Security Intelligence.
Think Integrated.

Inside the Threats through the X-Force Eye

IBM X-Force 2012 Mid-Year Trend and Risk Report

IBM X-Force 2012 Mid-Year 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

17B	analyzed Web pages & images
40M	spam & phishing attacks per month
68K	documented vulnerabilities
15B	security events monitored daily

Provides Specific Analysis of:

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

What are we seeing? Key Findings from the 2012 Trend Report

Progress in Internet Security

- Fewer vulnerabilities disclosed for mobile
- Sandbox used to block PDF attacks
- Better patching from Top 10 Vendors

But…

New Attack Activity

- SQL Injection & XSS still at the top
- Obfuscation techniques to evade IPS & AV
- Mac Malware bypasses OS X security

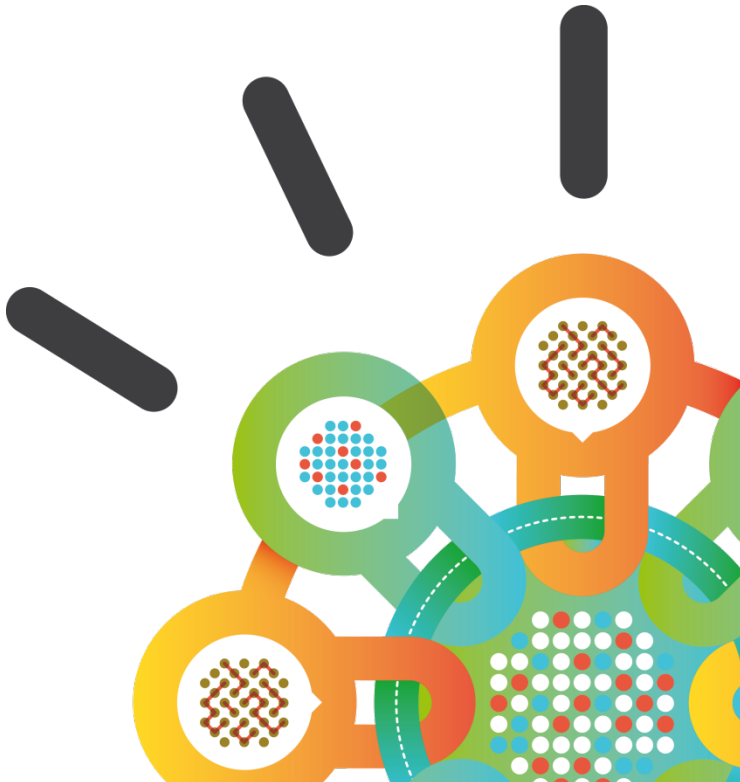
The Challenges

- Password security
- Bring Your Own Device (BYOD)
- Advanced Persistent Threats (APT)

Security Intelligence.
Think Integrated.

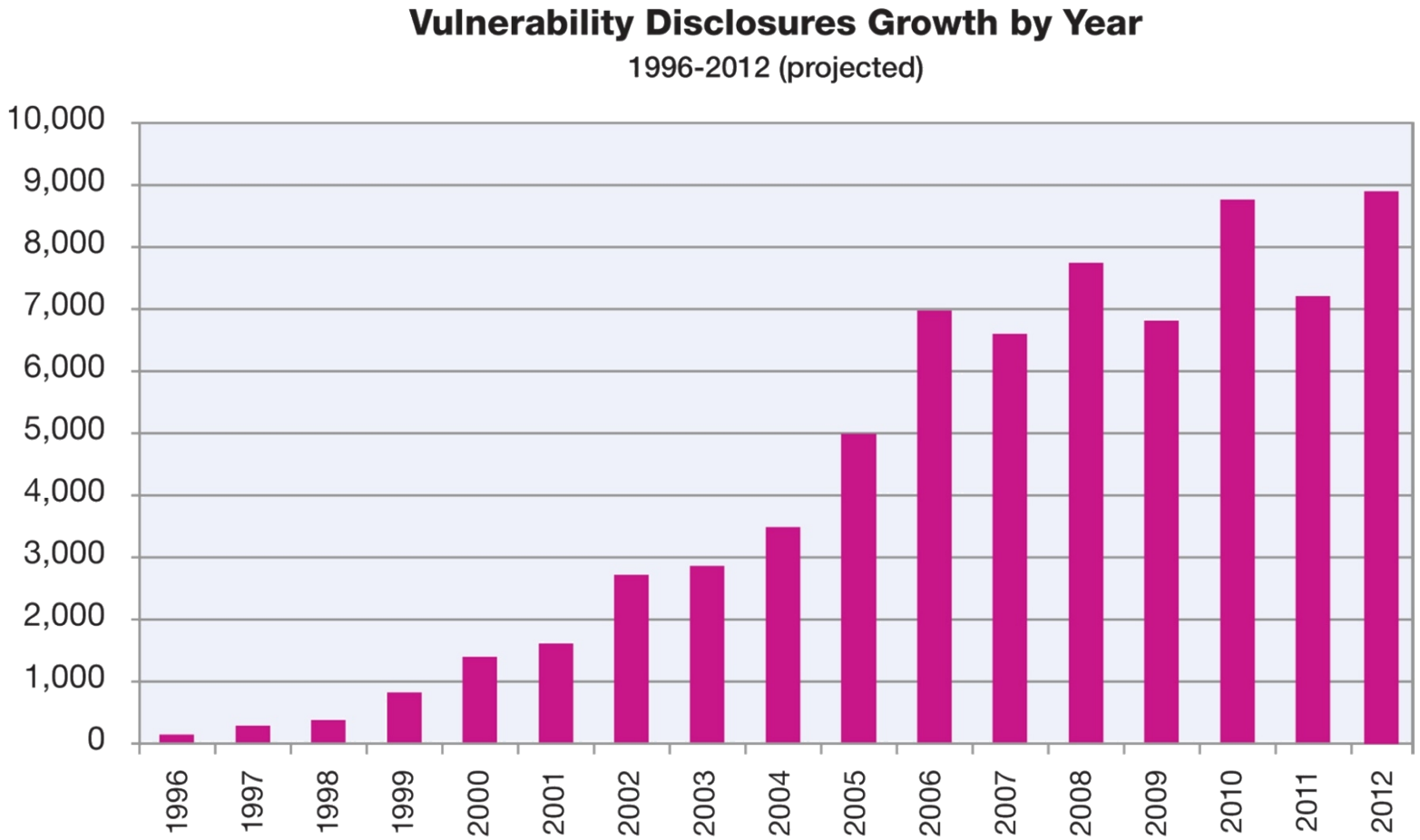
Progress in Internet Security

- Fewer vulnerabilities disclosed for mobile
- Sandbox used to block PDF attacks
- Better patching from Top 10 Vendors



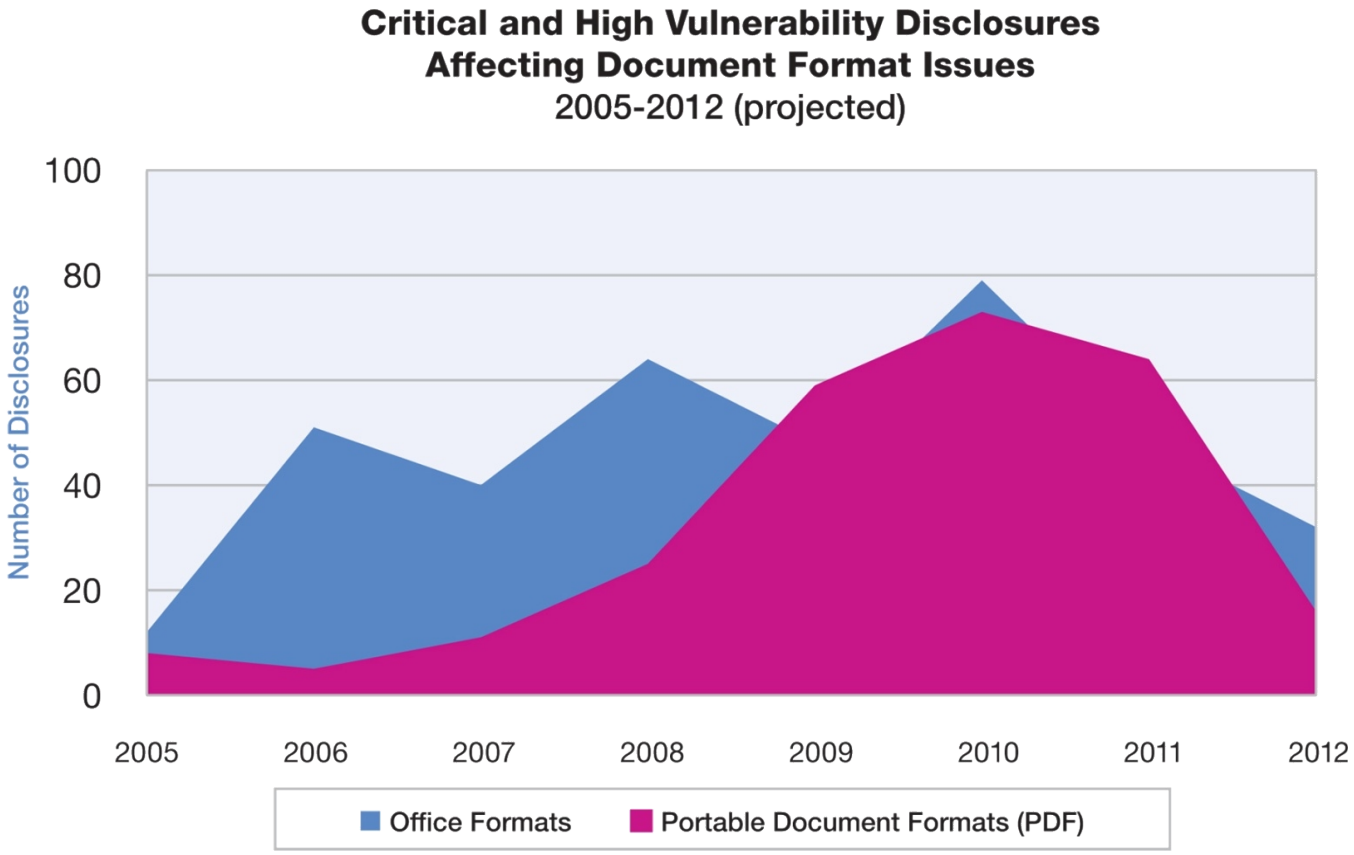
Vulnerability disclosures up in 2012

- Total number of vulnerabilities grew (4'400 in 1H 2012)
  - the projection is for an all time high in 2012

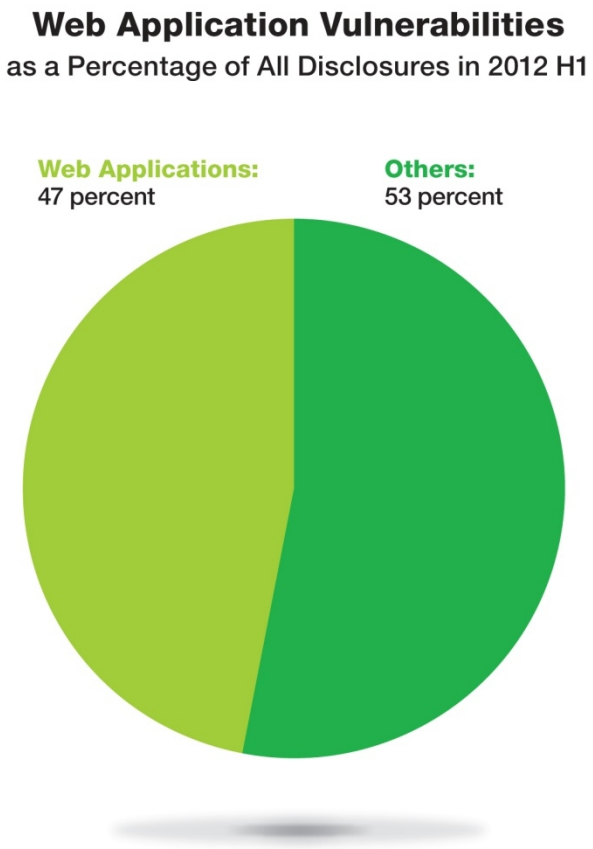


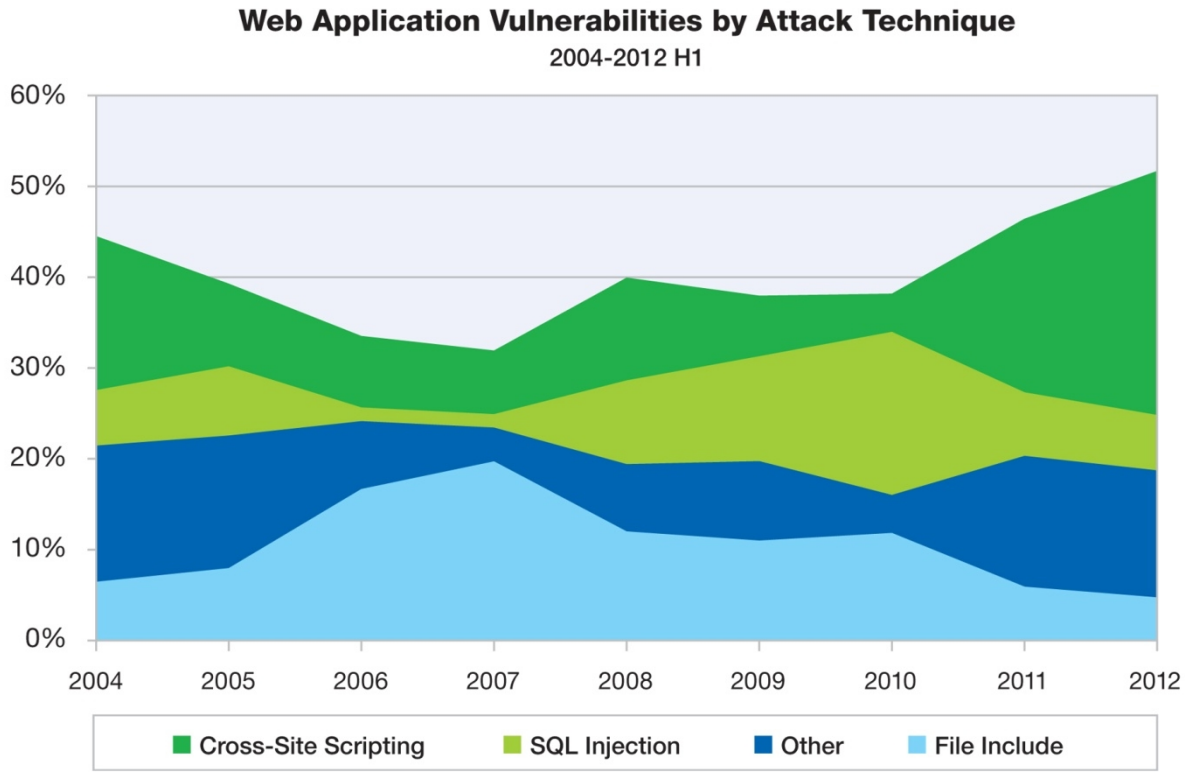
Dramatic Drop of PDF Vulnerabilities

- Sandbox is proving successful
  - We have to keep alert against enhanced attack techniques



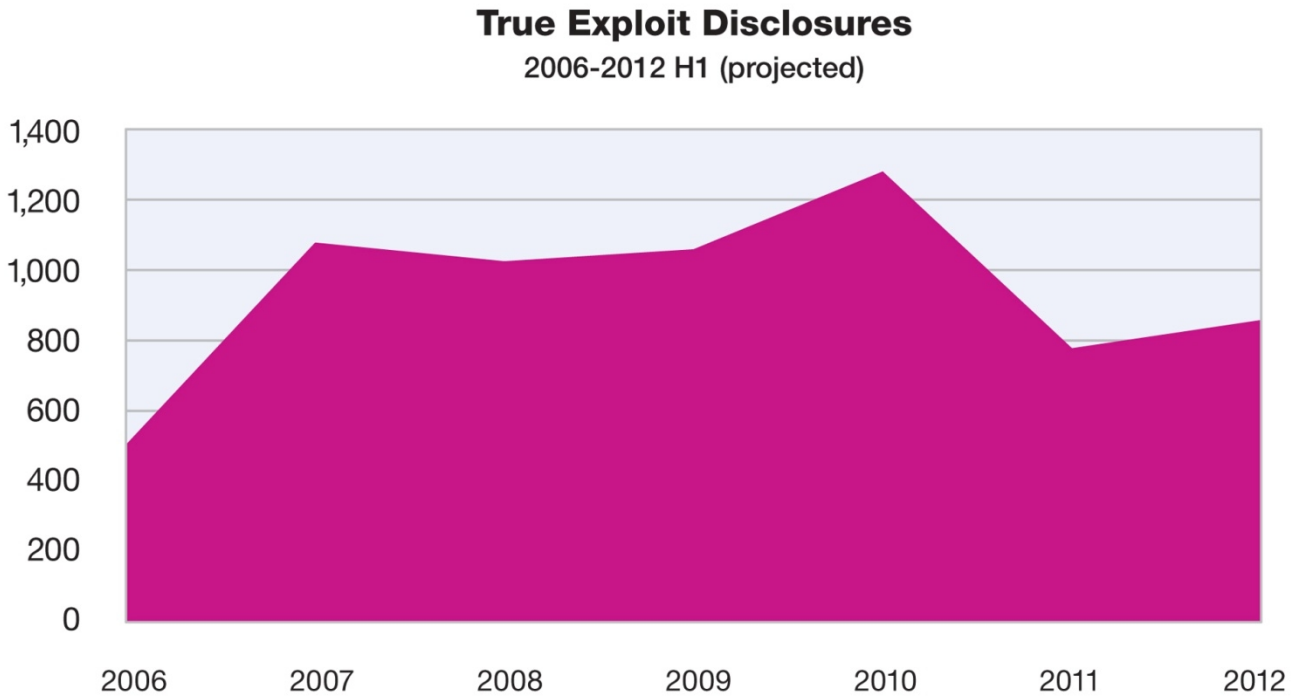
Web Application Vulnerabilities Raise Again





Public Exploit Disclosures

- Decrease in percentage of vulnerabilities
- Slightly up in actual numbers compared to 2011

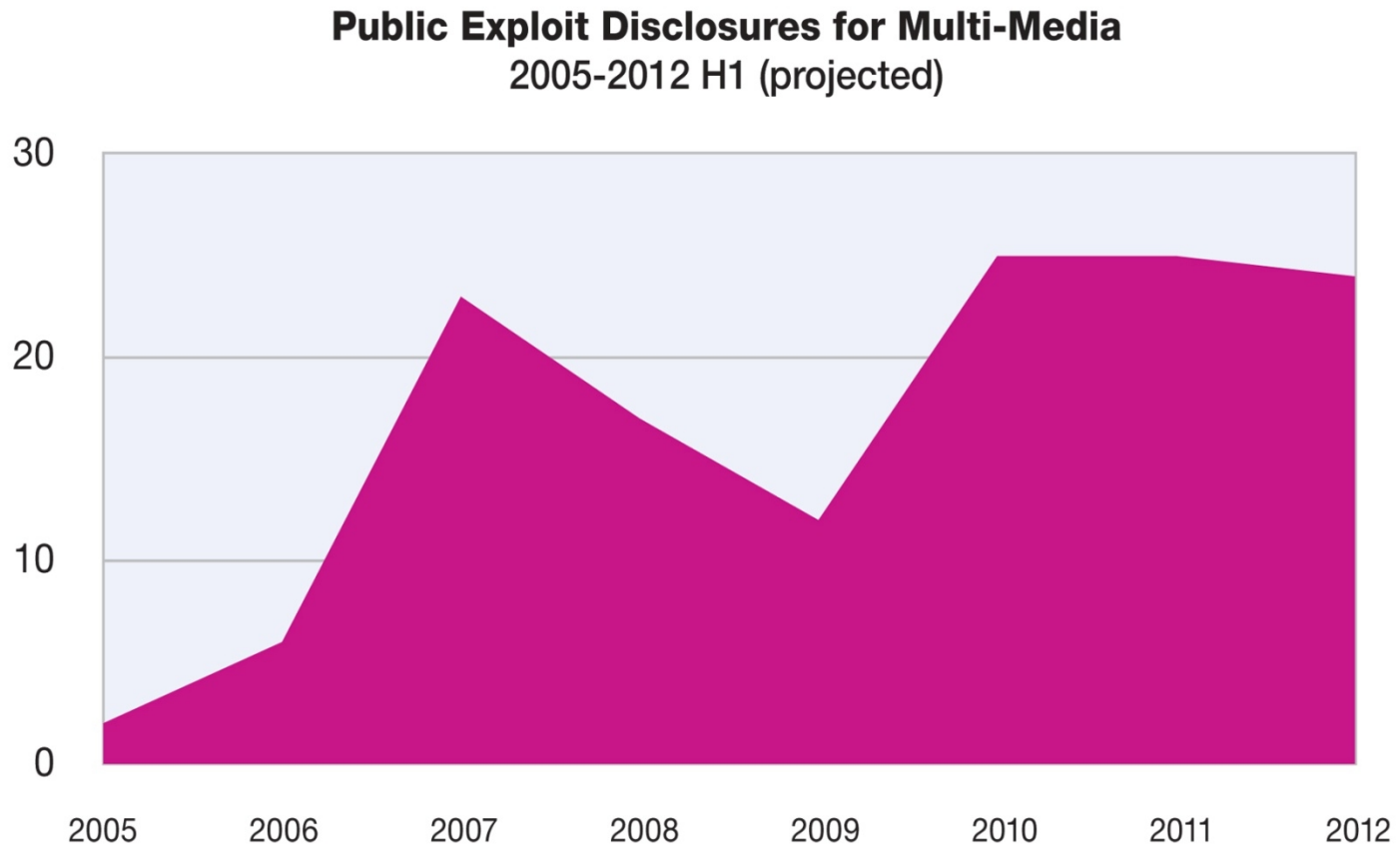


	2006	2007	2008	2009	2010	2011	2012
True Exploits	504	1078	1025	1059	1280	778	858
Percent of Total	7.3%	16.5%	13.3%	15.7%	14.7%	10.9%	9.7%

Source: IBM X-Force® Research and Development

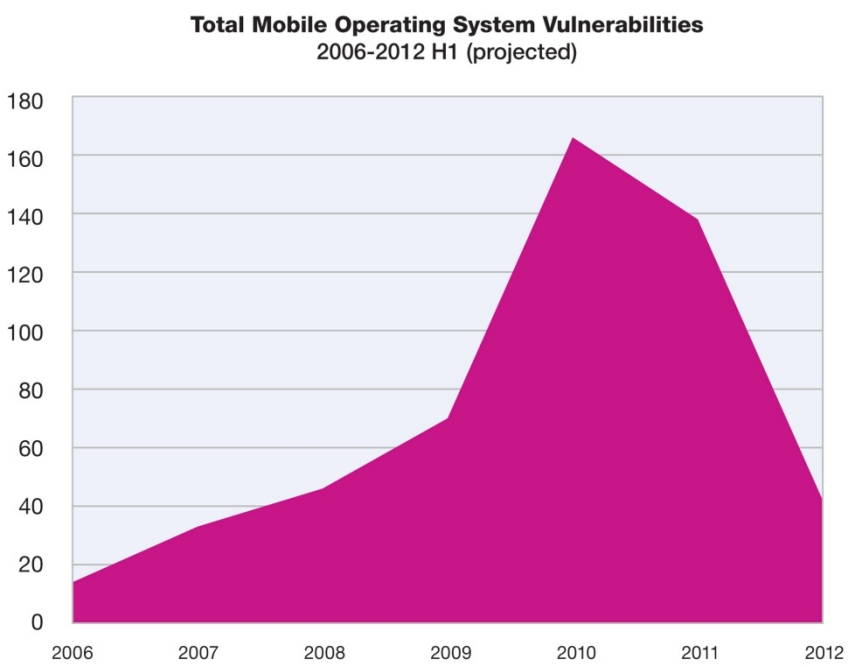
Multi-Media Exploitation Remains the Same Since 2010

- Social Networking sites are an ideal distribution media

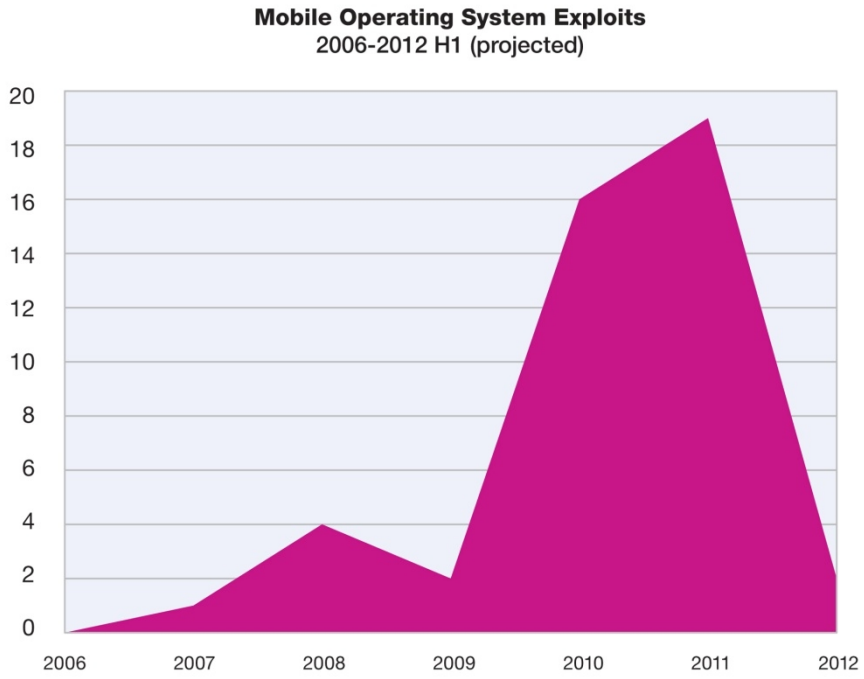


No need to exploit the Mobile Operating System

- Most smartphone users are still the most at risk of premium SMS scams and the like
- Easier to get the user to install malicious apps



Source: IBM X-Force® Research and Development

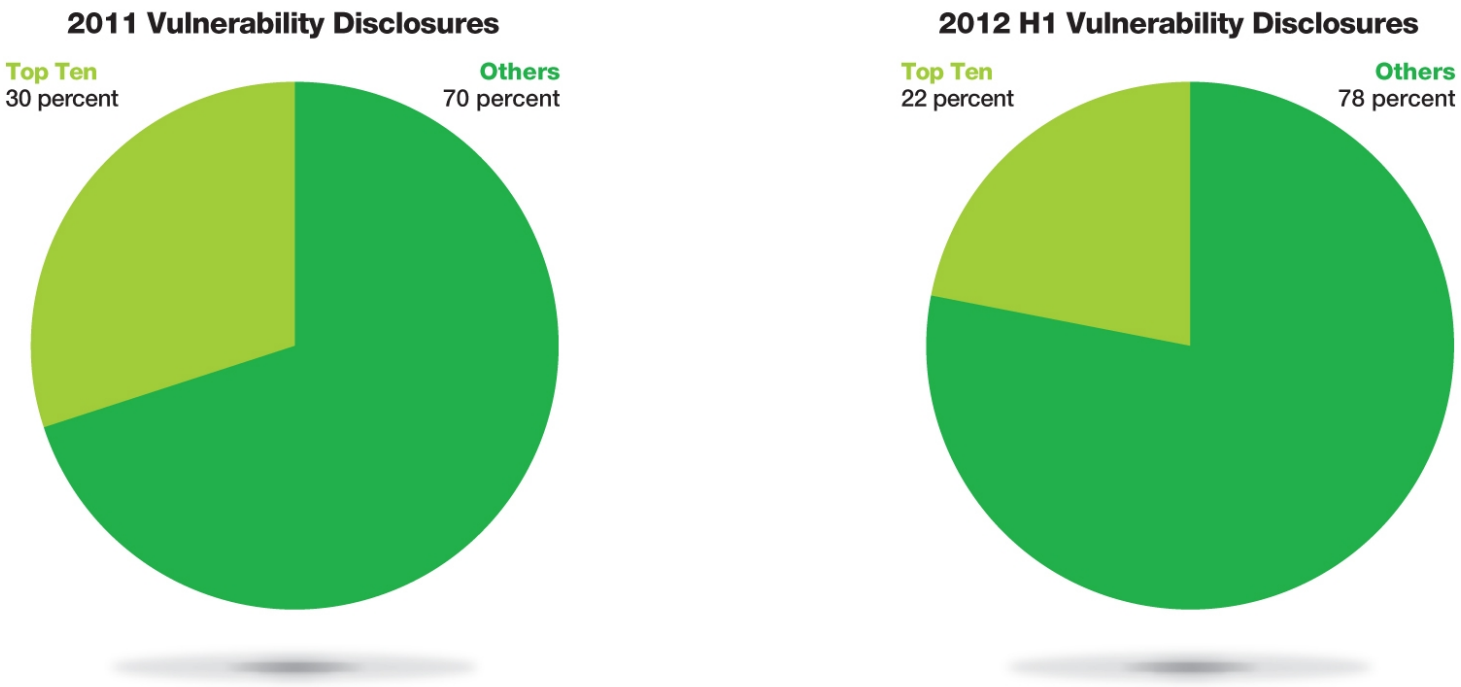


Source: IBM X-Force® Research and Development

Better Patching

Top Ten Software Vendors with the Largest Number of Vulnerability Disclosures

2011-2012 H1

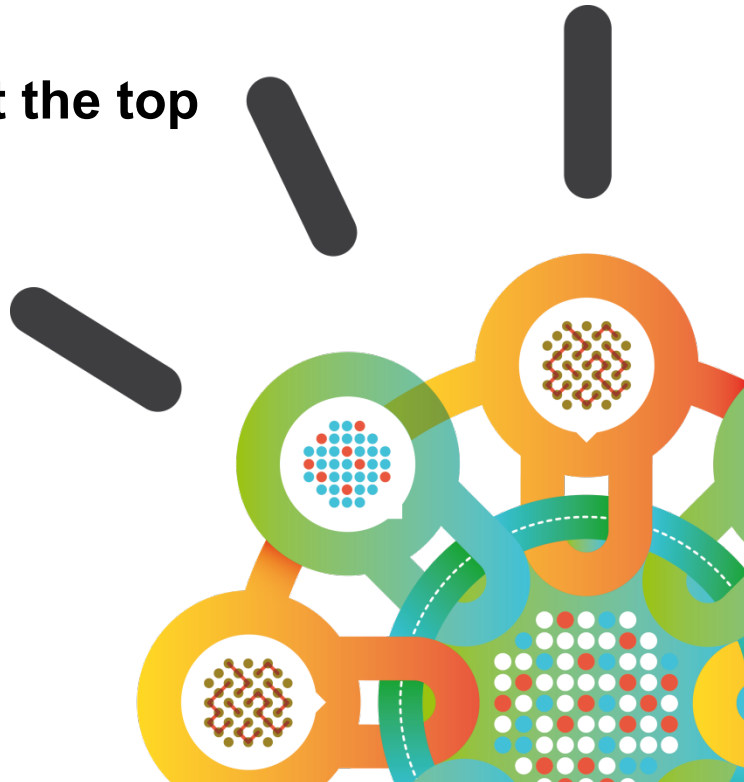


Source: IBM X-Force® Research and Development

Security Intelligence.
Think Integrated.

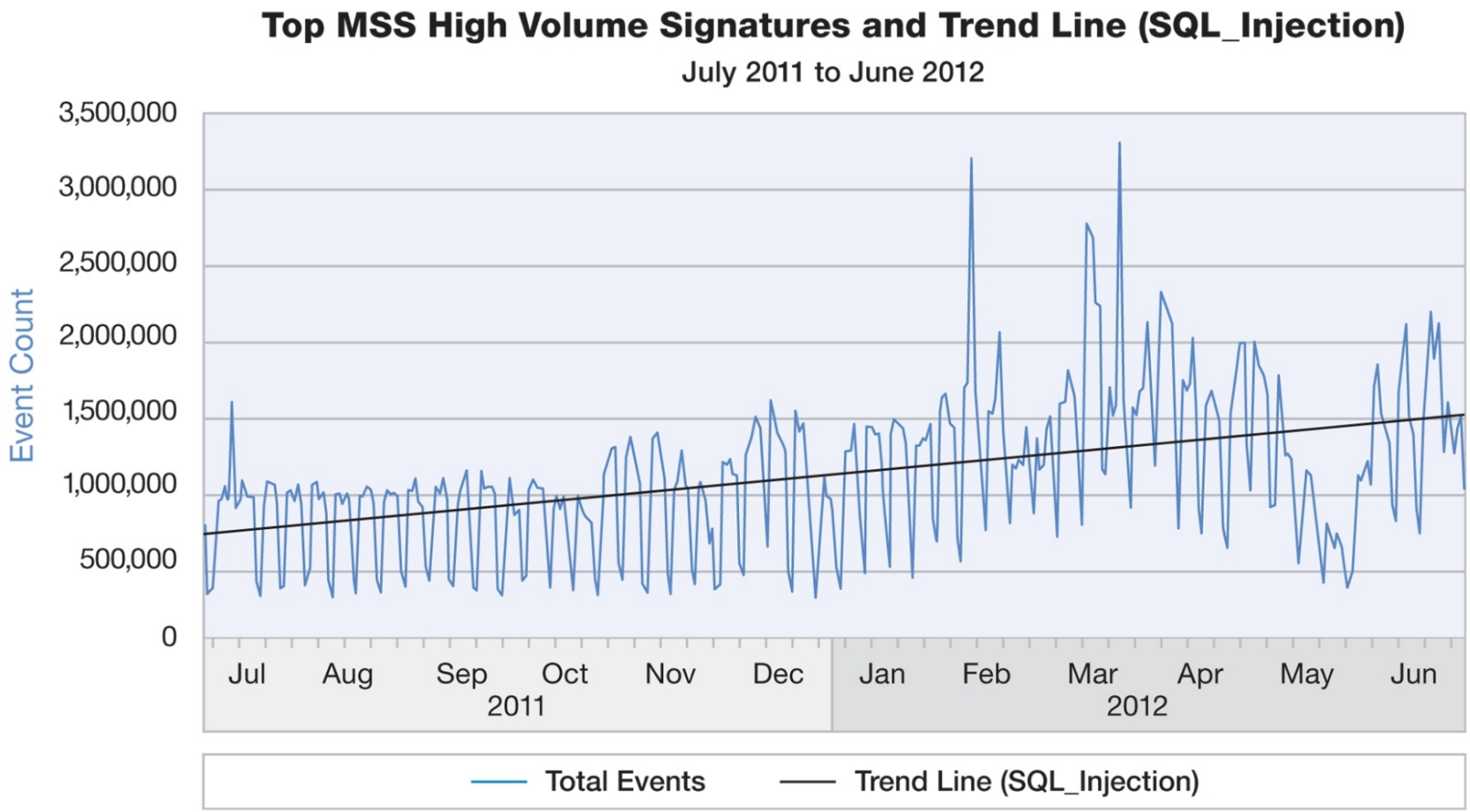
New Attack Activity

- SQL Injection & Cross Site Scripting still at the top
- Obfuscation techniques to evade IPS & AV
- Mac Malware bypasses OS X security




LEVEL LOAD
NO FIRES
LEVEL LOAD
A.J. PAIN
020 7732 0044

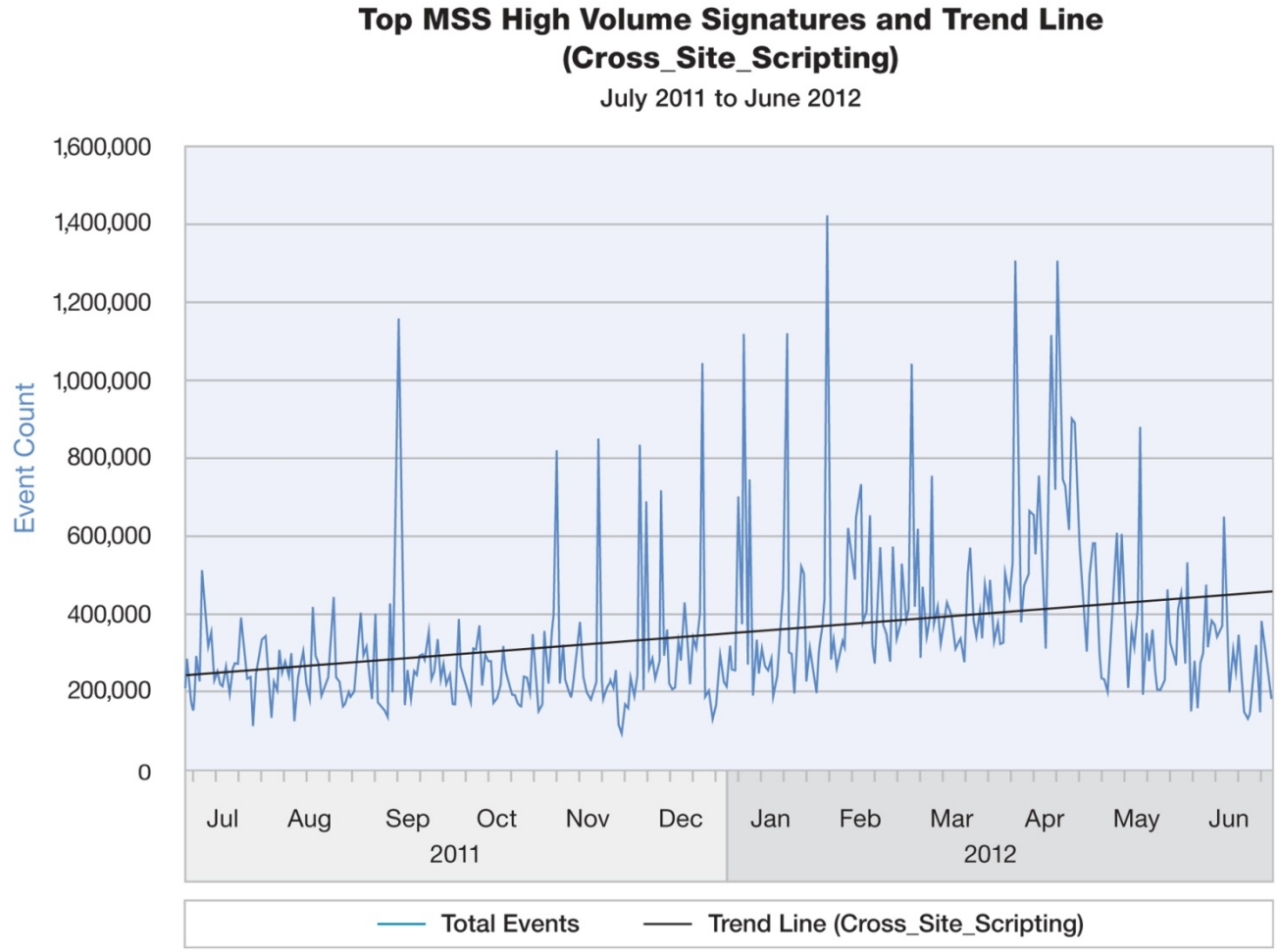
SQL Injection Attacks against Web Servers



Source: IBM X-Force® Research and Development

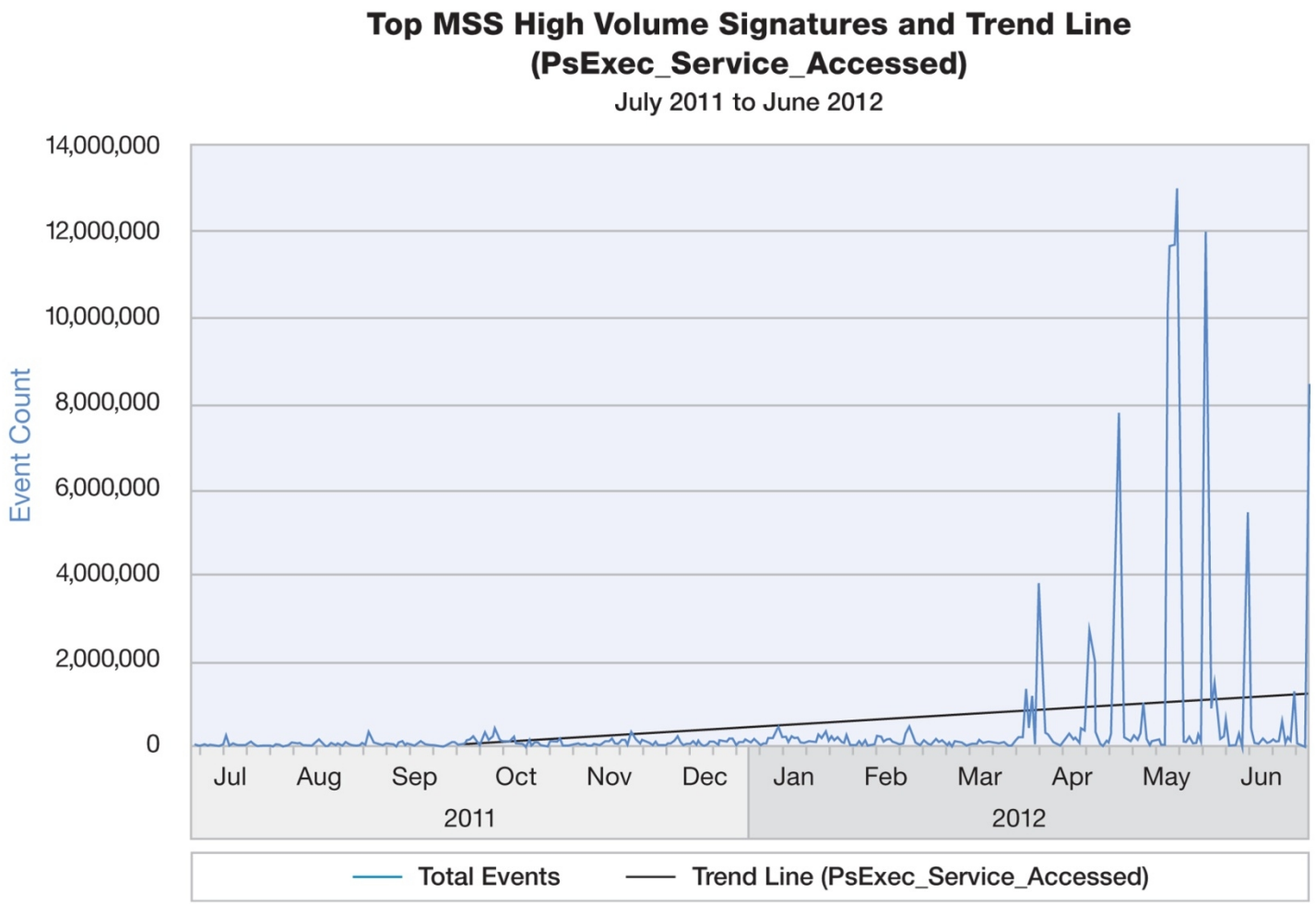
XSS reaching new highs in 1H 2011

- More than 6,000 variants of this vulnerability, with uses ranging from hijacking a browser session to a total system web-server-based takeover.



PsExec Services being used … again

- Part of Sysinternal tools
- worms and advanced threats sometimes take advantage of PsExec



Source: IBM X-Force® Research and Development

MAC Platforms Continue to Draw Attention

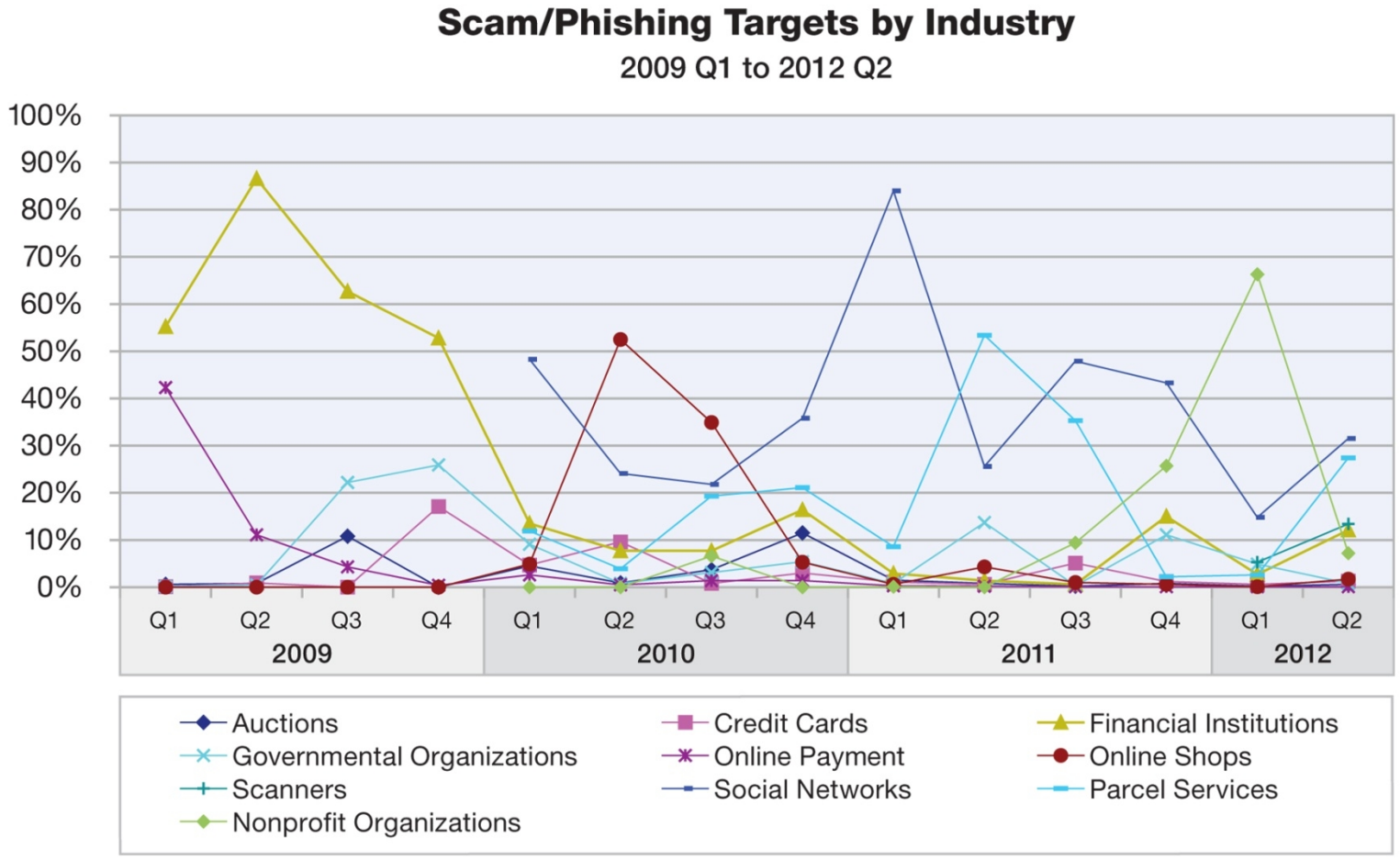
Flashback

- First variant discovered in September of 2011.
- 2012 variants were somewhat special
  - Employed drive-by-download techniques through compromised Wordpress blog sites
  - Works around this by using multi-platform exploits through Java vulnerabilities.
  - The Apple version of Java was updated later than Oracle: 600,000 infection estimated.

Mac APT

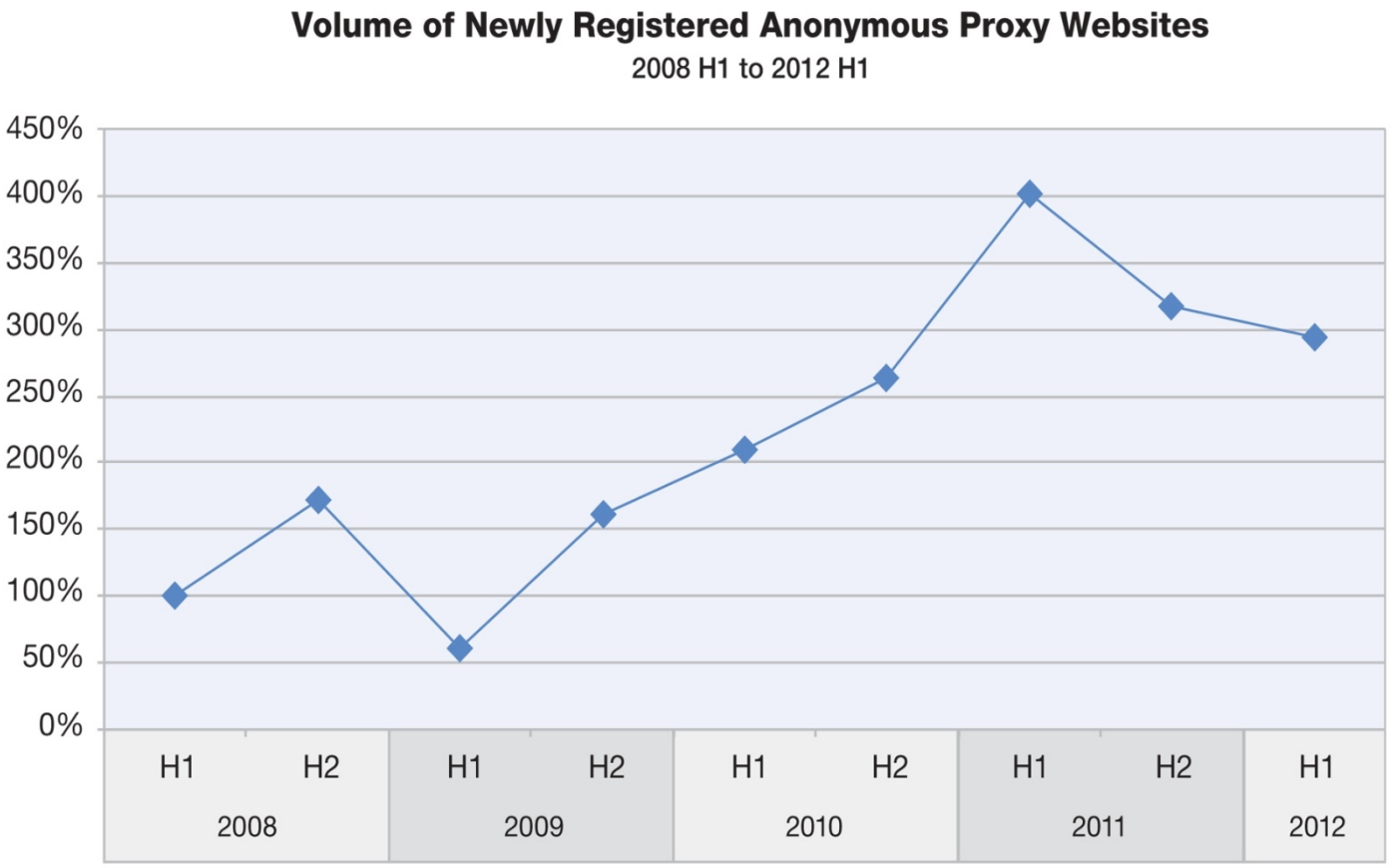
- Tibet malware discovered in March.
  - The first variants used Java exploit to spread.
  - Next variants use an MS Word vulnerability that affects the 2004 and 2008 versions of Word for Mac
- SabPub backdoor discovered in April.
  - The first variant did not initially show any sign that it was a targeted attack
  - Uses the same Java exploit as Flashback
  - The next variant is similar to the Tibet malware (using Word)

Scammers/Phishers keep moving around



Source: IBM X-Force® Research and Development

Anonymous Proxies Still used to Bypass Web Filtering

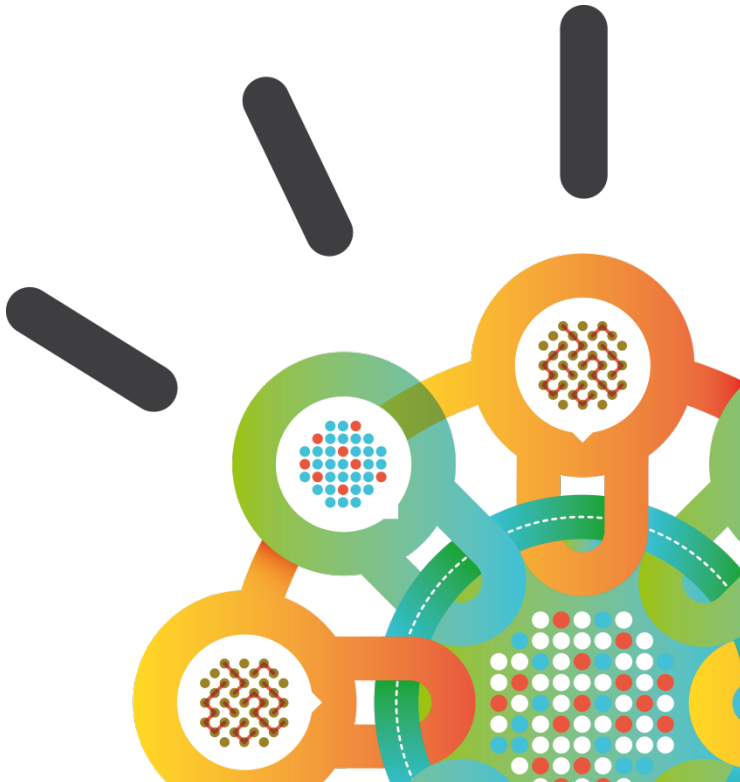


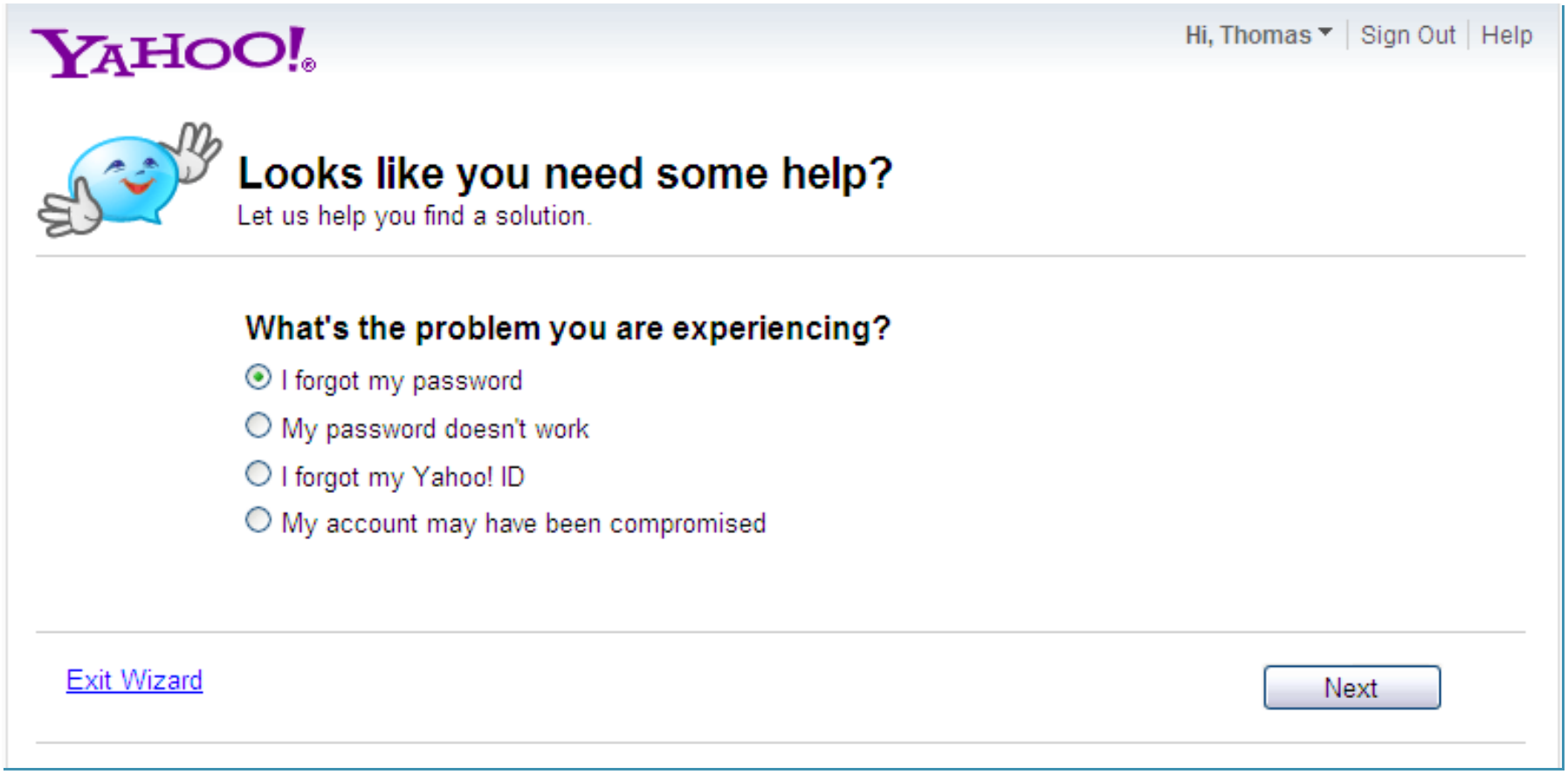
Source: IBM X-Force® Research and Development

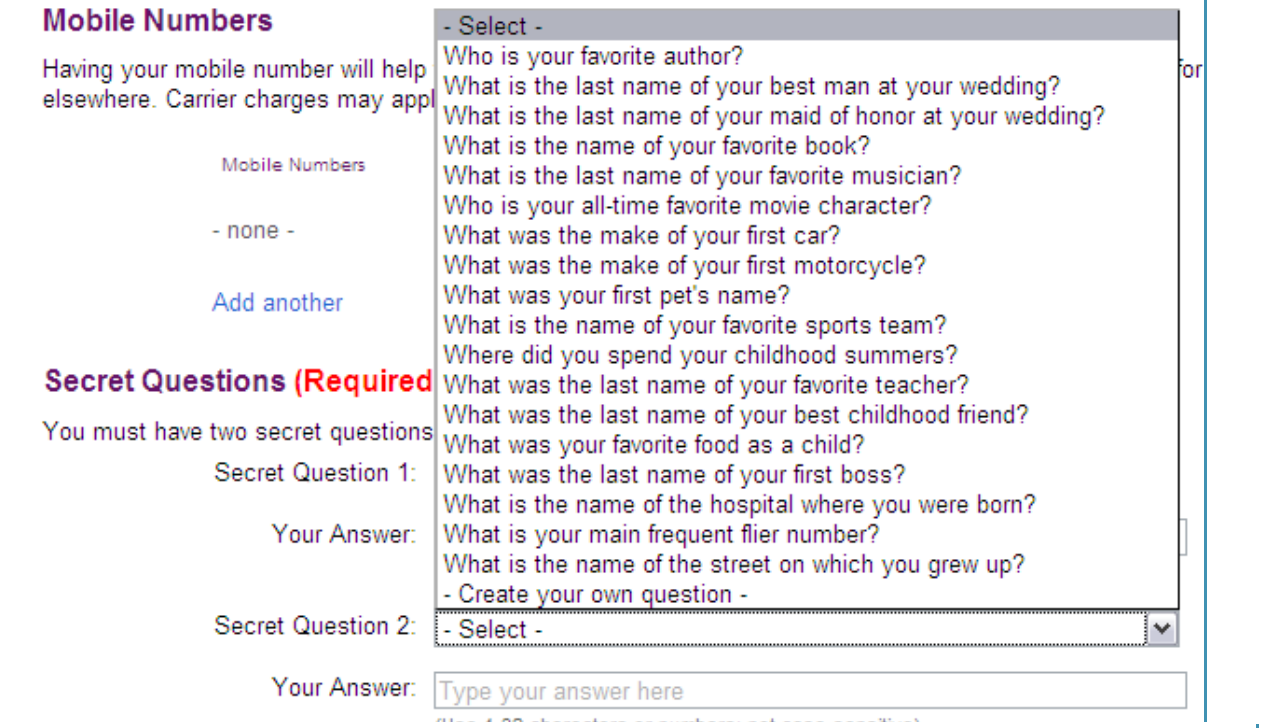
Security Intelligence.
Think Integrated.

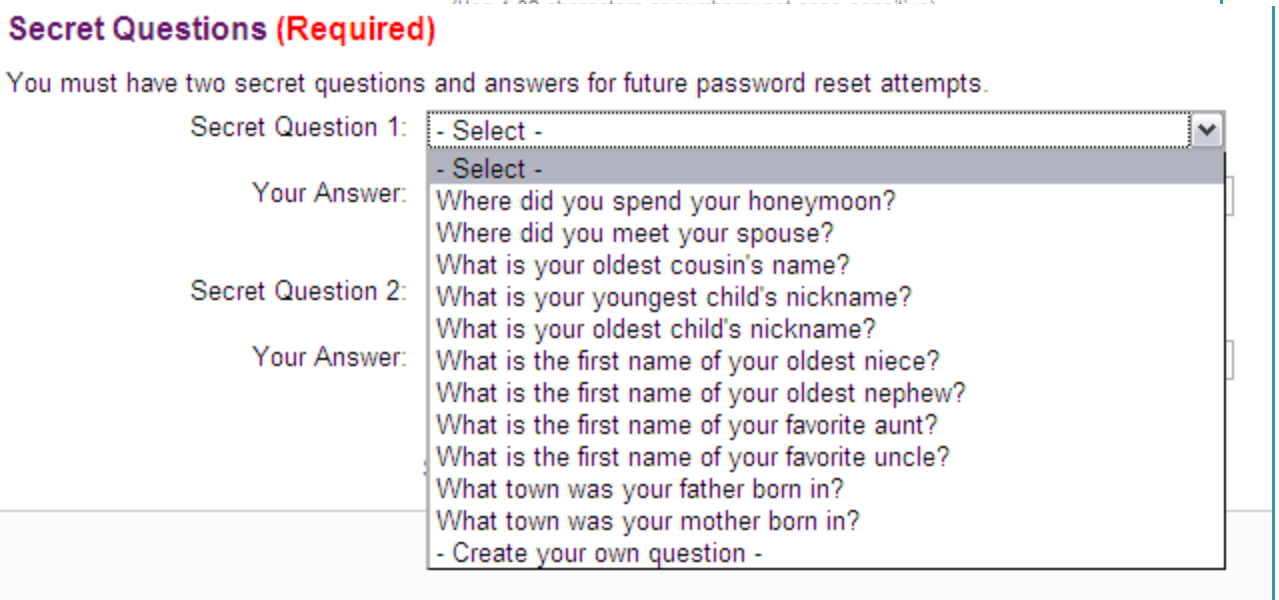
The Challenges

- **Password security**
- **Bring Your Own Device (BYOD)**
- **Advanced Persistent Threats (APT)**

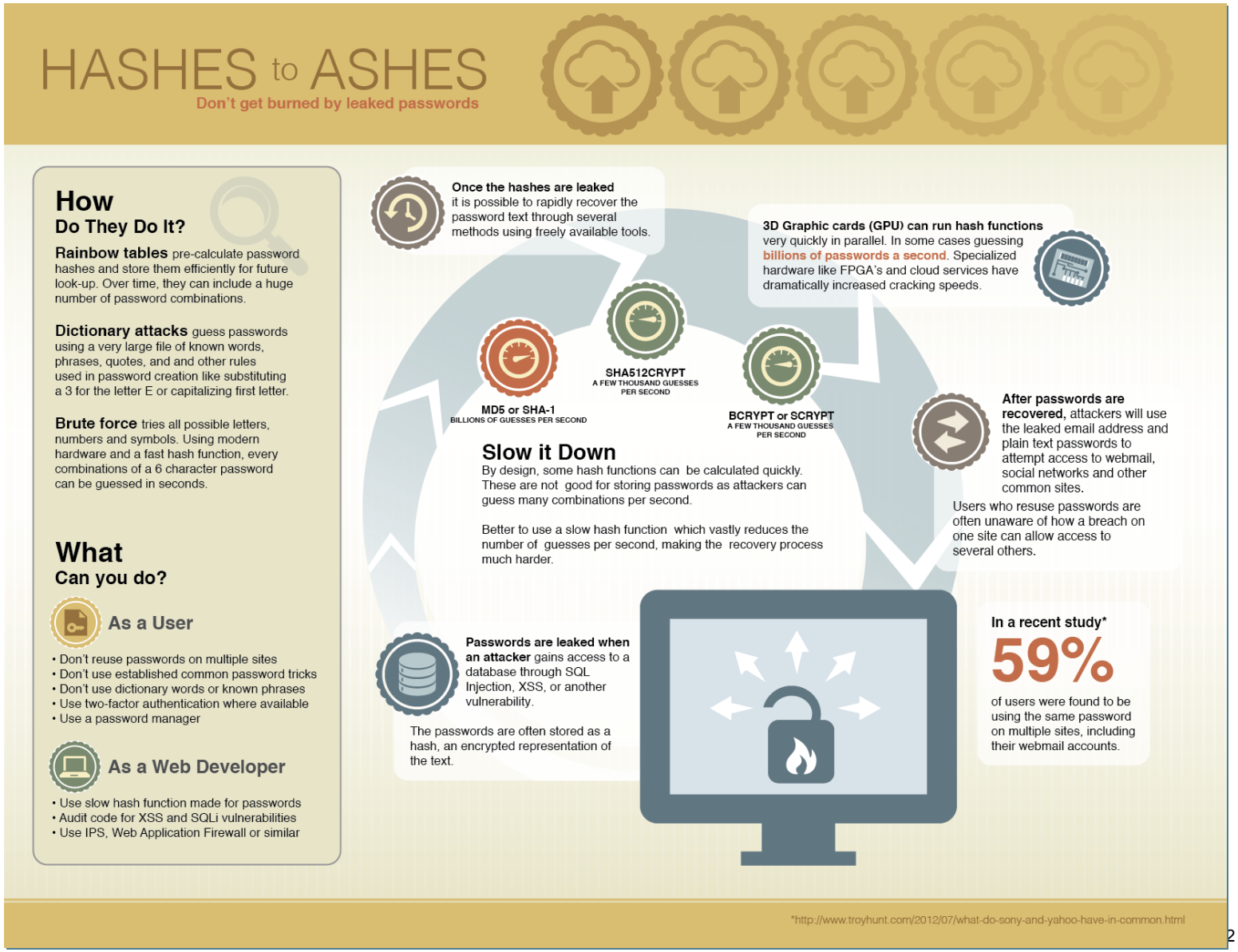








Leaked passwords emphasize going back to basics



Bring Your Own Device (BYOD)

- Making BYOD work
  - Identification and authentication
  - Access authorization
  - Information protection
  - Operating system and application integrity
  - Assurance
  - Incident response

- Challenges
  - BYOD program definition and review
  - Mobile platform vulnerability management

An Approach to Identify Advance Persistent Threats

O	Observation
C	Concealment
O	Obstacles
K	Key Terrain
A	Avenues of Approach

Defender: Observe the activities of the attacker

Attacker: ability to view and obtain data

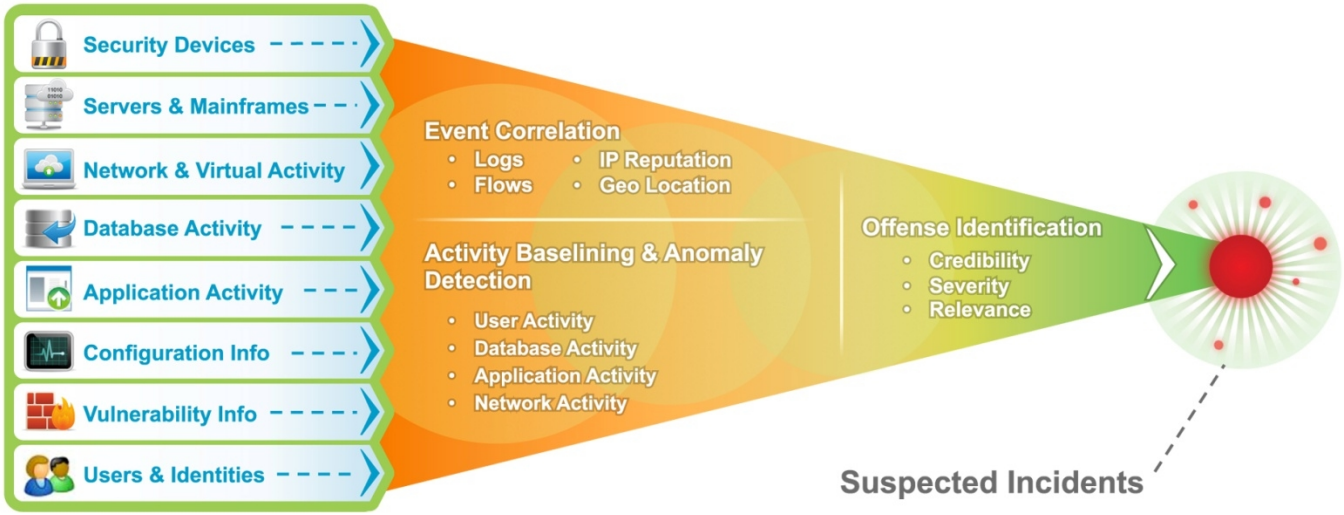
Defender: conceal the network architecture and data

Attacker: hide their malicious actions

Place obstacles in each other's way in order to deter or obstruct the ability to successfully defend or attack the network

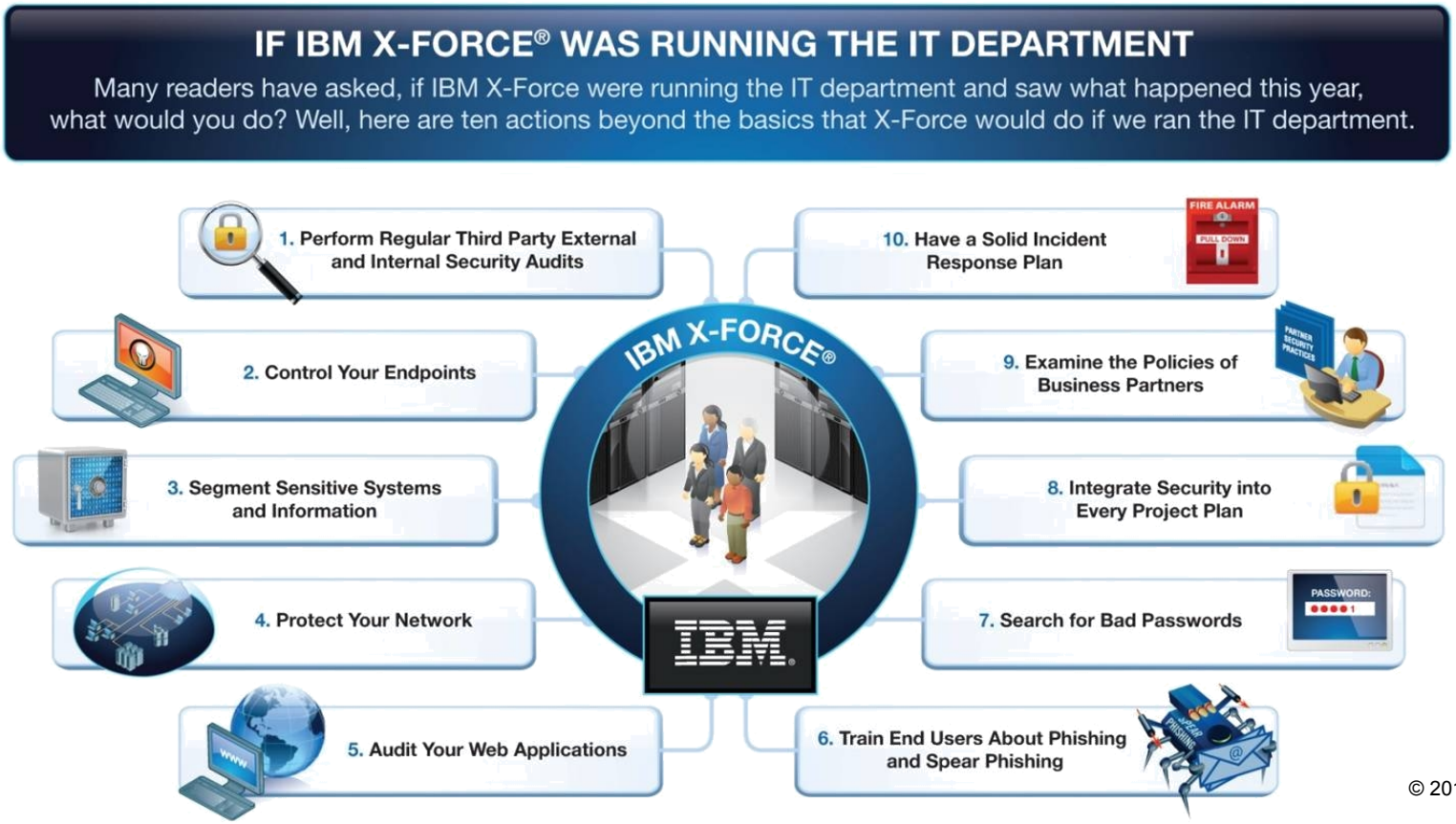
areas within the network which contain high profile, high value, or high payoff targets.

areas within the network which contain high profile, high value, or high payoff targets.



Not a technical problem, but a business challenge

- Many of the recent 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?



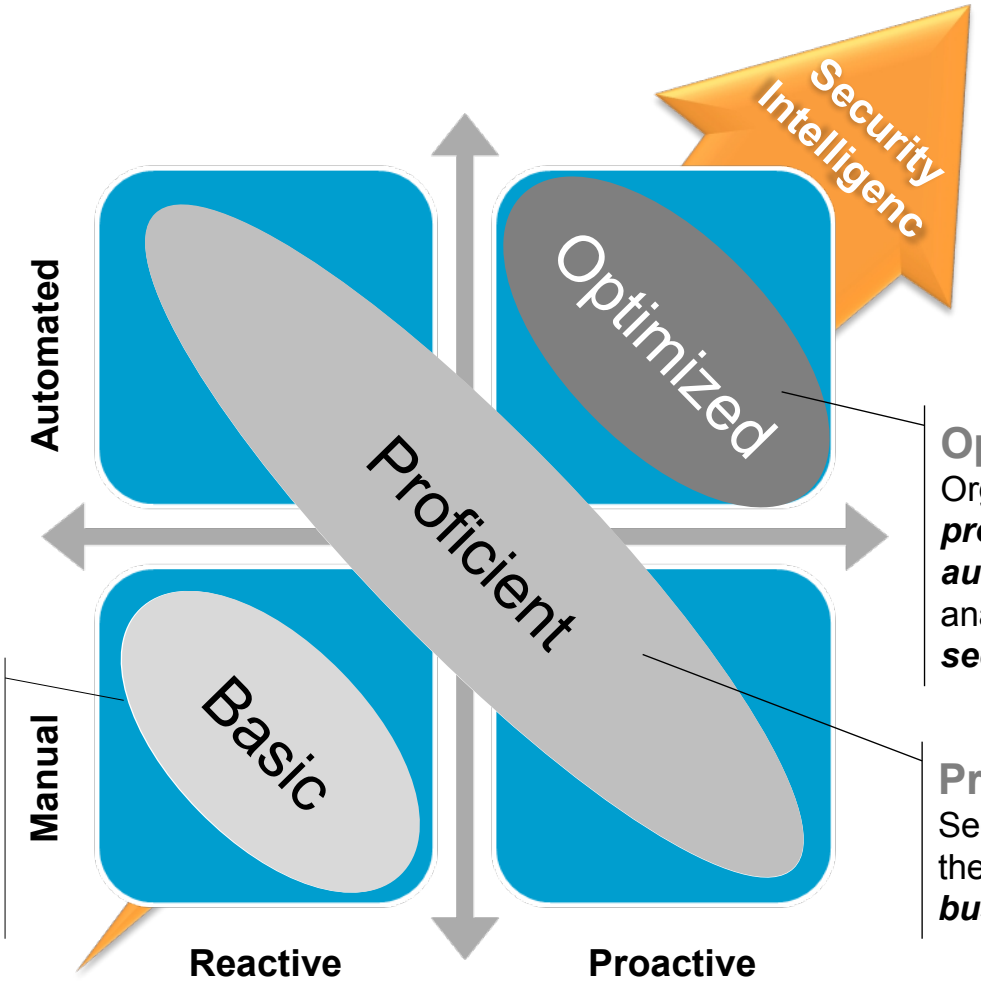
IBM Security: Delivering intelligence, integration and expertise across a comprehensive framework

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

In this “new normal”, organizations need 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

ibm.com/security