

Phishing and Online Scams in China

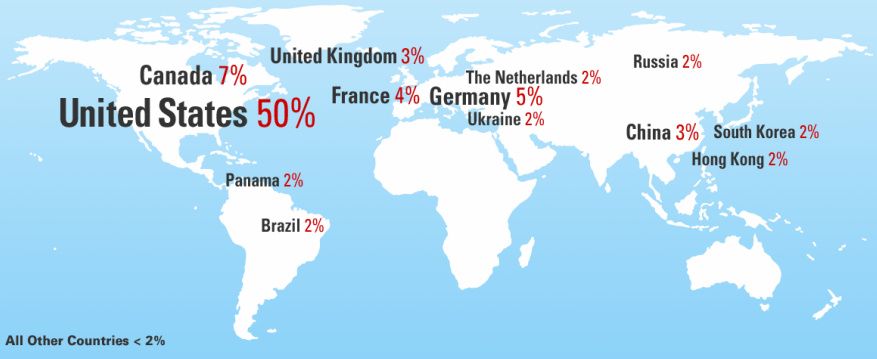
Joey Zhu

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**

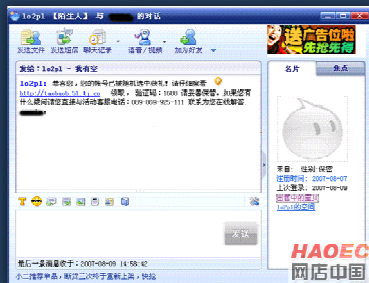
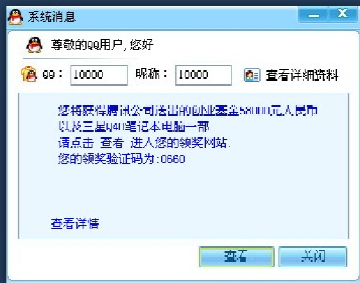


A typical lottery scam

- 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

The screenshot shows a web browser window with the address bar displaying `www.ccbak.com/kaoshizixun/394.html`. The page content includes a navigation menu, a search bar, and several image-based advertisements. A red-bordered pop-up window titled "腾讯qq 系统消息" (Tencent QQ System Message) is overlaid on the bottom right of the page. The message text reads: "尊敬的QQ用户您好! 恭喜您,您的QQ账号已被系统后台随机抽选为'QQ周年庆'第23万等用户!双喜临门!提供丰厚惊喜奖金¥80000元以及三星Q40笔记本一台!" (Dear QQ user, congratulations! Your QQ account has been randomly selected by the system backend as the 230,000th user for 'QQ Anniversary'! Double happiness! Providing rich surprise prizes of ¥80,000 and a Samsung Q40 laptop!). The browser's taskbar at the bottom shows the date as 2011/4/17.

Fraudulent Websites

New Phishing without Target Brand

Delivered by AdWords

The image displays two side-by-side screenshots of a fraudulent website designed to impersonate Hainan Airlines. Both screenshots show a browser window with a search bar containing the URL `www.frijian123.net` (left) and `www.hangkongair.com` (right). The website layout is identical, featuring the Hainan Airlines logo, the text "全国统一客服受理专线: 400-6887-030", and a search form for flights. The search form includes fields for "出发城市" (Origin City), "目的地" (Destination), "起飞日期" (Departure Date), "航空公司" (Airline), and "舱位" (Cabin Class). A large red watermark "Share Same Template" is overlaid on the right screenshot.

Scams with Stocks & Securities for membership fees

The screenshot shows a web browser window displaying a scam website. The browser's address bar shows a URL from Baidu.com. The website's header includes the company name '上海森洋投资咨询有限公司' and the slogan '合理规避风险 稳健创造财富'. Below the header, there is a navigation menu with various service categories. The main content area features a large red banner with the text '请点击查看04月18日一只必涨股票已公开验证!' (Click to view! A stock that is guaranteed to rise on April 18th has been publicly verified!). To the right of the banner, there is a table with columns for '证券名称' (Security Name), '最新价' (Latest Price), and '涨跌幅' (Change). The table lists several securities with their respective prices and changes. Below the table, there is a section for '联系我们' (Contact Us) and a list of services. The website also includes a search bar and a '百度一下' (Baidu Search) button.

Taobao Phishing == Money

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

https://cashier.alipay.com/standard/payment/cashier.htm?orderId=6c26de45b17248209fbccb2bbbe9e6778&bizIdentity=tra...
新浪网 Google 阅读器 阅读器中的注释 Trend Micro Incorp... MMO-Champion - L... 在线翻译_在线词典... Idea Discussion

订单名称: 24小时电脑充值 江苏穆... 详单
收款方: 重庆中融广告传媒有限...
订单金额: 1.18 元

您的支付宝账户: zxwww@163.com
可支付余额: 0.00 元 账户充值

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。

您可以使用其他方式付款: 储蓄卡 信用卡 网点 消费卡 找人代付

选择您的付款方式

网上银行: 需要通过网上银行付款

<input checked="" type="radio"/> 中国工商银行	<input type="radio"/> 招商银行	<input type="radio"/> 中国建设银行	<input type="radio"/> 中国银行
<input type="radio"/> 中国农业银行	<input type="radio"/> 交通银行	<input type="radio"/> 中国邮政储蓄银行	<input type="radio"/> Bank 中国光大银行
<input type="radio"/> 民生银行	<input type="radio"/> 广发银行 CGB	<input type="radio"/> 中信银行	<input type="radio"/> 兴业银行
<input type="radio"/> 深圳发展银行	<input type="radio"/> 中国民生银行	<input type="radio"/> 北京银行 BANK OF BEIJING	<input type="radio"/> 杭州银行
<input type="radio"/> 上海银行	<input type="radio"/> 北京农村商业银行	<input type="radio"/> 华夏银行 HUAXIA BANK	<input type="radio"/> 富信银行
<input type="radio"/> 温州银行	<input type="radio"/> 宁波银行	<input type="radio"/> 中国工商银行 企	<input type="radio"/> 中国建设银行 企
<input type="radio"/> 中国农业银行 企	<input type="radio"/> 浦发银行 SPDBANK 企		

下一步

Taobao Phishing Demo

The screenshot shows a browser window with the address bar containing a URL that appears to be a phishing site. The page layout includes a top navigation bar with the Taobao logo, a search bar, and a main content area with various promotional banners and product listings. A large blue play button is overlaid on the page, indicating a video or demo recording. A watermark 'Instant Demo' is visible in the bottom right corner.

金眼鱼! 领取50张价值优惠券共需1元, 为打造惊喜, 特价商品, (3分钟到账) - 淘宝网 - Windows Internet Explorer

File Edit View Favorites Tools Help

Home 全国通用! 领取50张价值优惠券共需1元, 为打造惊喜...

淘宝网

淘宝网小助手: 商家帮助中心 | 买家帮助中心 | 卖家帮助中心 | 消费者帮助中心

全国通用! 领取50张价值优惠券共需1元, 为打造惊喜, 特价商品, (3分钟到账)

神州行 全球通 动感地带 全国通用 移动话费充值 50

价格: 1.00元

运费: 卖家承担运费

30天包退: 30件 (含运费险)

支付方式: 支付宝余额 网银支付 网上银行 货到付款

卖家: []

商品描述: 中山信通 特色服务: 此宝贝为...

掌柜档案

会员信用

好评率: 100%

好评率: 100%

宝贝描述相符: ★★★★★

卖家的服务态度: ★★★★★

宝贝的真实性: ★★★★★

支付宝: []

快速下单商品 真人审核店铺

收藏率店铺 卖家信用等级

友情链接: 招商银行 工商银行 建设银行 农业银行 交通银行 中信银行 中国工商银行 中信银行 深圳发展银行 兴业银行

宝贝评价 评价详情 或写评价(20字) 掌柜评价 买家评价 售后服务 留言簿

产品总价: 全国通用(¥50)

Done, but with errors on page.

Instant Demo™

Watermark displayed

Trial version only

Local Internet

0:00

Phishing Web Site Source Code

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

Google 钓鱼网站源码

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

Everything
Images
Videos
News
Shopping
More

Any time
Latest
Past 24 hours
Past 3 days
Past week
Past month
Past year
Custom range

All results
Sites with images
Wonder wheel
More search tools

[钓鱼软件源码 \(可制作任何网站钓鱼网站\) | 工...](#)
- [[翻译此网页](#) - Translate this page]
2010年6月10日 ... 点上进入下载 - yy源码.rar Visual Des
nlijian.tianyay.com/read.htm?id=177.html - Cached - Sim

[地下城与勇士钓鱼网站源码的 钓鱼网站源码 于...](#)
2011年6月18日 ... 地下城与勇士钓鱼网站源码 钓鱼网站
www.tanyay.com/shi/mao.php?url=duo/duoyi/2011/16/1

[QQ自由虫族的钓鱼网站源码 上网络版的鱼虫族...](#)
- [[翻译此网页](#) - Translate this page]
QQ自由虫族的钓鱼网站源码(源代码) : 点击进入前台
www.wbo360.com 网络版的鱼虫族 - Cached

[淘宝钓鱼网站源码_92 inn 网](#) [[翻译此网页](#) - Tr...

中国钓鱼网站源码网网站源码(源代码) | QQ自
由虫族的钓鱼网站源码 淘宝钓鱼网站源码的编程... | 网
www.92.inn.com/keyword/淘宝钓鱼网站源码/ - Cached

[458钓鱼网站源码带域名带程序一套_黑客社区](#)
2011年6月16日 ... 黑客软件, 黑客教程, 黑客
社区从零基础技术培训, 黑客安全技术, 黑客教程,
www.4xehack.com/article/29/210.html - Cached

[梦幻西游钓鱼网站源码 腾讯安全联盟](#) 网... | 再...

2011年2月8日 ... 梦幻西游钓鱼网站源码 ... 简介: 梦幻西游
(新云核心) 完美无删版 by CaHk99.Cn : admin 好评
www.caHk99.cn/caHk99/2011/03/06/2609.html - Cached

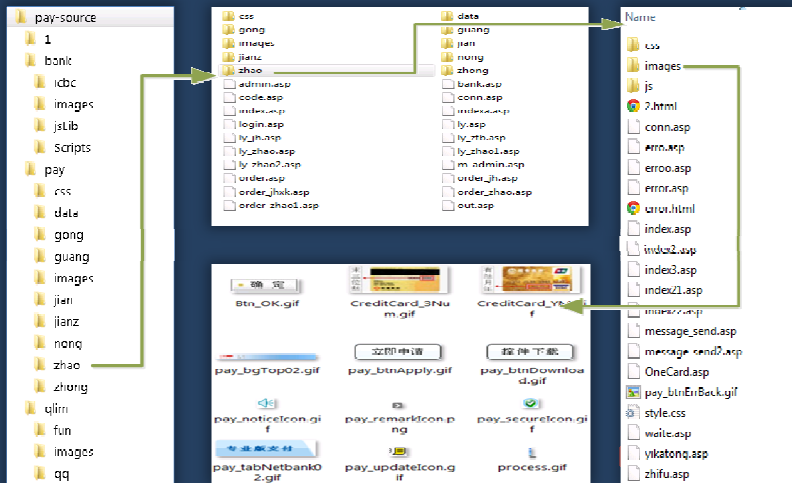
[QQ三国钓鱼网站源码\(普通版\) - QQ资源网](#) 网... | 再...

2010年11月13日 ... QQ三国钓鱼网站源码(普通版)是操作
本网站不仅证明QQ三国的钓鱼网站源码(普通版)的准确性安全
www.qqzy.com : 软件下载 - Cached

[求淘宝钓鱼网站源码的卖家!!! 已回信 - 找源码](#)
2011年6月4日 ... 求淘宝钓鱼网站源码的卖家!!! 要实用的
钓鱼网站源码急急!!! 要实用的就给我发到169933016
whw@whw.com : 全部转载, 电脑软件, 电脑安全

Googoo
Previous 1 2 3 4

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