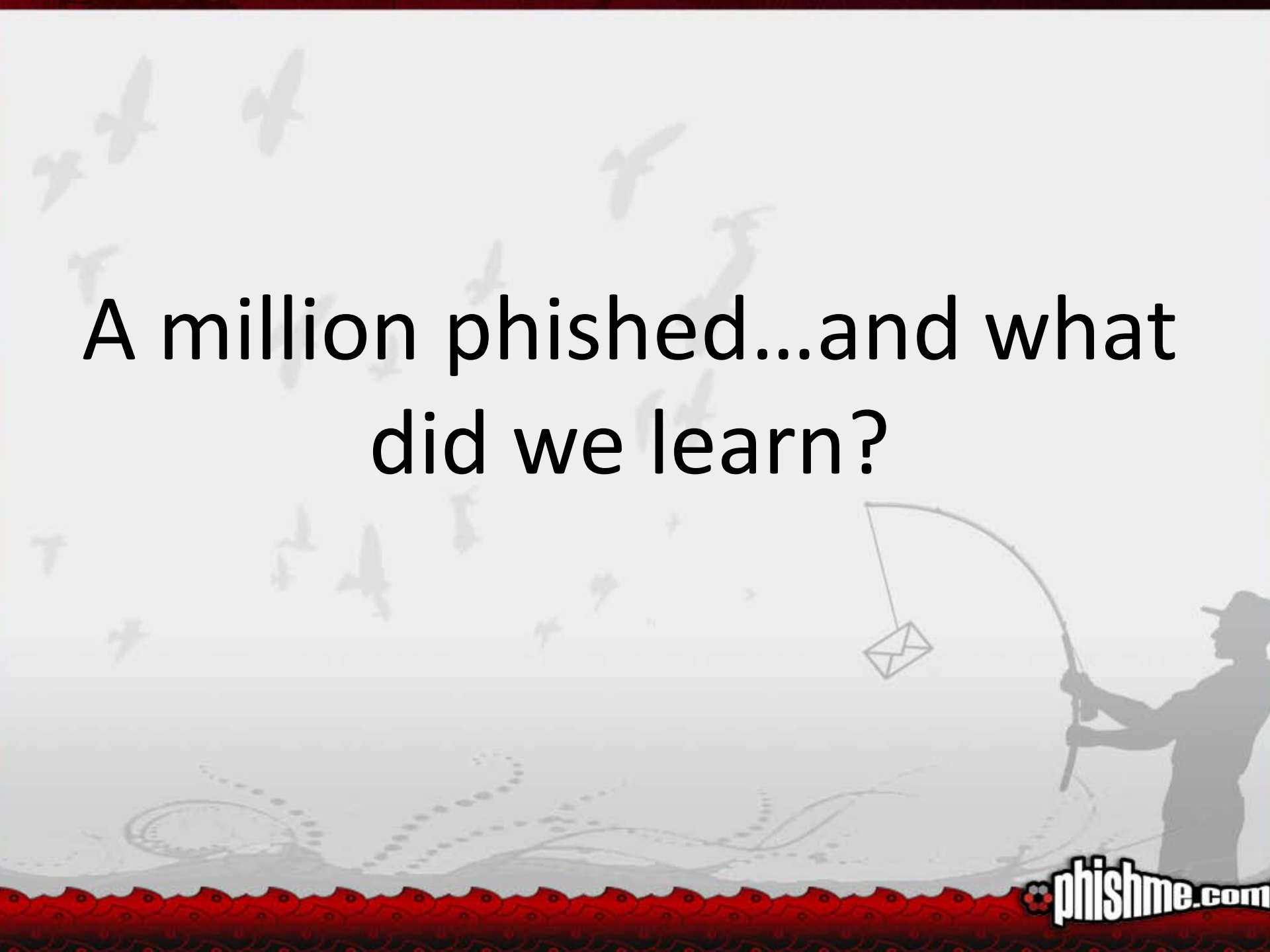
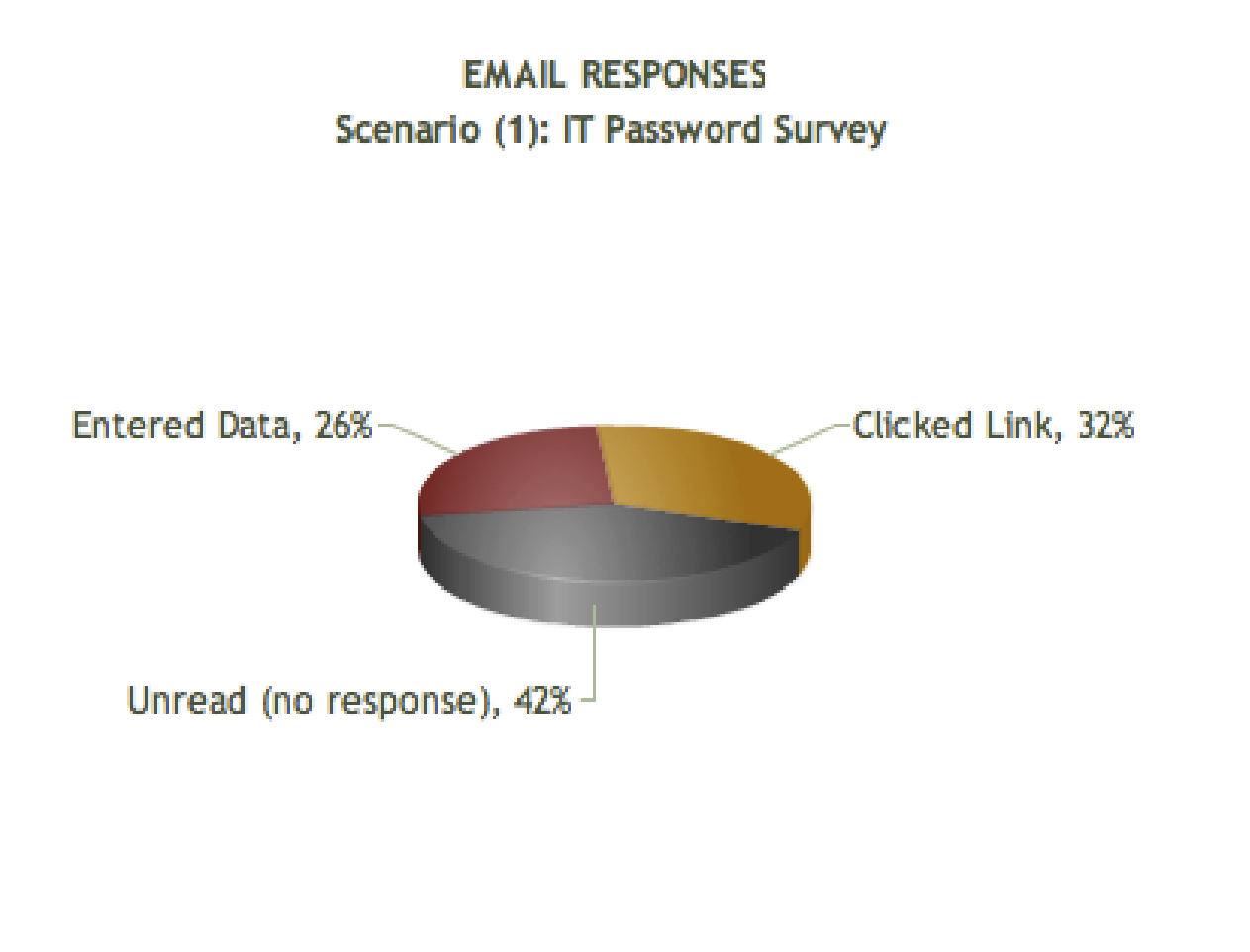
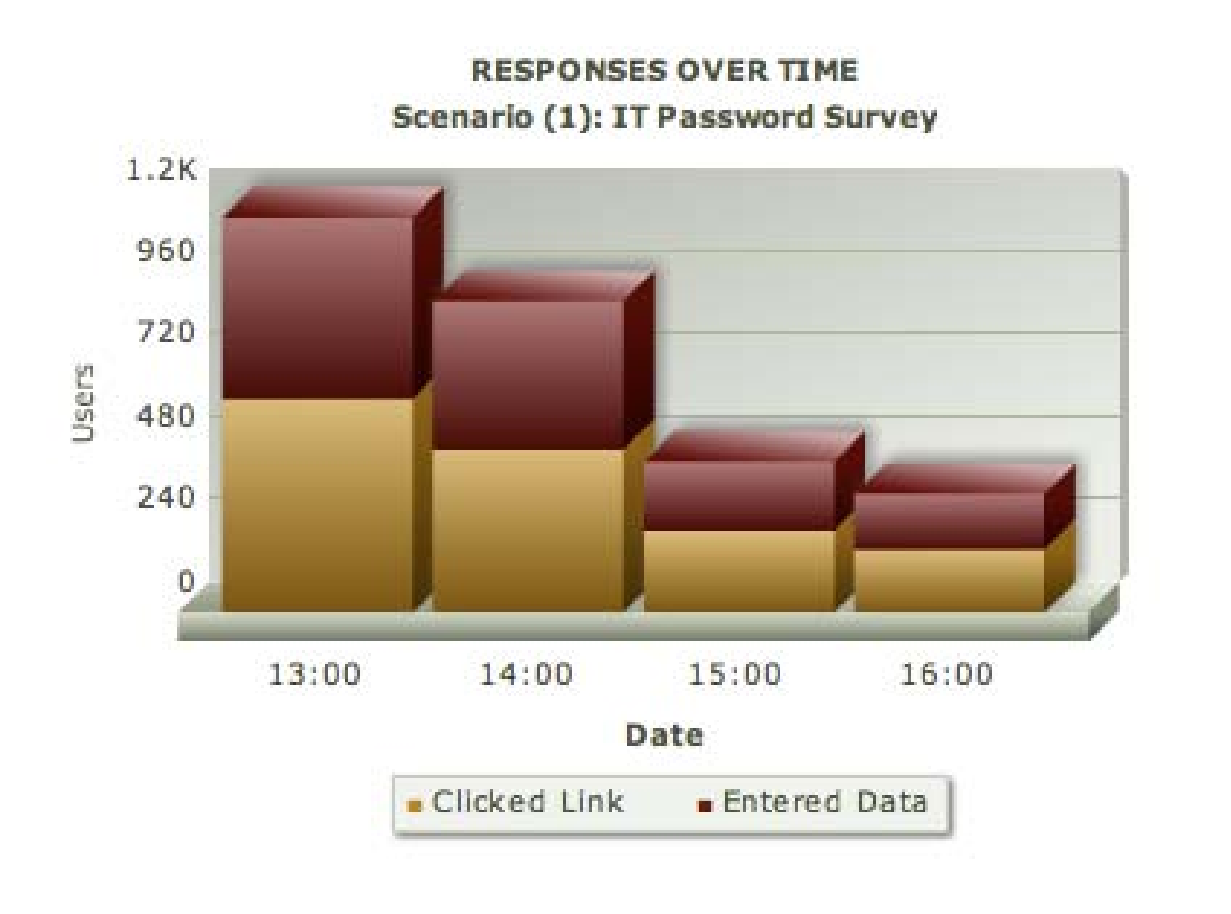
A million phished…and what did we learn?



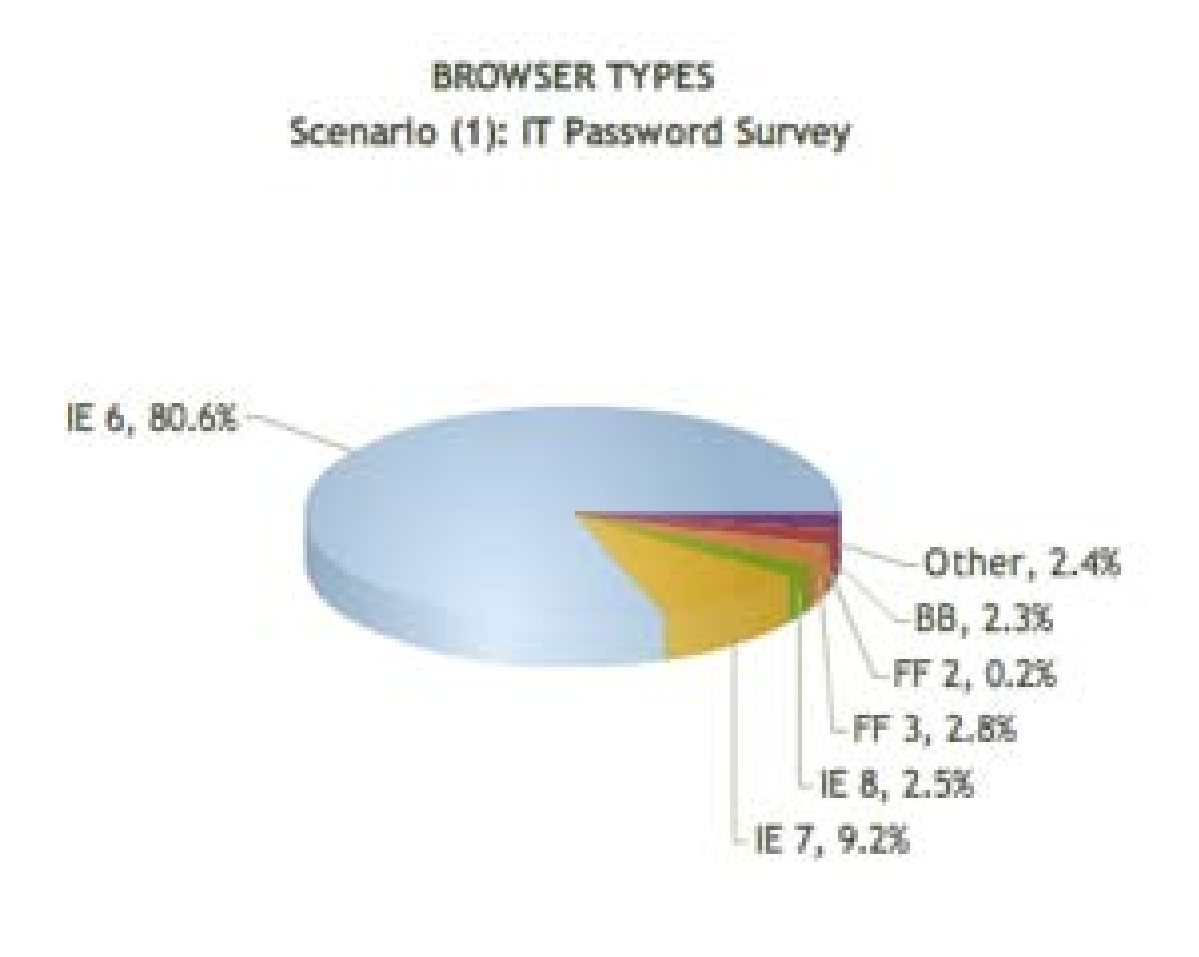
Spear Phishing works…58% of the time



…and within a few minutes



…and succeeds in exploiting the browser



Have You Heard of APT?

We Were Forewarned

SANS: Security Ignores the Two Biggest Cyber Risks

Client-side application vulnerabilities and insecure web apps deserve more attention than operating systems bugs, says new research from SANS Institute

» Comments

By Joan Goodchild, Senior Editor

September 15, 2009 — CSO —

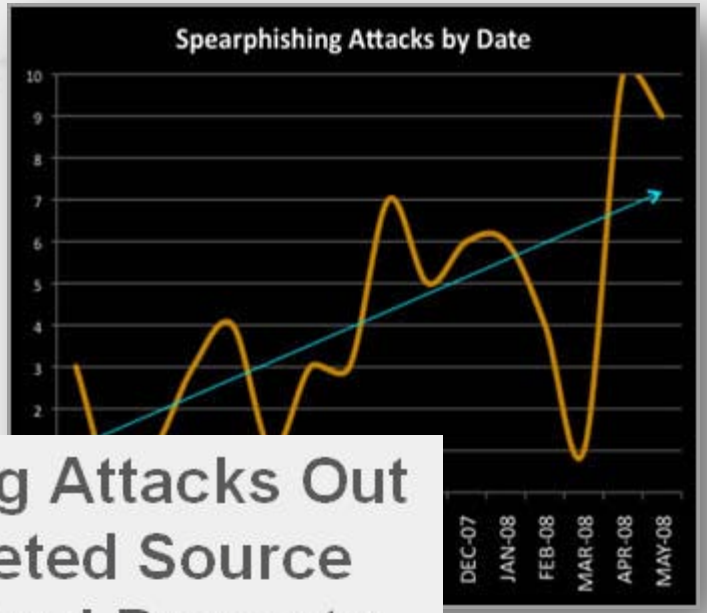
Two major cyber risks dwarf all others, but organizations are failing to invest in the proper tools to mitigate them, choosing instead to focus security attention on lower risk areas, according to a report released Tuesday by SANS Institute.

The research, which draws upon data collected from March to August claims companies give insufficient attention to today's risks and put th maintain the status quo with an emphasis on operating system patch Attack data for this research was drawn from TippingPoint appliances vulnerability data was collected via Qualys' scanning services.

Also see 7 Reasons Websites Are No Longer Safe

The most surprising conclusion may be that client-side application so threat to network security as opposed operating system vulnerabilities comes to patching. SANS claims many spear-phishing attacks exploi programs such as Adobe PDF Reader, QuickTime, Adobe Flash and

This is currently the primary initial infection vector used to compromis the repo states.



Spear-Phishing Attacks Out Of China Targeted Source Code, Intellectual Property

Attackers used intelligence, custom malware to access Google, Adobe, and other U.S. companies' systems

Jan 13, 2010 | 04:12 PM

By Kelly Jackson Higgins
DarkReading

The wave of targeted attacks from China on Google, Adobe, and more than 20 other U.S. companies, which has led the search giant to consider closing its doors in China and no longer censor search results there, began with end users at the victim organizations getting duped by convincing spear-phishing messages with poisoned attachments.

What It Boils Down To…

- Mining publicly available information
- Executing a spear phish
- Pushing malware to the victim machines
  - Advanced
    - Bypasses Anti-Spam/Anti-Phishing/Anti-Virus
    - Difficult to detect (little to no footprint in the file system)
  - Persistent
    - Dynamically evolves (Polymorphic)

Mining Publicly Available Information

Did You See This?

Records Say Chinese Gymnasts May Be Under Age - NYTimes.com - Microsoft Internet Explorer

File Edit View Favorites Tools Help

Back Search Favorites

Address http://www.nytimes.com/2008/07/27/sports/olympics/27gymnasts.html?_r=4&hp=&adxnnl=1&oref=slogin&pagewanted=print&adxnnlx= Go Links del.icio.us

The New York Times
nytimes.com

PRINTER-FRIENDLY FORMAT SPONSORED BY GO BEHIND THE SCENES

July 27, 2008

Records Say Chinese Gymnasts May Be Under Age

By JERÉ LONGMAN and JULIET MACUR

China named its Olympic women's gymnastics team on Friday, and the inclusion of at least two athletes has further raised questions, widespread in the sport, about whether the host nation for the Beijing Games is using under-age competitors.

Chinese officials responded immediately, providing The New York Times with copies of passports indicating that both athletes in question — He Kexin, a gold-medal favorite in the uneven parallel bars, and Jiang Yuyuan — are 16, the minimum age for Olympic eligibility since 1997.

Officials with the International Gymnastics Federation said that questions ab
reports, USA Gymnastics and fans of the sport, but that Chinese authorities p

Online records listing Chinese gymnasts and their ages that were posted on o
Chinese news media, however, seem to contradict the passport information, i
years below the Olympic limit.

Mary Lou Retton, the Olympic all-around gymnastics champion at the 1984 I
He and other Chinese gymnasts on the uneven bars.

"The girls are so little, so young," Retton said. Speaking of He, Retton rolled h
don't know."

Done

What Did Stryde Hax Do?

Google Search -

“site:cn 何可欣 filetype:xls 1994”

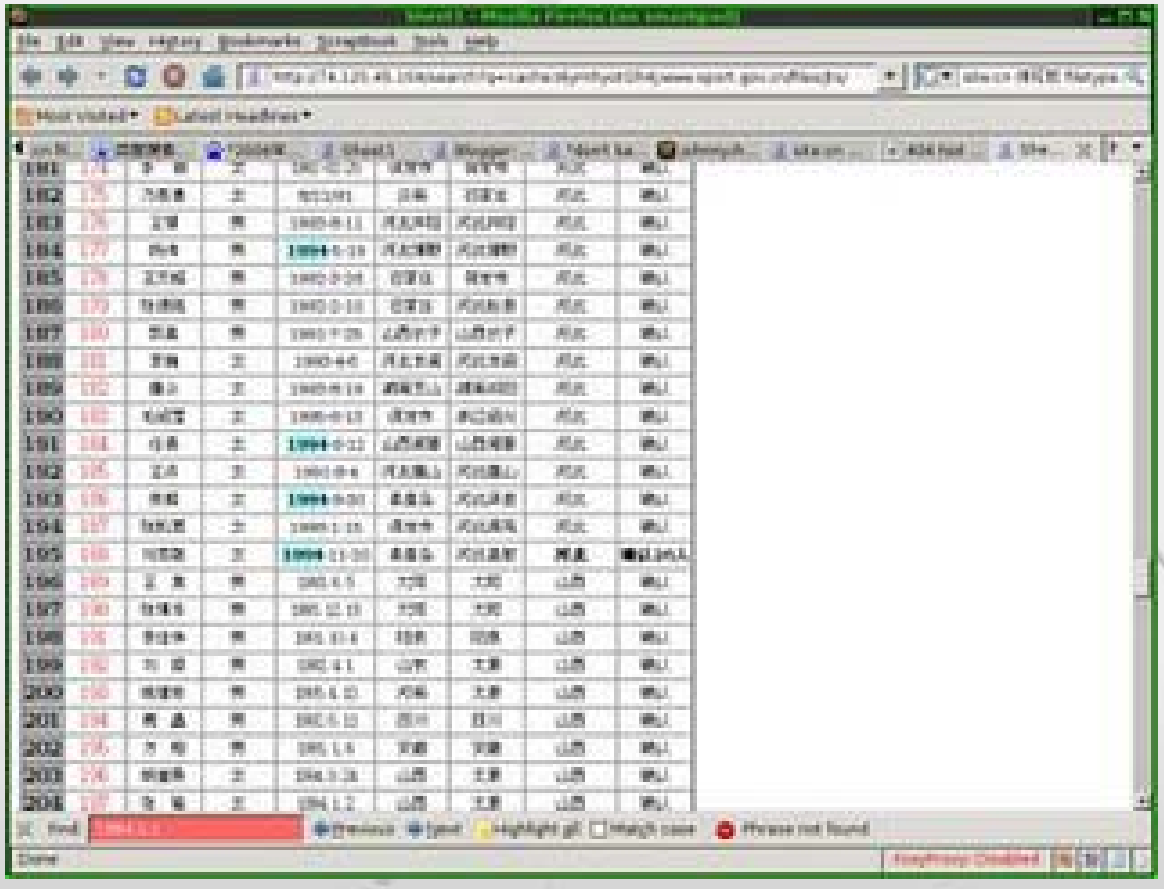
1. Search chinese websites
2. Look for He Kexin’s name
3. In an excel spreadsheet
4. That contains the string 1994 (assumed year of birth)

The Result…

http://www.sport.gov.cn/files/jts/reg2006/zctc.xls

Let’s open the file…

View as HTML

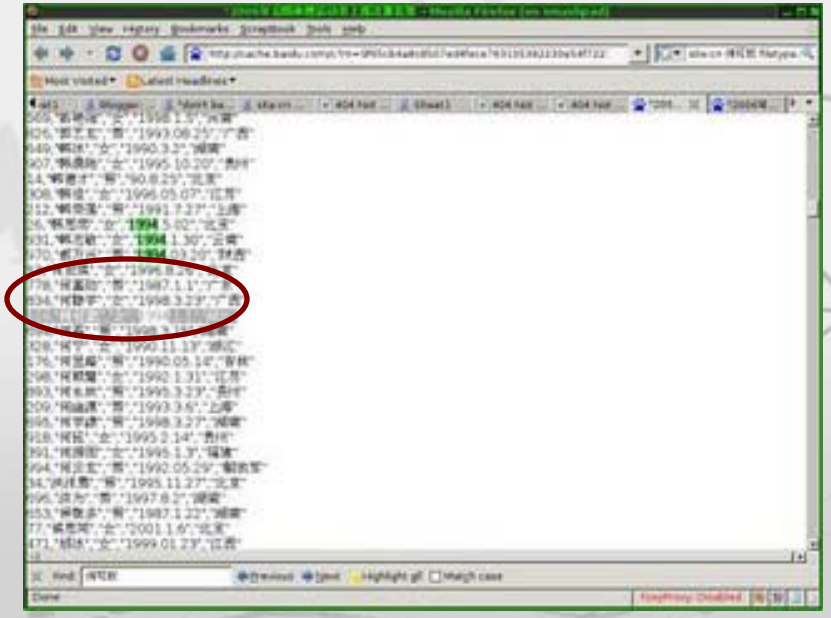


No He Kexin still …

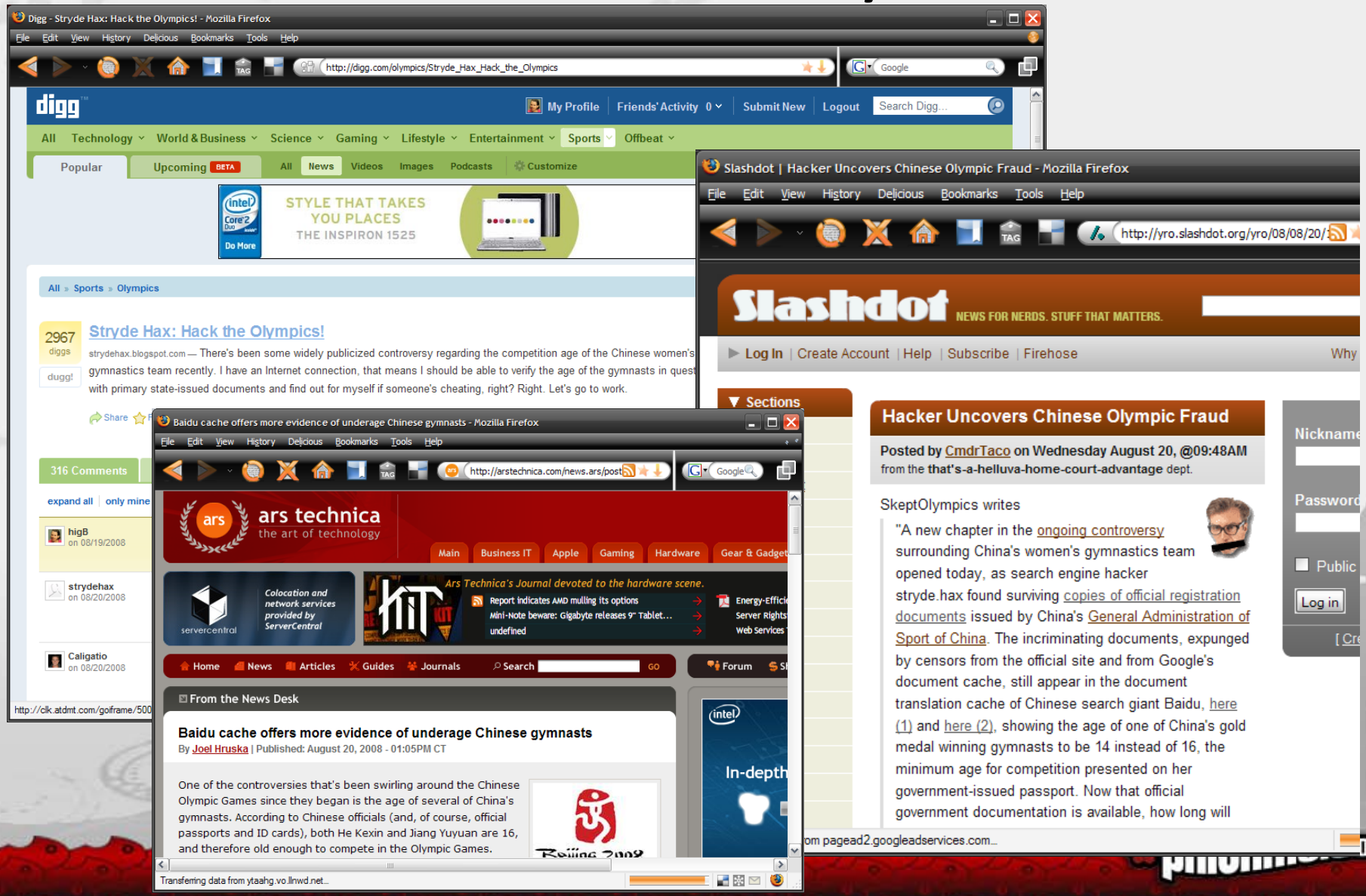
What about Baidu?

What about Baidu?

- New one discovered by Baidu is missing as well
- What about the cache?



Wednesday


Digg - Stryde Hax: Hack the Olympics! - Mozilla Firefox
http://digg.com/olympics/Stryde_Hax_Hack_the_Olympics
Stryde Hax: Hack the Olympics!
Slashdot | Hacker Uncovers Chinese Olympic Fraud - Mozilla Firefox
Hacker Uncovers Chinese Olympic Fraud
Posted by CmdrTaco on Wednesday August 20, @09:48AM
Baidu cache offers more evidence of underage Chinese gymnasts - Mozilla Firefox
Baidu cache offers more evidence of underage Chinese gymnasts
By Joel Hruska | Published: August 20, 2008 - 01:05PM CT

Thursday….

mike z (Do Not Disturb) Skype™ Chat

Add People | Send | Do More | Tools and Options | Bookmark

Messages in this chat are older than 23 hours

mike z says: 8/21/2008 2:41:47 PM

YO

8/21/2008 2:41:48 PM

URGENT

8/21/2008 2:41:53 PM

no joke, web server is down

8/21/2008 2:42:21 PM

http://207.46.222.11/

8/21/2008 2:42:27 PM

call me 201-916-4152

8/21/2008 2:44:53 PM

We're sorry.
This Microsoft Office Live service is being updated and is not currently available. We apologize for the inconvenience, please check back soon to use this updated service.

Find: Down | Find Next | Find Previous | Match case

Emoticons | Videos | Set Font

Online

mike z

Menu

Then to world news…

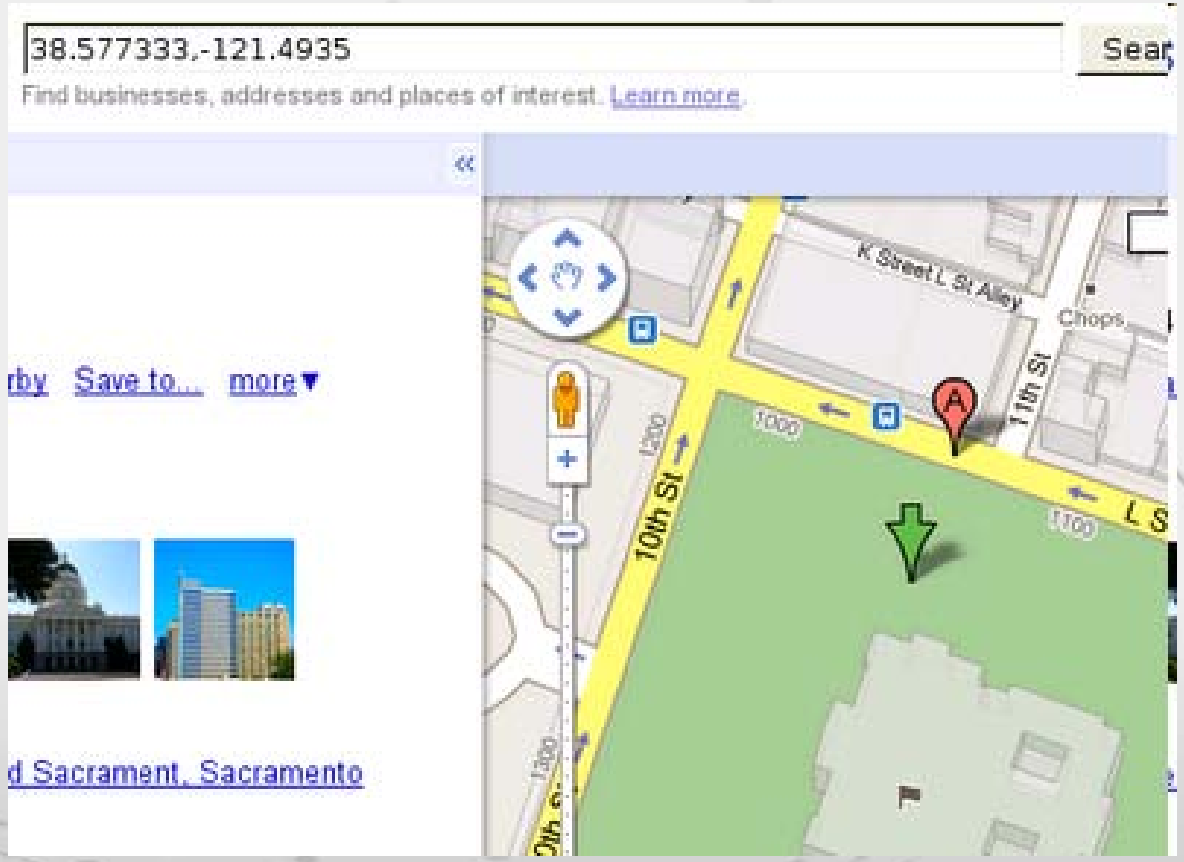
Friday Started at 5am

- IOC reopens investigation

Where's Waldo..err Arnold

http://twitter.com/schwarzenegger

Breakfast at the Capitol..



Conclusion

Q&A

Rohyt Belani, CEO Intrepidus Group

Rohyt.Belani@IntrepidusGroup.com