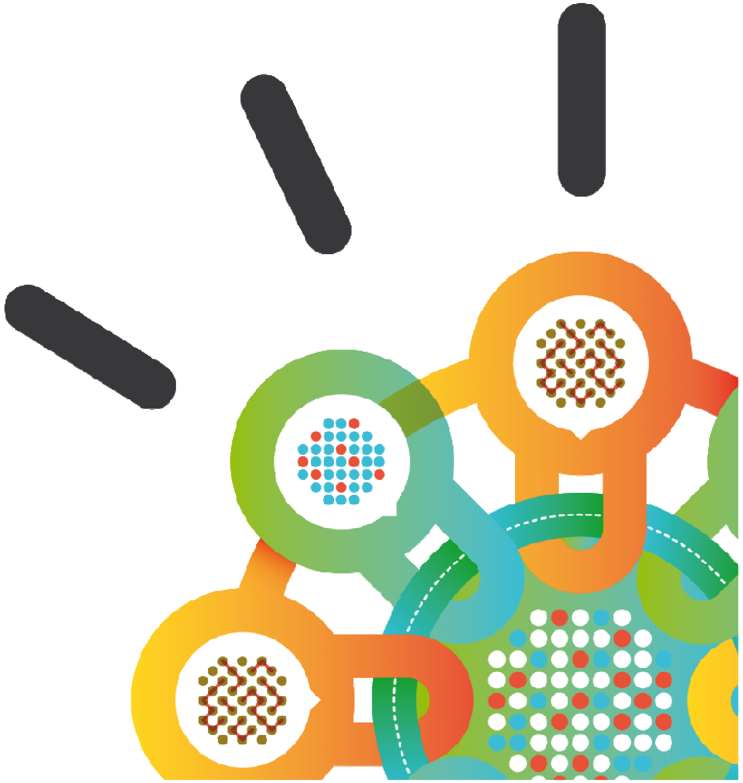
Security Intelligence.
Think Integrated.

IBM X-Force® 2012 Cyber Security Threat Landscape

Rohit Umashankar Satayanarayana,
Enterprise Security Architect, Tiger Team,
IBM Asia Pacific



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
54K	documented vulnerabilities
13 billion	security events monitored daily

Provides Specific Analysis of:

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

To find out how forward thinkers are harnessing all this data, we asked…

138 security leaders
– in seven counties across a wide
range of industries

With explosive growth in connectivity and collaboration, information security is becoming increasingly complex and difficult to manage

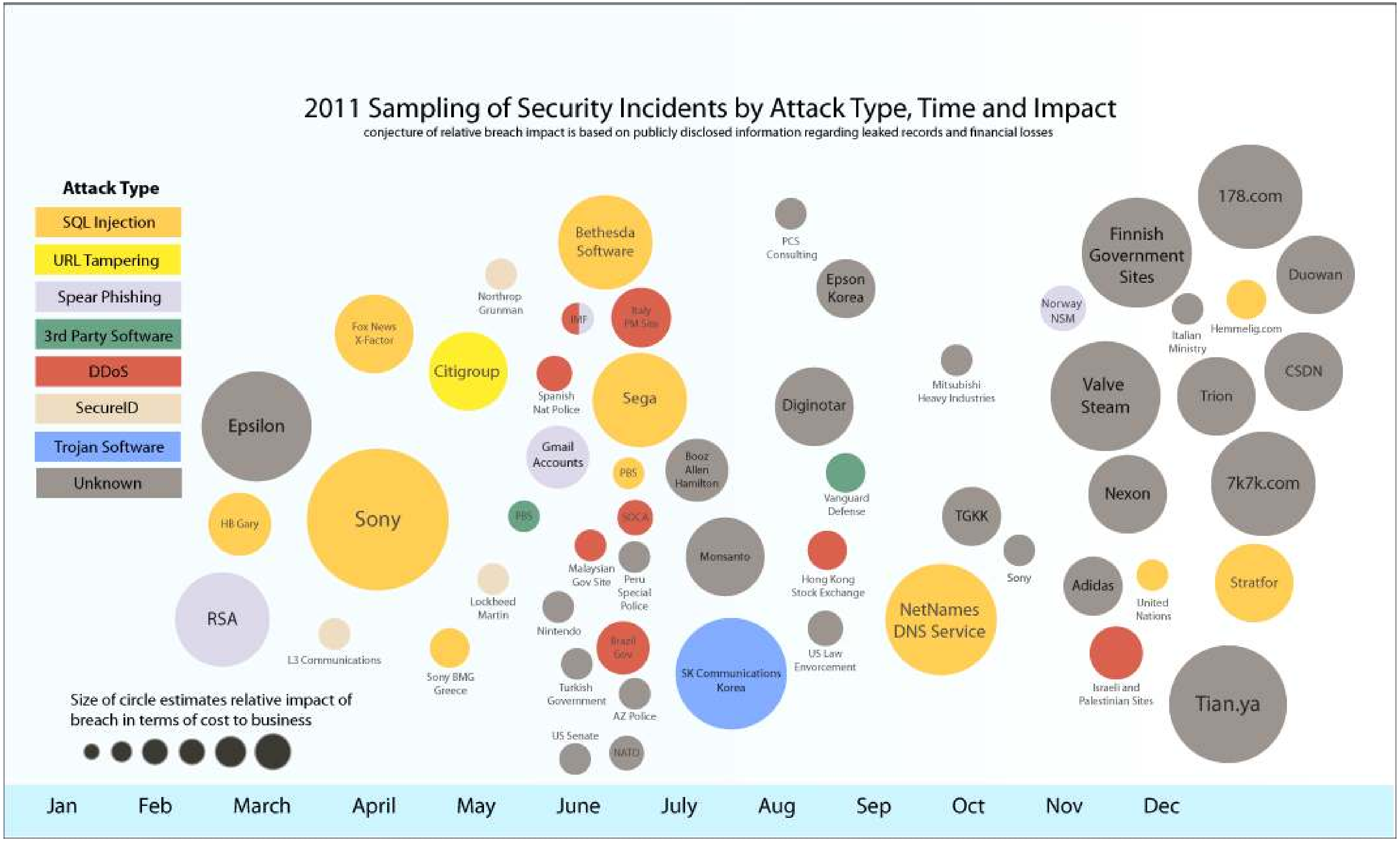
In 2011, the corporate world experienced the second highest data loss total since 2004

The number of mobile workers is expected to reach 1.3 billion by 2015

At the same time, mobile security threats are increasing – up almost 20 percent in 2011

Sources: Verizon 2012 Data Breach Investigations Report; IDC

2011: Year of the Security Breach



2011 Sampling of Security Incidents by Attack Type, Time and Impact

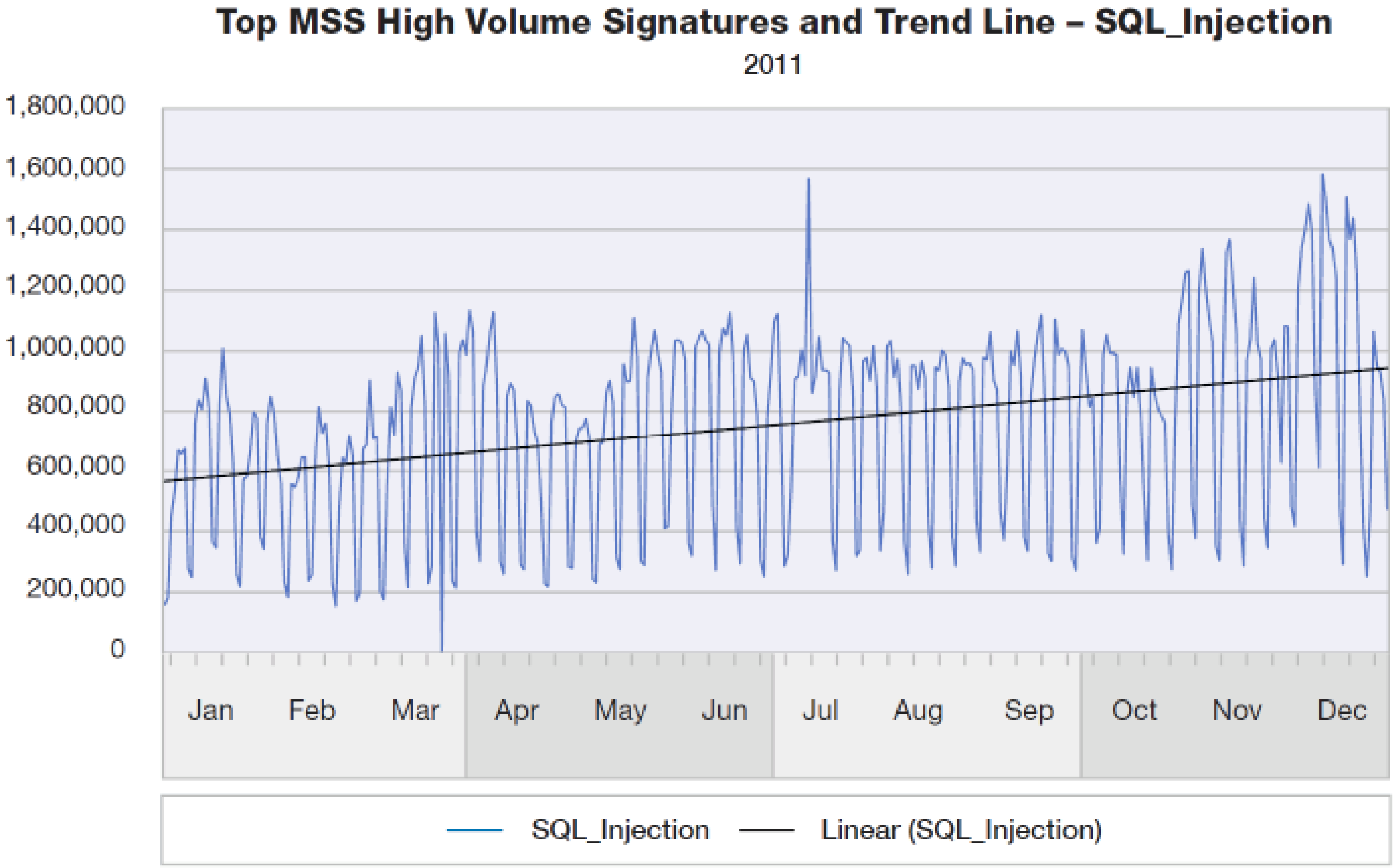
conjecture of relative breach impact is based on publicly disclosed information regarding leaked records and financial losses

Size of circle estimates relative impact of breach in terms of cost to business

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

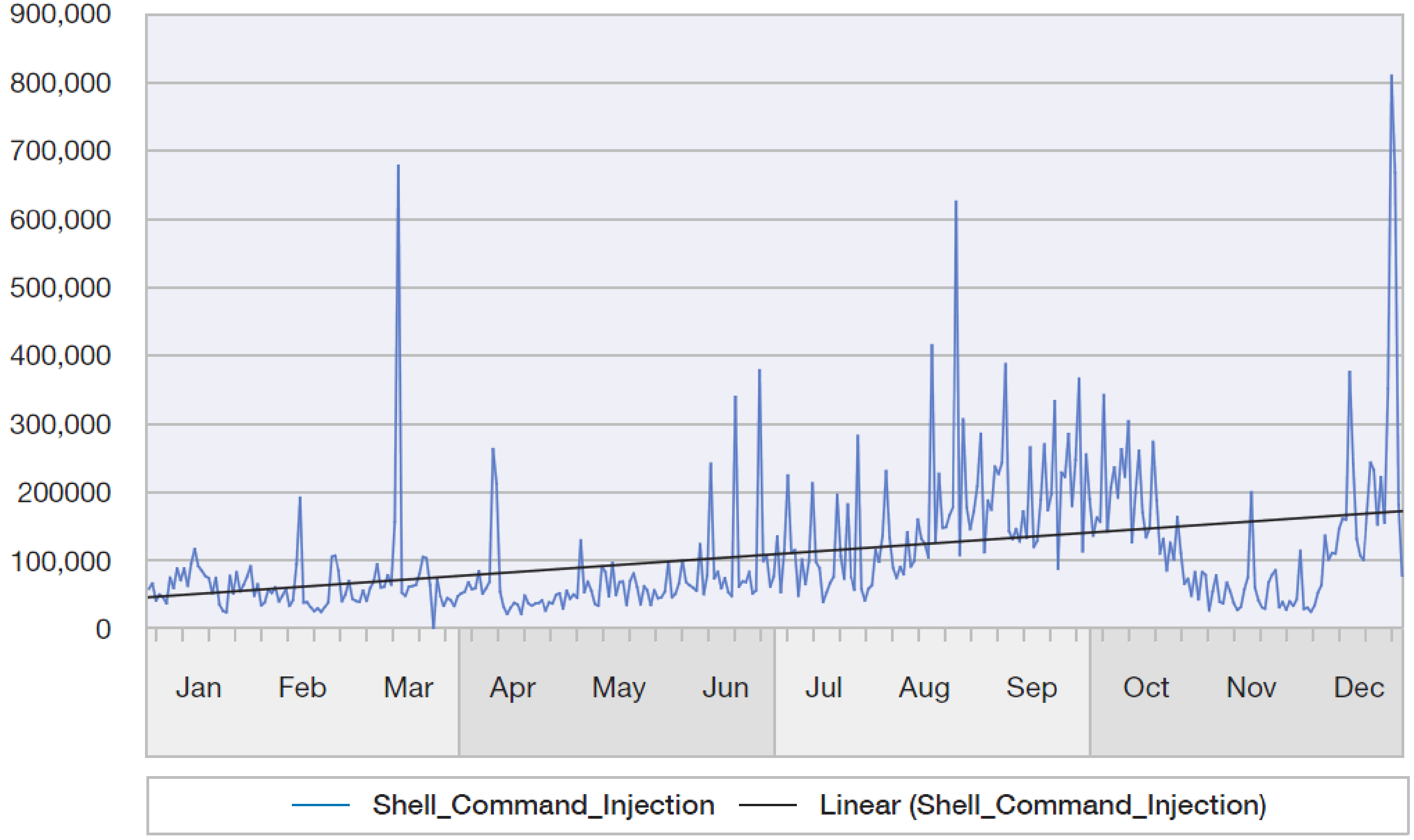
SQL Injection Attacks against Web Servers



Shell Command Injection Attacks

Top MSS High Volume Signatures and Trend Line – Shell_Command_Injection

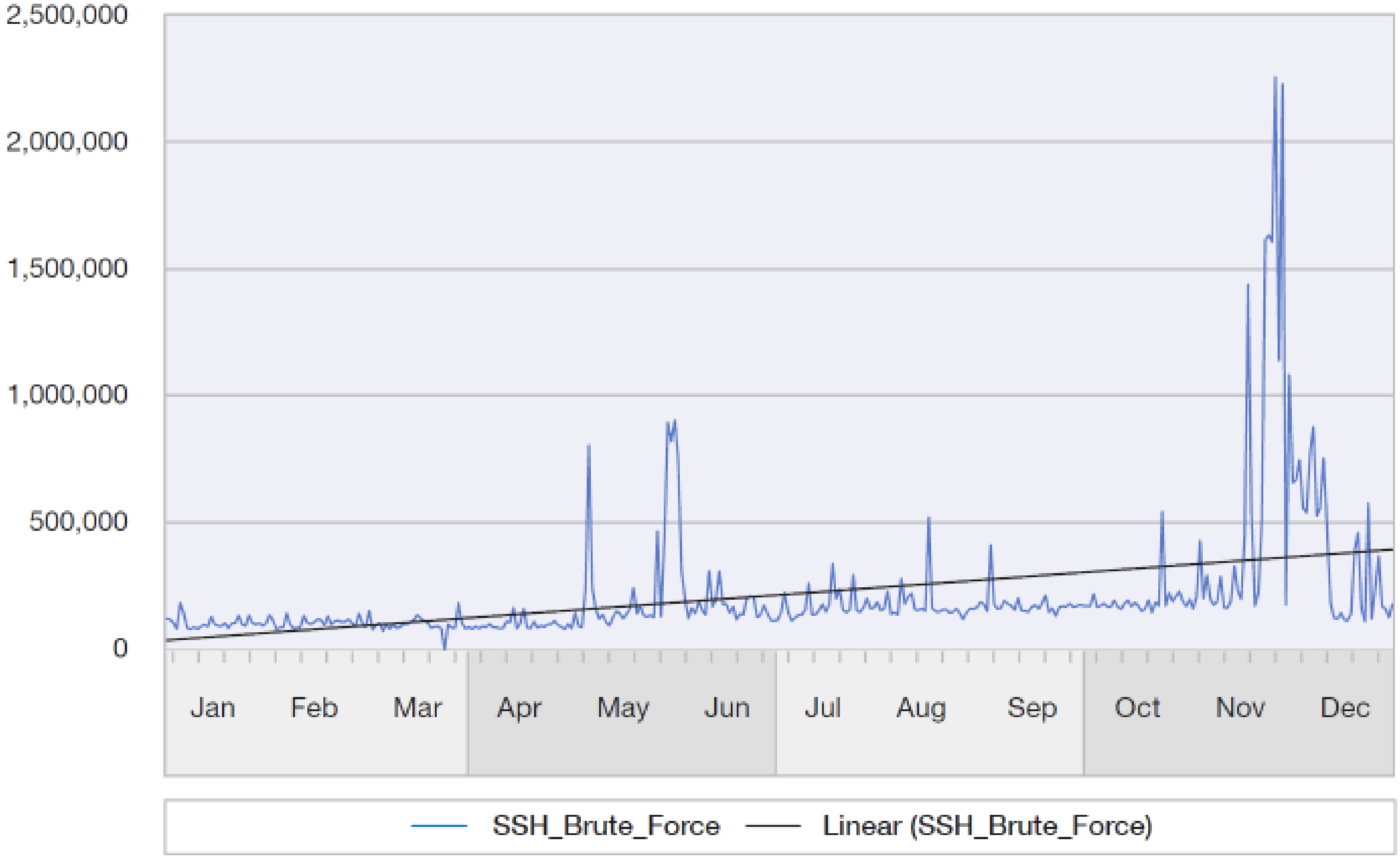
2011



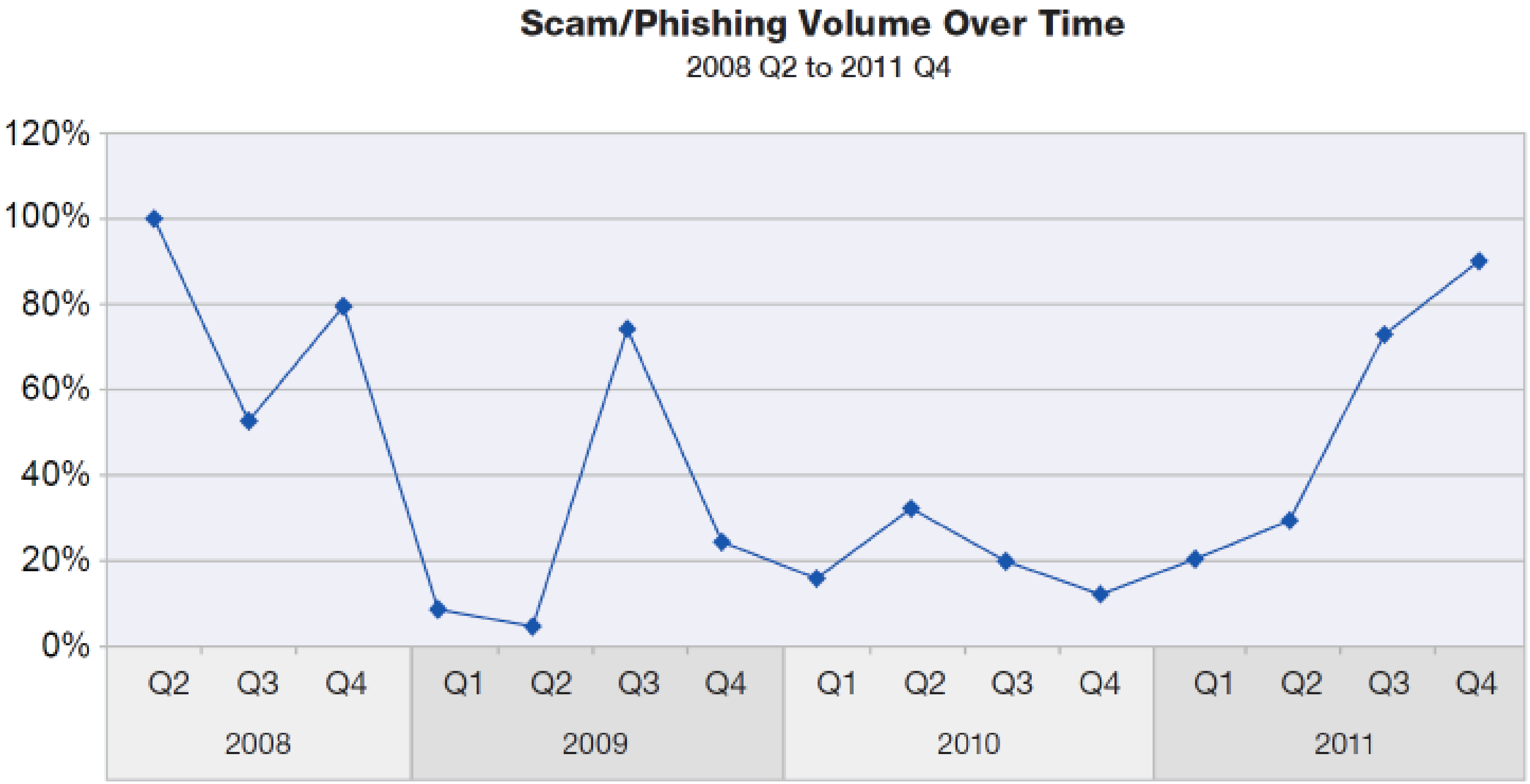
SSH Brute Force Activity

Top MSS High Volume Signatures and Trend Line – SSH_Brute_Force

2011

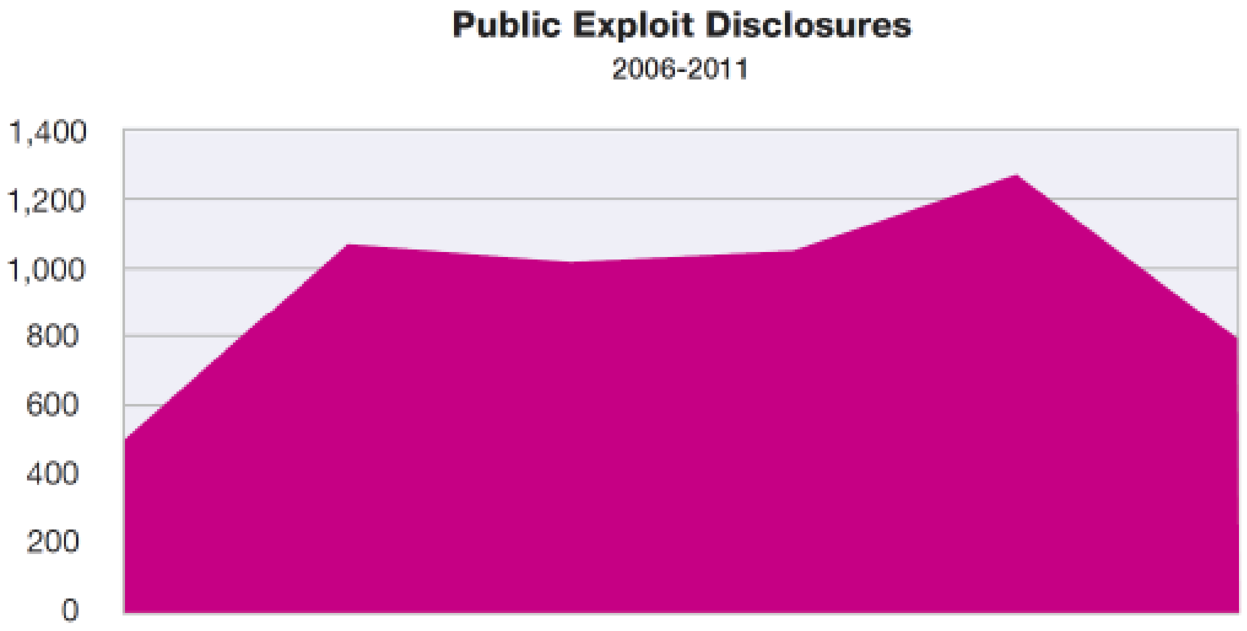


Phishing based malware distribution and click fraud



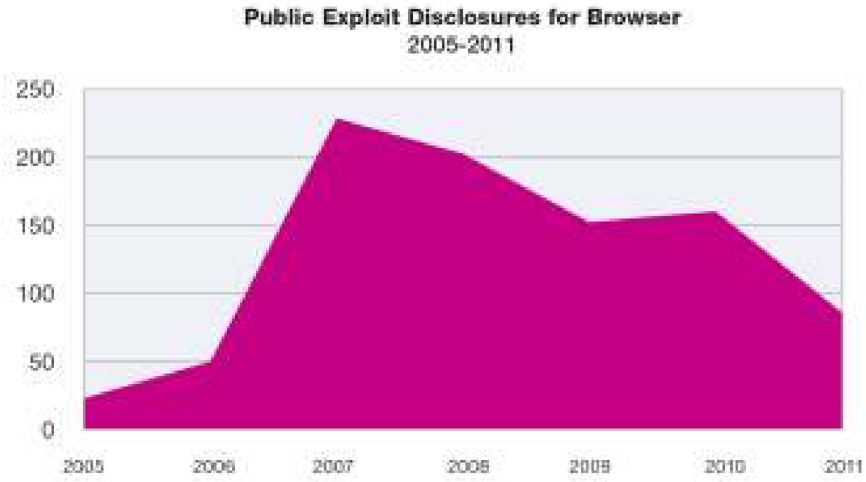
Public Exploit Disclosures

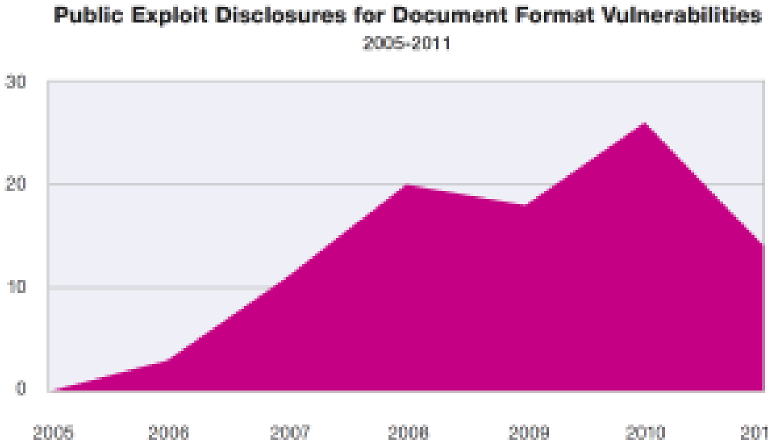
- Fewer exploits released so far this year since 2006
- Down as a percentage of vulnerabilities as well

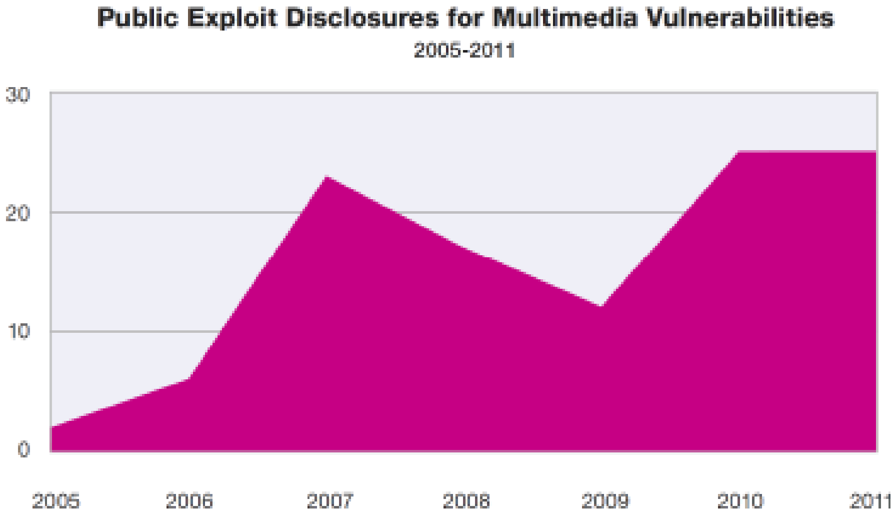


	2006	2007	2008	2009	2010	2011
Public Exploits	504	1078	1025	1059	1280	778
Percentage of Total	7.3%	16.5%	13.3%	15.6%	14.7%	11.0%

Public Exploits





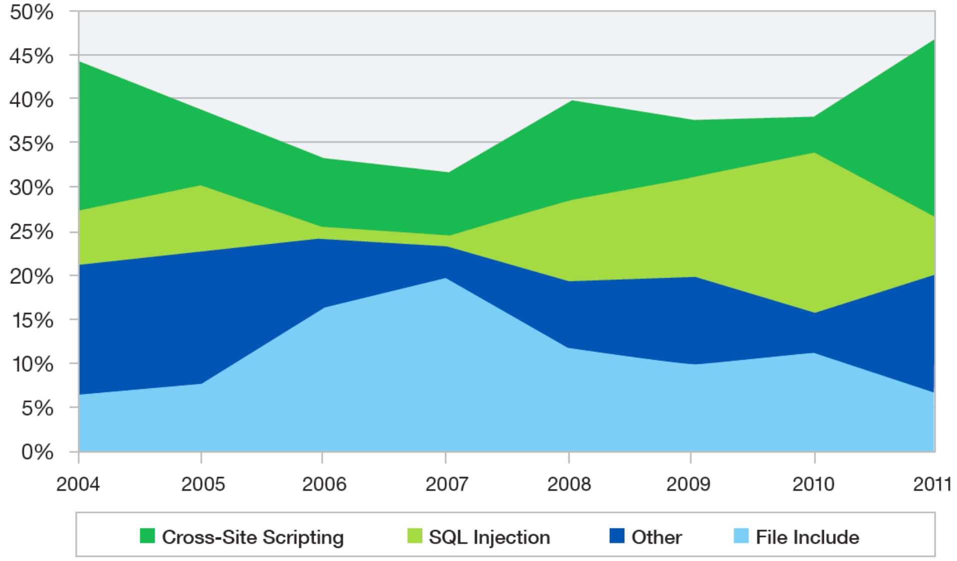


Decline in web application vulnerabilities in 2011

- In 2010 49% of security vulnerabilities affected web applications.
- In 2011 41% affected web applications.
- Big decline in SQL Injection

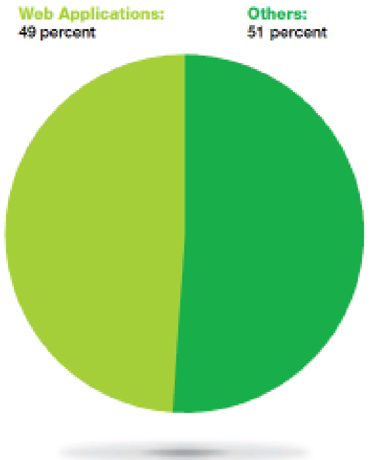
Web Application Vulnerabilities by Attack Technique

2004-2011



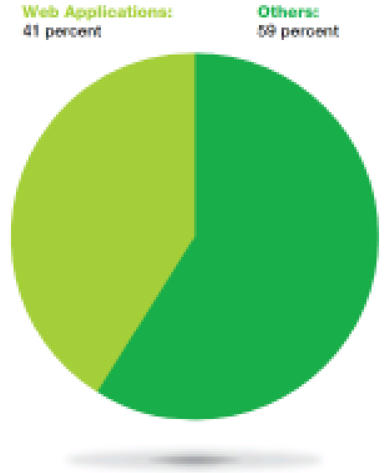
Web Application Vulnerabilities

as a Percentage of All Disclosures in 2010

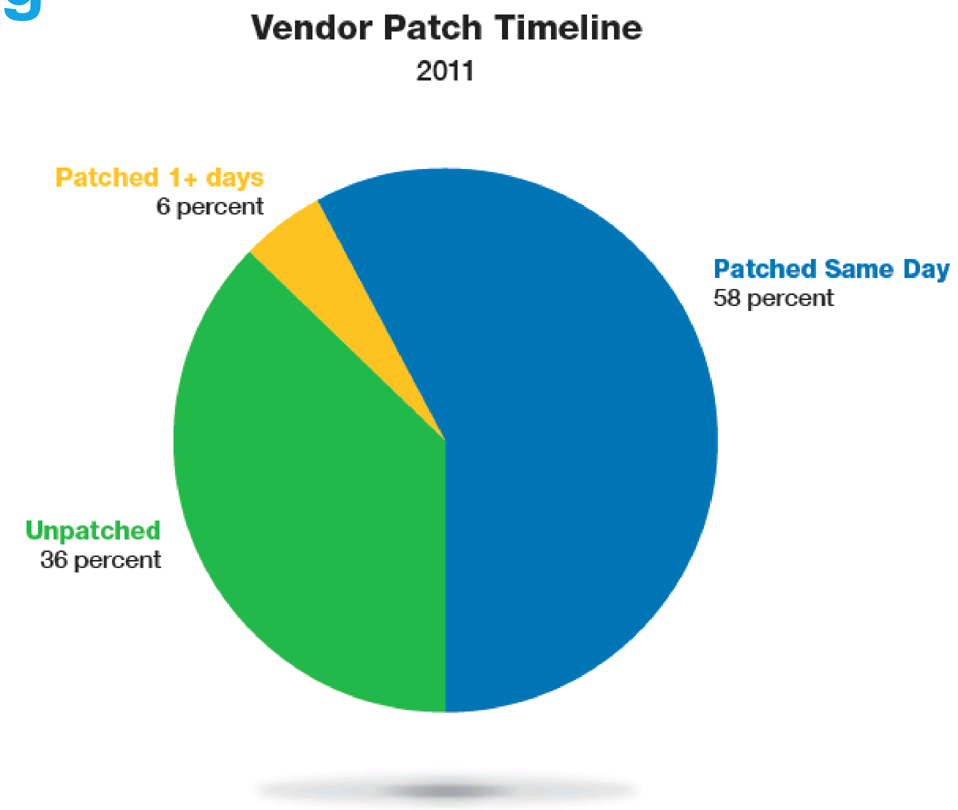


Web Application Vulnerabilities

as a Percentage of All Disclosures in 2011



Better Patching



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

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

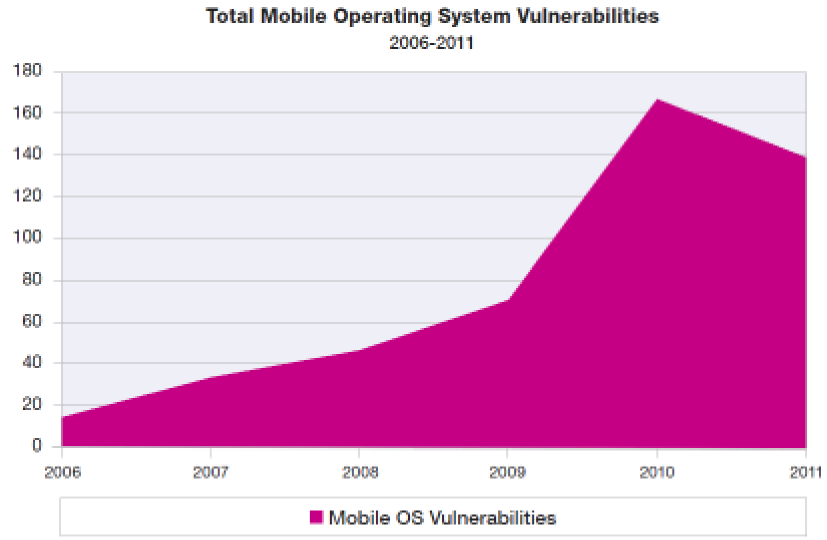
- Progress in Internet Security
  - Fewer exploit releases
  - Fewer web application vulnerabilities
  - Better patching

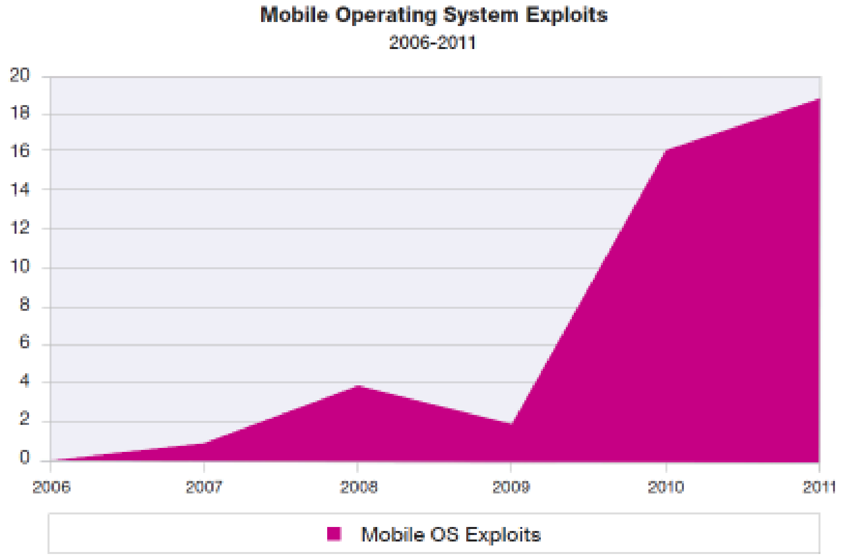
- The Challenge of Mobile and the Cloud
  - Mobile exploit disclosures up
  - Cloud requires new thinking

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

- In 2011, there were many high profile cloud breaches, affecting well-known organizations and large populations of their customers.

- Cloud Security Requires:
  - A cloud-appropriate workload
  - Effective due diligence on the part of the customer
  - Flexibility on the part of the cloud provider

- Cloud customers should take a lifecycle view of the cloud deployment, including what the exit strategy should be if things don't work out.

Get Engaged with IBM X-Force Research and Development

Follow us at @ibmsecurity and @ibmxforce

Download X-Force security trend & risk reports http://ibm.co/hksecurity

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