RSA®CONFERENCE
CHINA 2012
RSA信息安全大会2012

THE GREAT CIPHER

MIGHTIER THAN THE SWORD
伟大的密码胜于利剑

网络犯罪趋势 – 聚焦亚洲

Michal Blumenstyk-Braverman
RSA — 全球解决方案总经理

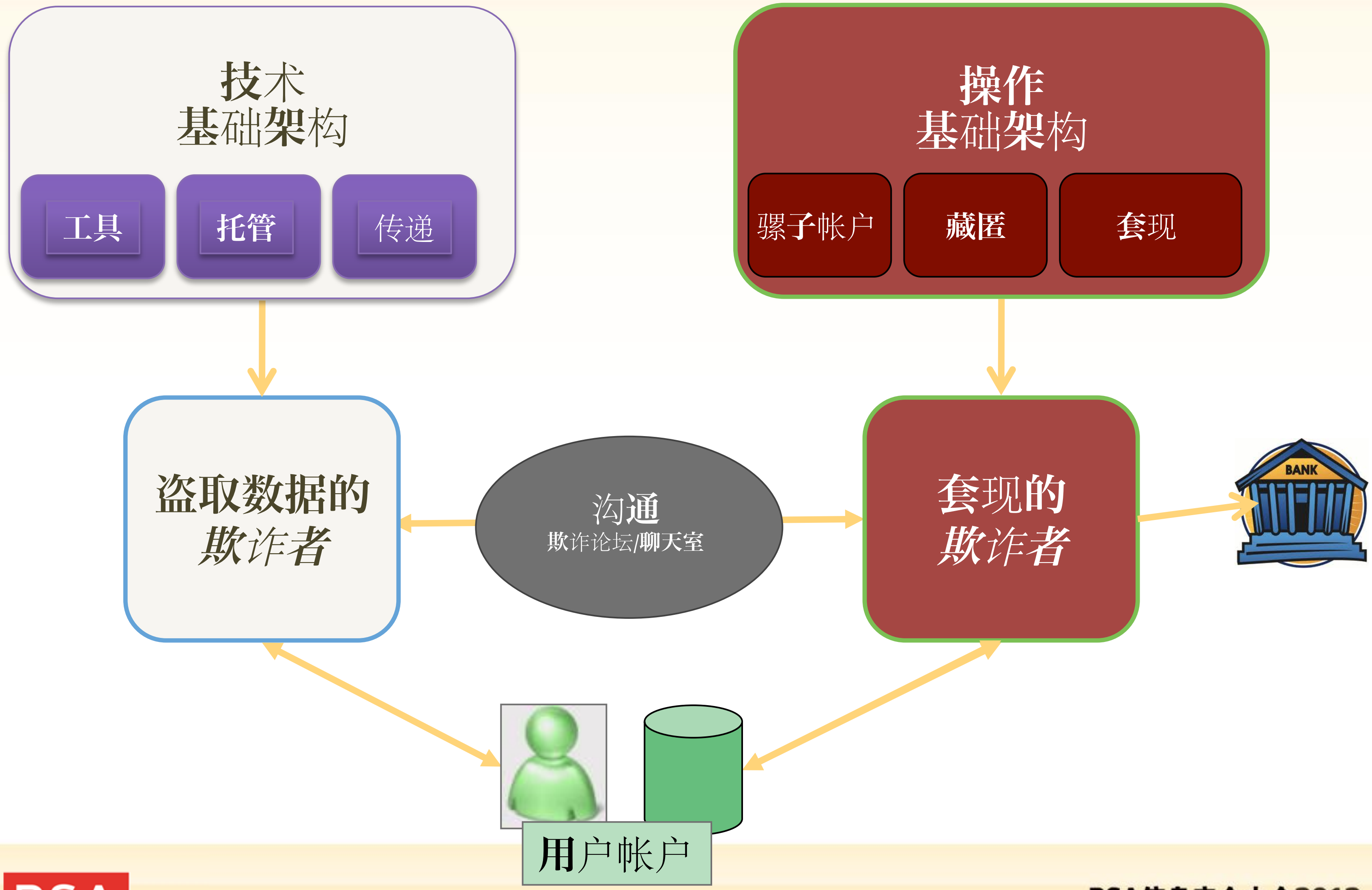
RSACONFERENCE
CHINA 2012
RSA信息安全大会2012

行业反击

- 运营规模：
  - 300,000,000 名用户受到 eFraudNetwork 的保护
  - 700,000 次钓鱼攻击受到反欺诈指挥中心的拦截
  - 受到保护的机构超过 10,000 家

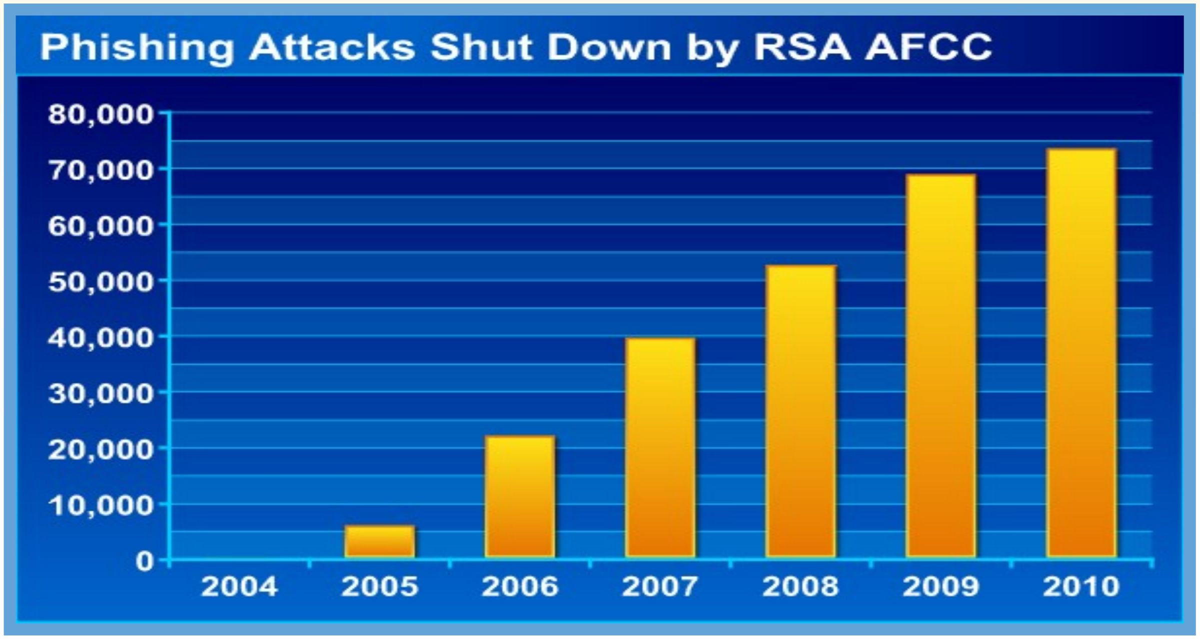
RSA FIGHTS FRAUD
$ 3,103,477,861
Losses Prevented Since 01.01.2011

网络犯罪/欺诈产业链


技术
基础架构
工具
托管
传递
操作
基础架构
骡子帐户
藏匿
套现
盗取数据的
欺诈者
沟通
欺诈论坛/聊天室
套现的
欺诈者
BANK
用户帐户

多防线防御：
应对外部威胁

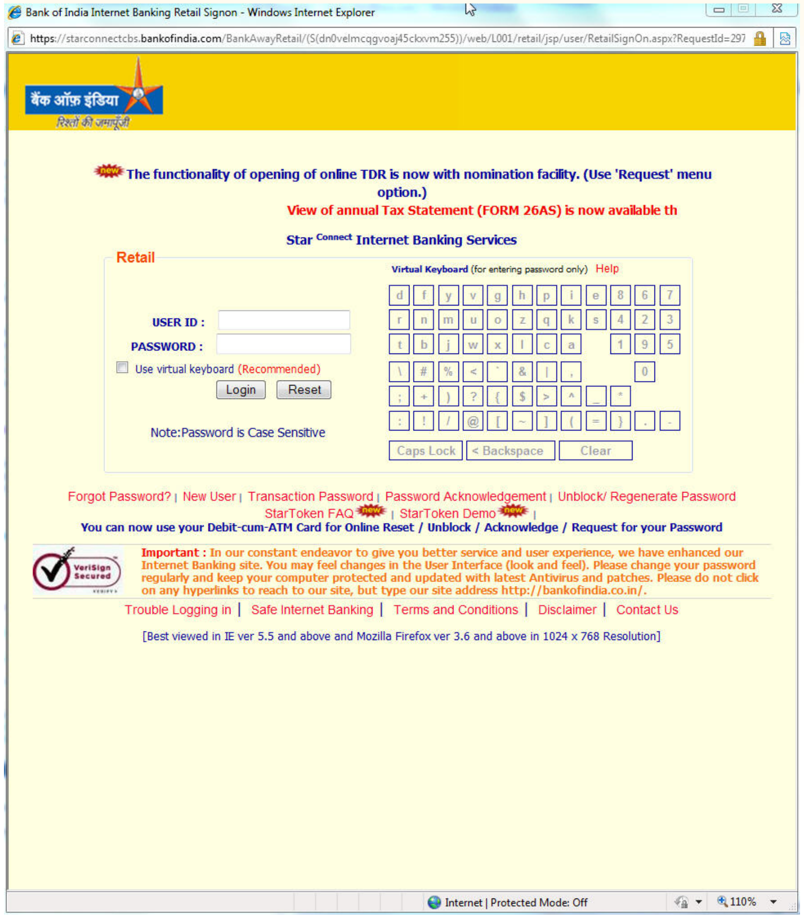
全天候反欺诈指挥中心



- 35% 来自美国境外；70% 来自被劫持的服务器
- 目标针对各行各业：金融、通信、医疗、保险等行业

钓鱼攻击情况比以前有所好转

哪一个是真正的页面？


Bank of India Internet Banking Retail Signon - Windows Internet Explorer
https://starconnectcbs.bankofindia.com/BankAwayRetail/(S(dn0velmcqgvoaj45ckxvm255))/web/L001/retail/jsp/user/RetailSignOn.aspx?RequestId=297
बैंक ऑफ़ इंडिया
रिश्तों की जमापूँजी
new
d f y v g h p i e 8 6 7
r n m u o z q k s 4 2 3
t b j w x l c a 1 9 5
\ # % < ` & | , 0
; +) ? { $ > ^ _ *
: ! / @ [~] (= } . -
Caps Lock
< Backspace
Clear
Login
Reset
VeriSign Secured
Internet | Protected Mode: Off
110%

The functionality of opening of online TDR is now with nomination facility. (Use 'Request' menu option.)

View of annual Tax Statement (FORM 26AS) is now available th

Star Connect Internet Banking Services

Retail

Virtual Keyboard (for entering password only) Help

USER ID :

PASSWORD :

□ Use virtual keyboard (Recommended)

Note:Password is Case Sensitive

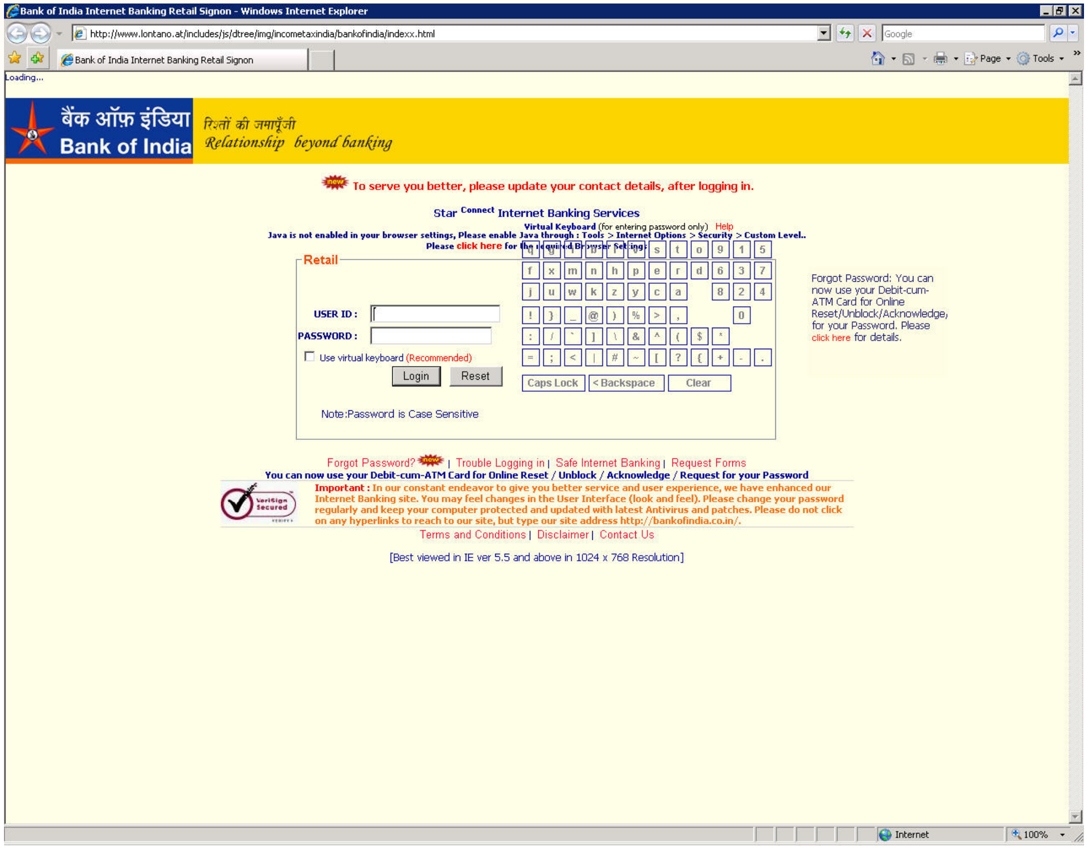
Forgot Password? | New User | Transaction Password | Password Acknowledgement | Unblock/ Regenerate Password
StarToken FAQ | StarToken Demo |

You can now use your Debit-cum-ATM Card for Online Reset / Unblock / Acknowledge / Request for your Password

Important : In our constant endeavor to give you better service and user experience, we have enhanced our Internet Banking site. You may feel changes in the User Interface (look and feel). Please change your password regularly and keep your computer protected and updated with latest Antivirus and patches. Please do not click on any hyperlinks to reach to our site, but type our site address http://bankofindia.co.in/.

Trouble Logging in | Safe Internet Banking | Terms and Conditions | Disclaimer | Contact Us

[Best viewed in IE ver 5.5 and above and Mozilla Firefox ver 3.6 and above in 1024 x 768 Resolution]



To serve you better, please update your contact details, after logging in.

Star Connect Internet Banking Services

Virtual Keyboard (for entering password only) Help

Java is not enabled in your browser settings, Please enable Java through : Tools > Internet Options > Security > Custom Level..
Please click here for the required Browser Settings

Retail

USER ID :

PASSWORD :

□ Use virtual keyboard (Recommended)

Note:Password is Case Sensitive

Forgot Password: You can now use your Debit-cum-ATM Card for Online Reset/Unblock/Acknowledge, for your Password. Please click here for details.

Forgot Password? | Trouble Logging in | Safe Internet Banking | Request Forms

You can now use your Debit-cum-ATM Card for Online Reset / Unblock / Acknowledge / Request for your Password

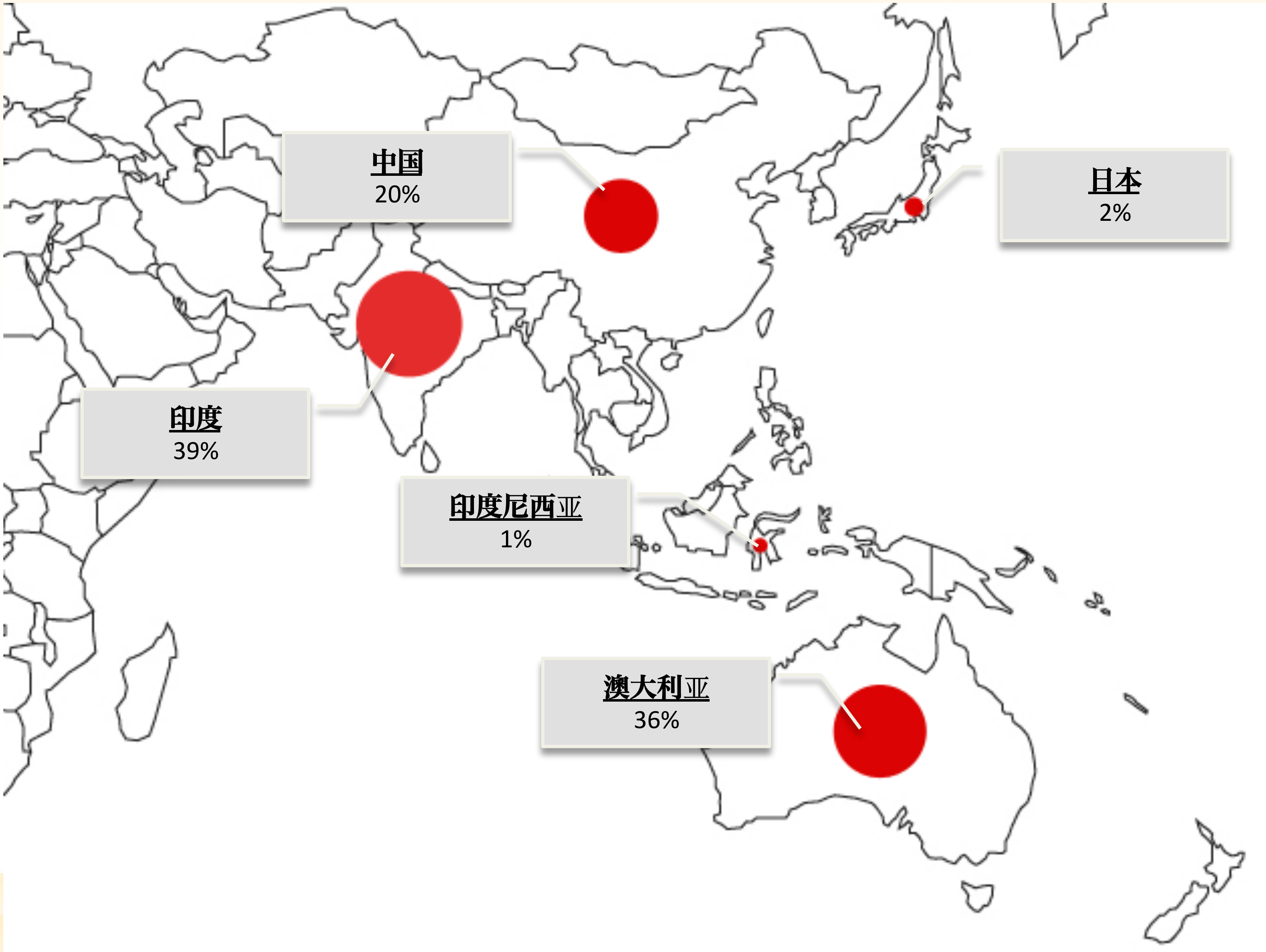
Important : In our constant endeavor to give you better service and user experience, we have enhanced our Internet Banking site. You may feel changes in the User Interface (look and feel). Please change your password regularly and keep your computer protected and updated with latest Antivirus and patches. Please do not click on any hyperlinks to reach to our site, but type our site address http://bankofindia.co.in/.

Terms and Conditions | Disclaimer | Contact Us

[Best viewed in IE ver 5.5 and above in 1024 x 768 Resolution]

gle.com/store/apps/details?id=com.paijwar.smsbanking&feature=search_result

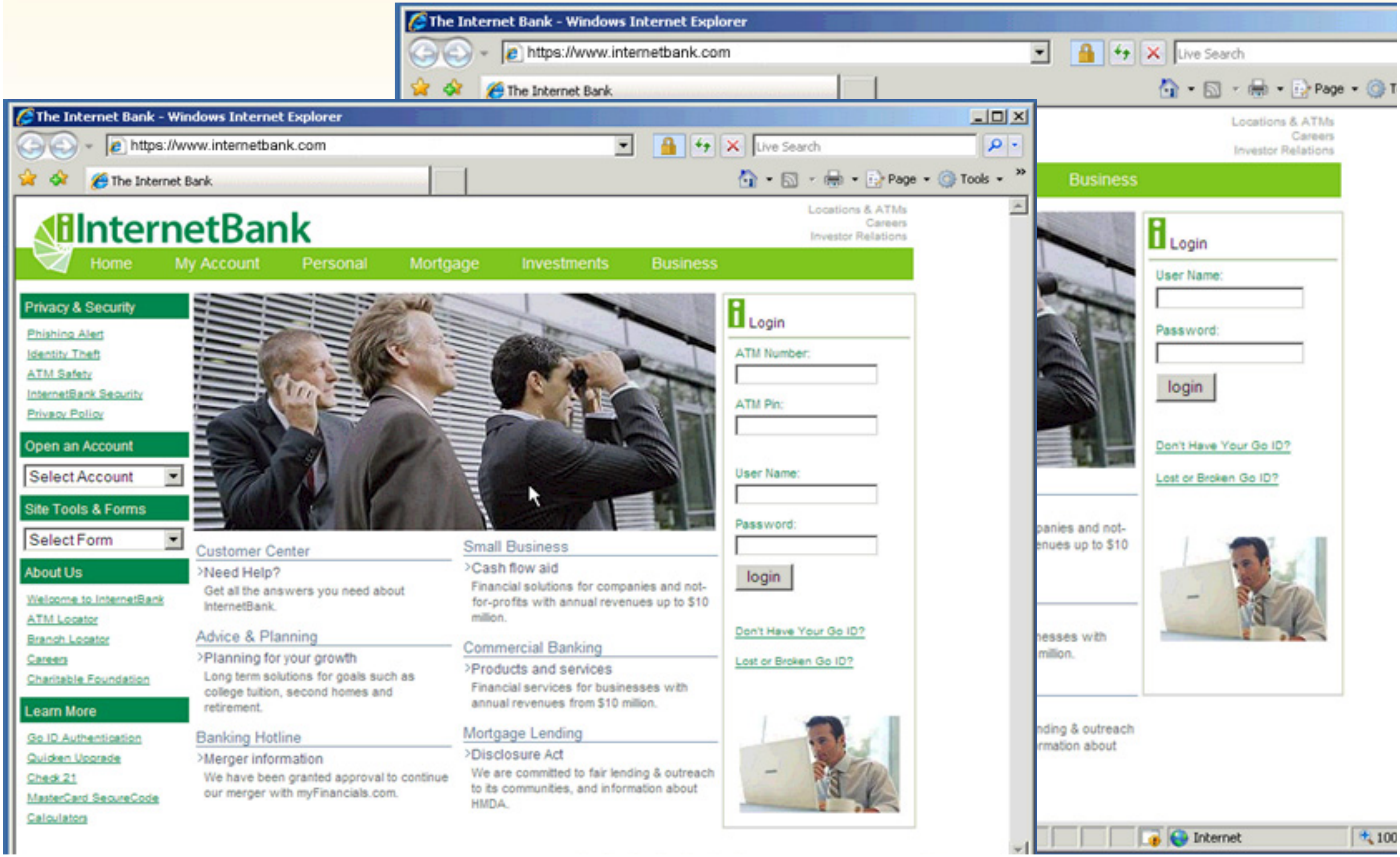
亚太及日本地区的比例（钓鱼攻击分布图 2012）



最严重

特洛伊木马

RSACONFERENCE
CHINA 2012



Customer Center
>Need Help?
Get all the answers you need about InternetBank.

Advice & Planning
>Planning for your growth
Long term solutions for goals such as college tuition, second homes and retirement.

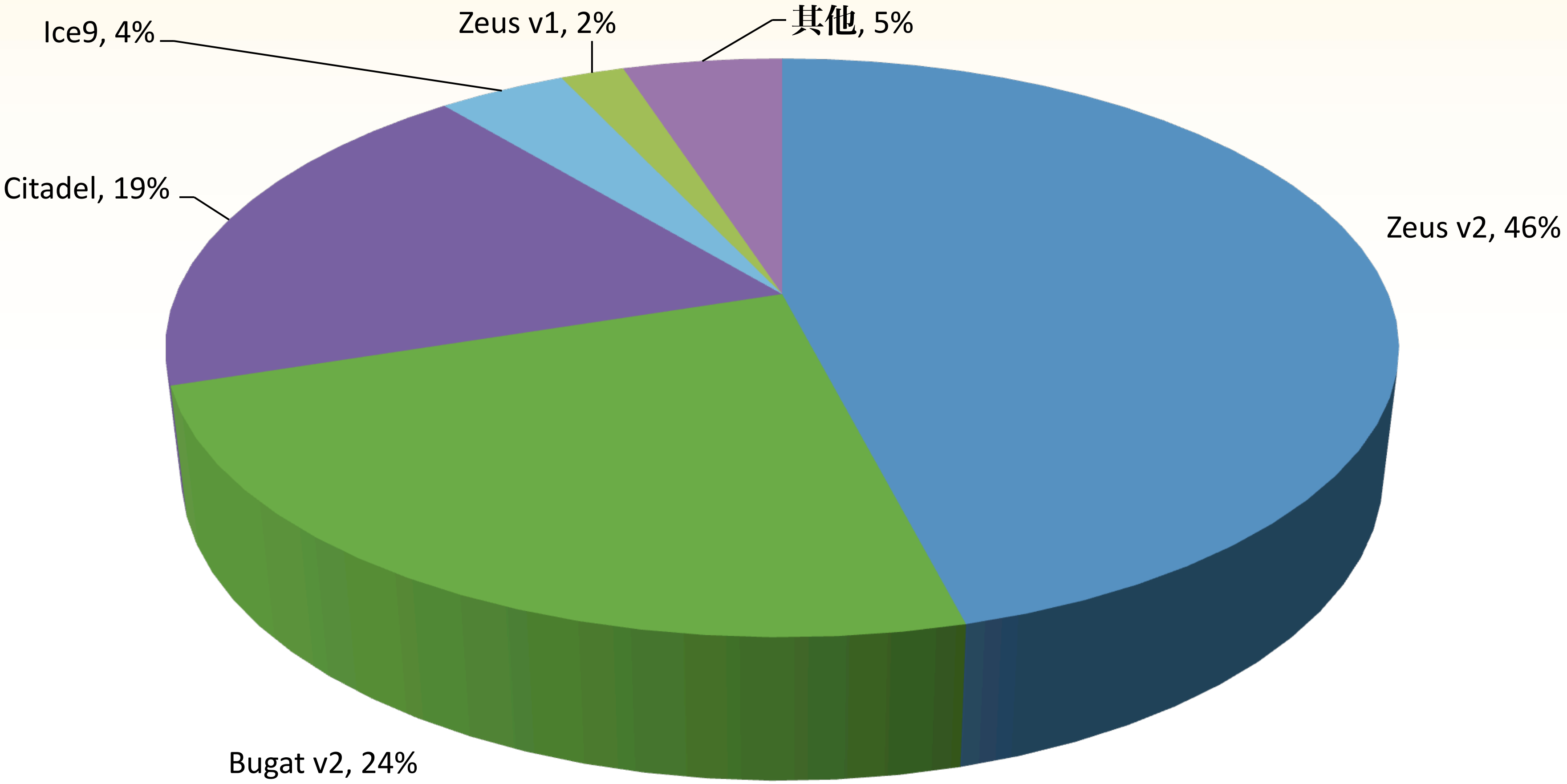
Banking Hotline
>Merger information
We have been granted approval to continue our merger with myFinancials.com.

Small Business
>Cash flow aid
Financial solutions for companies and not-for-profits with annual revenues up to $10 million.

Commercial Banking
>Products and services
Financial services for businesses with annual revenues from $10 million.

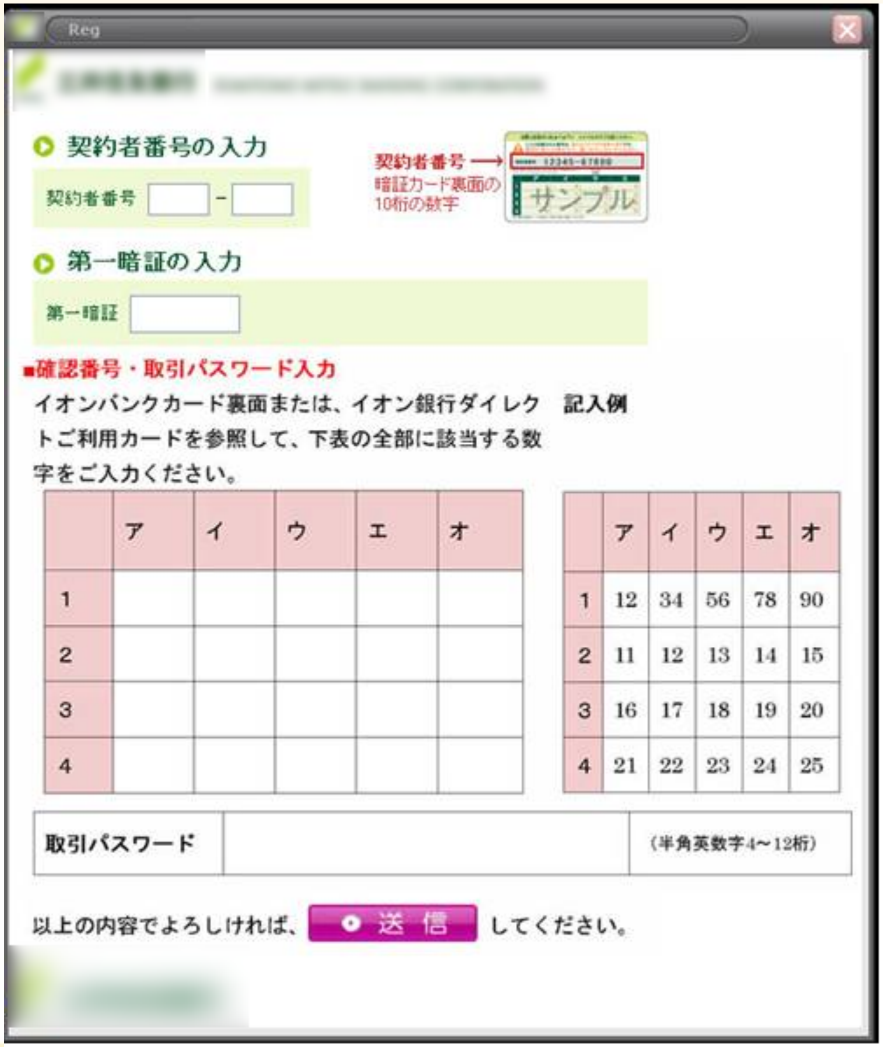
Mortgage Lending
>Disclosure Act
We are committed to fair lending & outreach to its communities, and information about HMDA.

主动型特洛伊木马系列的主要类型（2012 年第二季度）



特洛伊木马 Sudoku 攻击日本银行

- 该**特洛伊木马的攻**击目标为银行客户
- **申**请用户 **ID**、**密码和交易**验证代码



[redacted]

○ 契約者番号の入力

契約者番号 [　　] - [　　]

契約者番号 ⟶
暗証カード裏面の
10桁の数字

○ 第一暗証の入力

第一暗証 [　　]

■確認番号・取引パスワード入力

イオンバンクカード裏面または、イオン銀行ダイレクトご利用カードを参照して、下表の全部に該当する数字をご入力ください。

	ア	イ	ウ	エ	オ
1					
2					
3					
4					

記入例

	ア	イ	ウ	エ	オ
1	12	34	56	78	90
2	11	12	13	14	15
3	16	17	18	19	20
4	21	22	23	24	25

取引パスワード		（半角英数字4～12桁）

以上の内容でよろしければ、 ○ 送 信 してください。

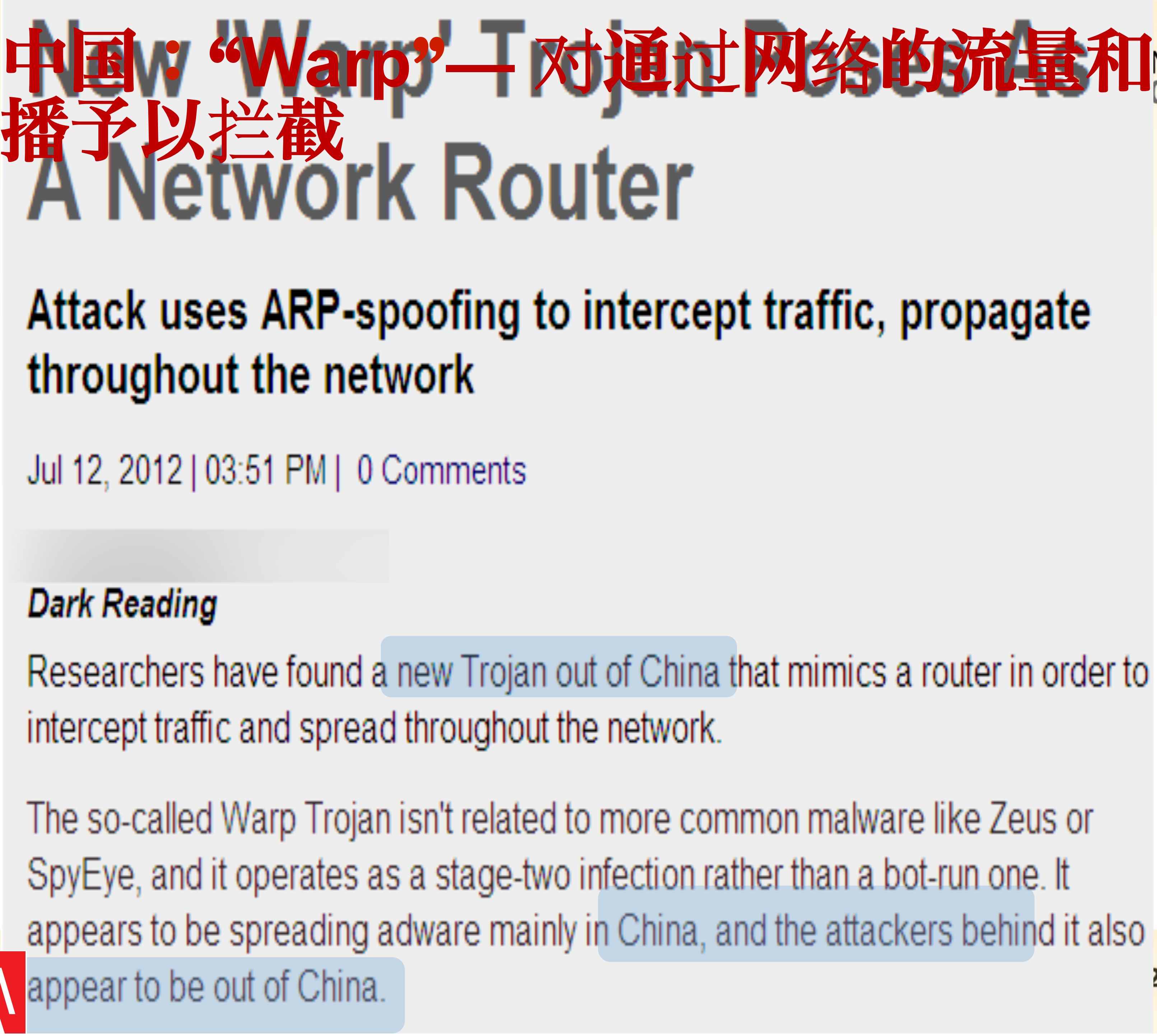
[redacted]

eDead 特洛伊木马攻击韩国和日本的银行

- 该特洛伊木马的攻击目标为银行客户

- 记录银行网站上输入的搜索字

在中国：“Warp”— 对通过网络的流量和传播予以拦截



New 'Warp' Trojan Poses As A Network Router

Attack uses ARP-spoofing to intercept traffic, propagate throughout the network

Jul 12, 2012 | 03:51 PM | 0 Comments

Dark Reading

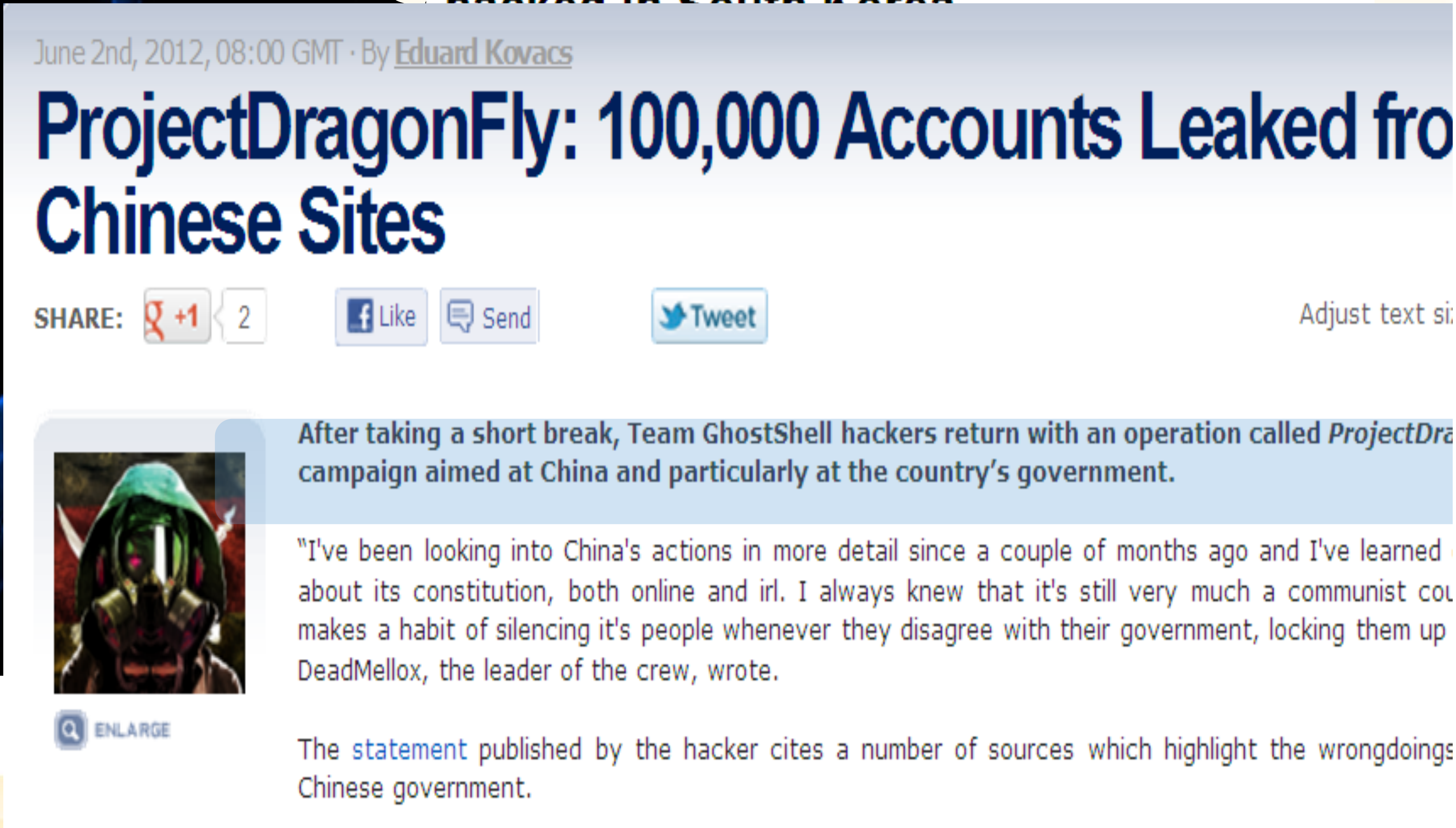
Researchers have found a new Trojan out of China that mimics a router in order to intercept traffic and spread throughout the network.

The so-called Warp Trojan isn't related to more common malware like Zeus or SpyEye, and it operates as a stage-two infection rather than a bot-run one. It appears to be spreading adware mainly in China, and the attackers behind it also appear to be out of China.

企业内的恶意软件

- 黑客入侵行为导 危

Data of 8.7 million KT subscribers hacked in South Korea



June 2nd, 2012, 08:00 GMT · By Eduard Kovacs

ProjectDragonFly: 100,000 Accounts Leaked fro Chinese Sites

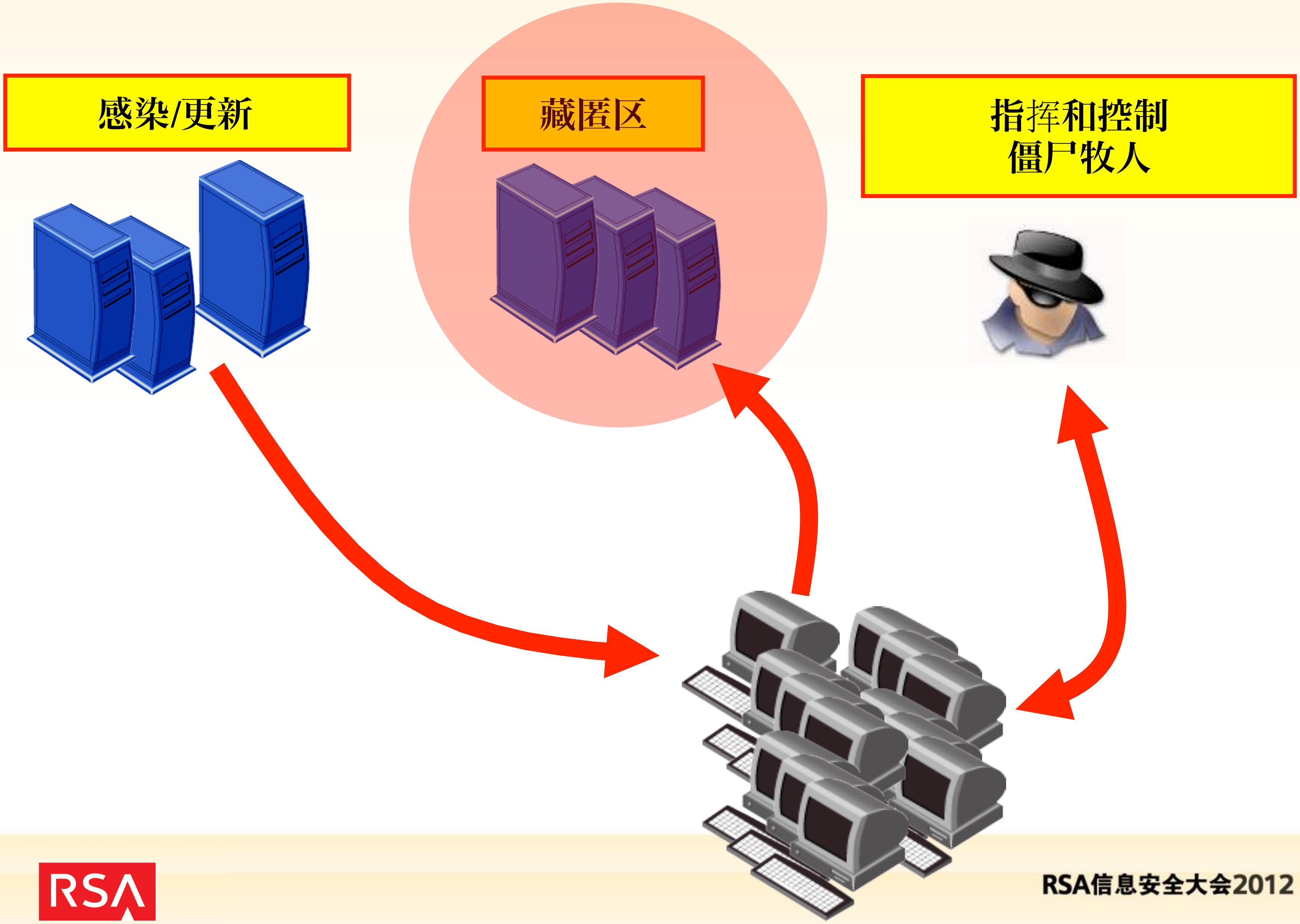
After taking a short break, Team GhostShell hackers return with an operation called *ProjectDra* campaign aimed at China and particularly at the country's government.

"I've been looking into China's actions in more detail since a couple of months ago and I've learned about its constitution, both online and irl. I always knew that it's still very much a communist cou makes a habit of silencing it's people whenever they disagree with their government, locking them up DeadMellox, the leader of the crew, wrote.

The statement published by the hacker cites a number of sources which highlight the wrongdoings Chinese government.

numbers and phone numbers.

特洛伊木马基础架构

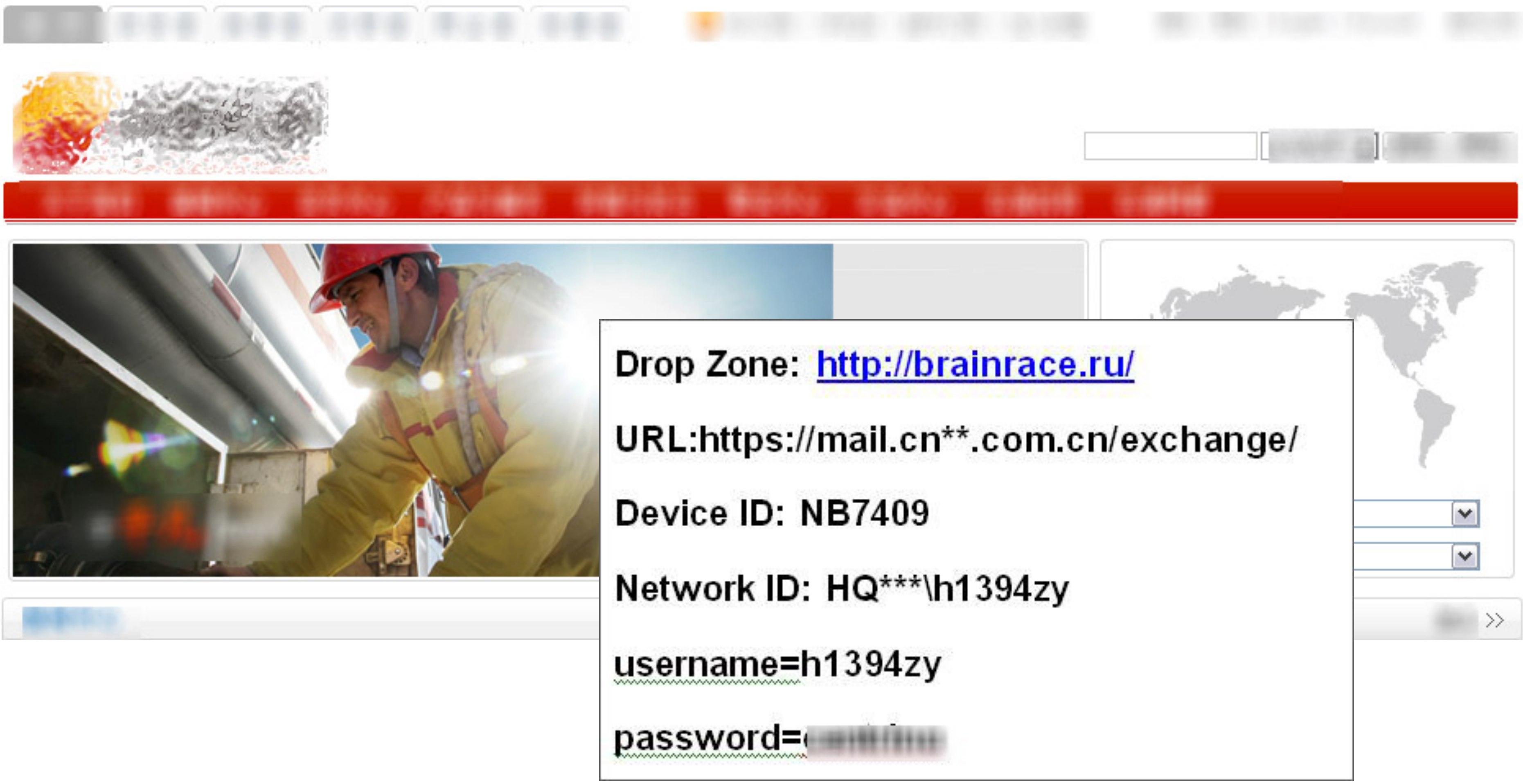


感染/更新

藏匿区

指挥和控制
僵尸牧人

中国石油巨头



Drop Zone: http://brainrace.ru/

URL:https://mail.cn**.com.cn/exchange/

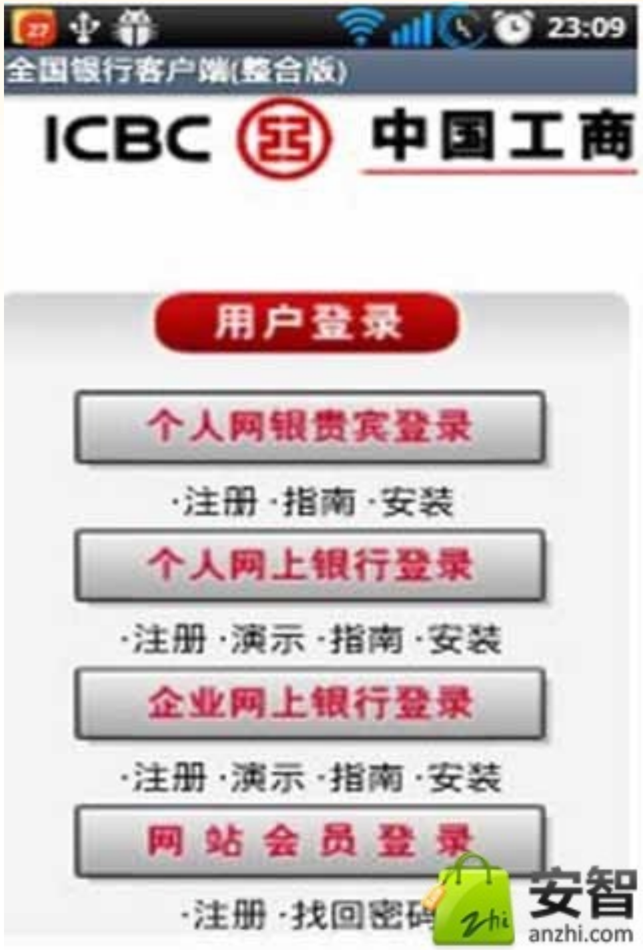
Device ID: NB7409

Network ID: HQ***\h1394zy

username=h1394zy

password=[redacted]

Rogue application - Samples



全国银行客户端(整合版)

ICBC 中国工商

用户登录

个人网银贵宾登录

·注册 ·指南 ·安装

个人网上银行登录

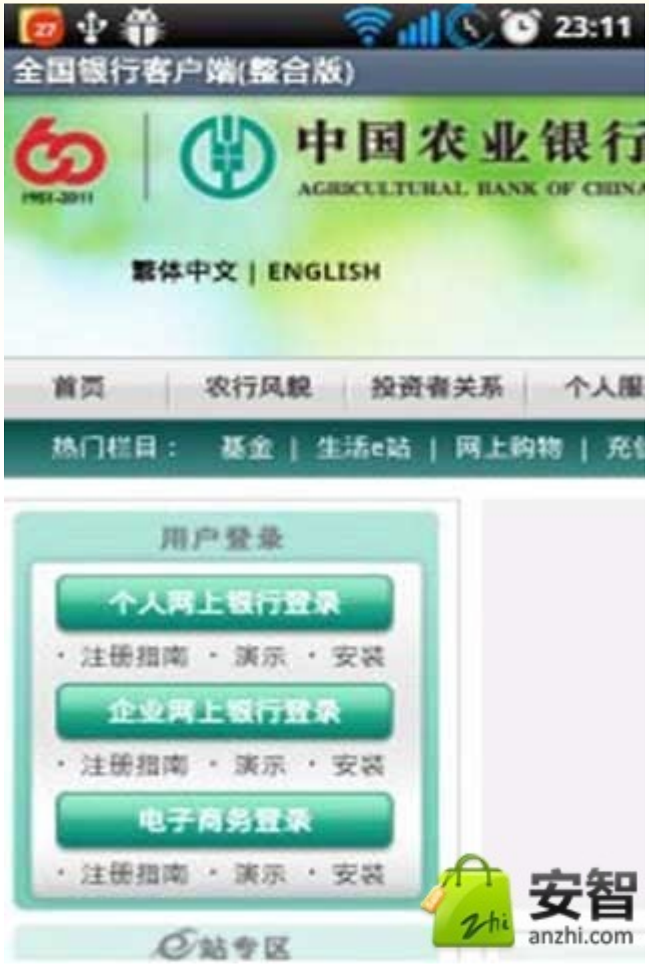
·注册 ·演示 ·指南 ·安装

企业网上银行登录

·注册 ·演示 ·指南 ·安装

网站会员登录

·注册 ·找回密码



全国银行客户端(整合版)

中国农业银行

AGRICULTURAL BANK OF CHINA

繁体中文 | ENGLISH

首页 农行风貌 投资者关系 个人服

热门栏目： 基金 | 生活e站 | 网上购物 | 充

用户登录

个人网上银行登录

· 注册指南 · 演示 · 安装

企业网上银行登录

· 注册指南 · 演示 · 安装

电子商务登录

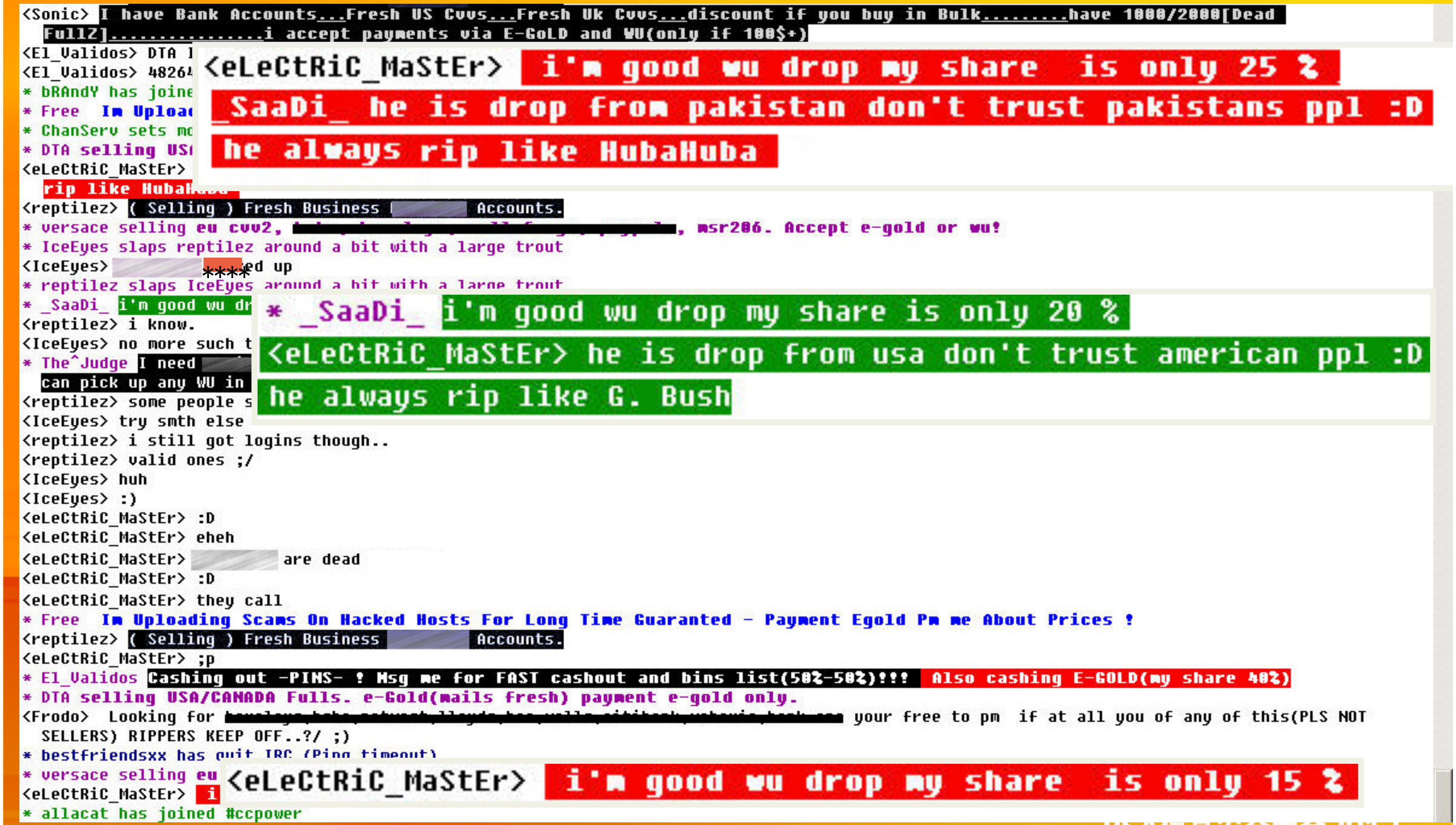
· 注册指南 · 演示 · 安装

e站专区

反欺诈应用程序服务

- 持续监控大型应用商店和检测欺诈应用程序
- 关闭 欺诈应用程序

聊天室：一个嘈杂的市场



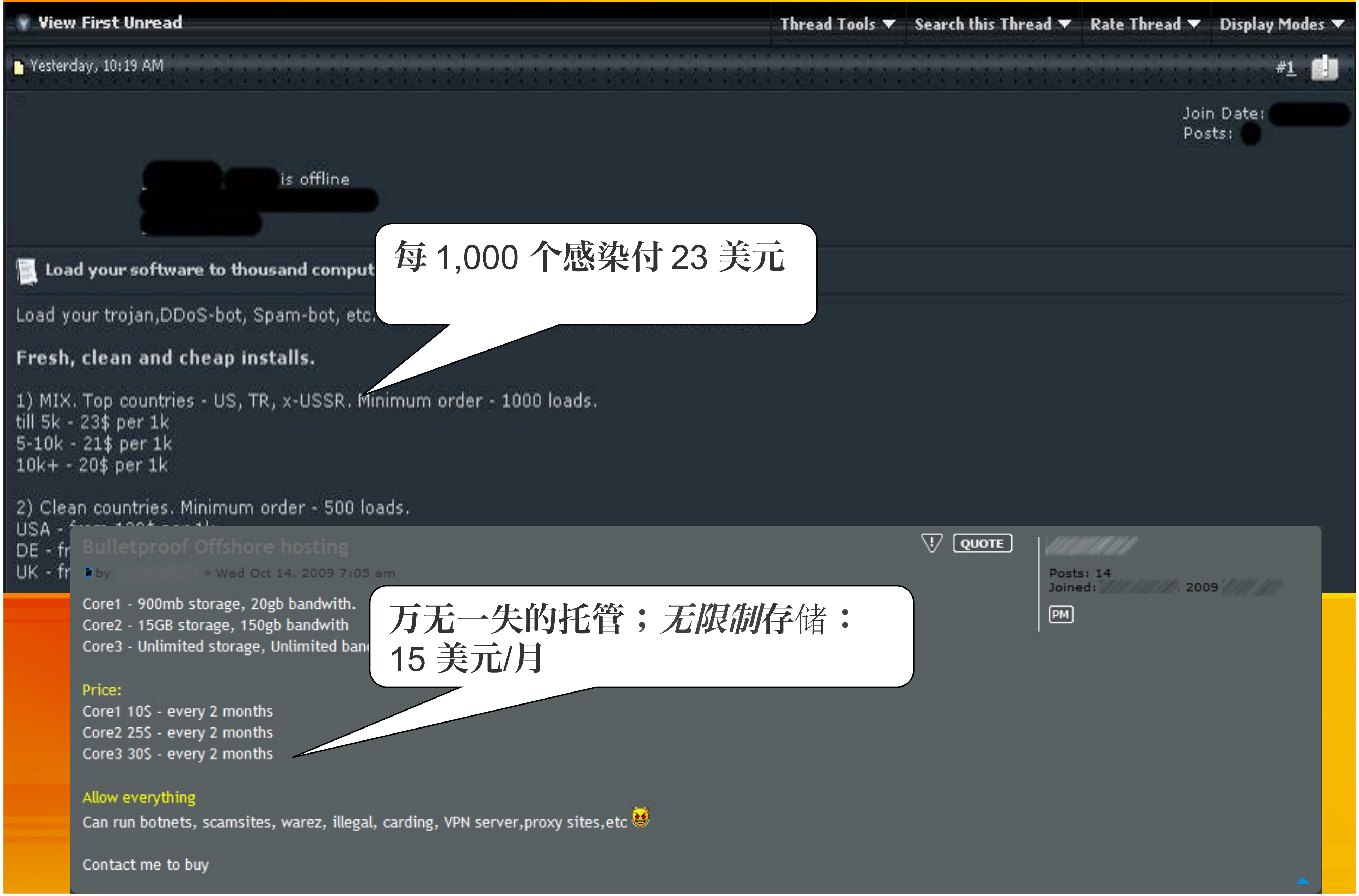
```
<Sonic> I have Bank Accounts...Fresh US Cvvs...Fresh Uk Cvvs...discount if you buy in Bulk.........have 1000/2000[Dead
  Fullz]................i accept payments via E-GoLD and WU(only if 100$+)
<El_Validos> DTA I
<El_Validos> 48264
* bRAndY has joine
* Free  Im Uploa
* ChanServ sets mo
* DTA selling USA
<eLeCtRiC_MaStEr>
  rip like HubaHuba
<reptilez> ( Selling ) Fresh Business [redacted] Accounts.
* versace selling eu cvv2, [redacted], msr206. Accept e-gold or wu!
* IceEyes slaps reptilez around a bit with a large trout
<IceEyes> [redacted] ****ed up
* reptilez slaps IceEyes around a bit with a large trout
* _SaaDi_ i'm good wu dr
<reptilez> i know.
<IceEyes> no more such t
* The^Judge I need [redacted]
  can pick up any WU in
<reptilez> some people s
<IceEyes> try smth else
<reptilez> i still got logins though..
<reptilez> valid ones ;/
<IceEyes> huh
<IceEyes> :)
<eLeCtRiC_MaStEr> :D
<eLeCtRiC_MaStEr> eheh
<eLeCtRiC_MaStEr> [redacted] are dead
<eLeCtRiC_MaStEr> :D
<eLeCtRiC_MaStEr> they call
* Free  Im Uploading Scams On Hacked Hosts For Long Time Guaranted - Payment Egold Pm me About Prices !
<reptilez> ( Selling ) Fresh Business [redacted] Accounts.
<eLeCtRiC_MaStEr> ;p
* El_Validos Cashing out -PINS- ! Msg me for FAST cashout and bins list(50%-50%)!!! Also cashing E-GOLD(my share 40%)
* DTA selling USA/CANADA Fulls. e-Gold(mails fresh) payment e-gold only.
<Frodo>  Looking for [redacted] your free to pm  if at all you of any of this(PLS NOT
  SELLERS) RIPPERS KEEP OFF..?/ ;)
* bestfriendsxx has quit IRC (Ping timeout)
* versace selling eu
<eLeCtRiC_MaStEr> i
* allacat has joined #ccpower
```

```
<eLeCtRiC_MaStEr> i'm good wu drop my share  is only 25 %
_SaaDi_ he is drop from pakistan don't trust pakistans ppl :D
he always rip like HubaHuba
```

```
* _SaaDi_ i'm good wu drop my share is only 20 %
<eLeCtRiC_MaStEr> he is drop from usa don't trust american ppl :D
he always rip like G. Bush
```

```
<eLeCtRiC_MaStEr> i'm good wu drop my share  is only 15 %
```

您也可以开始您的自己的业务…



Yesterday, 10:19 AM

Join Date: [redacted]
Posts: [redacted]

[redacted] is offline
[redacted]

每 1,000 个感染付 23 美元

Load your software to thousand comput

Load your trojan,DDoS-bot, Spam-bot, etc.

Fresh, clean and cheap installs.

1) MIX. Top countries - US, TR, x-USSR. Minimum order - 1000 loads.
till 5k - 23$ per 1k
5-10k - 21$ per 1k
10k+ - 20$ per 1k

2) Clean countries. Minimum order - 500 loads.
USA -
DE - fr
UK - fr

Bulletproof Offshore hosting

by [redacted] » Wed Oct 14, 2009 7:05 am

[redacted]
Posts: 14
Joined: [redacted]. 2009 [redacted]

Core1 - 900mb storage, 20gb bandwith.
Core2 - 15GB storage, 150gb bandwith
Core3 - Unlimited storage, Unlimited ban

万无一失的托管；*无限制存*储：
15 美元/月

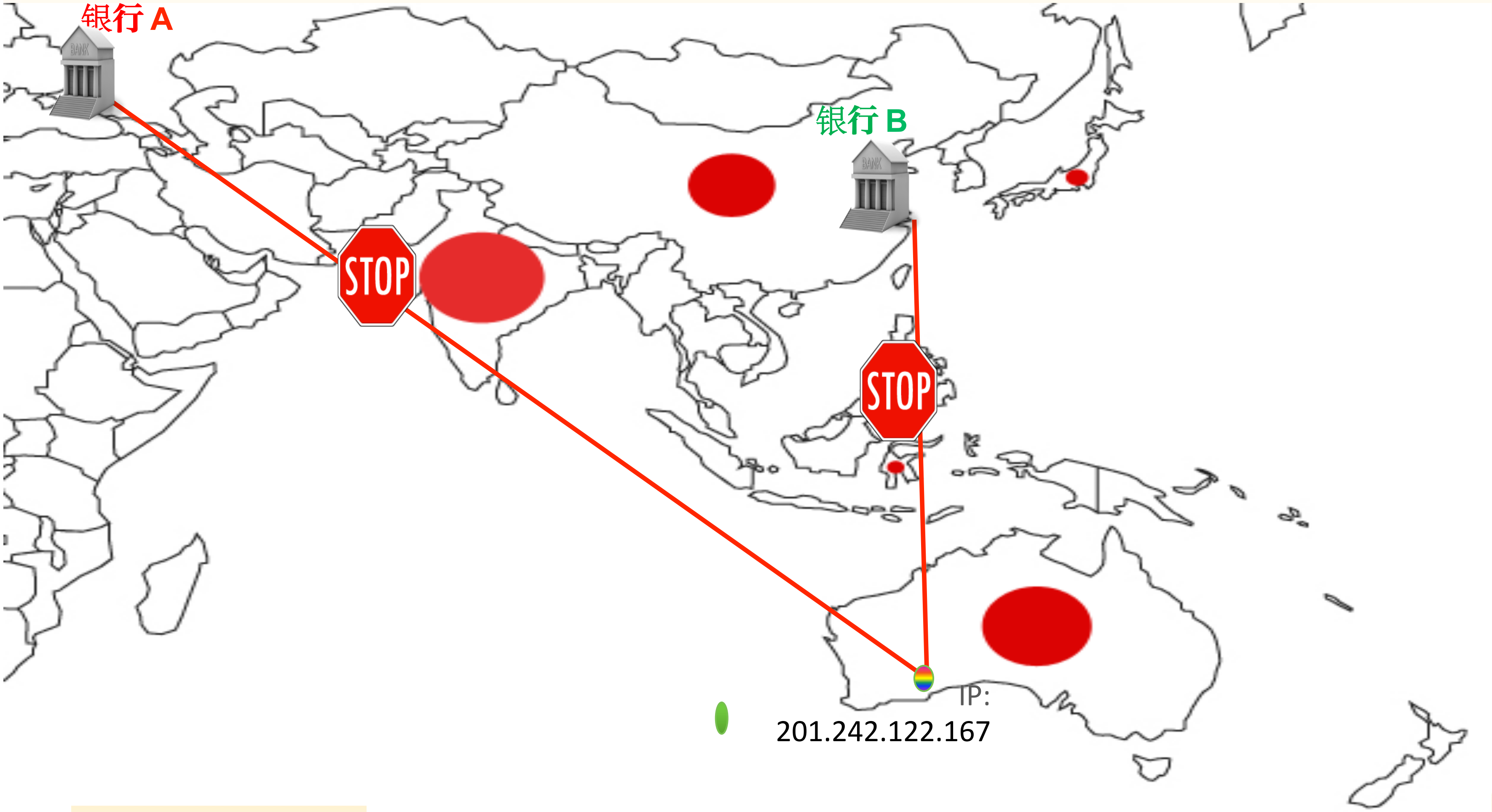
Price:
Core1 10$ - every 2 months
Core2 25$ - every 2 months
Core3 30$ - every 2 months

Allow everything
Can run botnets, scamsites, warez, illegal, carding, VPN server,proxy sites,etc 😈

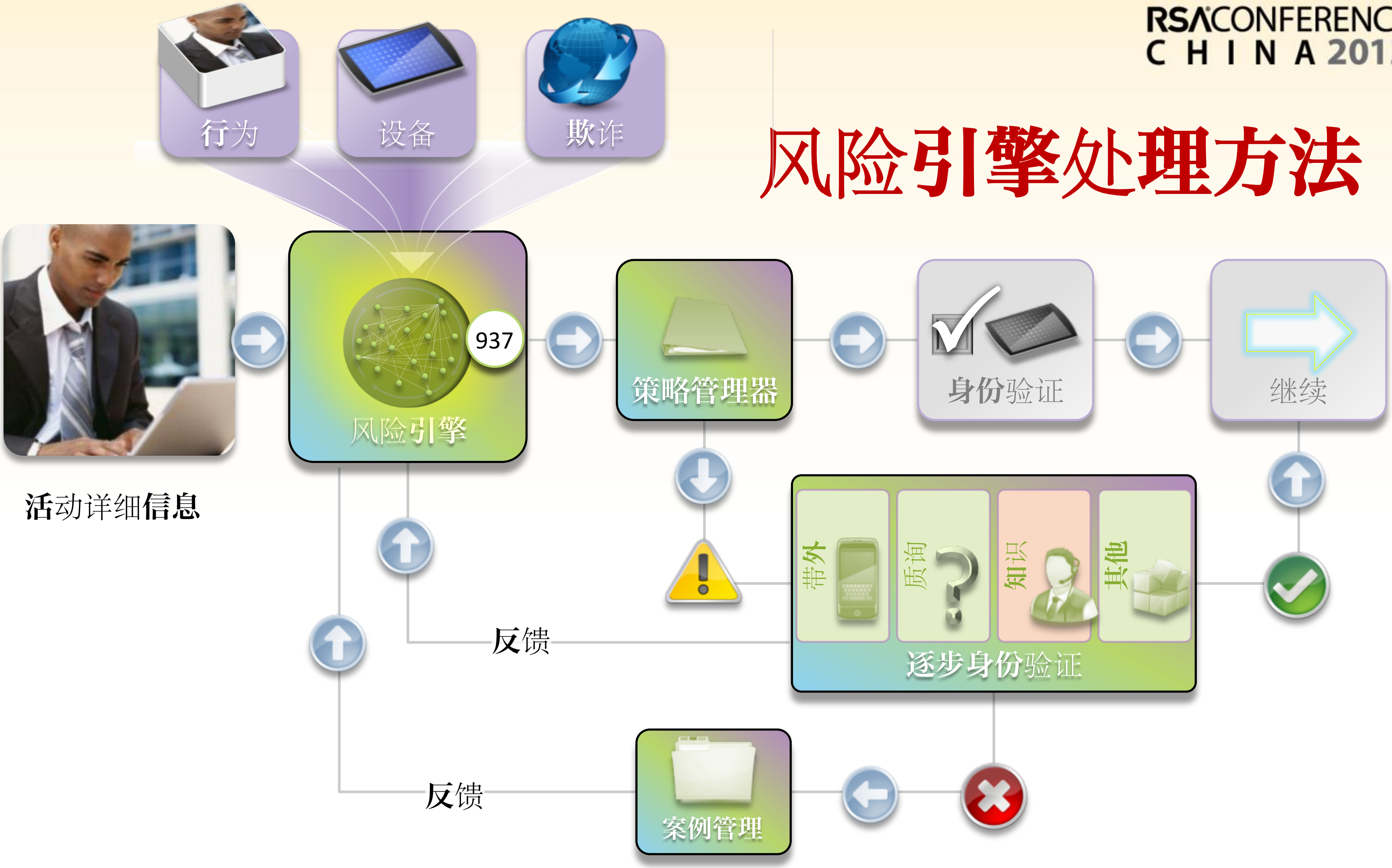
Contact me to buy

多防线防御：
大数据与分析

信息共享的重要性



风险引擎处理方法


行为
设备
欺诈
活动详细信息
937
风险引擎
策略管理器
身份验证
继续
带外
质询
知识
其他
逐步身份验证
反馈
反馈
案例管理

基于风险的分析和身份验证

$$Score = \sum \max(abs(1000 * \log_{10}\left(\frac{F(bucket) * \frac{\sum_{Buckets} F(bucket)}{\sum_{Buckets} G(bucket)} + m}{G(bucket) + m}\right)))$$

Network parameters

eFraudNetwork Mule accounts

Device ID IP geo location

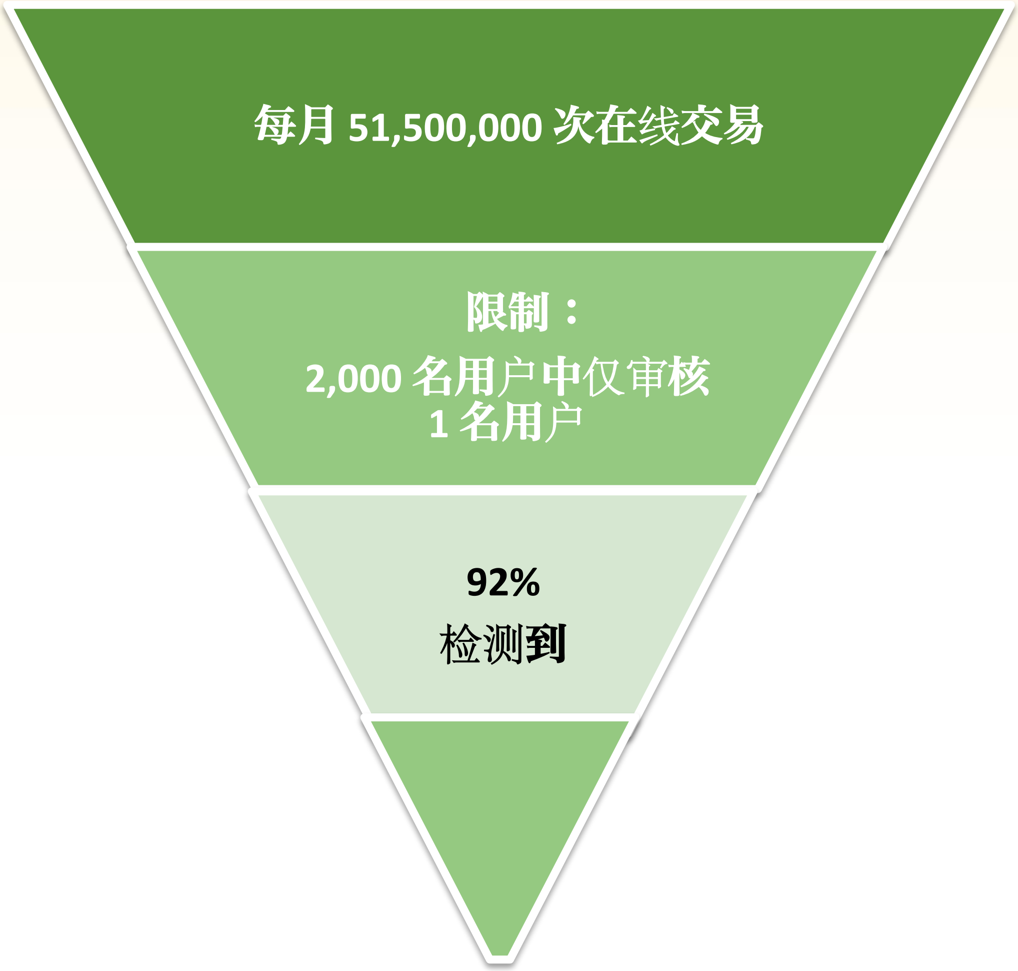
Behavioral Anomaly Payment amount Velocity checks

Back Coloring Ground speed Trojan Credentials

Fraud intelligence Payee reputation

HTML5 data Mobile GPS Location

一家英国大型银行的结果



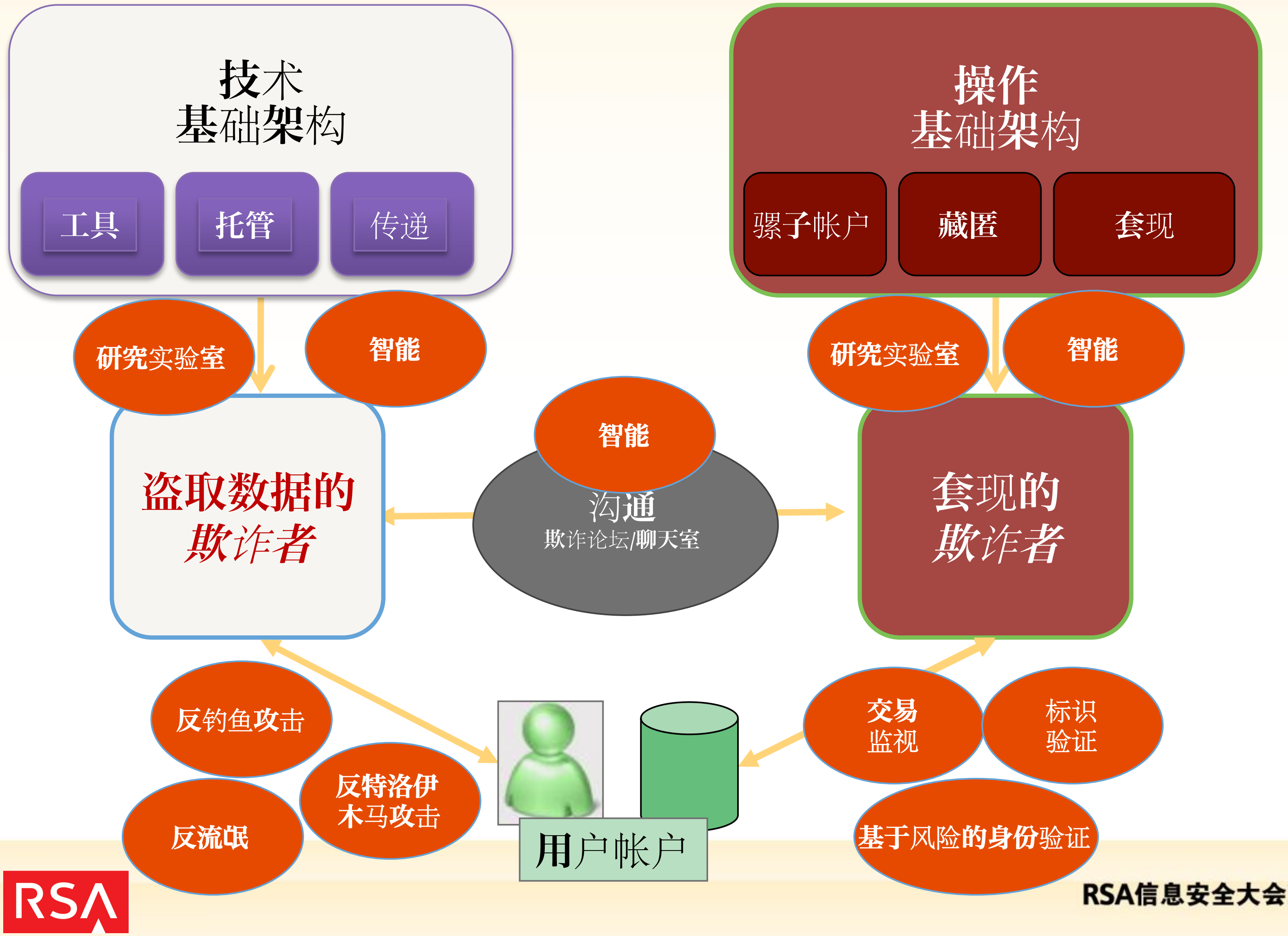
每月 51,500,000 次在线交易

限制：

2,000 名用户中仅审核
1 名用户

92%
检测到

反击



技术
基础架构

工具
托管
传递

操作
基础架构

骡子帐户
藏匿
套现

研究实验室
智能

研究实验室
智能

盗取数据的
欺诈者

智能
沟通
欺诈论坛/聊天室

套现的
欺诈者

反钓鱼攻击
反特洛伊
木马攻击
反流氓

用户帐户

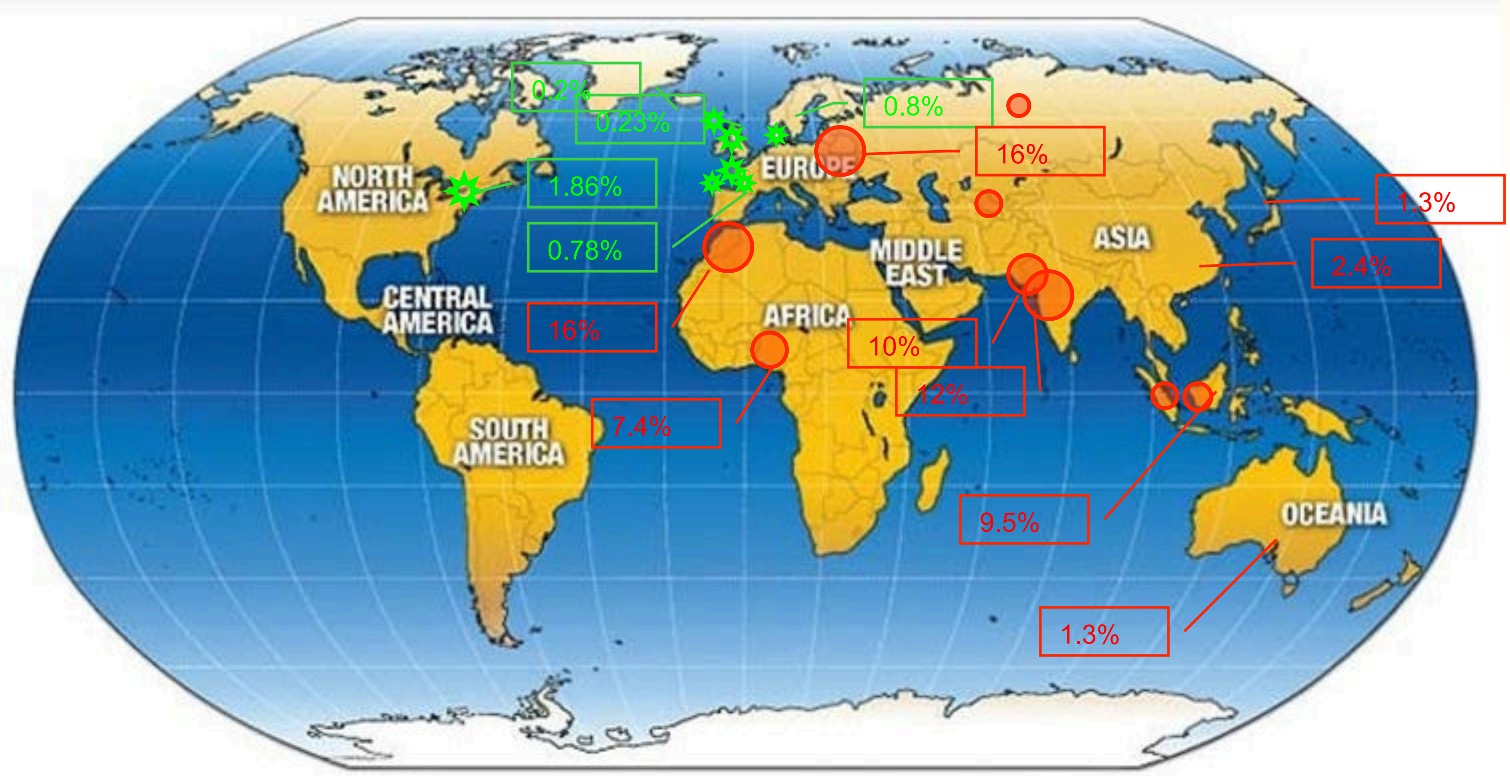
交易
监视

标识
验证

基于风险的身份验证

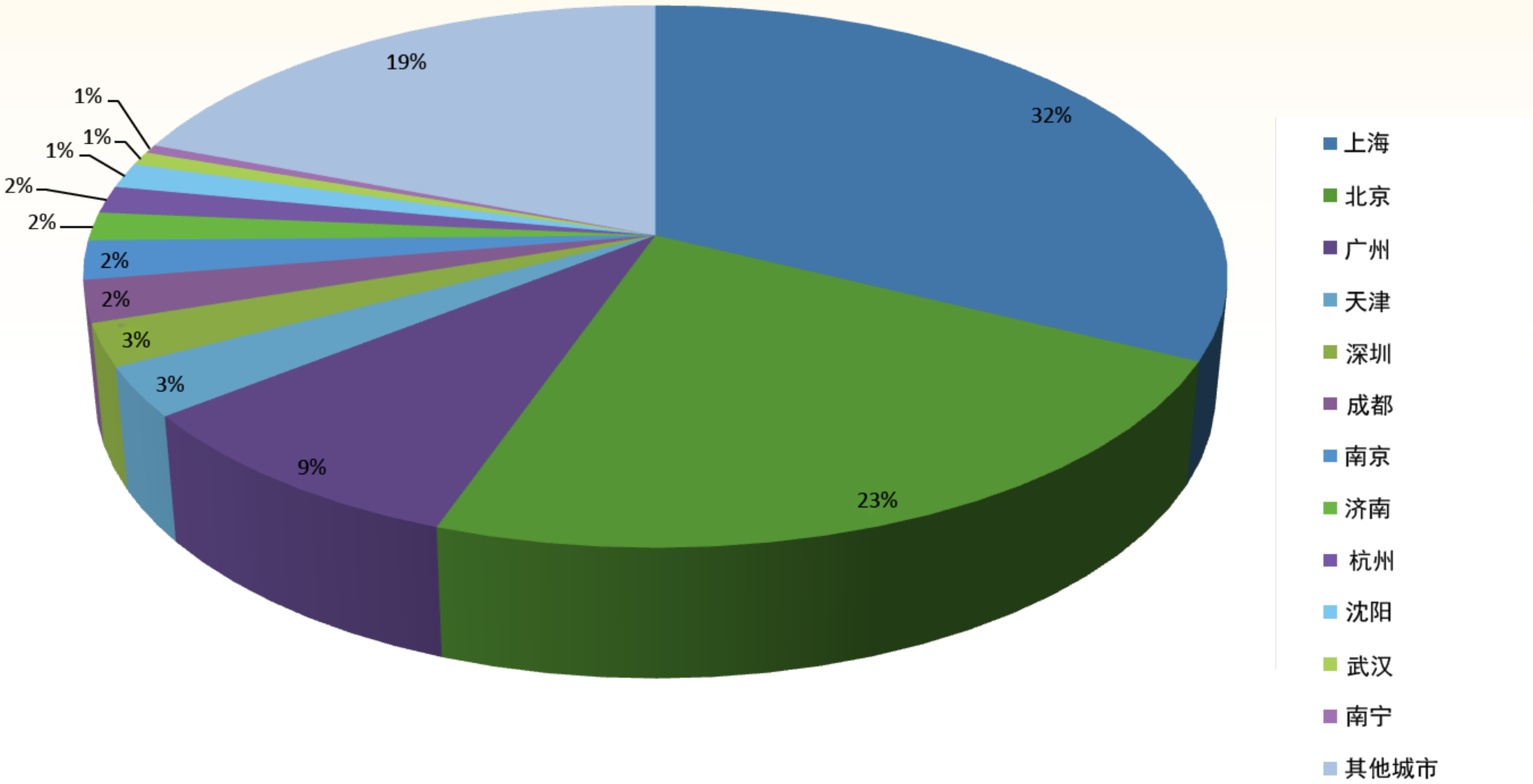
中国的具体趋势

全球欺诈－以总成交比率

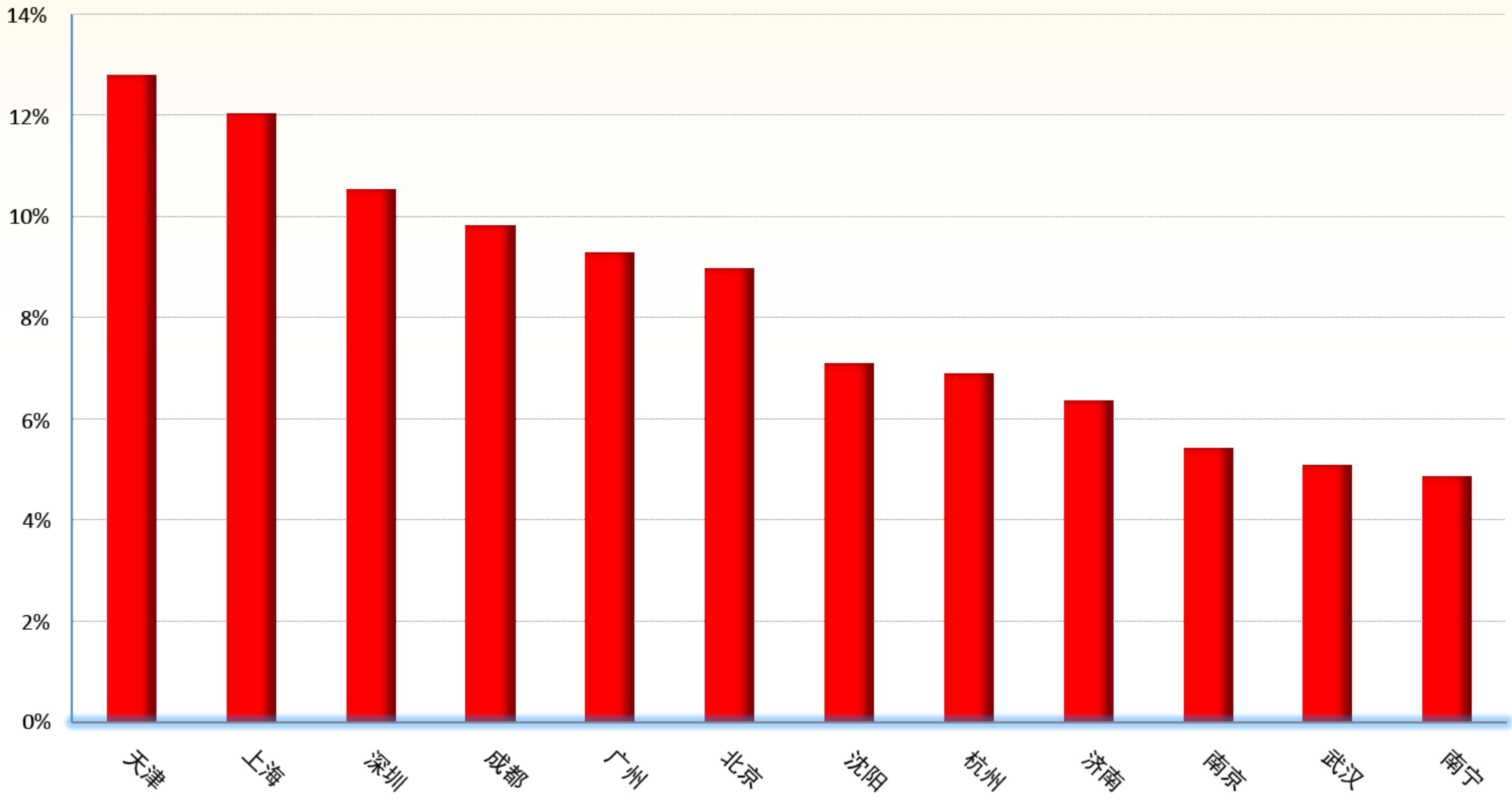

NORTH AMERICA
CENTRAL AMERICA
SOUTH AMERICA
EUROPE
MIDDLE EAST
AFRICA
ASIA
OCEANIA
0.2%
0.23%
0.8%
16%
1.86%
1.3%
0.78%
2.4%
16%
10%
12%
7.4%
9.5%
1.3%

中国各城市发生欺诈的总体情况

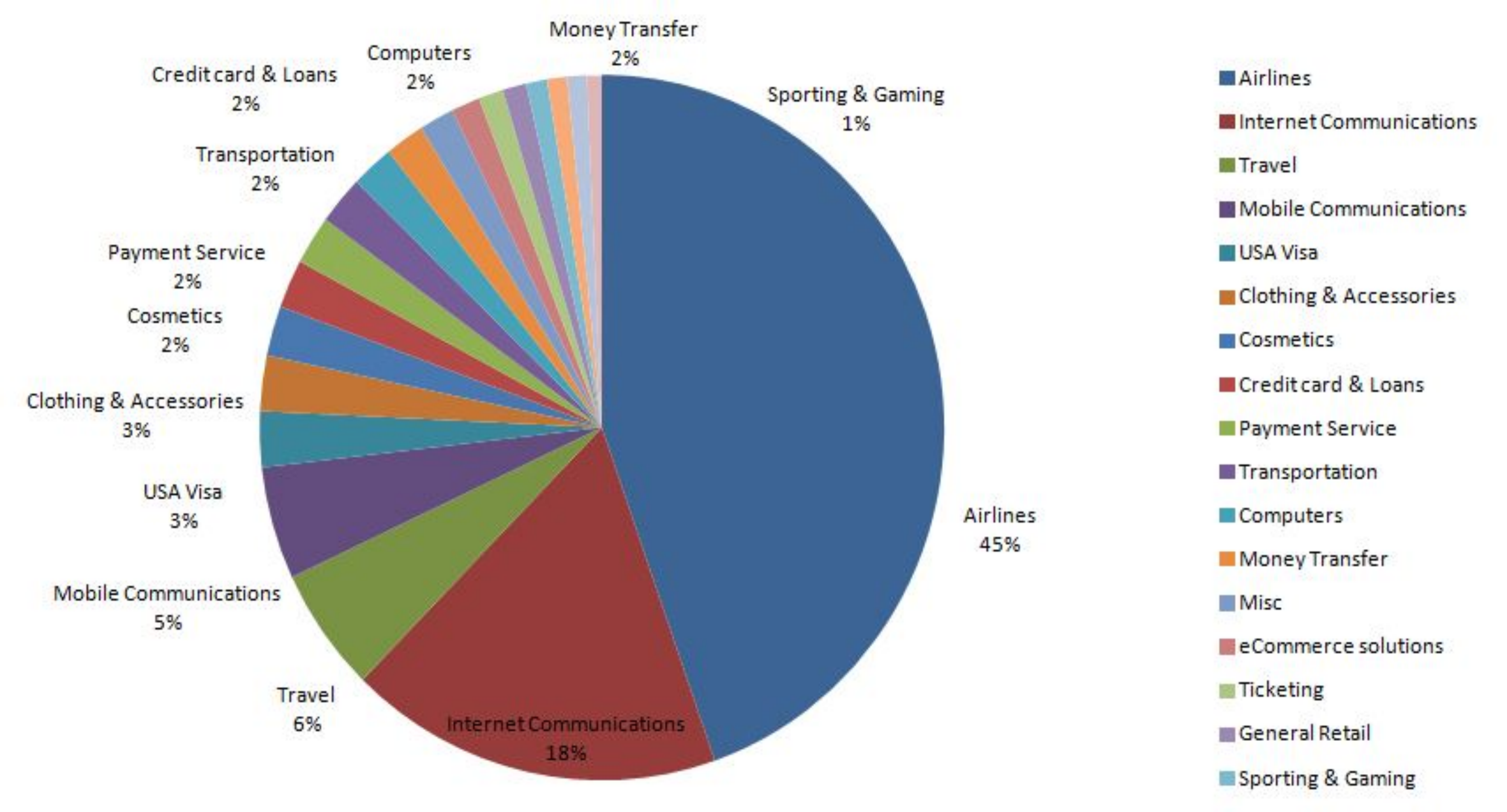
RSA CONFERENCE
CHINA 2012



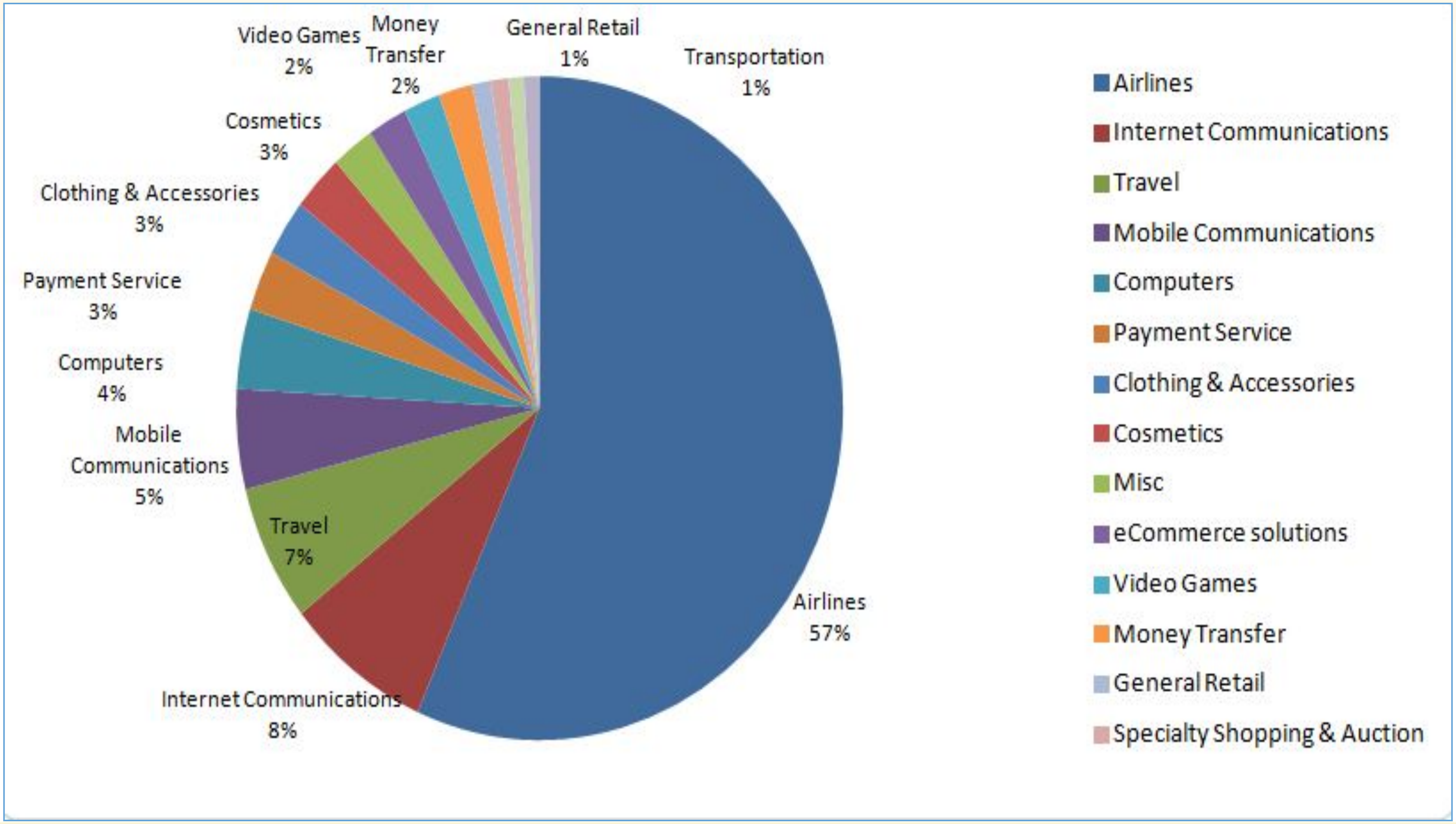
欺诈发生率最高的中国城市



China – Online Shopping by Category



How would a Online Fraudster make a living in China?



谢谢大家！