Global Chinese Phishing Sites Report

2nd Half 2012

Global Chinese Phishing Sites Report

(2nd Half 2012)

National Domain Name Security Center

and

Anti-Phishing Alliance of China (APAC)

in cooperation with the Anti-Phishing Work Group (APWG)

May 2013

Table of Contents

General Introduction

Definition of Phishing Attacks

Phishing is the act of attempting to acquire information such as usernames, passwords, and credit card details by masquerading as a trustworthy entity in an electronic communication. Phishing has spread beyond email to include instant messaging, and social networking sites. Phishing attacks can lead to damaging losses in terms of identity theft.

Scope & Methodology

The *Global Chinese Phishing Activity Trends Report（2nd half 2012）* analyzes the phishing attacks targeting Chinese brands and therefore Chinese users over the world in 2nd half 2012. The statistics insist of three sources: the phishing attacks reported to the **Anti-Phishing Alliance of China** (**APAC)**, the phishing attacks detected actively by **DNSCERT**, and the global Chinese phishing attacks reported to the **Anti-Phishing Working Group (APWG)** by its members. In the data set, 34% of the phishing attacks were from the APWG's repository.

The statistics of this report is based on the phishing URL, which is usually a combination of a hostname and a path. The statistics based on URL instead of hostname is based on the following reasons: 1. there are many phishing URLs, which use the same hostname, but target different brands; 2. there exist legitimate sites whose pages are exploited by phishers; 3. most of the anti-phishing tools block the phishing attacks via the full URLs.

Statistical Highlights

- The number of unique phishing sites targeting at Chinese users was 7,504 in H2, 2012, which is 53% decreased compared to that in H1, 2012.
- The top 5 most-targeted brands were: Taobao.com, Alibaba, SINA, TENCENT and CCTV.
- The top 5 TLDs used for the phishing sites were .COM, .CC, .TO, .TK, and .INFO.
- The detailed information of phishing sites is tabulated as follows.

	Jul.	Aug.	Sep.	Oct.	Nov.	Dec.
unique phishing sites	1363	1289	**1710**	934	1365	843
unique domain names	1289	1211	**1668**	904	1329	801
hijacked brands	22	**25**	24	19	18	19

Phishing Sites Trends

In the second half of 2012, 7,504 Chinese phishing sites were detected globally. The number of phishing sites detected reached the peak of the second half year of 2012 in September.

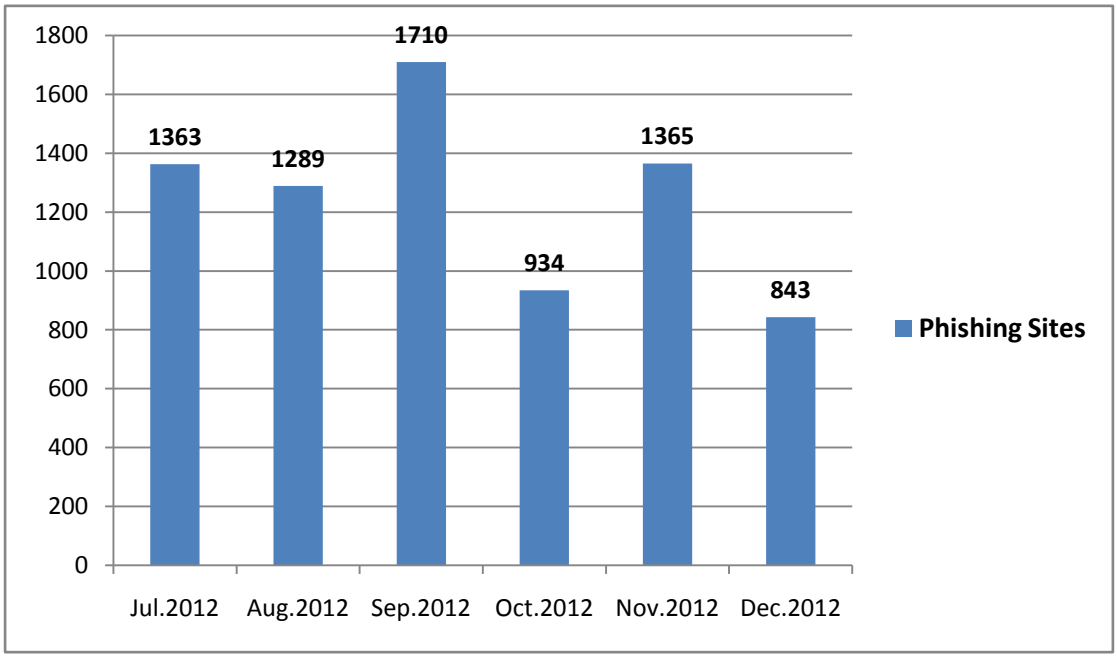

Fig. 1 Phishing URLs Trends

Targeted Brand

In the second half of 2012, there were 42 total brands that were the targets of phishing attacks. Taobao.com ranked first in all targeted brand, and 48.3% of the total reported attacks aimed at Taobao.com. Figure 2 shows the specific distribution of phishing attack targeted brands.

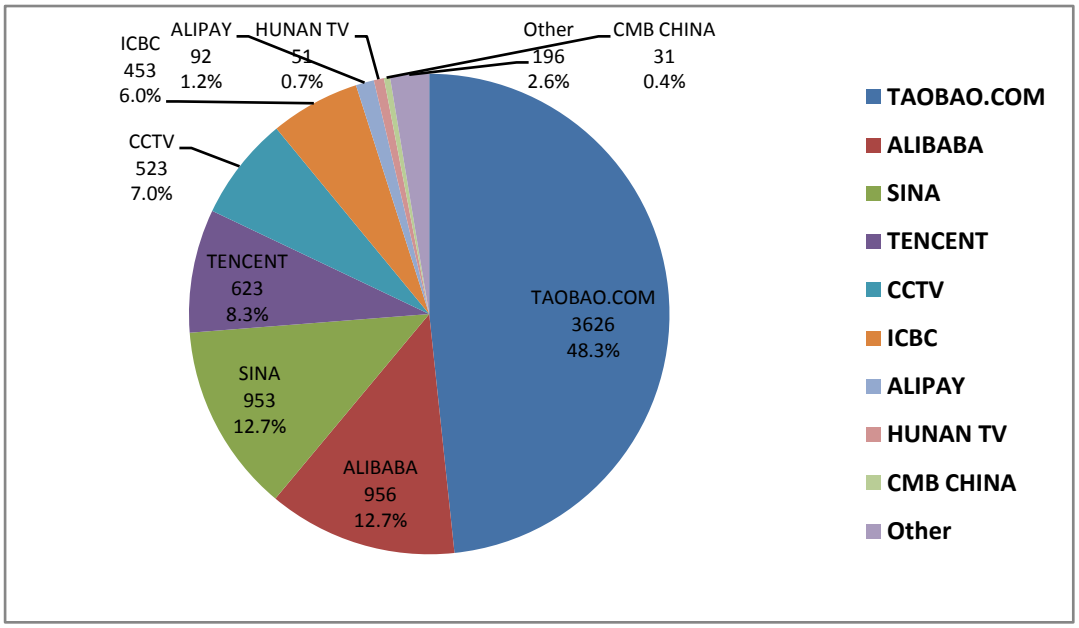

Fig. 2 Targeted brand sectors in the second half of 2012

We can find from the distributions that reported attacks on the top 6 targets accounted for 95.1% of all the reports. This indicates that phishing is concentrated in distribution. The trends of these main targeted brands are shown in Fig. 3.

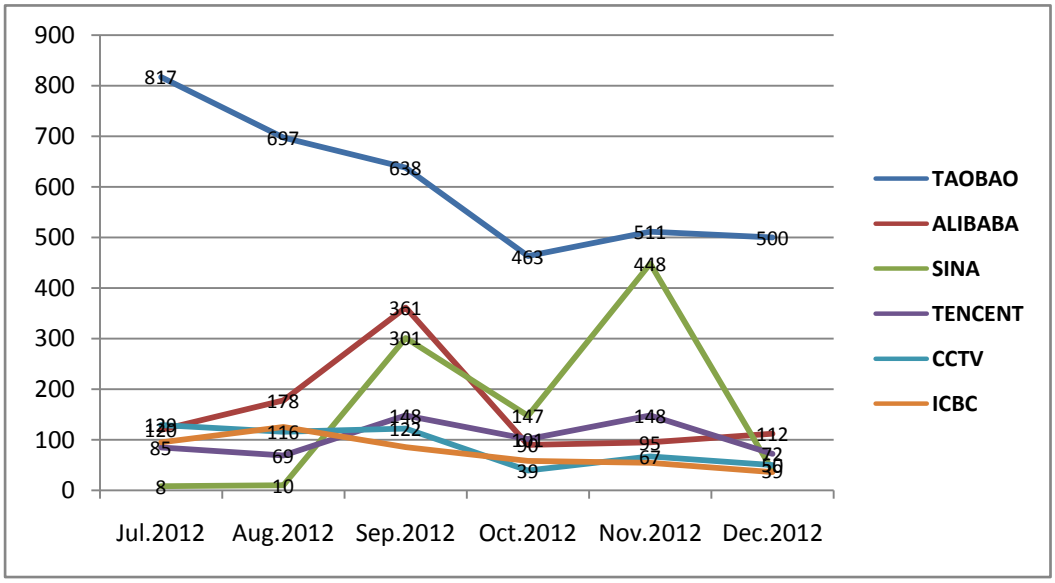

Fig. 3 Main Targeted Brand Trends

Phishing Domains

Except for a very few phishing websites that provided service only through an IP address, most phishing sites appear of websites hosted on domain names. Therefore, a large number of top-level-domains have been used for phishing attacks, and.COM was most commonly used. The distributions and the monthly trends are shown as follows.

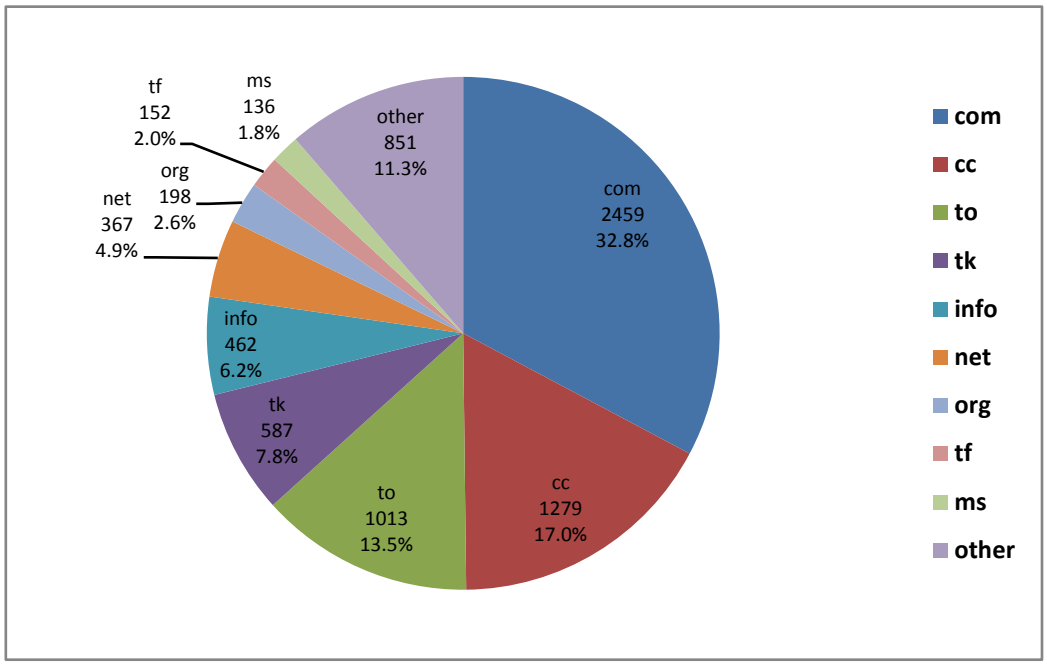

Fig. 4 Phishing Sites' Top-level-domain Sectors

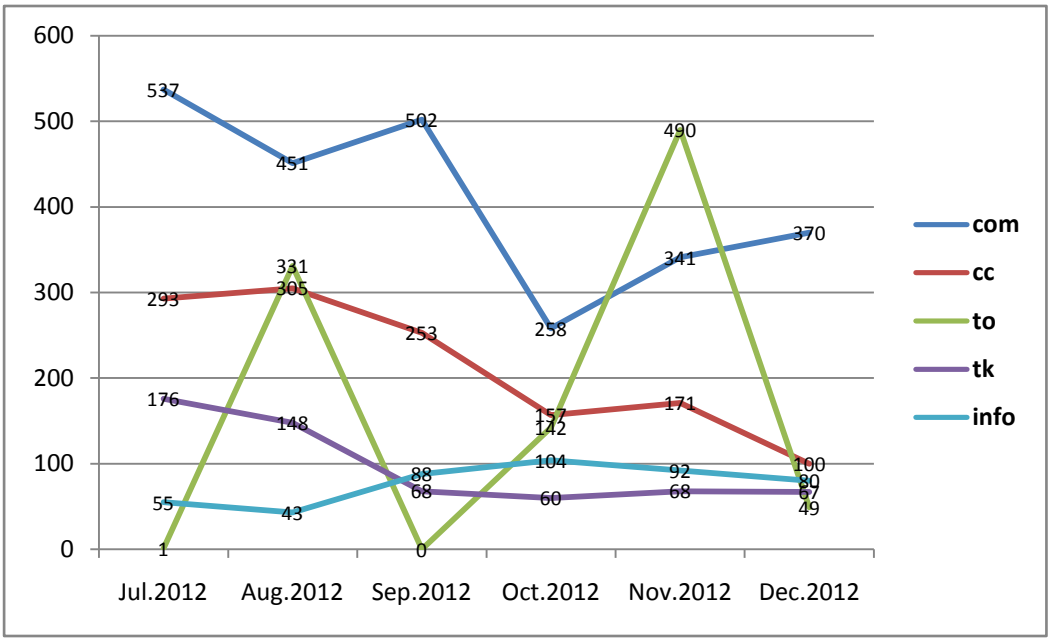

Fig. 5 Main TLD Trends

It is worthwhile to note that liberal domain registration and auditing mechanisms, including cheap or even free domain registration, make it easier for attackers to register phishing domain names. On the contrary, due to the real name auditing mechanism of .CN domain names, there were only 26 .CN domains used in phishing attacks during 2nd half 2012 while there were 7.5 millions of .CN registered. This reflects that appropriate management of domain name registering is good to improving the reliability of the Internet.

Phishing URL-Domain-Brand Trends

This section gives an introduction to the relationship among the phishing URL, domain and brand.

Unique phishing domains refer to the domains owned by the attackers who can configure it directly. It is often a second-level domain (such as “example.com”) domain, sometimes also can

be a third-level domain under a second-level domain (such as “free.example.com”).

Unique phishing domain – phishing brand is a pair between phishing name and phishing brand. If several URLs used the same phishing name for the same phishing brand, there will be only one pair to be count.

Distributions over months for the above two indicators are illustrated in Fig. 6.

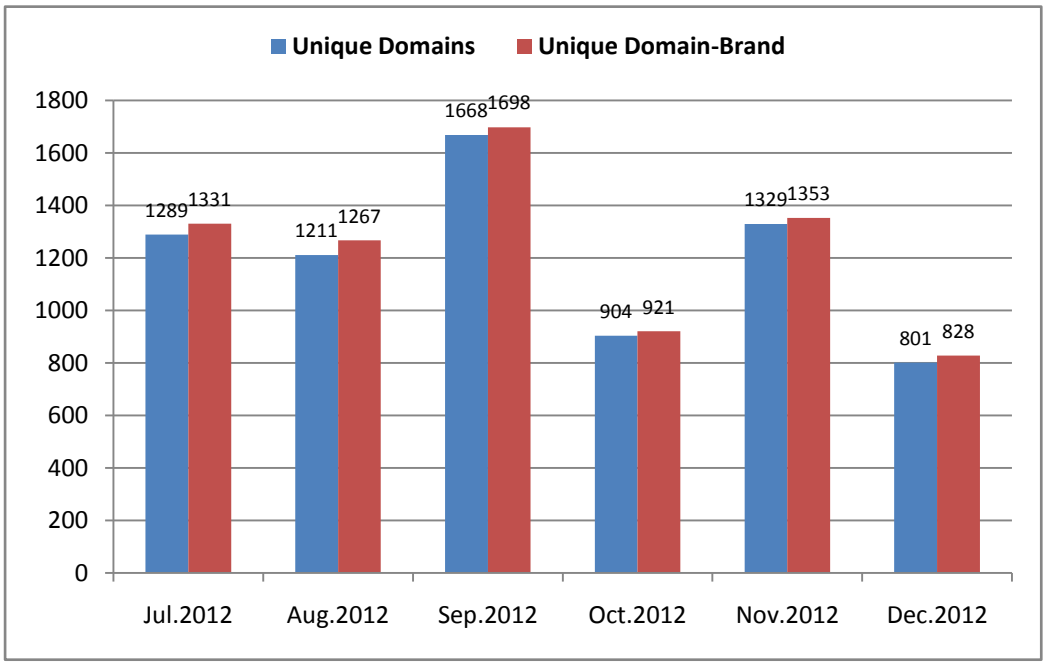

Fig. 6 Unique Phishing Domains & Unique Brand-Domain Pairs Trends

From Fig. 6, we can see the number of unique brand-domain pairs is larger than that of unique phishing domains, which indicates that attacker tends to use the same phishing domain to aim at multiple phishing brands in order to ensure the phishing domain’s usage rate.

Trends for targeted brand and URLs per brand are illustrated respectively in Fig. 7.

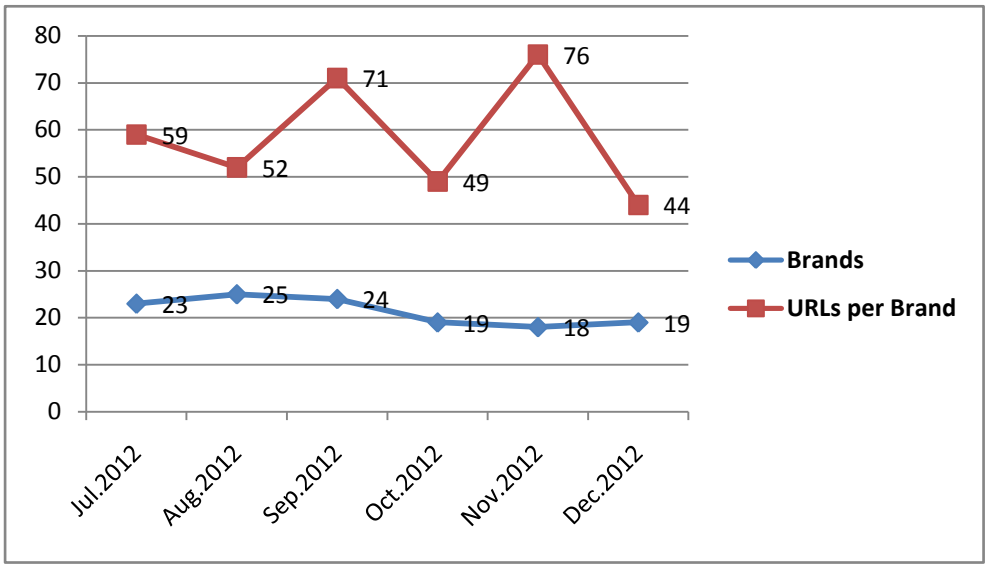

Fig. 7 Targeted Brand & URLs per Brand Trends

According to Fig. 7, URLs per Brand were unstable during 2nd half of 2012, which means large scales of phishing attacks burst sometimes. For example, SINA may suffer a large scale of phishing attacks on September and November according to Fig. 3.

Highlights in the Whole 2012

- In the year of 2012, there were **23,122** Chinese phishing sites reported globally. The peak number of Chinese Phishing Sites reported monthly occurred in May, in which 3,325 phishing sites were discovered.

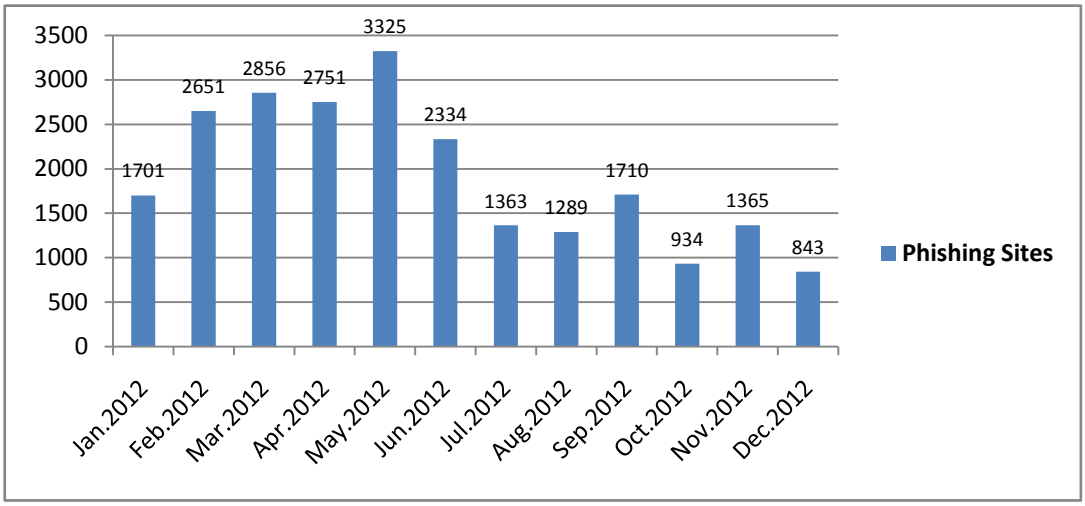

Fig. 8 Phishing URLs Trends in 2012

- In the year of 2012, **82** brands were involved in Chinese phishing attacks. Top 10 brands. The distribution of main brands is showed as follows.

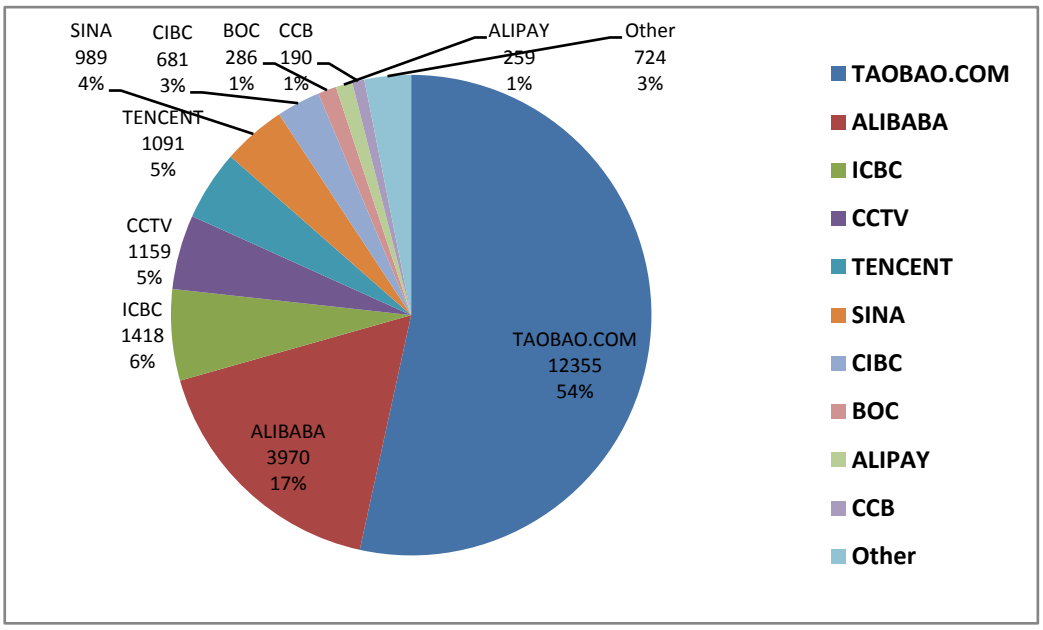

Fig. 9 Targeted brand sectors in 2012

- In the year of 2012, **130** Top-Level Domains were used in Chinese phishing attacks. .com, .tk and .cc are the most three TLDs used and accounted for 57.2% of the total number.

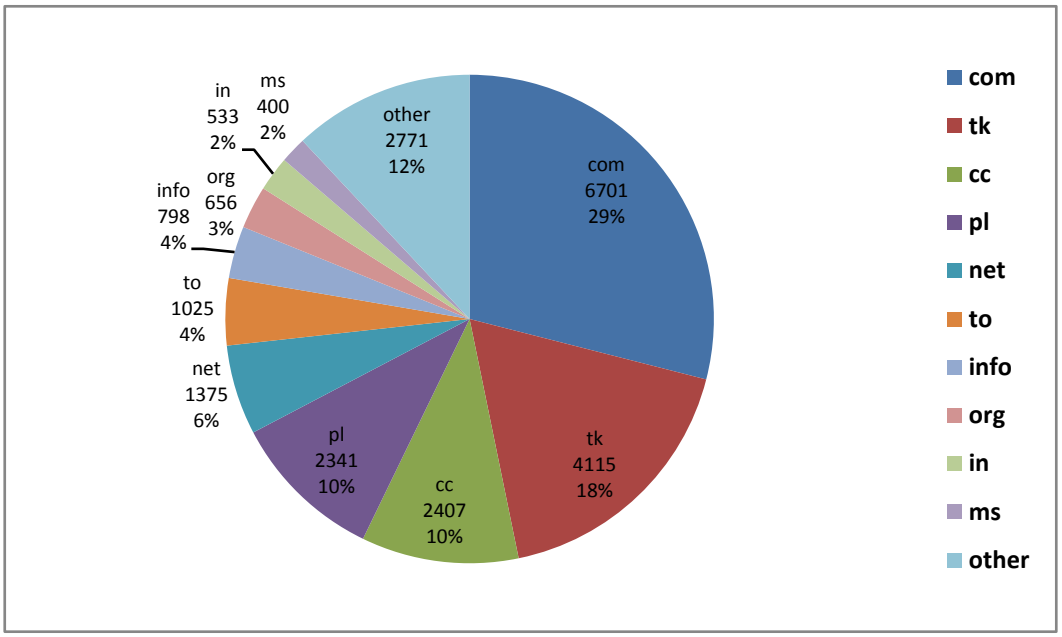

Fig. 10 Phishing Sites' Top-level-domain Sectors in 2012

Acknowledgments

We want to thank Greg Aaron from APWG for supplying data and providing advice. We want to thank Wang Liming, Hong Bo, Geng Guanggang, Chen Yong and Hu Anlei from National Domain Name Security Center in China for their work in composing this report. Meanwhile, we especially want to thank all the members in APAC and APWG for your phishing reporting and contributions to anti-phishing efforts.

Website: www.dnscert.cn
Tel: (010)58813000
Fax: (010)58812666
Email: ndsa_public@cnnic.cn