CYBER THREATS TO THE RETAIL INDUSTRY

Scott L. Howitt, Director IT Risk Management jcpenney

Quick Poll - Email

- JCPenney receives approximately 1,000,000 emails a day at the email gateway, how many of the emails are actually valid emails that are allowed to be delivered?

A. 920,000

B. 620,000

C. 513,000

D. 130,000

Quick Poll - Email

- The correct answer is 130,000!

- Of the approximate 1,000,000 emails that are received each day:

  - 800,000 e-mails are blocked due to reputational filters (from known bad guys)

  - 25,000 e-mails are blocked as spam

  - Once past the first two filters 130 e-mails are blocked due to virus attachments

  - In summary ~86% of our e-mail is blocked at the gateway

Quick Poll - Malware

- In 2000, approximately 5 new viruses were released daily. What was the daily activity in 2009?

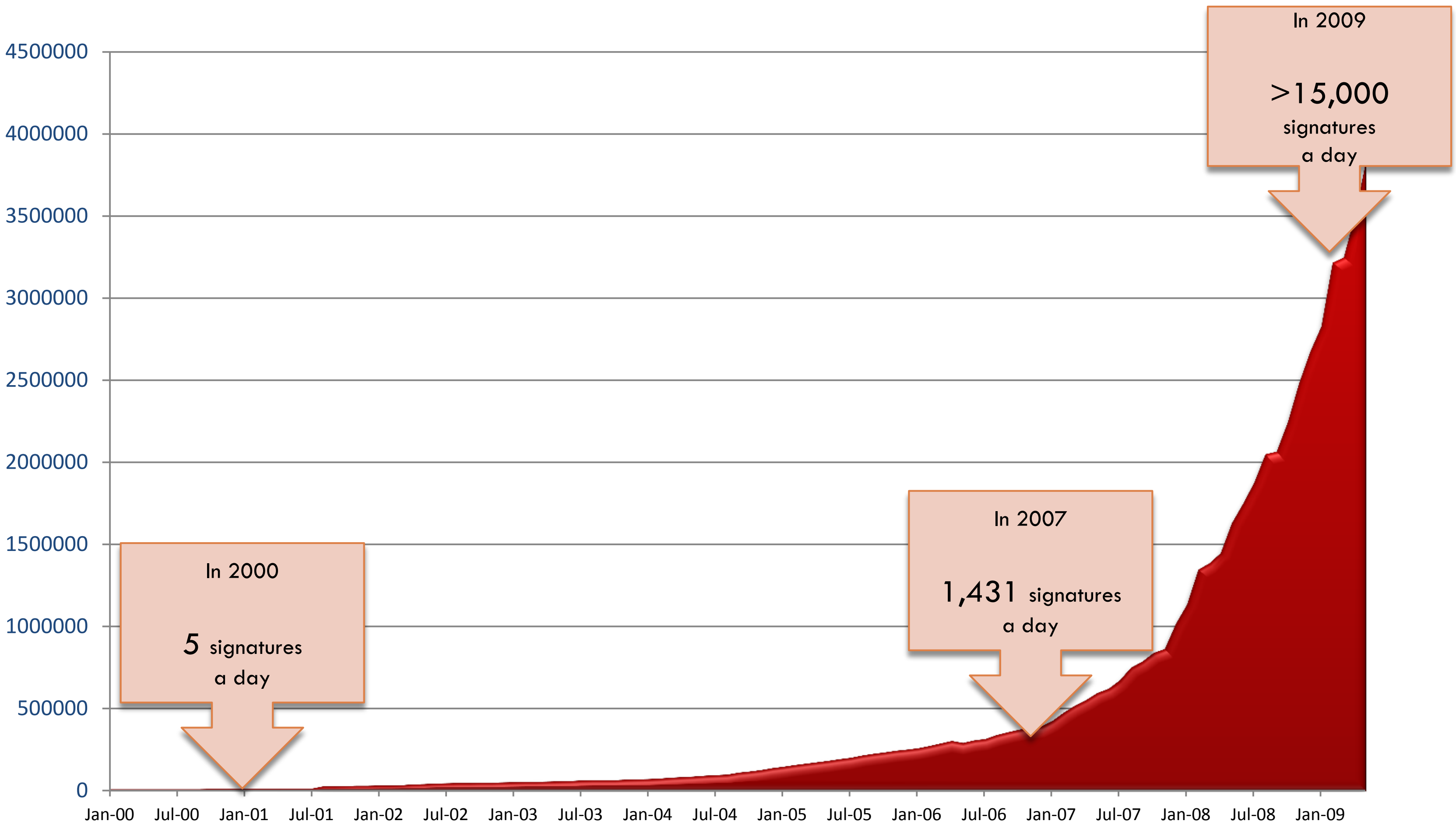
A. 50

B. 200

C. 4,000

D. 15,000+

Quick Poll - Malware



In 2000

5 signatures a day

In 2007

1,431 signatures a day

In 2009

>15,000 signatures a day

*source Symantec Global Intelligence Network

Why the exponential increase?

Data is worth real money on the black market. Here are some examples of what this information is worth to fraudsters.

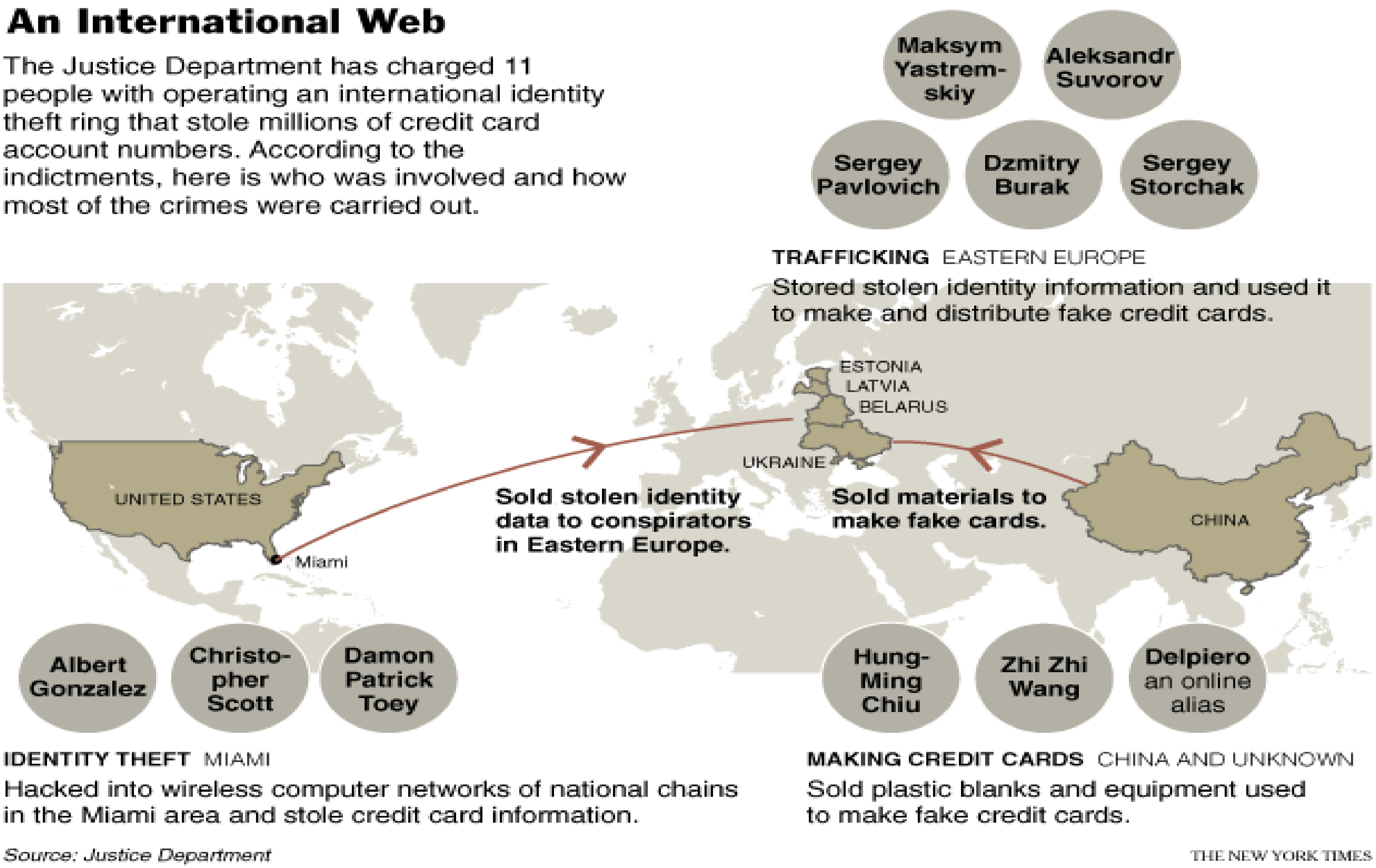
Sale Item	Underground Price
Full Credit Card Data	$1.50-$3.00 / card number
SSN / DoB / Mother's Maiden Name	SSN / DoB $1 - $3, MMN $5 - $6
Online Banking Logins	$50 - $1,000 per account
Full Track 2 Data (Mag Stripe)	$15 - $80 depending on card type

While the barrier to entry for the fraudster is very small.

Sale Item	Underground Price
Zues Trojan Kit	$3,000 - $5,000
Bulletproof Hosting	$400 per month
One infection Email Campaign	$70 per campaign
Estimated start-up costs	$5470

The geeky kid next door

Cybercrime is now rarely the realm of individuals, it now involves organized crime



An International Web

The Justice Department has charged 11 people with operating an international identity theft ring that stole millions of credit card account numbers. According to the indictments, here is who was involved and how most of the crimes were carried out.

Maksym Yastremskiy

Aleksandr Suvorov

Sergey Pavlovich

Dzmitry Burak

Sergey Storchak

TRAFFICKING EASTERN EUROPE

Stored stolen identity information and used it to make and distribute fake credit cards.

Sold stolen identity data to conspirators in Eastern Europe.

Sold materials to make fake cards.

Albert Gonzalez

Christopher Scott

Damon Patrick Toey

IDENTITY THEFT MIAMI

Hacked into wireless computer networks of national chains in the Miami area and stole credit card information.

Hung-Ming Chiu

Zhi Zhi Wang

Delpiero an online alias

MAKING CREDIT CARDS CHINA AND UNKNOWN

Sold plastic blanks and equipment used to make fake credit cards.

Source: Justice Department

THE NEW YORK TIMES

The "Hack Pack"

- The Hack Pack cost business and consumers hundreds of millions of dollars. It was able to fund their life of excess. One of the members had:
  - Cross-country charted flights
  - Lived in a suite at the National Hotel in Miami
  - Threw birthday parties that cost $75,000
  - Kept $400,000 in cash on hand and had buried $1,100, 000 in his parent's backyard
- Keep in mind, at the time, he was working for the Secret Service helping put other hackers in jail. Many whom he had partnered with.

The world is changing

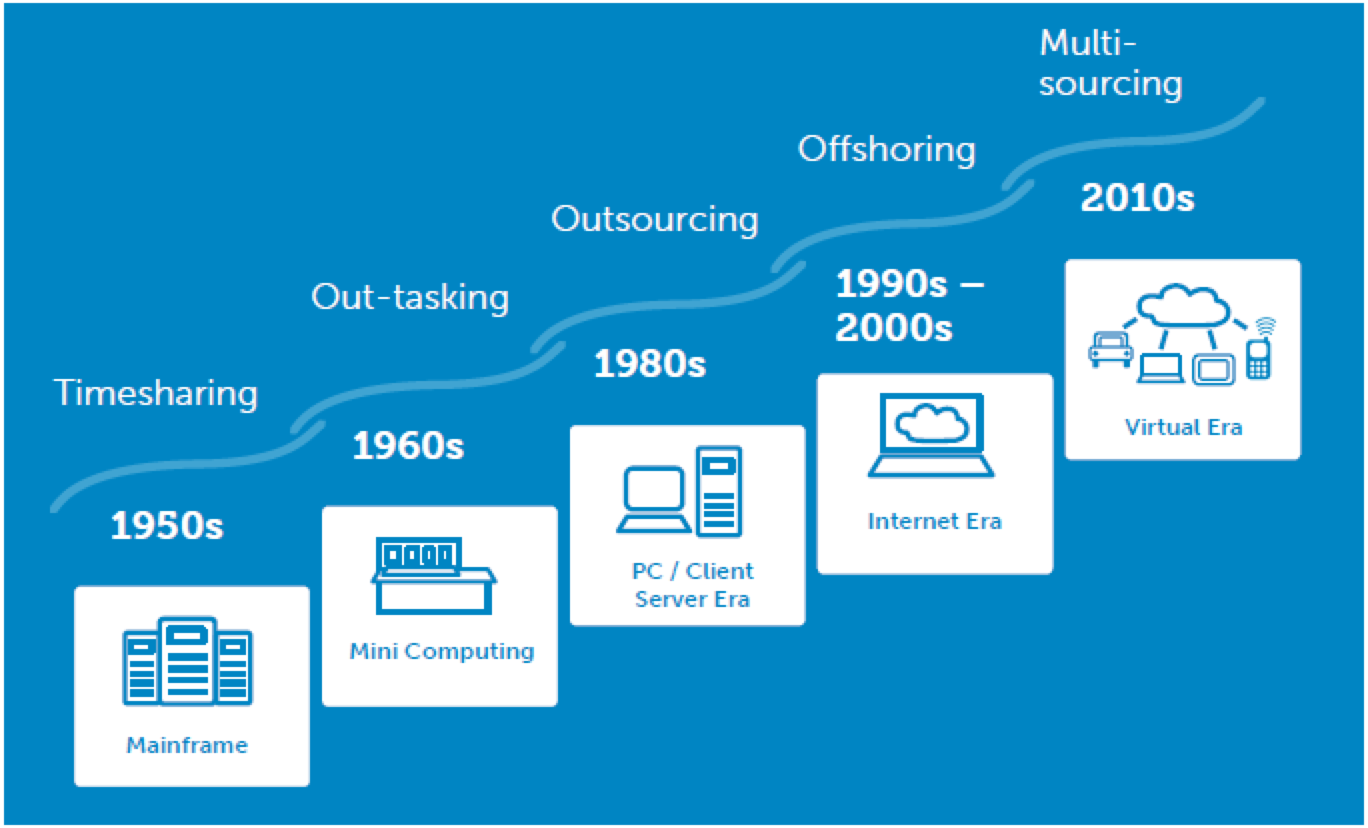
Information is more at risk today than ever before due to the portability of high volumes of sensitive information

- Mobile Devices
  - Tablets (i.e., iPad, Slate)
  - Smart phones (i.e., iPhone, Android, Blackberry)
- Electronic Storage Media
  - USBs
  - CDs/DVDs
  - Portable backup drives
  - SIM card
- Cloud Services
  - Dropbox
  - Carbonite

Solving the Soft Trend misses the Hard

- Verizon FIOS solves the speed issue but missed the obvious technology trend
  - Howitt household contains 29 IP devices:
    - Kindle (2)
    - Android Tablet
    - iPad
    - iPod Touch
    - Laptops (5)
    - Desktops (3)
    - SqueezeBoxes (2)
    - Xboxes (2)
    - Wii
    - iPhones (4)
    - Windows Phone
    - Nintendo DS
    - Roku
    - Internet Enabled TV
    - NAS
    - Routers (2)

The times, they are a changin'



The phone in your pocket vs. a 1980 Mainframe

- Your smartphone harkens back to the 3270 terminal that used to sit on your desk
  - The cloud is the new mainframe
  - Unless you are a developer, your PC is becoming obsolete
  - You will only load what you need
- Kindle Fire is predictive of what is to come
  - Buy once run anywhere
  - Pick up your book/movie where you left off on your phone/media player/computer/TV
  - Predictive browsing (cloud based caching)
  - Only load for your immediate (0r near immediate) need

The undeniable Hard Trend

- Risk Management must learn to enable the business enterprise
  - The Tower of London analogy
    - During the time of the Tudors, the perimeter was the defense
    - Today, access is totally open while still protecting the crown jewels
- We know cornerstones of next generation computing
  - Social Media
  - Wireless
  - Data Everywhere
  - Cloud