全球中文钓鱼网站现状统计报告

2012年上半年

全球中文钓鱼网站现状统计报告

（2012 年上半年）

CNNIC 国家域名安全中心

中国反钓鱼联盟（APAC）

反钓鱼工作组（APWG）

2012 年 11 月

总体情况

1. 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、帐号、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。

2. 本报告的统计范围和统计方法

《全球中文钓鱼网站现状统计报告》汇总并统计了全球范围内，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，**国家域名安全中心**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 49%。

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公司的钓鱼网页的情况；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. 重要数据摘要

- 2012 年上半年，针对中国网民的钓鱼网站数量为 15618 个。

- 钓鱼攻击的目标公司统计前五位分别为：淘宝，阿里巴巴，中国工商银行，加拿大帝国商业银行（中国区业务），中央电视台。

- 钓鱼网站采用的顶级域名分布前五位为：.COM、.TK、.PL、.CC、.NET。

- 重要指标的按月变化趋势，如下表所示：

	1月	2月	3月	4月	5月	6月
钓鱼网站数量	1701	2651	2856	2751	3325	2334
独立域名数量	1607	2524	2717	2638	3141	2240
钓鱼目标数量	23	28	29	28	38	31

钓鱼网站按月统计趋势

2012 年上半年，全球共发现中文钓鱼网站 15618 个。在第一季度内，钓鱼网站数量呈现逐月上升的趋势。2012 年 5 月份，钓鱼网站数量达到上半年的最大值，然后于 2012 年 6 月份大幅回落。

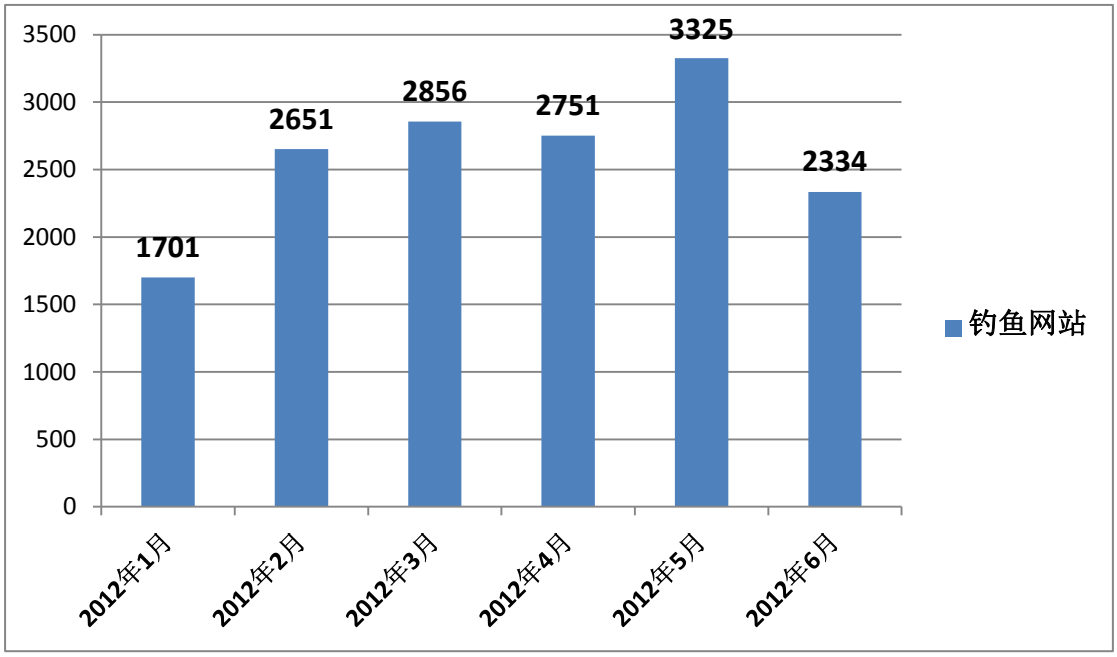

图 1：钓鱼网站数量按月统计趋势

钓鱼攻击目标单位的统计分布

网络钓鱼由于其本质上采用的是社会工程学手段，利用的是网民对于网页视觉效果和内容信息的信任感，因此其攻击的目标单位，即伪装仿冒的对象，呈现出涉及范围广，分布较集中的特点。2012 年上半年，共有 59 个单位被当做过钓鱼攻击的目标，其中，仿冒攻击淘宝网的钓鱼网站以超过总量 50%的举报量位列第一。钓鱼攻击目标单位具体分布如图 2 所示。

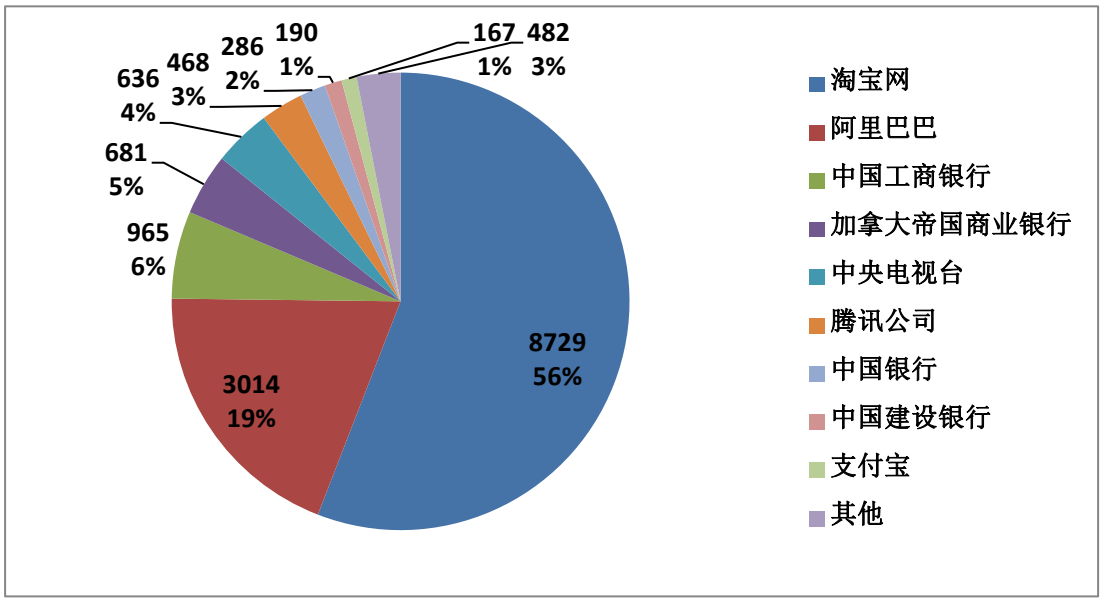

图 2：2012 年上半年钓鱼攻击目标统计分布

从分布可以看出，排名前五的攻击目标的举报量，占到了总举报量的 90%，表明了钓鱼攻击目标范围广，分布集中的特点。主要攻击目标的按月举报量的趋势如图 3 所示：

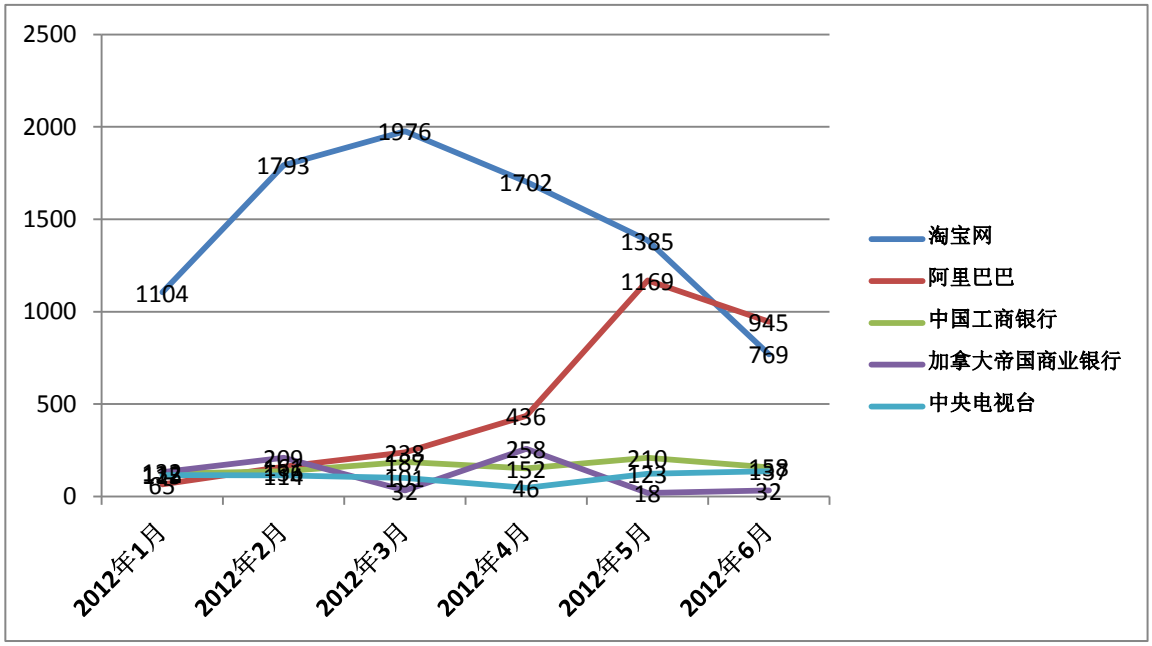

图 3：主要钓鱼目标公司按月举报量趋势

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，因此，大量的顶级域名都被钓鱼网站使用过。其中，COM 域名是被使用最多的顶级域。具体分布和按月趋势如下所示：

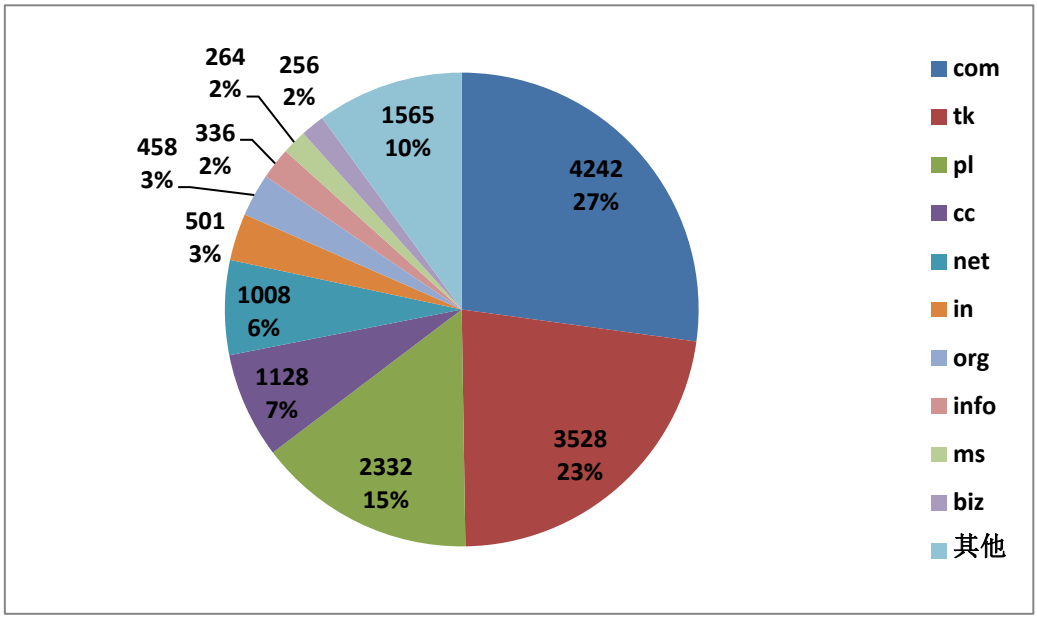

图 4：钓鱼网站顶级域名分布

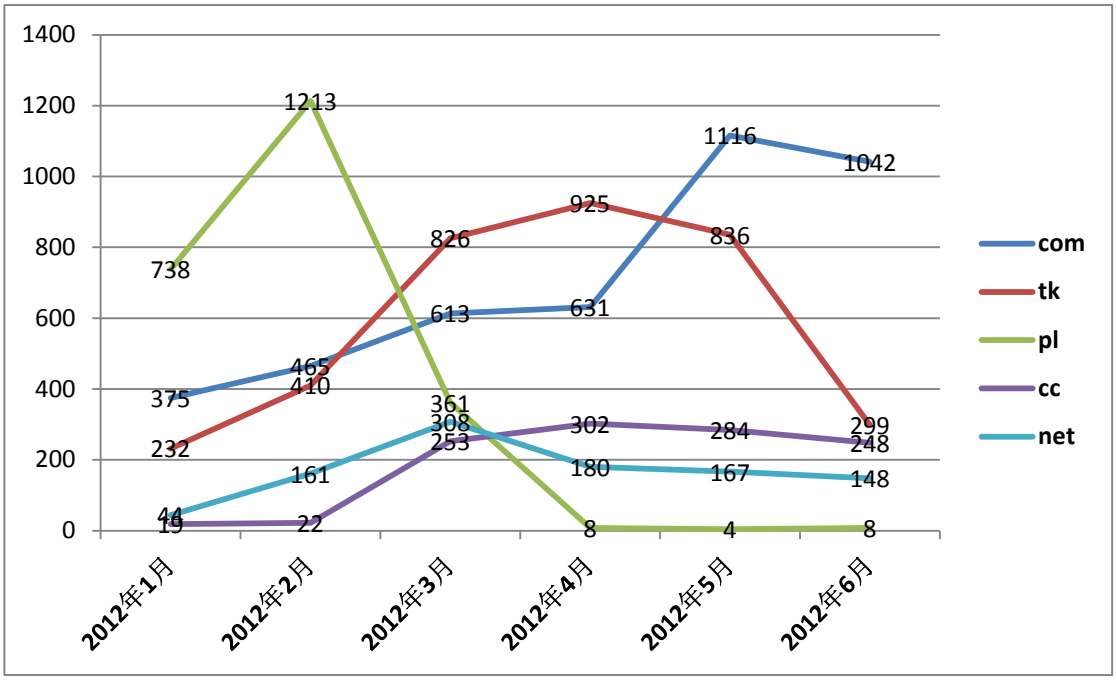

图 5：主要钓鱼网站顶级域按月统计趋势

值得注意的是，宽松的域名注册和审核机制，过于低廉甚至免费的域名注册，更容易被钓鱼者利用来注册钓鱼域名，比如.PL 排名靠前，就是因为 OSA.PL 和 BEE.PL 等免费注册的二级域名造成的。相对的，由于 CN 域名的实名审核机制，针对中国网民的钓鱼网站反而极少使用 CN 域名。这从侧面也反映出，良好的域名注册管理机制有利于提高互联网的可信度。

URL-域名-钓鱼目标的比较和分布

本节旨在比较钓鱼 URL、钓鱼目标和钓鱼攻击所使用的独立域名三者之间的相互关系。

独立域名，指钓鱼攻击者拥有的可由其直接设置解析的域名，包括但不只有一级域名（如 example.com）。比如某些提供免费二级域使用的一级域名常常会被攻击者申请用做钓鱼，那么此处攻击者实际控制的独立域名就是二级域名（如 free.example.com）。

独立域名-钓鱼目标，是指独立域名和钓鱼目标的配对组合。多个 URL，如果采用同样

的独立域名，面对同样的钓鱼目标，那么会被认为是一个独立域名-钓鱼目标对。

上述两个指标的按月分布如图 6 所示：

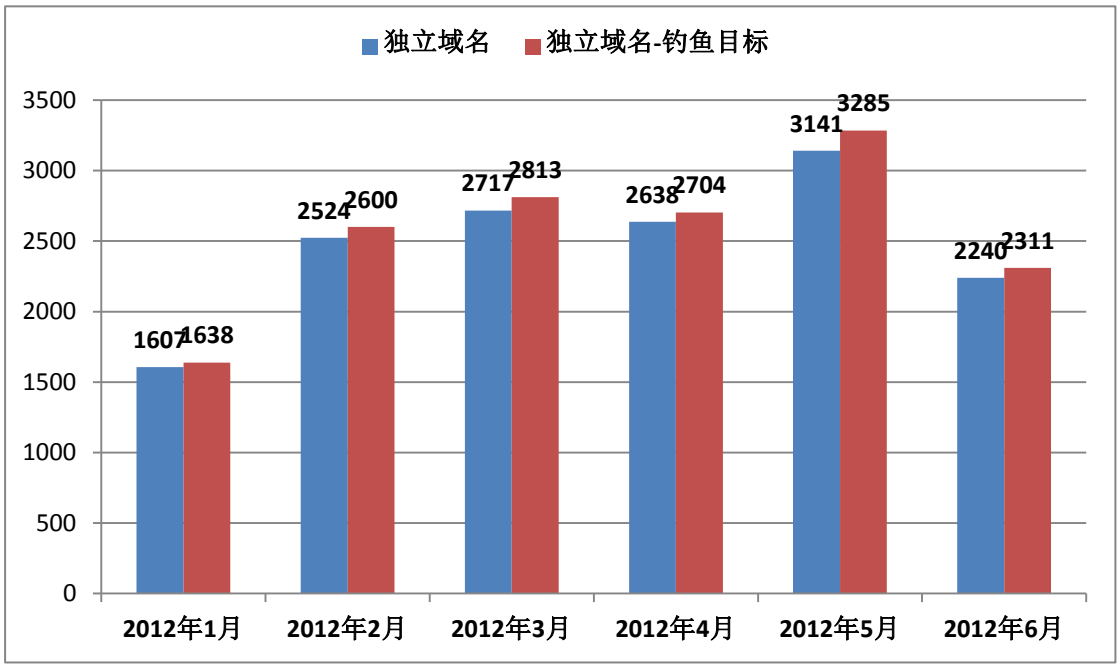

图 6：独立域名和（独立域名-钓鱼目标）按月统计趋势

从图 6 可以看出，独立域名-钓鱼目标大于独立域名的数量，说明钓鱼攻击者在使用域名时，会采取在同一个独立域名下，提供多个针对不同目标的钓鱼网站的策略，以提高独立域名的使用率。钓鱼举报数据的案例分析也验证了统计结果。

钓鱼目标和平均每个钓鱼目标对应钓鱼 URL 数量的统计趋势如图 7 所示：

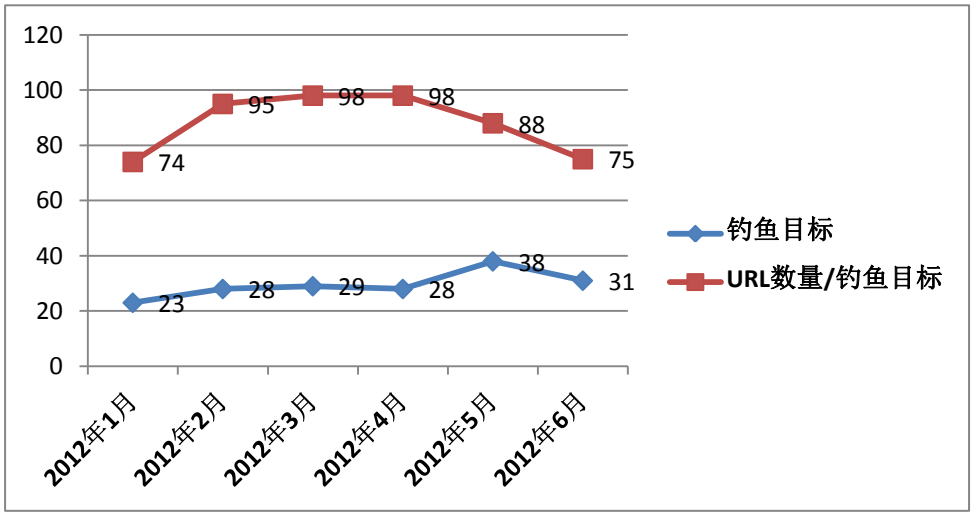

图 7：钓鱼目标及平均对应的 URL 数量按月统计趋势

从图 7 可以看出，在 2012 年上半年，每月的钓鱼目标，以及每个钓鱼目标平均对应的 URL 数量都基本趋于稳定。

致谢

感谢 APWG 的 Greg Aaron 为本报告的撰写所提供的数据支持和帮助。感谢国家域名安全中心的王利明、洪博、耿光刚等工作人员为本报告的撰写所做的工作。同时，更感谢广大 APAC 和 APWG 成员提供的钓鱼举报，为推动反钓鱼事业做出的重要贡献。

地　　址：北京中关村南四街四号
邮政地址：北京349信箱6分箱(100190)
电　　话：(010)58813000
传　　真：(010)58812666
网　　址：www.dnscert.cn
邮　　件：ntsa_public@cnnic.cn