UNDER THE HOOD

DARIUS POVILAITIS

DARIUS@ESEC.LT

HTTPS://TYRIMAI.ESEC.LT

O365 AUTHENTICATION METHODS

Most organizations using Office365 have authentication setup which might expose them to the social-technical attacks.

- User / password
- User / password + 2FA (e.g. SMS or Microsoft Authenticator)
- Federation (here you can use digital certificates)

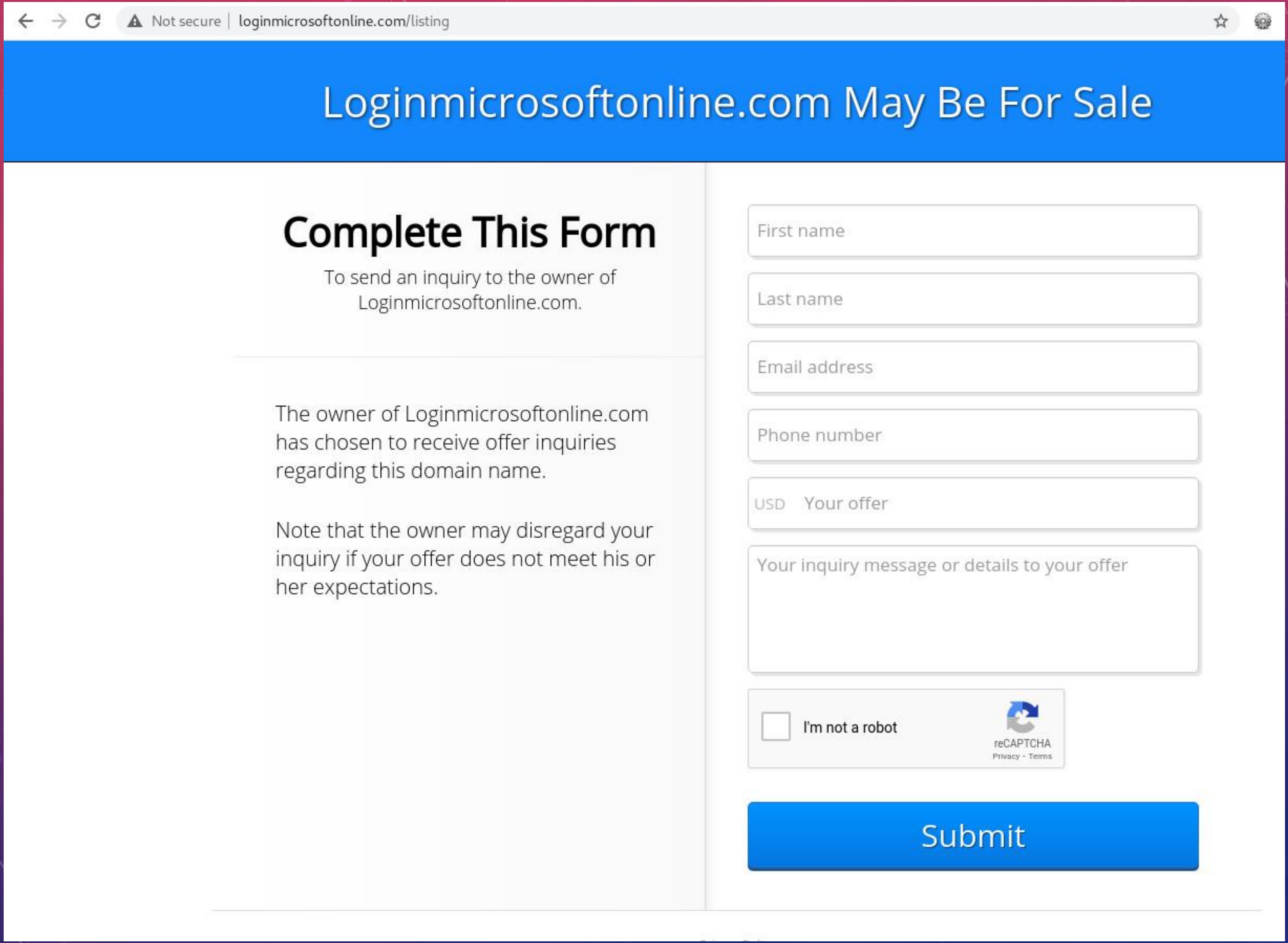
O365 - TWO FACTOR AUTHENTICATION

If an organization wants to implement O365 in a secure way, they are considering all the above-mentioned authentication solutions. User/password authentication is insecure – everyone understands that. Federation with certificates – are legacy – that's what I was told by local solution providers. The winner here is two factor authentication – 2FA – that's what is said

- Username / password with SMS (or Microsoft Authenticator) solves all authentication risks. Really ?

Do you have such a setup ?

- What would you say if just one email or SMS could break all your security ?
- The biggest problem here is that organizations don't even understand that they could be very easy target since they are assured that 2FA is very secure.



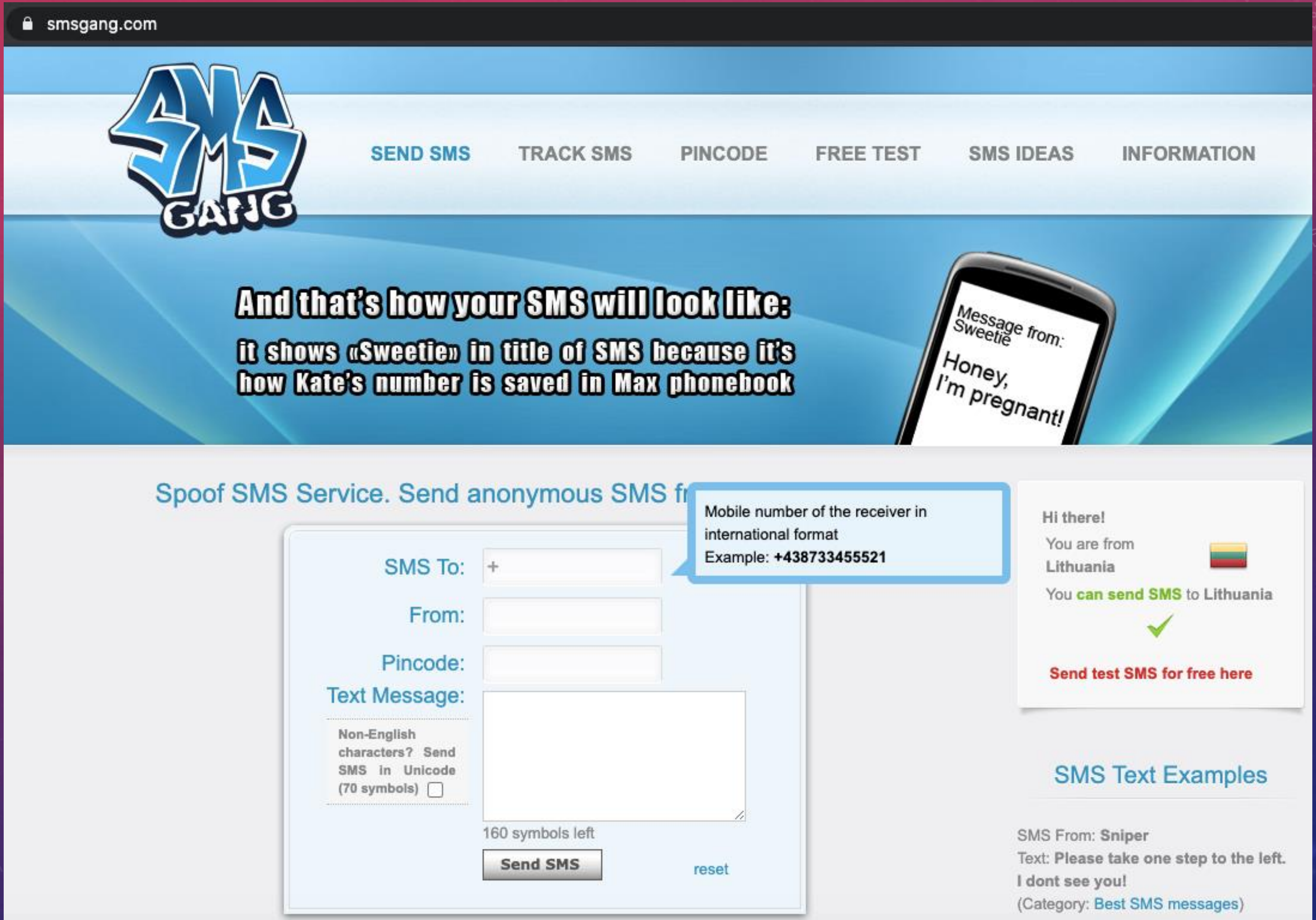
Loginmicrosoftonline.com May Be For Sale

Complete This Form

To send an inquiry to the owner of Loginmicrosoftonline.com.

The owner of Loginmicrosoftonline.com has chosen to receive offer inquiries regarding this domain name.

Note that the owner may disregard your inquiry if your offer does not meet his or her expectations.



And that's how your SMS will look like:

it shows «Sweetie» in title of SMS because it's how Kate's number is saved in Max phonebook

Spoof SMS Service. Send anonymous SMS fr

Mobile number of the receiver in international format
Example: **+438733455521**

SMS To:	+
From:	
Pincode:	
Text Message:	

Non-English characters? Send SMS in Unicode (70 symbols) □

160 symbols left

Hi there!

You are from **Lithuania**

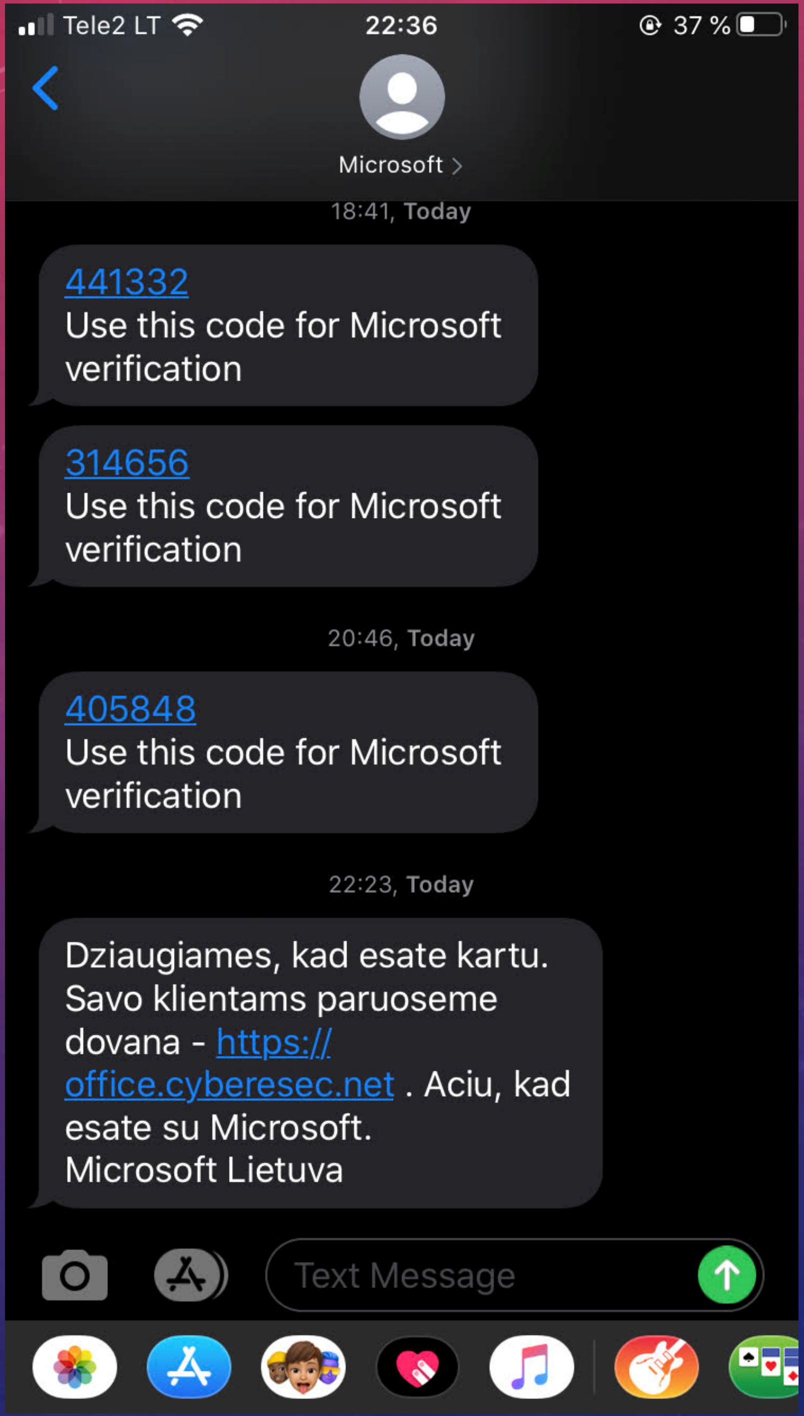
You **can send SMS** to **Lithuania**

✓

Send test SMS for free here

SMS Text Examples

SMS From: **Sniper**
Text: **Please take one step to the left. I dont see you!**
(Category: Best SMS messages)



18:41, Today

441332
Use this code for Microsoft verification

314656
Use this code for Microsoft verification

20:46, Today

405848
Use this code for Microsoft verification

22:23, Today

Dziaugiames, kad esate kartu. Savo klientams paruoseme dovana - https://office.cyberesec.net . Aciu, kad esate su Microsoft.
Microsoft Lietuva

DEMO / MOVIE

- https://tyrimai.esec.lt/movies/ivairus/o365/all1.mp4

MICROSOFT O365

- It was nothing new from technical point of view:) The time to setup the interception just took several hours. But did you know those dangers ?
- It is very easy to enumerate the organizations which are using O365
- After that – just some spoofed SMS or emails – and you might be exposed
- Do you carefully estimate the risks that might arise when you introduce new services ?
- Do you understand those risks and are you able to mitigate them ?

CHECK YOUR ORGANIZATION SETUP

During the break you can ask to try that on your organization. Sometimes it is very challenging to see that someone else is inside in your organization :)

ORGANIZATIONS USING O365

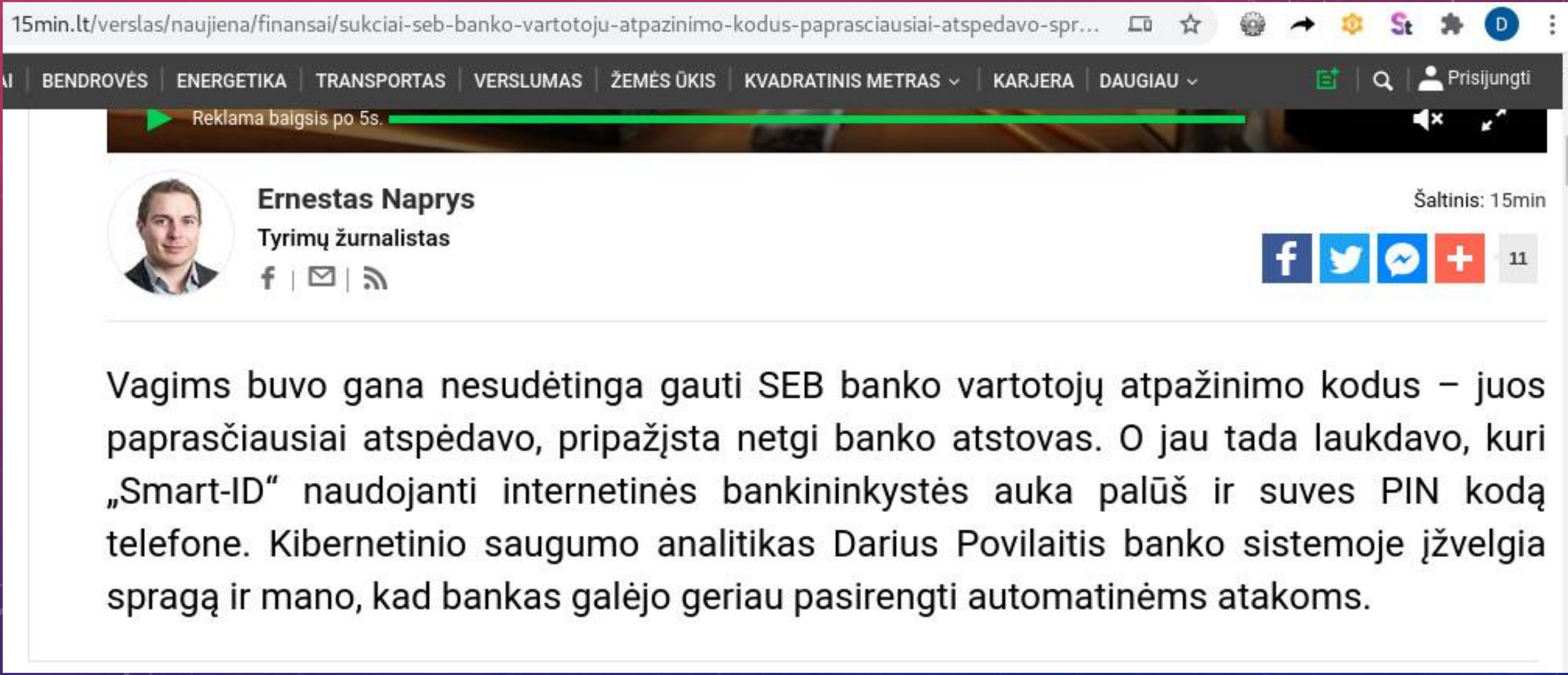
Just to name a few:

- zum.lt. 599 IN MX 100 zum-lt.mail.**protection**.outlook.com.
  rrt.lt. 7199 IN MX 0 rrt-lt.mail.**protection**.outlook.com.
  vatzum.lt. 3599 IN MX 0 vatzum-lt.mail.**protection**.outlook.com.
  klaipedos-r.lt. 3599 IN MX 0 klaipedosr-lt02c.mail.**protection**.outlook.com.
  sam.lt. 599 IN MX 0 sam-lt.mail.**protection**.outlook.com.

There are and some more interesting entries :)

SMART-ID / MSIGNATURE

- Attack hit banks. To be more precise – the banks users. Remember – target is money.
- Due to the incorrect authentication implementation also all Egovernment services (more than 600) were impacted
- It took more than half a year for Egovernment services to become not impacted (still not sure – not verified recently)
- Some organizations were very fast fixing that problem – took it seriously (State Enterprise Centre of Registers)
- Some organizations are still impacted



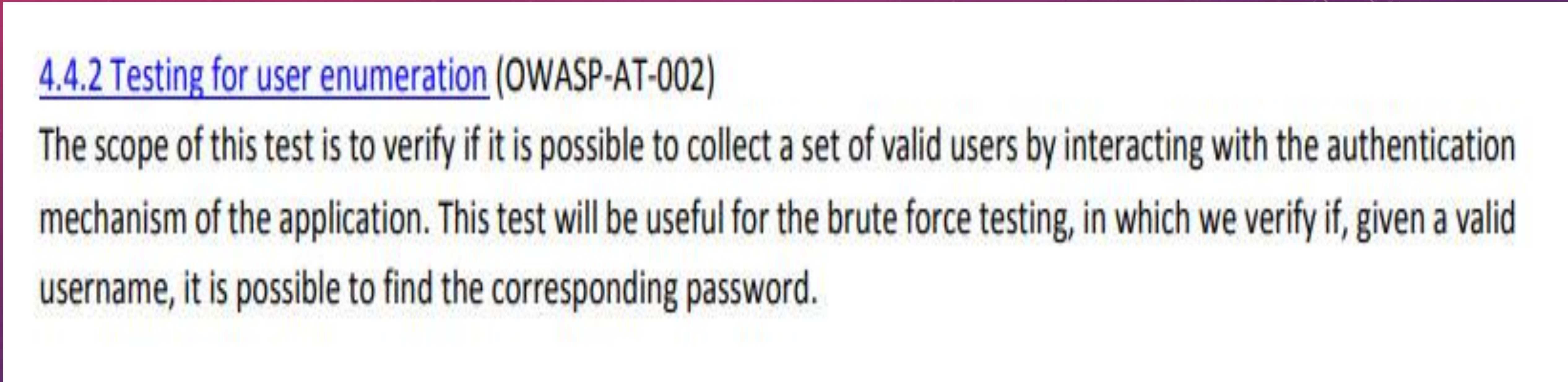
Ernestas Naprys

Tyrimų žurnalistas

Šaltinis: 15min

Vagims buvo gana nesudėtinga gauti SEB banko vartotojų atpažinimo kodus – juos paprasčiausiai atspėdavo, pripažįsta netgi banko atstovas. O jau tada laukdavo, kuri „Smart-ID“ naudojanti internetinės bankininkystės auka palūš ir suves PIN kodą telefone. Kibernetinio saugumo analitikas Darius Povilaitis banko sistemoje įžvelgia spragą ir mano, kad bankas galėjo geriau pasirengti automatinėms atakoms.

OWASP TESTING GUIDE



4.4.2 Testing for user enumeration (OWASP-AT-002)

The scope of this test is to verify if it is possible to collect a set of valid users by interacting with the authentication mechanism of the application. This test will be useful for the brute force testing, in which we verify if, given a valid username, it is possible to find the corresponding password.

DEMO / MOVIE

- https://tyrimai.esec.lt/index.php?option=com_content&view=article&id=48
- https://tyrimai.esec.lt/movies/ivairus/ivpk/ivpk1.mp4

LINKS

- https://www.15min.lt/verslas/naujiena/finansai/sukciai-seb-banko-vartotoju-atpazinimo-kodus-paprasciausiai-atspedavo-spraga-bandoma-uzlopyti-662-1256248
- https://tyrimai.esec.lt/index.php?option=com_content&view=article&id=48

THANK YOU!

DARIUS@ESEC.LT