Informatikai Oktatási Konferencia
és Akadémiai Nap

2014

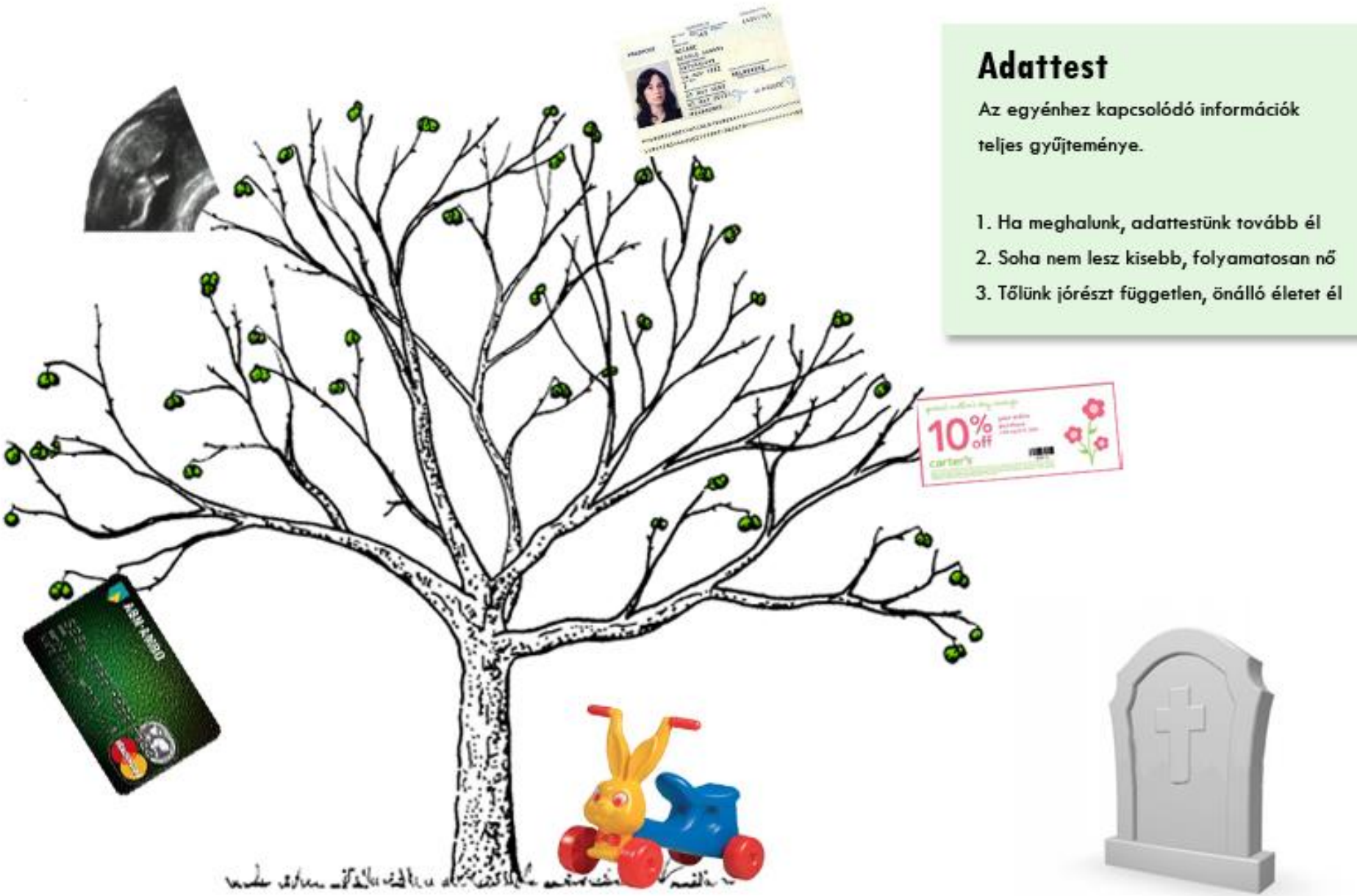
Kiberfenyegetettség napjainkban

Vargha Gergely
Hálózatbiztonsági szakértő
Cyber Defence Management Authority
Nemzeti Biztonsági Felügyelet

Nemzeti
Biztonsági
Felügyelet

Személyes védelmünk határvonalai túlmutatnak kerítésünkön


Kibertér



Adattest

Az egyénhez kapcsolódó információk teljes gyűjteménye.

1. Ha meghalunk, adattestünk tovább él
2. Soha nem lesz kisebb, folyamatosan nő
3. Tőlünk jórészt független, önálló életet él

Titokzatos metaprofilok

Fogalmunk sincs, mi folyik a háttérben


Befolyásolhatjuk-e az adattestünket?
CHEEZ-IT


Neknomination

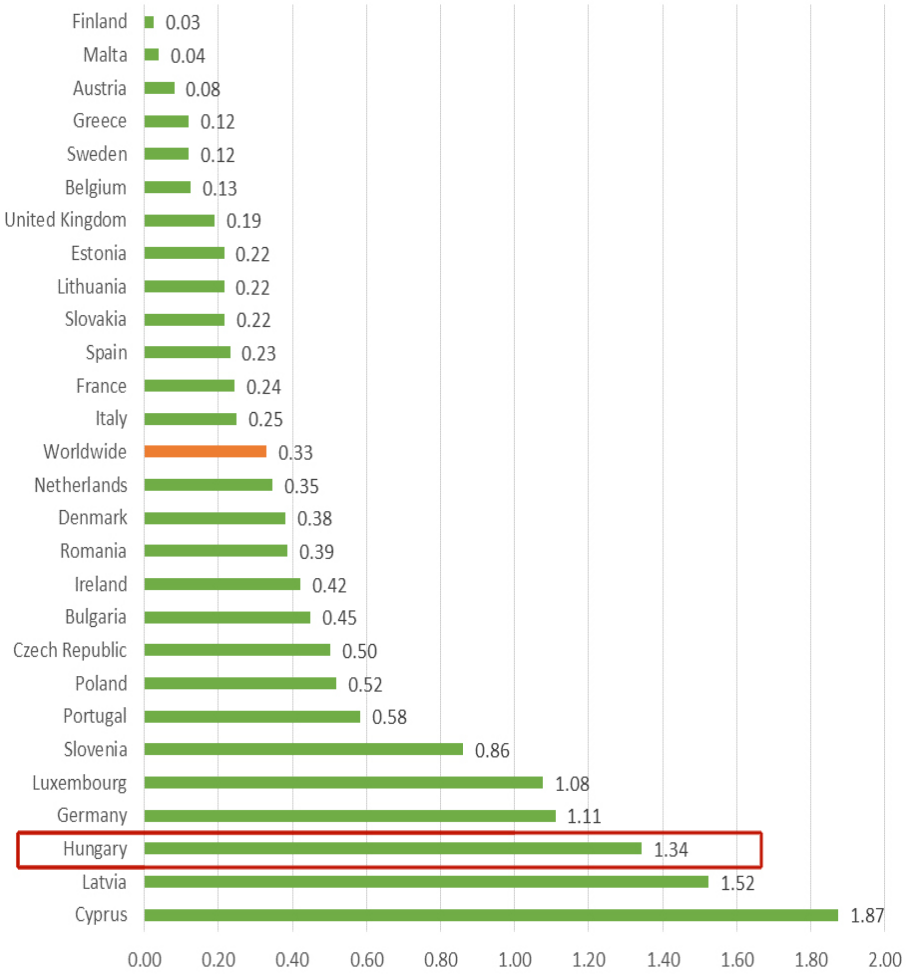

Virtuális valóság


Egyszerűbb, mint gondolnánk!

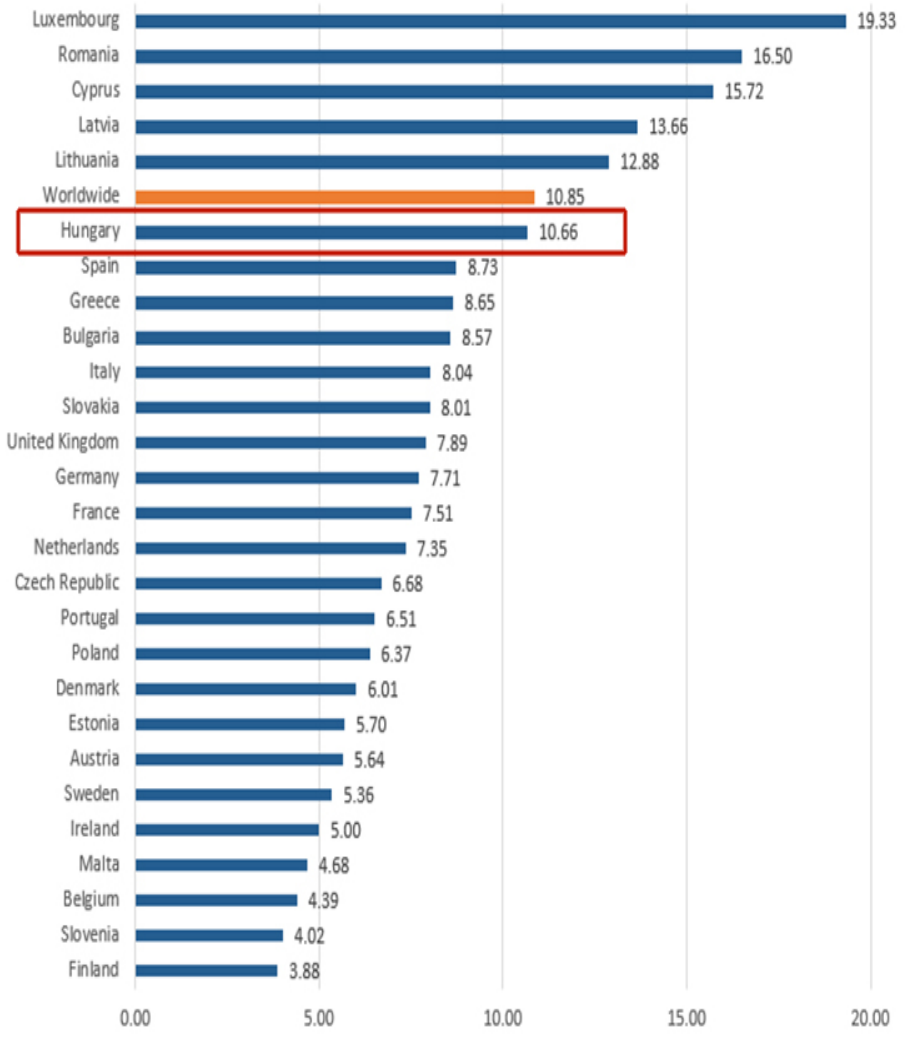

OP-ISRAEL

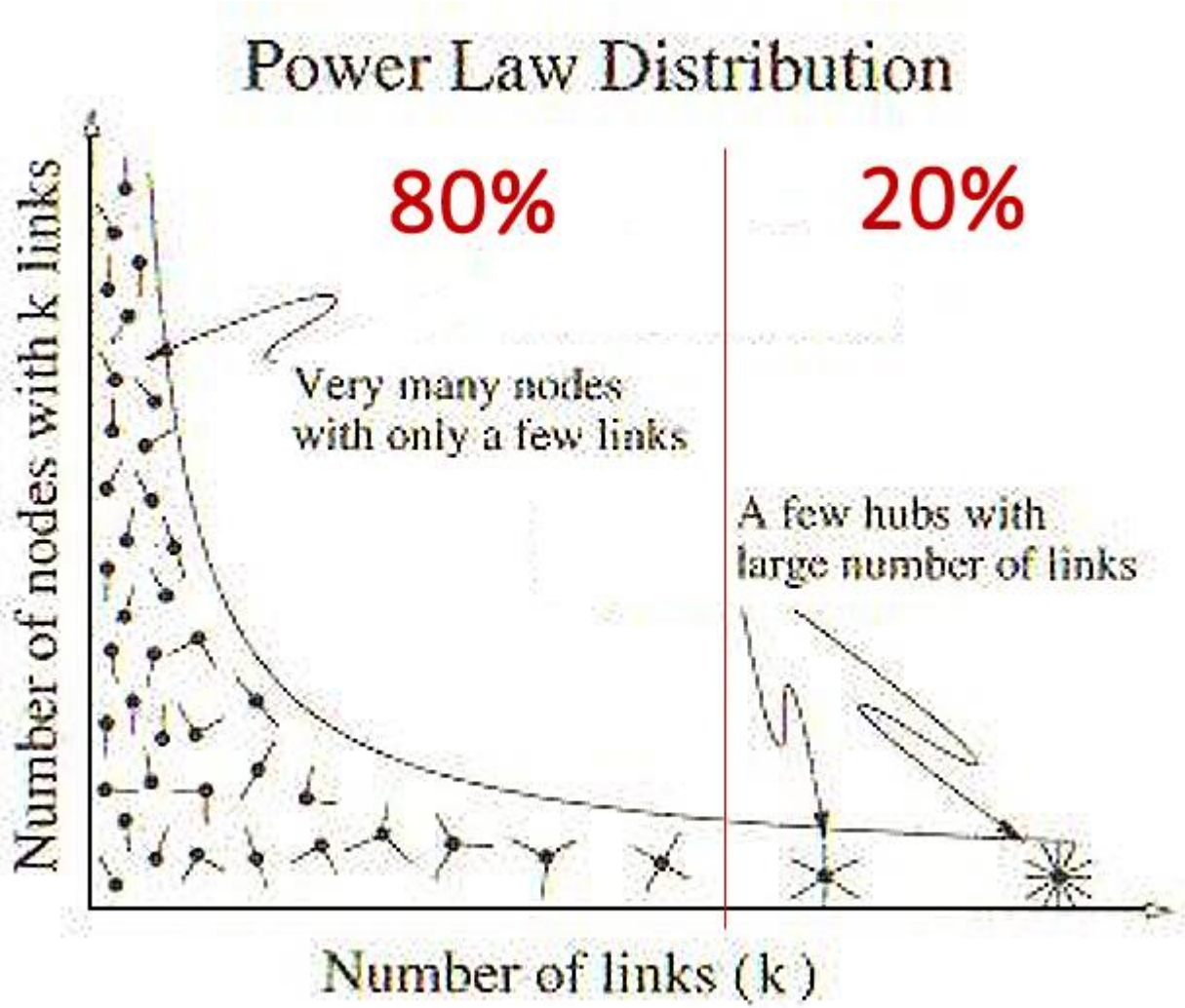

Advanced Persistent Threat

Drive-by download pages per 1000 URLs in the EU in 4Q12



Malware distribution sites per 1,000 Internet hosts in the EU in 4Q12

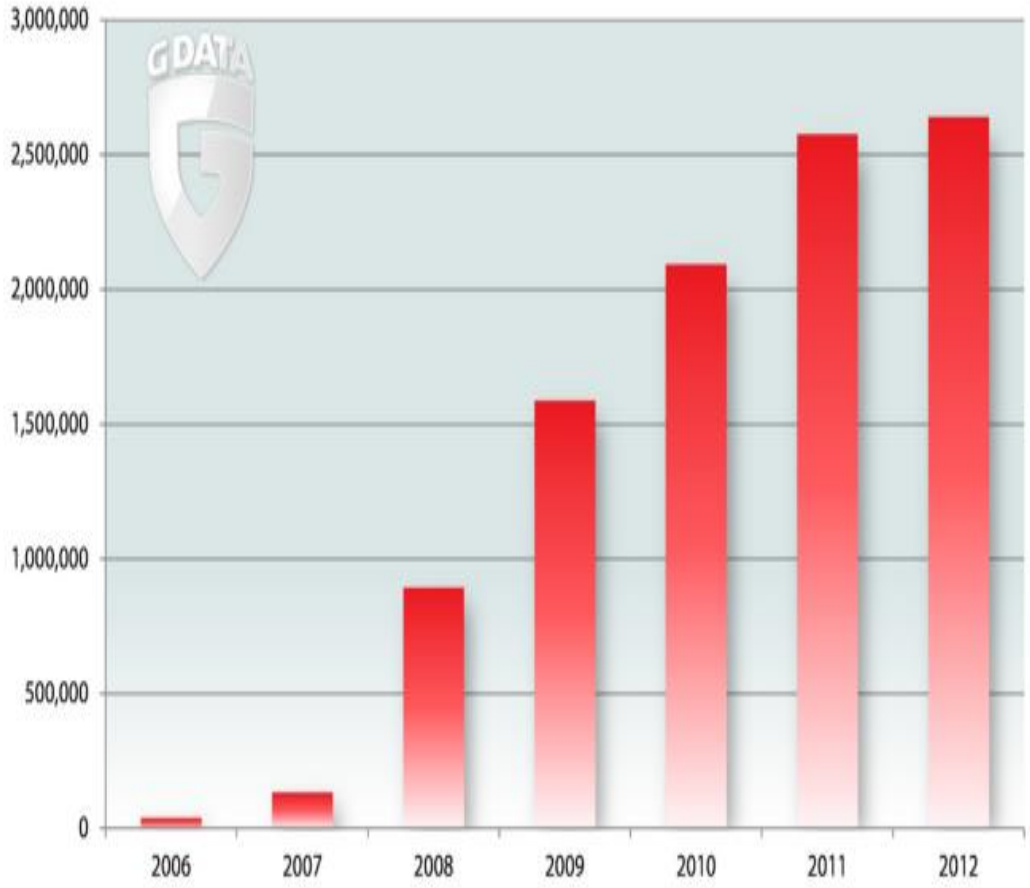



Power Law Distribution
80%
20%
Very many nodes
with only a few links
A few hubs with
large number of links
Number of nodes with k links
Number of links (k)

KIBER TÁMADÁSI TRENDEK

- Célzott támadások
- Új hírszerzési technikák
- Russian Business Network
- Állami szponzoráció

Malware –ek és az APT (Advanced Persistent Threat)



Általános megközelítés:

- REAKTÍV: a probléma bekövetkezése utáni eseménykezelés

Problémák:

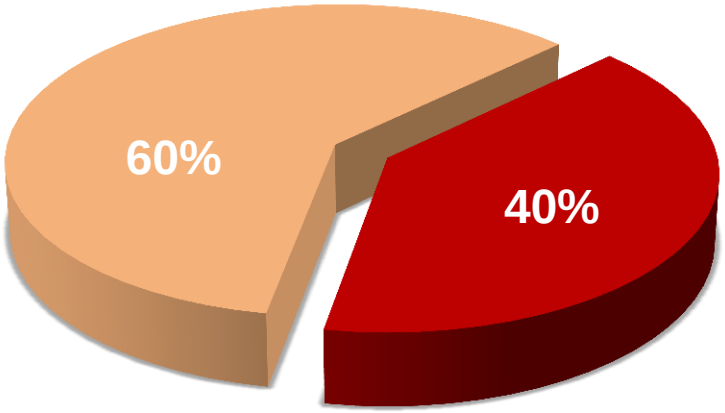
- Sodródás
- Információ szivárgás
- Hatalmas költségek

Kibervédelmi megközelítés:

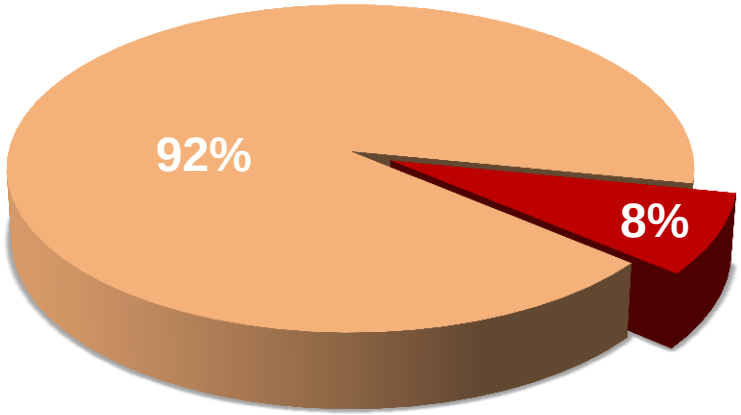
- PROAKTÍV: sérülékenység monitorozás a teljes IT rendszeren
- PREVENTÍV:sérülékenységek javítása

„Nincs pénz a kritikus sérülékenységek javítására!”

Preventív intézkedések előtt



Preventív intézkedések után



Az együttműködés elve

Stratégiai döntéshozatal	Megelőzés	Üzemeltetés, auditálás	Reagálás	Oktatás, tudatosítás
• Tanács •Egyeztetés a szektorok között	•KIM-NBF •Sérülékenység manaement •Forensics •Awareness	•NFM, KIM-NBF •Osztálybasorolás •Ellenőrzés •Esemény gyűjtés és monitoring	•BM •GovCERT •Koordináció •Esemény elemzés •Vészhelyzet kezelés •Tájékoztatás •KIVCSIRT •Esemény elemzés •Vészhelyzet és Incidens kezelés •HM •MilCert •Esemény elemzés •Vészhelyzet és Incidens kezelés •SzakCertek	• NKE • KIM-NBF •.Pannon Egyetem


Hátsó ajtó? Nálunk? Kizárt!
D-Link


Megoldás?

Personal vulnerability

A személyes sérülékenység csillapítása