APAC

Anti-Phishing Alliance of China

中 国 反 钓 鱼 网 站 联 盟

Briefing on Handling of Phishing Websites in September 2017

Secretariat of APAC

October 2017

Contents

1 Overview

- 2624 phishing websites were handled by APAC in September 2017.
- 402239 phishing websites have been verified and managed by APAC by September 2017.
- Monthly handling of phishing websites is as follows:

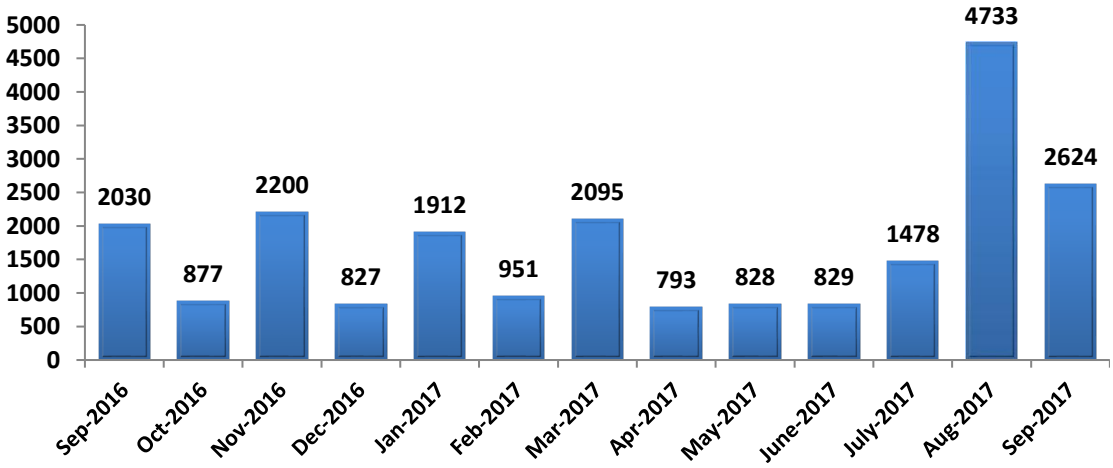

Fig. 1 Monthly handling of phishing websites

2 Analysis of Handling Types

2.1 Sources of reports about phishing websites

In this month, the reports about phishing websites are mainly from Alliance members, Alliance lab and the public.

The number of phishing websites reported by members of APAC accounted for 96.7% of all the reported phishing websites in this month.

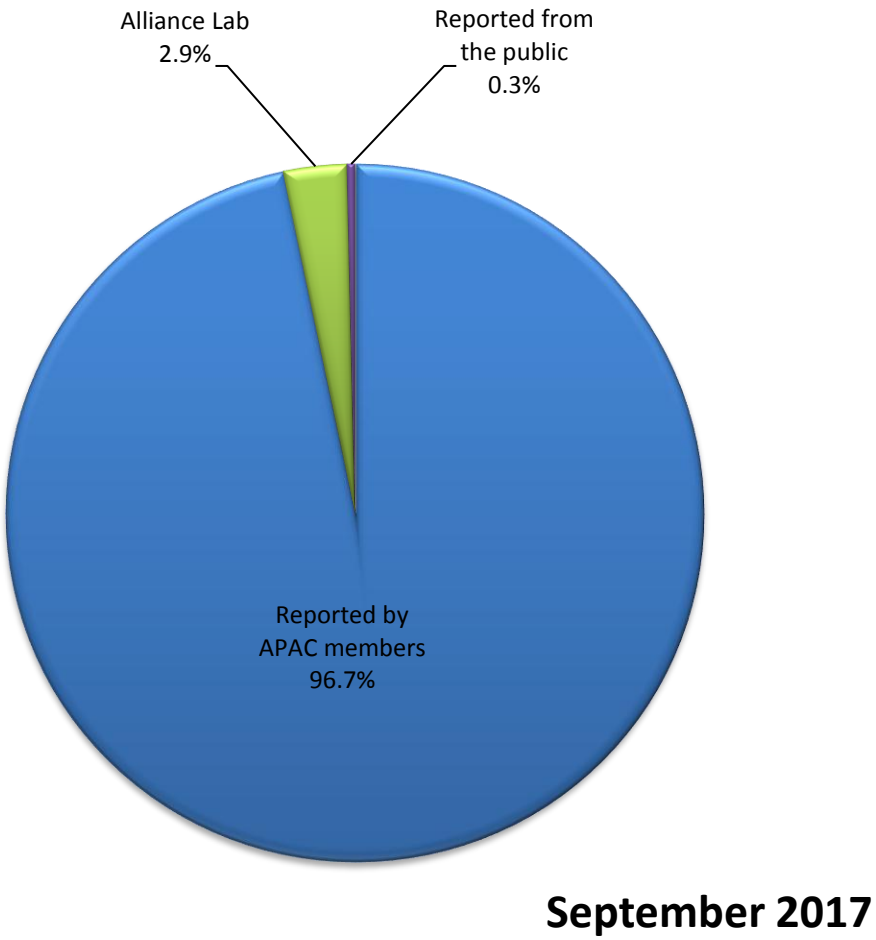

Fig. 2 Sources of reports about phishing websites

2.2 Distribution of the counterfeit objects of phishing websites this month

Among all reports about phishing websites received by APAC this month, 97.5% of all the reported phishing websites counterfeited the websites of taobao.com, ICBC, CMB and CCB. Percentage of counterfeit websites of taobao.com ranked the first in all counterfeit phishing websites.

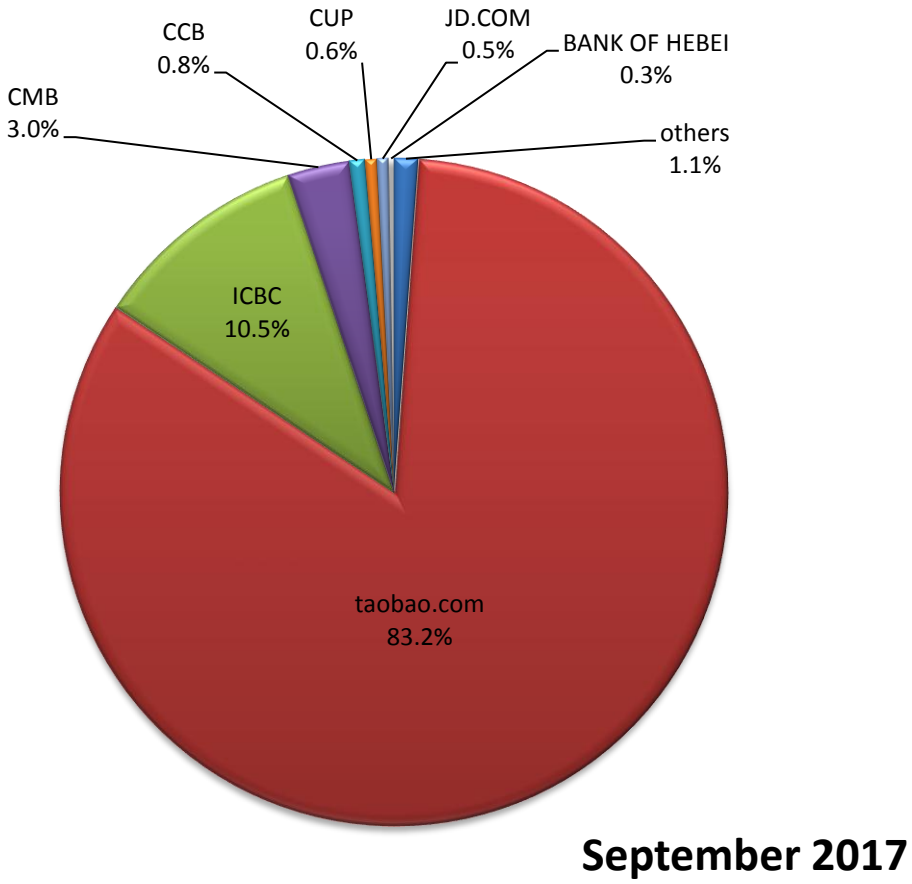

Fig. 3 Counterfeit objects of phishing websites

2.3 Distribution of industries relating to the phishing websites

The top three industries involving phishing websites in this month include payment and transactions, finance and securities, E-commerce. They made up of 99.9% of all the handled sites. The proportion of phishing websites involving payment and transactions accounts for 83.2%，ranking first of all handled websites in this month.

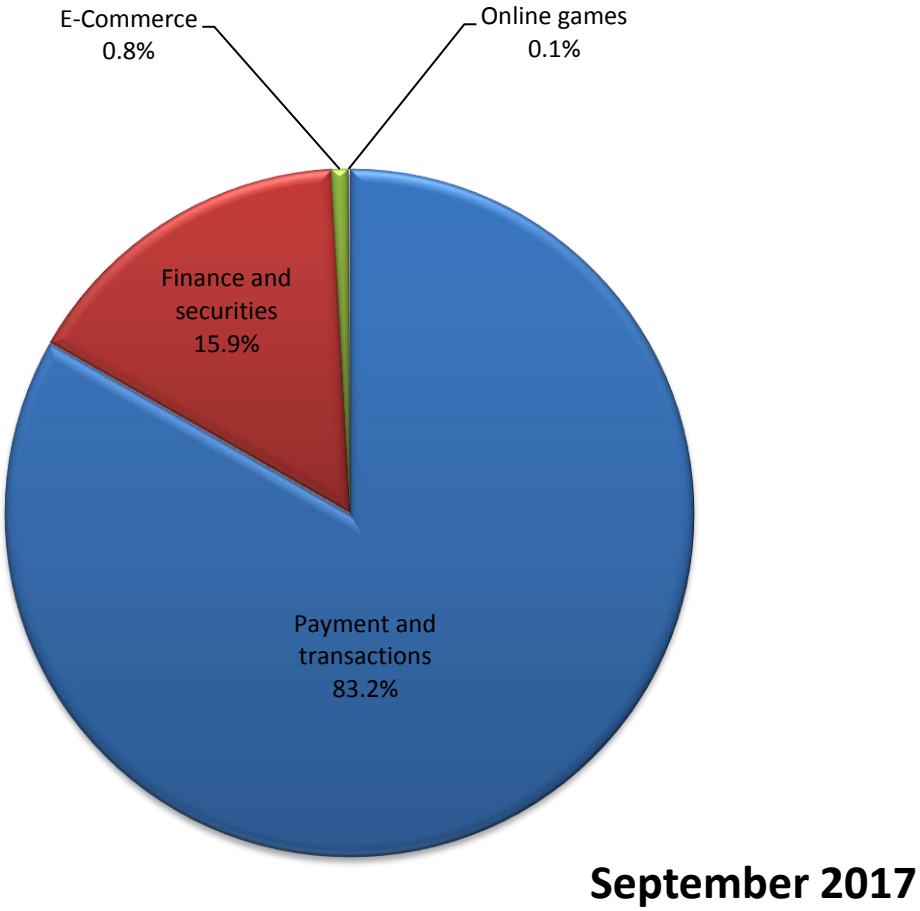

Fig. 4 Distribution of industries involving the phishing websites

2.4 Domain names distribution of phishing websites this month

a. Phishing websites with .CN domain name and non-.CN domain names

52 phishing websites with .CN domain name were reported this month, accounting for 2.0% of all the handled phishing websites of the month. Strict enforcement and unremitting improvement of the real-name registration system of .CN domain name contribute to the low percentage of phishing websites involving .CN domain name.

Phishing websites with non-.CN domain names handled this month reached 2572. The details are as follows:

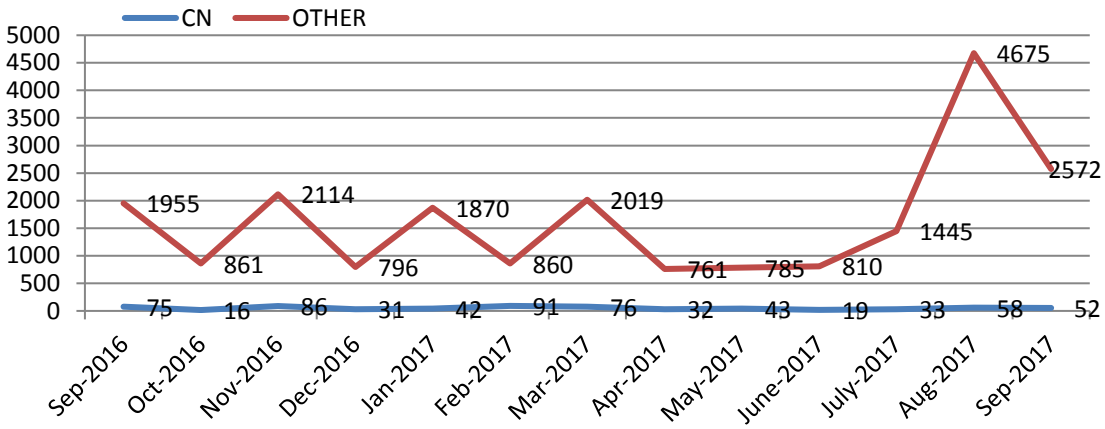

Fig. 5 Tendency chart of phishing websites with .CN(-) and non-.CN(-) domain names

2.5 Distribution of phishing website domain names in all TLDs

Phishing websites with domain names of .COM, .PW, .TK and .CC accounted for 87.1% of all the handled phishing websites, in which the phishing websites with .COM ranked the first among all domain names. Phishing websites under such unpopular domain names as .US and .TOP increased this month, with the percentage being 4.0% and 1.0% respectively of all the handled phishing websites of the month.

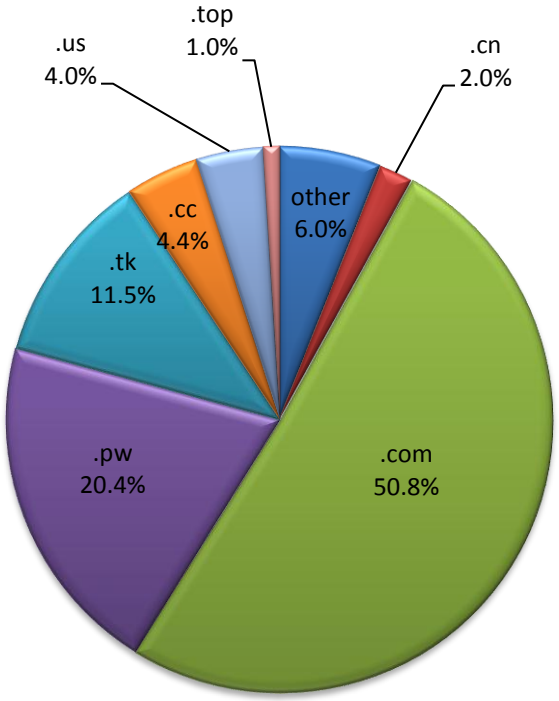

Fig. 6 Distribution of TLDs relating to the phishing websites

2.6 Distribution of registrars for phishing website domain names

a. Analysis of domestic domain name registrars

As for the registrars of phishing website domain names, the top four domestic domain name registrars are Alibaba, west.cn, Xinnet and Lanhai.cn. Percentage of phishing website domain names related to BIZCN grew this month. For the phishing websites with their domain names registered in China, their domain name resolutions have been suspended or their phishing pages have been deleted.

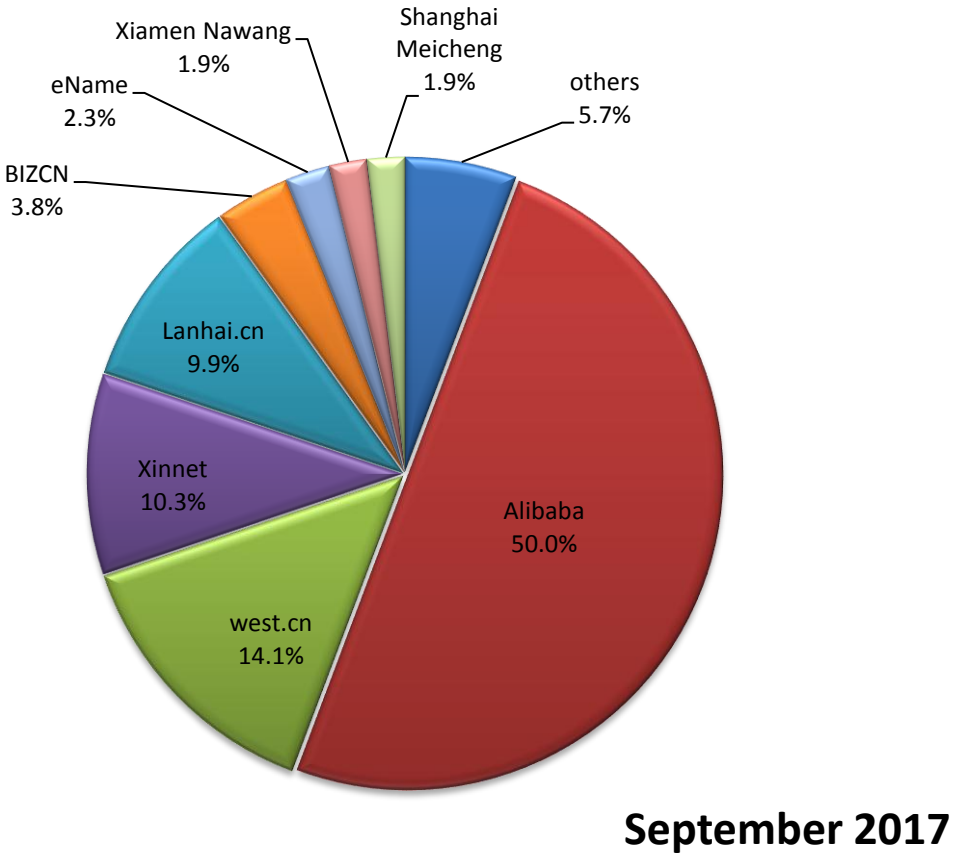

Fig. 7 Distribution of domestic registrars for phishing website domain names

b. Analysis of overseas domain name registrars

Top three overseas domain name registrars are GODADDY, DOT TK and PDR. For phishing websites with the domain names registered overseas, APAC had delivered the addresses to a third party partner to block the visit. Meanwhile, APAC delivered all phishing websites with .TK domain name to DOT TK, which would assist in suspending the resolution.

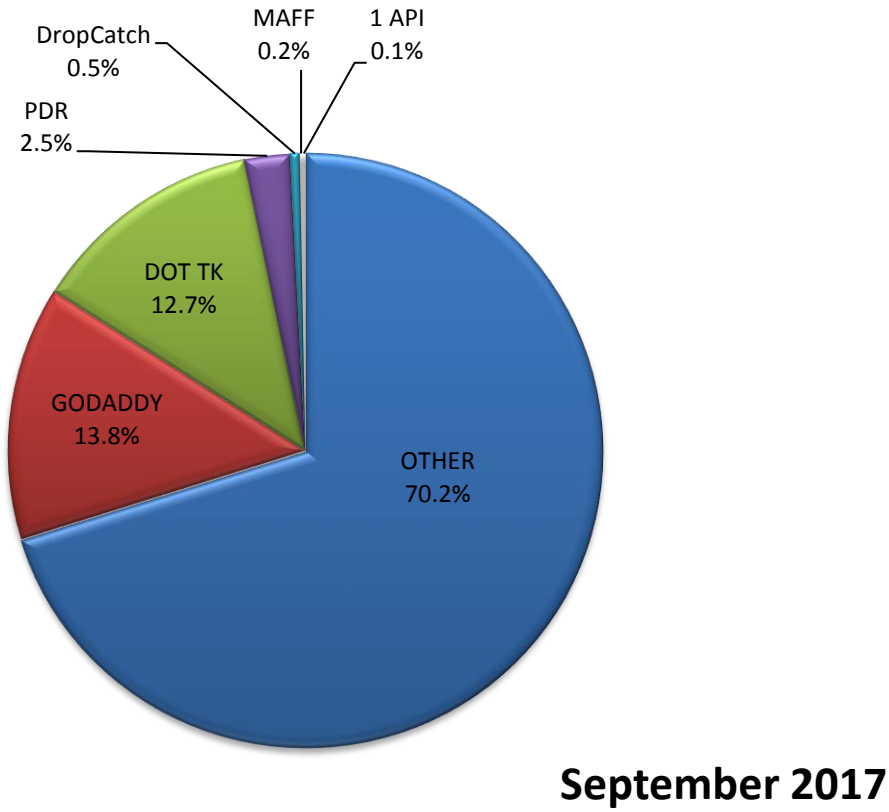

Fig. 8 Distribution of major overseas registrars for phishing website domain names

Profile of Anti-Phishing Alliance of China

Founded on July 18, 2008, the Anti-Phishing Alliance of China ("APAC") is made up of domestic banks, securities institutions, e-business websites, domain name registries, domain name registrars, experts and scholars, serving as the only coordination organization for the purpose of solving the problem of phishing websites. At present, it has more than 500 member units. APAC has established a quick handling mechanism to address the problem. By stopping resolution services for phishing websites with a CN domain name or non-CN domain name or by giving warnings, APAC terminates the harm of such websites in a timely manner to ensure a trusted network. China Internet Network Information Center ("CNNIC"), the domain name registry in China, fulfills the responsibility of the secretariat of APAC.

At present, various phishing websites in the world have had a severe impact on online financial services and e-business development, jeopardized public interest and shaken the confidence of the public in using the Internet. Due to the features of the Internet, the cross-boarder distribution and hazard of phishing websites have become an intractable problem that draws the worldwide attention. Therefore, it is a top priority to stop the harm of phishing websites in a timely and effective manner by establishing a quick handling mechanism. APAC is devoted to establishing an anti-phishing coordination mechanism, facilitating the construction of a comprehensive management system, enhancing cooperation and exchange on anti-phishing efforts, sharing information in this regard, and organizing its members to jointly prevent, discover and tackle phishing websites.

APAC is the first non-governmental industrial coordination organization in China established for the sole purpose of solving this problem. By borrowing international experience and practices and focusing on the "short survival but great harm" feature of these websites, APAC has coordinated the efforts of all interested parties and established a quick handling mechanism against phishing websites so as to prevent any potential harm. It cracks down on phishing websites from the root of Internet application—domain name, aiming at constructing a trusted network.
To best safeguard public interest, APAC will first protect financial institutions such as major banks and securities institutions, famous e-business enterprises and online payment systems which are closely related to the property of the public. Phishing websites have frequently shown up in these fields, causing great losses.

In particular, APAC has set up an Expert Guiding Committee which is made up of experts and leaders to guide APAC in its work. The National Computer Virus Emergency Response Center and the National Computer Network Emergency Response Technical Team/Coordination Center of China act as the third-party technical validation institutions of APAC.

APAC is a non-governmental organization whose members include domain name registries, domain name registrars, banks, securities institutions, e-business enterprises and network security enterprises, and whose purpose is to discover and tackle phishing websites, especially those that pretend to be its members. So far, APAC has included more than three hundred financial

institutions and dozens of e-business websites, as well as major domestic registrars of domain names.

The Secretariat of APAC is based at CNNIC, and is responsible for the daily operation, meeting convening and emergency handling of APAC.

Experts of APAC are reminding netizens to be cautious during online shopping and E-bank payment so as not to be harmed by phishing websites.