La criminalità su Internet e la sicurezza applicativa

V.Q.A. Tommaso Palumbo

Responsabile CNAIPIC

ORGANIZZAZIONE E COMPETENZE DELLA POLIZIA POSTALE E DELLE COMUNICAZIONI:

Dipartimento della Pubblica Sicurezza
Servizio Polizia Postale e delle Comunicazioni (Roma)

20 COMPARTIMENTI REGIONALI

76 SEZIONI TERRITORIALI

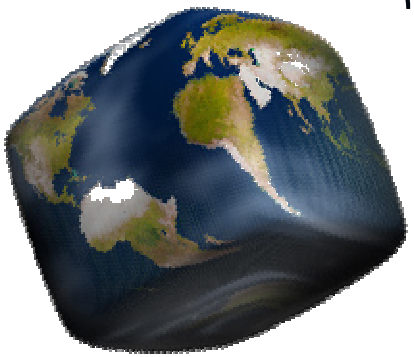
Forza effettiva **1854**

- Compartimenti Polizia Postale
- Sezioni della Polizia Postale

- *Pedofilia on-line*
- *Protezione infrastrutture critiche*
- *Cyberterrorismo*
- *Copyright*
- *Pirateria satellitare*
- *Sorveglianza del mercato (D.lgs 269/2001)*
- *E-Commerce*
- *Hacking*
- *Reati postali e falsi filatelici*
- *Controllo radio frequenze*
- *Giochi e scommesse on line (legge 266/'05)*
- *Collaborazione operativa con Forze di Polizia straniere (h. 24/7)*
- *Computer forensic*

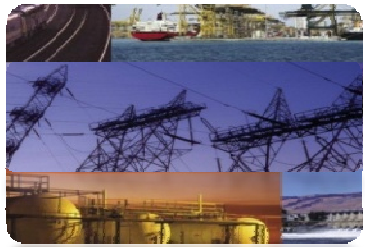
Le minacce di Internet

Crimini informatici



Utilizzo web per finalità terroristiche

Minaccia Globale



Attacco infrastrutture critiche

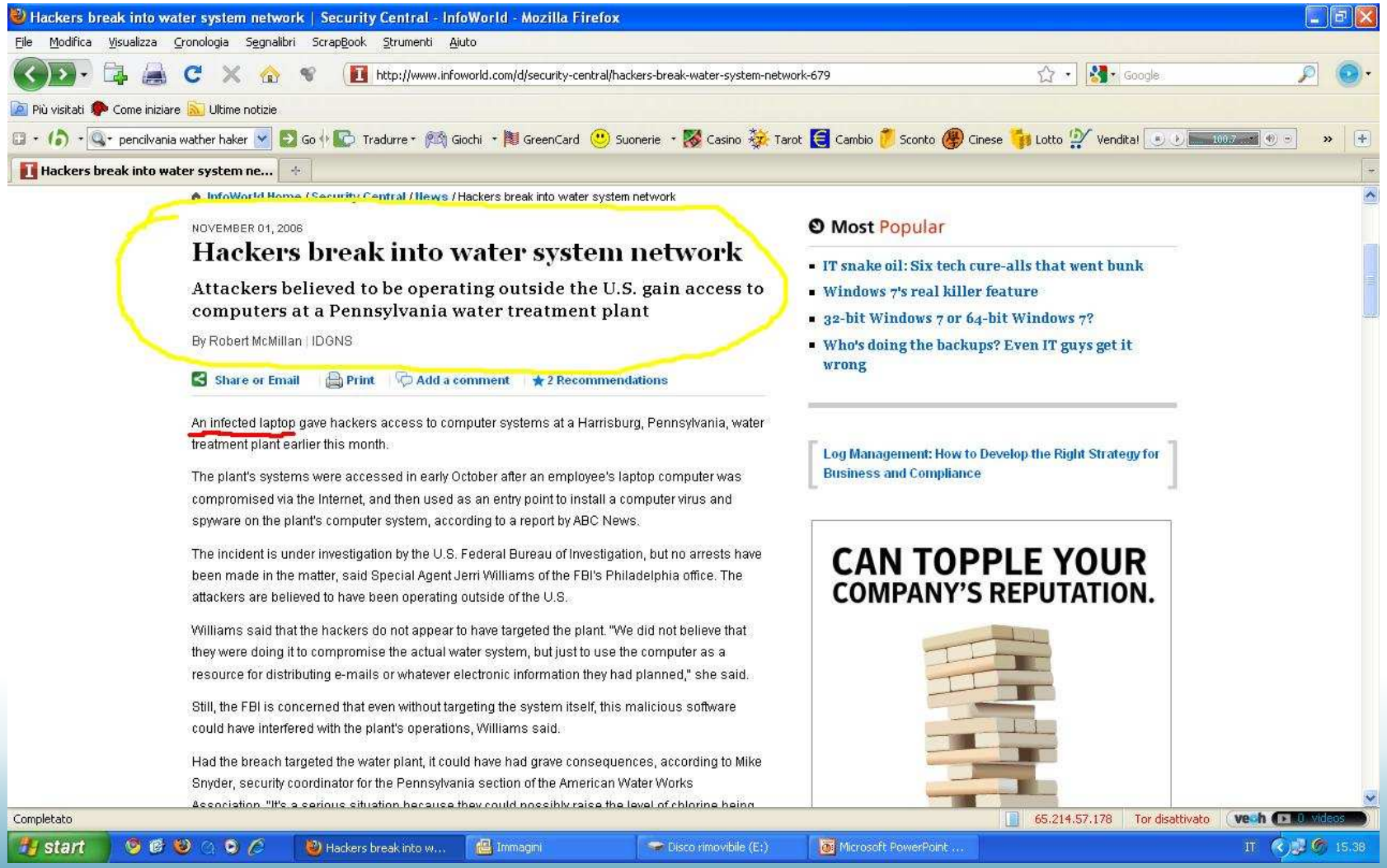
Abbiamo l’esatta percezione del pericolo?

Abbiamo l’esatta percezione del pericolo?

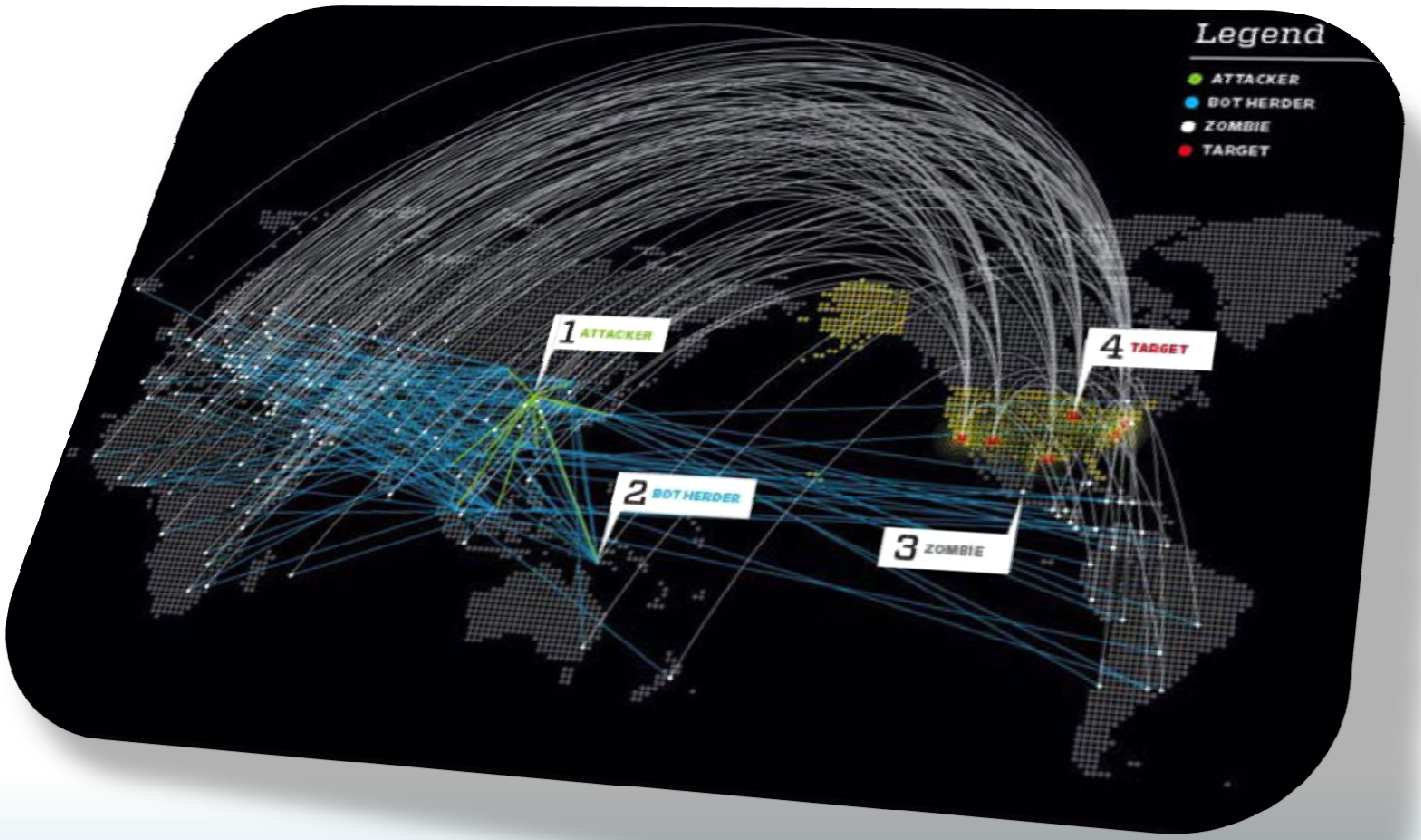
La network security basta?

Ne siamo sicuri?

Un piccolo esempio



BOT NET


Legend
ATTACKER
BOT HERDER
ZOMBIE
TARGET
1 ATTACKER
2 BOT HERDER
3 ZOMBIE
4 TARGET

Una possibile soluzione : WAPT

- Conoscenza dell’applicazione
- Ricerca delle vulnerabilità (approccio whitebox *versus* blackbox)
- Quantificazione del rischio per ogni singola vulnerabilità
- Documentazione per decisori e sviluppatori


Infrastrutture Critiche
CNAIPIC
-Interpol High Tech Crime Network
-G8 High Tech Crime subgroup
-International Watch and Warning Network
CNAIPIC
-ICT Leader Companies
-Vendors
-CERTs
Squadre operative anticrimine informatico
Autorità Giudiziaria