
• Wireguard Handshake Initiate recognizes by DPI very well
WireGuard’s easily detected

Figure 6: wireshark captured wireguard handshake
## Methods comparing

<table>
<thead>
<tr>
<th></th>
<th>HTTP headers</th>
<th>VPN both</th>
<th>public DNS plain</th>
<th>DoH/DoT</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Is it works?</strong></td>
<td>✗</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
</tbody>
</table>

- all methods marked as ✓ work on ISPs of Cyprus (tested on 4 different ISPs)
## Cost comparing

<table>
<thead>
<tr>
<th></th>
<th>VPN services</th>
<th>VPS server</th>
<th>Google DoH</th>
<th>1.1.1.1 UDP DNS</th>
</tr>
</thead>
<tbody>
<tr>
<td>price</td>
<td>4$</td>
<td>2$</td>
<td>0$</td>
<td>0$</td>
</tr>
</tbody>
</table>

- A research can save you money
- It is not always rational to pay for VPN solutions
What we haven’t discussed

• naiveproxy
• Hysteria
• Shadowsocks
• and others...
If you want the securest one (future readings)

- habr.com/ru/articles/799751/ - highly recommend
- VLESS
Final word

If you don’t want to be blocked, don’t bypass the locks)
Thank you!
If you have any questions, do not hesitate to contact me

Dmitrii Stepul,
d.stepul@nup.ac.cy