Nedávné útoky hackerů a ochrana Internetu v České republice

Andrea Kropáčová / andrea@csirt.cz

14. 5. 2013

CZ.NIC | SPRÁVCE DOMÉNY CZ

CZ.NIC

- CZ.NIC, z. s. p. o.
- Založeno 1998 významnými ISP
- Aktuálně 107 členů (otevřené členství)
- Neziskový, neutrální
- 50+ zaměstnanců
- Hlavní role – provoz domény .cz
- MoU s Vládou ČR, NBÚ
- Další aktivity
  - výzkum a vývoj v oblasti bezpečnosti
  - provoz CSIRT.CZ (Národní CSIRT ČR)
  - Akademie – školicí středisko

(D)DOS útoky

- Období 4. 3. – 7. 3.
  - každý den dvě vlny: 9 – 11, 14 – 16
- Cíle: www služby
  - uživatelsky zajímavé, dobře viditelné ==> mediálně atraktivní
- Skvělá posloupnost cílů
  - pondělí 4. 3. – zpravodajské www (ihned, idnes, zive, novinky...)
  - úterý 5. 3. – Seznam.cz
  - středa 6. 3. – banky (ČS, ČSOB, Raiff, KB, ČNB ...)
  - čtvrtek 7. 3. – mobilní operátoři (O2, T-Mobile)

(D)DOS útoky – technické aspekty

- Zdroj: RETN
- (D)DOS
- Metody: SYN-Flood, IP-Spoofing, metoda „odražení“ (bounce)
- Dobře zvolená síla a metody:
  - pro ISP
    - objemově slabé (do 1Gbps)
    - paketově detekovatelné (packet rate ~ 1 – 1.5 ps)
  - pro koncovou síť (službu) dostatečně „silné“
    - koncentrace provozu do jednoho místa
    - zatížení zdrojů o vrstvu výš – TCP (FW, LB ...)

(D)DOS útoky – řešení, obrana

- ISP i správci v koncových sítích (a služeb)
  - věděli, co dělat
  - komunikovali a spolupracovali
  - dle možností sdíleli relevantní informace
  - VC meeting ve 6. 3. odpoledne – eliminace útoků na ČS
- Použitá řešení
  - filtrace, blokace, pračky ...
  - stopnutí služby (ať útok odezní, ochrana služby)
  - přestěhování služby do jiného adresového prostoru
  - omezení provozu pouze pro sítě ČR

(D)DOS útoky – dopady

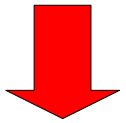
- Především mediální
  - Vhodně zvolené cíle
  - Vhodně zvolená posloupnost cílů (po = zpravodajské weby)
- Dobře vyvážený útok = způsoboval problémy poskytovatelům obsahu, ale ne problémy na transportní úrovni (ISP)
- Škody
  - Lidské zdroje, práce, konzultační služby
  - Nedostupnost služeb = únik zisku z reklamy, bankovní transakce
  - Renomé? ...
- Zachována důvěra v systém
  - Soukromí uživatelů **nenarušeno**
  - Peníze **neodcizeny**
  - Citlivá data **nezneužita**

(D)DOS útoky – lesson learned

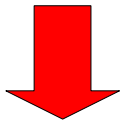
- Skvělé cvičení :-)
- Požadavky na CSIRTy, správce, ISP
  - informace, informace, informace ... (média, provozovatelé služeb)
  - „být připraven“ - doporučená obrana
- Správci věděli, co dělat, komunikace fungovala
- Nedostatky v zabezpečení některých technologií (honeypoty)
- Legislativa jako brzda spolupráce?
- Facebook má i své klady
- Média
  - nepodceňovat, komunikovat
  - různý přístup uživatelů k problému (pozorováno v diskusích)

Uživatel

- Špatná péče o PC, notebook, mobil, tablet
- Slabá znalost principů fungování Internetu a služeb
- Ignorování pravidel ochrany soukromí a citlivých údajů (hesla apod.)



- Zcizení a zneužití identity
- Zcizení a zneužití citlivých dat
- Brána pro vnik malware, virů, trojských koní



vstup do **botnetu**

Uživatel

- Uživatele je nutné vzdělávat, informovat, připravovat na problém
  - musí o nebezpečí vědět
  - musí vědět jak se mu vyhnout
  - musí vědět co dělat a kam se obrátit, když se něco stane
    - rodič, učitel, soc. pracovník
    - administrátor, správce sítě a služeb
    - PČR, NCBI, CSIRT
- **Musí mít pocit osobní zodpovědnosti!**
- Péčí o výpočetní prostředek se na bezpečnosti podílí
- Svým chování v prostředí Internetu se na bezpečností podílí

→ chrání tím sebe a své blízké!

Děkuji za pozornost

Děkuji za pozornost

CSIRT.CZ
Andrea Kropáčová / andrea@csirt.cz

CERT/CSIRT v ČR

- CESNET-CERTS (2004)
  - Operuje nad sítí CESNET2 (AS2852)
- CZ.NIC-CSIRT (2008)
  - Operuje nad sítí CZ.NIC a TLD doménou .cz
- CSIRT-MU (2008)
  - Operuje nad sítí Masarykovy university v Brně
- ACTIVE24-CSIRT (2012)
  - Operuje nad sítí Active24 (AS25234)
- CSIRT.CZ, Národní CSIRT České republiky (2008)
  - Operuje nad všemi sítěmi provozovanými v ČR
- *Ve výstavbě Vládní CERT ČR – provozuje NBÚ*

Útoky – resumé (každý má důležitou roli)

- Správce služby
- Správce koncové sítě
- ISP (transportní vrstva)

} *obrana*
komunikace
spolupráce
výměna informací

- Management
  - vynakládáme dost na obranu?
  - jaká je „cena“ služby?
  - nechceme po správcích nemožné?
- CERT/CSIRT týmy („bezpečáci“)
  - domýšlení slabých míst (správce – ISP – management)
  - monitorování stavu, sběr a distribuce informací, komunikace s médii
  - poskytnutí komunikačních prostředků