

**RSA[®]CONFERENCE
C H I N A 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**



CyberCrime Trends - Focus on Asia

Michal Blumenstyk-Braverman
RSA – General Manager of Global Solutions



Session ID:

Session Classification:

RSA CONFERENCE
C H I N A 2012
RSA信息安全大会2012

The Industry fights back

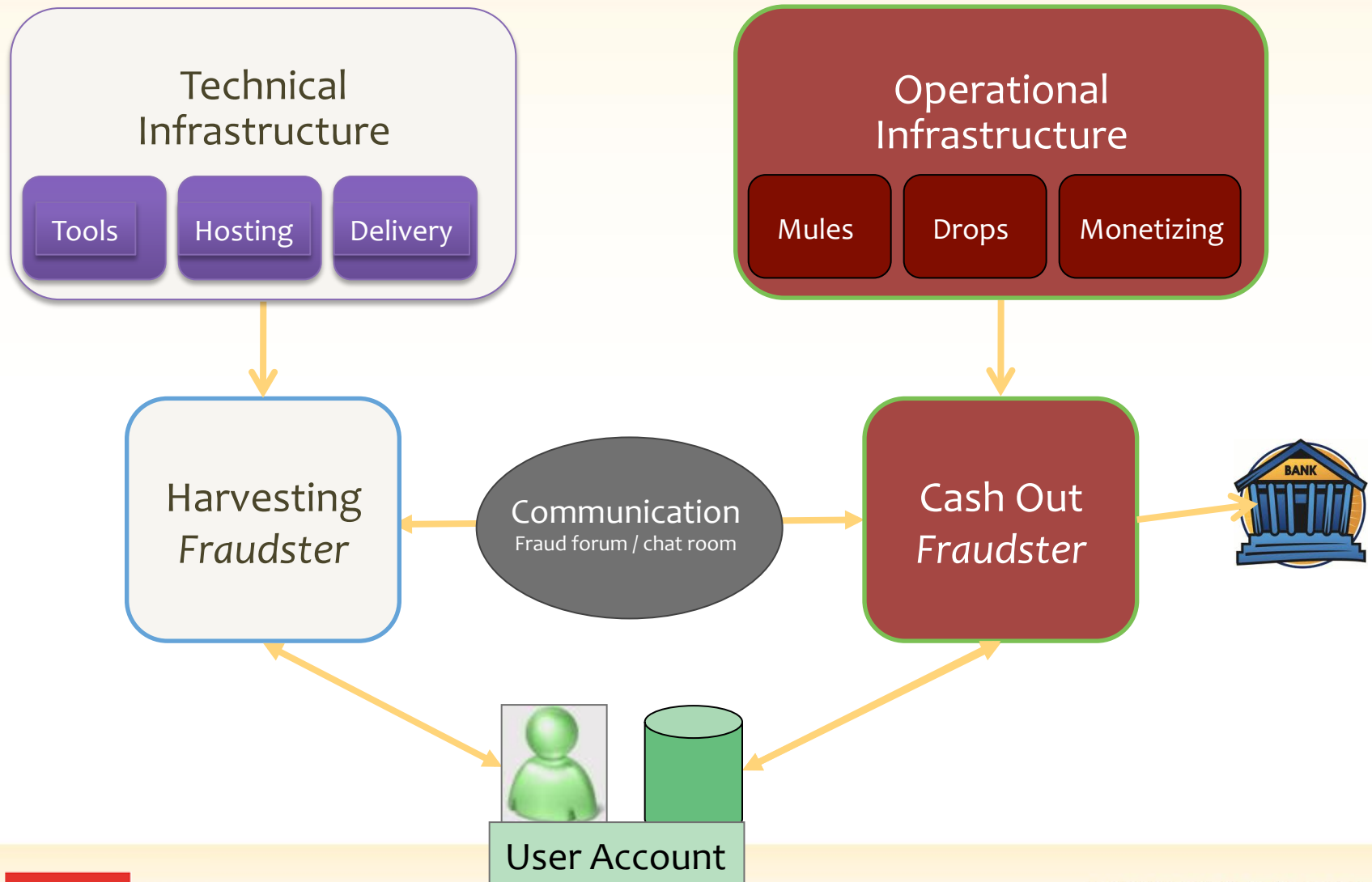
RSA CONFERENCE
C H I N A 2012

- Scale of Operation:
 - **300,000,000** users protected by our **eFraudNetwork**
 - **700,000** Phishing attacks stopped by the Anti Fraud Command Center
 - More **10,000** Institutes protected



CyberCrime/ Fraud Supply Chain

RSA CONFERENCE
C H I N A 2012



Multi-Line of Defense: Handling External Threats

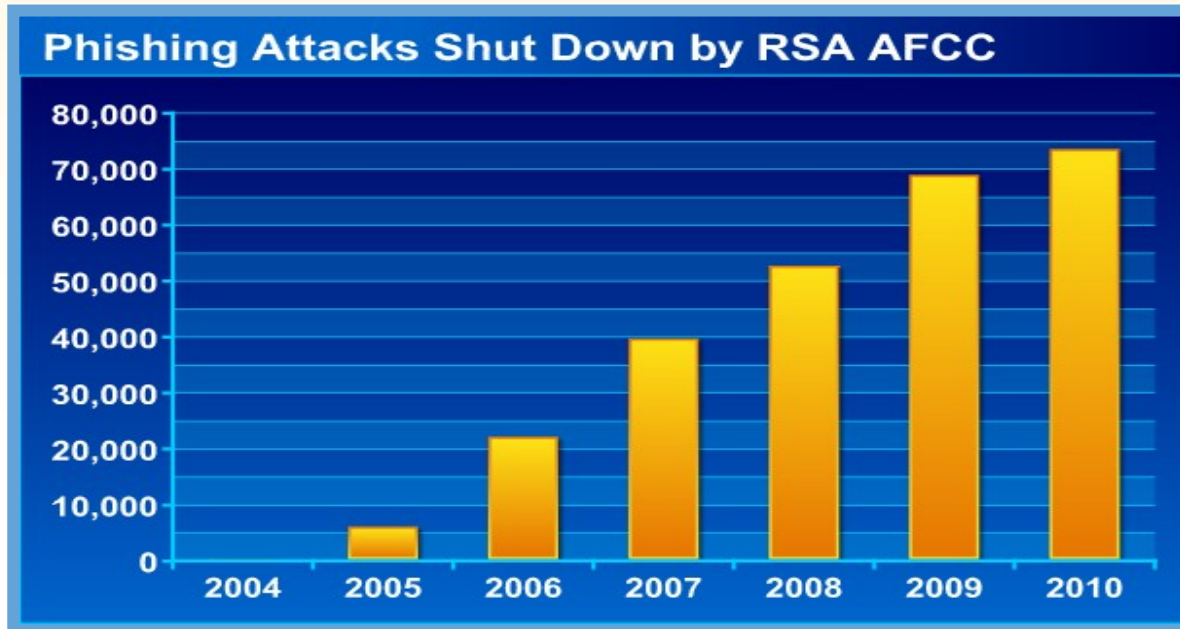


Session ID:

Session Classification:

RSA CONFERENCE
C H I N A 2012
RSA信息安全大会2012

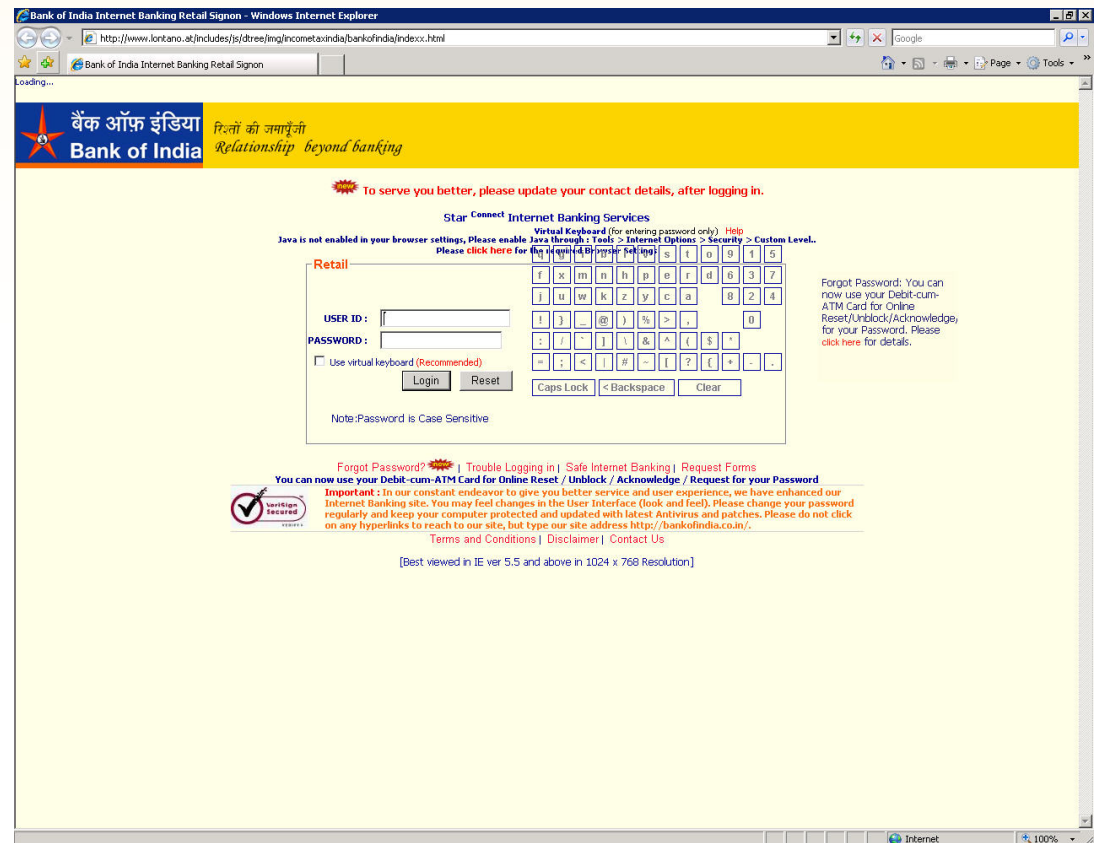
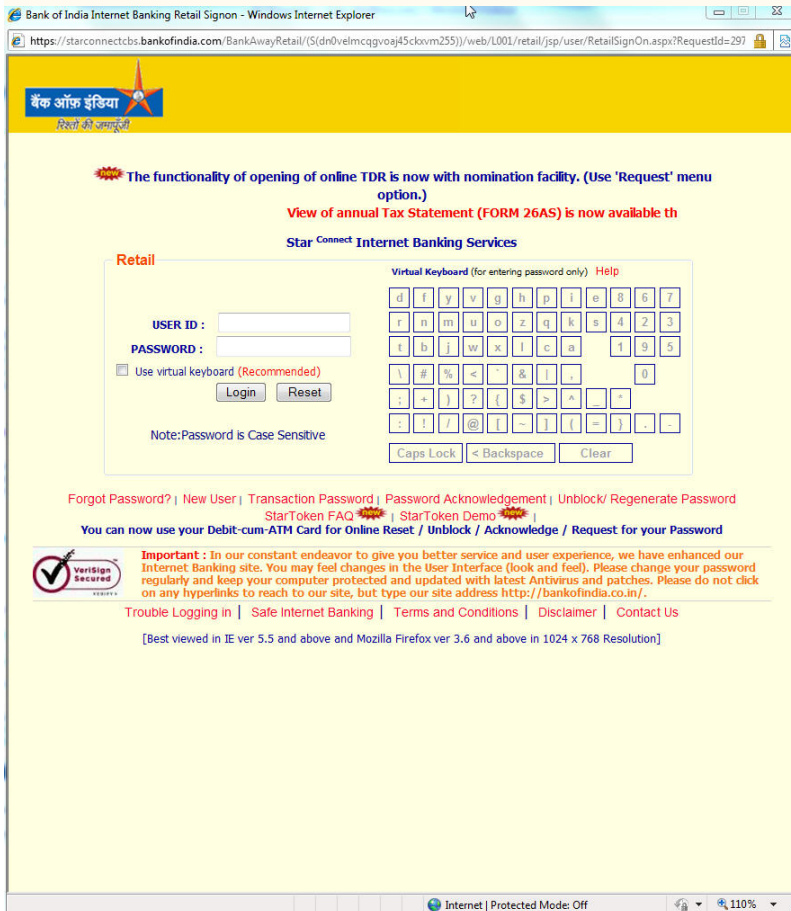
24/7 Anti Fraud Command Center



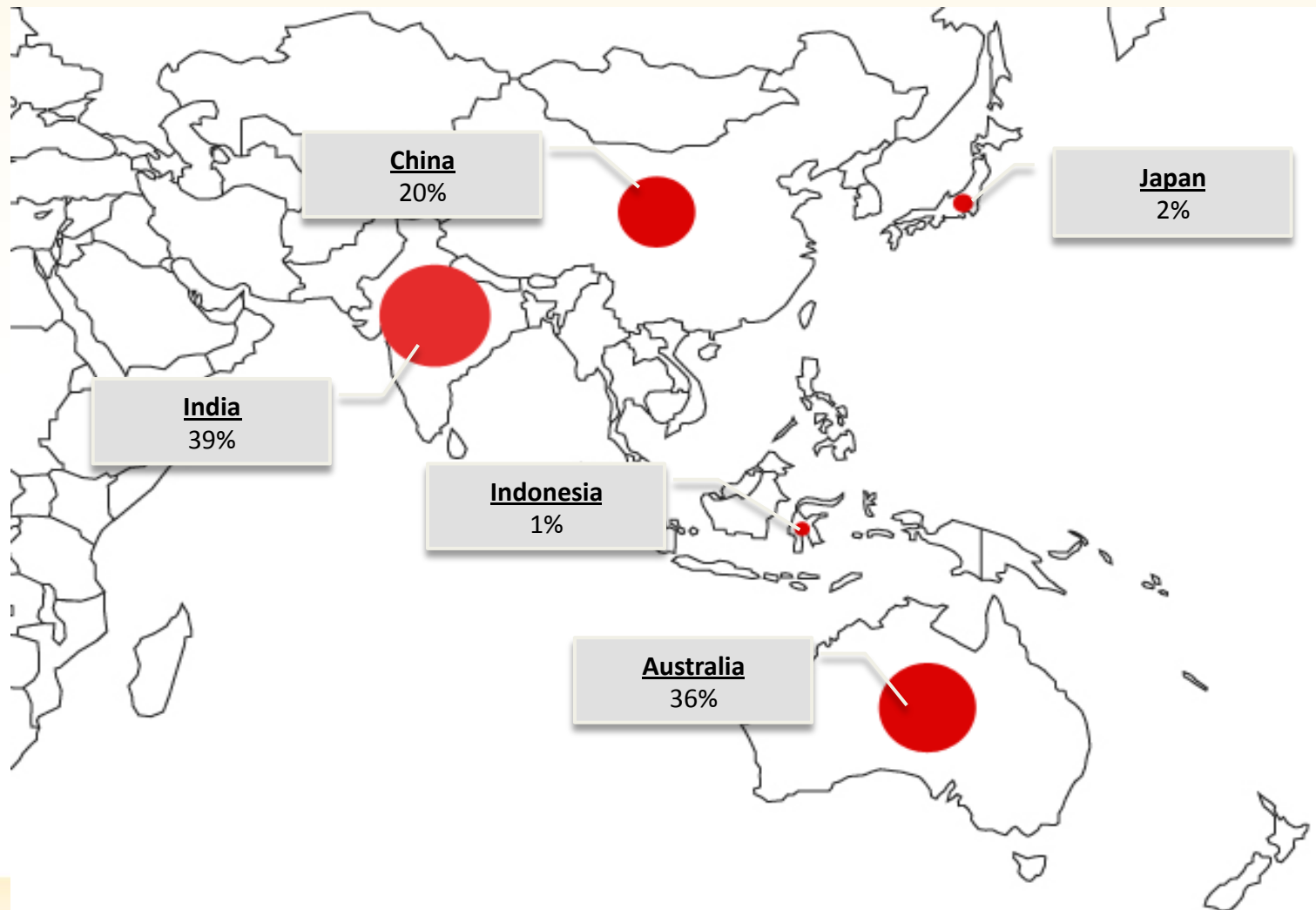
- 35% hosted outside the U.S.; 70% hosted on hijacked servers
- Targeting various sectors: finance, telecom, medical, insurance and more...

Phishing attacks are better than ever

Which one is the real page?



APJ Phishing Heat Map (2012)



Trojans

RSA CONFERENCE
C H I N A 2012

The image shows a screenshot of a Windows Internet Explorer browser displaying the InternetBank website. The browser's address bar shows the URL <https://www.internetbank.com>. The website's navigation menu includes Home, My Account, Personal, Mortgage, Investments, and Business. A prominent green banner at the top of the page reads "Business".

On the left side of the page, there are several menu sections:

- Privacy & Security**: Includes links for Phishing Alert, Identity Theft, ATM Safety, InternetBank Security, and Privacy Policy.
- Open an Account**: Features a "Select Account" dropdown menu.
- Site Tools & Forms**: Features a "Select Form" dropdown menu.
- About Us**: Includes links for Welcome to InternetBank, ATM Locator, Branch Locator, Careers, and Charitable Foundation.
- Learn More**: Includes links for Go ID Authentication, Quicken Upgrade, Check 21, MasterCard SecureCode, and Calculator.

The main content area is divided into several columns:

- Customer Center**: Includes a "Need Help?" section with a link to "Get all the answers you need about InternetBank." and an "Advice & Planning" section with a link to "Planning for your growth" and a description of long-term solutions for goals such as college tuition, second homes and retirement.
- Small Business**: Includes a "Cash flow aid" section with a link to "Financial solutions for companies and not-for-profits with annual revenues up to \$10 million." and a "Commercial Banking" section with a link to "Products and services" and a description of financial services for businesses with annual revenues from \$10 million.
- Mortgage Lending**: Includes a "Disclosure Act" section with a link to "We are committed to fair lending & outreach to its communities, and information about HMDA."

On the right side of the page, there is a "Login" section with the following fields and options:

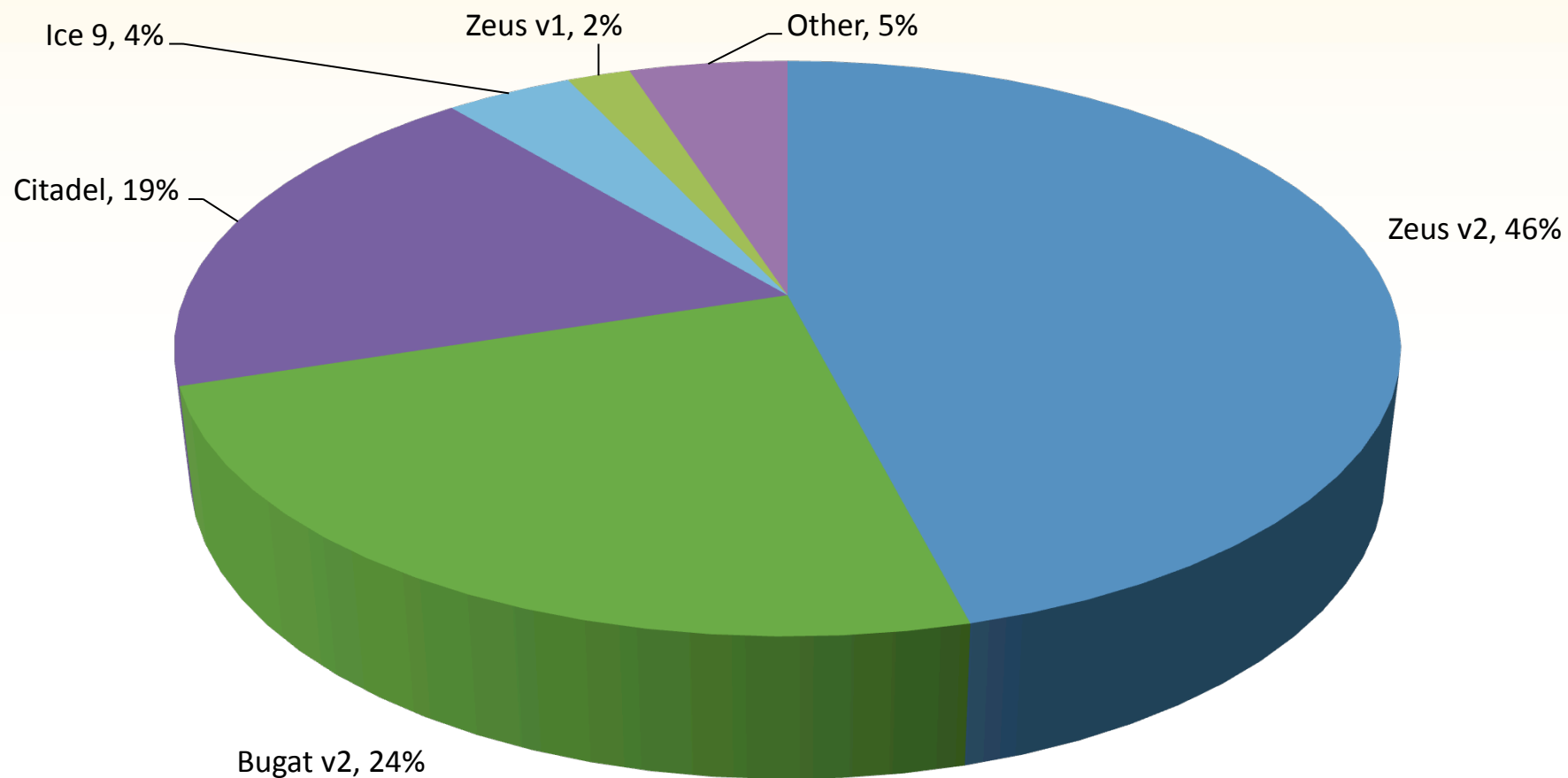
- ATM Number:** Input field
- ATM Pin:** Input field
- User Name:** Input field
- Password:** Input field
- login** button
- [Don't Have Your Go ID?](#)
- [Lost or Broken Go ID?](#)

Below the login section, there is a small image of a man sitting at a desk with a laptop, and a partially visible text snippet: "panies and not-venues up to \$10".

The browser's taskbar at the bottom shows the "Internet" icon and the system tray with the time "100".

Most Active Trojan Families (Q2'12)

RSA CONFERENCE
CHINA 2012



Trojan Sudoku Attacking Japanese Bank

RSA CONFERENCE
C H I N A 2012

- This Trojan aimed at banking customers
- Requested User ID, Password and a Transaction Authentication Code

The screenshot shows a web browser window titled 'Reg' displaying a banking login form. The form includes fields for '契約者番号' (Contractor Number) and '第一暗証' (First PIN). A red arrow points to the '契約者番号' field with the text '契約者番号 → 暗証カード裏面の10桁の数字' (Contractor Number → 10-digit number on the back of the PIN card). A small image of a PIN card is shown with 'サンプル' (Sample) written on it. Below the PIN field, there is a section for '確認番号・取引パスワード入力' (Confirmation Number/Transaction Password Input). It includes a table for inputting a 4-digit transaction authentication code (TAC) based on a 4x5 grid of numbers. The table has columns labeled 'ア', 'イ', 'ウ', 'エ', 'オ' and rows numbered 1 to 4. An example of the numbers to be entered is provided in a second table. Below the TAC table is a field for '取引パスワード' (Transaction Password) with a note '(半角英数字4~12桁)'. At the bottom, there is a '送信' (Send) button and the text '以上の内容でよろしければ、送信してください。' (If you are satisfied with the above content, please click Send).

契約者番号の入力

契約者番号 -

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					

	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、 してください。

The eDead Trojan attacks Banks in Korea and Japan

- This Trojan aimed at banking customers in Korea and Japan
- Recorded search words entered on the banks' websites



In China: 'Warp' – intercepting traffic and spreading via networks

New 'Warp' Trojan Poses As A Network Router

NCE
012

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.


Attacks on Enterprises

RSA CONFERENCE
C H I N A 2012



June 2nd, 2012, 08:00 GMT · By [Eduard Kovacs](#)

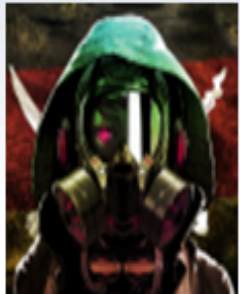
ProjectDragonFly: 100,000 Accounts Leaked from Chinese Sites

SHARE:  +1  2

 Like  Send

 Tweet

Adjust text size:  



 ENLARGE

After taking a short break, Team GhostShell hackers return with an operation called *ProjectDragonFly*, a 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 quite a bit about its constitution, both online and irl. I always knew that it's still very much a communist country, that makes a habit of silencing it's people whenever they disagree with their government, locking them up or worse," DeadMellox, the leader of the crew, wrote.

The [statement](#) published by the hacker cites a number of sources which highlight the wrongdoings of the Chinese government.

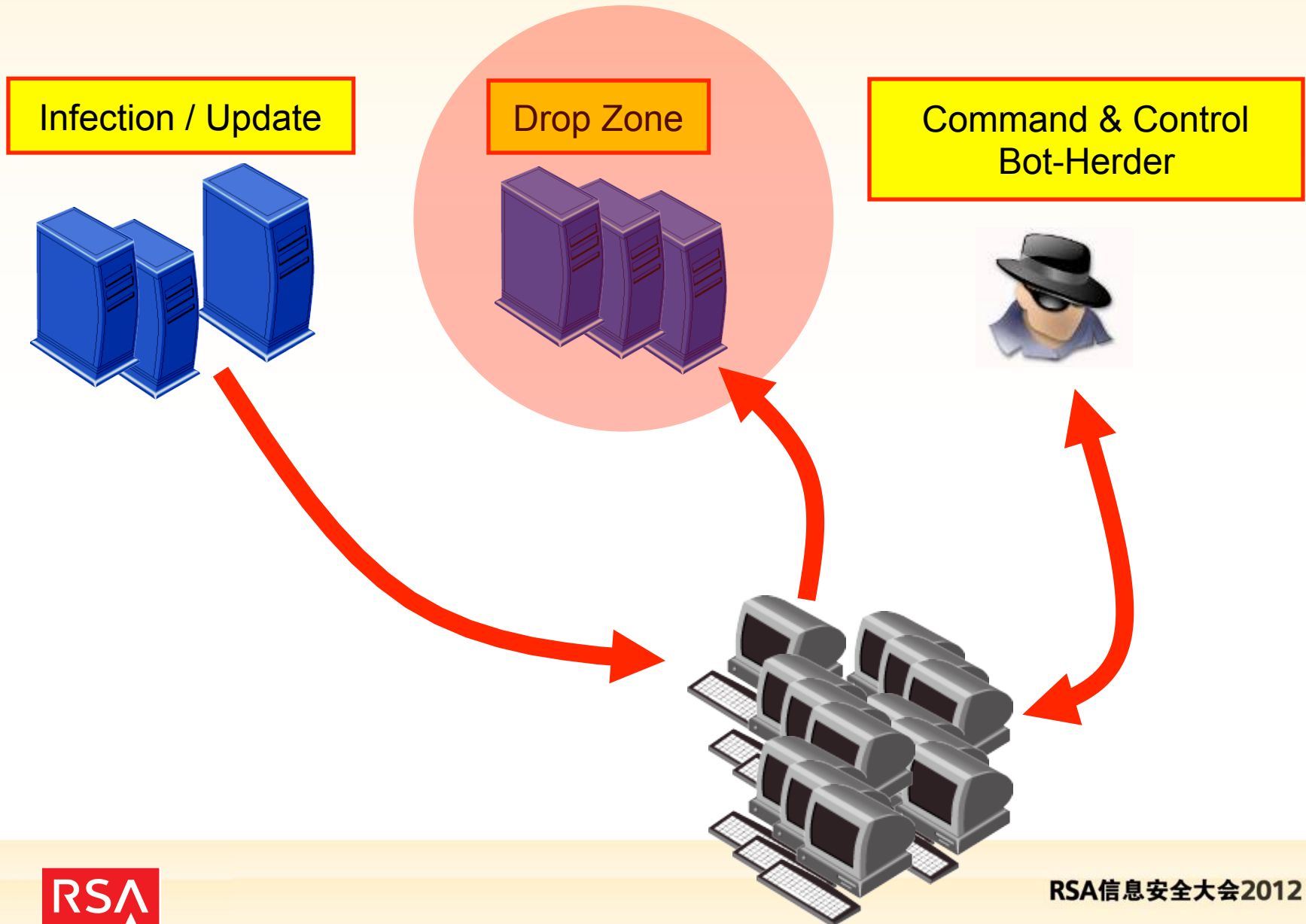
and used the hacked KT data, which included names, resident registration numbers and phone numbers.

RSA

2

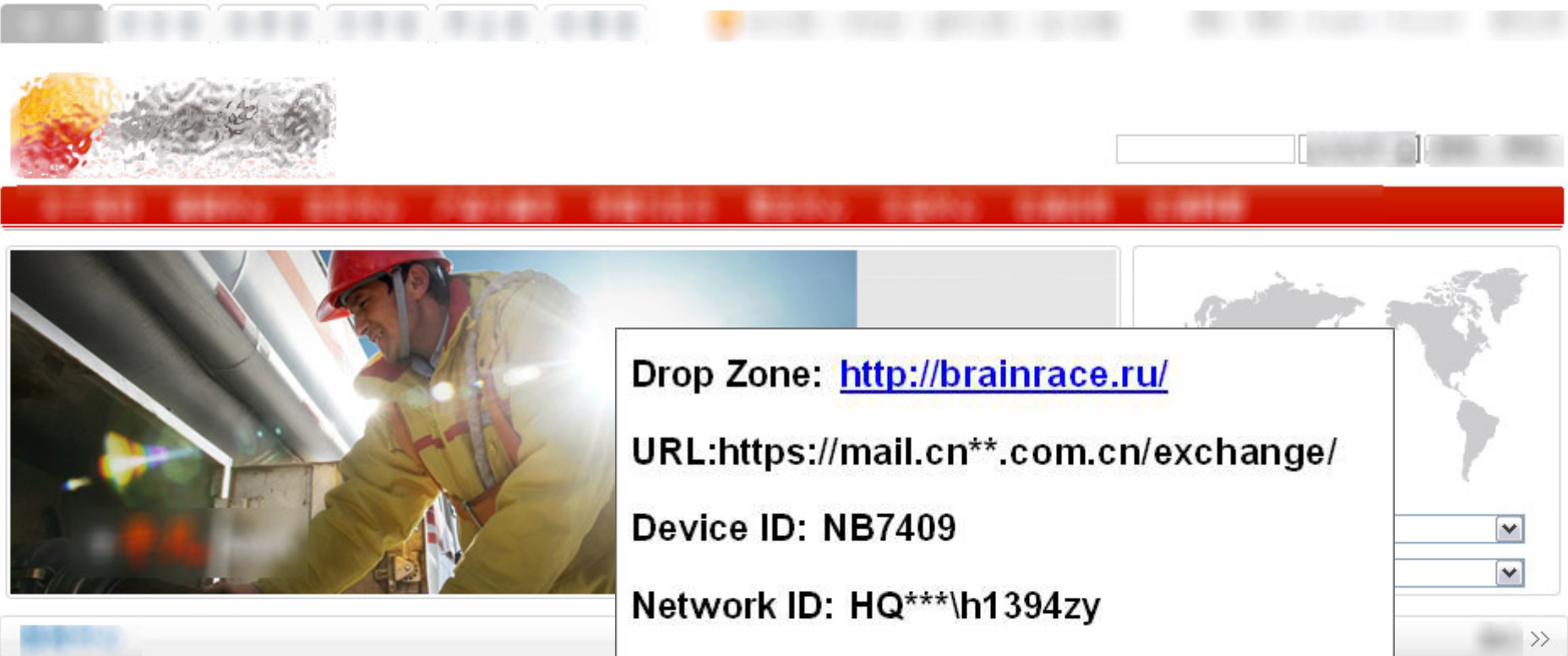
Trojan Infrastructure

RSA CONFERENCE
C H I N A 2012



Example : China Oil Giant

RSA CONFERENCE
C H I N A 2012



Drop Zone: <http://brainrace.ru/>
URL: https://mail.cn**.com.cn/exchange/
Device ID: NB7409
Network ID: HQ***\h1394zy
username=h1394zy
password=

Rogue application - Samples

RSA CONFERENCE
C H I N A 2012



Anti Rogue App Service

RSA CONFERENCE
C H I N A 2012

- Continuous monitoring of major app stores and detection of rogue apps
- Shutdown of rogue apps



Chat Rooms: A Noisy Marketplace

```
<Sonic> I have Bank Accounts...Fresh US Cvv2...Fresh Uk Cvv2...discount if you buy in Bulk.....have 1000/2000[Dead FullZ].....i accept payments via E-GOLD and WU(only if 100$+)
```

<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

rip like HubaHuba

```
<reptilez> ( Selling ) Fresh Business Accounts.
* versace selling eu cvv2, msr206. Accept e-gold or wu!
* IceEyes slaps reptilez around a bit with a large trout
<IceEyes> ***** up
* reptilez slaps IceEyes around a bit with a large trout
* _Saadi_ i'm good wu drop my share is only 20 %
<reptilez> i know.
<IceEyes> no more such t
* The^Judge I need
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> are dead
<eLeCtRiC_MaStEr> :D
<eLeCtRiC_MaStEr> they call
* Free Im Uploading Scams On Hacked Hosts For Long Time Guaranteed - Payment Egold Pm me About Prices !
<reptilez> ( Selling ) Fresh Business Accounts.
<eLeCtRiC_MaStEr> ;p
* El_Validos Cashing out -PINS- ! Msg me for FAST cashout and bins list(502-502)!!! Also cashing E-GOLD(my share 40%)
* DTA selling USA/CANADA Fulls. e-Gold(mails fresh) payment e-gold only.
<Frodo> Looking for 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'm good wu drop my share is only 15 %
* allacat has joined #ccpower
```

You too can start your own business...

View First Unread Thread Tools Search this Thread Rate Thread Display Modes

Yesterday, 10:19 AM #1

Join Date: [redacted]
Posts: [redacted]

[redacted] is offline

Load your software to thousand computers \$23 per 1,000 infections

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 - [redacted]
DE - fr
UK - fr

Bulletproof Offshore hosting

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

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

Posts: 14
Joined: [redacted] 2009

QUOTE

PM

Multi-Line of Defense: Big data and analytics



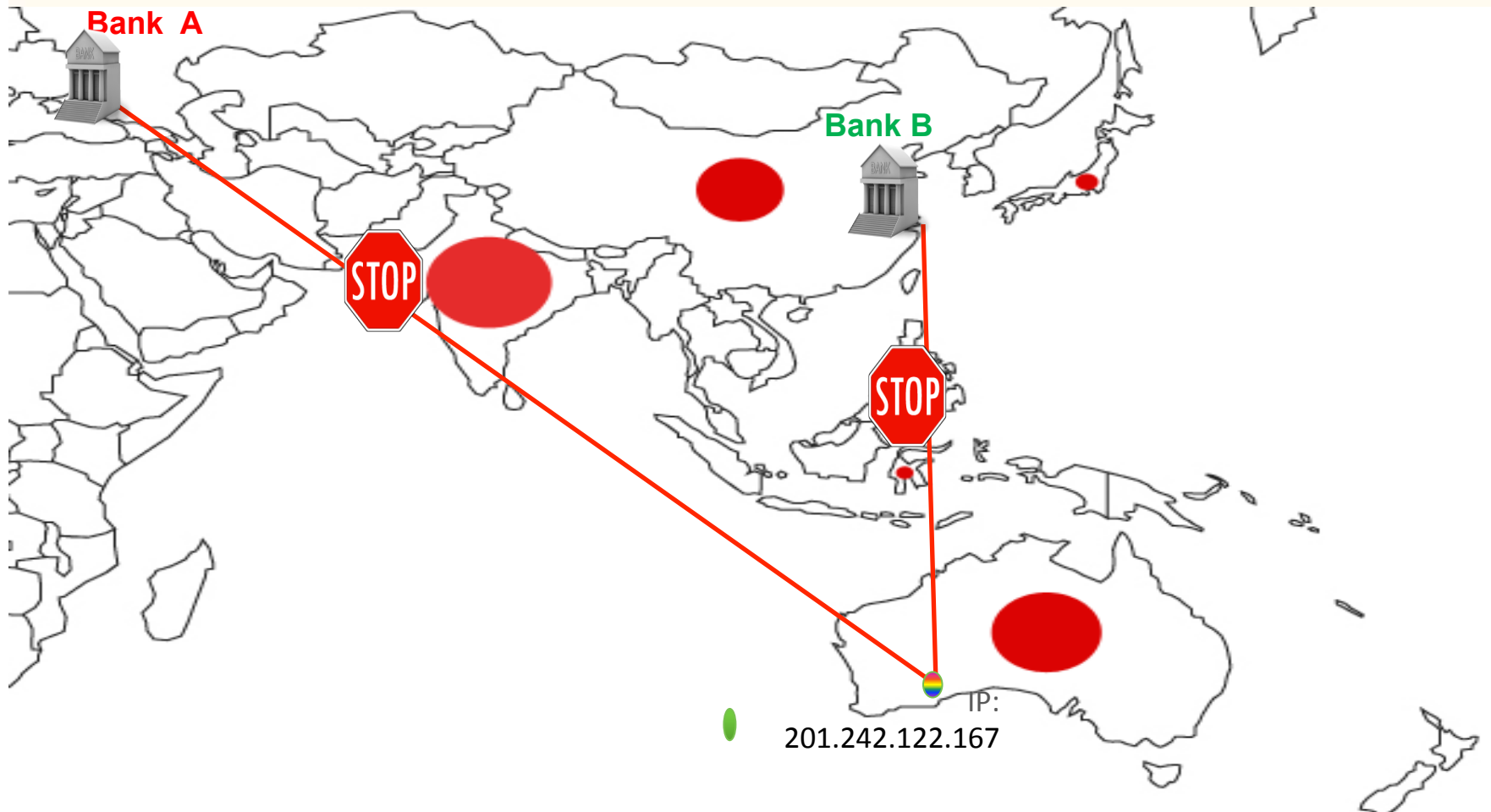
Session ID:

Session Classification:

RSACONFERENCE
C H I N A 2012
RSA信息安全大会2012

The Importance of Information Sharing

RSA CONFERENCE
C H I N A 2012



The Risk Engine Approach



Risk-Based Analytics and Authentication

RSA CONFERENCE
C H I N A 2012

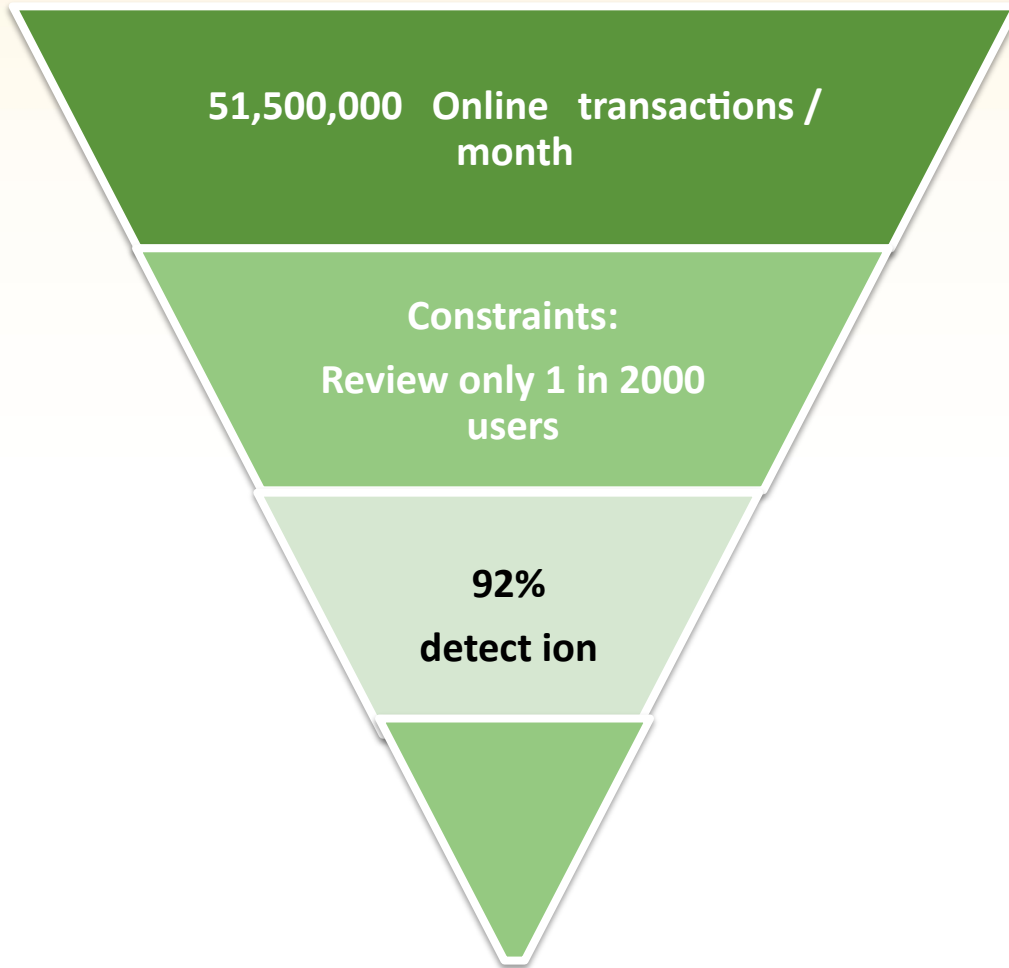


$$Score = \sum \max(abs(1000 * \log_{10} \left(\frac{F(bucket) * \frac{\sum Buckets}{\sum Buckets} + m}{G(bucket) + m} \right)))$$

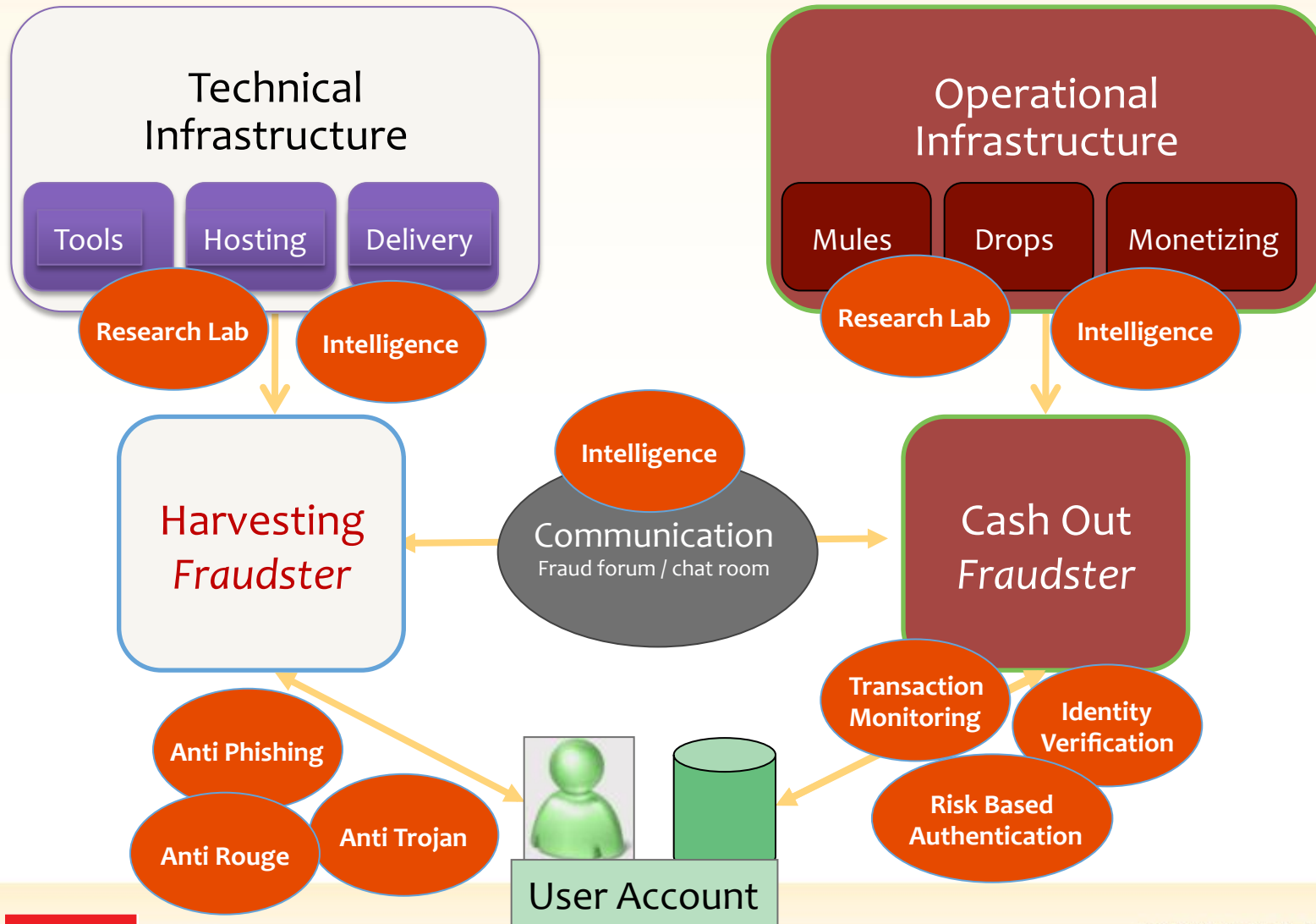
Network parameters
 eFraudNetwork Mule accounts
 Device ID IP geo location
 Behavioral Anomaly Payment amount Velocity checks
 Back Coloring Ground speed Trojan Credentials
 Fraud intelligence Payee reputation
 HTML5 data Mobile GPS Location

Results from a major UK bank

RSA CONFERENCE
C H I N A 2012



Fighting Back



Specific Trends in China

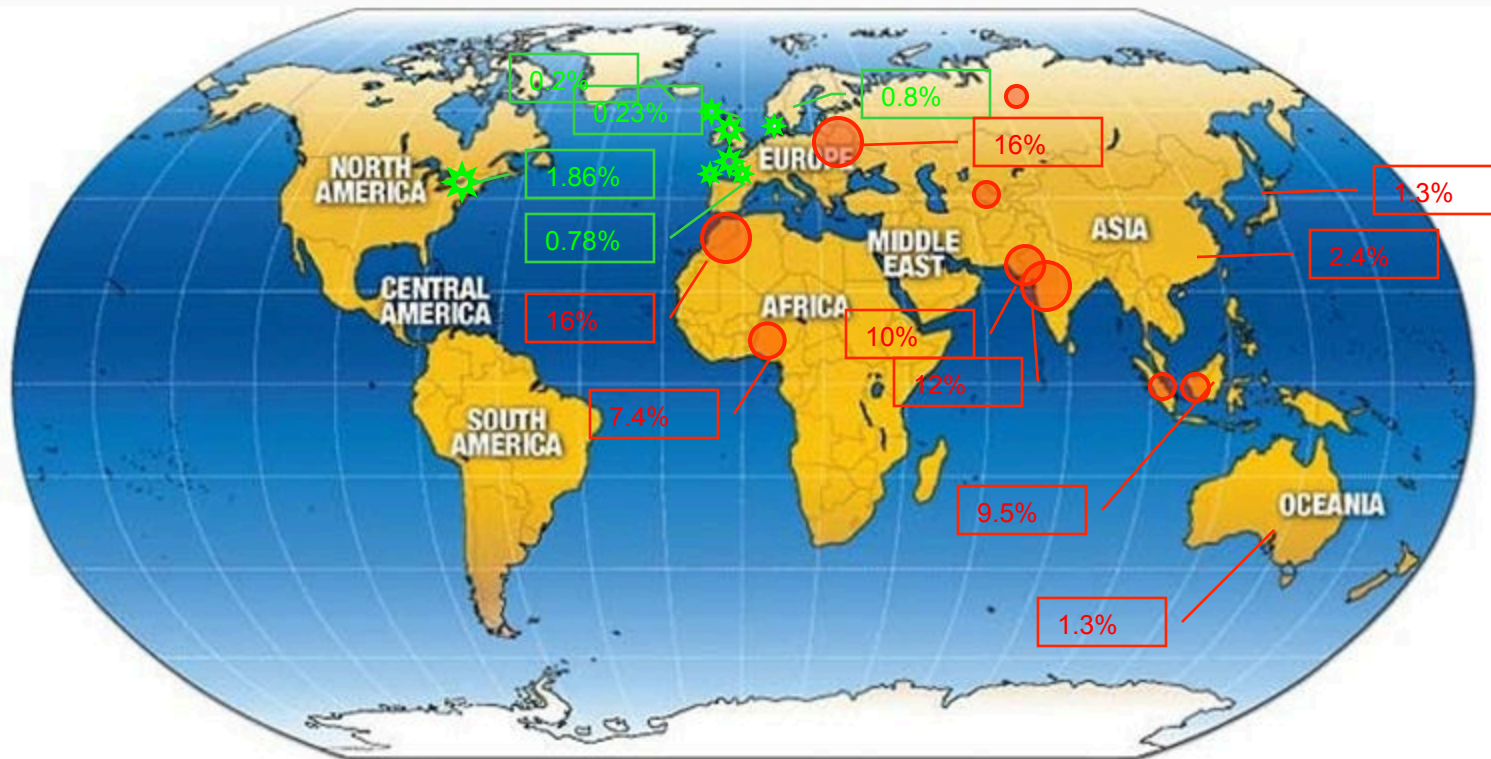


Session ID:

Session Classification:

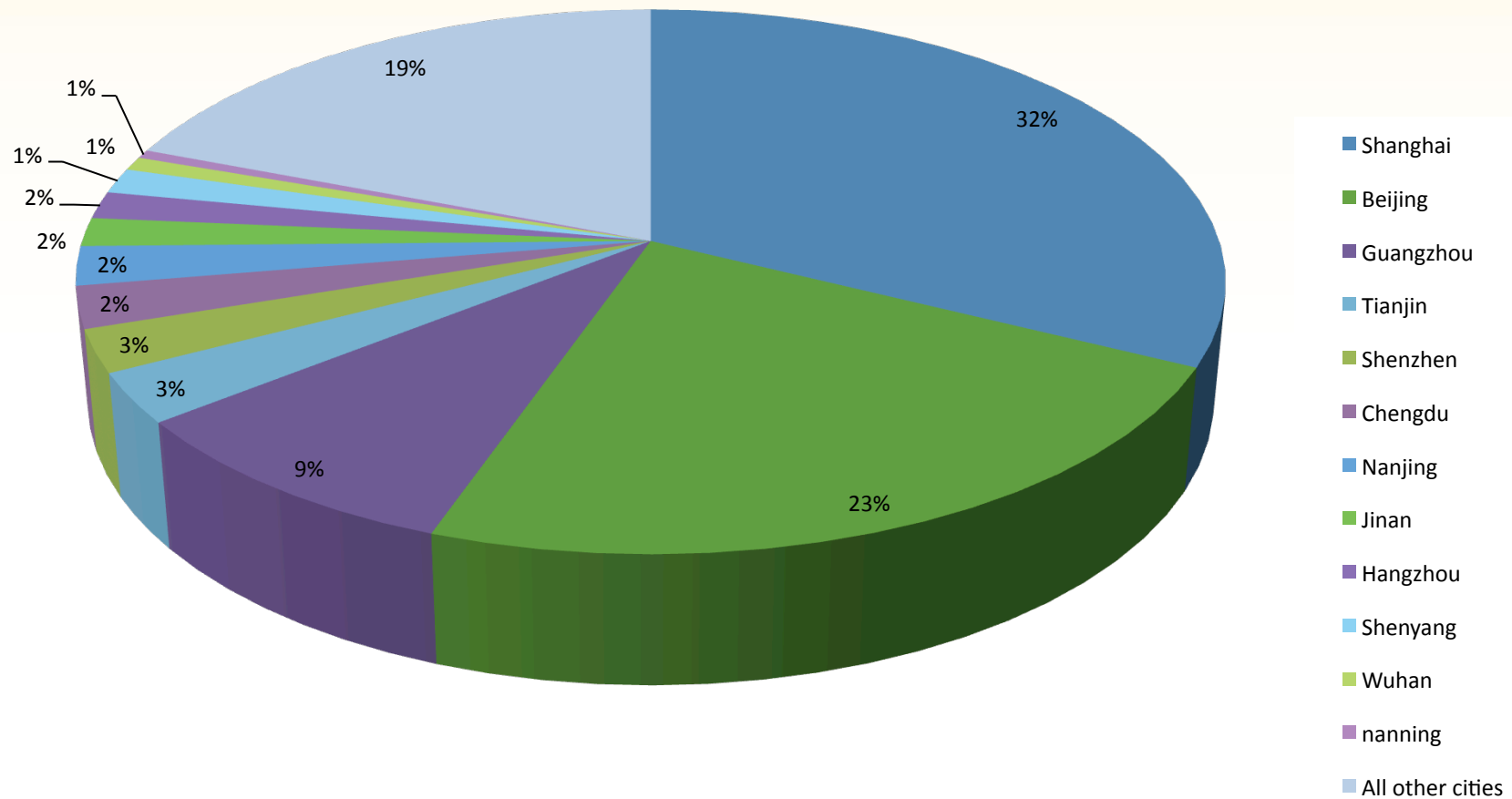
RSA CONFERENCE
C H I N A 2012
RSA信息安全大会2012

Global Fraud as % Total Transaction



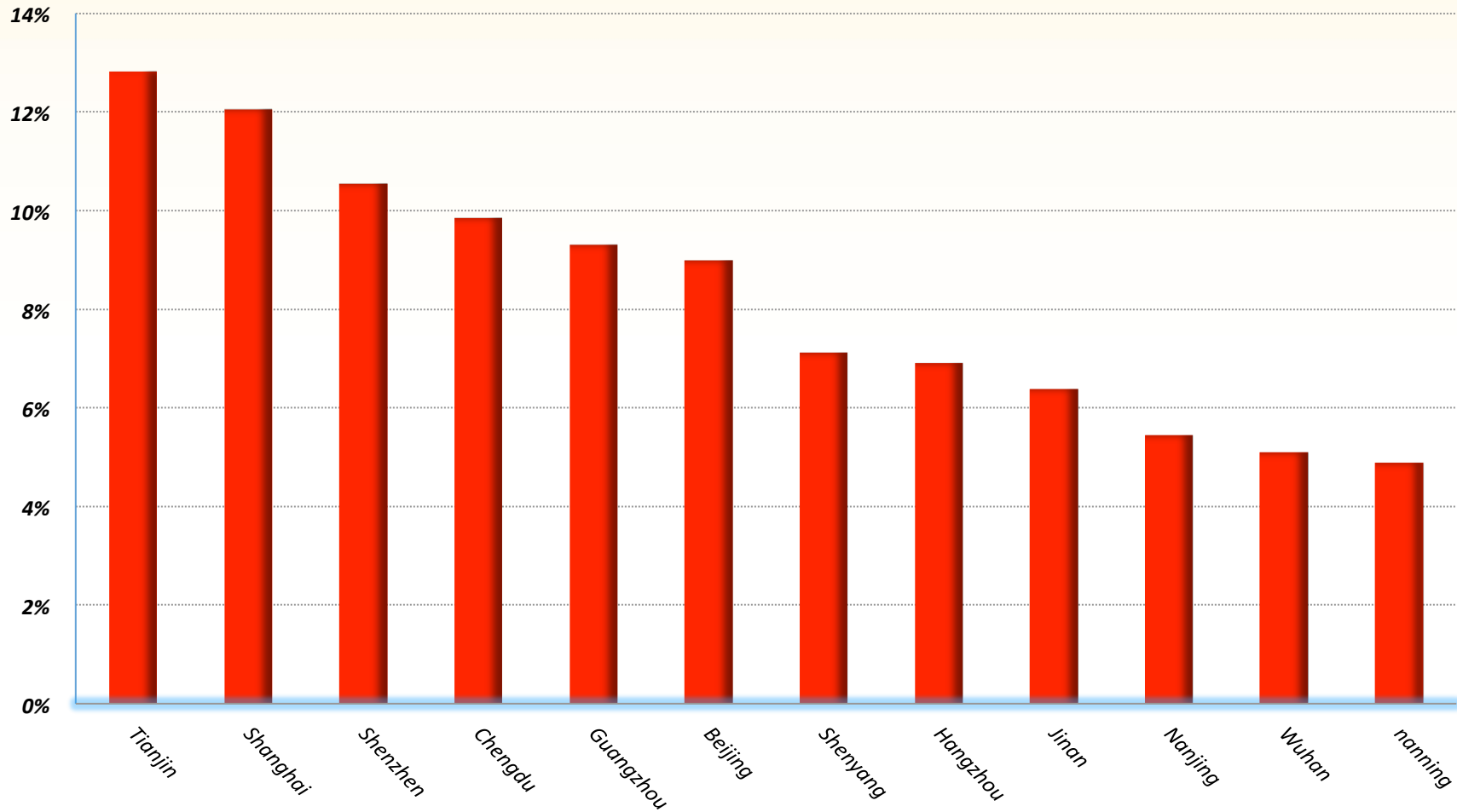
Total Fraud Share of Chinese Cities

RSA CONFERENCE
CHINA 2012



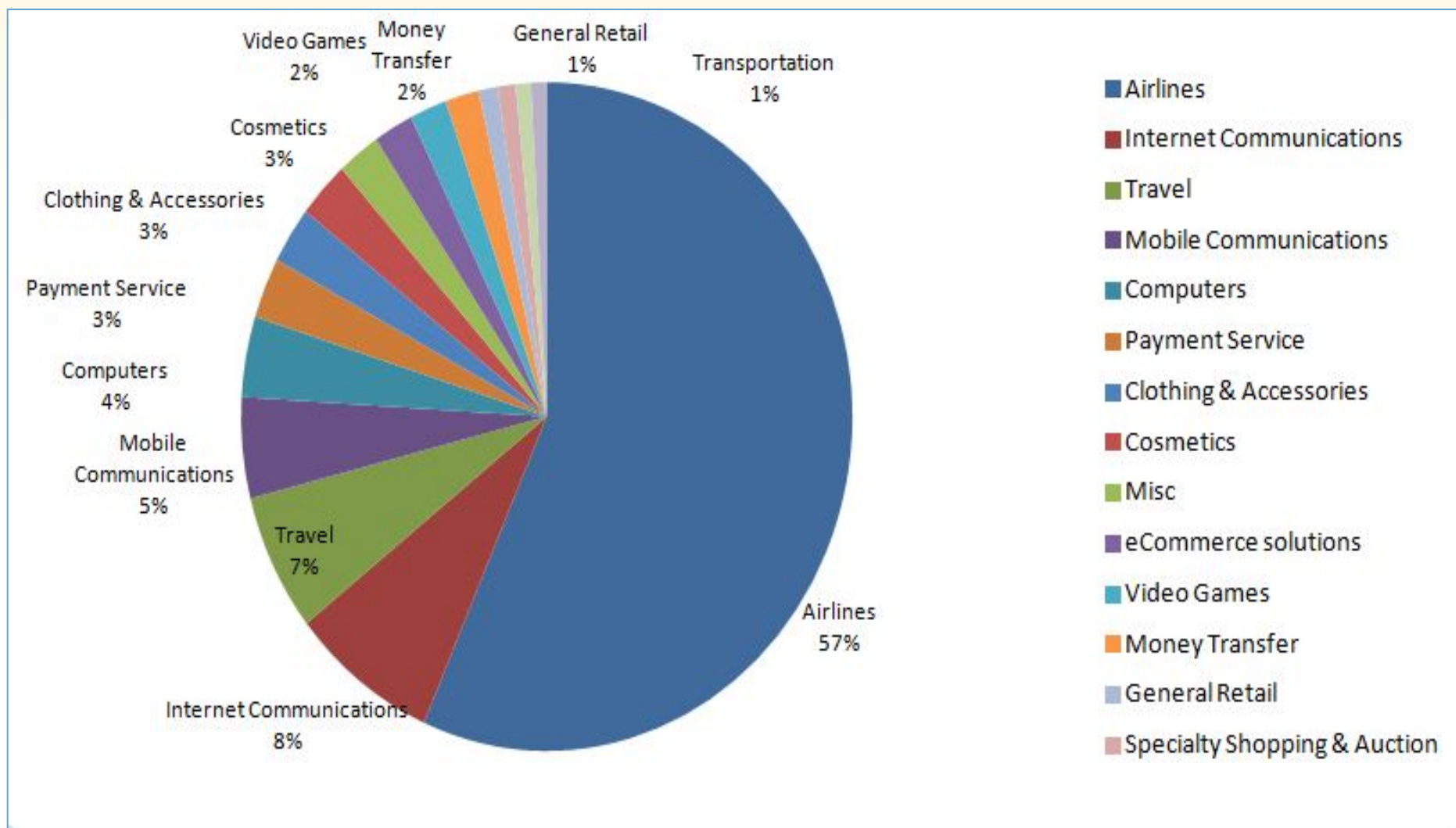
Chinese Cities with the Highest Fraud Rates

RSA CONFERENCE
C H I N A 2012

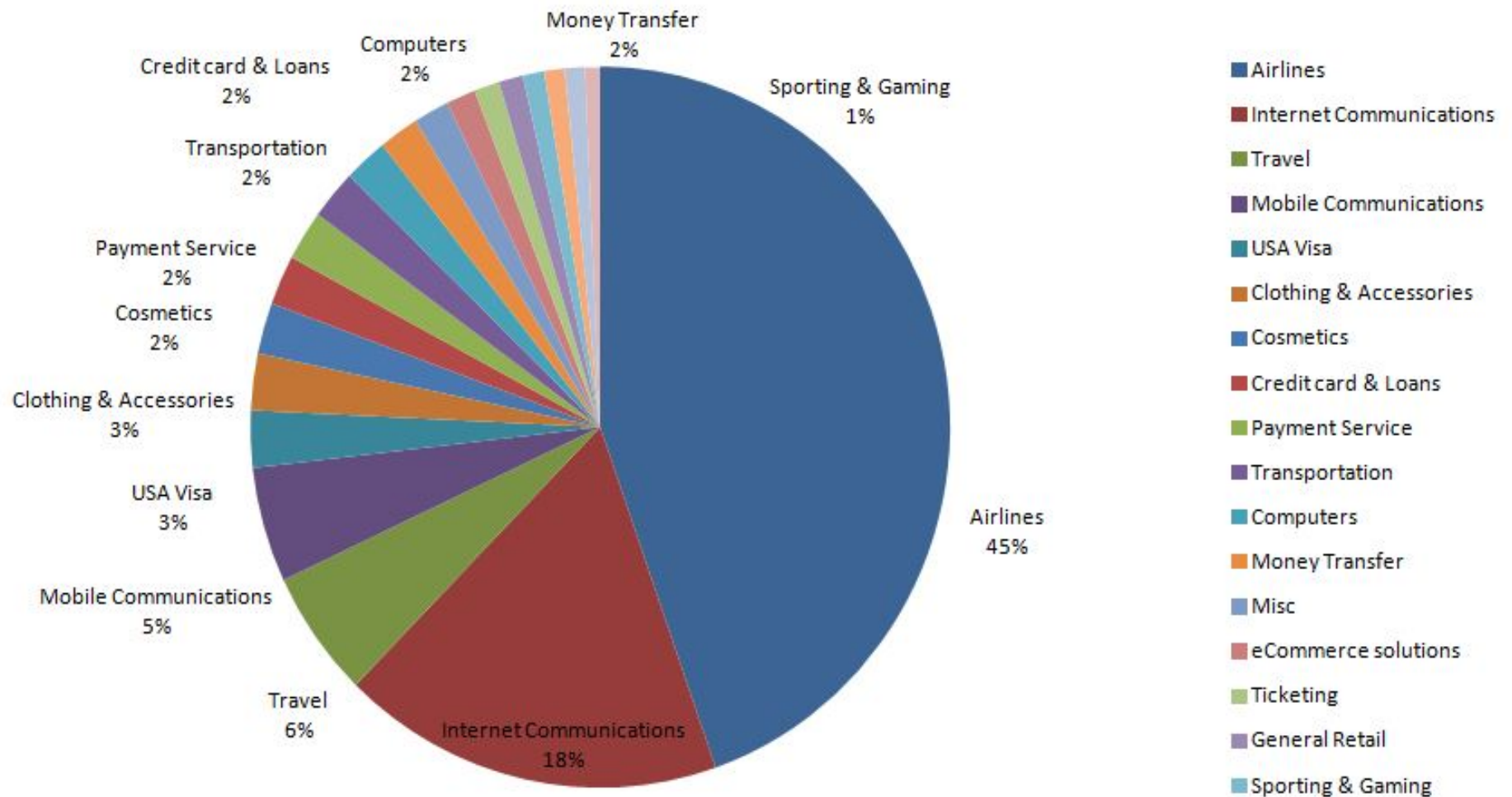


How would a Online Fraudster make a living in China?

RSA CONFERENCE
C H I N A 2012



China – Online Shopping by Category



Thank You



RSA CONFERENCE
C H I N A 2012
RSA信息安全大会2012