Weapons of Mass Distraction
Sock Puppetry for Fun & Profit
@azhrdesai  @haroonmeer  @marcoslaviero

http://thinkst.com
THE MASTER SWITCH
THE RISE AND FALL OF INFORMATION EMPIRES

Tim Wu

‘A must-read for those who want to know more about the future of the Internet’

Josh Siverman, CEO, Skype
Already seen clear signs of this
Egypt Cuts Off Most Internet and Mobile Network Service

Autocratic governments often limit phone and Internet service during tense times. But the Internet has never faced anything like what happened in Egypt on Friday, when the government cut access to the network and shut down cellphone service.

Libya cuts off Internet service: network monitor

(Reuters) - Internet service has been cut off in Libya for a second consecutive day as protesters step up demonstrations against longtime leader Muammar Gaddafi, a U.S. company that monitors Internet traffic said on Saturday.
Amateurs cut access
Tunisia plants country-wide keystroke logger on Facebook

Gmail and Yahoo! too

By Dan Goodin, 25 Jan 2011

Malicious code injected into Tunisian versions of Facebook, Gmail, and Yahoo! stole login credentials of users critical of the North African nation's authoritarian government, according to security experts and news reports.

The rogue JavaScript, which was individually customized to steal passwords for each site, worked when users tried to login without availing themselves of the secure sockets layer protection designed to prevent man-in-the-middle attacks. It was found injected into Tunisian versions of Facebook, Gmail, and Yahoo! in late December, around the same time that protestors began demanding the ouster of Zine el-Abidine Ben Ali, the president who ruled the country from 1987 until his ouster 10 days ago.

Danny O'Brien, internet advocacy coordinator for the Committee to Protect Journalists, said the code was injected into Tunisian versions of Facebook, Gmail, and Yahoo! in late December, around the same time that protestors began demanding the ouster of Zine el-Abidine Ben Ali, the president who ruled the country from 1987 until his ouster 10 days ago.
Law enforcement technology
London police use smartphones, social network to identify rioters
Published 10 August 2011

The rioters in London — and now, in other British cities — have been using Blackberries to outmaneuver the police; communicating via BlackBerry instant-message technology, as well as by social networking sites like Facebook and Twitter, the rioters repeatedly signaled fresh target areas to those caught up in the mayhem; RIM has now agreed to cooperate with Scotland Yard to turn over protestors using the service to coordinate their assaults; the police is also releasing CCTV images of the rioters to a group using face recognition technology to identify and condemn rioters; the police is also using Flickr, Twiblr, and Twitter to spot and identify participants in the riots.

Smartphones, especially Blackberries, have been a helpful information transmission and coordination tool for anti-government activists in a score of Arab countries – and they have played a major role in helpful information transmission and coordination tool for anti-government activists in a score of Arab countries – and they
Overt censorship is routed around
UGC - User Generated Content
UGC is a new(ish) paradigm
Nothing truly new under the sun
rent-a-crowds
How will Censorship handle UGC?
“So it’s not only certain people have a license to speak, now everyone has a license to speak. It’s a question of who gets heard.”
Censorship 2.0
Censorship 2.0
This is Profoundly Important
Censorship 2.0
This is Profoundly Important

OPEN TECHNOLOGY FUND
rent-a-crowds
sock puppet

noun

a false online identity, typically created by a person or group in order to promote their own opinions or views: both sides in the debate use sock puppets to make it seem as if scores of people are arguing a point.

DERIVATIVES

sock puppetry noun
If we were evil-corp
(or evil.gov)
what can be done?

what will be done?

what is being done?
Challenge:
How to measure efficacy
<table>
<thead>
<tr>
<th>mail lists</th>
<th>![Image]</th>
</tr>
</thead>
<tbody>
<tr>
<td>online polls</td>
<td></td>
</tr>
<tr>
<td>twitter</td>
<td></td>
</tr>
<tr>
<td>reddit</td>
<td></td>
</tr>
<tr>
<td>news sites</td>
<td></td>
</tr>
<tr>
<td>comment systems</td>
<td></td>
</tr>
</tbody>
</table>
Why mailing lists?

- “Interesting” people still use it
- Personal curiosity
what we wanted to do
Assume:
An email is going to a mail list

Can we make more people read it?
Assume:
An email is going to a mail list

Can we make less people read it?
How do we measure if more (or less) people read our mail?
Link Clicks
How do we write mail content worth clicking on?
Plagiarize, Pilfer, Plunder & Pitch*

*but don’t be too exciting
Control email

1. Send email with link
2. Wait 48 hours
3. Count clicks

Experimental email

1. Send email with link
2. Puppets send several replies to make a longer discussion thread
3. Wait 48 hours
4. Count clicks
- [liberatiotn_tech] Breaking Tor for $3K  Maxim Kammerer
  - [liberatiotn_tech] Breaking Tor for $3K  Griffin Boyer
- [liberatiotn_tech] Recent iOS privacy checks  Cody Tarrant
  - [liberatiotn_tech] Recent iOS privacy checks  Amin Sabeti
  - [liberatiotn_tech] Recent iOS privacy checks  Keira Cran
    - [liberatiotn_tech] Recent iOS privacy checks  Todd Weiler
    - [liberatiotn_tech] Recent iOS privacy checks  duncan at openmailbox.org
    - [liberatiotn_tech] Recent iOS privacy checks  Keira Cran
- [liberatiotn_tech] [cryptome] Cryptome Kickstart Project  Eugen Leitl
- [liberatiotn_tech] The Ex-Google Hacker Taking on the World’s Spy Agencies  Eugen Leitl
- [liberatiotn_tech] data mine the snowden files [was: open the snowden files]  coderman
Control email

1. Send email with link
2. Wait 48 hours
3. Count clicks

Experimental email

1. Send email with link
2. Sock puppets send several separate emails starting new threads
3. Wait 48 hours
4. Count clicks
- [liberationtech] New Citizen Lab report on Hacking Team's Government Surveillance Malware  Ronald Deibert
  - [liberationtech] RIPE NCC Internet-wide measurement project  duncan at openmailbox.org
  - [liberationtech] Nsa-observer: organising nsa leaks by attack vector  Todd Weiler
    - [liberationtech] Nsa-observer: organising nsa leaks by attack vector  Alexey Zakhlestin
    - [liberationtech] Nsa-observer: organising nsa leaks by attack vector  Tom Ritter
- [liberationtech] Mapping out physical surveillance across a city  Cody Tarrant
  - [liberationtech] Mapping out physical surveillance across a city  duncan at openmailbox.org
    - [liberationtech] Mapping out physical surveillance across a city  Seeta Peña Gangadharan
      - [liberationtech] Mapping out physical surveillance across a city  Tim Schwartz
      - [liberationtech] Mapping out physical surveillance across a city  Lucas Gonze
      - [liberationtech] Mapping out physical surveillance across a city  Patrick
      - [liberationtech] Mapping out physical surveillance across a city  Lucas Gonze
coderman
      - [liberationtech] Mapping out physical surveillance across a city  Blibbet
      - [liberationtech] Mapping out physical surveillance across a city  Axel Simon
      - [liberationtech] Mapping out physical surveillance across a city  Dan O'Huiginn
  - [liberationtech] Mapping out physical surveillance across a city  The Doctor
- [liberationtech] New open access journal from Usenix  Ryan Bartos
- [liberationtech] [SPAM:###] FSF email self defence project  Greg White
- [liberationtech] The Hacking Team Commercial and are there others?  Karen Dunnes
- [liberationtech] Viber features being blocked by the Gambian govt?  Mary Bukowski
“rai” also had another success
Mac OS X stack_chk_guard not always safe from overwrite rai (May 15)
VulDB: Apple Mac OS X up to 13.1.0 Stack Guard stack_chk_guard buffer overflow

General

scipID: 13247
Affected: Apple Mac OS X up to 13.1.0
Published: 05/15/2014 (rai)
Risk: problematic

Created: 05/18/2014
Entry: 74.7% complete

Summary

A vulnerability was found in Apple Mac OS X up to 13.1.0. It has been rated as problematic. This issue affects the function stack_chk_guard of the component Stack Guard. The manipulation with an unknown input leads to a buffer overflow vulnerability. Impacted is confidentiality, integrity, and availability.

The weakness was disclosed 05/15/2014 by rai as Mac OS X stack_chk_guard not always safe from overwrite as mailinglist post (Full-Disclosure). The advisory is shared for download at seclists.org. The vendor was not involved in the public release. The advisory contains:

All credit due to the anon pastebin poster.

The exploitation is known to be difficult. Attacking locally is a requirement. A single attempt or multiple attempts are not enough for exploitation. Technical details as well as a public exploit are known.

A public exploit has been developed by rai in ANSI C and been published immediately. It is declared as proof-of-concept. The exploit is shared for download at maker.fea.st. The exploit is:

```c
#include

extern long __stack_chk_guard;
```
Improved Distract Att From X

- combine both approaches
- when a email on X appears, start several distraction threads
- attract attention to the distractor threads by lengthen the threads with sock puppet mails
- prepare juicy distractor threads ahead of time
Uses for evil.{corp,gov}

- start distractor threads around emails from opponents others you wish not to get as much attention

- add light discussion to attract attention to your emails

- discredit opponents by doing a bad sock puppetry operation on their behalf
<p>| | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>mail lists</td>
<td></td>
</tr>
<tr>
<td>online polls</td>
<td></td>
</tr>
<tr>
<td>twitter</td>
<td></td>
</tr>
<tr>
<td>reddit</td>
<td></td>
</tr>
<tr>
<td>news sites</td>
<td></td>
</tr>
<tr>
<td>comment systems</td>
<td></td>
</tr>
<tr>
<td>mail lists</td>
<td>?</td>
</tr>
<tr>
<td>-----------------</td>
<td>----</td>
</tr>
<tr>
<td>online polls</td>
<td>?</td>
</tr>
<tr>
<td>twitter</td>
<td>✓</td>
</tr>
<tr>
<td>reddit</td>
<td>?</td>
</tr>
<tr>
<td>news sites</td>
<td></td>
</tr>
<tr>
<td>comment systems</td>
<td></td>
</tr>
</tbody>
</table>
Why Polls?

- Used by a few major news sites
  - Huffington Post, Al Jazeera, etc.
  - Many more random bloggers
  - Even a Golden Globe movie awards poll
- Readers see the results of polls
The World's Most Influential Person Is...

By TIME Staff | Monday, Apr. 27, 2009

In a stunning result, the winner of the third annual TIME 100 poll and new owner of the title World's Most Influential Person is moot. The 21-year-old college student and founder of the online community 4chan.org, whose real name is Christopher Poole, received 16,794,368 votes and an average influence rating of 90 (out of a possible 100) to handily beat the likes of Barack Obama, Vladimir Putin and Oprah Winfrey. To put the magnitude of the upset in perspective, it's worth noting that everyone moot beat out actually has a job.
In a stunning result, the winner of the 2009 TIME Person of the Year poll is moot. The college student and founder of the internet bulletin board 4chan.org, whose real name is Christopher Chan, received 16,794,368 votes and an average rating of 90 (out of a possible 100) to beat out the likes of Barack Obama, Vladimir Putin, and Oprah Winfrey. To put the magnitude of the result in perspective, it's worth noting that even the highest-rated candidates actually have a job.
Surely this is a solved problem
Landslide Win

Subtle Win
HuffPo Readers Poll

THE HUFFPOST/YOUGOV POLL

How closely are you following news about the group known as the Islamic State, ISIS or ISIL that has been operating in Syria and Iraq?

- YouGov: All Americans 18+
- HuffPost Readers

**Very closely**
- 27%

**Somewhat closely**
- 41%

**Not very closely**
- 54%

**Not closely at all**
- 19%
THE HUFFPOST/YOUGOV POLL

How closely are you following news about the group known as the Islamic State, ISIS or ISIL that has been operating in Syria and Iraq?

- YouGov: All Americans 18+  
- HuffPost Readers

- **Very closely**
  - 27%  
  - 32%

- **Somewhat closely**
  - 41%
  - 20%

- **Not very closely**
  - 19%
  - 4%

- **Not closely at all**
  - 13%
  - 44%
How closely are you following news about the group known as the Islamic State, ISIS or ISIL that has been operating in Syria and Iraq?

- Very closely: 27% (21% for All Americans 18+ and 13% for HuffPost Readers)
- Somewhat closely: 41% (13% for All Americans 18+ and 63% for HuffPost Readers)
- Not very closely: 19%
- Not closely at all: 13% (63% for All Americans 18+)
these polls have a serious credibility problem
<p>| mail lists | ![Green Checkmark] | ![Meh] |
| online polls | ![Question Mark] | ![Meh] |
| twitter | ![Meh] | ![Meh] |
| reddit | ![Meh] | ![Meh] |
| news sites | ![Meh] | ![Meh] |
| comment systems | ![Meh] | ![Meh] |</p>
<table>
<thead>
<tr>
<th>mail lists</th>
<th>✅</th>
</tr>
</thead>
<tbody>
<tr>
<td>online polls</td>
<td>✅</td>
</tr>
<tr>
<td>twitter</td>
<td></td>
</tr>
<tr>
<td>reddit</td>
<td></td>
</tr>
<tr>
<td>news sites</td>
<td></td>
</tr>
<tr>
<td>comment systems</td>
<td></td>
</tr>
</tbody>
</table>
| mail lists        | ✅  
|------------------|-----
| online polls     | ✅  
| twitter          | 🧐  
| reddit           |       
| news sites       |       
| comment systems  |       |
in 140 seconds..
Gilad Lotan bought followers and did some cool analysis of the network graph*

*https://medium.com/i-data/fake-friends-with-real-benefits-eec8c4693bd3
Timeline Crowding
Balaji S. Srinivasan @balajis · 11h
These communications were:
- too trivial for movies
- too voluminous for mail
- too scandalous for news
Only feasible w/ decentralization.

Balaji S. Srinivasan @balajis · 11h
New transactions of many kinds to appear.
Will there be Bitcoin analogs for the:
- upvote
- like
- tweet
- blogpost
- email
- chat room
- IM

Balaji S. Srinivasan @balajis · 11h
That is, what new transactions are akin to new kinds of communications (likes, tweets, blog posts) newly feasible in decentralized channels?

Balaji S. Srinivasan @balajis · 11h
Internet permitted new comm types: trivial, voluminous, scandalous. What new txs does Bitcoin permit?
<table>
<thead>
<tr>
<th>mail lists</th>
<th>![Checkmark] ![Checkmark] ![Unknown]</th>
</tr>
</thead>
<tbody>
<tr>
<td>online polls</td>
<td>![Checkmark] ![Unknown]</td>
</tr>
<tr>
<td>twitter</td>
<td>![Unknown]</td>
</tr>
<tr>
<td>reddit</td>
<td>![Unknown]</td>
</tr>
<tr>
<td>news sites</td>
<td></td>
</tr>
<tr>
<td>comment systems</td>
<td></td>
</tr>
<tr>
<td>mail lists</td>
<td>![Checkmark]</td>
</tr>
<tr>
<td>------------</td>
<td>-------------</td>
</tr>
<tr>
<td>online polls</td>
<td>![Checkmark]</td>
</tr>
<tr>
<td>twitter</td>
<td>![Checkmark]</td>
</tr>
<tr>
<td>reddit</td>
<td></td>
</tr>
<tr>
<td>news sites</td>
<td></td>
</tr>
<tr>
<td>comment systems</td>
<td></td>
</tr>
<tr>
<td>mail lists</td>
<td>🧐 ✔️</td>
</tr>
<tr>
<td>-------------</td>
<td>------</td>
</tr>
<tr>
<td>online polls</td>
<td>🧐 ✔️</td>
</tr>
<tr>
<td>twitter</td>
<td>🧐 ✔️</td>
</tr>
<tr>
<td>reddit</td>
<td></td>
</tr>
<tr>
<td>news sites</td>
<td></td>
</tr>
<tr>
<td>comment systems</td>
<td></td>
</tr>
<tr>
<td>mail lists</td>
<td>![Green Check] ![Question Mark]</td>
</tr>
<tr>
<td>------------</td>
<td>---------------------------------</td>
</tr>
<tr>
<td>online polls</td>
<td>![Green Check] ![Green Check]</td>
</tr>
<tr>
<td>twitter</td>
<td>![Green Check] ![Green Check]</td>
</tr>
<tr>
<td>reddit</td>
<td>![Question Mark] ![Question Mark]</td>
</tr>
<tr>
<td>news sites</td>
<td>![Green Check] ![Green Check]</td>
</tr>
<tr>
<td>comment systems</td>
<td>![Question Mark] ![Question Mark]</td>
</tr>
</tbody>
</table>
TIL When Alan Shepard was asked what he thought about as he sat atop the Redstone rocket, waiting for liftoff, he had replied, "The fact that every part of this ship was built by the low bidder." (en.wikipedia.org)

Submitted 3 hours ago by whoa1019 to /r/todayilearned

709 comments share

One-star yelp reviews of national parks (imgur.com)

Submitted 5 hours ago by GallowBoob to /r/funny

1319 comments share

HBO to offer HBO GO without cable subscription in 2015.

/r/all (deadline.com)

Submitted an hour ago by yuppieByDay to /r/television

460 comments share

I caught Slash's guitar pick in Atlantic City. Thought I'd share :)

(.imgur.com)

Submitted 6 hours ago by Pivec to /r/pics

447 comments share

This is Lucy. Every time she goes outside she grabs a leaf and just walks around with it in her mouth :)

(imgur.com)

Submitted 6 hours ago by mluyster to /r/aww
It's cold outside. Don't forget the sweater I made you.

The Flag of Connacht, a province in Ireland

Put arms on a bird they said . . .

X-post from /r/gaming. Hotline Miami badass chicken arms!

"I have eyes on the target, over."

I am the Kingslayer

Ninja Bird

Bird Arm Billboard. This anyone's work?
Check this very active LIVE feed for the latest on Occupy Central in Hong Kong.

Greece Is In Full Blown Stock Market Collapse (businessinsider.com)

‘Anonymous’ Hacker Group Goes After ISIS (anqh.com)

Hong Kong Police filmed beating protester (online.wsj.com)

Saddam-Era Chemical Weapons Now Under ISIS Control

Iconic 2,500 year old Siberian princess 'died from breast cancer', reveals MRI scan. Preserved by ice, the 25 year old ancient woman covered in tattoos used cannabis to cope with her ravaging illness.

Activists use GPS to track illegal loggers in Brazil's Amazon rainforest: Hi-tech undercover operation used GPS tracking on timber trucks for the first time, as well as satellite and aerial images to reveal extent of illegal logging in Brazilian Amazon.
Score factors
Upvote articles we want to promote
Downvote articles we want to kill
So first we needed accounts..
Our accounts seemed broken

reddits secret sauce
But we have > 50 accounts

What we can do with 50 accounts?
On small subreddits it’s easy to get a new article on to front page by up voting
TCP reassembly bug in FreeBSD can cause kernel crash, possible memory disclosure. (freebsd.org)

How to Safely Generate a Random Number (like 6ae51281cde590) (sockpuppet.org)

Tails 1.0 released! (tails.boum.org)

OpenSSH make compiling against OpenSSL optional (article.gmane.org)

An overview of how reddit's new CSS filter works. (self.netsec)

Revocation still doesn't work (imperialviolet.org)

How To Setup Darkcomet RAT with download! (skullforums.com)
On large subreddits like worldnews, 50 isn’t enough for a full win
Upvote articles we want to promote
Downvote articles we want to kill
Let’s also try down voting..
downvote stuff to knock into moderation queue
below user/subreddit preference
Trickle Downvoting: only down vote as many up votes as new articles have.
Up-vote our target
Trickle down-vote others
Mass-DownVoting

What would happen if we down voted all new articles as they appeared?
Began with worldnews
In eastern Ukraine, the mob rules (reuters.com)

Note: We may remove bigoted or hateful comments, including those directed towards any race, religion, ethnic group, nationality, gender, or sexual orientation. Repeat offenders may be banned.

[•] Tyacre 19 points an hour ago
How the heck is this at 56 downvotes after 4 minutes?!
permalink save report give gold reply

[•] Musierra 13 points 53 minutes ago
If you look at r/worldnews/new, all posts that mention "russia" in title are massively downvote count
edit: they now switched it so it downvotes all submissions....
permalink save parent report give gold reply

[•] Tyacre 19 points an hour ago
How the heck is this at 56 downvotes after 4 minutes?!
Then..
We're under attack, comrades! Stay calm and don't move - we're fighting this thing with everything we've got! (reddit.com)

submitted 5 months ago by jamie_byron_dean to /r/circlebroke2
You've probably noticed that the up/down vote numbers have suddenly turned very strange in the past few hours, with everything being downvoted below zero. This is because /r/worldnews is under attack. The source of the downvoting is currently unknown but we and the admins are investigating and doing our best to find out.

The purpose of this attack is to disrupt the subreddit. It does this by delivering enough downvotes to render posts invisible by reddit's default settings, and to discourage your participating by downvoting everything below zero.

**Here's what you need to know:**

- Don't worry about the downvotes affecting your karma. The unusual votes (in this case, downvotes) will be wiped out when the source of the problem is identified. This will probably take a few days.
- One of the goals of the attack is to render posts invisible by downvoting them below the default threshold in users' preferences settings. The way you can neutralize that part of the attack is by changing the threshold of invisibility in your user preferences. Here's how: 1. In the upper right of your screen in the area with your username, click preferences. 2. In preferences, go to the "link options" section, and change the final line, where it says "don't show me sites with a score of less than ___". You can set it to any negative number (ex. -100), but even better than filling in a negative number is just leaving the box blank. By leaving the box blank you will completely neutralize the attackers' ability to make posts invisible.
- The "hot" tab will be broken for the duration of the attack, but we recommend browsing by the "new" tab (/r/worldnews/new).
- We also recommend voting; obviously we can't tell you how to vote, but human votes help minimize the impact of the attackers, and it only takes a fraction of a second to click the arrows.

If you like reading and participating in /r/worldnews, following the above tips can help restore most of the everyday /r/worldnews experience for you, and with your participating in voting, you can help to weaken and expose the attackers, so the admins can solve the problem faster.

We apologize for the disruption, we appreciate your patience, and we welcome any tips you have for how we can improve the /r/worldnews user experience in this time of difficulty.
Much speculation ensued ..
*** For the record, we had nothing to do with /r/technology
Simultaneously, we ran the same thing on netsec...
But netsec moderators responded with intelligent discussion and roped in official reddit admins to talk about the problem..
You had a group of about 20 bots that were being used to downvote posts in the subreddit. We rendered the voting from those accounts ineffective, but to make it more difficult for the controller of the bots to realize that they've been disabled, we still need to make it look like their votes are applying. If we just throw away their votes entirely, the controller's going to see that their bots have been blocked, and change up what they're doing immediately.

Because there's no way to tell which viewers are associated with the blocked voters, we have to show a score to everyone that looks like the votes are still applying (even though, as you said, we don't actually rank using it internally). The fake score can't be only shown to bot accounts. If the controller opens a submission in an incognito window via TOR or something, we'd have no way of linking them back to the bots. So when their 20 downvotes are gone there, they'd know what happened. This is /r/netsec, I'm sure I don't need to elaborate on how many other options there are for separating yourself from this sort of thing. The only feasible option is showing the fake scores to everyone unless we want detection to be trivial.

Being able to hide scores on submissions temporarily like you suggested might help some, but it really just delays the problem, it doesn't solve it. There are also various undesirable side effects from hiding submission scores that don't apply as much to comments. Over the years, a number of subreddits have tried experiments with hiding all submission scores using CSS like you've done, and they pretty much universally decided that it was a bad idea. Because the "hot" ranking involves both score and time, with things dropping in rank based on how old they are, being able to see the scores lets the viewer easily get an idea of how popular/significant different submissions are. Without that information available, it becomes extremely difficult for someone to look at a subreddit's front page and quickly figure out which submissions were the most popular recently.

I was the one that added the ability for moderators to temporarily hide comment scores, and I've definitely thought about extending it to submissions as well. But seeing how poorly all of those experiments that tried to do the same thing with CSS ended up going has made me hesitant about it. We do already have a very "light" score-hiding for submissions, where you can't see the score for the first 2 hours unless you actually visit the comments page. I'm not fully convinced that allowing true hiding like we have for comments would be a good thing, and most likely especially not for longer time periods since it makes the front page more and more confusing the longer the scores are hidden for.
This should have been much easier to spot
This should have been much easier to spot

- voting in synch
- signup times
- some common email domains
- pattern of names
- ip-addresses from known open proxies
- user-agents: headers
- low karma interactors
BTW… Two months later

to
This should have been much easier to spot

- voting in synch
- signup times
- some common email domains
- pattern of names
- ip-addresses from known open proxies
- user-agents: headers
- low karma interactors
Growing Personas for Karma
Everything i needed to know about managing hackers, i learnt from my DVD collection..

Does twitter kill the blogging star?

Memory Corruption Attacks. The (almost) complete history..

Some Computer Security Prezi's

Anonymity loves Company

Tell HN: Toy app thrown together for fun

Too many InfoSec Conferences? (Infographic Inside)

Tell HN: Subscription Service that covers InfoSec Happenings..

What Anonymous taught us about Cyber War

Searchable Security Conference Site

LulzSec will be used to Usher in Regulation (few of us will like)

Create graphs/nodes/edges in JavaScript (an arbor.js tutorial)

Automated Shoulder Surfing Attacks (Computer Vision meets on screen keyboards)

BlackHat 2011 (according to Twitter)

(Simple) Chrome plugin for GPG/PGP in GMail

Update: (Simple)Chrome plugin to enable GPG in Gmail

Oracles Mary Ann Davidson lashes out at Security Firm

Poll: Spotted the Polls/Karma Link?

Etsy's Office-Hacker Job shows established companies the way..

You and Your Research, a modern take
23 Links - Karma: 99
<table>
<thead>
<tr>
<th>mail lists</th>
<th>✅</th>
</tr>
</thead>
<tbody>
<tr>
<td>online polls</td>
<td>✅</td>
</tr>
<tr>
<td>twitter</td>
<td>✅</td>
</tr>
<tr>
<td>reddit</td>
<td>?</td>
</tr>
<tr>
<td>news sites</td>
<td></td>
</tr>
<tr>
<td>comment systems</td>
<td></td>
</tr>
<tr>
<td>mail lists</td>
<td></td>
</tr>
<tr>
<td>------------------</td>
<td>---</td>
</tr>
<tr>
<td>online polls</td>
<td></td>
</tr>
<tr>
<td>twitter</td>
<td></td>
</tr>
<tr>
<td>reddit</td>
<td></td>
</tr>
<tr>
<td>news sites</td>
<td></td>
</tr>
<tr>
<td>comment systems</td>
<td></td>
</tr>
<tr>
<td>mail lists</td>
<td>💬</td>
</tr>
<tr>
<td>--------------</td>
<td>----</td>
</tr>
<tr>
<td>online polls</td>
<td>💬</td>
</tr>
<tr>
<td>twitter</td>
<td>💬</td>
</tr>
<tr>
<td>reddit</td>
<td>💬</td>
</tr>
<tr>
<td>news sites</td>
<td>💬</td>
</tr>
<tr>
<td>comment systems</td>
<td></td>
</tr>
<tr>
<td>mail lists</td>
<td>✔️</td>
</tr>
<tr>
<td>online polls</td>
<td>✔️</td>
</tr>
<tr>
<td>twitter</td>
<td>✔️</td>
</tr>
<tr>
<td>reddit</td>
<td>✔️</td>
</tr>
<tr>
<td>news sites</td>
<td>?</td>
</tr>
<tr>
<td>comment systems</td>
<td>☹️</td>
</tr>
</tbody>
</table>
Why News Sites?
Cyclone Hudhud leaves trail of devastation; 6 killed in Andhra Pradesh, Odisha

Cyclone Hudhud pounded the coastal districts of Andhra Pradesh and Odisha with heavy rain and winds of almost 195 kmph leaving six people dead and a trail of devastation with Visakhapatnam, where the very severe storm made landfall, bearing the brunt. **NDRF** helpines: 01126107953; 09711077372

Pakistan targets 15 posts in Jammu, seeks UN intervention

Pakistan heavily shelled 15 border outposts and hamlets in Arnia sector of Jammu and Kashmir early Sunday even as it wrote to UN chief Ban Ki-moon blaming India for the escalation in border clashes and sought UN intervention on Kashmir.

Rahul Gandhi to do a BJP, veterans will make way for Gen Next

In what may set off alarm bells for many powerful Congress veterans, Rahul Gandhi is learnt to be planning to introduce some drastic measures, including bringing up a new set of leaders to replace the existing ones in...
Can we influence this panel? Get articles on it or keep articles off it?
Megachurches: The hidden pillar of Nigeria's economy

Exactly how much of Nigeria’s $510bn GDP megachurches make up is difficult to assess, since they are, like the oil sector, largely opaque entities.

Related articles:
- TB Joshua’s church: Built, like others, on shifting sands
- ANCYL to block TB Joshua from entering SA
- Press pause on prophet TB Joshua’s power

Obituary: The warmth and laughter of Chris van Wyk

Why is Ebola being treated as an 'African disease?'

The head of the African Development Bank has criticised the international response to the Ebola outbreak as too little, too late.

Related articles:
- Dewani describes meeting Anni in plea document
- Lesetja Kganyago named new Reserve Bank governor
- Megachurches: The hidden pillar of Nigeria's economy
- Union demands Telkom retract retrenchment letters to staff
Panel features recent articles with the most page views.
Page views we can control!
The forgotten battlefields

Most Popular This Week

Zuma could testify before Nkandla disciplinary

The PSA has not ruled out the possibility of President Jacob Zuma being called to testify during the public works departmental hearings.

No timeline for return of Nigerian church collapse bodies

The class issue
Hong Kong withdraws riot police

In Zimbabwe, preaching is politics

The art of twar: Malema vs Mbalula

Botswana’s clean image hides the dirt
THE WALL STREET JOURNAL.
The U.S. credit-card industry has found its sweet spot: a combination of moderate economic growth, low interest rates and consumers who have struck a balance between spending more and paying their bills on time. 23 min ago

**Retailers See Winds Filling Holiday Sales**

*Ahead of the Tape:* The National Retail Federation is expecting a 4.1% rise in holiday sales overall. With pump prices near three-year lows, more dollars should find their way to the mall.

**Irish Tax Loophole Could Close**

Ireland is expected on Tuesday to unveil changes to its tax code that could eventually close a well known corporate-tax loophole, the Double Irish.

**OPEC Members’ Rift Deepens**

A rift between OPEC members deepened over the weekend, as rival producers in the cartel moved in sharply different directions amid recently falling oil prices.

**Banks Back Crisis Plan**

**U.K. Government Launches Sale of Eurostar Stake**

**Fed’s Tarullo Concerned About U.S. Productivity**

**‘Gone Girl’ Leads Box Office Again**

**Asia Makes a Move in Gold Trading**

**Hyundai Land Deal: Short on Oversight**

**CVC to Start Taking Share Orders for**

---

**Judges Step Up Electioneering**

Out-of-state groups are pouring money into judicial elections, upsetting genteel traditions under which judges in some states faced little opposition and avoided the ethnically tricky process of stumping for votes.

**World**

**In Hong Kong, Both Sides Dig In**

Protest leaders and authorities dug in over the weekend, as Hong Kong’s pro-democracy demonstration looked to start a third week with increasingly pointed rhetoric and key roads still blocked.

- China, U.S. Standoff Deepens Over Protests
- Bolivian Leader Poised for Third Term
- Silva Endorses Former Rival for Brazilian Presidency
- Moscow, Kiev Take Steps to Ease Tensions

---

**Popular Now**

1. CDC Confirms Texas Health Worker Has Ebola
2. A Musical Fix for American Schools
3. Canadian Pacific Approached CSX About Merger
4. ‘Maximizer’ or ‘Satisficer’—Which Are You?
5. OPEC Members’ Rift Deepens Amid Falling Oil Prices
Content engaging our readers now, with additional prominence accorded if the story is rapidly gaining attention. Our WSJ algorithm comprises 30% page views, 20% Facebook, 20% Twitter, 20% email shares and 10% comments.
Laila Blunt @LailaBlunt · Jun 26
Only if for 1629 online.wsj.com/articles/egypt...

Laila Blunt @LailaBlunt · Jun 26
Only if for 1628 online.wsj.com/articles/team-

Laila Blunt @LailaBlunt · Jun 26
Only if for 1627 online.wsj.com/articles/gore-

Laila Blunt @LailaBlunt · Jun 26
Only if for 1626 online.wsj.com/articles/want-

Laila Blunt @LailaBlunt · Jun 26
Only if for 1625 online.wsj.com/articles/fifa-

Laila Blunt @LailaBlunt · Jun 26
Only if for 1624 online.wsj.com/articles/want-

Laila Blunt @LailaBlunt · Jun 26
Only if for 1623 online.wsj.com/articles/losse...
Coulson Guilty, Brooks Cleared in Tabloid Trial
Two former senior News Corp editors met sharply different fates in the long-running phone-hacking case, as the jury cleared Rebekah Brooks of all charges but found Andy Coulson guilty of illegally intercepting voice-mail messages.
- Prosecutors Have Little to Show
- Cameron Issues Apology
-raphic: Verdicts in the Trial

At Least 90 More Kidnapped in Nigeria

Top Picks

LeBron James to Opt Out of Heat Deal

Under Ousted CEO, Target Lost Its Way

Food Makers' Secret Ingredient: Less Salt

Opinion: Fouad Ajami, Great American
Deep Germany Ready to Break U.S. Hearts
For the millions of Americans who have gotten swept onto the U.S. soccer bandwagon, be warned before this critical third game of the 2014 World Cup—Germany is the international soccer version of a bucket of cold water.

Popular Now

1. Opinion: Fouad Ajami, Great American

2. U.S. Set to Export First Oil Since '70s

3. Social Media Fail to Live Up to Early Marketing Hype

4. Google Readiies TV Set-Top Box

5. The Gluten-Free Craze: Is It Healthy?
but we need an account on the site to share the article
At the time of writing, we have at least 30,000 accounts.

** NYT Admins - Sorry!
15. OP-ED CONTRIBUTOR
An Adirondack Wilderness Imperiled
By EDWARD ZAHNISER
A plan set in motion by Gov. Andrew Cuomo would allow an open pit mine in forest preserve land.
Go to Article | Email

16. Making Quinoa and Rice Bowls
Jenny Woodward
Melissa Clark assembles a hearty meal with quinoa, kale, kimchi, egg and a simple dressing.
Go to Article | Email

17. YOUR MONEY
Beware of Shifting Options Within Medicare Plans
By TARA SIEGEL BERNARD
Open enrollment for Medicare starts Oct. 15, and offers older Americans a dizzying array of health care options.
Go to Article | Email

18. MUSIC REVIEW
Swept Up in Bach’s All-Consuming Passion
By ANTHONY TOMMASINI
The Berlin Philharmonic’s performance of “St. Matthew Passion” at the Park Avenue Armory, conducted by Simon Rattle, showed why Bach chose other ways besides opera to tell stories through music.
Go to Article | Email

19. A Twist Adds Complexity to a Pasta Dish
By MARK BITTMAN
Mark Bittman’s take on a great pasta dish for the fall, pasta alla Norma.
Go to Article | Email

20. Restaurant Cocktails That Aim Too High
By PETE WELLS
New restaurants in New York City are offering cocktail lists that are becoming more creative, and not in a good way.
Go to Article | Email
14. Cave Paintings in Indonesia May Be Among the Oldest Known
By JOHN NOBLE WILFORD
The paintings of hands and animals in seven limestone caves on Sulawesi had previously been dismissed as no more than 10,000 years old.
NYT spends millions on their news gathering apparatus
NYT spends millions on their news gathering apparatus
NYT spends millions on their news gathering apparatus

Cost to register 30k accounts: $ 0.12
NYT spends millions on their news gathering apparatus

<table>
<thead>
<tr>
<th>Description</th>
<th>Cost</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cost to register 30k accounts</td>
<td>$0.12</td>
</tr>
<tr>
<td>Cost to share 30k stories</td>
<td>$0.18</td>
</tr>
</tbody>
</table>
NYT spends millions on their news gathering apparatus

Cost to register 30k accounts: $0.12
Cost to share 30k stories: $0.18
Trivially manipulate the NYT front page: Priceless
NYT spends millions on their news gathering apparatus

Cost to register 30k accounts: $0.12
Cost to share 30k stories: $0.18
Trivially manipulate the NYT front page: Priceless
<table>
<thead>
<tr>
<th></th>
<th>![Icon]</th>
<th>![Checkmark]</th>
</tr>
</thead>
<tbody>
<tr>
<td>mail lists</td>
<td>![Icon]</td>
<td>![Checkmark]</td>
</tr>
<tr>
<td>online polls</td>
<td>![Icon]</td>
<td>![Checkmark]</td>
</tr>
<tr>
<td>twitter</td>
<td>![Icon]</td>
<td>![Checkmark]</td>
</tr>
<tr>
<td>reddit</td>
<td>![Icon]</td>
<td>![Checkmark]</td>
</tr>
<tr>
<td>news sites</td>
<td>![Icon]</td>
<td>?</td>
</tr>
<tr>
<td>comment systems</td>
<td>![Icon]</td>
<td></td>
</tr>
<tr>
<td>mail lists</td>
<td>![Checkmark]</td>
<td></td>
</tr>
<tr>
<td>------------</td>
<td>-------------</td>
<td></td>
</tr>
<tr>
<td>online polls</td>
<td>![Checkmark]</td>
<td></td>
</tr>
<tr>
<td>twitter</td>
<td>![Checkmark]</td>
<td></td>
</tr>
<tr>
<td>reddit</td>
<td>![Checkmark]</td>
<td></td>
</tr>
<tr>
<td>news sites</td>
<td>![Checkmark]</td>
<td></td>
</tr>
<tr>
<td>comment systems</td>
<td>![Human Figure]</td>
<td></td>
</tr>
<tr>
<td>mail lists</td>
<td>✅</td>
<td></td>
</tr>
<tr>
<td>online polls</td>
<td>✅</td>
<td></td>
</tr>
<tr>
<td>twitter</td>
<td>✅</td>
<td></td>
</tr>
<tr>
<td>reddit</td>
<td>✅</td>
<td></td>
</tr>
<tr>
<td>news sites</td>
<td>✅</td>
<td></td>
</tr>
<tr>
<td>comment systems</td>
<td>✅</td>
<td></td>
</tr>
<tr>
<td>mail lists</td>
<td>🧐 ✔️</td>
<td></td>
</tr>
<tr>
<td>-------------------------</td>
<td>------</td>
<td></td>
</tr>
<tr>
<td>online polls</td>
<td>🧐 ✔️</td>
<td></td>
</tr>
<tr>
<td>twitter</td>
<td>🧐 ✔️</td>
<td></td>
</tr>
<tr>
<td>reddit</td>
<td>🧐 ✔️</td>
<td></td>
</tr>
<tr>
<td>news sites</td>
<td>🧐 ✔️</td>
<td></td>
</tr>
<tr>
<td>comment systems</td>
<td>🧐 ?️</td>
<td></td>
</tr>
</tbody>
</table>
In Brief

• Disqus let’s you drop a few lines of .js in your page which magically gives you an entire commenting system.

• Comments can be voted up/down which affects order.

• User profiles are visible across sites and your comments are gathered in your Disqus profile page.

• Admins get a nifty interface to moderate and maintain their comment threads.
Used by Wordpress blogs, Tumblrs, soccer mom forums
They don’t control the full message
abbot:disqus marco$
• Login: left as an exercise for the reader

• Mass post:

```bash
export thread="threadid"; export msg="mymessage"; (for i in `seq -f "userprefix%g" 1 100`; do echo "curl -b "${i}.cookies" -d "thread=${thread}&message=${msg}&api_key=${API_KEY}" http://disqus.com/api/3.0/posts/create.json"; done;) | parallel
```

• Mass vote:

```bash
export post="postid"; export vote="1"; (for i in `seq -f "userprefix%g" 1 100`; do echo "curl -b "${i}.cookies" -d "post=${post}&vote=${vote}&api_key=${API_KEY}" http://disqus.com/api/3.0/posts/vote.json"; done;) | parallel
```
• Mass downvote:

```bash
export post="postid"; export vote="-1"; (for i in `seq -f "userprefix%g" 1 100`; do echo "curl -b "${i}.cookies" -d "post=${post}&vote=${vote}&api_key=${API_KEY}" http://disqus.com/api/3.0/posts/vote.json"; done;) | parallel
```

• Bonus: Flag posts to temporarily make them disappear

```bash
export post="postid"; (for i in `seq -f "userprefix%g" 1 100`; do echo "curl -b "${i}.cookies" -d "post=${post} &api_key=${API_KEY}" http://disqus.com/api/3.0/posts/report.json"; done;) | parallel
```
abbot:disqus marco$
abbot:disqus marco$
Pretty much complete control of Disqus forums (with 1 line of bash script)
Wut?
• User registration isn’t IP-limited that we’ve encountered

• Email verification isn’t a requirement

• Guest voting _is_ IP-limited

• Open proxy lists bypass this trivially
ALL OF THE SAME ATTACKS
PSObama

Thanks Obama!  Edit (in 6 minutes)

boiseboy12

I recommend you read Jeremy Rifkins book "The Third Industrial Revolution" about how the Europeans are addressing their energy needs, and how it is producing not just power, but a lateral society.

IBM has created a computer system that coordinates individually
Flag as spam 4/5 times to remove
(try it yourself on fox news :)
livefyre: one more thing..
"There might still be some adjustments to my schedule moving forward. I definitely need to play well for that to happen. If I don't play well, I guess I can also play everything," he said.

Federer could reach No. 2 with a good performance in Shanghai.

Before commenting, please read our Posting Guidelines.

normaluser4

Dan Last
I pretty much doubt that he will skip Basel or Paris if he does well in Shanghai and could gain points on Novak. If he has a chance to end year end No. 1 he will play as much as he can.

This would be his ultimate achievement, to get back that year end No 1 and he is close, considering that Novak may take some time off due to his private situation.

If Novak wins Shanghai he probably will end up No 1 as his lead over Fed would be at least 2,000 pts with only about 3,000 pts up for grabs for the rest of the season.

Rafa pretty much has no more chance to end as year end No 1. He would have to win everything and hope Novak does not bag more than 1000 points in the 4 events. Given Nadal's injury, form and also past history at indoor events I just don't see that. He never won London but would have to win all 5 matches at London to get the 1,500 pts needed.
2 comments

normaluser4

I

Newest | Oldest | Top Comments

epsilon0 | moderator
test | Edit
Latest blog post: Scr New | Sep 23, 2014

epsilon0 | moderator
eof | Edit
Latest blog post: New collection | Sep 23, 2014
"GET /lftoken/eyJhbGciOiAiSFMyNTYiLCAidHlwIjogIkpXVCJ9.eeyJjb21haW4iOiJ0OTgsICJ1c2VyX2lkIjogIl91cDY2NDY3ODUyIn0.CwvDr6oXnz1d0P8rch4-jzfU4jqR2VNVdzsLbkopAD0?r=e1ws1nel3lw HTTP/1.1" 200
"We are told about the world before we see it. We imagine most things before we experience them. And those preconceptions, unless education has made us acutely aware, govern deeply the whole process of perception." Walter Lippmann, Public Opinion
<table>
<thead>
<tr>
<th>mail lists</th>
<th>![check mark]</th>
</tr>
</thead>
<tbody>
<tr>
<td>online polls</td>
<td>![check mark]</td>
</tr>
<tr>
<td>twitter</td>
<td>![check mark]</td>
</tr>
<tr>
<td>reddit</td>
<td>![check mark]</td>
</tr>
<tr>
<td>news sites</td>
<td>![check mark]</td>
</tr>
<tr>
<td>comment systems</td>
<td>![question mark]</td>
</tr>
<tr>
<td>Feature</td>
<td>Status</td>
</tr>
<tr>
<td>-------------------------</td>
<td>---------</td>
</tr>
<tr>
<td>mail lists</td>
<td>![checkmark]</td>
</tr>
<tr>
<td>online polls</td>
<td>![checkmark]</td>
</tr>
<tr>
<td>twitter</td>
<td>![checkmark]</td>
</tr>
<tr>
<td>reddit</td>
<td>![checkmark]</td>
</tr>
<tr>
<td>news sites</td>
<td>![checkmark]</td>
</tr>
<tr>
<td>comment systems</td>
<td>![checkmark]</td>
</tr>
<tr>
<td>mail lists</td>
<td>✅</td>
</tr>
<tr>
<td>------------</td>
<td>----</td>
</tr>
<tr>
<td>online polls</td>
<td>✅</td>
</tr>
<tr>
<td>twitter</td>
<td>✅</td>
</tr>
<tr>
<td>reddit</td>
<td>✅</td>
</tr>
<tr>
<td>news sites</td>
<td>✅</td>
</tr>
<tr>
<td>comment systems</td>
<td>✅</td>
</tr>
</tbody>
</table>
Are these attacks happening?
4chan polls
HamBaconEggs · 7 months ago  
"The jew cries out in pain as he strikes you." -Polish proverb

DeShawn S. Williams  
Pro-White/Black, anti-jew

Palestine in Chile

HamBaconEggs · 7 months ago  
If you don't like what you see here, Shlomo, then go hide in your synagogue and study Talmud all day. Progressives, among others, are sick and tired of Zionist jews committing heinous crimes and then using their disproportionate financial and media control to justify or underwrite them. The complete rejection of "anti-Semitism" is just a way to shut up those who call you out on your tactics. Time to stop acting as though you're better than the "goyim." You're no better than anyone else; indeed, a majority of your tribe have proven themselves far worse.

HamBaconEggs · Guest · 10 months ago  
Just imagine how many millions of people would have been saved from the scourge of Judeo-imperialist wars and Jewish financial predations had Hitler actually finished the job.

http://www.commondreams.org/hambaconeggs
Palestine in Chile

HamBaconEggs • 7 months ago
"The jew cries out in pain as he strikes you." - Polish proverb

DeShawn S. Williams
Pro-White/Black, anti-jew

Palestine in Chile

HamBaconEggs • 7 months ago
If you don't like what you see here, Shlomo, then go hide in your synagogue and study Talmud all day. Progressives, among others, are sick and tired of Zionist Jews committing heinous crimes and then using their disproportionate financial and media control to justify or underwrite them. The constant drumbeat of "anti-Semitism" is just a way to shut up those who call you out on your tactics. Time to stop acting as though you're better than the "goyim." You're no better than anyone else; indeed, a majority of your tribe have proven themselves far worse.

HamBaconEggs • Guest • 10 months ago
Just imagine how many millions of people would have been saved from the scourge of Judeo-imperialist wars and Jewish financial predations had Hitler actually finished the job.

http://www.commondreams.org/hambaconeggs
Remember:

We discovered that flagging posts got them killed?
Please help us by marking any antisemitic and anti Israeli comments as spam!

434 Likes 86 Comments

IDF
Saturday at 12:10 PM

Will you help?

IDF
July 7 at 2:04 PM
EFFECTS: Definition

- "Using online techniques to make something happen in the real or cyber world"

- Two broad categories:
  - Information Ops (influence or disruption)
  - Technical disruption

- Known in GCHQ as **Online Covert Action**

- The 4 D’s: **Deny / Disrupt / Degrade / Deceive**
<table>
<thead>
<tr>
<th><strong>Swamp donkey</strong></th>
<th>Is a tool that will silently locate all predefined types of file and encrypt them on a target's machine.</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>TORNADO ALLEY</strong></td>
<td>Is a delivery method (Excel Spreadsheet) that can silently extract and run an executable on a target's machine.</td>
</tr>
<tr>
<td><strong>UNDERPASS</strong></td>
<td>Change outcome of online polls (previously known as NUBILO)</td>
</tr>
<tr>
<td><strong>VIPERS TONGUE</strong></td>
<td>Is a tool that will silently Denial of Service calls on a Satellite Phone or a GSM Phone.</td>
</tr>
<tr>
<td><strong>WARPATH</strong></td>
<td>Mass delivery of SMS messages to support an Information Operations campaign</td>
</tr>
</tbody>
</table>

**Work Flow Management**

- **UNDERPASS**: Change outcome of online polls (previously known as NUBILO)
  - In development.
Disqus seems ripe for the picking. So we went looking active armies.
Most commented thread on CNN’s highest voted comment

Mimi Satterlee  ·  3 months ago

I wish you a speedy and full recovery from your condition.

Thanks Son.

665  ·  Share
Most commented thread on CNN's highest voted comment

46324 Comments

Sort by Best

octo

664 Guest Votes

THANKS SORT.

665 → ▼ • Share ›
Approach
Pick slightly controversial topic
Pick news orgs that cover this topic
Then

• Use Disqus API to get a list of popular stories

• For each story, use the API to pull user info

• Link users to stories they commented on

• and...
Cue a bunch of similar attempts to look at the data
Decided to focus on voting
Voting metric

- Pull all comments for random story.
- For each comment pull the non-guest voters.
- For each voter retrieve their registration time.
- Calculate the variation in voter age on each comment.
What stood out

• Accounts had been registered within minutes of each other.

• Their usernames and profile names had a regular pattern:
  • Username: <Firstname><Surname>
  • Profile name: <Firstname> <Surname>
[*] Looking up comment 1540287681
[*] Looking up voters on comment 1540287681

NatalyaMcalpin - Natalya Mcalpin (109616253) 2014-06-05T17:46:08 117d
OdessaOgilvie - Odessa Ogilvie (109616307) 2014-06-05T17:46:32 117d
PaigeSwanger - Paige Swanger (109616327) 2014-06-05T17:46:42 117d
PaulinaPrivett - Paulina Privett (109616340) 2014-06-05T17:46:48 117d
RandaBallance - Randa Ballance (109616381) 2014-06-05T17:47:07 117d
RodgerRansom - Rodger Ransom (109616473) 2014-06-05T17:47:41 117d
RogerReddix - Roger Reddix (109616481) 2014-06-05T17:47:46 117d
SorayaPiotrowski - Soraya Piotrowski (109616699) 2014-06-05T17:49:34 117d
TeriClerk - Teri Clerk (109616781) 2014-06-05T17:50:07 117d
TerinaTurrell - Terina Turrell (109616790) 2014-06-05T17:50:13 117d
ThaoMcanulty - Thao Mcanulty (109616811) 2014-06-05T17:50:22 117d
TyrellTennyson - Tyrell Tennyson (109616851) 2014-06-05T17:50:40 117d
VertieValliere - Valliere (109616881) 2014-06-05T17:50:54 117d

Guests Likes: 23
Meanwhile, ISIS rapists and kidnappers are admired followers of ISIS's...
What about their emails addresses?

(Hint: you really shouldn’t be able to retrieve a Disqus user’s email address)
We found an unmask attack that returns an email address for a profile name*

*Already reported and fixed
Supposed puppets had emails in the form:

<Firstname><Surname>@gmail.com
We had our suspicions, but thought the puppet army would be larger.

Time to enumerate.
User Enumeration

• Disqus users get a unique ID

• This ID is a counter (yay!)

• There are unrestricted APIs to query user information (yay! yay!)
  • https://disqus.com/api/3.0/users/details.json

• We can lookup email addresses for each enumerated user with our unmask attack (yay! yay! yay!)

• So we pick a lower and upper bound beyond the lowest and highest known puppet IDs, making a range of 5k users.

• Pull details for all users.
5k users. Now what?

- Filter on known values:
  - Must have username, name and email patterns, and not be verified.
  - Age is already taken into account with the ID, so less relevant.
So Far

• Accounts with
  • Patterned profile names
  • Patterned usernames
  • Patterned emails
  • Similar registration times
  • Regular inter-registration delays
  • Alphabetical progression in usernames
Disqus lets us map usernames to forums where they’re active
Disqus also lets us map usernames to comments*

*Including “Private” profiles
<p>There no hasbaRats defending the indefensible i</p>
So Far

• Accounts with
  • Patterned profile names
  • Patterned usernames
  • Patterned emails
  • Similar registration times
  • Regular inter-registration delays
  • Alphabetical progression in usernames

• And
  • Active on the same set of sites
  • Shared duplicate comments across accounts
  • Vote for each other’s comments to push them up
<table>
<thead>
<tr>
<th>category</th>
<th>value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Puppet army size</td>
<td>186 confirmed</td>
</tr>
<tr>
<td>Period of activity</td>
<td>Four months (2014-06-5)</td>
</tr>
<tr>
<td>Comments posted</td>
<td>7269</td>
</tr>
<tr>
<td>Unique comments</td>
<td>5782 (1487 dups)</td>
</tr>
<tr>
<td>Primary targeted forums</td>
<td>CNN, Al Jazeera, Jerusalem Post</td>
</tr>
</tbody>
</table>
What are they saying?
Consistent multi-faceted views

- Pro-Palestine
- Anti-Israel
- Anti-ISIS/L
- Writes “We (USA)”, presents as Western
- Anti-Syria
- Anti-Obama
- Pro-Islam (Writes “I am Christian and I know that Christianity is worst religion in the world” :)

So who is this?
No idea. Anything is pure speculation.
Ways out?
Shut down this puppet army
Disqus limiting their API. (This would be a bad idea.)
• Puppetry is very likely happening in other places.

• But without the same amount of data, we can’t tell.

• Disqus’ open data approach is great for identifying these relationships and patterns, and we want to give them shouts for it.

• (But fix the unmask attacks.)
Summary ?
Slide 223/225
• Without exception, all of the UGC sites we have looked at have proven to be fairly trivial to manipulate

• It is clear that this abuse is already taking place on many of them
  
  • Be aware of it;
  
  • Build tools to help deal with it;