ALEF

How TLS 1.3 adoption (and disposal of SSL) is going

Jan Kopřiva

jan.kopriva@alef.com @jk0pr

ALEF CSIRT

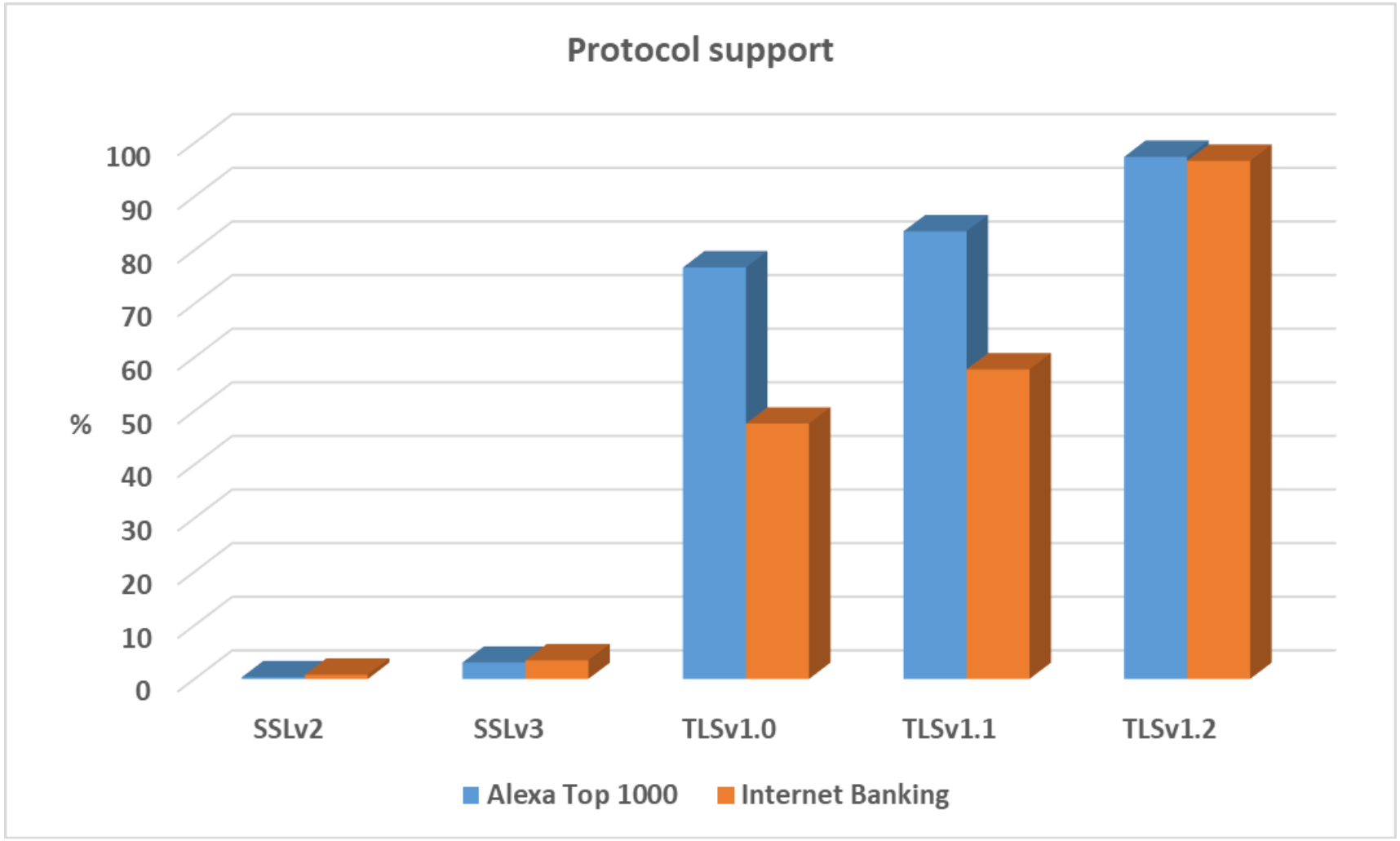
TLP: WHITE

Quick overview of SSL/TLS versions

Protocol	Published	Status
SSL 1.0	Unpublished	Unpublished
SSL 2.0	1995	Deprecated in 2011 (RFC 6176)
SSL 3.0	1996	Deprecated in 2015 (RFC 7568)
TLS 1.0	1999	Deprecated in 2020 (RFC 8996)[8][9][10]
TLS 1.1	2006	Deprecated in 2020 (RFC 8996)[8][9][10]
TLS 1.2	2008	
TLS 1.3	2018	

Source: Wikipedia

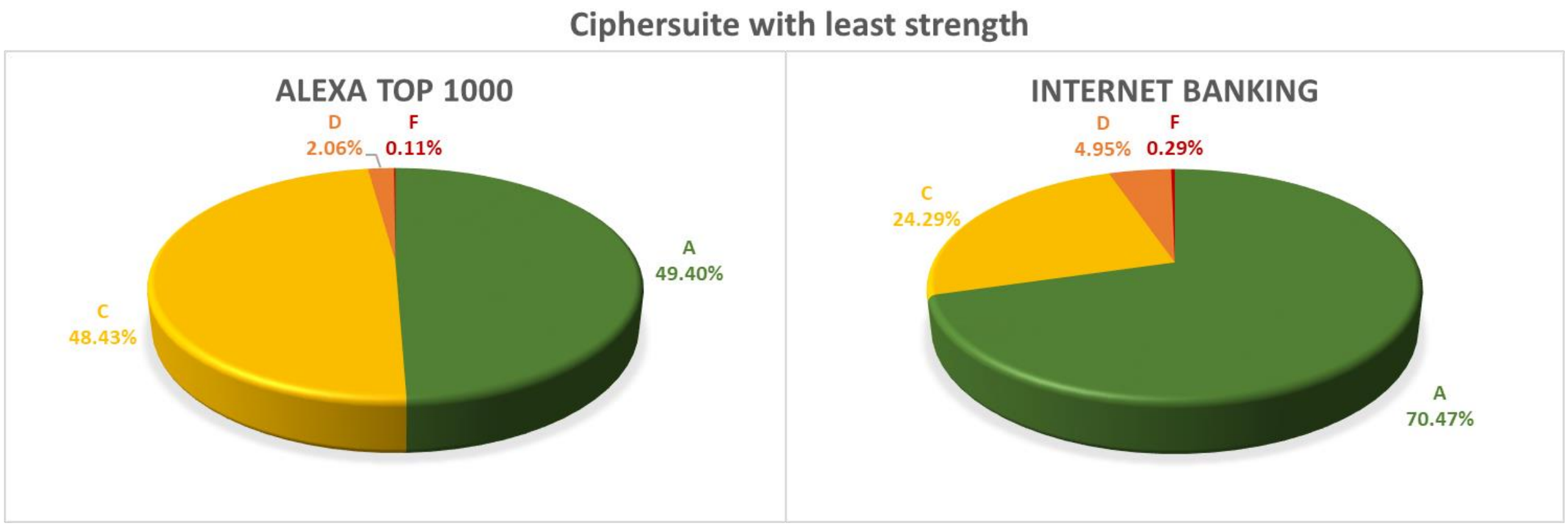
Interesting historical data – internet banking 2019



ALEF

Source: SANS Internet Storm Center

Interesting historical data – internet banking 2019



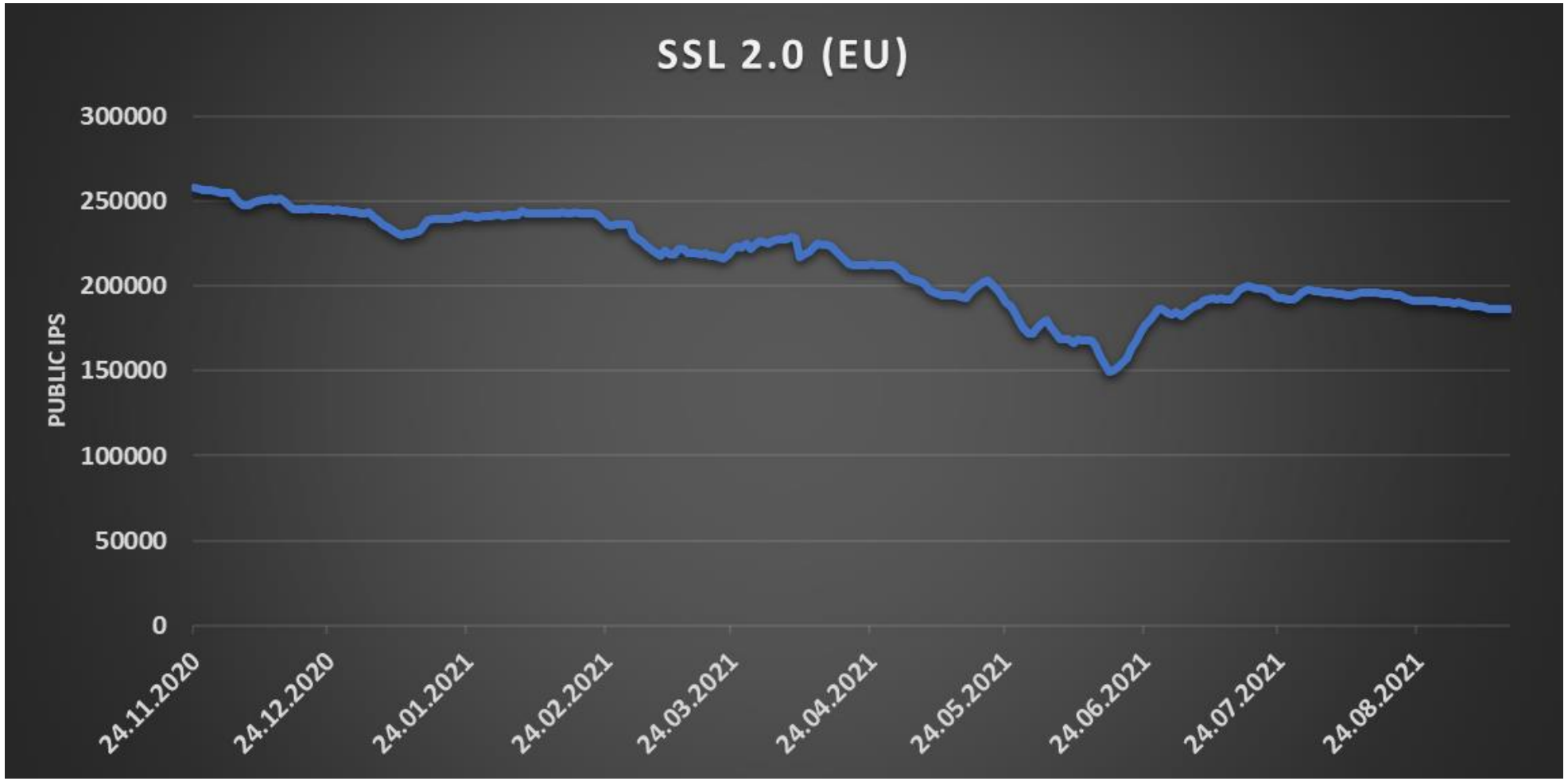
Source: SANS Internet Storm Center

How does SSL/TLS use look now?

ALEF

Source: Shodan

How does SSL/TLS use look now?



ALEF

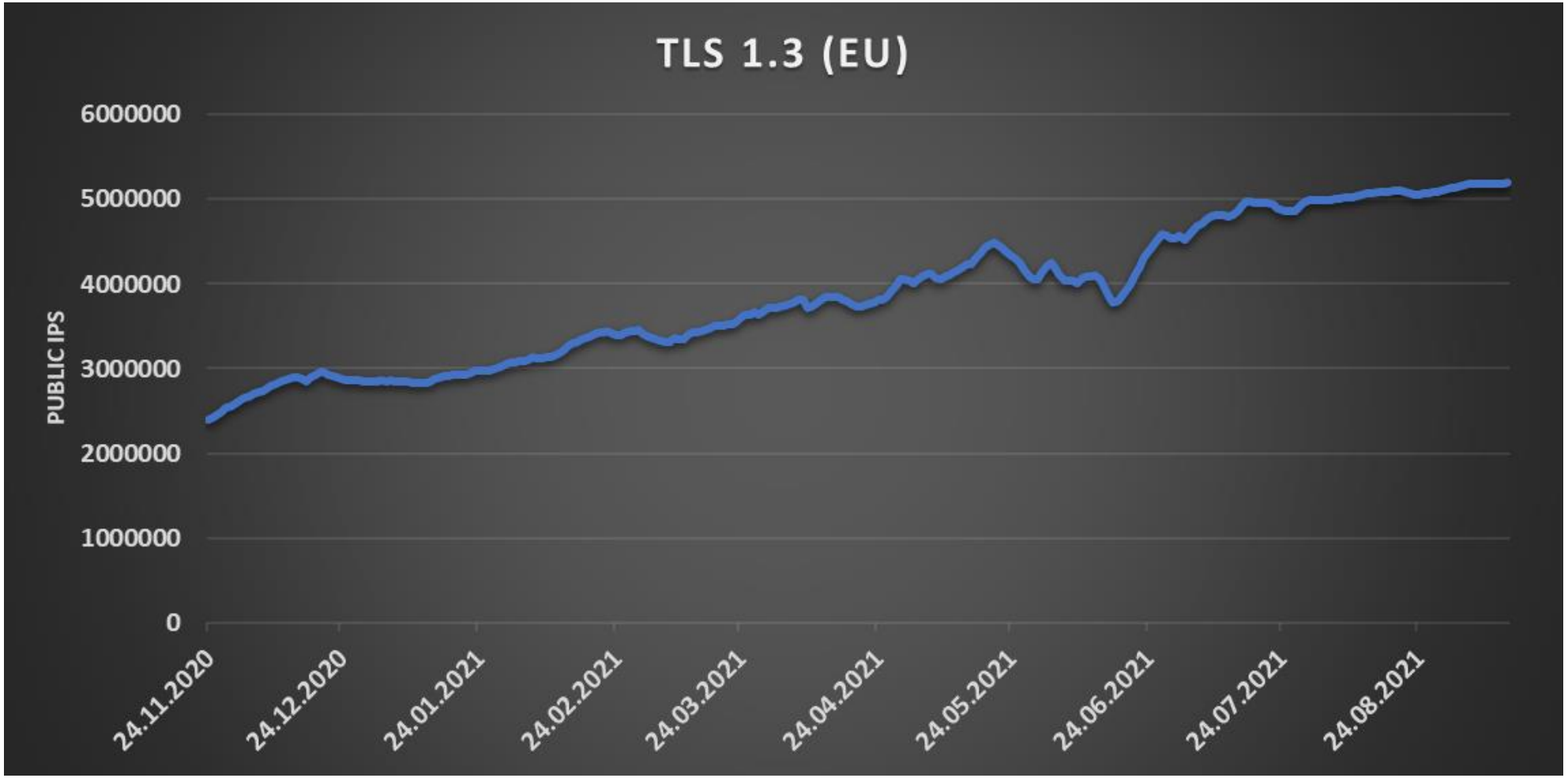
Source: Shodan

How does SSL/TLS use look now?

ALEF

Source: Shodan

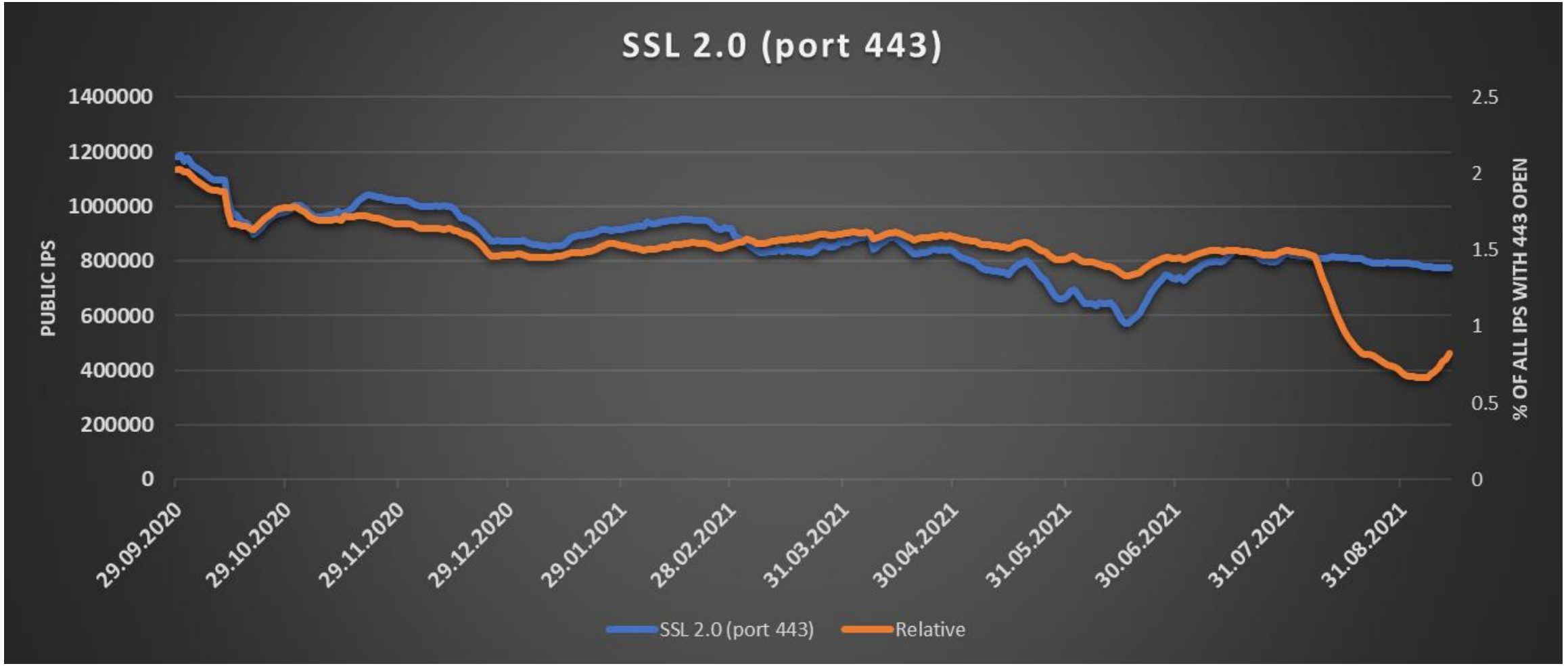
How does SSL/TLS use look now?



ALEF

Source: Shodan

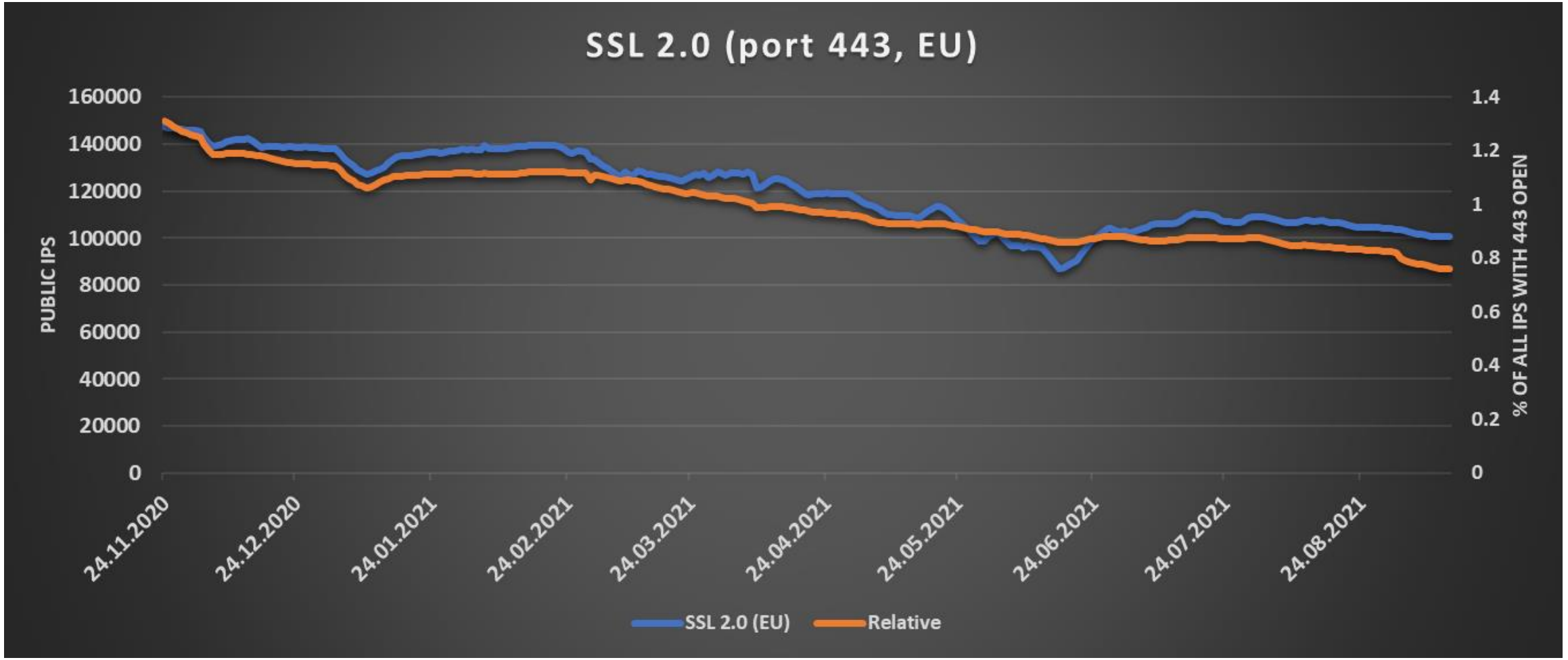
SSL/TLS on port 443



ALEF

Source: Shodan

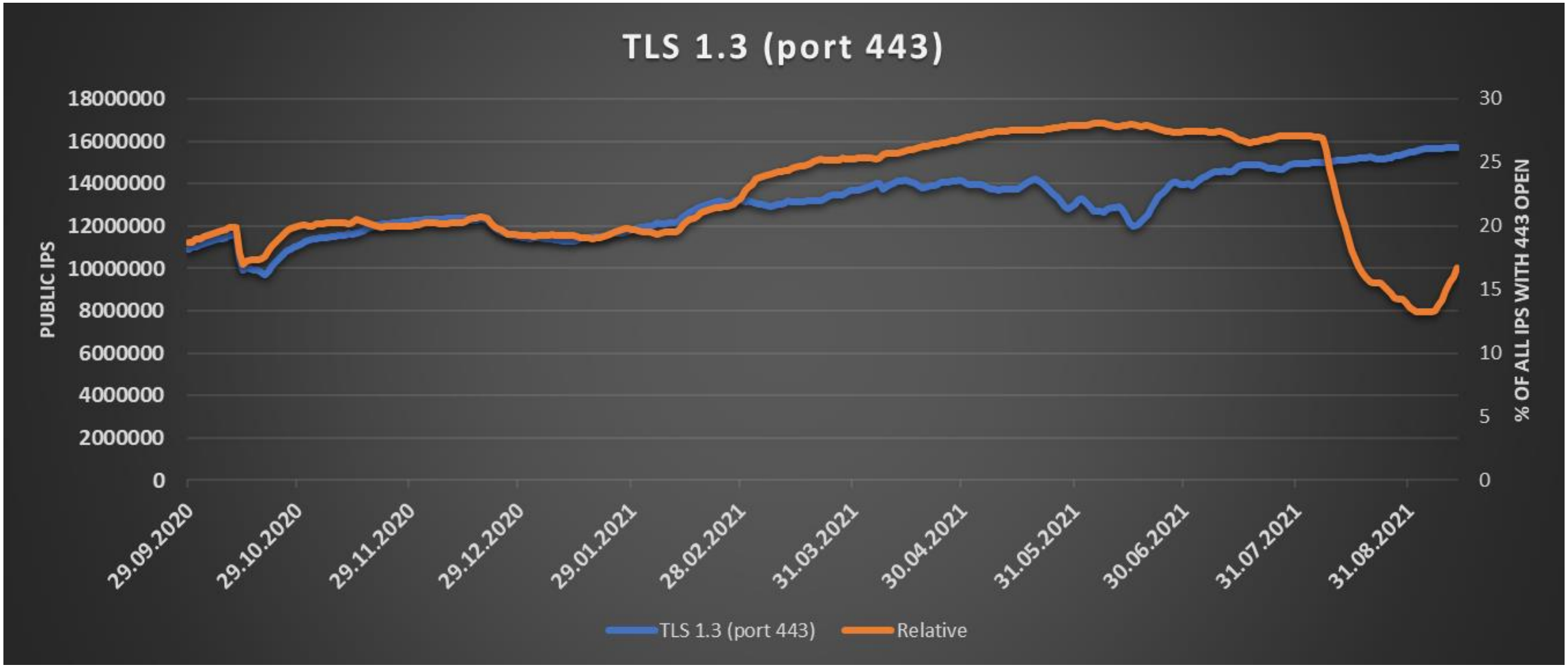
SSL/TLS on port 443



ALEF

Source: Shodan

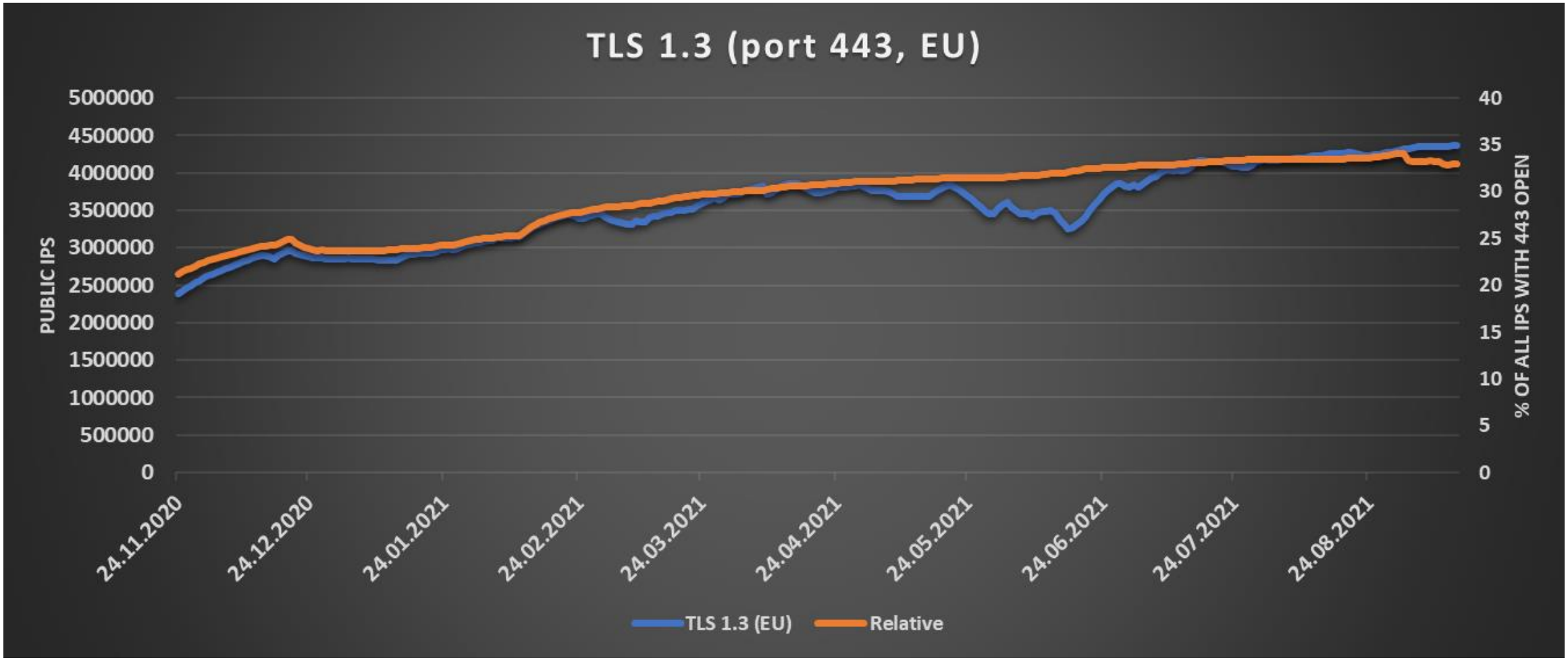
SSL/TLS on port 443



ALEF

Source: Shodan

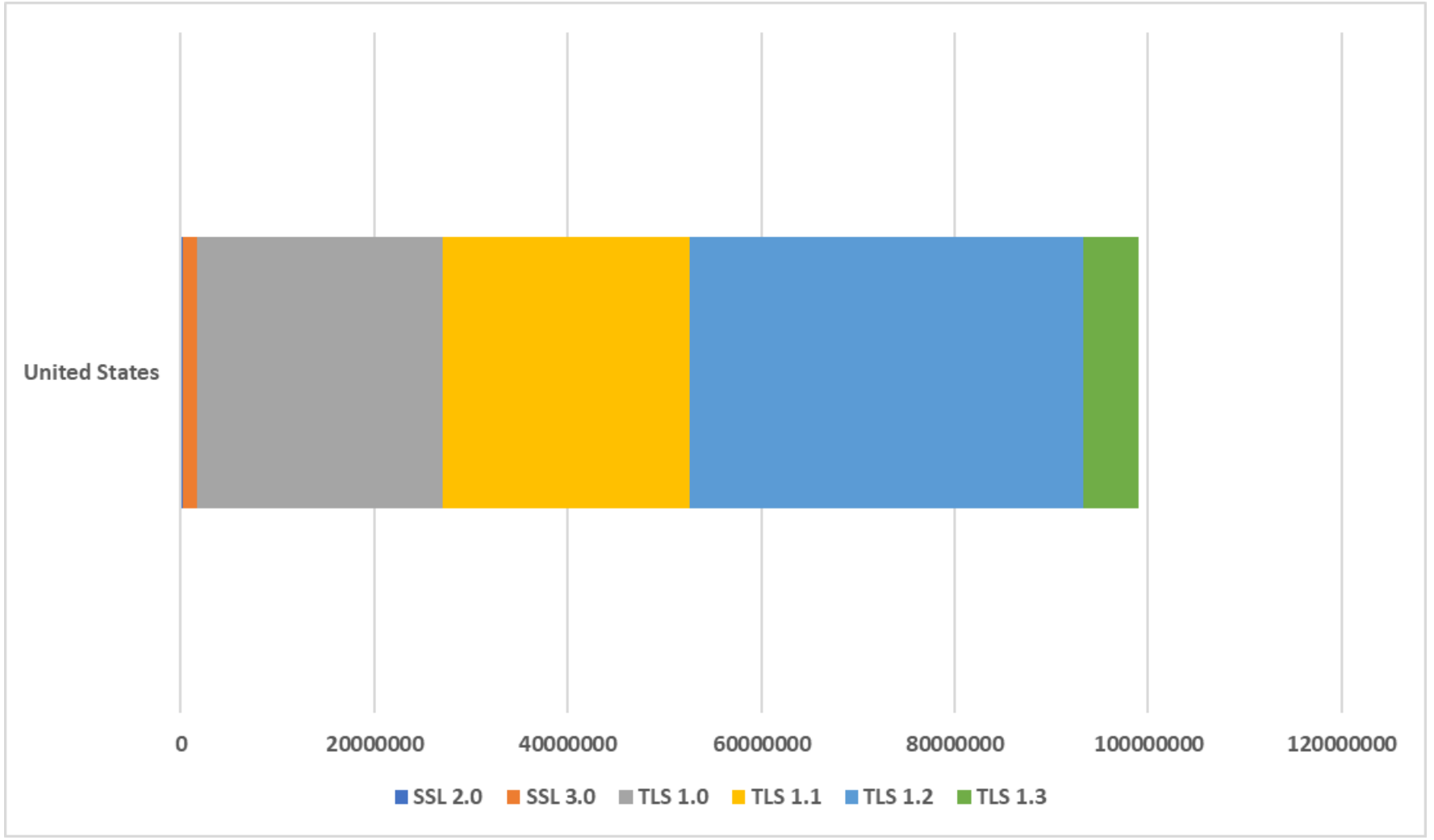
SSL/TLS on port 443



ALEF

Source: Shodan

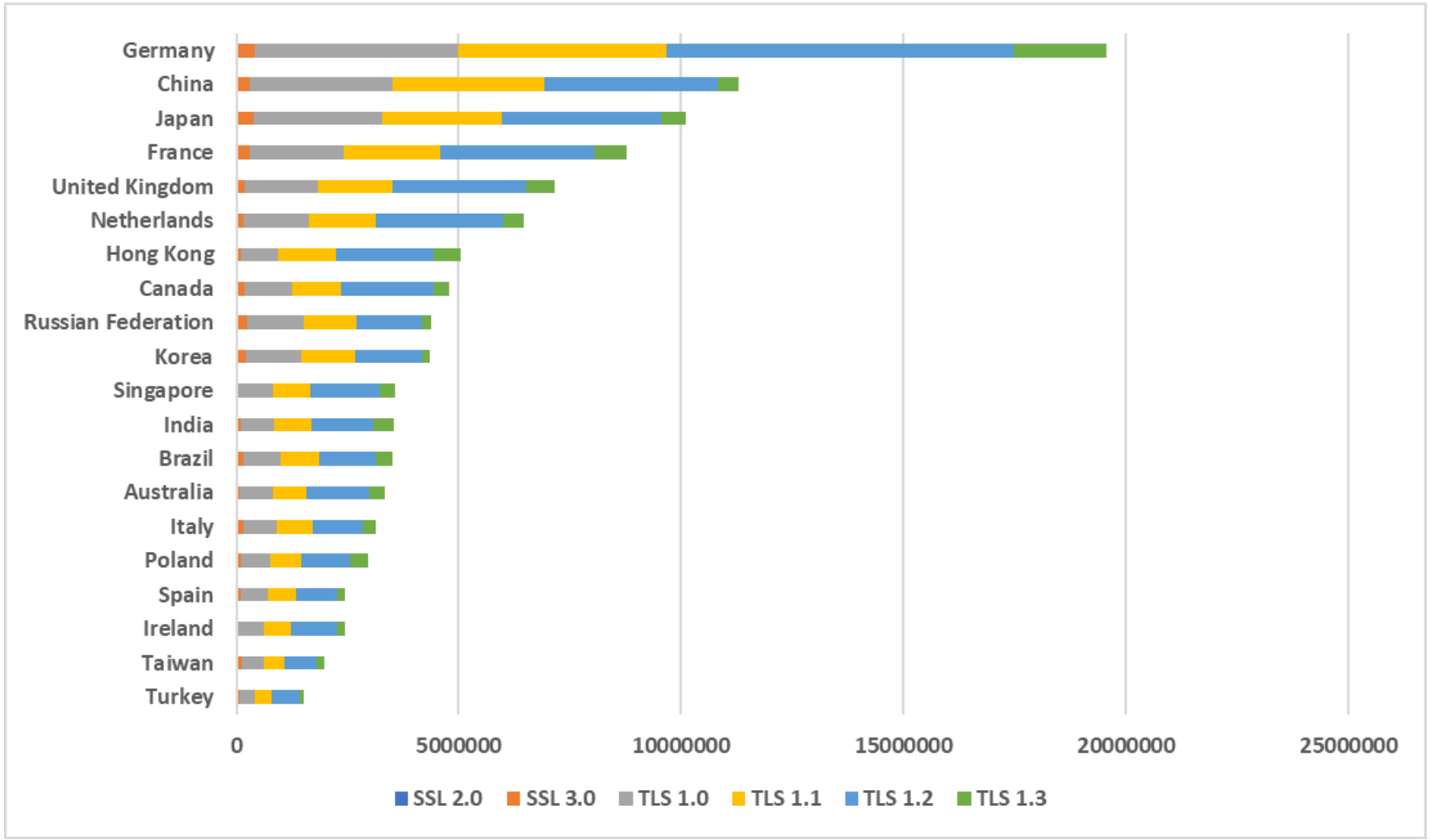
Differences between countries



ALEF

Source: Shodan

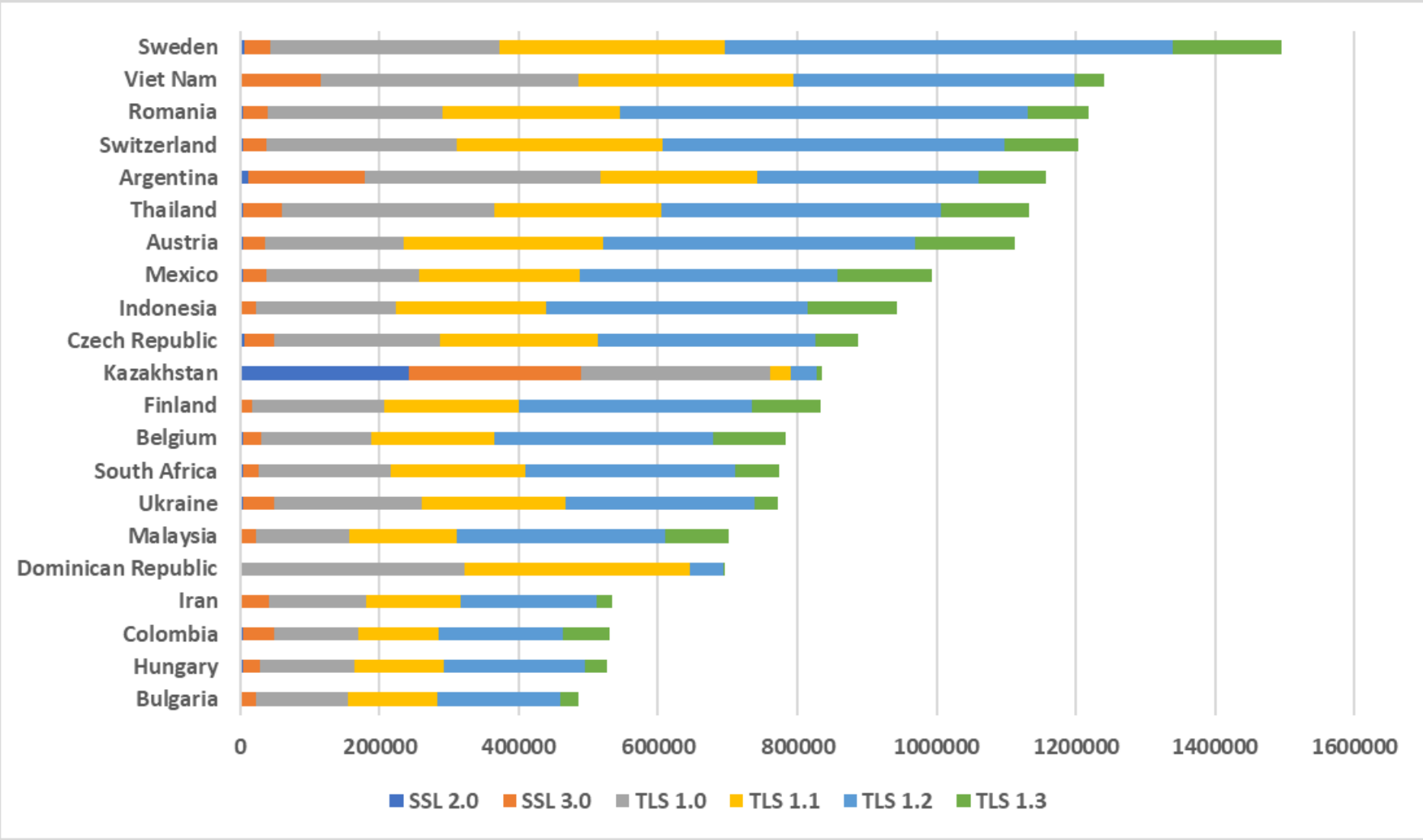
Differences between countries



ALEF

Source: Shodan

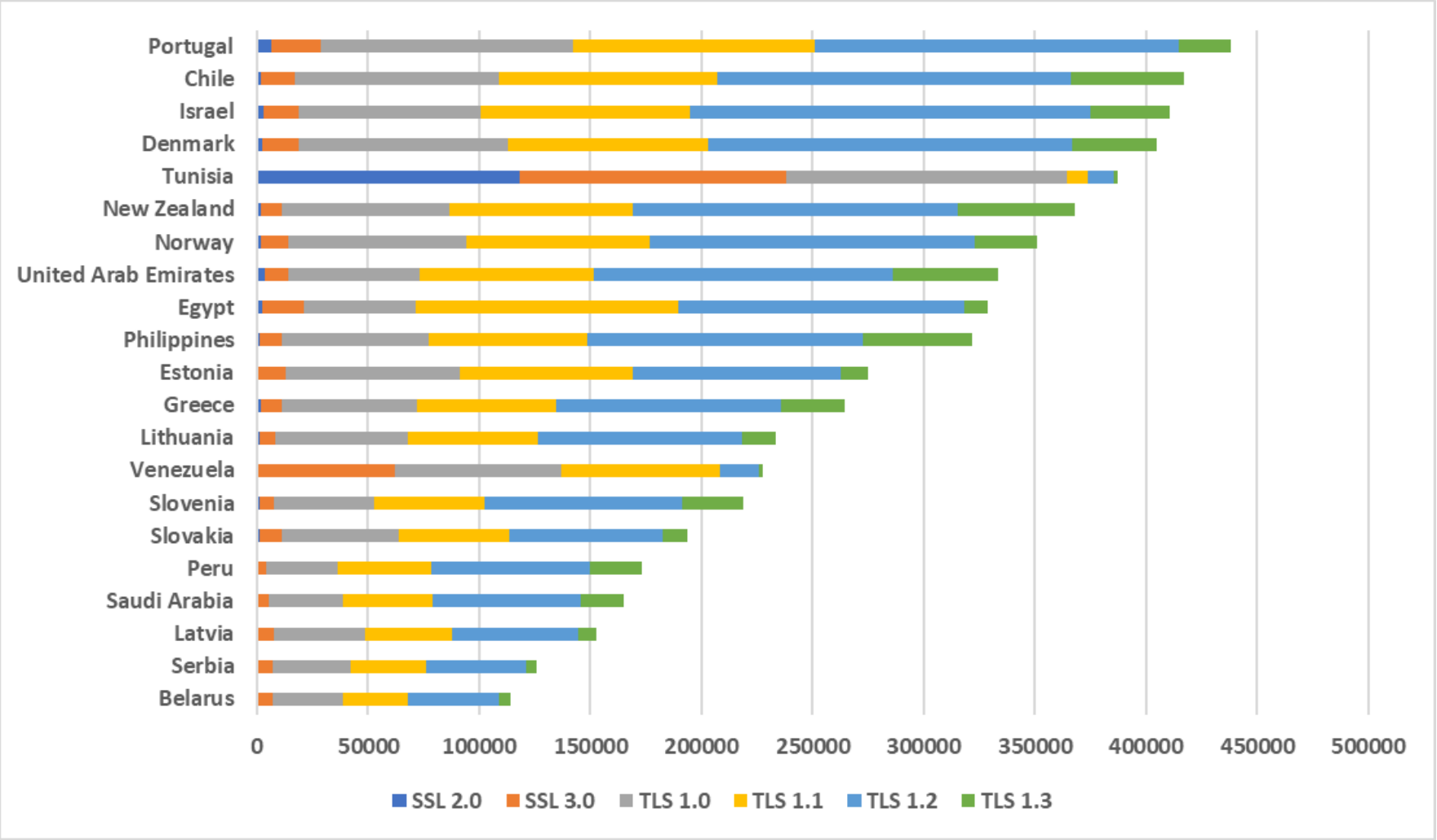
Differences between countries



ALEF

Source: Shodan

Differences between countries



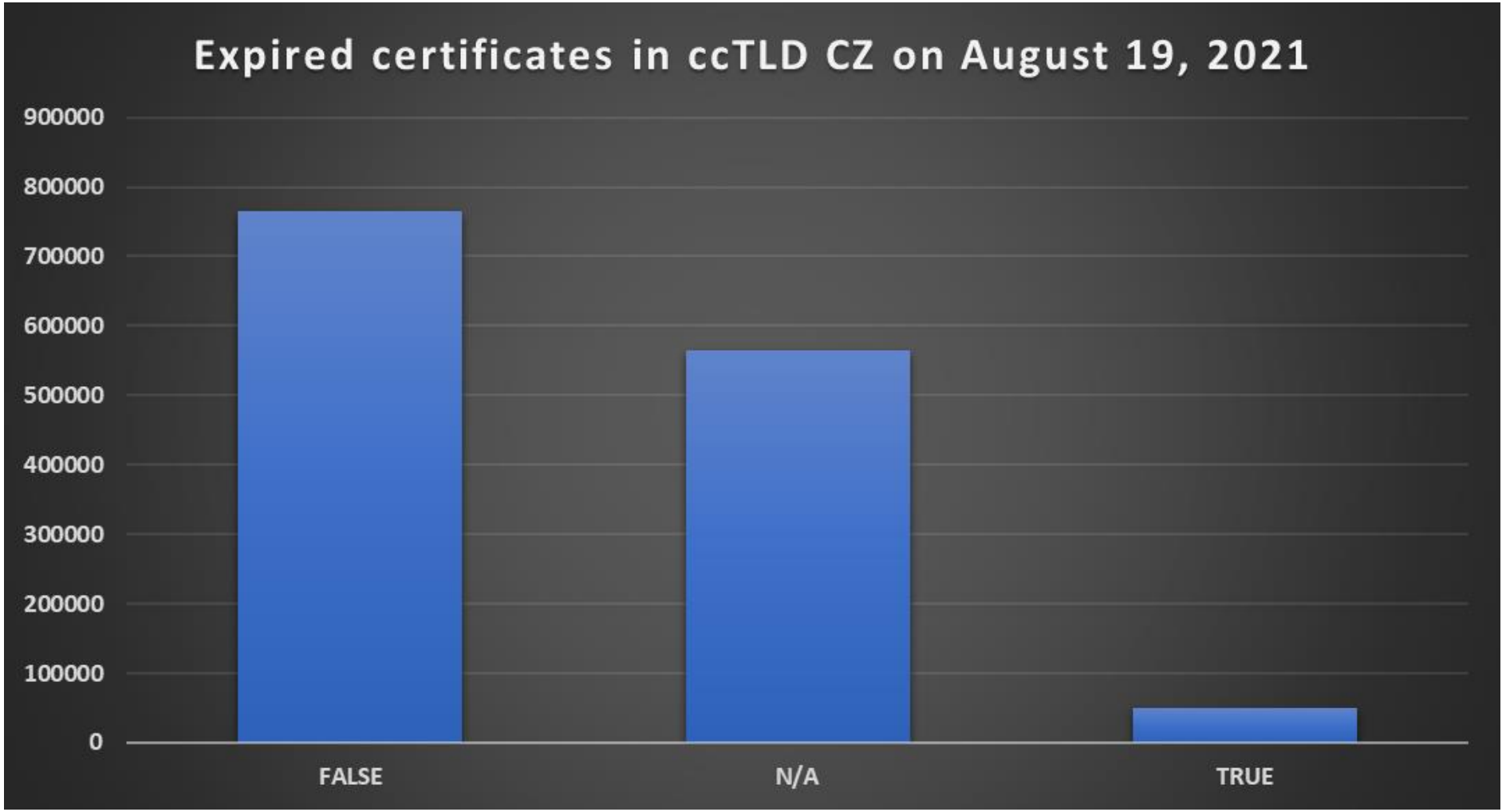
ALEF

Source: Shodan

That‘s not all…

- To get a more thorough overview we‘d need numbers for:
  - Trusted vs. Untrusted (self-signed/expired/…) certificates
  - Supported ciphersuites
  - Issuing CAs
  - …

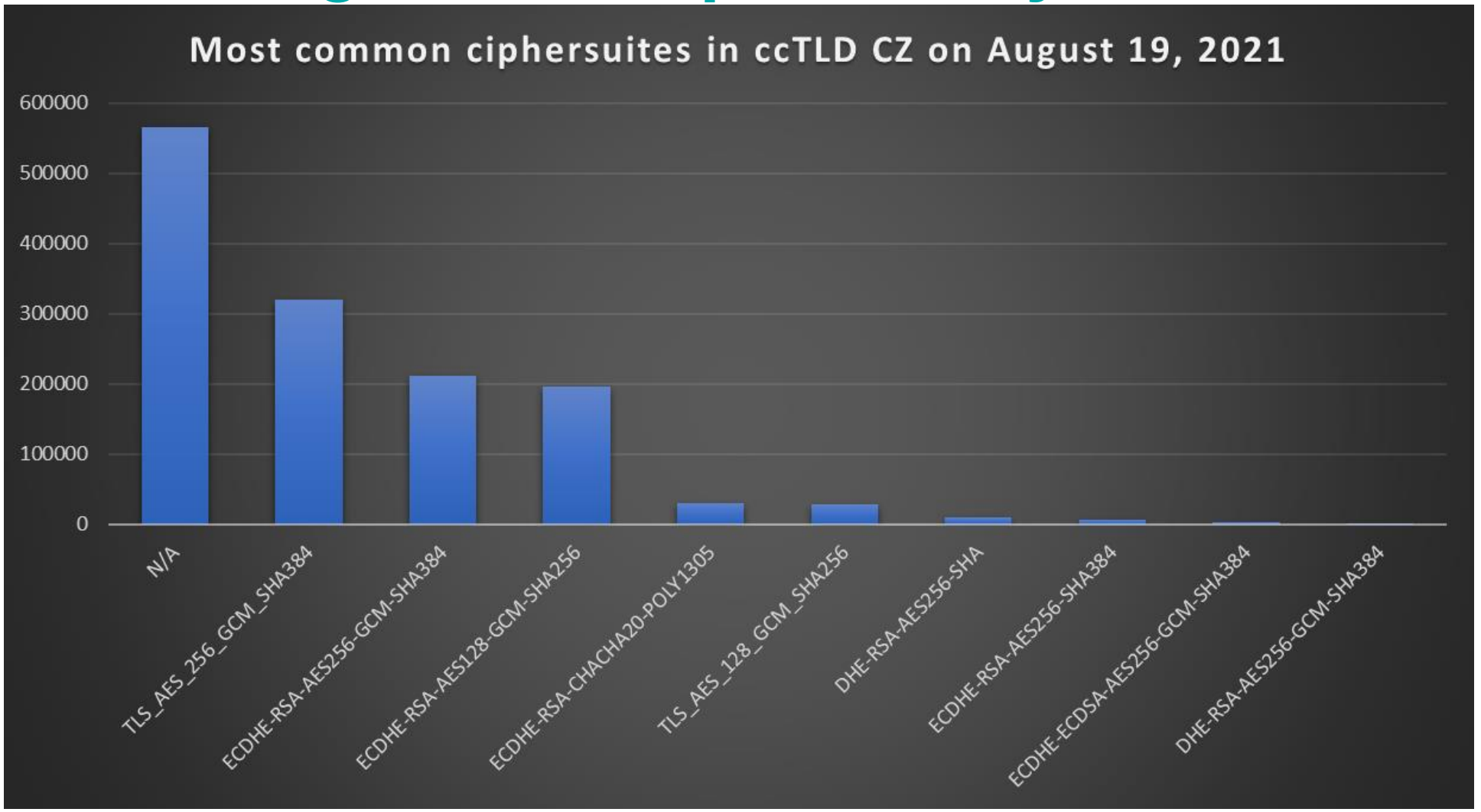
The remaining data can potentially be obtained



ALEF

Source: CZ.NIC

The remaining data can potentially be obtained



ALEF

Source: CZ.NIC

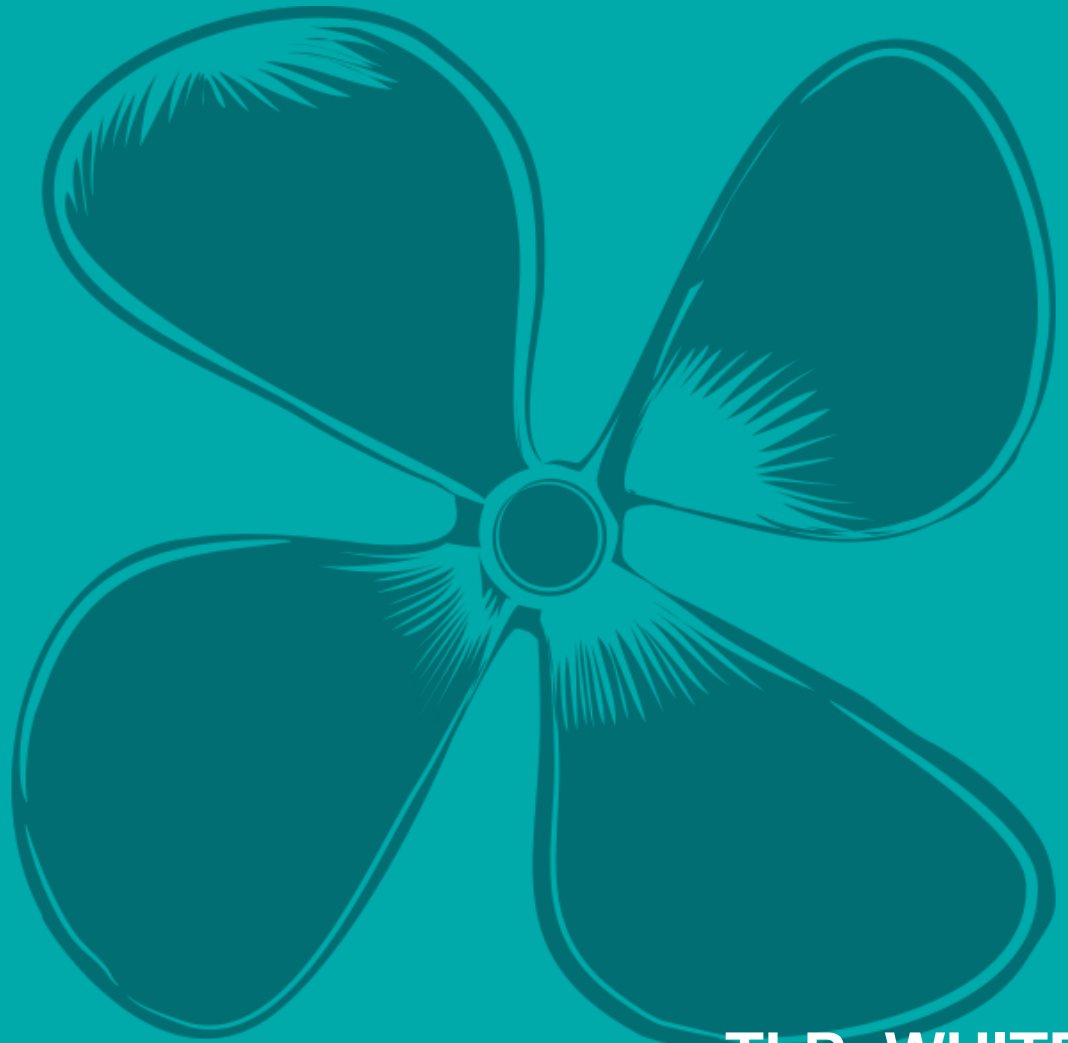
Do you want to take a look at your constituency?

- Passive option
  - Shodan (+TriOp) or similar platform

- Active option
  - Nmap or similar tool
  - ADAM from CZ.NIC

ALEF

Thank you for your attention



TLP: WHITE