



Secure Banking Expert Community: Unire forze e competenze tecniche per arginare il crimine (sempre più) organizzato"

Claudio Santacesaria
Head of R&D – Rototype

OWASP-Italy Day2012
Rome, 23° November 2012



Copyright © 2008 - The OWASP Foundation
Permission is granted to copy, distribute and/or modify this document
under the terms of the GNU Free Documentation License.

The OWASP Foundation
<http://www.owasp.org>

Sicurezza e banche

- Reti ben ingegnerizzate
- Policy rigide
 - ▶ Password complesse
 - ▶ Chiavette USB
 - ▶ Utenti con permessi limitati
 - ▶ Antivirus
 - ▶ Firewall
 - ▶ Encryption
 - ▶ Firme digitali e certificati
 - ▶ Usano bene la tecnologia disponibile



Ma...

- “Why do you rob banks?”
- “Because that’s where the money is!”
 - ▶ Da quanto un reporter ha pubblicato questa intervista (falsa), Sutton è famoso
 - ▶ Legge di Sutton: “tenta l’ovvio / massimizza il guadagno”
- Non basta la sicurezza allo stato dell’arte
- Le banche sono nel mirino della “criminal innovation”



Willie Sutton
Rapinatore
1901-1980



Il confronto

🌐 IT manager



Rag. Filini

🌐 Direttore della Banca



J.P. Morgan



Man in the middle attack (1)



L'utente se ne può accorgere osservando la barra

U.S. Bank Online Banking - Mozilla Firefox

U.S. Bank Online Banking

http://www4.usbank.com/internetBanking/RequestRouter?requestCmdId=DisplayC

usbank

Online Banking

Save time and money with Bill Pay!

Welcome to Online Banking

Log In

Personal ID [Forgot ID?](#)

Enter

[Where do I enter my password?](#)

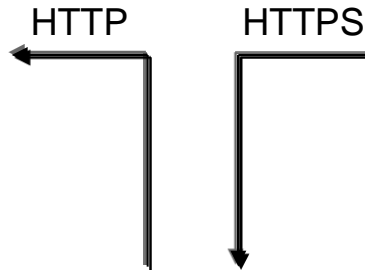
FDIC Update

View the latest notice of changes in the temporary FDIC insurance coverage for transaction accounts. [Learn more.](#)

Connection Secured

Privacy Pledge | Security Standards

USB Column:DBC 3



U.S. Bank Online Banking - Mozilla Firefox

U.S. Bank Online Banking

U.S. Bank National Association (US) https://www.usbank.com/internetBanking/

usbank

Online Banking

Save time and money with Bill Pay!

Welcome to Online Banking

Log In

Personal ID [Forgot ID?](#)

Enter

[Where do I enter my password?](#)

FDIC Update

View the latest notice of changes in the temporary FDIC insurance coverage for transaction accounts. [Learn more.](#)

Connection Secured

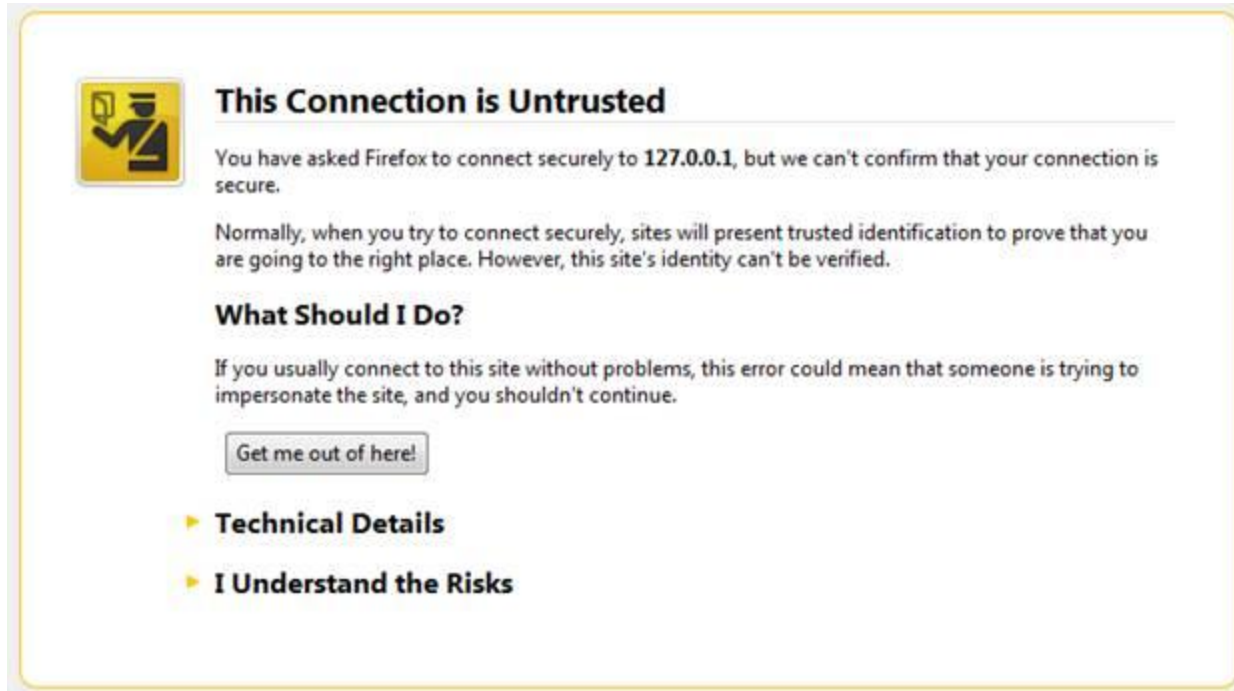
Privacy Pledge | Security Standards


USB Column:DBC 3



Man in the middle attack (2)

🌐 ... o riceve un warning



 **This Connection is Untrusted**

You have asked Firefox to connect securely to **127.0.0.1**, but we can't confirm that your connection is secure.

Normally, when you try to connect securely, sites will present trusted identification to prove that you are going to the right place. However, this site's identity can't be verified.

What Should I Do?

If you usually connect to this site without problems, this error could mean that someone is trying to impersonate the site, and you shouldn't continue.

[Get me out of here!](#)

- ▶ **Technical Details**
- ▶ **I Understand the Risks**



Man in the middle (3)

Sito sicuro

The screenshot shows a web browser window displaying a banking website. The browser's address bar shows a URL starting with 'www.'. The website's navigation menu includes 'Filiali e Bancomat', 'Help & FAQ', 'Contatti', 'Corporate & Press', and 'Live Chat'. The main content area features a navigation bar with 'INVESTING', 'TRADING', and 'BANKING' sections, along with buttons for 'APRI IL CONTO' and 'AREA CLIENTI'. A large promotional banner on the left reads 'Più energia al tuo conto Passaparola.' and offers a '50€ DI BONUS' or '100€ IN COMMISSIONI TRADING'. To the right, the 'Area Clienti' login form is visible, with fields for 'Codice utente:' and 'Password:', and buttons for 'ENTRA' and 'CHIUDI'. Below the login form, there are links for 'Nuovo cliente?', 'Attiva i codici', and 'Codici persi'. At the bottom, a market ticker shows the date '15 giugno 2012' and various stock indices: Ftse MB +1.86%, All Share +1.86%, Star +0.67%, Nasdaq +0.00%, and Dow +0.00%.



Man in the middle (4)

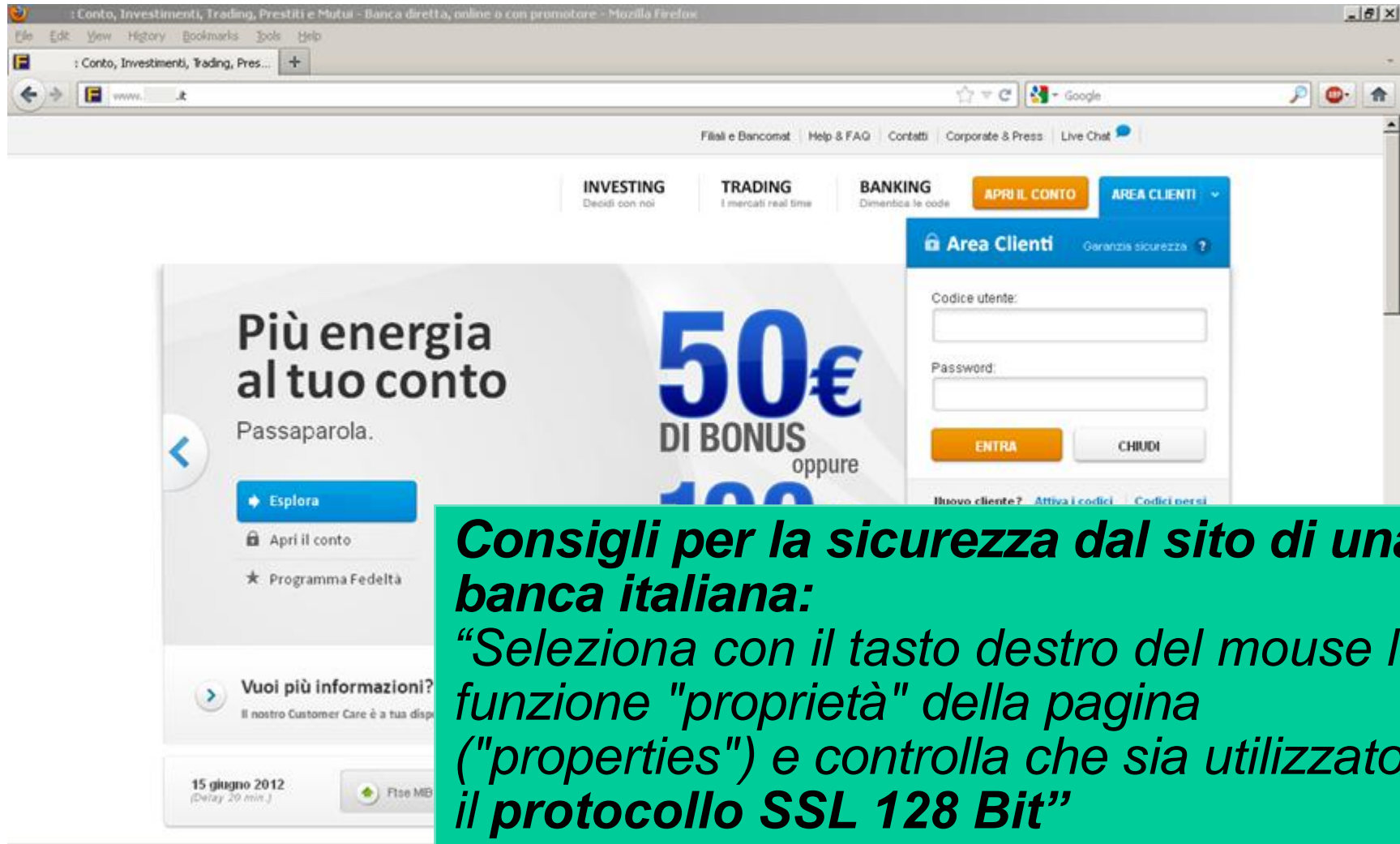
Attacco in corso

The screenshot shows a web browser window displaying a banking website. The browser's address bar shows a URL starting with 'www.'. The website's navigation bar includes links for 'Filiali e Bancomat', 'Help & FAQ', 'Contatti', 'Corporate & Press', and 'Live Chat'. Below the navigation bar, there are three main categories: 'INVESTING' (Decidi con noi), 'TRADING' (I mercati real time), and 'BANKING' (Dimentica le code). To the right of these categories are buttons for 'APRI IL CONTO' and 'AREA CLIENTI'. The 'AREA CLIENTI' section is expanded, showing a login form with fields for 'Codice utente:' and 'Password:', and buttons for 'ENTRA' and 'CHIUDI'. Below the login form are links for 'Nuovo cliente?', 'Attiva i codici', and 'Codici persi'. The main content area features a large promotional banner for 'Più energia al tuo conto' with a 'Passaparola.' section and a '50€ DI BONUS oppure 100€ IN COMMISSIONI TRADING' offer. Below the banner are three sections: 'Vuoi più informazioni?' (Il nostro Customer Care è a tua disposizione), 'Personal Financial Adviser' (Richiedi il contatto di un nostro consulente), and 'Corsi & Eventi' (Trova i più vicini a te). At the bottom, there is a market data section showing the date '15 giugno 2012 (Delay 20 min.)' and various market indices: Ftse MB +1.86%, All Share +1.86%, Star +0.67%, Nasdaq +0.00%, and Dow +0.00%.



Man in the middle (4)

Sito via SSL Strip (non sicuro)



The screenshot shows a web browser window displaying a bank's website. The browser's address bar shows a URL starting with 'www.'. The website has a navigation menu with links for 'Filiali e Bancomat', 'Help & FAQ', 'Contatti', 'Corporate & Press', and 'Live Chat'. Below the navigation, there are sections for 'INVESTING', 'TRADING', and 'BANKING'. A prominent 'Area Clienti' login form is visible, featuring fields for 'Codice utente:' and 'Password:', and buttons for 'ENTRA' and 'CHIUDI'. To the left of the login form, there is a promotional banner for 'Più energia al tuo conto' with a '50€ DI BONUS' offer. A green text box is overlaid on the bottom right of the screenshot, containing security advice.

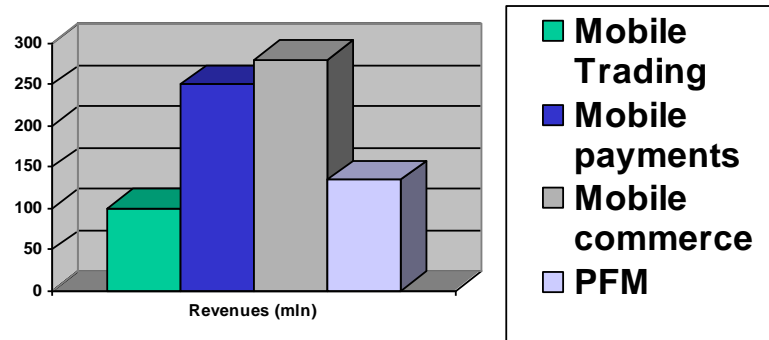
Consigli per la sicurezza dal sito di una banca italiana:
“Seleziona con il tasto destro del mouse la funzione "proprietà" della pagina ("properties") e controlla che sia utilizzato il protocollo **SSL 128 Bit**”



I commenti della banca



- Questo scenario non è economicamente rilevante perchè un attacco di questo tipo colpirebbe i pochi clienti che si collegano al sito della banca dalla rete controllata dal criminale
- Il mobile invece è rilevante oggi!: *"Investendo in piattaforme all'avanguardia e riducendo le commissioni del trading su smartphone, le revenues annue per la banca potrebbero di 100 milioni solo sulle commissioni di trading"*



Fonte: G.C., Dal mobile banking allo smartphone banking, AziendaBanca, Marzo 2012



Evoluzione degli attacchi

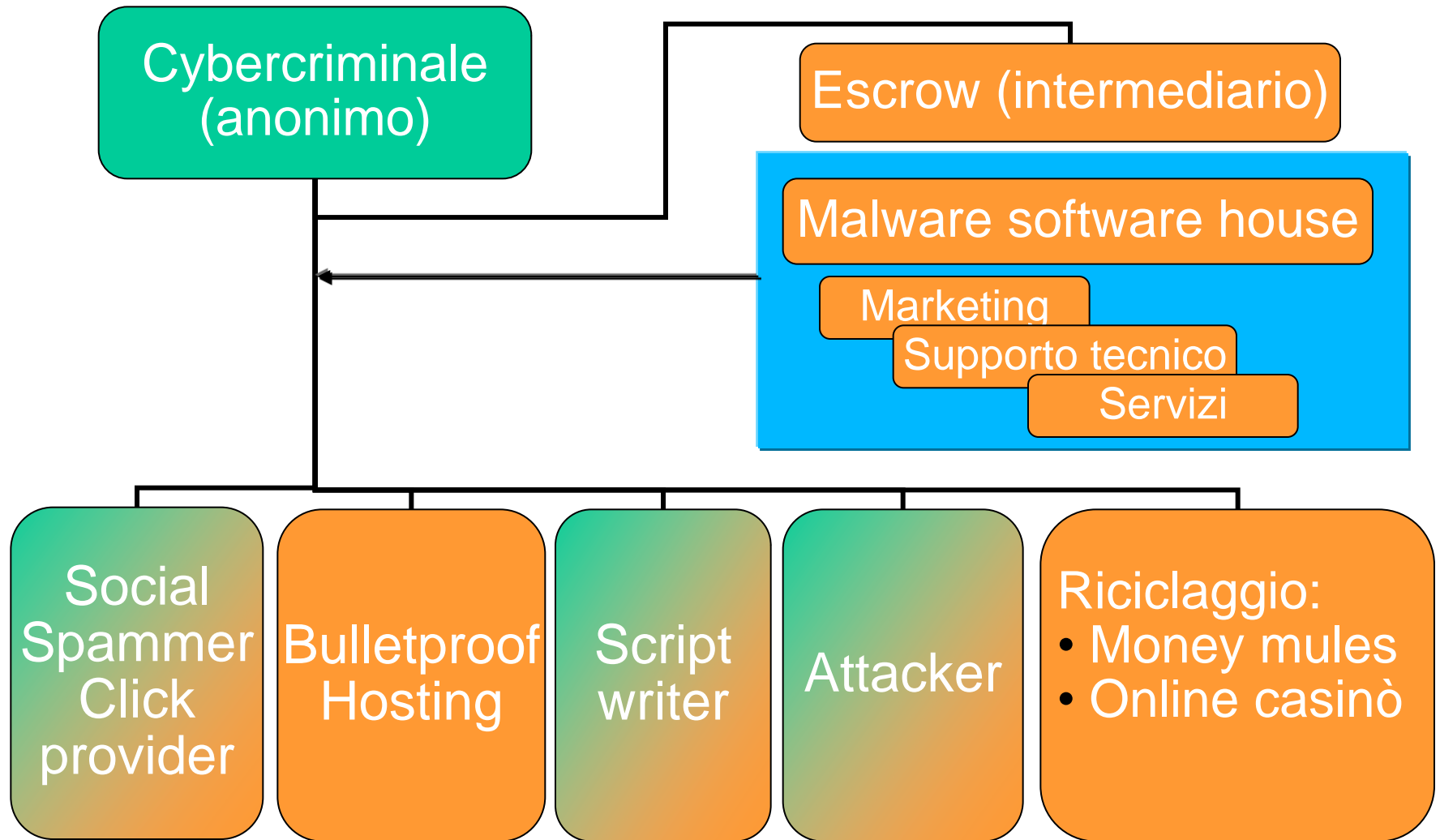


- Bisogna procedere con cautela con le nuove tecnologie, gli attacchi evolvono più velocemente delle contromisure:
 - ▶ Si attacca il PC e/o lo smartphone dell'end user che è l'anello debole
 - ▶ ...ma si automatizzano gli attacchi
 - ▶ ...attraverso l'installazione di "malware" che attiva il man in the browser

- e c'è un'organizzazione criminale, "organizzata"



Il nuovo assetto del cybercrime



Malware toolkits (prezzi indicativi)

CP :: OS statistics

ZEUS LISTINO PREZZI

Zeus kit: 3000\$

BackConnect: 1500\$

Firefox form grab: 2000\$

Jabber notifier: 500\$

Hosting: 200\$ / mese

SpyEye / ZS Builder v1.4.1 [harderman]

Full feature: US\$8400 + 3 months free hosting

Offerta 2012: US\$600

Citadel Universal Spyware System

CP :: Summary statistics

Information:

Current user: temp
GMT date: 27.12.2011
GMT time: 19:32:48

Statistics:

- Summary
- OS

Botnet:

- Bots
- Scripts

Reports:

- Search in database
- Search in files
- Jabber notifier

System:

- Information
- Options
- User
- Users
- Logout

Information

Total reports in database: 276 289

Time of first activity: 15.08.2011 17:59:34

Total bots: 2 224

Total active bots in 24 hours: 66.32% - 1 475

Minimal version of bot: 1.0.5

Maximal version of bot: 1.0.5

Current botnet: [All] >>

Actions: Reset "New bots"

New bots (0)

— Empty —

US\$3391

ICE IX

Information

Total reports in database: 276 289

Time of first activity: 15.08.2011 17:59:34

Total bots: 2 224

Total active bots in 24 hours: 66.32% - 1 475

Minimal version of bot: 1.0.5

Maximal version of bot: 1.0.5

Current botnet: [All] >>

Actions: Reset "New bots"

New bots (283) Online bots (264)

GB	260	GB	
--	22	--	
CA	1	US	2

US\$1800



Attacchi agli OTP basati su smartphone

Da qui vado sul sito della banca



Questo è il mio token di autenticazione



Il servizio di sincronizzazione delle app ha sincronizzato il malware



Scenari di attacco tramite malware

- 🌐 Cattura delle credenziali inserite
 - ▶ anche in tempo reale per OTP
- 🌐 Modifica delle pagine web
 - ▶ per chiedere altre credenziali non richieste dalla banca (es. OTP, il numero di telefono)
 - ▶ per nascondere le transazioni criminali
- 🌐 Uso del PC dell'utente per la transazione criminale
 - ▶ per evitare i meccanismi di controllo della banca
- 🌐 Intercettazione del traffico SMS via mobile malware
 - ▶ inoltro delle OTP al criminale
 - ▶ soppressione delle notifiche per le transazioni criminali



Le nuove frontiere

- 🌐 Il malware as a service con tariffa mensile
 - ▶ ottimo per chi non ha in mente di fare il cybercriminale a tempo pieno
- 🌐 I call center
 - ▶ Si può scegliere la voce, l'accento, le frasi e l'algoritmo di risposta
 - ▶ Personale altamente qualificato
 - ▶ 10\$ a telefonata gestita



Le domande della banca



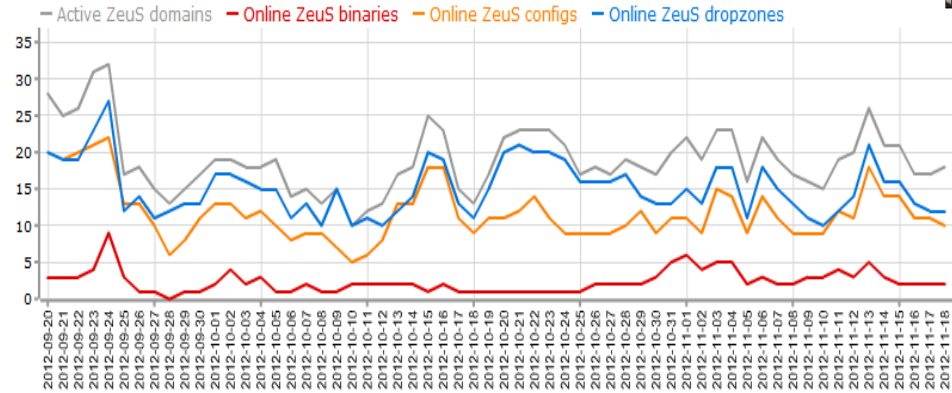
- Quanti soldi abbiamo perso?
- Vediamo i numeri! (finanziari, n.d.r.)



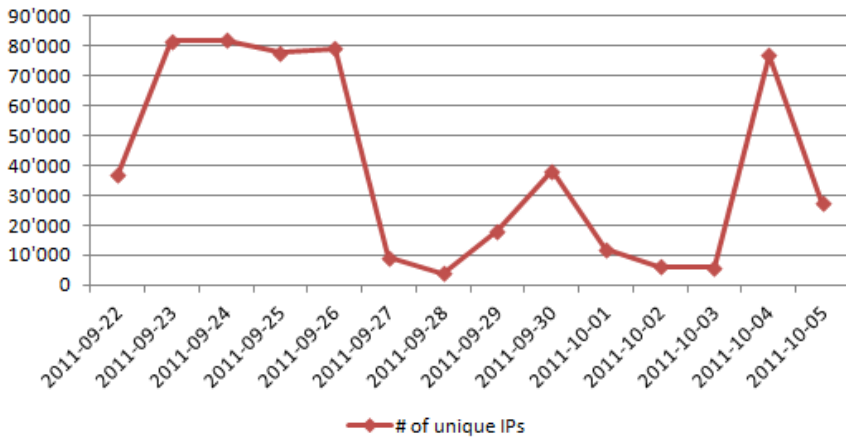
I numeri?



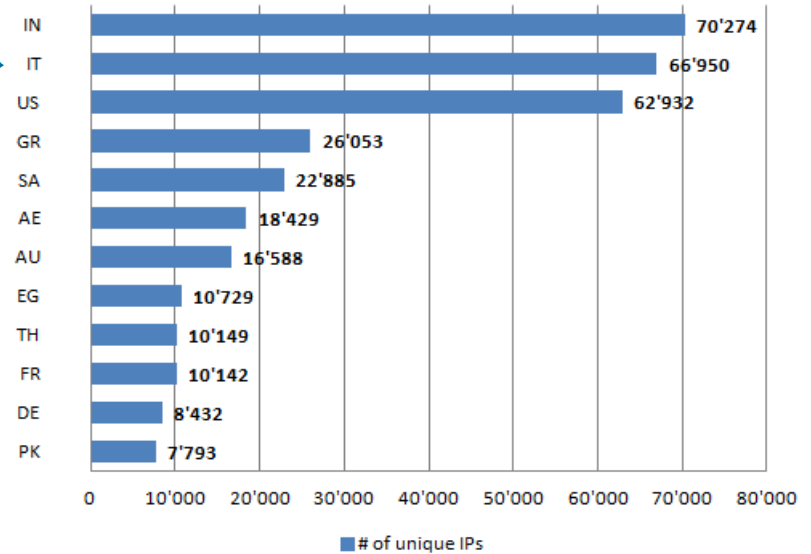
Tecnologie > Ict
Cyber crime: agli italiani è costato 617 milioni di euro



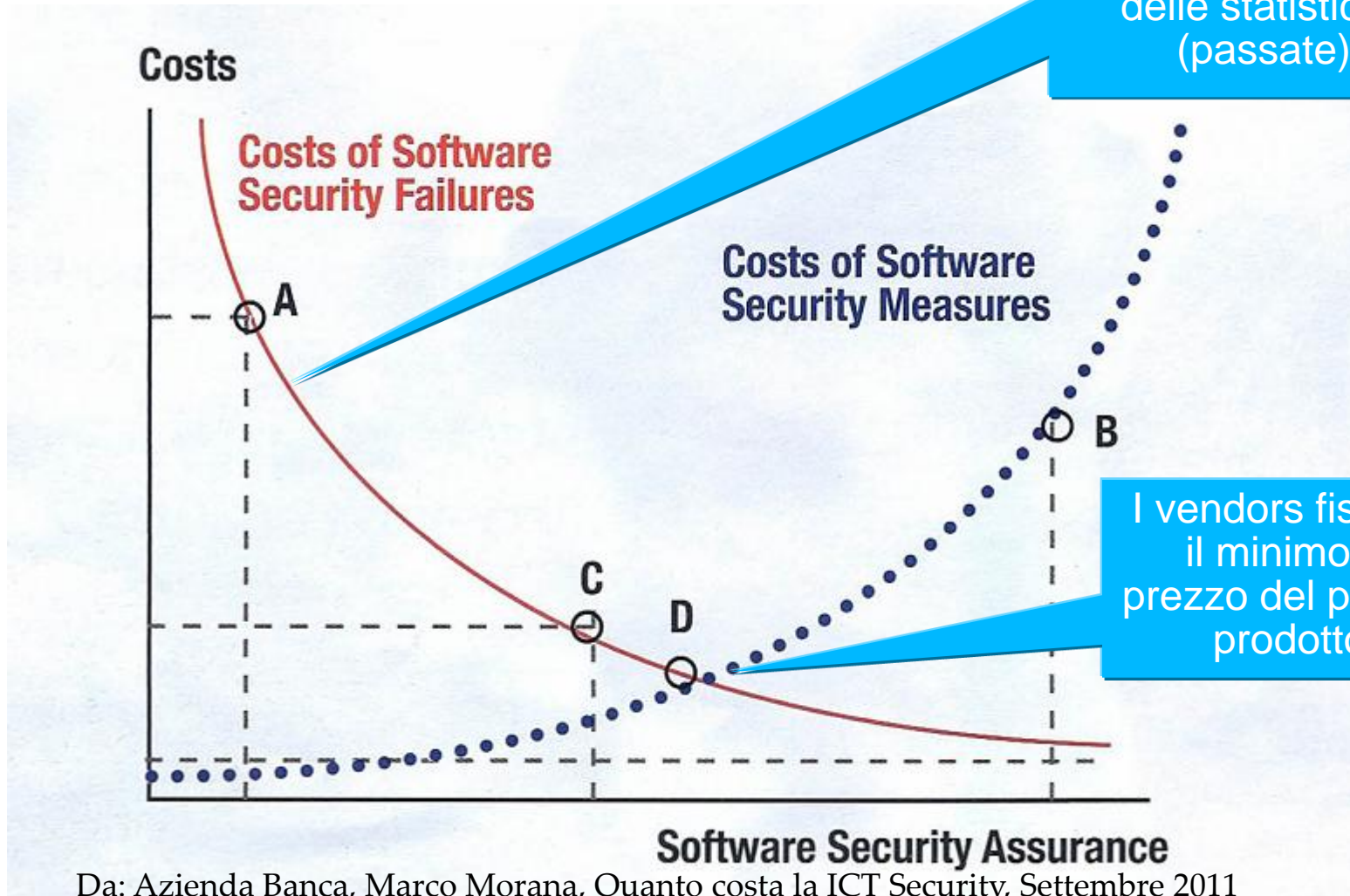
ZeuS Botnet size



ZeuS Botnet Geo Location



I numeri!



Analisti e banche determinano la curva dei costi sulla base delle statistiche (passate)

I vendors fissano il minimo al prezzo del proprio prodotto



www.securebanking.it



- Luogo di incontro (soprattutto online) per professionisti della sicurezza in ambito bancario
 - ▶ Sistemi Informativi
 - ▶ Sistemi di pagamento
- Banca + Aziende + Università



SICUREZZA, SVILUPPO E CONDIVISIONE

Secure Banking Expert Community

UN LUOGO DI RITROVO PER CONDIVIDERE INFORMAZIONI,
PER CREARE SICUREZZA, PER CONOSCERSI E FARE SQUADRA,
PER INFORMARE, PER PREVENIRE PRIMA ANCORA CHE
COMBATTERE LE FRODI CON SOLUZIONI TECNICHE
E IMPLEMENTAZIONI ROBUSTE.

Obiettivi di Secure Banking

- Costruzione knowledge base pubblica in italiano
 - ▶ Training
 - ▶ Divulgazione ➔ Consapevolezza
- Condividere informazioni tecniche non strategiche ma vitali tra CIO e CSO delle banche
- Technology scouting e analisi preventiva delle minacce sulle nuove tecnologie

Analisi delle tecnologie, valutazione dei punti di debolezza, indicazione della best practice; lo scopo è irrobustire le tecnologie prima dell'introduzione sul mercato
- Risk analysis (metodi adeguati al cybercrime)



Regole e Principi Etici

🌐 Due livelli di Forum e Documenti

- ▶ PUBBLICO: materiale divulgativo totalmente aperto
- ▶ RISTRETTO: per dare alle banche la possibilità di condividere temi più delicati

🌐 Principi Etici

- ▶ Non divulgazione: gestione delle informazioni riservate
- ▶ Obbiettività e correttezza: dati veri e certi
- ▶ Etica dell'hacker: dare il tempo di risolvere il problema
- ▶ Indipendenza: no pubblicità o condizionamenti



I Fondatori



Ernesto Damiani
Università degli Studi di Milano



Claudio Santacesaria
Rototype



Giorgio Fedon
Minded Security, OWASP



Raoul Chiesa
Cyberdefcon, CLUSIT



Marco Tempra
Banca Popolare di Sondrio



Mario Monitillo
Istituto Centrale delle Banche Popolari Italiane

Kick Off IEEE DEST

Sito web

+ 10 banche?
+ 1 università
+ 2 industrie

Maggio 2012

Novembre 2012



Grazie (e buon appetito)

Claudio Santacesaria

claudio.santacesaria@rototype.com



www.securebanking.it



www.rototype.com

