

Indagini tra le nuvole

Università degli Studi
di Catania

29 aprile 2013

Cloud Computing

Servizi popolari

Facebook

Google

Dropbox

Acquisizioni

Protocollo

Strumenti

Credits



Università degli Studi di Catania

Cloud Computing e Cloud Investigation

Catania, 29 aprile 2013

Davide Gabrini
Human, Forensic,
Chaotic Good

Indagini tra le nuvole

Università degli Studi
di Catania

29 aprile 2013

Cloud Computing

Servizi popolari

Facebook

Google

Dropbox

Acquisizioni

Protocollo

Strumenti

Credits

Davide Gabrini
Human, Forensicator,
Chaotic Good

Chi sono

Davide 'Rebus' Gabrini

Per chi lavoro non è un mistero.

Oltre a ciò:

- ▶ Consulente tecnico e Perito forense
- ▶ Docente di sicurezza informatica e computer forensics per privati e P.A.
- ▶ Socio IISFA, DEFTA, Tech&Law fellow
- ▶ Certificazioni CIFI, ACE, AME

Come vedete **non** sono qui in divisa.





Indagini tra le nuvole

Università degli Studi
di Catania

29 aprile 2013

➔ Cloud Computing

Servizi popolari

Facebook

Google

Dropbox

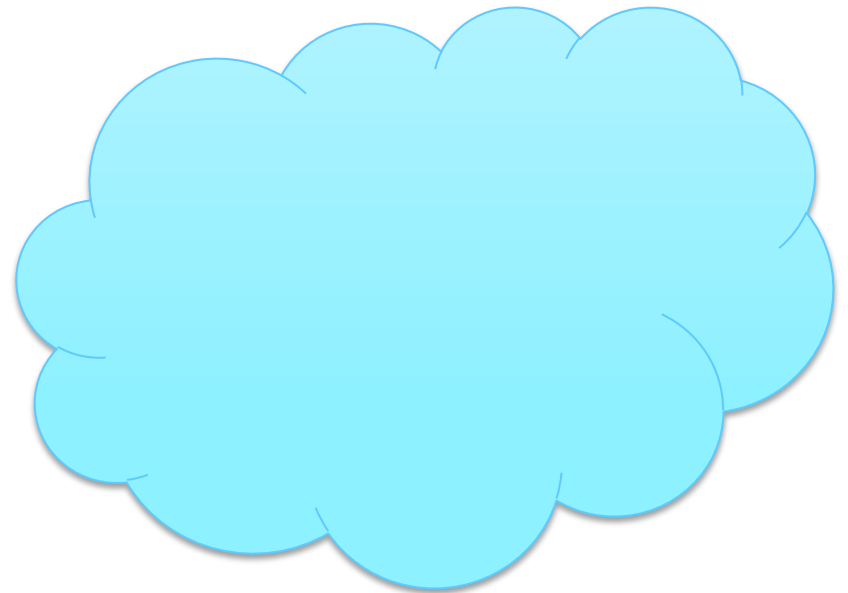
Acquisizioni

Protocollo

Strumenti

Credits

Davide Gabrini
Human, Forensicator,
Chaotic Good



Cloud Computing

Indagini tra le nuvole

Cloud Computing

▶ Il termine *cloud computing* indica un insieme di risorse hardware e software distribuite e remotamente accessibili e usabili

▶ Il cloud computing si è affermato pervasivamente come modello di riferimento

▶ Non si basa su nuove tecnologie, ma su un nuovo paradigma



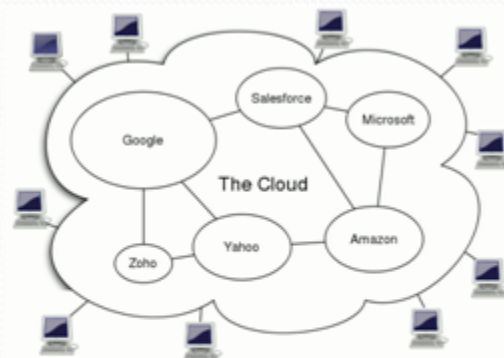
1960's
Mainframe

digital
IBM



1980's
Client/server

ORACLE
Microsoft



Today
The Cloud

Indagini tra le nuvole

Università degli Studi
di Catania

29 aprile 2013

Cloud Computing

Servizi popolari

Facebook

Google

Dropbox

Acquisizioni

Protocollo

Strumenti

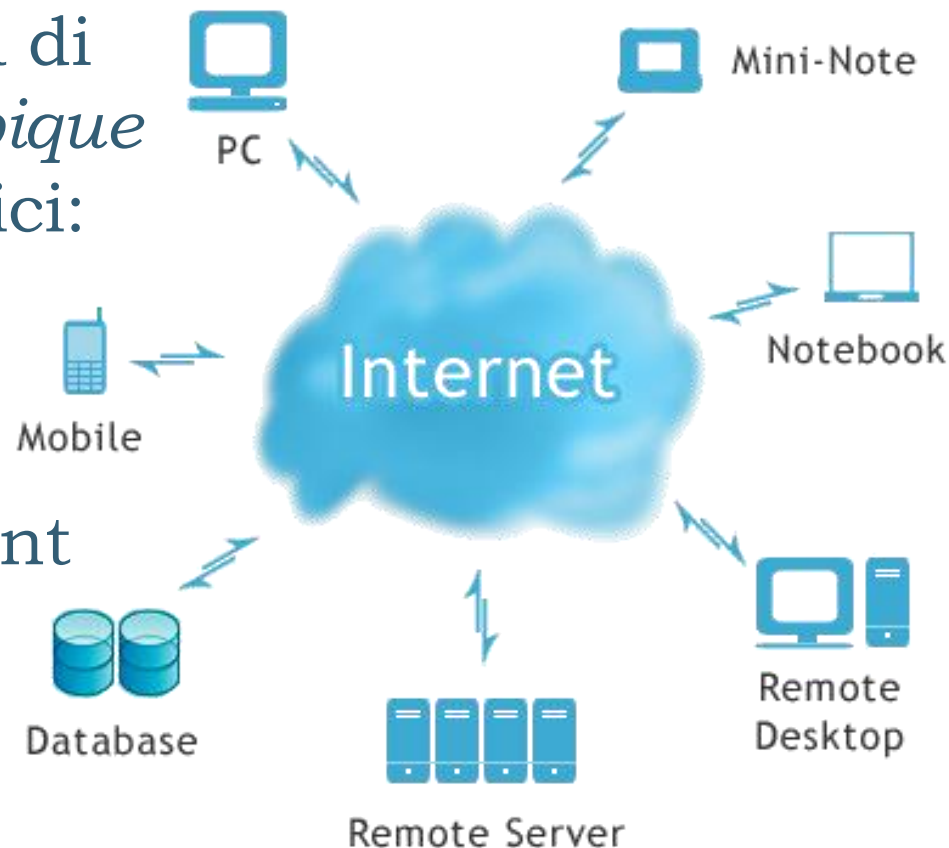
Credits

Cloud Computing

La tendenza è quella di rendere le risorse *ubique*
Gli usi sono molteplici:

- ▶ E-mail
- ▶ Database
- ▶ Storage on-line
- ▶ Project Management
- ▶ Snail Mail
- ▶ Voicemail
- ▶ e molto altro...

Tutte cose che esistono da tempo, ma per cui è cambiata rapidamente l'offerta da parte ISP



Indagini tra le nuvole

Frammentazione

▶ Allocare risorse in cloud può portare ad un impoverimento del patrimonio informativo sui device locali

▶ Limitazioni in potenza di calcolo, capacità di storage, connessione...

▶ D'altro canto però, moltiplica i device disponibili per l'acquisizione e l'analisi



Indagini tra le nuvole

Concentrazione

▶ Inoltre spesso concentra fortemente le informazioni in **un unico punto** nevralgico fuori dal controllo diretto dell'utente, raggiunto il quale non c'è più bisogno di rincorrere i singoli device

- ▶ Google Products
- ▶ iCloud
- ▶ Amazon EC2
- ▶ Dropbox
- ▶ ...





Indagini tra le nuvole

Università degli Studi
di Catania

29 aprile 2013

Cloud Computing

Servizi popolari

Facebook

Google

Dropbox

Acquisizioni

Protocollo

Strumenti

Credits

Esempi di servizi in Cloud

▶ **Storage e altri servizi**

- ▶ SkyDrive, Gdrive, Amazon S3...
- ▶ PayPal, Google Maps, Flickr, Youtube...

▶ **Applicazioni** (SaaS: Software as a Service)

- ▶ Webmail, Google Docs, Windows Live, Photoshop, Meebo, Spoon...

▶ **Piattaforme** (PaaS: Platform as a Service)

- ▶ Windows Azure, Facebook, Amazon Web Services, ajaxWindows, GlideOS...
- ▶ eyeOS, gOS, Chrome OS, JoliCloud...

▶ **Infrastrutture** (IaaS: Infrastructure as a Service)

- ▶ Amazon EC2, GoGrid, ElasticHost...



Indagini tra le nuvole

Università degli Studi
di Catania

29 aprile 2013

Cloud Computing

Servizi popolari

Facebook

Google

Dropbox

Acquisizioni

Protocollo

Strumenti

Credits

Cloud Computing, VPS e indagini

▶ Le risorse usate per crimini informatici possono essere allocate remotamente, anche al di fuori dei confini nazionali

▶ Non solo lo storage, ma anche le risorse computazionali!

▶ Interi sistemi possono essere allocati dinamicamente, utilizzati e deallocati

▶ Le possibilità di analisi vengono così drasticamente ridotte



Indagini tra le nuvole

Università degli Studi
di Catania

29 aprile 2013

Cloud Computing

Servizi popolari

Facebook

Google

Dropbox

Acquisizioni

Protocollo

Strumenti

Credits

Davide Gabrini
Human, Forensic,
Chaotic Good

Cloud Computing

- ▶ L'approccio tradizionale che prevede perquisizione-sequestro-analisi è vanificato
- ▶ Già l'identificazione potrebbe essere problematica: *cosa si trova dove?*
- ▶ Le risorse sono probabilmente distribuite su diversi sistemi, di diversi provider, in diversi paesi...
 - ▶ limiti giurisdizionali
 - ▶ scarsa armonizzazione delle norme in materia
 - ▶ mancanza di accordi internazionali
 - ▶ scarsa collaborazione delle autorità locali
 - ▶ ritardi burocratici
 - ▶ problemi di data-retention



Indagini tra le nuvole

Università degli Studi
di Catania

29 aprile 2013

Cloud Computing

Servizi popolari

Facebook

Google

Dropbox

Acquisizioni

Protocollo

Strumenti

Credits

Cloud Computing e acquisizioni

Informazioni di interesse investigativo possono essere ricercate:

▶ **Lato server:** acquisizione presso i provider di dati giacenti, log, dati di registrazione...

▶ **Lato client:** artefatti dei browser e di altre eventuali applicazioni client

▶ **In transito:** intercettazione delle comunicazioni tra utente e cloud (sempre che non siano cifrate)



Indagini tra le nuvole

Università degli Studi
di Catania

29 aprile 2013

Cloud Computing

Servizi popolari

Facebook

Google

Dropbox

Acquisizioni

Protocollo

Strumenti

Credits

Acquisizioni da remoto

▶ Copia eseguita da o presso ISP

- ▶ Art. 254bis cpp: L'autorità giudiziaria, quando dispone il sequestro, presso i fornitori di servizi informatici [...] dei dati da questi detenuti [...] può stabilire [...] che la loro acquisizione avvenga mediante copia di essi [...] con una procedura che assicuri la conformità dei dati acquisiti a quelli originali e la loro immutabilità. In questo caso è, comunque, ordinato al fornitore dei servizi di conservare e proteggere adeguatamente i dati originali.

▶ Congelamento, messa off-line, distruzione...?

▶ Sequestro tramite inibizione account?

- ▶ Disponibilità, modalità, certezza...

▶ Acquisizione mediante intercettazione telematica

- ▶ Dati cifrati
- ▶ Spyware lato client



Indagini tra le nuvole

Università degli Studi
di Catania

29 aprile 2013

Cloud Computing

Servizi popolari

Facebook

Google

Dropbox

Acquisizioni

Protocollo

Strumenti

Credits

Daide Gabrini
Human, Forensic,
Chaotic Good

Acquisizioni da remoto

▶ Accesso con credenziali

▶ tramite API

▶ tramite UI e Macro

▶ tramite UI e utente

▶ Verifiche di integrità?

▶ Che risorse esistono per le
piattaforme più popolari?

▶ Ci sono regole generali?



Indagini tra le nuvole

Università degli Studi
di Catania

29 aprile 2013

Cloud Computing

Servizi popolari

➡ Facebook

Google

Dropbox

Acquisizioni

Protocollo

Strumenti

Credits

Facebook



Daide Gabrini
Human, Forensicator,
Chaotic Good



Indagini tra le nuvole

Università degli Studi
di Catania

29 aprile 2013

Cloud Computing

Servizi popolari

➡ Facebook

Google

Dropbox

Acquisizioni

Protocollo

Strumenti

Credits

Statistiche

- ▶ Lanciato il 4 febbraio 2004
- ▶ E' il secondo sito più visitato al mondo
- ▶ Un miliardo di utenti attivi per mese
- ▶ 604 milioni accedono da mobile
- ▶ 23 milioni di utenti italiani
- ▶ Più di metà si collega ogni giorno
- ▶ in buona parte da dispositivi mobili

Penetration of population 38.60%

Penetration of online population 71.66%

<https://www.socialbakers.com/facebook-statistics>



Indagini tra le nuvole

Università degli Studi di Catania

29 aprile 2013

Cloud Computing

Servizi popolari

➔ Facebook

Google

Dropbox

Acquisizioni

Protocollo

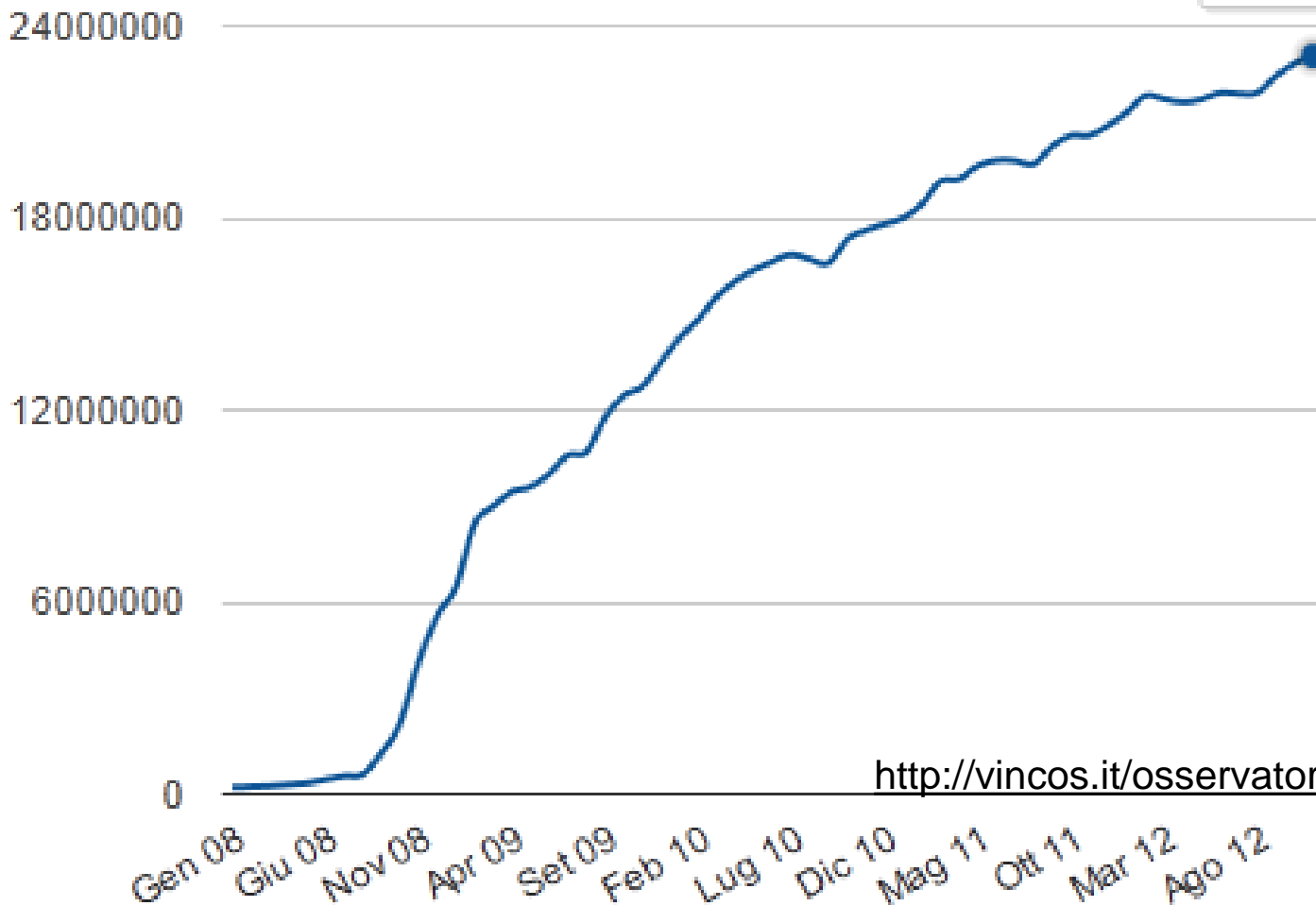
Strumenti

Credits

Statistiche

Facebook - italiani iscritti

Nov
mesi: 23072640



<http://vincos.it/osservatorio-facebook/>



Indagini tra le nuvole

Università degli Studi
di Catania

29 aprile 2013

Cloud Computing

Servizi popolari

➡ Facebook

Google

Dropbox

Acquisizioni

Protocollo

Strumenti

Credits

Statistiche

▶ Ogni utente è connesso in media a 130 utenti e a 80 community, gruppi, eventi

▶ 300 milioni di foto caricate. Al giorno.

▶ 9 miliardi mese, o 12.5 milioni all'ora

▶ 500 TB di nuovi dati al giorno

▶ Oltre 42 milioni di pagine

▶ Oltre 9 milioni di applicazioni



Indagini tra le nuvole

Università degli Studi
di Catania

29 aprile 2013

Cloud Computing

Servizi popolari

➡ Facebook

Google

Dropbox

Acquisizioni

Protocollo

Strumenti

Credits

Servizi

▶ Quelli che conoscono tutti: profilo personale, link, album fotografici, agenda eventi, fanpage, applicazioni...

▶ Advertising

▶ Risorse per gli sviluppatori:

▶ API: Application Programming Interface

▶ FBML: Facebook Markup Language

▶ FQL: Facebook Query Language



Indagini tra le nuvole

Università degli Studi
di Catania

29 aprile 2013

Cloud Computing

Servizi popolari

➡ Facebook

Google

Dropbox

Acquisizioni

Protocollo

Strumenti

Credits

Davide Gabrini
Human, Forensic, Chaotic Good

Consapevolezza

▶ Scarsa, ovviamente. Su un miliardo di utenti, ce ne saranno **sempre** milioni disposti a credere a **qualsiasi** cosa

▶ Configurare le impostazioni di privacy é considerato difficile e noioso

▶ Secondo Sophos, 600.000 account Facebook vengono compromessi **ogni giorno**: 7 ogni secondo!

<http://nakedsecurity.sophos.com/2011/10/28/compromised-facebook-account-logins>

▶ Cosa ci si può aspettare da utenti che usano il nome dei figli come password?



Indagini tra le nuvole

Università degli Studi
di Catania

29 aprile 2013

Cloud Computing

Servizi popolari

➔ Facebook

Google

Dropbox

Acquisizioni

Protocollo

Strumenti

Credits

Davide Gabrini
Human, Forensicator,
Chaotic Good

A cartoon illustration featuring two pig-like characters. The character on the left says, "ISN'T IT GREAT? WE HAVE TO PAY NOTHING FOR THE BARN". The character on the right replies, "YEAH! AND EVEN THE FOOD IS FREE". The cartoon is set within a frame with the word "geek" written vertically on the right side.

FACEBOOK AND YOU

If you're not paying for it, you're not the customer. You're the product being sold.



Indagini tra le nuvole

Università degli Studi
di Catania

29 aprile 2013

Cloud Computing

Servizi popolari

➡ Facebook

Google

Dropbox

Acquisizioni

Protocollo

Strumenti

Credits

Privacy

▶ Le possibilità per una configurazione abbastanza granulare ci sono, ma restano poco sfruttate

▶ In ogni caso, stiamo concedendo dati ad un soggetto esterno, delegandogliene la custodia

▶ Pur con tutte le restrizioni di privacy e i controlli di sicurezza, non bisognerebbe mai caricare contenuti che non si sia disposti a vedere un giorno disvelati

▶ *Una cosa scritta in cloud é una cosa scritta in cielo ;-)*



Indagini tra le nuvole

Università degli Studi
di Catania

29 aprile 2013

Cloud Computing

Servizi popolari

➡ Facebook

Google

Dropbox

Acquisizioni

Protocollo

Strumenti

Credits

Davide Gabrini
Human, Forensicator,
Chaotic Good

Vulnerabilità

La piattaforma non é inviolabile: periodicamente si scoprono vulnerabilità per

▶ visualizzare foto riservate

<http://www.webnews.it/2011/12/07/facebook-risolta-una-grave-vulnerabilita>

▶ inviare eseguibili a qualunque utente

<http://www.webnews.it/2011/10/29/facebook-scoperta-una-nuova-vulnerabilita/>

▶ accedere ai dati sensibili degli utenti

<http://www.webnews.it/2011/07/16/facebook-ricercatore-scopre-una-vulnerabilita/>

▶ inviare messaggi per conto di altri utenti

<http://www.protezioneaccount.com/2011/12/grave-vulnerabilita-e-mail-su-facebook.html>

▶ prendere il completo controllo di un account

https://blogs.technet.com/b/feliciano_intini/archive/2011/07/22/microsoft-scopre-vulnerabilit-224-critiche-in-facebook-e-google-picasa.aspx

▶ ecc. ecc.



Indagini tra le nuvole

Università degli Studi
di Catania

29 aprile 2013

Cloud Computing

Servizi popolari

➔ Facebook

Google

Dropbox

Acquisizioni

Protocollo

Strumenti

Credits

Davide Gabrini
Human, Forensicator,
Chaotic Good

Vulnerabilità

▶ lanciare attacchi DoS su qualsiasi utente

<http://www.ehackingnews.com/2012/11/facebook-hack-vulnerability-allows.html>

▶ inviare comandi SMS spoofati

<http://www.ehackingnews.com/2012/11/facebook-hack-vulnerability-allows.html>

▶ scoprire i numeri di telefono degli utenti

<http://hothardware.com/News/Facebook-Confirms-Massive-Data-Breach-and-Vulnerability>

E non vale solo per la piattaforma:

▶ catturare le sessioni aperte di altri utenti

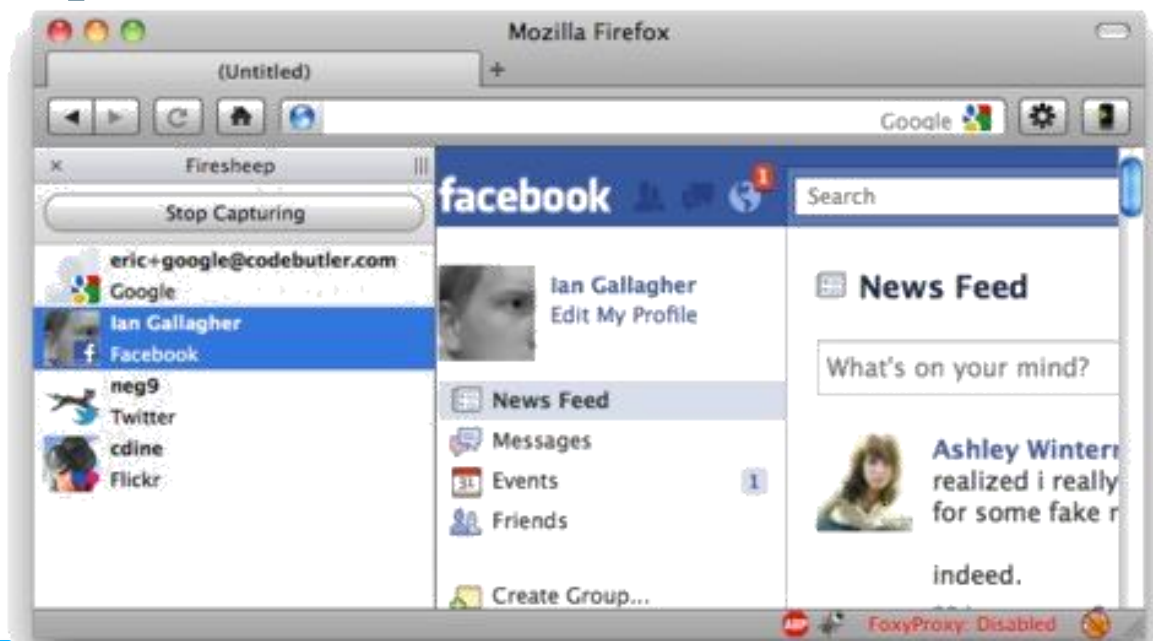
<http://www.breakthesecurity.com/2012/10/exploit-code-firefox-privacy-vulnerability.html>

▶ ecc. ecc.

Indagini tra le nuvole

Sidejacking

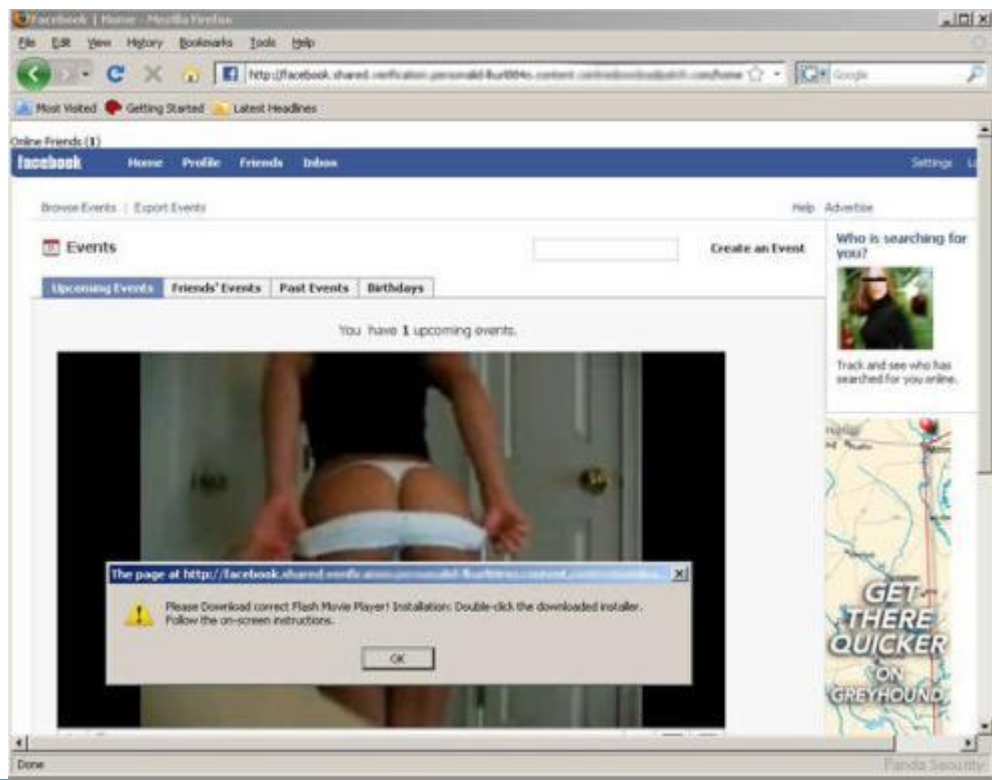
- ▶ Il session hijacking consiste nell'appropriarsi indebitamente di una sessione valida
- ▶ Ciò può avvenire tramite l'intercettazione dei magic cookie di sessione
- ▶ Poco tempo fa, Firesheep ha reso la tecnica alla portata di chiunque...



Indagini tra le nuvole

Malware

- ▶ Malicious/Rogue applications
- ▶ Malvertising: l'advertising come canale di diffusione del malware
- ▶ Viral marketing: tecniche di marketing virale per diffondere veri virus



Università degli Studi
di Catania

29 aprile 2013

Cloud Computing

Servizi popolari

Facebook

Google

Dropbox

Acquisizioni

Protocollo

Strumenti

Credits

Davide Gabrini
Human, Forensicator,
Chaotic Good



Indagini tra le nuvole

Università degli Studi
di Catania

29 aprile 2013

Cloud Computing

Servizi popolari

➔ Facebook

Google

Dropbox

Acquisizioni

Protocollo

Strumenti

Credits

Davide Gabrini
Human, Forensicator,
Chaotic Good

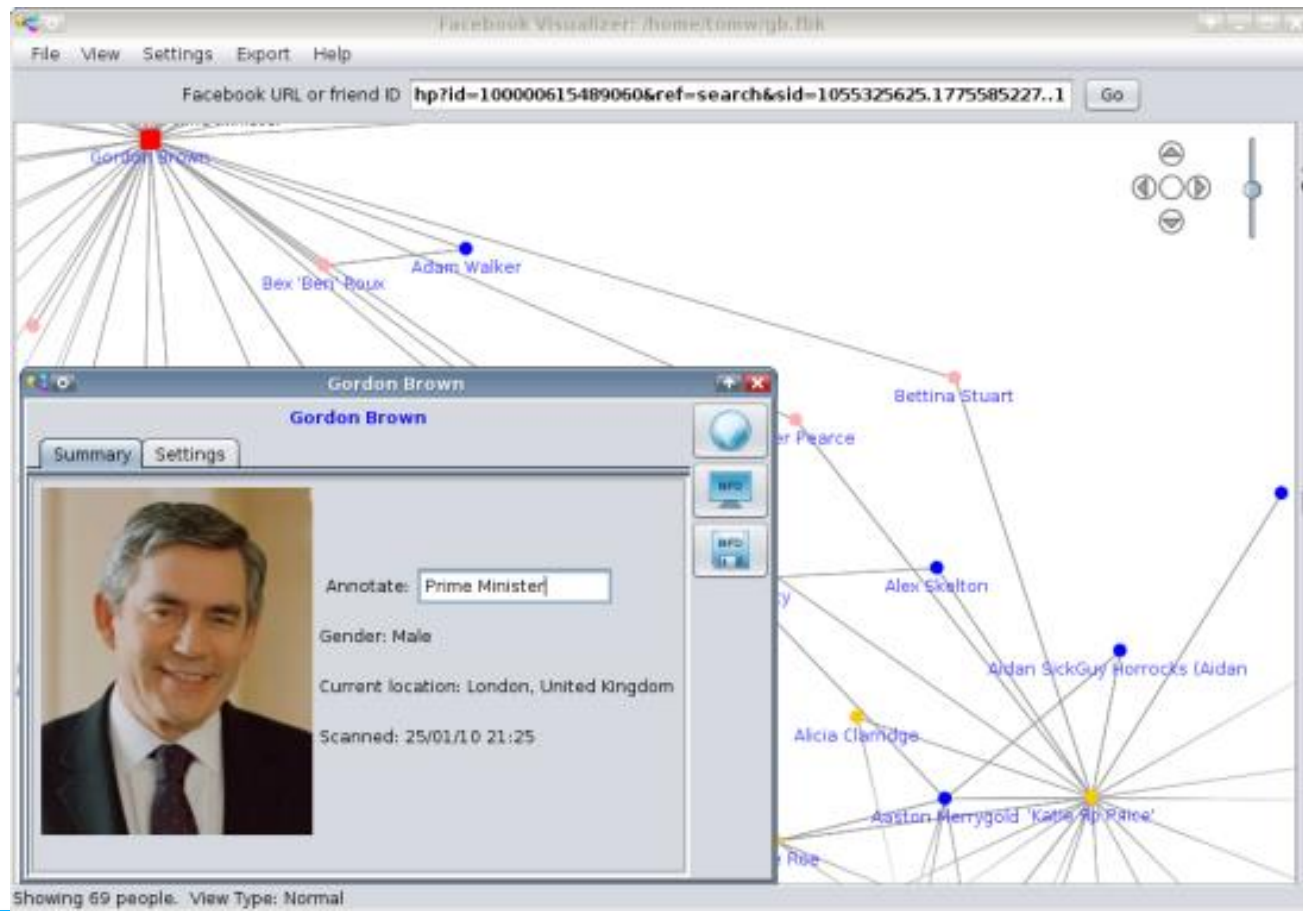
Koobface

- ▶ **Koobface** è il piú famoso worm di Facebook
- ▶ diretta la connessione su pagine di rogue antivirus o, nei casi piú fortunati, di spam
- ▶ tenta di ottenere informazioni sensibili dalle vittime (numeri di carta di credito, credenziali di accesso a servizi online)
- ▶ si diffonde inviando richieste di amicizia o link a video del tipo "Guarda come sei buffo qui..." agli altri utenti di Facebook
- ▶ il link porta ad un sito esterno a dove viene richiesto un aggiornamento (fasullo) di Flash, che infetta il PC
- ▶ dietro Koobface ci sarebbe una crew russa...
<http://ddanchev.blogspot.com/2012/01/whos-behind-koobface-botnet-osint.html>
- ▶ ...ancora in attività:
<http://ddanchev.blogspot.it/2012/11/koobface-botnet-master-krotreal-back-in.html>

Indagini tra le nuvole

Altri strumenti

- ▶ Unofficial Maltego Facebook transform
- ▶ Facebook Visualizer



Università degli Studi
di Catania

29 aprile 2013

Cloud Computing

Servizi popolari

▶ Facebook

Google

Dropbox

Acquisizioni

Protocollo

Strumenti

Credits

Daide Gabrini
Human, Forensic, Chaotic Good

Indagini tra le nuvole

Università degli Studi
di Catania

29 aprile 2013

Cloud Computing

Servizi popolari

Facebook

Google

Dropbox

Acquisizioni

Protocollo

Strumenti

Credits

Davide Gabrini
Human, Forensicator,
Chaotic Good

Acquisizione con credenziali

Generale

- Protezione
- Notifiche
- Applicazioni
- Mobile
- Pagamenti
- Inserzioni di Facebook

Puoi visitare anche le tue impostazioni sulla privacy o modificare il tuo diario per controllare chi può visualizzare queste informazioni.

Impostazioni generali dell'account

Nome	Davide Gabrini	Modifica
Nome utente	http://www.facebook.com/gabrini	Modifica
E-mail	Principale: rebus@tipiloschi.net	Modifica
Password	L'ultima modifica alla password risale a più di un anno fa.	Modifica
Reti	Nessuna rete.	Modifica
Account collegati	Hai 0 account collegati.	Modifica
Lingua	Italiano	Modifica

[Scarica una copia](#) dei tuoi dati di Facebook.

Facebook © 2012 · Italiano

Scarica le tue informazioni

Otteni una copia dei contenuti che hai condiviso su Facebook.

Scarica ed esplora facilmente un archivio personale delle tue foto, dei tuoi post e messaggi di Facebook. Ottieni maggiori informazioni su come scaricare una copia delle tue informazioni.

Avvia al mio archivio

Cosa include il tuo archivio?

- Tutte le foto o i video che hai condiviso su Facebook
- I tuoi post in bacheca, messaggi e conversazioni in chat
- I nomi dei tuoi amici e alcuni dei loro indirizzi e-mail

(Nota: includeremo solo gli indirizzi e-mail degli amici che hanno attivato questa opzione nelle loro impostazioni account).

Cosa non include il tuo archivio?

- Le foto e gli aggiornamenti di stato dei tuoi amici
- Informazioni personali di altre persone
- Commenti che hai fatto sui post di altre persone

Attenzione: proteggi il tuo archivio

Il tuo archivio di Facebook include informazioni riservate, come i tuoi post in bacheca privati, le tue foto e le informazioni del tuo profilo. Tienilo a mente prima di salvare, inviare o caricare il tuo archivio su altri siti o servizi.



Indagini tra le nuvole

Università degli Studi
di Catania

29 aprile 2013

Cloud Computing

Servizi popolari

Facebook

Google

Dropbox

Acquisizioni

Protocollo

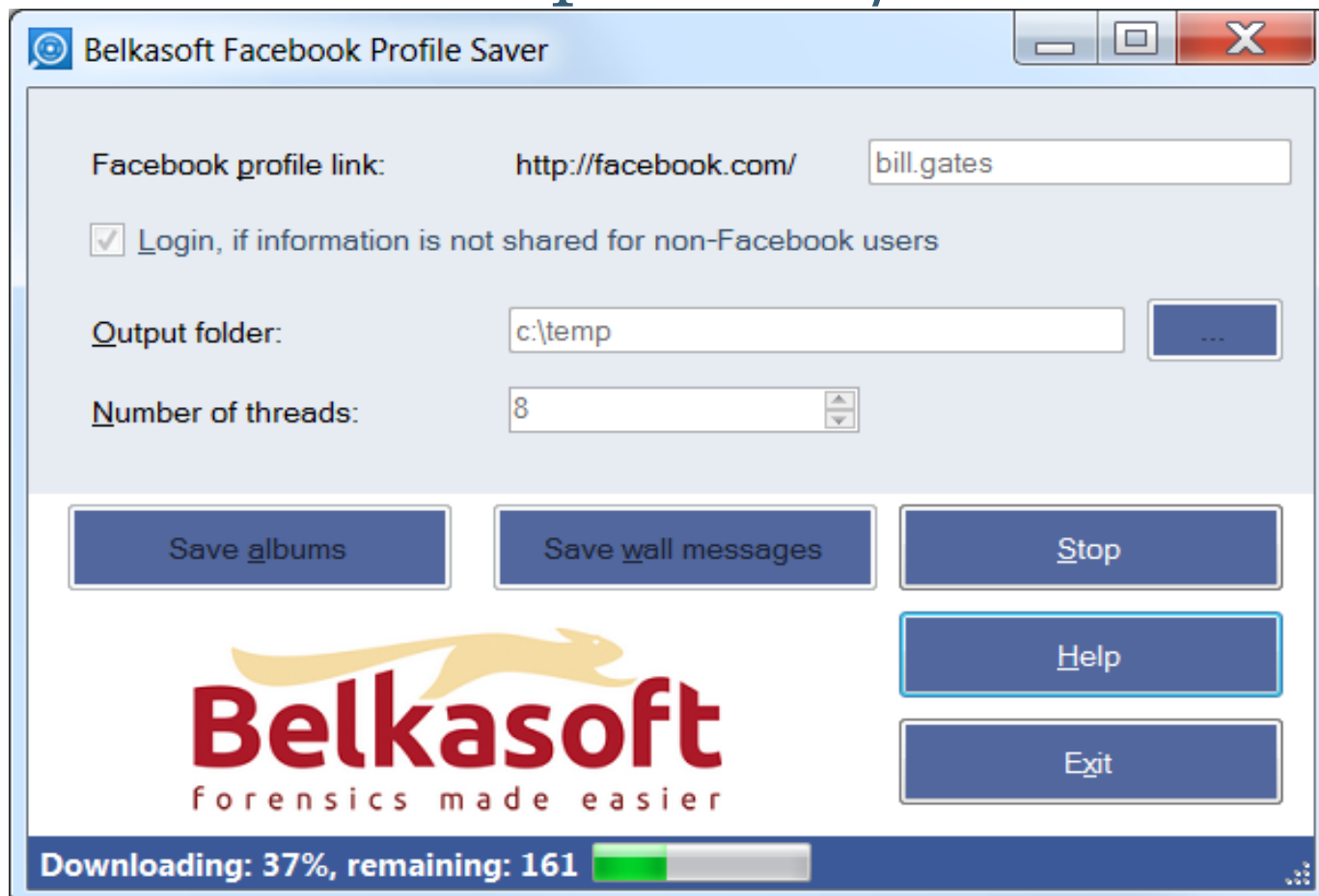
Strumenti

Credits

Davide Gabrini
Human, Forensicator,
Chaotic Good

Facebook Profile Saver

► Applicazione freeware per
l'acquisizione di dati pubblici/visibili





Indagini tra le nuvole

Università degli Studi
di Catania

29 aprile 2013

Cloud Computing

Servizi popolari

Facebook

➡ Google

Dropbox

Acquisizioni

Protocollo

Strumenti

Credits

Google



Indagini tra le nuvole

Università degli Studi
di Catania

29 aprile 2013

Cloud Computing

Servizi popolari

Facebook

→ Google

Dropbox

Acquisizioni

Protocollo

Strumenti

Credits

Statistica

▶ Nasce nel 1998

▶ È il sito web piú visitato al mondo

▶ Nel 2010 il numero di server utilizzati è stato stimato a 900.000

▶ Google+ nasce nel luglio 2011

▶ A dicembre 2012 conta 500 milioni di iscritti, di cui *solo* 235M attivi al mese

▶ l'iscrizione é pressoché coatta

Indagini tra le nuvole

Università degli Studi
di Catania

29 aprile 2013

Cloud Computing

Servizi popolari

Facebook

→ Google

Dropbox

Acquisizioni

Protocollo

Strumenti

Credits

Servizi

▶ Google+ è solo l'ultima di una numerosa famiglia di applicazioni

▶ Gmail, Docs, Blogger, Calendar, Gtalk, Contacts, Orkut, Picasa, YouTube, Maps...

▶ ...oltre ai servizi per aziende e webmaster...





Indagini tra le nuvole

Università degli Studi
di Catania

29 aprile 2013

Cloud Computing

Servizi popolari

Facebook

→ Google

Dropbox

Acquisizioni

Protocollo

Strumenti

Credits

Dalle norme sulla privacy

▶ Registreremo le informazioni relative all'attività dell'utente, ad esempio i post per cui inserisce un commento e gli utenti con cui interagisce, per ottimizzare l'esperienza di tutti gli utenti (mah, ndr)

▶ Potremmo anche raccogliere informazioni sull'utente da altri utenti, ad esempio da qualcuno che inserisce l'utente in una delle proprie cerchie o lo tagga in una foto.

▶ Alcuni utenti potrebbero decidere di visualizzare pubblicamente informazioni relative a un altro utente, ad esempio il nome e la foto

▶ quando si condivide un contenuto tramite Google+, chiunque lo riceva potrà dividerlo con altri.

▶ Se qualcuno tagga l'utente in una foto o un video condiviso, l'utente può rimuovere il tag. (solo a posteriori, ndr)

▶ Se le persone in contatto con l'utente utilizzano delle applicazioni, è possibile che tali applicazioni siano in grado di accedere a quei contenuti e quelle informazioni sull'utente che sono normalmente accessibili dalle suddette persone.



Indagini tra le nuvole

Università degli Studi
di Catania

29 aprile 2013

Cloud Computing

Servizi popolari

Facebook

→ Google

Dropbox

Acquisizioni

Protocollo

Strumenti

Credits

Dashboard

▶ La Dashboard è uno strumento con cui gli utenti possono controllare i dati associati al loro account

▶ Riepiloga i prodotti attivati per l'account e i dati associati a ciascun prodotto

▶ Include oltre 20 prodotti e servizi, tra i quali Gmail, Calendar, Documenti, Cronologia web, Google Alert, YouTube ecc. ecc.

▶ Non ci sono davvero *tutti* i dati relativi all'utente che Google conserva ed elabora...

▶ Log, cookies, profilazione delle preferenze...

Indagini tra le nuvole

Università degli Studi
di Catania

29 aprile 2013

Cloud Computing

Servizi popolari

Facebook

➡ Google

Dropbox

Acquisizioni

Protocollo

Strumenti

Credits

Davide Gabrini
Human, Forensicator,
Chaotic Good

Google Takeout

▶ Con Takeout gli utenti possono creare un backup dei loro dati










Takeout

Tutti i tuoi dati

Scegli i servizi

Download

Data creazione: 29/gen/2012 13:56:22

 Buzz	File: Dimensione:	
 Cerchie	File: Dimensione:	
 Documenti	File: Dimensione:	
 Contatti	File: Dimensione:	
 Knol	File: Dimensione:	
 Picasa Web Album	File: Dimensione:	
 Profilo	File: Dimensione:	
 Stream	File: Dimensione:	
 +1	File: Dimensione:	
 Voice	File: Dimensione:	

Disponibile fino al:

Scaduto il:

Inviarmi un'email quando è pronto

Indagini tra le nuvole

Cloud Forensics con F-Response

<http://computer-forensics.sans.org/blog/2013/04/09/cloud-forensics-with-f-response>

The screenshot displays the F-Response software interface. It features two main windows: 'F-Response® Cloud Storage Connector' and 'F-Response® Email Connector'. The 'Email Connector' window is open to the 'Configure Credentials' menu, which includes options for 'Configure GMail Email Account Credentials', 'Configure Yahoo! Email Account Credentials', and 'Generic IMAP Account Credentials'. A 'Configure GMail Credentials' dialog box is also visible, showing fields for 'Description' (Forensic Methods Mail), 'Email Address' (chad@forensicmethods.com), and 'Password'. A 'Test Credential' button is present. Below these windows, a table lists the configured email accounts. The table has columns for 'F-Response Email Account Target', 'Description', 'Message...', 'Provider', 'Connected', and 'Local Volume'. The entry for 'chad@forensicmethods.com' is highlighted in yellow, with the 'Local Volume' column containing '\\.\J:'.

F-Response Email Account Target	Description	Message...	Provider	Connected	Local Volume
chad@forensicmethods.com	Forensic Methods	51	Google Mail ...	Connected	\\.\J:

Università degli Studi
di Catania

29 aprile 2013

Cloud Computing

Servizi popolari

Facebook

Google

Dropbox

Acquisizioni

Protocollo

Strumenti

Credits

Davide Gabrini
Human, Forensicator,
Chaotic Good



Indagini tra le nuvole

Università degli Studi
di Catania

29 aprile 2013

Cloud Computing

Servizi popolari

Facebook

Google

➡ Dropbox

Acquisizioni

Protocollo

Strumenti

Credits

Dropbox

Davide Gabrini
Human, Forensicator,
Chaotic Good



Indagini tra le nuvole

Università degli Studi
di Catania

29 aprile 2013

Cloud Computing

Servizi popolari

Facebook

Google

Dropbox

Acquisizioni

Protocollo

Strumenti

Credits

Daide Gabrini
Human, Forensic,
Chaotic Good

Descrizione

- ▶ Servizio di storage cloud based
- ▶ Superati i 100 milioni di utenti
- ▶ Un miliardo di file salvati ogni giorno
- ▶ Utilizzabile via web o con client multiplatforma (Windows, Mac OS X, Linux, iOS, BlackBerry OS e Android)
- ▶ Nell'ultimo caso, mantiene sincronizzata una cartella locale
- ▶ I trasferimenti avvengono via SSL
- ▶ Lo storage remoto é cifrato AES-256



Indagini tra le nuvole

Università degli Studi
di Catania

29 aprile 2013

Cloud Computing

Servizi popolari

Facebook

Google

➡ Dropbox

Acquisizioni

Protocollo

Strumenti

Credits

Davide Gabrini
Human, Forensic,
Chaotic Good

Privacy

▶ A seguito di un esposto alla Federal Trade Commission, le condizioni d'uso del servizio sono state modificate:

Tutti i file memorizzati su server di Dropbox sono criptati (AES - 256) e sono inaccessibili senza la password del vostro account.

è diventato:

Tutti i file memorizzati su server di Dropbox sono cifrati (AES - 256).

*i dipendenti di Dropbox **non sono in grado** di accedere ai file degli utenti*

è diventato:

ai dipendenti di Dropbox è fatto divieto di visualizzare il contenuto dei file memorizzati negli account degli utenti



Indagini tra le nuvole

Università degli Studi
di Catania

29 aprile 2013

Cloud Computing

Servizi popolari

Facebook

Google

Dropbox

Acquisizioni

Protocollo

Strumenti

Credits

Daide Gabrini
Human, Forensicator,
Chaotic Good

Consapevolezza

▶ Public is **public!**

▶ La cartella pubblica non é “sfogliabile”,
ma occorre conoscere l’URL di ogni
risorsa per potervi accedere

▶ l’URL però può essere indovinato...

▶ `http://dl.dropbox.com/u/[user-ID]/[nomefile]`

▶ Una ricerca **RingoBongo Ltd.™** ha
dimostrato la presenza di numerosi
documenti con dati sensibili
abbandonati nelle cartelle public



Indagini tra le nuvole

Università degli Studi
di Catania

29 aprile 2013

Cloud Computing

Servizi popolari

Facebook

Google

Dropbox

Acquisizioni

Protocollo

Strumenti

Credits

Davide Gabrini
Human, Forensicator,
Chaotic Good

Strumenti di analisi

▶ Dropbox Reader di CyberMarshall

cybermarshal.com/index.php/cyber-marshall-utilities/dropbox-reader

▶ Dropbox Decryptor di Maget Forensics

info.magnetforensics.com/dropbox-decryptor

▶ Applicazioni per la lettura di dati e metadati di una casella Dropbox

▶ lavorano sugli artefatti locali, non sulla casella remota!

▶ Il metodo piú raccomandabile per acquisizione da remoto rimane al momento l'interfaccia web



Indagini tra le nuvole

Università degli Studi
di Catania

29 aprile 2013

Cloud Computing

Servizi popolari

Facebook

Google

Dropbox

Acquisizioni

➡ Protocollo

Strumenti

Credits

Protocollo di acquisizione

Daide Gabrini
Human, Forensicator,
Chaotic Good

Indagini tra le nuvole

Dossier

Formazione di un dossier articolato in 5 punti:

- ▶ Setup
- ▶ Screencast
- ▶ Network dump
- ▶ Log applicativi
- ▶ Relazione/Verbale



Università degli Studi
di Catania

29 aprile 2013

Cloud Computing

Servizi popolari

Facebook

Google

Dropbox

Acquisizioni

▶ Protocollo

Strumenti

Credits



Indagini tra le nuvole

Università degli Studi
di Catania

29 aprile 2013

Cloud Computing

Servizi popolari

Facebook

Google

Dropbox

Acquisizioni

➡ Protocollo

Strumenti

Credits

Davide Gabrini
Human, Forensicator,
Chaotic Good

Setup

- ▶ Descrizione del sistema, delle componenti hardware e software
- ▶ Configurazione di rete
 - ▶ Topografia, interfacce, IP, routing, DNS, proxy... NTP...
- ▶ Configurazione applicativi
 - ▶ Browser, versione, estensioni, plug-in...
- ▶ Possibilmente, file di configurazione inclusi nel dossier
- ▶ L'utilizzo di live CD idonei, come BackTrack o DEFT, agevola il lavoro di documentazione



Indagini tra le nuvole

Università degli Studi
di Catania

29 aprile 2013

Cloud Computing

Servizi popolari

Facebook

Google

Dropbox

Acquisizioni

➔ Protocollo

Strumenti

Credits

Daide Gabrini
Human, Forensicator,
Chaotic Good

Screencast

▶ Cattura video

▶ Commento e lettura dati in presa diretta

▶ Eventuali screenshot maggiormente significativi

▶ File generati sottoposti ad hash o meglio ancora firma digitale



Indagini tra le nuvole

Network dump

► Acquisizione dell'intero traffico di rete della workstation durante lo svolgimento delle operazioni

► File risultanti sottoposti ad hash o firma digitale



Università degli Studi
di Catania

29 aprile 2013

Cloud Computing

Servizi popolari

Facebook

Google

Dropbox

Acquisizioni

► Protocollo

Strumenti

Credits

Davide Gabrini

Human, Forensicator,
Chaotic Good



Indagini tra le nuvole

Università degli Studi
di Catania

29 aprile 2013

Cloud Computing

Servizi popolari

Facebook

Google

Dropbox

Acquisizioni

➡ Protocollo

Strumenti

Credits

Log applicativi

▶ Log del (personal) firewall

▶ Log dell'antivirus

▶ Log dei programmi applicativi

▶ Salvataggio di eventuali cache o
cartelle temporanee dei client

▶ Indovina? Hash o firma digitale 😊

Davide Gabrini

Human, Forensicator,
Chaotic Good



Indagini tra le nuvole

Università degli Studi
di Catania

29 aprile 2013

Cloud Computing

Servizi popolari

Facebook

Google

Dropbox

Acquisizioni

➡ Protocollo

Strumenti

Credits

Davide Gabrini
Human, Forensicator,
Chaotic Good

Relazione/Verbale

- ▶ Tutta l'attività deve essere opportunamente documentata e "giustificata" anche dal punto di vista formale e procedurale
- ▶ Un verbale è indispensabile per dare validità ad un atto e inquadrarlo nella fattispecie più corretta
- ▶ Una relazione è necessaria per illustrare l'operato in forma riassuntiva e di facile comprensione



Indagini tra le nuvole

Università degli Studi
di Catania

29 aprile 2013

Cloud Computing

Servizi popolari

Facebook

Google

Dropbox

Acquisizioni

➡ Protocollo

Strumenti

Credits

Applicazione del protocollo



Indagini tra le nuvole

Applicazione del protocollo

▶ Se dovesse mancarci il tempo (o la connettività) per una dimostrazione live sulla creazione di un dossier, potete trovarne una registrata e commentata su TipiLoschi.net

www.tipiloschi.net/drupal/?q=acquisizioni-web-con-DEFT-Linux



Università degli Studi
di Catania

29 aprile 2013

Cloud Computing

Servizi popolari

Facebook

Google

Dropbox

Acquisizioni

➡ Protocollo

Strumenti

Credits

Davide Gabrini
Human, Forensic, Chaotic Good



Indagini tra le nuvole

Università degli Studi
di Catania

29 aprile 2013

Cloud Computing

Servizi popolari

Facebook

Google

Dropbox

Acquisizioni

Protocollo

➔ **Strumenti**

Credits

Strumenti dedicati



Daide Gabrini
Human, Forensicator,
Chaotic Good



Indagini tra le nuvole

Università degli Studi
di Catania

29 aprile 2013

Cloud Computing

Servizi popolari

Facebook

Google

Dropbox

Acquisizioni

Protocollo

➡ Strumenti

Credits

Davide Gabrini
Human, Forensicator,
Chaotic Good

FAW Project

- ▶ Progetto di Davide Bassani e Matteo Zavattari
- ▶ Browser Windows specificamente dedicato all'acquisizione forense di contenuti web
 - ▶ Acquisizione parziale o totale delle pagine web
 - ▶ Acquisizione delle pagine contenenti streaming video
 - ▶ Acquisizione pagine con frame
 - ▶ Acquisizione di tutti gli elementi grafici
 - ▶ Acquisizione dei tooltip
 - ▶ Acquisizione codice html della pagine Web
 - ▶ Possibilità di cambiare user agent
 - ▶ Gestione dei casi e delle acquisizioni
 - ▶ Multiutente (utilizzo da diversi investigatori)
 - ▶ Calcolo automatico di hash md5 e sha1 di tutti i file acquisiti
 - ▶ File di riepilogo di ogni acquisizione

▶ <http://www.fawproject.com>

Indagini tra le nuvole

FAW Project

Università degli Studi
di Catania

29 aprile 2013

Cloud Computing

Servizi popolari

Facebook

Google

Dropbox

Acquisizioni

Protocollo

➡ Strumenti

Credits

Davide Gabrini
Human, Forensicor,
Chaotic Good

The screenshot shows a web browser window titled "FAW - Forensics Analysis of Website" with the URL "https://www.facebook.com/". The browser has several tabs open: "F10 - Navigazione", "F11 - Acquisizione", and "F12 - Acquisizione". The Facebook page is for "Davide Bassani" (Davide Bassani). The profile picture shows a man. The main content area displays a post from "Parco Campo Dei Fiori" with the text "Parco Campo Dei Fiori è stato taggato nelle foto di Mirko Tomasi. — presso Parco Del Campo Dei Fiori." and three photos of white fabric-like structures. Below this is another post titled "Estate" with the text "Bella :) Vi piace?". The right sidebar contains several sponsored posts and advertisements, including "Corso di giardinaggi...", "Single su Facebook", "Michela Barzi - ETICO A", "Visto che buono", "Guadagna €600 al giorno", and "CONFERENZA ALLA COOP". The bottom of the browser window shows a "Documento completo" status.

Indagini tra le nuvole

Live Network Evidence Collector

► Progetto del Dipartimento di Informatica dell'Università di Salerno

► «A forensically-sound proxy method to collect network digital evidence»

► Introduce un elemento **terzo** nella fase di accertamento, con i pro e i contro che la scelta comporta

► Maggiori informazioni su <http://netforensic.dia.unisa.it>



Università degli Studi
di Catania

29 aprile 2013

Cloud Computing

Servizi popolari

Facebook

Google

Dropbox

Acquisizioni

Protocollo

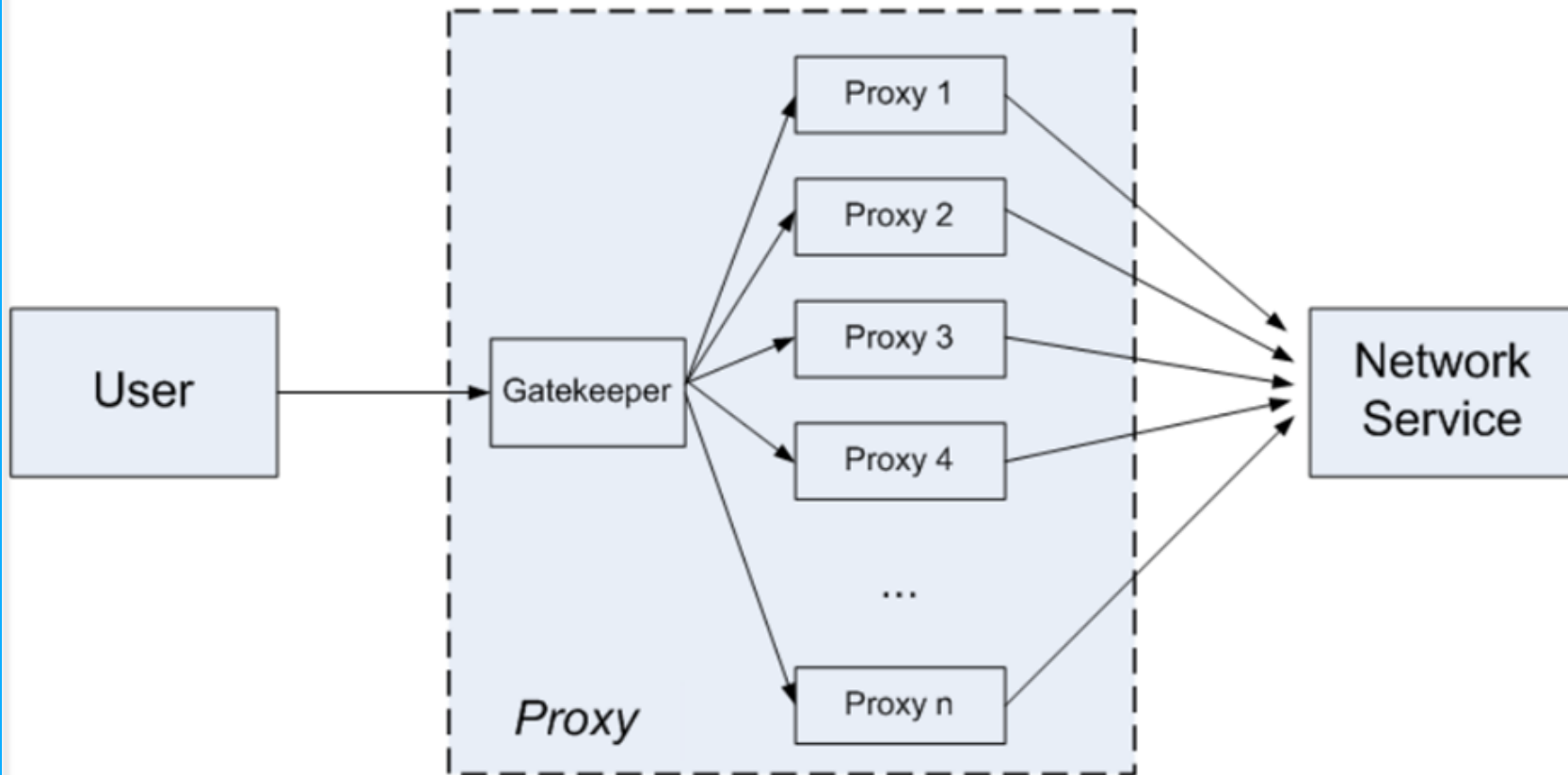
► Strumenti

Credits

Davide Gabrini
Human, Forensicator,
Chaotic Good

Indagini tra le nuvole

Acquisizioni tramite proxy



Università degli Studi
di Catania
29 aprile 2013

Cloud Computing

Servizi popolari

Facebook

Google

Dropbox

Acquisizioni

Protocollo

➡ Strumenti

Credits

Davide Gabrini
Human, Forensicator,
Chaotic Good

Indagini tra le nuvole

Università degli Studi
di Catania

29 aprile 2013

Cloud Computing

Servizi popolari

Facebook

Google

Dropbox

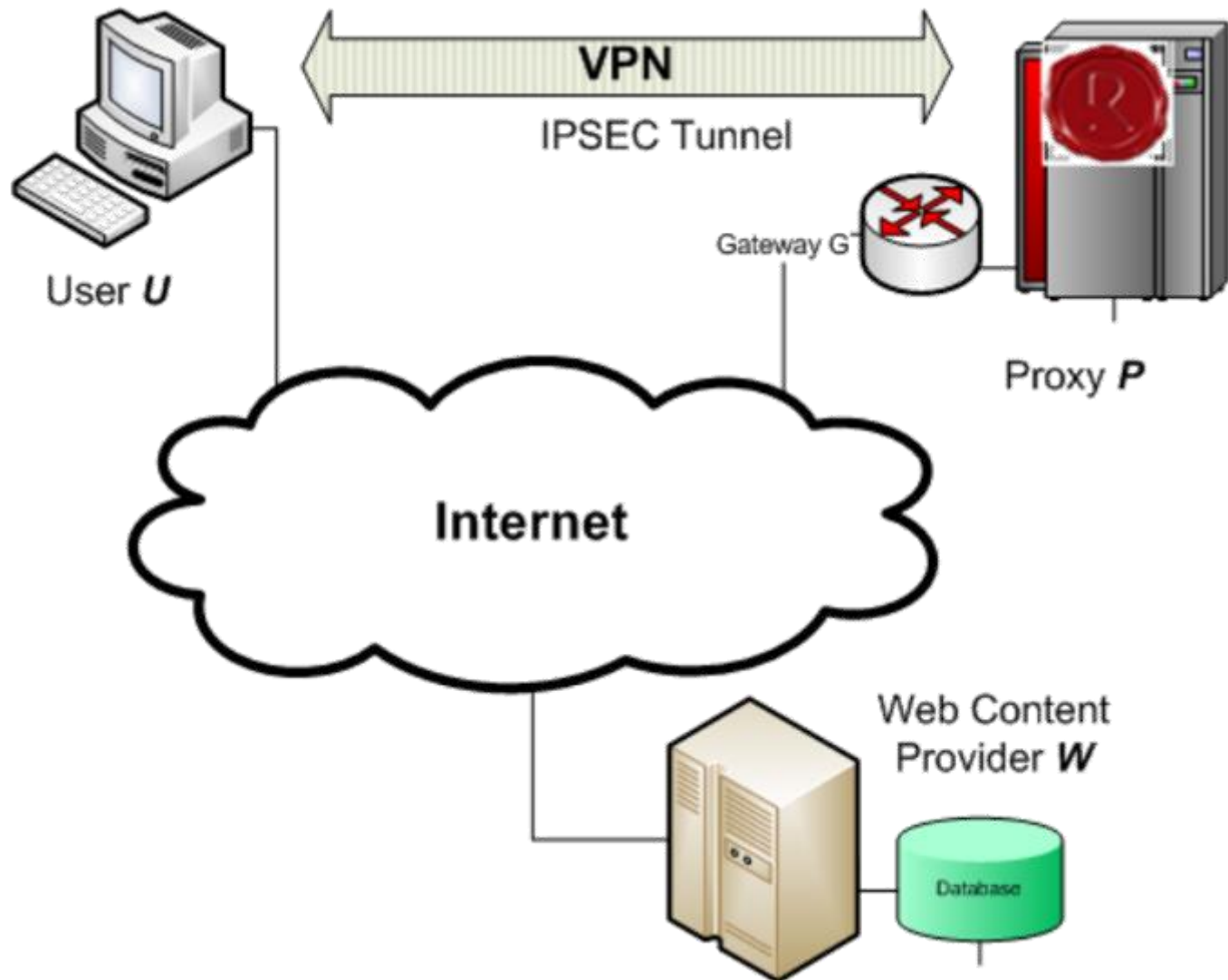
Acquisizioni

Protocollo

➡ Strumenti

Credits

Utilizzo via Internet



Indagini tra le nuvole

Reportistica certificata automatizzata

Università degli Studi
di Catania

29 aprile 2013

Cloud Computing

Servizi popolari

Facebook

Google

Dropbox

Acquisizioni

Protocollo

Strumenti

Credits

Davide Gabrini
Human, Forensicator,
Chaotic Good

The screenshot shows a desktop environment with a blue background. A Facebook profile window for 'NetForensic.dia.unisa.it' is open. In the foreground, a browser window displays the 'Pagina iniziale - Fedora Project' website. A light blue 'Download Area' table is overlaid on the browser window, listing download records with dates, times, dimensions, and download links.

Data	Dimensioni	Scarica
15 maggio 2012 alle ore 15:51	27349KB	download
15 maggio 2012 alle ore 11:48	2201KB	download
15 maggio 2012 alle ore 11:46	436KB	download
14 maggio 2012 alle ore 15:51	39453KB	download
14 maggio 2012 alle ore 15:36	11094KB	download
14 maggio 2012 alle ore 15:19	2152KB	download



Indagini tra le nuvole

Università degli Studi
di Catania

29 aprile 2013

Cloud Computing

Servizi popolari

Facebook

Google

Dropbox

Acquisizioni

Protocollo

Strumenti

➡ Credits

Davide Gabrini
Human, Forensicator,
Chaotic Good

Teniamoci in contatto...

Davide **Rebus** Gabrini



e-mail:

rebus@mensa.it

davide.gabrini@giustizia.it

GPG Public Key: (available on keyserver.linux.it)

www.tipiloschi.net/rebus.asc

KeyID: 0x176560F7

Instant Messaging:

MSN therebus@hotmail.com

ICQ 115159498

Yahoo! therebus

Skype therebus

Mi trovate anche su Facebook, Twitter, **LinkedIn...**

Queste e altre cazzate su <http://www.tipiloschi.net>