Improving Domain Names Utilization

Ning Kong

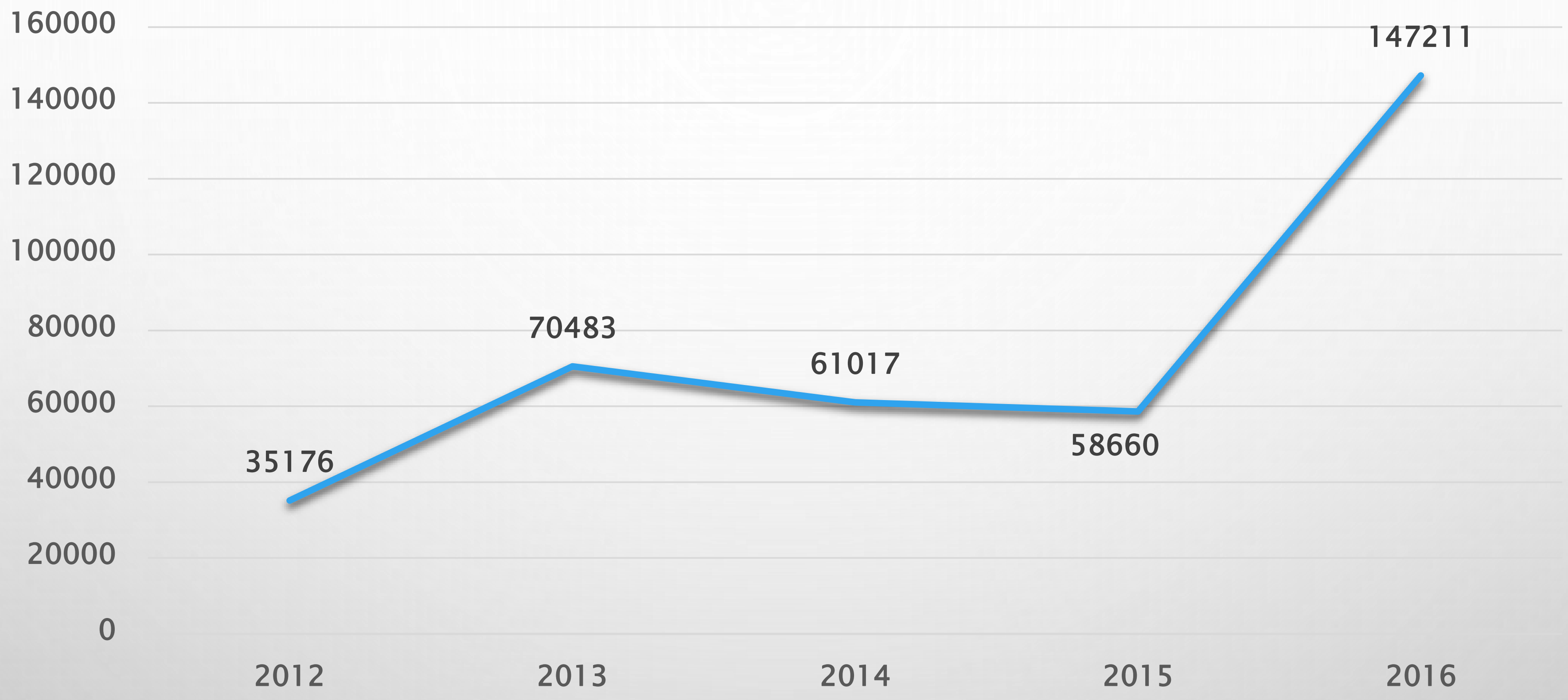
June 27, 2017

CNNIC
中国互联网络信息中心
CHINA INTERNET NETWORK INFORMATION CENTER

Content

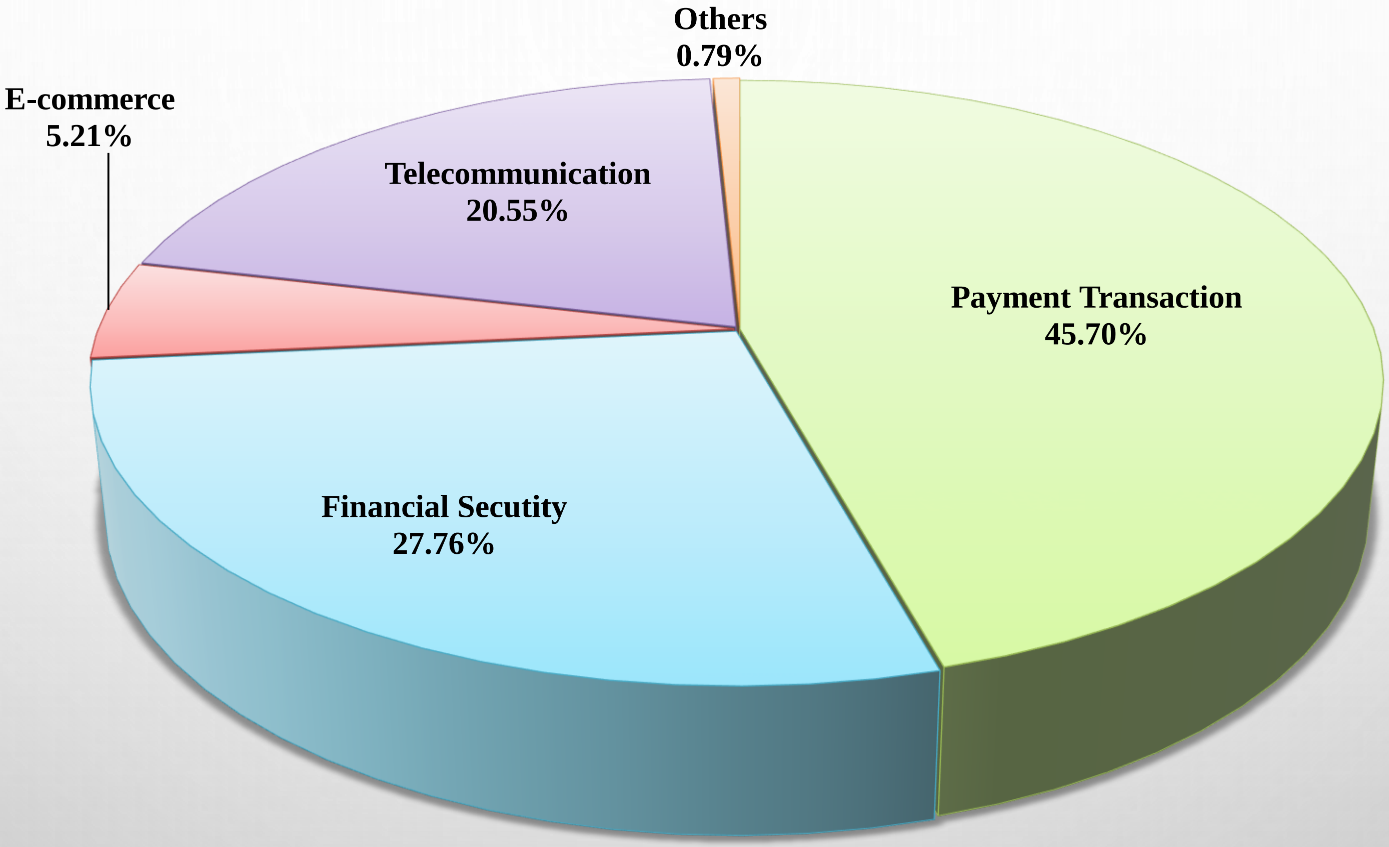
- Status Quo of Chinese Phishing Websites
- Anti-Phishing Alliance of China (APAC)
- Suggestions for Improving Domain Names Utilization
- Q & A

Status Quo of Chinese Phishing Websites



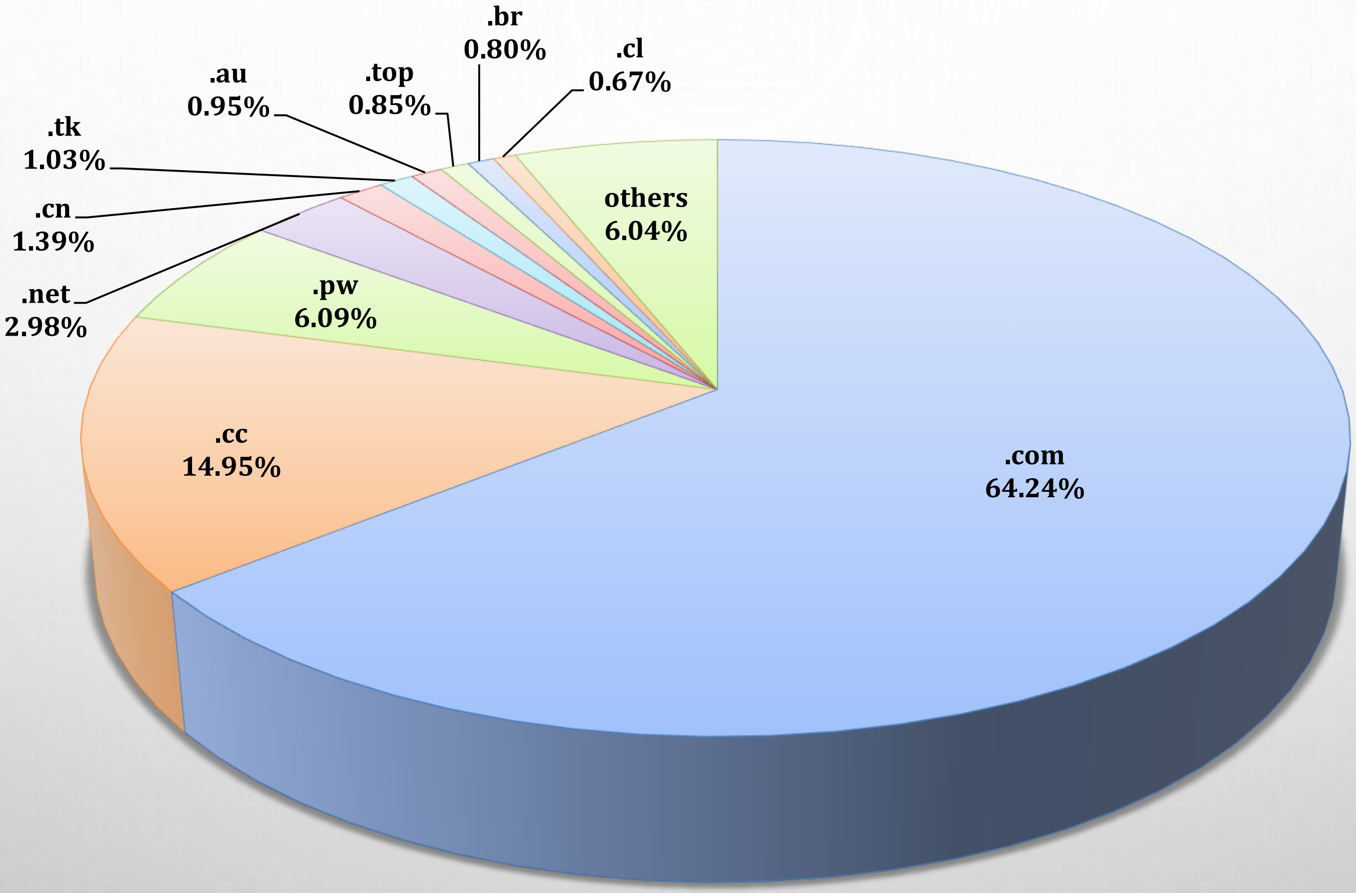
In 2016, The total amount of Chinese phishing websites is 147,211, which is 2.5 times bigger than that of 2015. Phishing attacks become more rampant and governance situation become more severe.

Status Quo of Chinese Phishing Websites



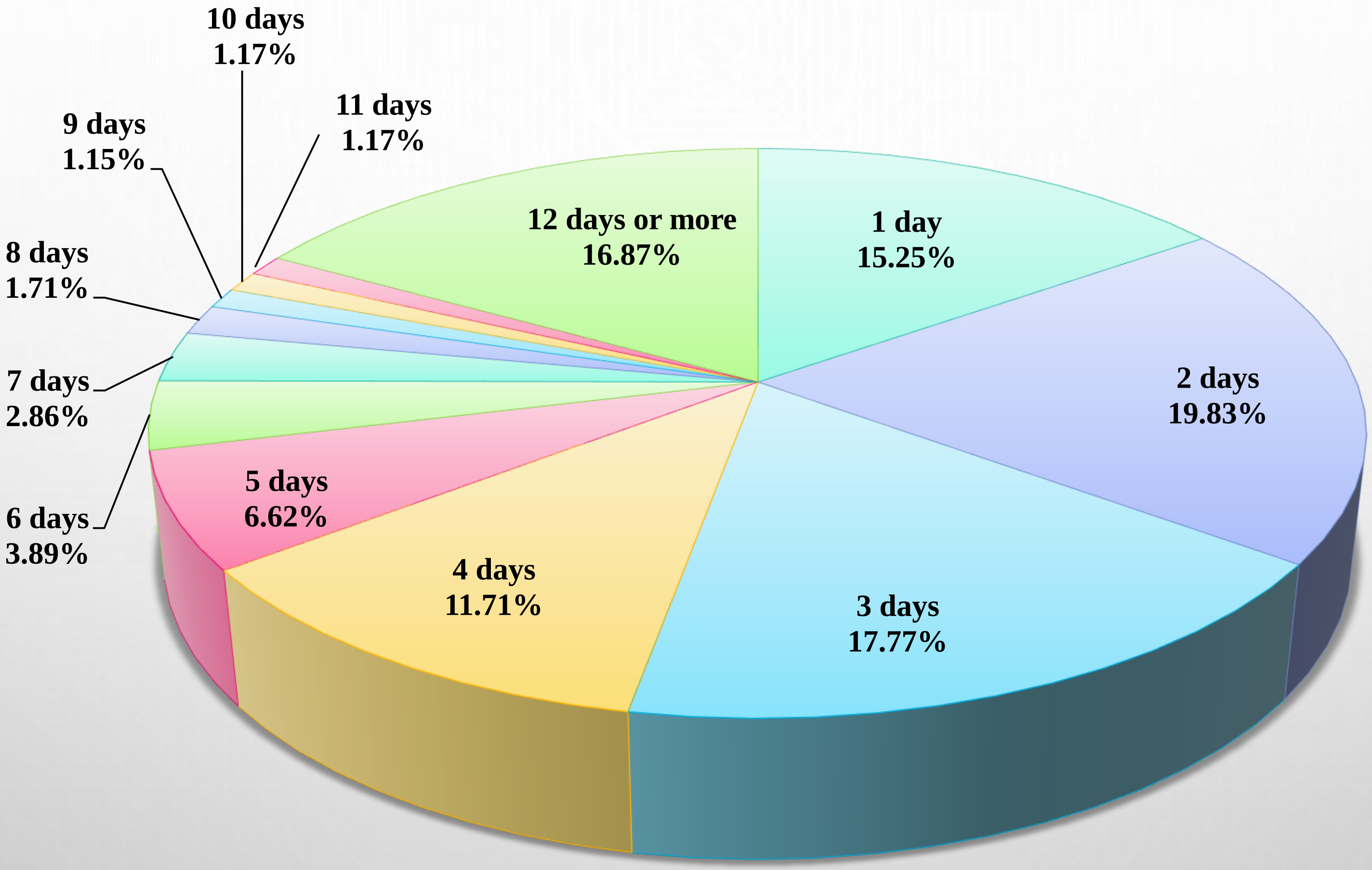
Distribution of Industries

Status Quo of Chinese Phishing Websites



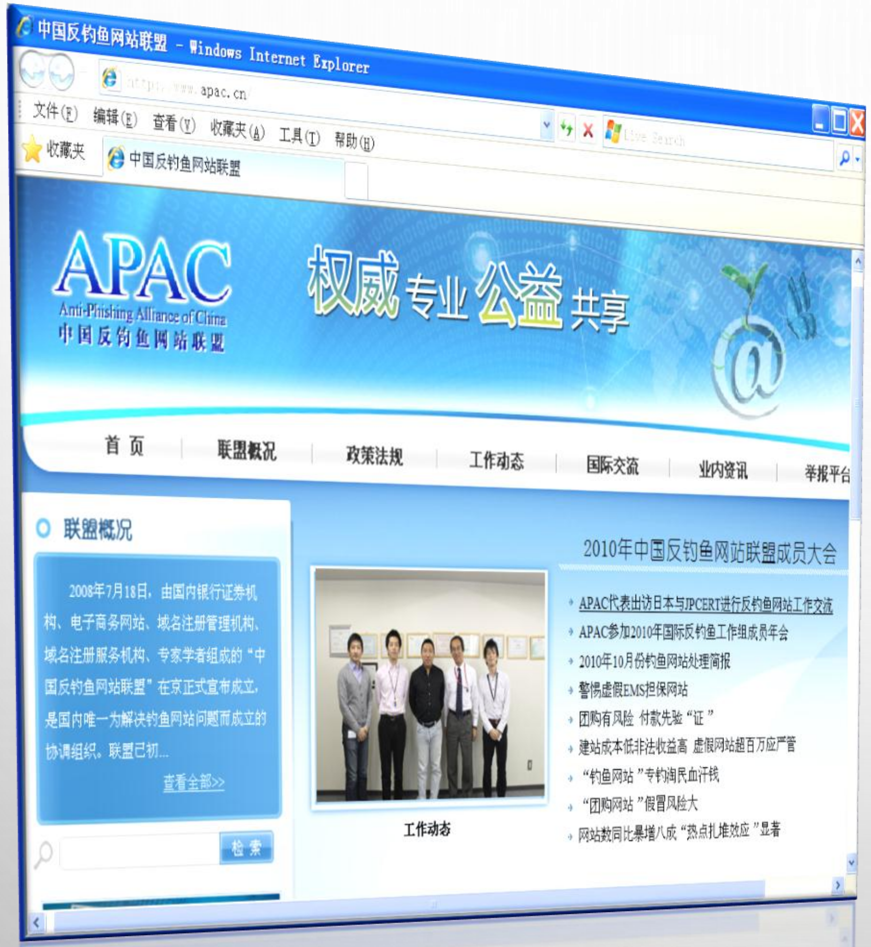
Distribution of TLDs

Status Quo of Chinese Phishing Websites



Distribution of Phishing Websites Life Duration

Anti-Phishing Alliance of China (APAC)



联盟概况

2008年7月18日，由国内银行证券机构、电子商务网站、域名注册管理机构、域名注册服务机构、专家学者组成的“中国反钓鱼网站联盟”在京正式宣布成立，是国内唯一为解决钓鱼网站问题而成立的协调组织。联盟已初...

查看全部>>

2010年中国反钓鱼网站联盟成员大会

- APAC代表出访日本与JPCERT进行反钓鱼网站工作交流
- APAC参加2010年国际反钓鱼工作组成员年会
- 2010年10月份钓鱼网站处理简报
- 警惕虚假EMS担保网站
- 团购有风险 付款先验“证”
- 建站成本低非法收益高 虚假网站超百万应严管
- “钓鱼网站”专钓淘民血汗钱
- “团购网站”假冒风险大
- 网站数同比暴增八成“热点扎堆效应”显著

- **Founded on July 18, 2008**
- **A nonprofit industry organization**
- **CNNIC assumes the duties of secretariat**
- **Official Website : www.apac.cn**
- **Reporting Email ： jubao@apac.cn**

APAC Members

APAC is mainly comprised of registries and registrars, financial agencies, e-commerce enterprises and cybersecurity companies. Up to the end of 2016, the number of APAC members increased to 523.

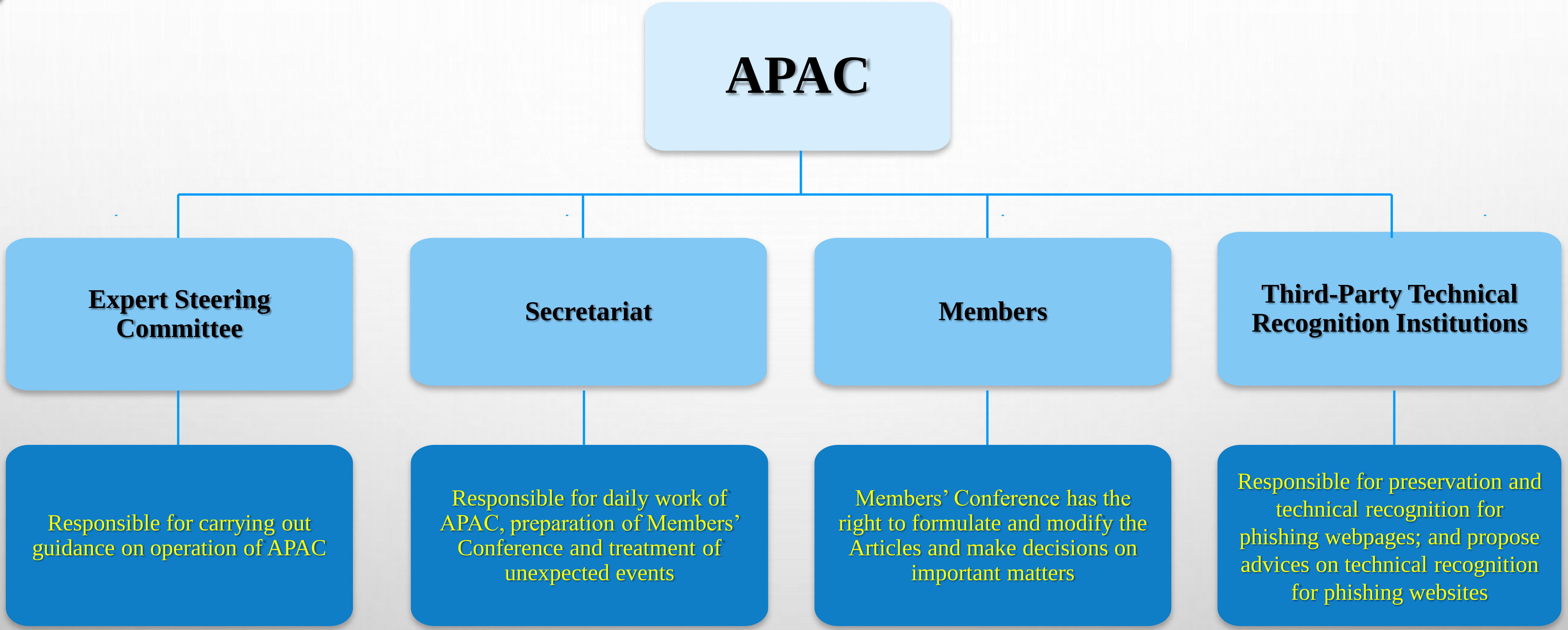
APAC Duties

Organize members in finding out, governing and preventing from phishing sites, share relevant information and promote construction of comprehensive governance system

Perform international exchange and cooperation concerning legislation research, technical application and standard formulation

Organize and carry out investigation and research on anti-phishing, provide relevant business and policy consultation services for members as well as offer decision support for government

APAC Architecture



APAC

Expert Steering Committee

Responsible for carrying out guidance on operation of APAC

Secretariat

Responsible for daily work of APAC, preparation of Members' Conference and treatment of unexpected events

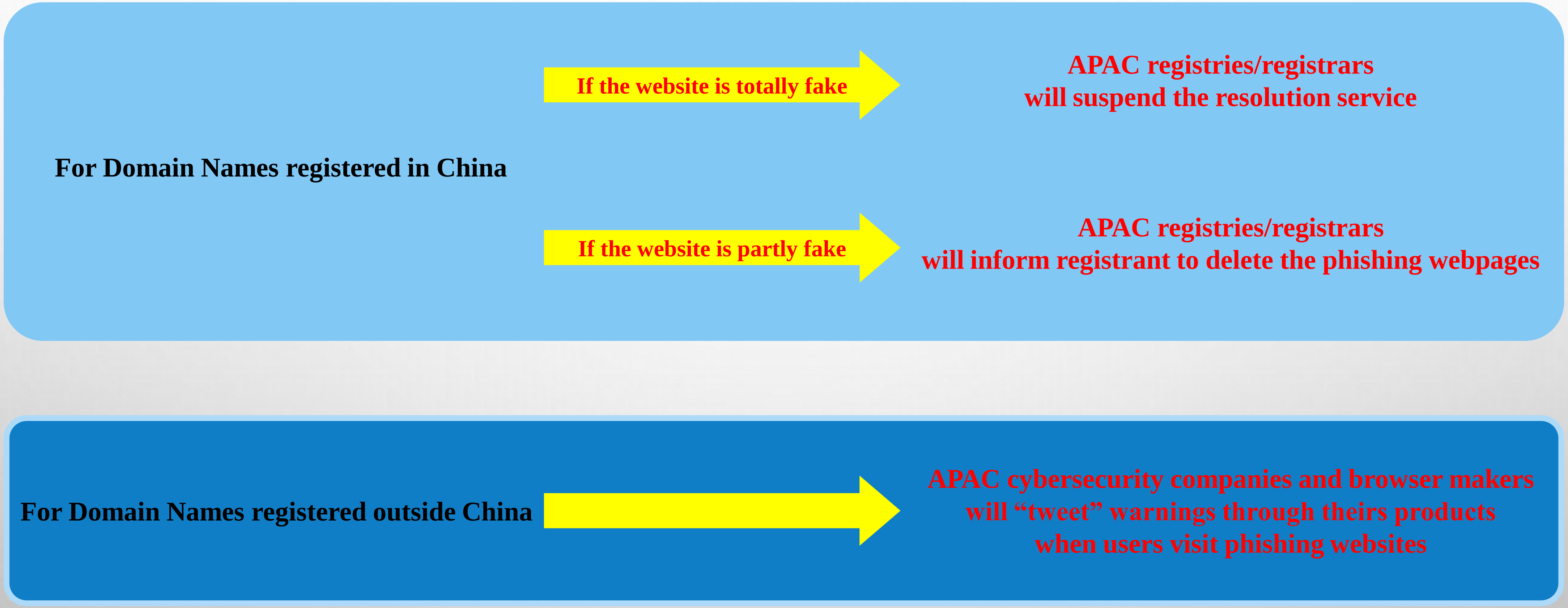
Members

Members' Conference has the right to formulate and modify the Articles and make decisions on important matters

Third-Party Technical Recognition Institutions

Responsible for preservation and technical recognition for phishing webpages; and propose advices on technical recognition for phishing websites

APAC Treatment Categories



For Domain Names registered in China

If the website is totally fake

APAC registries/registrars will suspend the resolution service

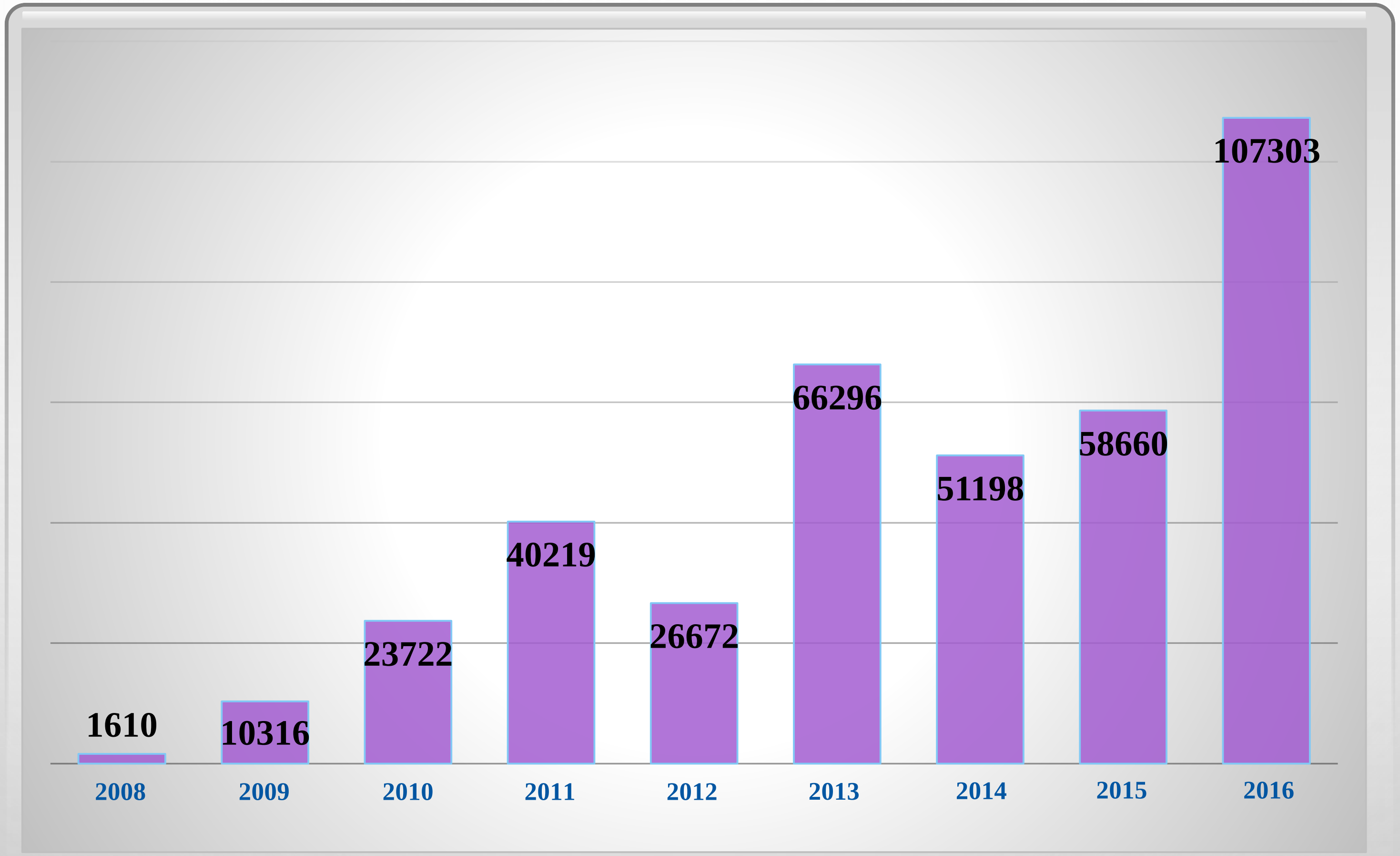
If the website is partly fake

APAC registries/registrars will inform registrant to delete the phishing webpages

For Domain Names registered outside China

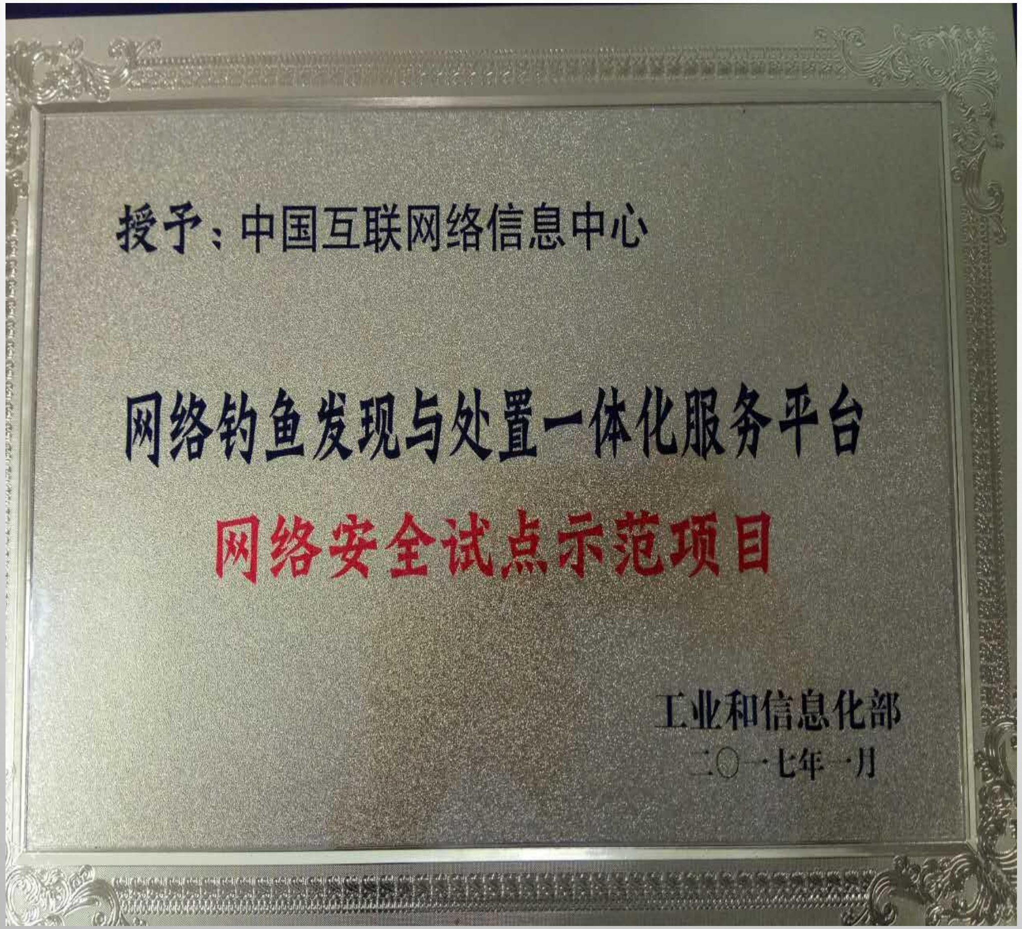
APAC cybersecurity companies and browser makers will “tweet” warnings through theirs products when users visit phishing websites

APAC Treatment Efficiency



In 2016, the APAC has identified and processed a total of 107,303 phishing websites, accumulatively up to 385,996.

CNNIC’s Contributions---Proactive Phishing Detection System



授予：中国互联网络信息中心

网络钓鱼发现与处置一体化服务平台

网络安全试点示范项目

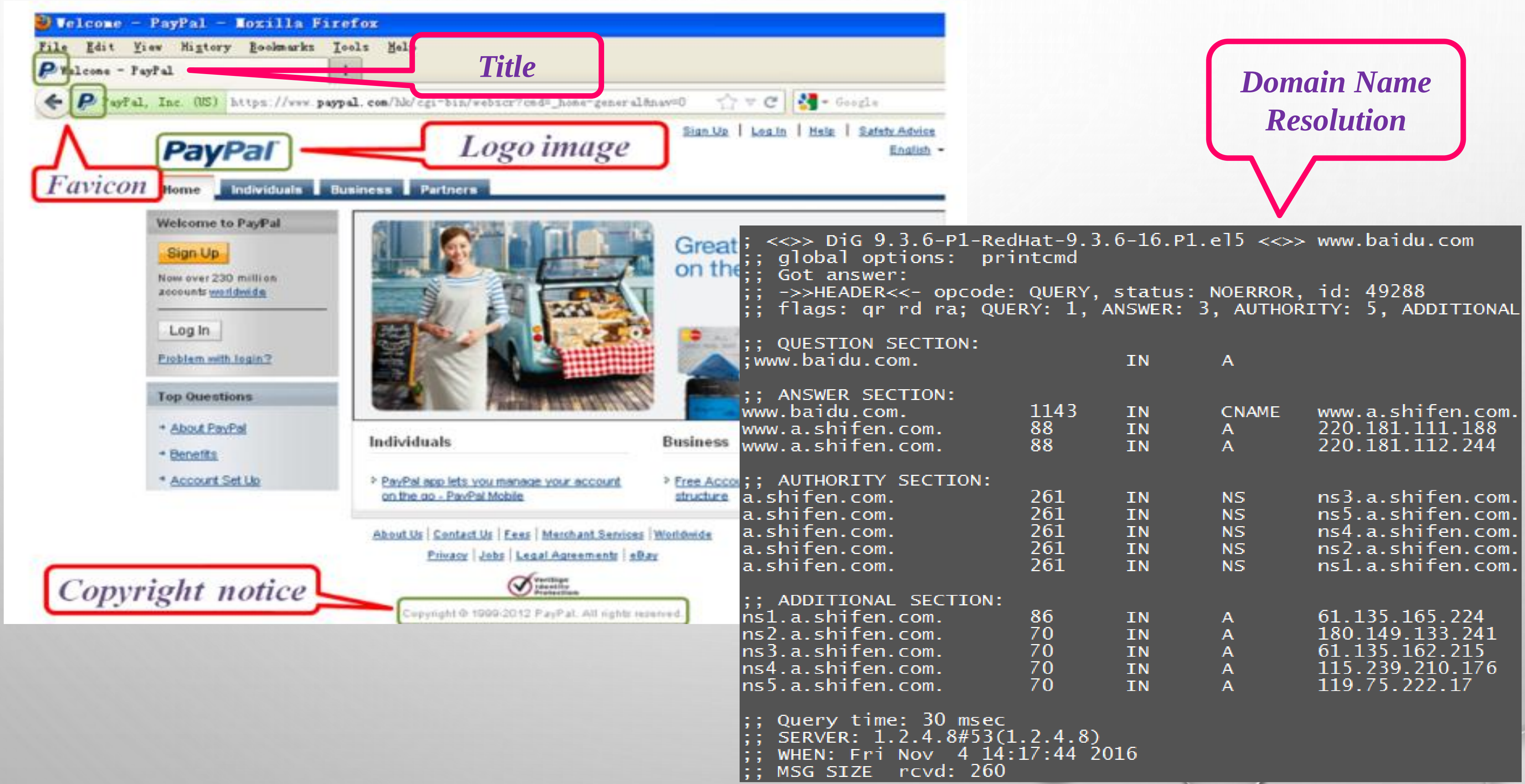
工业和信息化部
二〇一七年一月

Since 2009, CNNIC has been focusing on the anti-phishing technical research, the “**Proactive Phishing Detection System**” is an important achievement.

The core of the system is based on the Big Data analysis for the machine learning of domain name utilization.

The phishing websites can be monitored and tracked from the registration phase, and can be discovered and disposed when they online.

CNNIC's Contributions---Proactive Phishing Detection System


Welcome - PayPal - Mozilla Firefox
File Edit View History Bookmarks Tools Help
Welcome - PayPal
PayPal, Inc. (US) https://www.paypal.com/hk/cgi-bin/webscr?cmd=_home-general&nav=0
Title
Logo image
Favicon
Sign Up | Log In | Help | Safety Advice
English
Home Individuals Business Partners
Welcome to PayPal
Sign Up
Now over 230 million accounts worldwide
Log In
Problem with login?
Top Questions
About PayPal
Benefits
Account Set Up
Great on the
Individuals
Business
PayPal app lets you manage your account on the go - PayPal Mobile
Free Account structure
About Us | Contact Us | Fees | Merchant Services | Worldwide
Privacy | Jobs | Legal Agreements | eBay
Copyright notice
Copyright © 1999-2012 PayPal. All rights reserved.
Domain Name Resolution

```
; <<>> DiG 9.3.6-P1-RedHat-9.3.6-16.P1.el5 <<>> www.baidu.com
;; global options:  printcmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 49288
;; flags: qr rd ra; QUERY: 1, ANSWER: 3, AUTHORITY: 5, ADDITIONAL

;; QUESTION SECTION:
;www.baidu.com.                 IN      A

;; ANSWER SECTION:
www.baidu.com.          1143    IN      CNAME   www.a.shifen.com.
www.a.shifen.com.       88      IN      A       220.181.111.188
www.a.shifen.com.       88      IN      A       220.181.112.244

;; AUTHORITY SECTION:
a.shifen.com.           261     IN      NS      ns3.a.shifen.com.
a.shifen.com.           261     IN      NS      ns5.a.shifen.com.
a.shifen.com.           261     IN      NS      ns4.a.shifen.com.
a.shifen.com.           261     IN      NS      ns2.a.shifen.com.
a.shifen.com.           261     IN      NS      ns1.a.shifen.com.

;; ADDITIONAL SECTION:
ns1.a.shifen.com.       86      IN      A       61.135.165.224
ns2.a.shifen.com.       70      IN      A       180.149.133.241
ns3.a.shifen.com.       70      IN      A       61.135.162.215
ns4.a.shifen.com.       70      IN      A       115.239.210.176
ns5.a.shifen.com.       70      IN      A       119.75.222.17

;; Query time: 30 msec
;; SERVER: 1.2.4.8#53(1.2.4.8)
;; WHEN: Fri Nov  4 14:17:44 2016
;; MSG SIZE  rcvd: 260
```

CNNIC's Contributions---Proactive Phishing Detection System

Detection Capacity

❿In 2016, the system identified and processed more than 40,000 phishing websites of 80 brands

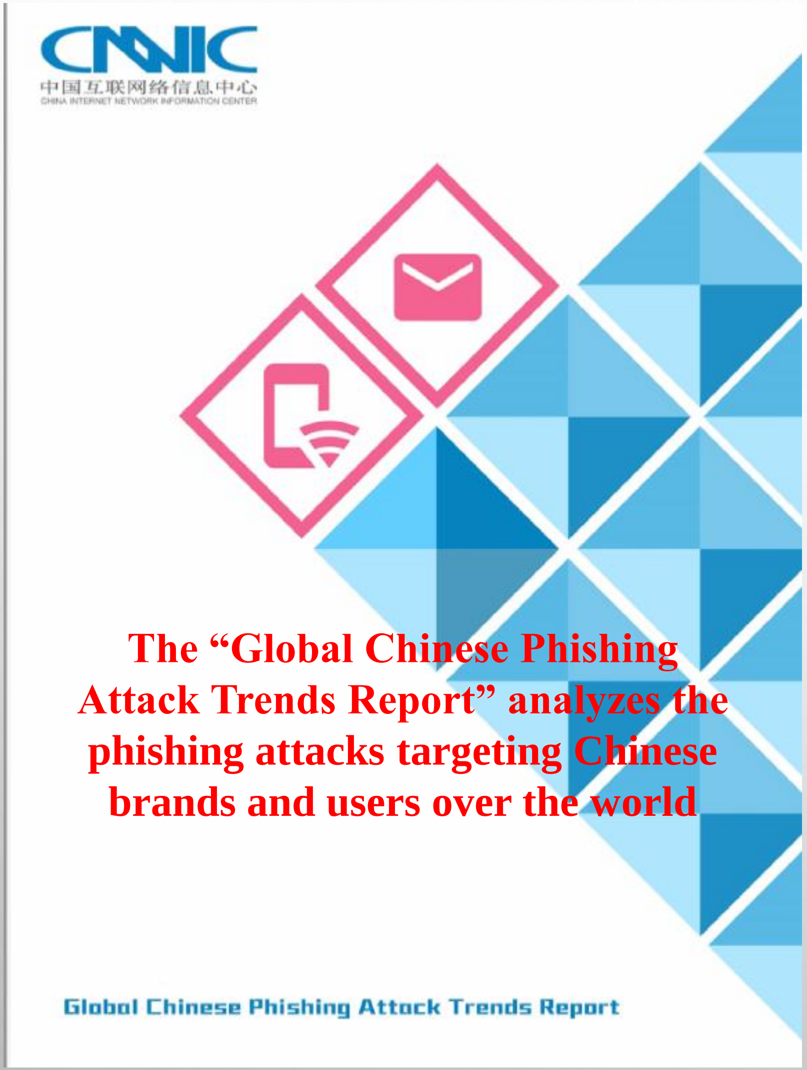
❿The life duration of phishing website detected by the system is 4.684 days, much shorter than the average number

Technical Achievements

❿CNNIC has published more than 10 academic papers and holds more than 10 anti-phishing patents

❿"Technical Specifications of Data Exchange for Reporting Phishing Attacks", the only anti-phishing industrial standard in China

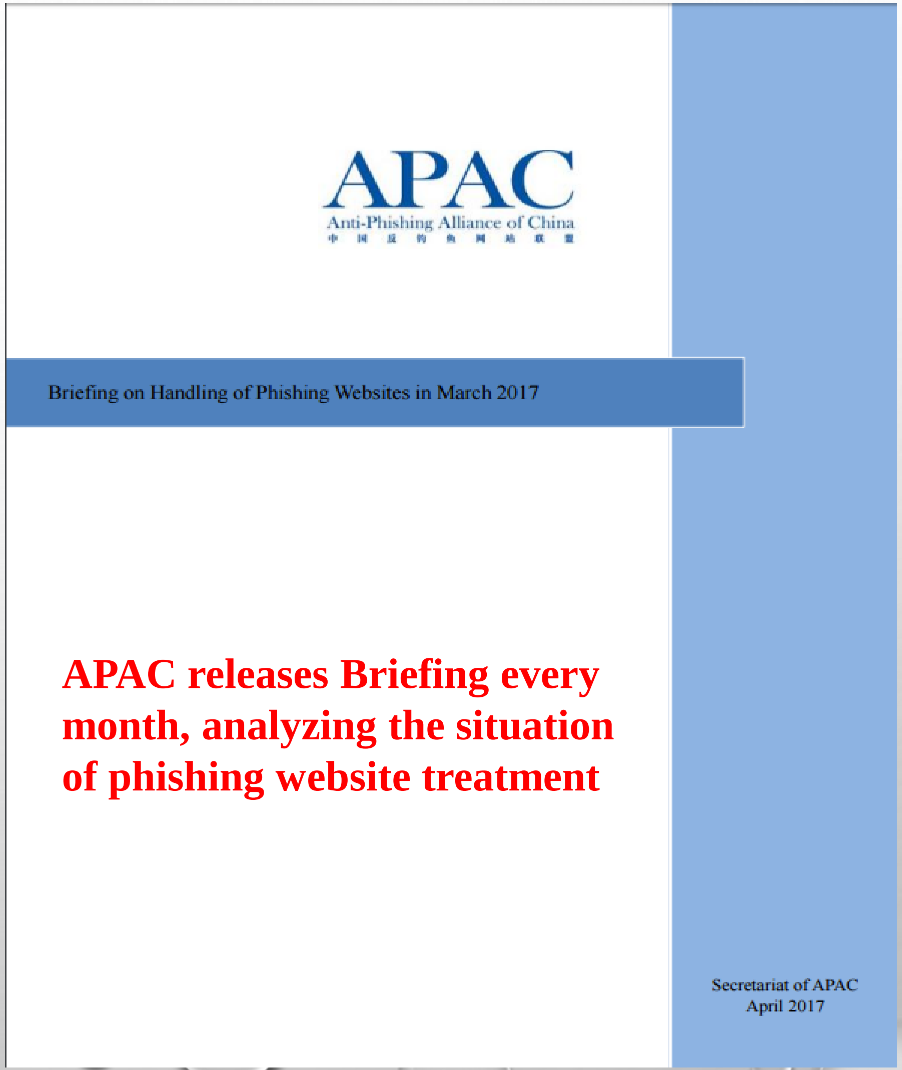
CNNIC’s Contribution---Reports & Briefings



CNNIC
中国互联网络信息中心
CHINA INTERNET NETWORK INFORMATION CENTER

The “Global Chinese Phishing Attack Trends Report” analyzes the phishing attacks targeting Chinese brands and users over the world

Global Chinese Phishing Attack Trends Report



APAC
Anti-Phishing Alliance of China
中国反钓鱼网站联盟

Briefing on Handling of Phishing Websites in March 2017

APAC releases Briefing every month, analyzing the situation of phishing website treatment

Secretariat of APAC
April 2017

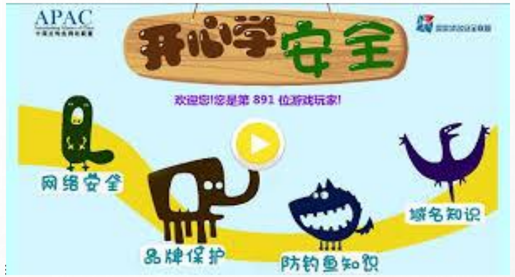
Suggestions for Improving Domain Names Utilization

- Encourage registries, registrars, academic institutions to facilitate scientific research, data exchanging and technology sharing

Capacity Building

- Promote standardization on identification, sharing and disposal, and seek more cooperative chances with government agencies

Enhance Supervision



欢迎您!您是第 891 位游戏玩家!

- Strengthen universal education for end users, and heighten their awareness of online risks

Strengthen Education

Technic

Disposal

Awareness

THANKS!

Q & A