A Hun-CERT 2017 évi fejlesztései

Networkshop 2018 – Eger, 2017.04.05.

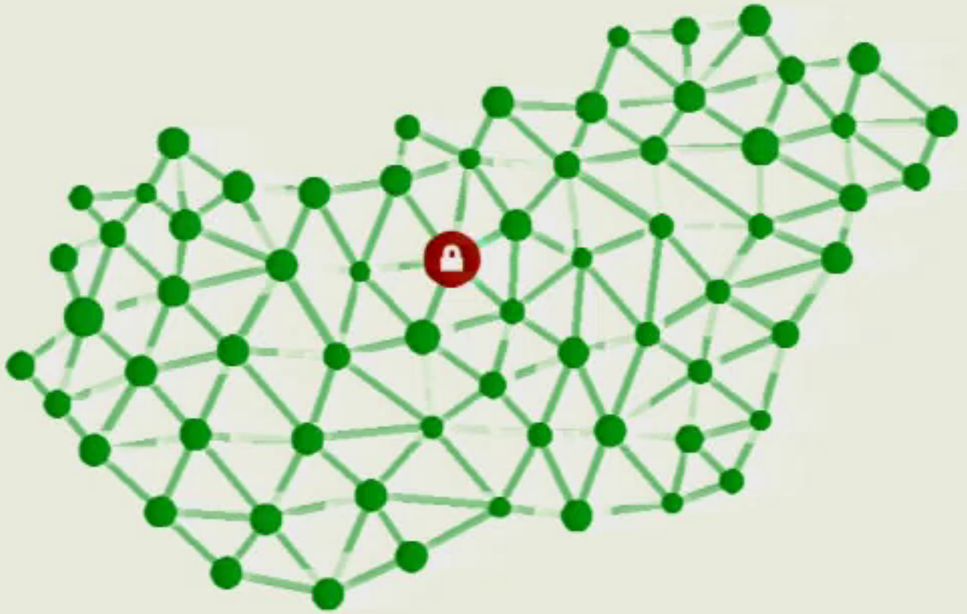
Internet Szolgáltatók Tanácsa (ISZT)

- Non-profit egyesület
  - Alapítva: 1997, Munkatársak: 5-10 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

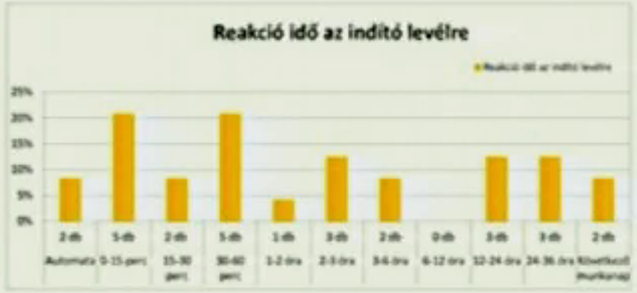


Mi az az „Incidens”?

- 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

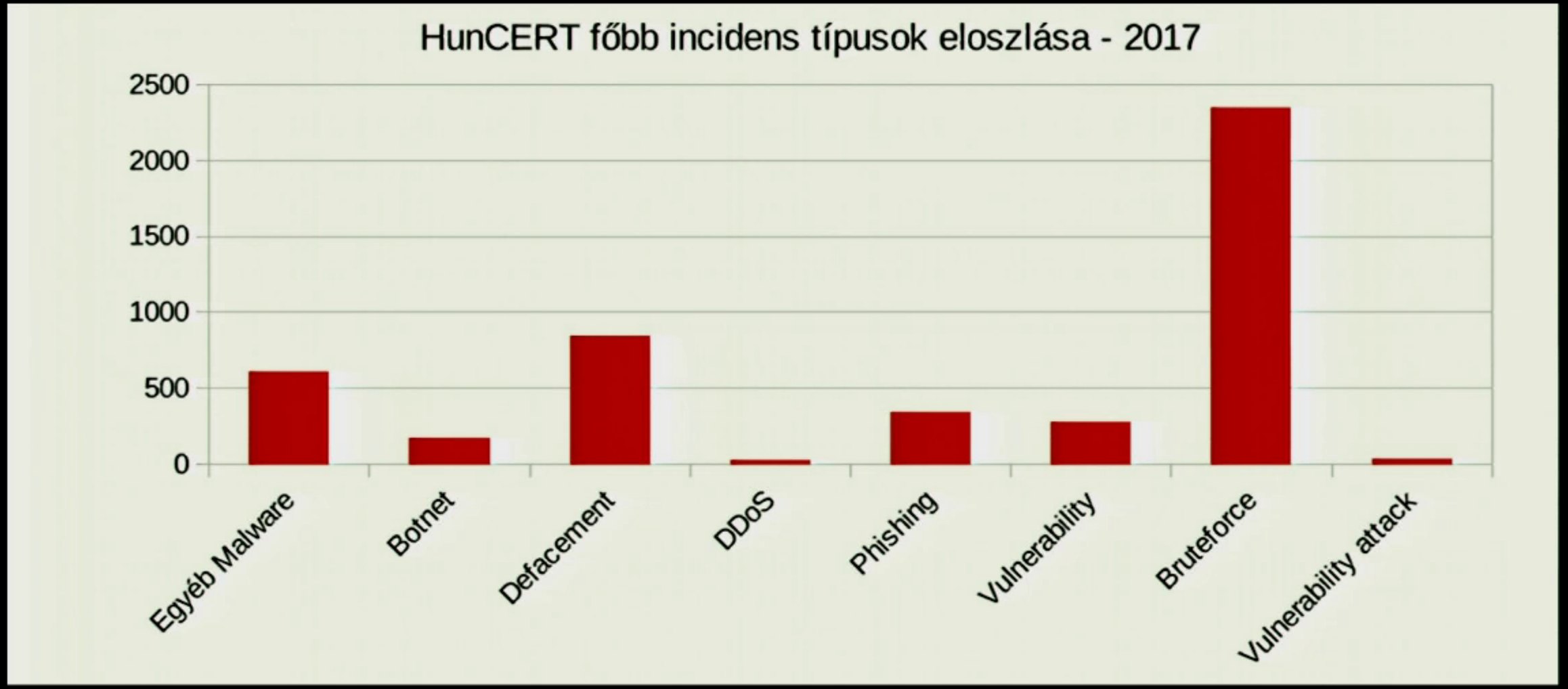
Aktuális eredményeink (2017-2018)

- 5806 darab egyedi incidens bejelentés kezelése és több mint **2.5 millió esemény** feldolgozása
- 4598 feldolgozott sérülékenység jelzés, 16 darab önálló, rendkívüli sérülékenységi riasztás („magas” kockázati besorolással)
- 28 kihelyezett és 17 saját hálózaton üzemelő PROBE eszköz, összesen 36 aktív hálózati adatforrás,
- részvétel 6 hazai szakmai konferencián, 2 önálló konferencia előadás



HUNCERT PROBE

2017-es incidenstípusok



Meltdown és Spectre

- HunCERT analízis: 2018.01.08
- Side channel támadások
  - CPU branch prediction cache leak
- Valós támadási vektor még nincs
- A kapkodó „javítás” eredményei
- Számos mikroarchitektúra érintett
  - Új sérülékenység típus született

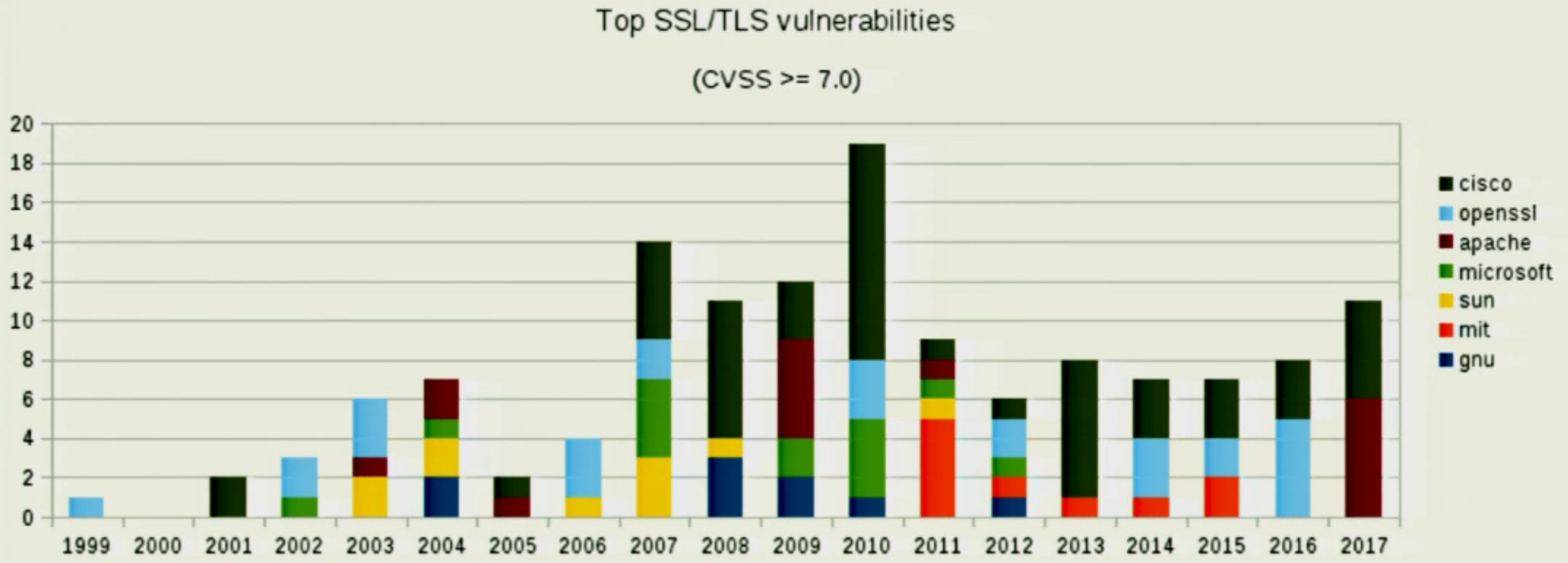
```
meltdown:
mov al, byte [rcx]
shl rax, 0xc
jz meltdown
mov rbx, qword [rbx + rax]
```

Egyéb kiemelt riasztásaink és összefoglalóink

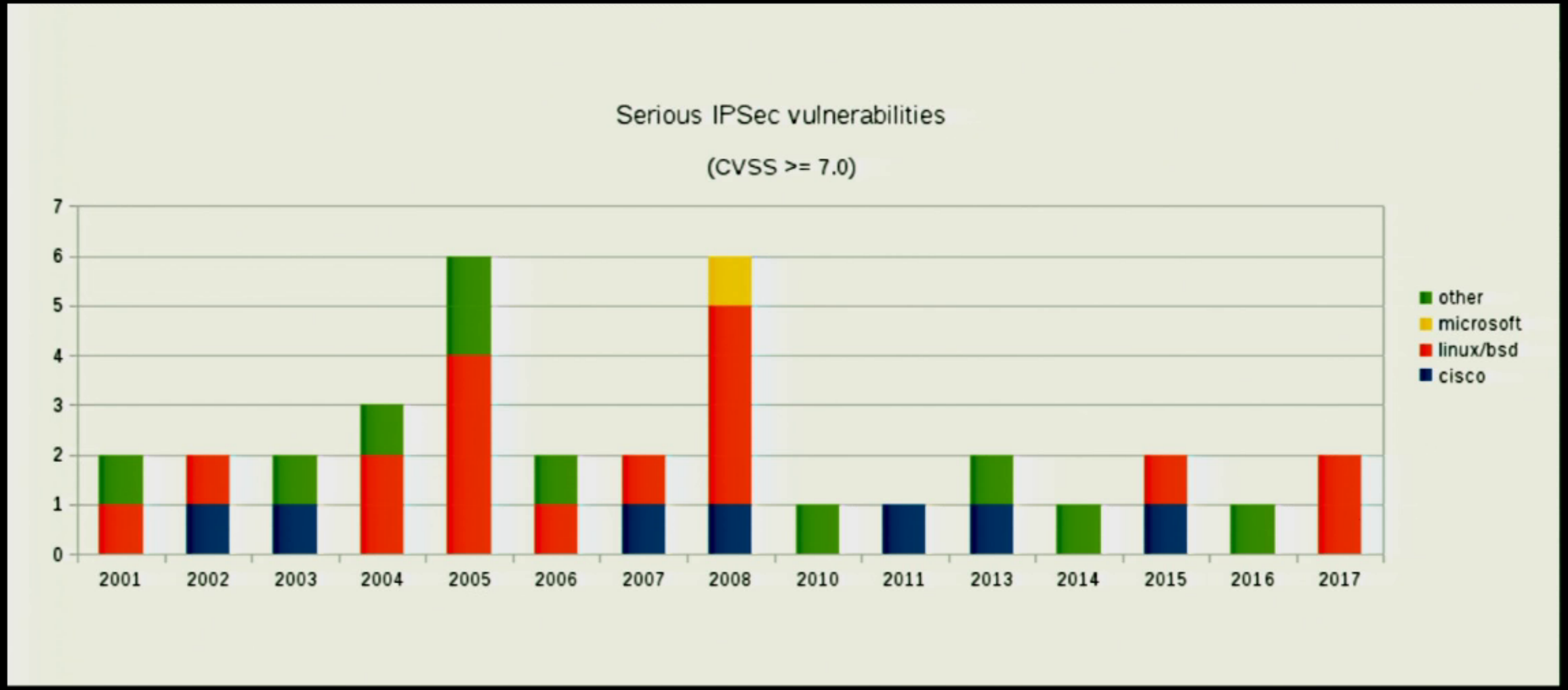
- Remote Execution
  - Drupal core
  - Cisco ASA
- DoS
  - VMware Workstation és Fusion
  - BIND sérülékenységek
- Egyebek
  - WannaMine kriptovaluta bányászszoftver
  - BadRabbit és WannaCry zsarolóvírusok
  - WPA és WPA2 többszörös sérülékenysége
  - Linux sudo sérülékenység

Aktuális riasztásaink: https://www.cert.hu/riasztasok (RSS ready)

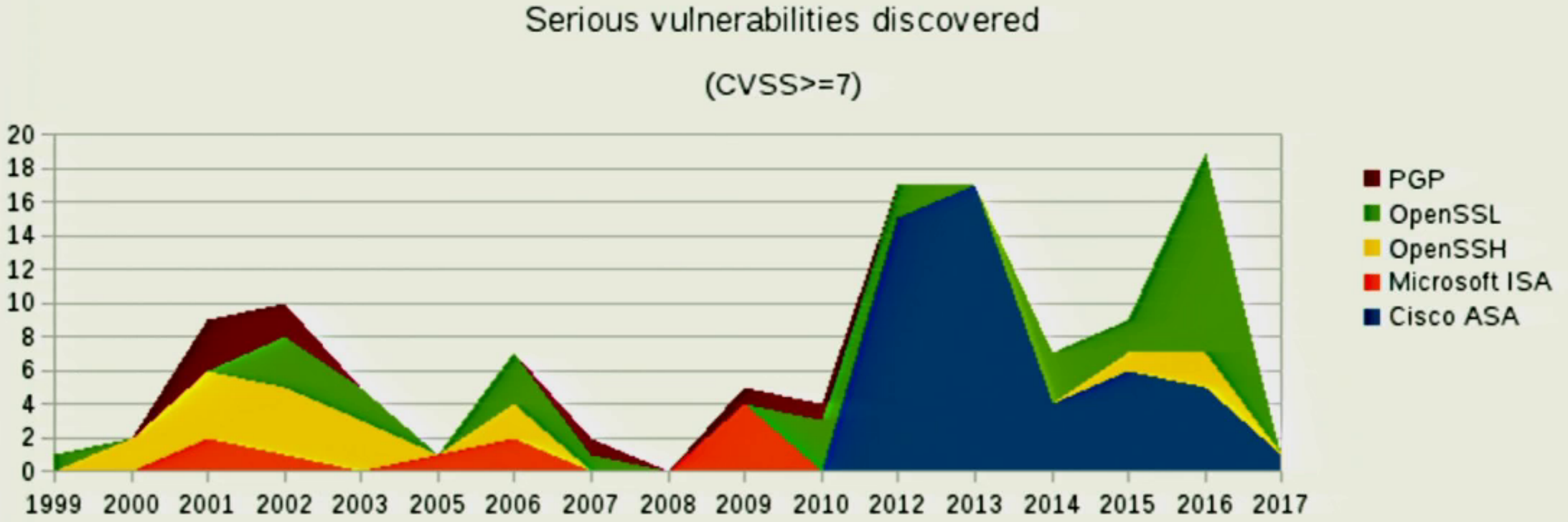
Sérülékenységi trendek



Sérülékenységi trendek



Sérülékenységi trendek



HunEX 2017

HunEX 2017 – Célok

- Incidenskezelési képességek gyakorlása
- Felkészülés egy komolyabb incidensre
- Kommunikációs csatornák tesztelése
- Kapcsolatok elmélyítése
- Belső eljárásrendek begyakorlása
- Sajtóval való kapcsolattartás gyakorlása

HunEX 2017 - Kerettörténet

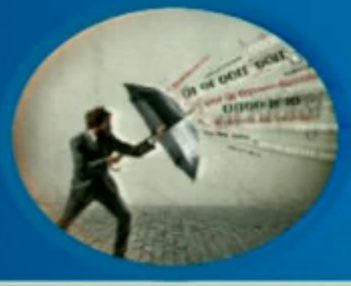
- Nemzetközi konfliktus
- Magyarország és elképzelt szomszédja Attakia között
- Attakia önhatalmúlag megszegte a kétoldalú megállapodást
- Magyarország bírósághoz fordult
- Országhatárokon átnyúló vízkészleten
- A pert megnyerte
- Az ítéletre reagálva hacktivista kampány indul

HunEX 2017 – Résztvevők

HunEX 2017 – Technikai tényezők

DDoS

Defacement



Ransomware

HunEX 2017 – Kommunikáció

- Játékosnak lehetősége volt figyelni a gyakorlat idején működő „Gyakorlott Hírmondó” nevű sajtóportált, Infó:
  - a kerettörténetről
  - a technikai feladatokról
- Összesített kommunikációs „eredmény”:
  - Üzemeltetési: 461 e-mail
  - Sajtó: 72 e-mail
  - Rest of world: 88 e-mail
- HunCERT eredmény: 112%

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

HUNCERT PROBE

Hun-CERT PROBE – DEMO (1)

Hun-CERT PROBE – DEMO (2)

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)

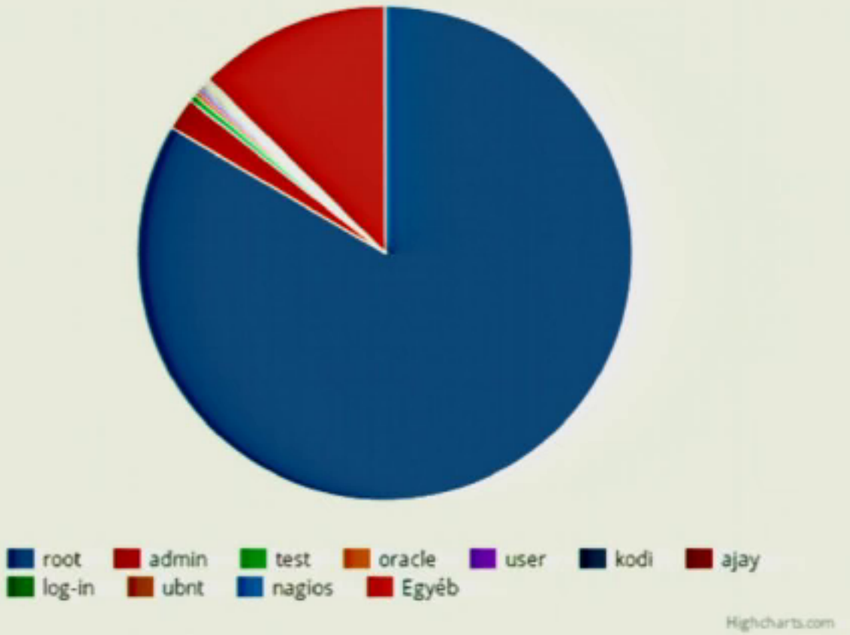
Konkrét események

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 - GDPR

- GDPR – General Data Protection Regulation (95/46/EC)
  - EU adatvédelmi jogharmonizációs **rendelet**
  - 2018. május 25-től kötelező érvényű (közvetlenül alkalmazandó)
- Legfontosabb újdonságok
  - Kiterjedt területi hatály (EU-n kívülre is!), adattranszport szabályok
  - Számonkérhetőség és adatvédelem „by design” elve
  - Értesítési kötelezettségek, transzparencia (cselekmények, incidensek)
  - Egyablakos ügyintézés („one stop shop”) - EU szintű intézményrendszer
  - Elfeledéshez való jog

Kérdések?

Köszönjük a figyelmet!

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