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

2014

Global Chinese Phishing Attack Trends Report

Global Chinese Phishing Attack Trends Report

(2014)

National Engineering Laboratory for Naming and Addressing

and

Anti-Phishing Alliance of China (APAC)

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

June 2015

Table of Contents

i. General Introduction

1. Definition of Phishing Attacks

Phishing (pronounced the same as *fishing*) is one of the most popular types of network attacks where the attacker posts a fraudulent message through spam, instant messaging, social networking sites and other information carriers, to trick Internet users into accessing his fake sites (i.e. phishing sites), luring them into disclosing their sensitive information (such as user name, password, account, ATM PIN code or credit card details). Consequences vary, ranging from breach of privacy all the way to severe economic losses.

"Chinese phishing attacks" herein refers specifically to phishing attacks targeting domestic brands (Taobao, Industrial and Commercial Bank of China (ICBC), Hunan Satellite TV, etc.).

2. Scope & Methodology

The *Global Chinese Phishing Attack Trends Report (2014)* analyzes the phishing attacks targeting Chinese brands and users over the world in 2014. The statistics insist of three sources: the phishing attacks reported to the **Anti-Phishing Alliance of China** (**APAC)**, the phishing attacks detected by **National Engineering Laboratory for Naming and Addressing**, and the global Chinese phishing attacks reported to the **Anti-Phishing Working Group (APWG)** by its members. In the data set, 20.4% 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 targeting different brands; 2. there are legitimate sites whose pages are exploited by phishers; 3. most of the anti-phishing tools block the phishing attacks via the full URLs.

3. Key Statistics

- The number of global Chinese phishing attacks continuously increased during the past three years. In 2014, there were at least **55,063** unique Chinese phishing attacks worldwide, which is a little lower than that of 2013 but still remains at a high level.
- In 2014, 78.4% of the Chinese phishing attacks used three TLDs:**.COM, .TK, and .PW**.
- The top ten Chinese phishing TLDs by the Domain score "Phishing Domains per 10,000" are: **.CF, .PW, .ML, .GA, .EDU, .SX, .CC, .GD, .BI, and .TL,** among which .**CF, .GA, and .ML** ccTLD registries offer free domain names. **.CF** is most likely to be used by the phishers, with the domain score as high as 228.
- **322** Chinese phishing attacks occurred in new gTLDs, including .**XYZ, .WANG, .SEXY and .CLUB.**
- The top three targets that accounting for **92.1%** of Chinese phishing attacks are: **Taobao, ICBC, and Human Satellite TV.**
- In 2014, the average uptime of Chinese phishing attacks is **33.1 hours**, compared with that of the global phishing attacks is **31.2 hours.**

ii. Phishing Attacks Trends

In 2014, a total of 55, 063 Chinese phishing attacks were detected worldwide, which is a little lower than that of 2013 but still remains at a high level. Figure 1 shows the yearly trend of global Chinese phishing attacks. As is shown in the figure, the number increased year by year, which indicates that phishing has become a prominent threat to network security and the network security situation and challenges are getting grimmer.

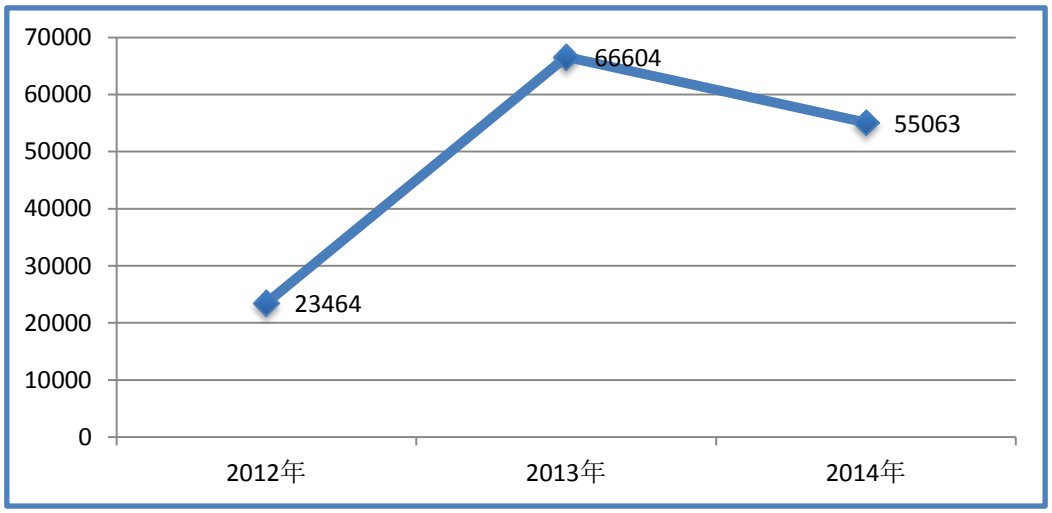

Fig. 1 The number of global Chinese phishing attacks by year

Figure 2 depicts the number of Chinese phishing attacks by month in 2014, which peaked in July .

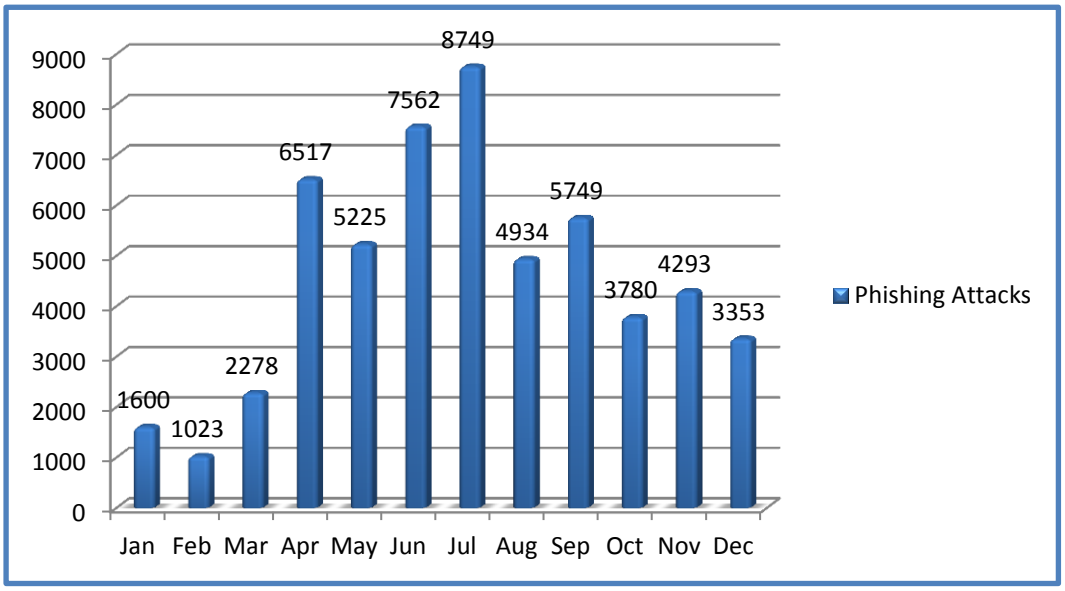

Fig. 2: Phishing attacks by month in 2014

iii. Phishing Domains Statistics

Except for a very few phishing websites that provided service only through IP addresses, most phishing sites appear of websites hosted on domain names.

1. Distribution of TLDs Used by Phishing attacks

Chinese phishing occurred in 143 top-level domains (TLDs), with 13 more than that of 2013.

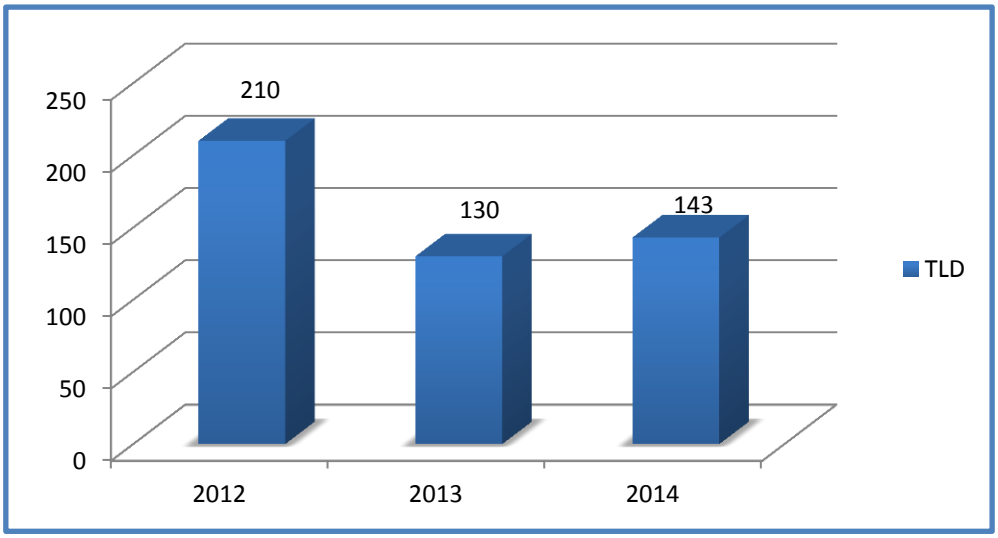

Fig. 3: The number of TLDs used by Chinese phishing attacks

78.4% of the phishing sites were just in three TLDs: .COM, .TK, .PW. As is the case in past years, .COM is still the most commonly used TLD by phishers in 2014.

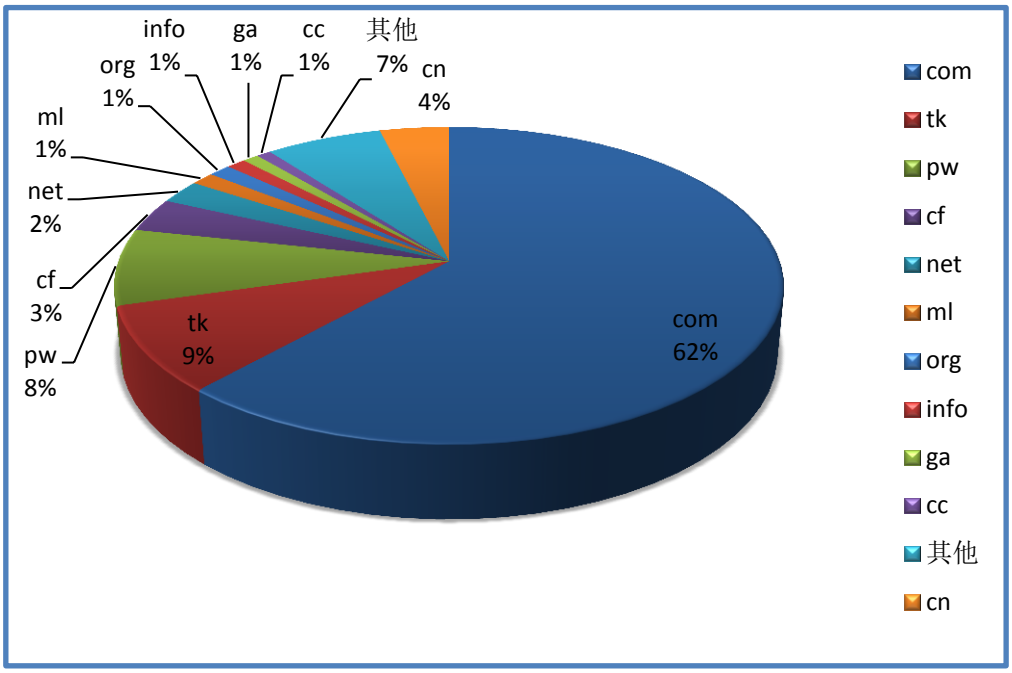

Fig. 4: Top ten TLDs used by phishing

The phishing attacks distribution of the top three TLDs are shown in Figure 5:

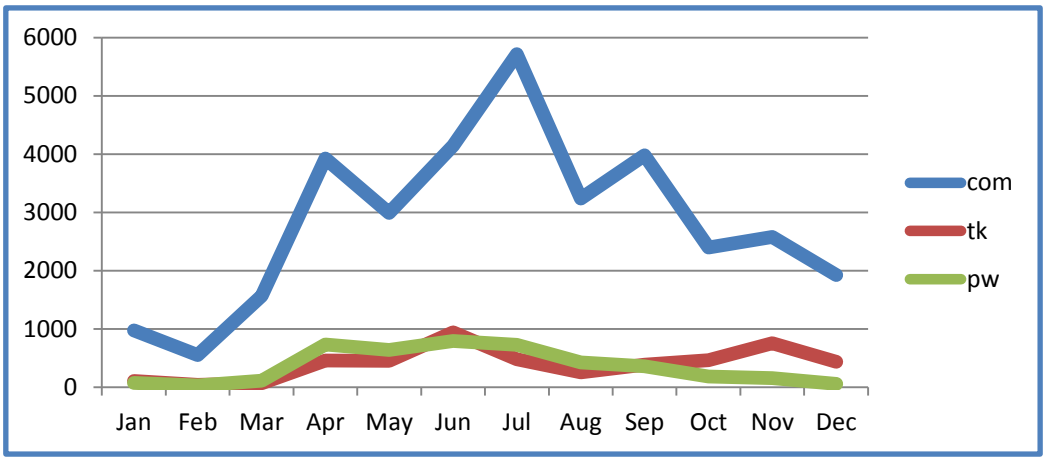

Fig. 5: The phishing attacks distribution of the top three TLDs by month

2. Chinese Phishing Domains Score[1]

To put the numbers in context and measure the prevalence of phishing in a TLD, we use the metric “Chinese Phishing Domains score”. “Chinese Phishing Domains score” is a ratio of the number of domain names used for Chinese phishing attacks in a TLD to the number of registered domain names of that TLD. This metric is a way of revealing whether a TLD has a higher or lower incidence of phishing relative to others.

Chinese Phishing Domains score

$$= Chinese\ Phishing\ attacks\ Amount\ in\ a\ \ TLD * 10000 / Total\ Registration\ Volume\ of\ \ theTLD$$

Table 1: TOP 10 Chinese Phishing Domains by Domain Score

Rank	TLD	TLD Location	Unique Chinese Phishing Attacks	Unique Domain Names Used for Phishing	Domains In Registry	Score: Chinese Phishing Domains per 10000
1	.CF	Central-African-Republic	1900	1850	81000	228
2	.PW	Palau	4293	3901	229639	170
3	.ML	Mali	718	684	86000	80
4	.GA	Gabon	497	471	98000	48
5	.EDU	U.S.-higher-education	9	8	7590	10.5
6	.SX	Sint-Maarten	5	4	4600	8.7
7	.CC	Cocos-(Keeling)-Islands	445	294	350000	8.4
8	.GD	Grenada	30	2	2800	7.1
9	.BI	Burundi	1	1	1400	7.1
10	.TL	Timor-Leste	6	1	2200	4.5

Table 1 shows the top ten TLDs with a higher domain score, among which the .CF, .GA, and .ML ccTLD registries were repurposed in 2013 to offer free domains names and they are operated by Freenom. Therefore, loose domain name registration and verification mechanism, as well as inexpensive or even free registration, make these domains more likely to be utilized for phishing.

We took a further analysis on the widely used TLDs in the world: .COM and.CN. .COM had a

[1] This score is based on the metric "Phishing Domains per 10,000" of APWG report *Global phishing Survey: Trends and Domain Name Use in 1H2014*.

domains-per-10,000 score of 4.1 while.CN gets a score of 1.57. Therefore, .CN is less likely to be used by Chinese phishing attacks. Considering that most of.CN domain names are registered for the purpose of Chinese web services and foreign domain names are mainly registered for foreign-language website services, we conclude that to domestic Internet users, websites that use .CN are more reliable.

3. Phishing Domain Names and Registrars Distribution

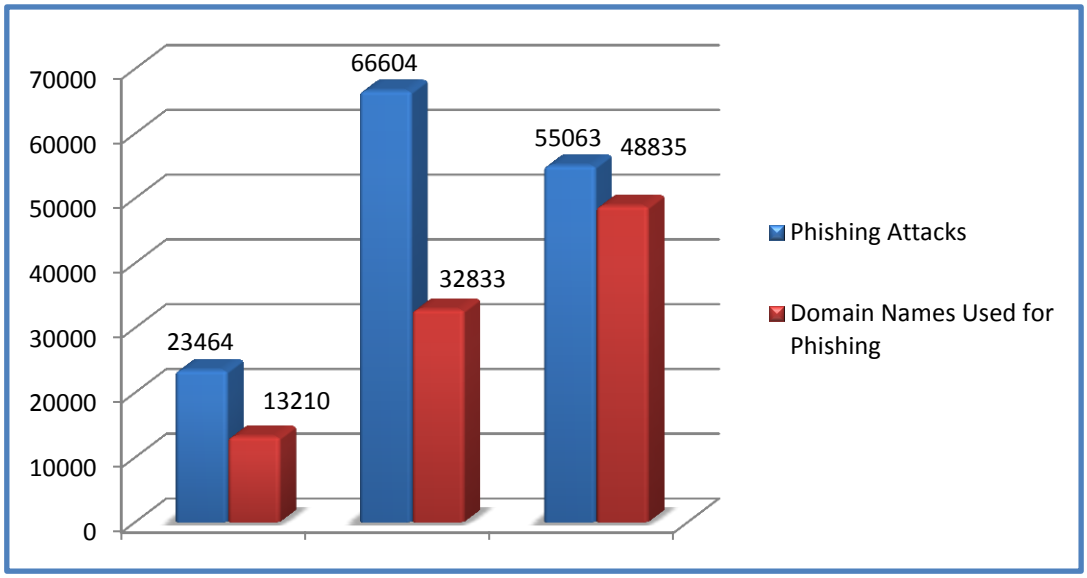

Fig. 6: The number of Chinese phishing attacks in the world and their domain names by year

The global Chinese phishing attacks number was 55,063 in 2014, wherein 48,835 were unique domain names, meaning a considerable part of the domain names were used by multiple phishing attacks.

According to our analysis, the top ten domain names that are most repeatedly used are listed in Figure 7, among which findhere.org has been used exclusively to counterfeit ICBC to launch phishing attacks; while t.cn and tinyurl.com are URL shortening services which reduce lengthy URLs into shortened ones. It is suggested that more inspection of phishing URLs are

required in order to avoid the abuse of URL shortening services.

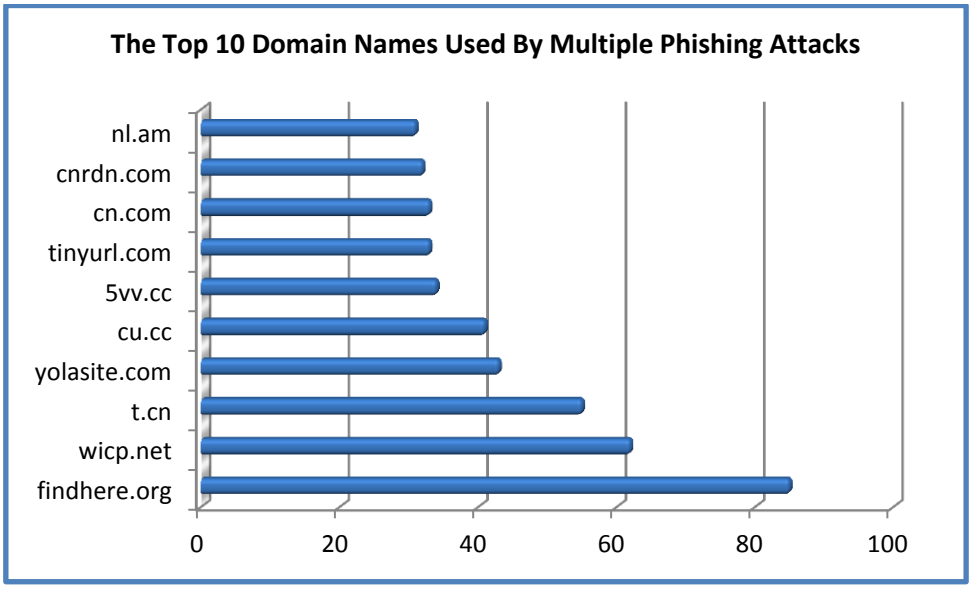

Fig. 7: Domain names repeatedly used by phishing attacks

We performed an analysis of how many domain names were registered by phishers, versus phish that appeared on compromised (hacked) domains. These different categories are important because they offer insights into how phishers commit their crimes. We flagged a domain as malicious if it was reported for phishing within a very short time of being registered, and/or contained a brand name or misleading string, and/or it was registered in a batch or in a pattern that indicated common ownership or intent.

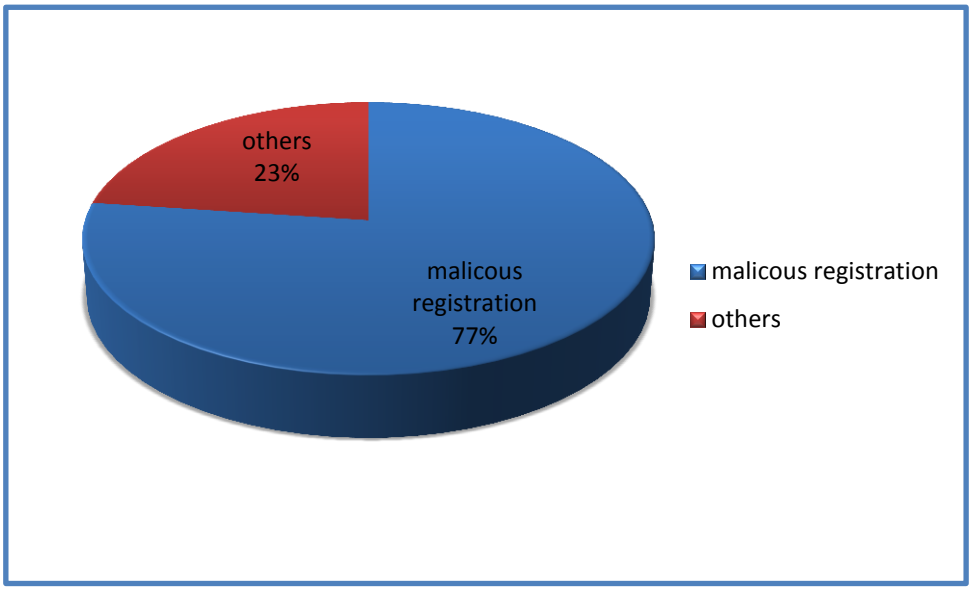

Fig. 8: Phishing attacks categories

Of the 55,063 phishing attacks, 42,460 (77%) attacks use domains names that we believe were registered maliciously by phishers. The other types include hacked domains, subdomain services and URL shortening services, among which hacked domains has the highest proportion of about 7.6%.

About 64% of malicious registrations are sponsored by registrars listed in Figure 9. Among them, Network Solutions, PDR, Freenom, GoDaddy and Register.com are foreign registrars, indicating that a large portion of the phishers prefer to utilize foreign registrars to avoid supervision.

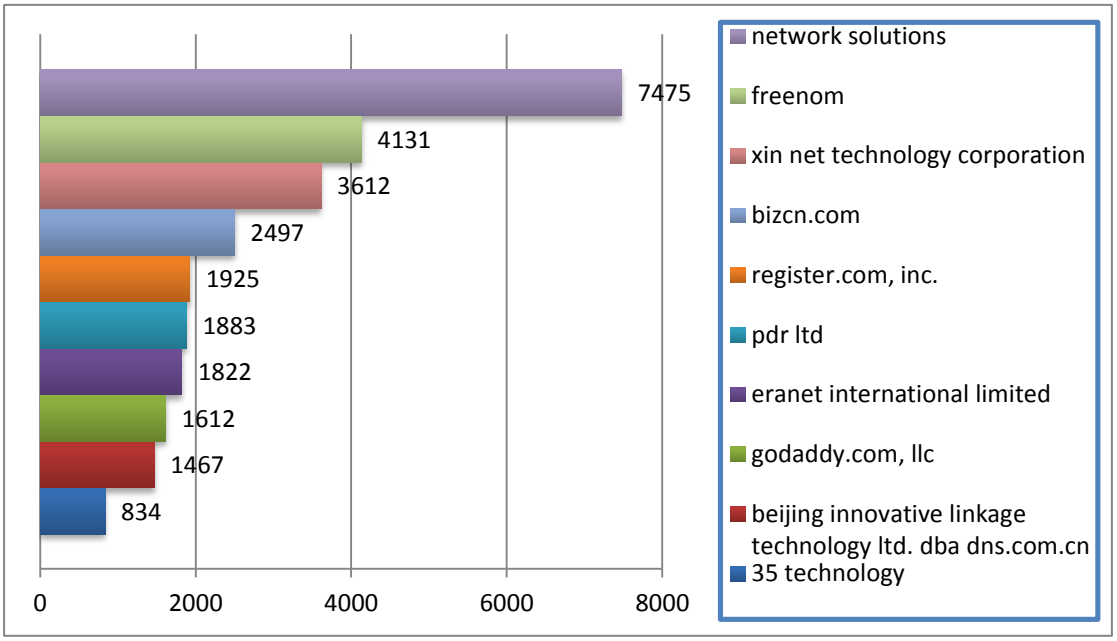

Fig. 9: Top ten registrars sponsoring maliciously registration

iv. The Distribution of Phishing Attacks in New gTLDs

At the beginning in January 2014, the first of the new generic top-level domains (gTLDs) began rolling out. Approximately 1,200 new gTLDs will launch from 2014 through 2016. So what the impact will the introduction of new TLDs bring in on phishing?

As Table 2 shows, a small number of phishing attacks were seen in the new gTLDs including .XYZ, .WANG, .SEXY and .CLUB. As of this writing, the new gTLD program has not resulted in a bonanza of phishing.

Table 2: Statistics of phishing attacks in new gTLDs

TLD	Unique Chinese Phishing Attacks	Unique Domain Names Used for Phishing	Domains In Registry	Score: Chinese Phishing Domains per 10000
.XYZ	308	272	796391	3.4
.WANG	12	10	97591	1.02
.SEXY	1	1	17645	0.57
.CLUB	1	1	160591	0.06

(Note: more Details about "Phishing domains per 10000 domains" in the table can be found in Section 2, Chapter 3)

Figure 10 shows that phishing attacks in new gTLDs did not appear until the second half of 2014. This is because most of the new gTLDs have been in their early phases of introduction. Those that have been available for purchase by the general public have usually been priced higher than .COM and other popular legacy TLDs. This situation will certainly change, though. As autumn 2014 begins, the new gTLD market is becoming more crowded and competitive, and some registries have begun to compete aggressively on price. As prices drop and the new gTLDs gain more adoption, we are seeing an increase in phishing on new gTLDs, due to both malicious registrations and compromised domains on hacked servers.

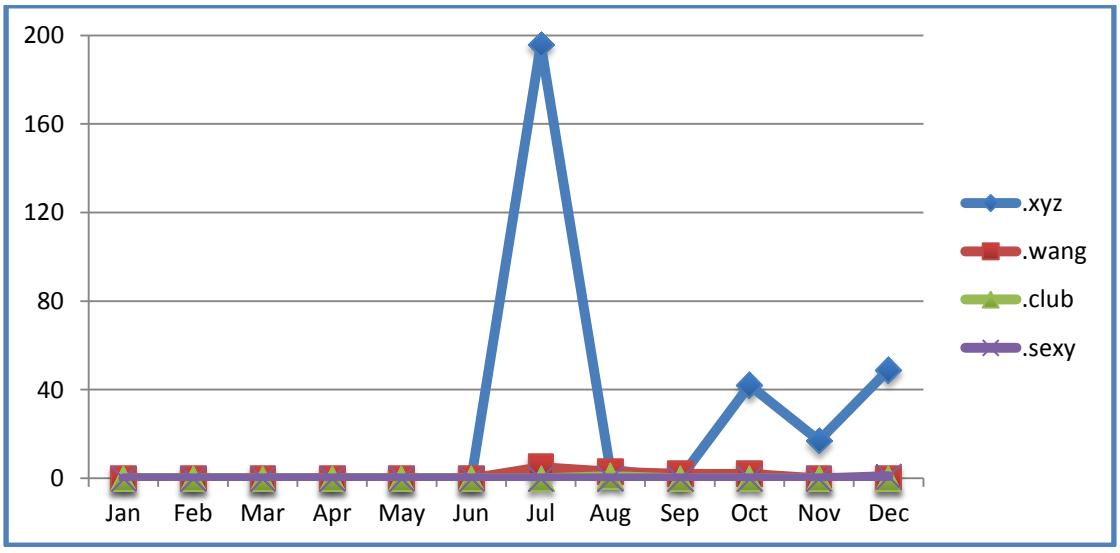

Fig. 10: Monthly phishing attacks trends in new gTLDs

v. Target Distribution

The 2014 phishing data shows that Taobao[2] is the target of 80.7 % of the Chinese phishing attacks. And the target distribution is shown in Figure 11.

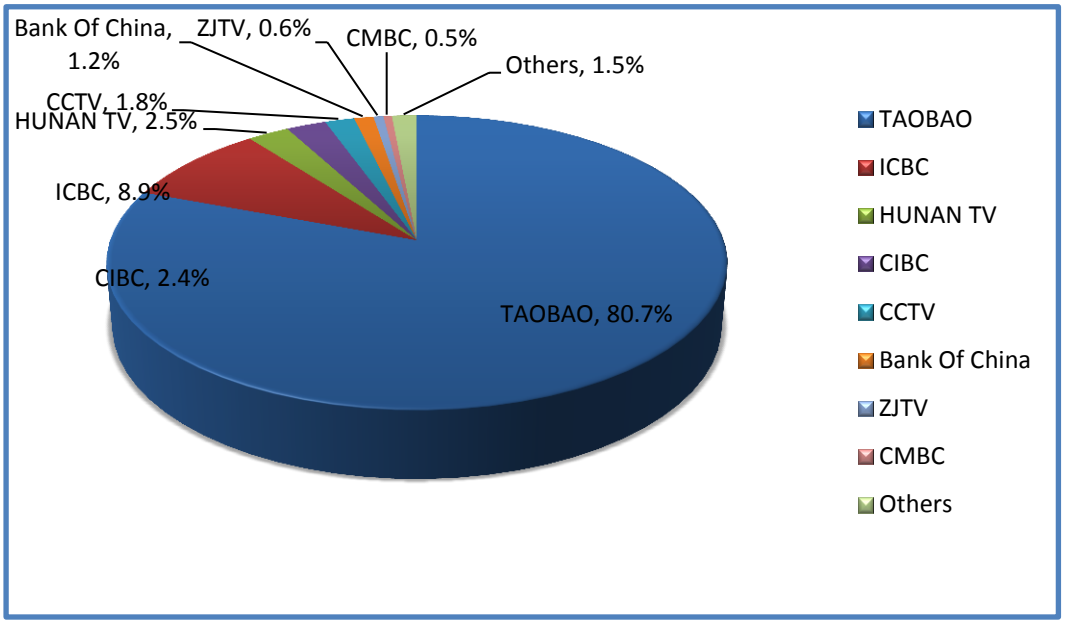

Fig. 11: Target distribution

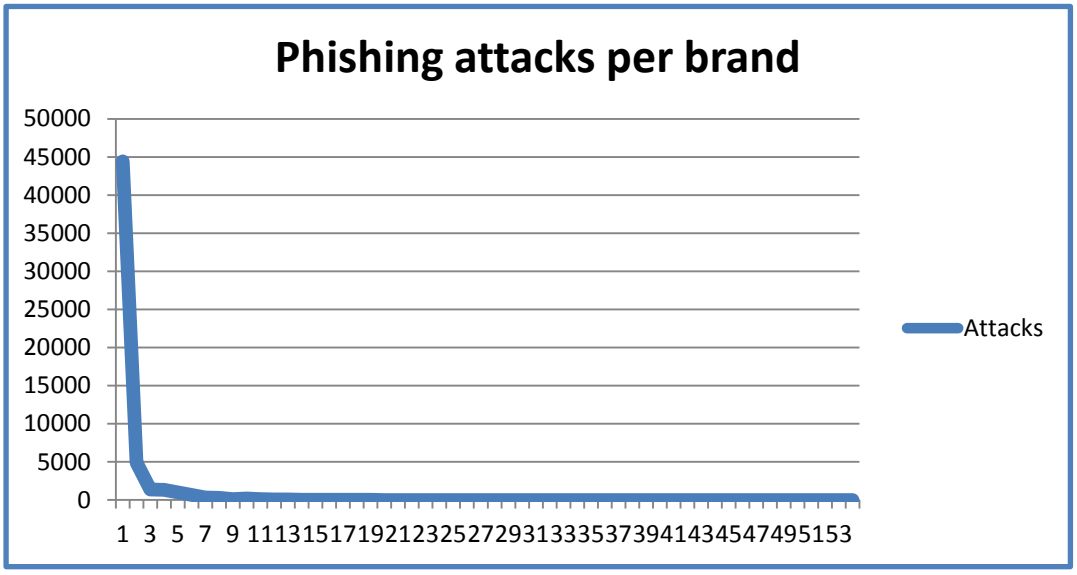

Fig. 12: Rank of brand by phishing attempts against it

[2] Including Taobao, Alibaba and AliPay

Figure 12 shows that the number of times that the targets were attacked follows a long tail. Despite that brands targeted by Chinese phishing attacks were diverse, most of the attacks are concentrated on a small group of brands. The top 3 targets (Taobao, ICBC, Hunan Satellite TV) accounting for 92.1% of all the phishing attacks observed worldwide; about a third of the targeted brands was attacked by only once in 2014. The monthly phishing attacks number of the top three targets is shown in Figure 13:

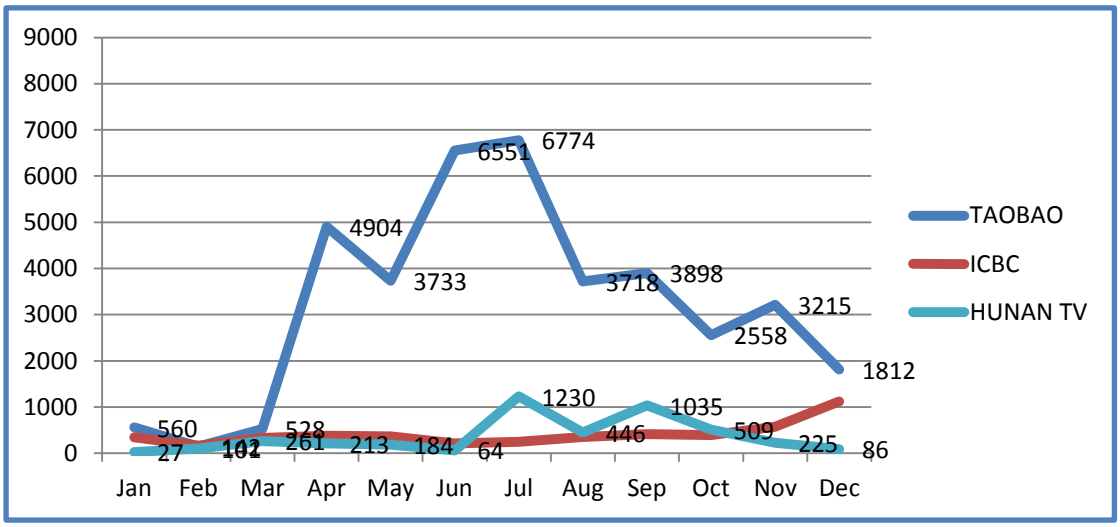

Fig. 13: Phishing attacks of the top three targets by month

vi. Uptime By Phishing

The “uptime” or “live” time of phishing attacks are a vital measurement of how damaging phishing attacks are, and are a metric of the success of mitigation efforts. The first day of a phishing attack is the most lucrative for the phisher, so quick take downs are essential.

Figure 14 shows the average uptime[3] of Chinese phishing attacks is 33.1 hours, while the

[3] The calculation of uptime is based on sampling data (about 20%of the total data).

average uptime of global phishing attacks is 31.2 hours[4].Combined with Figure 15,it is apparent that average uptime of Chinese phishing attacks in the first half of 2014 increased remarkably compared with the same period in 2013. And in the second half of 2014, after a decline in July, September and October, the average active time peaked in November, which is as long as 60 hours.

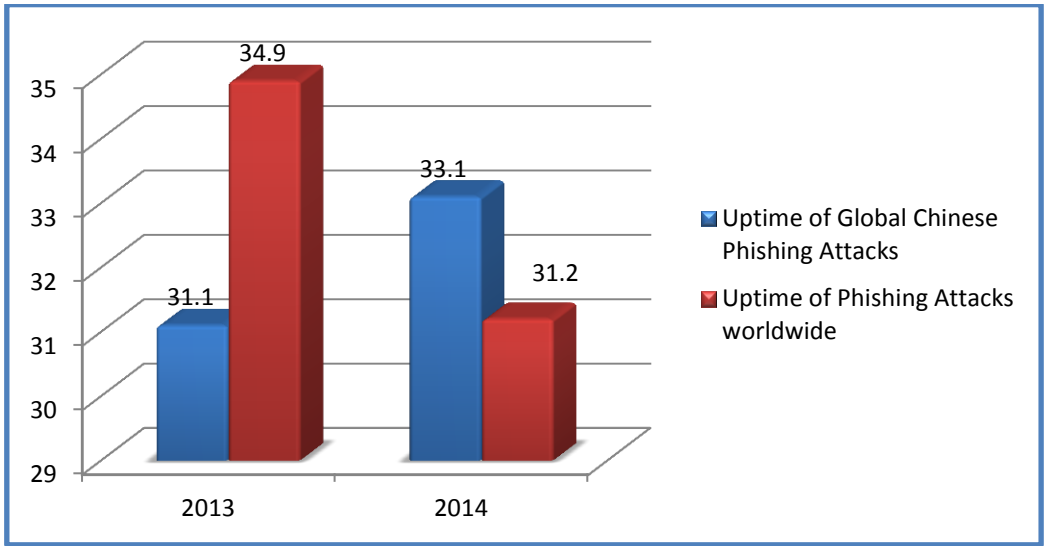

Fig. 14: Average uptimes: global phishing attacks vs. Chinese phishing attacks (Unit: hour)

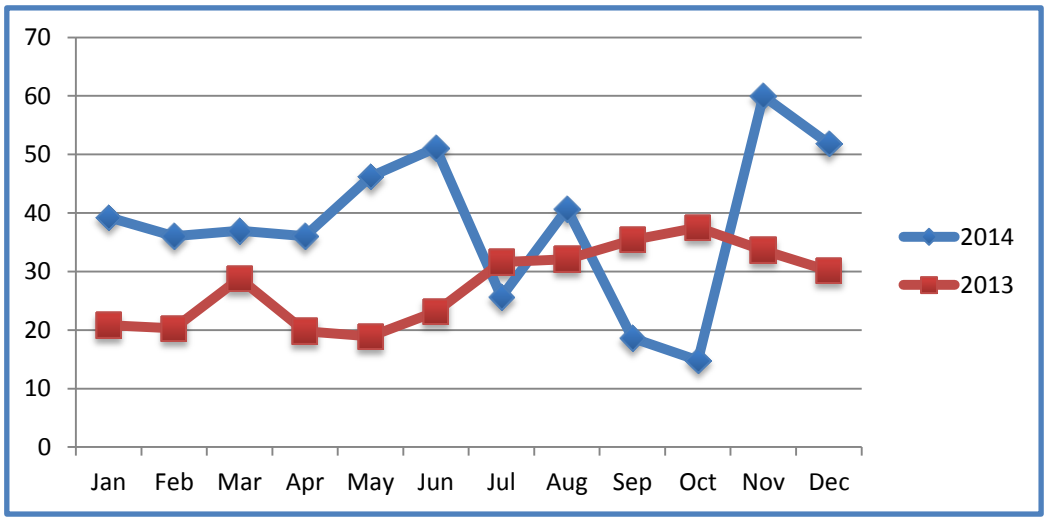

Fig. 15: Average uptimes of Chinese phishing attacks by month (Unit: hour)

[4] See the APWG reports *Global Fishing Survey: Trends and Domain Name Use in 1H2014* and *Global Fishing Survey: Trends and Domain Name Use in 2H2014*

Acknowledgments

This report is prepared by the Internet Fundamental Technology Lab of CNNIC, and jointly issued by the National Domain Name Security Center, the Anti-Phishing Alliance of China (APAC) and the Anti-Phishing Working Group (APWG). We would like to thank Greg Aaron from APWG for the contribution of phishing data for this report. We also acknowledge the work of APWG and APAC members who have contributed to anti-phishing programs and research.

ADD: 4 South 4th Street, Zhongguancun
POB: Beijing 349, Branch 6, CNNIC
TEL: 8610-58813000
FAX: 8610-58812666
WEB: www.dnscert.cn
E-Mail: ndsa_public@cnnic.cn