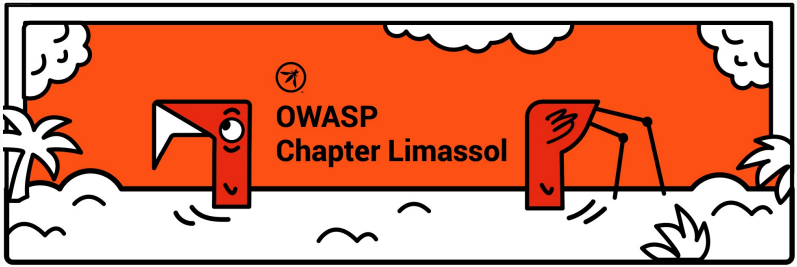
Content blocking systems in Cyprus



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 occured

- 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 [1]

[1] Website 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 [2]
- Russia is often mentioned because it is well-researched
- It all can also be applied to Cyprus

[2] Internet 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 [3]

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

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

[3] https://github.com/bol-van/zapret

Bypass DPI using RFC standards [4]


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

[4] https://habr.com/ru/articles/335436/

Bypass DPI using RFC standards [6]


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

> *3.2. Header Fields [5] Each header field consists of a case-insensitive field name followed by a colon (":"), optional leading whitespace, the field value, and optional trailing whitespace.*

[5] Source: RFC 7230
[6] https://habr.com/ru/articles/335436/

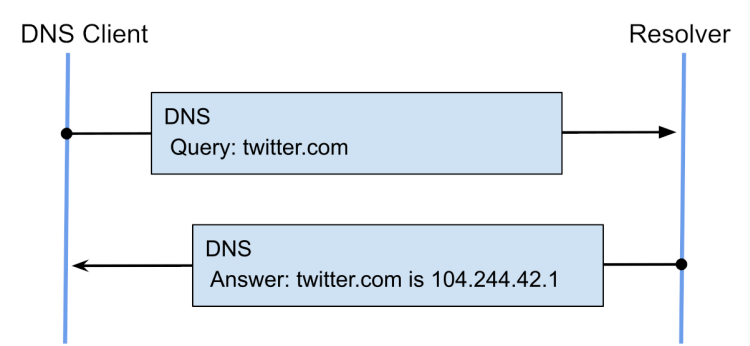
Bypass DPI using RFC standards [7]


```
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

[7] https://habr.com/ru/articles/335436/

DNS leaks



- DNS translates domain names, like "example.com" ->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

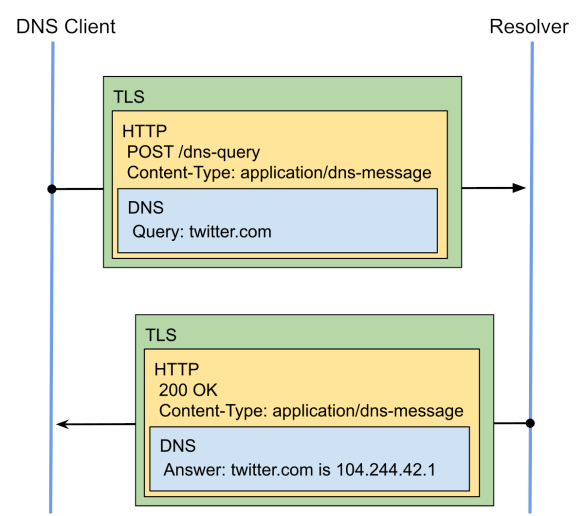
- DNS translates domain names, like "example.com" ->192.0.2.123.
- ISP can intercept our DNS queries.
- How to bypass it ?

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



8

[8] DNS over HTTPS example workflow

SNI-blocking

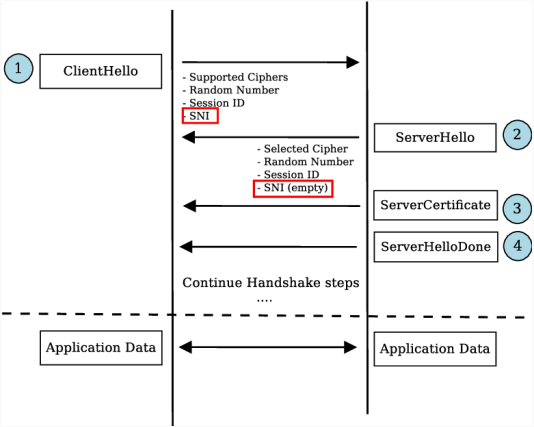


Figure 2: TLS scheme [9]

[9] Service-Level Monitoring of HTTPS Traffic, DOI: 10.13140/RG.2.2.32296.67849

SNI and Encrypted Client Hello

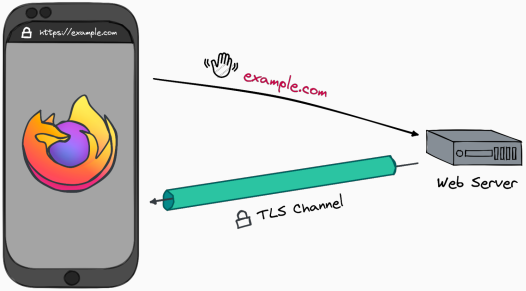


Figure 3: Client-hello[a]

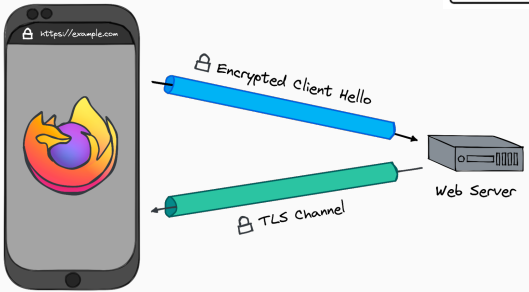
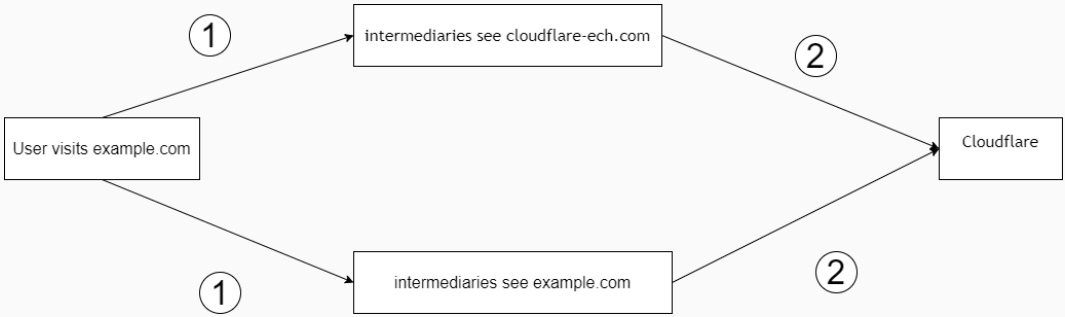


Figure 4: Encrypted Client Hello[a]

[a] https://support.mozilla.org/en/kb/understand-encrypted-client-hello

[a] https://support.mozilla.org/en/kb/understand-encrypted-client-hello

ECH underhood [10]



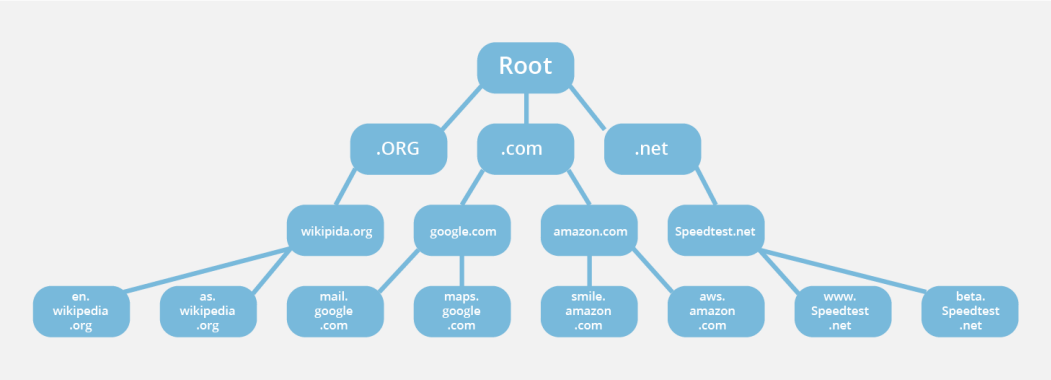
[10] https://developers.cloudflare.com/ssl/edge-certificates/ech/

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]

[11] www.zdnet.com/article/china-is-now-blocking-all-encrypted-https-traffic-using-tls-1-3-and-esni/

DoH / DoT possbible 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

citizenlab

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[12]

DNS type	ISP plain resolver	Google DoH	1.1.1.1 UDP DNS	Google DoT	Cloudflare DoH
Successful requests	54%	86%	86%	86%	86%

[12] github.com/citizenlab/test-lists

GEO-ip blocking

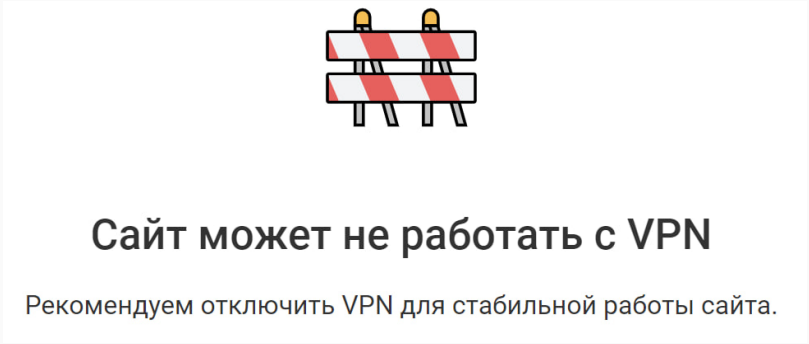


Figure 5: Blocking non-Russian IP addresses on the Russian side

Russian Trusted Root CA [13]

- curl -Lk admburla.ru

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

[13] certizdat.org/

Russian Trusted Root CA [14]

```
#!/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 [15]

- 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

[15] www.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 GPB, Администрация Партизанского городского округа, Kaliningrad, Sigma-REZERV, Moscow, Stavrolop, Saint Petersburg, Petrozavodsk, Bryansk, sklil, SAMARA, Samara, SPb, Vladimir, s-t-ORK, Donetsk, Kazelia, favi.ru, Flesk, Stavropol, Yaroslav, 77 Москва, tatarstan, Internet Widgits Pty Ltd, 77 г. Москва, KRSK, kb-CA, ddos-guard, jarnet-DCEAOS-CA, voronezh, GTN-SRV-CA, TULA, zostobr-SRV-DHCP-VLAN-CA, Rostov-on-Don, Pskov, SUB.CA.GOVRB.RU, N.Novgorod, RU, sovet-nso.ru, mx.all.culture.ru, CAP root CA, Certum Certification Authority, Khanty-Mansiysk, mail.khbr.meteorf.ru, Saransk, MT, SomeCity, krs, UserGate, XX, Finance Dept, Oldestatehotel, Axelname LLC, IT-Group Certificate Authority, No-Sni, Yekaterinburg, ca-83470554882603056 74.

```
https://old.volganet.ru – CA: Russian Trusted Sub CA
https://mru59.fmbaros.ru – CA: Russian Trusted Sub CA
https://mintrans.krskstate.ru – CA: Russian Trusted Sub CA
https://mru81.fmbaros.ru – CA: Russian Trusted Sub CA
https://25reg.roszdravnadzor.ru – CA: Russian Trusted Sub CA
https://trud.krskstate.ru – CA: Russian Trusted Sub CA
https://pricekontrol.krskstate.ru – CA: Russian Trusted Sub CA
https://urp.volganet.ru – CA: Russian Trusted Sub CA
https://czn.volgograd.ru – CA: Russian Trusted Sub CA
https://smsso.samregion.ru – CA: Russian Trusted Sub CA
https://socio.samregion.ru – CA: Russian Trusted Sub CA
https://iphone8usermanual.volgograd.ru – CA: Russian Trusted Sub CA
https://metropolisinternacional.volgograd.ru – CA: Russian Trusted Sub CA
https://elhovskiy.samregion.ru – CA: Russian Trusted Sub CA
https://my.krskstate.ru – CA: Russian Trusted Sub CA
https://homebank-trust.volgograd.ru – CA: Russian Trusted Sub CA
https://czn.volganet.ru – CA: Russian Trusted Sub CA
https://pv.samregion.ru – CA: Russian Trusted Sub CA
https://mru118.fmbaros.ru – CA: Russian Trusted Sub CA
https://dob.samregion.ru – CA: Russian Trusted Sub CA
https://minzdravao.ru – CA: Russian Trusted Sub CA
https://202ufc.volgograd.ru – CA: Russian Trusted Sub CA
```

VPN usage

With VPNs like Cloudflare WARP[16], and NordVPN[17] everything works fine. but:

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

[16] github.com/cloudflare/boringtun
[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

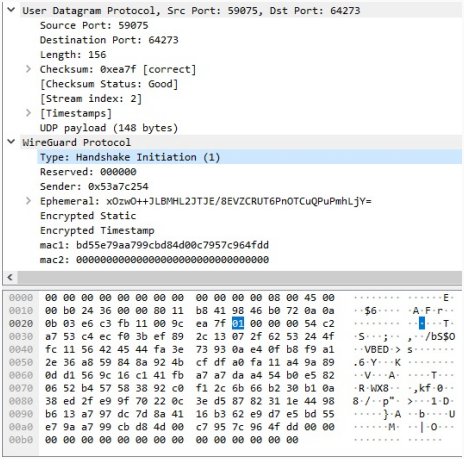


Figure 6: wireshark captured wireguard handshake

Methods comparing

	HTTP headers	VPN both	public DNS plain	DoH/DoT
Is it works?	✗	✓	✓	✓

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

Cost comparing

	VPN services	VPS server	Google DoH	1.1.1.1 UDP DNS
price	4$	2$	0$	0$

- 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

MATERIALS