全球中文钓鱼网站现状统计分析报告
（2016 年）

中国互联网络信息中心

互联网域名管理技术国家工程实验室

2017.6

目录

一、2016 年网络钓鱼攻击概况

1.1 关于网络钓鱼攻击

网络钓鱼，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虚假仿冒钓鱼网站，意图引诱用户泄露其敏感信息（如用户名、口令、账号 ID 或信用卡详细信息）的一种网络犯罪行为。这种攻击方式已成为当前互联网最大的安全威胁之一。

需要指出的是，由于互联网特性，钓鱼网站的分布和危害已跨越国界，成为全球性问题。本报告此次的分析对象的是全球中文钓鱼网站，具体来说就是面向中文用户、针对中国品牌的钓鱼网站。

1.2 数据来源说明

本报告数据来源包括：中国反钓鱼网站联盟（Anti-Phishing Alliance of China，以下简称“APAC”）成员单位举报数据、国际反钓鱼工作组（Anti-Phishing Working Group，以下简称“APWG”）共享数据、12321 网络不良与垃圾信息举报受理中心钓鱼举报数据、中国互联网络信息中心（CNNIC）接受的社会公众举报数据、CNNIC 网络钓鱼主动探测系统探测获取的数据等。

本次的分析数据源按照发现方式可以分为两类：各方举报类和主动探测发现类。其中 CNNIC 网络钓鱼主动探测系统（主动发现类）发现的钓鱼网站数量占整体数据集的 26.58%。

1.3 钓鱼网站现状概况

1) 2016 年的钓鱼网站量为 147211 例，较 2015 年增长 150.96%，表明我国网民面临愈发严峻的网络钓鱼攻击威胁。
2) 钓鱼网站的攻击目标品牌多达 113 家，主要集中在淘宝、中国移动、建设银行、工商银行、新浪等。

3) 钓鱼网站所使用的主要顶级域为：.COM、.CC、.PW、.NET。

4) 每 10000 个域名中出现中文钓鱼网站的数量（顶级域中文钓鱼指数）最高的前十个顶级域为：.KH、.CC、.PW、.GQ、.TOP、.CY、.BID、.GA、.CF、.ML。

5) CNNIC 主动探测发现的钓鱼网站的生命周期[1]为 4.684 天，远低于各方举报钓鱼网站的生命周期（18.454 天）。

6) 网络钓鱼从传统互联网向移动互联网转移，针对移动互联网用户的钓鱼网站数量占比超过 52%。

二、2016 年钓鱼网站现状分析

2.1 总体情况

2016 年，各方举报和主动探测发现的钓鱼网站有 147211 例，平均每月 12268 例。图 1[2]为 2012 年至 2016 年的钓鱼网站数量分布情况，可以看出近几年的钓鱼网站数量整体呈现上升趋势。尤其是 2016 年，其钓鱼攻击较 2015 年增长 150.96%，这表明钓鱼攻击越发猖獗，治理形势更加严峻。

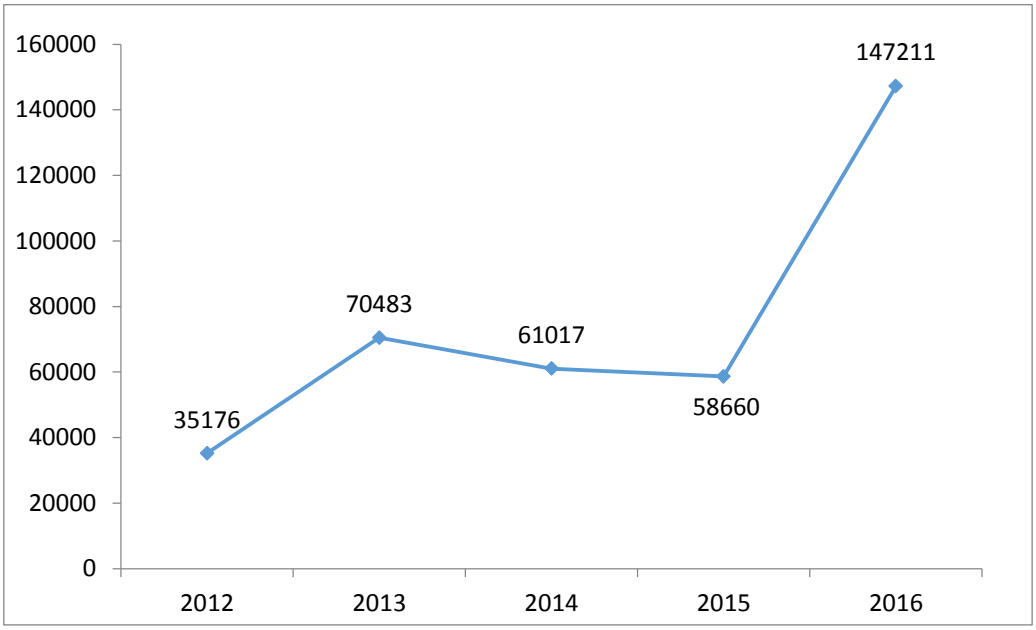

图 1. 2012 年至 2016 年钓鱼网站数量分布

2.2 钓鱼目标分析

[1] 本报告钓鱼生命周期指钓鱼网站所使用的域名从注册到该网站被举报所经历的时长，该时长大于等于钓鱼网站实际存活时间。

[2] 图 1 中 2015 年的数据不包括 APWG 的共享交换数据。

2016 年，钓鱼网站的攻击对象涉及 113 个企业品牌，其分布情况如图 2 所示。可以看出，淘宝的钓鱼网站数量高达全部总量的 40.89%，仍然是网络钓鱼的重灾区。排名前五位的淘宝、中国移动、建设银行、工商银行、新浪钓鱼网站占到总量的 94%以上，可见我国钓鱼网站攻击目标高度集中。

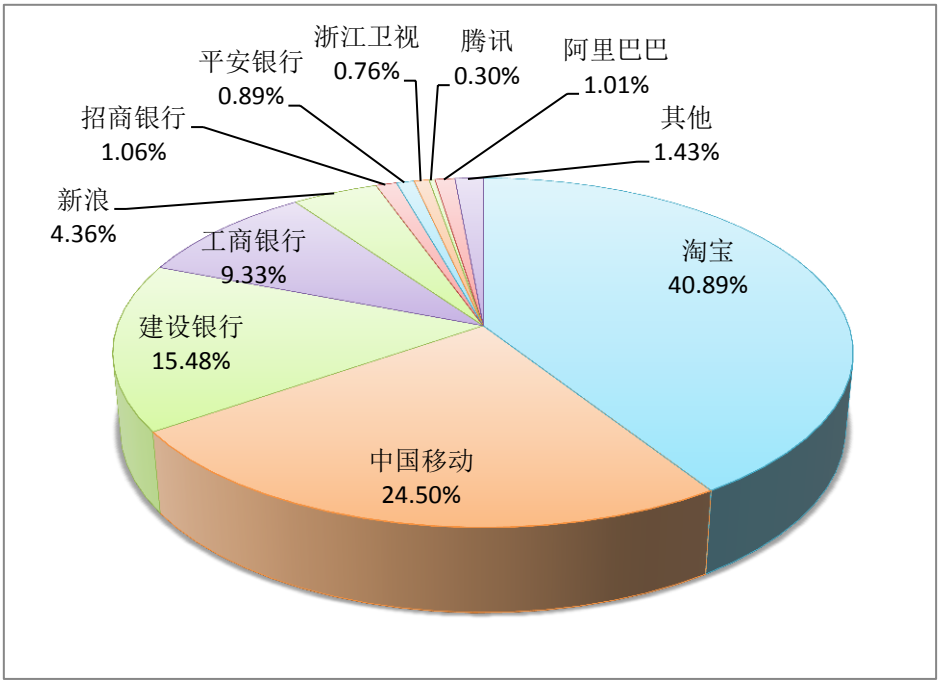

图 2. 钓鱼网站攻击目标分布

2.3 钓鱼行业分析

图 3 是钓鱼网站攻击目标所属行业的分布情况。可以看出钓鱼网站涉及行业的前三位是支付交易类、金融证券类、通讯类，占据了发现总量的 94.01%。其中，支付交易类钓鱼网站数量最多，是钓鱼仿冒的高危行业。其他行业包括媒体传播、电子邮箱、网络游戏等，钓鱼仿冒数量相对较少。

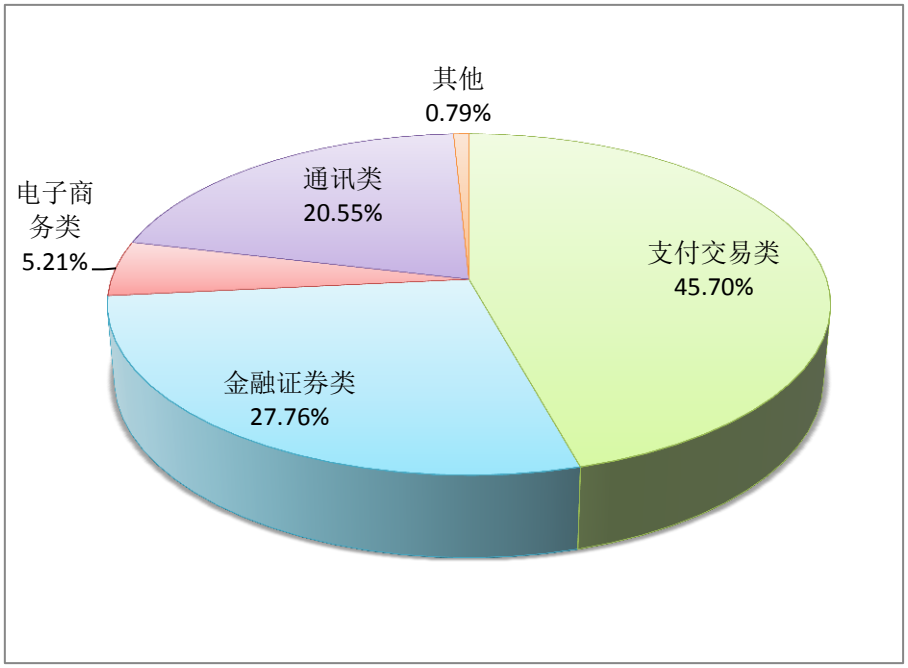

图 3. 钓鱼目标所属行业分布

2.4 钓鱼网站顶级域分析

钓鱼网站的顶级域分布情况及其在各顶级域的注册占比情况如下：

1) 经统计发现，2016 年，从.COM 顶级域发现的钓鱼网站数量超过总量半数，以 64.24%的占比高居首位。钓鱼网站所用顶级域分布详情如图 4 所示。可以看出，除了.COM、.NET 等常见顶级域之外，.CC、.PW、.TK、.AU、.TOP 等顶级域也是钓鱼网站的滋生温床。另外，从图 4 可以看出，与.COM、.NET 等主流顶级域相比，尽管.CN 域名的中文应用网站数量巨大，但.CN 钓鱼网站数量相对较少，只占到所有钓鱼网站的 1.39%。这是由于.CN 域名实名制工作的严格执行和不断完善，使得.CN 域名的钓鱼网站数量一直保持在较低的比例。

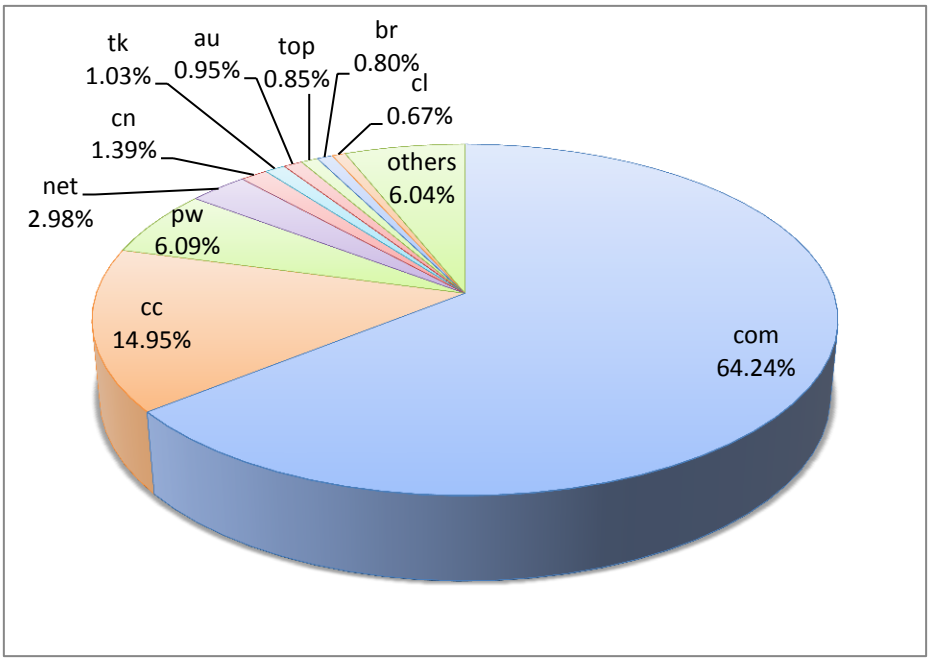

图 4. 钓鱼网站顶级域分布情况

2) 为了分析不同顶级域的钓鱼网站的集中程度，我们采用“顶级域中文钓鱼指数”来进行衡量，即每 10000 个域名中出现中文钓鱼网站的数量。具体计算公式如下：

$$\text{顶级域中文钓鱼指数} = \frac{\text{某顶级域中文钓鱼网站数量}}{\text{某顶级域域名注册数量}} * 10000,$$

通过对本次数据中的所有顶级域进行钓鱼指数分析，可得如表 1 所示 TOP10 结果。可以看出，由于松散的域名注册和验证机制，.KH、.CC、.PW 等顶级域的钓鱼指数很高；.GA、.CF 等提供免费或低价注册的顶级域也是钓鱼网站的滋生温床。

表 1. 顶级域钓鱼指数 TOP10

排名	TLD	顶级域钓鱼指数
1	.KH	834.62
2	.CC	618.23
3	.PW	384.08
4	.GQ	382.75

5	.TOP	329.58
6	.CY	177.70
7	.BID	95.66
8	.GA	77.14
9	.CF	47.04
10	.ML	35.58

2.5 钓鱼网站举报时效性分析

针对 2016 年的 147211 例钓鱼网站，我们抽样统计其发现时间及其域名注册时间间隔的情况，得到如图 5 所示的分布。可以看出，52.88%的钓鱼网站是在其域名注册后 3 天内被发现举报，77.94%在其域名注册后 7 天内被发现举报，平均时长为 13.327 天。

本次报告的分析数据源分别来自各方举报数据和 CNNIC 主动探测数据，我们对比分析这些数据的时效性如下：CNNIC 网络钓鱼主动探测发现的钓鱼网站平均生命周期为 4.684 天，而各方举报数据平均生命周期为 18.454 天。可见通过技术手段主动探测发现钓鱼网站是对其治理的有效途径，不断提升技术能力更快、更有效的打击网络钓鱼是反钓鱼工作下一步的努力方向之一。

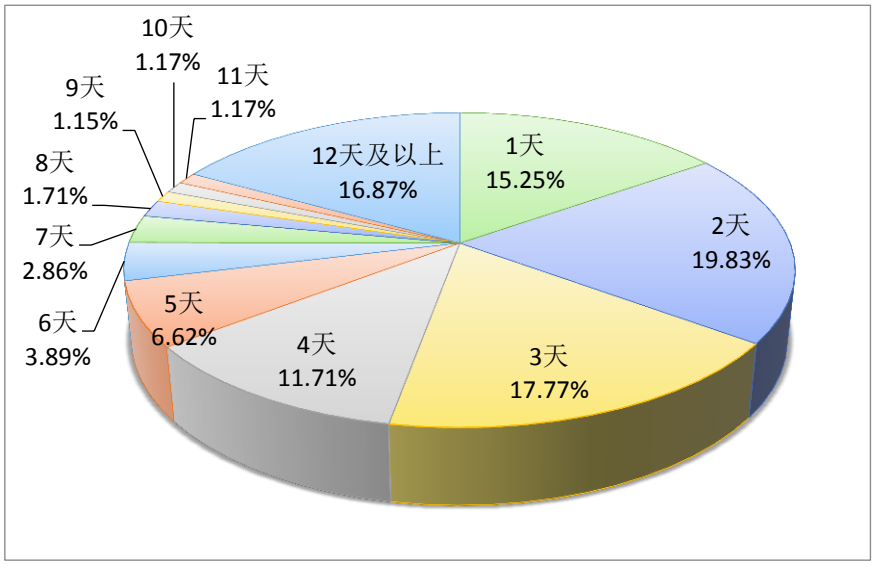

图 5. 钓鱼网站被发现举报时间与其域名注册时间差分布

2.6 钓鱼网站的域名注册者分析

通过对钓鱼网站域名持有人信息进行分析，结果如下：

1) 2016 年 147211 例钓鱼网站，其域名被 8055 位注册者持有，平均每个注册者持有 18 例钓鱼网站。注册者持有钓鱼网站数量的统计分析结果参见图 6，其横坐标表示持有的钓鱼网站数量范围，纵坐标表示该对应范围内的注册者个数。其中有 8.09%的注册者持有的钓鱼网站数量高于平均值，69.22%的注册者持有的钓鱼网站数量在 3 例及以内。

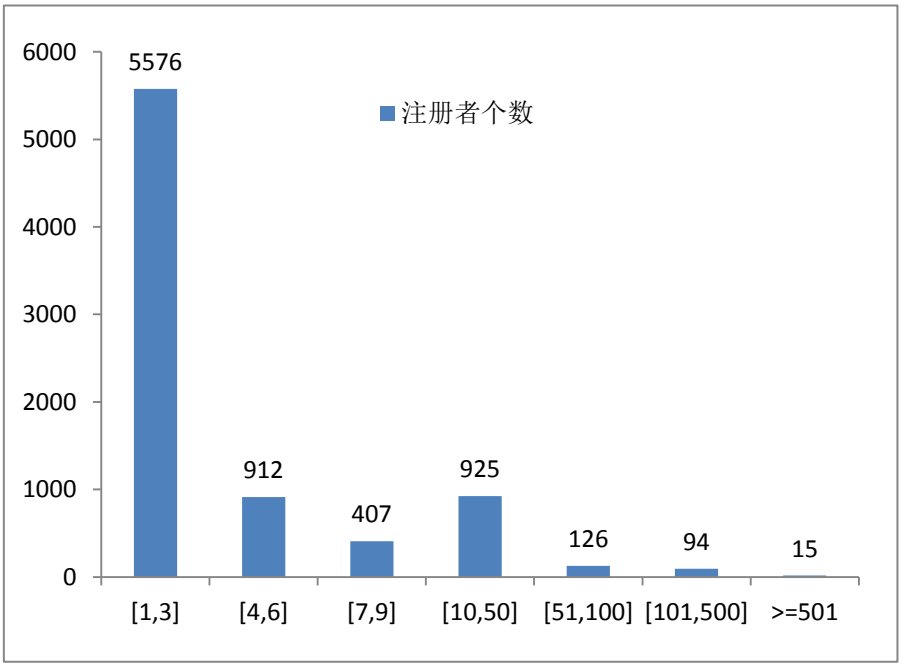

图 6. 钓鱼网站持有者个数分布情况

2) 表 2 是对钓鱼网站持有数排名前五位的注册者情况进行的统计。注册者“huwei”持有的钓鱼网站数量最多，高达 12239 个，其仿冒目标主要为中国移动、淘宝。建议相关域名注册管理机构将这些域名注册者加入黑名单，禁止其进一步注册域名；另外，建议执法部门重点关注并查处黑名单内的注册人。

表 2. 钓鱼网站持有量排名前五位的注册者

排名	注册者	钓鱼目标及占比
1	huwei	中国移动（94.56%）、淘宝（5.20%）、建设银行（0.13%）、工商银行（0.08%）、交通银行（0.02%）
2	michaelwong	淘宝（100%）
3	mahir tarlan	淘宝（100%）
4	liukenian	建设银行（86.57%）、淘宝（13.43%）
5	long cen	中国移动（72.17%）、淘宝（23.12%）、工商银行（4.06%）、建设银行（0.38%）、广发银行（0.12%）、中国银行（0.12%）

3) 表 3 是针对淘宝、中国移动、建设银行、工商银行、新浪这五个主要钓鱼目标的注册者进行统计所得结果。可以看出在这些主要的钓鱼仿冒目标中，很少有重复的注册者，这说明注册者在注册域名时，倾向于批量注册针对某同一品牌的钓鱼域名。

表 3. 主要钓鱼网站注册者前五位

钓鱼目标	注册者前五位				
淘宝	michaelwong	mahirtarlan	konstantinshaposhnikov	pablolopez	huwei
中国移动	huwei	longcen	xidhu	zhengguozhang	jiangzuo
建设银行	liukenian	wanglianjun	lichen	lirongshi	huanyuanlu
工商银行	wangsansi	jialin	wangbawangba	yangli	daifuyang
新浪	yedaofeng	xiaoshenyang	/	/	/

2.7 钓鱼网站涉及注册服务机构分析

通过对钓鱼网站域名所属的注册服务机构信息进行分析，结果如下：

1) 钓鱼网站域名所属国内外注册服务机构的分布情况如图 7 所示。可以看出，注册量较多的新网数码、上海美橙、阿里云，它们都是国内的注册服务机构，据统计 64.94%的钓鱼网站是通过国内注册服务机构注册的域名。

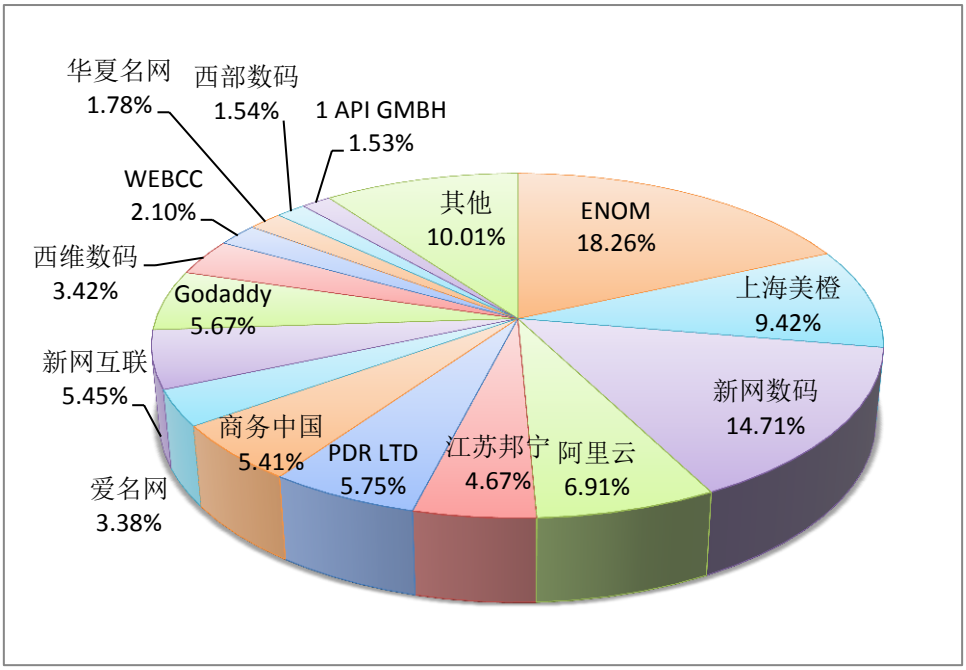

图 7. 国内外域名注册服务机构整体分布

2) 表 4 是针对淘宝、中国移动、建设银行、工商银行、新浪这五个主要钓鱼目标的注册服务机构进行统计后所得的结果。

表 4. 主要钓鱼目标注册服务机构前五位

钓鱼目标	**注册服务机构前五位**				
淘宝	新网数码	阿里云	上海美橙	GODADDY	PDR LTD
中国移动	ENOM	上海美橙	新网数码	华夏名网	PDR LTD
建设银行	新网数码	阿里云	22net	商务中国	江苏邦宁
工商银行	新网数码	江苏邦宁	上海美橙	新网互联	GODADDY
新浪	上海美橙	GODADDY	阿里云	西部数码	/

2.8 移动互联网与传统互联网钓鱼网站对比

通过分析得到如图 8 所示的钓鱼网站在传统互联网环境和移动互联网环境下的分布情况，可以看出针对移动互联网用户的钓鱼已超过传统互联网，占据全部数量的 51.95%，成为钓鱼攻击新趋势。

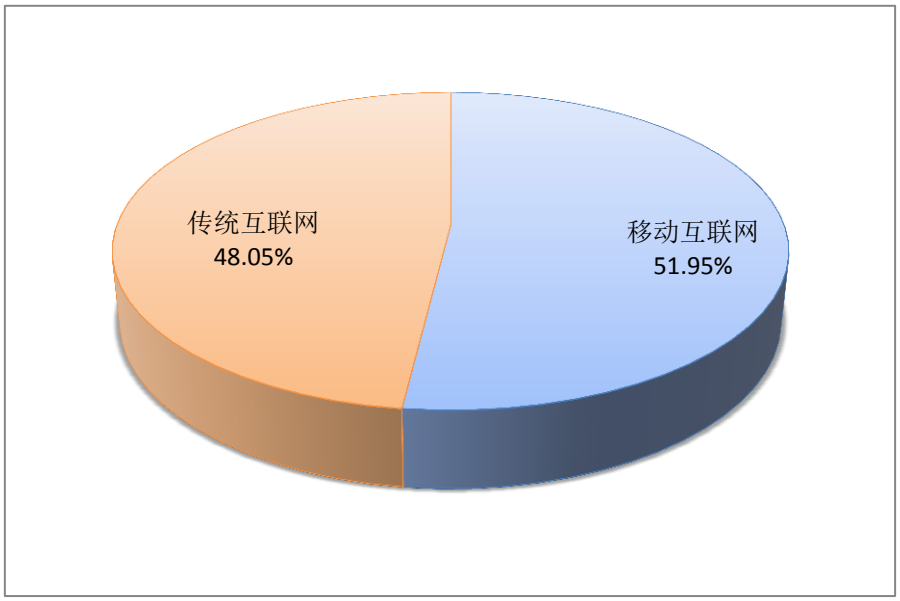

图 8. 钓鱼网站在传统和移动互联网的分布情况

三、附录

3.1 中国反钓鱼网站联盟简介

中国反钓鱼网站联盟（Anti-Phishing Alliance of China，简称“APAC”），成立于 2008 年 7 月 18 日。由国内银行证券机构、电子商务网站、域名注册管理机构、域名注册服务机构、专家学者共同组成，是国内唯一为解决钓鱼网站问题而成立的协调组织，目前拥有会员单位 500 多家。联盟已建立快速解决机制，借助停止 CN 域名或非 CN 域名钓鱼网站解析或警示等手段，及时终止其危害，构建可信网络。中国互联网络信息中心（CNNIC）承担联盟秘书处的职责。

3.2 国际反钓鱼工作组简介

国际反钓鱼工作组（Anti-Phishing Working Group，简称“APWG”）成立于 2003 年，是一个专注于消除日益严重的网络钓鱼、犯罪软件和电子邮件诈骗所带来的身份盗窃和欺诈问题的非营利行业协会。目前在全球拥有超过 2000 家的企业会员，包括合格的金融机构、零售商、ISP、解决方案提供商、执法部门、政府机构、多边条约组织、非政府组织。

3.3 CNNIC 网络钓鱼主动探测简介

CNNIC 自 2009 年开始长期专注于反钓鱼技术研究，形成了具有自主知识产权的网络钓鱼主动探测技术体系。探测技术的核心是基于机器学习的域名应用大数据分析，以主流通用顶级域的网站数据、网站解析数据等大规模数据为来源，学习出高准确率的分类模型进行网络钓鱼的判定工作。CNNIC 网络钓鱼主动探测发现的钓鱼网站，均在第一时间提交给中国反钓鱼网站联盟进行认定和处置。

近年来，该系统已累计发现并举报的钓鱼网站超过 50000 个，涉及近百个顶级域。这些钓鱼网站的快速发现与处置，让广大网民避免了不可估量的经济损失，为维护我国良好的互联网环境贡献力量。