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 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 Shachn 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 – Vulnerability management through cloud checklist

Russian politician: 'My assistant started Estonian cyberwar'

Dubious DDoS lols

By John Leyden • Get more from this author

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

Watch the Application c

A junior Russian pol played some part in

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

Comments by Serge, a cybercrime panel

to inflame tensions

internet attacks dur

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 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

**Votes for Ahmadinejad and Mousavi on 6 different official announcements**

![Graph showing votes for Ahmadinejad and Mousavi](image)

- **RIGGING INDICATORS**
  - **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.
  - **LOGICAL ANOMALIES**
    - Candidates fail to win (or to even do well) in their home districts, especially where their ethnicity should help.
  - **A BREAK WITH POLLS**
    - Election returns are wildly inconsistent with recent reliable, thorough polling data, assuming it exists.
  - **REVERSALS OF FORTUNE**
    - Compared with a recent earlier contest, parties and candidates experience a big swing in popularity.
  - **FISHY DIGITS**
    - Fair vote tallies have a reliably even distribution of digits. Phony numbers made by humans do not.
  - **LATE COMEBACKS**
    - If results are released on a rolling basis, you can tell if a panicked party starts stuffing ballot boxes.
  - **HASTY VERDICTS**
    - When voting is electronic, results come fast. But with paper ballots, a speedy victor is suspicious.

**DID IT HAPPEN IN IRAN?**

- **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.
- **YES**: Mir Hossein Mousavi, an Azeri, lost East Azerbaijan. Mehdi Karrubi won 5 percent of his home district, a tenth of his 2005 result.
- **NO**: One poll put Mahmoud Ahmadinejad up 2:1. But that was pre-debate, and most respondents refused to say who they'd vote for.
- **YES**: Despite economic woes, reformists did more poorly than in 2005. And Ahmadinejad won in previously hostile Tehran Province.
- **UNCLEAR**: Statisticians need precinct-level data to run their models, and Iran's rulers are unlikely to release that information.
- **UNCLEAR**: Again, not enough data. If Iran's rulers rigged the vote, they did it right at the start of announced returns.
- **YES**: The Interior Ministry declared victory for Ahmadinejad two hours after polls closed; results were authorized immediately.
Twitter is important
Create auto web-page re-loader
Add a dose of social outrage
DoS turns into DDoS pretty quickly
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…
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.
DDoS Increases Against Iran
Unwittingly, 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://hackers.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 [-]

Slowloris, meet 4chan. 4chan, Slowloris.
4chan: O HAI
Slowloris, meet Scientology. Scientology, ...
...
Scientology...?

permalink reply
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) * 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 :(
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.

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

slowloris is de-facto turned into a DDoS tool
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.

Mitigation 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
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 protesters and send addresses 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 caught...

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

1 - Download Slowloris here: http://www.megaupload.com/?d=PSBAPST4

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

3 - Execute QSlowloris.exe
3rd Party Implementations

- **PyLoris**

- **PHP version:**

- **Questionable EXE version**
  - [http://cyberwar4iran.blogspot.com/](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.
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 accounts. You don’t have to. If you haven’t already, take a look at Payment Service and our Payment Gateway.

As for PCI level 2 compliance, you have to build a PCI level 2 compliant system. And you have to review it if you have a data breach, you do. As a best practice, I recommend business continuity. From our perspective, we recommend testing the system because it is not inherently flexible. Our customers can keep the credit card data stored and have the ability to test and keep the card data stored. We do not require things like in-process authorizations or tokenization of card data so you don’t have to. Our PCI compliance tests are conducted by an independent third-party vendor. It is possible for you and your customers to achieve level 1 compliance through our PCI Level 2 Assessment process.

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

To: dvyrfe@yahoo.com
Subject: Re: Delivered: Re:

Dear [Name],

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

---

Done
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