SecTheory

Internet Security

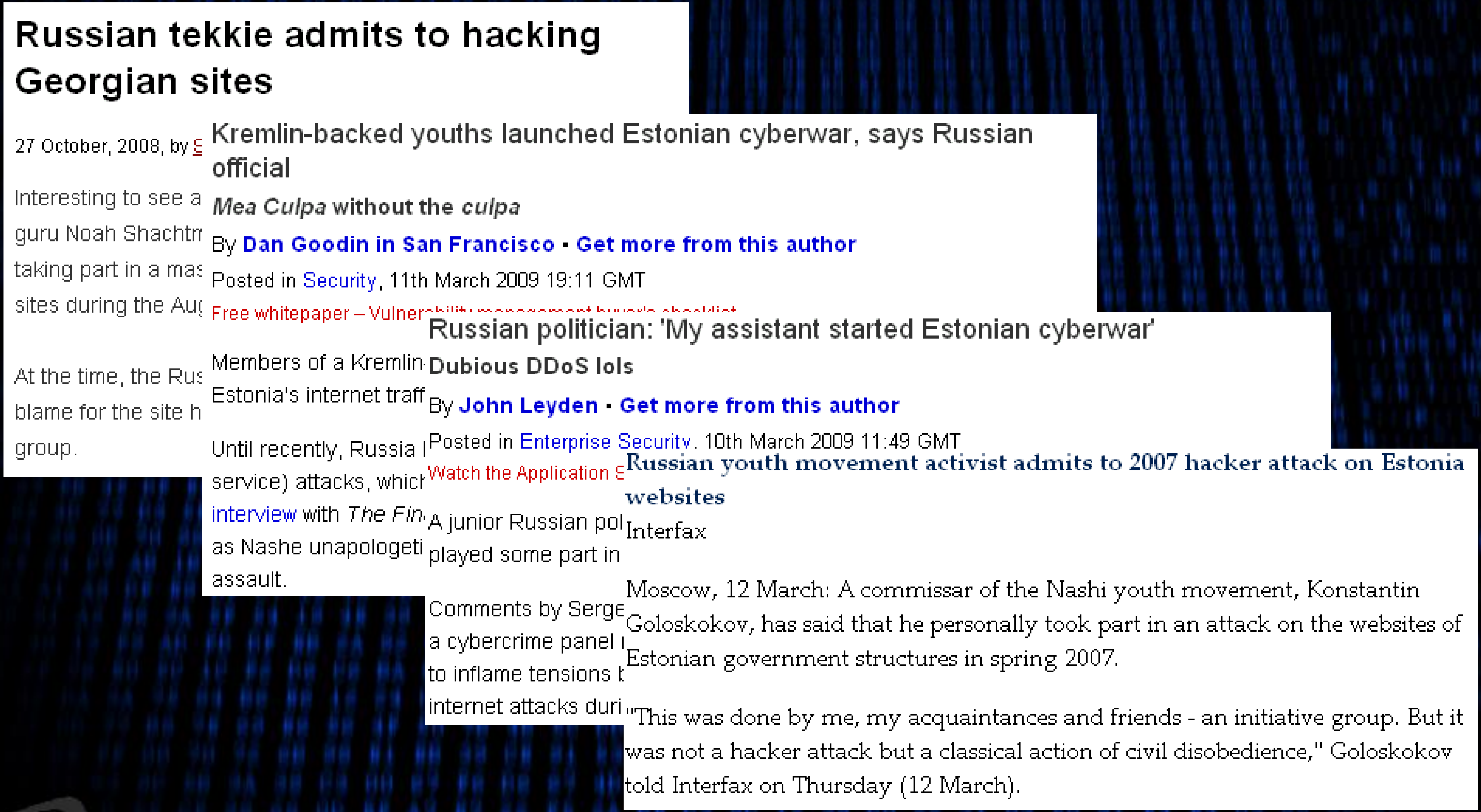
About Me

- Robert “RSnake” Hansen - CEO
- SecTheory LLC
  - Bespoke Boutique Internet Security
    - Web Application/Browser Security
    - Network/OS Security
    - Advisory capacity to VCs/start-ups
    - http://www.sectheory.com/
- Founded the web application security lab
    - http://ha.ckers.org/ - the lab
    - http://sla.ckers.org/ - the forum

What is War?

- "What do you do about that one machine that's left over?"
- "Oh, just blow it up."
- "You mean… kinetically?"

What is Cyber War?



Russian tekkie admits to hacking Georgian sites

27 October, 2008, by S

Interesting to see a
guru Noah Shachtm
taking part in a mas
sites during the Au

At the time, the Rus
blame for the site h
group.

Kremlin-backed youths launched Estonian cyberwar, says Russian official

Mea Culpa* without the *culpa

By **Dan Goodin in San Francisco** • **Get more from this author**

Posted in Security, 11th March 2009 19:11 GMT

Free whitepaper – Vulner

Members of a Kremlin
Estonia's internet traff

Until recently, Russia
service) attacks, which
interview with *The Fin*
as Nashe unapologeti
assault.

Russian politician: 'My assistant started Estonian cyberwar'

Dubious DDoS lols

By **John Leyden** • **Get more from this author**

Posted in Enterprise Security, 10th March 2009 11:49 GMT

Watch the Application S

A junior Russian pol
played some part in

Comments by Serge
a cybercrime panel
to inflame tensions
internet attacks duri

Russian youth movement activist admits to 2007 hacker attack on Estonia websites

Interfax

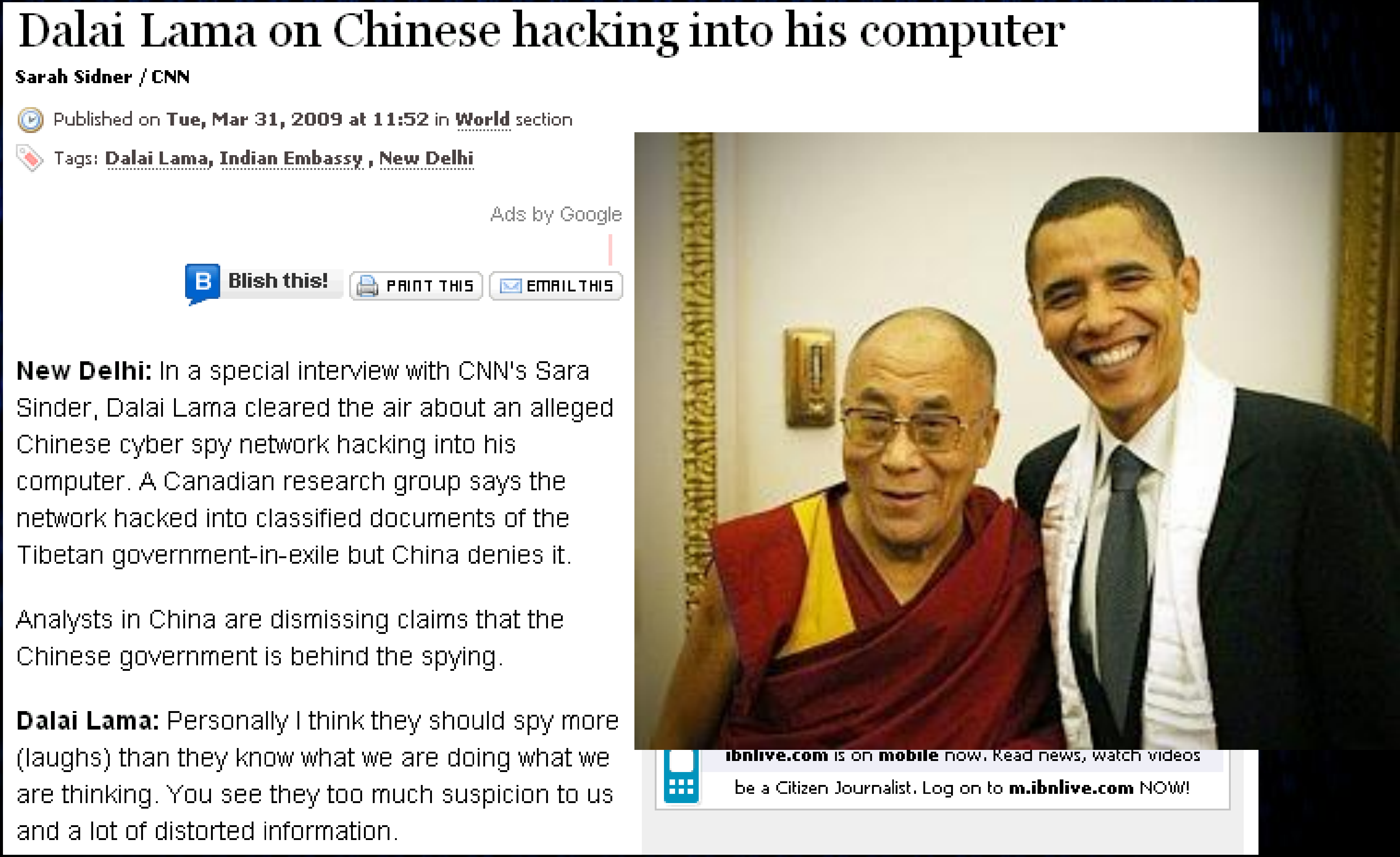
Moscow, 12 March: A commissar of the Nashi youth movement, Konstantin Goloskokov, has said that he personally took part in an attack on the websites of Estonian government structures in spring 2007.

"This was done by me, my acquaintances and friends - an initiative group. But it was not a hacker attack but a classical action of civil disobedience," Goloskokov told Interfax on Thursday (12 March).

Why Are Consumers Special?

- They're programmable
  - Must use social networking to be a part of the social herd
- They're ignorant
  - Do not understand technologies beyond the most simple
- When consumers think they're special, they're right but for completely the wrong reason.

Dalai Lama



Dalai Lama on Chinese hacking into his computer

Sarah Sidner / CNN

Published on **Tue, Mar 31, 2009 at 11:52** in **World** section

Tags: **Dalai Lama**, **Indian Embassy** , **New Delhi**

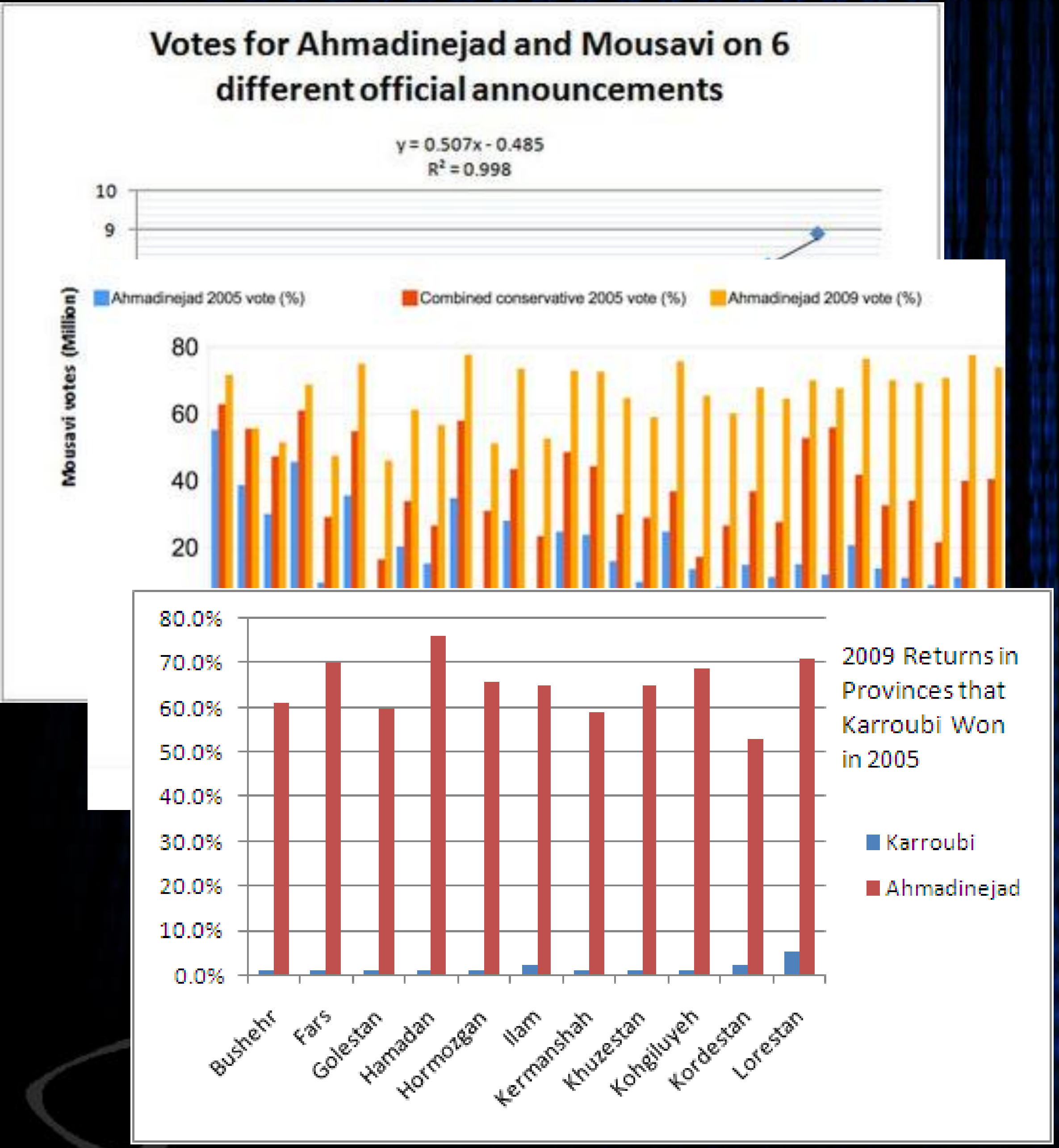
New Delhi: In a special interview with CNN's Sara Sinder, Dalai Lama cleared the air about an alleged Chinese cyber spy network hacking into his computer. A Canadian research group says the network hacked into classified documents of the Tibetan government-in-exile but China denies it.

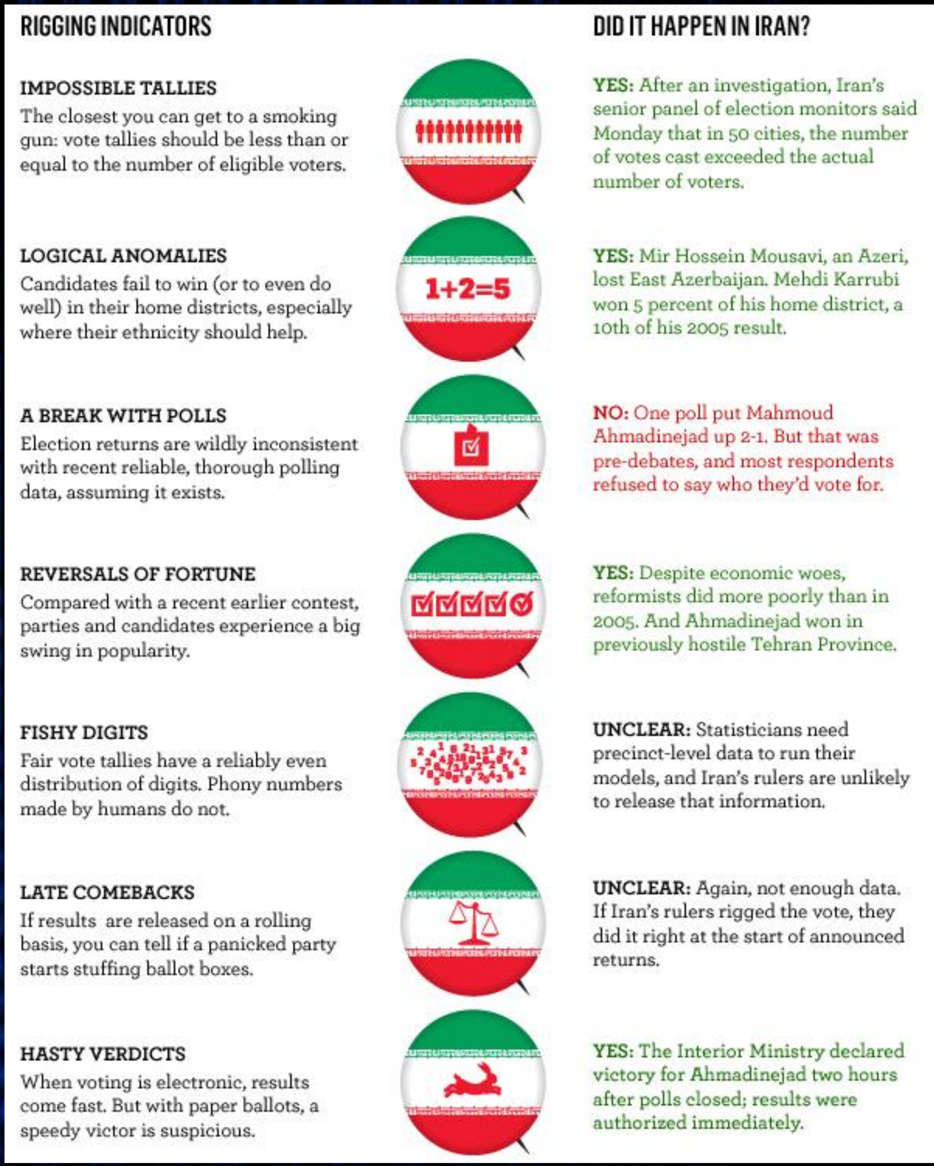
Analysts in China are dismissing claims that the Chinese government is behind the spying.

Dalai Lama: Personally I think they should spy more (laughs) than they know what we are doing what we are thinking. You see they too much suspicion to us and a lot of distorted information.

Iran in Turmoil

Voter Fraud

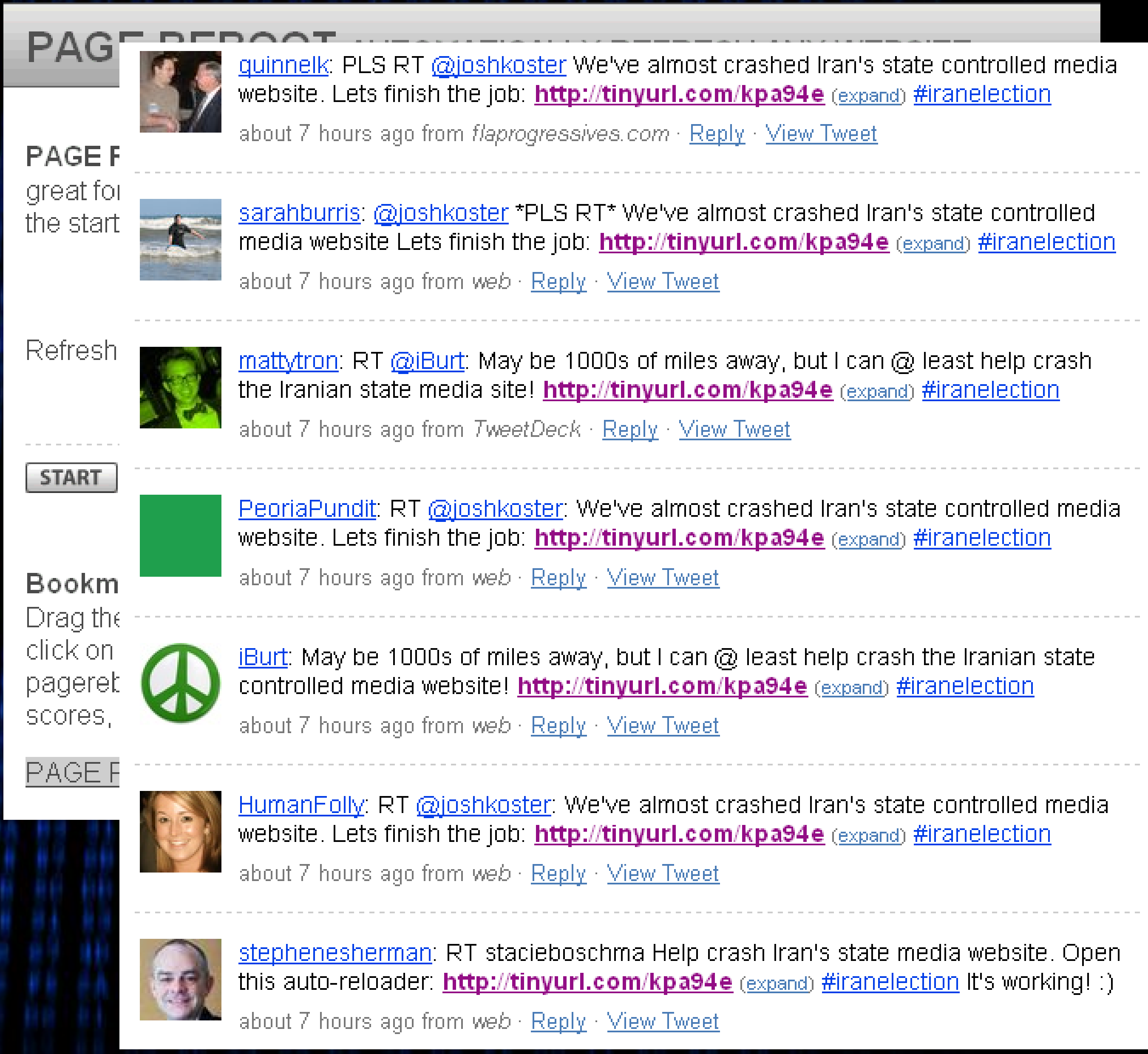




RIGGING INDICATORS	DID IT HAPPEN IN IRAN?
IMPOSSIBLE TALLIES The closest you can get to a smoking gun: vote tallies should be less than or equal to the number of eligible voters.	**YES:** After an investigation, Iran's senior panel of election monitors said Monday that in 50 cities, the number of votes cast exceeded the actual number of voters.
LOGICAL ANOMALIES Candidates fail to win (or to even do well) in their home districts, especially where their ethnicity should help.	**YES:** Mir Hossein Mousavi, an Azeri, lost East Azerbaijan. Mehdi Karrubi won 5 percent of his home district, a 10th of his 2005 result.
A BREAK WITH POLLS Election returns are wildly inconsistent with recent reliable, thorough polling data, assuming it exists.	**NO:** One poll put Mahmoud Ahmadinejad up 2-1. But that was pre-debates, and most respondents refused to say who they'd vote for.
REVERSALS OF FORTUNE Compared with a recent earlier contest, parties and candidates experience a big swing in popularity.	**YES:** Despite economic woes, reformists did more poorly than in 2005. And Ahmadinejad won in previously hostile Tehran Province.
FISHY DIGITS Fair vote tallies have a reliably even distribution of digits. Phony numbers made by humans do not.	**UNCLEAR:** Statisticians need precinct-level data to run their models, and Iran's rulers are unlikely to release that information.
LATE COMEBACKS If results are released on a rolling basis, you can tell if a panicked party starts stuffing ballot boxes.	**UNCLEAR:** Again, not enough data. If Iran's rulers rigged the vote, they did it right at the start of announced returns.
HASTY VERDICTS When voting is electronic, results come fast. But with paper ballots, a speedy victor is suspicious.	**YES:** The Interior Ministry declared victory for Ahmadinejad two hours after polls closed; results were authorized immediately.

International Protesters D/DoS

- Twitter is important
- Create auto web-page re-loader
- Add a dose of social outrage
- DoS turns into DDoS pretty quickly



quinnelk: PLS RT @joshkoster We've almost crashed Iran's state controlled media website. Lets finish the job: http://tinyurl.com/kpa94e (expand) #iranelection
about 7 hours ago from flaprogressives.com · Reply · View Tweet

sarahburris: @joshkoster *PLS RT* We've almost crashed Iran's state controlled media website Lets finish the job: http://tinyurl.com/kpa94e (expand) #iranelection
about 7 hours ago from web · Reply · View Tweet

mattytron: RT @iBurt: May be 1000s of miles away, but I can @ least help crash the Iranian state media site! http://tinyurl.com/kpa94e (expand) #iranelection
about 7 hours ago from TweetDeck · Reply · View Tweet

PeoriaPundit: RT @joshkoster: We've almost crashed Iran's state controlled media website. Lets finish the job: http://tinyurl.com/kpa94e (expand) #iranelection
about 7 hours ago from web · Reply · View Tweet

iBurt: May be 1000s of miles away, but I can @ least help crash the Iranian state controlled media website! http://tinyurl.com/kpa94e (expand) #iranelection
about 7 hours ago from web · Reply · View Tweet

HumanFolly: RT @joshkoster: We've almost crashed Iran's state controlled media website. Lets finish the job: http://tinyurl.com/kpa94e (expand) #iranelection
about 7 hours ago from web · Reply · View Tweet

stephenesherman: RT stacieboschma Help crash Iran's state media website. Open this auto-reloader: http://tinyurl.com/kpa94e (expand) #iranelection It's working! :)
about 7 hours ago from web · Reply · View Tweet

Meanwhile… in the land of the ever cute Slowloris

- Low bandwidth
- Keeps sockets alive
- Only affects certain web servers
- Doesn’t work through load balancers
- Managed to work around accf_http

Apache's Response

"DoS attacks by tying up TCP connections are expected. Please see:

http://httpd.apache.org/docs/trunk/misc/security_tips.html#dos

Regards, Joe"

- They've known about it for years…
- So I decide to release Slowloris in a few days' time when I have a chance to clean up the code… Meanwhile…

Anonymous

Hello, leaders of Iran. We are Anonymous.

As the eyes of the entire world hold you under close scrutiny, the eyes of the internet have taken a similar notice of your recent actions. While the governments of the world condemn you for your suppression of human rights, Anonymous has taken a particular interest in your recent attempts to censor the internet, not only for your own people, but for the citizens of the entire world.

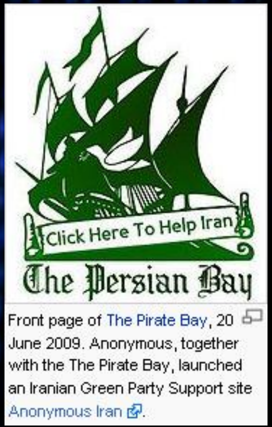
Such suppression of dissent cannot go unpunished. By cutting off communication of the Iranian citizens to the rest of the world, you have made it clear to us that the most revered of human rights - the right to free speech - is no longer important to you. By seeking to silence the voice of the people in an election and subsequently seeking to silence criticism of such a gross cover-up, you have perpetuated the anger and rage of your people. Anonymous has therefore made it our mission to see to it that the voice of the Iranian people can be heard around the world.

Just like another authoritarian religious extremist group, Anonymous will tear down the walls of silence using only the truth - the truth that you are trying so hard to suppress by use of violence, intimidation, and fascist laws.

As your people continue to riot and to speak out against you; as you continue to beat and shoot your own citizens in the street; as you continue to lie to the face of the entire world; know that the internet is watching - and we do not like what we see.

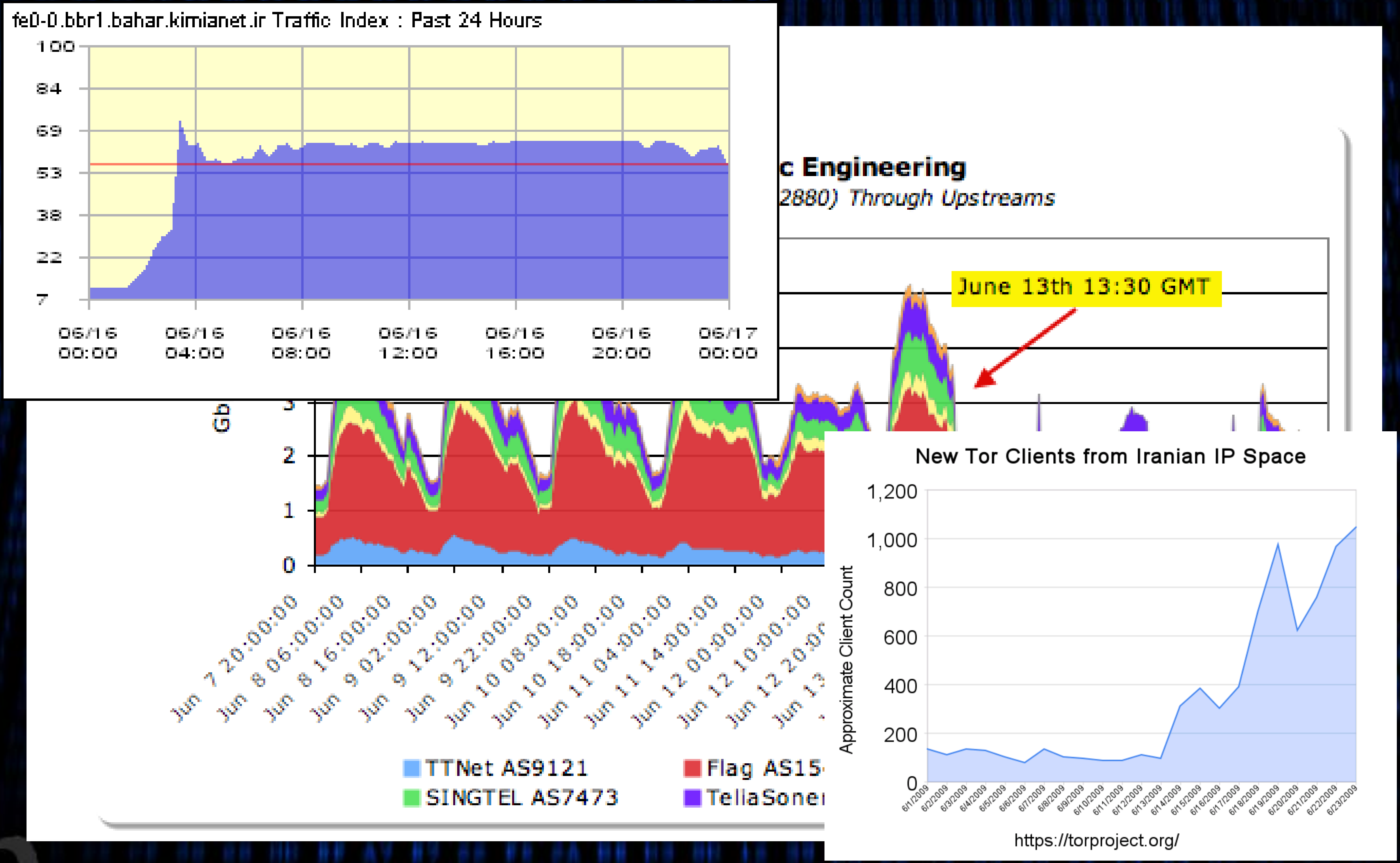
Knowledge is free.

We are Anonymous.
We are Legion.
We do not forgive.
We do not forget.



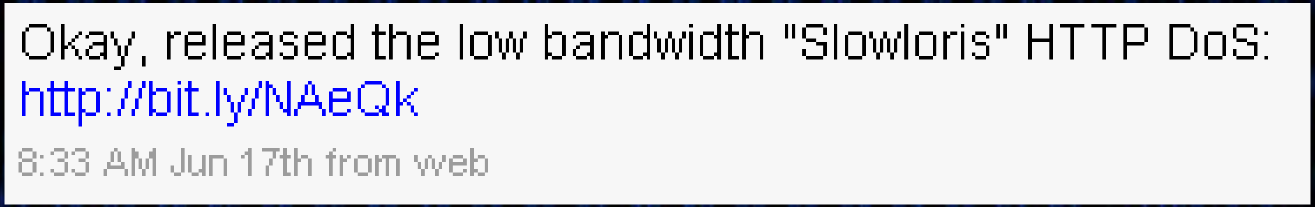
Front page of The Pirate Bay, 20 June 2009. Anonymous, together with the The Pirate Bay, launched an Iranian Green Party Support site Anonymous Iran.

DDoS Increases Against Iran



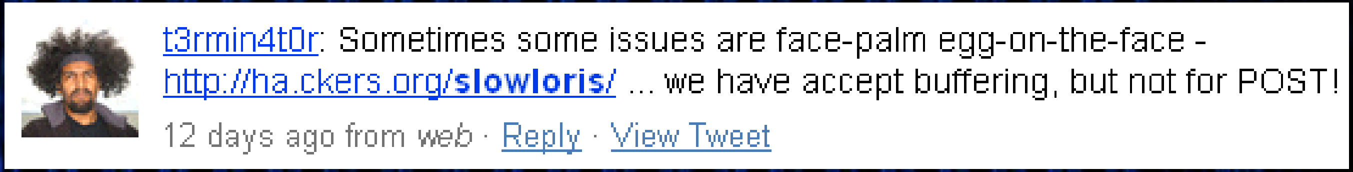
Unwitingly, I Release Slowloris

- I release it on my blog and on Twitter
- Expecting little to no attention
- For the first few hours things were pretty quiet…



Okay, released the low bandwidth "Slowloris" HTTP DoS: http://bit.ly/NAeQk

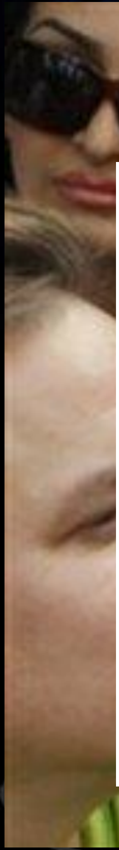
8:33 AM Jun 17th from web

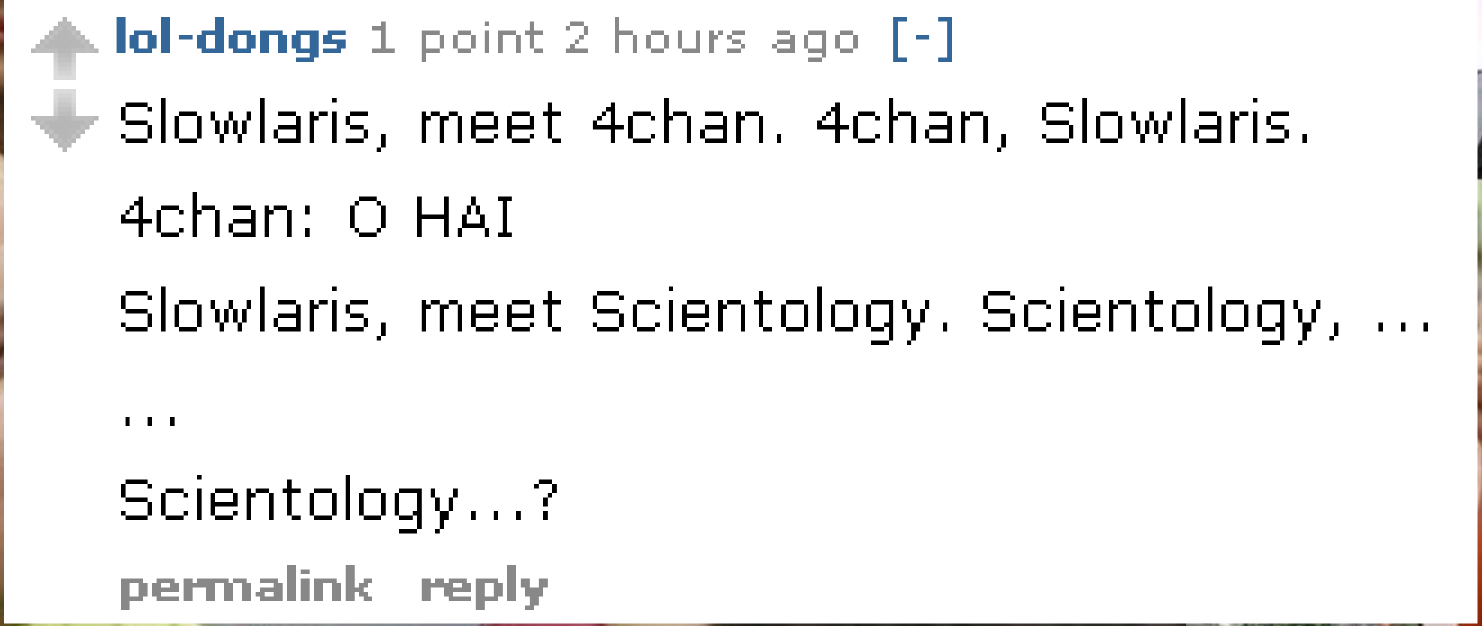


t3rmin4t0r: Sometimes some issues are face-palm egg-on-the-face - http://ha.ckers.org/**slowloris/** ... we have accept buffering, but not for POST!

12 days ago from *web* · Reply · View Tweet

Slowloris and Iran Elections Flare at the Same Time





lol-dongs 1 point 2 hours ago [-]

Slowlaris, meet 4chan. 4chan, Slowlaris.

4chan: O HAI

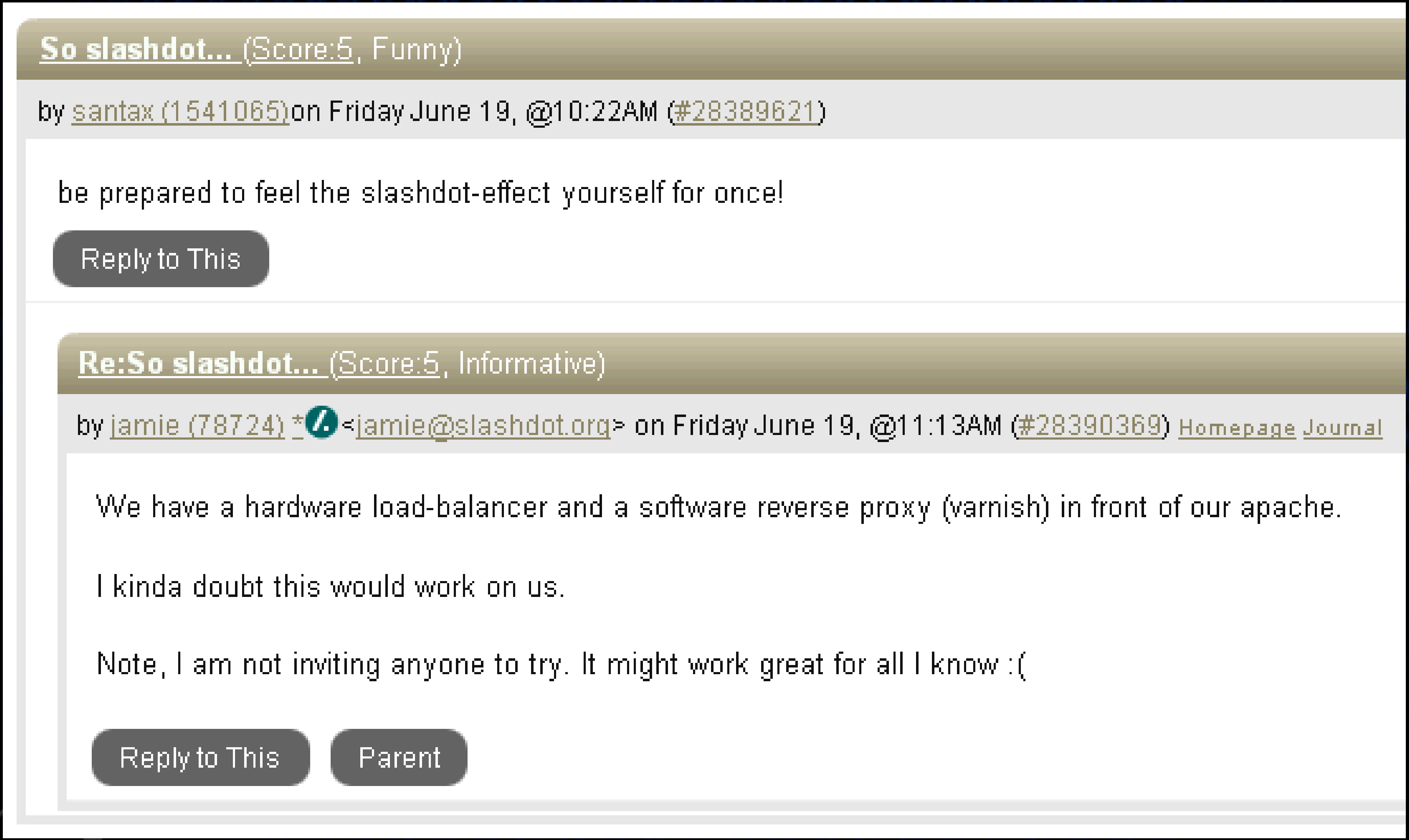
Slowlaris, meet Scientology. Scientology, ...

...

Scientology...?

permalink reply

Slashdot /.



So slashdot... (Score:5, Funny)

by santax (1541065)on Friday June 19, @10:22AM (#28389621)

be prepared to feel the slashdot-effect yourself for once!

Re:So slashdot... (Score:5, Informative)

by jamie (78724) * <jamie@slashdot.org> on Friday June 19, @11:13AM (#28390369) Homepage Journal

We have a hardware load-balancer and a software reverse proxy (varnish) in front of our apache.

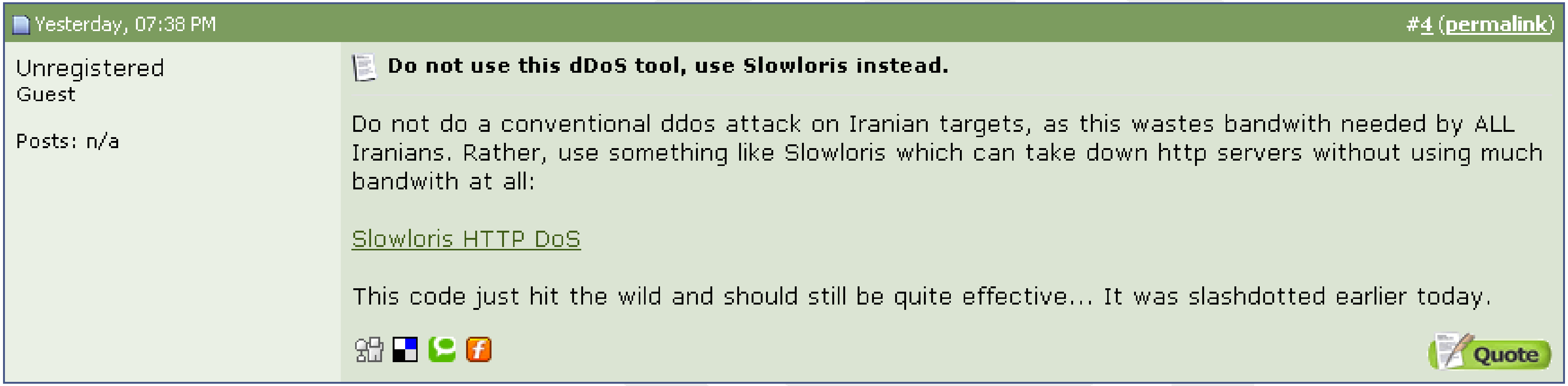
I kinda doubt this would work on us.

Note, I am not inviting anyone to try. It might work great for all I know :(

Don’t Kill All of Iran – Just The Government Websites

Anonymous Iran

From http://iran.whyweprotest.net/



Yesterday, 07:38 PM — #4 (permalink)

Unregistered
Guest

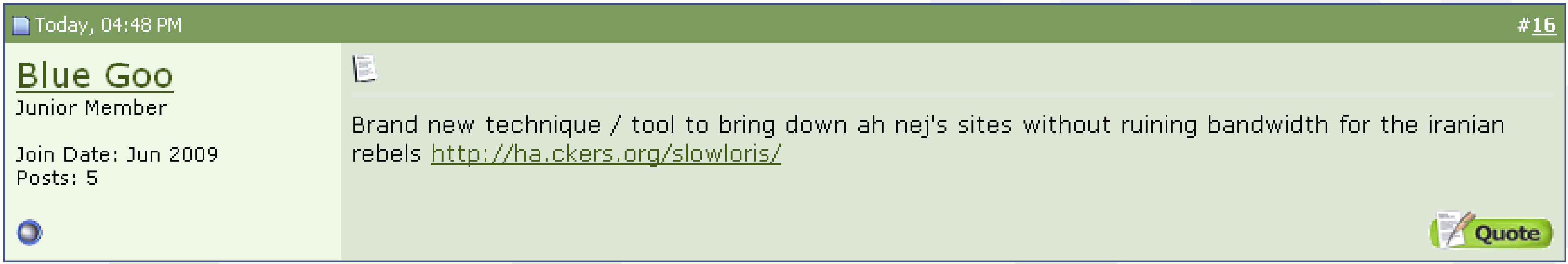
Posts: n/a

Do not use this dDoS tool, use Slowloris instead.

Do not do a conventional ddos attack on Iranian targets, as this wastes bandwith needed by ALL Iranians. Rather, use something like Slowloris which can take down http servers without using much bandwith at all:

Slowloris HTTP DoS

This code just hit the wild and should still be quite effective... It was slashdotted earlier today.



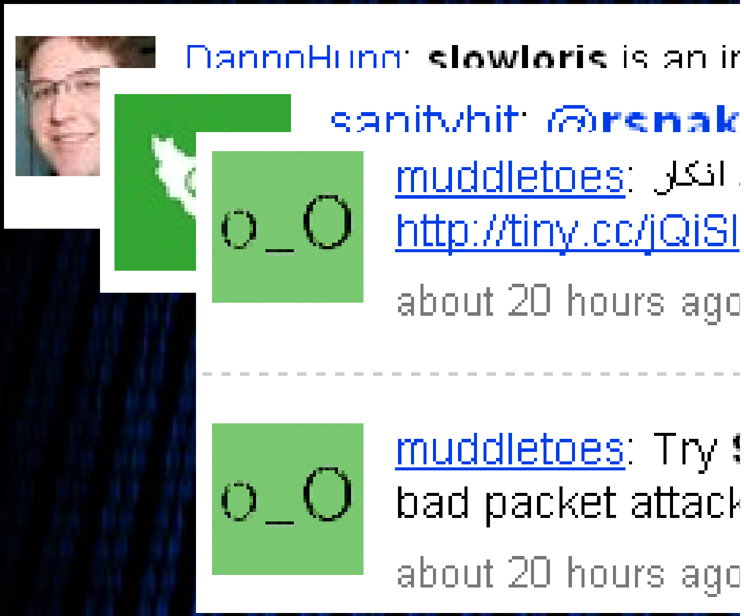
Today, 04:48 PM — #16

Blue Goo
Junior Member

Join Date: Jun 2009
Posts: 5

Brand new technique / tool to bring down ah nej's sites without ruining bandwidth for the iranian rebels http://ha.ckers.org/slowloris/

Twitter Explosion



DannoHung: **slowloris** is an ir

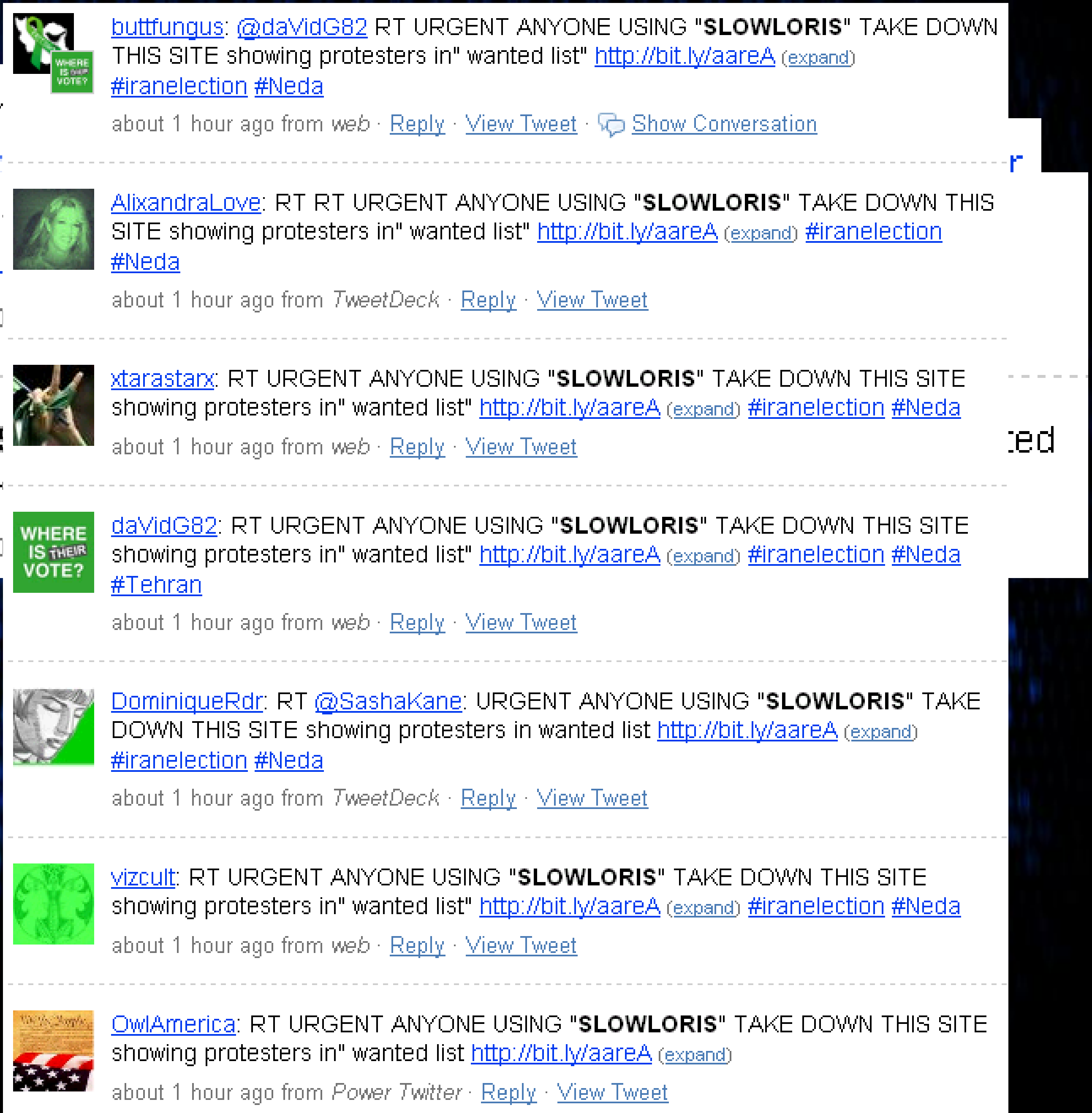
sanitybit: @rsnak

muddletoes: انكل
http://tiny.cc/jQiSl

about 20 hours ago

muddletoes: Try
bad packet attack

about 20 hours ago



buttfungus: @daVidG82 RT URGENT ANYONE USING "**SLOWLORIS**" TAKE DOWN THIS SITE showing protesters in" wanted list" http://bit.ly/aareA (expand) #iranelection #Neda

about 1 hour ago from *web* · Reply · View Tweet · Show Conversation

AlixandraLove: RT RT URGENT ANYONE USING "**SLOWLORIS**" TAKE DOWN THIS SITE showing protesters in" wanted list" http://bit.ly/aareA (expand) #iranelection #Neda

about 1 hour ago from *TweetDeck* · Reply · View Tweet

xtarastarx: RT URGENT ANYONE USING "**SLOWLORIS**" TAKE DOWN THIS SITE showing protesters in" wanted list" http://bit.ly/aareA (expand) #iranelection #Neda

about 1 hour ago from *web* · Reply · View Tweet

daVidG82: RT URGENT ANYONE USING "**SLOWLORIS**" TAKE DOWN THIS SITE showing protesters in" wanted list" http://bit.ly/aareA (expand) #iranelection #Neda #Tehran

about 1 hour ago from *web* · Reply · View Tweet

DominiqueRdr: RT @SashaKane: URGENT ANYONE USING "**SLOWLORIS**" TAKE DOWN THIS SITE showing protesters in wanted list http://bit.ly/aareA (expand) #iranelection #Neda

about 1 hour ago from *TweetDeck* · Reply · View Tweet

vizcult: RT URGENT ANYONE USING "**SLOWLORIS**" TAKE DOWN THIS SITE showing protesters in" wanted list" http://bit.ly/aareA (expand) #iranelection #Neda

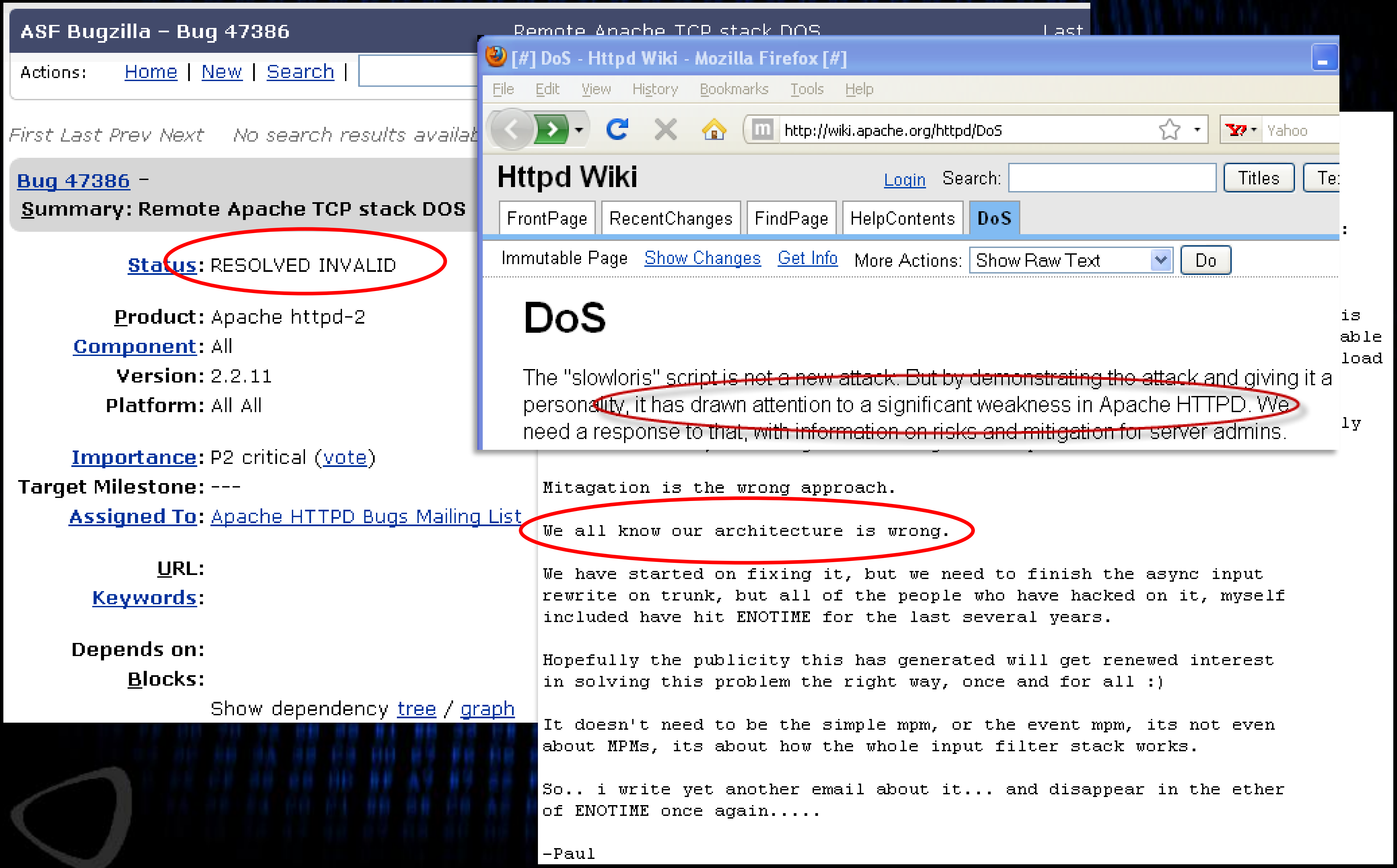
about 1 hour ago from *web* · Reply · View Tweet

OwlAmerica: RT URGENT ANYONE USING "**SLOWLORIS**" TAKE DOWN THIS SITE showing protesters in" wanted list http://bit.ly/aareA (expand)

about 1 hour ago from *Power Twitter* · Reply · View Tweet

- 42 pages later… slowloris is de-facto turned into a DDoS tool

Oh Apache… *sigh*



ASF Bugzilla – Bug 47386
Remote Apache TCP stack DOS
Last
Actions: Home | New | Search |
First Last Prev Next
No search results availab

Bug 47386 –
Summary: Remote Apache TCP stack DOS

Status: RESOLVED INVALID

Product: Apache httpd-2
Component: All
Version: 2.2.11
Platform: All All

Importance: P2 critical (vote)
Target Milestone: ---
Assigned To: Apache HTTPD Bugs Mailing List

URL:
Keywords:

Depends on:
Blocks:
Show dependency tree / graph

[#] DoS - Httpd Wiki - Mozilla Firefox [#]
File Edit View History Bookmarks Tools Help
http://wiki.apache.org/httpd/DoS
Yahoo
Httpd Wiki
Login
Search:
Titles
Te
FrontPage
RecentChanges
FindPage
HelpContents
DoS
Immutable Page
Show Changes
Get Info
More Actions:
Show Raw Text
Do

DoS

The "slowloris" script is not a new attack. But by demonstrating the attack and giving it a personality, it has drawn attention to a significant weakness in Apache HTTPD. We need a response to that, with information on risks and mitigation for server admins.

```
Mitagation is the wrong approach.

We all know our architecture is wrong.

We have started on fixing it, but we need to finish the async input
rewrite on trunk, but all of the people who have hacked on it, myself
included have hit ENOTIME for the last several years.

Hopefully the publicity this has generated will get renewed interest
in solving this problem the right way, once and for all :)

It doesn't need to be the simple mpm, or the event mpm, its not even
about MPMs, its about how the whole input filter stack works.

So.. i write yet another email about it... and disappear in the ether
of ENOTIME once again.....

-Paul
```

شماره 49

شماره 50

شماره 51

شماره 52

شماره 53

شماره 54

شماره 55

شماره 56

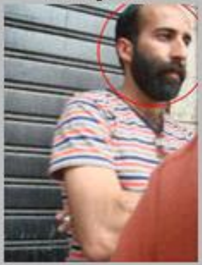
شماره 57

شماره 58

شماره 59

شماره 60

شماره 61

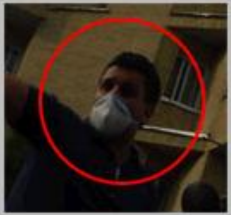

شماره 62

شماره 63

شماره 64

شماره 65

شماره 66


شماره 67

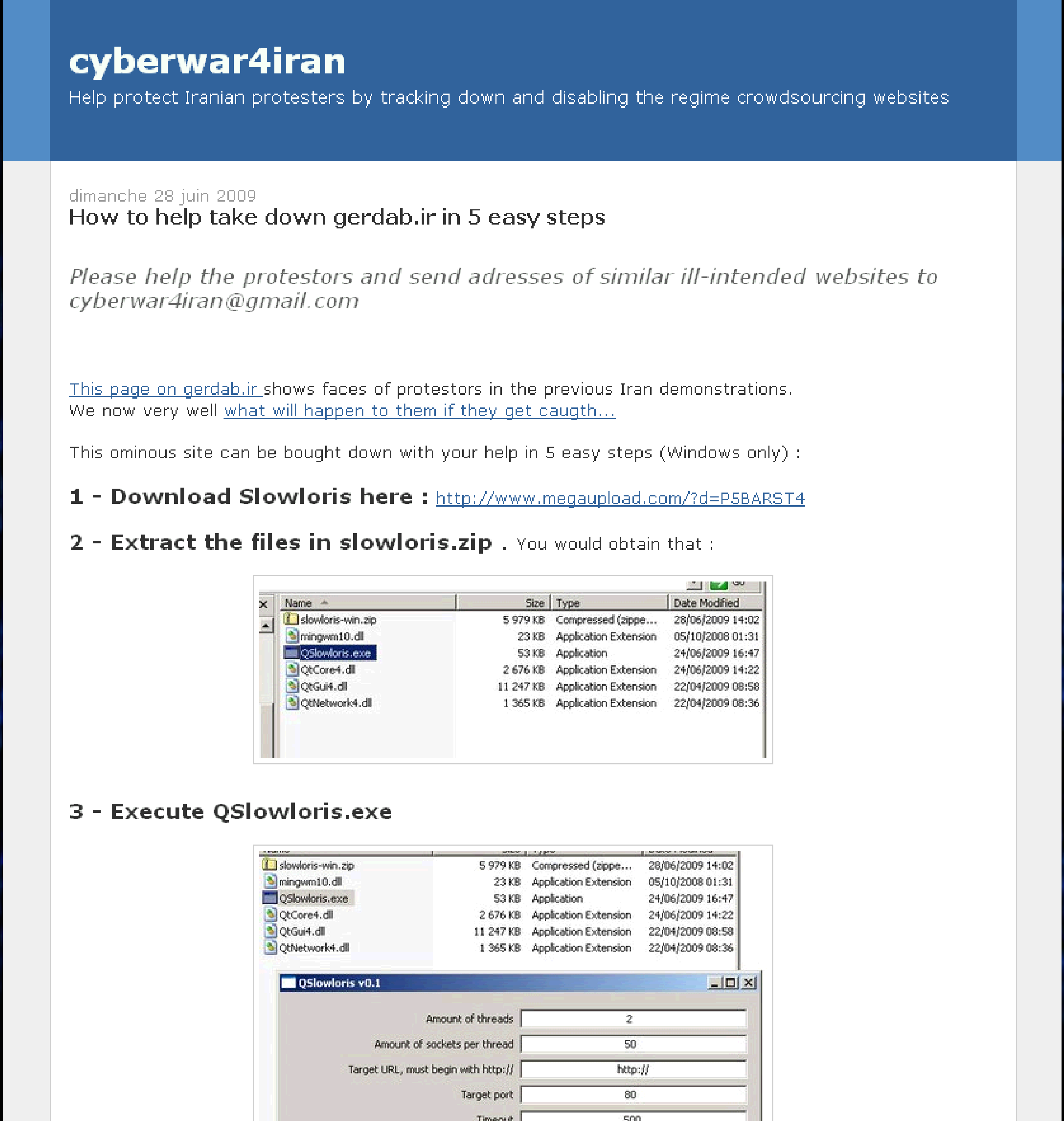
شماره 68

شماره 69

شماره 70

شماره 71

شماره 72



cyberwar4iran

Help protect Iranian protesters by tracking down and disabling the regime crowdsourcing websites

dimanche 28 juin 2009

How to help take down gerdab.ir in 5 easy steps

Please help the protestors and send adresses of similar ill-intended websites to cyberwar4iran@gmail.com

This page on gerdab.ir shows faces of protestors in the previous Iran demonstrations.
We now very well what will happen to them if they get caugth...

This ominous site can be bought down with your help in 5 easy steps (Windows only) :

1 - Download Slowloris here : http://www.megaupload.com/?d=P5BARST4

2 - Extract the files in slowloris.zip . You would obtain that :

Name	Size	Type	Date Modified
slowloris-win.zip	5 979 KB	Compressed (zippe...	28/06/2009 14:02
mingwm10.dll	23 KB	Application Extension	05/10/2008 01:31
QSlowloris.exe	53 KB	Application	24/06/2009 16:47
QtCore4.dll	2 676 KB	Application Extension	24/06/2009 14:22
QtGui4.dll	11 247 KB	Application Extension	22/04/2009 08:58
QtNetwork4.dll	1 365 KB	Application Extension	22/04/2009 08:36

3 - Execute QSlowloris.exe

slowloris-win.zip	5 979 KB	Compressed (zippe...	28/06/2009 14:02
mingwm10.dll	23 KB	Application Extension	05/10/2008 01:31
QSlowloris.exe	53 KB	Application	24/06/2009 16:47
QtCore4.dll	2 676 KB	Application Extension	24/06/2009 14:22
QtGui4.dll	11 247 KB	Application Extension	22/04/2009 08:58
QtNetwork4.dll	1 365 KB	Application Extension	22/04/2009 08:36

QSlowloris v0.1

Amount of threads: 2

Amount of sockets per thread: 50

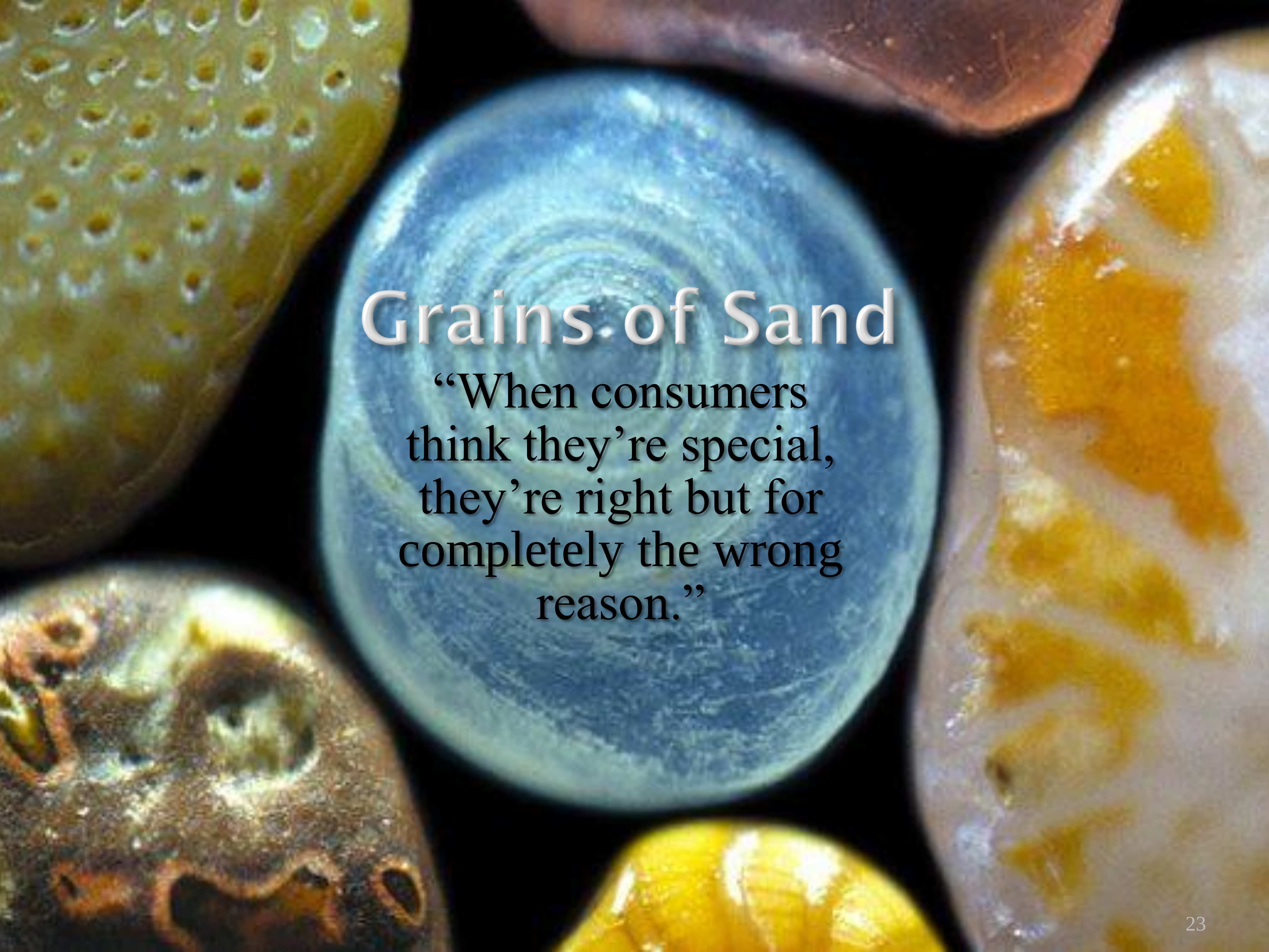
Target URL, must begin with http://: http://

Target port: 80

Timeout: 500

3rd Party Implementations

- PyLoris
  - http://motomastyle.com/pyloris-a-python-implementation-of-slowloris/
- PHP version:
  - http://seclists.org/fulldisclosure/2009/Jun/0207.html
- Questionable EXE version
  - http://cyberwar4iran.blogspot.com/
- "Slugsend"?



Grains of Sand

“When consumers think they’re special, they’re right but for completely the wrong reason.”

Passwords

- 100 embassy passwords
- 50% password re-use between social networking and web-mail (est. by phishers).
- Password management is not a solved problem for consumers.
- Single factor.

Kazakhstan Embassy in Egypt 213.131.64.229 kazaemb piramid

Mongolian Embassy in USA 209.213.221.249 n.tumenbayar@mongolianembassy.us temp

UK Visa Application Centre in Nepal 208.109.119.54 vfsuknepal@vfs-uk-np.com Password

Defense Research & Development Organization Govt. Of India, Ministry of Defense jpsingh@drdo.com password+1

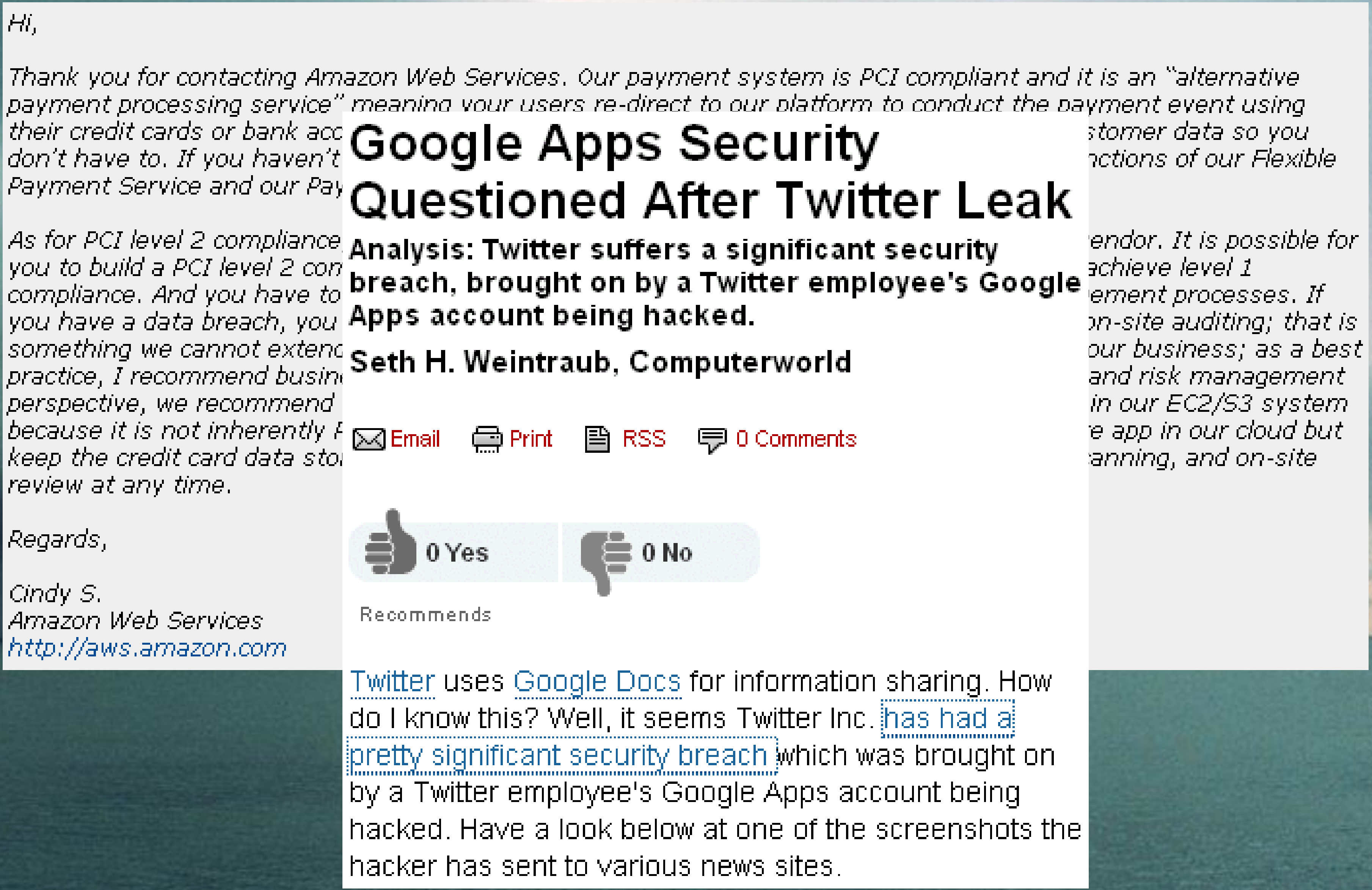
Indian Embassy in USA amb@indianembassy.org 1234

Iran Embassy in Ghana 217.172.99.19 iranemb_accra@mfa.gov.ir accra

Iran Embassy in Kenya 217.172.99.19 iranemb_kenya@mfa.gov.ir kenya

Hong Kong Liberal Party 202.123.79.164 miriamlau 123456

Clouds of Insecurity



Hi,

Thank you for contacting Amazon Web Services. Our payment system is PCI compliant and it is an "alternative
payment processing service" meaning your users re-direct to our platform to conduct the payment event using
their credit cards or bank acc
stomer data so you
don't have to. If you haven't
nctions of our Flexible
Payment Service and our Pay

As for PCI level 2 compliance
endor. It is possible for
you to build a PCI level 2 con
achieve level 1
compliance. And you have to
ement processes. If
you have a data breach, you
on-site auditing; that is
something we cannot extenc
our business; as a best
practice, I recommend busin
and risk management
perspective, we recommend
in our EC2/S3 system
because it is not inherently F
e app in our cloud but
keep the credit card data sto
anning, and on-site
review at any time.

Regards,

Cindy S.
Amazon Web Services
http://aws.amazon.com

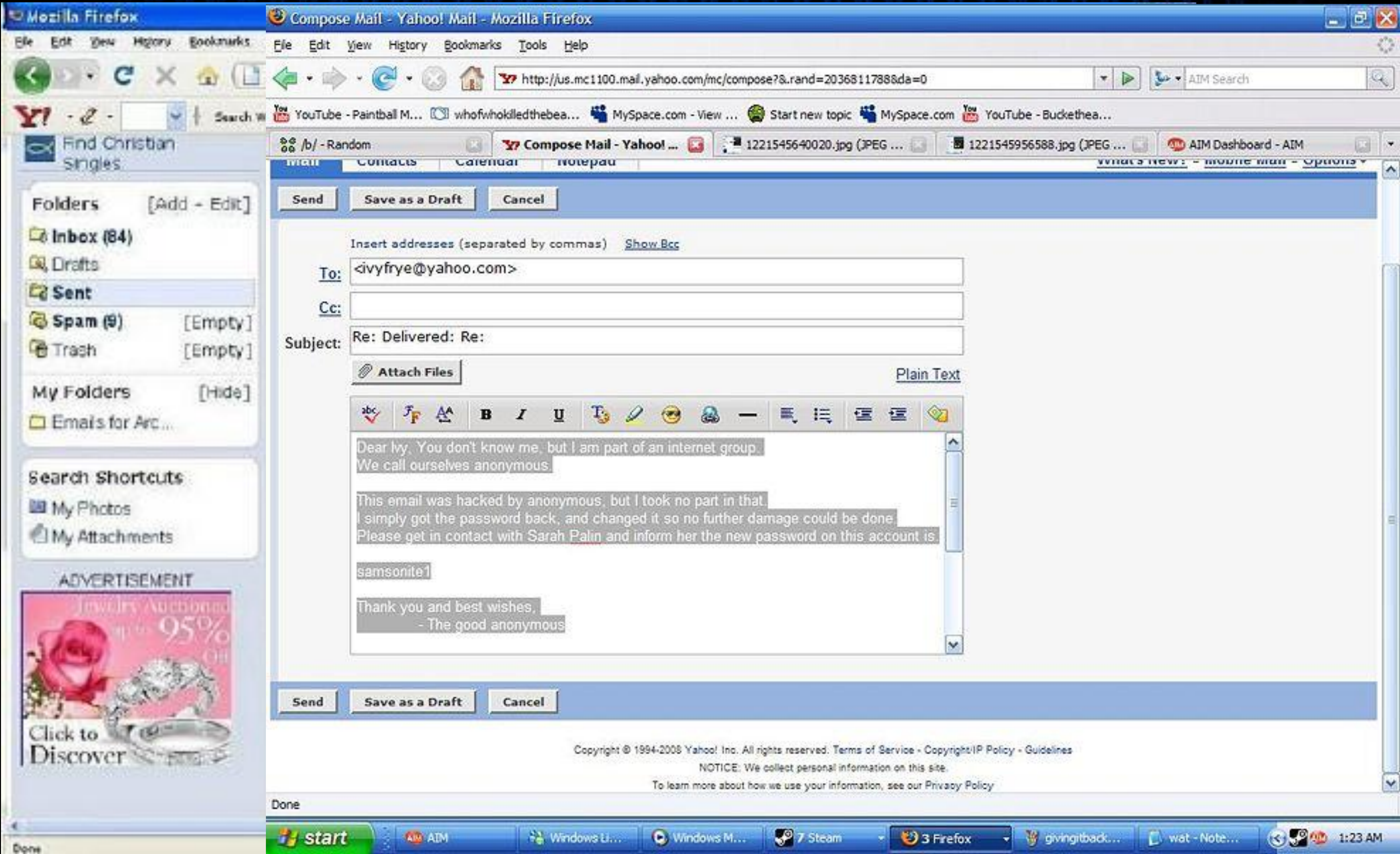
Google Apps Security Questioned After Twitter Leak

Analysis: Twitter suffers a significant security breach, brought on by a Twitter employee's Google Apps account being hacked.

Seth H. Weintraub, Computerworld

Twitter uses Google Docs for information sharing. How do I know this? Well, it seems Twitter Inc. has had a pretty significant security breach which was brought on by a Twitter employee's Google Apps account being hacked. Have a look below at one of the screenshots the hacker has sent to various news sites.

Sarah Palin


Mozilla Firefox
Compose Mail - Yahoo! Mail - Mozilla Firefox
File Edit View History Bookmarks Tools Help
http://us.mc1100.mail.yahoo.com/mc/compose?&.rand=2036811788&da=0
AIM Search
YouTube - Paintball M... whofwhokilledthebea... MySpace.com - View ... Start new topic MySpace.com YouTube - Buckethea...
/b/ - Random
Compose Mail - Yahoo! ...
1221545640020.jpg (JPEG ...
1221545956588.jpg (JPEG ...
AIM Dashboard - AIM
Find Christian Singles
Folders [Add - Edit]
Inbox (84)
Drafts
Sent
Spam (9) [Empty]
Trash [Empty]
My Folders [Hide]
Emails for Arc...
Search Shortcuts
My Photos
My Attachments
ADVERTISEMENT
Jewelry Auctioned up to 95% Off
Click to Discover
Mail Contacts Calendar Notepad
What's New? - Mobile Mail - Options
Send
Save as a Draft
Cancel
Insert addresses (separated by commas)
Show Bcc
Attach Files
Plain Text
Copyright © 1994-2008 Yahoo! Inc. All rights reserved. Terms of Service - Copyright/IP Policy - Guidelines
NOTICE: We collect personal information on this site.
To learn more about how we use your information, see our Privacy Policy
Done
start
AIM
Windows Li...
Windows M...
7 Steam
3 Firefox
givingitback...
wat - Note...
1:23 AM

To: <ivyfrye@yahoo.com>

Cc:

Subject: Re: Delivered: Re:

Dear Ivy, You don't know me, but I am part of an internet group.
We call ourselves anonymous.

This email was hacked by anonymous, but I took no part in that.
I simply got the password back, and changed it so no further damage could be done.
Please get in contact with Sarah Palin and inform her the new password on this account is:

samsonite1

Thank you and best wishes,
- The good anonymous

Future of Spamming

- Personas
  - Age
  - Demographic
  - Marital status
  - Interests
  - Zodiac
  - Birth date
  - Friends
  - Perfect weather
  - Locale
  - Etc…

Questions/Comments?

- Robert Hansen
  - Robert aT sectheory d0t c0m
  - http://www.sectheory.com/
  - http://ha.ckers.org/
  - TBD: Book – “Detecting Malice”
  - XSS Book: XSS Exploits and Defense
    - ISBN: 1597491543