Problematiche di sicurezza delle reti sociali online

yvette@yvetteagostini.it

XX Congresso AIP ÷Assisi÷ 9 e 10 maggio 2009

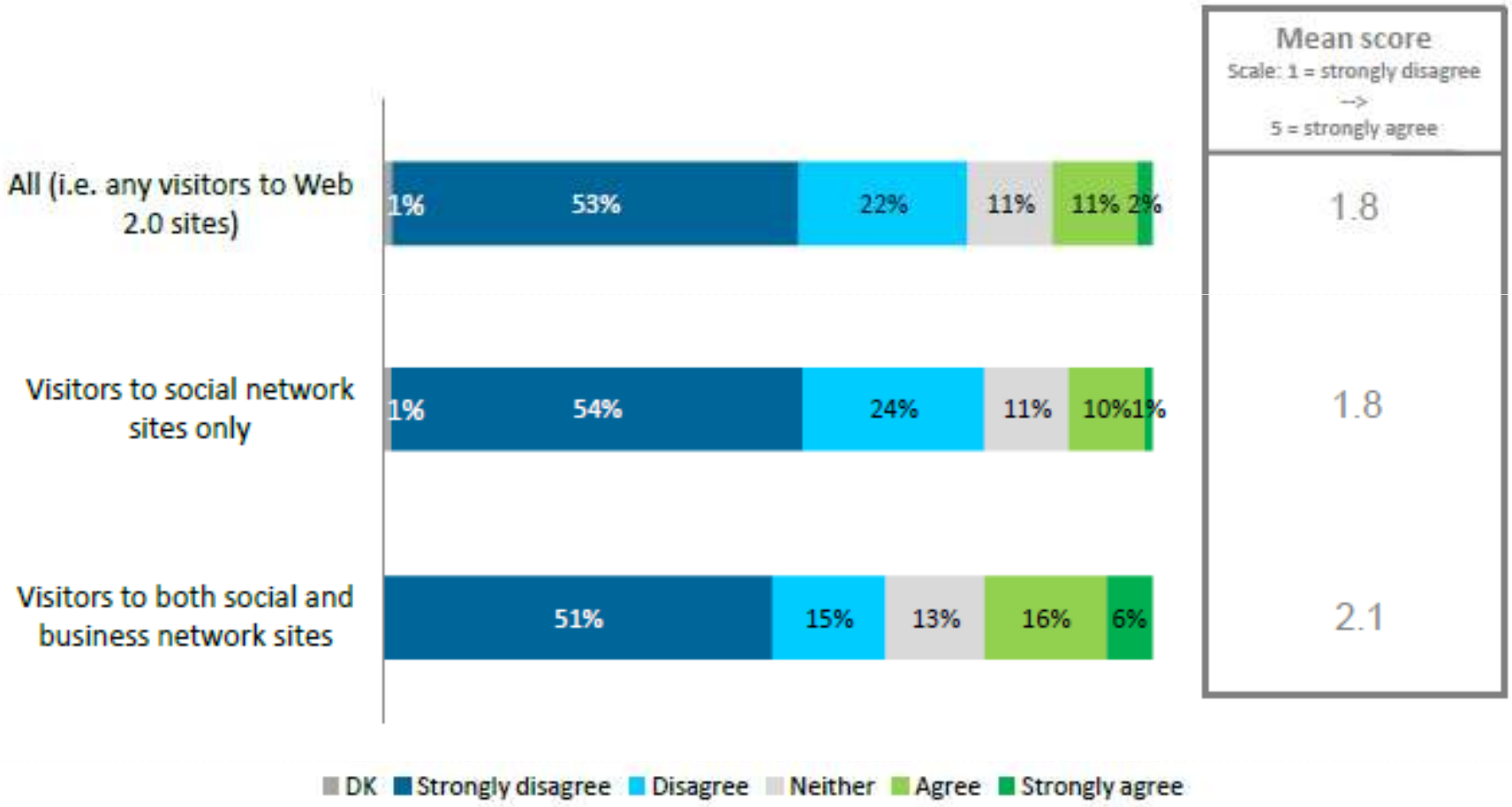
- Reti sociali (social networks) online
- … e relative problematiche di sicurezza e privacy
- Esempi:
  - Samy: il velocissimo worm di MySpace.com
  - re-identificazione : l’ago nel pagliaio ai tempi del web2.0
  - Twitter clickjacking: per qualche link in più
- Q&A

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

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

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

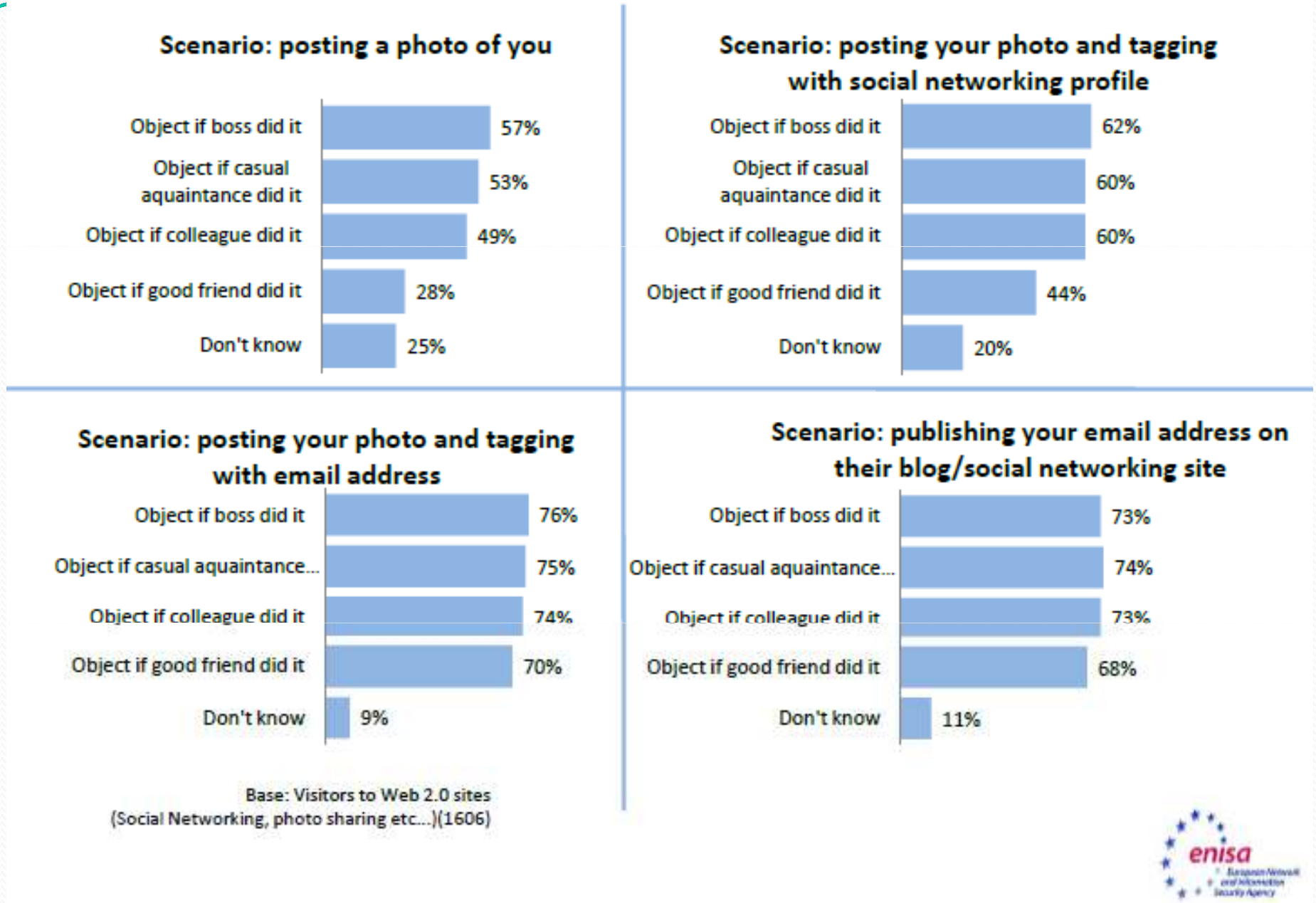
Level of agreement with '*I am willing to give my email account details, including password to invite friends to a social application*'



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

http://www.enisa.europa.eu/doc/pdf/deliverables/enisa_survey_web2.pdf

Scenarios when would object to specific actions taken without your permission



http://www.enisa.europa.eu/doc/pdf/deliverables/enisa_survey_web2.pdf

- 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)**

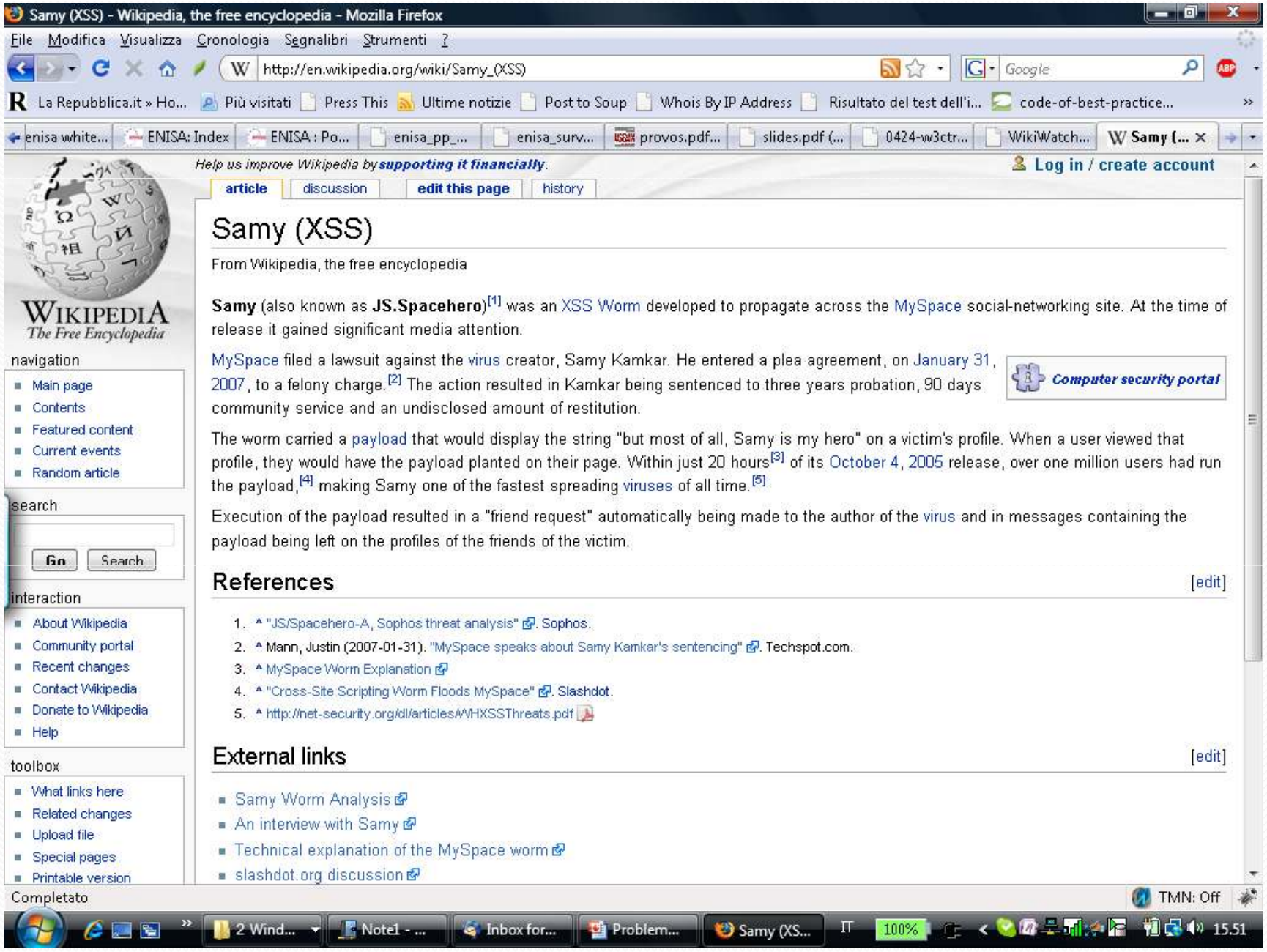
Il fattore umano

- **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**

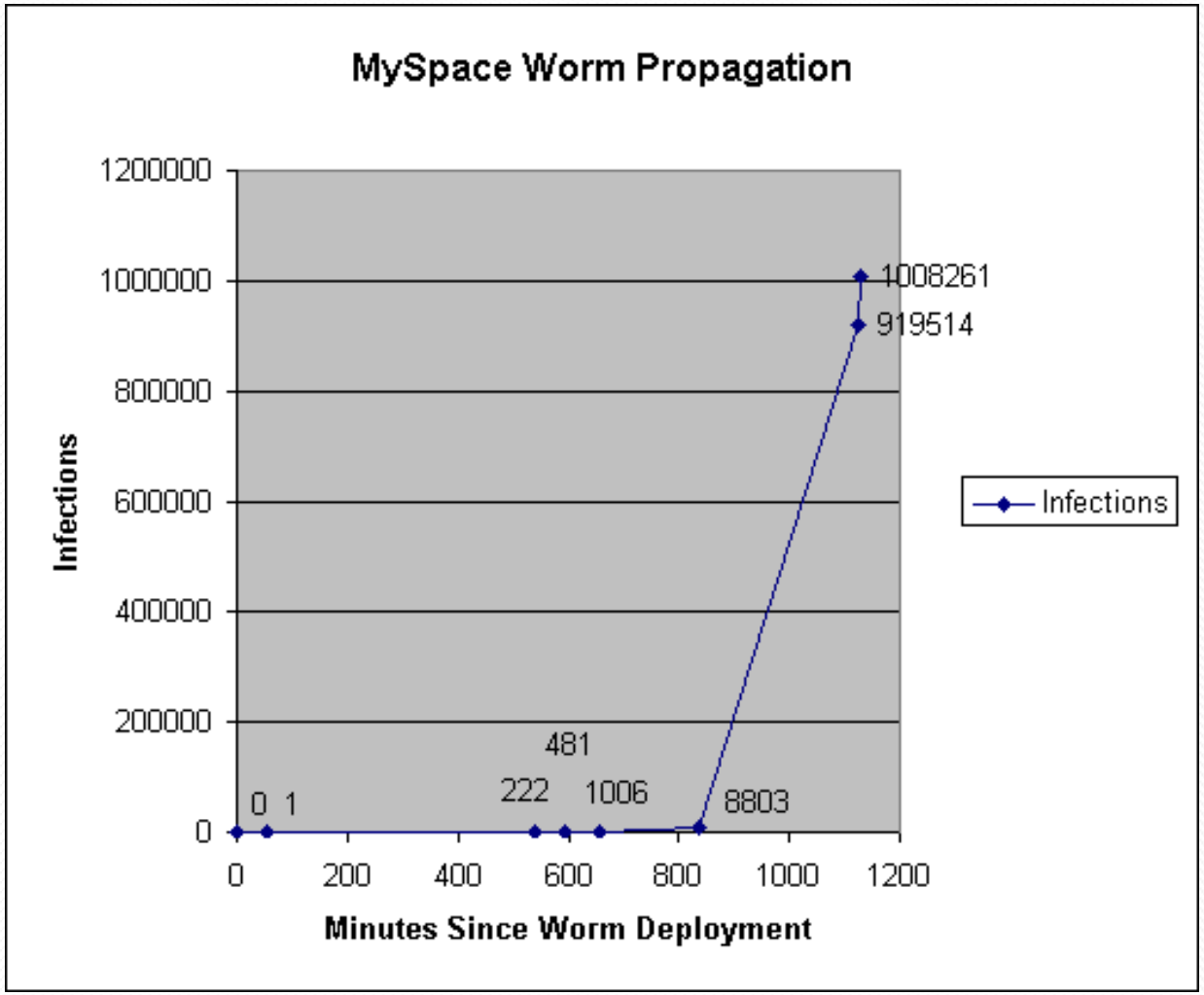
Meccanismi di injection di contenuto malevolo nei siti

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

Samy: MySpace XSS worm



Samy: 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...
BLOG
twitter
<< 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
TWITTER IS DEL.ICIO.US
I Power Blogger
Esecuzione script attualmente vietata | <SCRIPT>: 10 | <OBJECT>: 1
Opzioni...
Completato
TMN: Off

Je me suis fait Owed par tsukasagenesis | Facebook - Mozilla Firefox

File Modifica Visualizza Cronologia Segnalibri Strumenti ?

http://www.facebook.com/group.php?gid=48226044199

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...

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)
- 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_survey_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*