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
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
Taobao Phishing == Money

• Over 80 billion dollars in 2010
• AliPay = Paypal
• Supported by most Chinese eBanks
Phishing Web Site Source Code

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