



# Update on Anti-Phishing Alliance of China

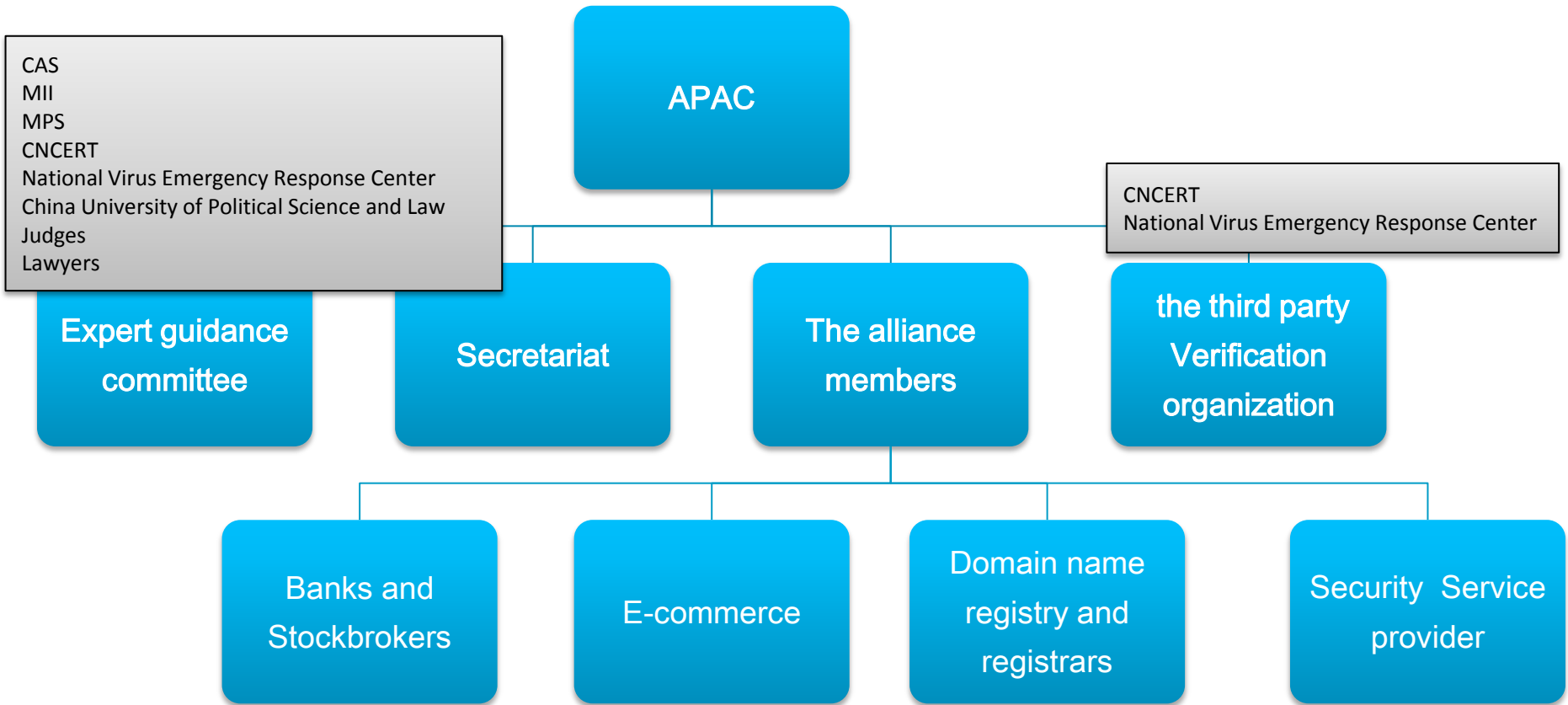
Tan Yaling

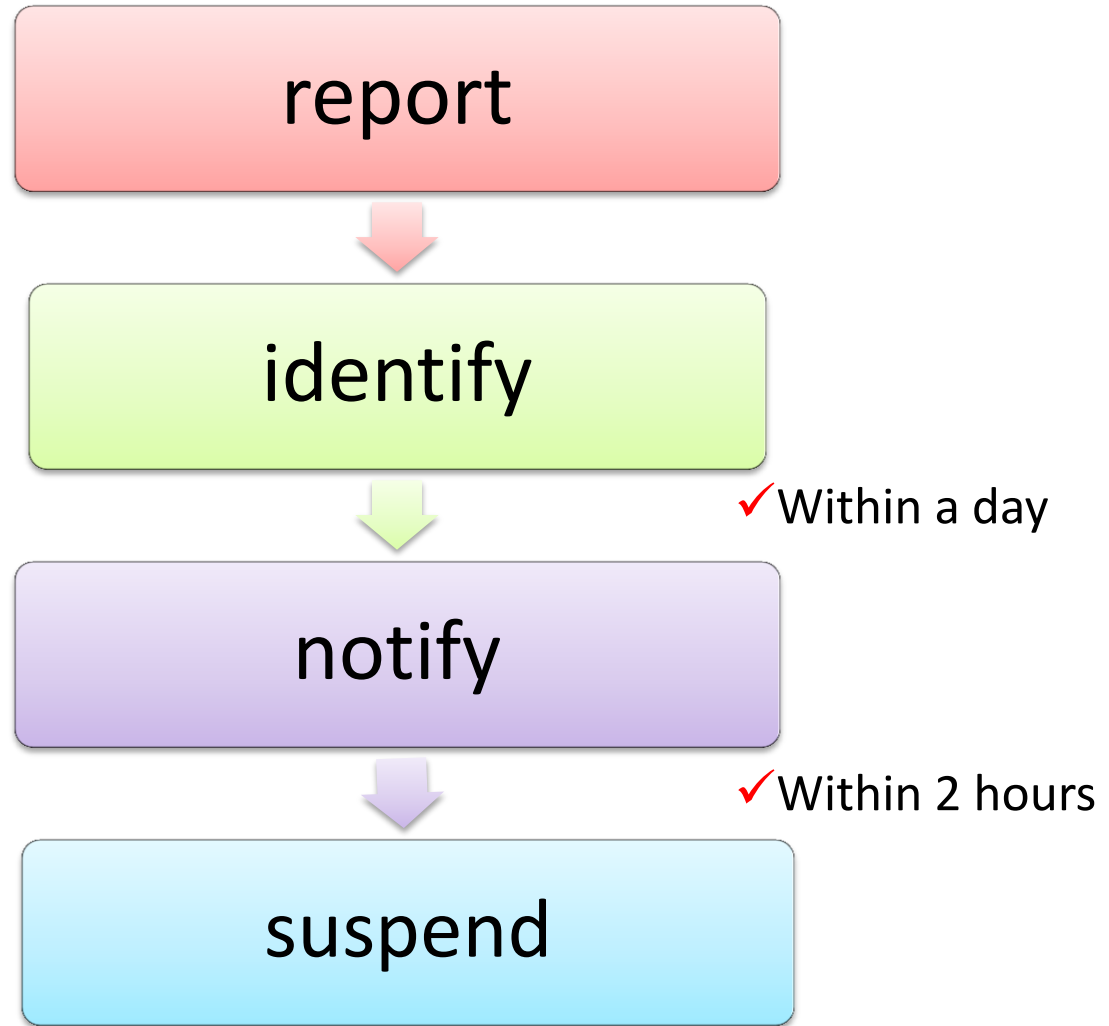
For APTLD Jordan Meeting

Oct, 2010

- founded on July, 2008
- 143 members
- the only one dedicated to tackling phishing problems
- a fast phishing domain names suspension process
- The secretariat at CNNIC.

# the organization structure of APAC





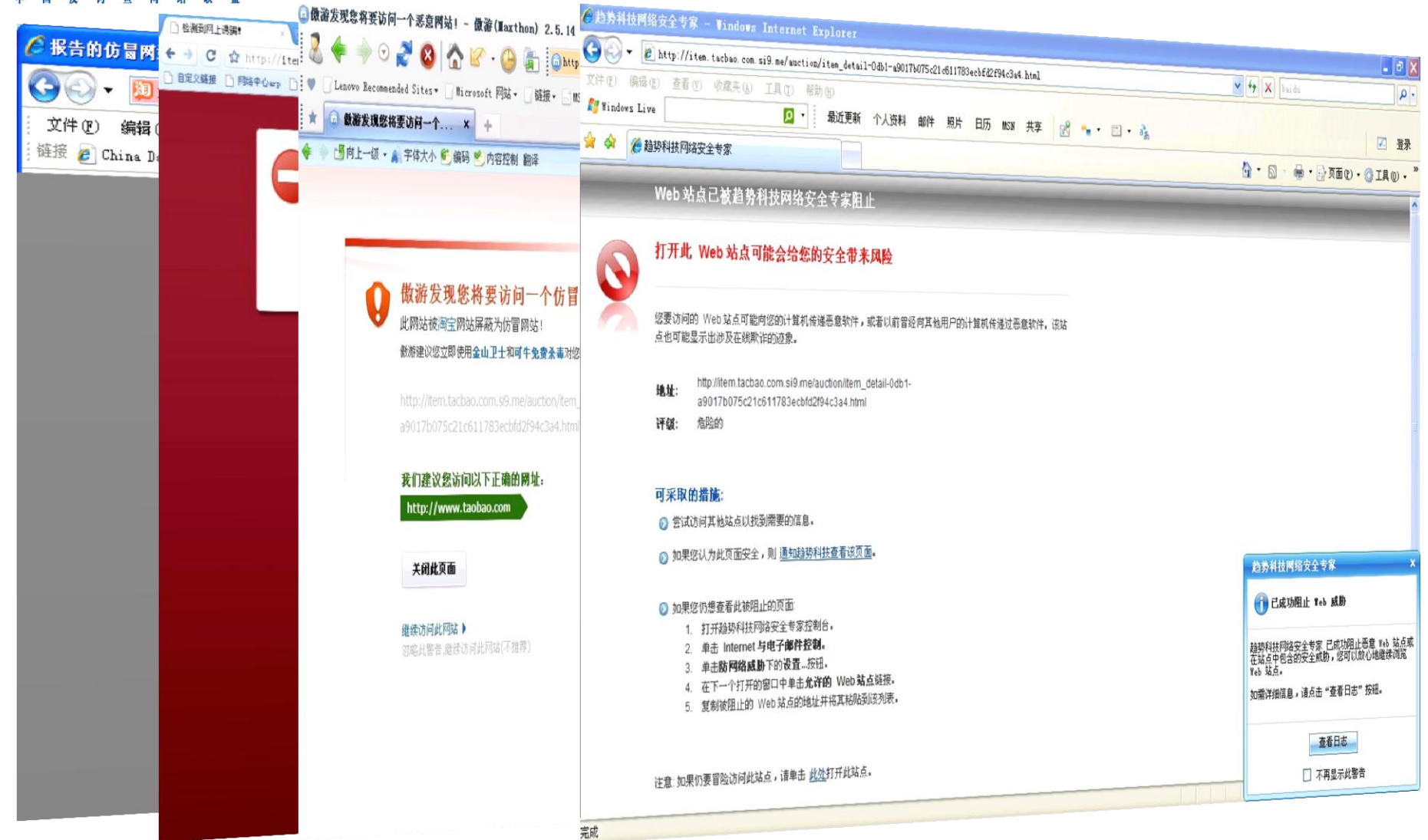


趋势科技



MarkMonitor®





# Phishing on Beijing Olympic Games

[Official:www.tickets.beijing2008.cn](http://www.tickets.beijing2008.cn)



[Phishing:www.beijing-tickets2008.com](http://www.beijing-tickets2008.com)  
[Phishing:www.beijingticketing.com](http://www.beijingticketing.com)  
More than 50 million USD.



- ◆ Both Wenchuan earthquake in 2008 and Yushu earthquake in 2010 become targets of phishing attacks.
- ◆ Emergency provides good chance for phishers.
- ◆ The examples of Phishing URL
  - ◆ <http://cctv-t2.com/jk/index.htm>
  - ◆ <http://jk.ez.to>
  - ◆ <http://www.688tx.com/>
  - ◆ <http://www.qq.com.indexq.cn/news/news.qq.com/a/20080512/index.htm>
- ◆ CNNIC checked the other domains which were registered by the registrant of indexq.cn. Fortunately, none of the rest domains are used for phishing.

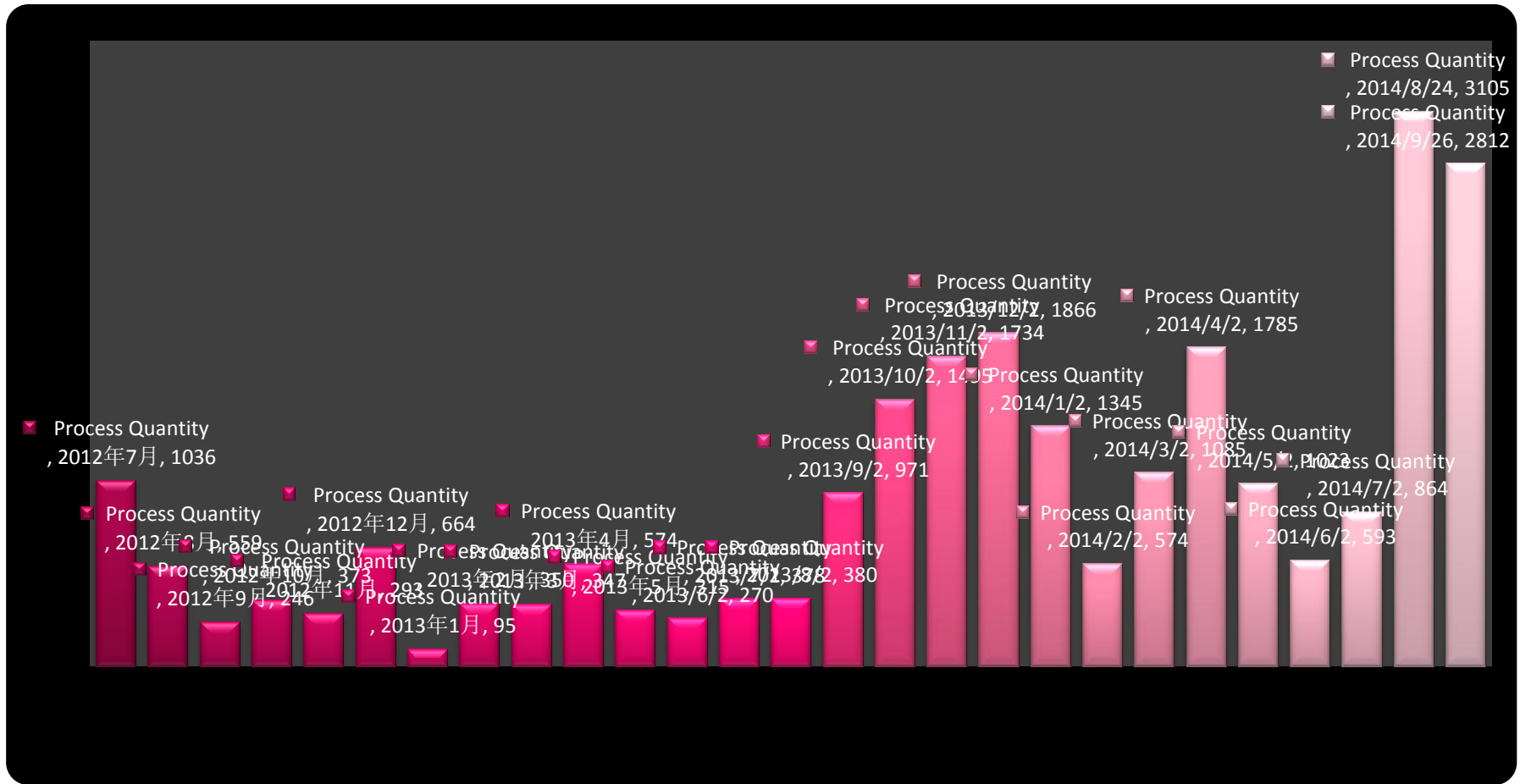
11 Jan, 2010

1. Hacker starts online chat session with Register.com representative, claiming to be an agent of Baidu.
2. Register.com representative asks hacker to provide verification information. Hacker provides invalid information, but Register.com goes ahead and e-mails a security code to the email address it has on file for Baidu anyway.
3. The hacker doesn't have access to that e-mail address, so he/she relays a bogus security code to the Register.com representative via chat. Baidu claims the representative didn't bother to compare the code to the actual one.
4. Hacker asks Register.com representative to change email address on file to antiwahabi2008@gmail.com, and representative does.
5. Hacker now uses "forgot password" link at Register.com to request the username and password to the account. Hacker can then log in and change the name servers.

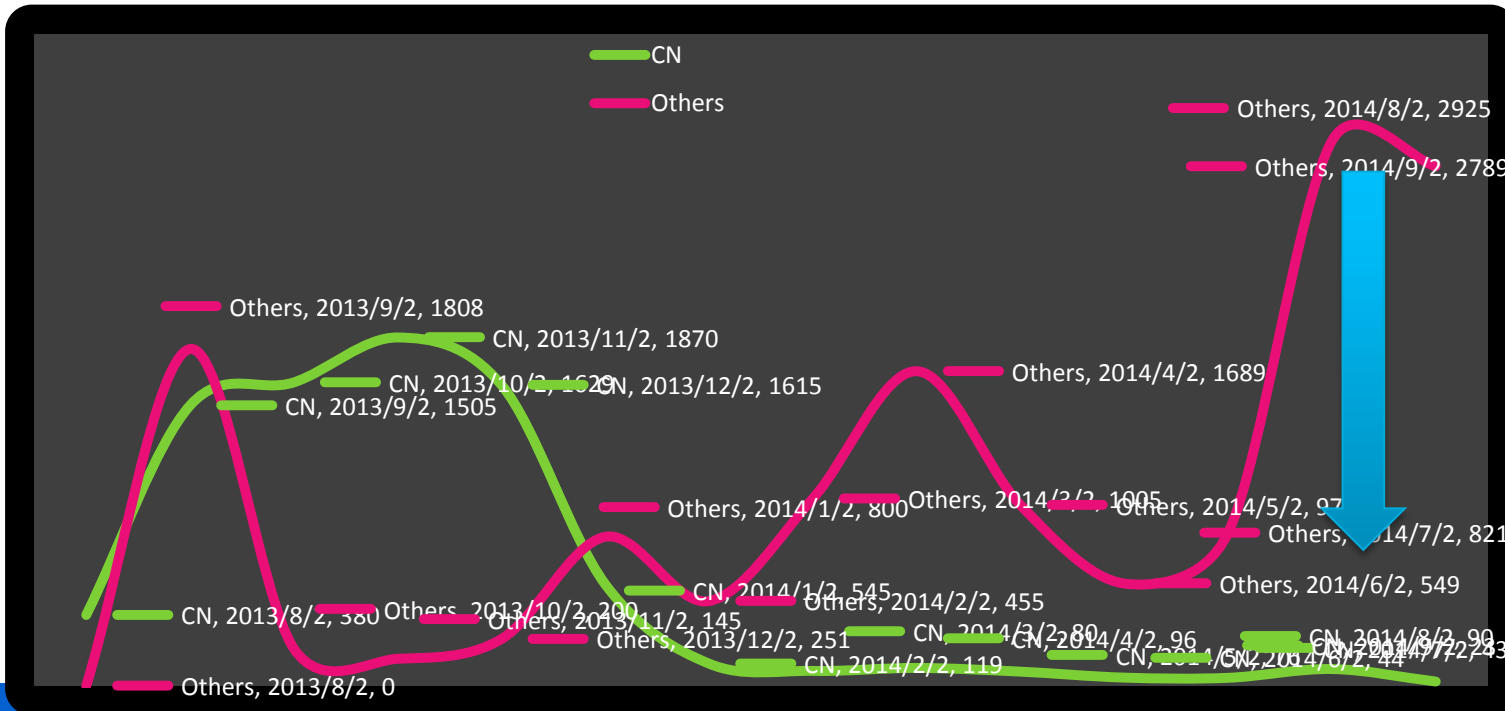
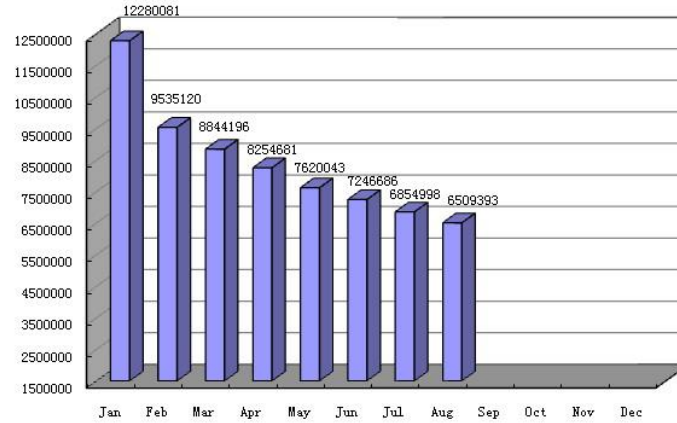
In CNNIC, we asked the VIP customer to provide paper documentation to change the information.



By September 2010, APAC has handled 25132 phishing cases.



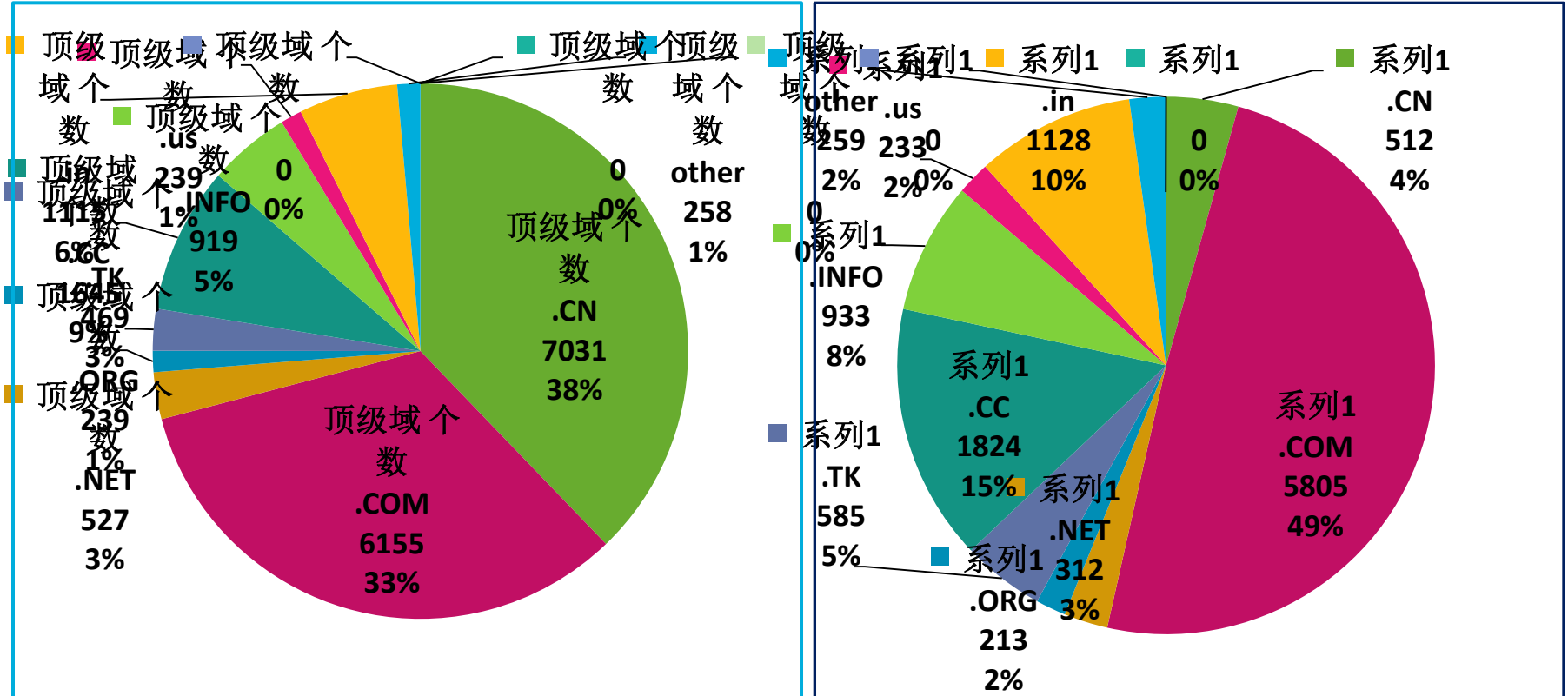
# The trend of phishing under CN domain



# The distribution of phishing in each domains

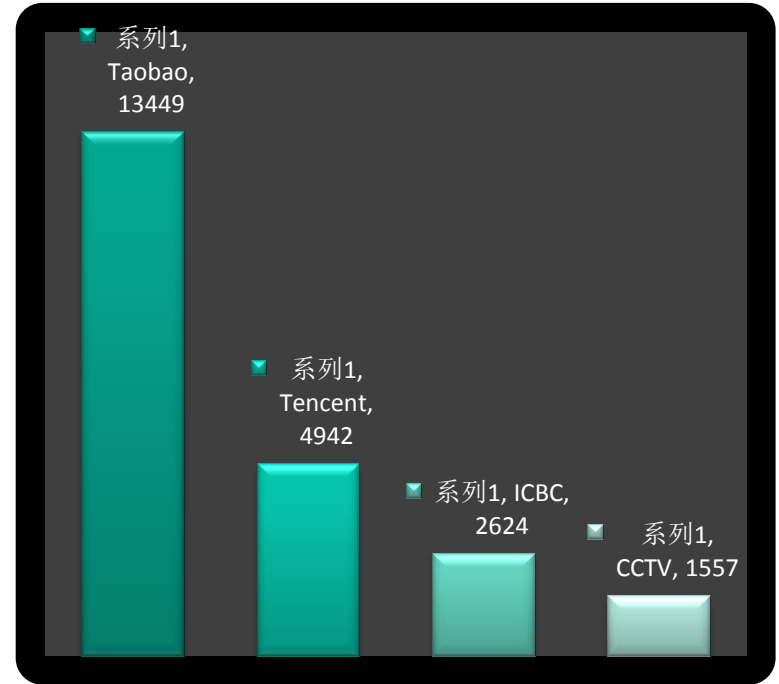
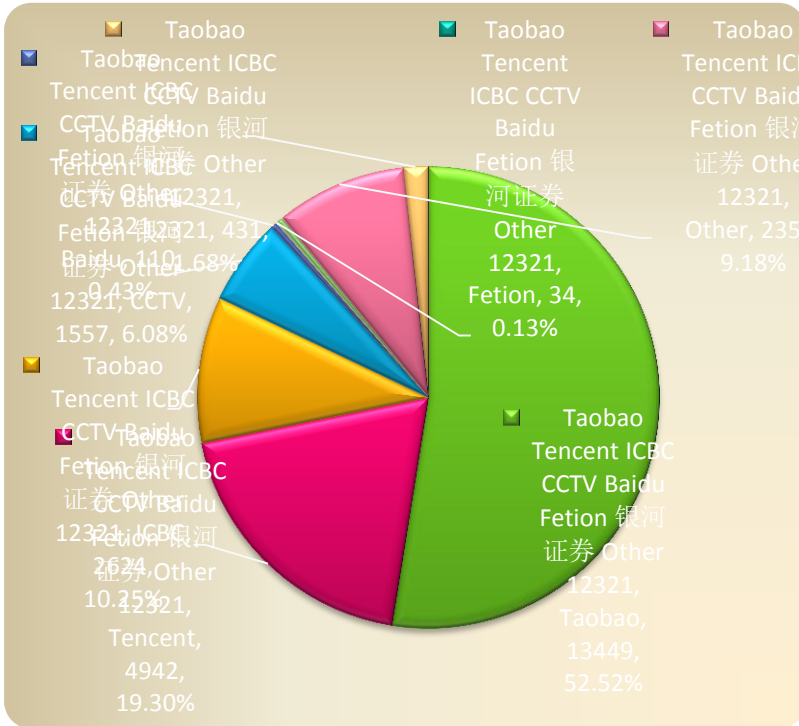
2008-2009

2010-



# The statistics of Phishing in China

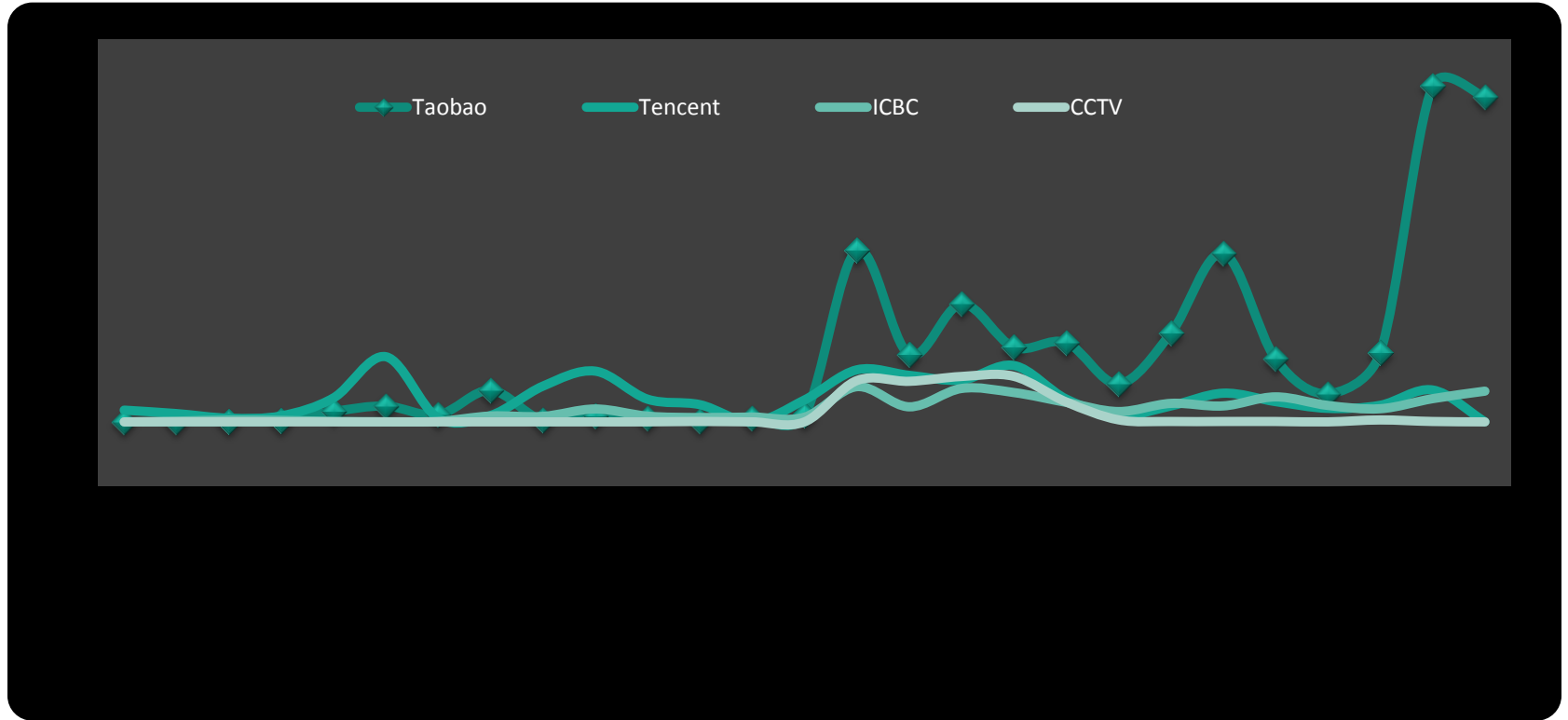
E-commerce sites are main targets of phishing attack in China



Taobao, biggest e-commerce company in China, 200 million users, annual business transaction is over 30 billion USD.

Tencent, biggest instant message service provider in china, more than 500 million active users, 100 million online at the same time.

# The trend of phishing on each target



## ■ Domain Name similarity detection

➤ *Taobao.com VS Toobao.com*

## ■ CDN similarity detection

➤ *康师傅.中国 VS 康帅博.中国*

## ■ Heuristic analysis in websites' content

➤ Detect web pages' landing box

➤ Verify the website's claimed Identity

➤ copyright、ICP、search ranking、whois、...

➤ Analyze websites' internal and external links

## How to report phishing attack?

Personal Report Email : [anti-phishing@apac.cn](mailto:anti-phishing@apac.cn)

The Alliance member Report Email : [fdy@apac.cn](mailto:fdy@apac.cn)

Report Phone : 010-58813000

Report Platform : [jubao.apac.cn](http://jubao.apac.cn)

权威、专业、公益、共享

Haidian District, NO.4,Zhongguancun South Street, Beijing ,CAS Software Park

**Code** : 100190

[www.apac.cn](http://www.apac.cn)