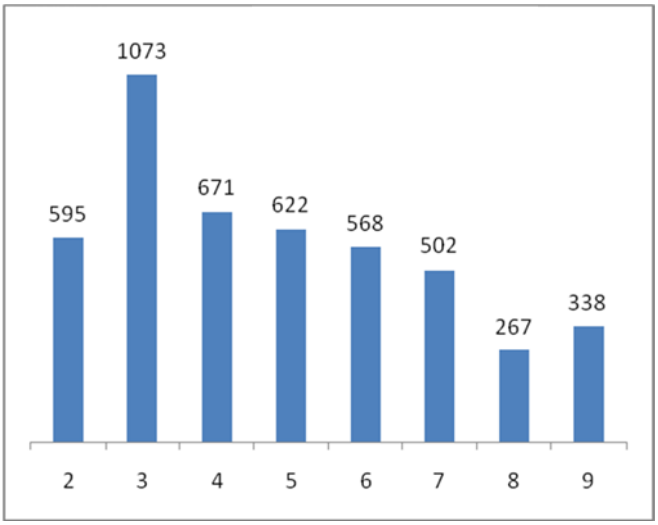
[趋势科技新闻稿]

趋势科技发布《2012 年中国金融行业网络威胁报告》

金融行业钓鱼网站半年即达 4639 个 约 99%攻击由海外发起

[趋势科技中国]– [2013 年 1 月 7 日] 近日，全球服务器安全、虚拟化及云计算安全领导厂商趋势科技与中国反钓鱼网站联盟共同发布了《2012 年中国金融行业网络威胁报告》。报告显示: 在 2012 年 2 月至 9 月期间 趋势科技钓鱼网站侦测系统——MUYU 共发现了 4636 个针对金融行业的钓鱼网站，在个别月份，钓鱼网站的数量增幅甚至达到了 80%。在这些攻击中，98.72%由海外发起，大大增加了安全监管的难度。此外，针对金融行业的移动安全威胁、高级持续性威胁也出现了迅速的增长。

趋势科技全球研发长暨中国区执行副总裁张伟钦表示：“金融行业关系到国计民生并直接关联着用户的财产安全，因此金融网络安全威胁的变动情况值得社会充分关注。作为网络安全的领导厂商，趋势科技服务中国金融行业已经拥有十余年的经验，不仅致力于提供全面的产品及解决方案，同时还密切追踪并分析各种网络威胁，及时提供准确的网络威胁信息及发展趋势。”



【2012 年 2~9 月钓鱼网站每月数量统计】

趋势科技发现，针对金融行业的钓鱼网站呈现出两大趋势变化：

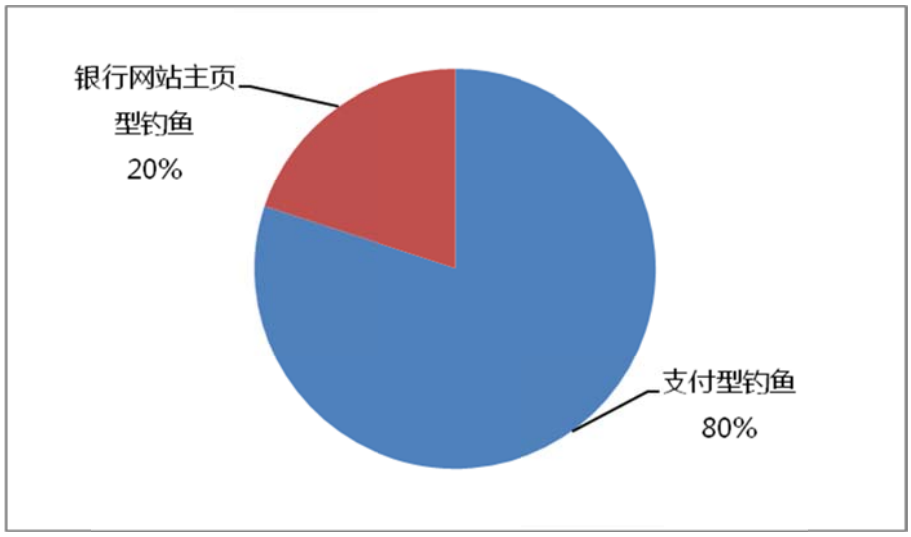
趋势一：钓鱼网站的威胁虽有所减弱，但特殊情况可能迅速反弹

报告中显示：金融钓鱼网站数量在 2012 年 3 月的月度增幅高达 80%，并达到监测时间段的峰值，此后，钓鱼网站的总体数量呈现逐月下降的趋势。但是，从 8 月份开始，钓鱼网站的数量又开始抬头，增幅接近 30%。这说明，钓鱼网站对金融行业的威胁虽有所减弱，但现状依然不容乐观，在特殊情况下完全有可能出现爆发式增长。

趋势二：钓鱼网站的攻击日益隐蔽、狡猾

在对数据的分析中，趋势科技发现，近期的金融钓鱼网站与过去有着显著的差异：从 IP 地址来源看，绝大部分的钓鱼网站不再以内地作为据点，而是将 IP 地址搬移到美国和中国香港，以逃避日益严厉的法律监管；从内容来看，将近三分之二的钓鱼网站将攻击目标对准了银行，并将获取网民的网银账户信息作为主要目的。

除了搬移 IP 地址，不法分子还改进了攻击方式，使其更加难以防范。根据趋势科技对某银行网银的钓鱼网站单独分析的结果：80%网银钓鱼页面是支付型钓鱼页面，也就是说网络犯罪分子先建立一个虚假的网购页面，诱使用户购买，最后将用户引导至虚假的网银支付页面套取网民的网银账户信息。这说明以网购的名义来骗取网民的网银账户信息是网络犯罪分



子最常用的伎俩。

【针对银行的钓鱼网站类型】

据趋势科技（中国区）资深安全研究员谷亮进一步介绍：“从这些攻击的特征来看，犯罪分子越来越狡猾，使用的手段也越来越复杂。这也警示我们，网络防护与网络攻击之间的博弈仍然没有到达终点，在我们的防护方式发展的同时，不法分子的攻击手段也随之发生着进化，并随时准备利用一切可以利用的漏洞进行攻击，获取非法利益。”

除了钓鱼网站，趋势科技建议企业需要关注的金融网络安全威胁还有以下两点：

一、移动威胁日益增长

进入 2012 年，Android 恶意应用程序出现了爆发式增长。趋势科技预估，到 2012 年 12 月，Android 恶意应用程序总数将突破 129,000 个。在这些恶意程序中，有相当多的一部分以窃取个人用户的金融资产信息为目的，对用户的金融安全构成严重威胁。趋势科技预计，移动威胁在之后几年会继续增长，而且会更多的利用 NFC（近场通信）等新功能进行攻击。

二、高级持续性威胁进入高发期

从 2012 年 1 月开始，高级持续性威胁进入了高发期，金融行业不断出现高级持续性威胁的攻击事件。高级持续性威胁不但在攻击频率上越加频繁，而且在攻击方式上日趋多样化。攻击者往往会持续不断地渗透并窃取金融企业的敏感数据，部分恶意程序潜伏周期甚至长达数年，这种威胁使企业面临极大的内部敏感数据外泄的风险。