Cukorkakeményítés

Megerősítő védelmek kliens oldali támadásokkal szemben

DISCLAIMER

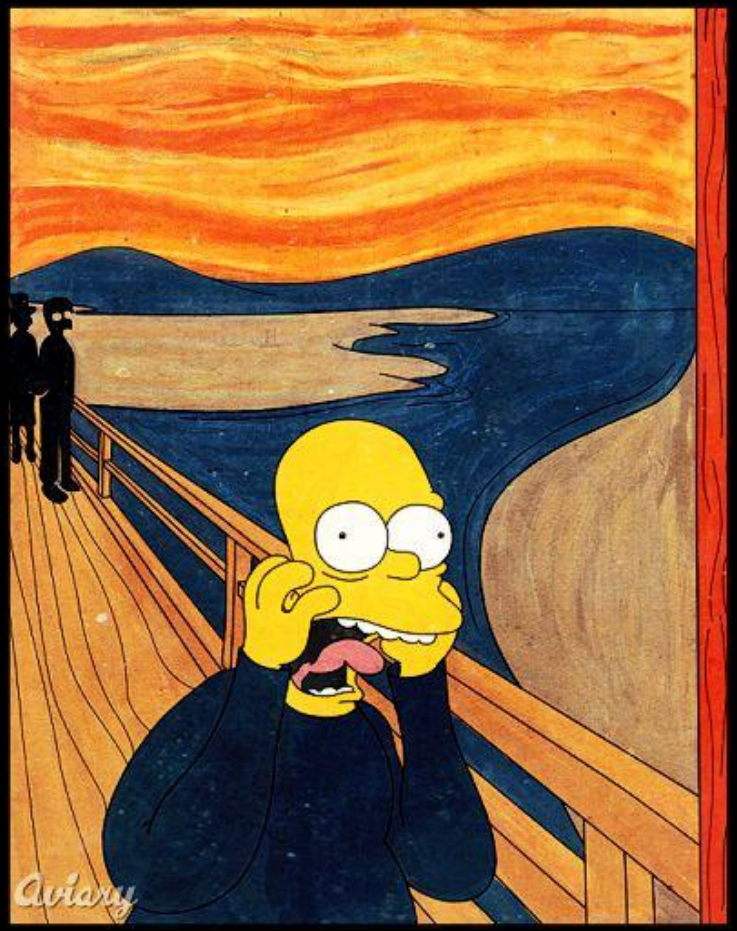
Cukorka biztonság

A rendszer határait megfelelően megvalósított, nehezen kijátszható biztonsági korlátok védik, a rendszeren belül hasonló védelem azonban nem érvényesül.

Helyzetjelentés

- A támadók módszerei folyamatosan fejlődnek
- A védekezés általában >=5 éves módszerekkel történik
  - Használj AV-t
  - Használj tűzfalat
  - Használj IDS/IPS rendszert
  - ???
- Nem a valódi fenyegetések ellen védekezünk!

Eredmény



- Google
- EMC/RSA
- Lockheed-Martin
- Boeing
- Illinois EPA BoW
- .no
- .ir
- **.hu?**

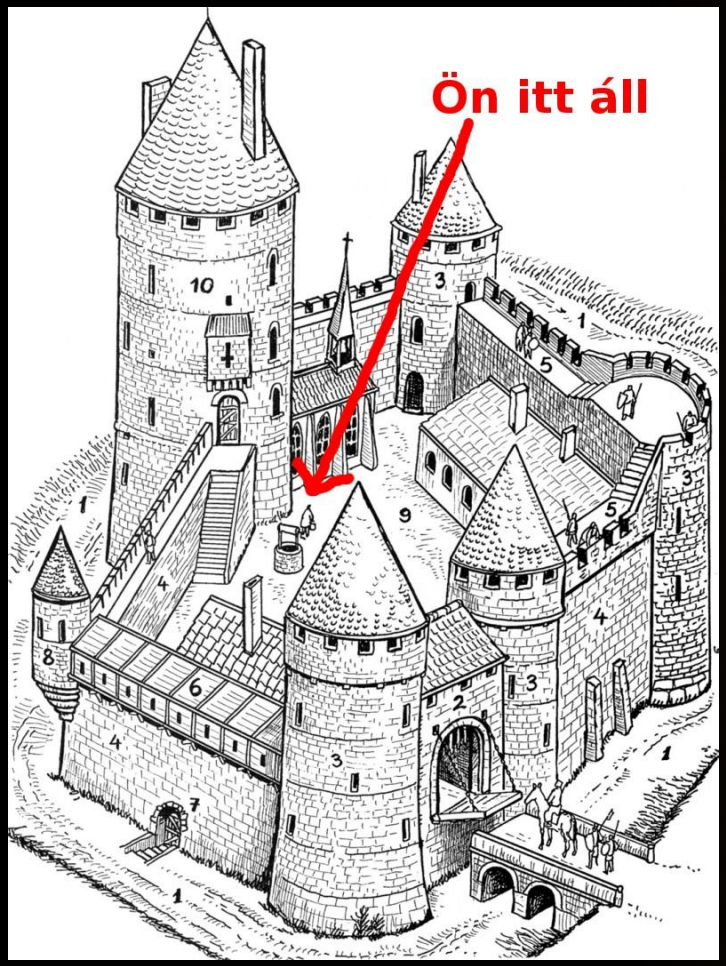
Miért?

- "Az alkalmazottaink megbízhatóak"
- "Az alkalmazottaink biztonságtudatosak"
- "A rendszerünk fizikailag szeparált"
- "Monitoring van"
- X termék nagyon drága => X termék nagyon jó

Kliens-oldali támadások

- Beviteli csatornák
  - E-mail – Spear phishing
  - CD/DVD/pendrive
    - Autorun.inf
  - WWW / Drive-by-download
    - QR-code :)
  - Közösségi oldalak
  - Instant messenger

Alapprobléma



SILENT SIGNAL
VÉSZJELZÉS HELYETT...

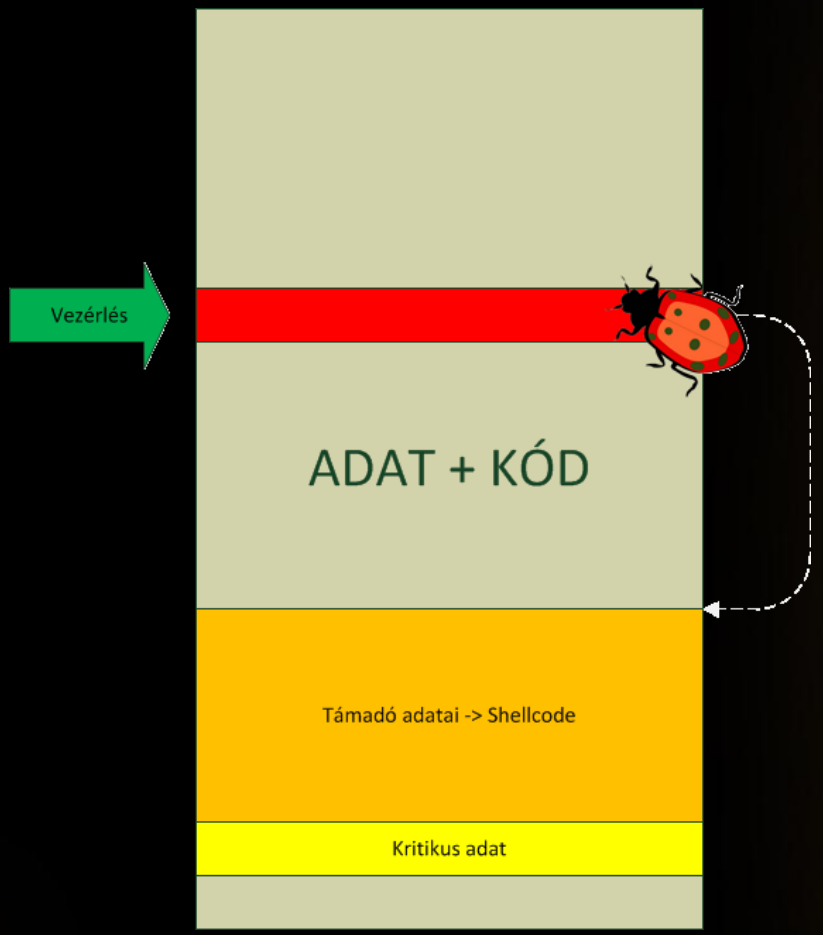
WWW.SILENTSIGNAL.HU

Szoftver célpontok

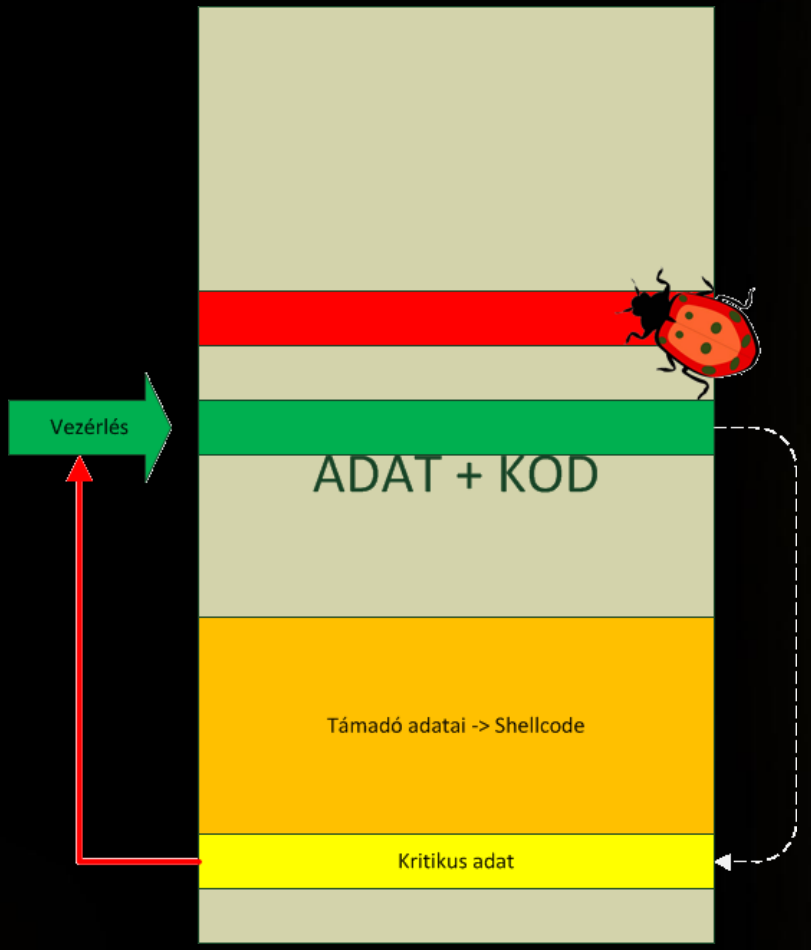
- Adobe Flash
- Oracle Java
- Adobe Reader (PDF)
- Webböngészők
- Microsoft Office alkalmazások
- … és ezek lineáris kombinációi

Gyorstalpaló

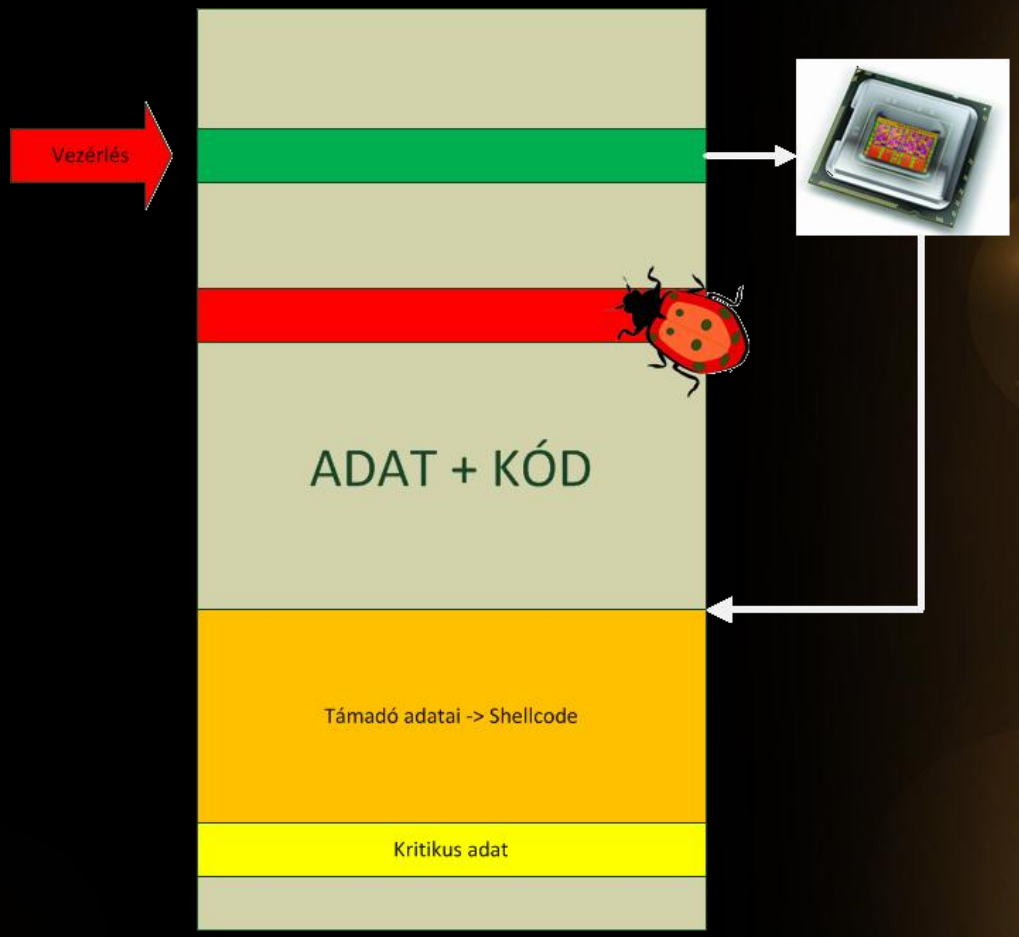
Gyorstalpaló



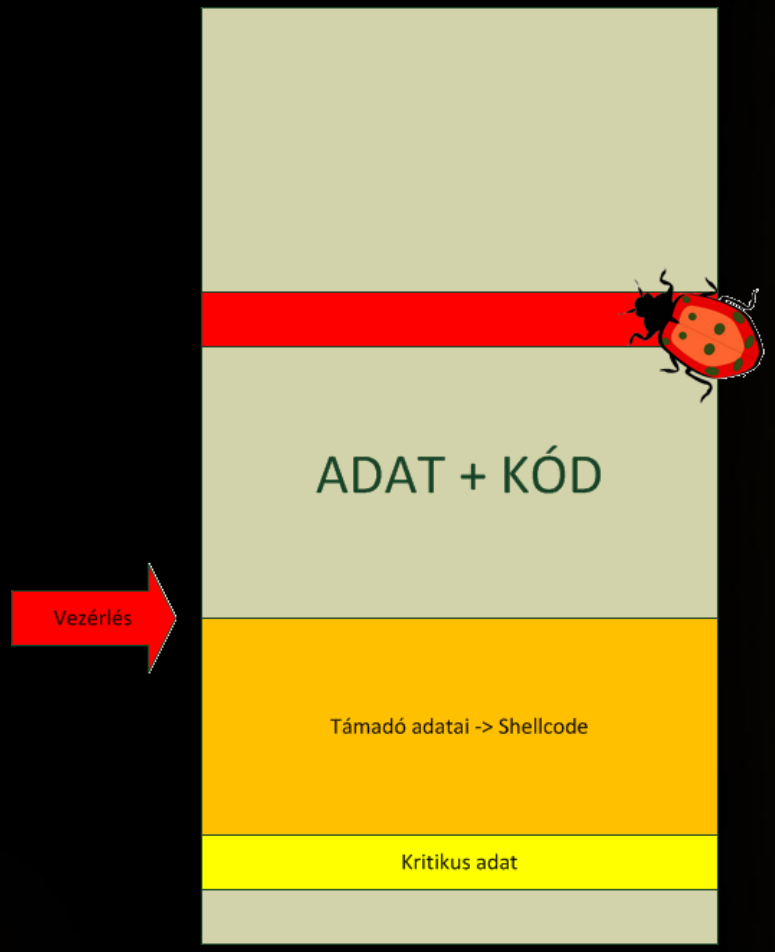
Gyorstalpaló



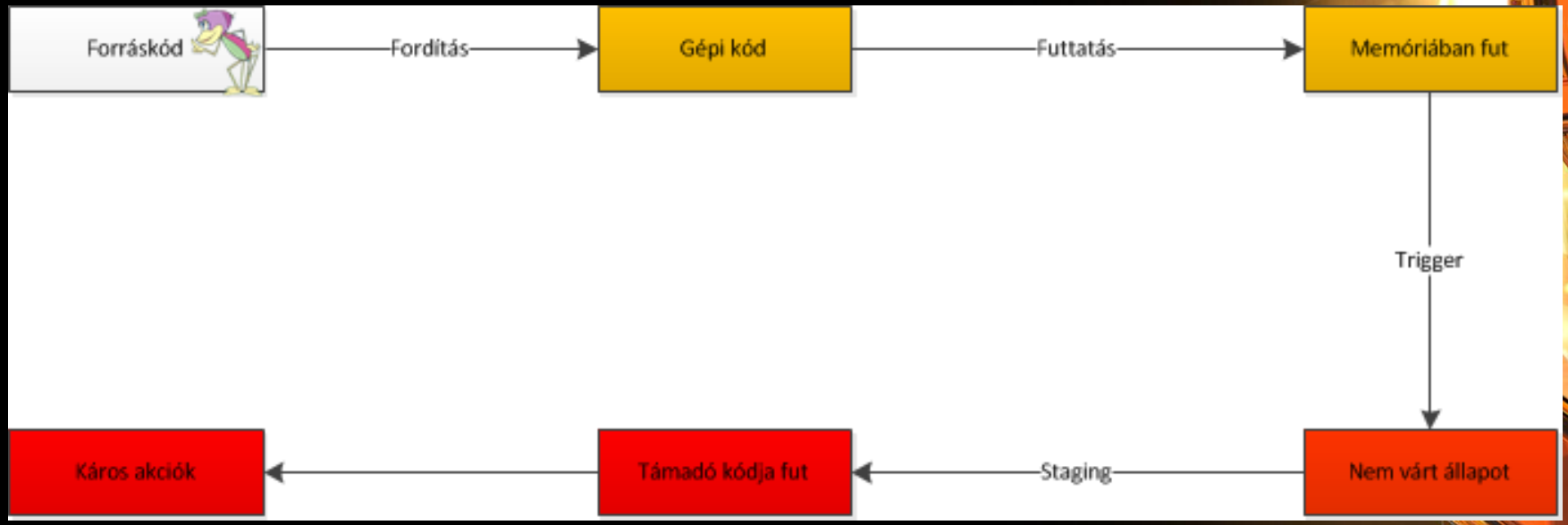
Gyorstalpaló



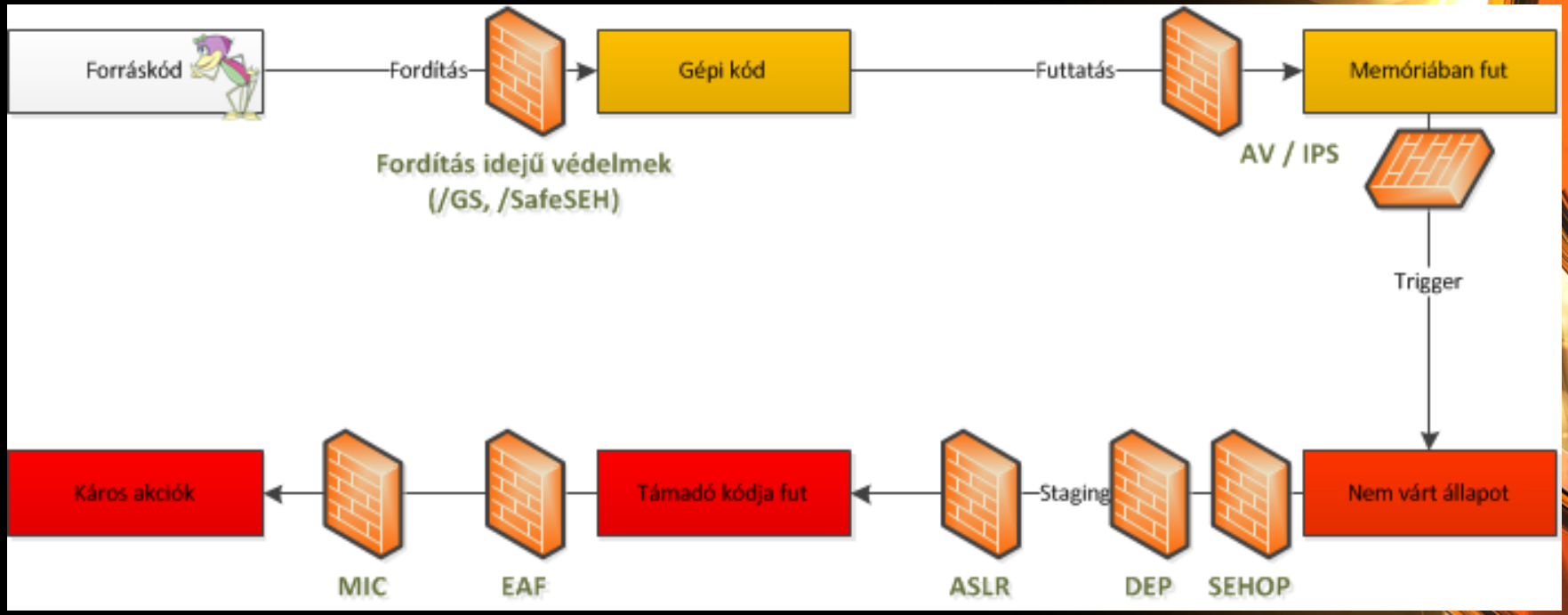
Gyorstalpaló



Kihasználási folyamat



Megerősítések



Cél: A támadás költségének növelése

Fordítás idejű védelmek

- Tipikus hibák eliminálása
- Plusz kód/adat generálása futásidejű hibadetektáláshoz
- Teljes hibaosztályokra hatástalan
- A gyártó felelőssége, hogy alkalmazza
- Néha maga a fordító vezeti be a hibát!

AV/IPS

AV/IPS

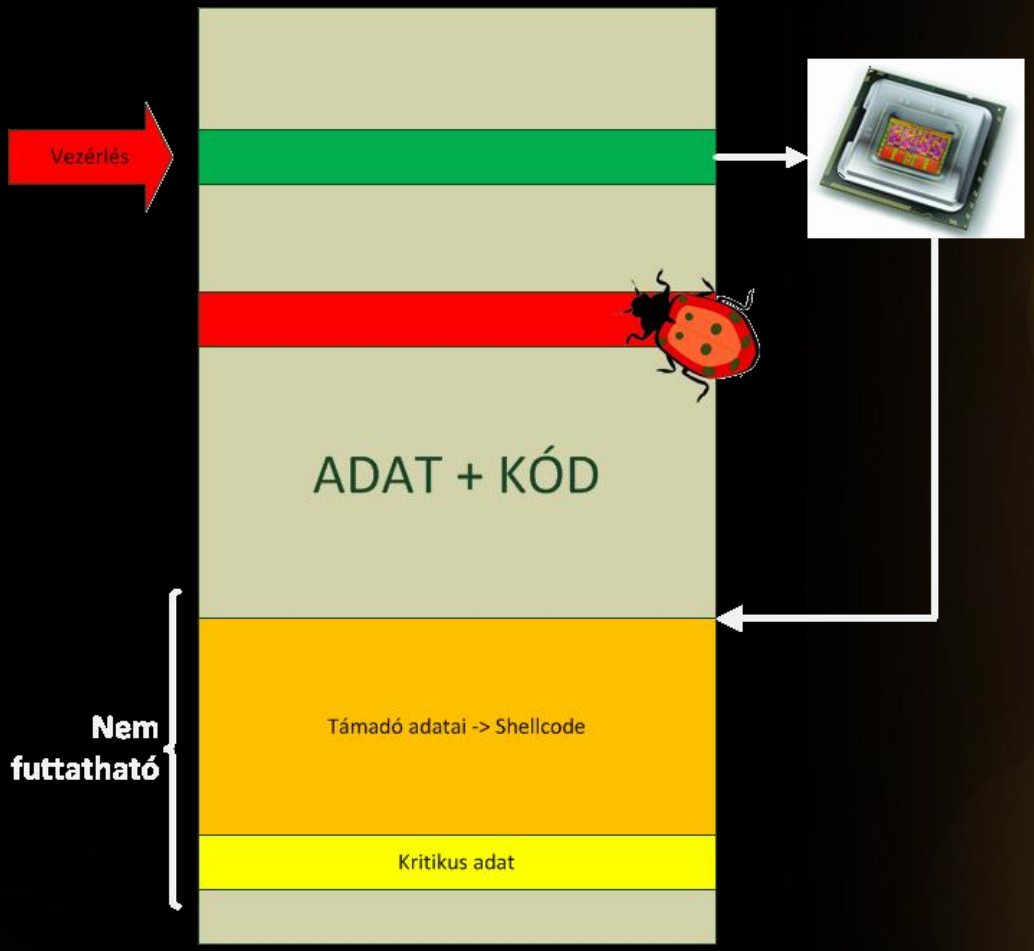
- Még mindig nagyrészt szignatúra alapon
- We are the 1%...
- Mi van, ha a biztonsági szoftverem hibás?

FUTÁS IDEJŰ VÉDELMEK

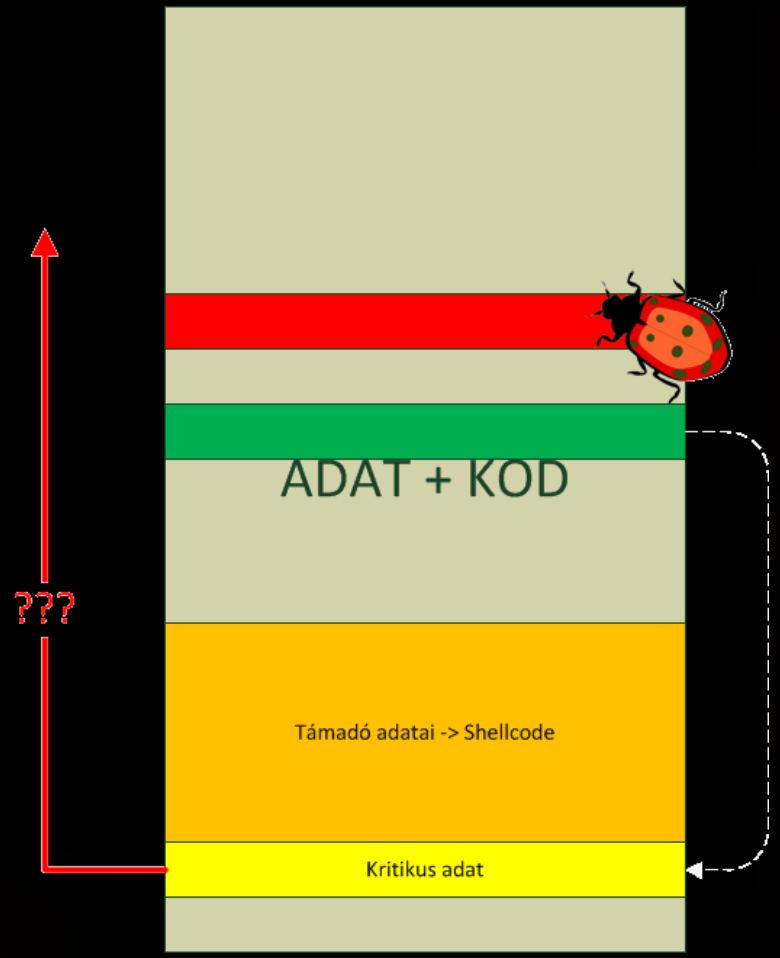
SILENT SIGNAL
VÉSZJELZÉS HELYETT...

WWW.SILENTSIGNAL.HU

Data Execution Prevention

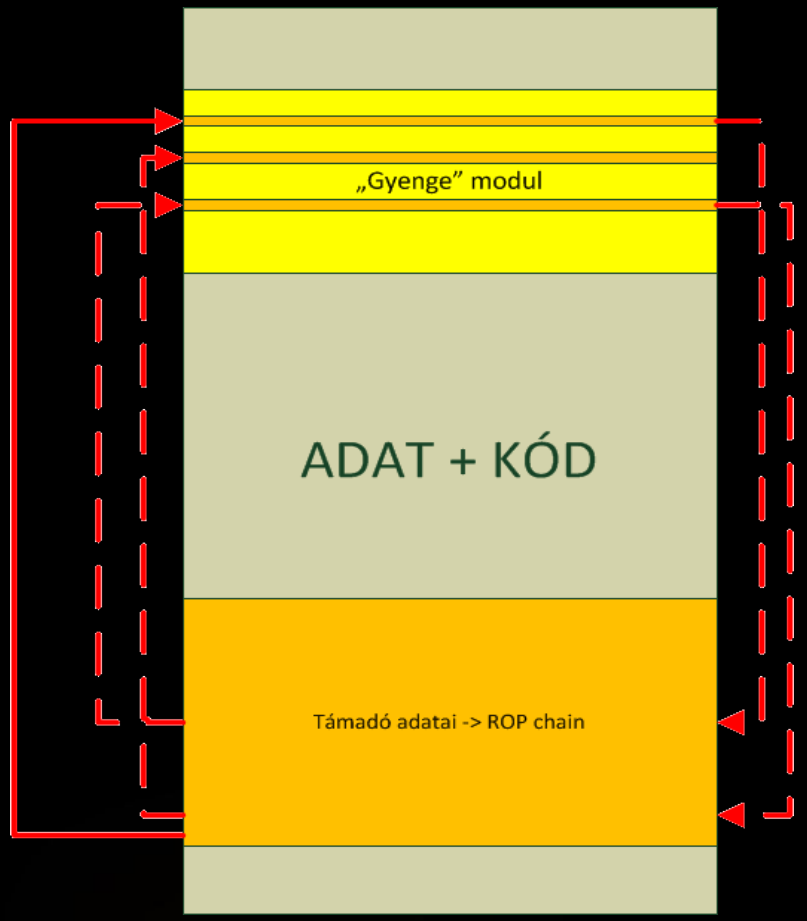


Address Space Layout Randomization



>= Vista

ASLR + DEP



- Az exploit fejlesztésre fordítandó idő megnövelhető
- "Exploitation Best Practictces"
  - Heap spraying
  - Msvcrt71.dll
  - Return Oriented Programming
- Logikai hibák ellen nem véd

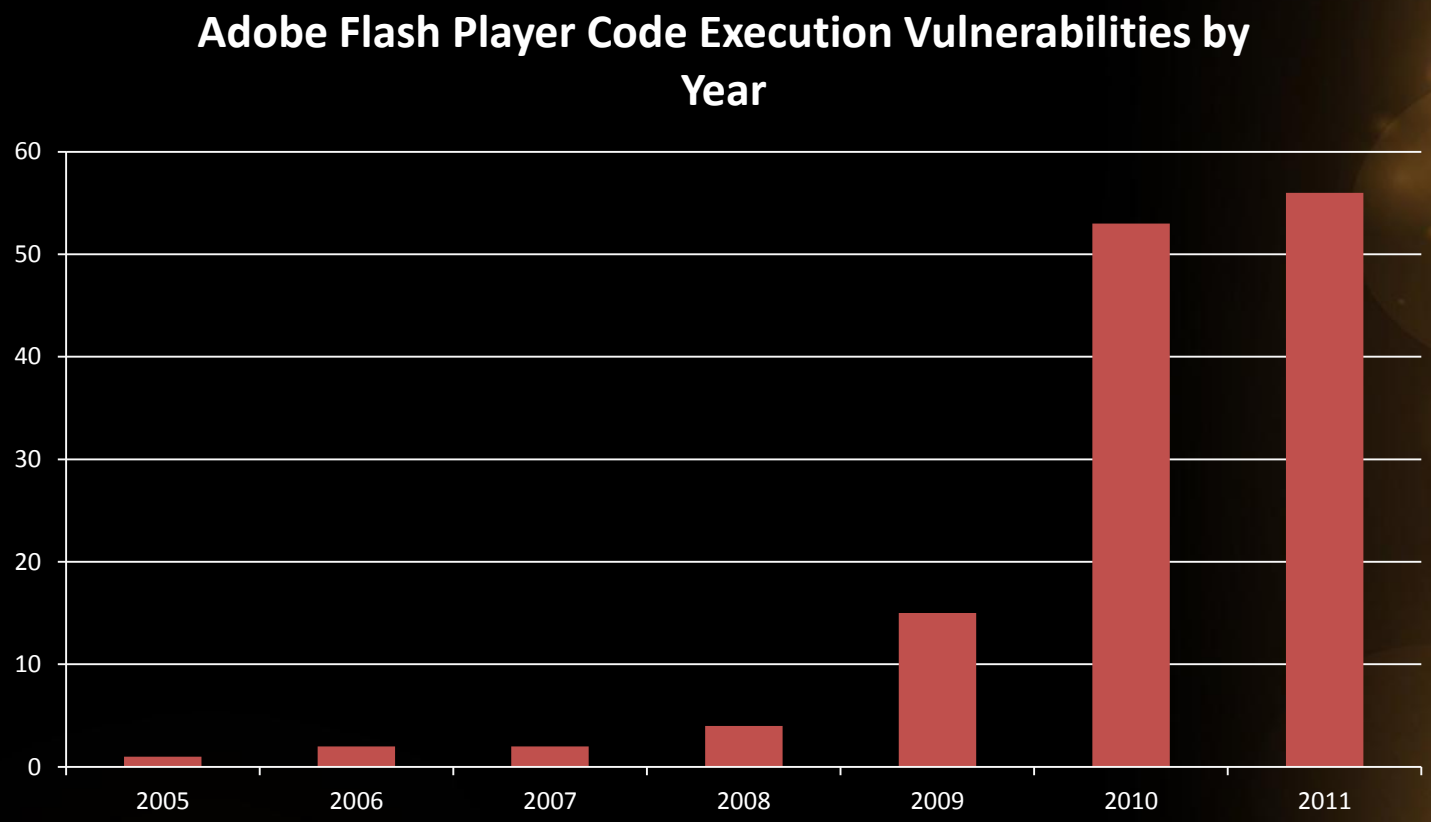
Mandatory Integrity Control

- Ha minden kötél szakad…
- Securable objects
  - Fájlok/könyvtárak
  - Csővezetékek
  - Folyamatok
  - Registry kulcsok
  - Stb.
- Integritási szintek
  - Alacsony, Közepes, Magas, Rendszer
- >= vizsgálat
- Vistától

Mandatory Integrity Control

- Meglepően hatékony
  - Akár logikai hibák ellen is
- Nem minden sandbox egyenértékű
- Megkerülés általában több hiba láncolásával
  - Nagyságrendi változás!
- >= Vista

Adobe Flash



Source: cvedetails.com

mms.cfg

- Adobe Flash Player Administration Guide
- Néhány érdekes paraméter:
  - AllowUserLocalTrust
  - DisableNetworkAndFilesystemInHostApp
  - DisableSockets
  - FileDownloadDisable
  - FileUploadDisable
  - ThirdPartyStorage

C:\Windows\System32\Macromed\Flash\

Recurity Labs - Blitzableiter

- Német Információbiztonsági Hivatal
- "Normalization through Recreation"
- Menedzselt kód
- Működési módok:
  - Parancssor
  - Firefox kiegészítő (NoScript)
  - Proxy (Squid)

Internet Explorer - Múlt

Internet Explorer 6

- Hosszú ideig piacvezető
- Kompatibilitási problémák
  - "Microsoftos internet"
  - Vendor lock-in
- Nincsenek megerősítések

Internet Explorer - Jelen

- Böngésző biztonság => Presztizskérdés
- Állatorvosi ló => Mintajószág
  - MIC
  - DEP (>=IE8)
  - ASLR (>=IE8)
  - SEHOP (>=IE9)
  - /SafeSEH (>=IE9)
- Flash Védett Módban
- IE6 még mindig támogatott…

Internet Explorer - ActiveX

*"**ActiveX** is a framework for defining reusable software components in a programming language-independent way"*

- 1996 –
- Killbitek napjainkig
- Windows Update -> Kigyilkolhatatlan
- Jelenleg 0-day: MS XML Core Services Uninitialized Memory Corruption (CVE-2012-1889)

DEMO

Kitérő: Immunity El Jefe

- "Központosított Process Explorer"
  - Adatgyűjtés
  - Monitorozás
  - Korreláció
- *"Miért nyitott meg az IE egy tftp.exe-t?"*
- Skálázódás?
- **Nem megelőzés!**

Google Chrome

- Security by Design
  - FOSS => rövid kiadási ciklusok
- Új piacvezető
- Védett Mód
- Saját Flash Player sandbox
  - \+ Fuzzing
- Saját PDF olvasó
- Saját média lejátszó

Mozilla Firefox

- ASLR+DEP van
- Védett mód nincs
- FF13-tól Flash védett módban
- NoScript
  - http://noscript.net
- Kiegészítők kezelése?
  - Public Fox?

Office alkalmazások

- ~= Internet Explorer
- Védett mód *megbízhatatlan forrásból származó* alkalmazások

esetén

  - NTFS – Attachment Execution Services
  - **Példa**
  - Group Policyból konfigurálható
    - <Office App 2010>\<App> Options\Security\Trust Centre\Protected View
- Beágyazható OLE objektumok
  - Flash

PDF

- Portable Document Format
- Szintén Adobe szabvány
- Néhány "létfontosságú" funkció:
  - Flash beágyazás
  - JavaScript
  - 3D rendering
  - Tetszőleges parancsfuttatás
- Ajánlott előadás:
  Julia Wolf - OMG WTF PDF (27C3)

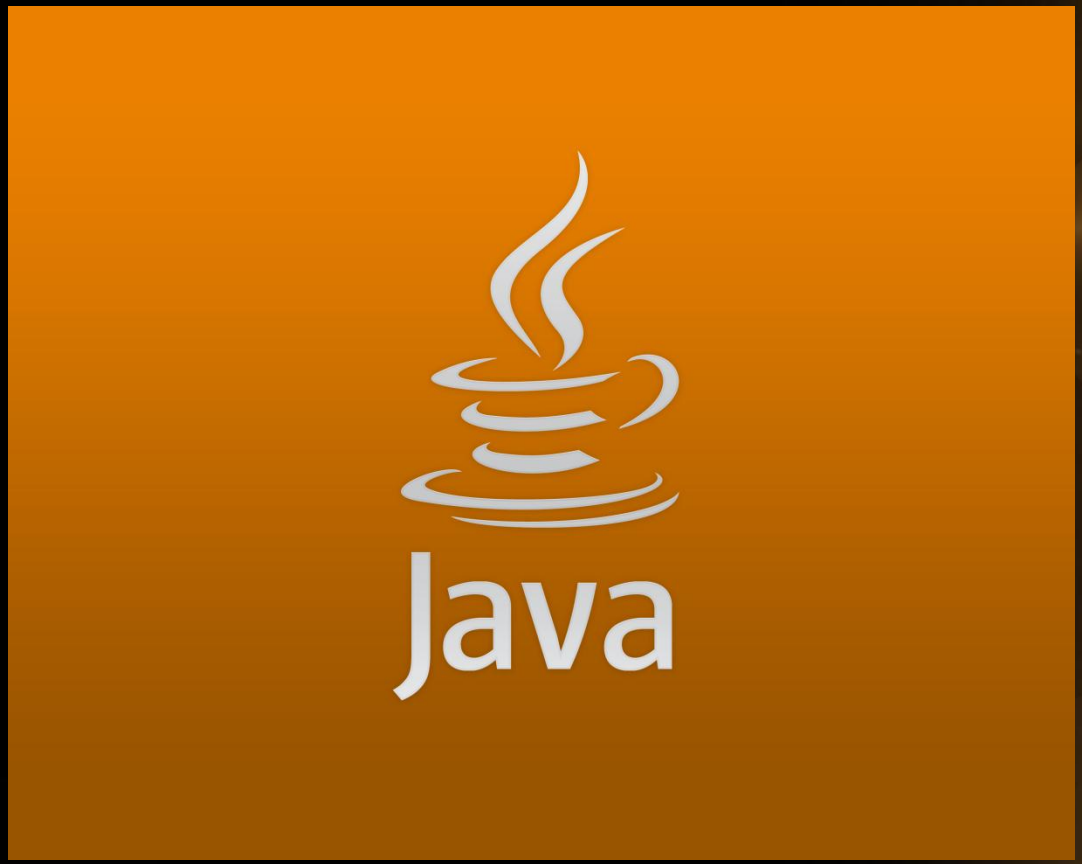
Adobe Reader

- Bugbánya
  - LOC(Adobe Reader) ~= 6 LOC(Firefox)
- 9.5.1-től
  - Nincs saját Flash lejátszó (authplay.dll)
  - 3D renderelés alapértelmezetten kikapcsolva
- Adobe Reader X – Védett Mód (>=Vista)
  - Fájlolvasás lehetséges
  - Hálózati hozzáférés lehetséges
  - Vágólap használható

Foxit Reader

- Biztonságosabb alternatíva?
  - Elterjedtség
- Védett mód nincs
- Safe Reading Mode
  - JavaScript letiltva
  - EXE futtatás korlátozva
  - Linkek nem nyílnak meg automatikusan

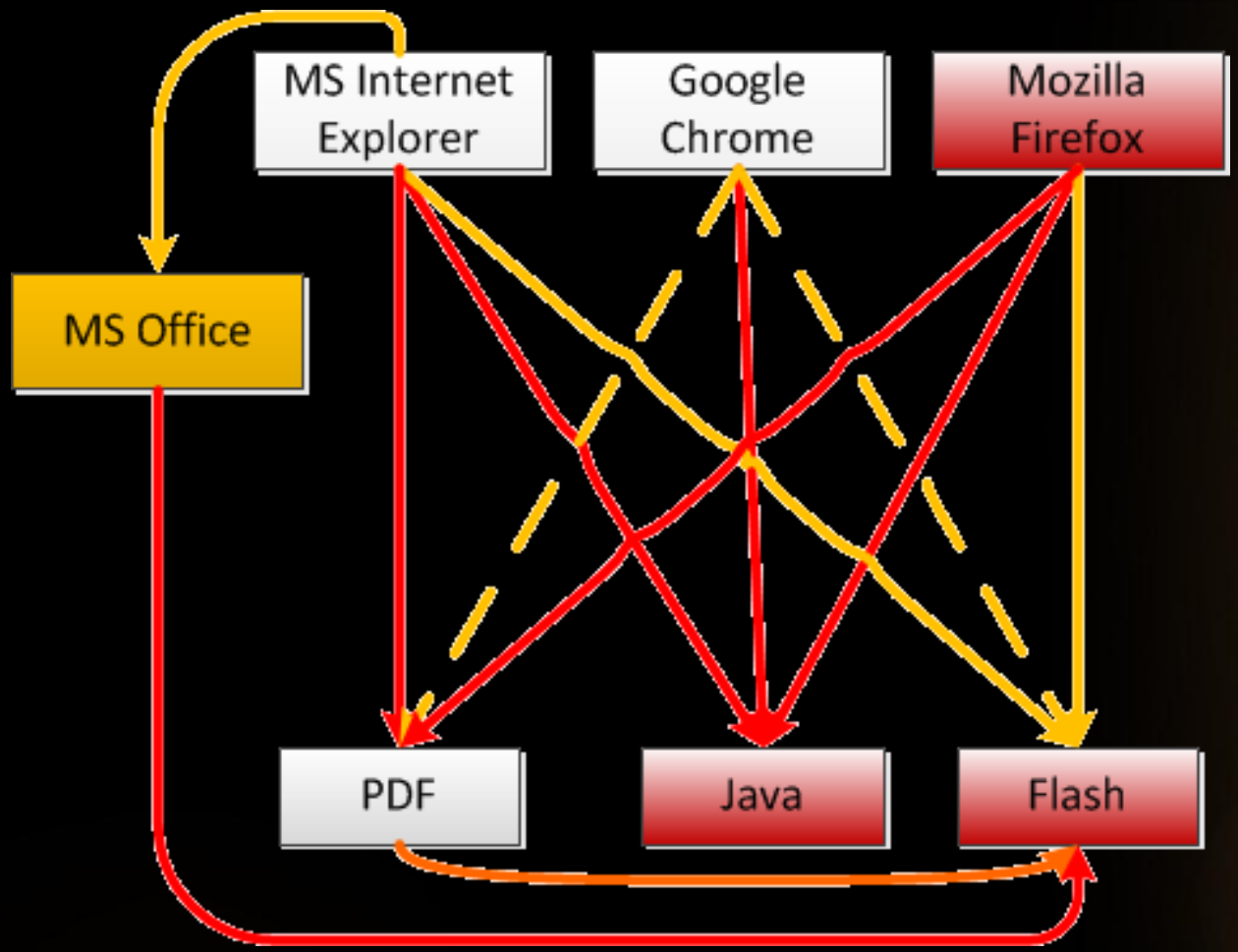
A feketeleves



Java

- Nagyon elterjedt
- Célbajuttatás weben (appletek)
- Általában elavult verziók
  - Kompatibilitás
- **Tervezési hibák**
  - A memória védelmek hatástalanok!
- Multiplatform támadások
  - DEMO

Egy kis gráfelmélet :)



Egyéb szoftverek

- Céleszköz
  - CAD
  - SCADA
  - Médialejátszó
  - Stb.
- Saját fejlesztés

Microsoft EMET

- Enhanced Mitigation Experience Toolkit
- Alkalmazás/rendszer szintű védelmi policy-k beállítása
- Védelmi funkciók backportolása
  - Ha lehetséges
- Új védelmek tesztelése

Microsoft EMET

	Mitigation	XP	Server 2003	Vista	Server 2008	Win7	Server 2008 R2
System Settings	DEP	Y	Y	Y	Y	Y	Y
	SEHOP	N	N	Y	Y	Y	Y
	ASLR	N	N	Y	Y	Y	Y
Application Settings	DEP	Y	Y	Y	Y	Y	Y
	SEHOP	Y	Y	Y	Y	Y	Y
	NULL Page	Y	Y	Y	Y	Y	Y
	Heap Spray	Y	Y	Y	Y	Y	Y
	Mandatory ASLR	N	N	Y	Y	Y	Y
	EAF	Y	Y	Y	Y	Y	Y
	Bottom-up	Y	Y	Y	Y	Y	Y

Source: EMET User's Guide

Microsoft EMET 3.0

- Terítés: System Center Configuration Manager
- Konfiguráció Group Policyból
- Reporting: EMET Notifier
- DEMO

Tanulságok

- Bugok vannak és lesznek
  - Nagy SW => Sok bug
- Univerzális 0-day védelem *nem létezik*
- Kulcsra kész megerősítő megoldások *léteznek*
  - "Ingyen"!
- Biztos alapok nélkül nincs győzelem
- A támadó racionális játékos, nehezítsük meg a dolgát!

Köszönöm a figyelmet!

e-mail

Facebook

vpbalint@silentsignal.hu

web

Linkek

- Immunity El Jefe: http://eljefe.immunityinc.com
- Flash Player Administration Guide: http://www.adobe.com/devnet/flashplayer/articles/flash_player_admin_guide.html
- Blitzableiter: http://blitzableiter.recurity.com
- Defending the Poor (Blitzableiter): http://www.youtube.com/watch?v=cmhK1g5QU
- NoScript: http://www.noscript.net
- Public Fox: https://addons.mozilla.org/en-US/firefox/addon/public-fox/
- OMG WTF PDF: http://www.youtube.com/watch?v=54XYqsf4JEY
- Microsoft EMET: http://support.microsoft.com/kb/2458544