

ThreatMetrix™

Cybercrime Protection

屏风

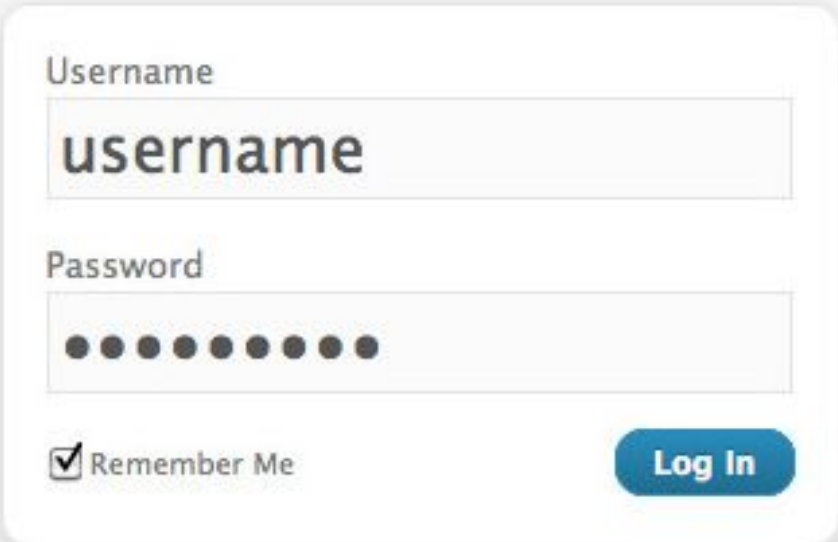
网络罪案防御

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

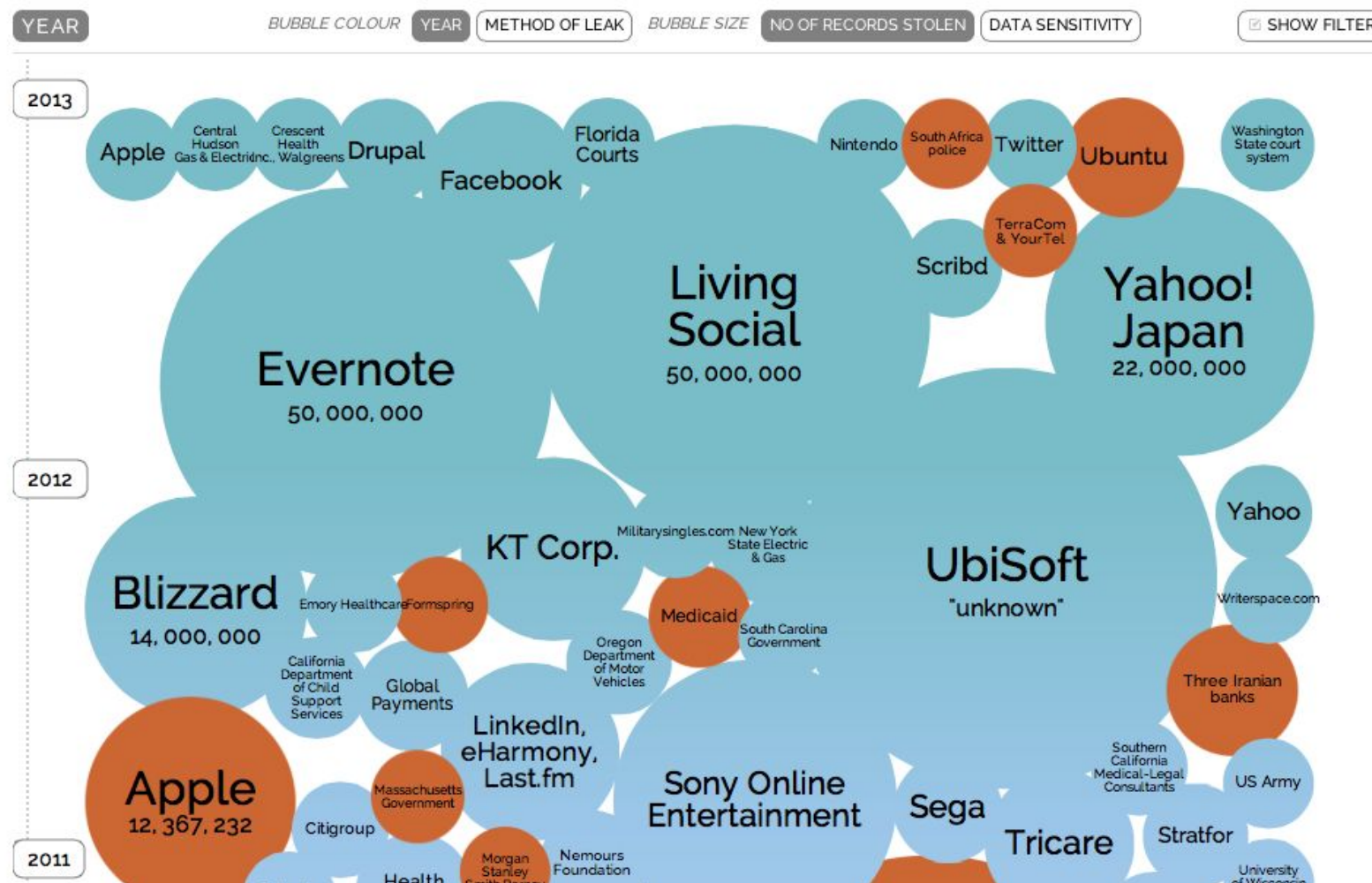
屏风

ThreatMetrix™

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

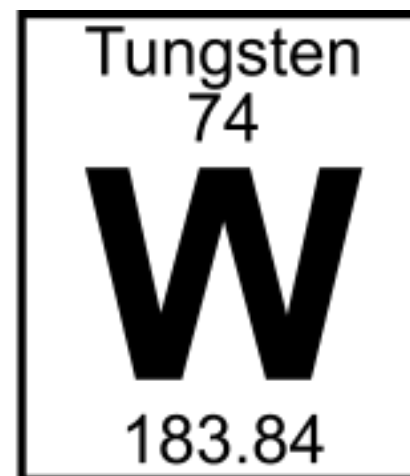
```
79985232-|--|a@fbi.gov-|-+ujciL90fBnioXG6CatHBw==|-anniversary|--
105009730-|--|gon@ic.fbi.gov-|-9nCgb38RHiw==|-band|--
108684532-|--|burn@ic.fbi.gov-|-EQ7fIpT7i/Q=-|-numbers|--
63041670-|--|iv-|-hRwtmq98mKzioXG6CatHBw==|-|--
94038395-|--|.n@ic.fbi.gov-|-MreVpEovYi7ioXG6CatHBw==|-eod date|--
116097938-|--|.-|-Tur7Wt2zH5CwIIHfjvcHKQ==|-SH?|--
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-|--|-k590@aol.com-|-9HT+kVHQfs4=-|-socialsecurity name|--
90331688-|--|-b.edu-|-nNiWEcoZTBmXrIXpAZiRHQ==|-ssn#|--
~
```

针对性攻击变得没有难度

```
jldusting@localhost:~$ grep EQ7fip cred | cut -d'|' -f5 | sort | uniq -c | sort -nr | head -n50
419496 -
53380 -lto6
23444 -numbers
14657 -123
14329 -654321
14080 -numeros
11076 -1-6
10758 -number
6888 -1
4443 -12
3959 -num
3570 -1234567
3407 -12345
3400 -123456789
3289 -??
2925 -numero
2840 -16
2509 -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

- 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

屏风

ThreatMetrix

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: SHA-512 (Unix)

Hash File: Choose File no file selected

Next »

Handshake Dictionary Delivery

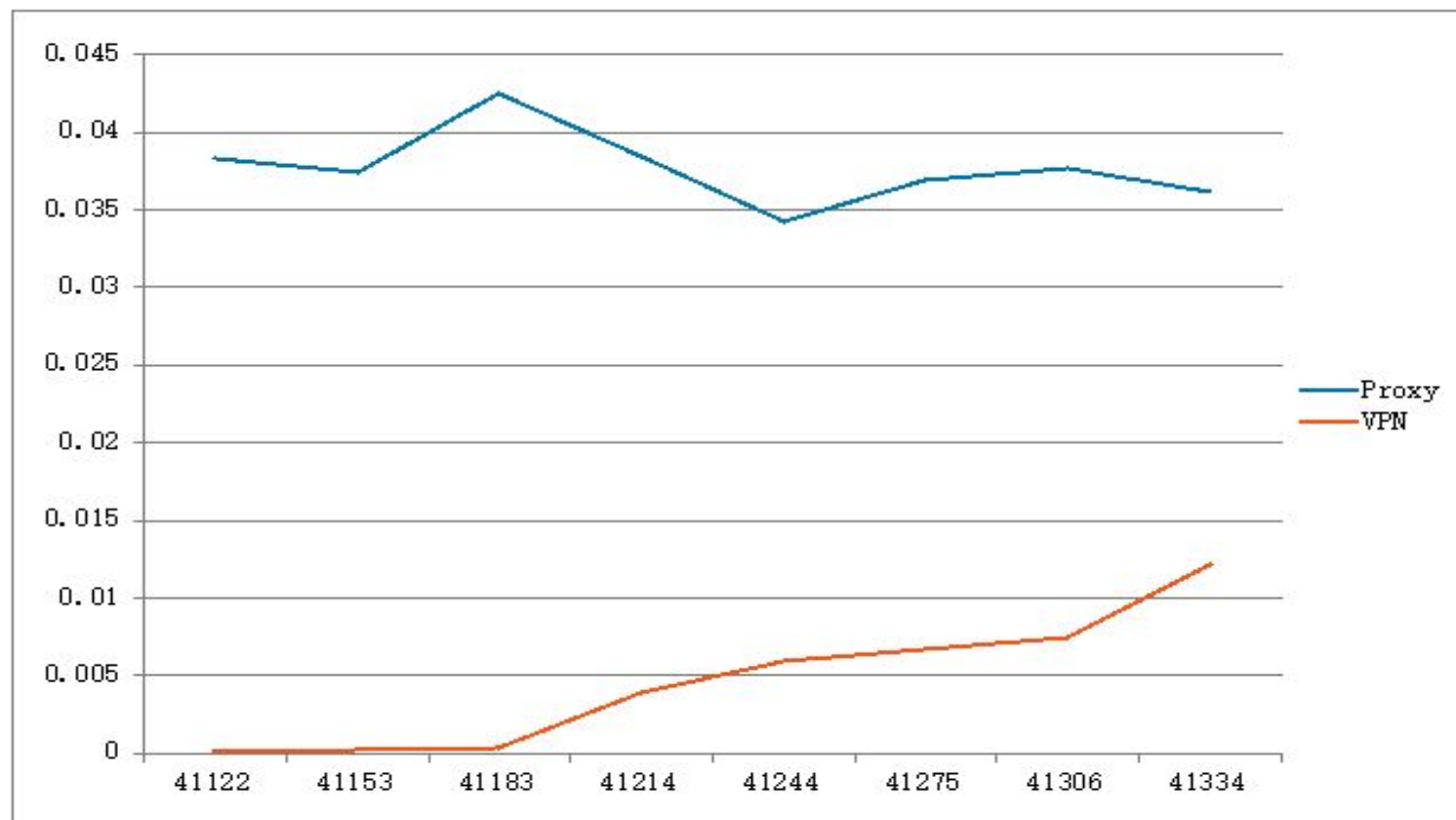
Big. Fast. Cheap.
Run your network handshake against
300,000,000 words
in 20 minutes
for \$17.

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

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

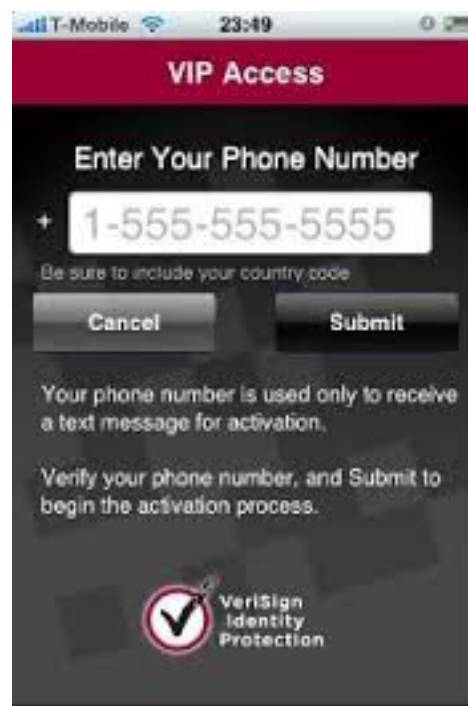
"This really is a great idea." - Hacker News

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

Bank of America | Online Banking | Enrollment - Windows Internet Explorer

https://sitekey.bankofamerica.com/sas/signon... Bank of America Corporation [US]

Bank of America Online Banking

Security Confirmation

To continue with Online Banking, please provide the information requested below.

Passcode:
(8 - 20 Characters, case sensitive)

Date of Birth (mm/dd/yyyy): / /

Social Security Number: - -

Mother's Maiden Name:

Card Number:
(16 digits, no dashes or spaces)

Card Expiration Date (mm/yyyy): /

Quick Help

What do I need to know?
We use your information, only to identify you. The information is safe and secure. No one else can access it. Entering either your SSN ensures you get access to your Bank of America accounts.

Bank of America is committed to keeping your information secure with our [Online Banking Guarantee](#).

PayPal – 正常网站

The screenshot displays the PayPal 'My Account' page. The browser address bar shows the URL: https://www.paypal.com/au/cgi-bin/webscr?cmd=_login-done&login_access=1339699250. The page features the PayPal logo and a navigation menu with tabs: My Account, Send Money, Request Money, Merchant Services, Auction Tools, and Products & Services. Below the navigation menu, there are sub-tabs: Overview, Add Funds, Withdraw, History, Resolution Centre, and Profile. The main content area welcomes the user, Andreas Baumhof, and displays account details: Account Type: Personal, Upgrade, Status: Verified, and Account Limits: View Limits. A prominent green banner encourages the user to 'LOSE THE PLASTIC, KEEP THE POINTS' with a 'PAY HAPPY' button. The PayPal balance is shown as \$0.00 AUD. A table lists the available balance in AUD (primary) and the total balance converted to AUD. The table has two columns: Currency and Total.

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

Below the table, there is a section for 'My recent activity' with links for 'Payments received', 'Payments sent', and 'View all my transactions'. The 'My recent activity' section shows the last seven days (8 Jun 2012-15 Jun 2012) and includes a table with columns: Date, Type, Name/Email, Payment status, Details, Order status/Actions, and Gross. A 'Payment status glossary' link is also present. On the right side, there is a 'Notifications' section with a link to 'Policy Updates' and a 'HAPPY TIP' section with a 'Find out more' link.

PayPal – 帶有 Zeus Trojan

The screenshot shows a web browser window displaying the PayPal 'My Account' page. A modal window is overlaid in the center, titled 'Welcome, Andreas Baumhof. Verify Your Identity'. The modal contains a message: 'In order to maintain higher security standards with our customers, we carry out selective personal information verification. To authorize in the system, please confirm following information:'. Below the message are four input fields: 'Credit Card', 'CVV', 'PIN', and 'Expiration Date'. The 'Expiration Date' field is set to '1 / 2011'. A 'Continue' button is at the bottom of the modal. The background page shows the PayPal logo, navigation tabs, account balance (\$0.00 AUD), and a table of recent activity.






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

Date	Type	Name/Email	Payment status	Details	Order status/Actions	Gross
My recent activity - Last seven days (6 Jun 2012-13 Jun 2012)						


Macys – 正常网站

Shopping Bag - Shopping Bag x

www1.macys.com/bag/index.ognc?CategoryID=7502&cm_sp=atlayer-_checkout-_n



the magic of **macys**  WE NOW SHIP TO OVER 100 COUNTRIES! [learn more](#)    sign in | my account | customer service shopping bag (1) 

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

SEARCH GO  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. remove	Sale \$159.99 Reg. \$400.00	1 	\$159.99

HAVE A PROMO CODE? [find one now](#)

[APPLY](#)
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:		FREE
Estimated Taxes (6%):	\$	9.60
Total:	\$	169.59

[CONTINUE SHOPPING](#) [CONTINUE CHECKOUT](#)

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](#)



Macys – 帶有 Zeus Trojan

The screenshot shows a web browser window with the URL `www1.macys.com/bag/index.ognc?CategoryID=7502&cm_sp=atblayer-_checkout-_n`. The page is titled "Shopping Bag - Shopping Bag". The Macy's logo is visible, along with a promotional banner for "EXTRA 20% OR 15% OFF" with the promo code "SUMMER". A shopping bag icon indicates 0 items. Navigation links include "for the home", "bed & bath", "women", "accessories", "jewelry & watches", "sale", "GIFT CARDS", and "WEDDING REGISTRY". A search bar is present with the placeholder text "Keyword, Web ID".

A security verification modal is displayed in the center of the screen. It features the Macy's logo and the following text: "IN ORDER TO PROVIDE YOU WITH EXTRA SECURITY, WE OCCASIONALLY NEED TO ASK FOR ADDITIONAL INFORMATION WHEN YOU ACCESS YOUR ACCOUNT ONLINE. PLEASE ENTER THE INFORMATION BELOW TO CONTINUE:". The modal contains several input fields:

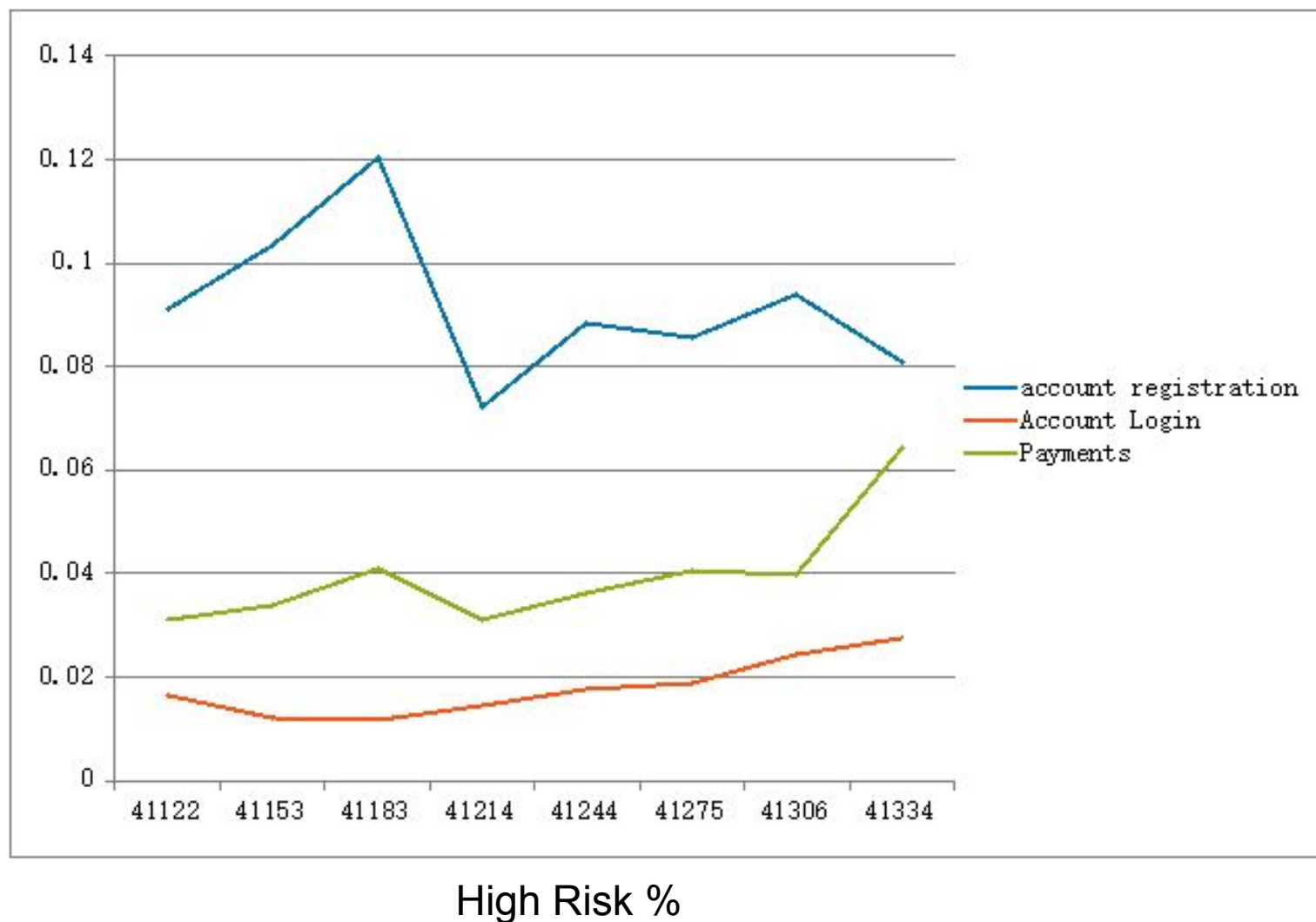
- MACY'S CARD NUMBER: (16 DIGIT \$) [Input field]
- EXP. DATE: (MM/YYYY) [Input field]
- CVV CODE: (3-4 DIGIT \$) [Input field]
- SOCIAL SECURITY NUMBER: (9 DIGIT \$) [Input field]
- MOTHER'S MAIDEN NAME: [Input field]
- DATE OF BIRTH: (MM/DD/YYYY) [Input field]

At the bottom of the modal, there is a "VERIFY" button. Below the modal, there are two buttons: "CONTINUE SHOPPING" and "CONTINUE CHECKOUT".

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

MALWARE

- > 设备
- > 身份
- > 行为
- > 威胁

横跨数以千计客户的 实时环球数据分析

屏风
ThreatMetrix™



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™

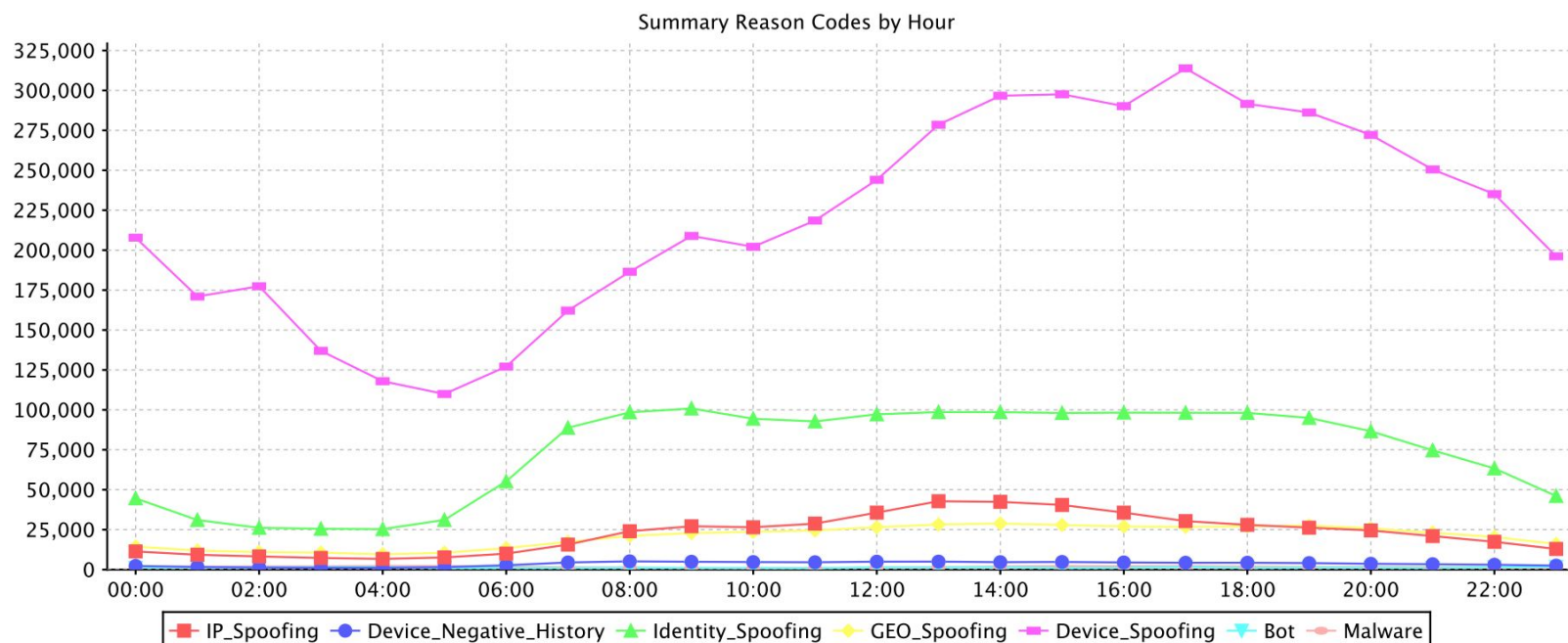


网络罪案的攻击维度 — 案例

Summary Reason Overview

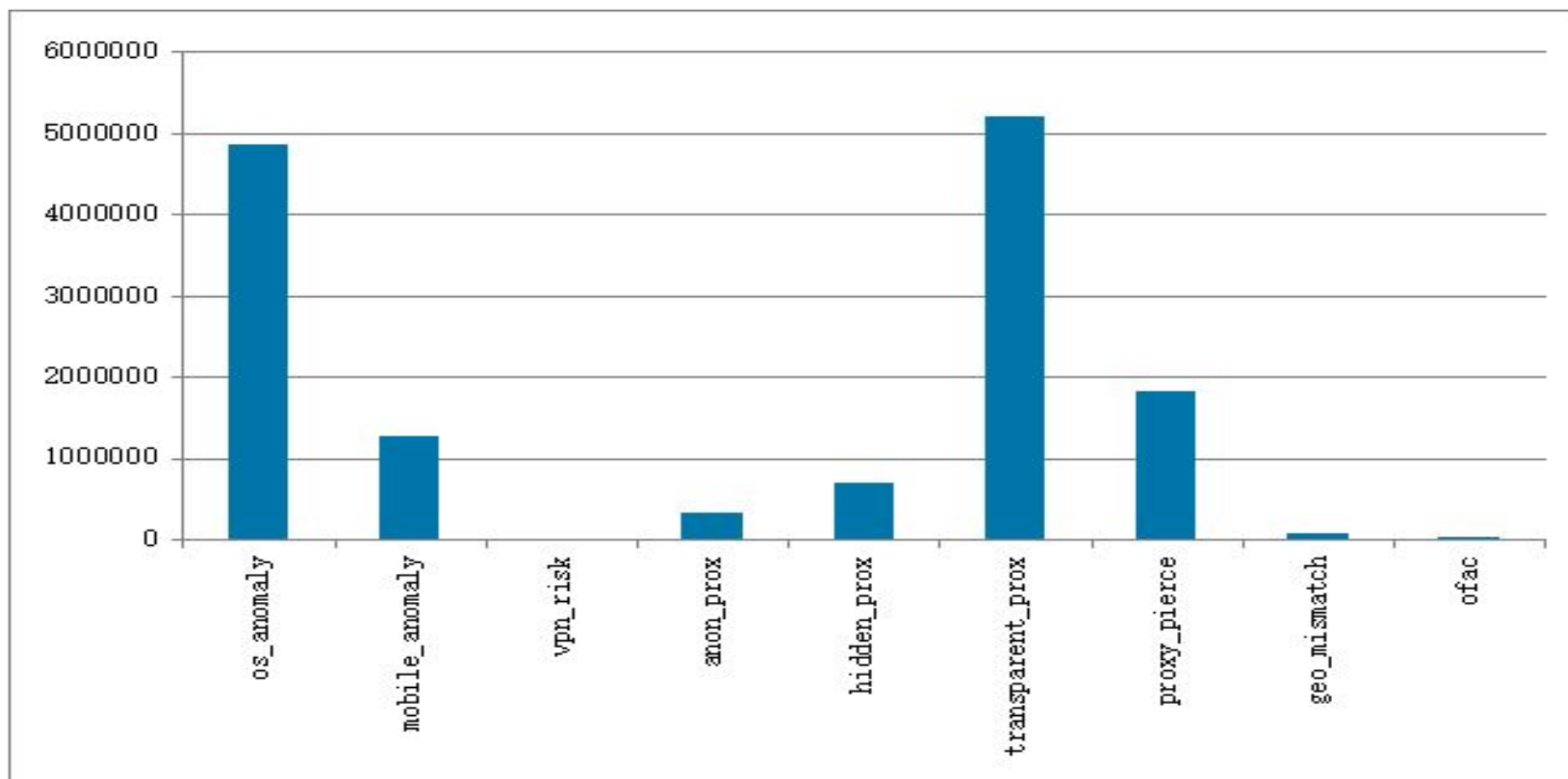
Past day from 2013-11-07

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%

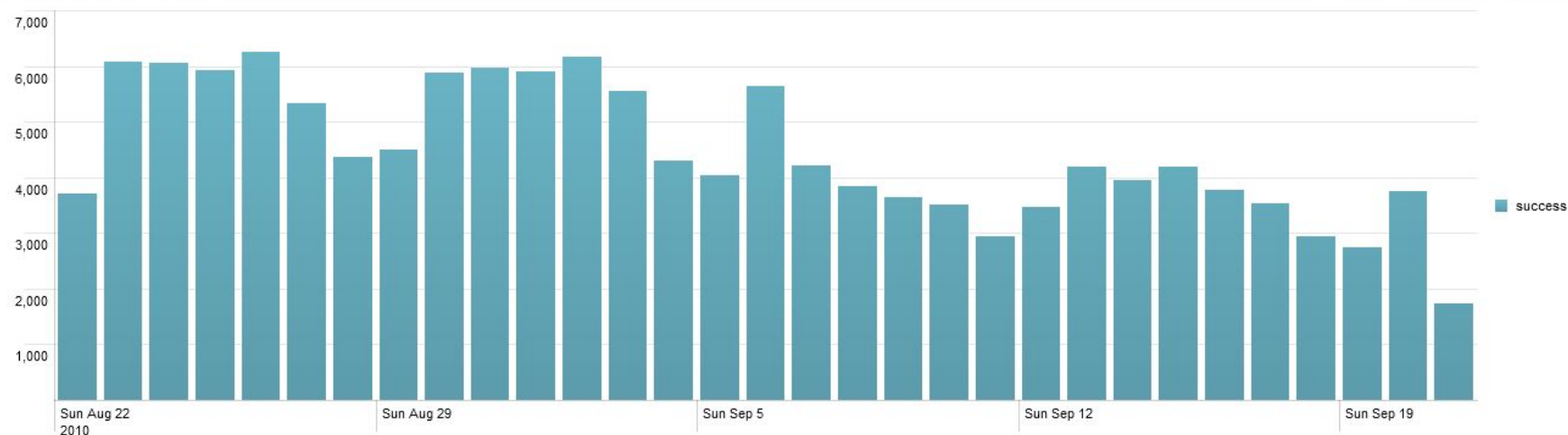


其中两个金融客户的例子

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

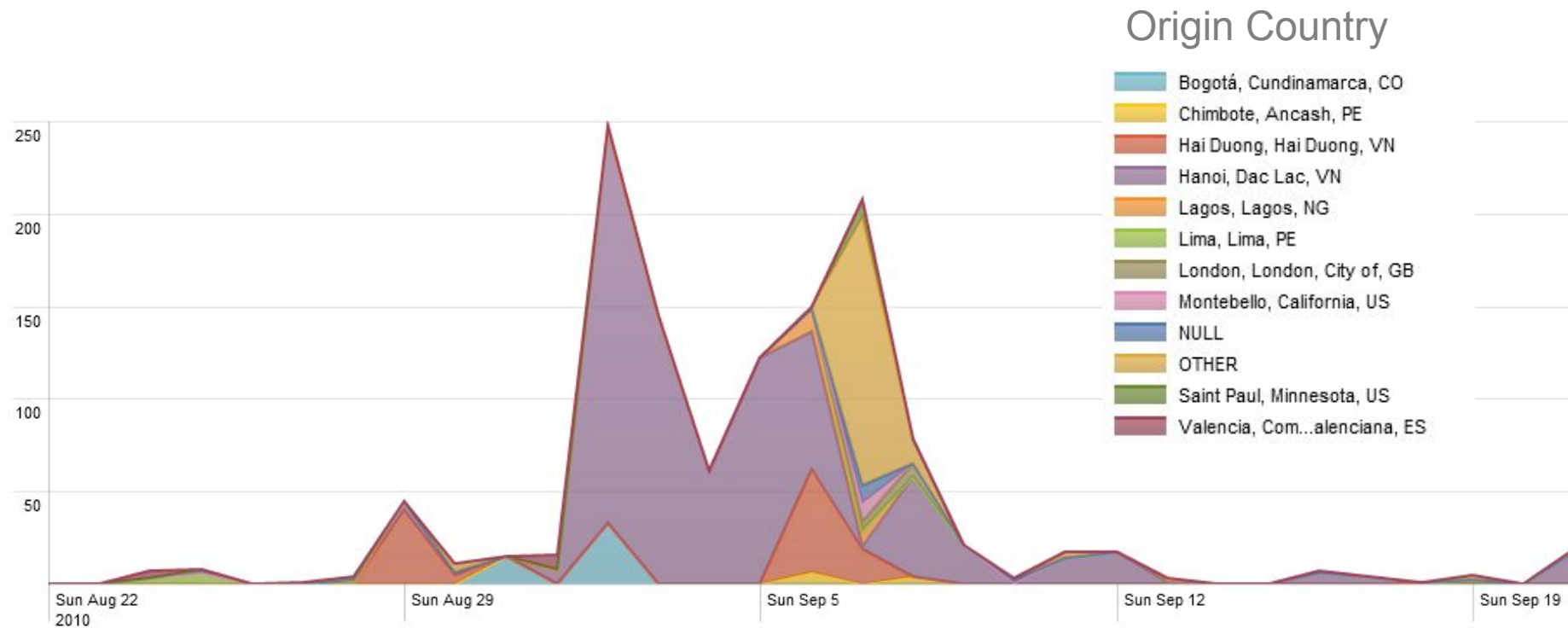
802 0.581%

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

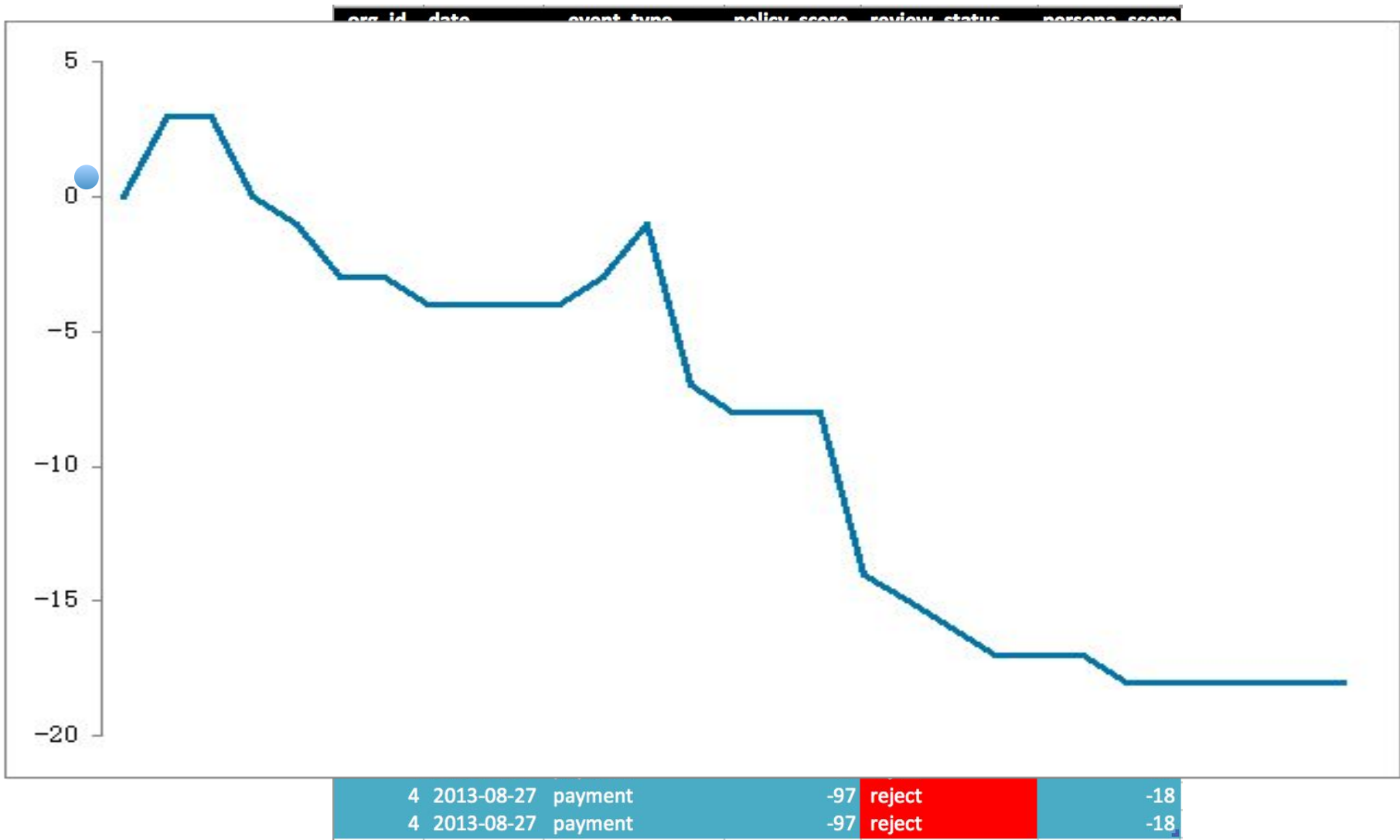
Honeypot Result: mismatch_black

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 %
Total:	23		

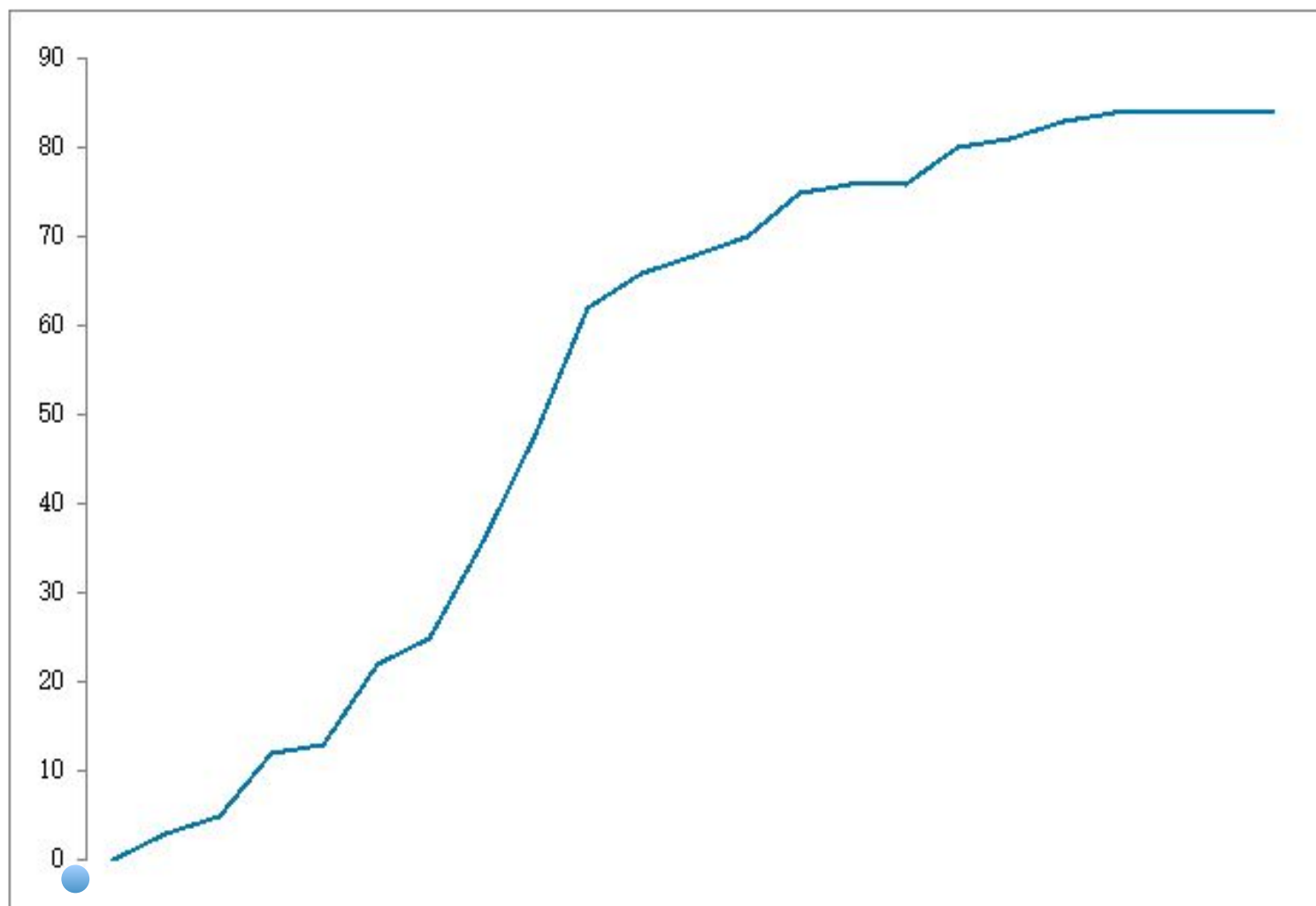
异常情况检测案例

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



基于环球行为的声誉评级







The Global Trust Intelligence Network



Questions

jma@threatmetrix.com +86-18601077772 +852-64649215

Jackal Ma 马骏驱

www.threatmetrix.com +1.408.200.5700

sales@threatmetrix.com