

# Hackertámadások a Távol-Keletről



Készítette: Serege Gábor fhdgy.

- 2010 -

# Előadásom főbb pontjai

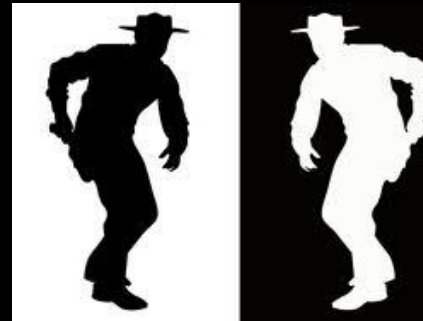
- „([Hacker])”???
- Az elmúlt évek „termése”.
- Ki áll a háttérben?
- USA doktrina
- Összegzés



# Ki az a Hacker?

- **A múltban:** nagy tudású szakember, aki munkáját művészi gondossággal űzi
- **Most:** olyan személy, aki képes bejutni a különböző informatikai rendszerekbe

- Fehér kalapos (Etikus)



- Fekete kalapos

- [„Script kiddie”]



# 2007

- **Június:** SecDef levelezőrendszer, 1500 PC (offline),

- **Szeptember:**

- Berlin (office-backdoor)
- GB (külügy)



- **Október:** USA Nemzeti Laboratórium (email 1100 alkalmazottnak)



# 2008

- **Március:** ausztrál titkosszolgálat
- **Május:**
  - belga kormányzat
  - Carlos Gutierrez laptop másolási botrány
- **November:**
  - Fehér Ház
  - USA ARMY, NASA, stb...
- **December:** francia követségek (Dalai Lama)



# 2009

- Március: Fülöp-szigetek
- Április:
  - Németország
  - Ausztrália
  - Dél-Korea
- Május: Észak-Korea: „Kiberhadtest”
- December: Google



## Top malware-hosting countries

Position	Last month	Country	Percentage of reports
1	1	China (inc. HK)	44.8%
2	2	United States	20.8%
3	3	Russia	11.3%
4	4	Ukraine	7.7%
5	8=	Poland	2.4%
6	5	Germany	1.6%
7	Re-entry	Netherlands	1.1%
8	Re-entry	Italy	0.9%
9=	8=	Canada	0.8%
9=	7	United Kingdom	0.8%
Others			7.8%

# HACKER



# Ki áll a háttérben?

- Németek: a támadások 60%-a kínából származik (Peking, Lanzhou, Guangdong)
- Új-Zélandia: a belső titkosszolgálati jelentés → a kínai vezetésnek igenis van köze a támadásokhoz
- MI5: állami vezetők és polgári vállalatok figyelmeztetése a kínai kémkedésre
- India: „mindennapos Kínai támadások”

# HACKER



# Ki áll a háttérben?



- 2009: Information Warfare Monitor felfedi a GhostNet létezését: 103 ország, 1300 célpont. A rendszer irányítása a kínai Hainan szigetről. Lingshui SIGINT



# HACKER

# **CYBERSPACE OPERATIONS**



**Air Force Doctrine Document 3-12  
15 July 2010**

# „Védeni a hálózatunkat és az országunkat” Gen Norton A. Swartz

- Az USA potenciális cyber célpont 24/7
- Az „ellenség” folyamatosan helyez el ártalmas kódokat weboldalakra, usb kulcsokra stb..
- Az „ellenség” egyaránt megjelenhet a munkahelyi és az otthoni hálózatban is.
- Ne nyiss meg „gyanús” csatolmányokat!
- Ne csatlakoztass, ne installálj, ne tölts le zenéket.... 😊

# Összegezve

- Növekvő hálózatok, növekvő cyber-bűnözés
- Kínai „hacker-paradicsom”
- Egyre képzettebb kínai hackerek
- Számos ország teszi felelőssé a kínai vezetést
- Kína teljes mértékben tagad
- USA Cyberspace Operations





[serege.gabor@zmne.hu](mailto:serege.gabor@zmne.hu)