



NETWITNESS
TOTAL NETWORK KNOWLEDGE

Understanding Social Networking Threats Using Active Threat Intelligence

Eddie Schwartz
CSO

NetWitness Corporation
eddie@netwitness.com

Agenda

- Facebook Numbers Game
 - A Look at “FaceBot” – a proof of concept for social networking malware
 - **“Antisocial Networks: Turning a Social Network into a Botnet”** by E. Athanasopoulos, et al of Institute of Computer Science (ICS), Foundation for Research & Technology Hellas (FORTH)
 - Seven Social Networking Hacks and Potential Countermeasures
 - Some Network Initial Network Captures and Thoughts About Network Monitoring and Ongoing Research
 - Q&A
-

Introduction to Social Networking

- Massive adoption in the consumer market
 - **MySpace, Facebook, LinkedIn, Friendster**
 - **SecondLife, There**
 - **Ning , etc.**
 - Statistics on Facebook
 - **Over 64,000,000 users**
 - **Over 250,000 new registrations per day**
 - **Over 200,000 developers have submitted some sort of Facebook application using basic programming skills and there are over 15,000 official apps**
 - **Users can add up to 20 friends per day**
 - **Facebook apps can be considered as XHTML snippets that inherit all the properties of web applications**
-

Ideal Exploitation Platform?

- Social networks have intrinsic properties that make them ideal to be exploited by an adversary:
 - **Difficult to police:** very large and distributed user base
 - **Trust network:** clusters of users sharing the same social interests developing trust with each other
 - **Platform openness** for developing applications that are attractive the general users who will install them
-



Other Precedents

- One of the ways to think about the broader risks of social networking against critical infrastructure is related to the problems of state-sponsored attackers
 - **“People’s War” concept a la Dragon Bytes – many home computers used as soldiers**
 - **Similar problem seen with Gnutella used as a DDOS platform**
 - **A rogue social network app could be used in the same manner or worse**
-

My Own Facebook Experience

- Began by simply receiving an invite from my niece in college
 - Months later received my first “friend” request from a noted InfoSec luminary
 - Now have many security “friends” mixed with press, college students, vendors and other random people I meet on planes
 - News items include people’s favorite dive sites, pictures of drunken college parties, best gay hotels in Greece, invitations to Battlestar Gallactica trivia contests and the political views of many people
-

Why Don't We Just Ban It All?

- Banning public social networking sites from corporate use may help with the distraction factor and with some of the other technical issues, but..
 - In many cases, there is just too much personal information posted on these sites
 - **Information such as the full names of parents, pets, schools and other “keys” that are used to unlock personal and professional accounts**
 - **Embarrassing or inappropriate pictures that could be used in blackmail scenarios (think Cold War)**
 - **Lifestyle information that may create personal or professional problems**
-



NETWITNESS
TOTAL NETWORK KNOWLEDGE

FaceBot “Photo of the Day” Application / Experiment

-
- Application designed to present a different National Geographic photo to an end-user every day
 - Although the app was only advertised to a research group and their friends, over 1000 people installed it in just a few days
 - **It is very common that Facebook applications require a user to invite a subset of his/her friends, and thus advertize the application to the Facebook community, prior to the installation. This practice helps in the further propagation of the application in Facebook. Typically, a user must announce the application to about 20 of her friends in order to proceed with the installation.**
-

Sample Code FaceBot

```
Facebook Content - Session 320
[Icons] [txt] [hex] [Email] [Globe] [Print]

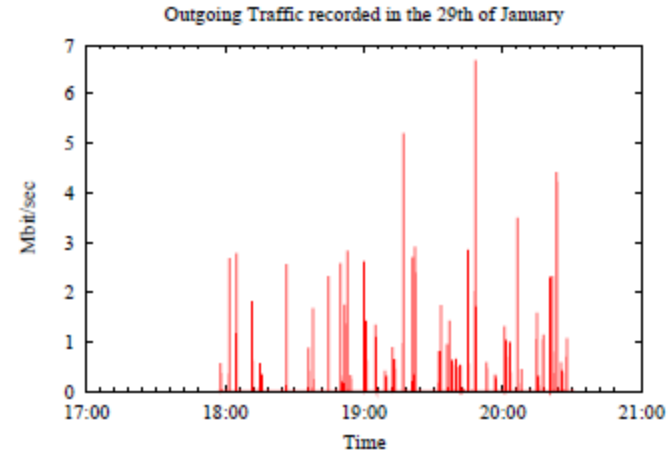
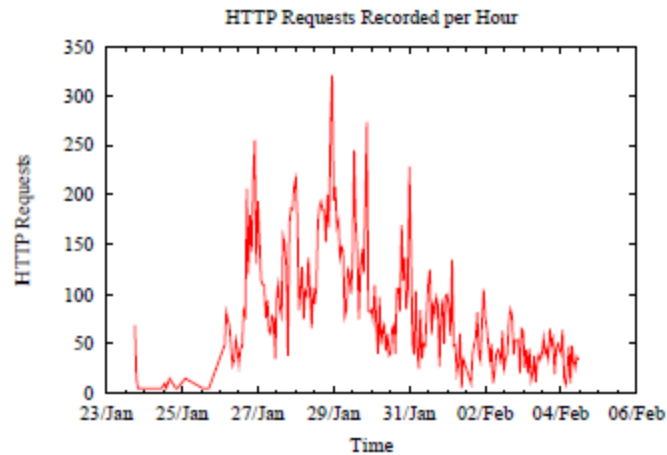
Session ID: 320
Time: 10/03/2008 13:20:40 to 10/03/2008 13:20:48  AppType: 80  Size: 23,4
192.168.17.100 : 58216
67.215.234.82 : 80
GET /fb_tracer.html?src=fb&session=%7B%22session_key%22%3A%223b05efc5b2d807781b593165-4
7D&t=1223054025&v=1&fb_sig_in_iframe=1&fb_sig_locale=en_US&fb_sig_in_new_facebook=1&fb
47700017&fb_sig_ss=3a84d7467c6f30bc73274c9ecc699a2b&fb_sig_expires=1223140425&fb_sig_api_k

• src=fb
• session={"session_key":"3b05efc5b2d807781b593165-47700017","uid":47700017,"expires":0,"s
• t=1223054025
• v=1
• fb_sig_in_iframe=1
• fb_sig_locale=en_US
• fb_sig_in_new_facebook=1
• fb_sig_time=1223054025.9772
• fb_sig_added=1
• fb_sig_profile_update_time=1221581221
• fb_sig_user=47700017
• fb_sig_session_key=3b05efc5b2d807781b593165-47700017
• fb_sig_ss=3a84d7467c6f30bc73274c9ecc699a2b
• fb_sig_expires=1223140425
• fb_sig_api_key=3f62a1b3689094a3cb03b67d969a8b24
• fb_sig=dca2a081c61e09802a5ee0dc505b46fd
```

Every time a Facebook user views a photo, HTTP requests are generated toward the victim host

- **These requests are hidden IFRAMES with inline images hosted at the victim**
- **When the victim clicks inside the application the inline images are fetched from the victim, causing the victim to serve a request of 600kb.**

Attack Magnitude and Significance



Source: E. Athanasopoulos, et al

- Even with a population in the low thousands, the request rate (HTTP) never fell below the tens and at peak times reached a few hundreds of requests
- There also seems to be a general “pack” mentality about the time when people login to check for updates

What Could This Application Do?

- A typical Facebook or MySpace user session ranges from a few to 10s of minutes
 - This test application was designed to absorb a fixed amount of traffic – limiting the application to pulling files and data off the network
 - More sophisticated techniques would involve the creation of a JavaScript snippet which could deal with more complex tasks
 - Another thought – a social engineering app – simply gather all the PII you can from the user's page and aggregate on a server somewhere – this information has more value than credit cards with CVV2 numbers
-



Other Possible Apps?

- Host Scanning: Using JavaScript, an attacker can make an application that identifies whether a host has arbitrary ports open.
 - **As browsers impose only few restriction on destination ports (some browsers like Safari even allow connection to sensitive ports like 25), an attacker can randomly select a host and a port, and request an object through normal HTTP requests. Based on the response time, which can be measured through JavaScript, the attacker can determine if the port is alive or not.**
 - Malware Propagation: An unsuspecting user can participate in malware and attack propagation.
 - **If a server can be exploited by a URL-embedded attack vector, then malicious social networking applications can contain this exploit. Every user that interacts with the application will propagate the attack vector.**
 - Attacking Cookie-based Mechanisms: Similarly to XSS worms, a malicious application can override authentication mechanisms that are based on cookies.
 - **Badly-designed sites that support automated login using cookies suffer from such attacks.**
-

Another Concern – Attack Firepower

- $F(t) = a_{out}U(t)$
 - **F(t) = Firepower of the malicious app**
 - **a_{out} = Outgoing traffic a Facebook app can pull from a victim host**
 - **U(t) = The number of users accessing the app over time**

Source: E. Athanasopoulos, et al

- We won't get into the detailed math behind how we calculate U(t), but let's look at some statistics
-

Taking It to the Extreme

Application	Installations	Daily Active Users
FunWall	23,797,800	2,379,780
Top Friends	24,955,200	2,245,970
Super Wall	23,274,800	1,861,980
Movies	15,934,700	1,274,780
Bumper Sticker	7,989,700	1,118,560

- If an adversary were able to develop an application as successful as FunWall, for example, a victim host would have to cope with about 23 Mbit/sec of unsolicited traffic and nearly 248GB a day of unwanted data!
- Of course, this assumes a lot about bandwidth and the lack of proper network and security management...
- But, adversaries don't need all that bandwidth...



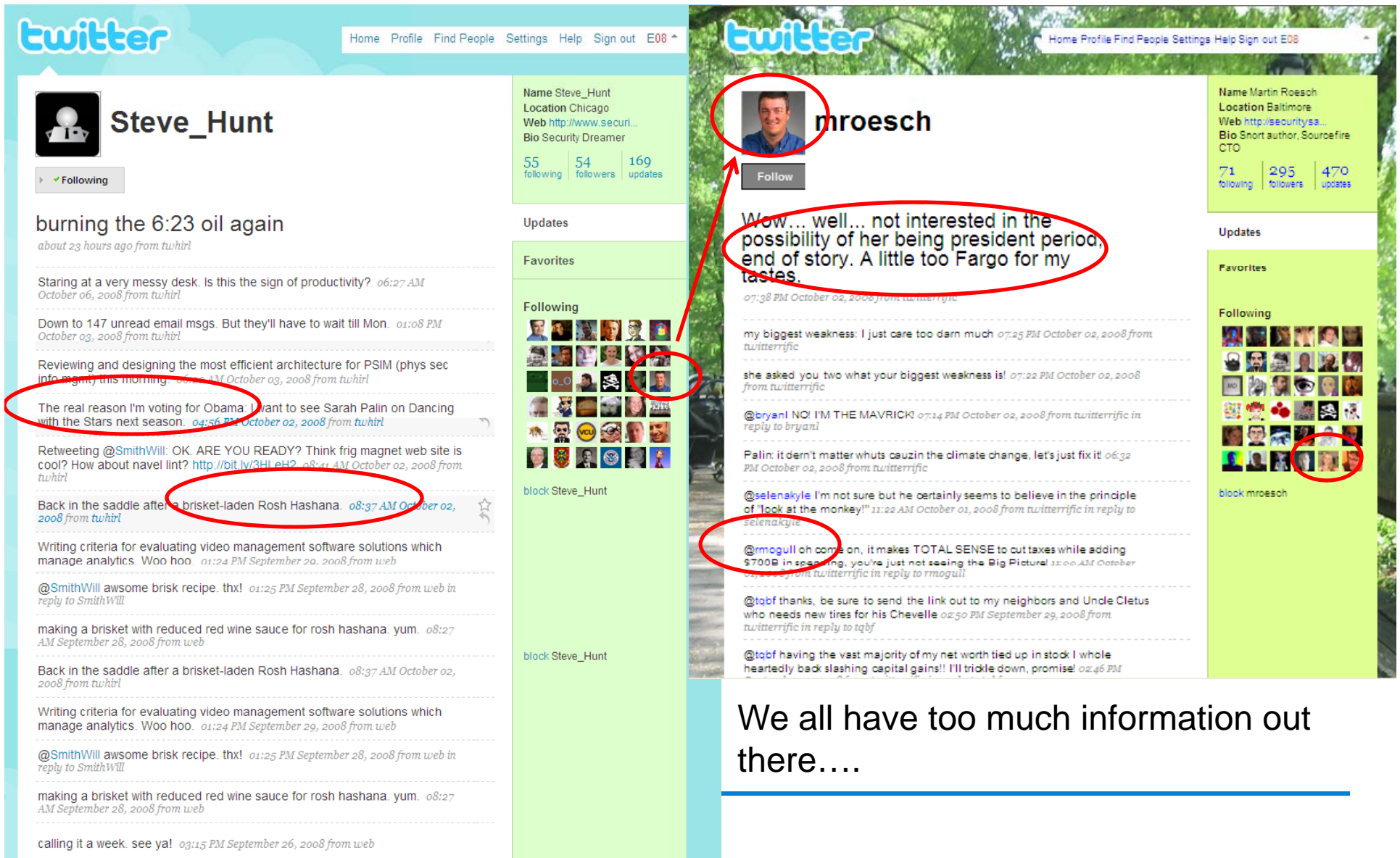
Countermeasures

- Again, banning social networking sites completely may be an option – but not necessary tenable over the long term
 - If that is not an option, you must start by closely monitoring and filtering traffic from social networking sites
 - **Perform full packet capture and session analysis of all HTTP requests**
 - **Perform an automated review of the content of the *referer* field to determine if the request originates from facebook.com or not**
 - **There are ways around the referer issue, so also look for zero byte IFRAMES in facebook HTTP requests**
-

Top 7 Social Networking Hacks

- 1) Impersonation and targeted personal attacks
- 2) Spam and bot infections
- 3) Weaponized OpenSocial and other social networking applications
- 4) Crossover of personal to professional online presence
- 5) XSS, CSRF attacks
- 6) Identity theft
- 7) Corporate espionage

Impersonation and Targeted Personal Attacks



The image displays two side-by-side screenshots of Twitter profiles. The left profile is for 'Steve_Hunt' and the right is for 'mroesch'. Red circles and arrows highlight specific elements: Steve_Hunt's bio, a tweet about Obama, and a tweet about a brisket recipe; mroesch's profile picture, a tweet about a story, and a tweet about taxes. The text 'We all have too much information out there....' is overlaid at the bottom right.

Steve_Hunt Profile:

- Name: Steve_Hunt
- Location: Chicago
- Web: <http://www.securi...>
- Bio: Security Dreamer
- 55 following, 54 followers, 169 updates
- Updates:
 - burning the 6:23 oil again (about 23 hours ago from tuhirl)
 - Staring at a very messy desk. Is this the sign of productivity? 06:27 AM October 06, 2008 from tuhirl
 - Down to 147 unread email msgs. But they'll have to wait till Mon. 01:08 PM October 03, 2008 from tuhirl
 - Reviewing and designing the most efficient architecture for PSIM (phys sec info mgmt) this morning. 06:41 AM October 03, 2008 from tuhirl
 - The real reason I'm voting for Obama: I want to see Sarah Palin on Dancing with the Stars next season. 04:56 PM October 02, 2008 from tuhirl
 - Retweeting @SmithWill: OK. ARE YOU READY? Think frig magnet web site is cool? How about navel lint? <http://bit.ly/3HLeH2> 08:41 AM October 02, 2008 from tuhirl
 - Back in the saddle after a brisket-laden Rosh Hashana. 08:37 AM October 02, 2008 from tuhirl
 - Writing criteria for evaluating video management software solutions which manage analytics. Woo hoo. 01:24 PM September 26, 2008 from web
 - @SmithWill awesome brisk recipe. thx! 01:25 PM September 28, 2008 from web in reply to SmithWill
 - making a brisket with reduced red wine sauce for rosh hashana. yum. 08:27 AM September 28, 2008 from web
 - Back in the saddle after a brisket-laden Rosh Hashana. 08:37 AM October 02, 2008 from tuhirl
 - Writing criteria for evaluating video management software solutions which manage analytics. Woo hoo. 01:24 PM September 29, 2008 from web
 - @SmithWill awesome brisk recipe. thx! 01:25 PM September 28, 2008 from web in reply to SmithWill
 - making a brisket with reduced red wine sauce for rosh hashana. yum. 08:27 AM September 28, 2008 from web
 - calling it a week. see ya! 03:15 PM September 26, 2008 from web

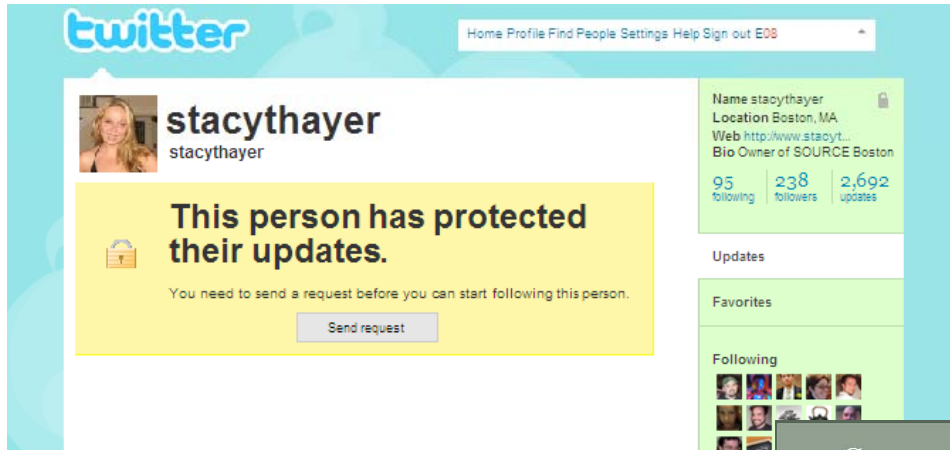
mroesch Profile:

- Name: mroesch
- Location: Baltimore
- Web: <http://securitysa...>
- Bio: Short author, Sourcefire CTO
- 71 following, 295 followers, 470 updates
- Updates:
 - Wow... well... not interested in the possibility of her being president period, end of story. A little too Fargo for my tastes. 07:38 PM October 02, 2008 from twitterrific
 - my biggest weakness: I just care too darn much 07:25 PM October 02, 2008 from twitterrific
 - she asked you two what your biggest weakness is! 07:22 PM October 02, 2008 from twitterrific
 - @bryani NO! I'M THE MAVRICK! 07:14 PM October 02, 2008 from twitterrific in reply to bryani
 - Palin: it dern't matter whuts cauzin the climate change. let's just fix it! 06:32 PM October 02, 2008 from twitterrific
 - @selenakyle I'm not sure but he certainly seems to believe in the principle of "look at the monkey!" 11:22 AM October 01, 2008 from twitterrific in reply to selenakyle
 - @rmogull oh come on, it makes TOTAL SENSE to out taxes while adding \$700B in spending, you're just not seeing the Big Picture! 12:00 AM October 02, 2008 from twitterrific in reply to rmogull
 - @tqbf thanks, be sure to send the link out to my neighbors and Uncle Cletus who needs new tires for his Chevelle 02:50 PM September 29, 2008 from twitterrific in reply to tqbf
 - @tqbf having the vast majority of my net worth tied up in stock I whole heartedly back slashing capital gains!! I'll trickle down, promise! 02:46 PM

We all have too much information out there....



Impersonation and Targeted Personal Attacks



- Ultimate Risks:
 - ID Theft
 - Burglary
 - Harassment
 - Social Engineering Use

- We have to be consistent in our use of technology....
- Once something is out there, Google caches it for a long time



Spam and bot Infections

- Malware via spam, phishing and spear phishing attacks is very popular
 - There is no fool proof countermeasure since users are in the loop and the threats are multi-dimensional
 - The application risks I mentioned earlier provide a fresh landscape for all kinds of attacks
- Recent Facebook Trojan downloaded malware onto end-users' machines once they opened the link





Weaponized, OpenSocial and Other Applications

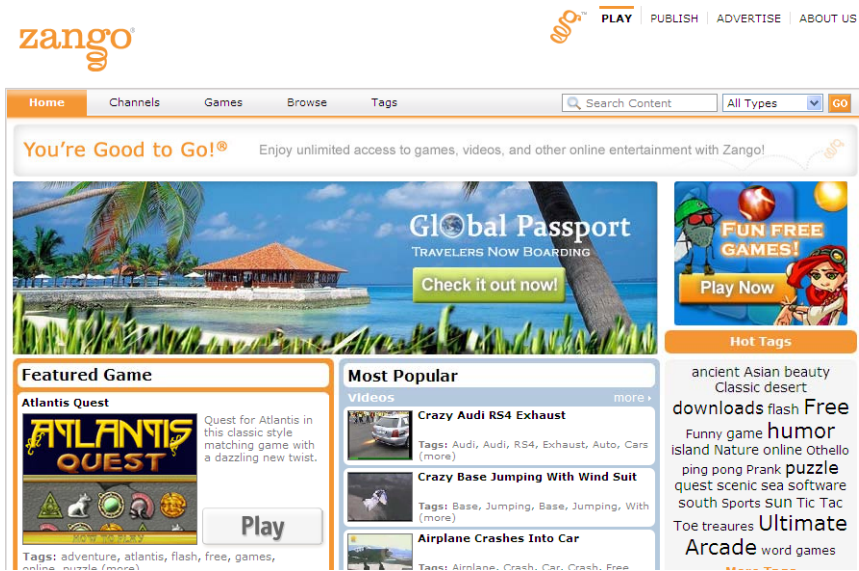
- Open Social
 - is a “set of common APIs for web-based social network applications, developed by Google along with MySpace and a number of other social networks.”
- No mature security model defined in either the Google / MySpace or Facebook models
- Difficult to police when hundreds of applications are running
- Could be used for good or evil, i.e., as a weapon

The image shows two screenshots. The top screenshot is the Google OpenSocial API Developer's Guide (v0.8.1). It features a search bar at the top with the text "e.g. 'ajax apis' or 'open source'". Below the search bar is a navigation menu with links for Home, Docs, FAQ, Articles, Blog, Group, and Terms. The main content area is titled "OpenSocial API Developer's Guide (OpenSocial API v0.8.1)" and includes an introduction, a "Contents" section with links to various topics like "Writing a Social Application" and "Importing the OpenSocial Library", and a "JavaScript API" section with links to "Developer's Guide (v0.8.1)", "Release Notes (v0.8.1)", "API Specification (v0.8.1)", and "API Reference (v0.8.1)".

The bottom screenshot is a search results page from the Facebook Developers Wiki. It shows a search for "security" with the following results:

- There is no page titled "security". You can create this page.
- For more information about searching Facebook Developers Wiki, see Help.
- Showing below up to 20 results starting with #1.
- View (previous 20) (next 20) (20 | 50 | 100 | 250 | 500).
- No page title matches
- Page text matches:
 1. Gotchas (8,169 bytes)
79: ...ernet Explorer to set the cookie under default IE security settings. See http://www.w3.org/P3P/ for more inf...
 2. FBML (6,043 bytes)
285: ...erties are stripped by the Facebook platform for security. This section needs updating. We'll get to it s...
 3. Fh:swf (7,361 bytes)

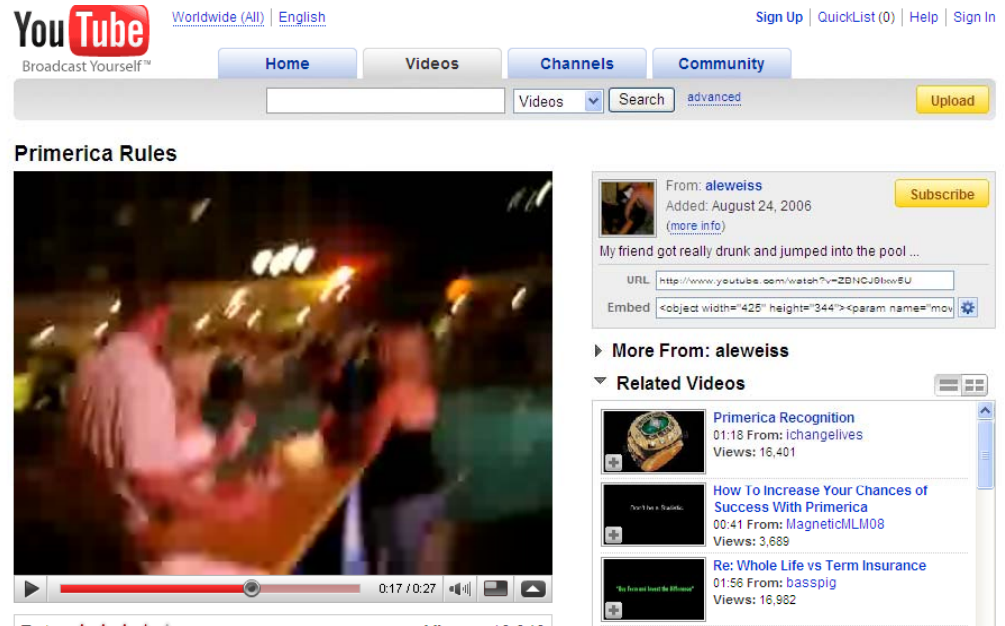
Weaponized, OpenSocial and Other Applications



- Facebook “Secret Crush” worm
- Invitation to find out who has a secret crush on you
- You had to invite 5 of your friends before the application would work
- Attack spreads adware /spyware via an IFrame
- Installs Zango software and gets revenue at a minimum

Crossover of Personal to Professional Online Presence

- Simple message – keep your personal and public life separate
 - YouTube Videos from conference late night parties
 - Pictures on social networking sites
 - Deeply personal information disclosed on any number of social networking sites



The screenshot shows a YouTube video player interface. At the top, the YouTube logo and navigation tabs (Home, Videos, Channels, Community) are visible. The video title is "Primerica Rules". The video player shows a blurry, dark scene of people at a party. To the right of the video player, there is a metadata box for the video, including the uploader's name "aleweiss", the date "August 24, 2006", and a "Subscribe" button. Below this, there is a "More From: aleweiss" section and a "Related Videos" section with three video thumbnails and titles: "Primerica Recognition", "How To Increase Your Chances of Success With Primerica", and "Re: Whole Life vs Term Insurance".



XSS, CSRF Attacks

- Cross site scripting attacks and cross-site request forgery attacks are serious concerns
 - Characteristics important to this problem:
 - **Attacks involve sites that rely on a user's identity**
 - **Exploit the site's trust in that identity**
 - **Trick the user's browser into sending HTTP requests to a target site**
 - **Involve HTTP requests that have undesired side effects**
 - Bottom line: Any time a user loads HTML, there is an opportunity for a browser exploit
 - **Recent discoveries of CSRF vulnerabilities in YouTube, ING and the NY Times**
 - **CSRF is not well understood in the web development community, but better researched in the attacker community**
-

Identity Theft

- General issue is similar to the targeted personal attack problem – users are disclosing too much information on “public” websites
- End users need to limit the amount of PII supplied on these sites



Password Reset Setup

Please indicate your preferences, and if you ever forget your password we will use them to verify that it is you.

- They don't have to be strong preferences — just a small preference is enough.
- You don't need to remember which items you choose, just whether you like or dislike them.

Look through the items in these 6 categories...

Items		
Music	Sports	Food
TV	Places	Interests
Watching extreme sports	<input type="button" value="Like"/>	<input type="button" value="Dislike"/>
Watching soccer	<input type="button" value="Like"/>	<input type="button" value="Dislike"/>
Watching baseball	<input type="button" value="Like"/>	<input type="button" value="Dislike"/>
Watching auto racing	<input type="button" value="Like"/>	<input type="button" value="Dislike"/>
Watching hockey	<input type="button" value="Like"/>	<input type="button" value="Dislike"/>
Watching diving	<input type="button" value="Like"/>	<input type="button" value="Dislike"/>

and choose 8 things you like (at least a little)...

Likes	
1. Heavy Metal music	<input type="button" value="x"/>
2. Blues music	<input type="button" value="x"/>
3. Doing martial arts	<input type="button" value="x"/>
4. Watching news	<input type="button" value="x"/>
5. Mediterranean food	<input type="button" value="x"/>
6. Politics	<input type="button" value="x"/>
7. Going to bookstores	<input type="button" value="x"/>
8.	<input type="button" value="x"/>

(Choose 1 more Like)

and 8 things you dislike (at least a little).

Dislikes	
1. Country music	<input type="button" value="x"/>
2. Electronica music	<input type="button" value="x"/>
3. Playing soccer	<input type="button" value="x"/>
4. Watching figure skating	<input type="button" value="x"/>
5. Reality shows	<input type="button" value="x"/>
6. Indian food	<input type="button" value="x"/>
7. Going to antique stores	<input type="button" value="x"/>
8. Game shows	<input type="button" value="x"/>

- Information that might be used to authenticate more sensitive aspects of online life should be omitted, but could be tough
 - **Names of parents, grandparents**
 - **Pets**
 - **Schools**
 - **DoB**
 - **Etc.**
- Some organizations are trying new forms of password reset and onward authentication

Corporate Espionage

- Blocking access to social networking sites is not viable long term strategy
 - **Social networking and virtual worlds as forms of collaboration are being adopted across the enterprise**
 - **Users will access these sites from home and write about work-related experiences**
 - The availability of corporate intel on people will facilitate spear phishing attacks and other types of corporate espionage:
 - **“Dear Fred Jones, Congratulations on joining XYZ Company. Click on this link to access our HR Intranet and then log in with your regular network username and password so we can update our files.”**
-



NETWITNESS

TOTAL NETWORK KNOWLEDGE

Illustrations



NETWITNESS

TOTAL NETWORK KNOWLEDGE

Thanks / Q&A

eddie@netwitness.com

<http://www.netwitness.com>
