RSAConference2015

Abu Dhabi | 4–5 November | Emirates Palace

SESSION ID: **CCT-W06**

Global & Regional Trends in Cybercrime & the Divergence of Cybercriminals

Bilal Baig

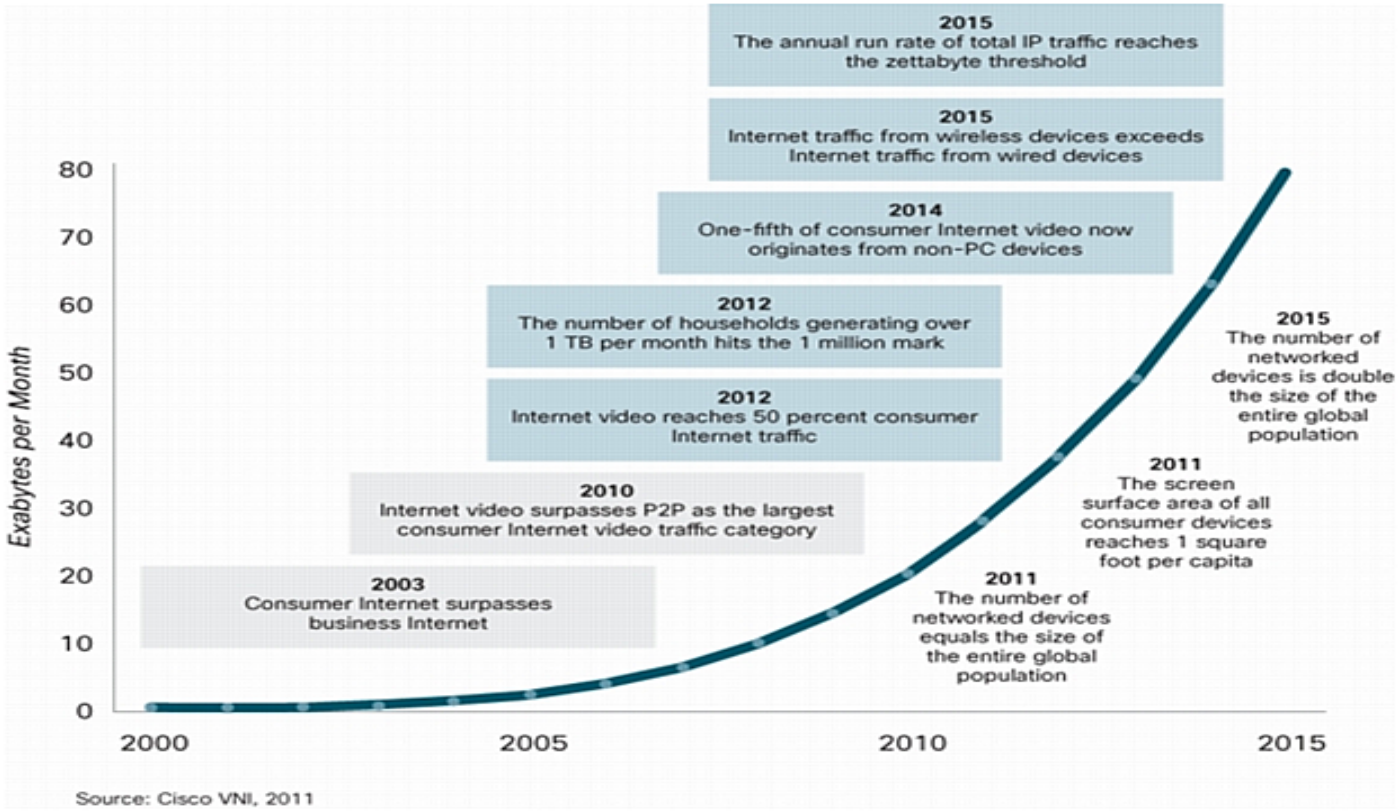
Technical Director. Middle East, Med, Africa & Russia
Trend Micro

#RSAC

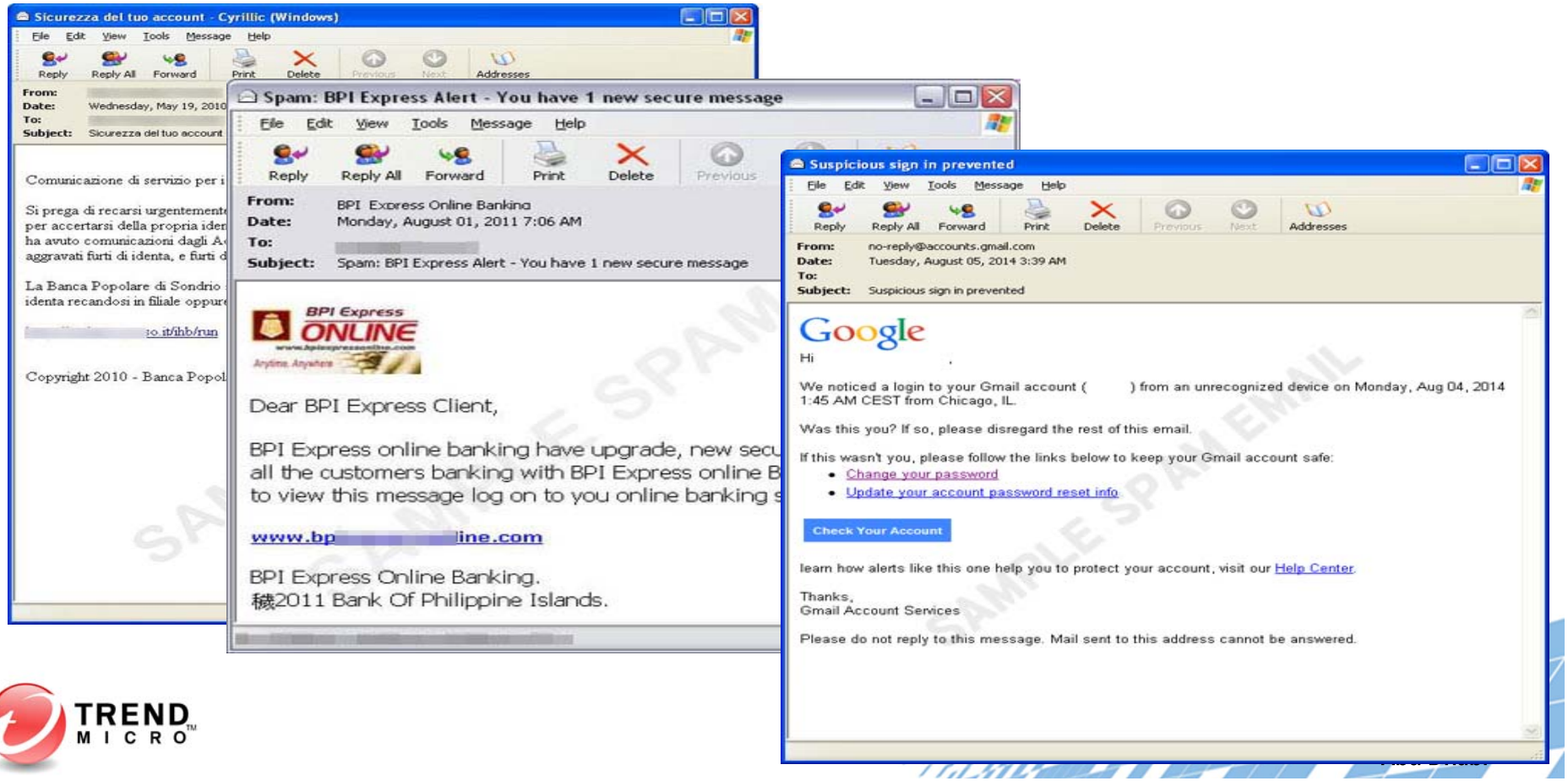
"Study the past if you would define the future."

Confucius

Figure 1. Five Traffic Milestones and Three Traffic Generator Milestones by 2015

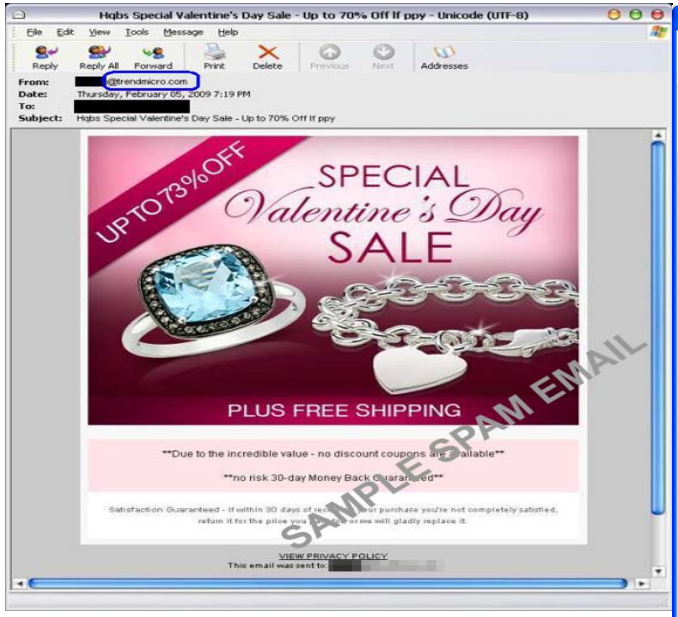


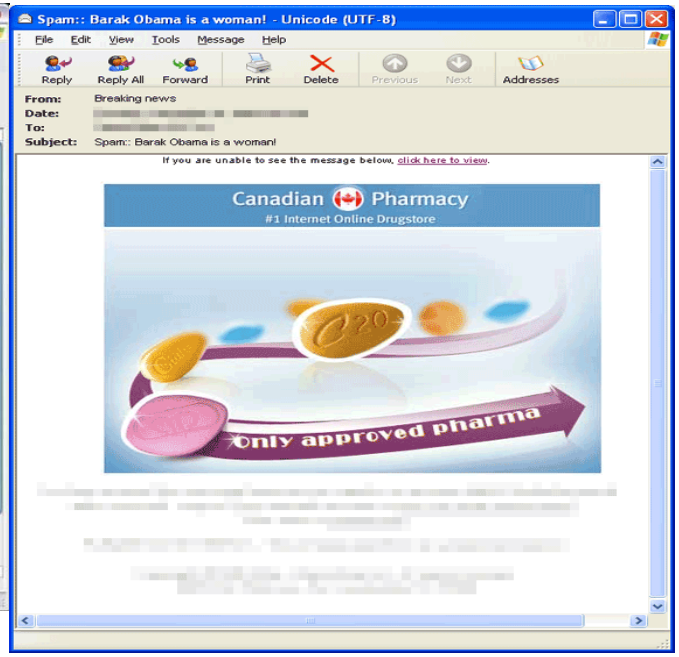
Cybercrime – Early 2000 – Till Now Phishing



TREND MICRO

Spam


Hqbs Special Valentine's Day Sale - Up to 70% Off If ppy - Unicode (UTF-8)
File Edit View Tools Message Help
Reply Reply All Forward Print Delete Previous Next Addresses
From: @trendmicro.com
Date: Thursday, February 05, 2009 7:19 PM
To:
Subject: Hqbs Special Valentine's Day Sale - Up to 70% Off If ppy
UPTO 73%OFF
SPECIAL
Valentine's Day
SALE
PLUS FREE SHIPPING
Due to the incredible value - no discount coupons are available
no risk 30-day Money Back Guaranteed
VIEW PRIVACY POLICY
SAMPLE SPAM EMAIL


Spam:: Barak Obama is a woman! - Unicode (UTF-8)
File Edit View Tools Message Help
Reply Reply All Forward Print Delete Previous Next Addresses
From: Breaking news
Date:
To:
Subject: Spam:: Barak Obama is a woman!
If you are unable to see the message below, click here to view.
Canadian Pharmacy
#1 Internet Online Drugstore
Only approved pharma

Email Based Cybercrime (2000s)

- Uses relevant medium at that time

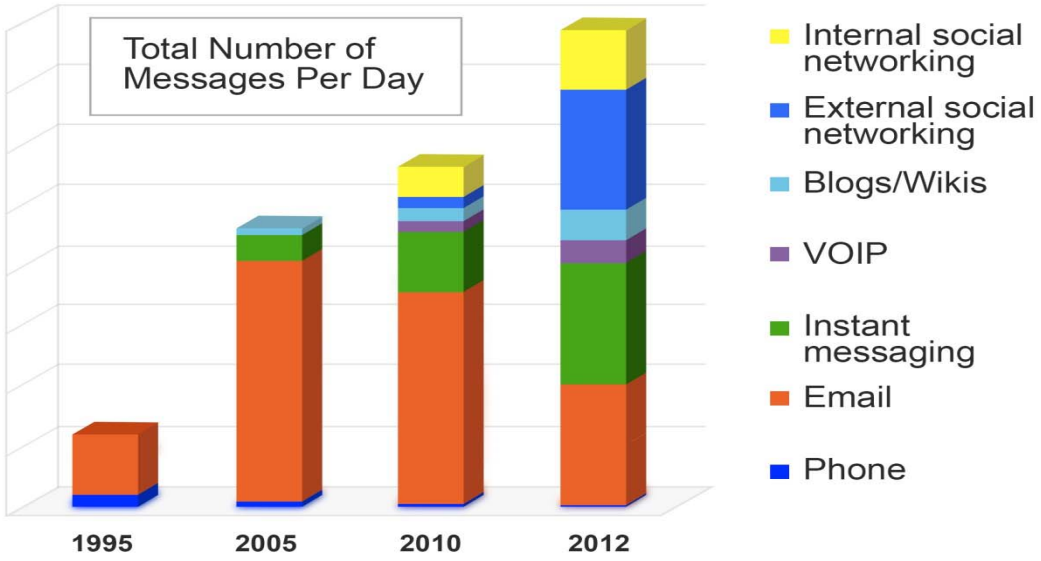
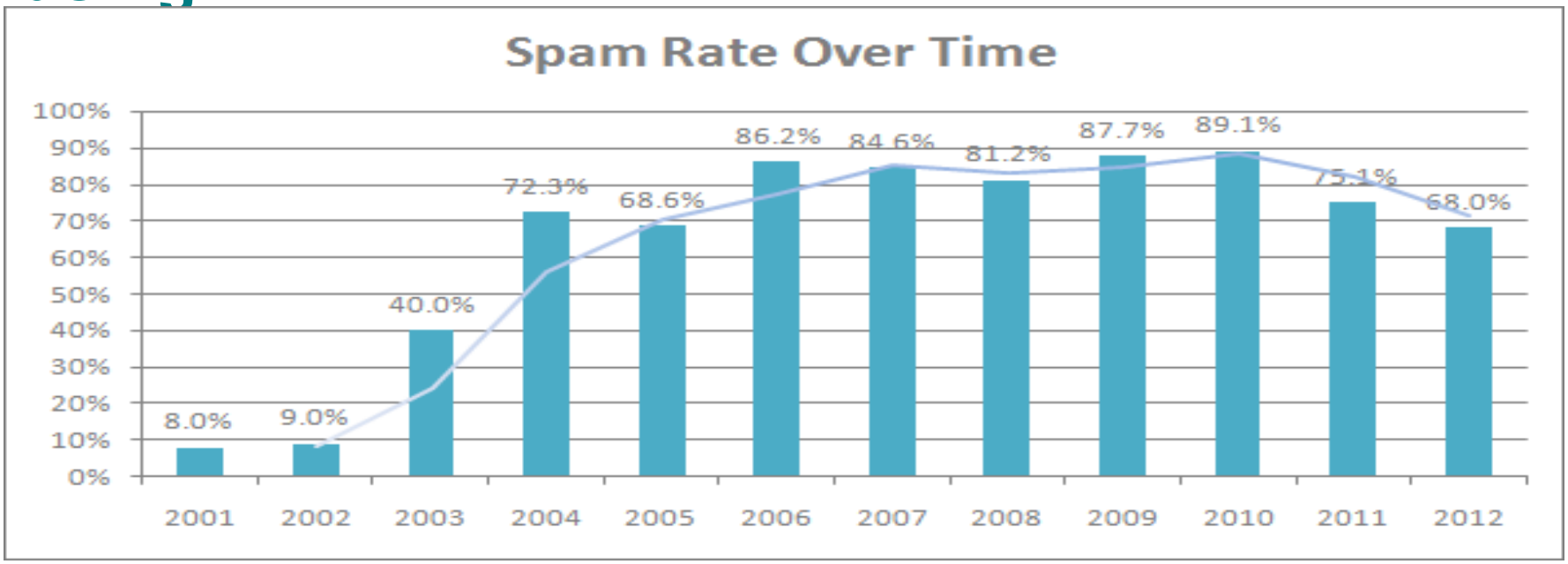


Image source: http://www.novaspivack.com/uncategorized/drowning-in-the-stream-new-challenges

Cybercriminals Target what the users are using

#RSAC

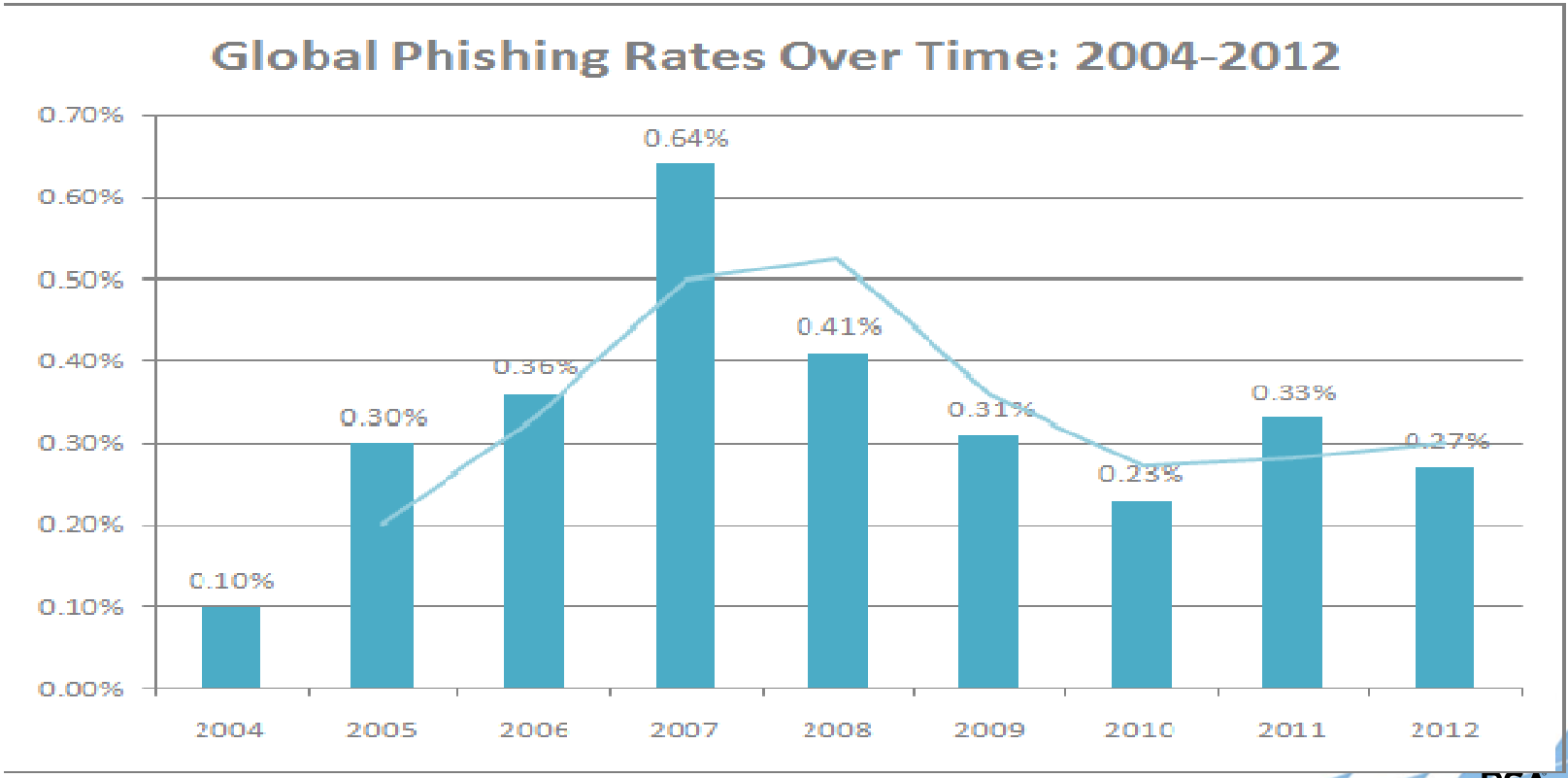


Source: http://www.emailtray.com/blog/email-spam-trends-2001-2012/

TREND MICRO

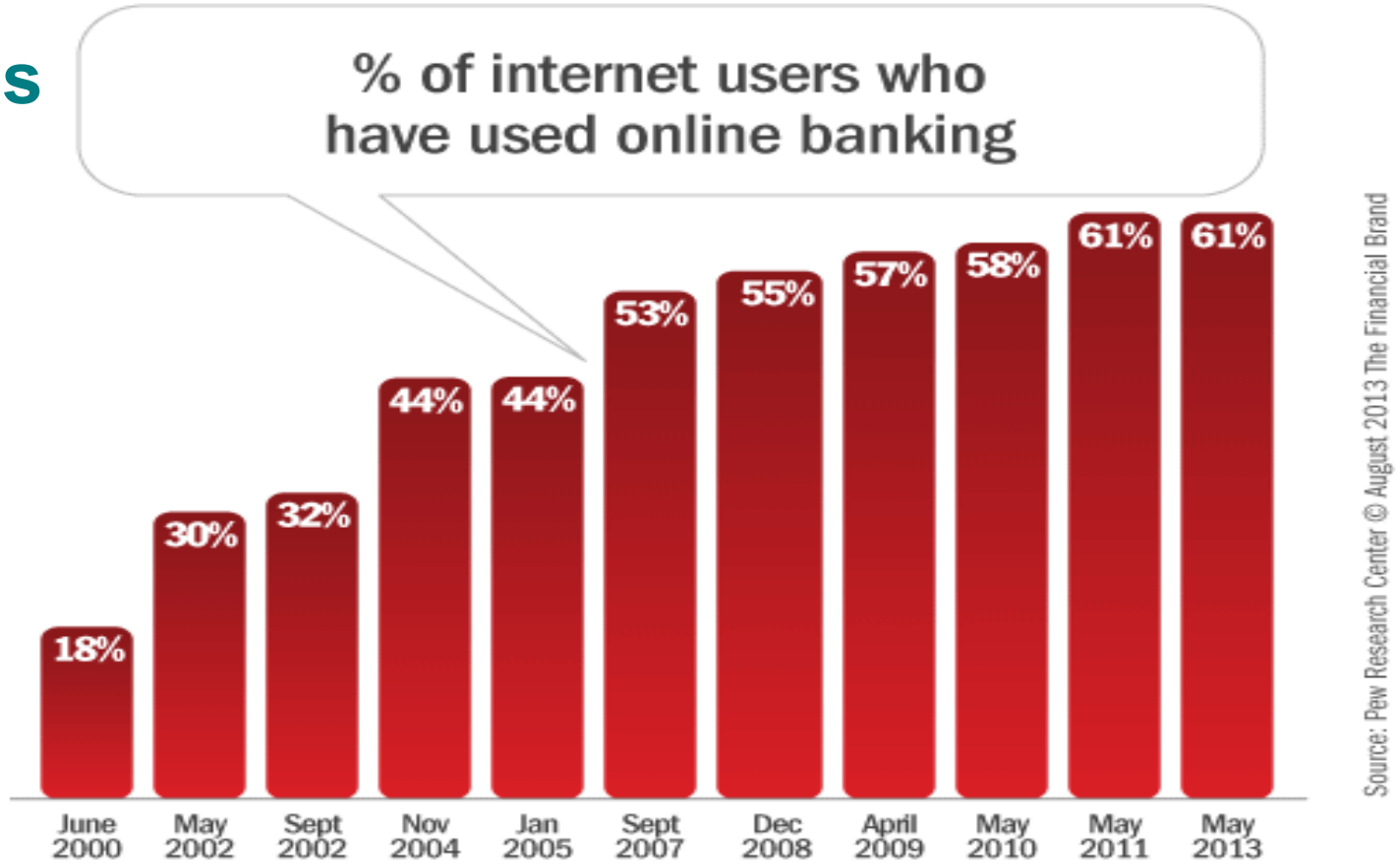
RSA Conference 2015 Abu Dhabi

2000's



Source: http://www.emailtray.com/blog/email-phishing-activity-over-time-2004-2012-in-figures/

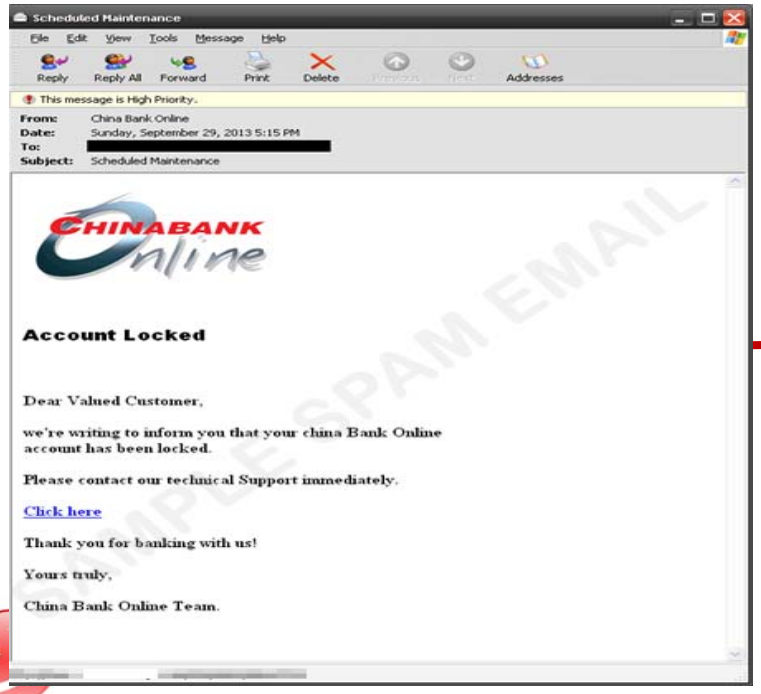
2000's

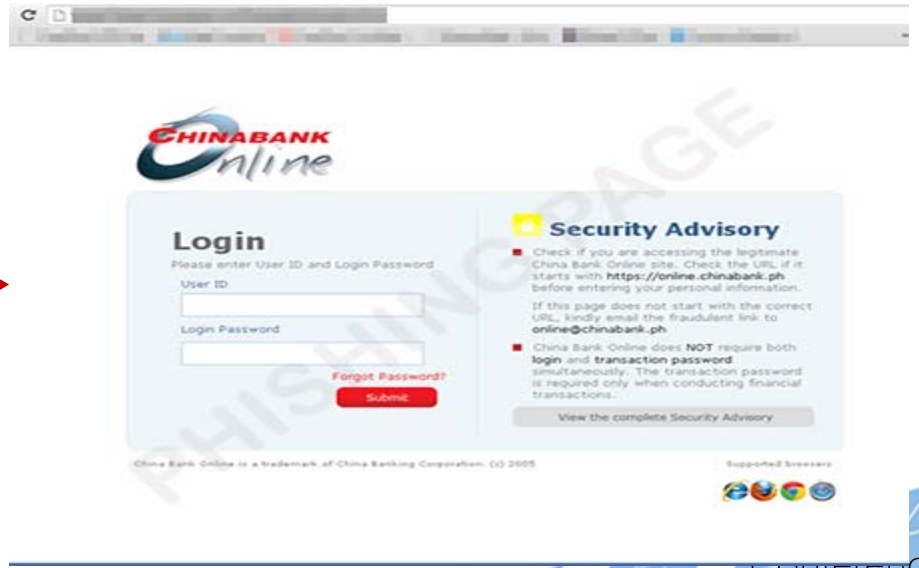


Source: http://www.huffingtonpost.com/casey-bond/afraid-to-try-an-online-banking_b_4613428.html

Email Based Cybercrime (2000s)

- Defeats security measures back then





Key Points

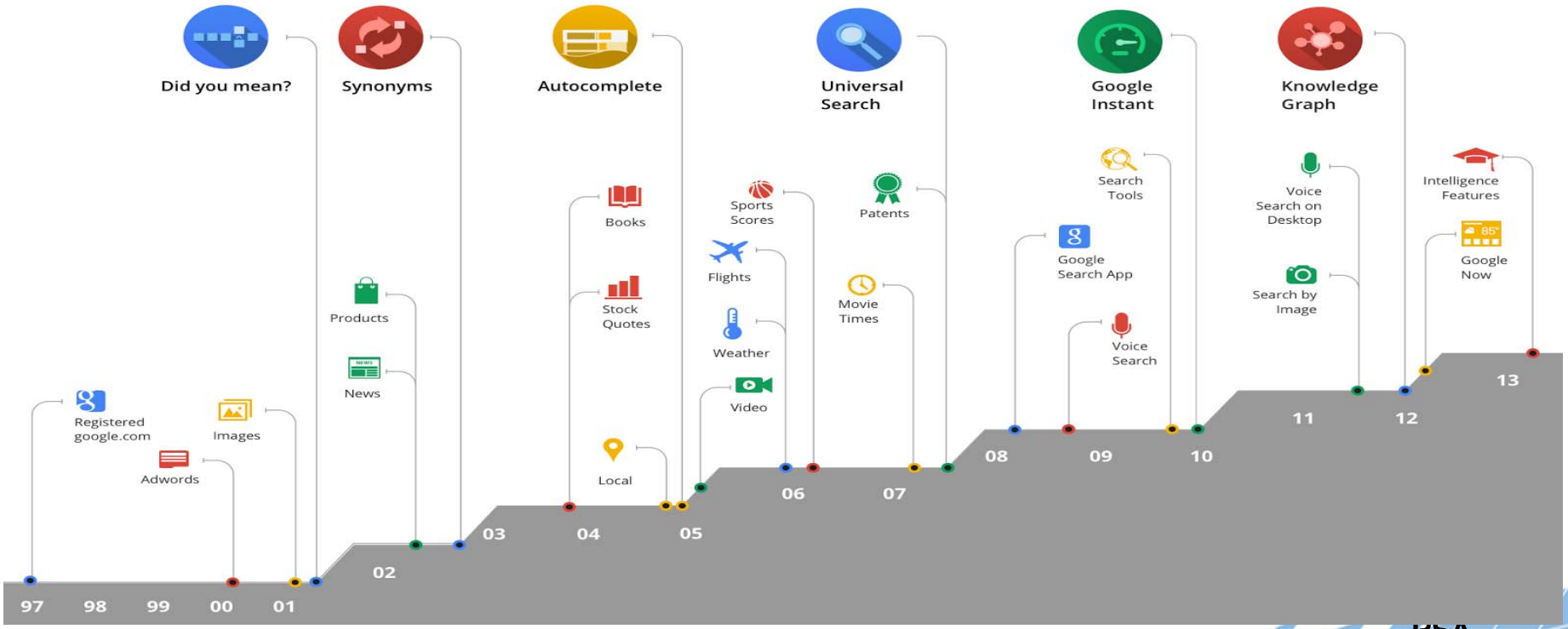
- Where the money is…
  - Phishing
  - Fraud
- Where the people are…
  - Email -> Spam
- Low hanging fruits…
  - Online banking

Challenges

- Everyone is not ready for cybercrime
  - The users who easily fell prey to basic social engineering tactics
  - Software companies don't have security features built in
  - Laws against cybercrime not yet enacted
  - Law enforcement capability not yet ready

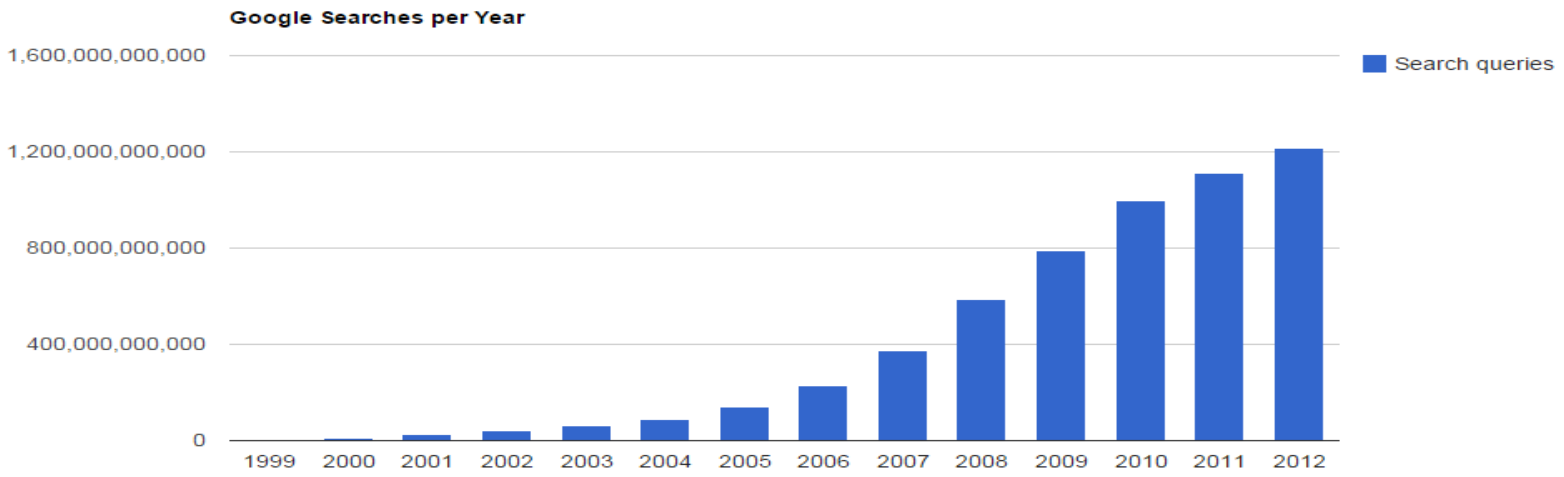
Google Search Timeline

Google



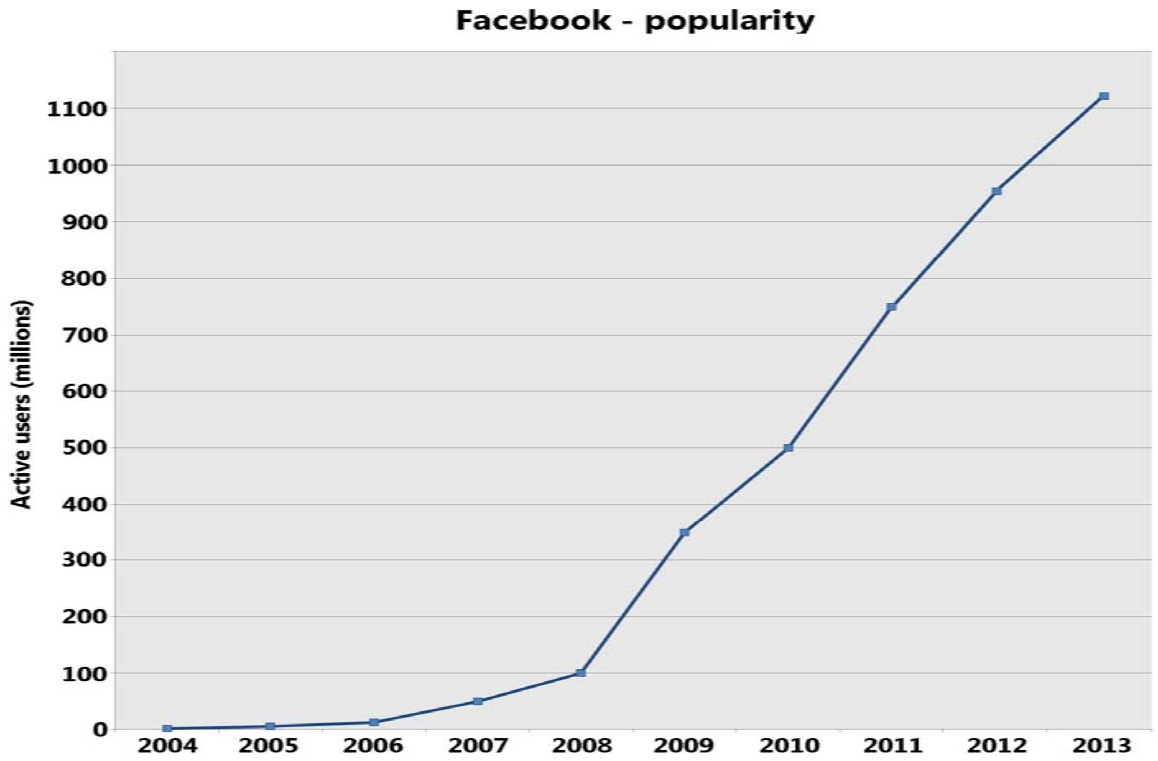
TREND MICRO

Source: http://professionalwebseo.blogspot.com/2013/10/google-search-celebrate-15-years.html



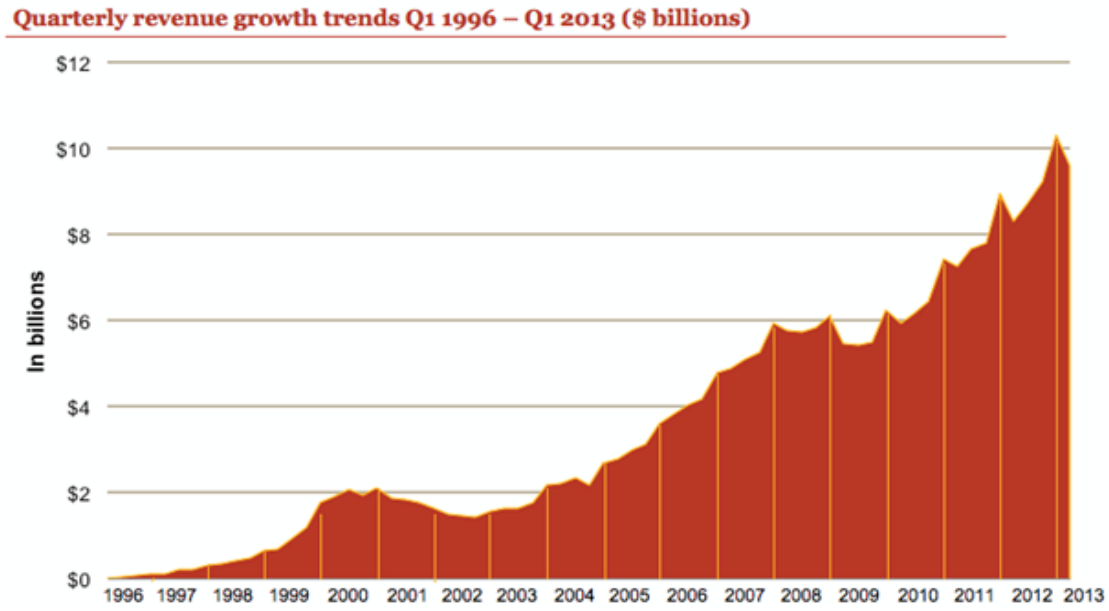
Source: http://www.internetlivestats.com/google-search-statistics/

Social Media



Source: http://en.wikipedia.org/wiki/Facebook

Online Advertisement Spending



Source: https://gigaom.com/2013/06/03/online-ad-spending-up-16-from-a-year-ago-report/

Key Points

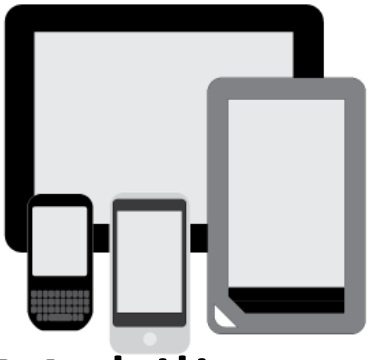
- Where the people are…
  - Browsing the internet
- Where the money is…
  - Ads
  - Fraud
- Low hanging fruit…
  - Ads
  - Scare mongering

Challenges

- Cybercriminals were more organized than public and private sectors
- 4 million infected users… so what?
  - What is the direct effect?
  - Those 4 million are not necessarily the victims

2010s

Cloud computing

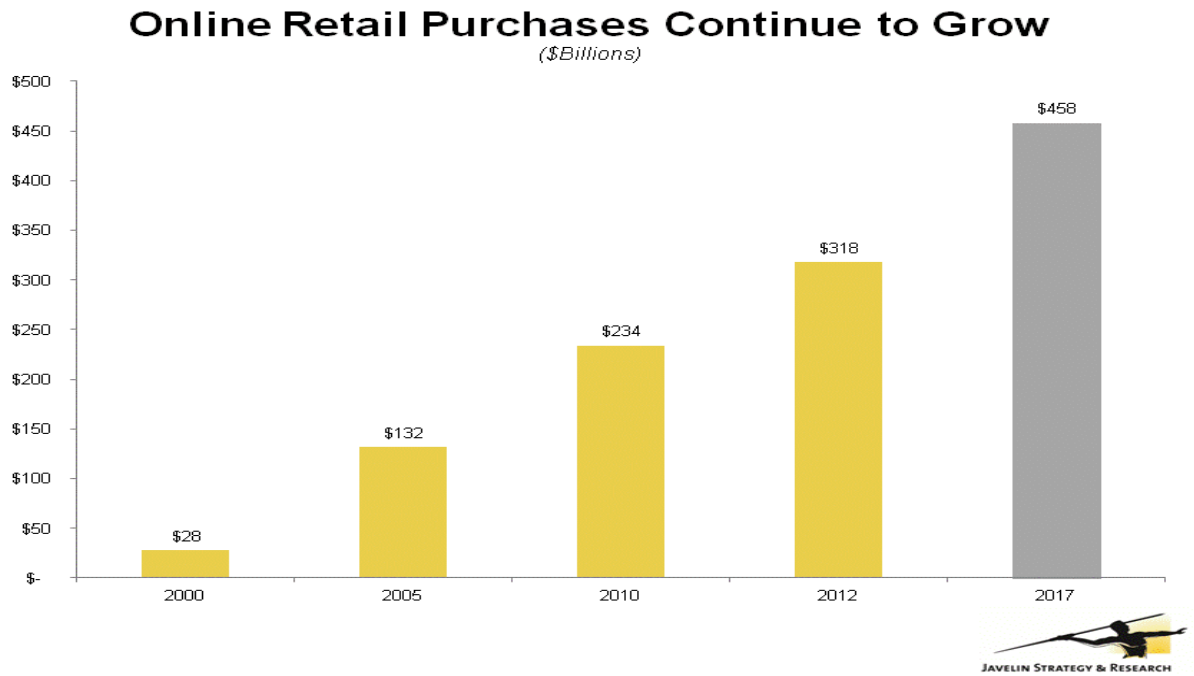


Mobility

Virtualization

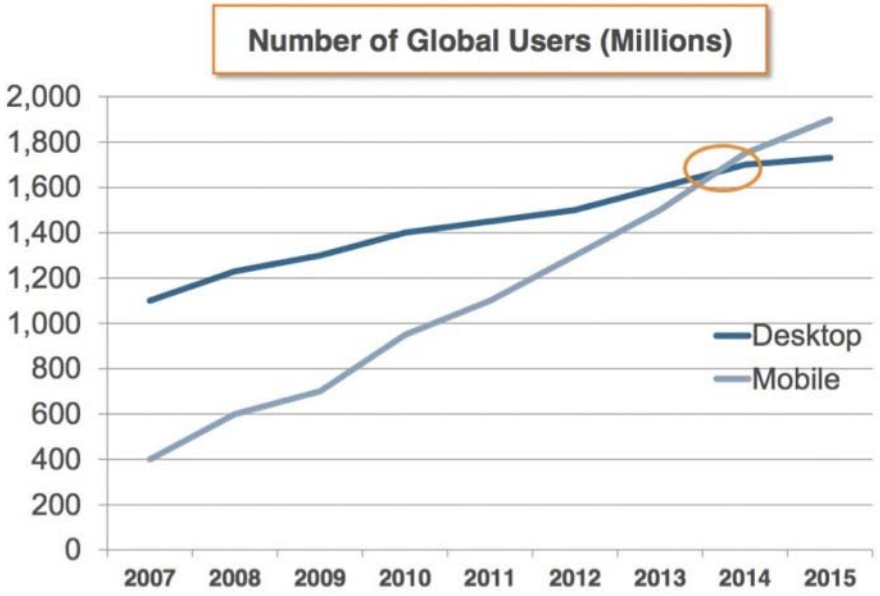
TREND MICRO

2010s



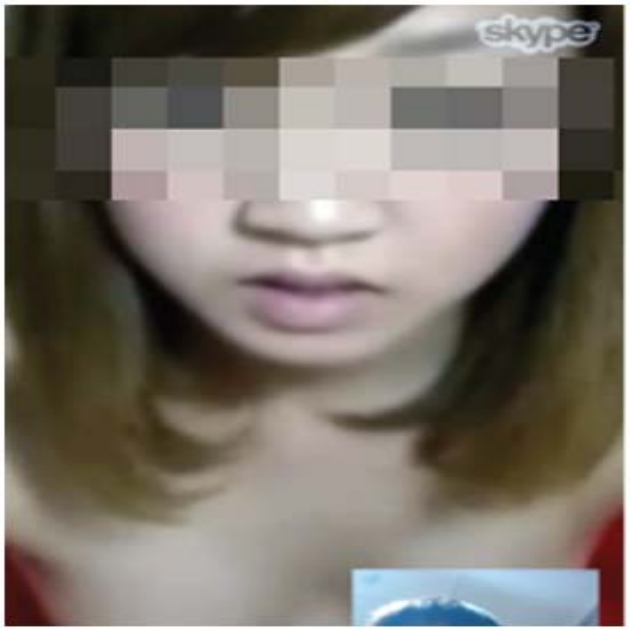
https://www.javelinstrategy.com/blog/2012/11/26/javelin-findings-supported-by-cyber-monday-activity/

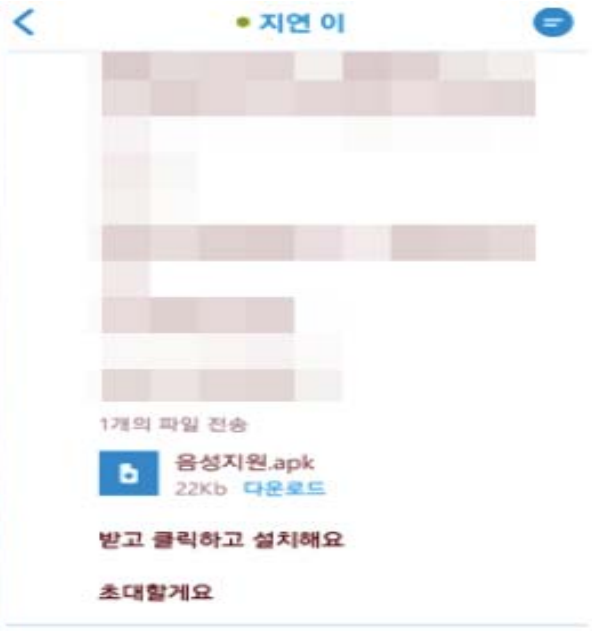
A computing category that **did not exist 8 years ago** has come to overtake one that has been around for 38 years!



Source: Morgan Stanley Research

Sextortion





TRANSLATION:

Attacker: {Text has been redacted due to explicit content] *audiosupport. apk* Download and install it.

Feigning audio problems to convince the victim to switch to an Android device

Source: http://feedpic.kr/?p=350

Key Points

- Where the people are…
  - Doing stuff on the Internet
- Where the money is…
  - e-commerce
  - Fraud
  - Niche systems
- Low hanging fruit…
  - Fraud
  - Blackmail

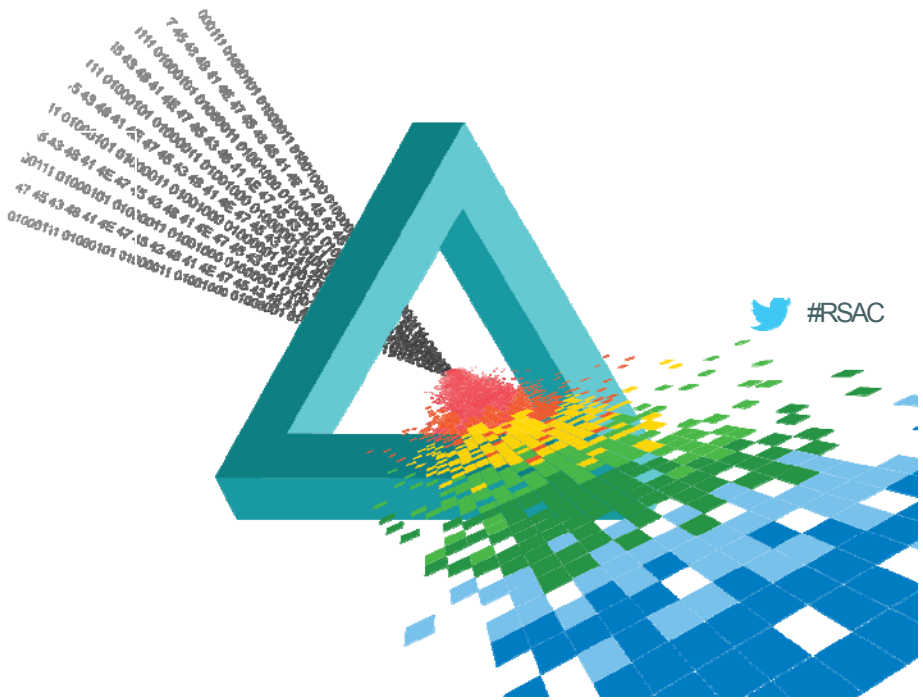
Challenges

- Fraud
- Niche systems
- Mobile Malware
- Region specific attacks

RSA Conference2015

Abu Dhabi | 4–5 November | Emirates Palace

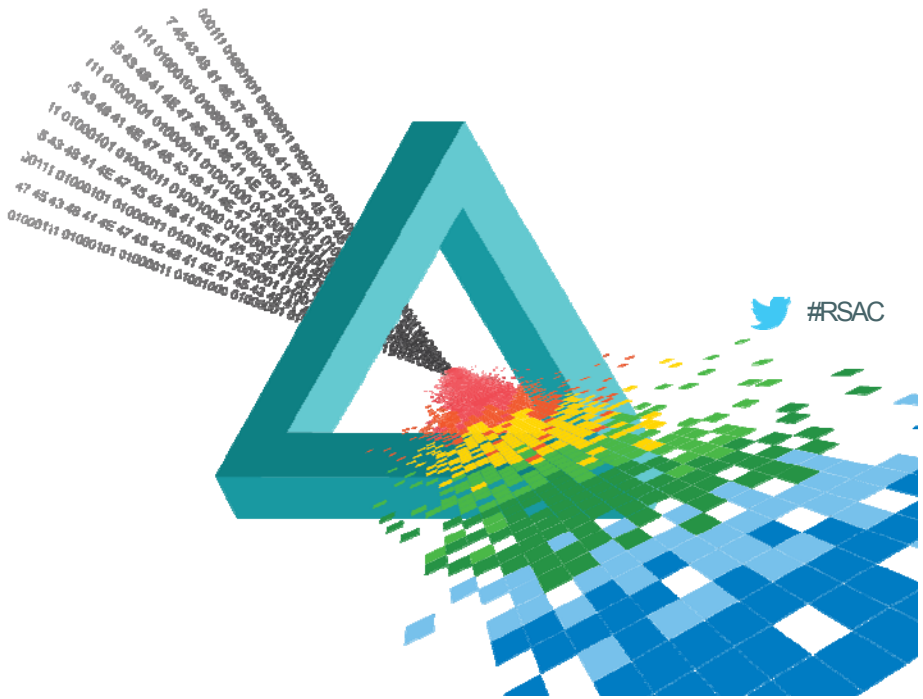
IN-DEPTH LOOK AT CYBERCRIME, WE NEED TO GO DEEPER -- INTO THE CYBERCRIMINAL UNDERGROUND



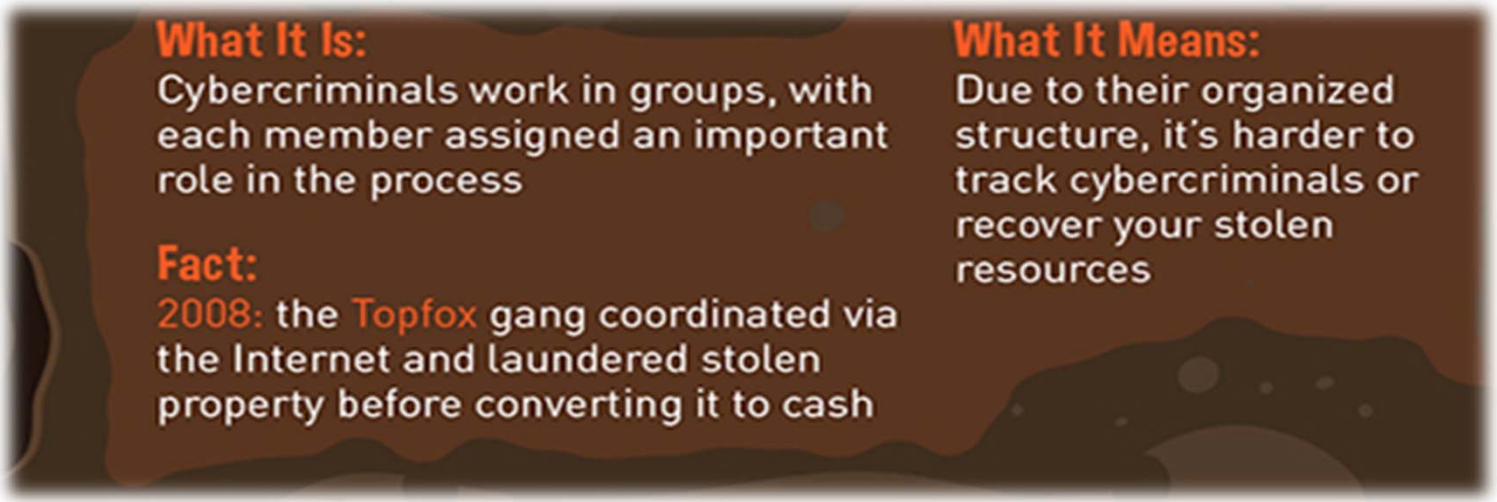
RSA Conference2015

Abu Dhabi | 4–5 November | Emirates Palace

THE UNDERGROUND OPERATES LIKE A LEGITIMATE BUSINESS



COMMERCIAL BUSINESS MODEL



ORGANISED CRIME BUSINESS MODEL

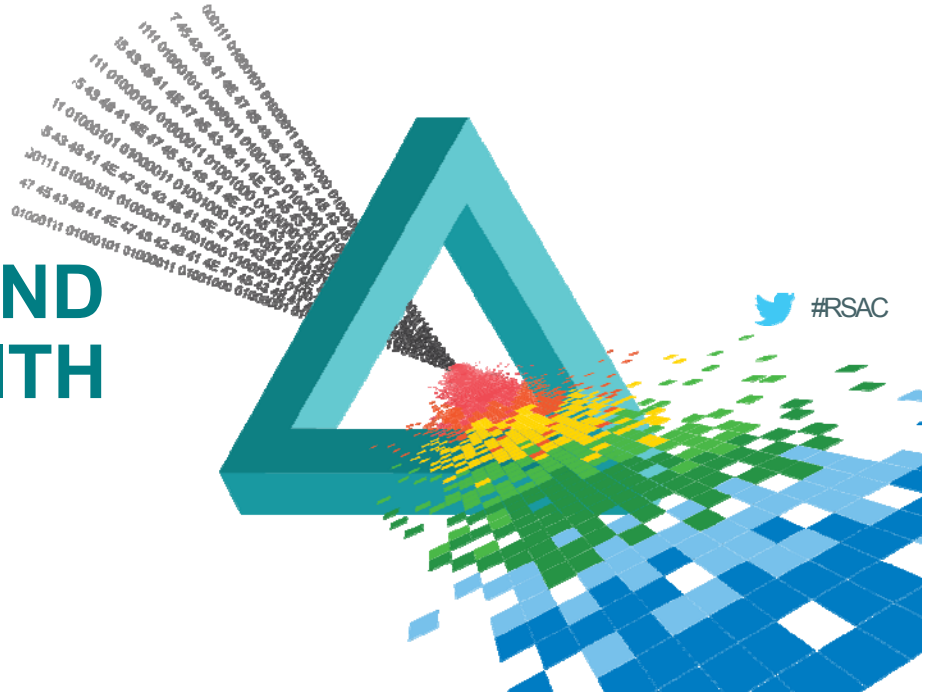
OUTSOURCING BUSINESS MODEL

MENTOR APPRECNTICE BUSINESS MODEL

RSAConference2015

Abu Dhabi | 4–5 November | Emirates Palace

REGIONAL UNDERGROUND MARKET EXIST, EACH WITH SPECIALIZATIONS



THE RUSSIAN MARKET

TRAFFIC DIRECTION SYSTEMS
TRAFFIC DIRECTION
PAY-PER-INSTALL SERVICE

THE CHINESE UNDERGROUND

DISTRIBUTED DENIAL-OF-SERVICE (DDOS) ATTACK SERVICES

COMPROMISED HOSTS/BOTNETS

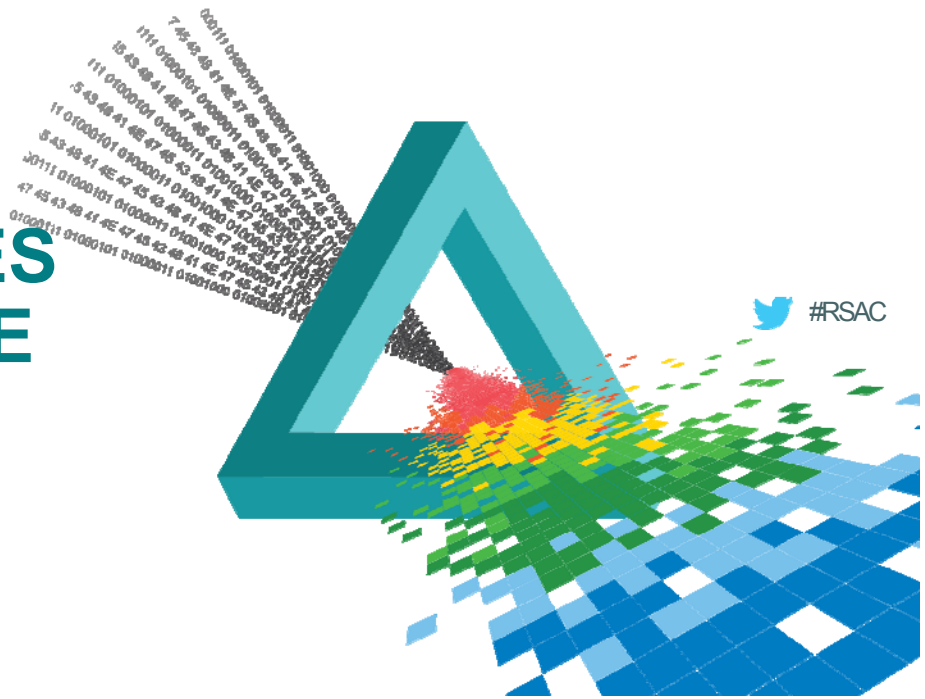
THE BRAZILLIAN UNDERGROUND

SMS SPAMMING SERVICES ; HOME PHONE NUMBER LISTING FOR BIG CITIES

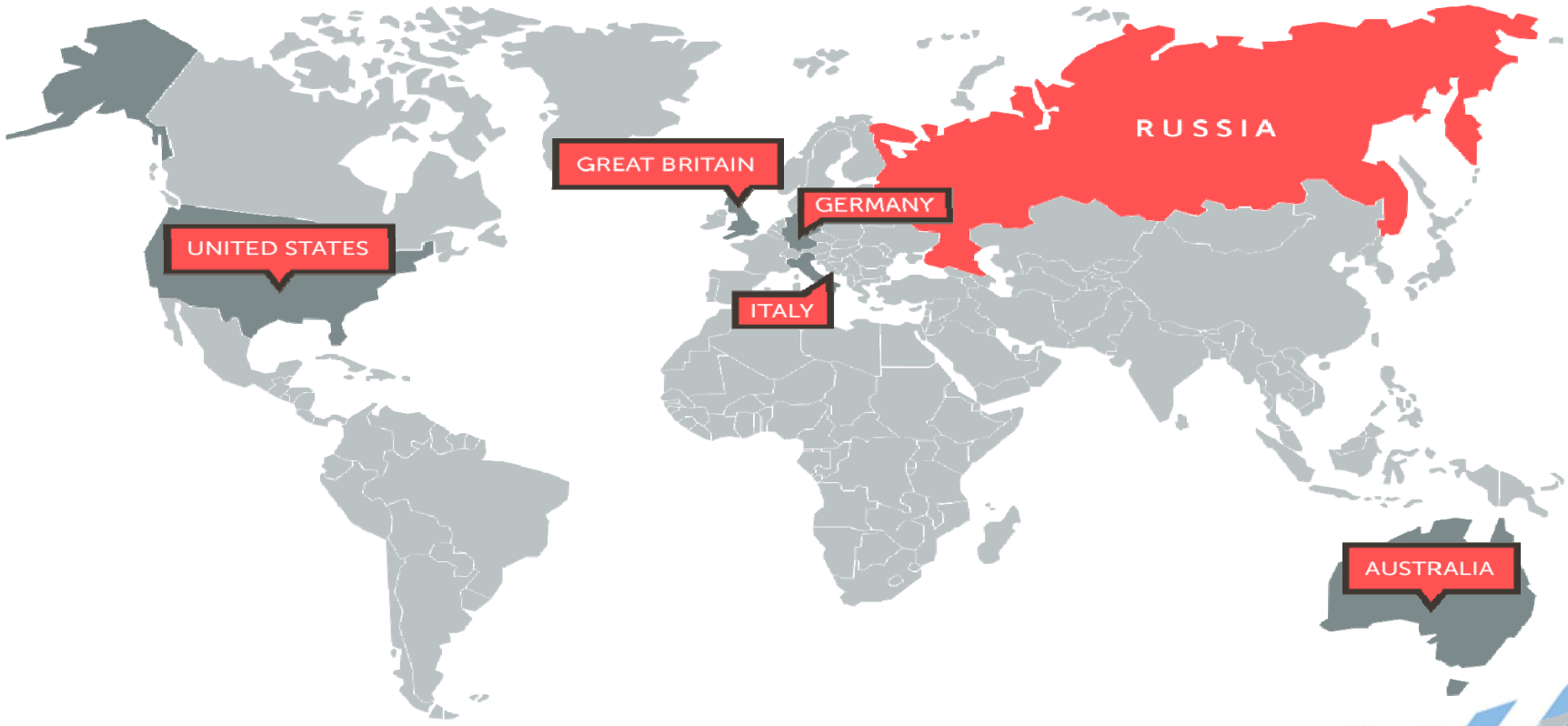
RSA Conference2015

Abu Dhabi | 4–5 November | Emirates Palace

REGIONAL MARKET DOES NOT MEAN THREATS ARE CONTAINED WITHIN THE REGION



#RSAC



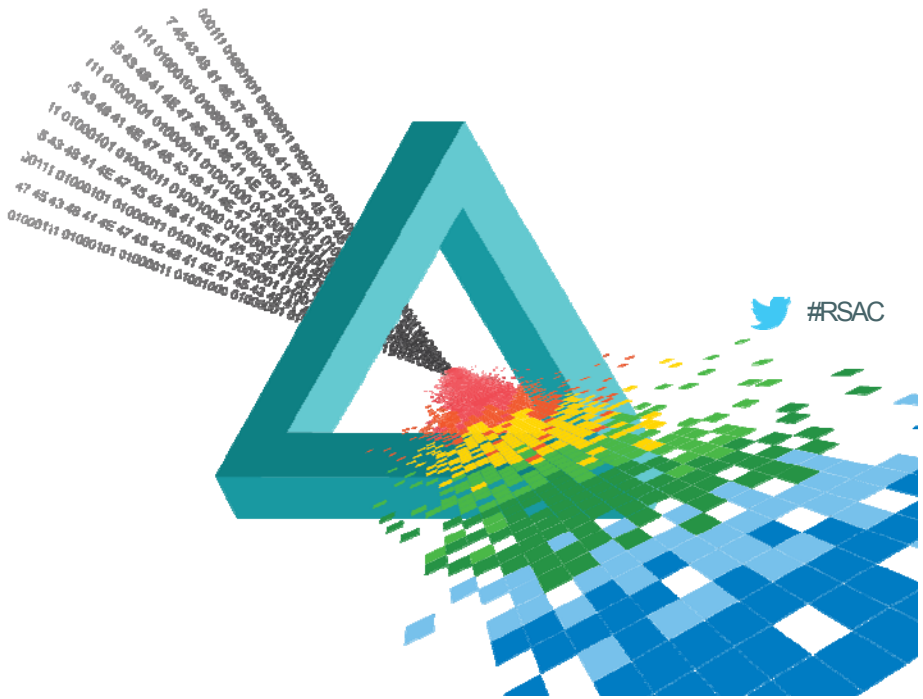
TREND MICRO™

RSA Conference 2015
Abu Dhabi

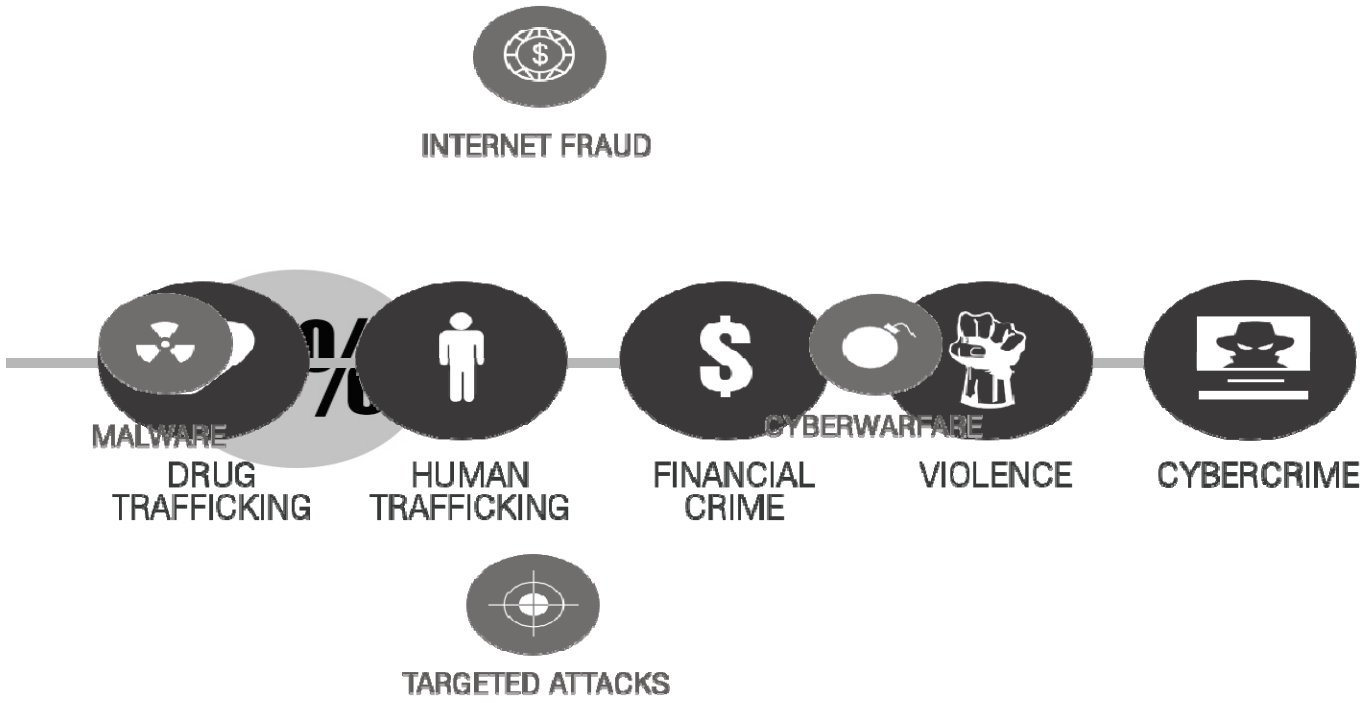
RSAConference2015

Abu Dhabi | 4–5 November | Emirates Palace

Lets Number Do the Talking…..




1% ATTRIBUTED TO ORGANIZED CRIME


INTERNET FRAUD
MALWARE
DRUG TRAFFICKING
HUMAN TRAFFICKING
FINANCIAL CRIME
CYBERWARFARE
VIOLENCE
CYBERCRIME
TARGETED ATTACKS

Underground Product Prices

Underground Product Prices

UAE THREAT LANDSCAPE

About **700k malicious URLs** hosted in the Middle East;
0.62% come from UAE

More than **17 Million** accesses to **malicious websites**;
26% come from UAE

Around **262 Million spam-sending IPs**;
3% coming from UAE

5M Malware Detections

TREND MICRO

TOP 10 ADWARE MIDDLE EAST

Adware Name	Total # of infections
ADW_OPENCANDY	
ADW_SSEARCH	
ADW_IBRYTE	
ADW_SPROTECT	
ADW_TOMOS	
ADW_RIDECROSS	
ADW_MULTIPLUG	
ADW_AGENT	
ADW_WEBSEARCH	
ADW_MONTIERA	

TOP 10 ADWARE UAE

Adware Name	Total # of infections
ADW_OPENCANDY	1,518
ADW_SSEARCH	1,230
ADW_IBRYTE	1,034
ADW_SPROTECT	901
ADW_TOMOS	495
ADW_AGENT	438
ADW_INSTALLCORE	425
ADW_WEBSEARCH	393
ADW_MONTIERA	392
ADW_MULTIPLUG	375

The **adware** problem also hounds online users

TOP 10 INFECTION MIDDLE EAST

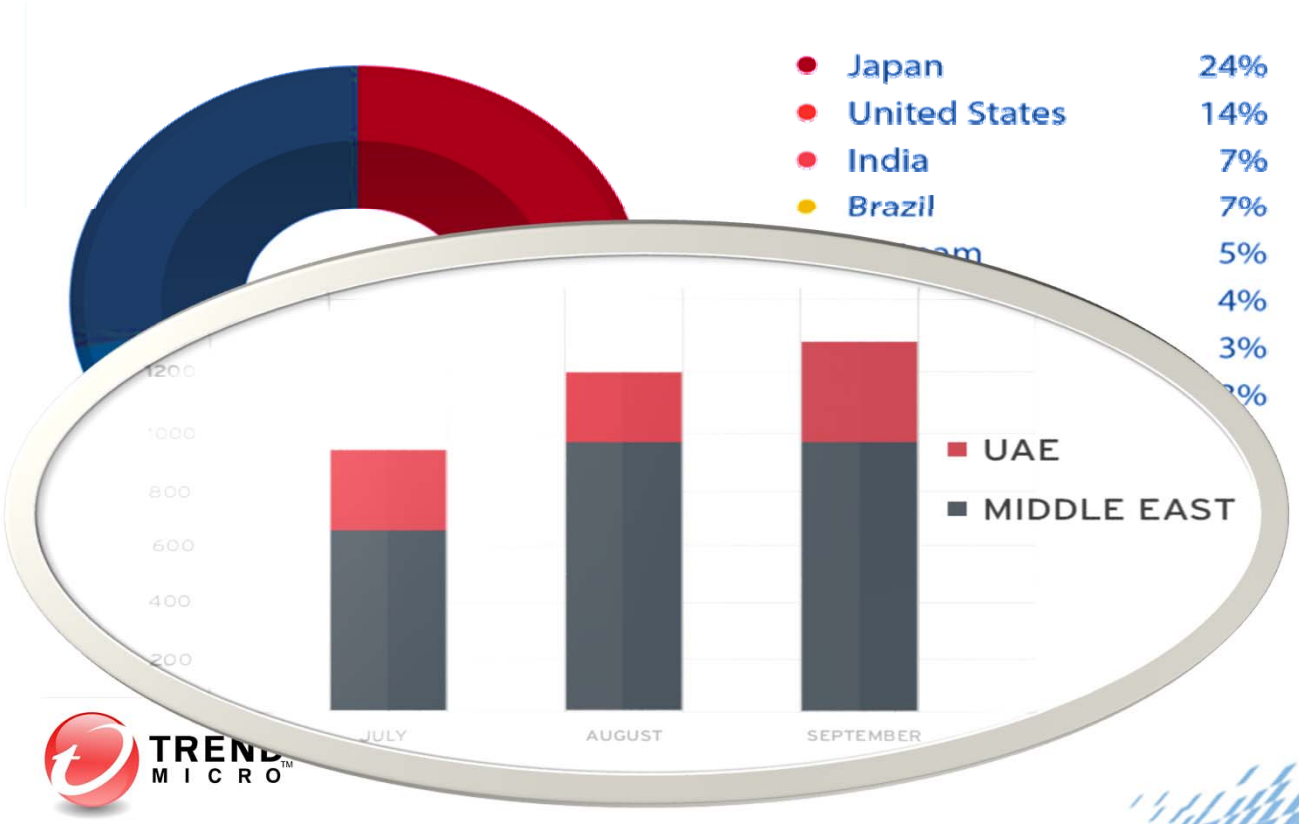
Malware Name	Total # of infections
LNK_DUNIHI.SMIX	1,711
WORM_DOWNAD.AD	
PE_SALITY.RL	
TROJ_GAMARUE.SM	
PE_SALITY.RL-O	
WORM_GAMARUE.SMB	
WORM_OTOIT.SMT	
PE_VIRUX.R	
BKDR_BLADABI.SMC	
WORM_OTORUN.SMXY	

TOP 10 INFECTION UAE

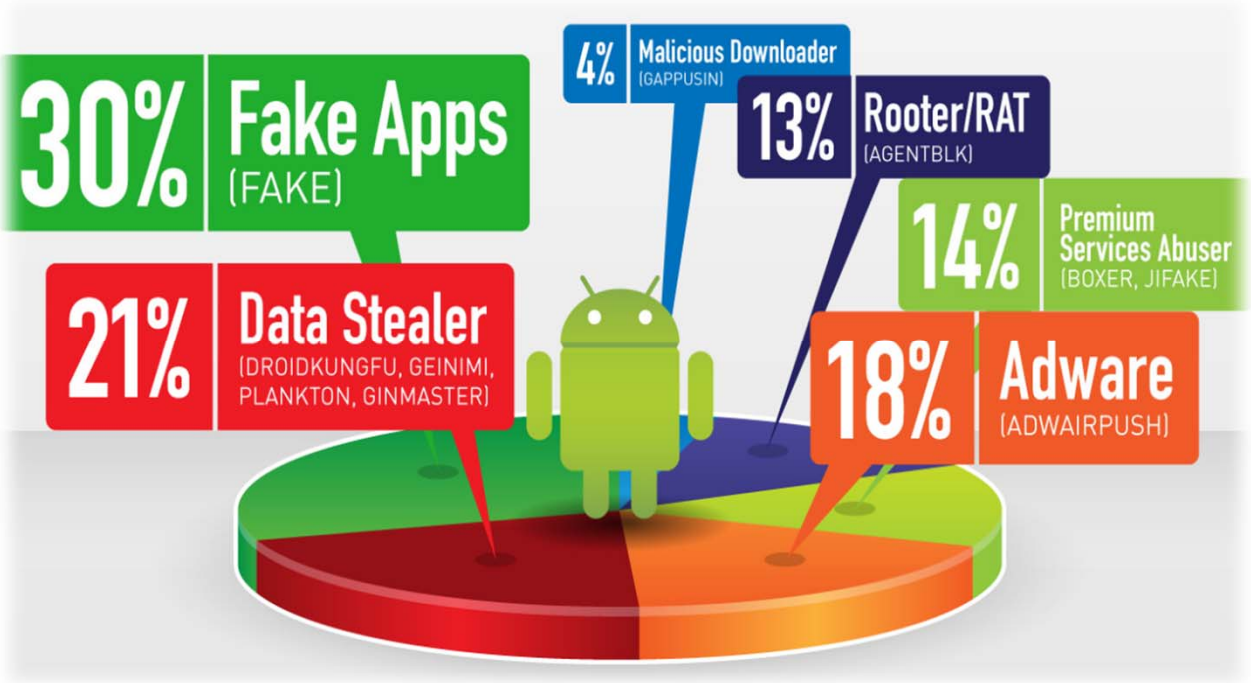
Malware Name	Total # of infections
PE_SALITY.RL	244
LNK_DUNIHI.SMIX	242
PE_SALITY.RL-O	208
WORM_DOWNAD.AD	172
TROJ_STARTER.SM	133
PE_RAMNIT.DEN	131
ALS_COPICAD.D	123
WORM_SOHAND.SM	117
TROJ_GAMARUE.SM	115
WORM_DELF.FKZ	99

The **old** malware still spreads in the region

TREND MICRO



1% online banking attacks victims **Middle East**



1% of total mobile apps scanned in the Middle East are malicious

TREND MICRO

Looking Forward…

- Fraud will continue to be a big problem
- Regional and niche specific attacks
- Home networks and the IoT devices behind them are feasible targets

How do you protect yourself …

- As Organizations….
- Pure play cloud users should consider that security is a shared responsibility
- Invest in Breach Detection Systems
- Employee Awareness Campaigns is the Key
- Create and Enforce IS Policy

How do you protect yourself …

- As Individuals…
- Aware on what you "Click"
- Protect Mobile Devices same as your Computers/Laptops
- Think before you post
- Use Multi-Factor Authentication
- Password Resets
- Child Online Safety/Social Media
- Early childhood education starts from home
- If "You" become victim talk to Authorities – Al Ameen & Aman Service

- ENJOY REST OF THE CONFERENCE