Update on Anti-Phishing Alliance of China

Tan Yaling

For APTLD Jordan Meeting

Oct, 2010
Overview

• 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

Expert guidance committee

Secretariat

The alliance members

the third party Verification organization

Banks and Stockbrokers

E-commerce

Domain name registry and registrars

Security Service provider

CAS
MII
MPS
CNCERT
National Virus Emergency Response Center
China University of Political Science and Law
Judges
Lawyers

CNCERT
National Virus Emergency Response Center

China University of Political Science and Law
Judges
Lawyers
The Mechanism of APAC

1. Report
2. Identify
   - Within a day
3. Notify
   - Within 2 hours
4. Suspend

The diagram outlines the process flow of the APAC mechanism, starting with the report, followed by identification and notification, culminating in suspension. Each step is accompanied by a time frame for completion.
The examples for browser blocking tips
Phishing on Beijing Olympic Games

Official: www.tickets.beijing2008.cn

Phishing: www.beijing-tickets2008.com
Phishing: www.beijingticketing.com

More than 50 million USD.
Phishing on Donation websites

◆ 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/

◆ 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.
The trend of phishing reports in APAC

By September 2010, APAC has handled 25132 phishing cases.

Process Quantity, 2012年7月, 1036
Process Quantity, 2012年8月, 558
Process Quantity, 2012年9月, 246
Process Quantity, 2012年10月, 95
Process Quantity, 2012年11月, 203
Process Quantity, 2012年12月, 664
Process Quantity, 2013年1月, 95
Process Quantity, 2013年2月, 114
Process Quantity, 2013年3月, 380
Process Quantity, 2013年4月, 574
Process Quantity, 2013年5月, 315
Process Quantity, 2013年6月, 270
Process Quantity, 2013年7月, 246
Process Quantity, 2013年8月, 359
Process Quantity, 2013年9月, 971
Process Quantity, 2013年10月, 1866
Process Quantity, 2013年11月, 1734
Process Quantity, 2013年12月, 1345
Process Quantity, 2014年1月, 1385
Process Quantity, 2014年2月, 574
Process Quantity, 2014年3月, 1785
Process Quantity, 2014年4月, 1022
Process Quantity, 2014年5月, 3105
Process Quantity, 2014年6月, 3022
Process Quantity, 2014年7月, 864
Process Quantity, 2014年8月, 2812
Process Quantity, 2014年9月, 1866
Process Quantity, 2014年10月, 1495
Process Quantity, 2014年11月, 1734
Process Quantity, 2014年12月, 1866
Process Quantity, 2015年1月, 1345
Process Quantity, 2015年2月, 574
Process Quantity, 2015年3月, 1085
Process Quantity, 2015年4月, 1785
Process Quantity, 2015年5月, 1022
Process Quantity, 2015年6月, 593
Process Quantity, 2015年7月, 864
Process Quantity, 2015年8月, 2812
The trend of phishing under CN domain

[Bar chart showing the trend of phishing under CN domain from January 2013 to December 2014, with data points for CN and Others categories for each month.

- CN: 2013/8/2, 380; 2013/9/2, 1505; 2013/10/2, 1629; 2013/11/2, 1870; 2013/12/2, 1615; 2014/1/2, 545; 2014/2/2, 80; 2014/3/2, 80; 2014/4/2, 1689; 2014/5/2, 97; 2014/6/2, 549; 2014/7/2, 821; 2014/8/2, 2925; 2014/9/2, 2789.

- Others: 2013/8/2, 0; 2013/9/2, 1808; 2013/10/2, 1620; 2013/11/2, 145; 2013/12/2, 251; 2014/1/2, 800; 2014/2/2, 455; 2014/3/2, 1005; 2014/4/2, 970; 2014/5/2, 549; 2014/6/2, 821; 2014/7/2, 2789; 2014/8/2, 2925; 2014/9/2, 2789.

]
The distribution of phishing in each domains

2008-2009

顶级域个数
- .CN: 7031 (38%)
- .COM: 6155 (33%)
- .NET: 527 (3%)
- .ORG: 239 (1%)
- .TK: 469 (3%)
- .CC: 1645 (9%)
- .INFO: 919 (5%)
- .us: 239 (1%)
- other: 258 (1%)

2010-

顶级域个数
- .CN: 512 (4%)
- .COM: 5805 (49%)
- .NET: 312 (3%)
- .ORG: 213 (2%)
- .TK: 585 (5%)
- .CC: 1824 (15%)
- .INFO: 933 (8%)
- .us: 233 (2%)
- other: 259 (2%)
- 0 (0%)
- 0 (0%)
- 0 (0%)
- 0 (0%)

系列1
- .CN: 512
- .COM: 5805
- .NET: 312
- .ORG: 213
- .TK: 585
- .CC: 1824
- .INFO: 933
- .us: 233
- other: 259
- 0
- 0
- 0
- 0
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

- Taobao
- Tencent
- ICBC
- CCTV
Technical Research and Development

- 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

The Alliance member Report Email : fdy@apac.cn

Report Phone : 010-58813000

Report Platform : jubao.apac.cn