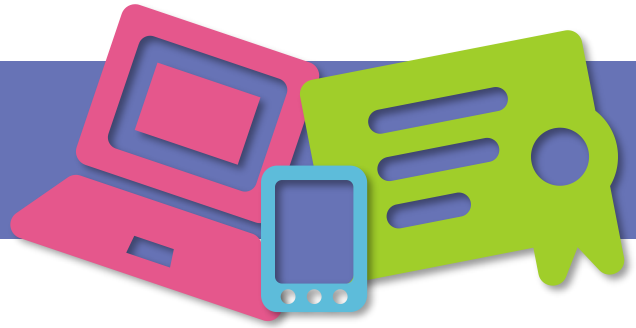
SECURITY 2015

23. ročník konference o bezpečnosti v ICT



Fraudulentní malware jako zdroj kybernetického rizika

Ing. Jan Guzanič, CISA

ČSOB/era

Aktuální hrozby a trendy

- Lokální trendy vývoje hrozeb internetového fraudu v elektronických platebních kanálech v roce 2015
  - Sociální inženýrství
  - Phishing
  - Moderní finanční/fraudulentní malware
    - Zde je klient zranitelný nejvíce
    - Co se děje, proč se děje

Digitální propast a past

- Akcelerace digitální migrace
  - Digital nomads, imigrants, aborginess, emigrants
  - *Lidé jsou v novém prostředí náchylnější k tomu stát se obětí neznámého*
  - Zvyšování komplexnosti technologií
  - Životního cyklu požadavků klientů a způsobů zajištění
  - Zvětšuje se ohrožená plocha/prostor
  - Související nárůst hrozeb
- Útočník využívá „Digital Gap“
- Risk society --> Cyber risk society

Bezpečnostní kampaně

Internetoví zloději se právě teď snaží získat přístup k vašim penězům

video, direct mailing, novinky na webu, zprávy v internetovém bankovnictví, sociální sítě, specializované stránky (bezpecnost.csob.cz) a v neposlední řadě také média

video **Kolik vás mohou stát přátelé na sociálních sítích?** zaznamenalo velice pozitivní reakce

Finanční malware – informování

Model penetrace útoku

Model obsahuje hrubý odborný odhad hypotetické kampaně a hypotetické banky	Klientů	Ohroženo klientů s AA metodou (metoda)	Poměr oslovených útočníkem	Klient otevírá malware	Antivir nezachytí	účet perspektivní	Zobrazení webinjectu	Klient vyplní údaje	Malware ve smartphonu	úspěšnost cash-out
Rozsah hodnot	(1-1000000)	(0,1 - 1)	(0,01 - 1)	(0,01 - 1)	(0,01 - 1)	(0,1-1)	(0,01 - 1)	(0,01 - 1)	(0,01 - 1)	(0,01 - 1)
Data modelu	**1000000**	**50%**	**50%**	**5%**	**20%**	**10%**	**50%**	**10%**	**50%**	**50%**
Klientů po fázi	**1000000**	**500000**	**250000**	**12500**	**2500**	**250**	**125**	**12,5**	**6,25**	**3,125**

$$N = R^* \cdot f_p \cdot n_e \cdot f_l \cdot f_i \cdot f_c \cdot L$$

Vztah mezi nastavením parametrů útoku a schopnostní cashout

Drakeova Rovnice života ve vesmíru *- teoreticky umožňuje určit počet komunikaceschopnýchteoreticky umožňuje určit počet komunikaceschopných mimozemských civilizací existujících ve stejném okamžiku civilizací existujících ve stejném okamžiku*

Fraud as a service

- „Cybercrime as as service“ --> „Fraud as a service“

- Komplexní dynamický (eko)systém
  - Ekonomické zákonitosti
  - Zisk , monetizace
  - Poměr Zisk vs. Náklady a riziko
  - Technologické platformy formou služby, doprovodné služby
  - Fraud scheme developers , operators and promoters

- Fraudsteři nyní nemusí vymýšlet svůj fraud ale jednoduše si obstará/objedná nejnovější úspěšné schéma způsob provedení
    - Viz kauza z počátku února– CC >> Phishing >> Malware

Pohled mikroskopem

- Multivektorová monetizace
  - **Finanční (MitB,**MitM,Overlay attacks**)**
  - **Ransomware**
  - Virtuální měny
  - Krádeže identit a osobních údajů
  - Click fraud, Computing power, Botnet…
- Akcelerace evoluce MW hrozeb
  - Vývoj virů, odolnost vůči aktuálním antivirům je samozřejmostí
  - Různé vektory infekce
  - Mezidruhové šlechtění finančního malware (uvolněné zdrojové kódy vícero významných malwarů → rozšíření dostupnosti, laicizace nástrojů/služeb
  - Mezidruhová kultivace fraudulentních metod, nástrojů a služeb
  - Self defense mechanismy
- Viralizace úspěšného vektoru útoku (fraud as a service)

Vybrané výzvy a principy

- Budování aktivní kybernetické ochrany
  - Systematický přístup
  - Agilita
  - Interdisciplinarita
  - Interoperabilita
    - Ochranné řetězce s přidanou hodnotou
    - Metody operativního informačního flow
    - Budování platforem
    - Externí výměna informací a early warnings

SECURITY 2015

23. ročník konference o bezpečnosti v ICT

Děkujeme za pozornost.

Ing. Jan Guzanič, CISA
ČSOB/era
guzanic@gmail.com

SECURITY 2015

23. ročník konference o bezpečnosti v ICT

Panelová diskuse

Internetové fraudy pohledem bank