Az ISZT Hun-CERT és a PROBE program

HBONE Workshop – 2016.11.16.

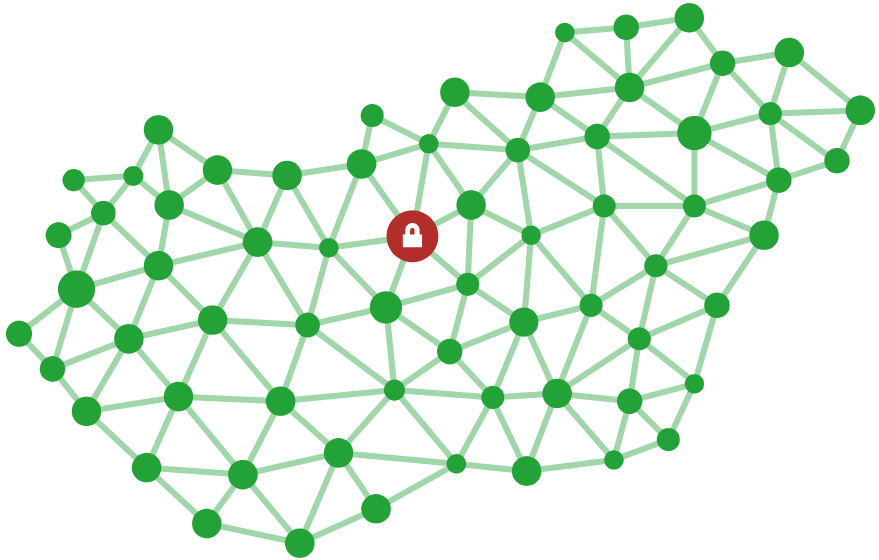
Internet Szolgáltatók Tanácsa (ISZT)

- Non-profit egyesület
  - Alapítva: 1997, Munkatársak: 5 fő
- Az ISZT tagjai
  - Jelenleg 35 magyarországi internet szolgáltató
    - Pl.: Antenna Hungária, Integrity, Magyar Telekom, UPC, stb...
  - A tagok összessége országos lefedettséget eredményez (2015 - 53%)
  - Jelentős méretkülönbségek

- Az ISZT feladatai
  - Koordináció (.hu ccTLD, BIX, belső problémák orvoslása)
  - Hatóság és ISP-k közti kapcsolatok koordinálása
  - Érdekvédelem (gazdasági, jogi)
  - Tájékoztatás, oktatás (technikai, tudományos)
  - Incidenskezelés → Hun-CERT

ISZT Hun-CERT

- Alapító és támogató:
  - Internet Szolgáltatók Tanácsa, MTA SZTAKI
- Üzemeltető: MTA-SZTAKI Hálózatbiztonsági és Internet Technológiák Osztálya (HBIT)
- Alapítva: 2003 október
- Tevékenységek, szolgáltatások
  - Hálózatbiztonsági incidensek kezelése
  - Biztonsági tudatosság növelése
  - Publikációk, oktatás, hírek, riasztások
  - Koordináció
  - Hálózatbiztonsági eszközfejlesztés

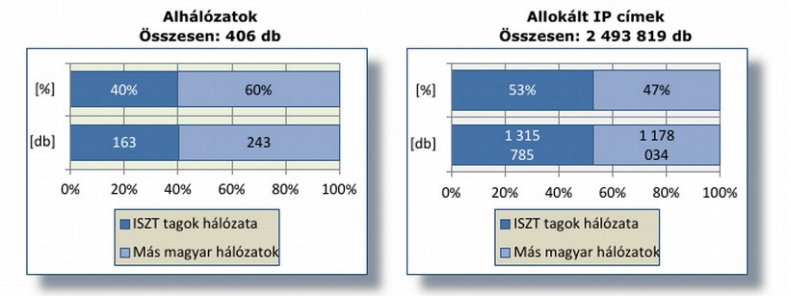


Mi az az „Incidens”?

- Az „incidens” fogalma változik
  - Eredetileg: számítógépes biztonsági incidens (SPAM, botnet, deface, DoS, phishing, data loss/leak, APT)
- Újfajta értelmezés: internettel kapcsolatos, jogszabályba ütköző tevékenység
  - Gyermekpornográfia, becsületsértés, hitelrontás, zaklatás
  - Gyűlöletkeltés, terrorizmus, adathalászat
  - Szerzői jogot sértő tartalom, … stb.
- A két kategória összemosódik
  - Incidenskezelés = technikai + jogi feladatok összessége
  - A Hun-CERT főként technikai feladatokat lát el
  - Jogi kérdésekben feladat-átadás ISZT-nek
- Az incidens elhárítása többnyire sok szereplőt érint
  - Országon belüli és/vagy nemzetközi kapcsolattartást igényel
  - ISP-k szerepe jelentős

Aktuális eredményeink (2015-2016)

- 2015-ben több, mint 4500 darab hazai, illetve nemzetközi forrásból származó biztonsági bejelentést kezeltünk
- 9 darab rendkívüli biztonsági jelentést adtunk ki
- Saját adatgyűjtő hálózat (PROBE) kiépítésébe kezdtünk
- Sikeres kommunikációs gyakorlatot tartottunk



HUNCERT PROBE

Korábbi eredményeink, partnereink

- ISZT Hun-CERT munkacsoport létrehozása, kapcsolódás az ISZT biztonsági munkacsoport munkájához
- Közös GovCERT (PTA) situational awareness megoldás fejlesztése
- Nemzeti Kiberbiztonsági Koordinációs Tanács CERT, Energetikai és Egészségügyi munkacsoportokban kommunikációs gyakorlat lefolytatása
- Kiemelt internet szolgáltatókkal személyes kapcsolat építése
- Saját szolgáltatói adatbázis építése (hab.cert.hu) – RIPE WHOIS helyett

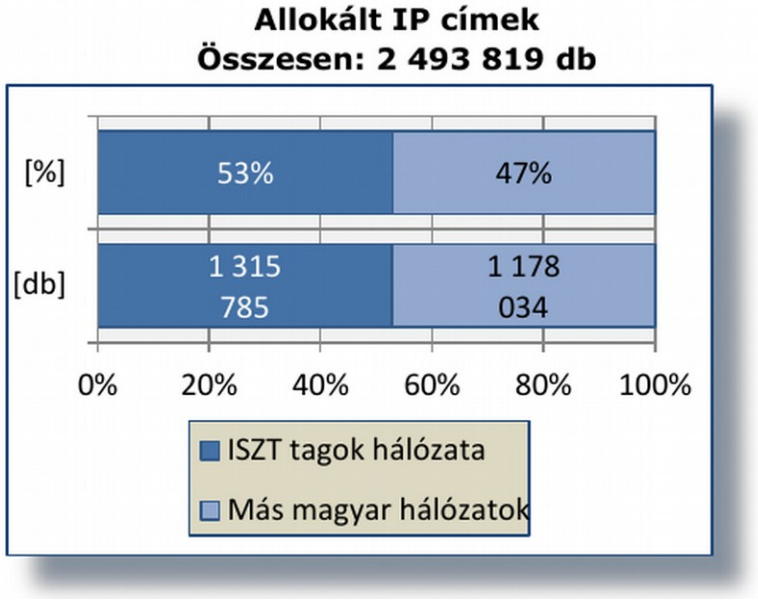
HAB.cert.hu

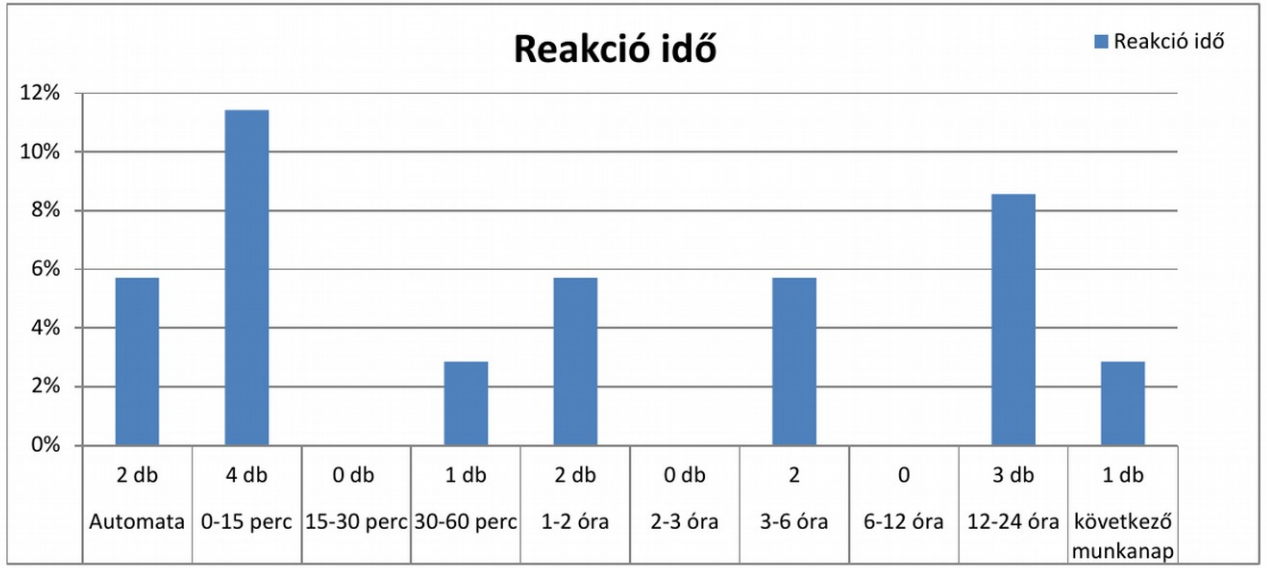
- Cél: a nyilvánosan elérhető adatbázisoknál használhatóbb kapcsolati nyilvántartás, incidenskezelési célra
- RIPE alapú, de annál bővebb és jóval pontosabb
- minden szolgáltató saját hozzáféréssel rendelkezik
- a Hun-CERT zárt körű adatcsere felülete
- Nyilvántartások:
  - kb. 300 db ISP kontakt (név, munkakör, tel, e-mail, kompetencia)
  - kb. 450 db IP alhálózat (ISP, netname, CIDR, ASN, IP kiosztási stratégia)

Hun-CERT kommunikációs gyakorlat – 2016

- A gyakorlatok célja: az együttműködés javítása
- 2016 március elején lebonyolított 2 napos gyakorlat
  - 22 hazai résztvevő
  - Szolgáltatókkal előzetesen nem egyeztetett, egyszerűsített forgatókönyv alapján zajlott le
  - Idén csak a RIPE abuse címeket használtuk
  - A feladat web szűrés megvalósítása volt
- Az hazai IP címtér 53%-át fedtük le
- A résztvevők 23%-a fél órán belül válaszolt

Hun-CERT kommunikációs gyakorlat – 2016

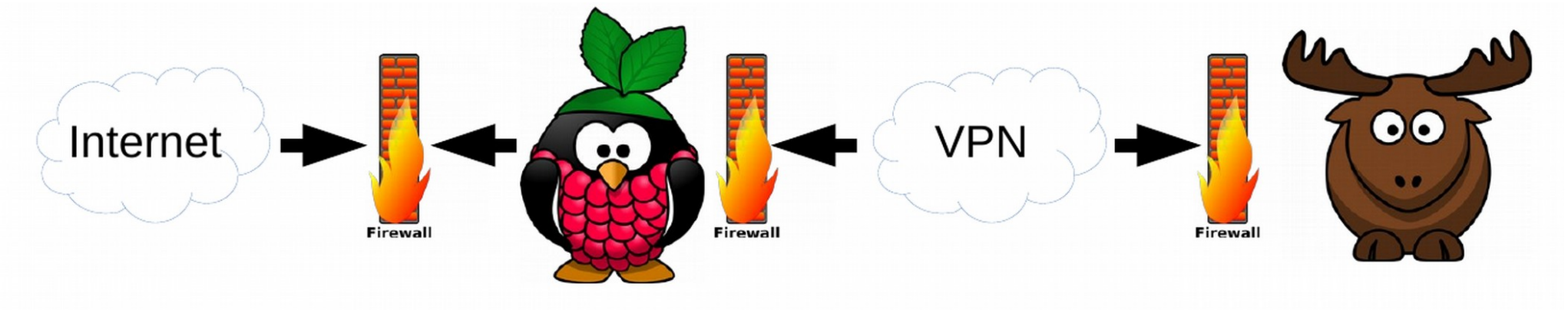




Hun-CERT PROBE – célok

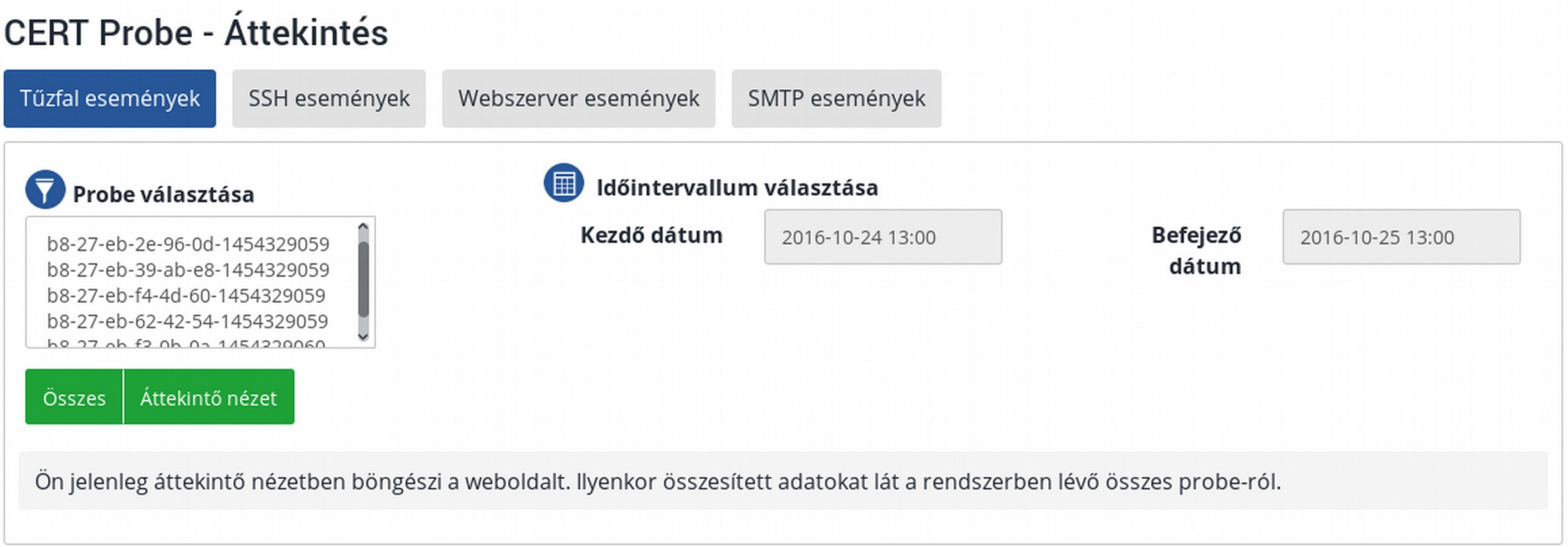
- A PROBE projekt céljai:
  - Hun-CERT incidens-érzékelési képességének javítása
  - Hazai szolgáltatókat érintő internetes biztonsági események/trendek rögzítése, elemzése, értékelése
  - Átfogó biztonsági információk elérhetővé tétele

Hun-CERT PROBE – architektúra



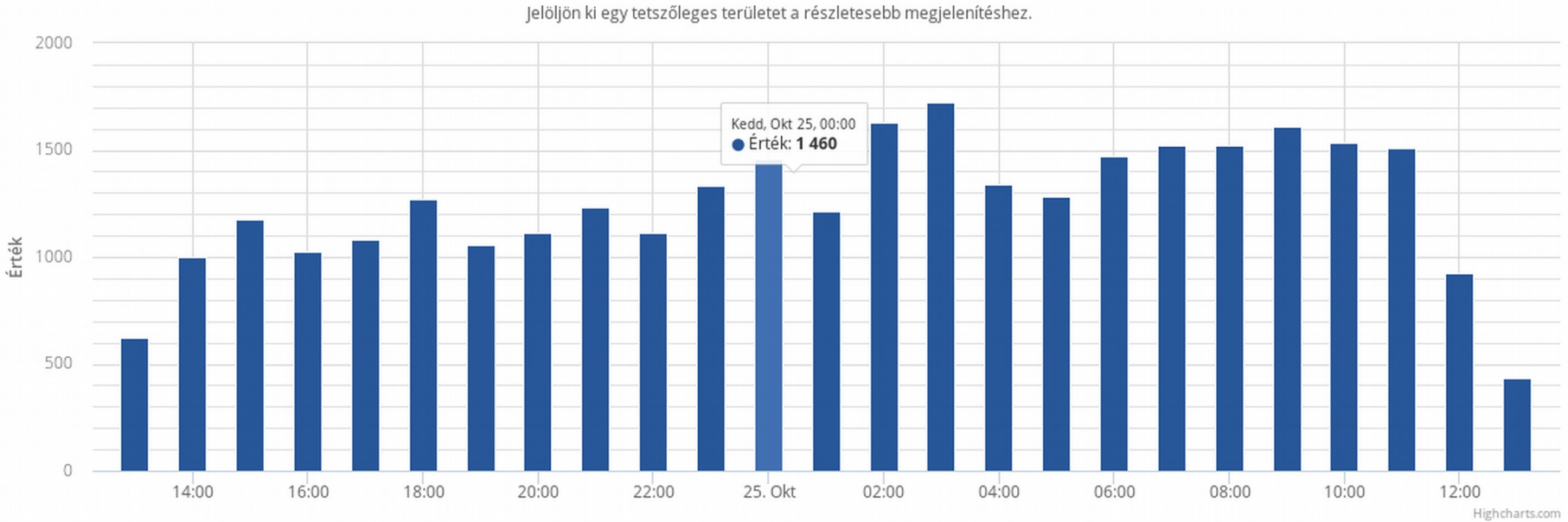
- docker
  - lightweight
  - easy to deploy
  - isolated
- ansible
  - lightweight
  - simple
  - idempotent
- ELK
  - robust
  - elastic (scalable)
  - search-optimised

Hun-CERT PROBE – DEMO (1)



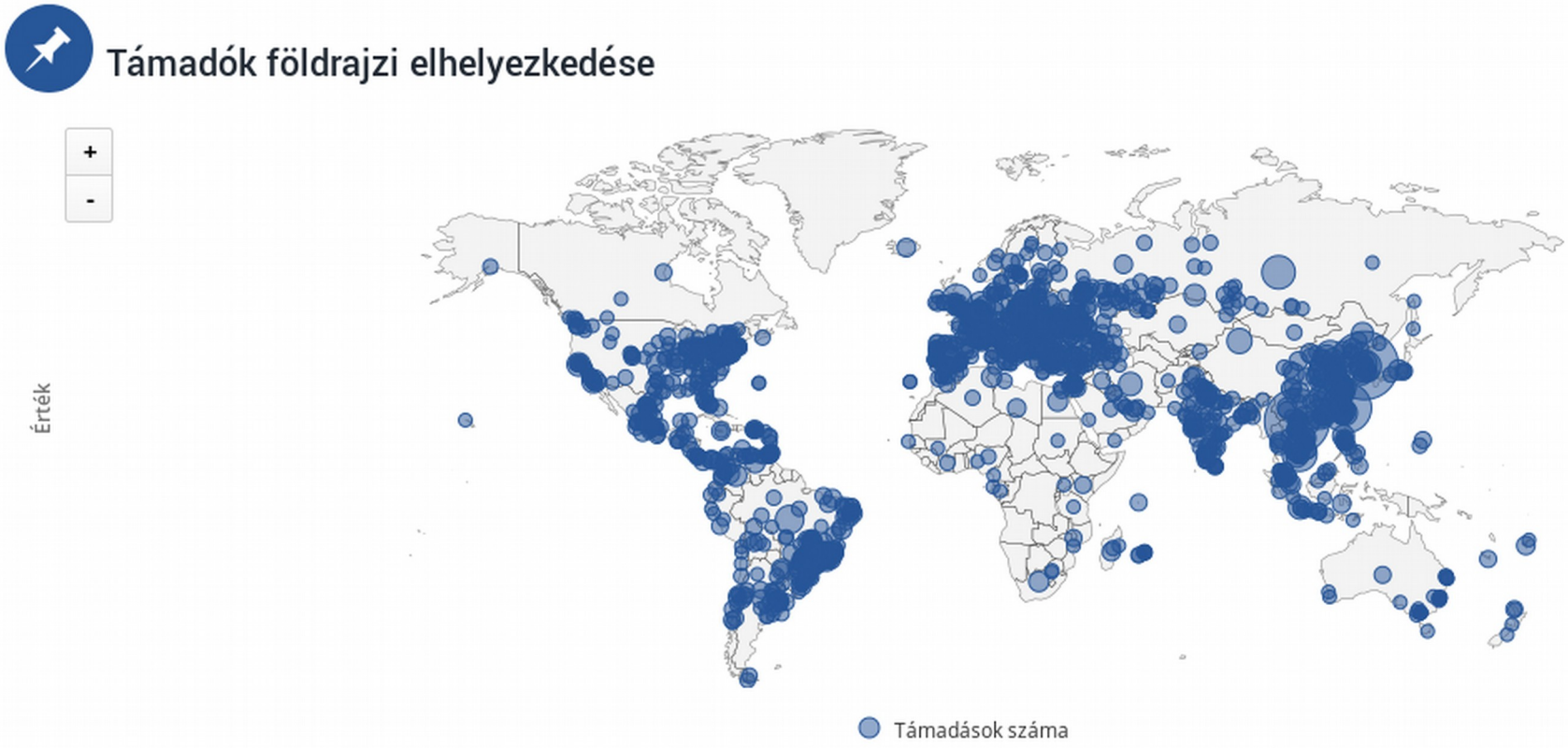
Hun-CERT PROBE – DEMO (2)

Eldobott csomagok számának alakulása



Min	Max	AVG	SUM
437 esemény/óra	1726 esemény/óra	1248.6 esemény/óra	31215

Hun-CERT PROBE – DEMO (3)



Hun-CERT PROBE – DEMO (4)

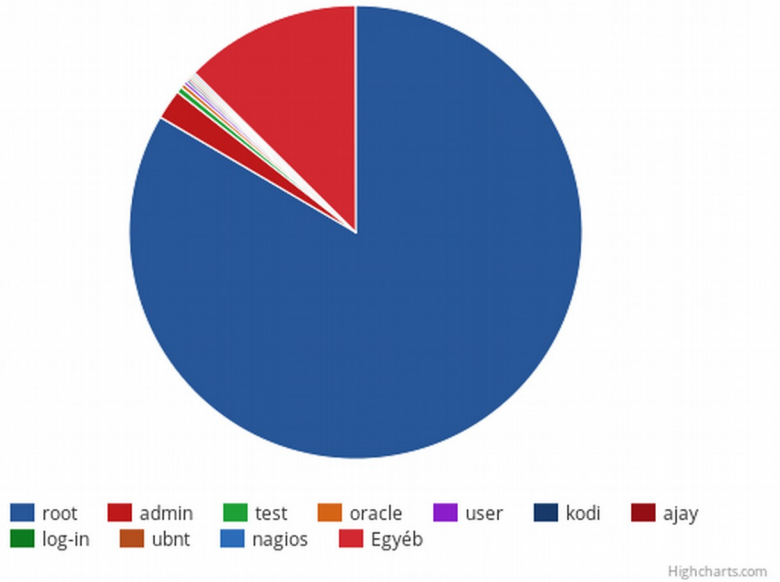
Konkrét események

Dátum (UTC)	Cél eszköz	Forrás IP	Forrás port	Protokoll	Cél Port	Csomag méret (bájt)	Ország	Város
2016-10-25T11:09:34.278Z	b8-27-eb-f3-0b-0a-1454329060	[redacted]	5167	UDP	5060	443	Germany	-
2016-10-25T11:09:34.276Z	b8-27-eb-39-ab-e8-1454329059	[redacted]	44107	TCP	23	40	Korea, Republic of	Yongin
2016-10-25T11:09:26.784Z	b8-27-eb-39-ab-e8-1454329059	[redacted]	35023	TCP	23	44	Vietnam	Hanoi
2016-10-25T11:09:24.305Z	b8-27-eb-39-ab-e8-1454329059	[redacted]	35023	TCP	23	44	Vietnam	Hanoi
2016-10-25T11:09:23.398Z	b8-27-eb-f4-4d-60-1454329059	[redacted]	36913	TCP	23	44	Poland	-
2016-10-25T11:09:23.397Z	b8-27-eb-62-42-54-1454329059	[redacted]	28884	TCP	23	40	Ukraine	Kiev
2016-10-25T11:09:19.424Z	b8-27-eb-f3-0b-0a-1454329060	[redacted]	8245	TCP	23	40	Russian Federation	Novosibirsk

Hun-CERT PROBE – DEMO (5)

Leggyakoribb felhasználónevek

root	17015
admin	432
test	88
oracle	63
user	49
kodi	38
ajay	35
log-in	34
ubnt	33
nagios	31
Egyéb	2564



Hun-CERT PROBE – adatkezelés és -megosztás

- Az önkéntes adatszolgáltatás során begyűjtött adatok hasznosítása:
  - A program **nyilvános** weblapján trend jellegű adatok, havi és éves grafikonok megjelenítése (forrás és cél IP címek megadása nélkül)
  - A programban **részt vevő** támogatók (tagok) számára szűrhető összesített grafikonok, toplisták megjelenítése (forrás IP címekkel)
  - **Saját hálózaton** elhelyezett PROBE eszközökön begyűjtött teljes információ (részletes eseménynaplók, forrás és cél IP címek) az adott tag számára
  - A rendszerből származó adatokat a **Hun-CERT** saját incidenskezelési tevékenysége, valamint az ezzel kapcsolatos kutatási tevékenysége során felhasználhatja

Hun-CERT PROBE – továbbfejlesztési lehetőségek

- További terveink:
  - külső biztonsági tanúsítvány megszerzése a rendszerre
  - érzékelő képesség bővítése (például: NTP, DNS támadásokra)
  - dinamikus szűrőszolgáltatás (DNSBL, blackhole routing)
  - adatlekérdező felület fejlesztése (UX design)
  - virtualizált szondák (könnyebb terjesztés)
  - hálózatosodás, nemzetközi kapcsolatok kialakítása
- Várjuk a programhoz csatlakozók jelentkezését (ingyenes!)

Kérdések?

Köszönjük a figyelmet!

http://www.cert.hu
cert@cert.hu