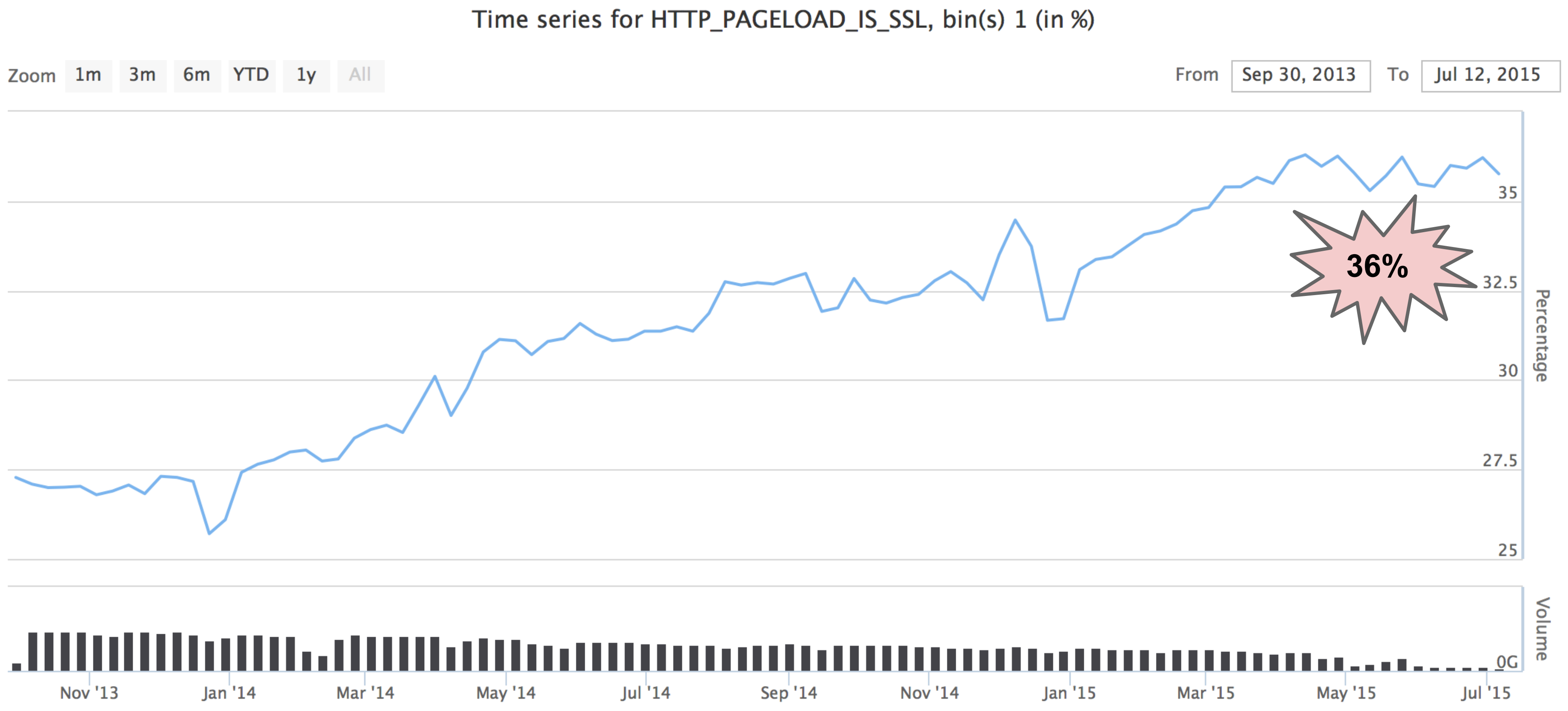
Some observations of TLS in the web

Perspectives

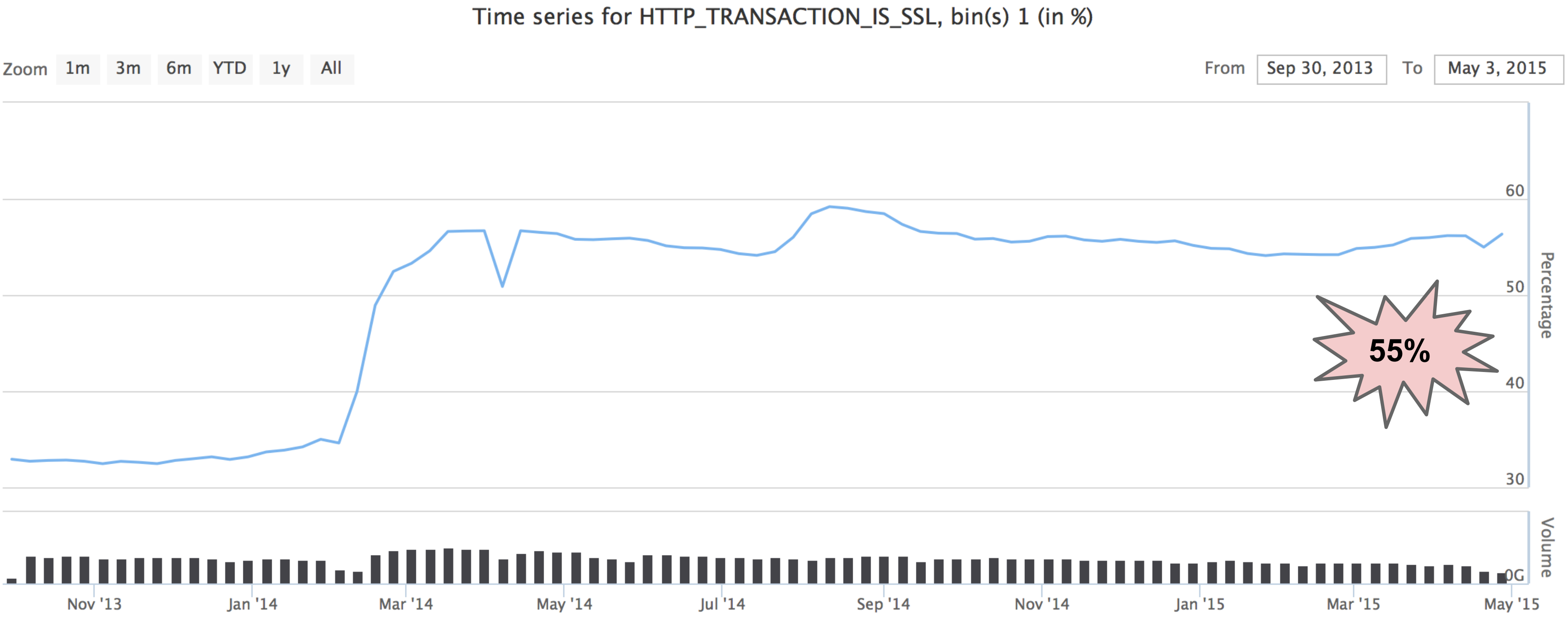
	Easy	Hard
Browser	% of transactions	% of sites
Servers / hosting providers	% of clients, transactions	% of sites
Scanning	% of sites*	% of transactions

How much TLS is there?



36%

How much TLS is there?

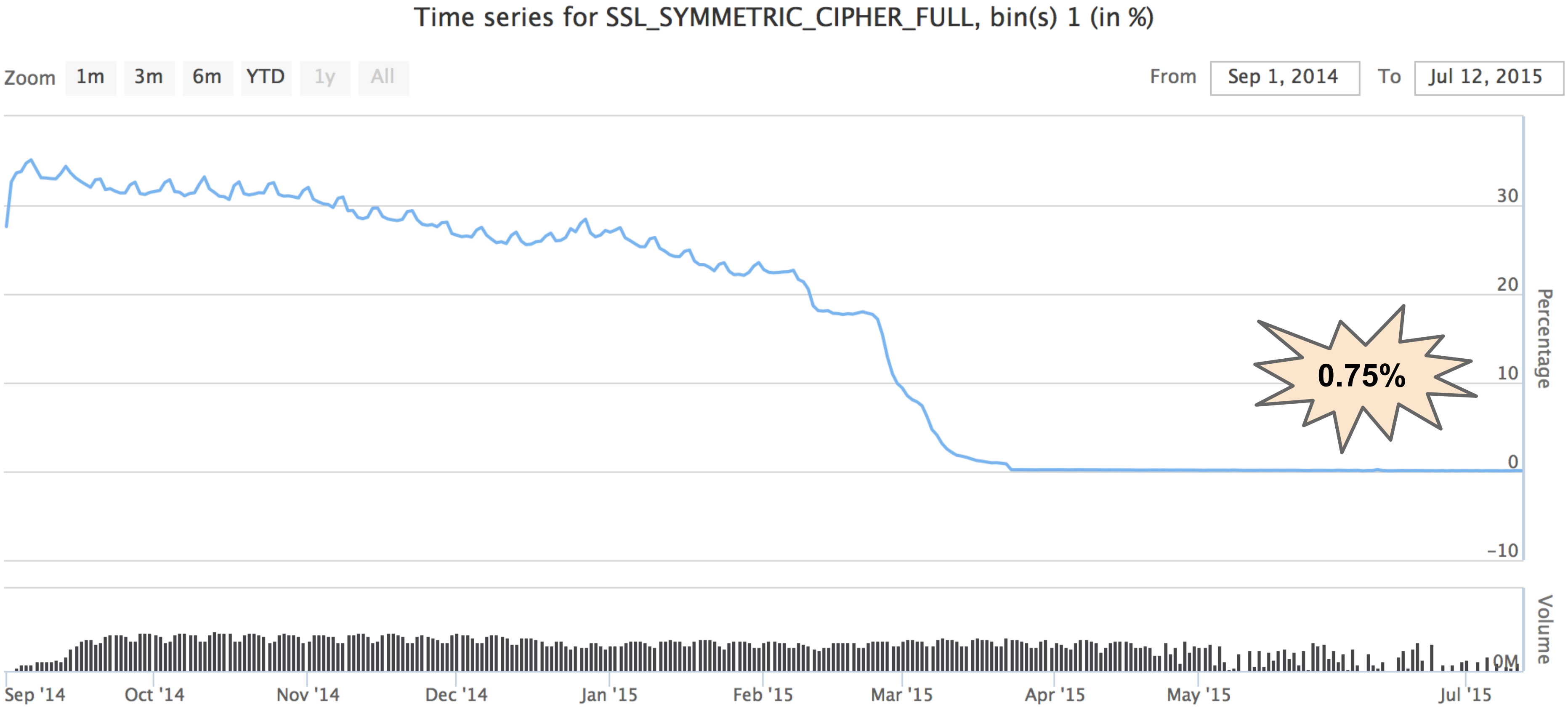


Time series for HTTP_TRANSACTION_IS_SSL, bin(s) 1 (in %)

From Sep 30, 2013 To May 3, 2015

55%

How much RC4?

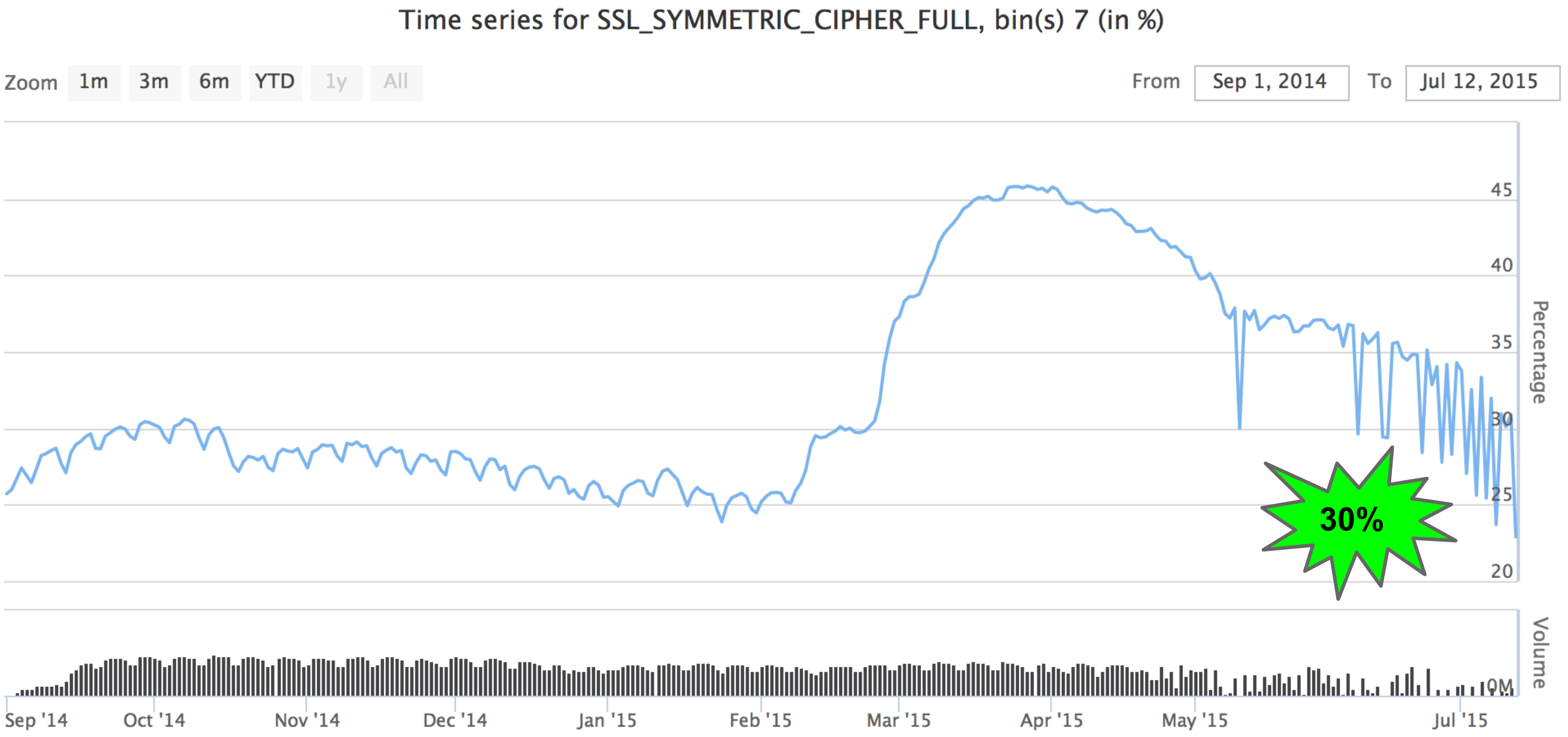


Time series for SSL_SYMMETRIC_CIPHER_FULL, bin(s) 1 (in %)

From Sep 1, 2014 To Jul 12, 2015

0.75%

Where did the RC4 go?



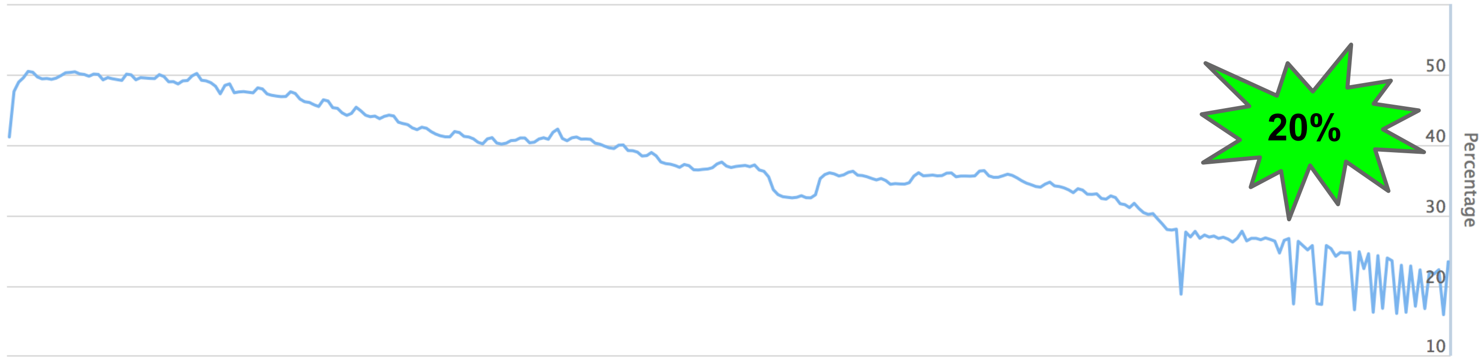
Time series for SSL_SYMMETRIC_CIPHER_FULL, bin(s) 7 (in %)

From Sep 1, 2014 To Jul 12, 2015

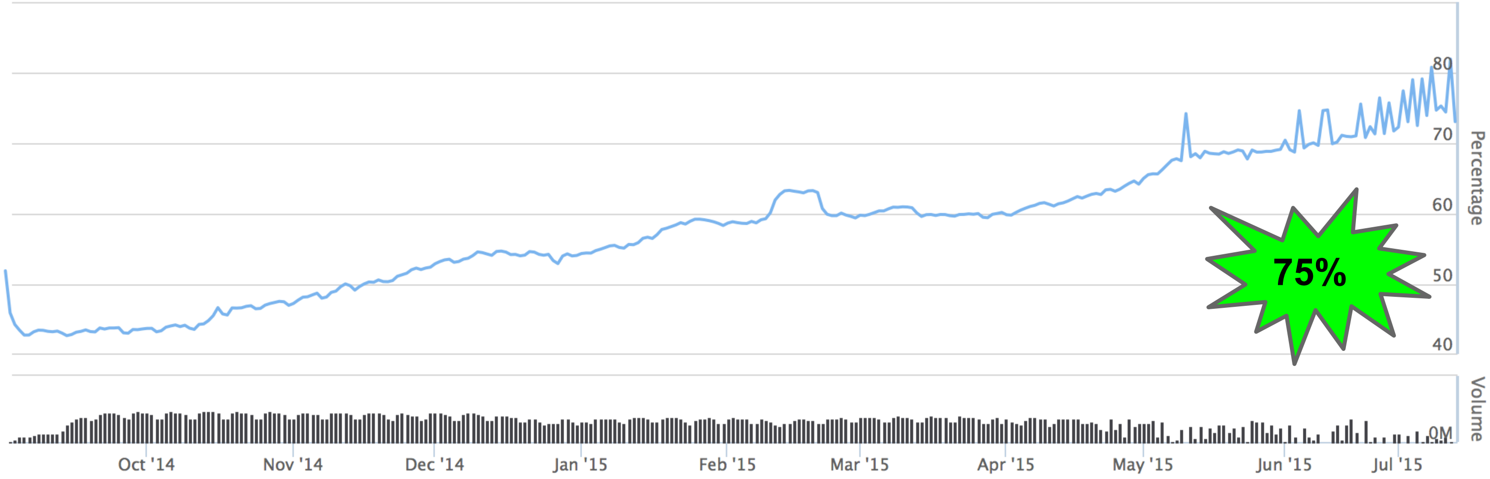
30%

How about key exchange?

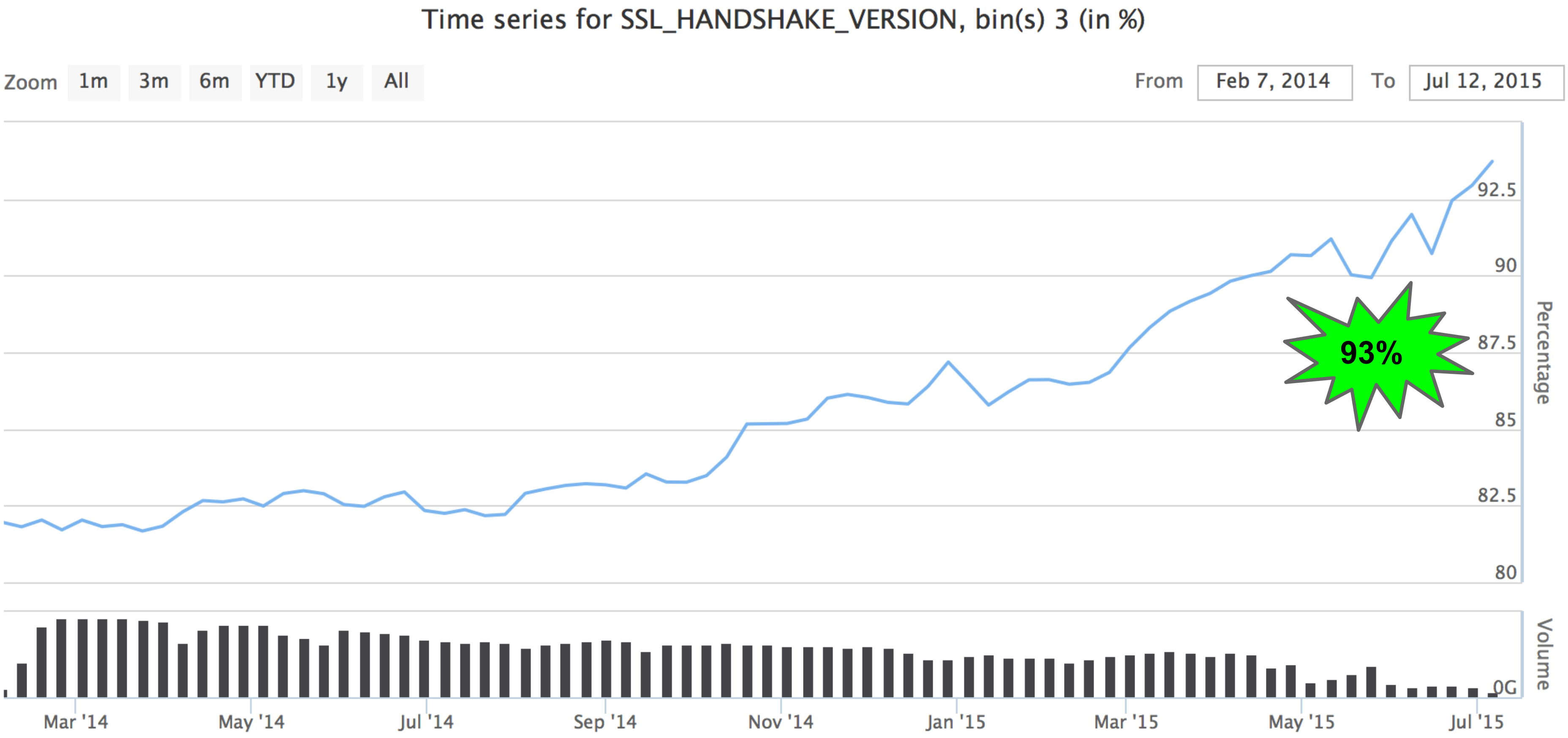
RSA



ECDH



TLS 1.2 on the march!



Time series for SSL_HANDSHAKE_VERSION, bin(s) 3 (in %)

93%

Summary

Need to bend the curve on TLS adoption

Ciphers and versions moving in the right direction

[[All data sets shown in this preso are public. Ask me about how to use them!]]