IMC’25
[OONI - Project 2] Encrypted Client Hello (ECH) blocking

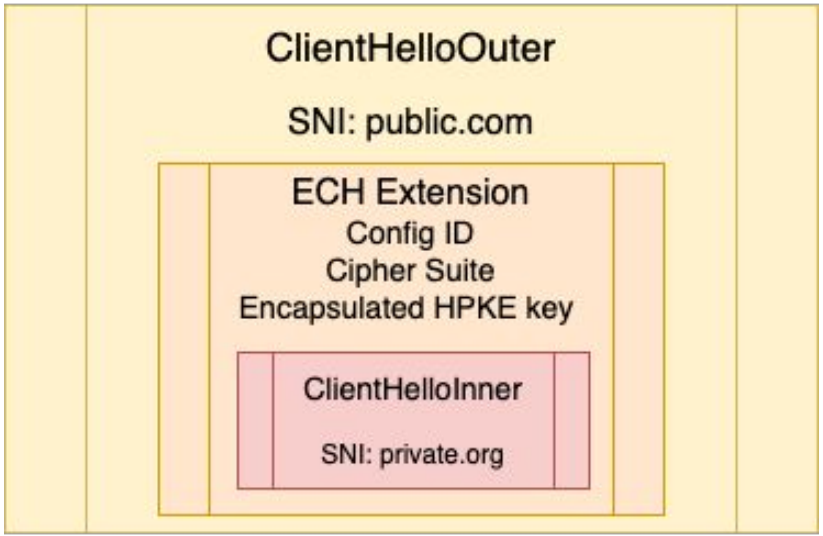
Yejin Cho, Xiao Song

Encrypted Client Hello is blocked in Russia

- Cloudflare's deployment of Encrypted Client Hello (ECH) is blocked in multiple networks in Russia since 2024-11-05.

Two triggers:

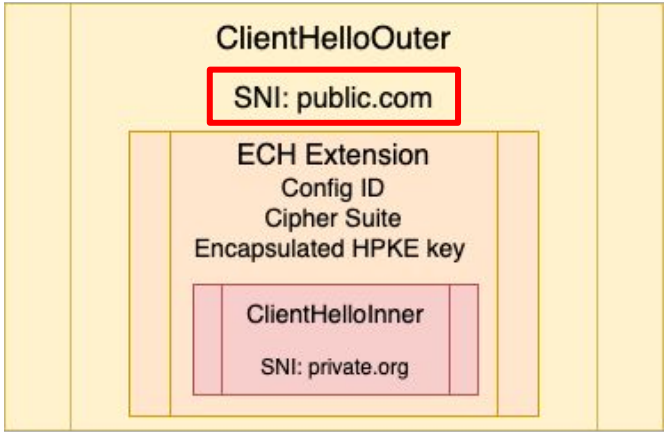
- An SNI extension with the value cloudflare-ech.com.
- An ECH extension.



OONI built-in ECN-block measurement

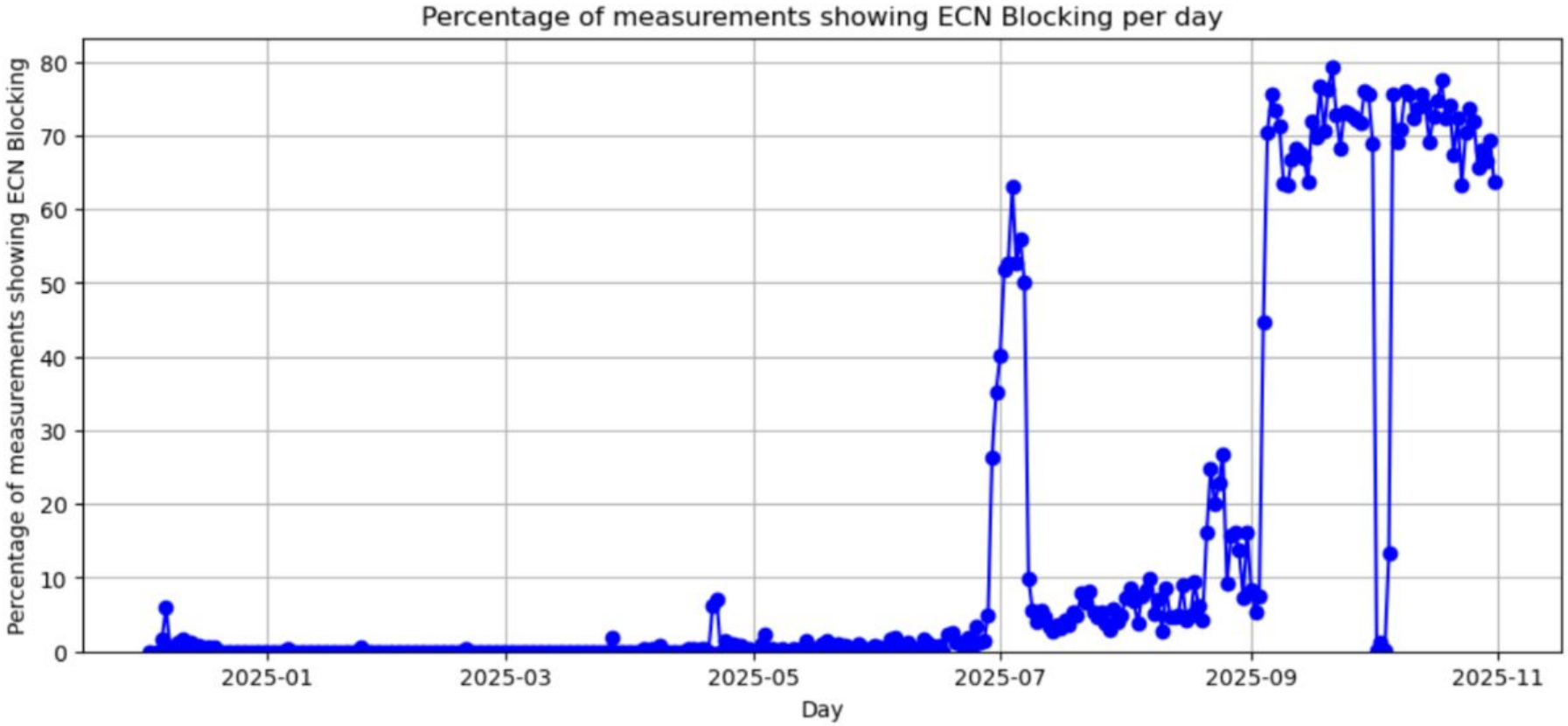
- VP resolves the given target URL and establish a TCP connection
- makes three TLS handshake attempts
  - 1) Outer SNI == ‘cloudflare-ech.com’
  - 2) Outer SNI == ‘cloudflare.com’
  - 3) No ECH
- Intuitively, if 1) and 2) fail but 3) succeeds

  -> ECN-block!

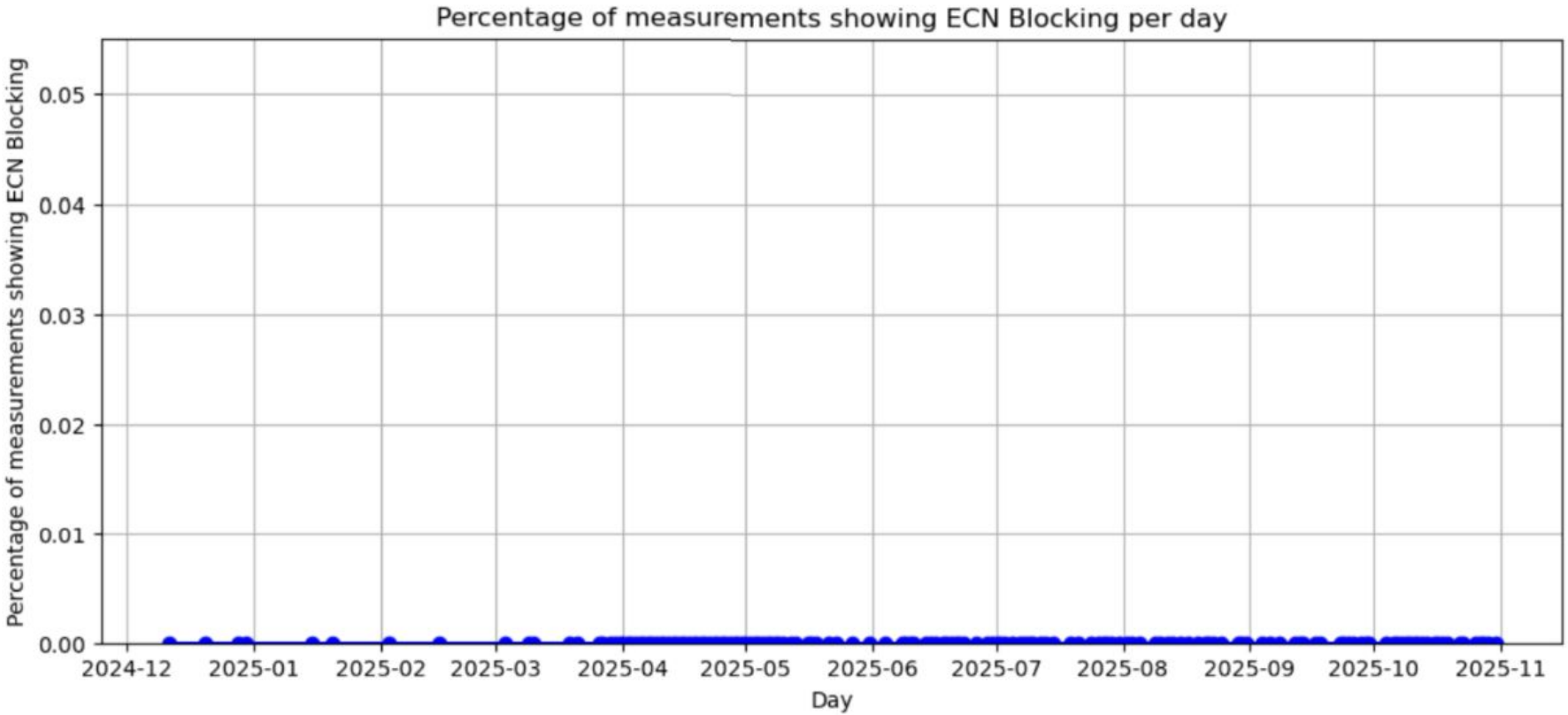



"tls_handshakes" : [
0 : {
"address" : string "8.47.69.0:443" ,
"cipher_suite" : string "" ,
"echconfig" : string "GREASE" ,
"failure" : string "timed_out" ,
"negotiated_protocol" : string "" ,
"network" : string "tcp" ,
"no_tls_verify" : bool fal
"outer_server_name" : str
"peer_certificates" :
"server_name" : string "cl
"t" : float 968.513963076 ,
"t0" : float 0.216476653 ,
"tags" : [], 0 items
"tls_version" : string ""
}, 14 items
1 : {
"address" : string "8.47.69.0:443" ,
"cipher_suite" : string "TLS_CHACHA20_POLY1305
"failure" : NULL ,
"negotiated_protocol" : string "" ,
"network" : string "tcp" ,
"no_tls_verify" : bool false ,
"peer_certificates" : [...], 3 items
"server_name" : string "cloudflare-ech.com" ,
"t" : float 0.2717825 ,
"t0" : float 0.216349692 ,
"tags" : [], 0 items
"tls_version" : string "TLSv1.3"
2 : {
"address" : string "8.47.69.0:443" ,
"cipher_suite" : string "" ,
"echconfig" : "AEX+DQBBjgAgACAzxgKI7KV7j2kx8yL
string A="
"failure" : string "timed_out" ,
"negotiated_protocol" : string "" ,
ork" : string "tcp" ,
ls_verify" : bool false ,
r_server_name" : string "cloudflare-ech.com" ,
er_certificates" : [], 0 items
er_name" : string "cloudflare-ech.com" ,
float 968.513963076 ,
: float 0.212790115 ,
gs" : [], 0 items
version" : string ""
ems

Russia’s ECH blocking status



China’s ECH blocking status



Thank you!