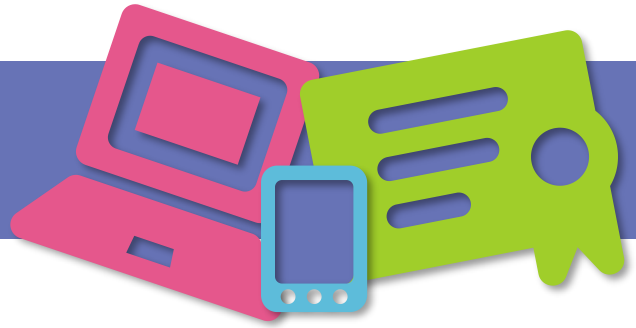
SECURITY 2015

23. ročník konference o bezpečnosti v ICT



Elektronické důkazy v on-line finanční kriminalitě a podvodech spáchaných s elektronickými platebními prostředky: Zkušenosti a praxe v České republice

JUDr. Josef Donát, LLM

Rowan Legal

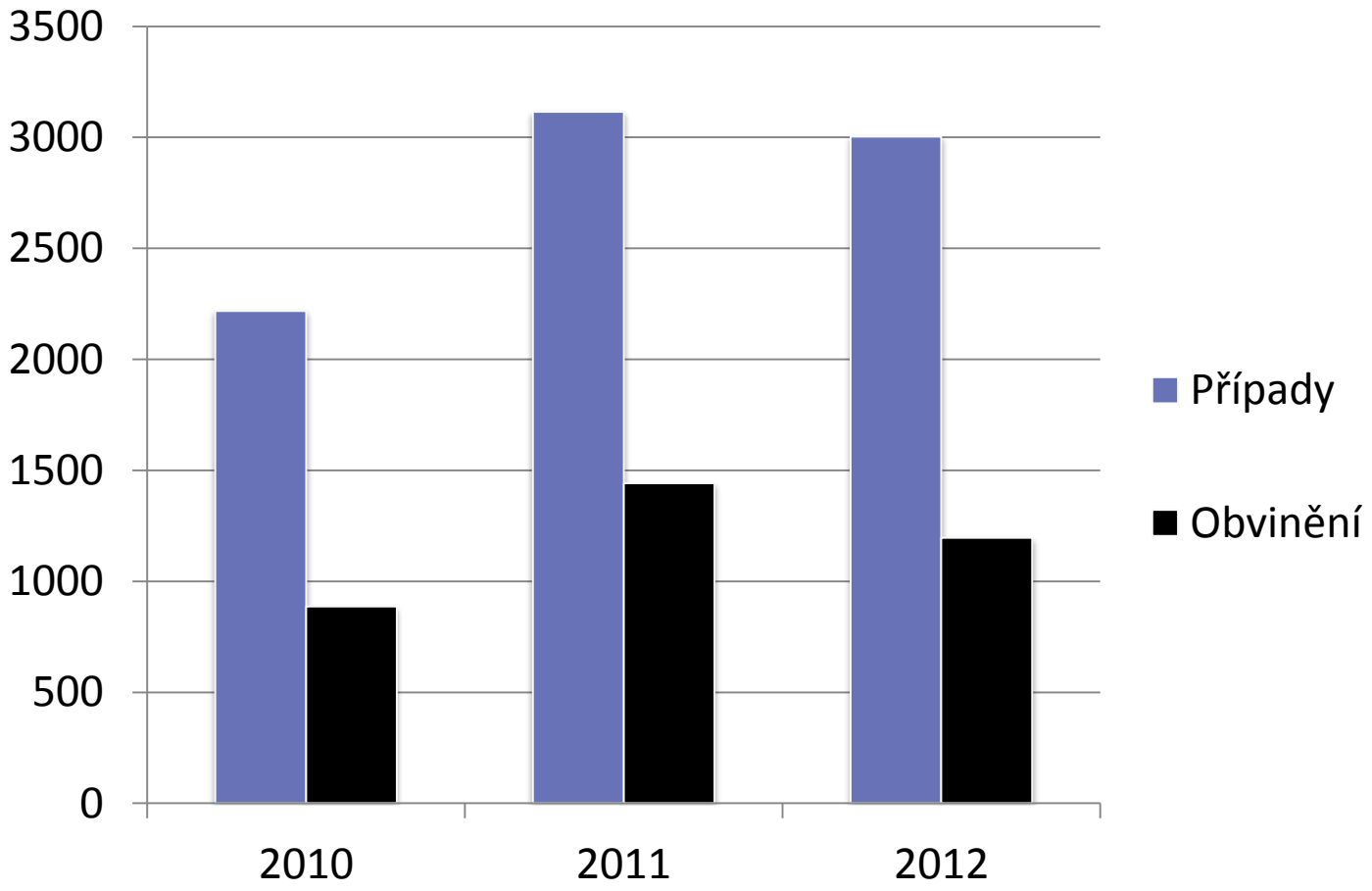
Právní úprava

- **Úmluva** Rady Evropy **o počítačové kriminalitě**
- Zákon 40/1990 Sb., **trestní zákoník** (TrZ)
- Zákon 141/1961 Sb., **trestní řád** (TrŘ)

Relevantní trestné činy

- Neoprávněné opatření, padělání a pozměnění platebního prostředku (§ 234 TrZ)
  - Platební karty (i jejich čísla)
  - Platební příkazy v internetovém bankovnictví
  - **Skutečné zneužití není nutné**
  - Až 12 let vězení
  - Příprava je také trestná
- V platnosti: krádež (§ 205 TrZ) a podvod (§ 209 TrZ)

Statistika § 234 TrZ



Dostupné důkazní nástroje

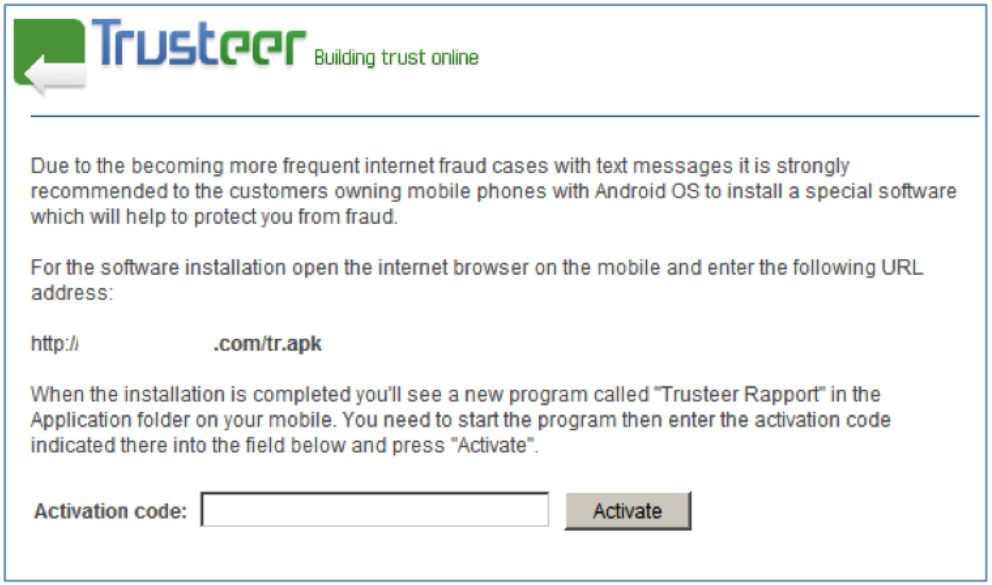
- Sledování osob a věcí (§ 158d TrŘ)
- Odposlech a záznam telekomunikačního provozu (§ 88 TrŘ)
- Telekomunkační provoz („uchovávání provozních a lokalizačních údajů”) (§ 88a TrŘ)
- Věcné a listinné důkazy (§ 112 odst. 2 TrŘ)
- Ohledání (§ 113 TrŘ)
- Znalecký posudek (§ 105 odst. 2 TrŘ)

Náležitosti důkazů

- Důkazní přípustnost
  - Postup
  - Zdroj
- Autentičnost

Případ Trusteer Rapport

- Reálné útoky na zákazníky jedné z českých bank
- **Sofistikovaná kombinace různých technik**
- Cíl: převést peníze pomocí internetového bankovnictví



Illustrative, source: kindsight.net

Fáze 1: Phishing e-mail

- Padělaný e-mail z České pošty
- Odkaz na stažení viru

Česká pošta

NETservis s.r.o.,

Kurýr nevydal zásilku s podacím číslem **DR6878456545C**, na Vaši adresu 05.8.2013, protože nikdo nebyl na adrese v tomto okamžiku. Prosím, podívejte se na informace o zásilku , vytisknout a jít na poštu dostávat balíček.

http://www.ceskaposta.cz/cz/nastroje/sledovani-zasilky.php

Pozor

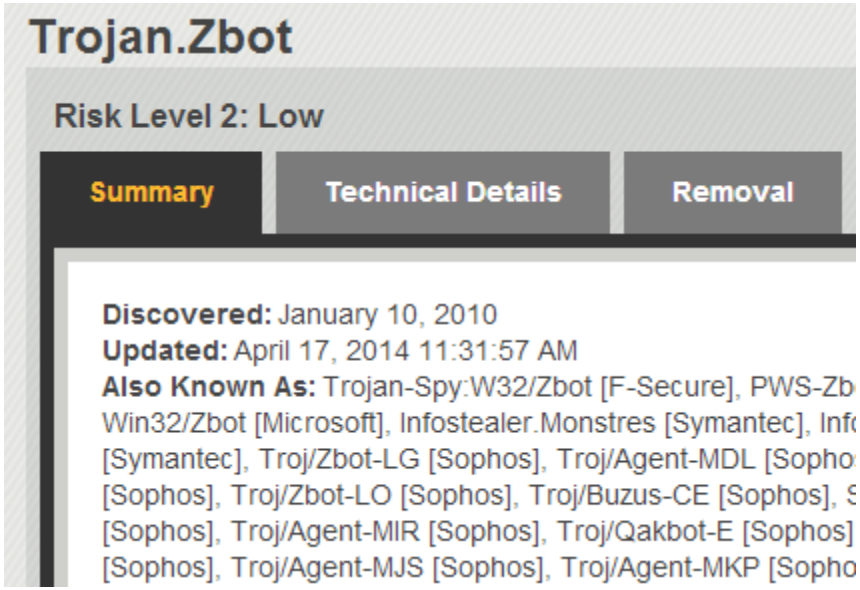
Pokud je zásilku nedostali do 30 pracovních dnů Česká pošta bude mít právo nárokovat odškodnění od tebe jde o to udržet ve výši 45 Kč za každý den udržet. Zde najdete informace o postupu a podmínkách parcely vedení v nejbližší pobočce. Děkujeme, že využíváte naše doručovací služby. S přáním příjemného dne Vaše Česká pošta

2013 Česká pošta **Telefonicky : 840 111 244**

Source: viry.cz

Fáze 2: Počítač

- ZEUS (Zbot) virus
- **Záznam přihlašovacích údajů** do internetového bankovnictví
- Falešná stránka s bezpečnostním upozorněním
- Instalace „bezpečnostní“ mobilní aplikace

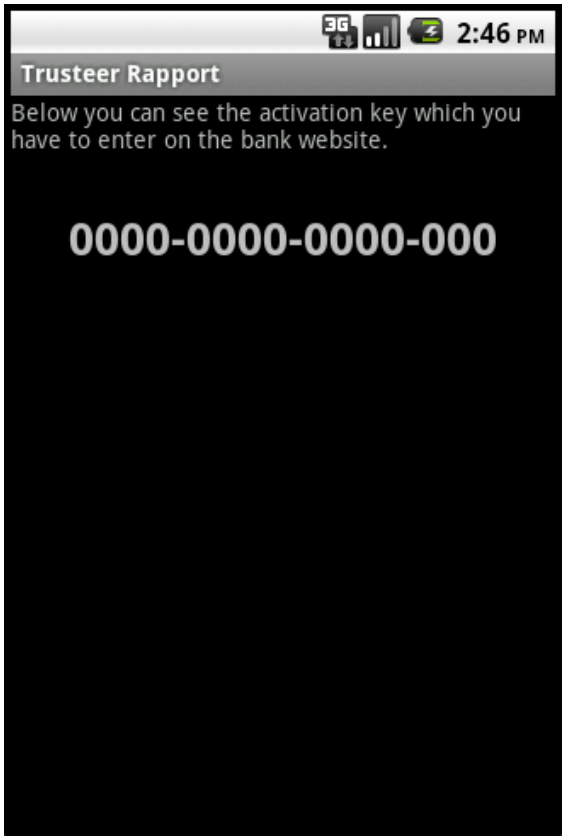


Source: symantec.com

Fáze 3: Mobilní telefon

- ZITMO (Zeus In The Mobile)
- Skrývá a přeposílá textové zprávy s autorizačními kódy

- Výsledek: veškeré finance až do výše nastavených limitů převedeny z účtů napadených



Illustrative, source: blog.fortinet.com

Důkazy

- **Kam vedly odkazy?**
  - IP adresy + Telekomunikační provoz (§ 88a TrŘ)
- **Kdo se do internetového bankovnictví přihlásil a kam peníze odešly?**
  - Záznamy internetového bankovnictví
  - Porušení bankovního tajemství (§ 8 TrŘ) – souhlas klienta nebo státního zástupce

Důkazy II.

- **Kam virus data odesílá?**
  - Digitální forenzní analýza (§ 112 TrŘ)
  - IP adresy + Telekomunikační provoz (§ 88a TrŘ)

- **Kam odcházely textové zprávy?**
  - Provoz a lokalizace dat mobilních telefonů (§ 88a TrŘ)

Kdo je poškozený?

- Článek 61 (2) Směrnice 2007/64 / ES

- Primárně odpovědnost banky
- Klient – hrubá nedbalost
- Soulad s "podmínkami, které upravují vydávání a používání platebního nástroje“

- Antivirové a anti-phishingové povinnosti?

Závěrečný komentář

- Design útoku
- Policejní spolupráce
- Role finančních převodců
- Případ k uchovávání údajů?

SECURITY 2015

23. ročník konference o bezpečnosti v ICT

Děkuji za pozornost.

JUDr. Josef Donát, LLM
ROWAN LEGAL
donat@rowanlegal.com
+420 224 216 212
cz.linkedin.com/in/josefdonat

SECURITY 2015

23. ročník konference o bezpečnosti v ICT

Panelová diskuse

Internetové fraudy trojím pohledem