

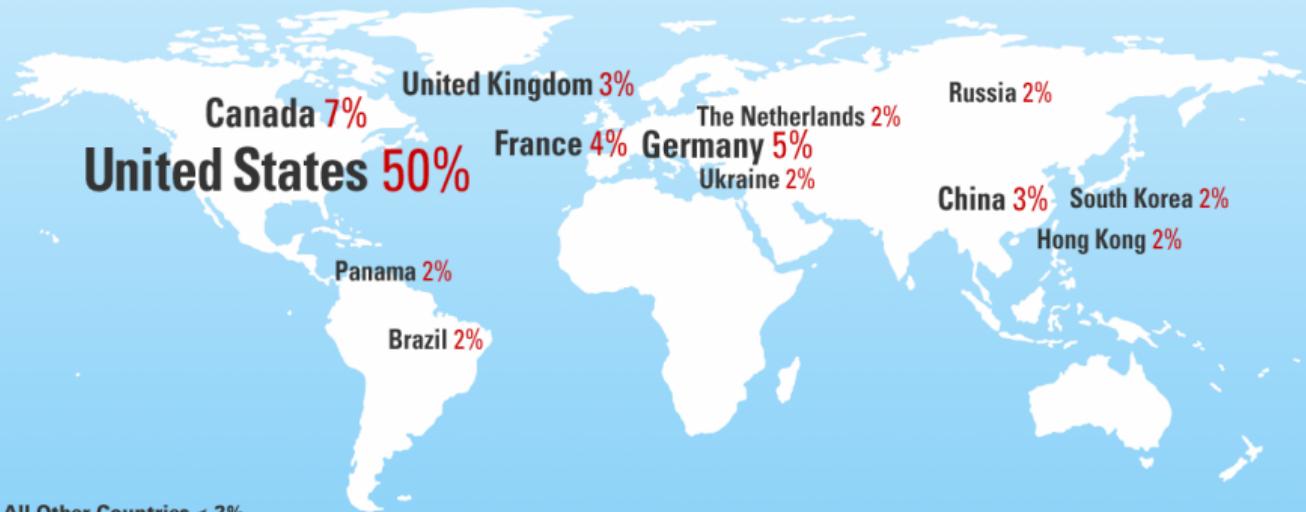
Phishing and Online Scams in China

Joey Zhu
Trend Micro Inc.

Who I am:

- Worked for Trend Micro Inc. *(2005 – Present)*
- Rich experience with virus sandbox *(2005 – 2008)*
- Rich experience as a JavaScript analyzer
(2008 – Present)
- Web threat expert, focusing on HTML/Javascript exploits
- Now interested in phishing in China

Only 3% of phishing occurs in China



Do you believe this number?

All vendors
don't focus on **China**



100+ phishing QQ sites found among 4M traffic
(reported by Trend Micro)



Phisher's bonus:
Large population

QQ.com: 640 Million

Taobao.com: 300 Million

Passengers at Spring Festival: 280 Million

Global WoW: 10 Million

Hot Phishing Event

target www.boc.com

- Over 500 phishing site in Feb
- Spread via SMS message
- Also includes other banks
 - CEB/SDB



Vulnerable Validation Procedures

E-Token from www.boc.com

- Password invalid after 60 seconds
- www.bocxx.com



Phishing in China

- More **prevalent** than drive-by websites
- **Three** categories:
 - lottery scams (**most common**), fake websites, fraudulent websites

fake websites/仿冒著名网站



fraudulent websites / 欺诈网站



lottery scam/中奖骗局



Lottery Scam

beyond traditional private information leakage

- Over 70% of scams, making it the **No. 1** category
- Fake webpages such as **QQ, games & CCTV**



A typical lottery scam

- Step 1. IM/Email message: "*Lucky you, go won a prize...*"
- Step 2. A phishing webpage pretends to be the official site like ***QQ.com*** or ***CCTV.com***, ...
- Step 3. After clicking, the phishing site will ask users to pay income tax or notary fees first.

Where does the Phishing URL come from? Chinese Instant Messenger

- A **special phenomenon** in China
- Notably from **QQ & Aliwangwang/阿里旺旺**



Where does the Phishing URL come from?
Comprised of a website & injected with Iframe
in order to deliver phishing message

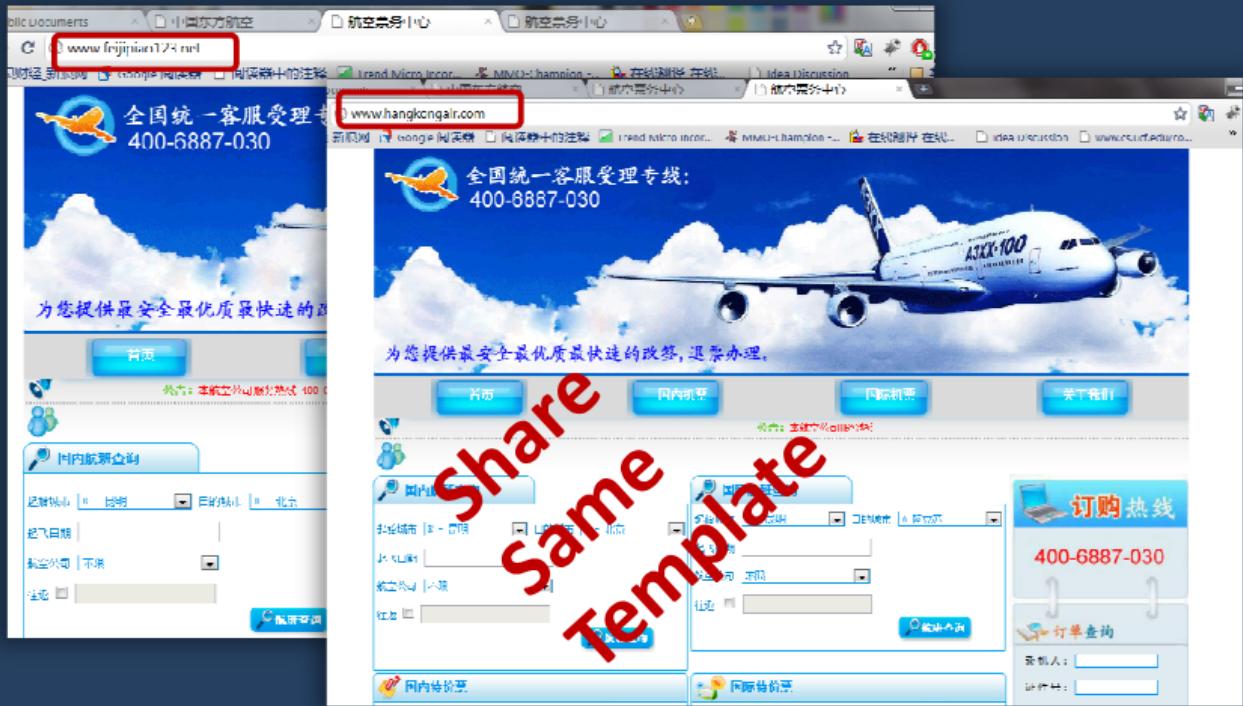
Money Driven



Fraudulent Websites

New Phishing without Target Brand

Delivered by AdWords



Scams with Stocks & Securities for membership fees

Screenshot of a search results page from Baidu (百度) showing various scam websites related to stocks and securities.

The main search result is for "长江证券 推荐 黑马统一服务电话" (Changjiang Securities Recommended Black Horse Unified Service Telephone).

Left side of the screenshot:

- mvaq.cn**: 网站价值 ¥145, 上海长江证券有限公司股票...
上海长江证券投资有限公司 中国股票
客服电话: 400-6949-918 值班手机: 全国统
12月11日主力净流入龙旗股份... 版权所有: 上海
www.myip.cn/mvaq.cn 2010-12-4 - 百度快照
- 上海长江证券投资有限公司**: 中国股票
客服电话: 400-6949-918 值班手机: 全国统
12月11日主力净流入龙旗股份... 版权所有: 上海
www.myweb.cn.yahoo.com/snapshot/f475a2bf5e3c
- 长江证券咨询电话/常用的证券分析软件**:
服务行稿 服务黑马 <http://qcjh110.co.boker.net/> 电话: 常用的证券分析软件字体大小: 大 中 小
www.boker.net/company/note_vivere.html?5189
- 证券股票版版1.1版 (及营业部地址)**:
16章 同页 - 发帖时间: 2010年6月23日
b. 不得在证券股票版以“黑马推荐”等方式明示或
南宁的证券公司... 咨询服务电话: 0771-553881
bbs.gxsky.com/thread-7840603-1-1.html 2010-
- 欢迎光临本公司网站!**:
服务热线 服务时间: 8:45-22:30 全国统一服务
2007年6月26日公开验证的...
www.cjzqgzw.com/ 2010-8-29 - 百度快照

Right side of the screenshot (Google Reader interface):

- 上海森洋投资咨询有限公司**: 合理规避风险 稳健创造财富
合理规避风险 稳健创造财富
- 会员登录**:
用户名:
密码:
验证码: 验证码校验
- 推荐热帖**:
发帖时间: 2010-04-18 14:30 | 15:30 公开第二大股东公开持股量
请点击查看 04月18日一只必涨股票已公开请验证!
发帖时间: 2010-04-18 14:30 | 15:30 公开第二大股东公开持股量
请点击查看 04月18日一只必涨股票已公开请验证!
- 股票新闻**:
股票名称: 股票代码: 股票简称: 股票类型: 股票状态: 股票评级:
股票代码: 000708 | 000708 | 000708 | 000708 | 000708 | 000708
股票名称: 金牛能源 | 金牛能源 | 金牛能源 | 金牛能源 | 金牛能源 | 金牛能源
股票简称: 金牛能源 | 金牛能源 | 金牛能源 | 金牛能源 | 金牛能源 | 金牛能源
股票类型: 股票 | 股票 | 股票 | 股票 | 股票 | 股票
股票状态: 上市 | 上市 | 上市 | 上市 | 上市 | 上市
股票评级: 持有 | 持有 | 持有 | 持有 | 持有 | 持有
- 帮股民选准100%暴涨黑马**:
股票名称: 股票代码: 股票简称: 股票类型: 股票状态: 股票评级:
股票代码: 000708 | 000708 | 000708 | 000708 | 000708 | 000708
股票名称: 金牛能源 | 金牛能源 | 金牛能源 | 金牛能源 | 金牛能源 | 金牛能源
股票简称: 金牛能源 | 金牛能源 | 金牛能源 | 金牛能源 | 金牛能源 | 金牛能源
股票类型: 股票 | 股票 | 股票 | 股票 | 股票 | 股票
股票状态: 上市 | 上市 | 上市 | 上市 | 上市 | 上市
股票评级: 持有 | 持有 | 持有 | 持有 | 持有 | 持有

Taobao Phishing == Money

- Over 80 billion dollars in 2010
- AliPay = Paypal
- Supported by most Chinese eBanks

The screenshot shows a payment interface for Alipay. At the top, there's a navigation bar with tabs like 'Newspaper', 'Google Reader', 'Annotations in Reader', 'Trend Micro Incorp...', 'MMO-Champion - ...', 'Online Translation... Online Dictionary...', 'Idea Discussion', and a search bar. Below the bar, it says 'Order ID: 6c26de45b17248209fbccb2bbbe9e677&bizIdentity=tra...'.

The main area displays payment details: 'Order ID: 6c26de45b17248209fbccb2bbbe9e677&bizIdentity=tra...', '收货方: 重庆中融广告传媒有限公司', '订单金额: 1.18 元'.

Below this, it says '您的支付宝账户: zxwwww@163.com' and '可支付余额: 0.00 元 账户充值'. A note below states: '您的账户没有可支付余额, 请使用其他方式付款, 或充值后付款。'

A section titled '您可以使用其他方式付款:' lists several payment methods: '储蓄卡' (selected), '信用卡', '网点', '消费卡', and '找人代付'.

Under '选择您的付款方式:', it says '网上银行: 需要通过网上银行付款。' and lists numerous bank logos:

中国工商银行	招商银行	中国建设银行	中国银行
中国农业银行	交通银行	中国邮政储蓄银行	Bank of China
浦发银行	广发银行 CGB	中信银行	中国光大银行
深圳发展银行	中国民生银行	北京银行	兴业银行
上海银行	大连银行	平安银行	杭州银行
温州银行	宁波银行	中国工商银行	富滇银行
中国农业银行	浦发银行	中国建设银行	中国建设银行

At the bottom, there's a large orange '下一步' button.

Taobao Phishing Demo

金册通用！移动50面值冲值卡只要1元，为打造信誉，特价活动，（5分钟内到账） - 淘宝网 - Windows Internet Explorer

File Edit View Favorites Tools Help

Favorites ① 全国通用! 移动50面值的冲值卡只要1元，为打造信誉... Google

淘宝网首页 | 我的宝贝 | 我的淘宝 | 购物车 | 收藏夹 | Q搜索 | 浏览导航

淘宝网

全国通用! 移动50面值冲值卡只要1元，为打造信誉... 搜索

淘宝小铺： 安全购物中心 华强北商圈 华强南商圈 美妆饰品区 消费者维权中心 无差评

淘客推广

商品名称：神州行 全球通 动感地带 移动话费充值 50

一口价：1.00 元

速 度：快速充值速度

30天售后：30天（查看详情）

付款方式：支付宝担保 支付宝担保 加入收藏 添加到购物车

我 购 买

所在地： 展开

特色服务：

此宝贝为您推荐

店主动态评价分

店主信用评价： ★★★★★ 4.9
卖家的服务态度： ★★★★★ 4.9
卖家发货的速度： ★★★★★ 4.9

从区域： 展开

选择更多商品 进入本店店铺

收藏本店铺 立即购买

分享给别人 收藏宝贝

支持在线开通信用卡支付的银行： 招商银行

支持在线开通网上支付的银行： 中国光大银行

支持在线开通网上支付的银行： 兴业银行

支持在线开通网上支付的银行： 中国工商银行

支持在线开通网上支付的银行： 中国建设银行

支持在线开通网上支付的银行： 中信银行

支持在线开通网上支付的银行： 深圳发展银行

支持在线开通网上支付的银行： 兴业银行

宝贝详情 评价详情 反馈记录(30件) 掌柜档案 物流方式 售后服务 咨询师

产品描述：全国通用话费50元

Instant Demo™

Watermark displayed in trial version.

Done, but with errors on page

11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 26 27 28 29 30 31 32 33 34 35 36 37 38 39 40 41 42 43 44 45 46 47 48 49 50 51 52 53 54 55 56 57 58 59 60 61 62 63 64 65 66 67 68 69 70 71 72 73 74 75 76 77 78 79 80 81 82 83 84 85 86 87 88 89 90 91 92 93 94 95 96 97 98 99 100

Local Internet 100% 100% 6:00 i

Phishing Web Site Source Code

- Active market
- Sell at a price < ¥1000
- Copied from a template

The screenshot shows a Google search results page for the query "钓鱼网站源码". The results are filtered to show only "Everything" and include "Images", "Videos", "News", "Shopping", and "More". The search interface includes dropdown menus for "Any time", "Latest", "Past 24 hours", "Past 3 days", "Past week", "Past month", "Past year", and "Custom range". Below these are sections for "All results", "Sites with images", and "Wonder wheel", along with a link to "More search tools". The search results themselves are listed on the right, showing various links related to phishing website templates, such as "钓鱼软件源码 (可以制作钓鱼网站的钓鱼网站)" and "QQ自由钓鱼网站源码_94 inn". The results are paginated with a "Previous" button and page numbers 1, 2, 3, 4, 5.

钓鱼网站源码

Page 2 of about 184,000 results (0.12 seconds)

[钓鱼软件源码 \(可以制作钓鱼网站的钓鱼网站\)](#) | 工
- | 点击进入下载 - [rar Visual Basic
20104-5月10日 ... 点击进入下载 - \[rar Visual Basic
nian uneasy command.htm file 127.html Cached Sim\]\(#\)](#)

[地下城与勇士钓鱼网站源码_钓鱼网站论坛_天](#)
2011年8月18日 ... 地下城与勇士钓鱼网站源码_钓鱼网站
[www.fishyzz.com/thread-10000-1-1.html](#)

[QQ自由钓鱼网站源码_94 inn](#) | [简体中文 首页 Tra
QQ自由钓鱼网站源码_94 inn | 简体中文 首页 Tra
- | 点击进入前台 : [www.hbc20.com](#) | 网站前台由白程序 Cached

[淘宝钓鱼网站源码_94 inn](#) | [简体中文 首页 Tra
- | 点击进入前台 : [www.94.inn.com/keyword/t/淘宝钓鱼网站源码/](#) Cached

[458钓鱼网站源码带域名带远程一开一开兵工厂](#)
2011年6月16日 ... 黑客培训,黑客教程,黑客技术,黑客
让你从菜鸟到大神,黑客高手木马开发,黑客攻防,
[www.exehack.com/article/28/210.html](#) - Cached

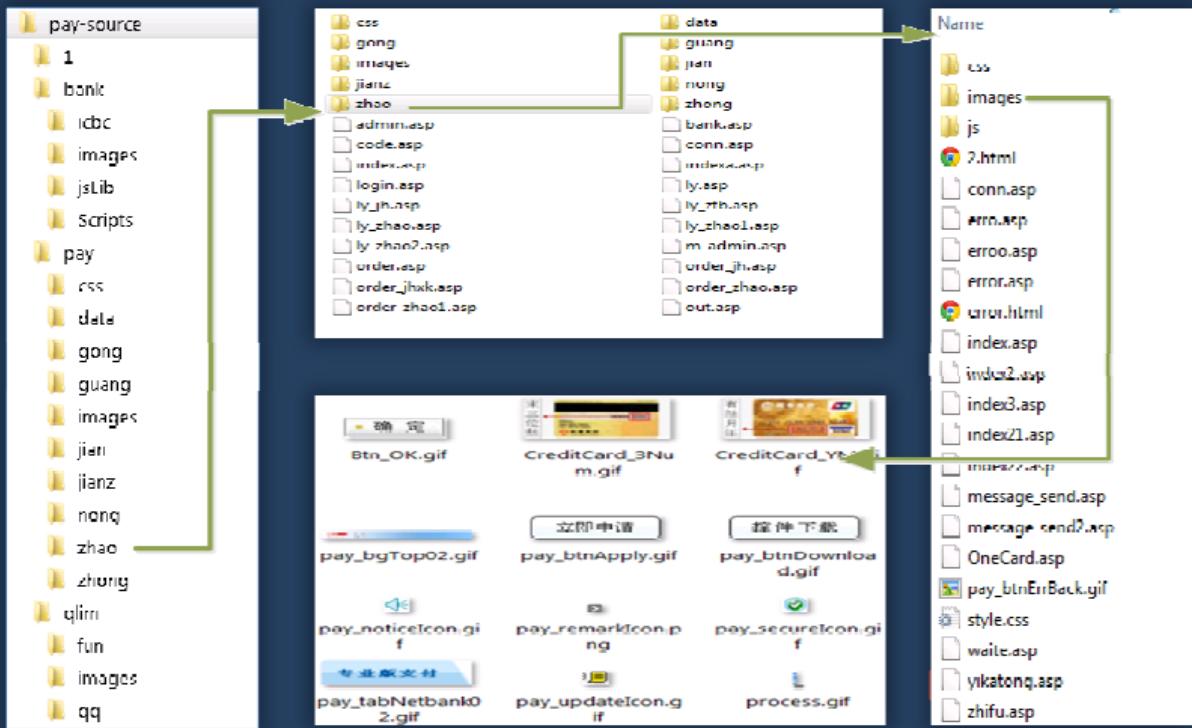
[梦幻西游钓鱼网站源码_暗黑必杀联盟](#) | [暗
2011年5月8日 ... 幻梦西游钓鱼网站源码_ ... 简介 : 幻梦同
络(梦幻西游)完美无损版, by CnH199 Ch : admin 好评
[www.cnh199.cn/conlanguan0111/2010/2919.html](#) Cached

[00一二网钓鱼网站源码\(普通版\)_00资源网](#) | [普
2010年11月13日 ... 00一二网钓鱼网站源码(普通版)是操作
本网站不仅正以二网的官网版源码(普通版)的便捷性,完全
[www.00yuanze.com](#) | 软件下载 - Cached

[术淘宝钓鱼网站源码高仿版！ - 已回答 - 技术问](#)
2011年4月4日 ... 求淘宝钓鱼网站源码高仿版！要能用的
淘宝钓鱼网站源码高仿版！要能用的最好是发到010990010
[www.00yuanze.com](#) | 全部问题 - 电脑数码 - 电脑技术全

◀ Goooooo
Previous 1 2 3 4 5

Source Code and Framework



Summary

Characteristics of Chinese Phishing Websites

- Lottery scam is targeted to **a few branded websites** which are then faked: QQ, Taobao, CCTV
- **Scams/fraudulent websites are** so popular and go beyond the traditional phishing scope
- **Short uptime** of phishing websites because they are easy to create
- **Visual/content similarity** among fake websites
- URLs are propagated by **IMs, BlackSeo** or **Comprised Servers**



Never Be Phished



Thanks