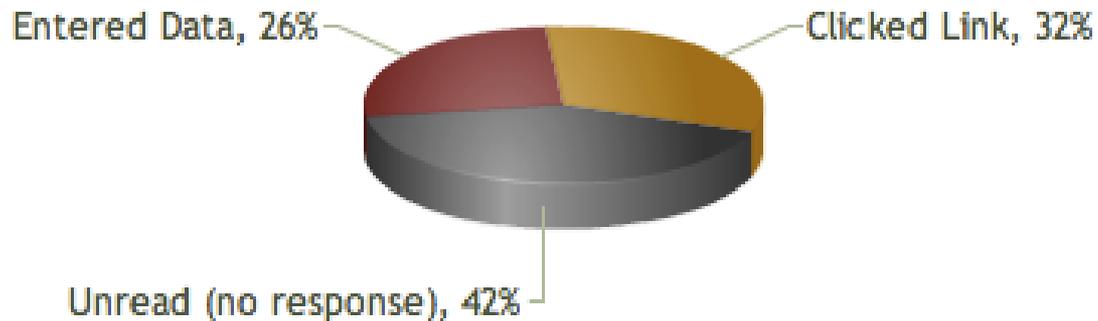


A million phished...and what
did we learn?

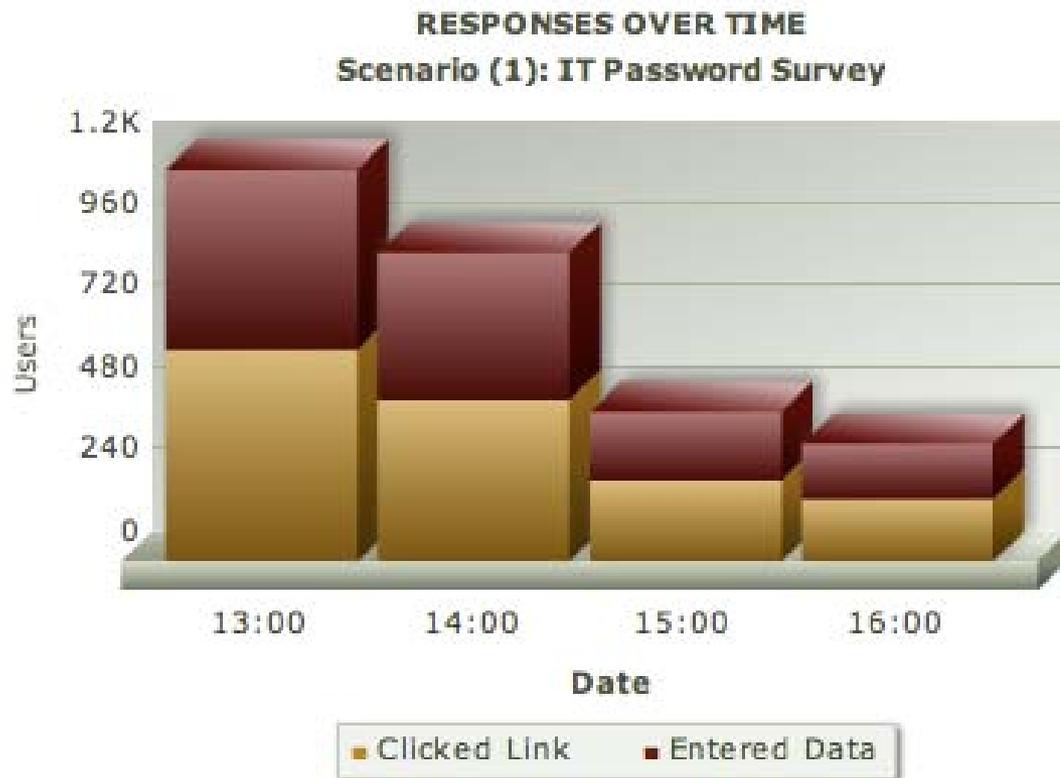


Spear Phishing works...58% of the time

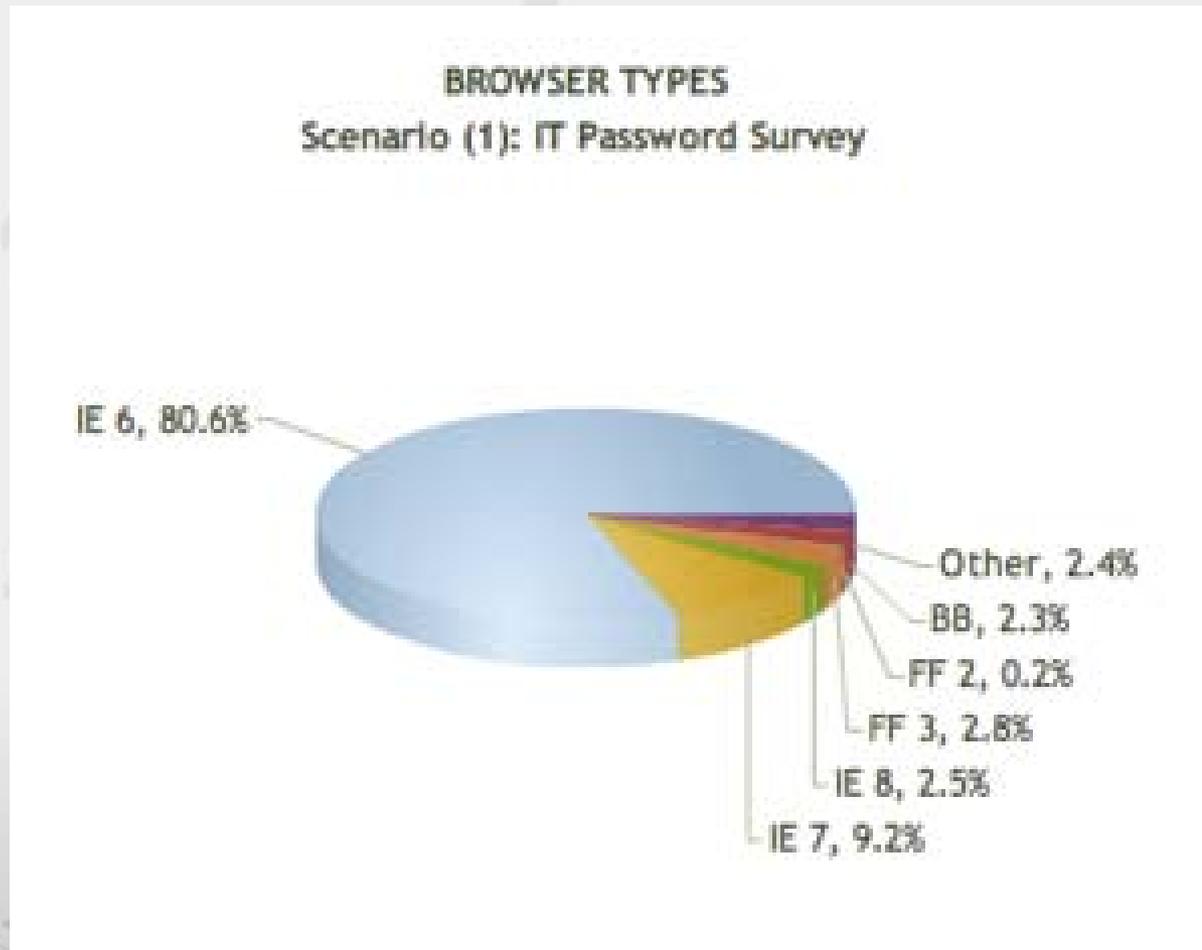
EMAIL RESPONSES
Scenario (1): IT Password Survey



...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 them off to maintain the status quo with an emphasis on operating system patches. 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 software is the biggest threat to network security as opposed to operating system vulnerabilities. SANS claims many spear-phishing attacks exploit programs such as Adobe PDF Reader, QuickTime, Adobe Flash and Internet Explorer.

This is currently the primary initial infection vector used to compromise systems, the report states.

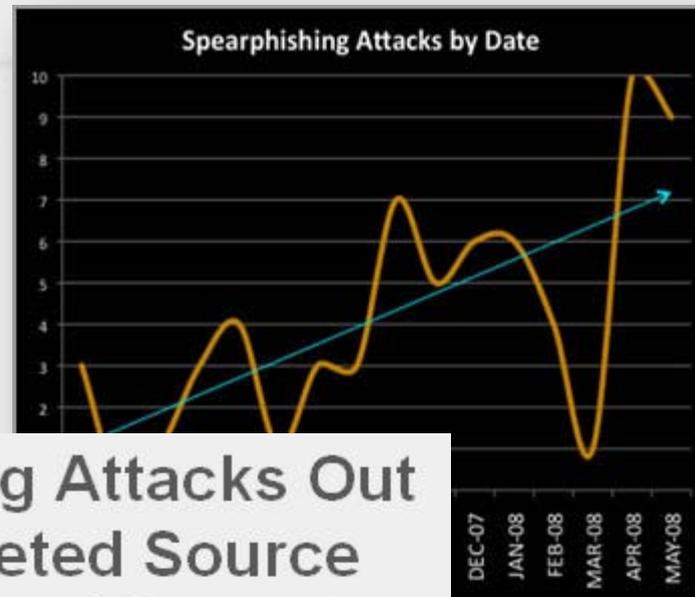
Spear-Phishing Attacks Out Of China Targeted Source Code, Intellectual Property

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.



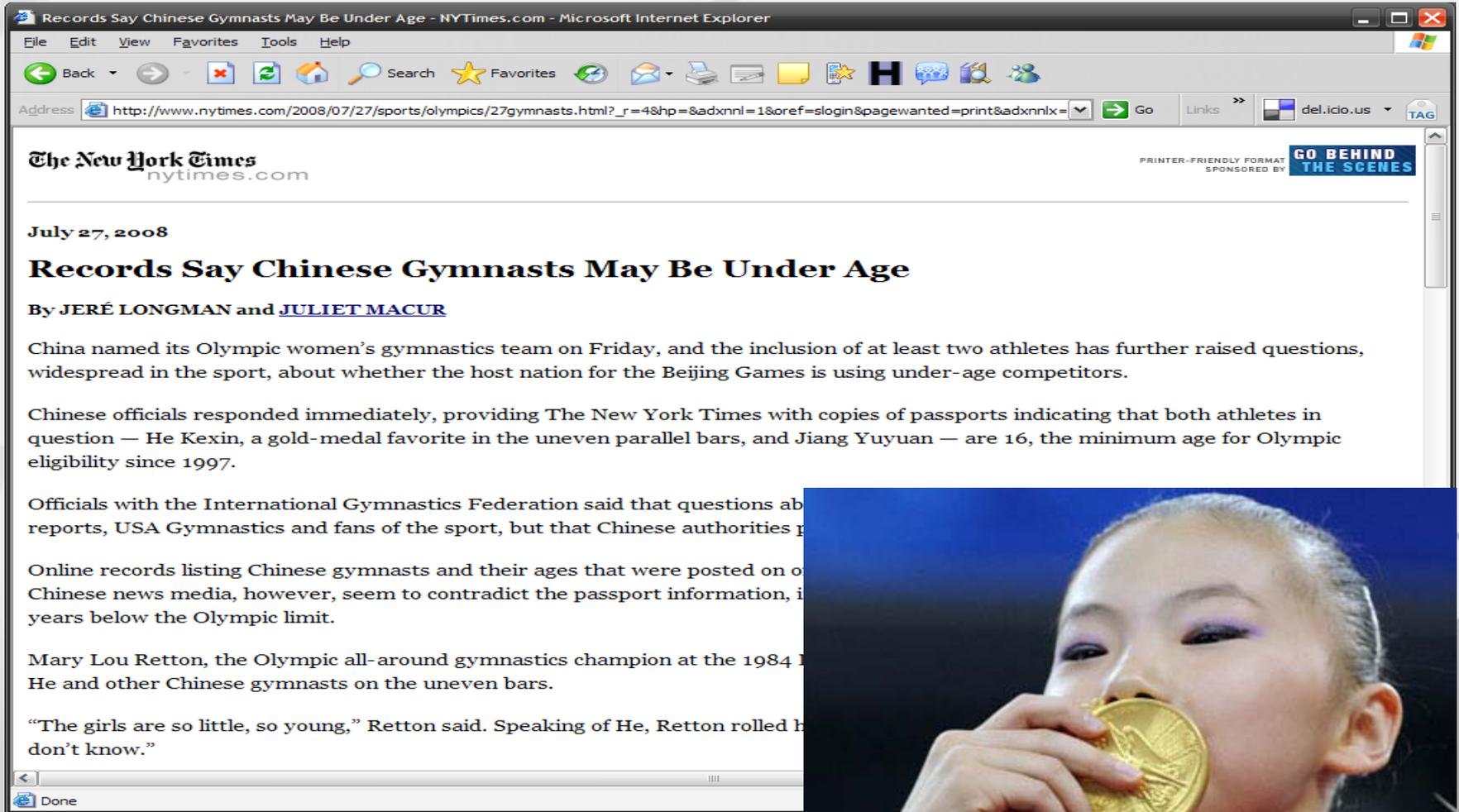
What It Boils Down To...

- 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 Forward Stop Home Search Favorites Refresh Mail Print Address Book Favorites H Chat Print

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 TAG

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 about the 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 -

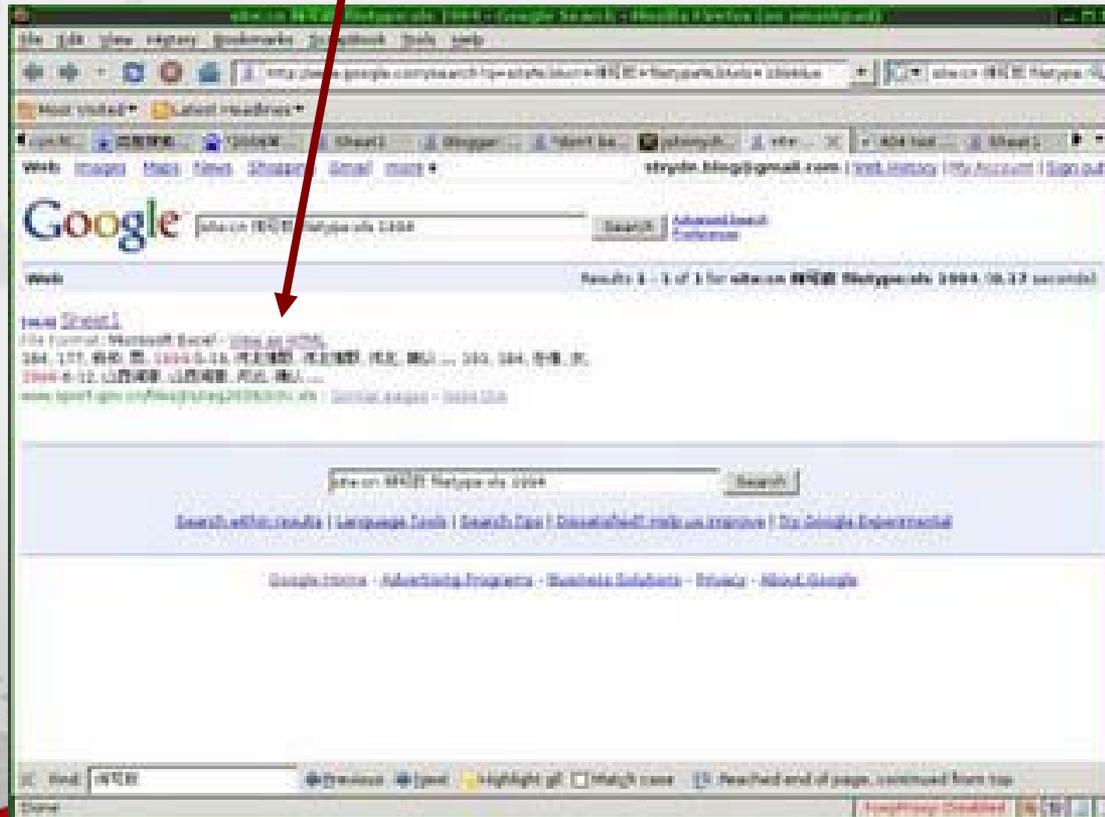
“site:cn 何可欣 filetype:xls 1994”

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



View as HTML

| No | Date | Time | Status | IP | Port | Country | City | ISP |
|-----|------|-------|--------|---------------|------|---------|-------------|------|
| 181 | 1/1 | 10:00 | 20 | 192.168.1.101 | 80 | USA | Los Angeles | AT&T |
| 182 | 1/1 | 10:00 | 20 | 192.168.1.101 | 80 | USA | Los Angeles | AT&T |
| 183 | 1/1 | 10:00 | 20 | 192.168.1.101 | 80 | USA | Los Angeles | AT&T |
| 184 | 1/1 | 10:00 | 20 | 192.168.1.101 | 80 | USA | Los Angeles | AT&T |
| 185 | 1/1 | 10:00 | 20 | 192.168.1.101 | 80 | USA | Los Angeles | AT&T |
| 186 | 1/1 | 10:00 | 20 | 192.168.1.101 | 80 | USA | Los Angeles | AT&T |
| 187 | 1/1 | 10:00 | 20 | 192.168.1.101 | 80 | USA | Los Angeles | AT&T |
| 188 | 1/1 | 10:00 | 20 | 192.168.1.101 | 80 | USA | Los Angeles | AT&T |
| 189 | 1/1 | 10:00 | 20 | 192.168.1.101 | 80 | USA | Los Angeles | AT&T |
| 190 | 1/1 | 10:00 | 20 | 192.168.1.101 | 80 | USA | Los Angeles | AT&T |
| 191 | 1/1 | 10:00 | 20 | 192.168.1.101 | 80 | USA | Los Angeles | AT&T |
| 192 | 1/1 | 10:00 | 20 | 192.168.1.101 | 80 | USA | Los Angeles | AT&T |
| 193 | 1/1 | 10:00 | 20 | 192.168.1.101 | 80 | USA | Los Angeles | AT&T |
| 194 | 1/1 | 10:00 | 20 | 192.168.1.101 | 80 | USA | Los Angeles | AT&T |
| 195 | 1/1 | 10:00 | 20 | 192.168.1.101 | 80 | USA | Los Angeles | AT&T |
| 196 | 1/1 | 10:00 | 20 | 192.168.1.101 | 80 | USA | Los Angeles | AT&T |
| 197 | 1/1 | 10:00 | 20 | 192.168.1.101 | 80 | USA | Los Angeles | AT&T |
| 198 | 1/1 | 10:00 | 20 | 192.168.1.101 | 80 | USA | Los Angeles | AT&T |
| 199 | 1/1 | 10:00 | 20 | 192.168.1.101 | 80 | USA | Los Angeles | AT&T |
| 200 | 1/1 | 10:00 | 20 | 192.168.1.101 | 80 | USA | Los Angeles | AT&T |
| 201 | 1/1 | 10:00 | 20 | 192.168.1.101 | 80 | USA | Los Angeles | AT&T |
| 202 | 1/1 | 10:00 | 20 | 192.168.1.101 | 80 | USA | Los Angeles | AT&T |
| 203 | 1/1 | 10:00 | 20 | 192.168.1.101 | 80 | USA | Los Angeles | AT&T |
| 204 | 1/1 | 10:00 | 20 | 192.168.1.101 | 80 | USA | Los Angeles | AT&T |

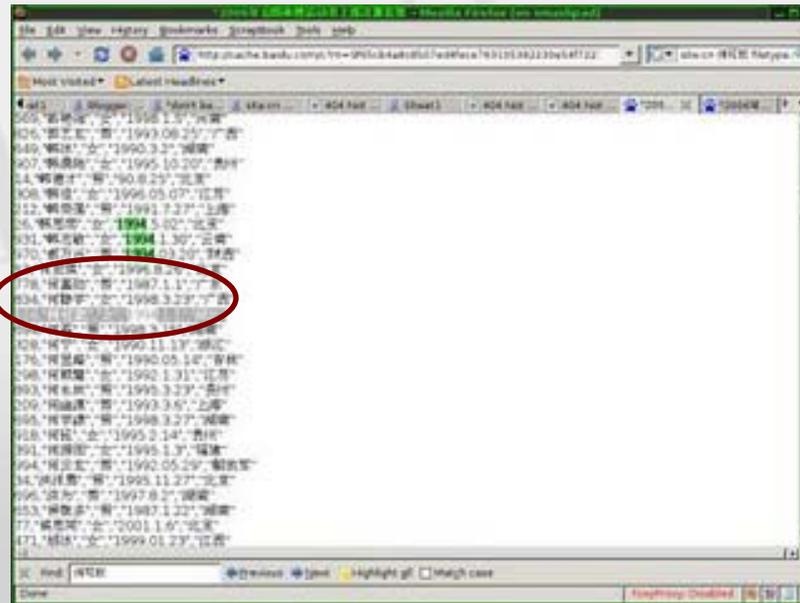
No He Kexin still ...

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

File Edit View History Delicious Bookmarks Tools Help

http://digg.com/olympics/Stryde_Hax_Hack_the_Olympics

Google

digg My Profile Friends' Activity 0 Submit New Logout Search Digg...

All Technology World & Business Science Gaming Lifestyle Entertainment Sports Offbeat

Popular Upcoming BETA All News Videos Images Podcasts Customize

intel STYLE THAT TAKES YOU PLACES THE INSPIRON 1525 Do More

All » Sports » Olympics

2967 diggs

Stryde Hax: Hack the Olympics!

strydehax.blogspot.com — There's been some widely publicized controversy regarding the competition age of the Chinese women's gymnastics team recently. I have an Internet connection, that means I should be able to verify the age of the gymnasts in quest with primary state-issued documents and find out for myself if someone's cheating, right? Right. Let's go to work.

Share

316 Comments

expand all only mine

higB on 08/19/2008

strydehax on 08/20/2008

Caligatio on 08/20/2008

http://clk.atdmt.com/goiframe/500

Slashdot | Hacker Uncovers Chinese Olympic Fraud - Mozilla Firefox

File Edit View History Delicious Bookmarks Tools Help

http://yro.slashdot.org/yro/08/08/20/

Slashdot NEWS FOR NERDS. STUFF THAT MATTERS.

Log In Create Account Help Subscribe Firehose Why

Sections

Hacker Uncovers Chinese Olympic Fraud

Posted by [CmdrTaco](#) on Wednesday August 20, @09:48AM from the [that's-a-helluva-home-court-advantage](#) dept.

SkeptOlympics writes

"A new chapter in the [ongoing controversy](#) surrounding China's women's gymnastics team opened today, as search engine hacker [stryde.hax](#) found surviving [copies of official registration documents](#) issued by China's [General Administration of Sport of China](#). The incriminating documents, expunged by censors from the official site and from Google's document cache, still appear in the document translation cache of Chinese search giant Baidu, [here \(1\)](#) and [here \(2\)](#), showing the age of one of China's gold medal winning gymnasts to be 14 instead of 16, the minimum age for competition presented on her government-issued passport. Now that official government documentation is available, how long will

ars technica the art of technology

Main Business IT Apple Gaming Hardware Gear & Gadgets

servercentral Colocation and network services provided by ServerCentral

KIT Ars Technica's Journal devoted to the hardware scene.

Report indicates AMD mulling its options

Mini-Note beware: gigabyte releases 9" Tablet... undefined

Energy-Efficient Server Rights Web Services

Home News Articles Guides Journals Search GO Forum

From the News Desk

Baidu cache offers more evidence of underage Chinese gymnasts

By [Joel Hruska](#) | Published: August 20, 2008 - 01:05PM CT

One of the controversies that's been swirling around the Chinese Olympic Games since they began is the age of several of China's gymnasts. According to Chinese officials (and, of course, official passports and ID cards), both He Kexin and Jiang Yuyuan are 16, and therefore old enough to compete in the Olympic Games.

Beijing 2008

intel In-depth

Transferring data from ytaahg.vo.llnwd.net.

om pagead2.googleadservices.com...

Thursday....

The image shows a screenshot of a Skype chat window titled "mike z (Do Not Disturb) Skype™ Chat". The chat history includes the following messages:

- 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

Below the messages, there is a system message: "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."

The chat interface includes a search bar with "Down" entered, and options for "Find Next", "Find Previous", and "Match case". There are also buttons for "Emoticons", "Videos", and "Set Font". At the bottom left, it shows a green checkmark and the word "Online".

On the right side of the chat window, there is a profile card for "mike z" with a profile picture of a woman and a "Menu" button.

In the bottom right corner, there is an inset photograph of a man sitting at a desk, working on a laptop. The desk is cluttered with various items, including a coffee mug, a water bottle, and a laptop.

Then to world news...



Friday Started at 5am

- IOC reopens investigation



Where's Waldo..err Arnold

<http://twitter.com/schwarzenegger>



Start my day.

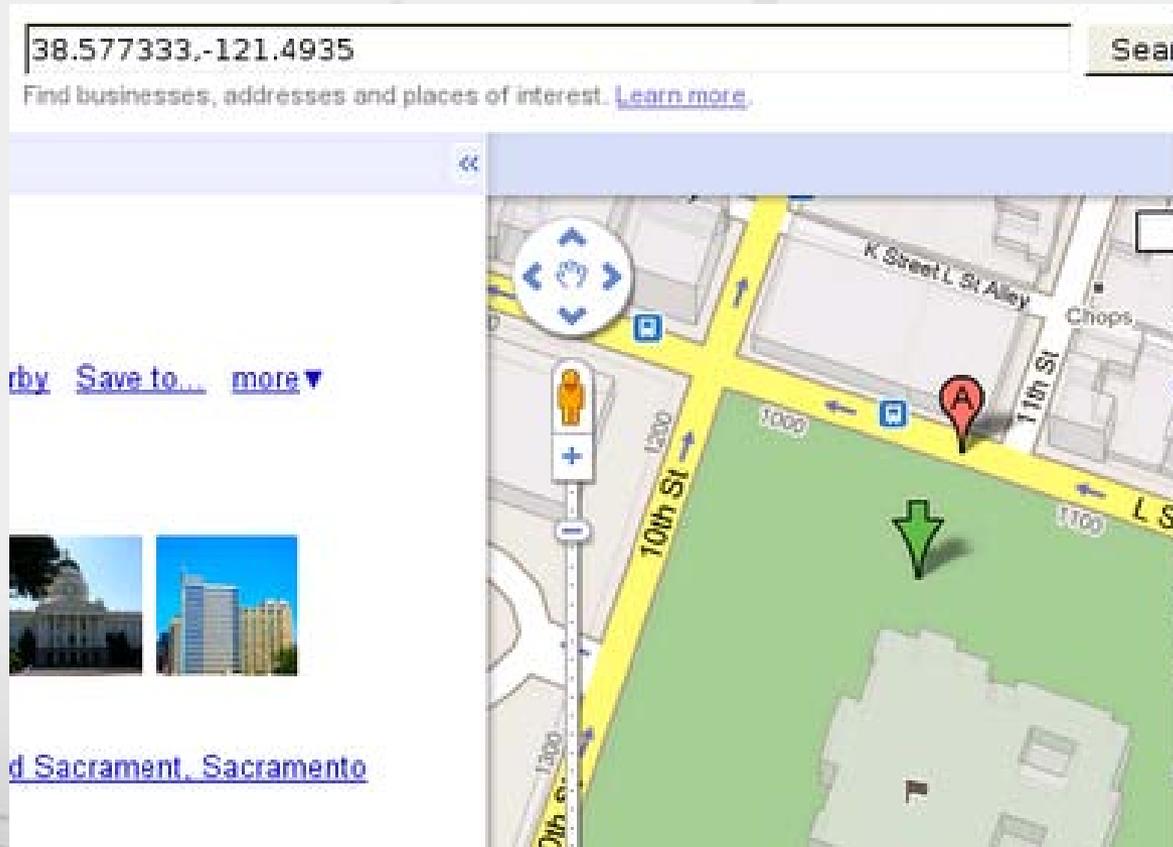
More photos by schwarzenegger



[Put this photo on your website](#)

Views: 7d (11)

Breakfast at the Capitol..



Conclusion



Q&A



Rohyt Belani, CEO Intrepidus Group

Rohyt.Belani@IntrepidusGroup.com

