
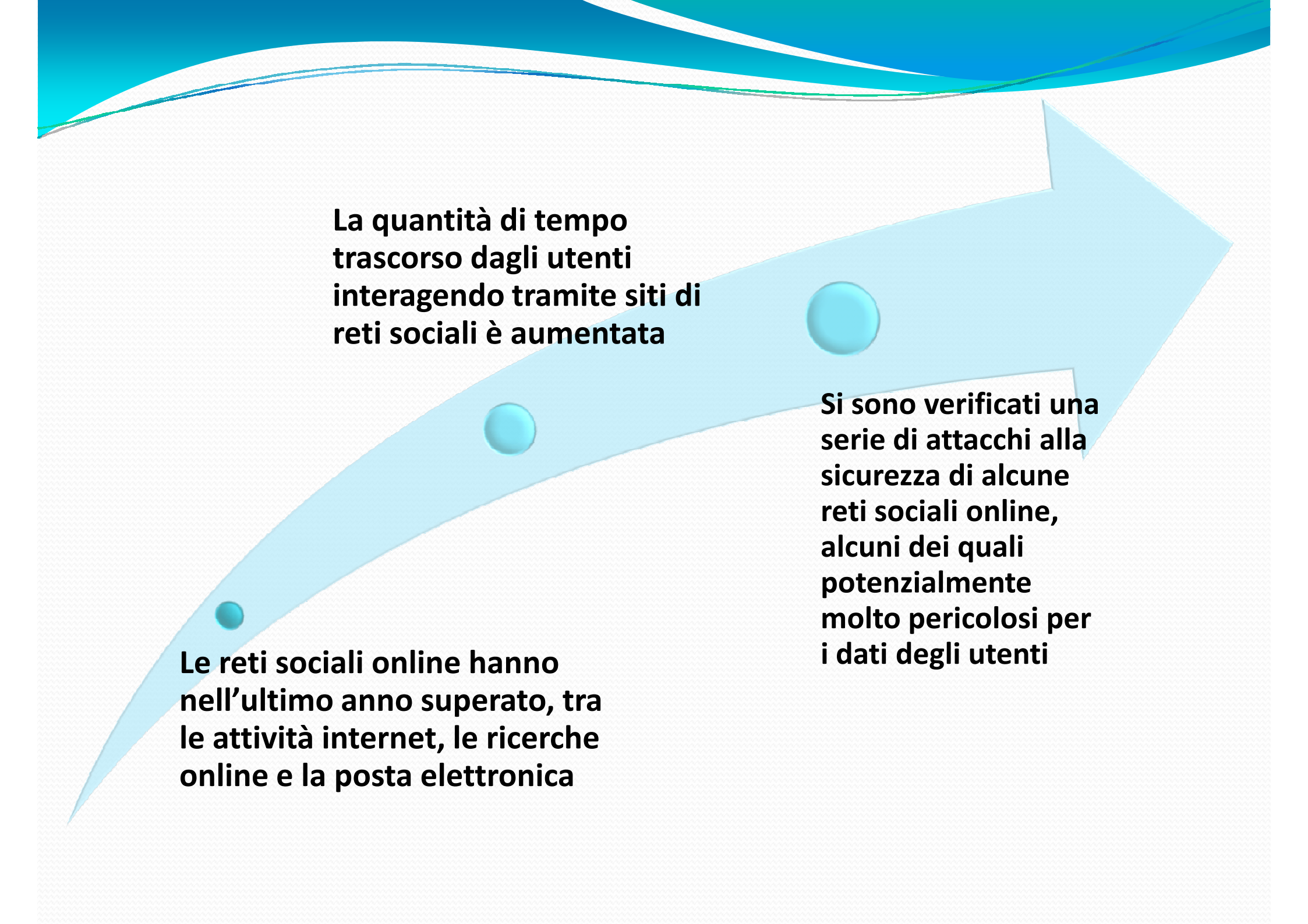


# Problematiche di sicurezza delle reti sociali online

yvette@yvetteagostini.it

- 
- Reti sociali (social networks) online
  - ... e relative problematiche di sicurezza e privacy
  - Esempi:
    - Samy: il velocissimo worm di MySpace.com
    - re-identificazione : l'ago nel pagliaio ai tempi del web2.0
    - Twitter clickjacking: per qualche link in più
  - Q&A

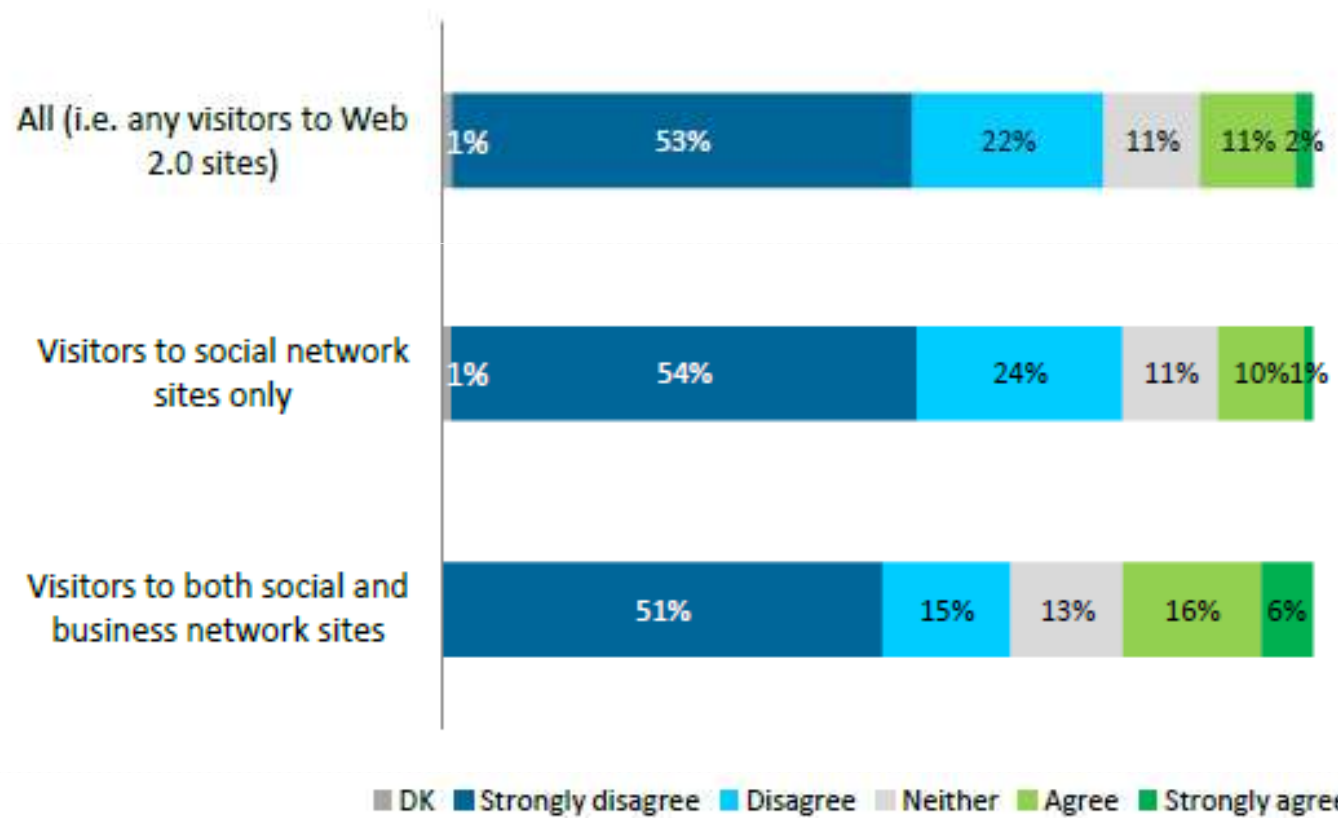
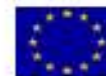


**La quantità di tempo  
trascorso dagli utenti  
interagendo tramite siti di  
reti sociali è aumentata**

**Le reti sociali online hanno  
nell'ultimo anno superato, tra  
le attività internet, le ricerche  
online e la posta elettronica**

**Si sono verificati una  
serie di attacchi alla  
sicurezza di alcune  
reti sociali online,  
alcuni dei quali  
potenzialmente  
molto pericolosi per  
i dati degli utenti**

Level of agreement with 'I am willing to give my email account details, including password to invite friends to a social application'



Mean score	
Scale: 1 = strongly disagree --> 5 = strongly agree	
All (i.e. any visitors to Web 2.0 sites)	1.8
Visitors to social network sites only	1.8
Visitors to both social and business network sites	2.1

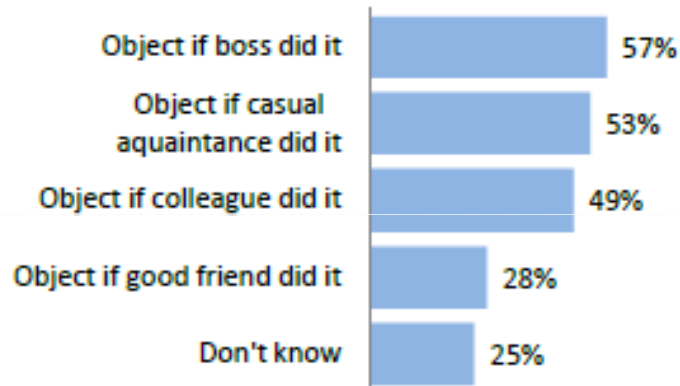
Base: Visitors to Web 2.0 sites (Social Networking, photo sharing etc...)(1606)/  
social site only (1336)/  
social and business site (270)



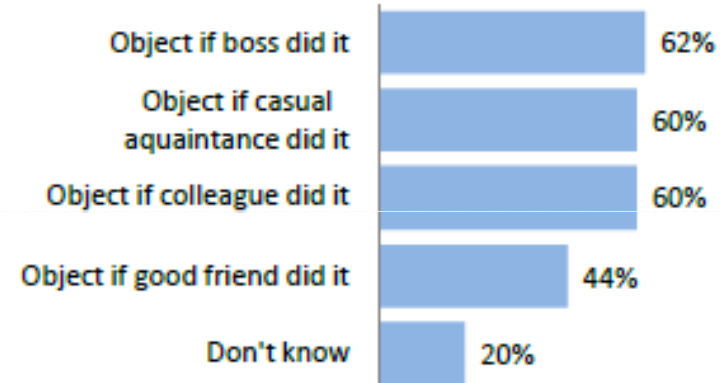
# Scenarios when would object to specific actions taken without your permission



## Scenario: posting a photo of you



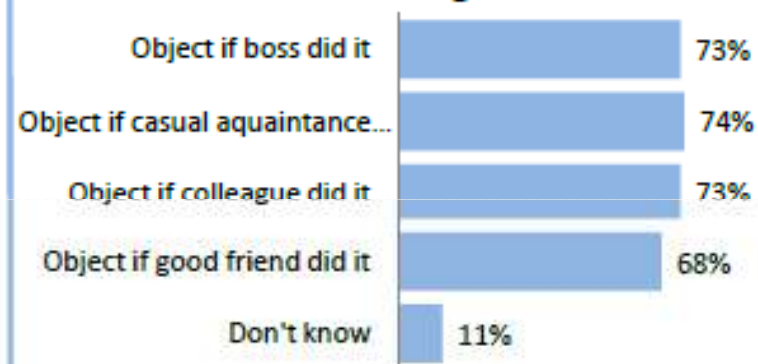
## Scenario: posting your photo and tagging with social networking profile



## Scenario: posting your photo and tagging with email address




## Scenario: publishing your email address on their blog/social networking site



Base: Visitors to Web 2.0 sites (Social Networking, photo sharing etc...)(1606)



- 
- Informazioni private
  - Informazioni di natura finanziaria
  - Reputazione individuale o aziendale
  - Segreti industriali
  - Proprietà intellettuali
  - Risorse di rete e di calcolo

## Tecnologie web2.0

- **Applicazioni che includono AJAX e flash**
- **Contenuti web generati dagli utenti usando applicazioni browser-based**
- **Codici lato client spesso intrinsecamente insicuri: widgets, iframes**
- **Servizi dinamici di natura cooperativa che trattano dinamicamente contenuti da sorgenti multiple (mashups, syndication)**

## Il fattore umano

- **Gestione della relazione di trust tra siti, tra utenti, tra diverse identità di stesso utente**
- **Tagging indiscriminato**
- **Incapacità di distinguere se un dato sistema è controllato da un umano o se si tratta di un bot (captcha)**
- **Behavioural marketing**
- **Divulgazione di informazioni riservate**

# Meccanismi di injection di contenuto malevolo nei siti

- Sicurezza del web server
- Contenuti contribuiti dagli utenti
- advertising
- third-party widgets

# Samy: MySpace XSS worm

Samy (XSS) - Wikipedia, the free encyclopedia - Mozilla Firefox

File Modifica Visualizza Cronologia Segnalibri Strumenti ?

http://en.wikipedia.org/wiki/Samy\_(XSS)

La Repubblica.it » Ho... Più visitati Press This Ultime notizie Post to Soup Whois By IP Address Risultato del test dell'i... code-of-best-practice...

enisa white... ENISA: Index ENISA: Po... enisa\_pp... enisa\_surv... provos.pdf... slides.pdf (... 0424-w3ctr... WikiWatch... W Samy (... x

Help us improve Wikipedia by **supporting it financially**. Log in / create account

article discussion edit this page history

## Samy (XSS)

From Wikipedia, the free encyclopedia

**Samy** (also known as **JS.Spacehero**)<sup>[1]</sup> was an XSS Worm developed to propagate across the MySpace social-networking site. At the time of release it gained significant media attention.

MySpace filed a lawsuit against the virus creator, Samy Kamkar. He entered a plea agreement, on January 31, 2007, to a felony charge.<sup>[2]</sup> The action resulted in Kamkar being sentenced to three years probation, 90 days community service and an undisclosed amount of restitution.

The worm carried a payload that would display the string "but most of all, Samy is my hero" on a victim's profile. When a user viewed that profile, they would have the payload planted on their page. Within just 20 hours<sup>[3]</sup> of its October 4, 2005 release, over one million users had run the payload,<sup>[4]</sup> making Samy one of the fastest spreading viruses of all time.<sup>[5]</sup>

Execution of the payload resulted in a "friend request" automatically being made to the author of the virus and in messages containing the payload being left on the profiles of the friends of the victim.

### References

[edit]

- <sup>1</sup> ^ "JS/Spacehero-A, Sophos threat analysis" Sophos.
- <sup>2</sup> ^ Mann, Justin (2007-01-31). "MySpace speaks about Samy Kamkar's sentencing" Techspot.com.
- <sup>3</sup> ^ MySpace Worm Explanation
- <sup>4</sup> ^ "Cross-Site Scripting Worm Floods MySpace" Slashdot.
- <sup>5</sup> ^ <http://net-security.org/dl/articles/WHXSSThreats.pdf>

### External links

[edit]

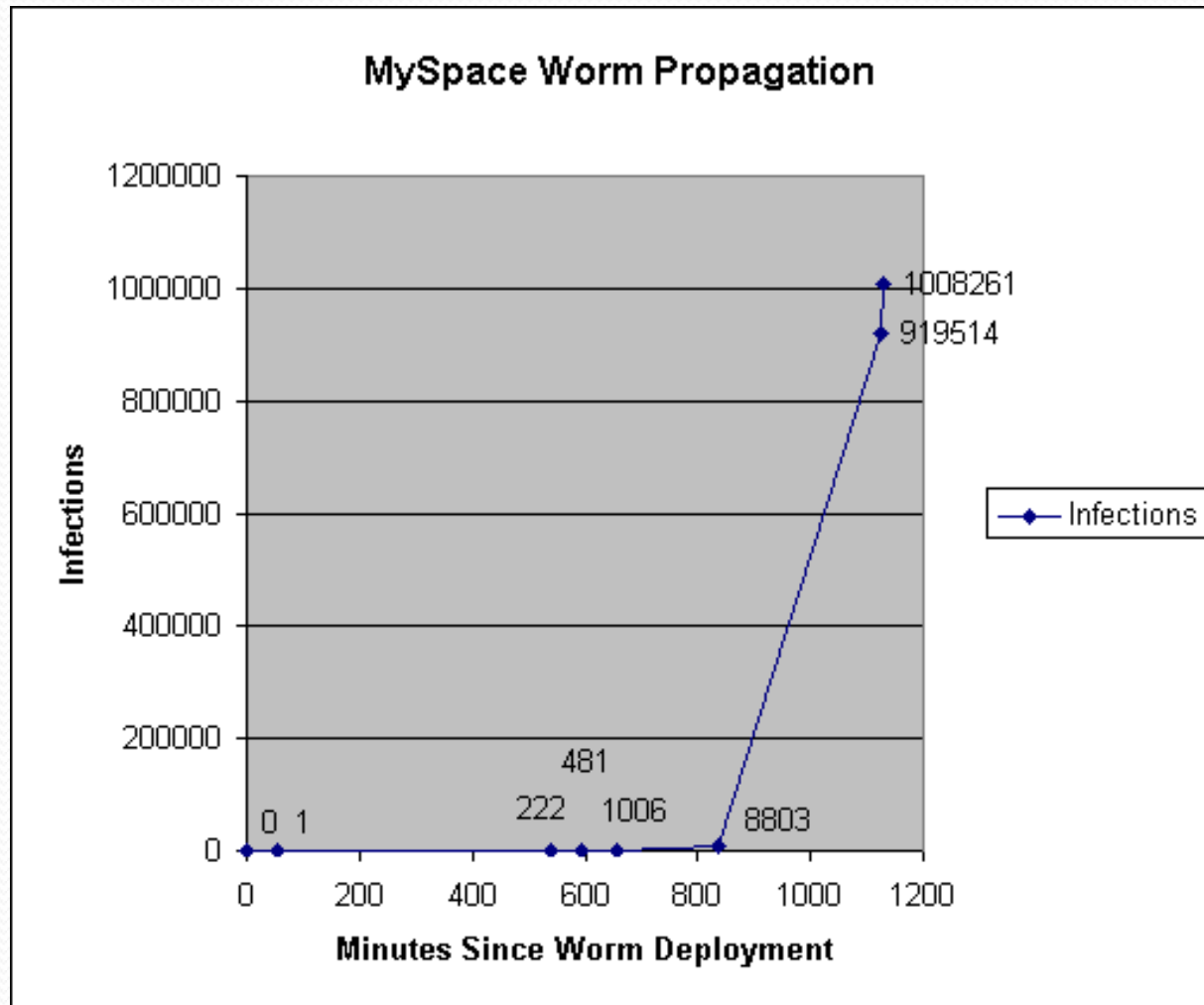
- Samy Worm Analysis
- An interview with Samy
- Technical explanation of the MySpace worm
- slashdot.org discussion

Completato TMN: Off

2 Wind... Note1 - ... Inbox for... Problem... Samy (XS... IT 100%

15.51

# Samy: MySpace XSS worm



# Twitter clickjacking: per qualche link in più

- Clickjacking attack
- Utilizza iframe
- Vettore per attacchi potenzialmente molto pericolosi (botnet, ad esempio)
- Vulnerabilità nota da mesi (OWASP APPSEC 09/2008) in altro contesto
- <http://www.korben.info/petit-cours-de-twitt-jacking.html>
- Lo stesso autore ha utilizzato lo stesso metodo su facebook

Twitter Blog: Clickjacking Blocked - Mozilla Firefox

File Modifica Visualizza Cronologia Segnalibri Strumenti ?

http://blog.twitter.com/2009/02/clickjacking-blocked.html

Google

La Repubblica.it » Ho... Più visitati Press This Ultime notizie Post to Soup Whois By IP Address Risultato del test dell'i... code-of-best-practice...



[<< Back to the main Twitter Blog page](#)

THURSDAY, FEBRUARY 12, 2009

## Clickjacking Blocked

Some folks have noticed links from accounts they follow prefaced by the words, "Don't click" which of course people want to click right away. The links take you to a web site employing technique called clickjacking. This technique seeks to trick web users and can take action on your behalf while you perform seemingly unrelated tasks.

[As wikipedia states](#), clickjacking is "A vulnerability across a variety of browsers and platforms, a clickjacking takes the form of embedded code or script that can execute without the user's knowledge, such as clicking on a button that appears to perform another function." In this case that "other function" was posting a link to your Twitter account so that more people could be tricked and the cycle could perpetuate.

Thankfully the harm was restricted to constant reposting of the link but

Esecuzione script attualmente vietata | <SCRIPT>: 10 | <OBJECT>: 1

Opzioni...

Completato

TMN: Off

facebook

Remember Me

Forgot your password?

Login

Sign Up

Sign up for Facebook to join Je me suis fait Owed par tsukasagenesis.

Je me suis fait Owed par tsukasagenesis

Global

Basic Info

Type: Just for Fun - Totally Random  
Description: Il est trop fort, je ne puis lutter  
Il a utiliser la ruse, mon dieu ><

Contact Info

Website: http://www.allofmanga.net

Members

Displaying 8 of 13 members



Théo

Manuel

Tsukasa



Jean-Claude



Lelouche



Etienne



Thierry



Paul



Group Type

This is an open group. Anyone can join and invite others to join.

Admins

There are no admins left in this group!

Related Groups

Korben  
Internet & Technology - General  
Pour que Coyote arrive enfin a

# De-anonimizzazione e re-identificazione

- Ricercatori dell'università del Texas ([http://www.cs.utexas.edu/~shmat/shmat\\_oak09.pdf](http://www.cs.utexas.edu/~shmat/shmat_oak09.pdf))
- dimostrare che l'anonimato non è sufficiente a salvaguardare la privacy degli individui, quando si tratta di social network online
- Hanno incrociato dati di twitter con altri di flicker e sono riusciti, mediante un algoritmo di calcolo apposito, a identificare correttamente centinaia di utenti, nonostante l'anonimato
- ...” The main lesson of this paper is that anonymity is not sufficient for privacy when dealing with social networks. We developed a generic re-identification algorithm and showed that it can successfully de-anonymize several thousand users in the anonymous graph of a popular microblogging service (Twitter), using a completely different social network (Flickr) as the source of auxiliary information.”

# Domande?



# Fonti

- [www.enisa.europa.eu/doc/pdf/deliverables/enisa\\_pp\\_social\\_networks.pdf](http://www.enisa.europa.eu/doc/pdf/deliverables/enisa_pp_social_networks.pdf)
- [http://www.enisa.europa.eu/doc/pdf/deliverables/enisa\\_survey\\_web2.pdf](http://www.enisa.europa.eu/doc/pdf/deliverables/enisa_survey_web2.pdf)
- [http://www.enisa.europa.eu/doc/pdf/deliverables/enisa\\_pp\\_web2.pdf](http://www.enisa.europa.eu/doc/pdf/deliverables/enisa_pp_web2.pdf)
- <http://www.w3.org/2008/Talks/0425-devtrack-tlr/slides.pdf>
- <http://www.w3.org/2008/Talks/0424-w3ctrack-tlr/0424-w3ctrack-tlr.pdf>
- <http://raven-seo-tools.com/blog/308/evil-genius-how-to-get-people-to-tweet-for-you-without-them-knowing>
- [http://www.cs.utexas.edu/~shmat/shmat\\_oak09.pdf](http://www.cs.utexas.edu/~shmat/shmat_oak09.pdf)