

# Cybercrime and TLS



Технический  
Центр  
Интернет



# Cybercrime and TLS

## Phishing, Browsers and Let's Encrypt

**Dmitry Belyavskiy, Technical Centre of Internet**

**Almaty, Kazakhstan**

**September 6-7 2017**

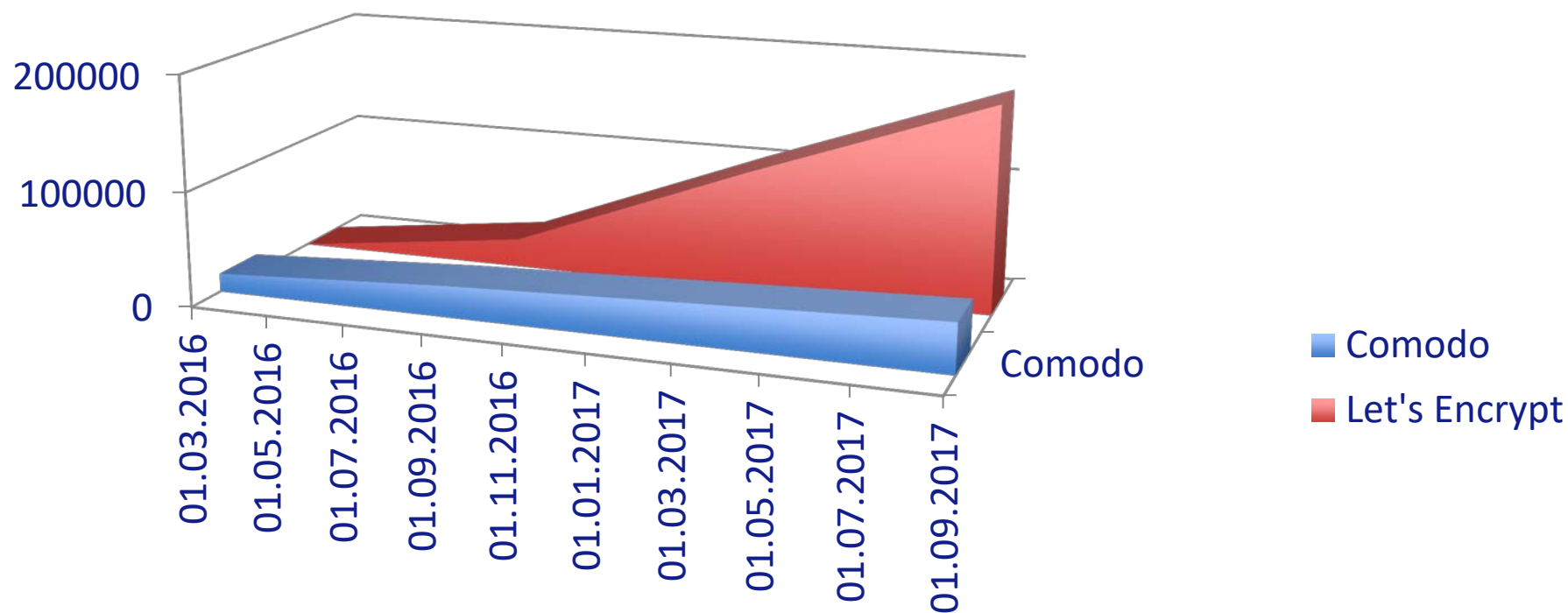


# Certificates for free!



Технический  
Центр  
Интернет

Source: <https://statdom.ru>

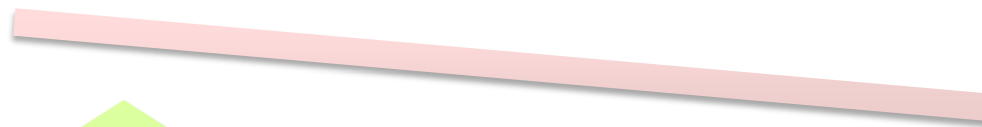
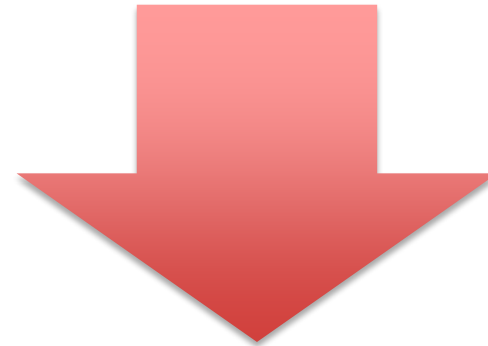


# Free certificates: bad news



Технический  
Центр  
Интернет

Phishing  
domains



Normal  
domains

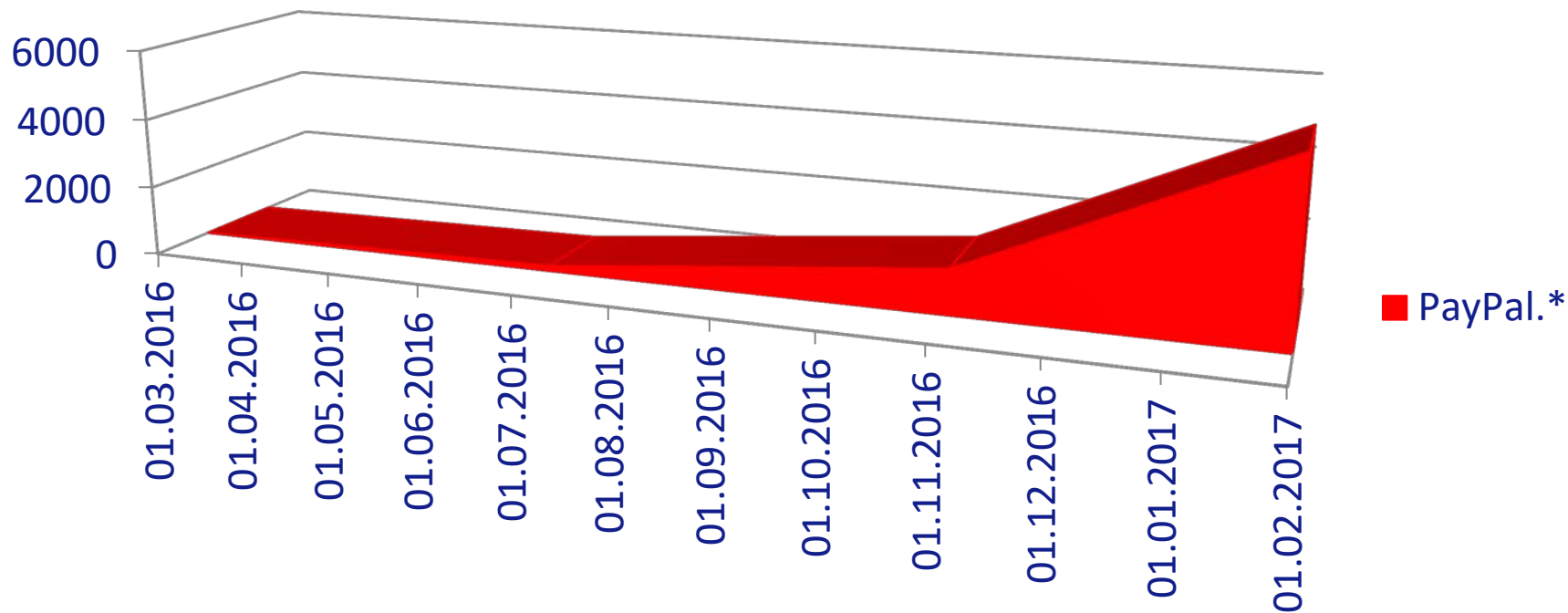
# PayPal phishing certificates



Технический  
Центр  
Интернет

Source:

<https://www.bleepingcomputer.com/news/security/14-766-lets-encrypt-ssl-certificates-issued-to-paypal-phishing-sites/>

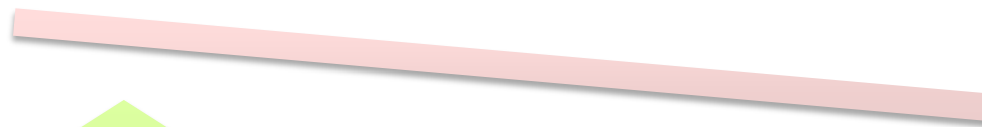
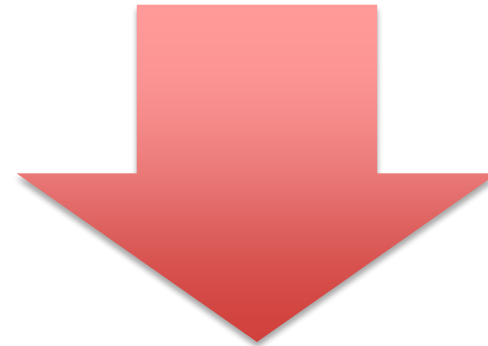


# Free certificates: balance



Технический  
Центр  
Интернет

Free wildcard  
certificates



CA/Browser forum  
recommendations

**Explain to users!**



**Технический  
Центр  
Интернет**

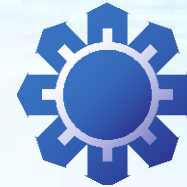
**Certificate is significant for reputation**

**DV certificates confirm only control over domain**

**EV certificates confirm the domains owner  
Sell more EV certificates!**

**Green lock means nothing**





**CAs: CA/Browser's Forum recommendations**  
**+ Check "dangerous" names**  
**- Automatic issuance**

**Browsers:**  
**Warn users about suspicious names**  
**False positives**



Questions?

[beldmit@tcinet.ru](mailto:beldmit@tcinet.ru)