IBM Security Systems: Trends and Strategy

IBM X-Force 2011 Trend and Risk Report

Jean Paul Ballerini
IBM X-Force Spokesperson
IBM Security Systems Subject Matter Expert

Pulse2012
Meet the Experts. Optimise your infrastructure.

May 31 – June1
Sheraton on the Park Hotel, Sydney

IBM X-Force 2011 Trend and Risk Report Highlights

The mission of the IBM X-Force® research and development team is to:

- Research and evaluate threat and protection issues
- Deliver security protection for today's security problems
- Develop new technology for tomorrow's security challenges
- Educate the media and user communities

X-Force Research

14B analyzed Web pages & images

40M spam & phishing attacks

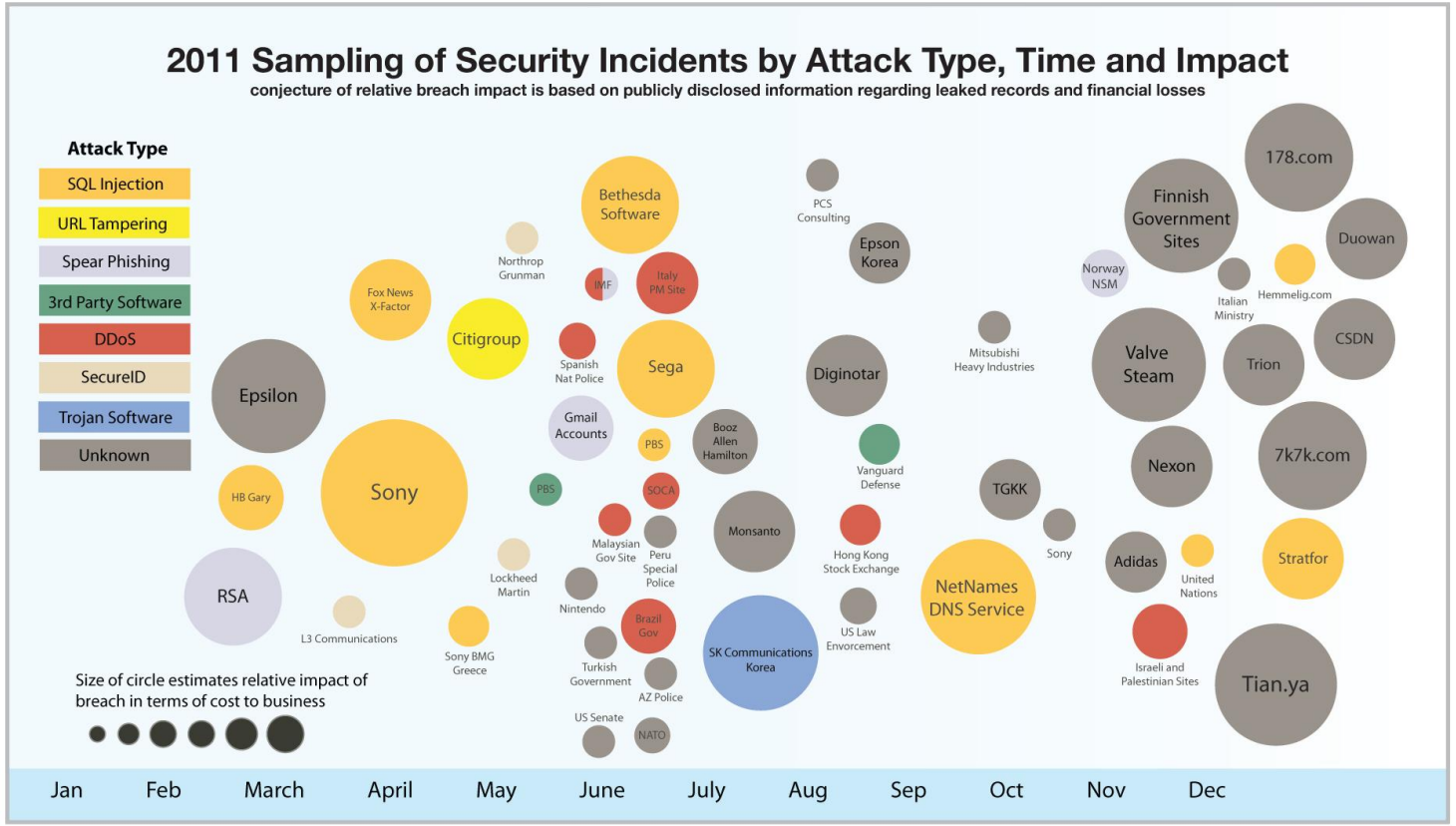
60K documented vulnerabilities

13 billion security events monitored daily

Provides Specific Analysis of:

- Vulnerabilities & exploits
- Malicious/Unwanted websites
- Spam and phishing
- Malware
- Other emerging trends

2011: Year of the Security Breach



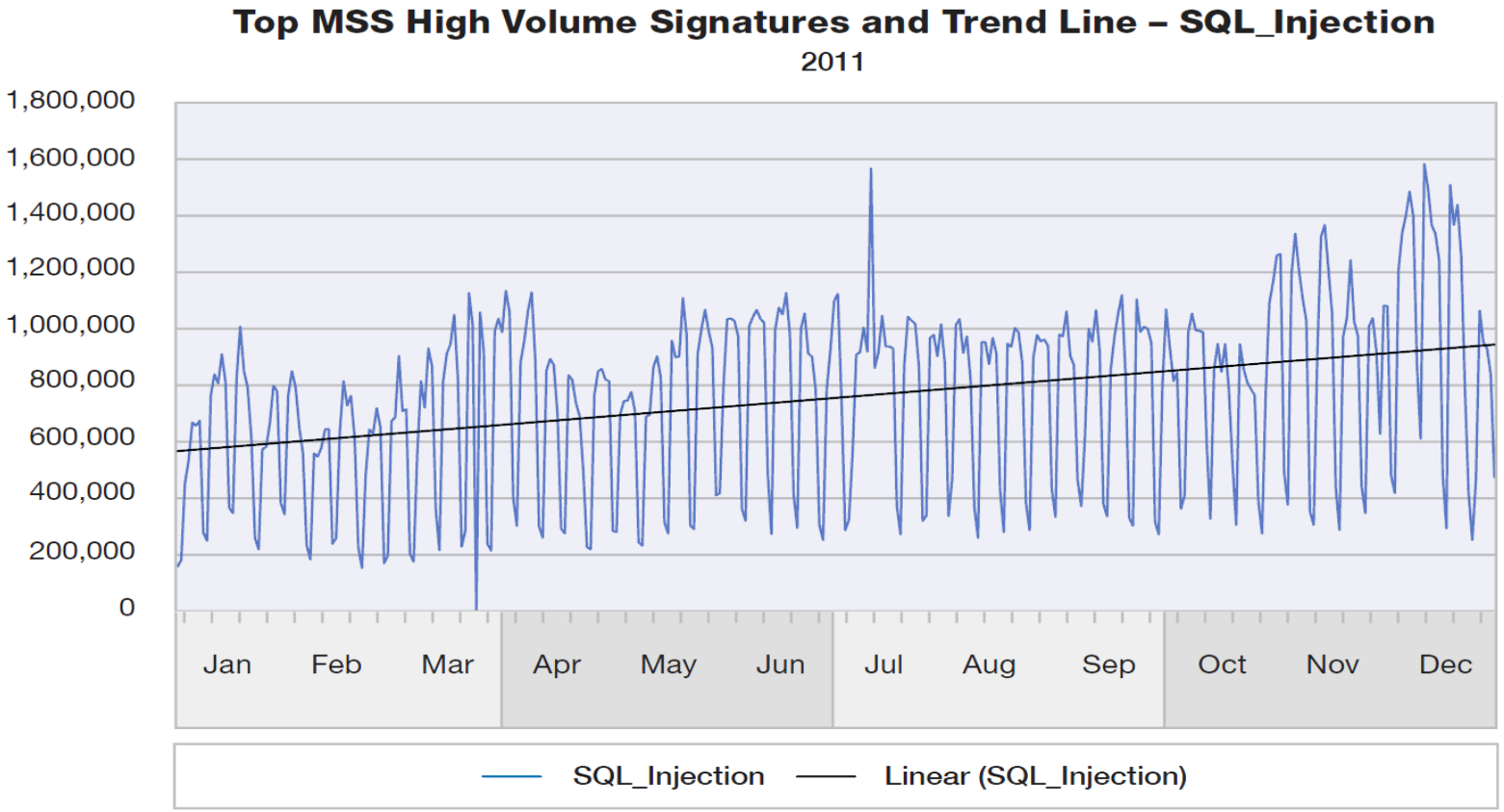
Key Findings from the 2011 Trend Report

- New Attack Activity
  - Rise in Shell Command Injection attacks
  - Spikes in SSH Brute Forcing
  - Rise in Click Fraud related Phishing
- The Challenge of Mobile and the Cloud
  - Mobile exploit disclosures up
  - Cloud requires new thinking
  - Social Networking no longer fringe pastime
- Progress in Internet Security
  - Fewer exploit releases
  - Fewer web application vulnerabilities
  - Better patching

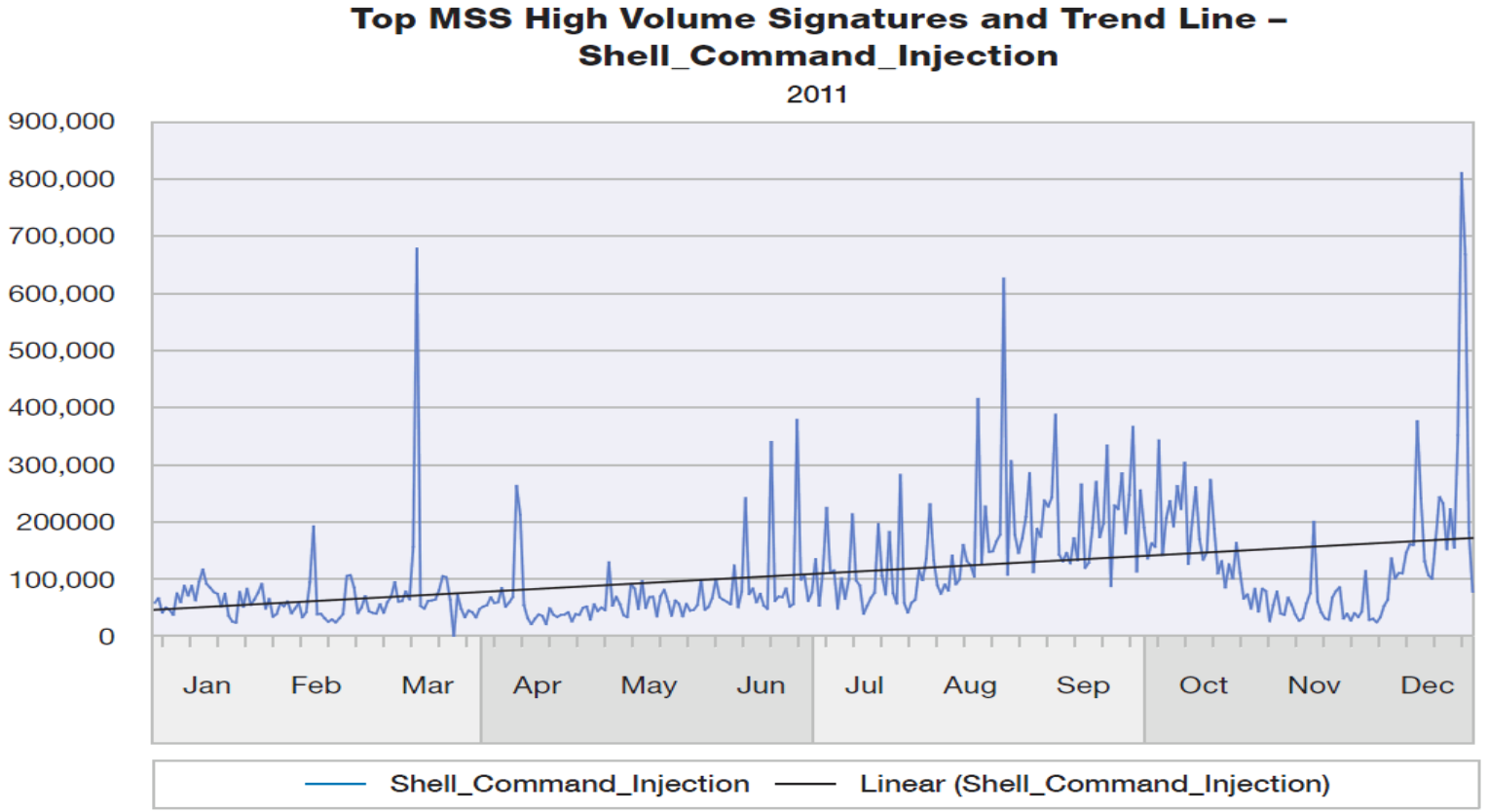
Key Findings from the 2011 Trend Report

- New Attack Activity
  - Rise in Shell Command Injection attacks
  - Spikes in SSH Brute Forcing
  - Rise in Click Fraud related Phishing
- The Challenge of Mobile and the Cloud
  - Mobile exploit disclosures up
  - Cloud requires new thinking
  - Social Networking no longer fringe pastime
- Progress in Internet Security
  - Fewer exploit releases
  - Fewer web application vulnerabilities
  - Better patching

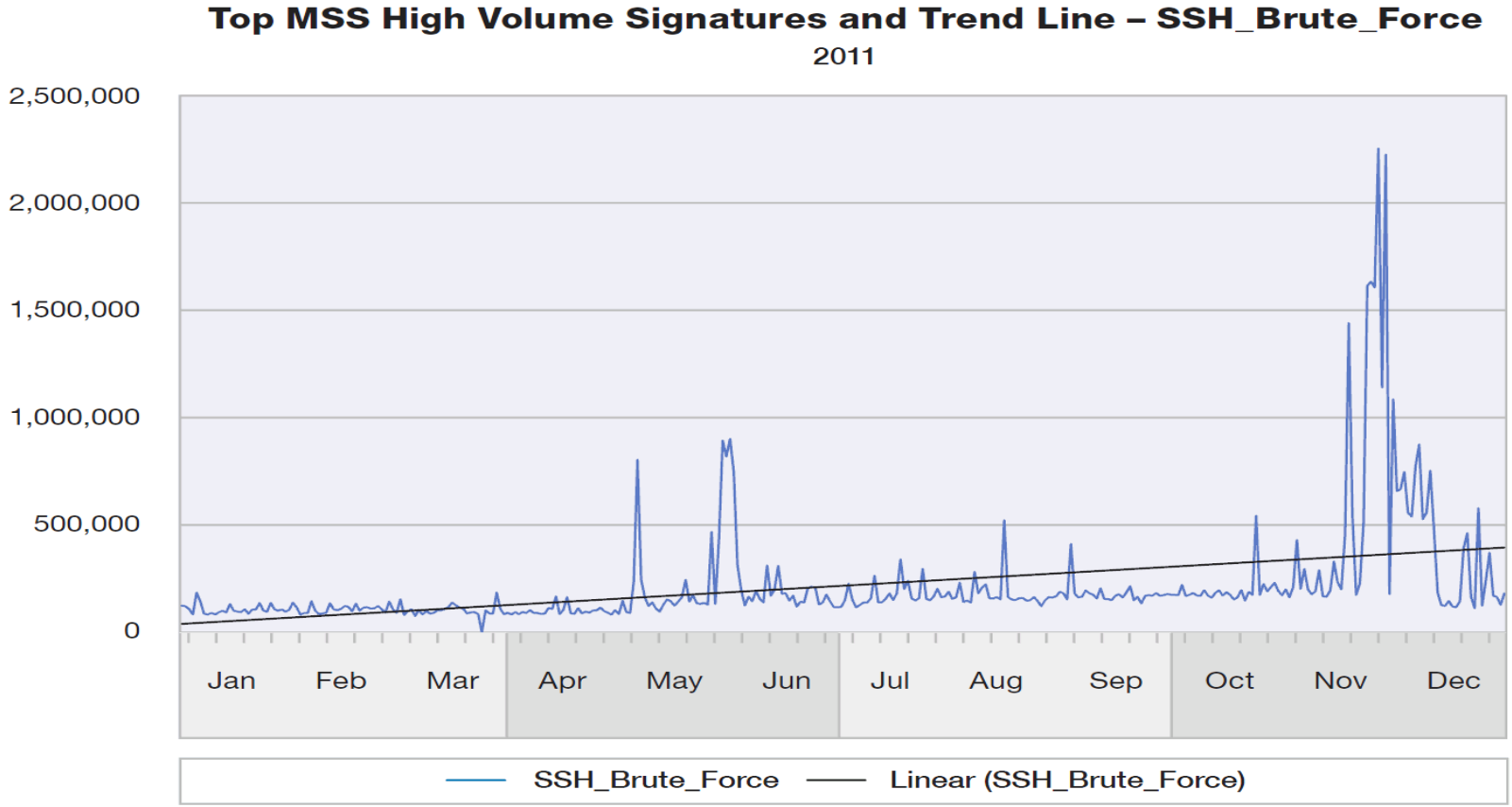
SQL Injection Attacks against Web Servers



Shell Command Injection Attacks



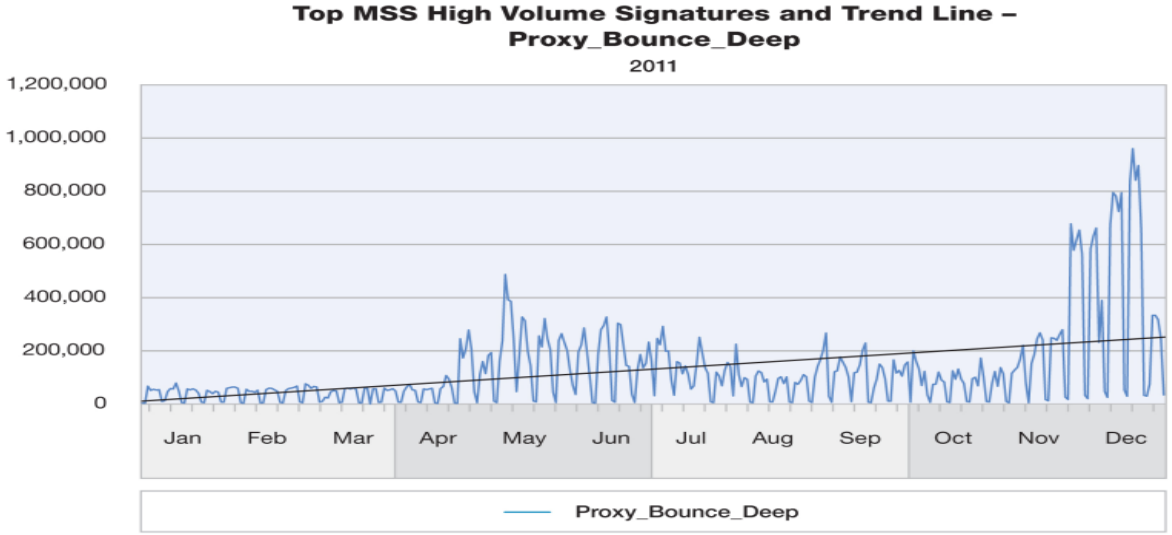
SSH Brute Force Activity



Phishing based malware distribution and click fraud

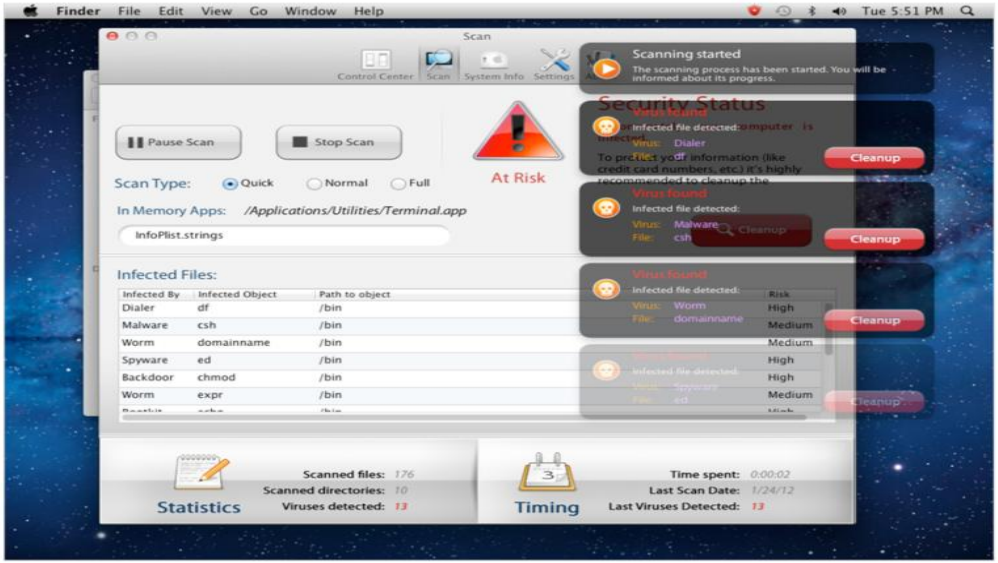
Anonymous proxies hopping on the rise

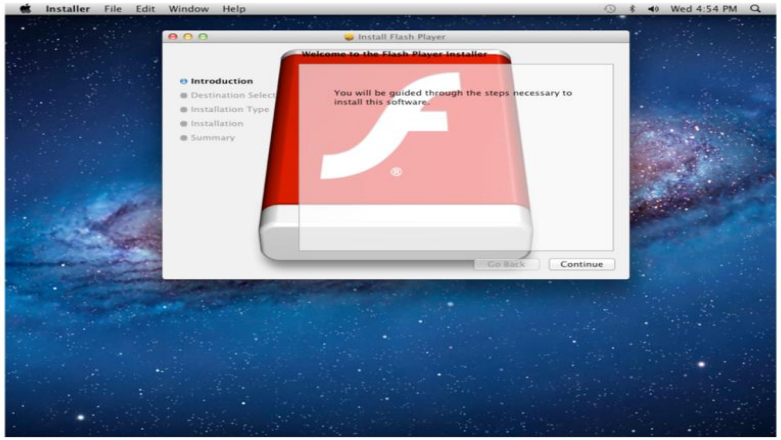
- Signature detects situations where clients are attempting to access websites through a chain of HTTP proxies
- Could represent
  - legitimate (paranoid) web surfing
  - attackers obfuscating the source address of launched attacks against web servers



MAC malware

- 2011 has seen the most activity in the Mac malware world.
  - Not only in volume compared to previous years, but also in functionality.





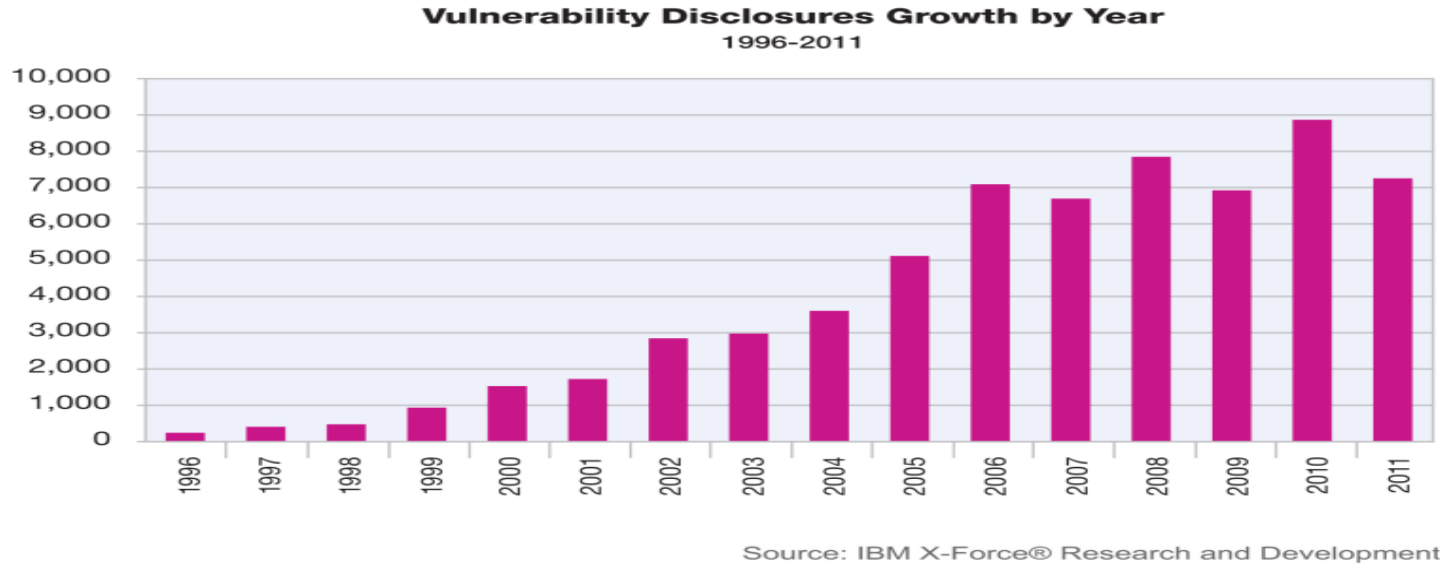
- In 2011, we started seeing Mac malware with functionalities that we've only seen before in Windows® malware.

Key Findings from the 2011 Trend Report

- New Attack Activity
  - Rise in Shell Command Injection attacks
  - Spikes in SSH Brute Forcing
  - Rise in Click Fraud related Phishing
- The Challenge of Mobile and the Cloud
  - Mobile exploit disclosures up
  - Cloud requires new thinking
  - Social Networking no longer fringe pastime
- Progress in Internet Security
  - Fewer exploit releases
  - Fewer web application vulnerabilities
  - Better patching

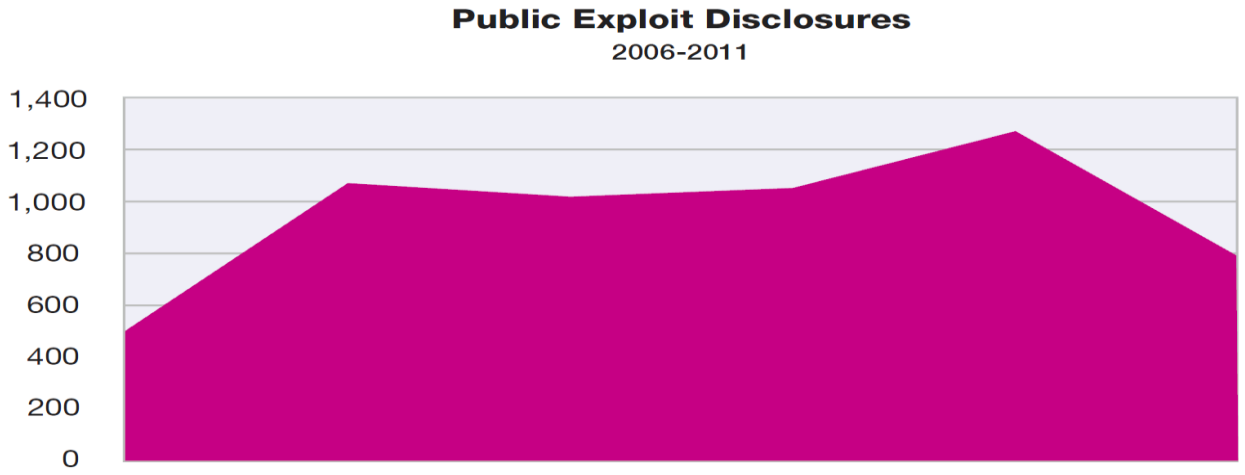
Vulnerability disclosures down in 2011

- Total number of vulnerabilities decline — but it's cyclical
  - We have witnessed a two year, high-low cycle in vulnerability disclosures since 2006



Public Exploit Disclosures

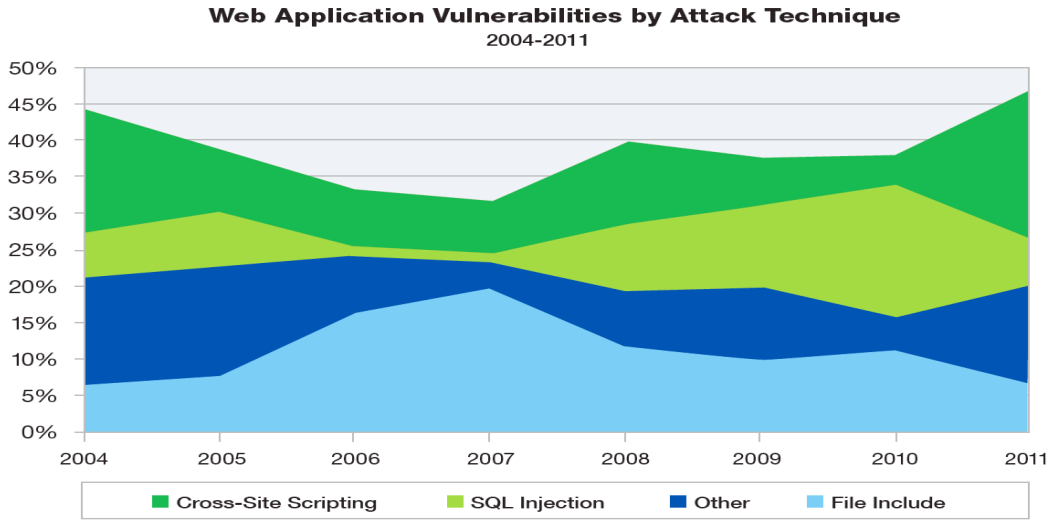
- Fewer exploits released so far this year since 2006
- Down as a percentage of vulnerabilities as well

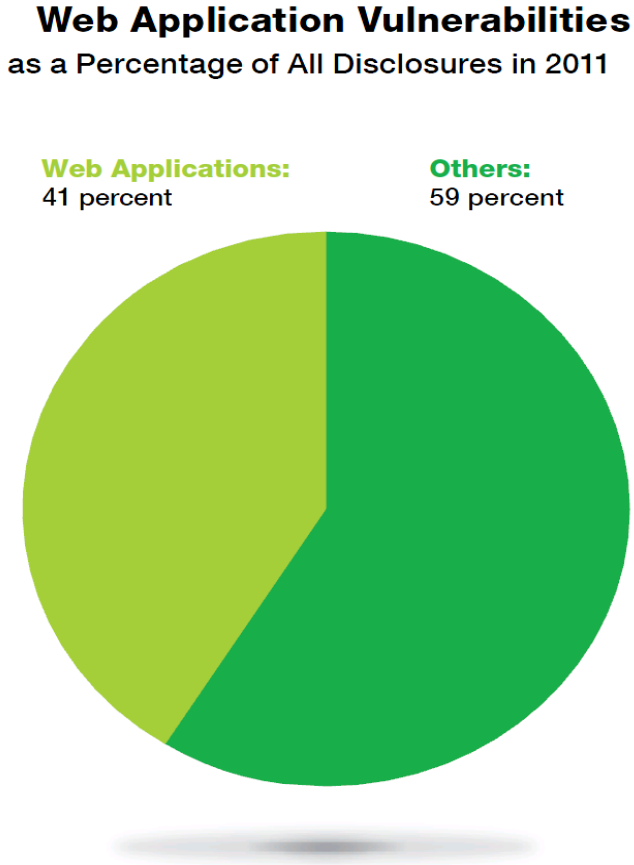


	2006	2007	2008	2009	2010	2011
Public Exploits	504	1078	1025	1059	1280	778
Percentage of Total	7.3%	16.5%	13.3%	15.6%	14.7%	11.0%

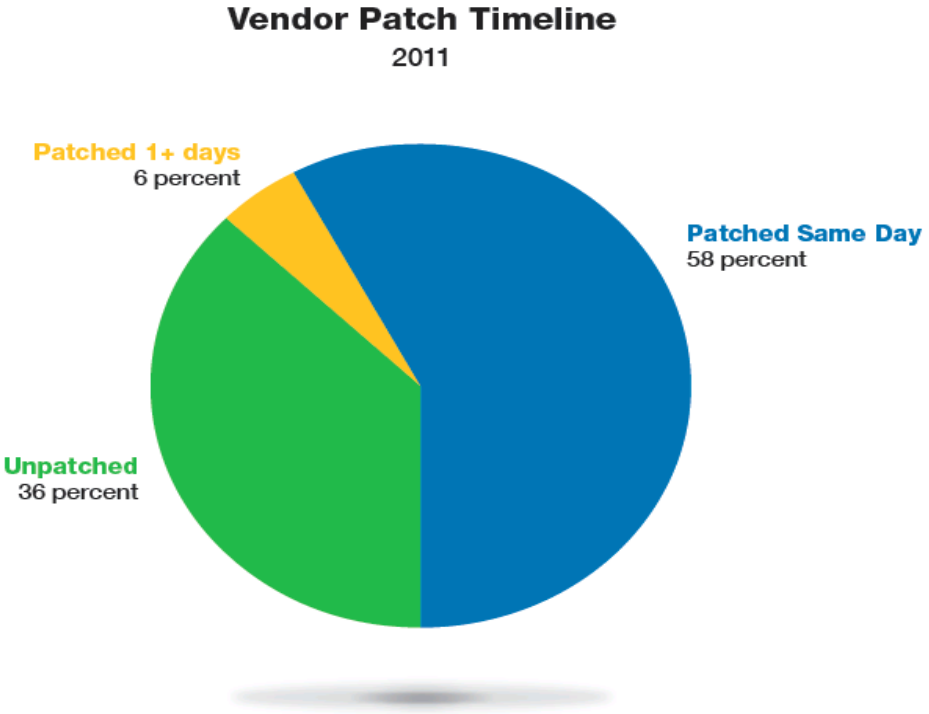
Decline in web application vulnerabilities in 2011

- In 2011 41% of security vulnerabilities affected web applications (-16% YoY) .
- Big decline in SQL Injection





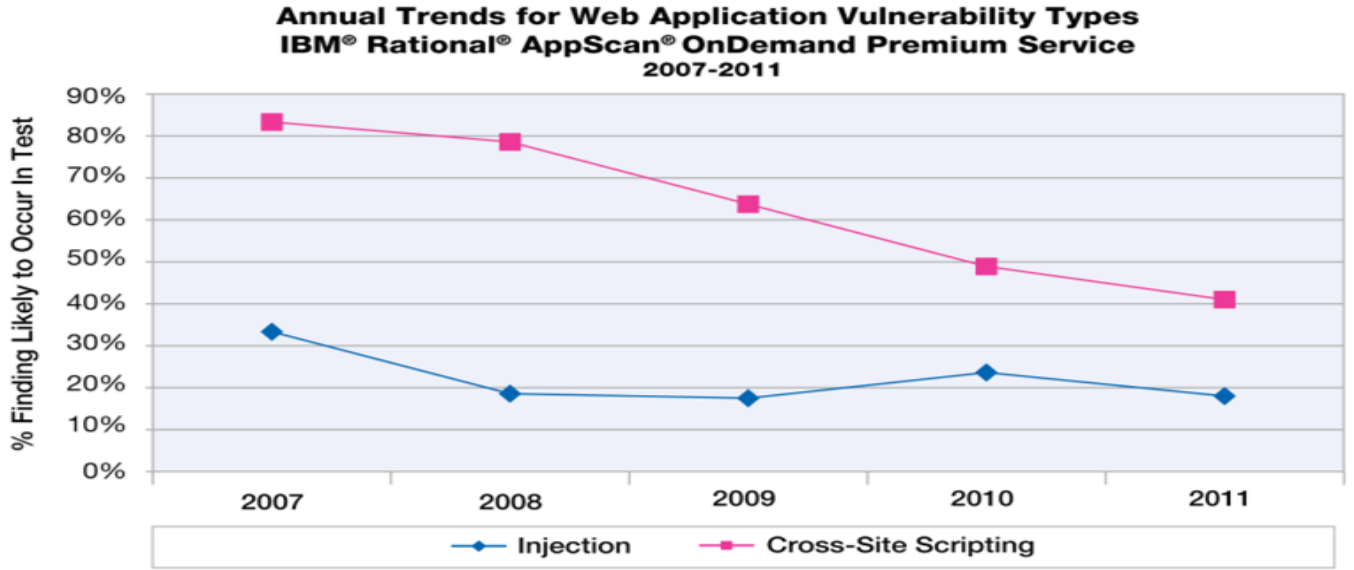
Better Patching



	2011	2010	2009	2008	2007	2006
Unpatched %	36.0%	43.3%	45.1%	51.9%	44.6%	46.6%

Cross Site Scripting (XSS) vulnerabilities

- In 2011 XSS vulnerabilities half as likely to exist in customer's as compared to 4 years ago
- However, XSS vulnerabilities still appear in about 40% of the applications IBM scans
  - High for something well understood and easily addressed

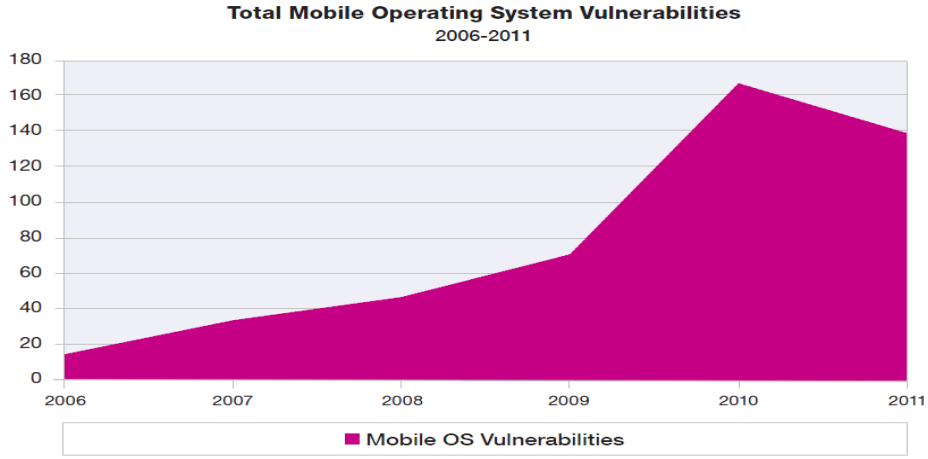


Key Findings from the 2011 Trend Report

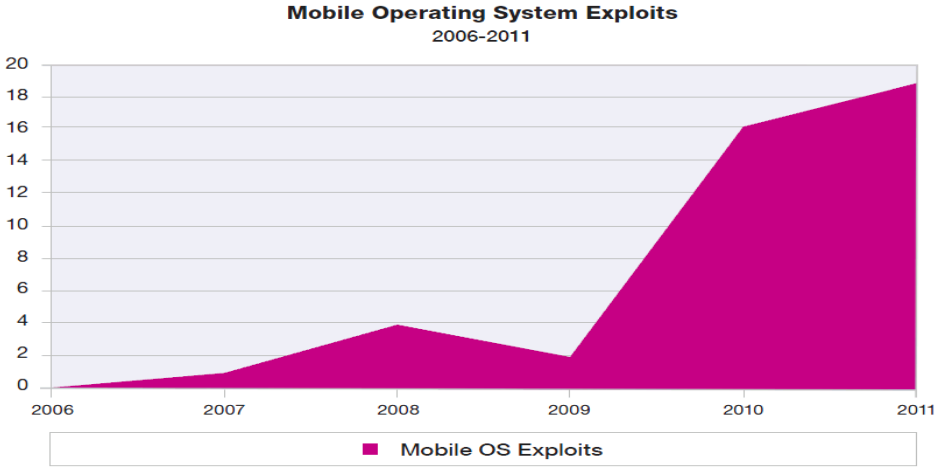
- New Attack Activity
  - Rise in Shell Command Injection attacks
  - Spikes in SSH Brute Forcing
  - Rise in Click Fraud related Phishing
- Progress in Internet Security
  - Fewer exploit releases
  - Fewer web application vulnerabilities
  - Better patching
- The Challenge of Mobile and the Cloud
  - Mobile exploit disclosures up
  - Cloud requires new thinking
  - Social Networking no longer fringe pastime

Mobile OS Vulnerabilities and Exploits

- Continued interest in Mobile vulnerabilities as enterprise users bring smartphones and tablets into the work place



- Attackers finally warming to the opportunities these devices represent

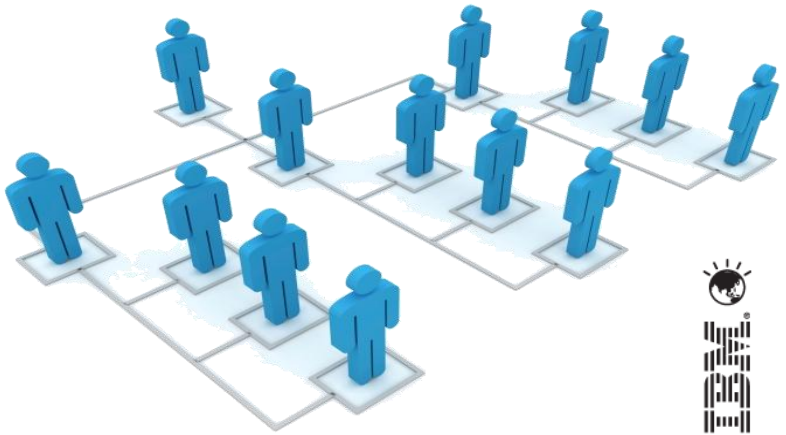


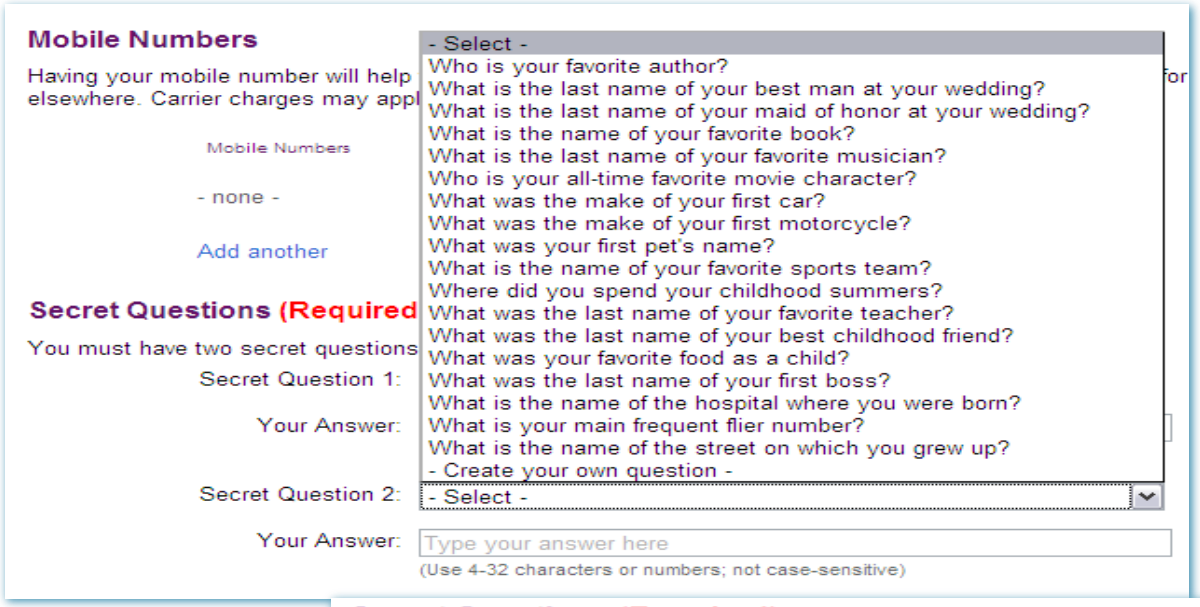
The Challenges of Cloud Security

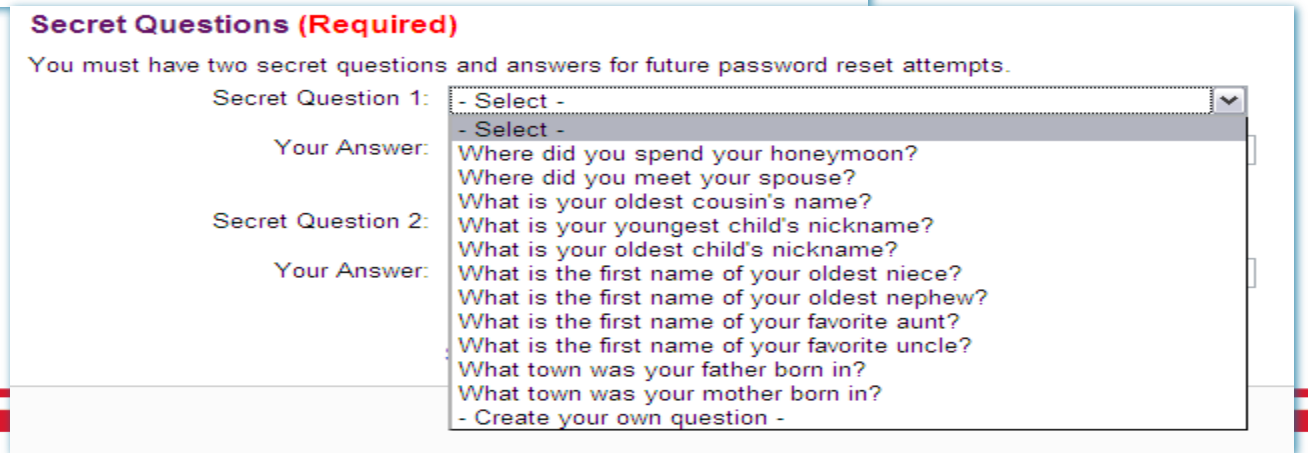
- There is still confusion on what Cloud is
  - Principles of web applications and SaaS apply
- Additionally Cloud Security Requires:
  - A cloud-appropriate workload
  - A well coordinated Identity and Access Management (e.g. federation)
  - Log Management and Security Intelligence fundamental
- Not everything is on a cloud architecture
  - Security must work across traditional and cloud.

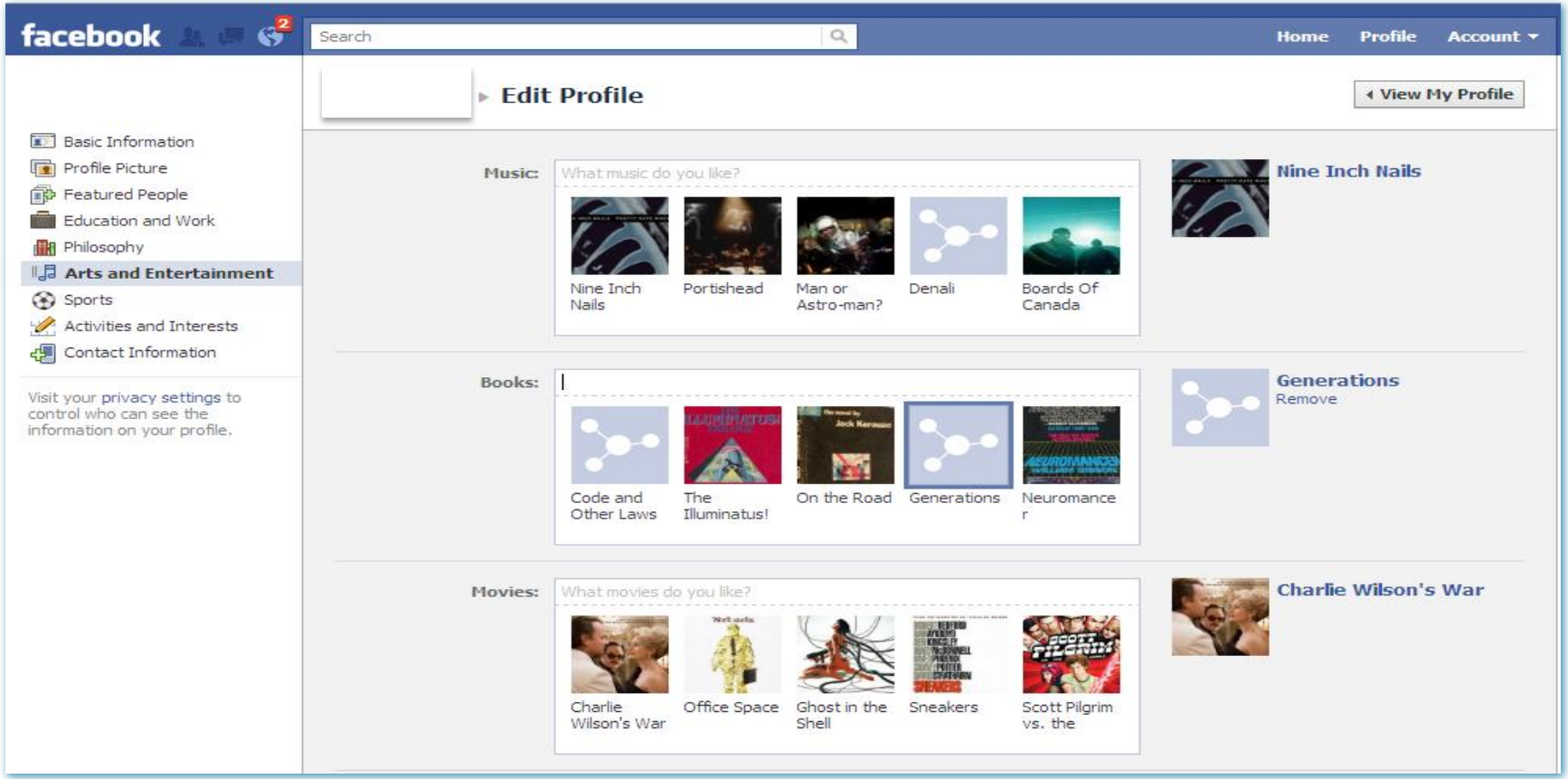
Social Networking – no longer a fringe pastime

- Attackers finding social networks ripe with valuable information they can mine to build intelligence about organizations and its staff:
  - Scan corporate websites, Google, Google News
    - Who works there? What are their titles?
    - Create index cards with names and titles
  - Search Linkedin, Facebook, Twitter profiles
    - Who are their colleagues?
    - Start to build an org chart
  - Who works with the information the attacker would like to target?
    - What is their reporting structure?
    - Who are their friends?
    - What are they interested in?
    - What are their work/personal email addresses?

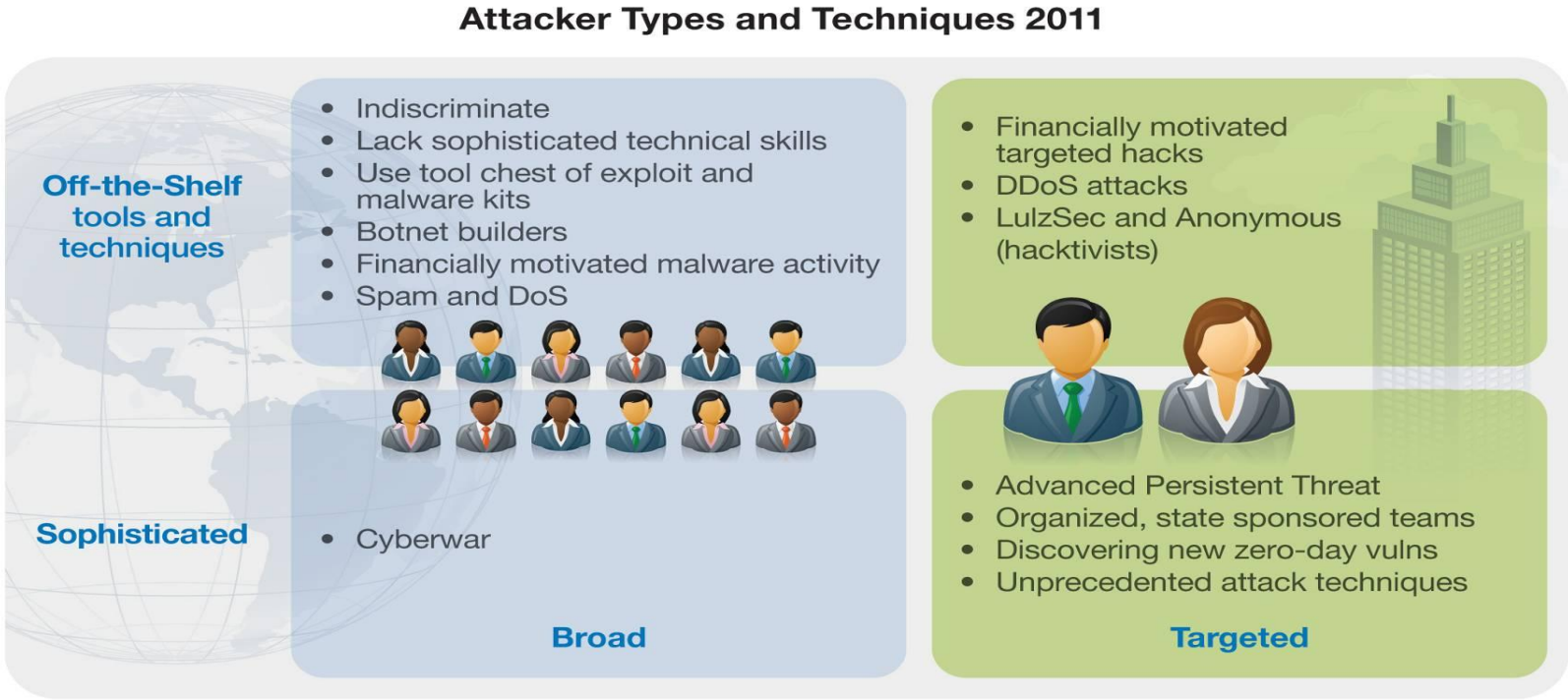



Mobile Numbers
Having your mobile number will help
elsewhere. Carrier charges may appl
for
Mobile Numbers
- none -
Add another
Secret Questions (Required
You must have two secret questions
Secret Question 1:
Your Answer:
Secret Question 2:
Your Answer:
- Select -
Who is your favorite author?
What is the last name of your best man at your wedding?
What is the last name of your maid of honor at your wedding?
What is the name of your favorite book?
What is the last name of your favorite musician?
Who is your all-time favorite movie character?
What was the make of your first car?
What was the make of your first motorcycle?
What was your first pet's name?
What is the name of your favorite sports team?
Where did you spend your childhood summers?
What was the last name of your favorite teacher?
What was the last name of your best childhood friend?
What was your favorite food as a child?
What was the last name of your first boss?
What is the name of the hospital where you were born?
What is your main frequent flier number?
What is the name of the street on which you grew up?
- Create your own question -
- Select -
Type your answer here
(Use 4-32 characters or numbers; not case-sensitive)


Secret Questions (Required)
You must have two secret questions and answers for future password reset attempts.
Secret Question 1:
Your Answer:
Secret Question 2:
Your Answer:
- Select -
- Select -
Where did you spend your honeymoon?
Where did you meet your spouse?
What is your oldest cousin's name?
What is your youngest child's nickname?
What is your oldest child's nickname?
What is the first name of your oldest niece?
What is the first name of your oldest nephew?
What is the first name of your favorite aunt?
What is the first name of your favorite uncle?
What town was your father born in?
What town was your mother born in?
- Create your own question -


facebook
Search
Home
Profile
Account
Edit Profile
View My Profile
Basic Information
Profile Picture
Featured People
Education and Work
Philosophy
Arts and Entertainment
Sports
Activities and Interests
Contact Information
Visit your privacy settings to control who can see the information on your profile.
Music:
What music do you like?
Nine Inch Nails
Portishead
Man or Astro-man?
Denali
Boards Of Canada
Nine Inch Nails
Books:
Code and Other Laws
The Illuminatus!
On the Road
Generations
Neuromancer
Generations
Remove
Movies:
What movies do you like?
Charlie Wilson's War
Office Space
Ghost in the Shell
Sneakers
Scott Pilgrim vs. the
Charlie Wilson's War

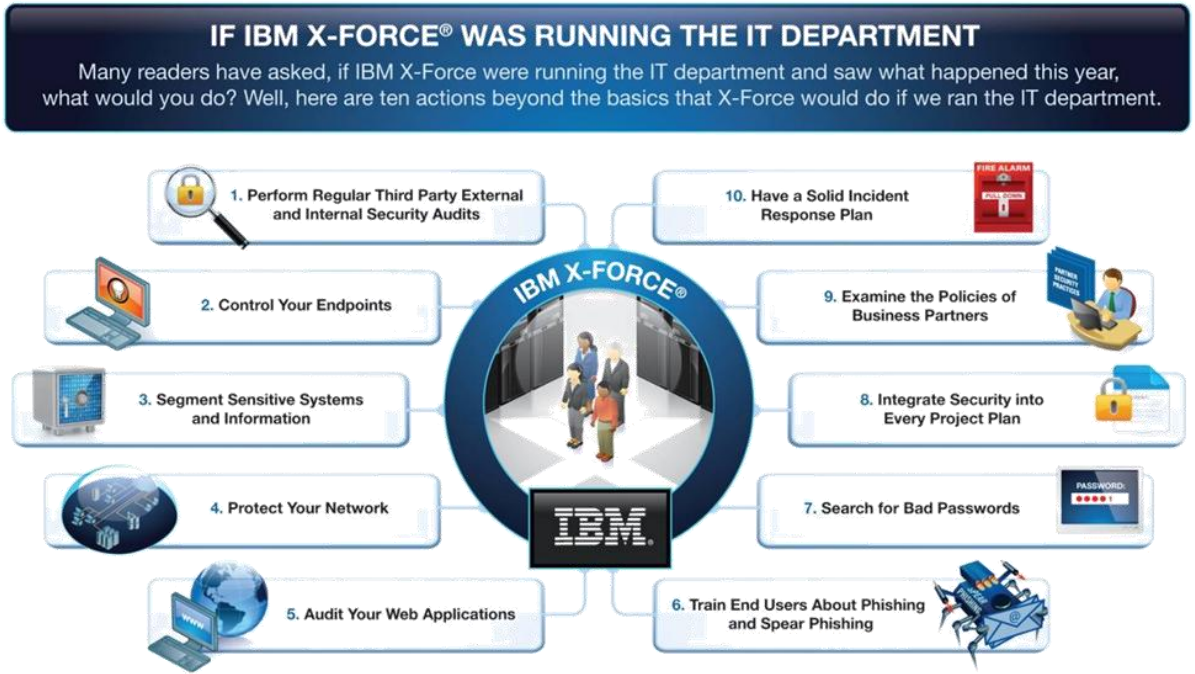
Who is attacking our networks?



Source: IBM X-Force® Research and Development

Not a technical problem, but a business challenge

- Many of the 2011 breaches could have been prevented
- Significant effort is required to inventory, identify, and close every vulnerability
- Financial & operational resistance is always encountered, so how much of an investment is enough?

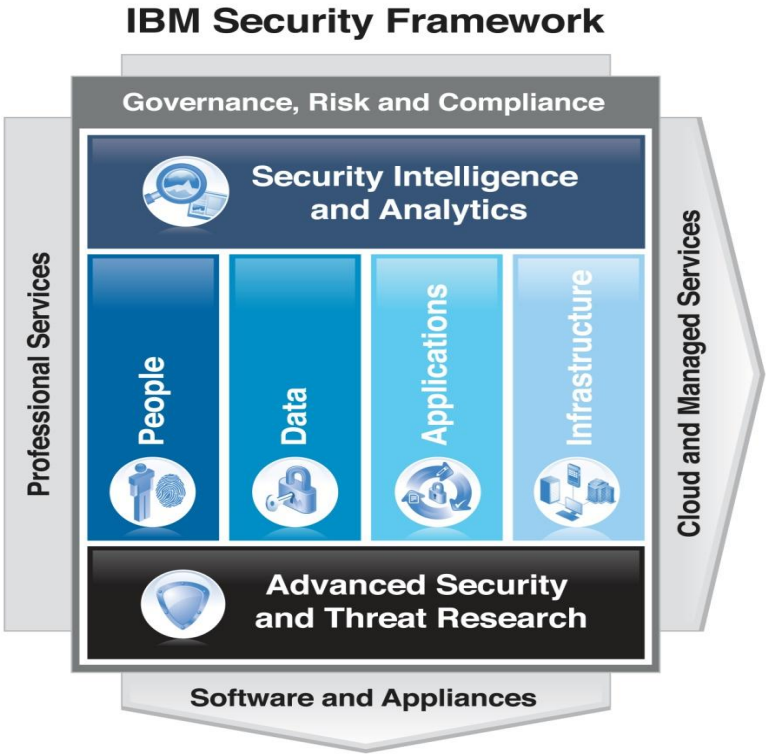


IBM Security: Delivering intelligence, integration and expertise across a comprehensive framework

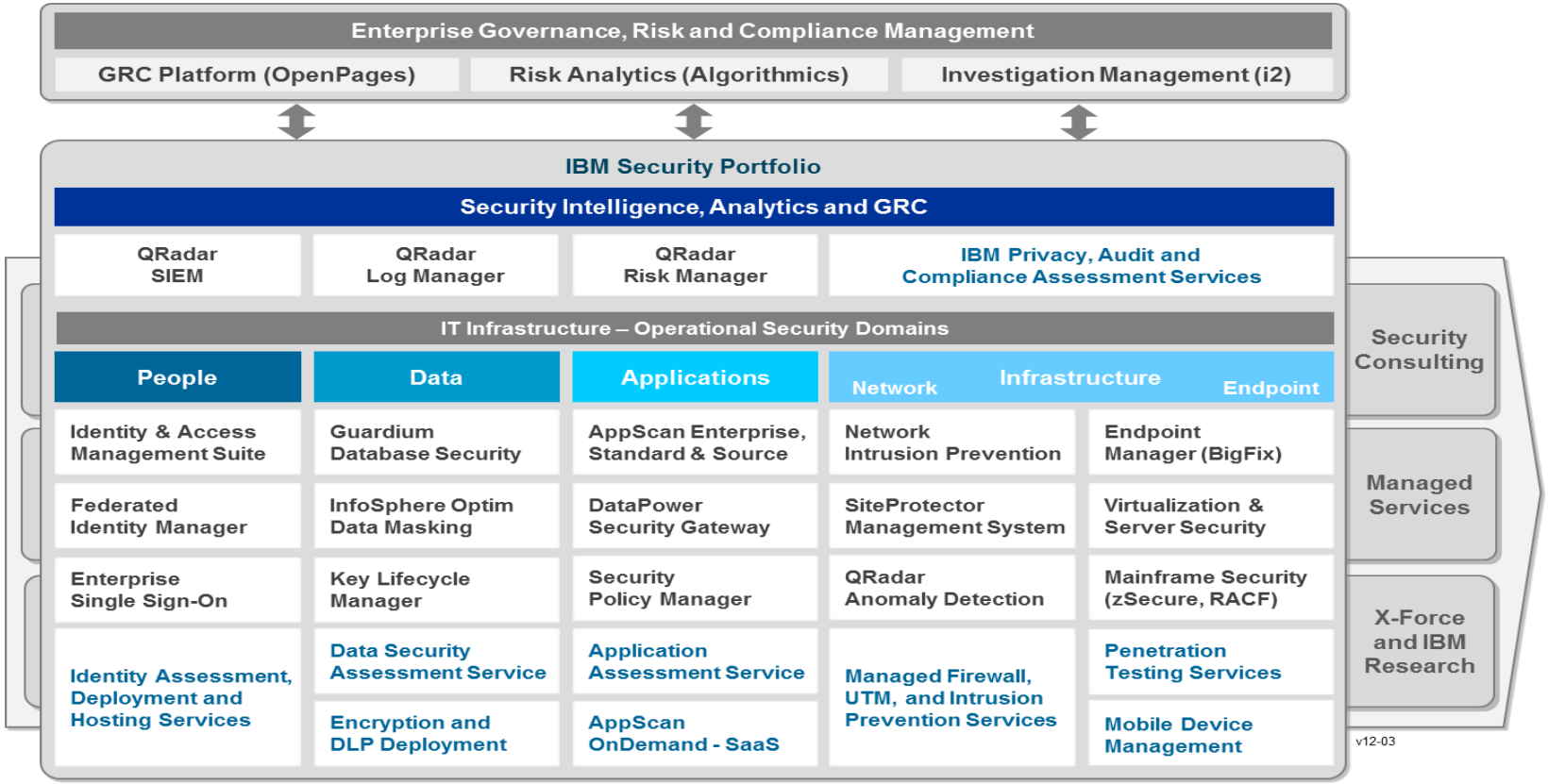
IBM Security Systems

- Only vendor in the market with end-to-end coverage of the security foundation
- 6K+ security engineers and consultants
- Award-winning X-Force® research
- Largest vulnerability database in the industry

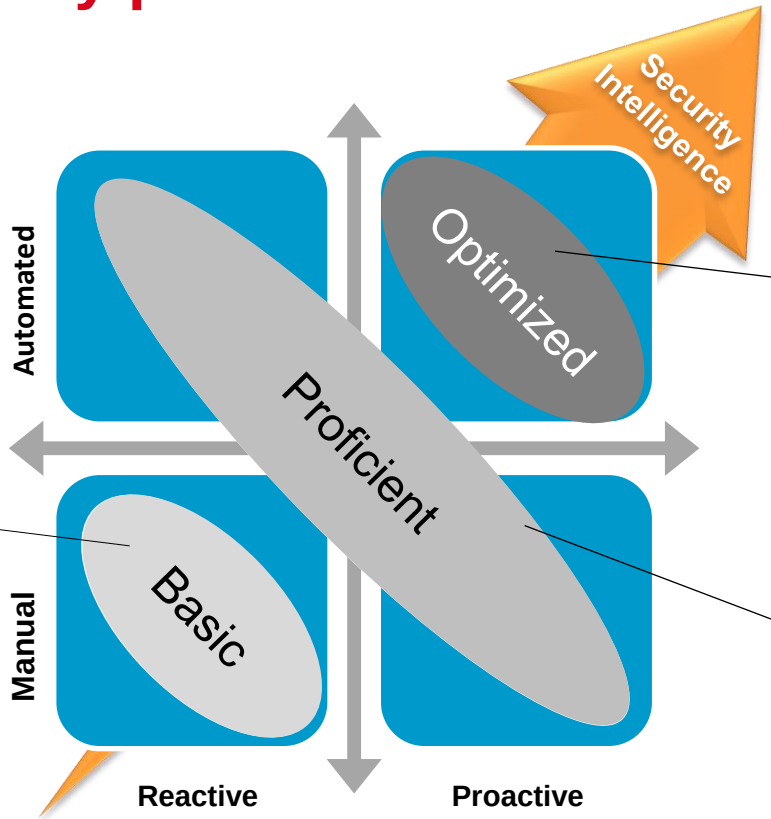
Intelligence . Integration . Expertise



Leading products and services in every segment



To help IBM's customer achieving an intelligent view of their security posture



Basic
Organizations employ ***perimeter protection***, which regulates access and feeds manual reporting

Optimized
Organizations use ***predictive and automated*** security analytics to drive toward ***security intelligence***

Proficient
Security is layered into the ***IT fabric*** and ***business operations***

Get Engaged with IBM X-Force Research and Development

Follow us at @ibmsecurity and @ibmxforce

Download X-Force security trend & risk reports

http://www-935.ibm.com/services/us/iss/xforce/

Subscribe to X-Force alerts at http://iss.net/rss.php or Frequency X at http://blogs.iss.net/rss.php

Attend in-person events

http://www.ibm.com/events/calendar/

Join the Institute for Advanced Security

www.instituteforadvancedsecurity.com

Subscribe to the security channel for latest security videos

www.youtube.com/ibmsecuritysolutions

Trademarks and disclaimers

The customer examples described are presented as illustrations of how those customers have used IBM products and the results they may have achieved. Actual environmental costs and performance characteristics may vary by customer.

Information concerning non-IBM products was obtained from a supplier of these products, published announcement material, or other publicly available sources and does not constitute an endorsement of such products by IBM. Sources for non-IBM list prices and performance numbers are taken from publicly available information, including vendor announcements and vendor worldwide homepages. IBM has not tested these products and cannot confirm the accuracy of performance, capability, or any other claims related to non-IBM products. Questions on the capability of non-IBM products should be addressed to the supplier of those products.

All statements regarding IBM future direction and intent are subject to change or withdrawal without notice, and represent goals and objectives only.

Some information addresses anticipated future capabilities. Such information is not intended as a definitive statement of a commitment to specific levels of performance, function or delivery schedules with respect to any future products. Such commitments are only made in IBM product announcements. The information is presented here to communicate IBM's current investment and development activities as a good faith effort to help with our customers' future planning.

Performance is based on measurements and projections using standard IBM benchmarks in a controlled environment. The actual throughput or performance that any user will experience will vary depending upon considerations such as the amount of multiprogramming in the user's job stream, the I/O configuration, the storage configuration, and the workload processed. Therefore, no assurance can be given that an individual user will achieve throughput or performance improvements equivalent to the ratios stated here.

Prices are suggested U.S. list prices and are subject to change without notice. Starting price may not include a hard drive, operating system or other features. Contact your IBM representative or Business Partner for the most current pricing in your geography.

Photographs shown may be engineering prototypes. Changes may be incorporated in production models.