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

2014年
全球中文钓鱼网站趋势分析报告

全球中文钓鱼网站趋势分析报告

（2014 年）

互联网域名管理技术国家工程实验室

中国反钓鱼联盟（APAC）

反钓鱼工作组（APWG）

2015 年 6 月

目 录

一、总体情况

1. 网络钓鱼定义

网络钓鱼（phishing，和钓鱼的英文 fishing 发音相同），是指攻击者通过垃圾邮件、即时通信、社交网络等信息载体，发布欺诈性消息，骗取网络用户访问其构建的仿冒网站（即钓鱼网站），引诱用户泄露其敏感信息（如用户名、口令、账号、ATM PIN 码或信用卡详细信息）的一种当前极为流行的网络攻击方式。被攻击的用户，轻者泄露个人隐私，重者遭受经济损失。

本报告“中文钓鱼网站”指针对国内品牌（淘宝、中国工商银行、湖南卫视等）的钓鱼网站。

2. 本报告的统计范围和统计方法

《全球中文钓鱼网站趋势分析报告_2014 年》汇总并统计了 2014 年全年在全球范围内针对中国网站和用户的中文钓鱼攻击事件。其使用的数据主要由三部分构成：**中国反钓鱼联盟（APAC）**的成员举报数据，**互联网域名管理技术国家工程实验室**的钓鱼检测数据和**反钓鱼工作组（Anti-phishing Working Group，APWG）**会员全球范围内举报的中文钓鱼数据。其中，APWG 贡献的全球中文钓鱼数据占到总数据量的 **20.4%**。

本报告针对钓鱼网站数量的统计是基于钓鱼 URL 进行的，即包括主机名和路径名在内的完整的钓鱼 URL 只要和其他钓鱼 URL 不完全相同，则认定为一个独立的钓鱼网站。采取该种统计方法，而不是直接统计钓鱼主机数量的原因如下：1.存在同一个钓鱼主机下挂载了多个仿冒不同目标品牌的钓鱼网页的情况；2.存在正常主机下面的子页面被篡改为钓鱼站点

的情况；3.网络安全工具针对钓鱼攻击的防护主要是基于完整 URL 进行访问拦截。

3. 2014 全球中文钓鱼网站重要数据摘要

- 近三年来，全球中文钓鱼网站数量逐年上升。2014 年全年，针对中文网民的钓鱼网站数量为 **55063** 个，同比 2013 年有所下降，但仍居于高位。7 月份，钓鱼网站数量达到峰值。
- 2014 年全球中文钓鱼网站使用最多的前三位顶级域为：**.COM、.TK、.PW，**占全年钓鱼网站总量的 **78.4%**。
- 每 10000 个注册域名中出现中文钓鱼网站比例最高前十个顶级域分别为：**.CF、.PW、.ML、.GA、.EDU、.SX、.CC、.GD、.BI、.TL**，其中**.CF、.ML、.GA** 均为提供免费注册服务的顶级域。**.CF** 钓鱼网站出现比例最高，达到$^{228}/_{10000}$。
- **322** 例钓鱼网站使用**新通用顶级域**，包括.**XYZ、.WANG、.SEXY、.CLUB**。
- 2014 年钓鱼网站攻击品牌统计前三位分别为：**淘宝，中国工商银行，湖南卫视，**占钓鱼网站总量的 **92.1%。**
- 2014 年中文钓鱼网站**平均活跃时间**为 **33.1** 小时，全球钓鱼网站平均活跃时间为 **31.2** 小时。

二、钓鱼网站数量统计

2014 年，共发现中文钓鱼网站 55063 个，较之 2013 年有所下降，但仍居于高位。图 1 描述了全球中文钓鱼网站数量按年统计趋势。该图显示近两年的中文钓鱼网站数量同比 2012 年大幅增加。网络钓鱼已成为威胁网络安全的突出问题，网络安全形势与挑战日益严

峻。

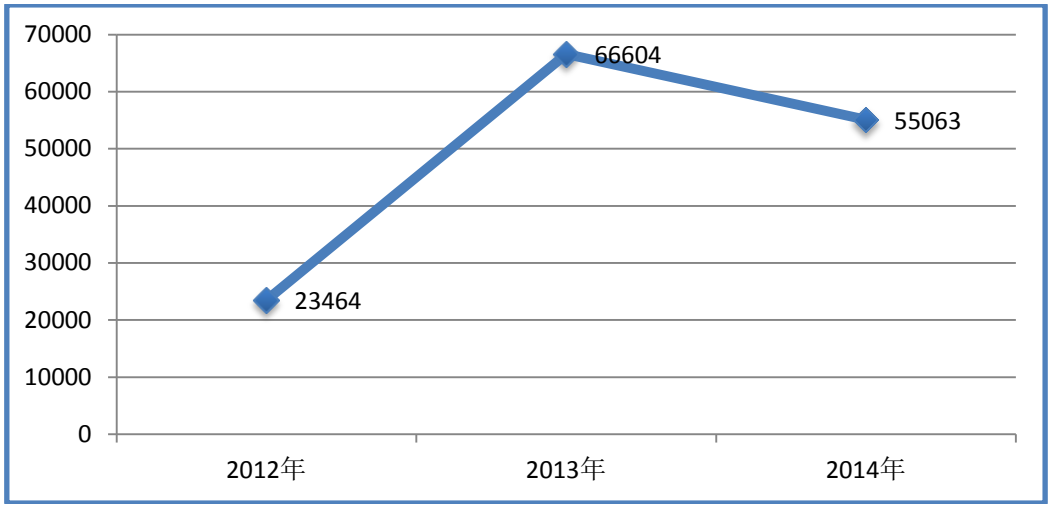

图 1：全球中文钓鱼网站数量按年统计趋势

图 2 描述了 2014 年全球中文钓鱼网站数量按月统计趋势，其中 2014 年 7 月份，钓鱼网站数量达到峰值。

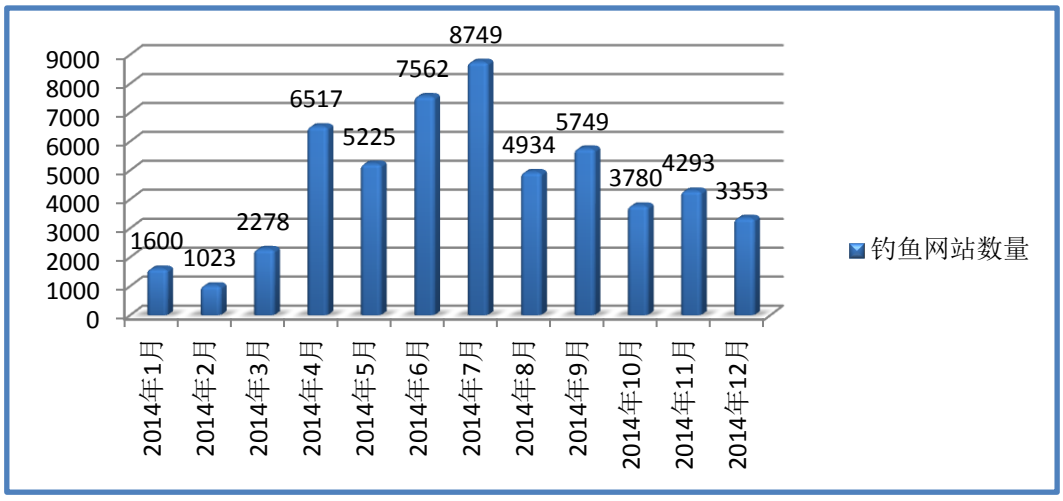

图 2：2014 年全球中文钓鱼网站数量按月统计趋势

三、钓鱼域名统计情况

除了极少数直接使用 IP 地址提供访问的钓鱼网站以外，绝大部分钓鱼网站采用域名作为其网站的访问入口。

1. 钓鱼网站顶级域分布趋势

2014 年，全球中文钓鱼网站共涉及 143 个顶级域，同比 2013 年增长 13 个。

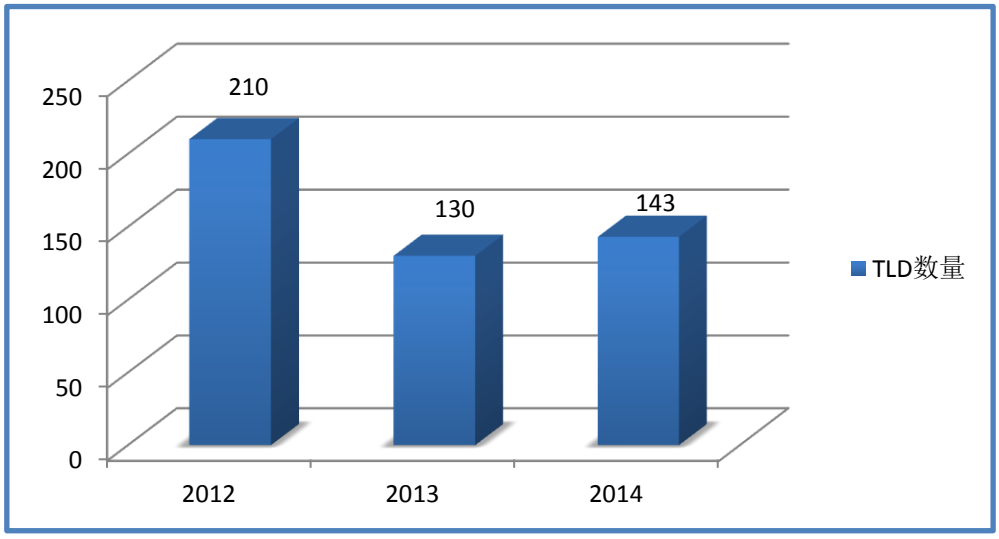

图 3：中文钓鱼网站顶级域数量变化趋势

2014 年钓鱼网站数量最多的前三位顶级域为：.COM、.TK、.PW，占钓鱼网站总量的 78.4%。和历史数据一样，.COM 域名依然是 2014 年全球中文钓鱼网站数量最多的顶级域。

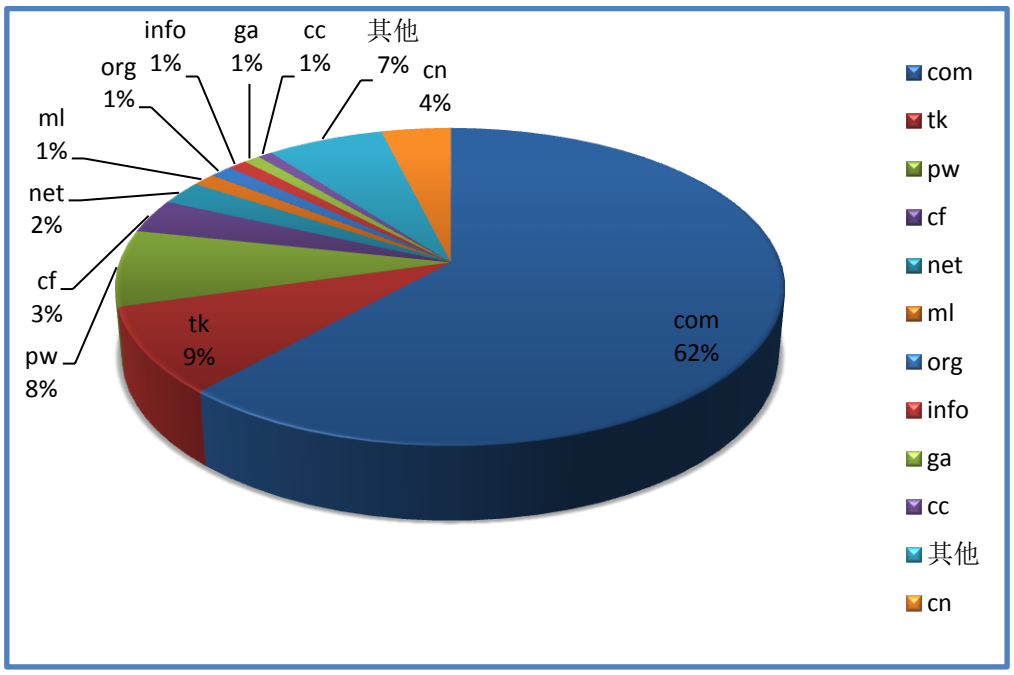

图 4：钓鱼网站顶级域分布

排名前三位顶级域具体分布和按月趋势如图 5 所示：

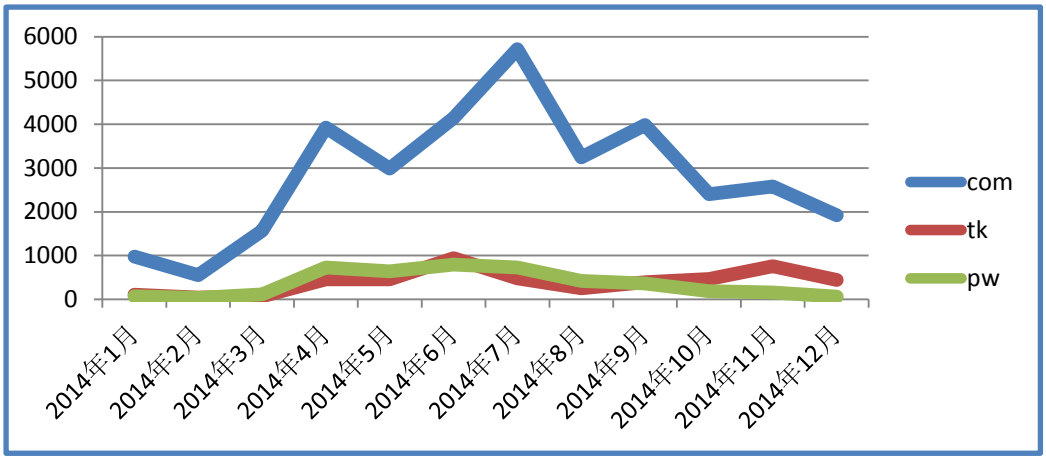

图 5：钓鱼网站使用的主要顶级域按月统计趋势

2. 顶级域中文钓鱼指数[1]

为了更合理的分析各顶级域中钓鱼网站的出现比例与分布情况，我们进一步统计了“顶级域中文钓鱼指数”，以描述某顶级域中文钓鱼网站的集中程度。

$$\text{顶级域中文钓鱼指数}=\frac{\text{某顶级域的中文钓鱼域名数量}}{\text{某顶级域域名注册总量}}*10000,$$

（即每 10000 个域名中出现中文钓鱼域名的数量）

表 1：顶级域中文钓鱼指数 TOP10

排名	TLD	所属地区	钓鱼网站数量	钓鱼域名数量	域名注册量	顶级域中文钓鱼指数
1	.CF	中非共和国	1900	1850	81000	228
2	.PW	帕劳	4293	3901	229639	170
3	.ML	马里	718	684	86000	80
4	.GA	加蓬	497	471	98000	48
5	.EDU	美国	9	8	7590	10.5
6	.SX	圣马丁	5	4	4600	8.7
7	.CC	科科斯岛	445	294	350000	8.4
8	.GD	格林纳达	30	2	2800	7.1
9	.BI	多明尼加共和国	1	1	1400	7.1
10	.TL	法国留尼汪岛	6	1	2200	4.5

从表 1 中可见，中文钓鱼指数较高的顶级域中，.CF 、.ML 以及.GA 等顶级域注册机构

[1] 该指数参照 APWG 报告《Global Fishing Survey: Trends and Domain Name Use in 1H2014》中的指标”Phishing Domains per 10,000”。

提供免费域名注册服务，均由 Freenom 进行管理和运行。可见，宽松的域名注册和审核机制，以及低廉价格甚至免费注册的域名，更容易被钓鱼者注册用于钓鱼。

本报告进一步分析了，在国内应用最为广泛的.COM 和.CN 域名的中文钓鱼指数，其中.COM 的顶级域中文钓鱼指数为 2.56，而.CN 的顶级域中文钓鱼指数为 1.57，可见.CN 注册域名用于中文钓鱼的概率更低。考虑到大多数的.CN 注册域名用于中文网站服务，而境外域名更多用于境外语种网站服务，本报告认为：对国内网民而言，访问.CN 域名的网站风险更低。

3. 钓鱼域名及注册商分布趋势

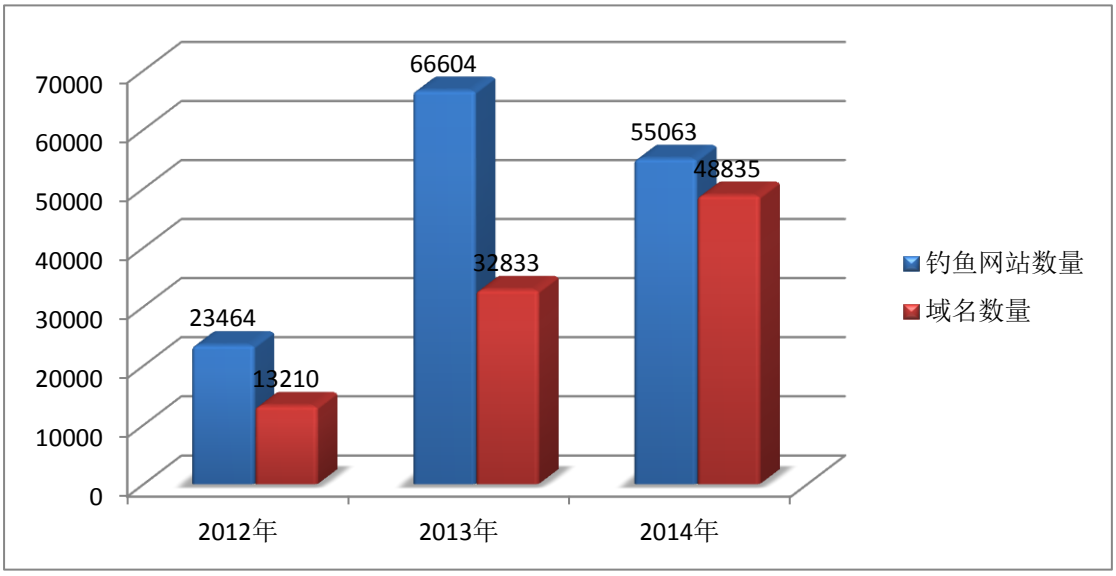

图 6：全球中文钓鱼网站数量及域名数量变化趋势

2014 年，全球中文钓鱼网站数量为 55063 个，其中独立域名数为 48835 个，可见有相当一部分域名被多个钓鱼网站使用。

经分析，重复使用次数最高的前十位域名如图 7 所示。其中，findhere.org 被全部被用于仿冒中国工商银行进行钓鱼攻击；t.cn、tinyurl.com 是有关机构推出的短网址服务，即可以将冗长的 URL 变为缩短的网址。建议相关机构加强对钓鱼 URL 的审查与检测，避免短网

址服务被滥用。

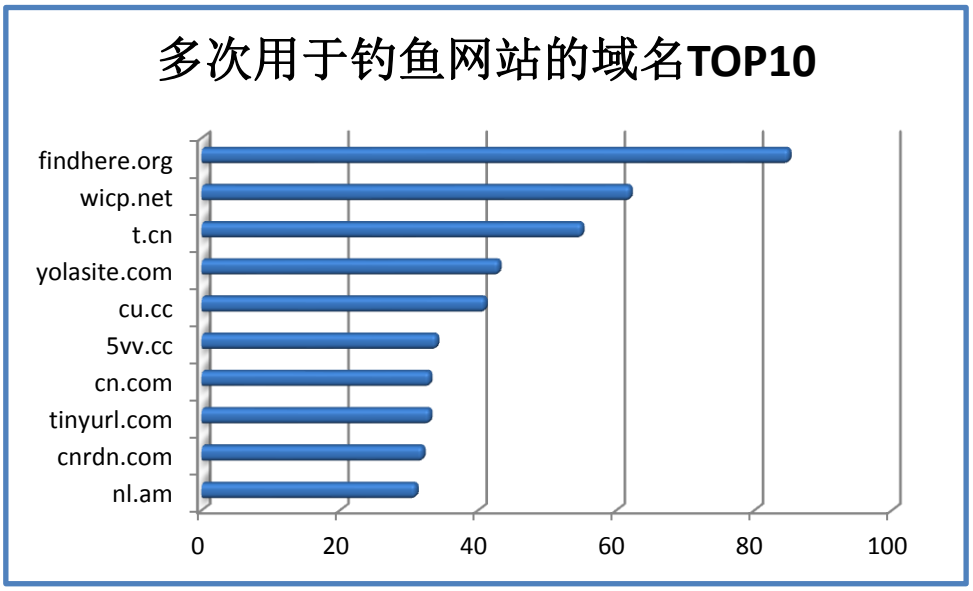

图 7：多次用于钓鱼网站的域名

为进一步了解钓鱼攻击者利用域名的方式和方法，本报告对钓鱼网站的域名进行分类：

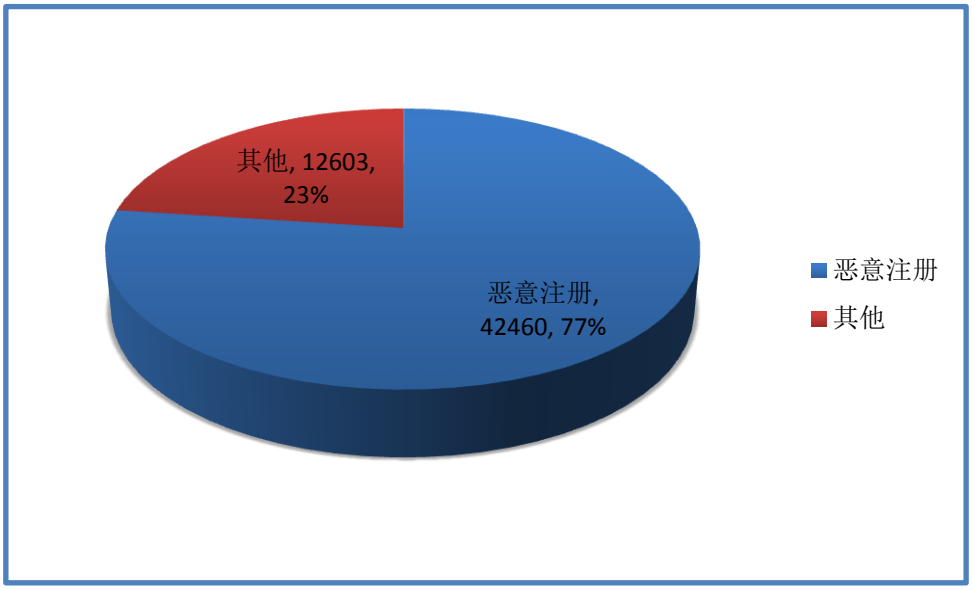

图 8：钓鱼网站分类

在全球发现的 55063 个中文钓鱼网站中，恶意注册类为 42460 个，占全部钓鱼网站总量的 77%，所谓的恶意注册类，指域名符合以下的其中一个或几个条件：1）注册后不久即被用于钓鱼攻击；2）包含品牌名称；3）包含容易误解为某个品牌名称的字符串；4）由同

一注册人批量进行的注册。其他类型主要包括被攻击域名、子域服务、短网址服务等，其中被攻击域名所占比例最高，约为 7.6%。

约 64%的恶意注册域名由图 9 中的注册商提供注册服务。其中，Network Solutions、PDR、Freenom、GoDaddy、Register.com 均为境外注册商，可见很大一部分钓鱼攻击者选择通过境外注册商注册域名，从而逃避监管。

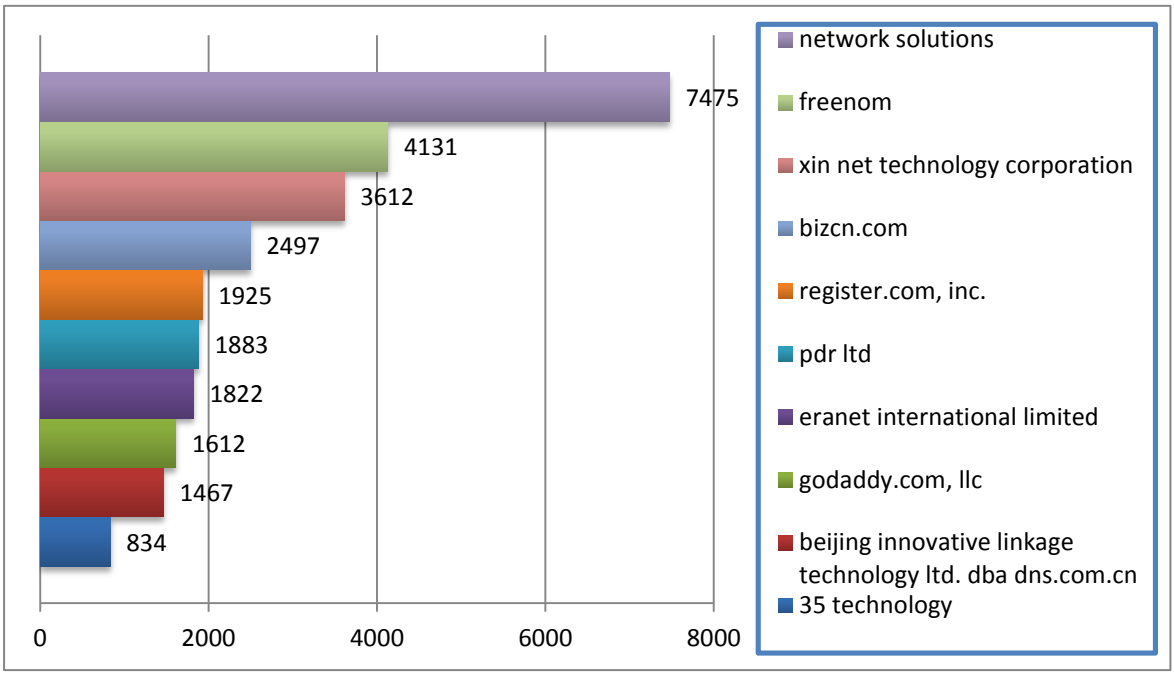

图 9：恶意注册域名注册商分布

四、钓鱼网站在新通用顶级域中的分布情况

2014 年 1 月，第一个新通用顶级域正式入根。截止至 2016 年底，将会有约 1200 个新通用顶级域被陆续推出。那么，新通用顶级域的引入会对钓鱼网站带来怎样的影响？

根据表 2 中统计数据可见，在 2014 年全球中文钓鱼网站中，已经出现利用新通用顶级域名的钓鱼网站，共计涉及的新通用顶级域包括：.XYZ、.WANG、.SEXY、.CLUB。从相关的钓鱼网站数量来看，新通用顶级域的引入暂时并没有给钓鱼网站带来较大的影响。

表 2：新通用顶级域钓鱼网站相关情况

TLD	钓鱼网站数量	钓鱼域名数量	域名注册量	顶级域中文钓鱼指数
.XYZ	308	272	796391	3.4
.WANG	12	10	97591	1.02
.SEXY	1	1	17645	0.57
.CLUB	1	1	160591	0.06

（注：表格中的“顶级域中文钓鱼指数”参考第三章第二节）

由图 10 可见，2014 年上半年，并没有出现新通用顶级域相关的钓鱼网站，而是从下半年开始陆续出现。这是由于上半年为新通用顶级域引入的早期阶段，相较.COM 以及其他顶级域，其注册价格较高。而随着越来越多的新通用顶级域的引入以及注册价格的下调，新通用顶级域名应用更加广泛，随之也带来新通用顶级域名被恶意注册以及用于钓鱼网站的问题。

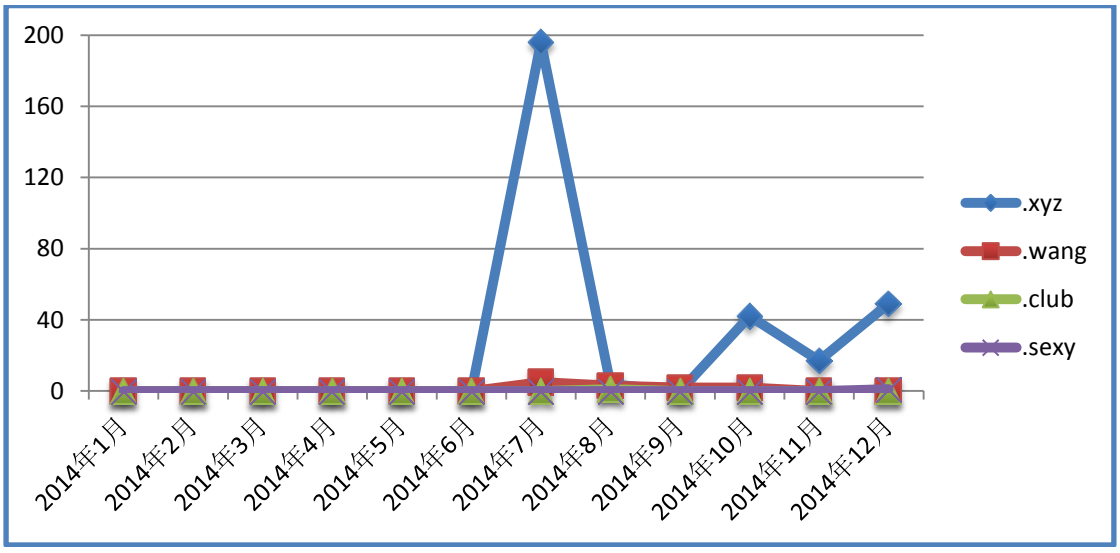

图 10：新通用顶级域钓鱼网站按月统计趋势

五、钓鱼网站攻击品牌分布

2014 年全年钓鱼数据中，仿冒攻击淘宝网[2]的钓鱼网站以 80.7%的举报量位列第一。主要的钓鱼攻击品牌分布如图 11 所示。

[2] 包含淘宝网、阿里巴巴、支付宝

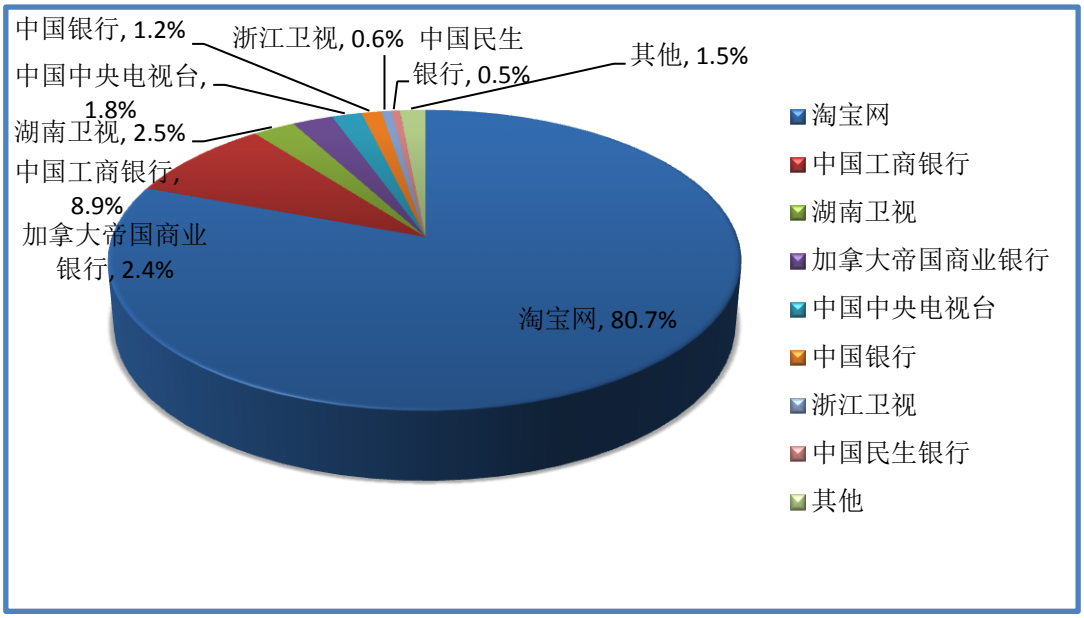

图 11：2014 年钓鱼攻击品牌统计分布

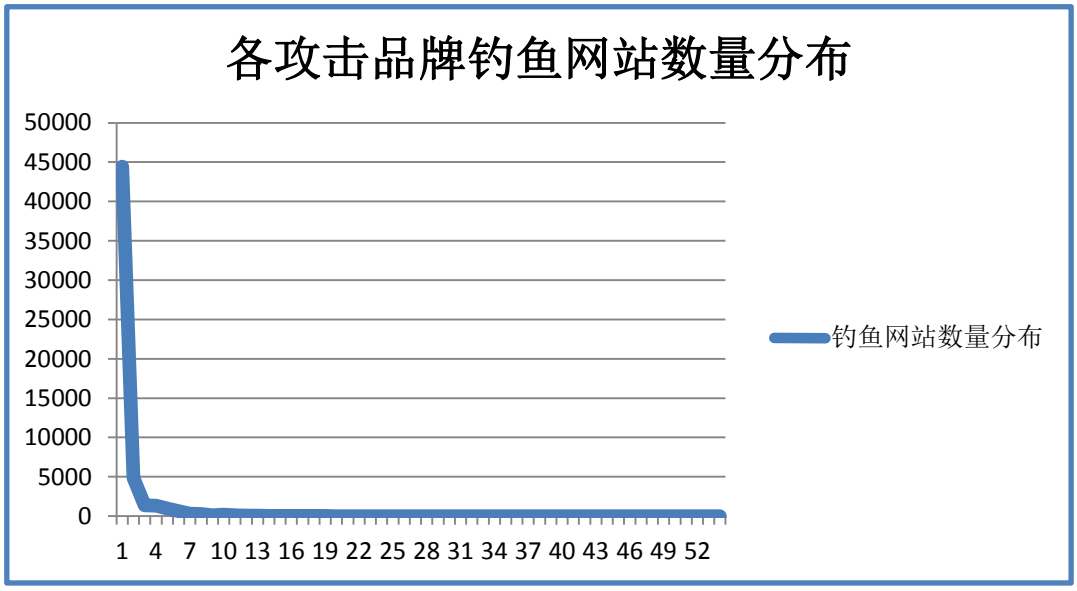

图 12：各攻击品牌钓鱼网站数量分布

图 12 可见，各攻击品牌的钓鱼网站数量符合长尾分布，表明我国的钓鱼网站攻击品牌虽然范围广泛，但是主要攻击品牌非常集中。其中，排名前三的攻击品牌（淘宝网、中国工商银行，湖南卫视）的举报量，占到了总举报量的 92.1%；约三分之一的攻击品牌在 2014 年内只出现过 1 例钓鱼网站。前三位攻击品牌的按月举报量的变化趋势如图 13 所示：

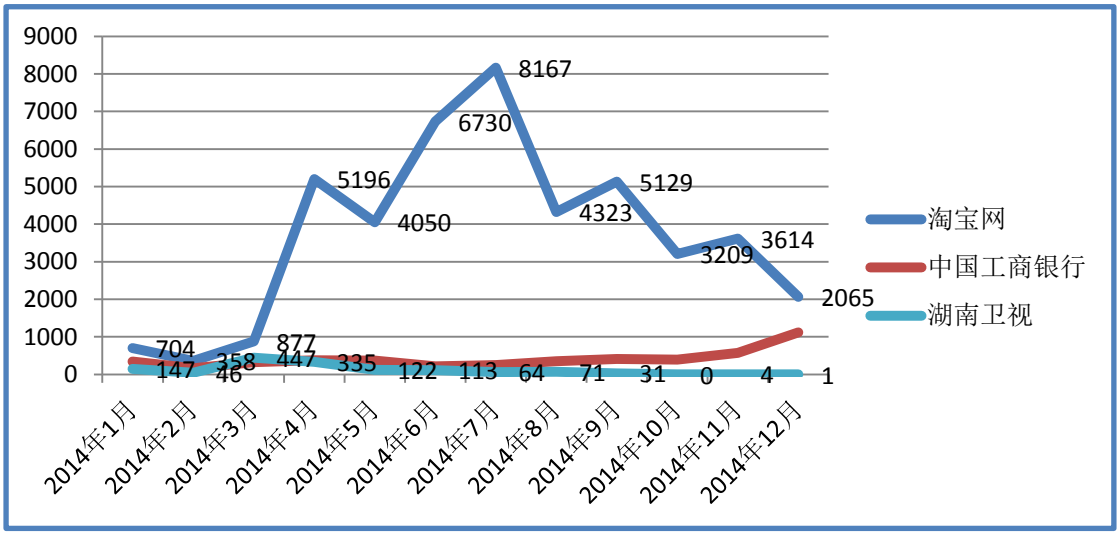

图 13：主要钓鱼目标品牌按月举报量趋势

七、 钓鱼网站活跃时间

钓鱼网站活跃时间是衡量钓鱼网站危害程度的一个重要标志，同时也是衡量钓鱼攻击防御及治理有效性的一个重要指标。由于发动钓鱼攻击的第一天其危害力最大，因此能否快速发现并关闭钓鱼网站尤为重要。

由图 14 可见，2014 年中文钓鱼网站平均活跃时间[3]为 33.1 小时，而全球钓鱼网站平均活跃时间[4]为 31.2 小时。同时结合图 15 中的分析，2014 年上半年，中文钓鱼网站平均活跃时间同比 2013 年大幅增长；2014 年下半年，在 7 月、9 月及 10 月平均活跃时间出现下降之后，于 11 月份达到峰值，活跃时间长达 60 小时。

[3] 本报告对中文钓鱼网站平均活跃时间的统计，基于采样数据（约占总量数据的 20%）。

[4] 参考 APWG 报告《Global Fishing Survey: Trends and Domain Name Use in 1H2014》与《Global Fishing Survey: Trends and Domain Name Use in 2H2014》

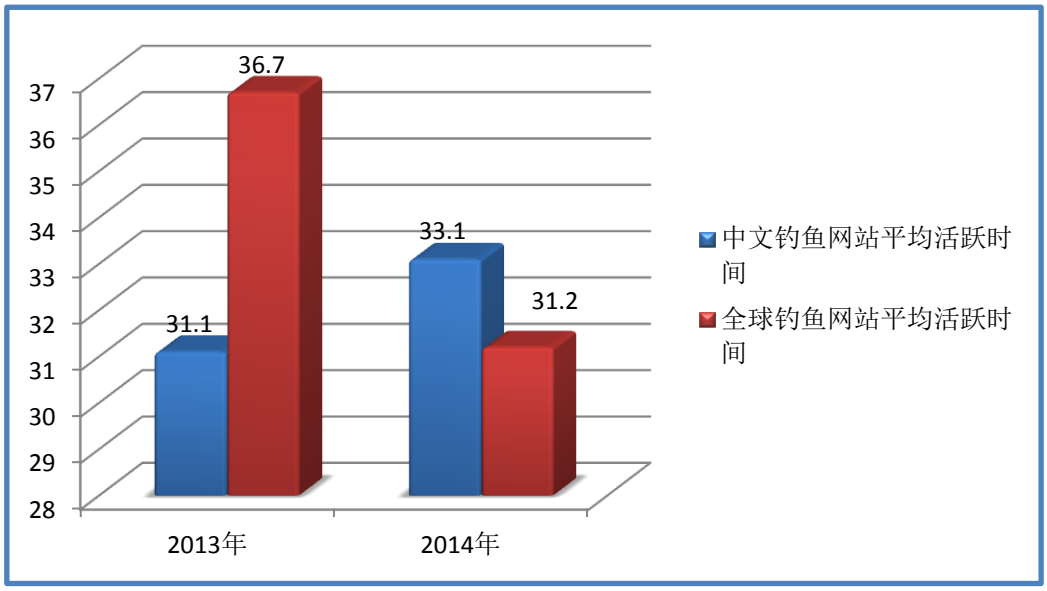

图 14：全球钓鱼网站与中文钓鱼网站平均活跃时间对比（单位：小时）

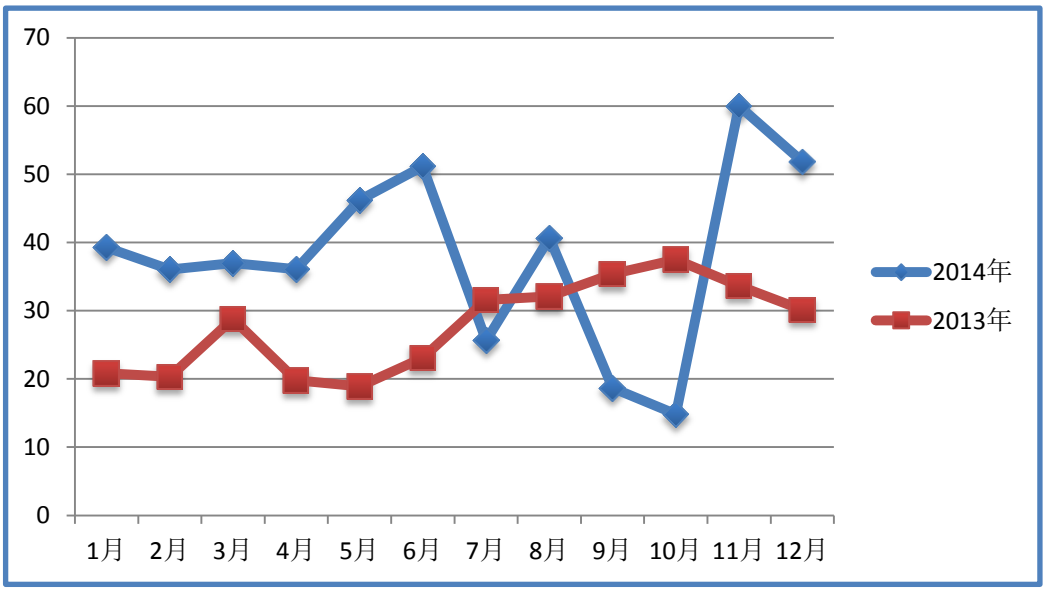

图 15：中文钓鱼网站平均活跃时间按月统计趋势（单位：小时）

致谢

本报告由 CNNIC 基础技术实验室撰稿，由互联网域名管理技术国家工程实验室、中国反钓鱼联盟（APAC）和反钓鱼工作组（APWG）三方联合发布。感谢 APWG 的 Greg Aaron 为本报告所提供的数据支持。感谢广大提供钓鱼举报的 APAC 和 APWG 成员做出的重要贡献。

地　　址：北京中关村南四街四号
邮政地址：北京349信箱6分箱 CNNIC
电　　话：+86-10-58813000
传　　真：+86-10-58812666
网　　址：www.dnscert.cn
邮　　箱：ndsa_public@cnnic.cn