DDoS na Seznam.cz

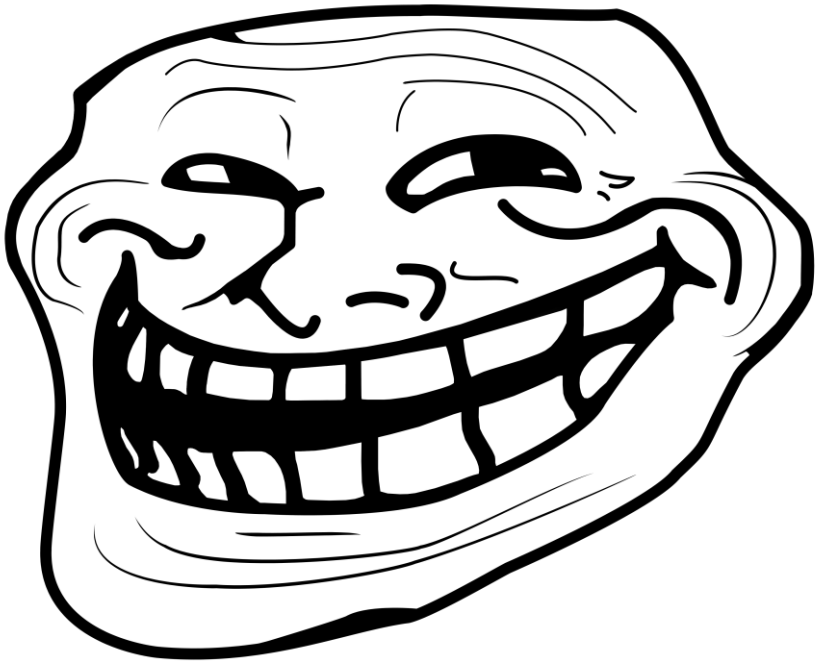
Průběh a poučení

Štefan Šafár, Bezpečnostní administrátor, stefan.safar@firma.seznam.cz

SEZNAM.CZ

Co je to DDoS?

Co je to DDoS?



DDoS na Seznam.cz. První stránka českého internetu je nedostupná

5.3.2013 | LUKÁŠ VÁCLAVÍK | (1)

DDoS útoky pokračují, jejich cílem se stal Seznam.cz [AKTUALIZOVÁNO]

Útoky na tuzemské weby nekončí. Zatímco včera byly terčem zpravodajské servery, dnes čelí podobným problémům Seznam.cz.

5. 3. 2013 11:19 Martin Vyleťal

Po zpravodajských serverech ochromili weboví útočníci i Seznam.cz

5. března 2013 10:43, aktualizováno 12:13

Český internet zaznamenal druhý den po sobě masivní DDoS útoky. Zatímco v pondělí byly ochromeny zpravodajské servery, v úterý se stal terčem největší český vyhledávač Seznam.cz.

5. 3. 2013 Seznam | Web | Internet | Kauzy

Včerejší útoky pokračují. Seznam.cz čelí DoS

Co už asi víte

- TCP SYN Flood
- Spoofnuté IP adresy
- Zdroj útoku - ruská síť ReTN
- V pondělí novinky.cz, v úterý seznam.cz
- Útok nešel z ČR, spoofnuté IP na české
- Spolupracujeme s CSIRT.cz
- Zvažujeme i právní kroky
- Motiv ani identitu útočníka neznáme

Co si myslí v zahraničí

Útok hackerov: Nefunguje server Seznam.cz

5.3.2013 11:10 : Aktuálně.cz

Hacker attackieren tschechische Medien

Neuer Skandal: Hacker haben die Internetseiten der drei meistgelesenen Zeitungen Tschechiens mit Anfragen bombardiert und lahmgelegt. Bei ihnen handelt es sich um www.ihned.cz, www.idnes.cz und www.novinky.cz. Im Januar waren bereits die "New York Times" sowie das "Wall Street Journal" Opfer von Hackern geworden. Die

Media hacking continues as Czech news sites suffer DDoS attacks

by **Will Dalton**, *04 March, 2013*

… a někdy i česká média

Hackerské útoky pokračují: dnes byl terčem Seznam.cz

AKTUALIZOVÁNO Po včerejší vlně útoků na české weby se mohlo zdát, že máme vše za sebou, dnes dopoledne má však pro změnu problémy

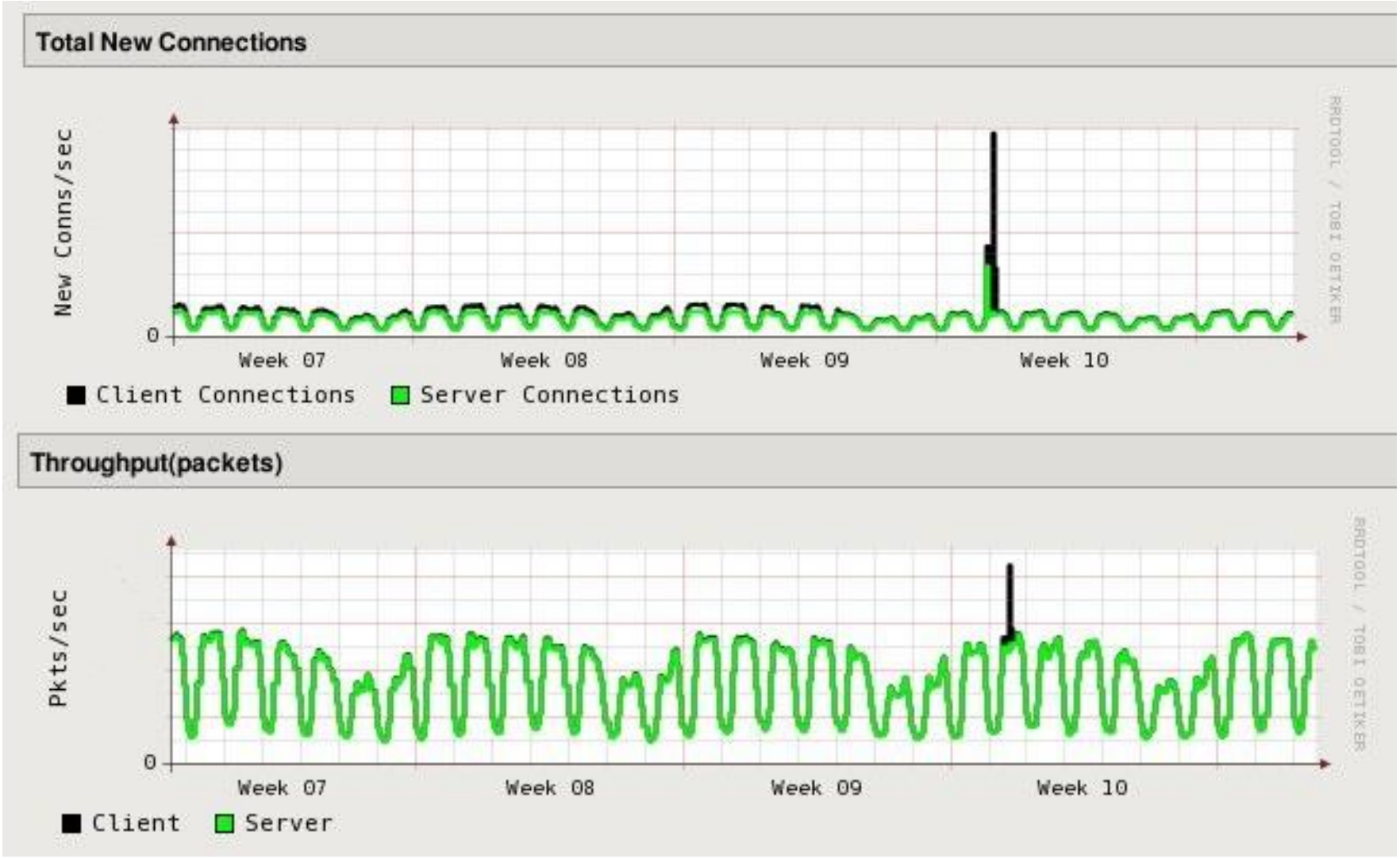
Druhý útok hackerů: Seznam.cz měl znovu problémy

16:06 | 5.3.2013 | Aktualizováno

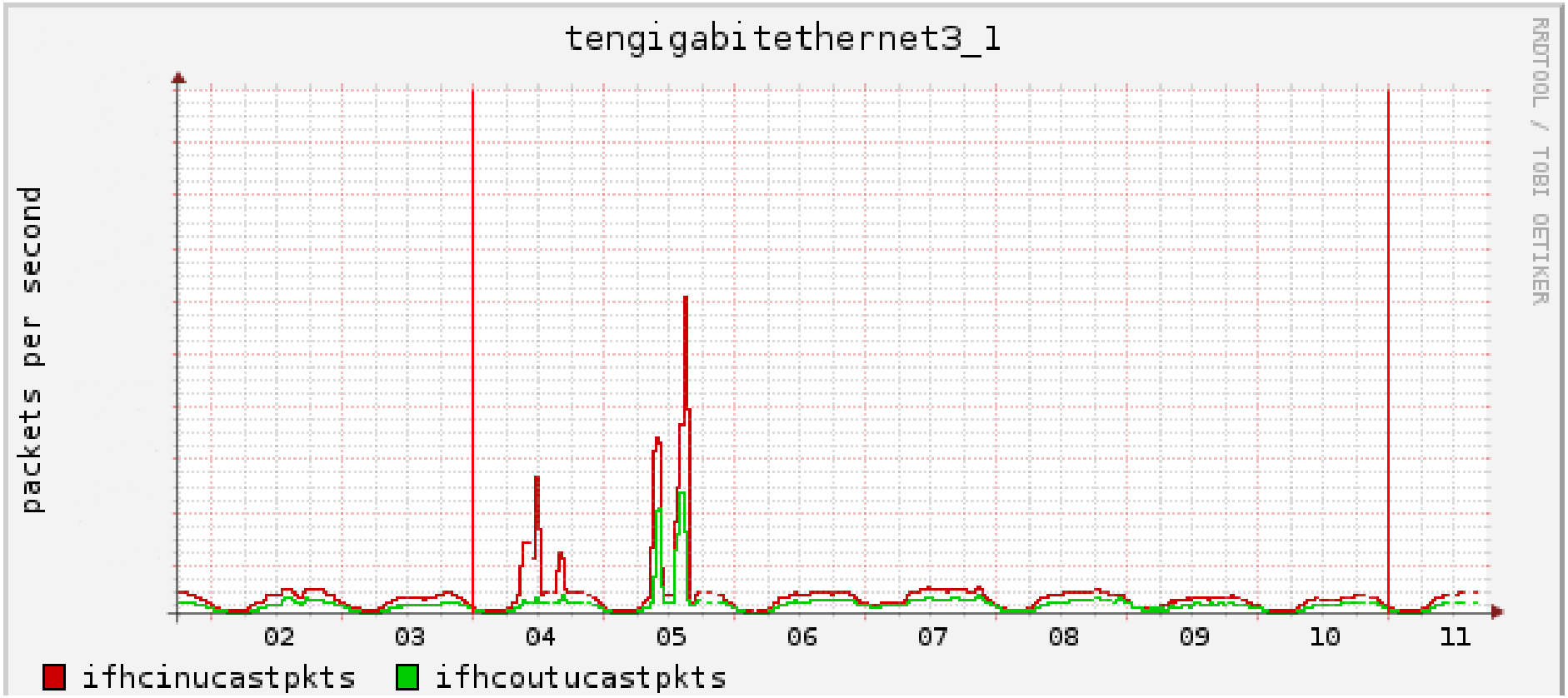
Co už možná nevíte

- Síť ReTN je v NIX.cz
- Seznam s ní nepeeruje
- Máme 2 lokality
- Útoky přímo na služby přes DNS záznamy
- Útoky během pracovní doby, několik hodin
- Ve středu/čtvrtek pak na celé IP rozsahy
- Přidal se i ICMP flood
- Sekundárně zasažené některé české sítě

Grafy


Total New Connections
New Conns/sec
0
Week 07
Week 08
Week 09
Week 10
Client Connections
Server Connections
Throughput(packets)
Pkts/sec
0
Week 07
Week 08
Week 09
Week 10
Client
Server

Grafy 2


tengigabitethernet3_1
packets per second
RRDTOOL / TOBI OETIKER
02
03
04
05
06
07
08
09
10
11
ifhcinucastpkts
ifhcoutucastpkts

Obrana proti SYN flood

- Syn Cookies na různých místech (hw/sw impl)
  - Aplikační servery
  - Routery
  - Dedikované TCP Proxy (Scrubber)
  - Firewally
  - Load balancery
- Specializovane Anti-DDoS boxy
- Služba u ISP
- Blokování trafficu od BGP peerů

Poučení

- Být připraven (+krizový management)
- Interní komunikace je důležitá
- Externí taky
- Mít robustně navrženou síť se vyplatí
- Redundance na všech místech
- Počítat i s možností 10x větší zátěže
- Využívat své zařízení na 100%
- Informace jsou všude(logy, monitoring, nix.cz)

...najdu tam, co neznám!

Děkuji za pozornost

Štefan Šafár, Bezpečnostní administrátor, stefan.safar@firma.seznam.cz