SecTheory

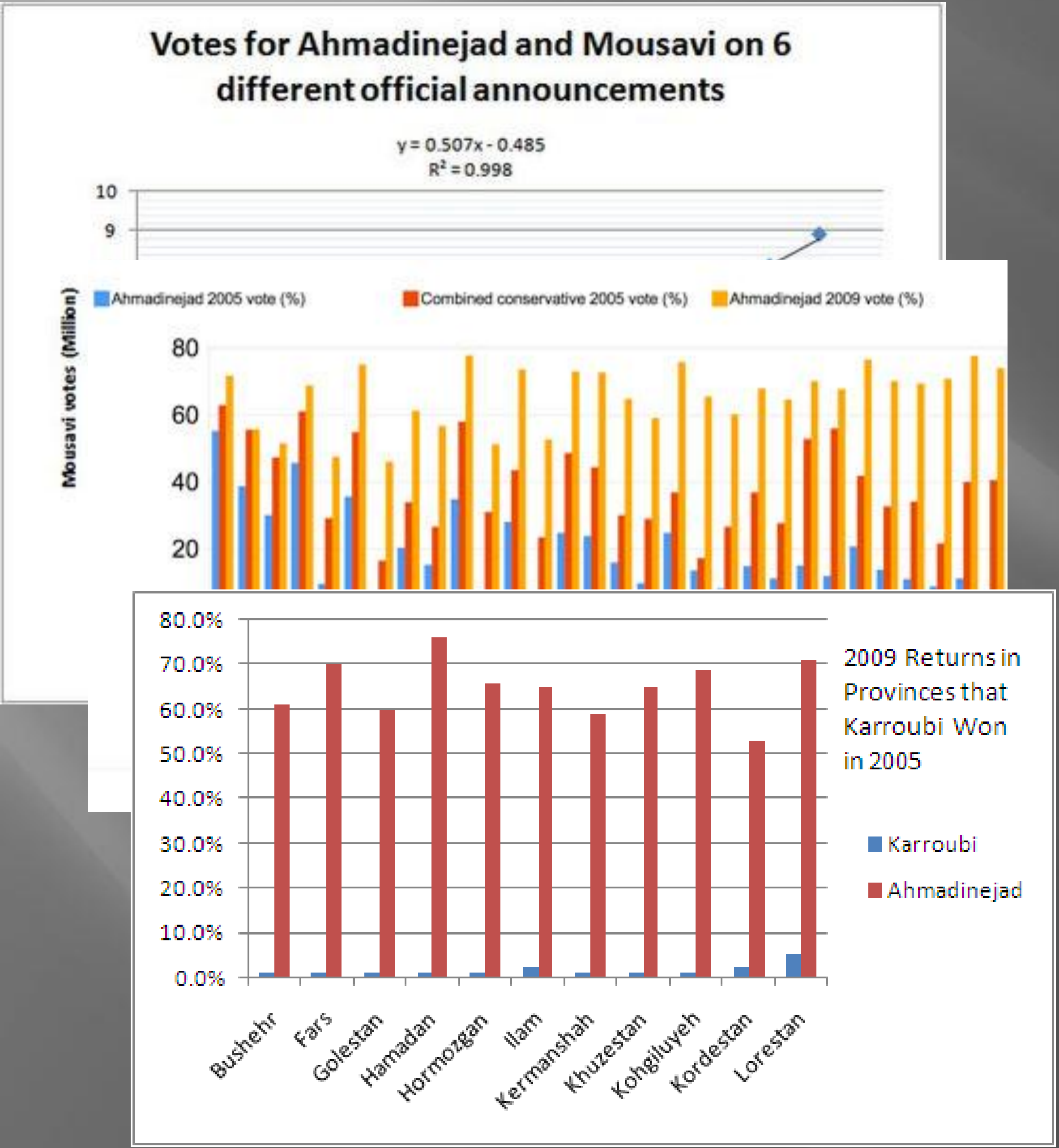
Internet Security

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

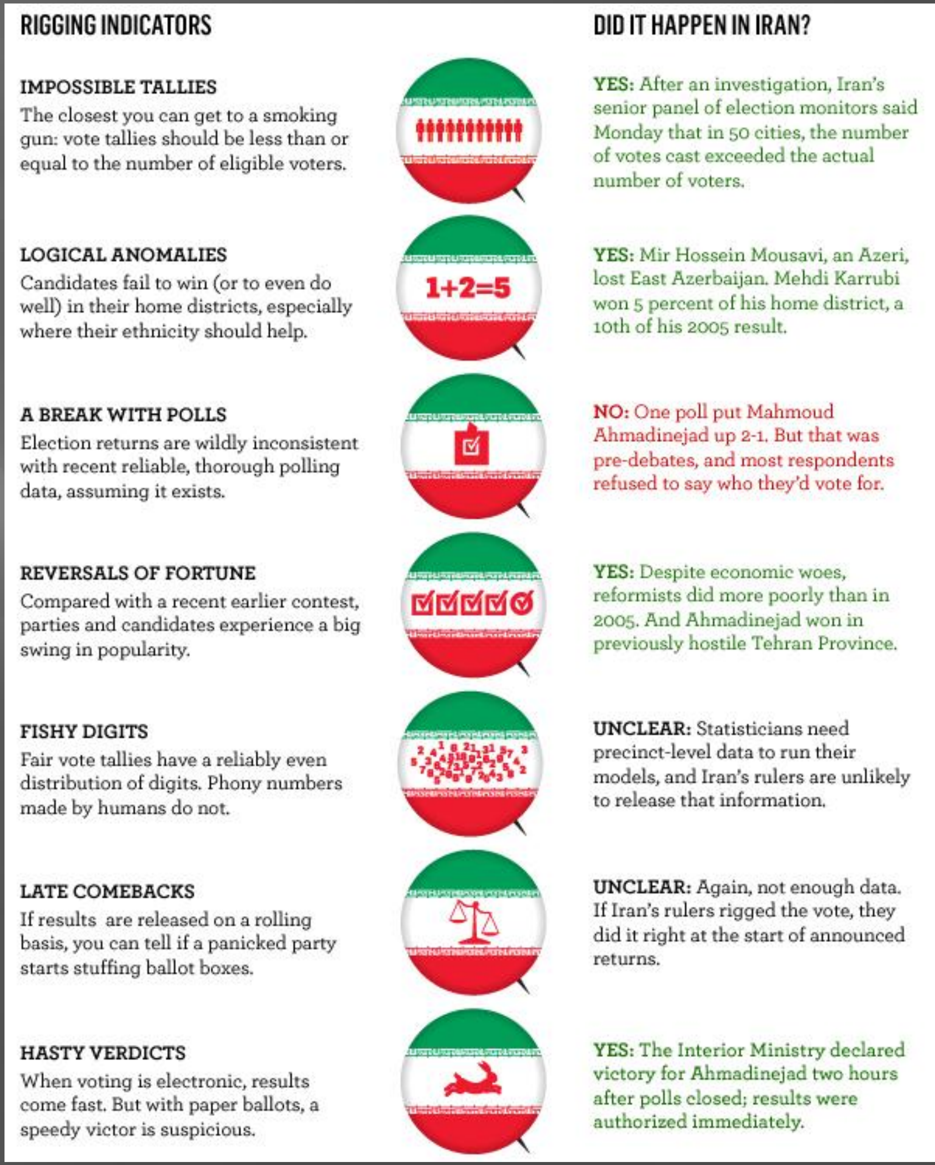
Iran in Turmoil

Voter Fraud



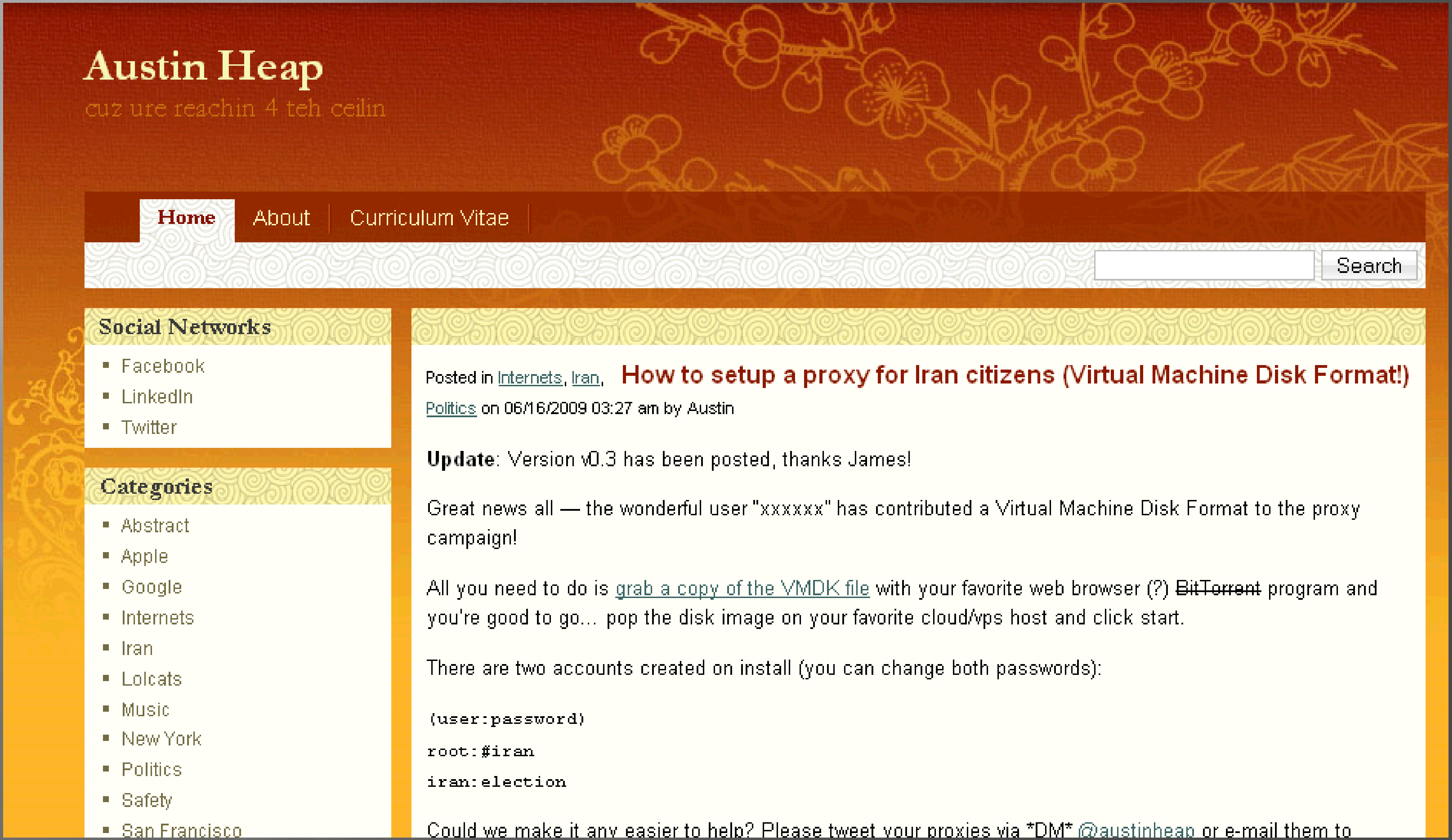
Votes for Ahmadinejad and Mousavi on 6 different official announcements

2009 Returns in Provinces that Karroubi Won in 2005



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.

Austin Heap + Twitter



Austin Heap

cuz ure reachin 4 teh ceilin

Social Networks

- Facebook
- LinkedIn
- Twitter

Categories

- Abstract
- Apple
- Google
- Internets
- Iran
- Lolcats
- Music
- New York
- Politics
- Safety
- San Francisco

How to setup a proxy for Iran citizens (Virtual Machine Disk Format!)

Posted in Internets, Iran, Politics on 06/16/2009 03:27 am by Austin

Update: Version v0.3 has been posted, thanks James!

Great news all — the wonderful user "xxxxxx" has contributed a Virtual Machine Disk Format to the proxy campaign!

All you need to do is grab a copy of the VMDK file with your favorite web browser (?) ~~BitTorrent~~ program and you're good to go… pop the disk image on your favorite cloud/vps host and click start.

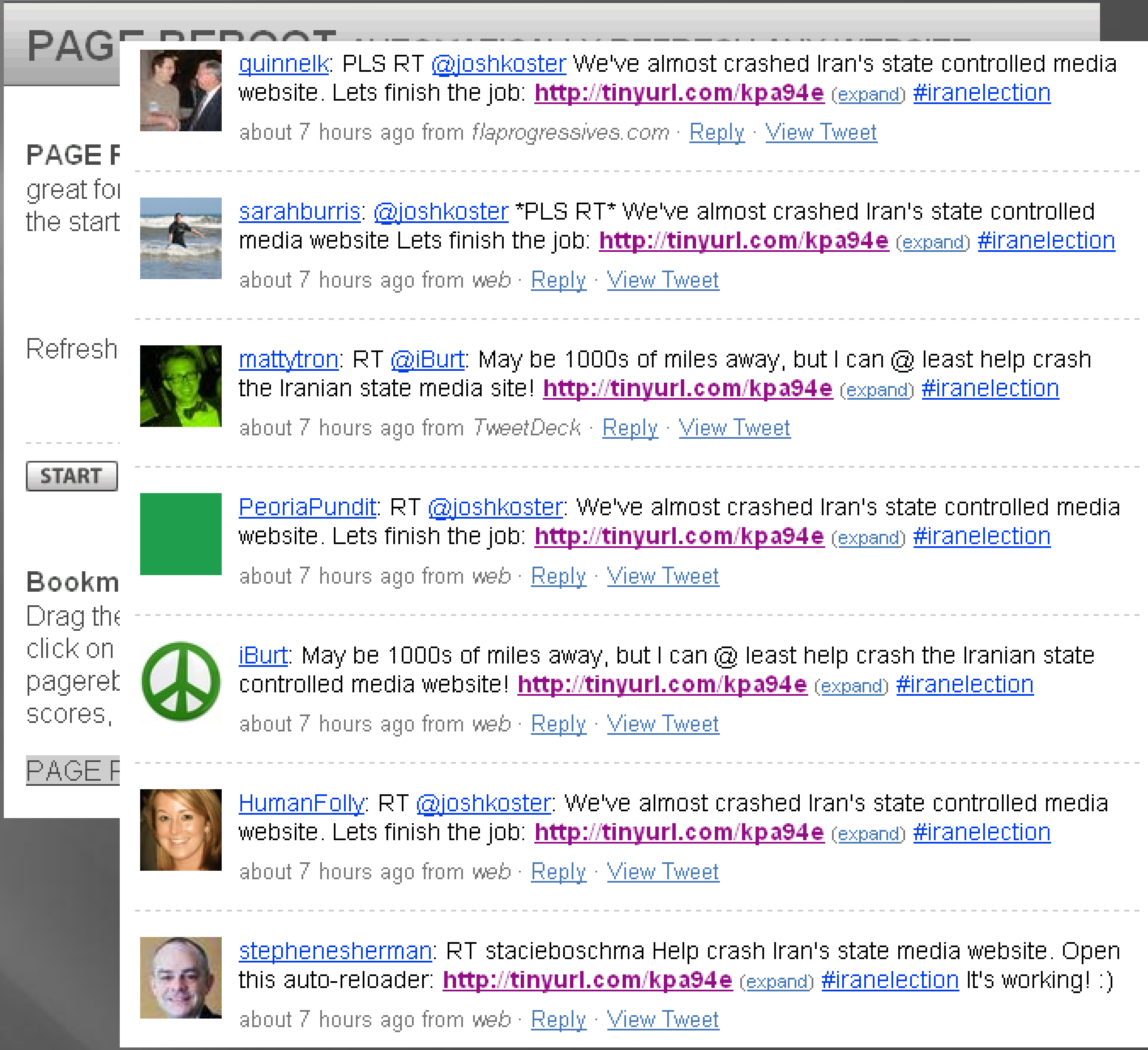
There are two accounts created on install (you can change both passwords):

```
(user:password)
root:#iran
iran:election
```

Could we make it any easier to help? Please tweet your proxies via *DM* @austinheap or e-mail them to

International Protesters D/DoS

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



PAGE REBOOT

PAGE F
great fo
the start

Refresh

START

Bookm
Drag the
click on
pageret
scores,

PAGE F

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

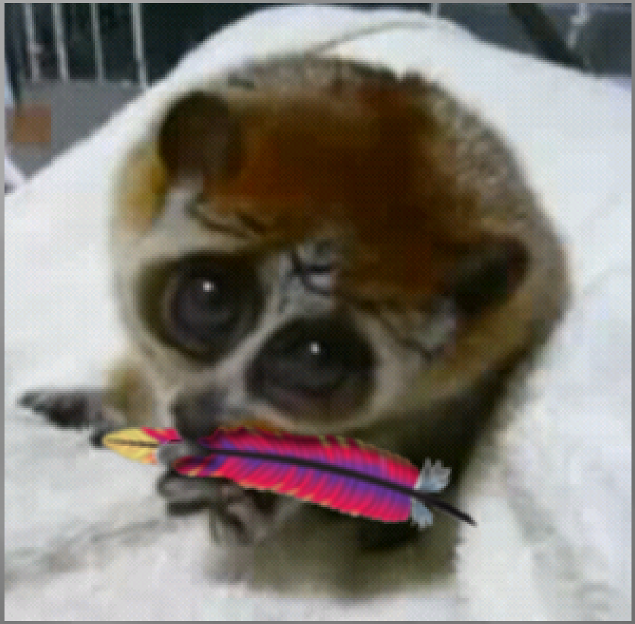
Slowloris

```
POST / HTTP/1.1\r\n
Host: spoofed.com\r\n
User-Agent:  Whatever\r\n
Content-Length: 42\r\n
X-a: b\r\n\r\n
```

Keeping Sessions Alive

```
GET / HTTP/1.1\r\n
Host: spoofed.com\r\n
User-Agent: Mozilla/4.0 …\r\n
Connection: Keep-Alive\r\n
Range: bytes=0-10\r\n
X-a: b\r\n\r\n
```

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.

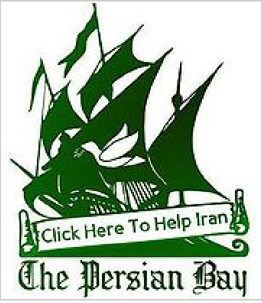
Such suppression of dissent cannot go unpunished. By cutting off communication of the Iranian citizens to the rest of the world, you have made it clear to us that the most revered of human rights - the right to free speech - is no longer important to you. By seeking to silence the voice of the people 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.

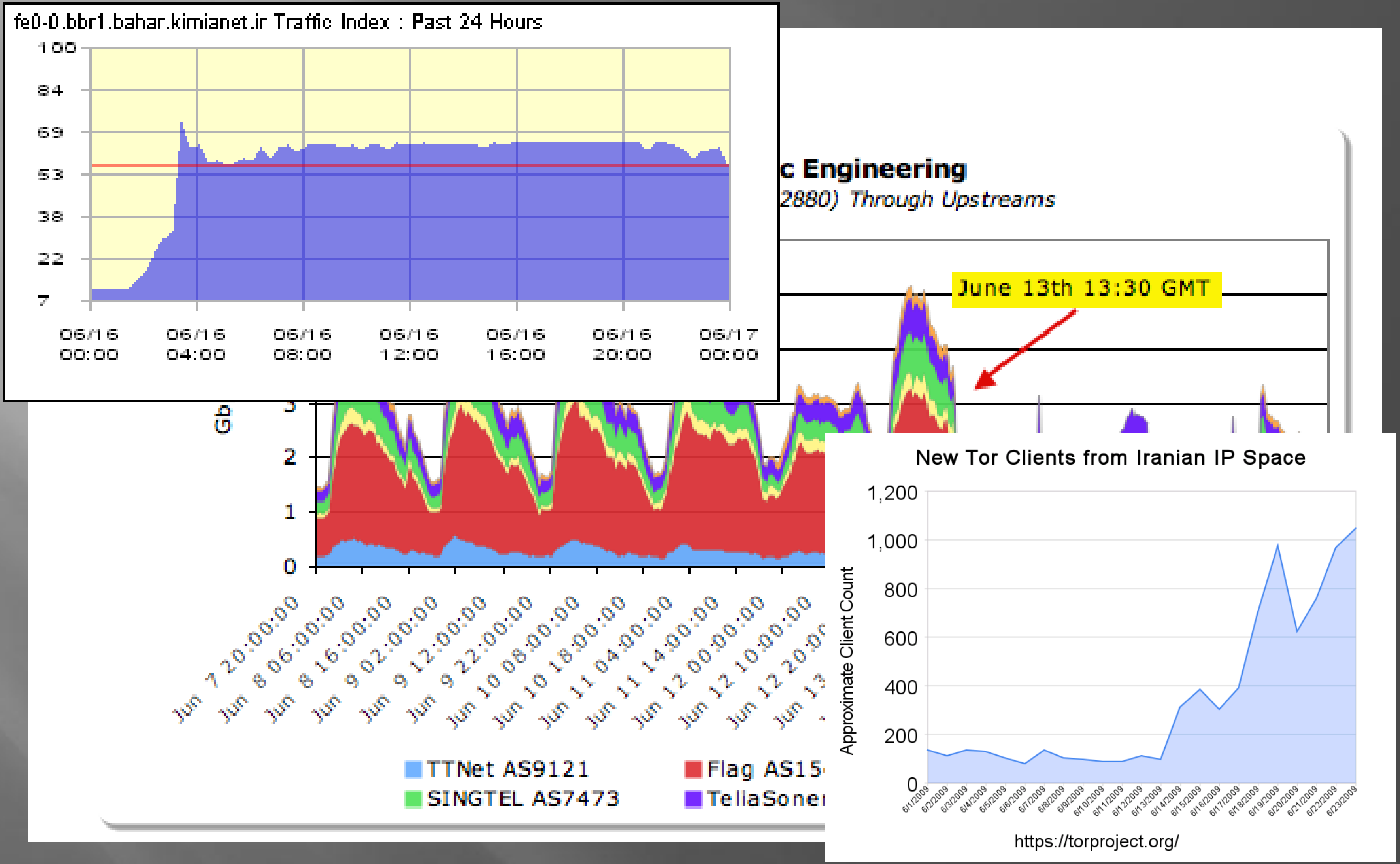
Knowledge is free.

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

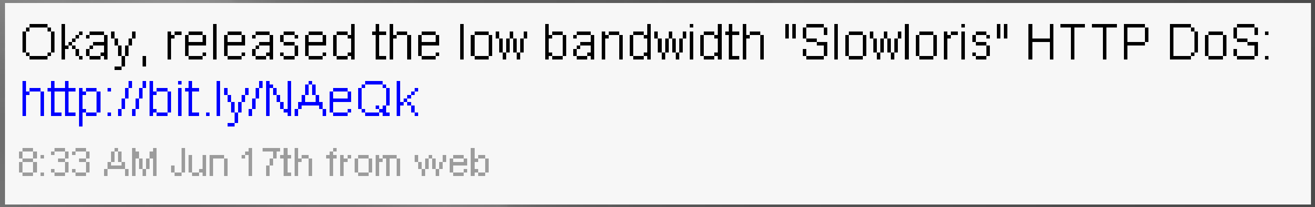


June 13th 13:30 GMT

https://torproject.org/

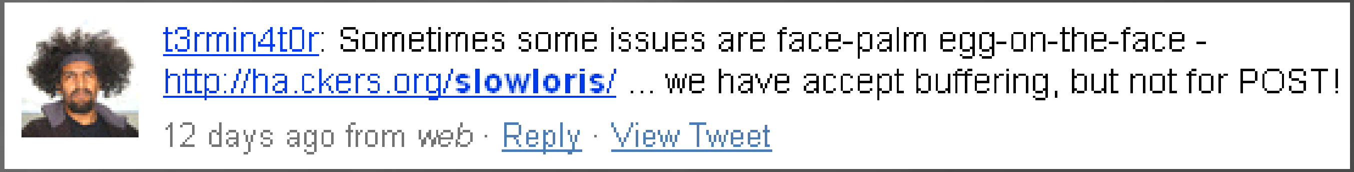
Unwitingly, I Release Slowloris

- 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

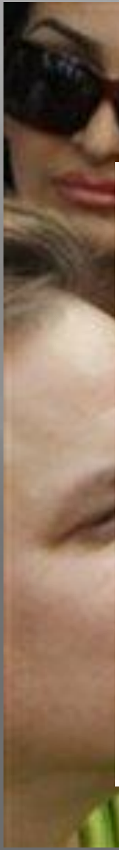
8:33 AM Jun 17th from web

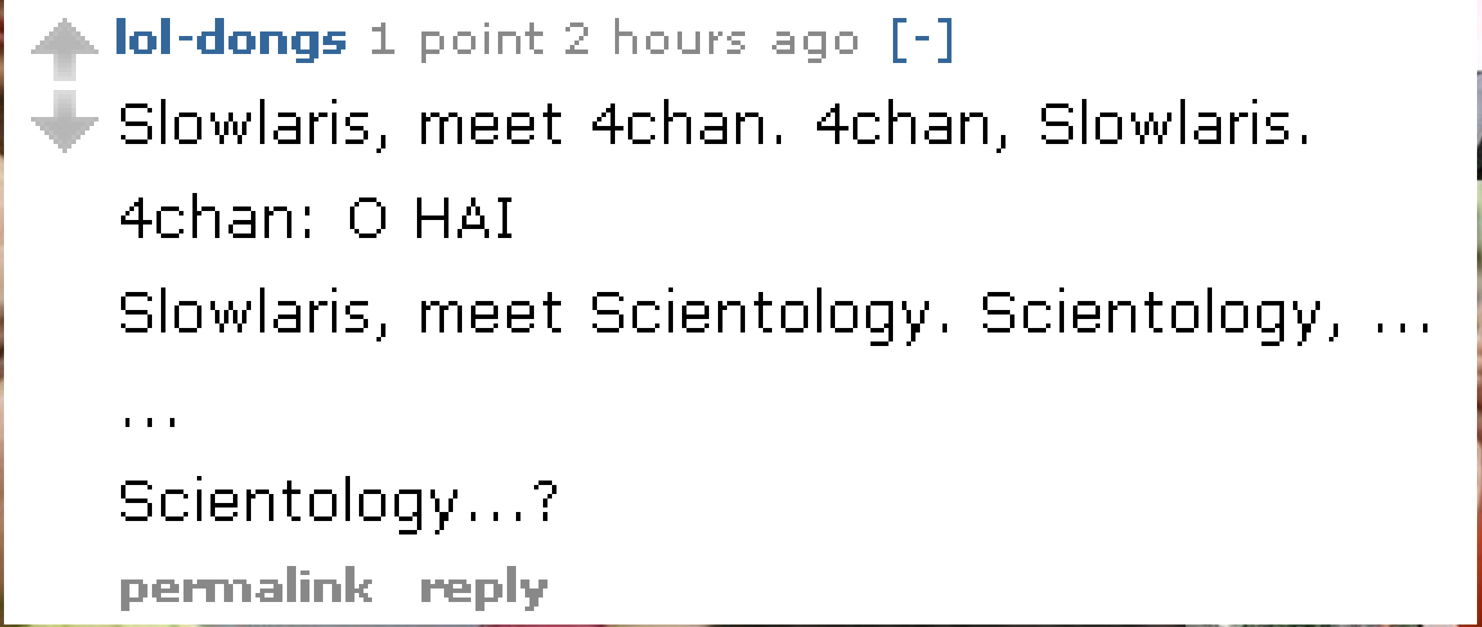


t3rmin4t0r: Sometimes some issues are face-palm egg-on-the-face - http://ha.ckers.org/**slowloris**/ ... we have accept buffering, but not for POST!

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.

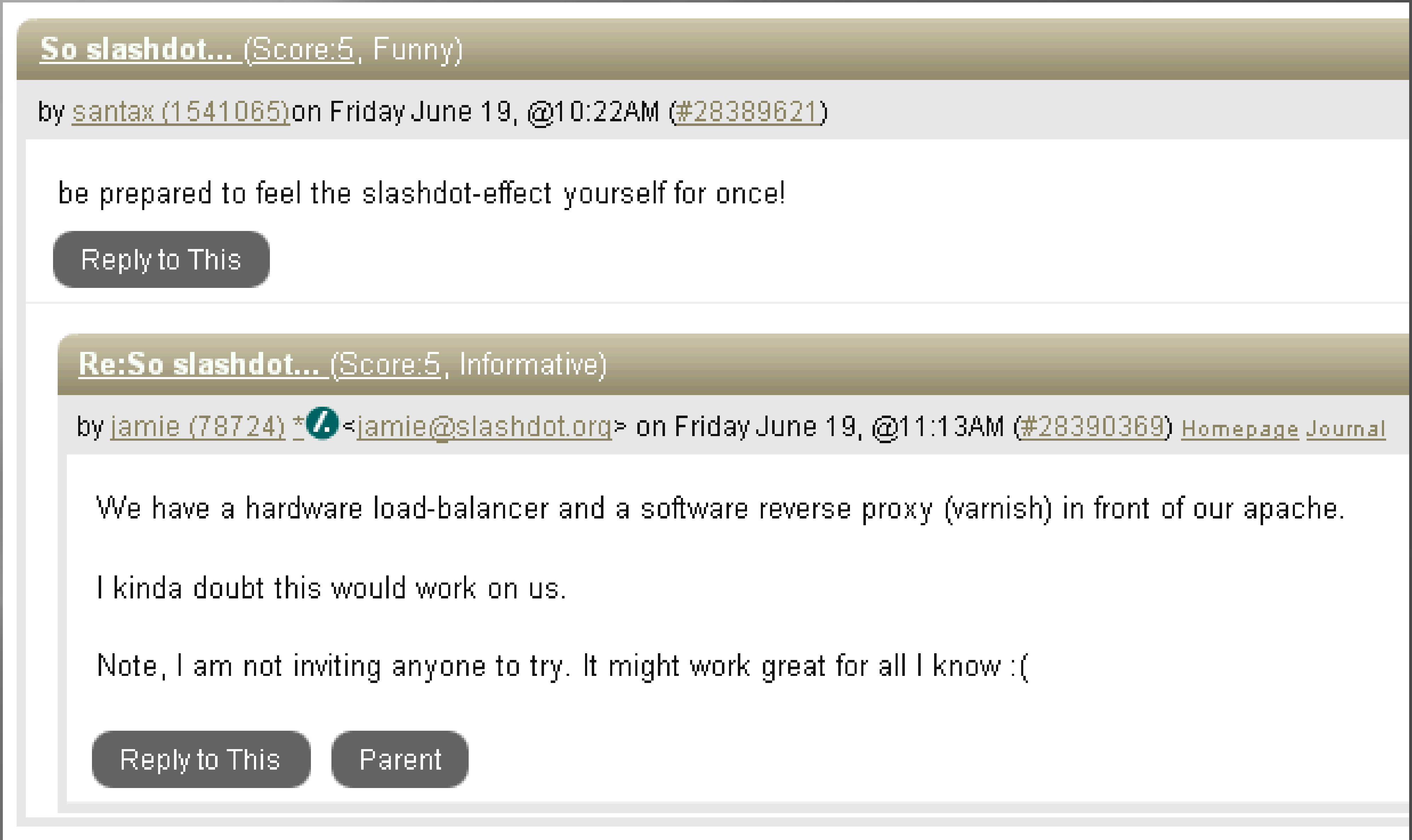
4chan: O HAI

Slowlaris, meet Scientology. Scientology, ...

...

Scientology...?

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.

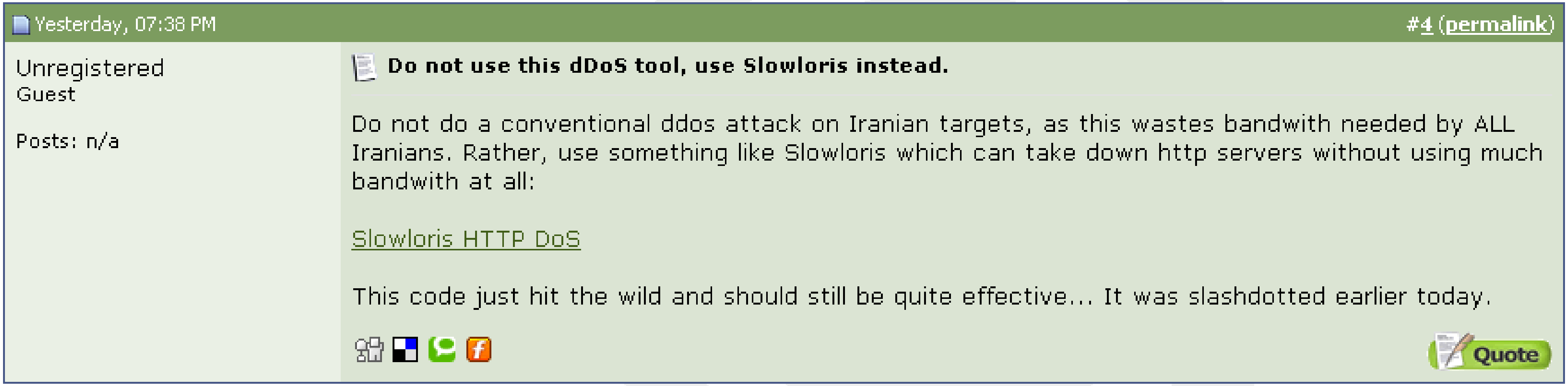
I kinda doubt this would work on us.

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

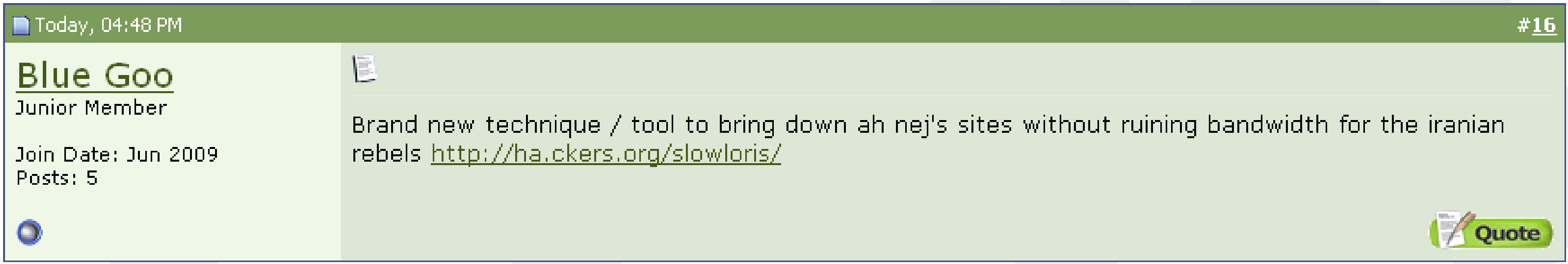
Posts: n/a

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

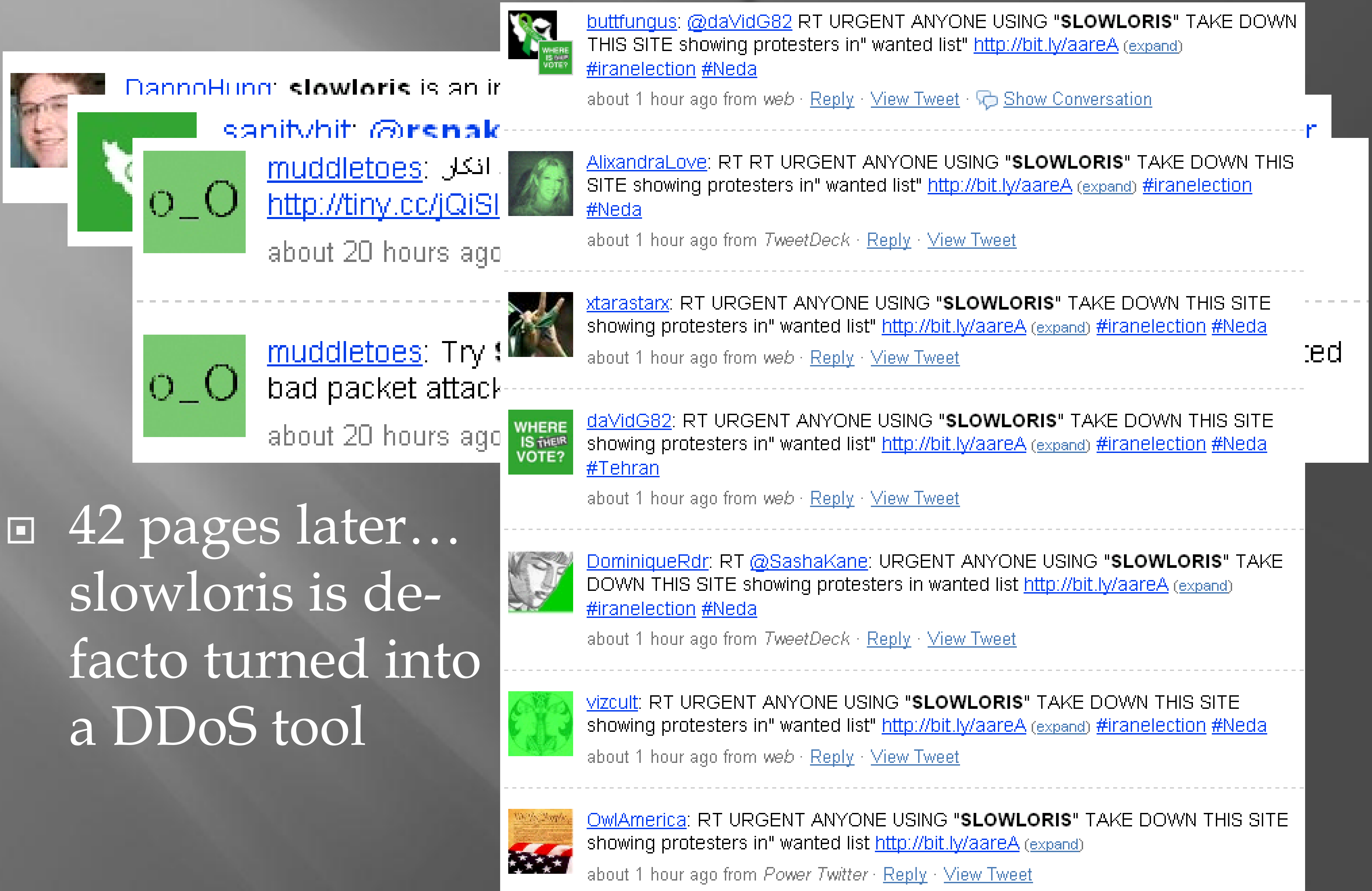
#16

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

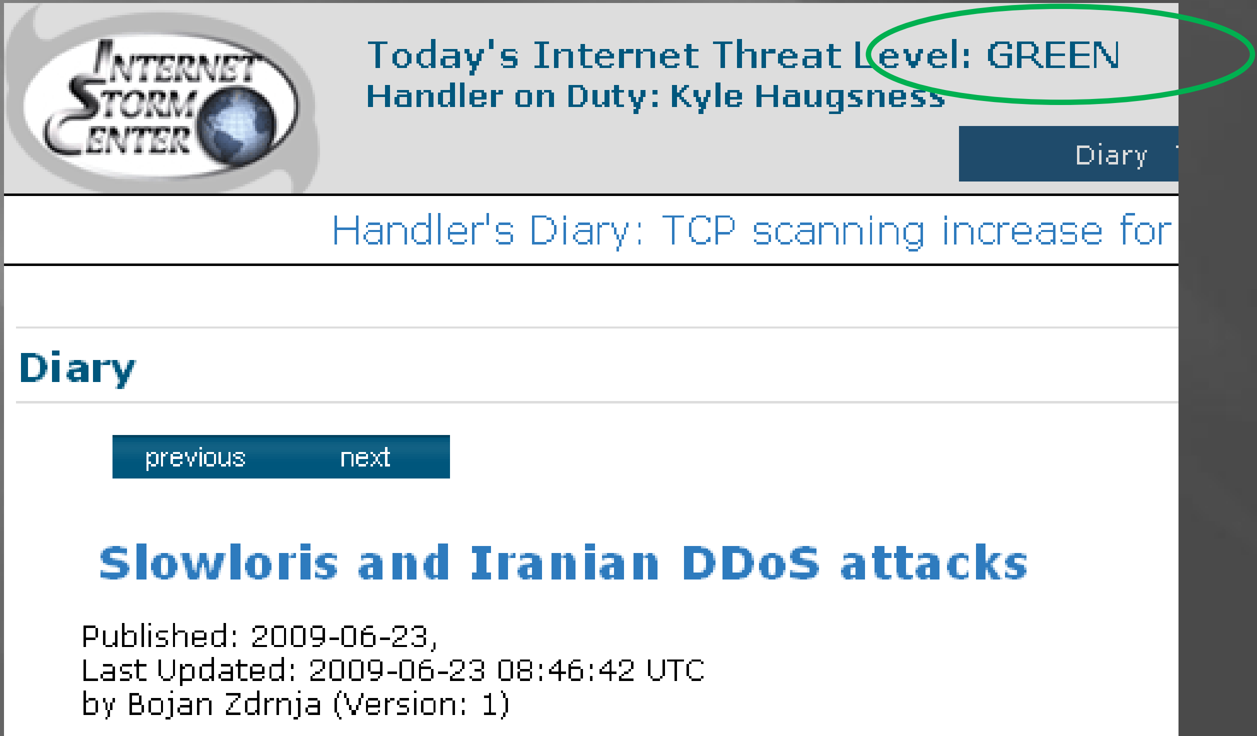
OwlAmerica: RT URGENT ANYONE USING "**SLOWLORIS**" TAKE DOWN THIS SITE showing protesters in" wanted list http://bit.ly/aareA (expand)
about 1 hour ago from *Power Twitter* · Reply · View Tweet

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

More servers are Affected…

- Apache 1.x, 2.x
- dhttpd
- GoAhead WebServer
- WebSense "block pages" (unconfirmed)
- Trapeze Wireless Web Portal (unconfirmed)
- Verizon's MI424-WR FIOS Cable modem (unconfirmed)
- Verizon's Motorola Set-Top Box (port 8082 and requires auth - unconfirmed)
- BeeWare WAF (unconfirmed)
- Deny All WAF (unconfirmed)

CERT and Internet Storm Center



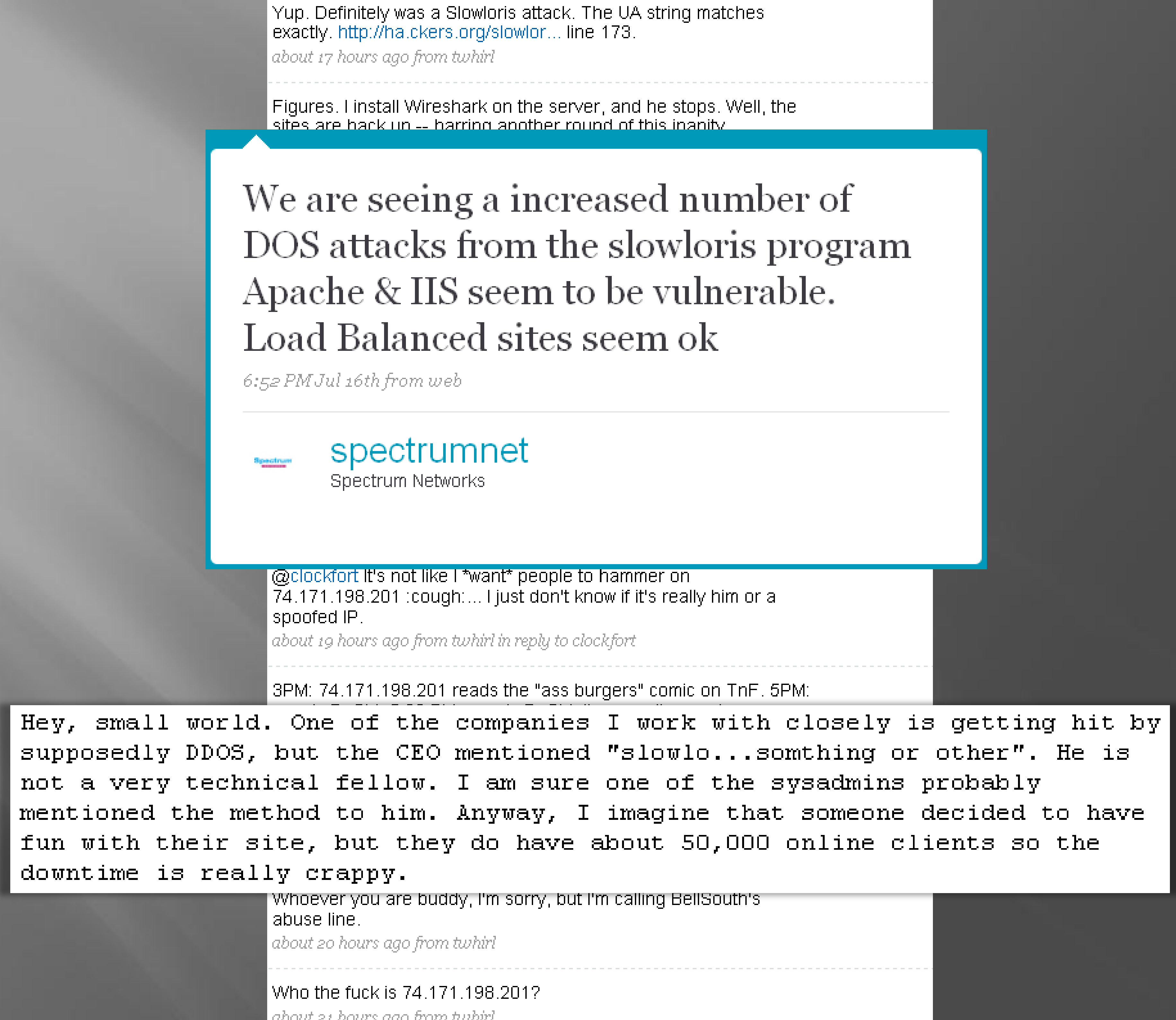
Today's Internet Threat Level: GREEN
Handler on Duty: Kyle Haugsness

Handler's Diary: TCP scanning increase for

Diary

Slowloris and Iranian DDoS attacks

Published: 2009-06-23,
Last Updated: 2009-06-23 08:46:42 UTC
by Bojan Zdrnja (Version: 1)



Yup. Definitely was a Slowloris attack. The UA string matches exactly. http://ha.ckers.org/slowlor... line 173.

about 17 hours ago from twhirl

Figures. I install Wireshark on the server, and he stops. Well, the sites are back up -- barring another round of this inanity

We are seeing a increased number of DOS attacks from the slowloris program Apache & IIS seem to be vulnerable. Load Balanced sites seem ok

6:52 PM Jul 16th from web

spectrumnet
Spectrum Networks

@clockfort It's not like I *want* people to hammer on 74.171.198.201 :cough:... I just don't know if it's really him or a spoofed IP.

about 19 hours ago from twhirl in reply to clockfort

3PM: 74.171.198.201 reads the "ass burgers" comic on TnF. 5PM:

Hey, small world. One of the companies I work with closely is getting hit by supposedly DDOS, but the CEO mentioned "slowlo...somthing or other". He is not a very technical fellow. I am sure one of the sysadmins probably mentioned the method to him. Anyway, I imagine that someone decided to have fun with their site, but they do have about 50,000 online clients so the downtime is really crappy.

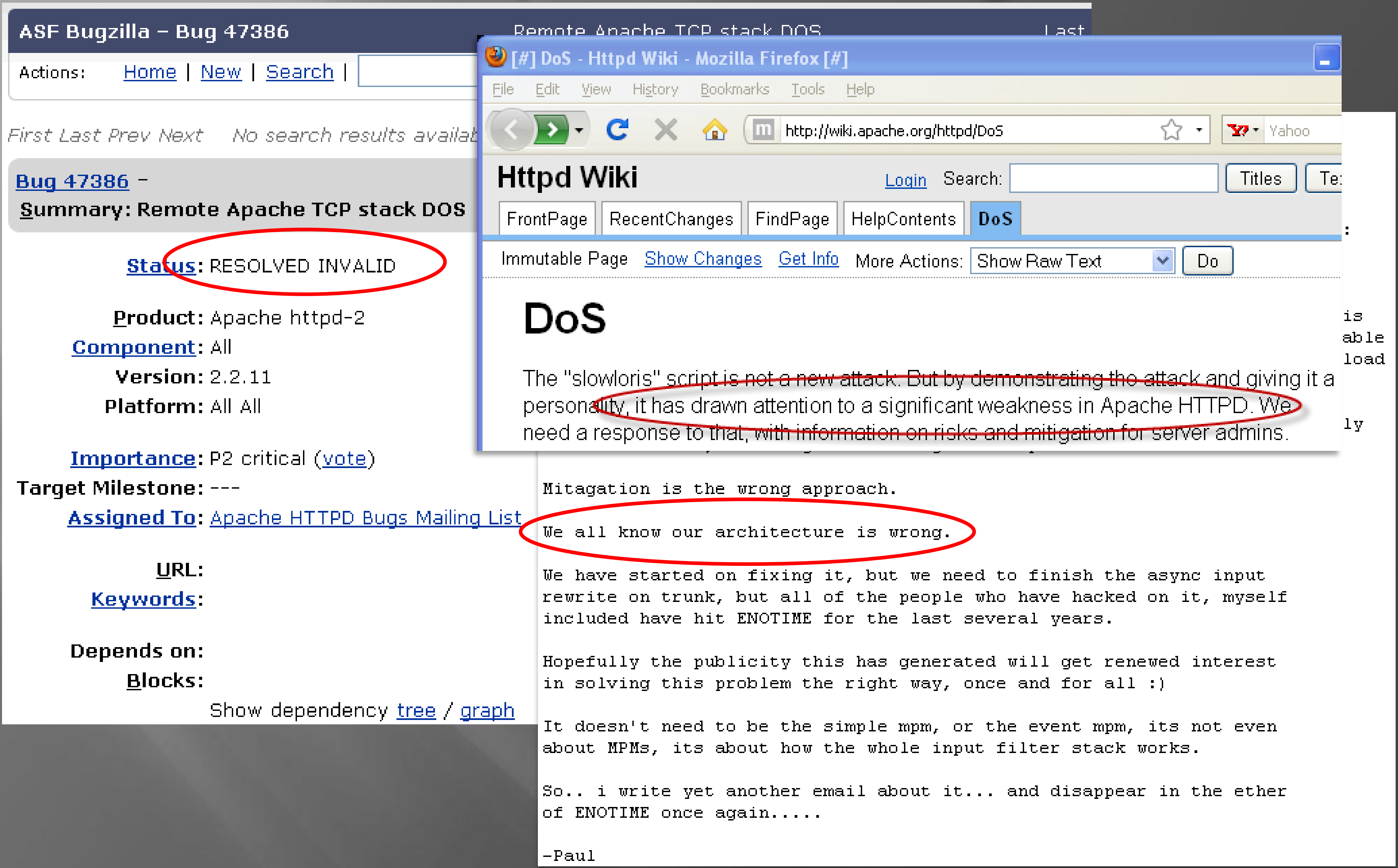
Whoever you are buddy, I'm sorry, but I'm calling BellSouth's abuse line.

about 20 hours ago from twhirl

Who the fuck is 74.171.198.201?

about 21 hours ago from twhirl

Oh Apache… *sigh*



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

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.

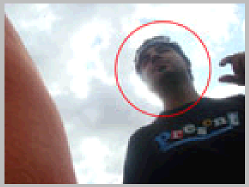
We have started on fixing it, but we need to finish the async input rewrite on trunk, but all of the people who have hacked on it, myself included have hit ENOTIME for the last several years.

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

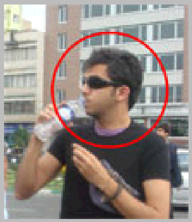
It doesn't need to be the simple mpm, or the event mpm, its not even about MPMs, its about how the whole input filter stack works.

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

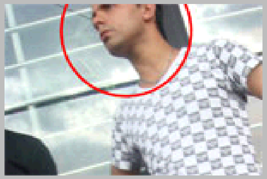
-Paul



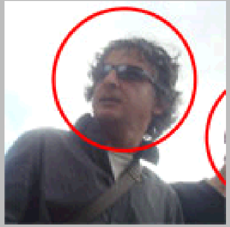
شماره 49



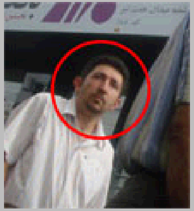
شماره 50



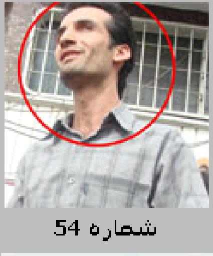
شماره 51



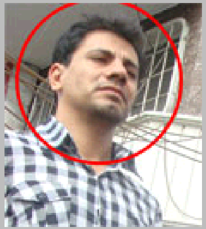
شماره 52



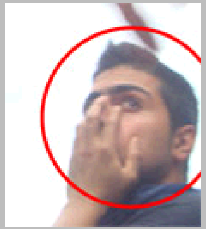
شماره 53



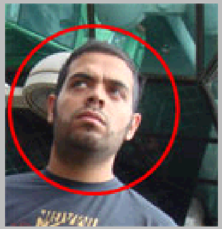
شماره 54



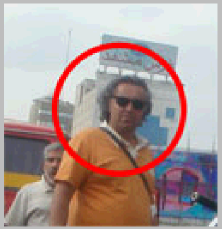
شماره 55



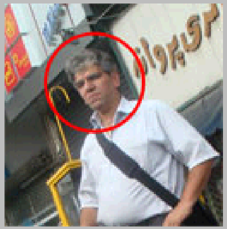
شماره 56



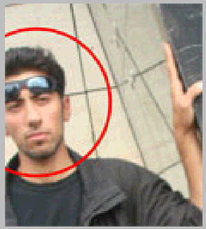
شماره 57



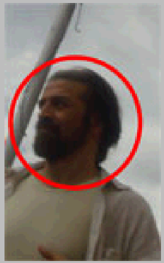
شماره 58



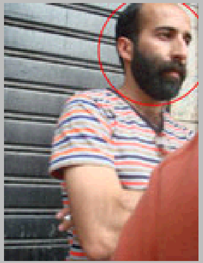
شماره 59



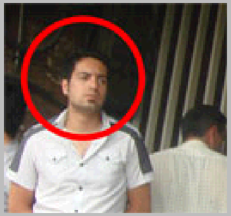
شماره 60



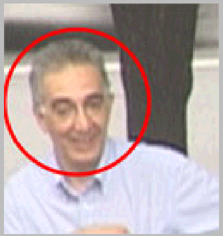
شماره 61



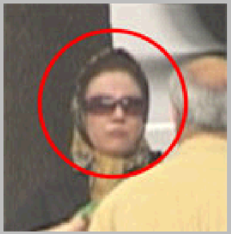
شماره 62



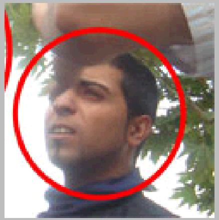
شماره 63



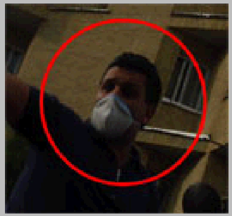
شماره 64



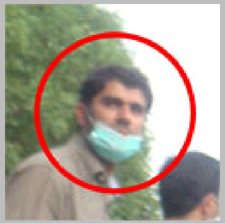
شماره 65



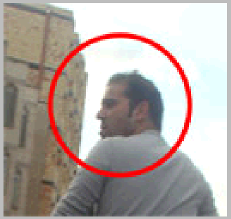
شماره 66



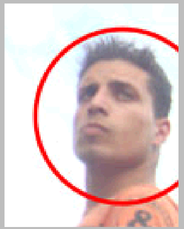
شماره 67



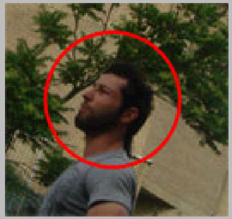
شماره 68



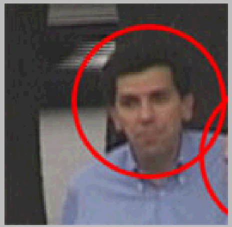
شماره 69



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

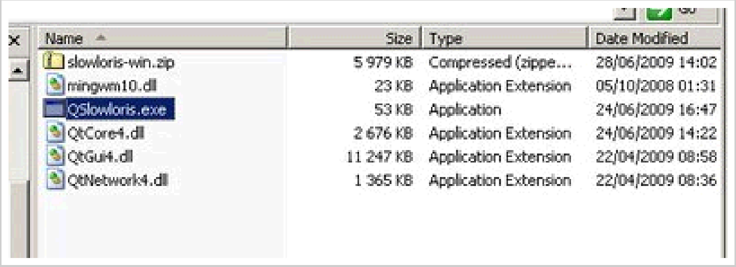
Please help the protestors and send adresses of similar ill-intended websites to cyberwar4iran@gmail.com

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) :

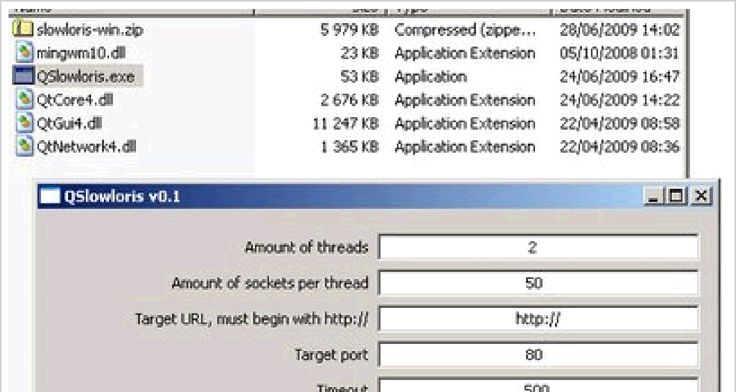
1 - Download Slowloris here : http://www.megaupload.com/?d=P5BARST4

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

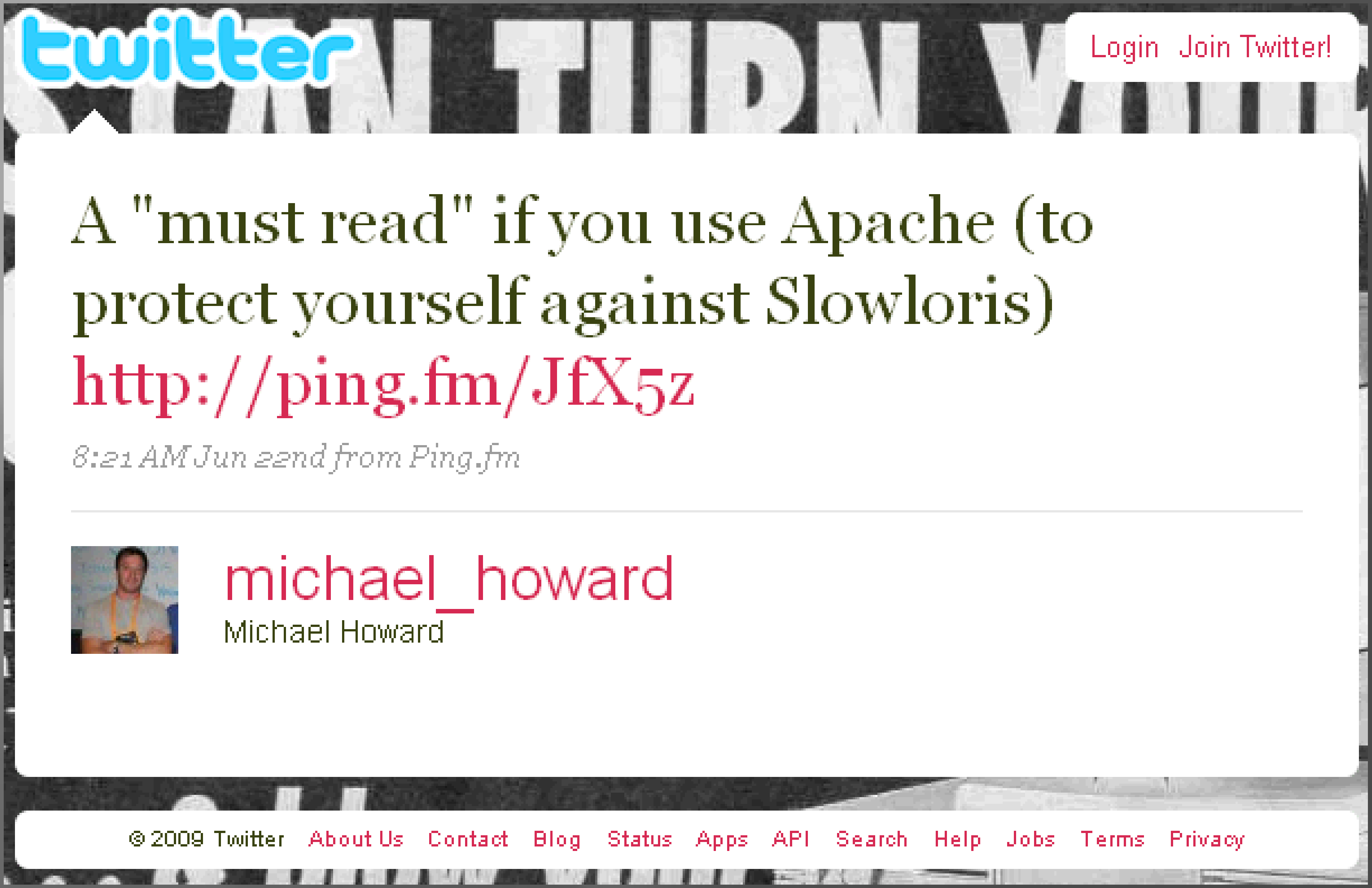
QSlowloris v0.1

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"?

Microsoft Even Gets In On The Action



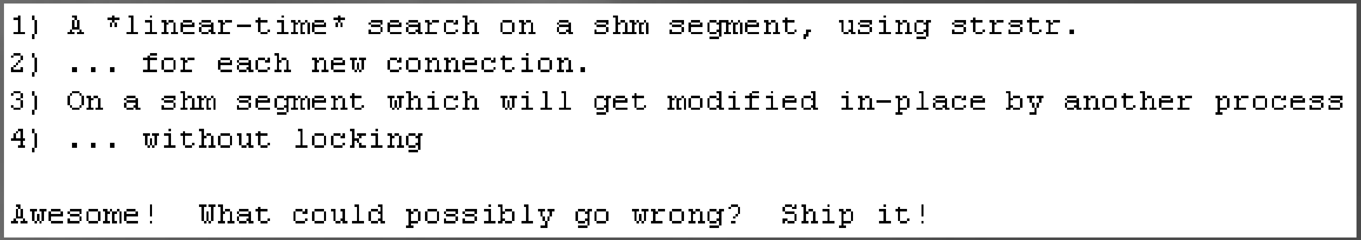
A "must read" if you use Apache (to protect yourself against Slowloris) http://ping.fm/JfX5z

8:21 AM Jun 22nd from Ping.fm

michael_howard
Michael Howard

Mitigating Slowloris

- Scary to Devs:
  - Use a different web server
- Scary to networking guys:
  - Use a proxy that has a worker pool model
  - “Use a firewall” – Inadvertent DoS?
- Scary to everyone:
  - mod_antiloris
  - mod_noloris
  - User MPM (experimental)



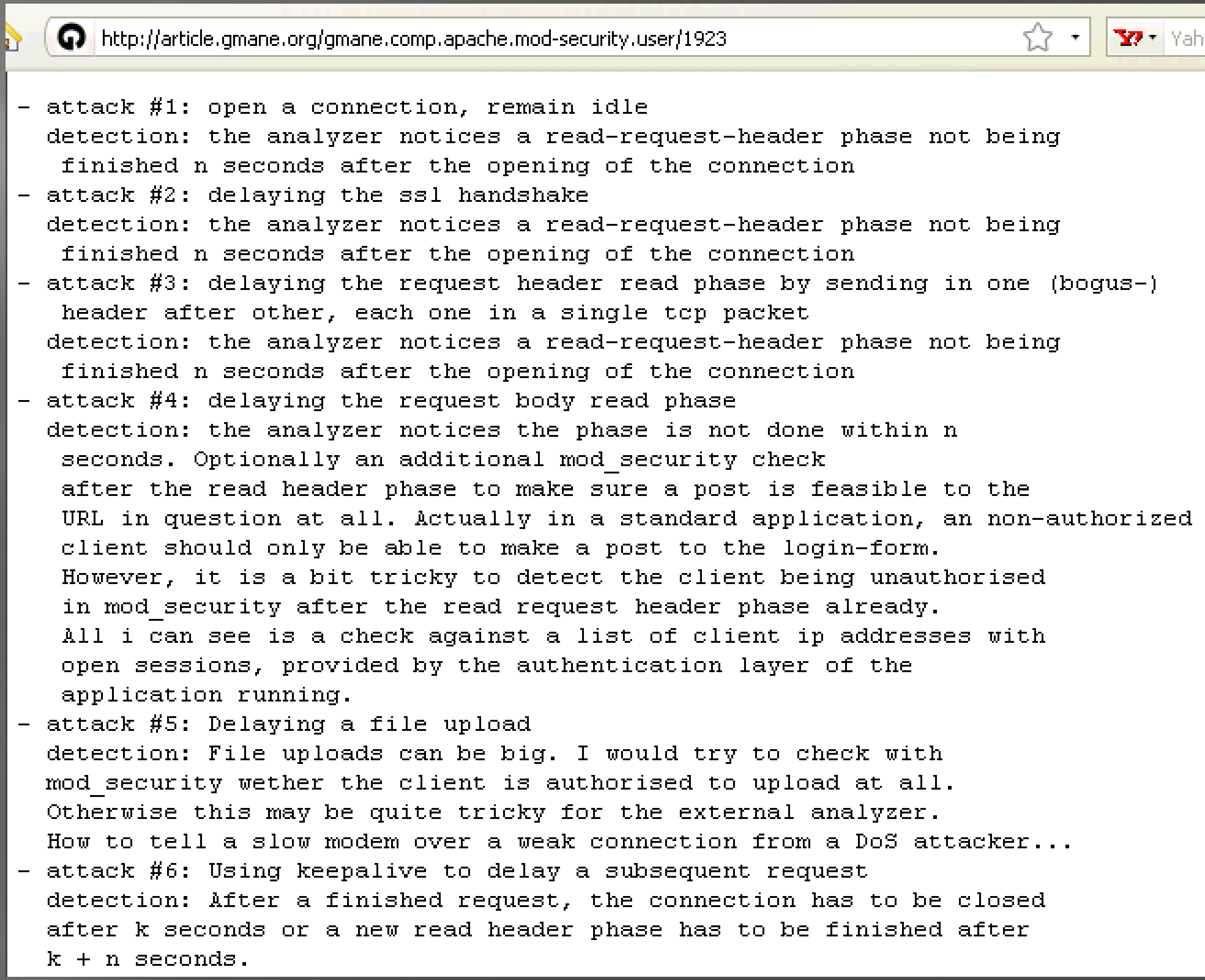
```
1)  A *linear-time* search on a shm segment, using strstr.
2)  ... for each new connection.
3)  On a shm segment which will get modified in-place by another process
4)  ... without locking

Awesome!  What could possibly go wrong?  Ship it!
```

- Scary, but only to Apache:
  - Fix Apache so it no longer uses a single thread-per-user model.

Improvements to Slowloris

- ToR
- Proxy
- _D_DoS
- Configurable (user agent, etc…)
- More payloads
- Etc…


http://article.gmane.org/gmane.comp.apache.mod-security.user/1923
Yah

```
- attack #1: open a connection, remain idle
  detection: the analyzer notices a read-request-header phase not being
   finished n seconds after the opening of the connection
- attack #2: delaying the ssl handshake
  detection: the analyzer notices a read-request-header phase not being
   finished n seconds after the opening of the connection
- attack #3: delaying the request header read phase by sending in one (bogus-)
   header after other, each one in a single tcp packet
  detection: the analyzer notices a read-request-header phase not being
   finished n seconds after the opening of the connection
- attack #4: delaying the request body read phase
  detection: the analyzer notices the phase is not done within n
   seconds. Optionally an additional mod_security check
   after the read header phase to make sure a post is feasible to the
   URL in question at all. Actually in a standard application, an non-authorized
   client should only be able to make a post to the login-form.
   However, it is a bit tricky to detect the client being unauthorised
   in mod_security after the read request header phase already.
   All i can see is a check against a list of client ip addresses with
   open sessions, provided by the authentication layer of the
   application running.
- attack #5: Delaying a file upload
  detection: File uploads can be big. I would try to check with
  mod_security wether the client is authorised to upload at all.
  Otherwise this may be quite tricky for the external analyzer.
  How to tell a slow modem over a weak connection from a DoS attacker...
- attack #6: Using keepalive to delay a subsequent request
  detection: After a finished request, the connection has to be closed
  after k seconds or a new read header phase has to be finished after
  k + n seconds.
```

Questions/Comments?

- Robert Hansen
  - h _at_ ckers d0t org
  - http://www.sectheory.com/
  - http://ha.ckers.org/
  - TBD: Book – "Detecting Malice"
  - XSS Book: XSS Exploits and Defense
    - ISBN: 1597491543