

**ThreatMetrix™**

Cybercrime Protection

屏风

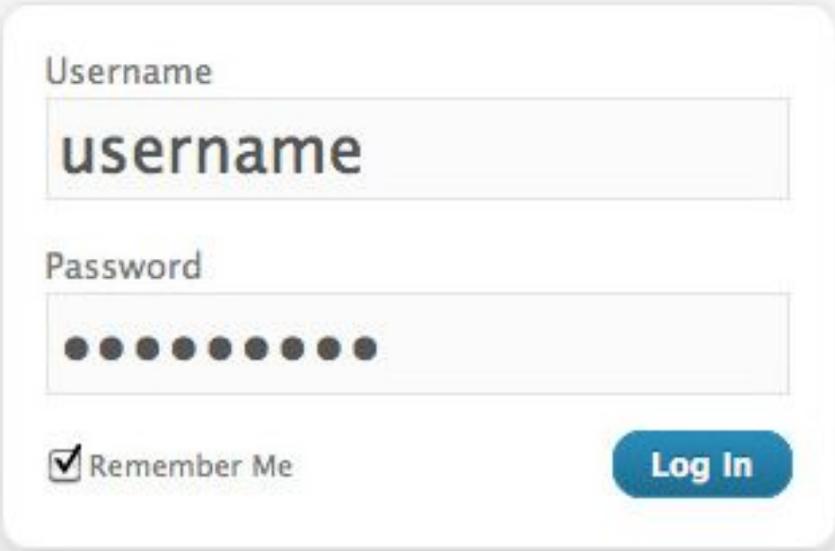
网络罪案防御

# 环球诚信智能 云计算与大数据新世界里 转变中的诈骗与安全前景

Jackal Ma, VP of Asia Operation, ThreatMetrix, Inc.  
马骏驱, 屏风亚洲运营副总裁

Nov 2013

# 新的進階持續性威脅 APT



Username  
username

Password  
●●●●●●●●

Remember Me Log In

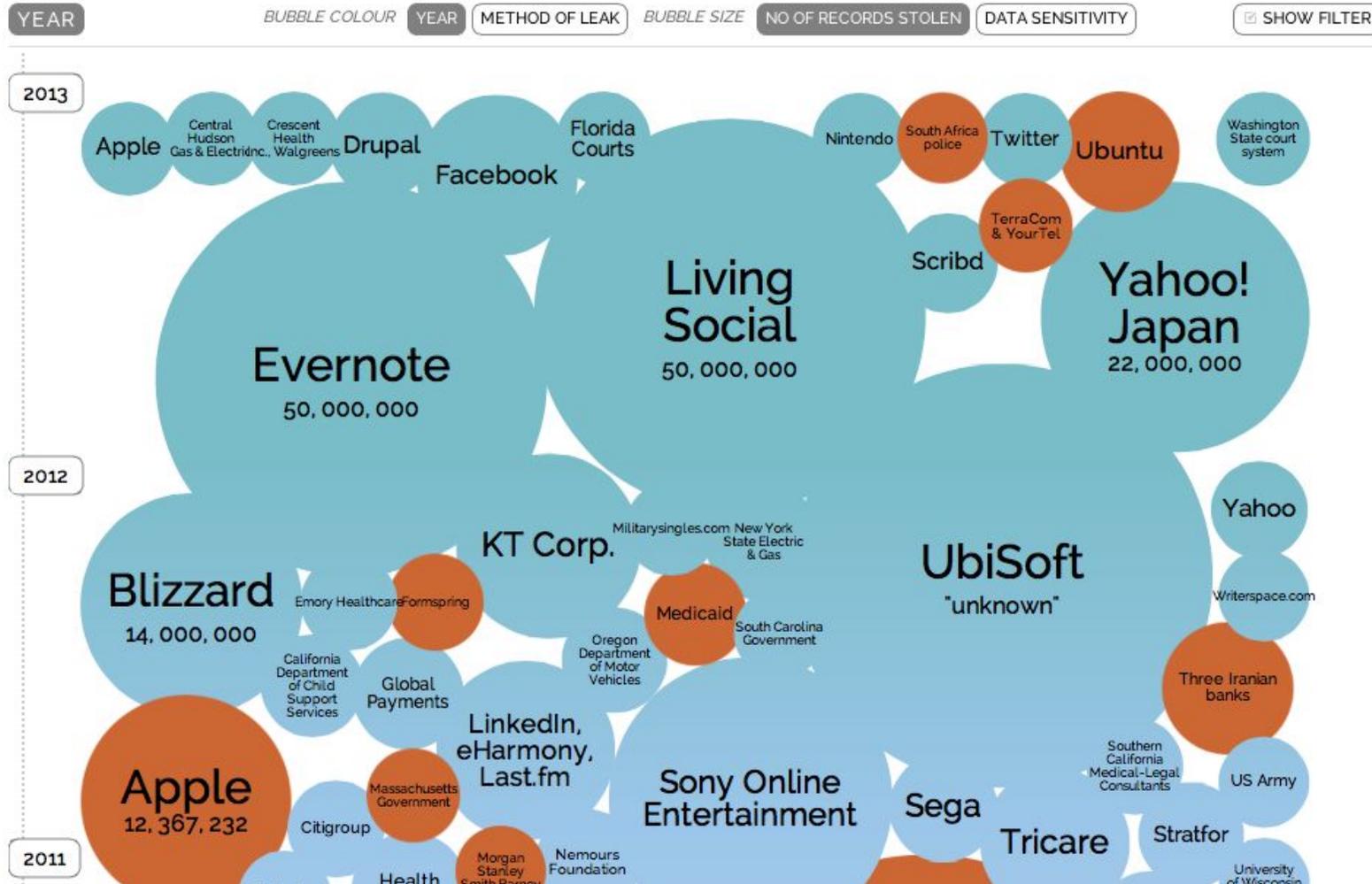
[Register](#) | [Lost your password?](#)

# 假设每个用户名都被妥协了

## World's Biggest Data Breaches

Selected losses greater than 30,000 records

interesting story



# 有足够的上下文脈 (CONTEXT) 去猜想每一个密码

Adobe入侵中泄漏的1.53亿电邮，加密了的密码与明码的密码提示

```
79985232-|--|-- a@fbi.gov-|+ujciL90fBnioXG6CatHBw==|-anniversary|--
105009730-|--|-- gon@ic.fbi.gov-|-9nCgb38RHw==|-band|--
108684532-|--|-- burn@ic.fbi.gov-|-EQ7fIpT7i/Q=-|-numbers|--
63041670-|--|-- iv-|-hRwtmq98mKzioxG6CatHBw==|-|--
94038395-|--|-- .n@ic.fbi.gov-|-MreVpEovY17ioxG6CatHBw==|-eod date|--
116097938-|--|-- -|-Tur7Wt2zH5CwIIHfjvcHKQ==|-SH?|--
83310434-|--|-- c.fbi.gov-|-NLupdfyYrsM=-|-ATP MIDDLE|--
113389790-|--|-- iv-|-iMhaearHXjPioxG6CatHBw==|-w|--
113931981-|--|-- @ic.fbi.gov-|-lTmosXxYnP3ioxG6CatHBw==|-See MSDN|--
114081741-|--|-- lom@ic.fbi.gov-|-ZcDbLlvCad0=-|-fuzzy boy 20|--
106145242-|--|-- @ic.fbi.gov-|-xc2KumNGzYfioxG6CatHBw==|-4s|--
106437837-|--|-- i.gov-|-adIewKvmJEsFqx0HFoFrxg==|-|--
96649467-|--|-- ius@ic.fbi.gov-|-lsYW5KRKNT/ioxG6CatHBw==|-glass of|--
96670195-|--|-- .fbi.gov-|-X4+k4uhyDh/ioxG6CatHBw==|-|--
105095956-|--|-- earthlink.net-|-ZU2tTTFIZq/ioxG6CatHBw==|-socialsecurity#|--
108260815-|--|-- r@genext.net-|-MuKnZ7KtsiHioxG6CatHBw==|-socialsecurity|--
83508352-|--|--h @hotmail.com-|-ADEcoaN2oUM=-|-socialsecurityno.|--
83023162-|--|--k 590@aol.com-|-9HT+kVHQfs4=-|-socialsecurity name|--
90331688-|--|--b .edu-|-nNiWEcoZTBmXrIXpAZiRHQ==|-ssn#|--
]
```

<http://7habitsofhighlyeffectivehackers.blogspot.com/2013/11/can-someone-be-targeted-using-adobe.html>

# 针对性攻击变得没有难度

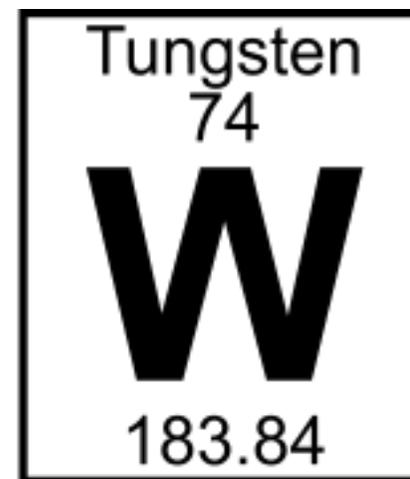
屏风

ThreatMetrix™

```
[justing@localhost passwords]$ grep E07fip cred | cut -d'|' -f5 | sort | uniq -c | sort -nr | head -n50
419496 -
53380 -1to6
23444 -numbers
14657 -123
14329 -654321
14080 -numeros
11876 -1-6
10758 -number
6888 -1
4443 -12
3959 -num
3570 -1234567
3407 -12345
3400 -123456789
3299 -??
2925 -numero
2848 -16
2599 -6
2489 -1234
2394 -no
2198 -count
1489 -????
1475 -#
1369 -Numbers
1268 -???
1183 -zahlen
1183 -sequencia
1166 -1 to 6
1121 -one to six
1043 -a
1034 -hola
1021 -del 1 al 6
978 -dog
976 -six
947 -12345678
898 -abc
867 -name
860 -abcdef
847 -111111
800 -??????
777 -easy
767 -hi
755 -?????
750 -?
713 -none
674 -lol
635 -numbers 1-6
622 -usual
```

e.g. [edwardsnowden@\\*\\*\\*\\*\\*mail.com](mailto:edwardsnowden@*****mail.com)

- 207 账号用同一密码
- 明码提示包括:
  - 硬金属
  - 元素表 74W



密码是Tungsten吗?

<http://7habitsofhighlyeffectivehackers.blogspot.com/2013/11/can-someone-be-targeted-using-adobe.html>

# 用一张被盗的信用卡可以引起大型的暴力攻击

**CloudCracker**

An online password cracking service for penetration testers and network auditors who need to check the security of WPA protected wireless networks, crack password hashes, or break document encryption.

**Start Cracking**

File Type

Hash File  no file selected

Handshake Dictionary Delivery

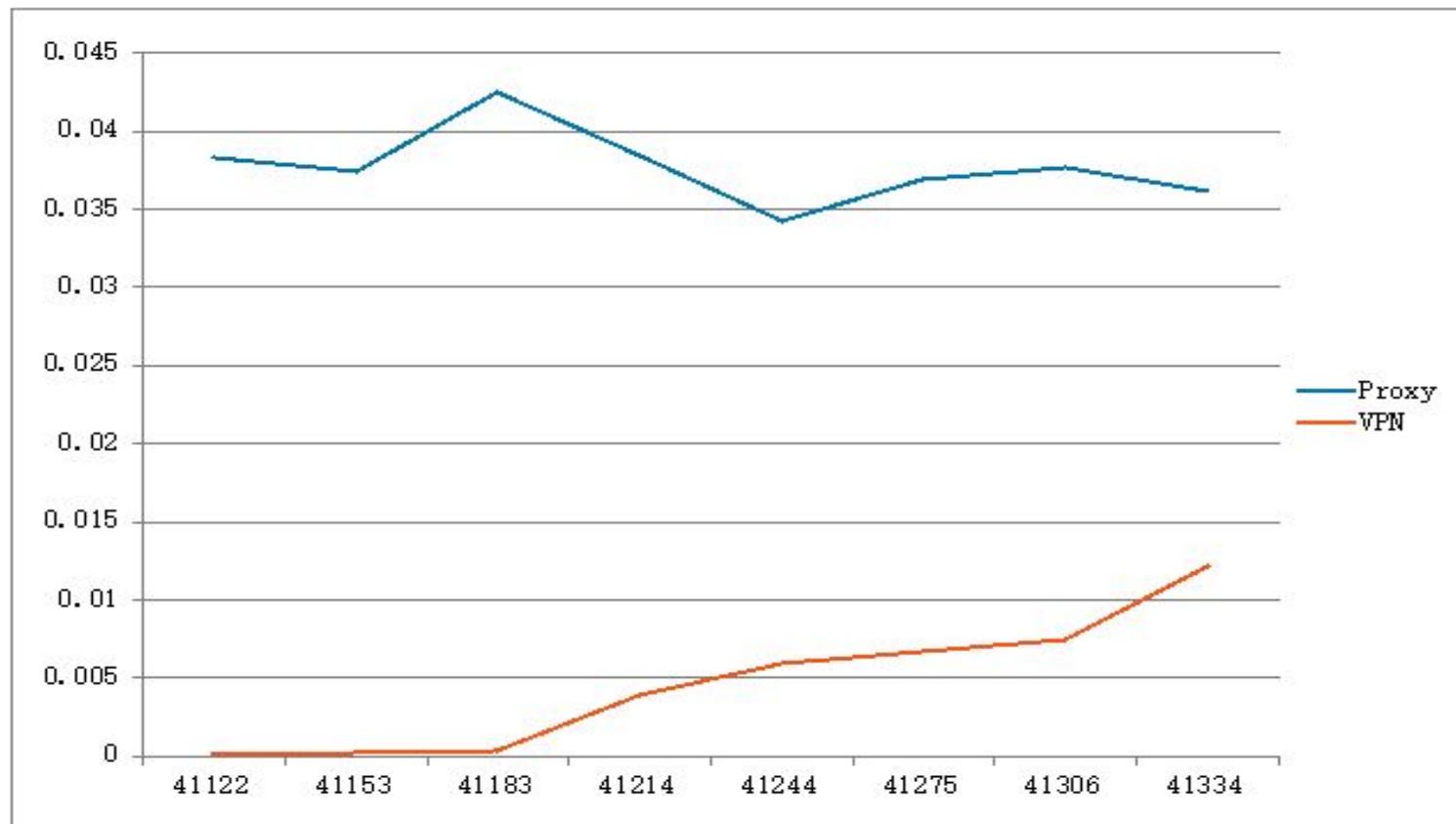
**Big. Fast. Cheap.**  
Run your network handshake against  
**300,000,000 words**  
**in 20 minutes**  
**for \$17.**

"Welcome to the future: cloud-based WPA cracking is here!" -  
- TechRepublic

"Low cost service cracks wireless passwords from the cloud..." -  
- TheRegister

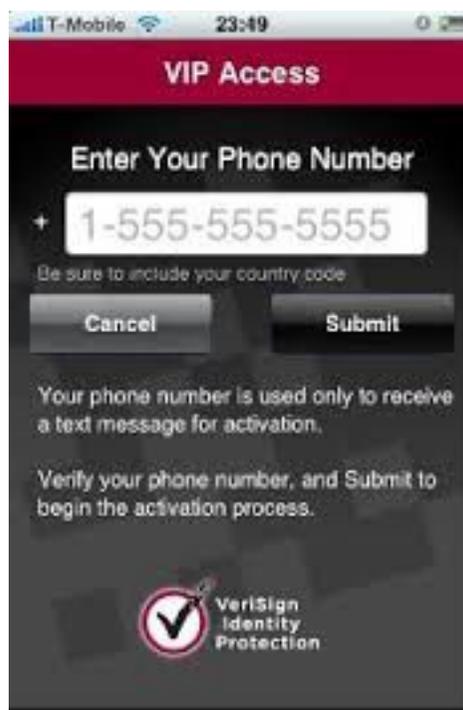
"This really is a great idea." -  
- Hacker News

# 用机器人，代理与VPN隐藏他们的轨迹



ThreatMetrix Trust Intelligence Network

所以我们要用多因子认证，对吗？



# 所以我们有恶意软件

## In-session malware 会话中恶意软件

- 能操控当前银行会话
- e.g. Man-in-the-Browser 中间人攻击

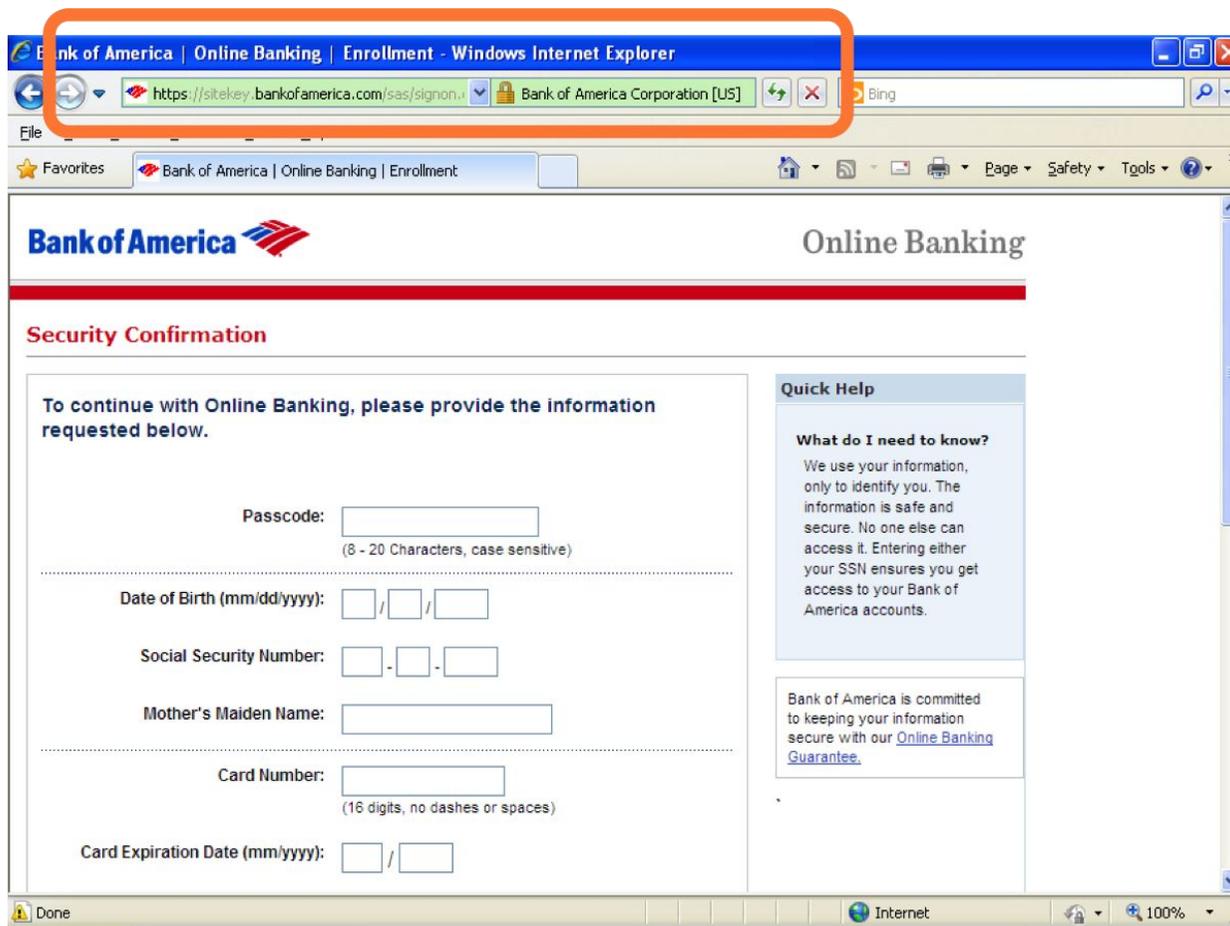


## Out-of session 会话外恶意软件

- 一般用于盗窃个人资料用于日后攻击
- E.g. Keyloggers 录键器



# 一般帐户控制案例



# PayPal – 正常网站

The screenshot displays the PayPal 'My Account' page for user Andreas Baumhof. The page includes a navigation menu with options like 'Send Money', 'Request Money', and 'Merchant Services'. A prominent green banner encourages users to 'LOSE THE PLASTIC KEEP THE POINTS'. The account balance is shown as \$0.00 AUD. A table lists the user's recent activity, including payments received and sent, with columns for Date, Type, Name/Email, Payment status, Details, Order status/Actions, and Gross.

My Account - PayPal

PayPal, Inc. [US] https://www.paypal.com/au/cgi-bin/webscr?cmd=\_login-done&login\_access=1339699250

Log Out | Help | Safety Advice

Search

**PayPal**

My Account | Send Money | Request Money | Merchant Services | Auction Tools | Products & Services

Overview | Add Funds | Withdraw | History | Resolution Centre | Profile

Welcome, **Andreas Baumhof**

Account Type: Personal [Upgrade](#) | Status: **Verified** | Account Limits: [View Limits](#)

Last log in 15 June 2012 03:10 AEST

**LOSE THE PLASTIC  
KEEP THE POINTS** PAY HAPPY **PayPal**

Notifications  
Policy Updates

**HAPPY TIP  
DID YOU KNOW?**  
You can use PayPal to buy just about anything. PayPal is available at over 50,000 online and mobile stores.  
Find out more  
PAY HAPPY **PayPal**

Questions? We're here to help.  
[Contact us](#)

PayPal balance: **\$0.00 AUD** [Currency converter](#)

Available balance in AUD (primary): \$0.00 AUD  
Total balance (all currencies, available and pending) converted to AUD: \$0.00 AUD [Hide](#)

Currency	Total
AUD (Primary)	\$0.00 AUD
USD	\$0.00 USD

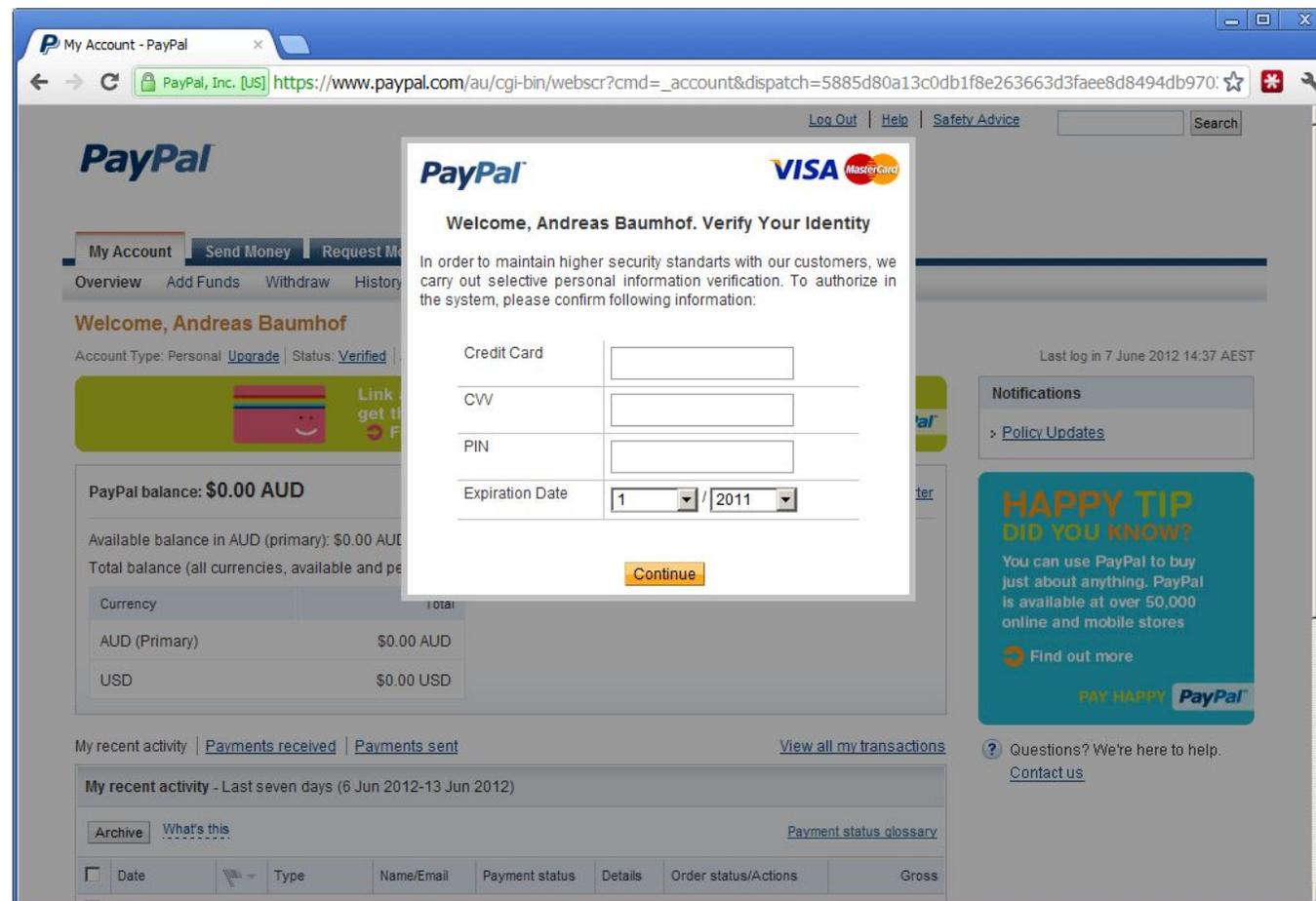
My recent activity | [Payments received](#) | [Payments sent](#) | [View all my transactions](#)

**My recent activity** - Last seven days (8 Jun 2012-15 Jun 2012)

[Archive](#) | [What's this](#) | [Payment status glossary](#)

Date	Type	Name/Email	Payment status	Details	Order status/Actions	Gross
------	------	------------	----------------	---------	----------------------	-------

# PayPal – 帶有 Zeus Trojan



# Macys – 正常网站

Shopping Bag - Shopping Bag x

www1.macys.com/bag/index.ognc?CategoryID=7502&cm\_sp=atblayer-\_checkout\_-\_n

the magic of **macy's** WE NOW SHIP TO OVER 100 COUNTRIES! learn more

shopping bag (1)

for the home bed & bath women men juniors kids beauty & fragrance shoes handbags & accessories jewelry & watches sale

SEARCH Keyword, Web ID GO **Brasil** the gift guide STORES DEALS & PROMOTIONS GIFT CARDS WEDDING REGISTRY

### your shopping bag

Prices are subject to change based on the price in effect the day you checkout Bag ID: 1469-99373

Item	Price	Qty.	Total
 Lauren Ralph Lauren Bedding, Marrakesh Jacquard Twin Duvet Cover Color: Marrakesh Tan Web ID: 591800 In Stock: Usually ships within 2 business days. <a href="#">remove</a>	Sale \$159.99 Reg. \$400.00	1	\$159.99

**HAVE A PROMO CODE?** [find one now](#)  
   
only one promo code may be used per order

**You Saved \$240.01**  
[How is this calculated?](#)

**free shipping every day of the year!**  
with \$99 purchase, no code, no end date, exclusions apply.

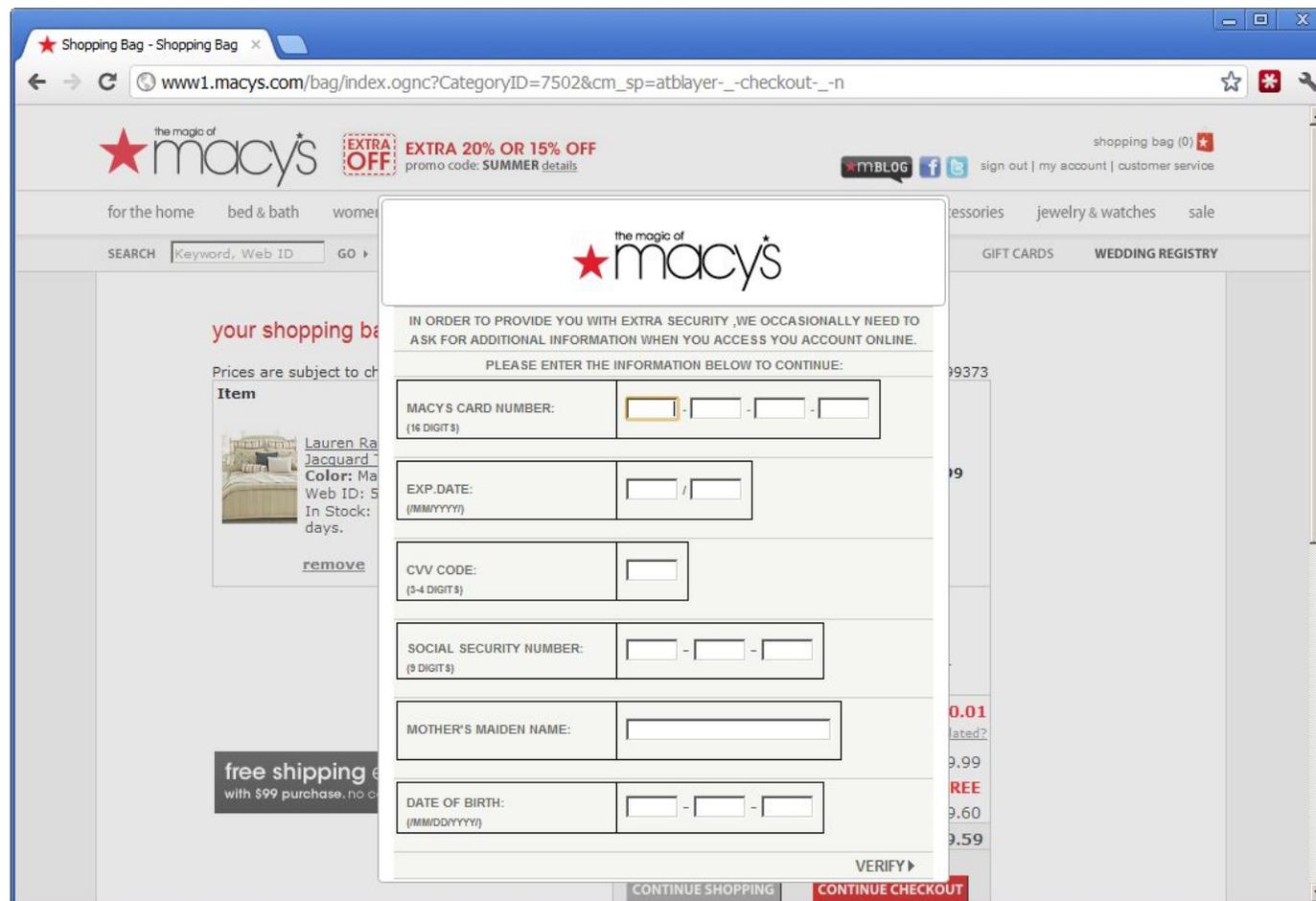
Merchandise Total:	\$ 159.99
Estimated Shipping:	<b>FREE</b>
Estimated Taxes (6%):	\$ 9.60
<b>Total:</b>	<b>\$ 169.59</b>

#### customers also loved

  
**LOWEST PRICE OF THE SUMMER SEASON!**  
Lauren Ralph Lauren Bedding, Marrakesh Rug Standard Pillowcase Set  
Reg. \$115.00  
Was \$79.99  
Sale \$45.99  
[FIND IT IN STORE](#)



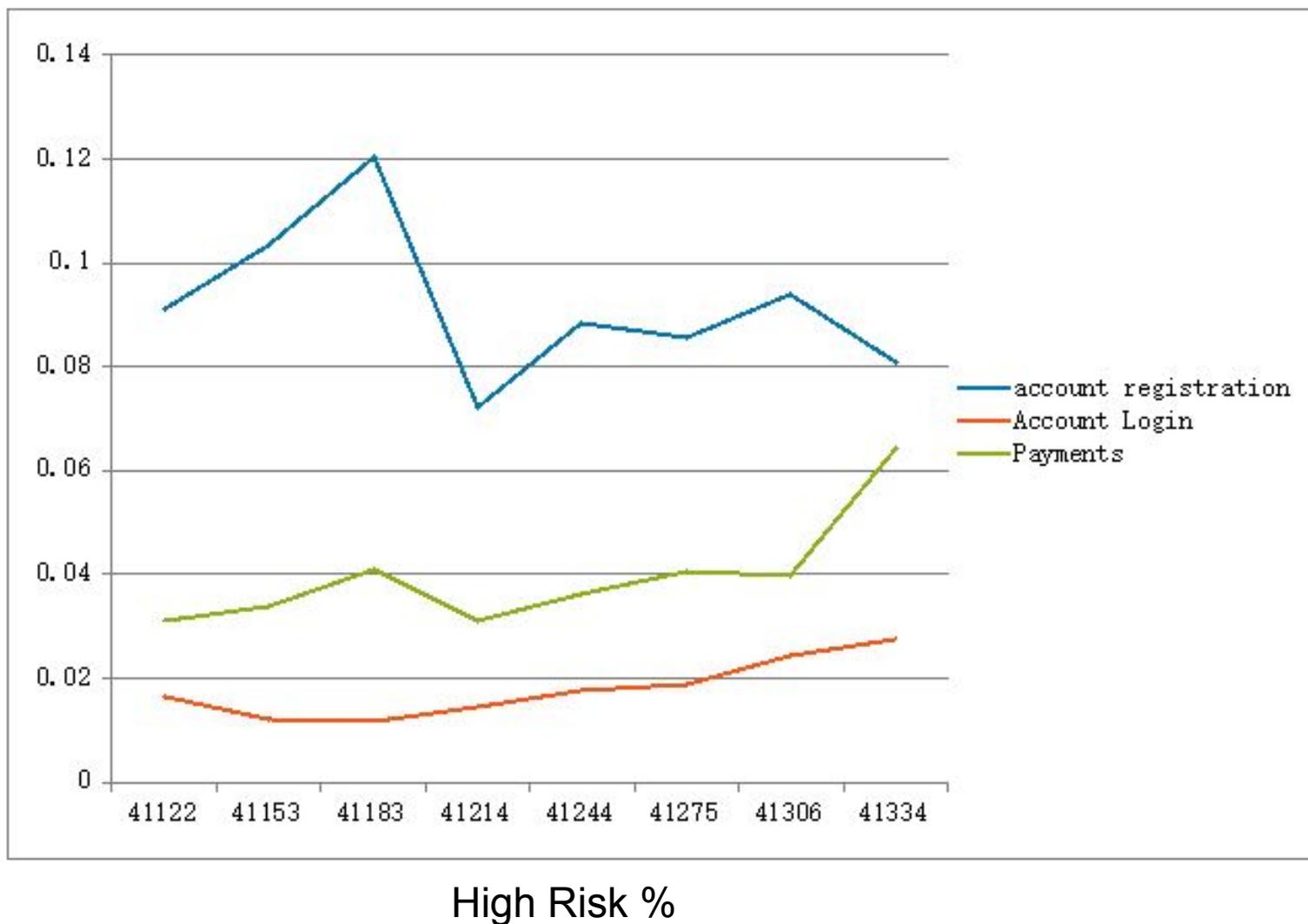
# Macy's – 帶有 Zeus Trojan



ThreatMetrix™ 屏风

我们需要改变思路

# 网络罪案已经变得“先进”与“可持续”— 我们应该醒醒



安全不是有关“好”和“坏”— 好人可以有坏事发生在他们身上

屏风

ThreatMetrix™



百分之**95**的网络罪案防御在于可信客户的鉴别

屏风  
ThreatMetrix™



# Global Trust Intelligence Network

环球诚信智能网路

屏风  
ThreatMetrix™



## Global Trust Intelligence Network 环球诚信智能网络

可信客户还是网  
络威胁？

保护 帐户与收入

全面的设备检测  
与  
用户行为勾画

横跨数以千计客户的  
实时环球数据分析

基于个别企业业务需求的优  
化 — 可个性化引擎

## 全面的设备检测与用户行为勾画

- 
- > Device
  - > Identity
  - > Activity
  - > Threats

# 全面的设备检测与用户行为勾画

- > 设备
- > 身份
- > 行为
- > 威胁

**MALWARE**

# 横跨数以千计客户的 实时全球数据分析



基于个别企业业务需求的优化 — 可个性化引擎 — 增加  
利润与降低客户摩擦

屏风  
ThreatMetrix™

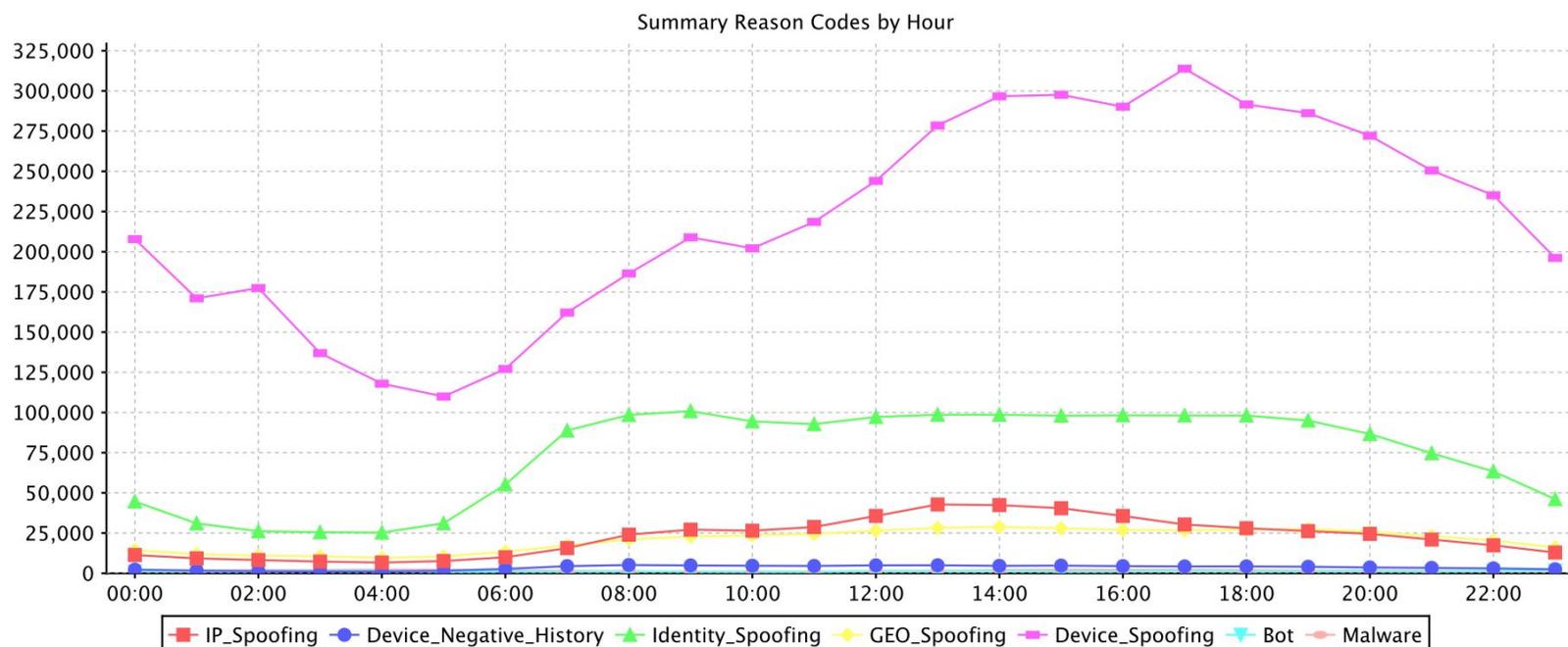


# 网络罪案的攻击维度 — 案例

## Summary Reason Overview

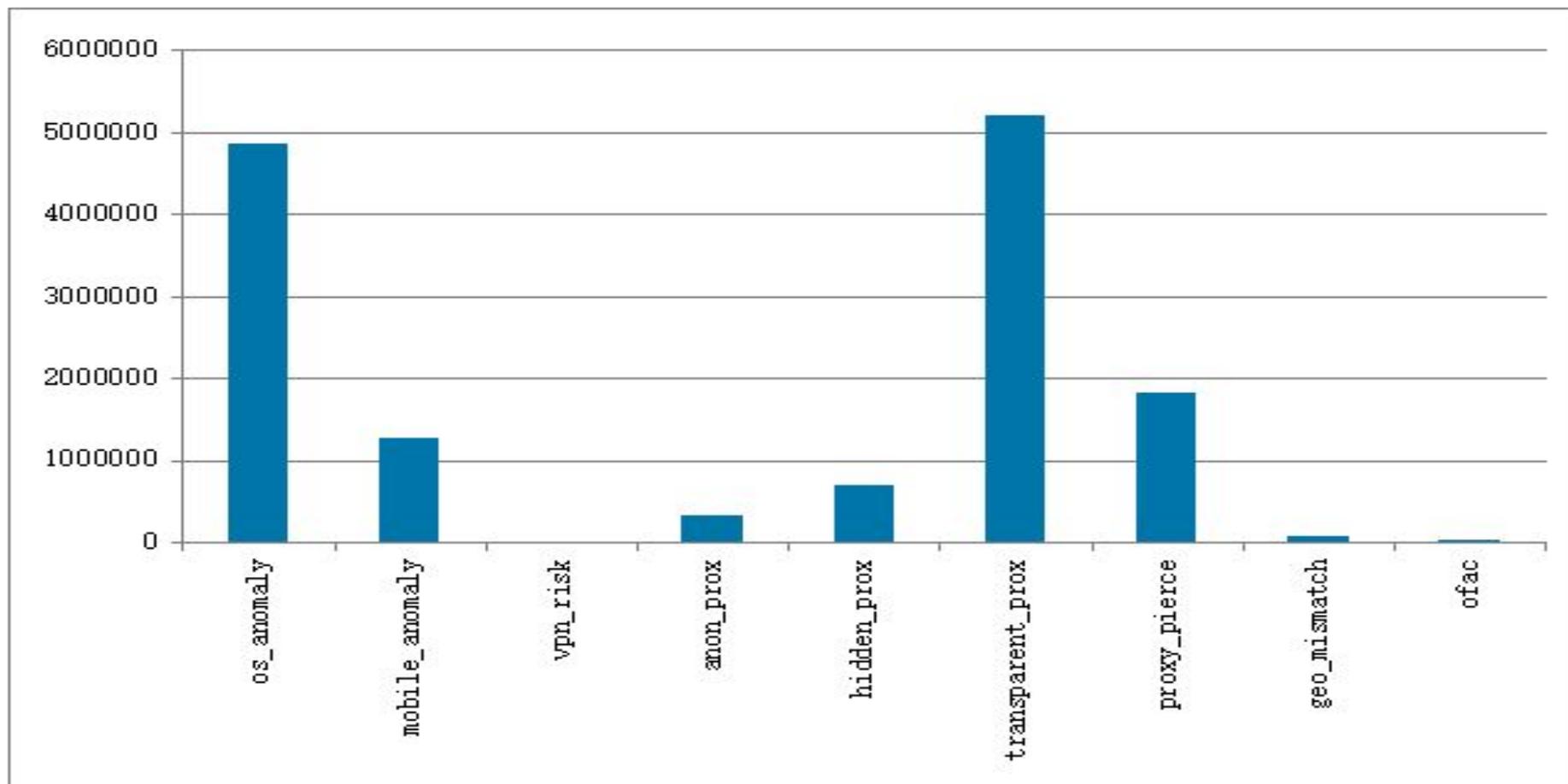
Past day from 2013-11-07

Summary	Total	%
Device_Spoofing	5,279,005	64.08%
Identity_Spoofing	1,767,162	21.45%
IP_Spoofing	540,020	6.56%
GEO_Spoofing	496,183	6.02%
Device_Negative_History	84,887	1.03%
Malware	40,671	0.49%
Bot	29,857	0.36%

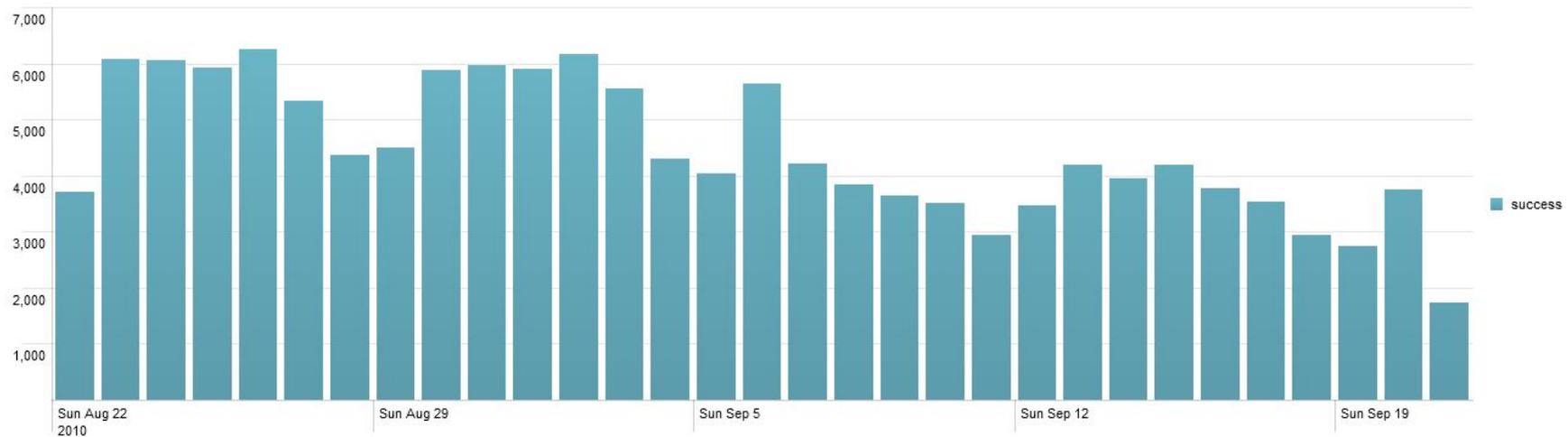


## 其中两个金融客户的例子

Total Authentications: 151,586,490 Percentage Mobile: 34%



# 代理检测与分类 — 案例



Value

#

%

none

130,660 94.602%

hidden

6,552 4.744%

transparent

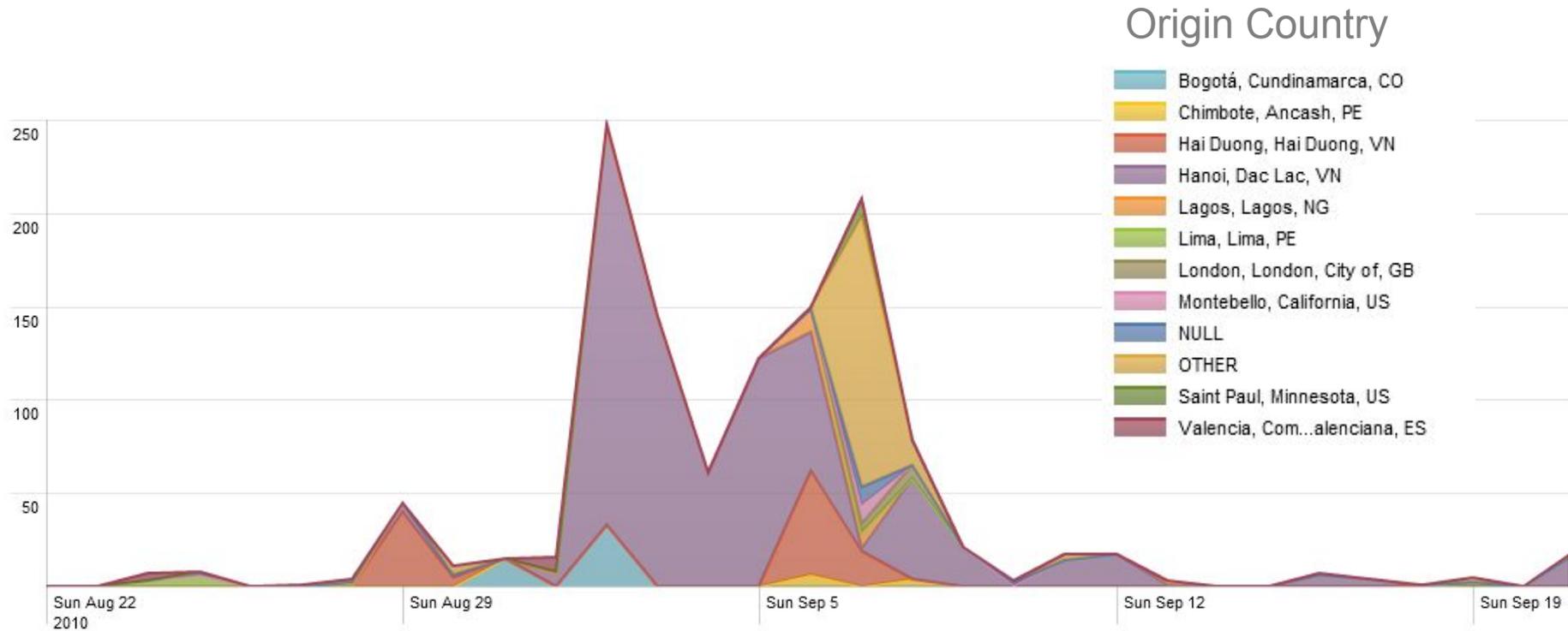
802 0.581%

anonymous

101 0.073%

ThreatMetrix Trust Intelligence Network

# 代理检测分类案例 — True IP 与 代理穿透 (Proxy Piercing)



Proxy IP Network Owner = “The Planet” US

# 远程恶意软件检测案例 — 蜜罐 HONEYPOT

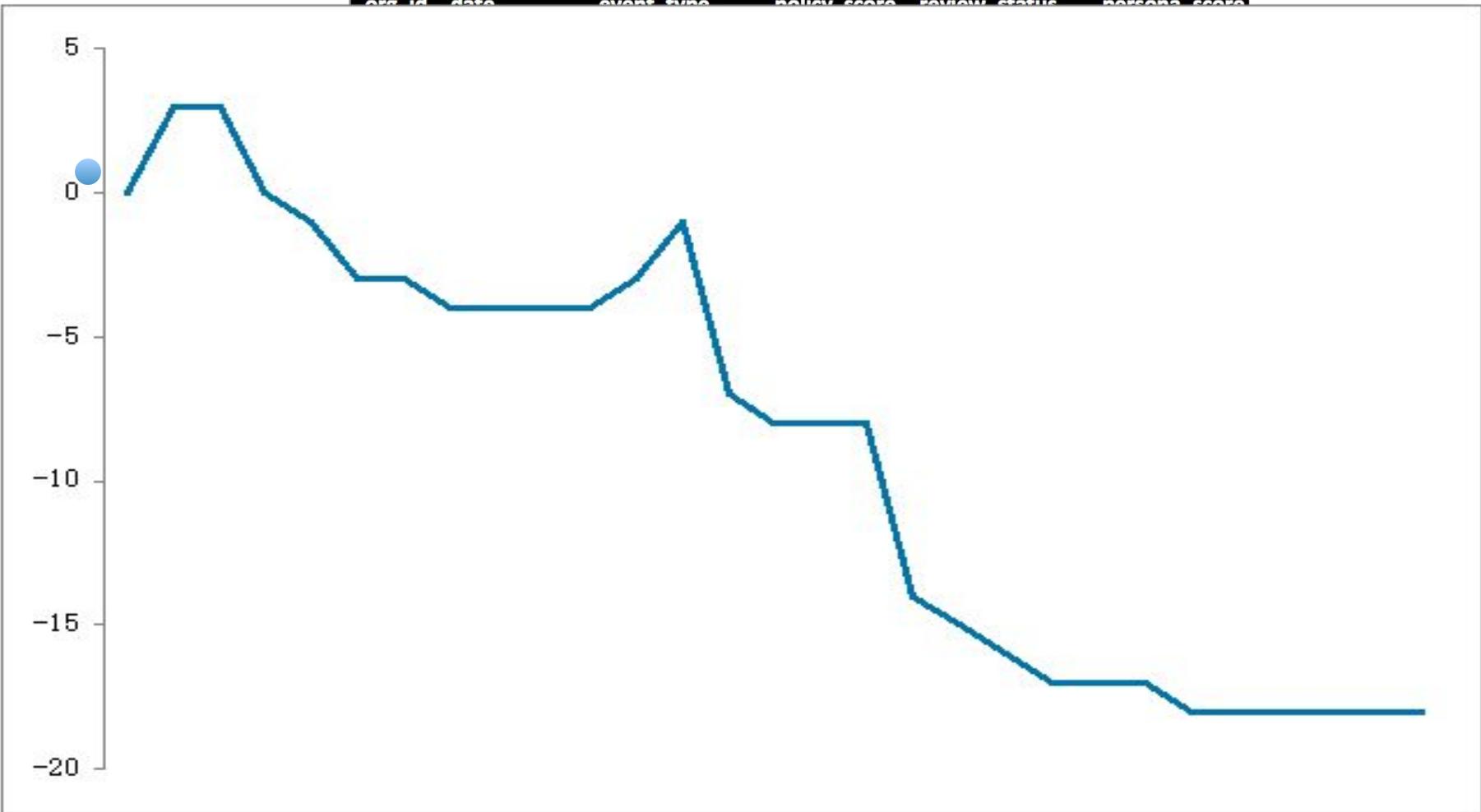
## Honeypot Result: mismatch\_black

Honeypot Fingerprint Diff	Count	Percentage In Group	Percentage Overall
Blacklist : ZeuS config hash (0011b76316076a96cab606b8f85cc2a) targeting wells Fargo.com#1-0011b76316076a96cab606b8f85cc2a-1.dat	6	26.09 %	0.01465 %
Blacklist : Possible Wells Fargo malware	6	26.09 %	0.01465 %
Blacklist : JollyWallet	5	21.74 %	0.01220 %
Blacklist : ZeuS config hash (0011b76316076a96cab606b8f85cc2a) targeting wells Fargo.com#1-0011b76316076a96cab606b8f85cc2a-0.dat	4	17.39 %	0.00976 %
Blacklist : ENTER YOUR THREE DIGIT MASTERKEY Malware	2	8.70 %	0.00488 %
<b>Total:</b>	<b>23</b>		

# 异常情况检测案例

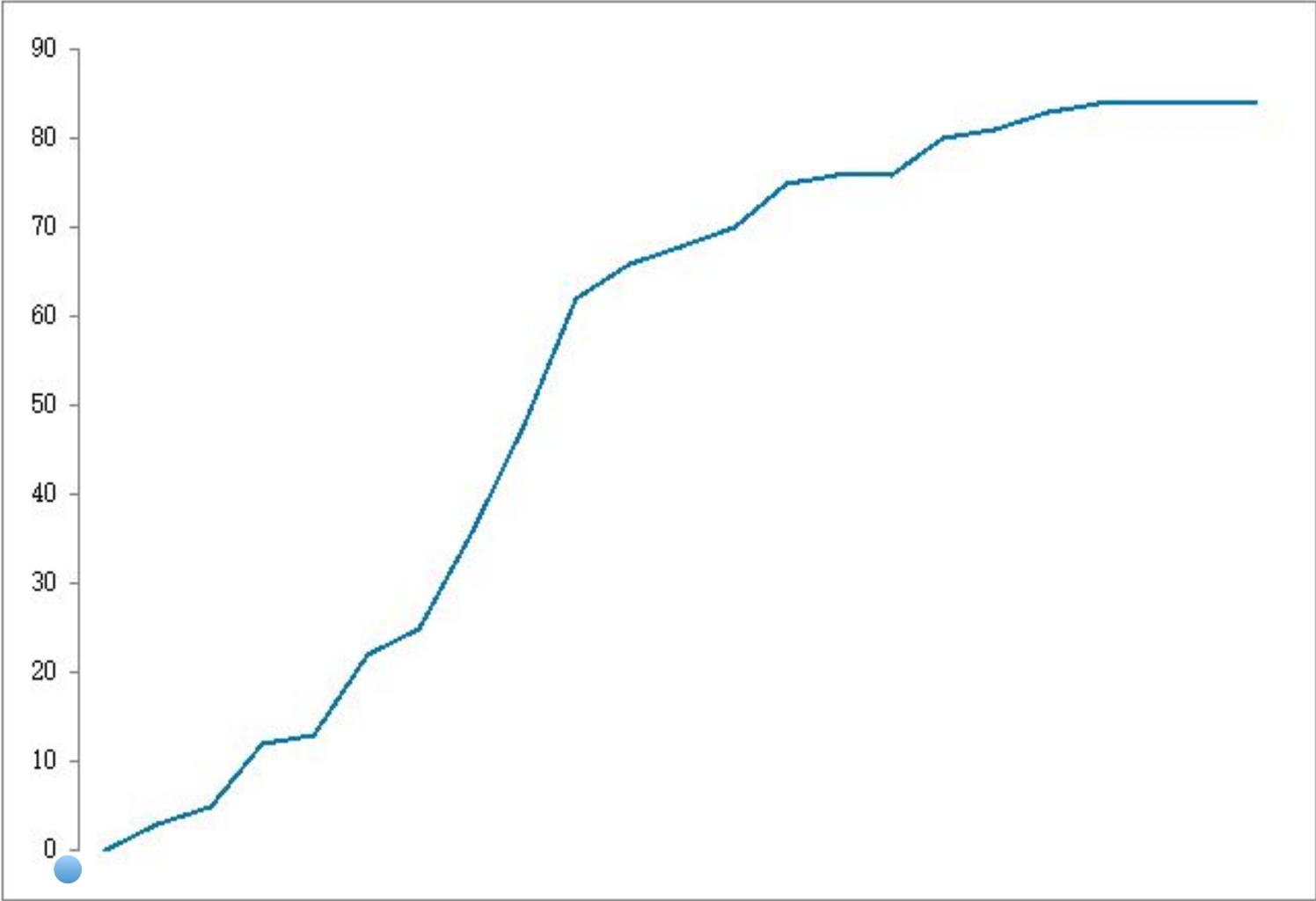
异常情况	符合异常的交易百分比%	攻击维度	攻击方法
同一账号, 多个设备	14.04%	账号挟持	手动 / 机器人 / 脚本
同一电邮地址, 多个设备	13.97%	账号挟持	手动 / 机器人 / 脚本
浏览器 / 操作系统语言不匹配	12.15%	账号挟持, 新账号登记	机器人 / 脚本
单日多IP多次登录	13.93%	账号挟持	机器人
机器人交易指标 (无浏览器数据)	5.39%	账号挟持	机器人
高风险代理	1.24%	账号欺诈	手动 / 机器人
同一设备多帐户登录 / 交易	0.81%	账号欺诈	手动 / 机器人

# 基于环球行为的声誉评级



4	2013-08-27	payment	-97	reject	-18
4	2013-08-27	payment	-97	reject	-18

# 基于环球行为的声誉评级





**ThreatMetrix™** 屏风

The Global Trust Intelligence Network



## Questions

[jma@threatmetrix.com](mailto:jma@threatmetrix.com) +86-18601077772 +852-64649215  
Jackal Ma 马骏驱

[www.threatmetrix.com](http://www.threatmetrix.com) +1.408.200.5700

[sales@threatmetrix.com](mailto:sales@threatmetrix.com)