# Egy lépéssel a lavina előtt!

## Hatékony védekezés DDoS támadásokkal szemben

Orbán Attila – vezető architect

Szabó István - szenior rendszermérnök

T · · Systems ·

# Online sajtó morzsák

## SatoshiDice hit by DDoS attack, but bets continue

September 6, 2013 - admin - 0 Comment

Bitcoin gambling site SatoshiDice has recovered after being felled for several days by a DDoS attack. The site went down several days ago, and was inaccessible from the Internet. Erik Voorhees, who created the site and sold it for $11.5 million in July, no longer runs the site, but naturally still has insights into how it operates. DDoS attacks happen…

## Cybercrooks use DDoS attacks to mask theft of banks' millions

August 22, 2013 - admin - 0 Comment

Distributed denial of service attacks have been used to divert security personnel attention while millions of dollars were stolen from banks, according to a security researcher. At least three US banks in recent months have been plundered by fraudulent wire transfers while hackers deployed "low powered" DDoS attacks to mask

## DDoS Attacks Strike Three Banks

August 20, 2013 - admin - 0 Comment

Izz ad-Din al-Qassam Cyber Fighters' so-called Phase 4 of distributed-denial-of-service attacks against major U.S. banks hasn't stalled, it's just been ineffective at disrupting online availability, security experts say The latest attacks have been sporadic and seemingly less targeted. U.S. banking institutions, which have been under attack since September 2012, have adapted their

## UCAS under DDoS attack

August 16, 2013 - admin - 0 Comment

Ucas has been the victim of a hacking attempt, when its website was the target of a denial of service attack. The site was unavailable late on 14 August, the day before thousands of A-level students were due to receive their results across the country. A spokesperson for Ucas said: "The UCAS website suffered a sustained, criminal 'denial of service'…

SECURITY

## Chinese authorities say massive DDoS attack took down .cn domain

### Middle Kingdom pledges immediate action

By Iain Thomson, 26th August 2013 Follow 1,619 followers

## Megtámadták a TEK, az OTP és a Híradó oldalát


Az Anonymous este negyed 10 körül te
online bástyáját. Bejelentésük szerint a
weboldala, majd az OTP Banké.

2012. november 05., hétfő, 21:36

## Túlterheléses támadást indítottak weboldalak ellen

2012-09-08 12:40:35

**Egy 16 éves fiú vezette hacker-csoport törte fel nemrég az Alkotmánybíróság honlapját, ahol átírták az Alaptörvényt. További négy társa, köztük egy 26 éves kaposvári férfi is segédkezett a bűncselekményben.**

A gyanú szerint egy 16 éves dunaújvárosi fiú és négy, általa személyesen nem ismert társa volt a magát Anonymousnak nevező számítógépes hackercsoport magyarországi tagja - mondta az Országos Rendőr-főkapitányság szóvivője szombaton az MTI-nek.

vg.hu/vallalatok/kozlekedes

2013. szeptember 10. kedd Belép

CÍMLAP VÁLLALATOK KKV GAZDASÁG PÉNZÜGY KÖZÉLET TŐZSDE

Előfizetés Egészségügy Energia Infokommunikáció Ingatlan Ipar Kereskedelem Köz

Itt vagyok jelenleg » Címoldal » Vállalatok » Közlekedés » Túlterheléses támadás érte az e-útdíjrendszert

VÁLLALATOK / KÖZLEKEDÉS

## Túlterheléses támadás érte az e-útdíjrendszert

2013. 7. 1. 09:12 | Vállalatok » Közlekedés

## léses támadás érte az Indexet

2013. október 23., szerda 18:22 |

Címkék ddos, index, szerver

Október 23-án délután négy óra körül, éppen, amikor az eredeti tervek szerint Orbán Viktor beszéde kezdődött volna a Békemenet tagjai előtt a Hősök terén, váratlan probléma lépett fel az Indexet kiszolgáló szerverek körül. Amint olvasóink is jelezték, az oldal először csak lelassult, aztán akadozni kezdett, végül teljesen elérhetetlenné vált.

Rendszergazdáink nyomozása szerint túlterheléses támadás érte az Indexet. Ez azt jelenti, hogy a támadók direkt erre készített támadó szoftverek segítségével hatalmas mennyiségű, másodpercenként több millió adatlekéréssel bombázták az Index.hu-t kiszolgáló gépeket, amelyek a brutális terhelés alatt összeomlottak. A támadás kifinomult módszerrel, hamisított ip-címek használatával történt, így a védekezés sem volt túl egyszerű (alapállapotban egy ilyen támadást ki lehet védeni azzal, ha a támadó gépek címeit tiltólistára teszi a rendszergazda, most azonban véletlenszerű címekről érkeztek az adatcsomagok).

T · · Systems ·

# Motivációk

## Támadó

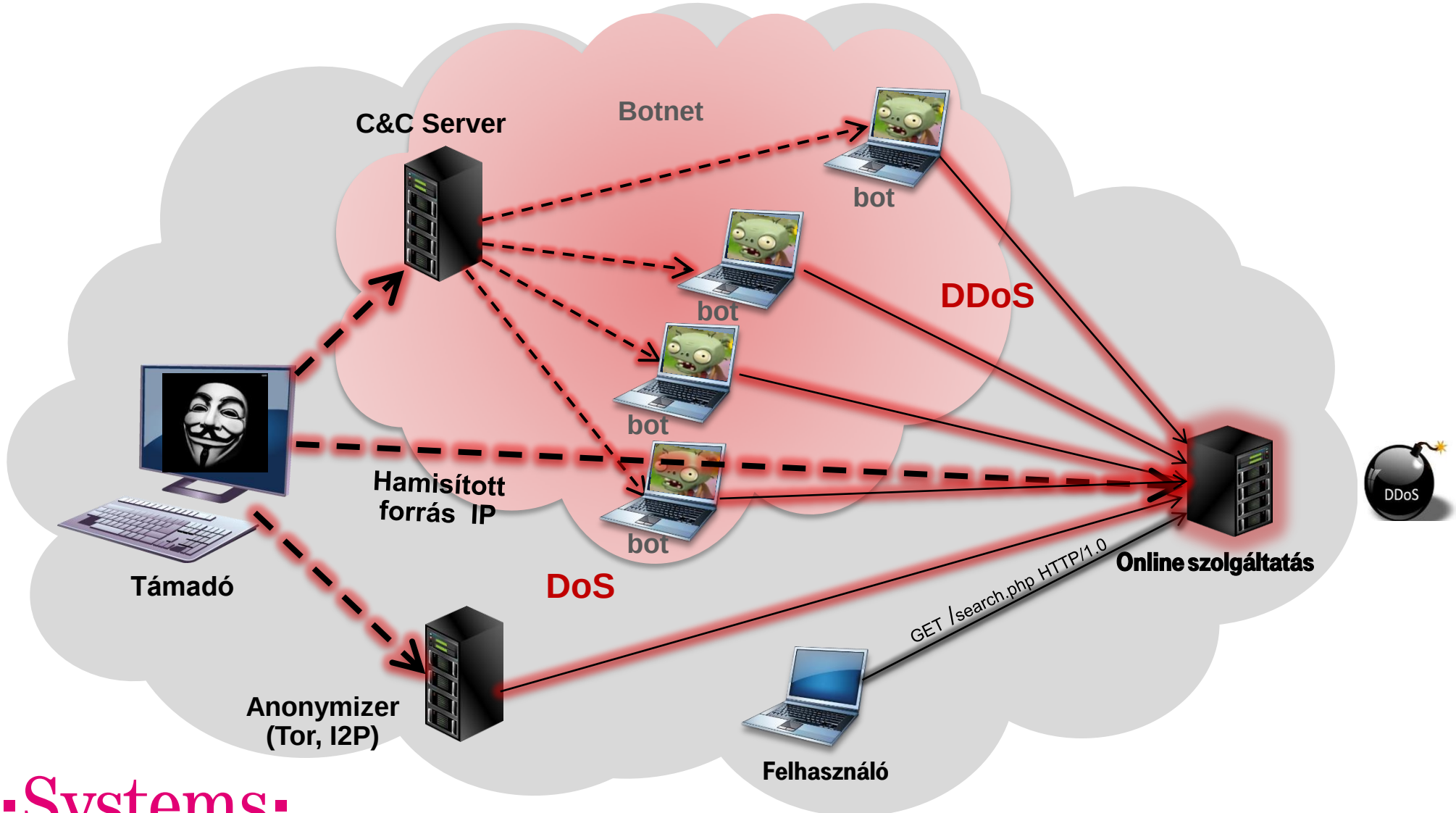
- Hacktivisták (hacker+aktivista)
- Nemzeti érdekek (kiber hadviselés)
- Anyagi haszonszerzés

## Áldozat

- Szolgáltatás elérhetőségét biztosítani, akár kompromisszumok árán is ...


T · · Systems ·

# Támadások (DoS, DDoS)




T · · Systems ·

# Támadási technikák

## Volumetrikus

- L3-L4 „flood”
  - ICMP/UDP
  - TCP SYN
- reflexiós támadások
  - TCP SYN+ACK
  - DNS reply
- L7 „high-rate”

## Állapottáblát célzó

- L4-L7 „low and slow”
  - csepegtető üzemmód
  - késleltetett kapcsolat lezárások

## Sérülékenységet kihasználó

- „Zero-Day”
- ismert sérülékenység kihasználása

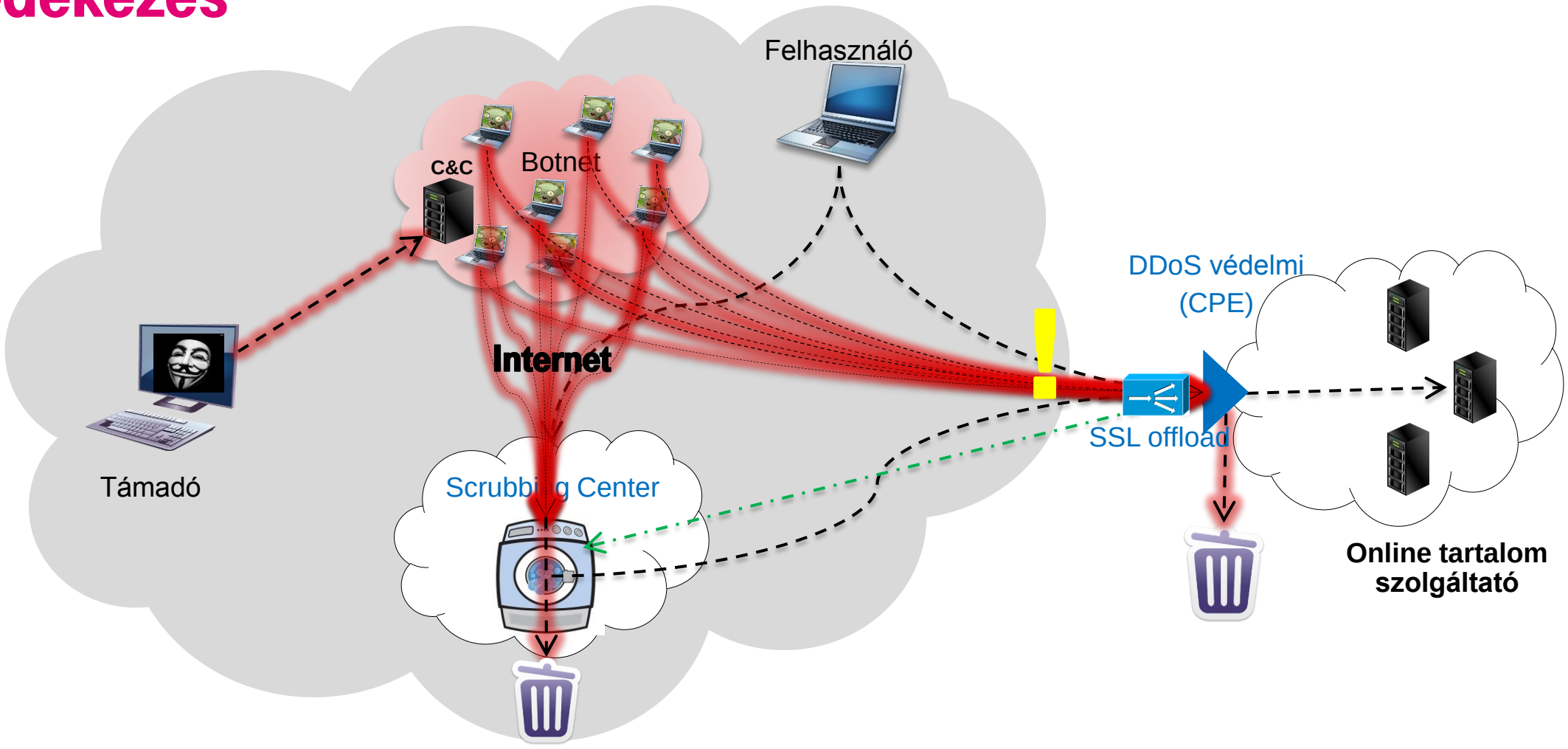
T · · Systems ·

# Védekezési technikák

- **Kapacitás bővítés ☹**
  - Eszköz
  - Sávszélesség
- **Célzott védelem a határfelületen (CPE):**
  - Rate-limit (volumetrikus) – nem hatékony ☹
  - DDoS védelmi funkciók:
    - L4 SYN cookie
    - L7 challenge – response (http 302, Javasript)
    - Day-Zero + szignatúra alapú
- **Szolgáltatói közreműködés**
  - Black-Hole Routing (RTBH)
  - Scrubbing Center (cloud alapú DDoS védelem)
- **Hibrid megoldás (CPE + cloud)**
  - CPE (SSL forgalomra is)
  - Szolgáltatói „Mosóda” - Scrubbing Center

T · · Systems ·

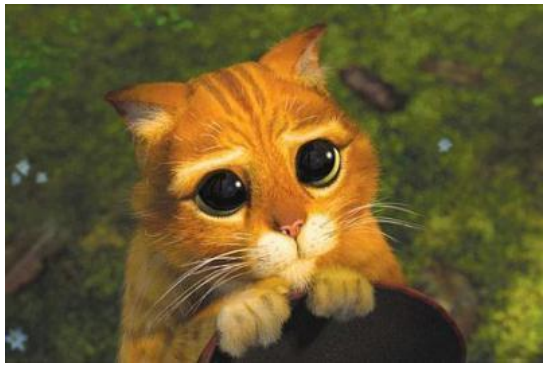
# Védekezés

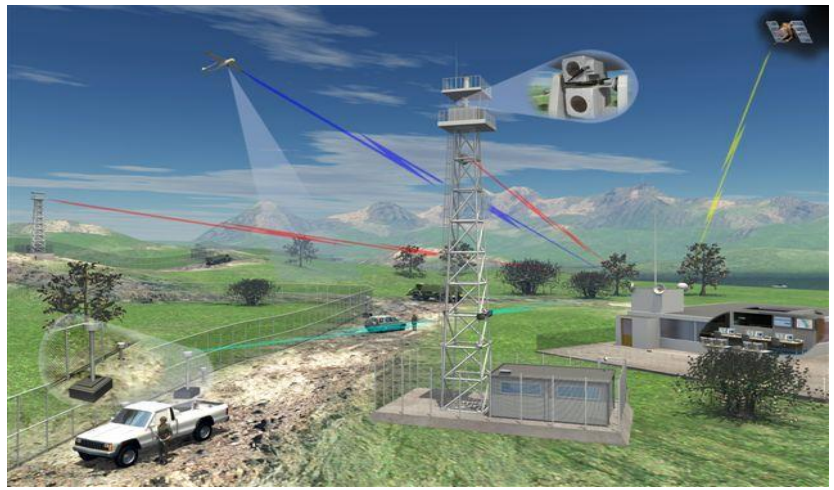



T · · Systems ·

# Hátradőlhetek, mert ...

- Nem vagyok célpont, nincs ellenségem, sosem voltam még DDoS támadás alatt ...





- A határvédelmi rendszerem fel van készítve ...

- CDN-t (Content Delivery Network) használok ...

T · · Systems ·

# SECaaS szolgáltatás - [D]DoS védelem

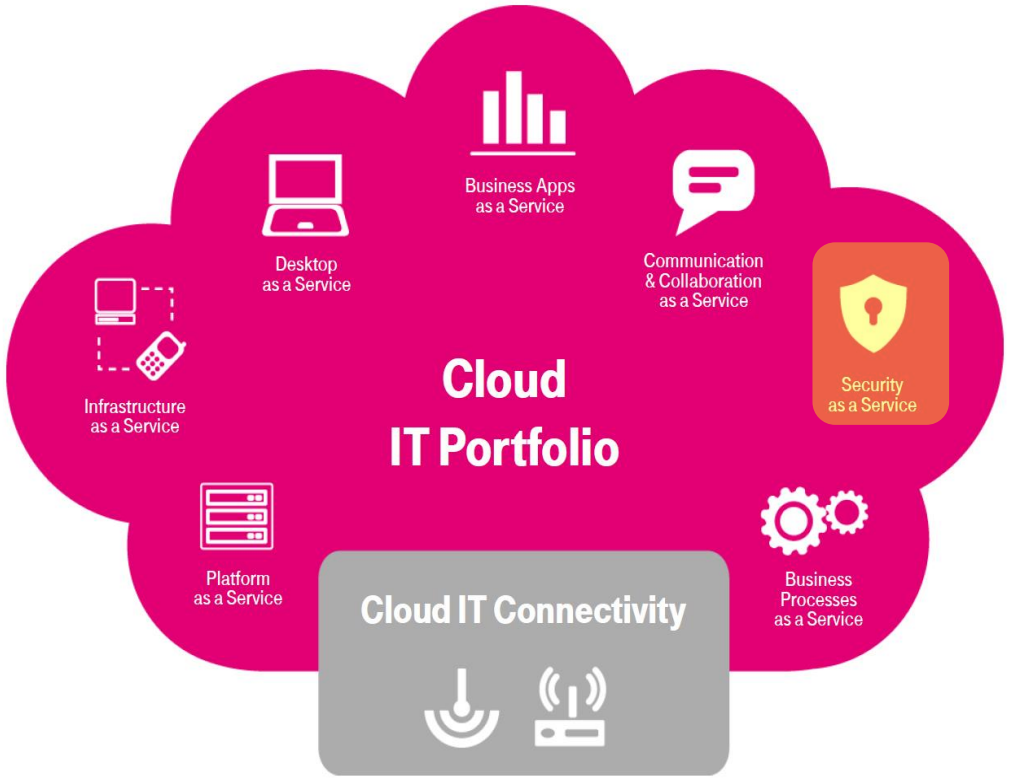
**Szolgáltatási modell/architektúra:**

- Hibrid modell, kihelyezett CPE-vel
- Többfelhasználós (multi-tenant) környezet
- Testreszabható felhasználói portál
- Scrubbing Center helyi DDoS megoldás back-endjeként

**Jelenleg:**

- Tesztek
- Gyártók kiválasztása

**Várható start 2014 Q1**




T · · Systems ·

# Demó

Szabó István - szenior rendszermérnök

T · · Systems ·

# Arbor DDOS védelem

- Arbor megoldás bemutatása
- Tesztelrendezés
- Élő demonstráció
- Összefoglalás

ARBOR NETWORKS

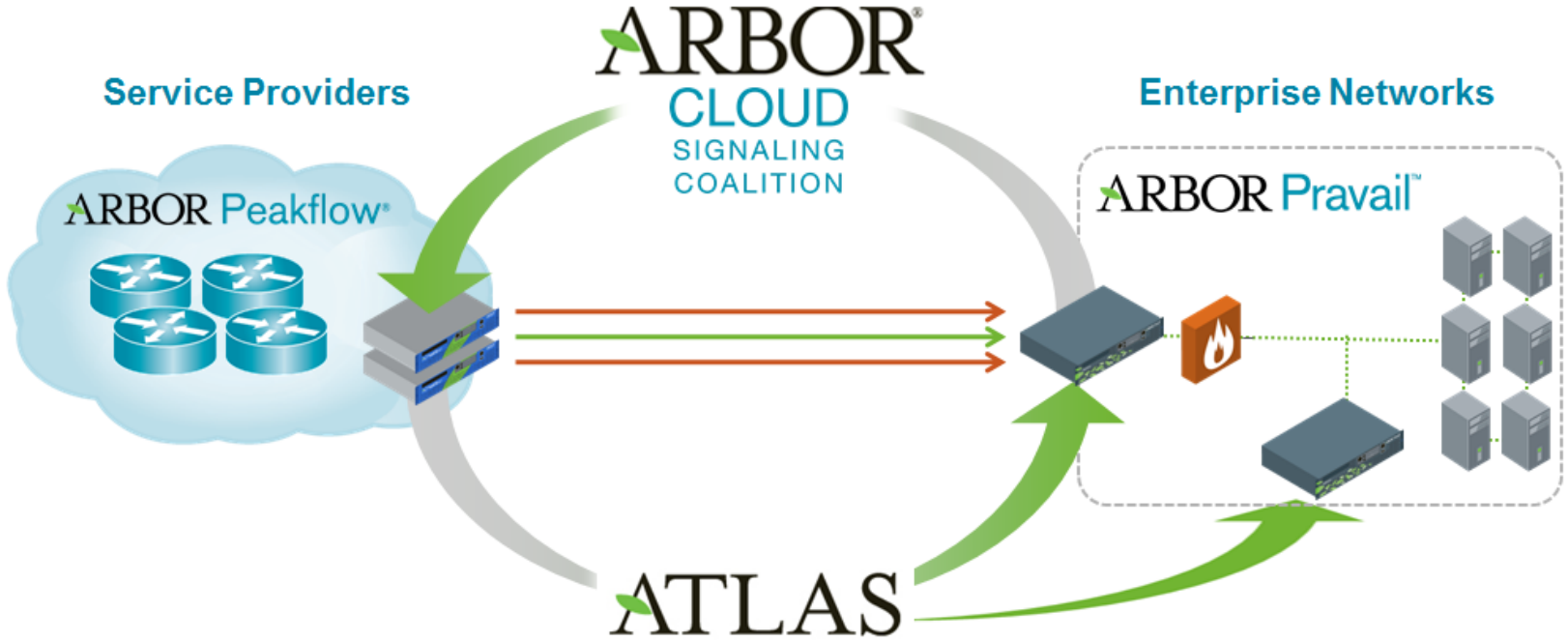
# Arbor hibrid DDOS védelem

## Peakflow SP

- SP oldali megoldás
- SP és ügyfelek védelmére

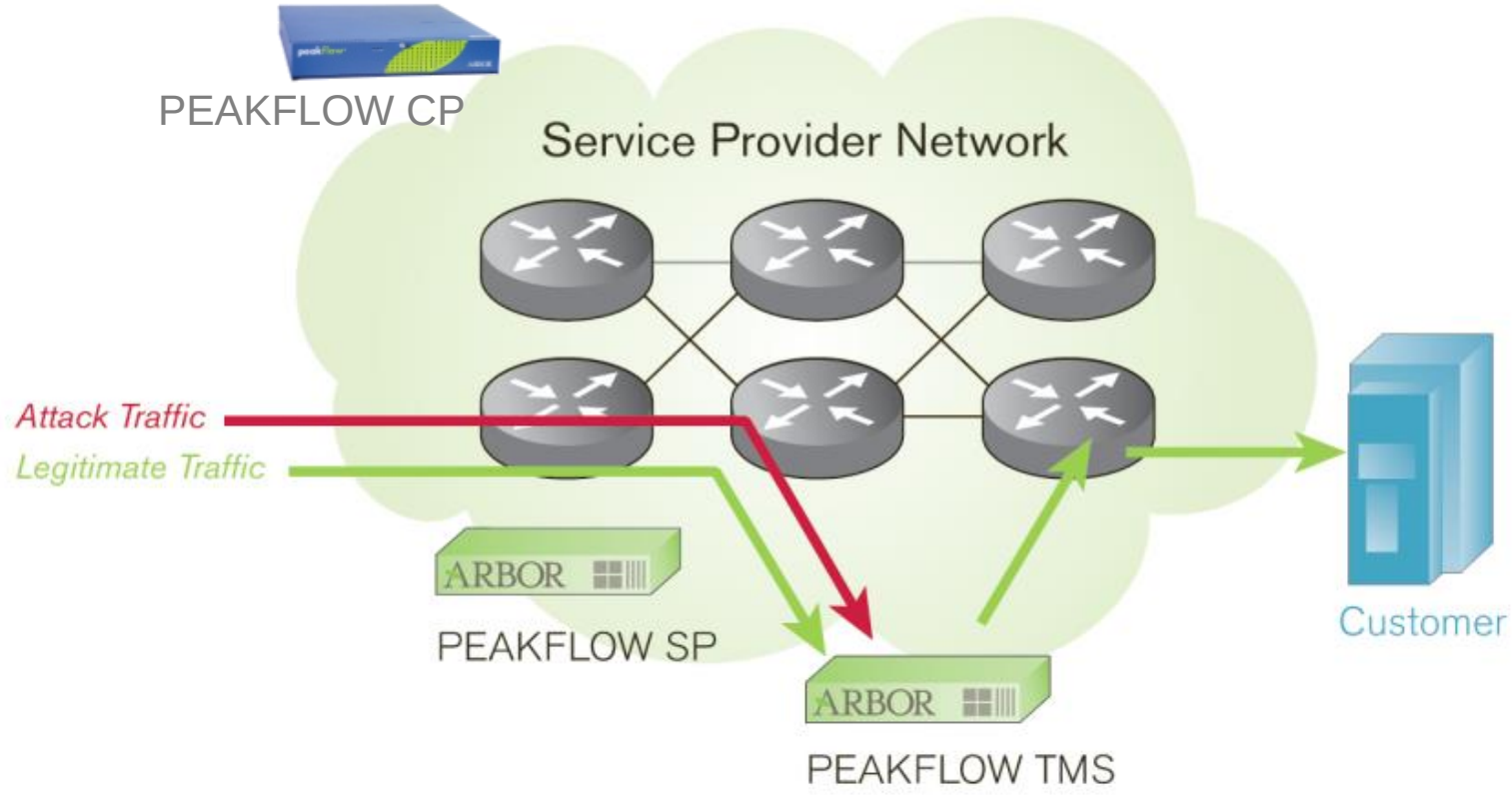
## Pravail (APS)

- Nagyvállalati megoldás
- Saját hálózat védelmére



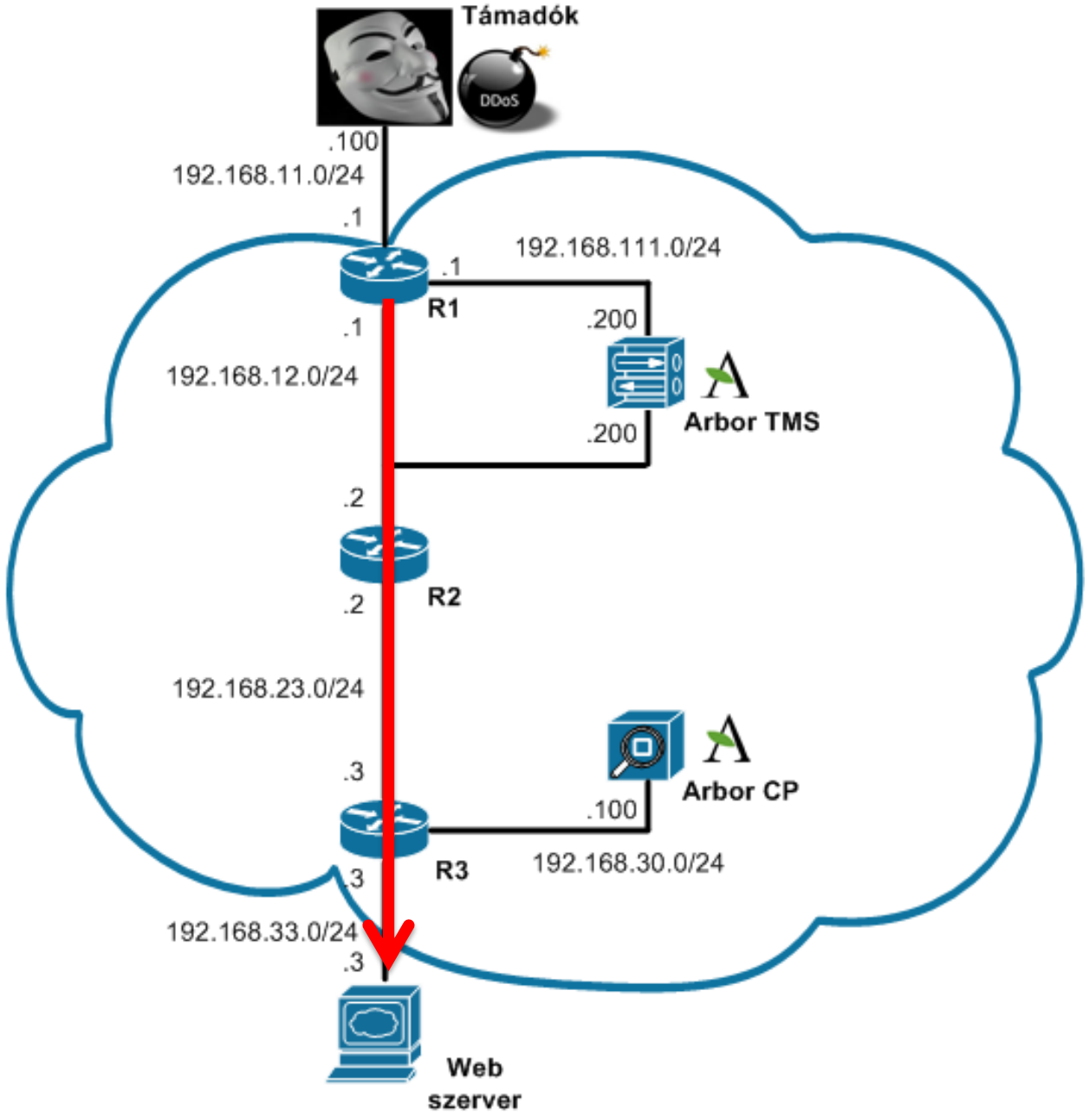
# Arbor Peakflow SP

- **Peakflow CP**
  - Központi menedzsment
  - Netflow Collector
  - Out Of Band
- **Peakflow TMS**
  - Forgalom elemzés
  - A CP vezérli
  - Inband



# Tesztelrendezés - normál

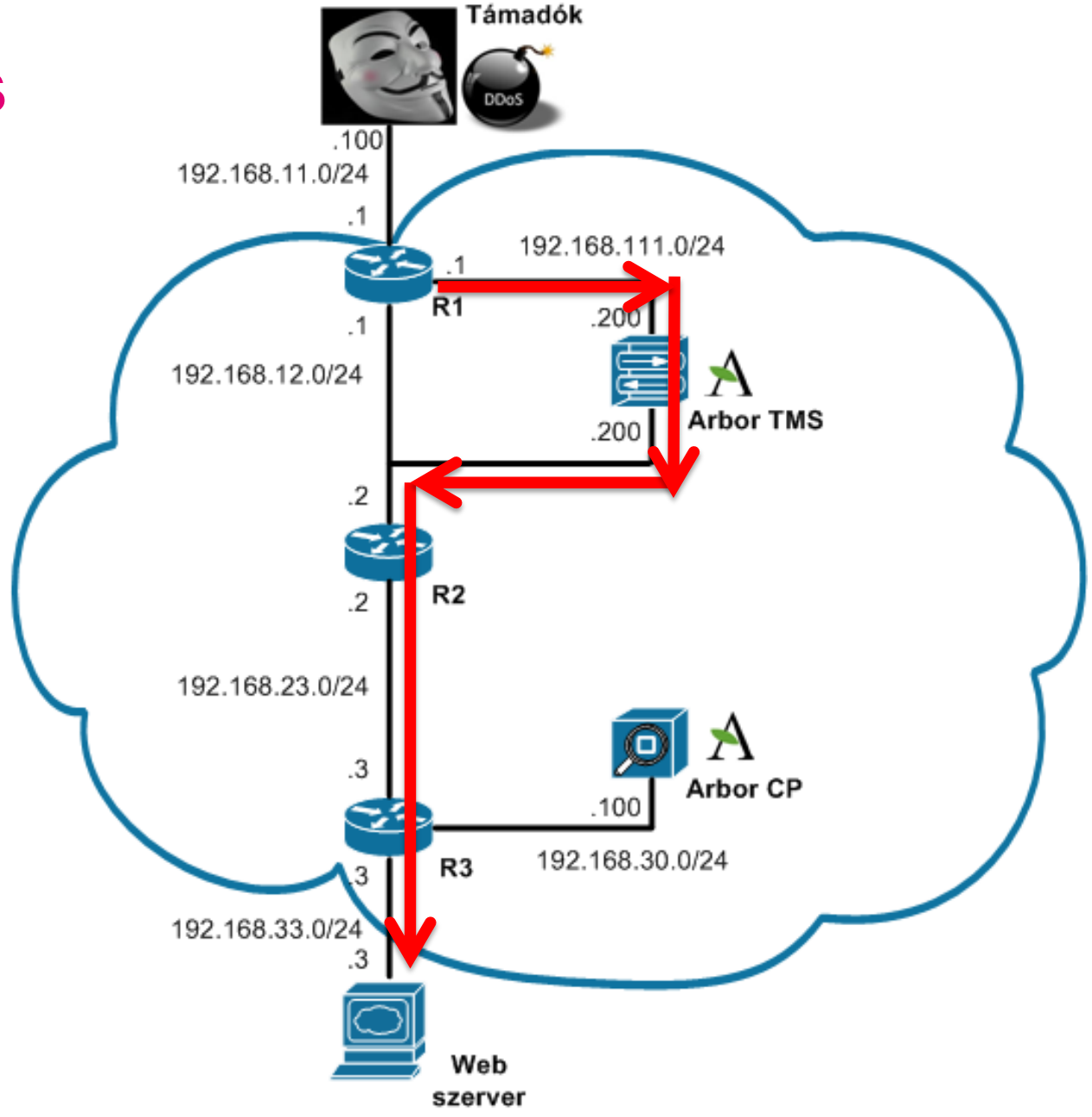
- Támadó: DDOS célszoftver
- R1, R3 PE routerek
- R2: P router
- Arbor TMS: inband, ha szükséges
- Arbor CP: out of band, GUI + netflow




T · · Systems ·

# Tesztelrendezés - támadás

- Támadó: DDOS célszoftver
- R1, R3 PE routerek
- R2: P router
- Arbor TMS: inband, ha szükséges
- Arbor CP: out of band, GUI + netflow




T · · Systems ·

# [D]DoS - záró gondolatok

- Támadások mindig lesznek ...
- Tökéletes védelem nincs ...
- Építhet mindenki saját bástyát, de ... igénybe veheti szolgáltatásként is ...
- Jelenleg csak külföldi (cloud alapú) szolgáltatók érhetők el ...
- Hamarosan indul a helyi, T · · [D]DoS védelmi szolgáltatás

T · · Systems ·

# Köszönjük a figyelmet!

T · · Systems ·