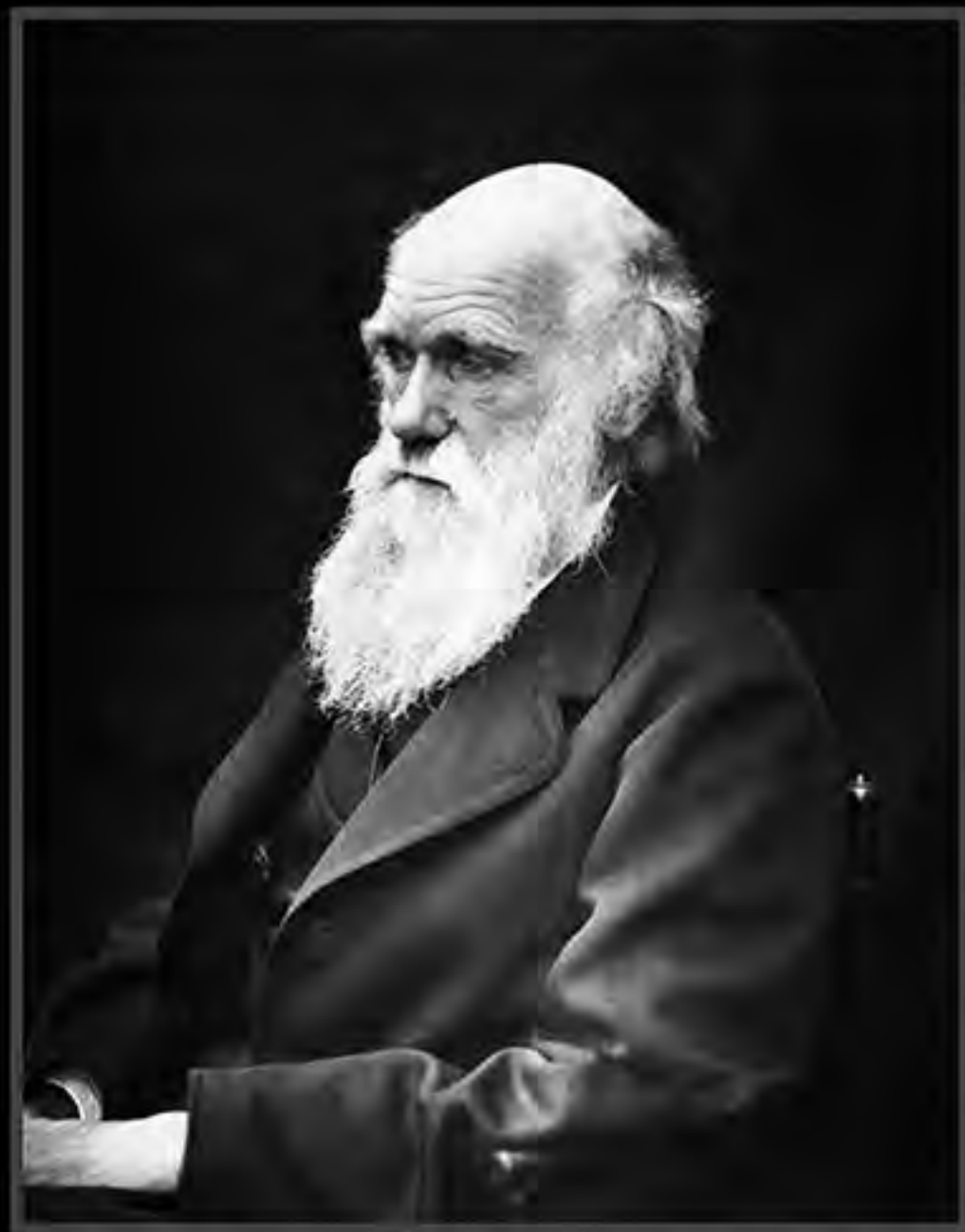


# HTTPS时代

从HTTP到HTTPS的进化



















感谢你！

HTTP

帶我們進入互聯網世界

你的进化带动了互联网的进化.....



# HTTP → HTTPS



1960年, Ted Nelson  
HTTP 之父



1994年  
创建HTTPS



如果不进化？

# HTTP



数据裸奔！



```
username=demo&password=demo123HTTP/1.1 200 OK
Date: Fri, 19 Jun 2015 09:05:30 GMT
Server: Apache/2.2.15 (CentOS)
Last-Modified: Fri, 19 Jun 2015 09:02:24 GMT
ETag: "22996-139-518db2eb7492d"
Accept-Ranges: bytes
Content-Length: 313
Connection: close
Content-Type: text/html; charset=UTF-8

<table border="userinfo">
```



如果不进化？

# HTTP



您的账户异常，请及时登录确认，以免损失

[http://www.tenpay.com/v2/trade/bank\\_deduction.shtml?ADTAG=TENPAY\\_V2.NAV.TOP\\_RIGHT.HELP\\_QUERY](http://www.tenpay.com/v2/trade/bank_deduction.shtml?ADTAG=TENPAY_V2.NAV.TOP_RIGHT.HELP_QUERY)

您的账户异常，请及时登录确认，以免损失

[http://www.tenpay.com.imagedetail.jm2dx9mhpv.html.com/v2/trade/bank\\_deduction.shtml?ADTAG=TENPAY\\_V2.NAV.TOP\\_RIGHT.HELP\\_QUERY](http://www.tenpay.com.imagedetail.jm2dx9mhpv.html.com/v2/trade/bank_deduction.shtml?ADTAG=TENPAY_V2.NAV.TOP_RIGHT.HELP_QUERY)

防不胜防的钓鱼网站！





如果不进化？

# HTTP

FREE  
Wi-Fi

Normal Flow



Man-in-the-Middle Flow



无声无息的中间人攻击！



为什么很安全

HTTPS



# HTTP

- 明文传输
- 无法验证网站身份
- 无法保证传输数据的完整性

# HTTPS

- 加密传输（保密性）
- 可以验证网站身份（唯一性）
- 保证传输数据的完整性

验证身份的数字证书

SECURITY



HTTPS

非对称加密

RSA

37年



# HTTPS

非对称加密

# RSA

RSA目前主流的密钥长度

RSA	ECC
2048	224
3072	256
7680	384

# ECC



安全

# HTTPS

同等加密强度条件

- 级别高的数字证书

具备保密性的数字证书

身份唯一性

确保数据完整性

显著可视的安全特征

不安全

# HTTPS

- 级别低的数字证书

仅具备保密性的数字证书

- 不可信的证书

- 非认可自签发证书

• 人为原因





真正安全的

HTTPS



需要解决一些问题  
才是真正安全的

# HTTPS

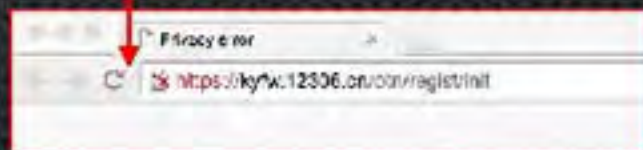
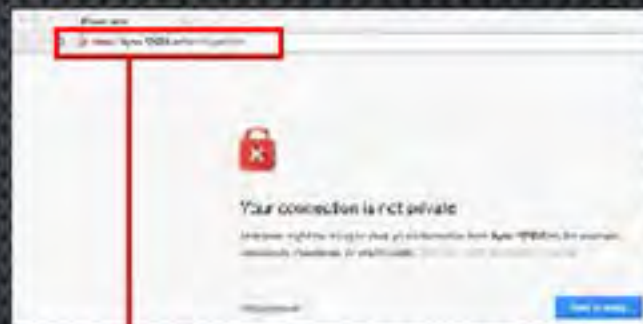
DNS解析异常  
连接主机超时  
与主机会话异常(通信超时 或 通信中断)

SSL 证书不可信  
SSL 证书是自签名证书  
SSL 使用了弱签名算法的证书  
SSL 使用了低加密强度的证书  
SSL 证书是为其他网站地址颁发的  
SSL 使用了不安全的会话协议  
SSL 使用了不安全的加密套件  
SSL 证书指纹不匹配

SSL 证书时间无效  
SSL 证书即将到期  
SSL 证书被吊销  
SSL 证书链不完整

SSL 页面包含不安全的外链  
SSL 页面未强制使用HTTPS

SSL 存在Heartbleed漏洞  
SSL 存在OpenSSL CCS漏洞  
SSL 存在POODLE漏洞





谁需要

HTTPS







HTTPS

必然性



**Secure** https://

2014.08

优先收录和排名HTTPS  
建议使用2048位  
及以上加密的证书

The screenshot shows a Google search results page for the keyword '登录' (Login). The browser's address bar shows a secure HTTPS connection. The search results list several login pages, with green boxes and arrows highlighting the secure ones.

**登录 - Google 帐户**  
<https://accounts.google.com/login?hl=zh-CN>  
 使用您的Google 帐户登录。电子邮件 密码 保持登录状态。为了...  
 框。如果您的设备有多人共用，建议您采取其他防范措施。

**登录 - 腾讯企业邮箱**  
<https://exmail.qq.com/login>  
 登录腾讯企业邮箱，请填写完整邮件地址，或管理员帐号。支...  
 Foxmail，无需设置，极速收发。

**支付宝: 登录**  
<https://my.alipay.com/>  
 欢迎登录支付宝。支付宝-全球领先的独立第三方支付平台，支...  
 速的电子支付/网上支付/安全支付/手机支付体验以及便捷收...

**登录豆瓣**  
<https://www.douban.com/website/login>  
 手机扫码登录，帐号、密码，下次自动登录(忘记密码?) 忘记密码?>  
 点击下载豆瓣移动应用。©2005-2015 douban.com, all rights reserved...

**登录百度账号**  
<https://passport.baidu.com/>  
 登录百度帐号。2015 Baidu.

**163网易企业邮箱-中文邮箱第一品牌**  
[mail.163.com/](http://mail.163.com/)  
 为商务设计，二极码登录，邮箱帐号登录... 邮箱帐号/手机号码，密码，均可登录... 1天内...  
 免登录，为了您的信息安全，请不要在网吧或公用电脑上使用此功能！



Secure https://

2015.05

优先收录HTTPS





# HTTPS

# 全站必要性



HTTPS

The screenshot shows a web browser displaying the TRUSTAsia website. The browser's address bar shows the URL <https://www.trustasia.com>. The website header includes the TRUSTAsia logo, Symantec Website Security Platinum Partner logo, Norton Secured logo, a phone number 400 880 8600, and a chat button labeled "在线客服". The navigation menu includes links for 首页 (Home), 数字证书 (Digital Certificates), 产品方案 (Product Solutions), 渠道合作 (Channel Partners), 客户服务 (Customer Service), SSL工具 (SSL Tools), and 关于我们 (About Us). The main content area features the title "SSL云监控服务, SSL Cloud™ 强大的分布式云监控" (SSL Cloud Monitoring Service, SSL Cloud™ Powerful Distributed Cloud Monitoring). Below the title, there are four bullet points: "全球多点跨区跨运营商分布式云监控" (Global multi-point, cross-region, cross-operator distributed cloud monitoring), "多DNS轮询、多台服务器负载均衡" (Multiple DNS round-robin, multiple server load balancing), "深度SSL综合检测(这是业内独有)" (Deep SSL comprehensive detection (this is unique in the industry)), and "7\*24小时全天候告警" (7\*24 hours all-day alarm). At the bottom of the main content area, there is a link "SSL Cloud 入口" (SSL Cloud Entry) with a downward arrow icon and a button "了解更多" (Learn More). To the right of the text, there is a circular diagram with icons representing various aspects of the service: a cloud with servers, a network diagram, a download icon, a heart rate monitor, a location pin, and a magnifying glass.

SSL云监控服务, SSL Cloud™ 强大的分布式云监控

- 全球多点跨区跨运营商分布式云监控
- 多DNS轮询、多台服务器负载均衡
- 深度SSL综合检测(这是业内独有)
- 7\*24小时全天候告警

SSL Cloud 入口 了解更多



HTTPS

市场数据



# HTTPS

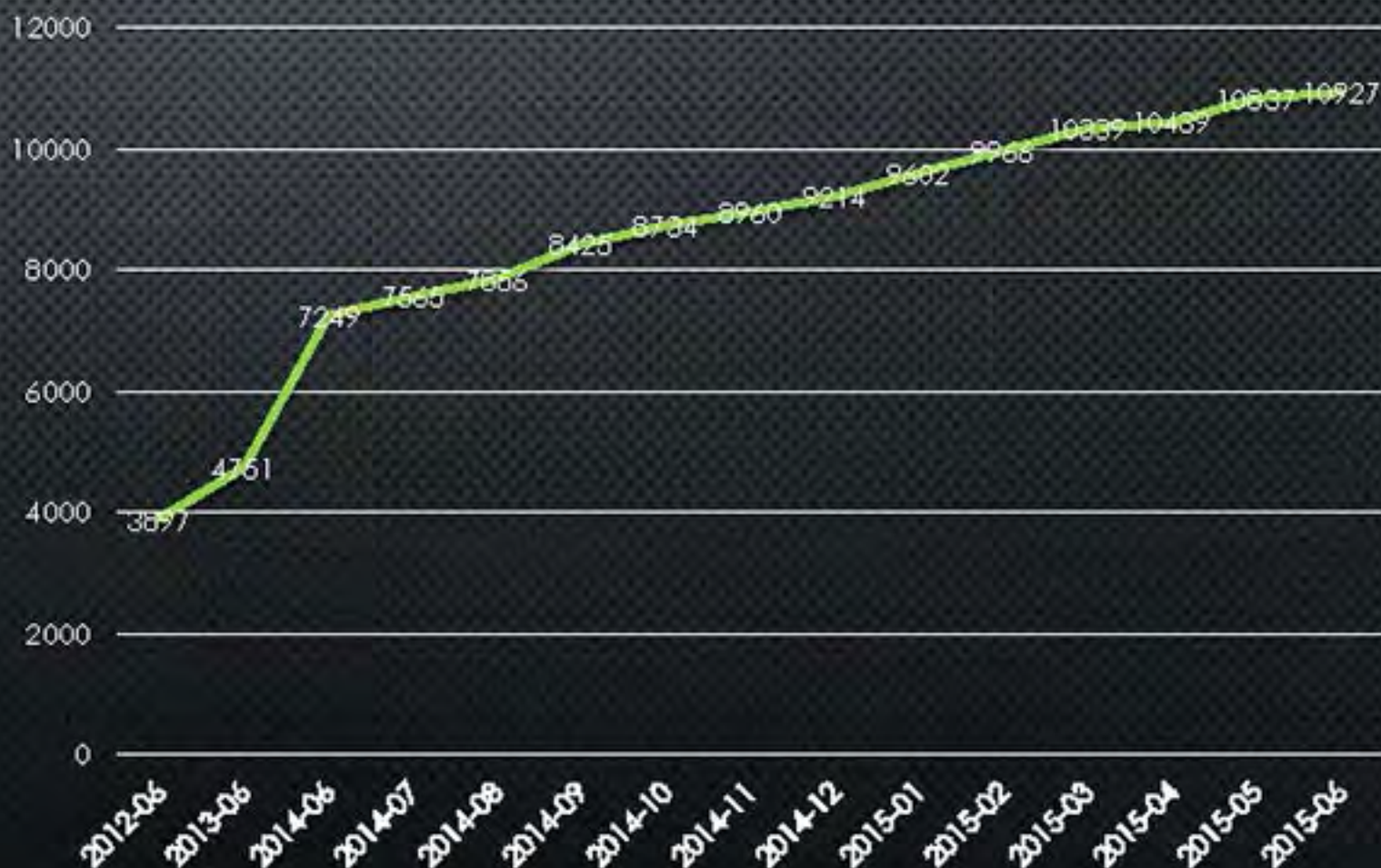
中国3年增长

2.8倍

## 中国数字证书增长 2012年~2015年

数据不包含：

- 不验证身份的证书（域名型证书）
- 自签发证书
- 无效证书





# HTTPS

## 各品牌数字证书在中国的市场占有率 数据截止2015.06

数据不包含：

- 不验证身份的证书（域名型证书）
- 自签发证书
- 无效证书

# TOP1



■ Symantec ■ WoSign ■ GlobalSign ■ DigiCert

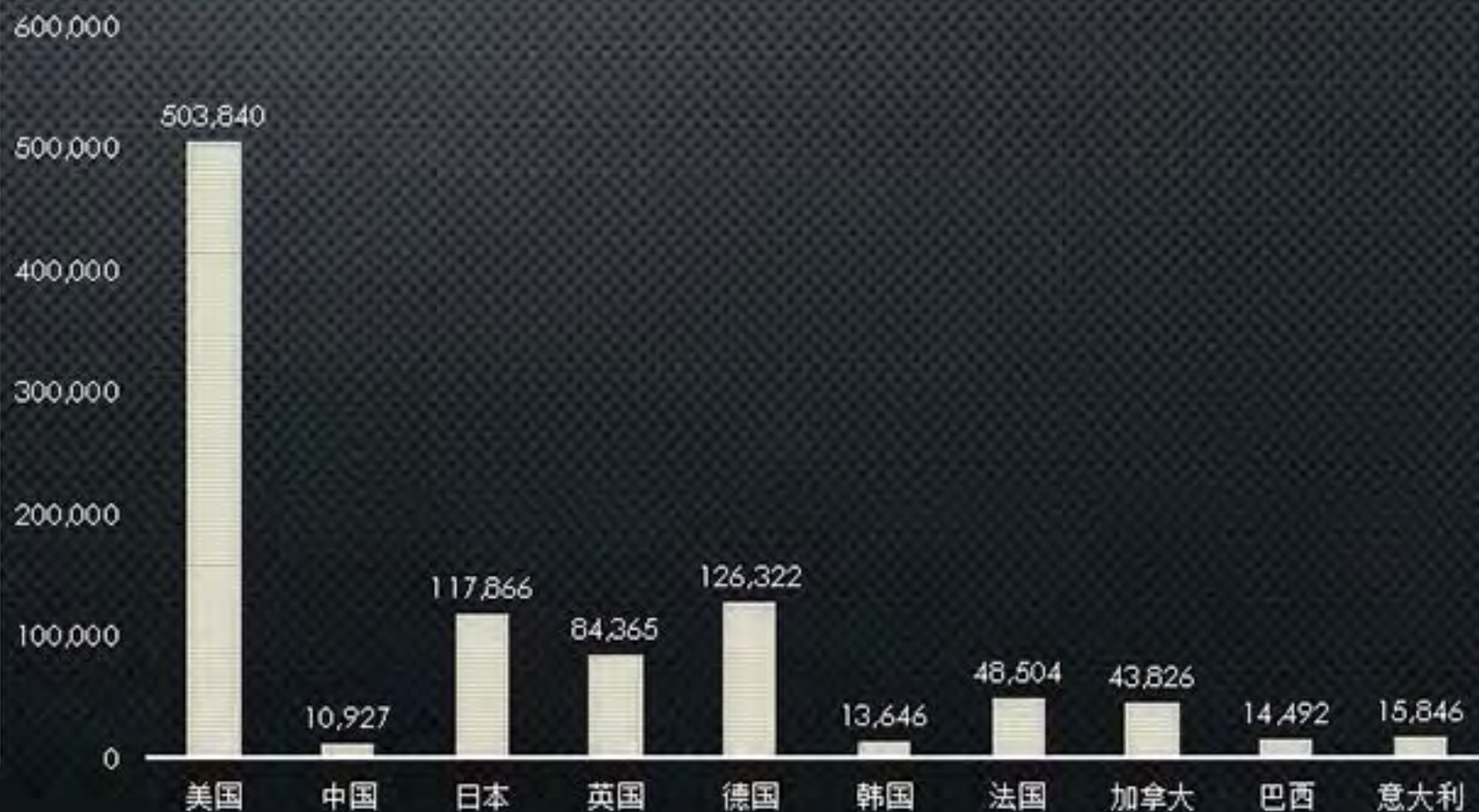


# HTTPS

## 中国与世界其他国家对比 数据截止2015.06

数据不包含：

- 不验证身份的证书（域名型证书）
- 自签发证书
- 无效证书





# HTTPS

## 中国域名数量与已经部署数字证书域名对比 数据截止2015.06

数据不包含：

- 不验证身份的证书（域名型证书）
- 自签发证书
- 无效证书

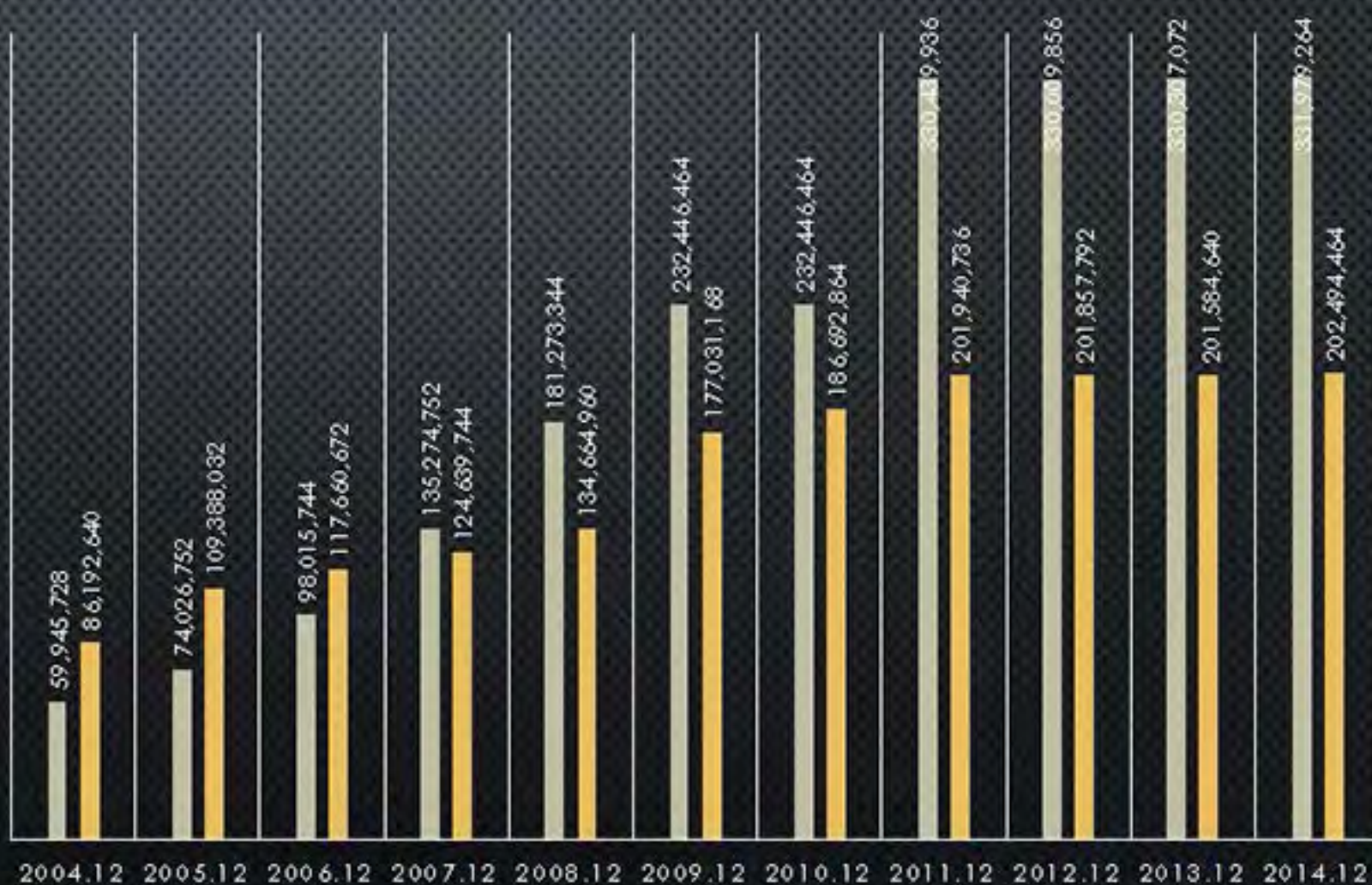




# IP

## 中国10年的IP增长与对比 数据截止2014.12

中国IP数量  
日本IP数量







7号展位



# 谢谢！



市场部

DERICKXU@TRUSTASIA.COM

400 880 8600

WWW.TRUSTASIA.COM