Anti-Phishing Alliance of China
アンチフィッシングアライアンスチャイナのご紹介

Nov, 2010

APAC
Anti-Phishing Alliance of China
中 国 反 钓 鱼 网 站 联 盟

APAC
Anti-Phishing Alliance of China
中 国 反 钓 鱼 网 站 联 盟

CONTENTS

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

Overview

- Anti-Phishing Alliance of China(APAC) は2008年7月18日に創設された
- 銀行、Eコマース、ドメイン名販売事業者などを中心に現在 145社の会員がいる
- APACの使命は、フィッシング及び個人情報窃取や金融犯罪を引き起こすスパムメールを抑制すること
- 中国ではフィッシング問題について公に認められた唯一組織
- APACは、ドメイン名の利用停止処理プロセスを導入した
- APAC事務局は、CNNICが務める

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

The positioning and slogan of APAC

我々の役割:

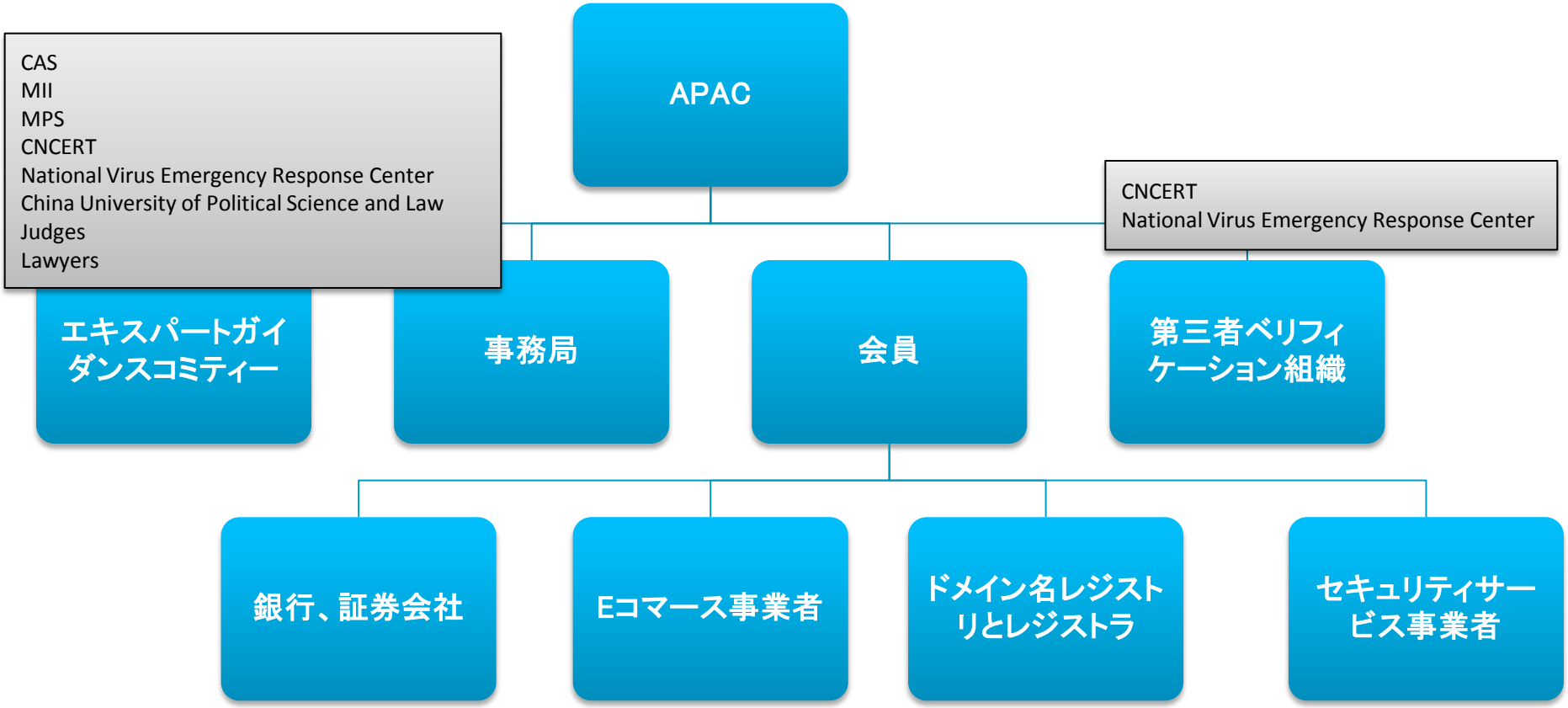
- 中国のフィッシング対策活動を推進する権威となる
- 中国での知見やデータを共有するためのプラットフォーム機能を果たす
- フィッシングやその他の好ましくないインターネットアプリケーションの問題について、中国政府の政策決定のアドバイザーとなる
- 中国政府と中国の企業との架け橋となり、相互の連携を手助けする

我々のゴール:

Authoritative, professional, commonweal, sharing

APAC
Anti-Phishing Alliance of China
中 国 反 钓 鱼 网 站 联 盟

the organization structure of APAC



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

管理の手続き

- 報告の受付
  - 電話
  - メール
  - Webから
- 検査と確認
  - 事務局
  - 第三者機関
- テイクダウン(サイト停止)
  - .CN ドメインを使っている場合
    - レジストリとレジストラは2時間以内に、該当のドメイン名をサスペンドする
  - .CN ドメインを使っていないが、中国の事業者で登録したドメイン名をつかっている場合
    - レジストラーに対して該当ドメイン名の解決を停止するよう要請する
  - .CN ドメインを使っておらず、外国で登録されている場合
    - フィッシングサイトのURLはブロックリストサービス事業者に送られる (ファイヤウォールベンダ, ウイルス対策ソフトベンダ, アンチスパムベンダなどなど)
- アピール
  - 利用者からのアピールが認められると、APACはブロックリストからURLを削除し、レジストリ/レジストラにドメイン名の利用再開を通達する。
- 調査研究
  - フィッシングに関する調査研究(例えばフィッシングのヒューリスティック/パターン検知認識方法など)をおこなっている

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

フィッシングURL提供先

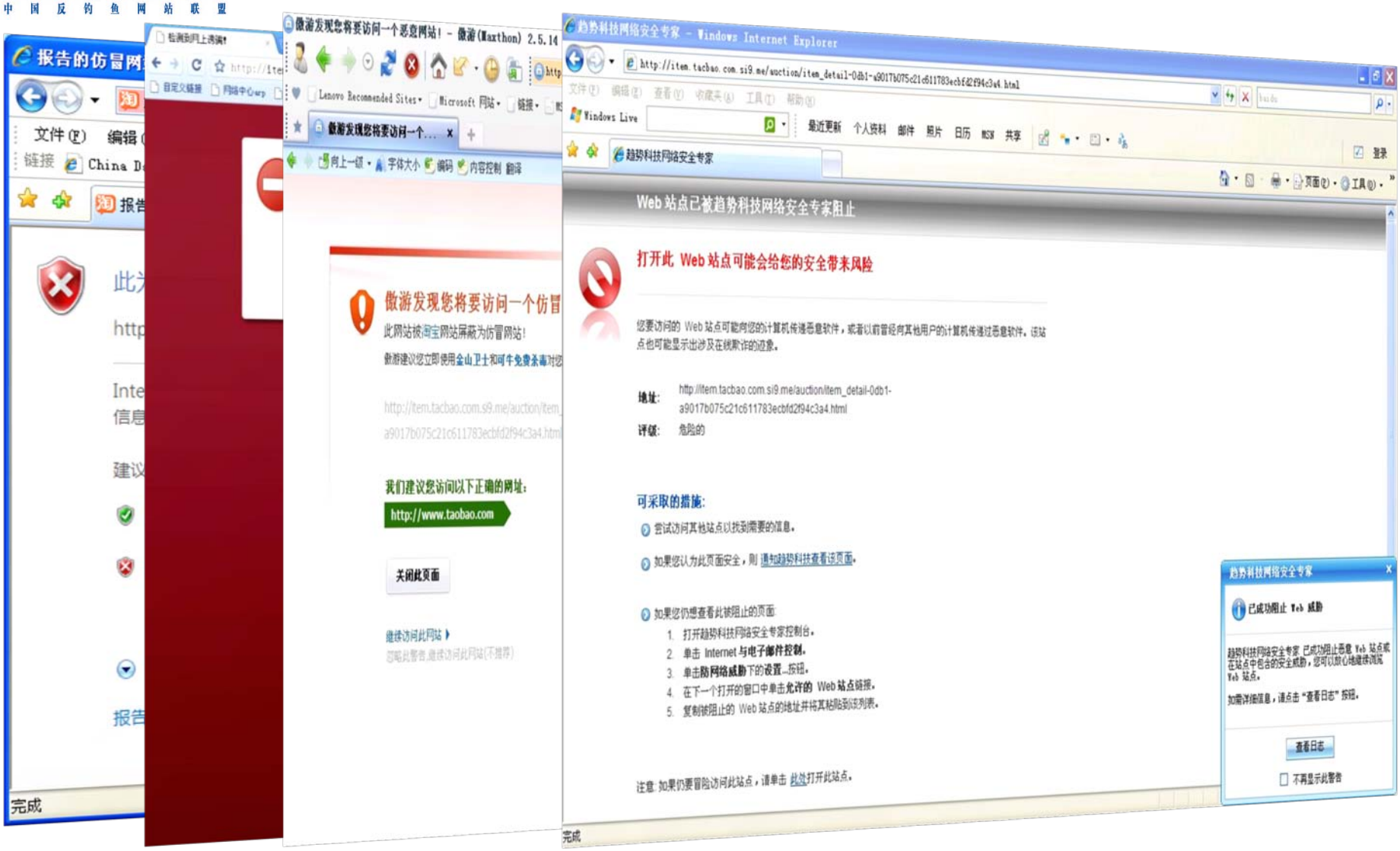






APAC
Anti-Phishing Alliance of China
中 国 反 钓 鱼 网 站 联 盟

ブラウザでのブロック実例



APAC
Anti-Phishing Alliance of China
中 国 反 钓 鱼 网 站 联 盟

北京五輪を狙ったフィッシング

Official:www.tickets.beijing2008.cn

Phishing:www.★ ★ ★ -tickets2008.com
Phishing:www.★ ★ ★ ticketing.com
More than 50 million USD.

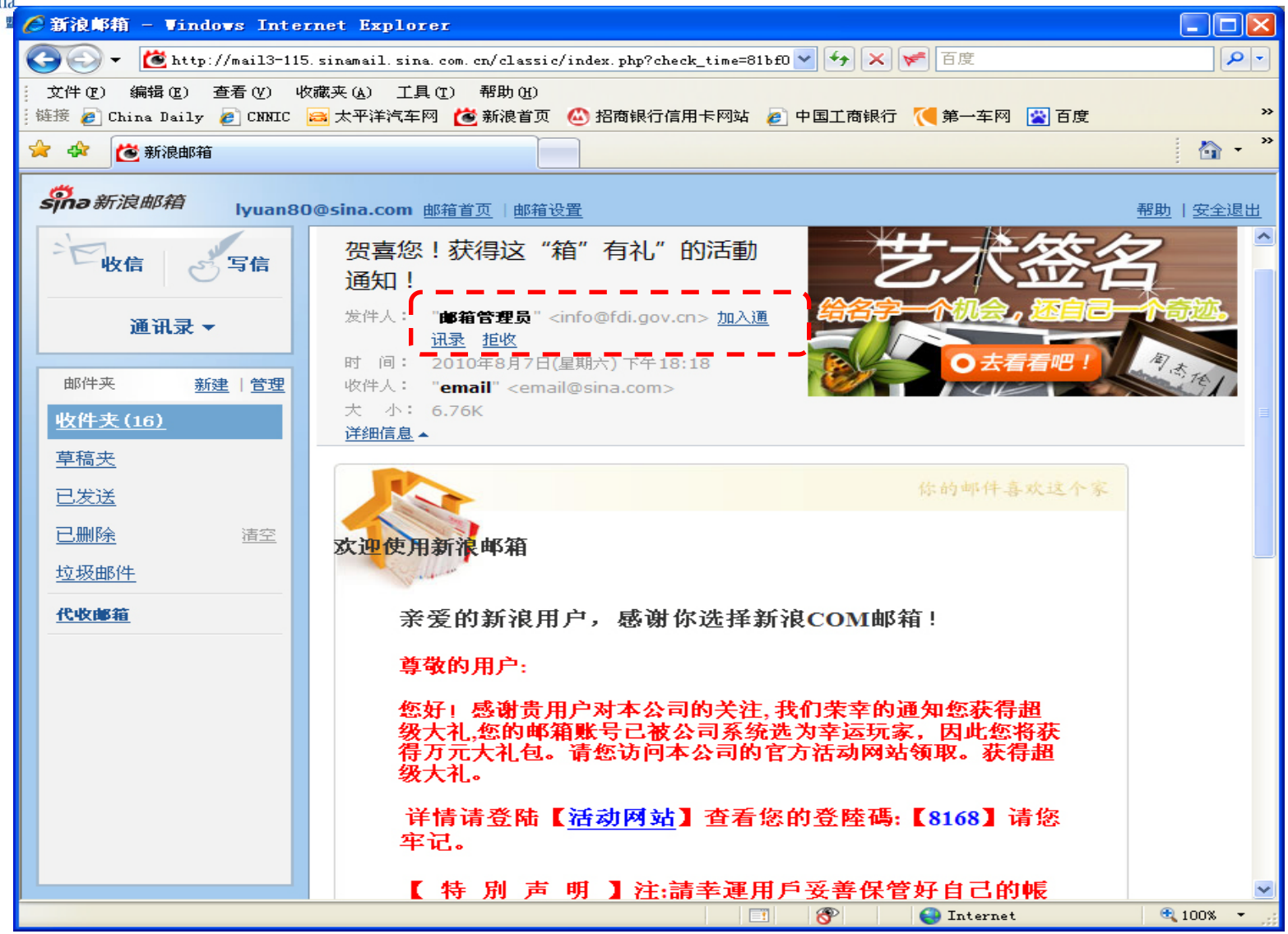
APAC
Anti-Phishing Alliance of China
中国反钓鱼网站联盟

寄付サイトを狙ったフィッシング

- 2008年の四川地震、2010年の青海省地震の際にはこれに乗じたフィッシングが行われた
- 災害救助支援活動はフィッシャーにとってチャンス
- フィッシングURLの実例
  - http://cctv-t2.★ ★ ★ /jk/index.htm
  - http://www.688 ★ ★.com/
  - http://www.qq.com.indexq.cn/news/news.qq.com/a/20080512/index.htm
- CNNICはindexq.cnの登録者によって登録された別のドメイン名を監視した。それらがフィッシングに使われることはなかった。

APAC
Anti-Phishing Alliance of China
中 国 反 钓 鱼 网 站 联 盟

公式メールボックスをつかったフィッシング



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

レジストリやレジストラーのフィッシング被害

2010年1月11日

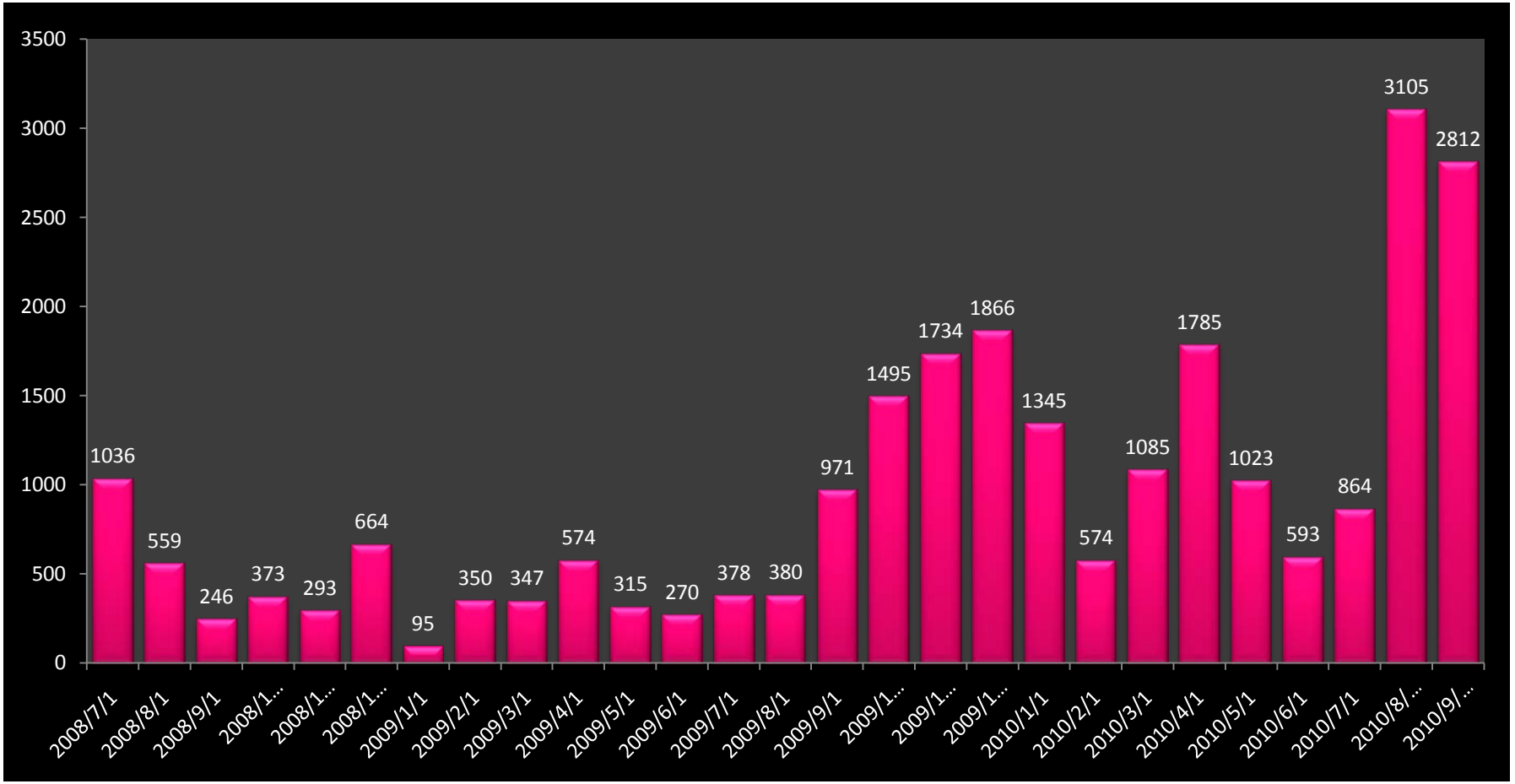
1. 攻撃者はBaiduの担当者を名乗ってRegister.comとのチャットを開始
2. Register.comの担当は確認情報の提供を申し出た。攻撃者は無効な情報を送付したが、 Register.comはこれに気づかず手続きを続行。Baiduのメールアドレスにセキュリティコードを送付した
3. ハッカーはそのメールを読めないため、デタラメのセキュリティコードをチャットでRegister.comに送付した。Register.comはセキュリティコードの確認を行わなかった
4. 攻撃者はRegister.comの担当に登録メールアドレスをantiwahabi2008@gmail.comに変更するよう依頼し、これが変更された。
5. 攻撃者は “forgot password” リンクを使ってユーザ名とパスワードを取得。Baiduのネームサーバに関する設定変更権限を得た

CNNNICではVIPカスタマーについては書面での変更依頼を必要としている

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

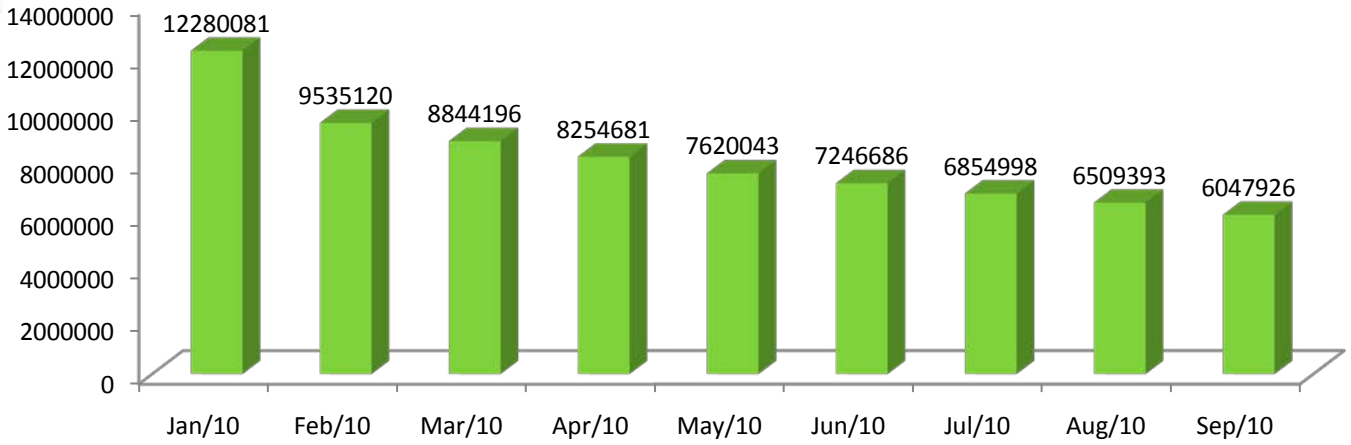
APACに寄せられるフィッシングの傾向

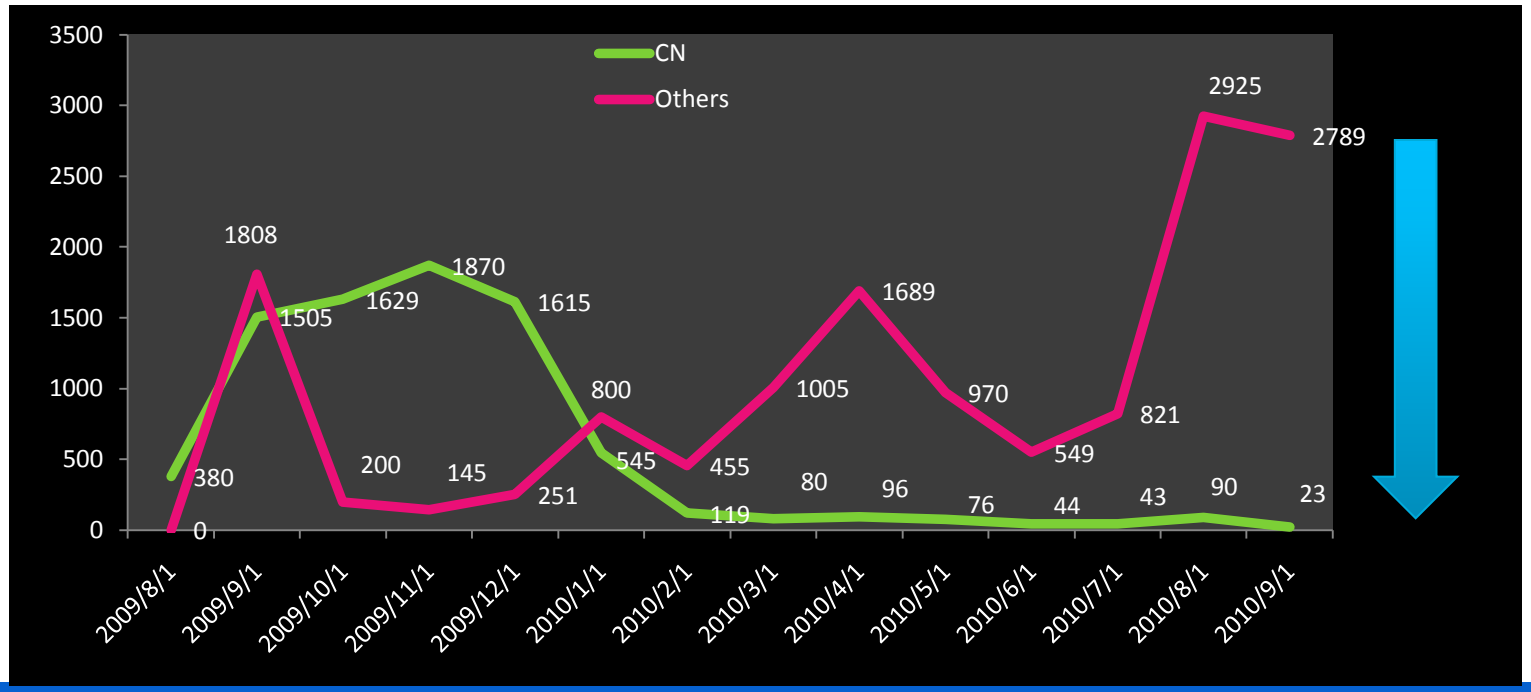
2010年9月までにAPACは25,132件のフィッシング報告をうけている。



APAC
Anti-Phishing Alliance of China
中 国 反 钓 鱼 网 站 联 盟

CNドメインのフィッシングの傾向

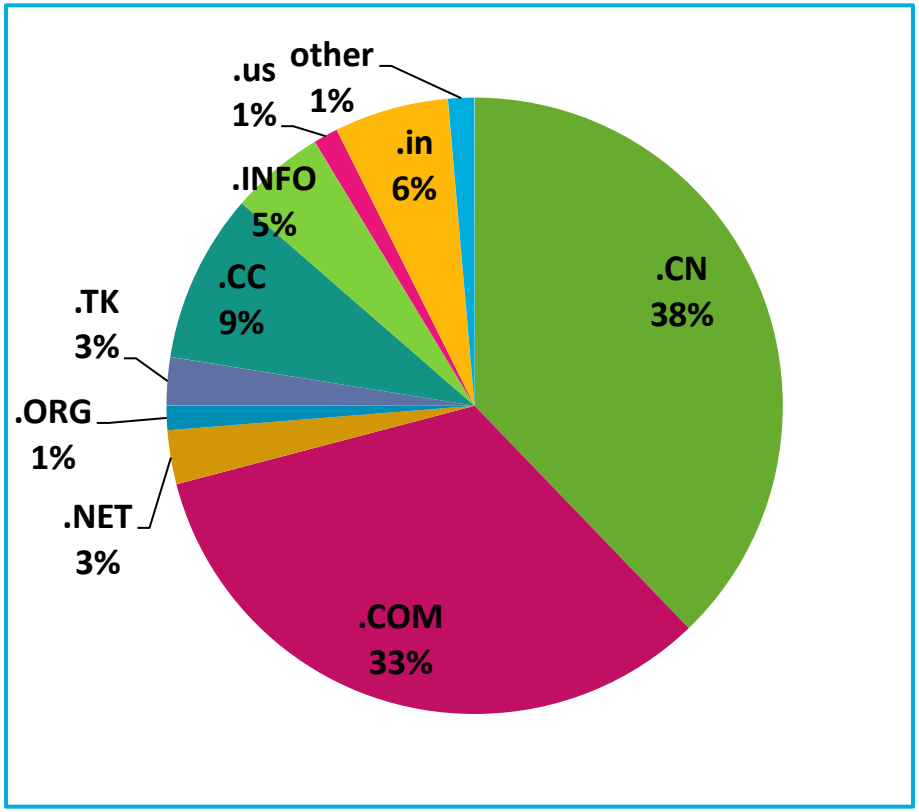




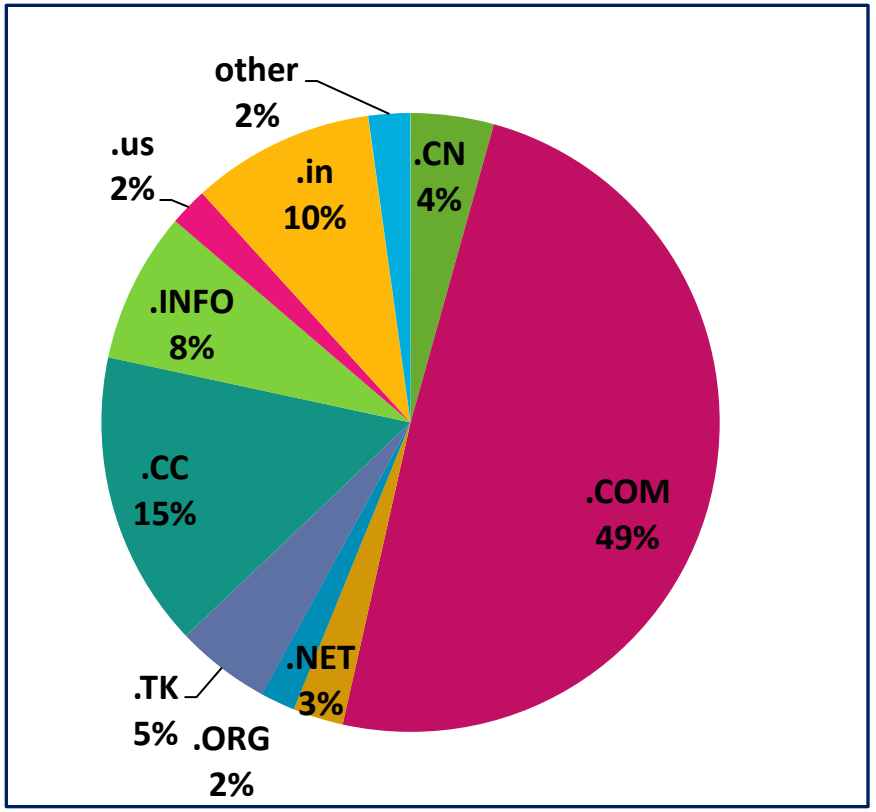
APAC
Anti-Phishing Alliance of China
中国反钓鱼网站联盟

ドメイン名別、フィッシングサイト件数

2008-2009



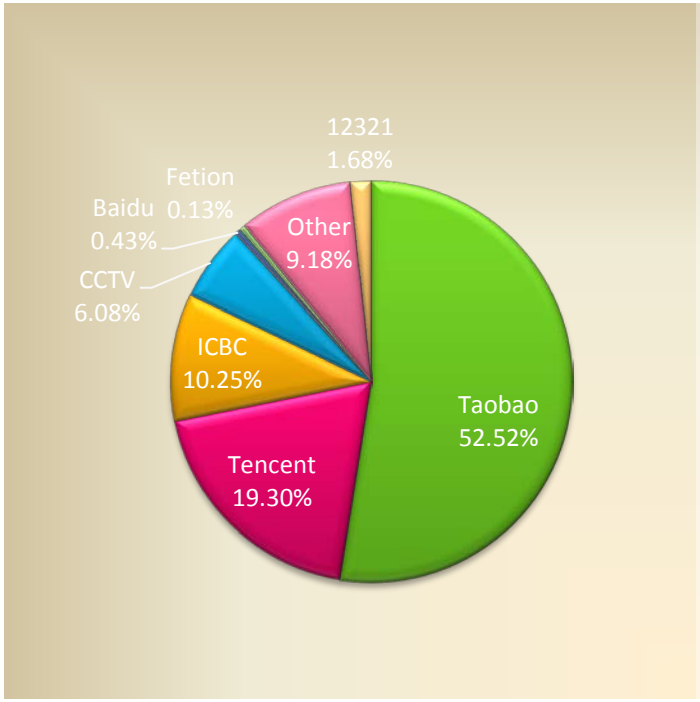
2010-

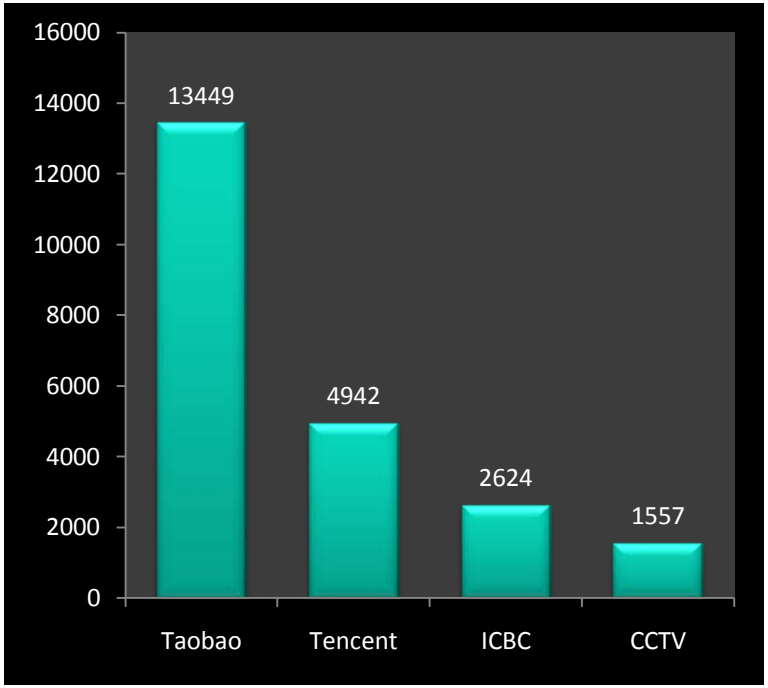


APAC
Anti-Phishing Alliance of China
中 国 反 钓 鱼 网 站 联 盟

フィッシングに関する統計

Eコマースが中国国内のフィッシングの主な被害者である

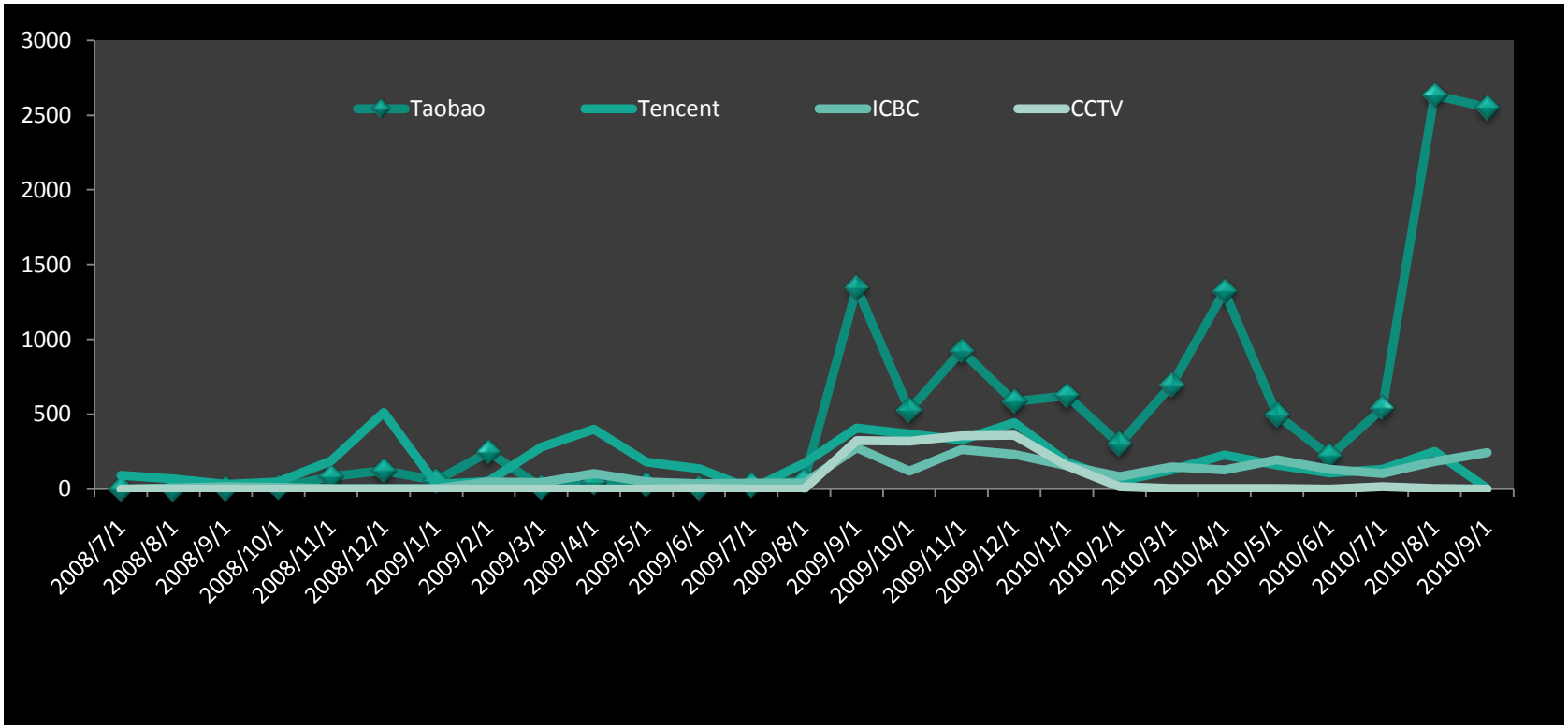




•淘宝网(Taobao), 中国最大のEコマース事業者, 2億のユーザ, 年間売り上げは300億ドル(2.4兆円)
• Tencent, 中国最大のインスタントメッセージングサービス, 5億を超えるアクティブユーザ, 1億がオンライン状態

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

被害ブランド別のフィッシング



調査研究

APACからのサンプル

http://item.taobao.com-oo.info/login.asp

http://item-taoobao.co.cc/auction/buy_nowxn.asp?item_detail-0db2-1wj7vl12tsf1t8bq7pae7trk526t062e

http://ltem.taoboa.auciaczs.com/auction/buy_nowxn.asp?item_detail-0db2-rnaxmcr3kj72k93h8g26xkibvs7k1736

http://item.taobao.scoai.tk/login.khdel.html

http://www.taobro.tk/auction/buy_nowsw.asp?item_detail-0db2-62z2116798uf9cq6l5pt297z07k9elgt

http://item.taebao.con.aluoni.co.cc/member/login.html.asp

http://item.tacbao.com.pouy.co.cc/tao/auction/buy_nowsw.asp?item_detail-0db2-d97i99do662w7u844372j748gd36w3y1

http://item.taobao.cn.jiaxinwl.com/member/login.tb.jhtml.asp?f=top

http://item.teobao.com.detar.tk/login.asp?id=169&numbers=1

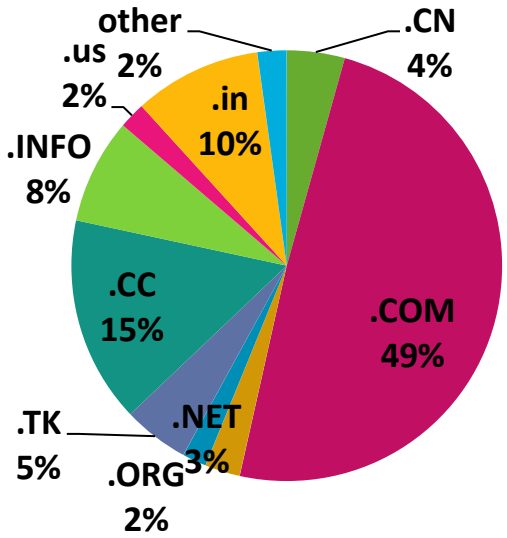
http://www.qq.com.trwjn.info/2010/index.html

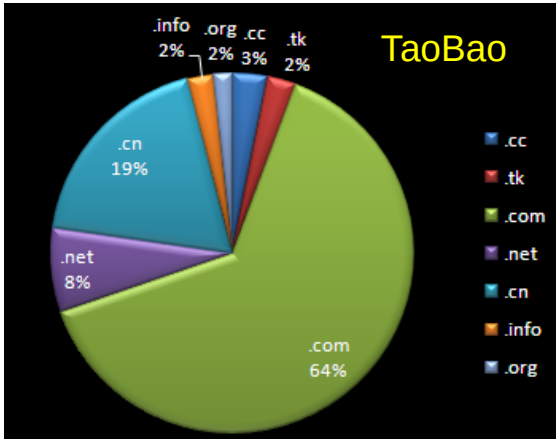
技術研究と開発

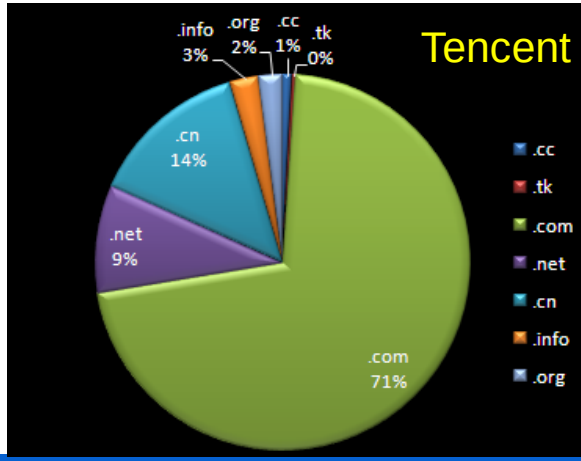
- ドメイン名の類似度判定
  - *Taobao.com VS Toobao.com*
- CDN の類似度判定
  - *康师傅.中国 VS 康帅博.中国*
- Webサイトの特徴による検知
  - Detect web pages’ landing box
  - Webサイトの所有者情報を確認
    - コピーライト、ICP、検索ランキング、whois情報などなど
  - 内部リンクと外部リンクの分析

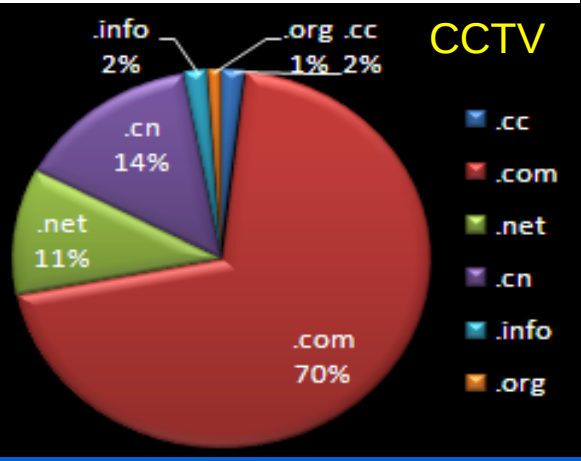
予備実験の結果

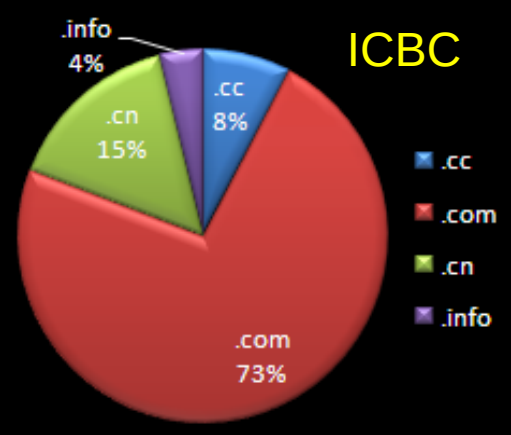
- Dig in recursive DNS logs for suspicious phishing hosts
  - 類似度を検出
    - Levenshtein Distance
    - Character pixel comparison
- 結果
  - www.qq.qqhw.tk
  - Item.taobao.mao-u.tk
  - Item.baotao.mae-ep.tk
  - www.cctv33v.co.cc
  - …





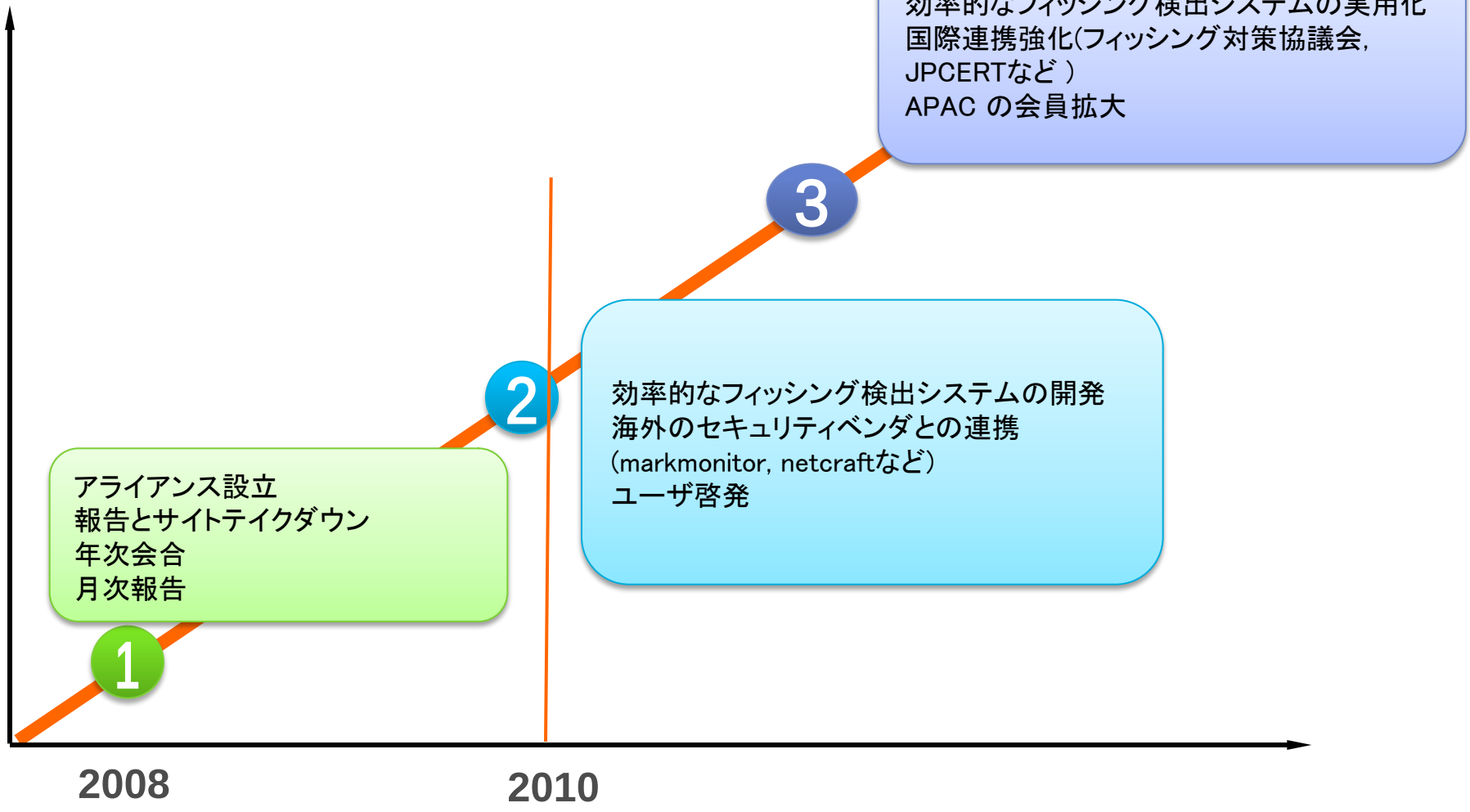






APAC
Anti-Phishing Alliance of China
中国反钓鱼网站联盟

APACの今後について



フィッシング届出方法

Personal Report Email：**anti-phishing@apac.cn**

The Alliance member Report Email ：**fdy@apac.cn**

Report Phone：**010-58813000**

Report Platform：**jubao.apac.cn**

APAC

Anti-Phishing Alliance of China

中 国 反 钓 鱼 网 站 联 盟

Authoritative, Professional, Commonweal, Sharing

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

Code : 100190

www.apac.cn