PESCARA 24+25+26.08.2012
http://moca.olografix.org

There are only 10 types
of people in the world:
Those who understand binary,
and those who don't

(Who + What) && (Where + When) == Why

APPLICATION SECURITY FOR THE MASSES

Andrea Pompili
apompili@hotmail.com – Xilogic Corp.

Perché la solita minestra?

Application Security = SQL INJECTION e i suoi fratelli

Bah. Roba vecchia, le faceva mio nonno nel '98

<#1> Interessa solo perchè una banda di Lamer ha fatto casino nel 2011.

<#2> E' la solita tecnica per vendere qualche scatolone in più.

<#3> Basterebbe avere programmatori che sanno fare il loro dovere.

<#4> Se avessi gestito io quella roba lì non sarebbero mai entrati.

Andrea Pompili
apompili@hotmail.com – Xilogic Corp.

PESCARA 24+25+26.08.2012

http://moca.olografix.org

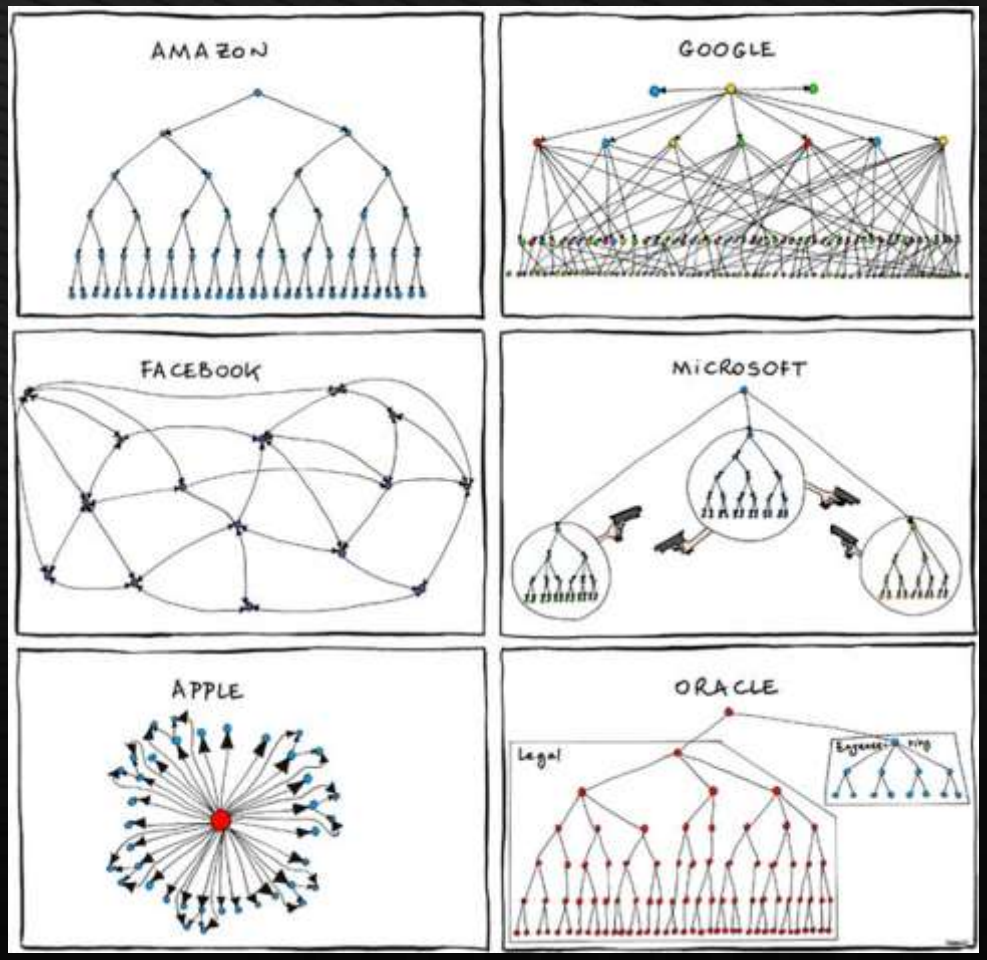
Limiti dell'Application Security

Andrea Pompili
apompili@hotmail.com – Xilogic Corp.

The Contenders

Andrea Pompili
apompili@hotmail.com – Xilogic Corp.

L'Azienda e la sua Organizzazione



Andrea Pompili
apompili@hotmail.com – Xilogic Corp.

Gli Hacker dell'IKEA

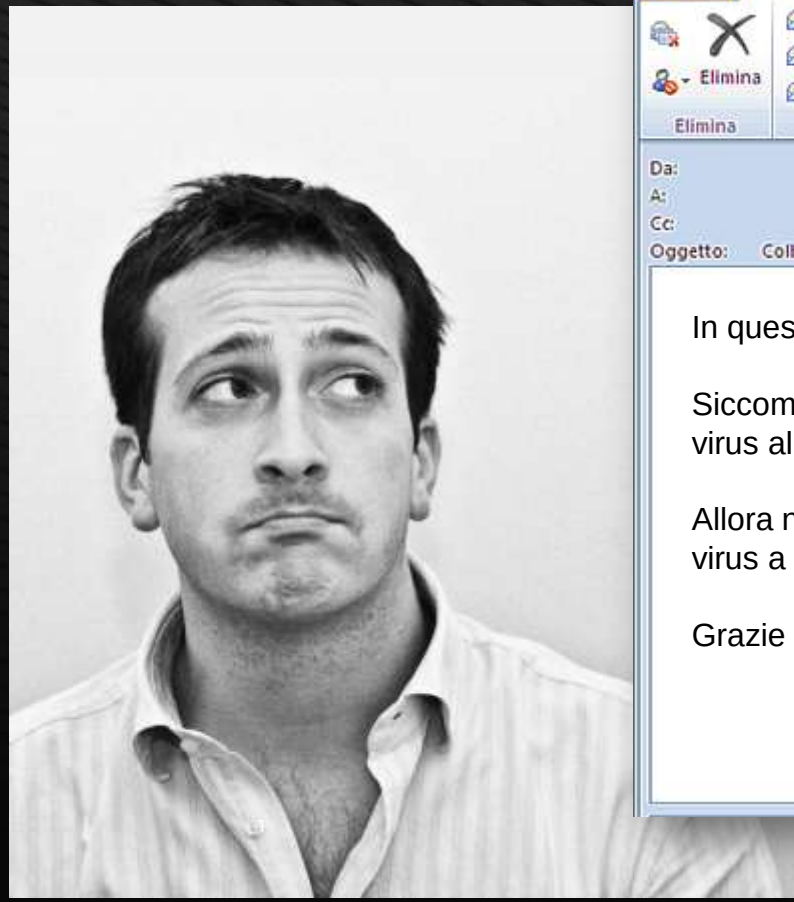
Andrea Pompili
apompili@hotmail.com – Xilogic Corp.

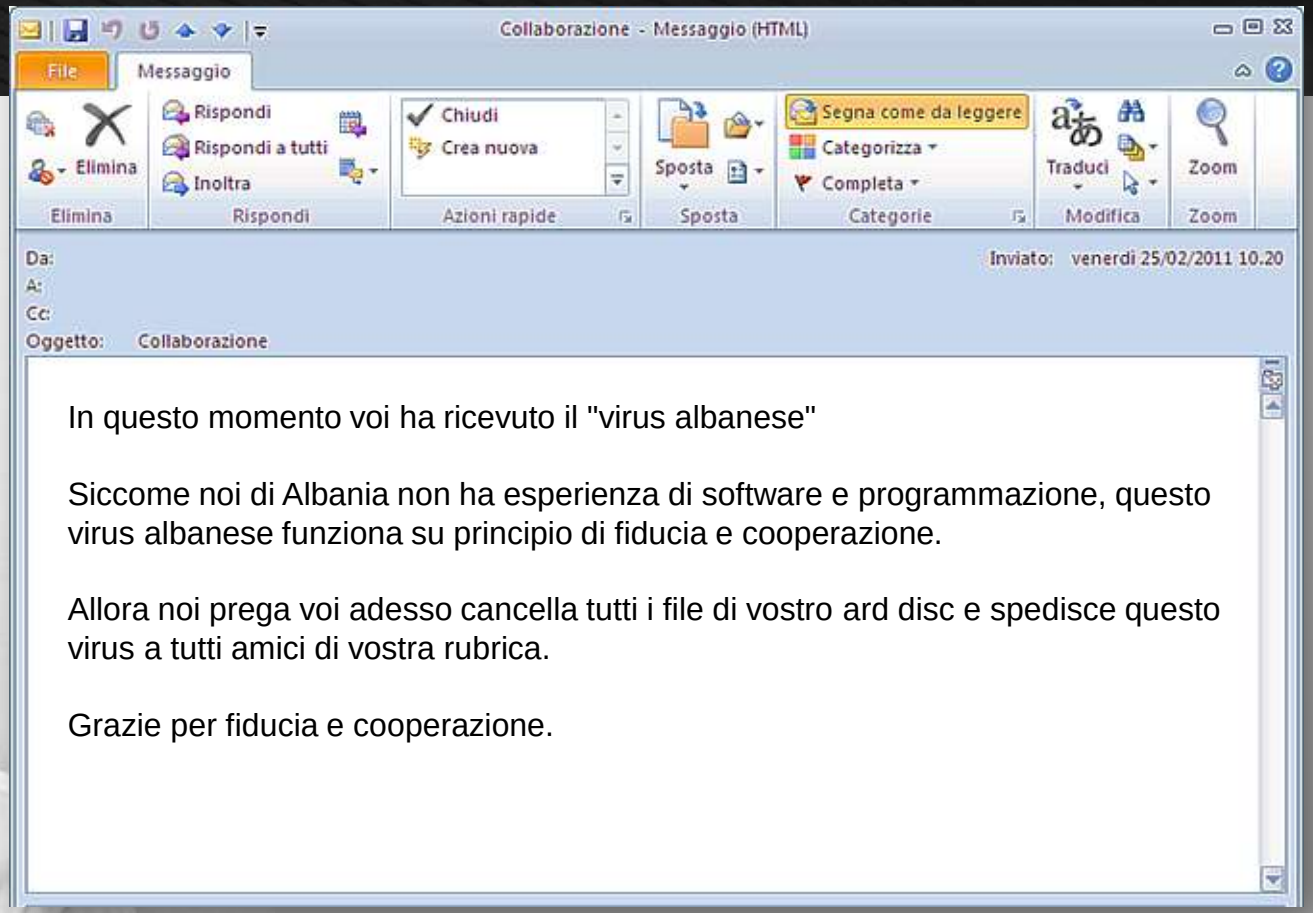
MOCA 2012
fino alla fine del mondo

PESCARA 24+25+26.08.2012
http://moca.olografix.org

Andrea Pompili
apompili@hotmail.com – Xilogic Corp.

Utenti=Ut0nti





Andrea Pompili
apompili@hotmail.com – Xilogic Corp.

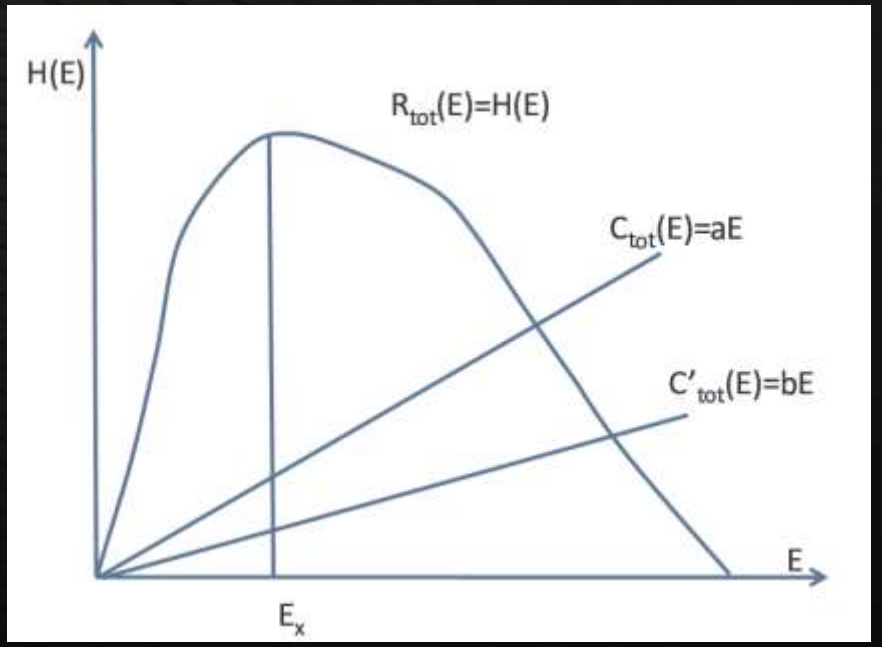
The Motivation

Andrea Pompili
apompili@hotmail.com – Xilogic Corp.

Il business del lato Oscuro della Forza

Example of a Typical Campaign	Mass Phishing Attack (Single Campaign)	Spearphishing Attack (Single Campaign)
(A) Total Messages Sent in Campaign	1,000,000	1,000
(B) Block Rate	99%	99%
(C) Open Rate	3%	70%
(D) Click Through Rate	5%	50%
(E) Conversion Rate	50%	50%
Victims	**8**	**2**
Value per Victim	$2,000	$80,000
Total Value from Campaign	**$16,000**	**$160,000**
Total Cost for Campaign	$2,000	$10,000
Total Profit from Campaign	**$14,000**	**$150,000**

Source: Cisco - "Email Attacks: This Time It's Personal" – 30/06/2011



Source: "A Profitless Endeavor: Phishing as Tragedy of the Commons" – 2008

H(E) = Curva della raccolta di denaro sostenibile in funzione **dell'**effort sostenuto

Andrea Pompili
apompili@hotmail.com – Xilogic Corp.

MOCA 2012
fino alla fine del mondo

PESCARA 24+25+26.08.2012
http://moca.olografix.org

La Contestazione Sociale nel XXI secolo

Andrea Pompili
apompili@hotmail.com – Xilogic Corp.

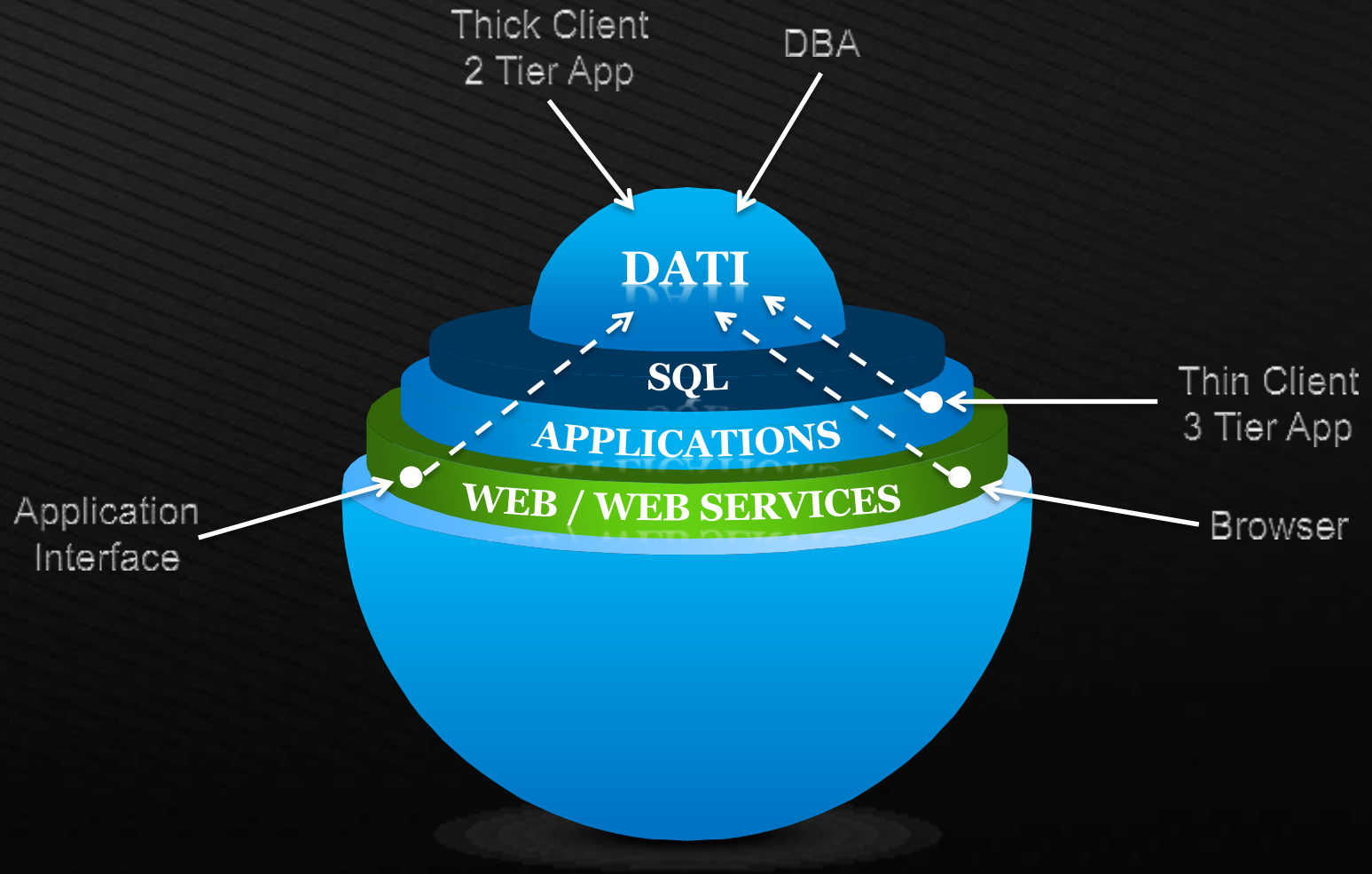
The BattleField

Andrea Pompili
apompili@hotmail.com – Xilogic Corp.

PESCARA 24+25+26.08.2012

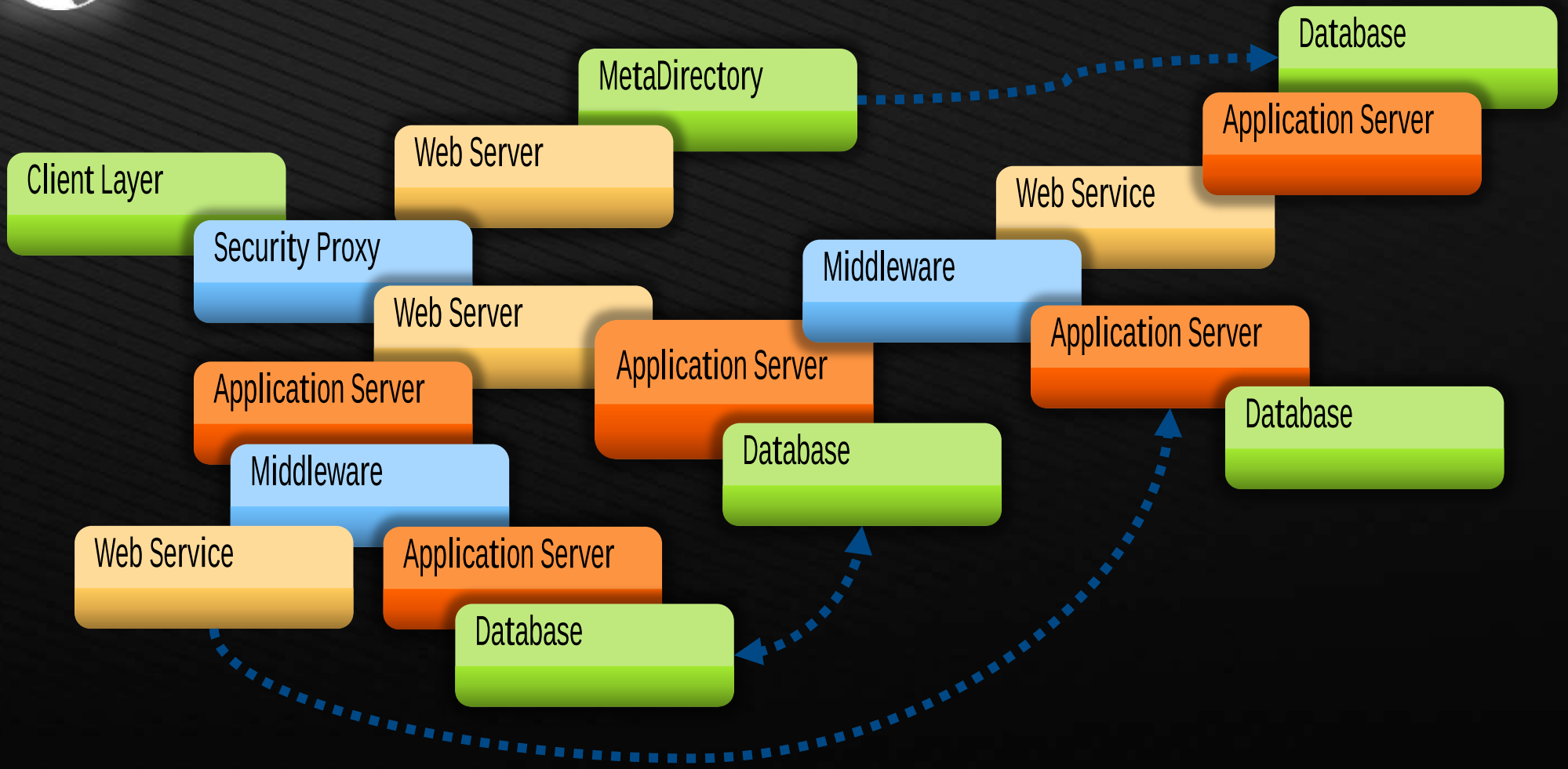
http://moca.olografix.org

The Onion Application Framework



Andrea Pompili
apompili@hotmail.com – Xilogic Corp.

... and its Current Evolution



Andrea Pompili
apompili@hotmail.com – Xilogic Corp.

MOCA 2012
Fino alla fine del mondo

PESCARA 24+25+26.08.2012
http://moca.olografix.org

To Code or not to Code


Giallo a Parigi, mobilitati i servizi di sicurezza
Pirata nel computer della Difesa francese
Quali segreti è

Hacker nel sito dell'Onu
"Non uccidete i bambini"
Pacifisti protestano on line contro Usa e Israele

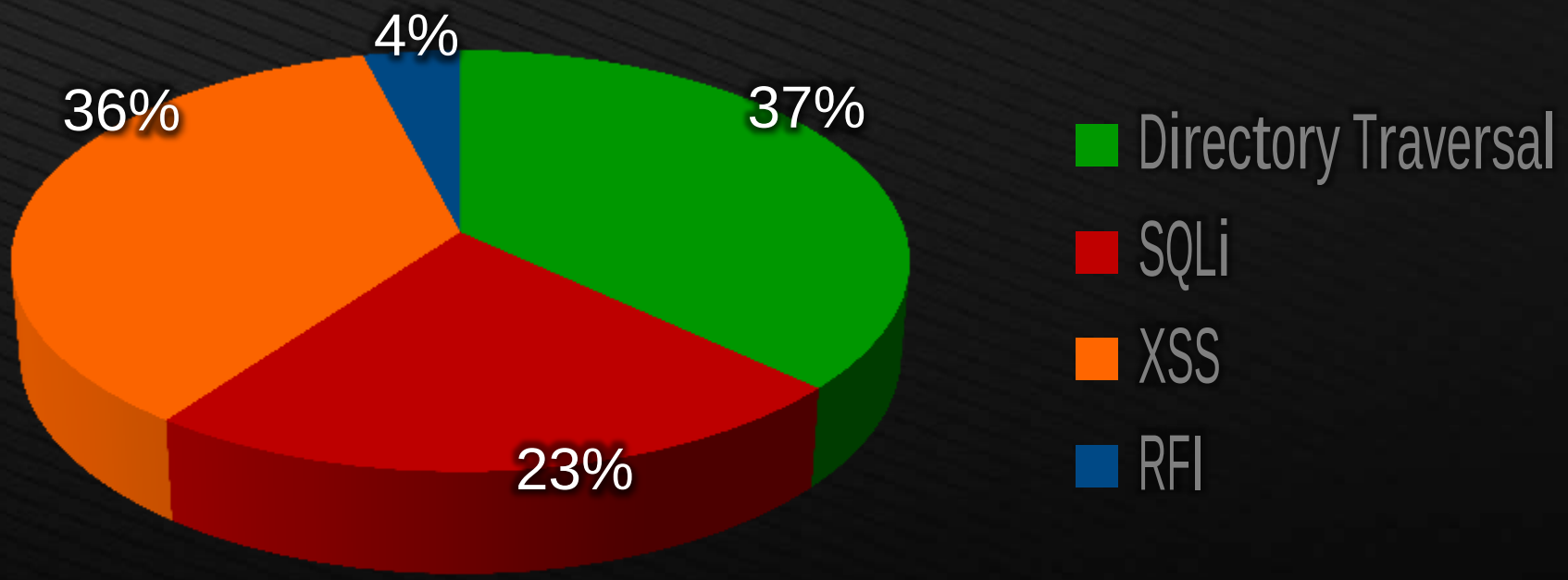
Pirati informatici scatenati: blog nel mir
Tre assalti in un mese per il forum virtuale de "Il Giornale del

Andrea Pompili
apompili@hotmail.com – Xilogic Corp.

The Weapons?

Andrea Pompili
apompili@hotmail.com – Xilogic Corp.

Il mondo dei Fantastici 4



Andrea Pompili
apompili@hotmail.com – Xilogic Corp.

MOCA 2012
fino alla fine del mondo

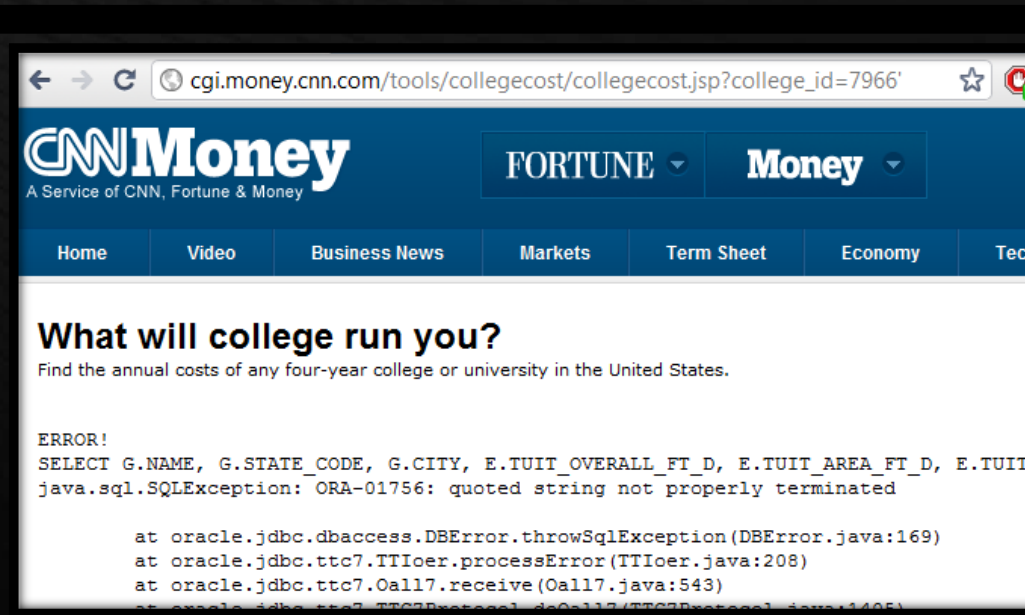
PESCARA 24+25+26.08.2012
http://moca.olografix.org

Sua Maestà SQL Injection e i suoi sudditi

Def. «Le Injection Flaws, come SQL Injection, XML Injection, e LDAP Injection, si verificano quando dati non validati vengono inviati come parte di un comando o di una query al loro interprete. Il dato infetto può quindi ingannare tale interprete, eseguendo comandi non previsti o accedendo a dati per i quali non si **ha l'autorizzazione**».

http://www.blackhat.com/presentations/bh-europe-09/Guimaraes/Blackhat-europe-09-Damele-SQLInjection-slides.pdf

http://www.modsecurity.org/archive/amit/blind-xpath-injection.pdf



Andrea Pompili
apompili@hotmail.com – Xilogic Corp.

PESCARA 24+25+26.08.2012

http://moca.olografix.org

A World of SQL Injection...

<01> INBAND SQL INJECTION

Visto che ci sei aggiungimi anche i risultati di questa **SELECT**...

<02> ERROR BASED SQL INJECTION

Siccome sei bravo a mostrare gli errori, fammi questa piccola conversione...

<03> BOOLEAN-BASED BLIND

Quando la risposta dipende dal numero di risultati della **SELECT**...

<04> TIME-BASED BLIND

Quando il Database è anche bravo ad aspettare...

Andrea Pompili
apompili@hotmail.com – Xilogic Corp.

Perché conviene?

Nel 2009, 94% di tutte le violazioni dei dati sono hanno coinvolto i Database o hanno compromesso applicazioni

Asset Attacked	Volume of Data Stolen
Database	74%
Application	19%
Other	7%

Ancora una volta, piu' del 90% dei $16B spesi in sicurezza nel 2009 e' stato "altro"

Andrea Pompili
apompili@hotmail.com – Xilogic Corp.

MOCA 2012
fino alla fine del mondo

PESCARA 24+25+26.08.2012
http://moca.olografix.org

The way to Application Security

Files

Databases

Applications

Development

ICT Operations

IT Security

Andrea Pompili
apompili@hotmail.com – Xilogic Corp.

... e perché non funziona

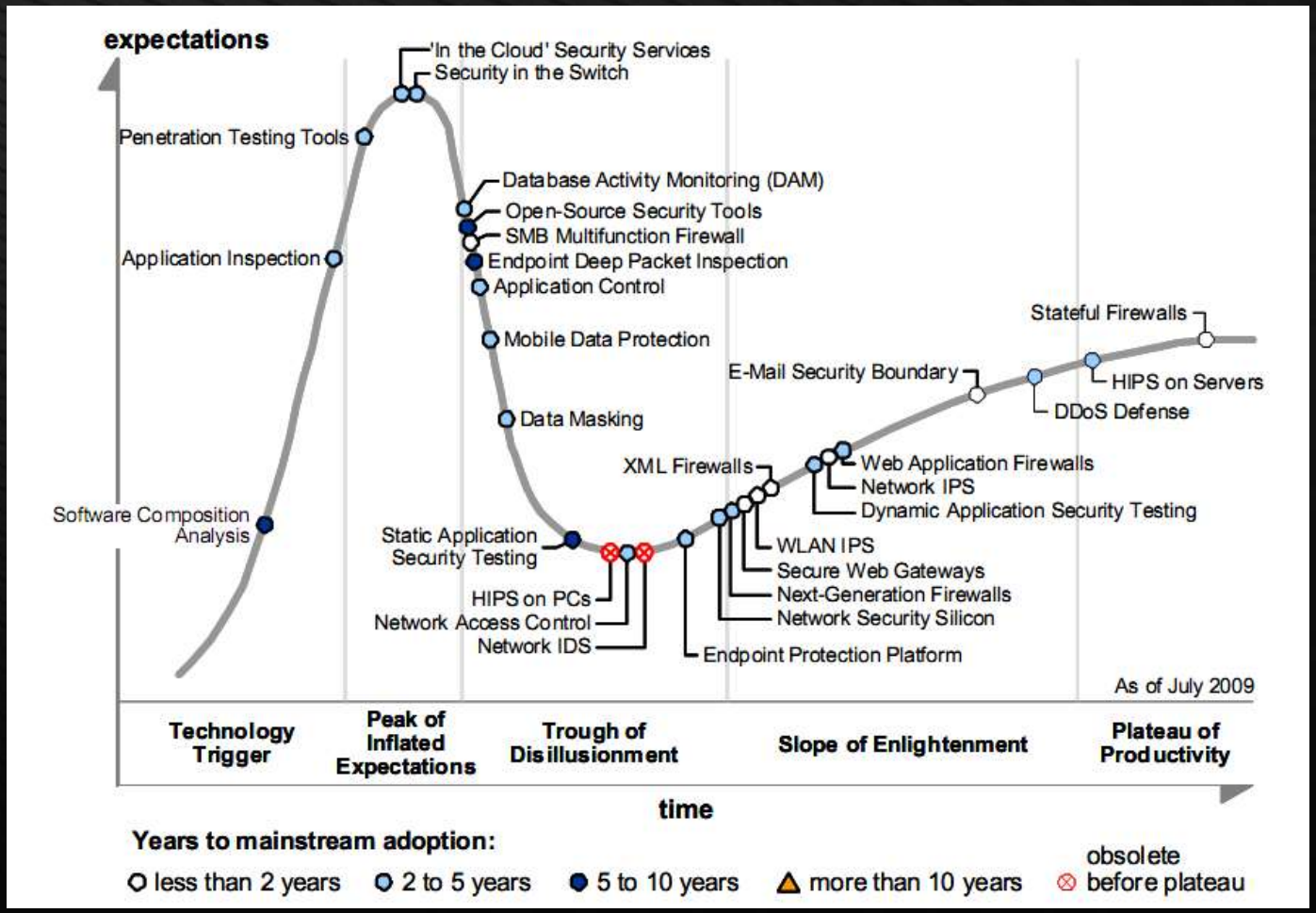
1

2

3

Andrea Pompili
apompili@hotmail.com – Xilogic Corp.

Current Application Security market



Andrea Pompili
apompili@hotmail.com – Xilogic Corp.

#2 Choices and #1 Combined Approach

<01> SORCE CODE AUDITING

I Bambini imparano più facilmente da piccoli...

<02> APPLICATION SECURITY INFRASTRUCTURE

Il Neoclassico della sicurezza informatica...

Apparentemente...

Andrea Pompili
apompili@hotmail.com – Xilogic Corp.

The Idea of a Self-Enforcement Environment

FAM

DAM

Files

Databases

Applications

WAF

DLP
Classificazione

IAM
Autenticazione
Autorizzazione

Usage Policy
Interne

Andrea Pompili
apompili@hotmail.com – Xilogic Corp.

PESCARA 24+25+26.08.2012

http://moca.olografix.org

LESSON #1

INPUTS & BACKDOORS

Andrea Pompili
apompili@hotmail.com – Xilogic Corp.

Attacco a Poste Italiane

Andrea Pompili
apompili@hotmail.com – Xilogic Corp.

MOCA 2012
fino alla fine del mondo

PESCARA 24+25+26.08.2012
http://moca.olografix.org

Application Firewall

x'; DROP TABLE users; --

```
POST http://www.sito.it/vulnpage.php HTTP/1.1
username: test
password: x'; DROP TABLE users; --
```

Applications

Virtual Patch

Andrea Pompili
apompili@hotmail.com – Xilogic Corp.

LESSON #2

THE GOOD OF ERRORS

Andrea Pompili
apompili@hotmail.com – Xilogic Corp.

Ricariche e Contatori elettrici

Andrea Pompili
apompili@hotmail.com – Xilogic Corp.

LESSON #3

CONTROL YOUR FILES

Andrea Pompili
apompili@hotmail.com – Xilogic Corp.

Il caso Wikileaks

Andrea Pompili
apompili@hotmail.com – Xilogic Corp.

File Security & Monitoring

1

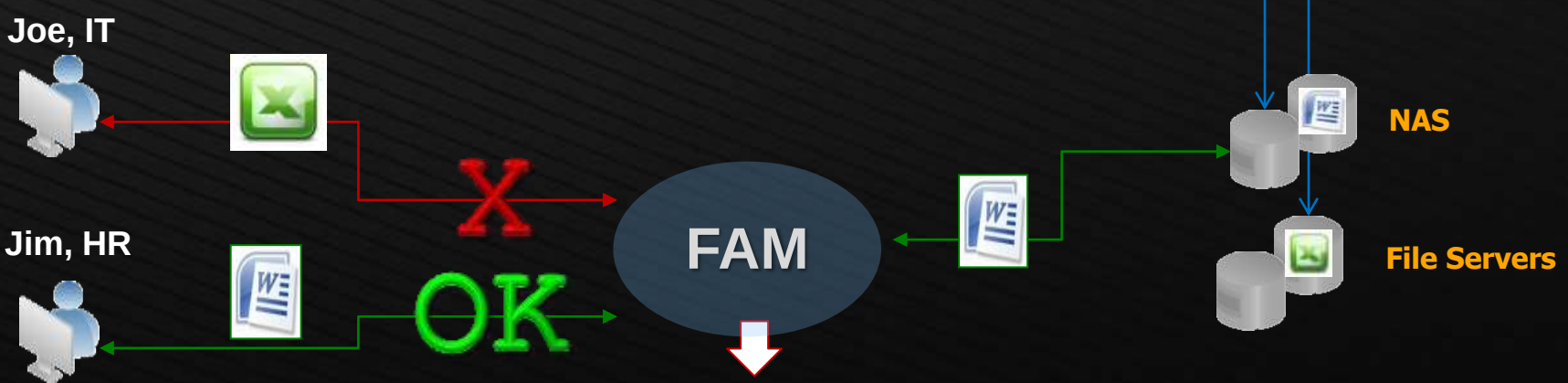
- Crawl File Systems
  - Find name, type, owner, permissions…
- Apply Classification Policies
  - Owner, Org, Location
  - Automatic content classification

2 Build Data/Permission Map

Who	Group	What	Class
Joe, IT	Fin-CC	Read cc.xls	Financials
Jim, HR	HR-Exec	Read PII.doc	PII

3 Enforce Policies

Who	What	Action
Non Finance	Update Financials	Block
Any	Read PII	Audit



Audit Log

Who	What	When	Action
Joe	Read CC.xls	1/1/2010 12:50	Block
Jim	Read PII.doc	1/1/2010 12:51	Audit

Andrea Pompili
apompili@hotmail.com – Xilogic Corp.

LESSON #4

SELF-DESTRUCTION APPS

Andrea Pompili
apompili@hotmail.com – Xilogic Corp.

MOCA 2012
fino alla fine del mondo

PESCARA 24+25+26.08.2012
http://moca.olografix.org

Into the Wireless World

Andrea Pompili
apompili@hotmail.com – Xilogic Corp.

Database Security & Monitoring

Chi, Dove, Come e Quando

SKO URM 1 - Effective Rights Raw Data

Filter: Account Department is [RnD] and Object Category is [credit cards] and Sensitive ...

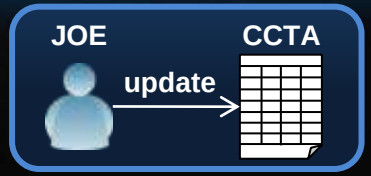
Select Columns | 1 | Showing records 1-3 out of 3 available | Show Paths

Account Name	Department	Priv Type	System Priv.	Object Name	Schema Name	Object Type	Sensitive Object	Object Category	Object Last Used
acourtney	RnD	SELECT	Normal Priv.	fullcustomerdata	skotrain	Table	Sensitive	credit cards	2009-12-31
atipton	RnD	SELECT	Normal Priv.	fullcustomerdata	skotrain	Table	Sensitive	credit cards	2009-12-31
eho	RnD	SELECT	Normal Priv.	fullcustomerdata	skotrain	Table	Sensitive	credit cards	2009-12-31

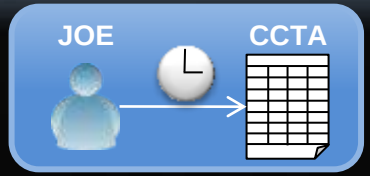
Chi | **Come** | **Dove** | **Cosa** | **Quando**

DAS
Who Is? Sensitive?

URM
What Rights?

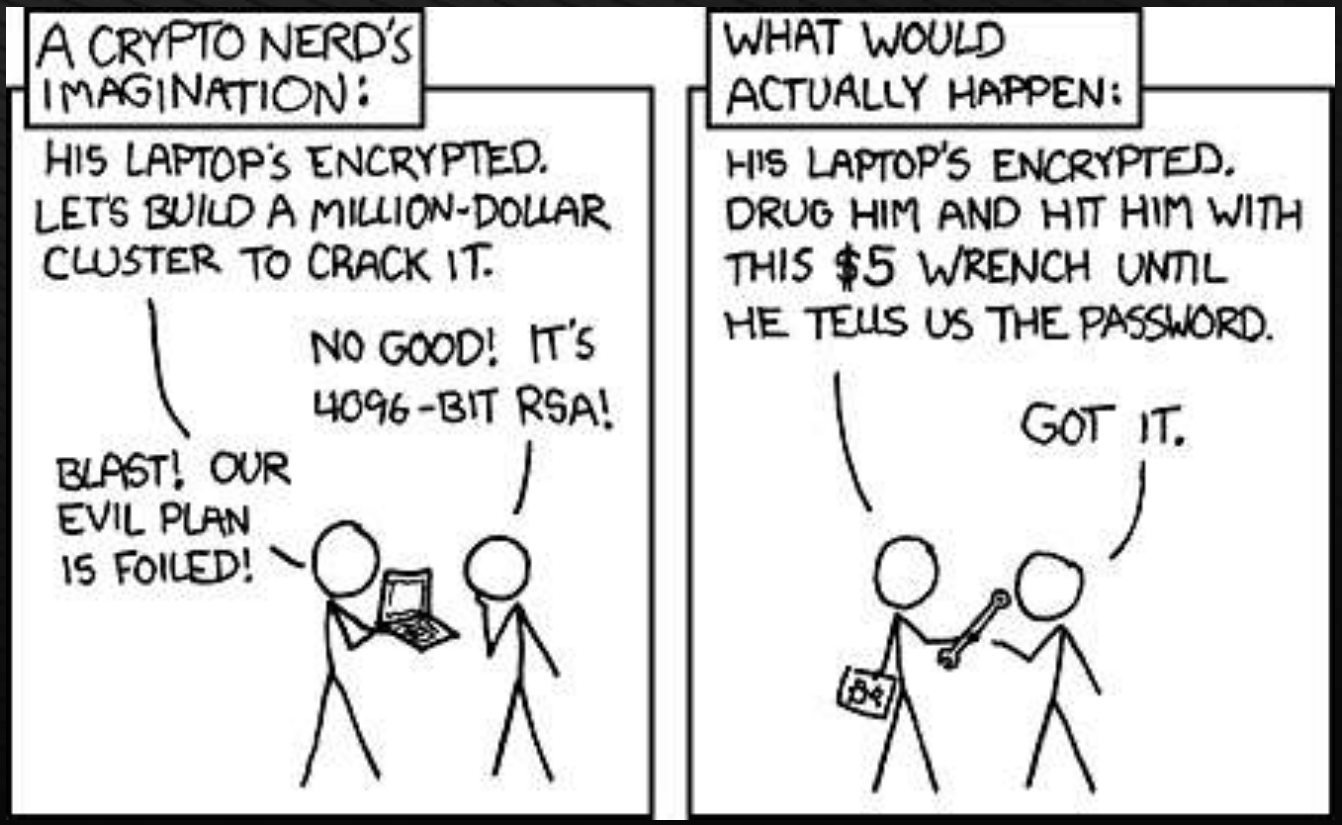


DAM
When Used?
Is it dormant?



Andrea Pompili
apompili@hotmail.com – Xilogic Corp.

La naturale conclusione...



Andrea Pompili
apompili@hotmail.com – Xilogic Corp.

MOCA 2012
fino alla fine del mondo

PESCARA 24+25+26.08.2012
http://moca.olografix.org

Questions?
English

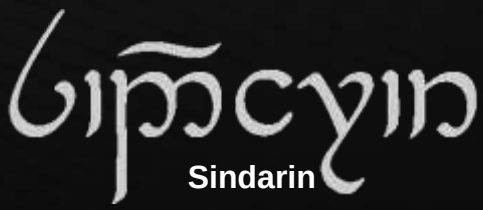
¿Preguntas?
Spanish

مَطَالِب أَيَّة
Arabic

вопросы?
Russian

Domande?
Italian

Ερωτήσεις?
Greek



Sindarin

tupoQghachmey
Klingon

質問
Japanese

Andrea Pompili
apompili@hotmail.com – Xilogic Corp.