Security Trends in 2012 analyzed by IBM X-Force

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

Jean Paul Ballerini

Especialista en Soluciones de Seguridad de Infraestructuras

IBM Software Summit #START013. Madrid 06/11/2012.

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)

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

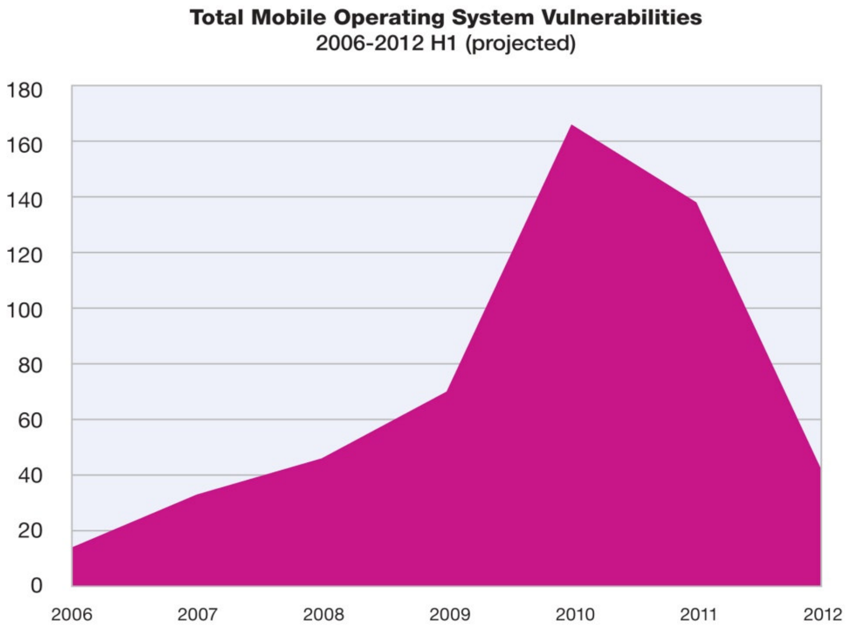
September 2012

Progress in Internet Security

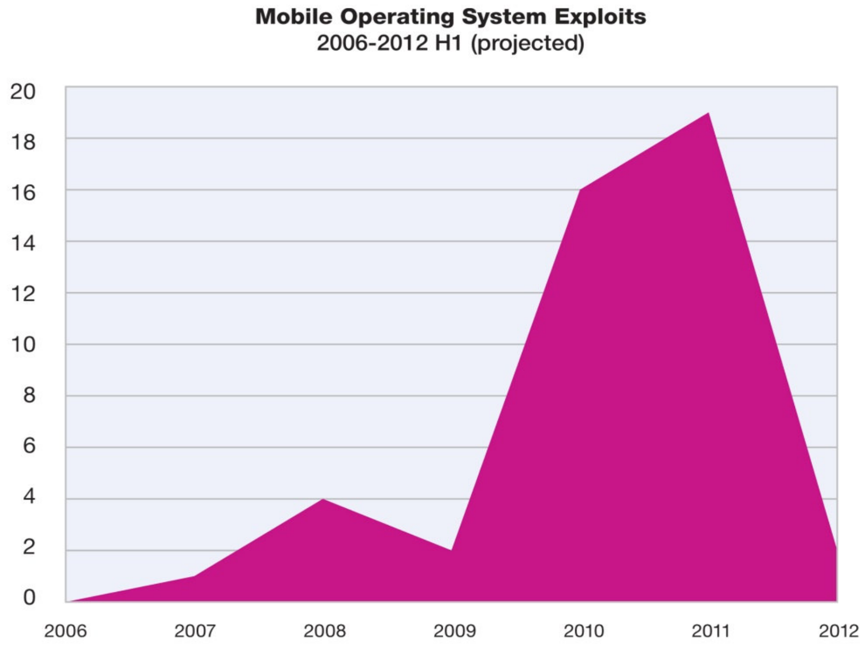
- Fewer vulnerabilities disclosed for mobile
- Sandbox used to block PDF attacks
- Better patching from Top 10 Vendors

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



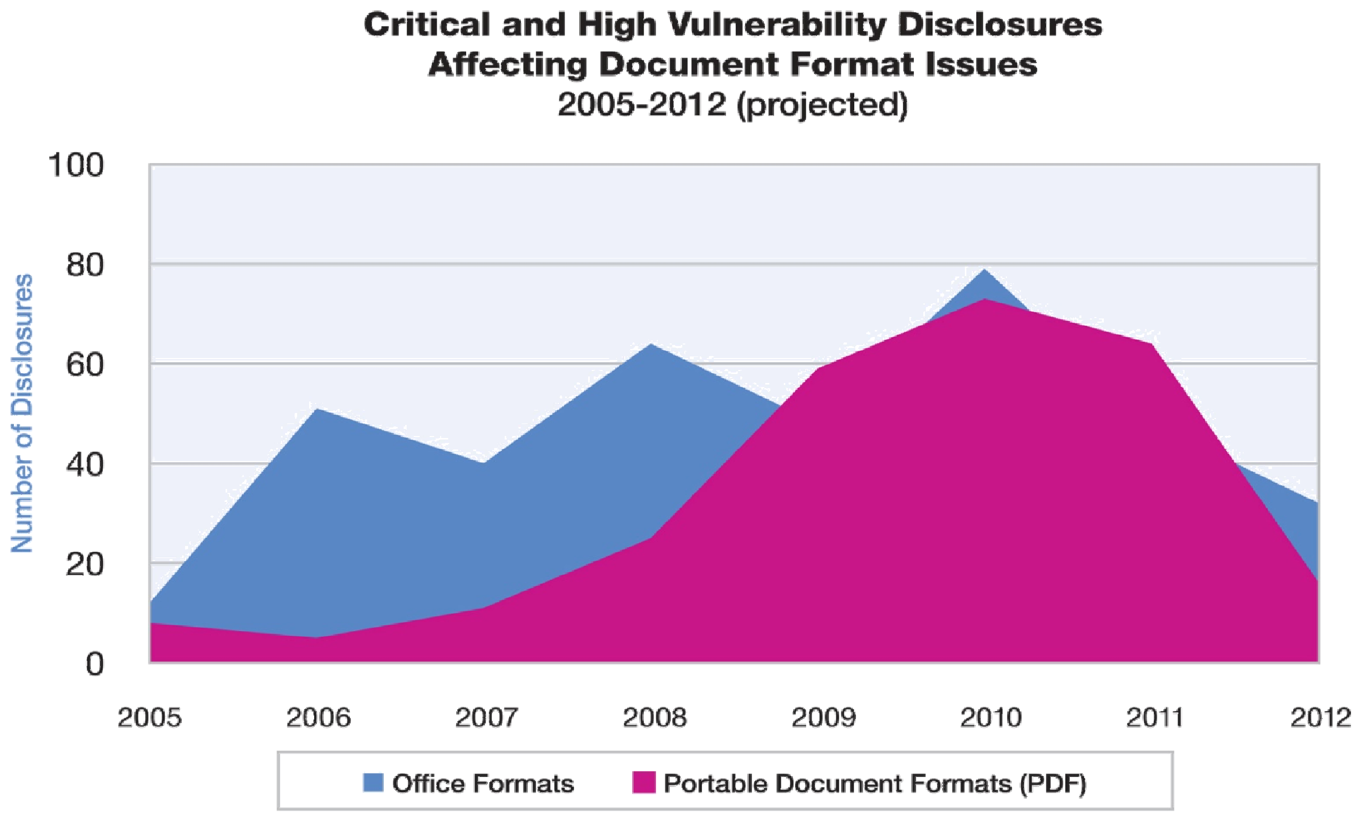
Source: IBM X-Force® Research and Development



Source: IBM X-Force® Research and Development

Dramatic Drop of PDF Vulnerabilities

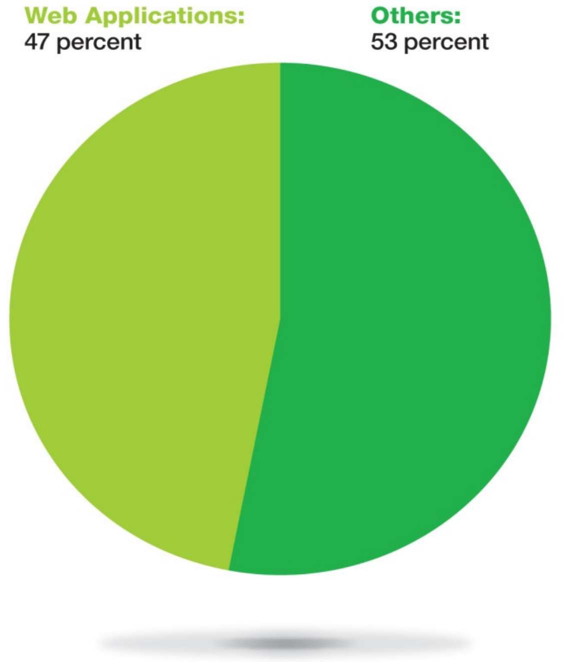
- Sandbox is proving successful
  - We have to keep alert against enhanced attack techniques



Web Application Vulnerabilities Raise Again

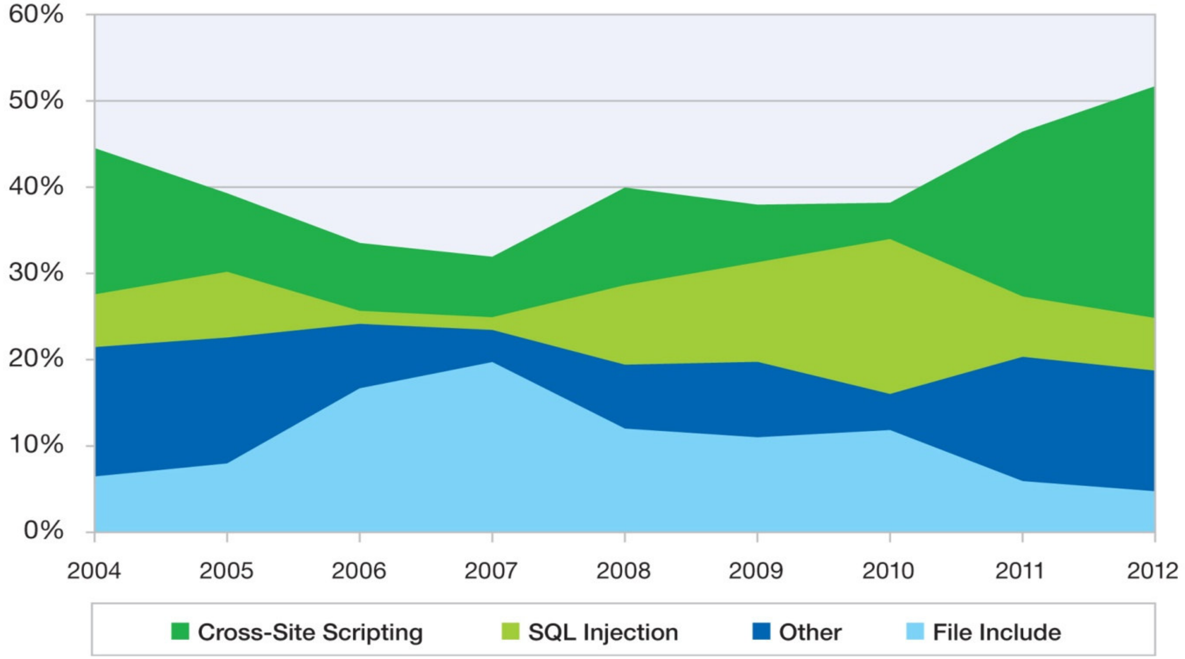
Web Application Vulnerabilities

as a Percentage of All Disclosures in 2012 H1



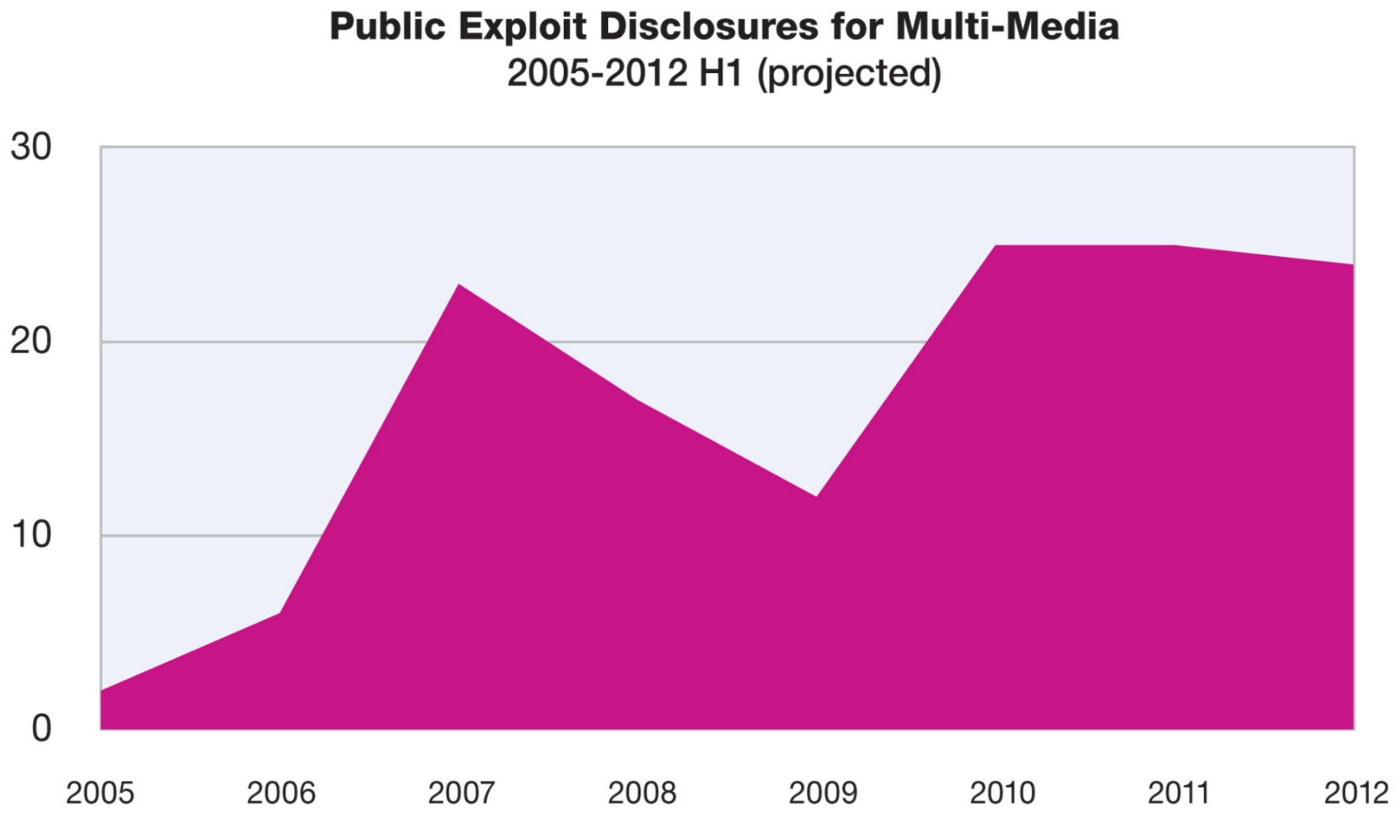
Web Application Vulnerabilities by Attack Technique

2004-2012 H1



Multi-Media Exploitation Remains the Same Since 2010

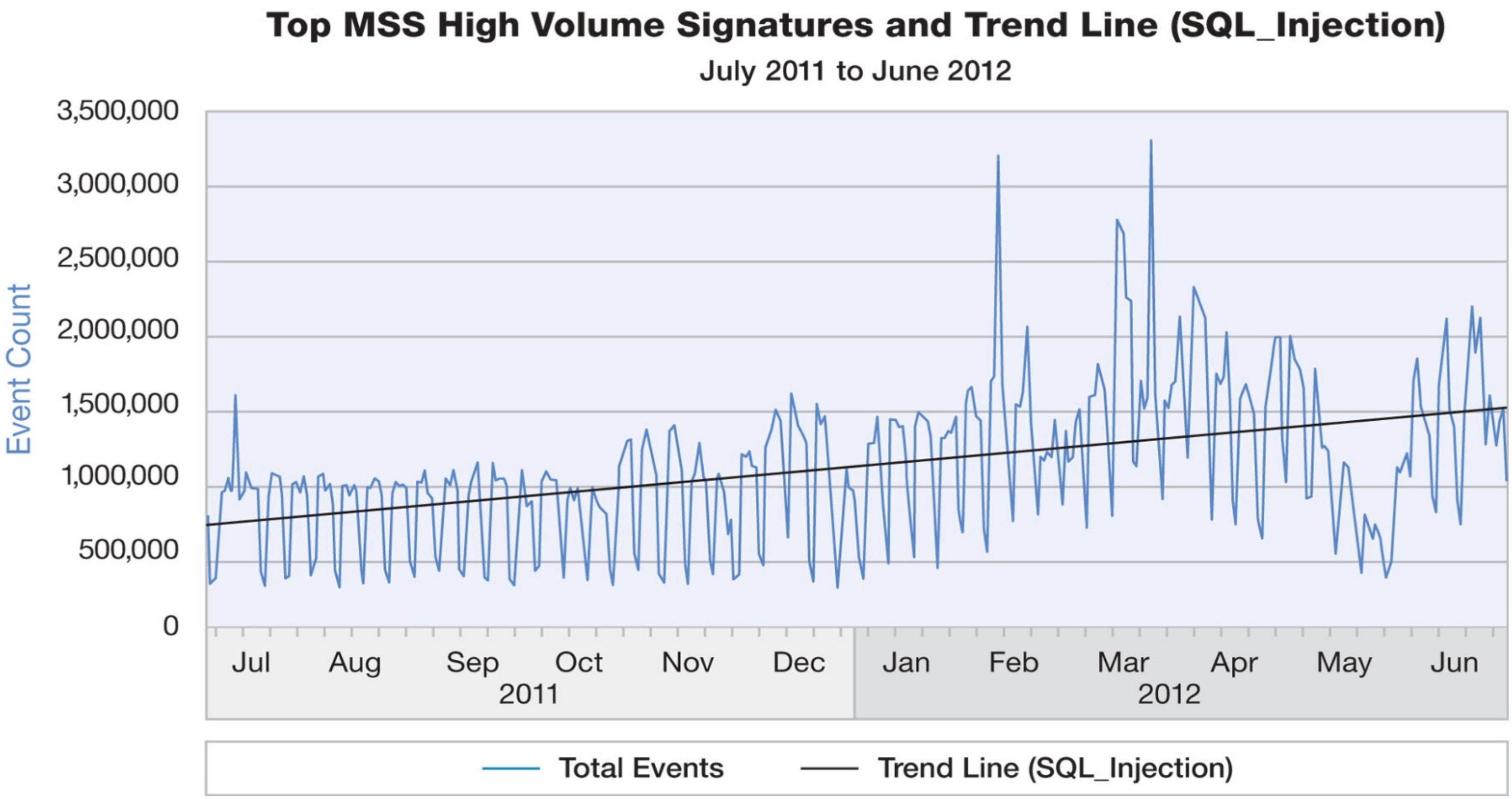
- Social Networking sites are an ideal distribution media



New Attack Activity

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

SQL Injection Attacks against Web Servers



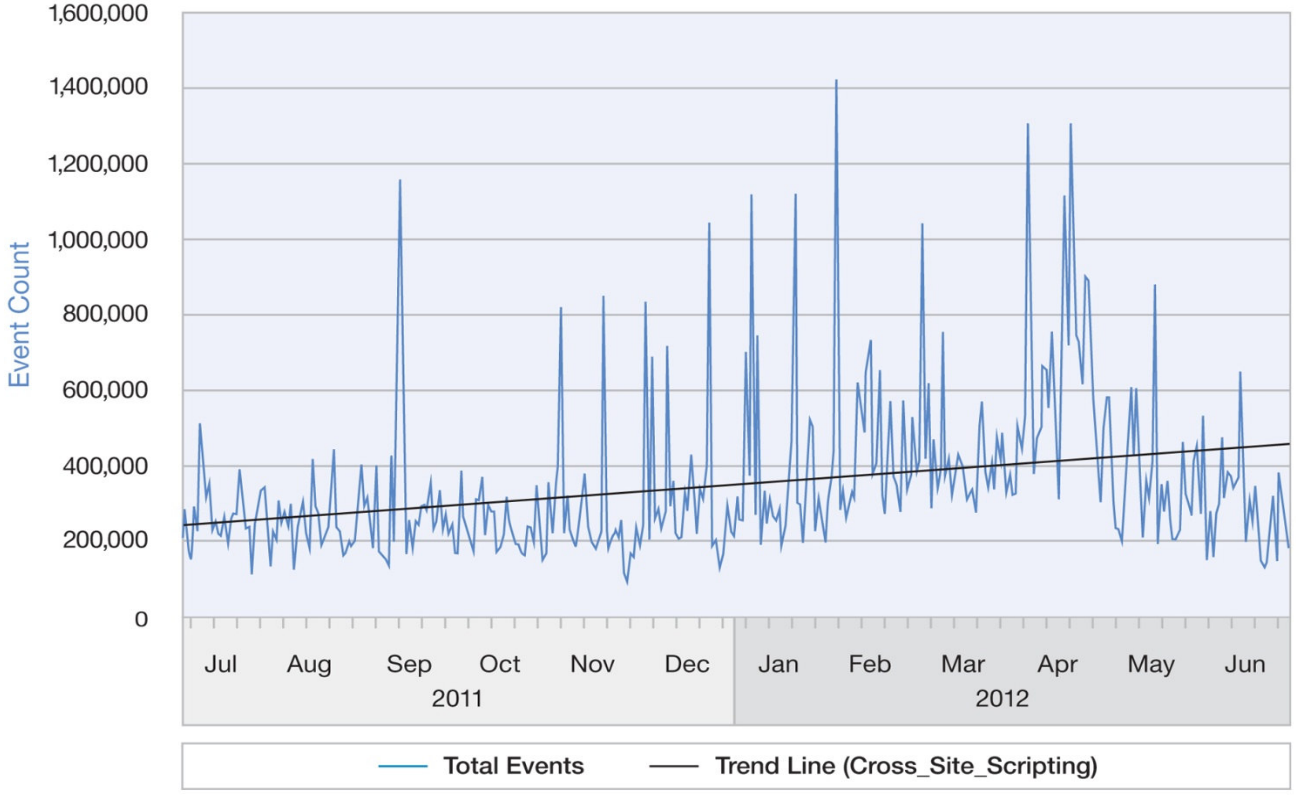
Source: IBM X-Force® Research and Development

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.

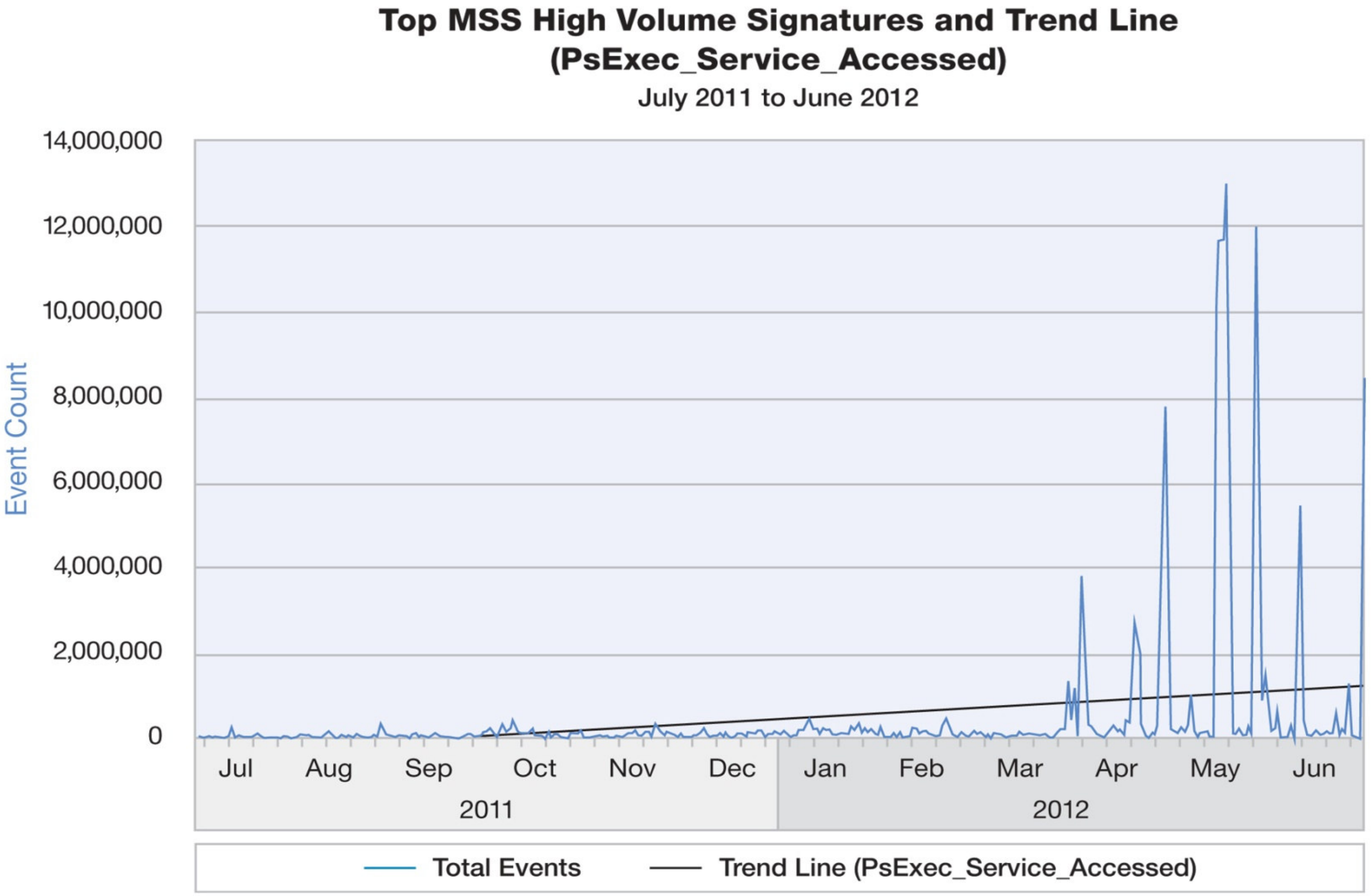
Top MSS High Volume Signatures and Trend Line (Cross_Site_Scripting)

July 2011 to June 2012



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

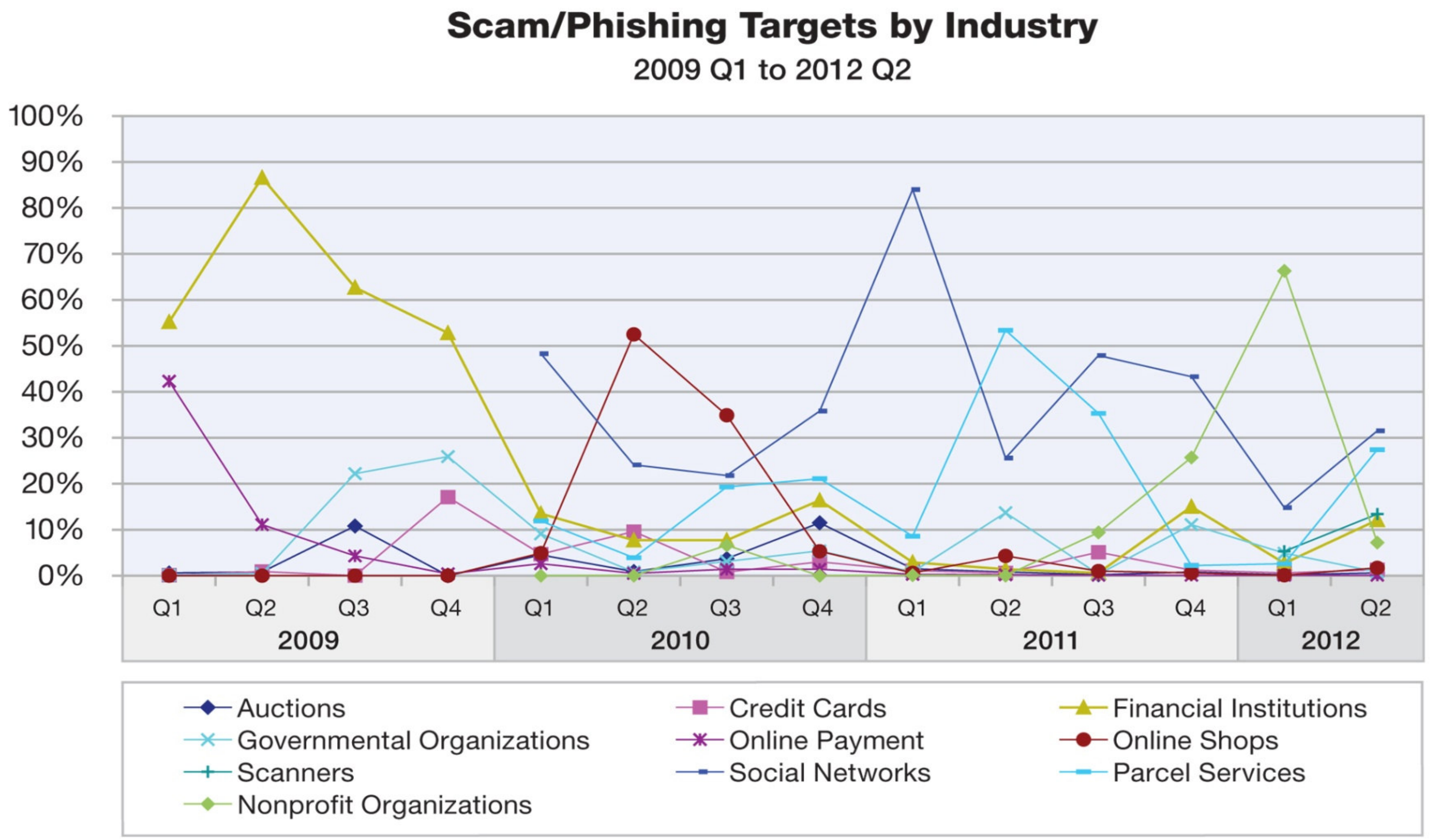
Flashback

- 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

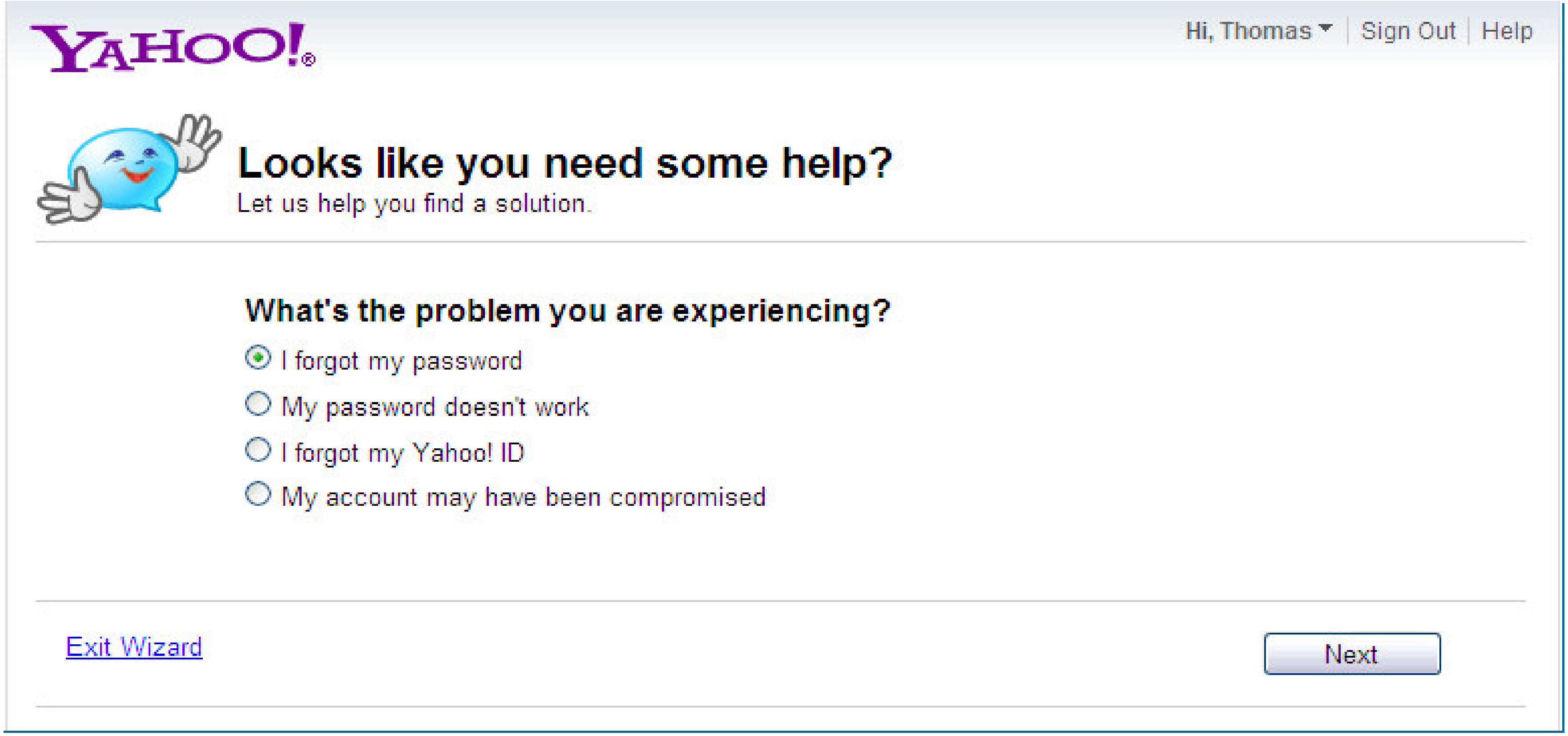


Source: IBM X-Force® Research and Development

The Challenges

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

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

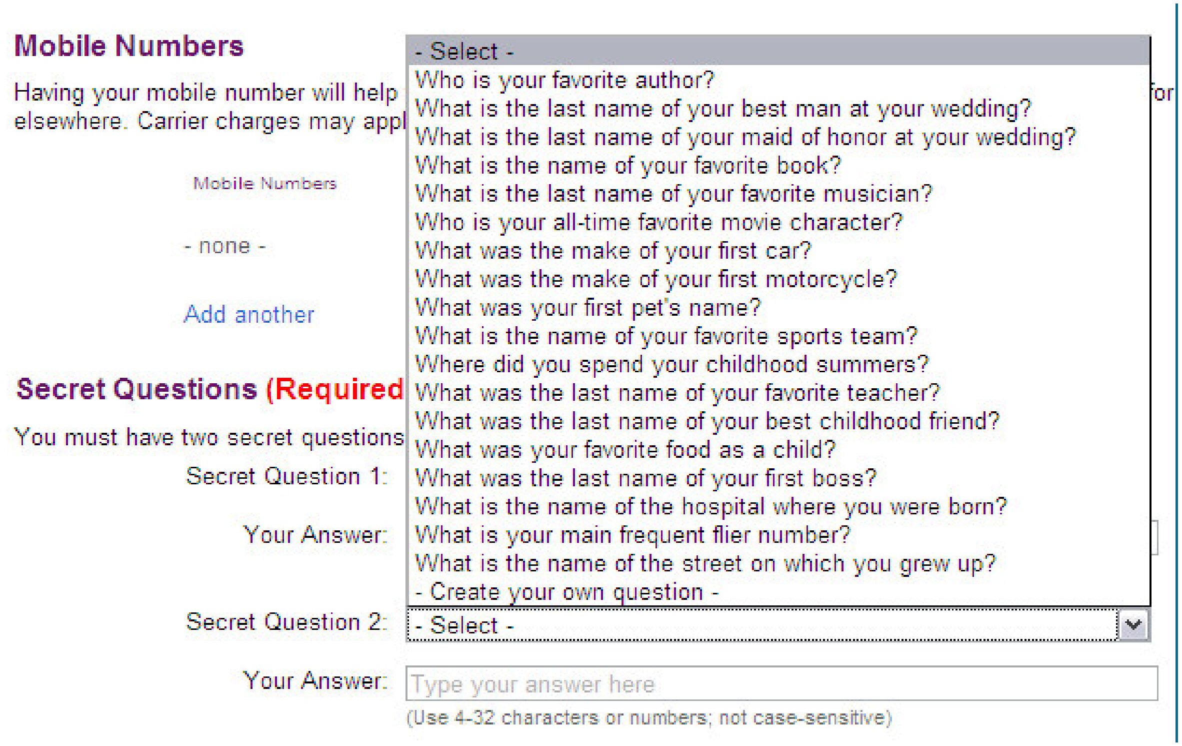


Looks like you need some help?

Let us help you find a solution.

What's the problem you are experiencing?

● I forgot my password
○ My password doesn't work
○ I forgot my Yahoo! ID
○ My account may have been compromised



Mobile Numbers

Having your mobile number will help ... for
elsewhere. Carrier charges may appl

Mobile Numbers

- none -

Add another

Secret Questions (Required

You must have two secret questions

Secret Question 1:

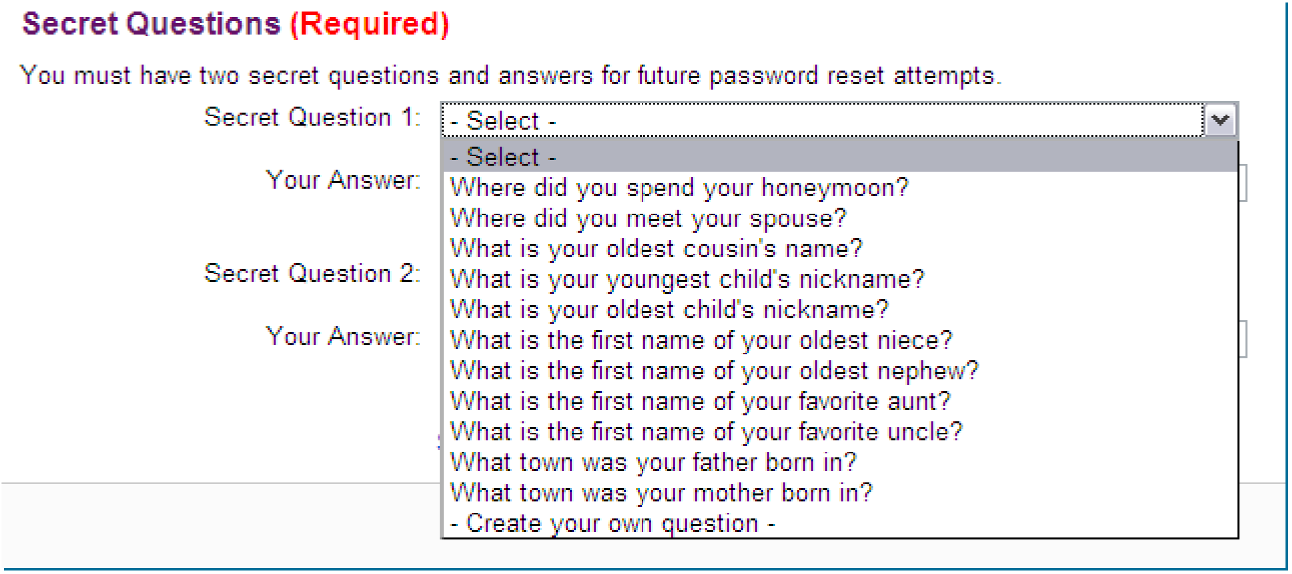
Your Answer:

Secret Question 2: - Select -

Your Answer: Type your answer here

(Use 4-32 characters or numbers; not case-sensitive)

- 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 -



Secret Questions (Required)

You must have two secret questions and answers for future password reset attempts.

Secret Question 1: - Select -

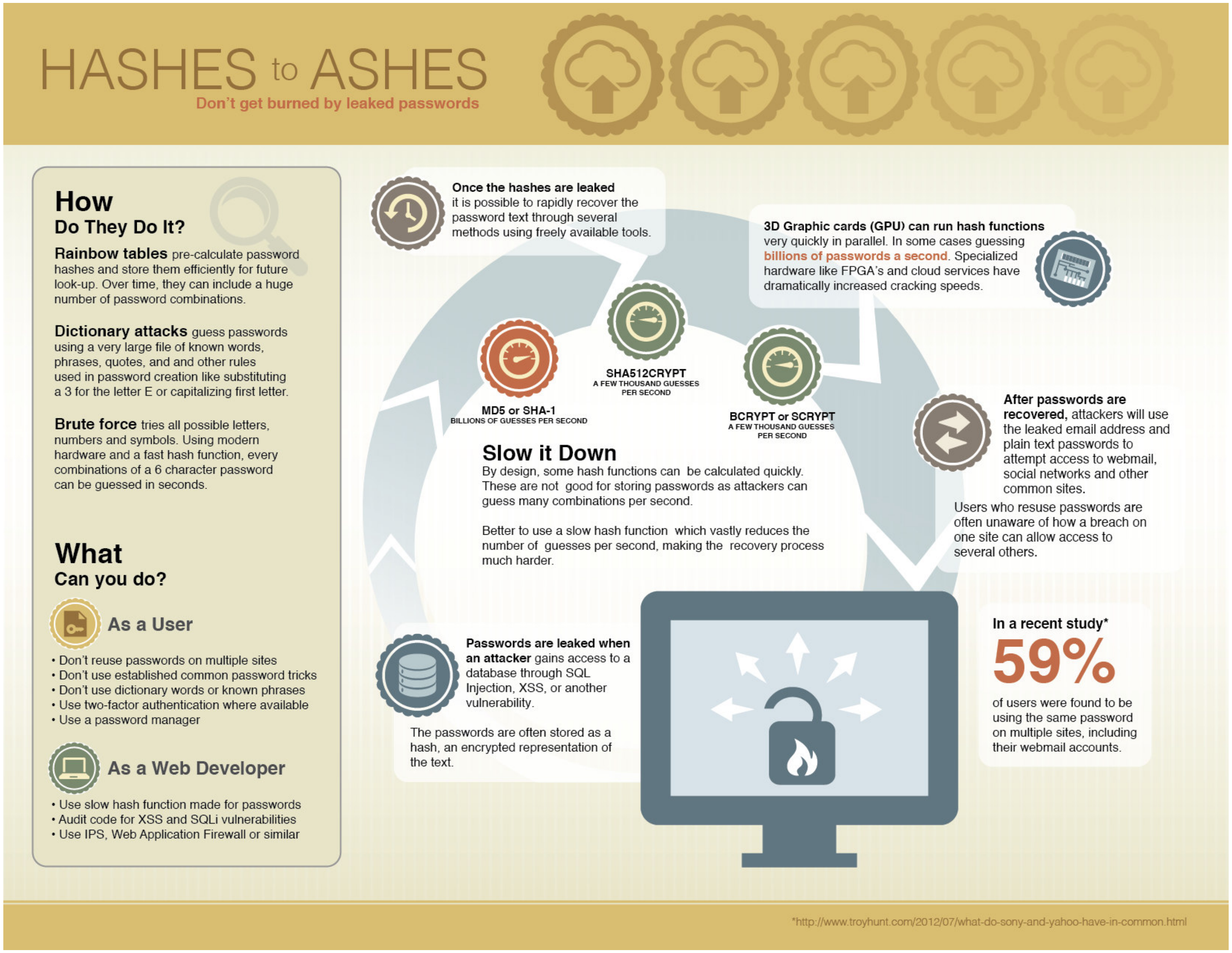
Your Answer:

Secret Question 2:

Your Answer:

- 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 -

Leaked passwords emphasize going back to basics



HASHES to ASHES

Don't get burned by leaked passwords

How
Do They Do It?

Rainbow tables pre-calculate password hashes and store them efficiently for future look-up. Over time, they can include a huge number of password combinations.

Dictionary attacks guess passwords using a very large file of known words, phrases, quotes, and and other rules used in password creation like substituting a 3 for the letter E or capitalizing first letter.

Brute force tries all possible letters, numbers and symbols. Using modern hardware and a fast hash function, every combinations of a 6 character password can be guessed in seconds.

What
Can you do?

As a User

- Don't reuse passwords on multiple sites
- Don't use established common password tricks
- Don't use dictionary words or known phrases
- Use two-factor authentication where available
- Use a password manager

As a Web Developer

- Use slow hash function made for passwords
- Audit code for XSS and SQLi vulnerabilities
- Use IPS, Web Application Firewall or similar

Once the hashes are leaked it is possible to rapidly recover the password text through several methods using freely available tools.

3D Graphic cards (GPU) can run hash functions very quickly in parallel. In some cases guessing **billions of passwords a second**. Specialized hardware like FPGA's and cloud services have dramatically increased cracking speeds.

After passwords are recovered, attackers will use the leaked email address and plain text passwords to attempt access to webmail, social networks and other common sites.

Users who resuse passwords are often unaware of how a breach on one site can allow access to several others.

MD5 or SHA-1
BILLIONS OF GUESSES PER SECOND

SHA512CRYPT
A FEW THOUSAND GUESSES PER SECOND

BCRYPT or SCRYPT
A FEW THOUSAND GUESSES PER SECOND

Slow it Down

By design, some hash functions can be calculated quickly. These are not good for storing passwords as attackers can guess many combinations per second.

Better to use a slow hash function which vastly reduces the number of guesses per second, making the recovery process much harder.

Passwords are leaked when an attacker gains access to a database through SQL Injection, XSS, or another vulnerability.

The passwords are often stored as a hash, an encrypted representation of the text.

In a recent study*

59%

of users were found to be using the same password on multiple sites, including their webmail accounts.

*http://www.troyhunt.com/2012/07/what-do-sony-and-yahoo-have-in-common.html

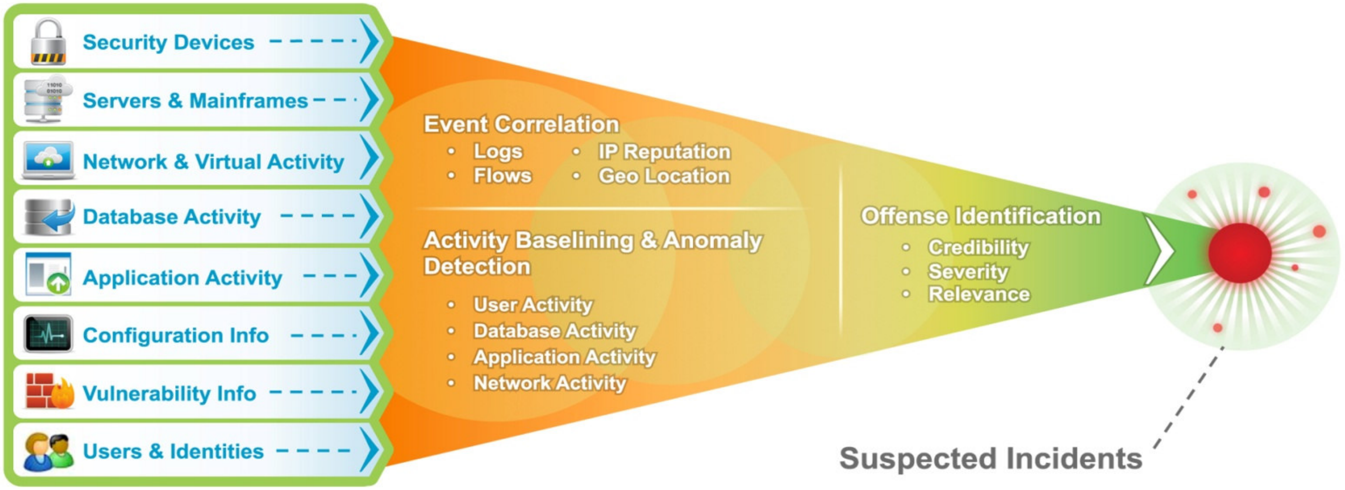
Bring Your Own Device (BYOD)

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

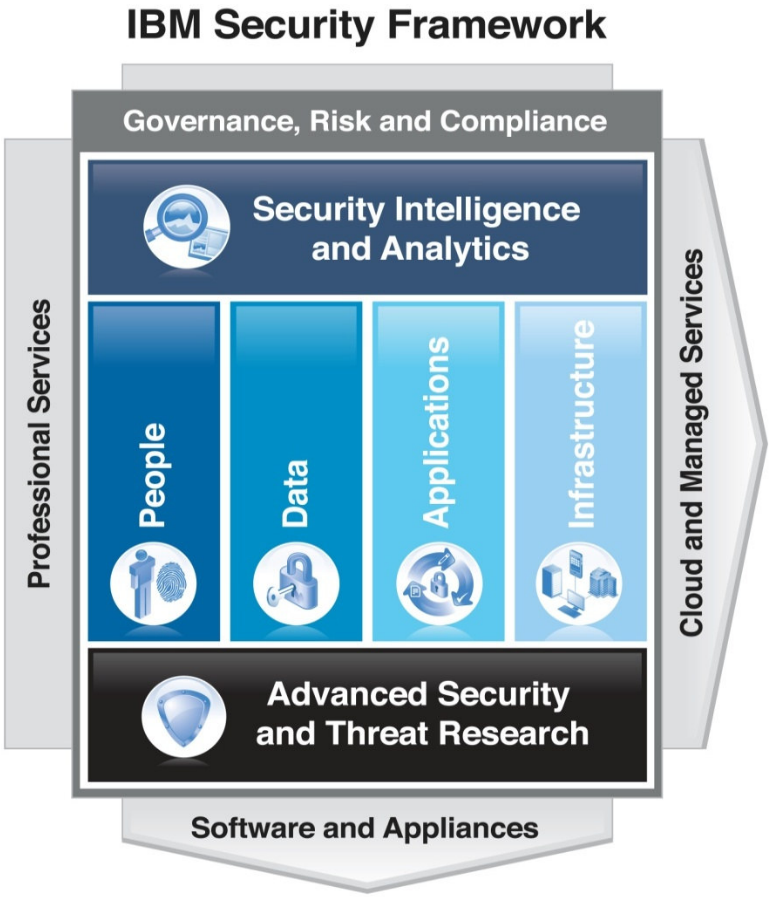
- Challenges
  - BYOD program definition and review
  - Mobile platform vulnerability management

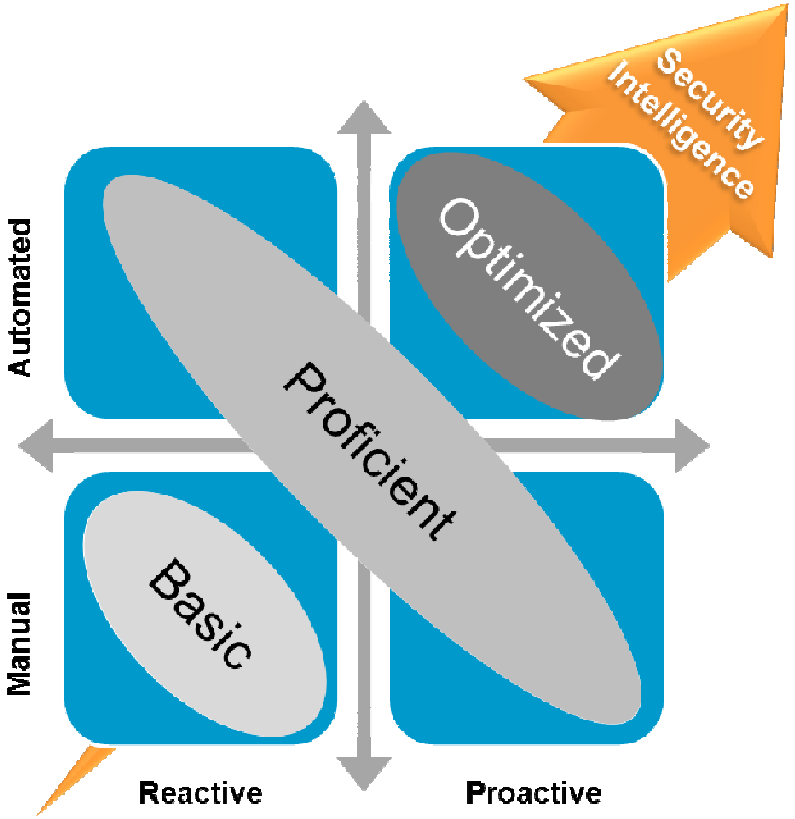
An Approach to Identify Advance Persistent Threats

O	Observation	Defender: Observe the activities of the attacker	Attacker: ability to view and obtain data
C	Concealment	Defender: conceal the network architecture and data	Attacker: hide their malicious actions
O	Obstacles	Place obstacles in each other's way in order to deter or obstruct the ability to successfully defend or attack the network	
K	Key Terrain	areas within the network which contain high profile, high value, or high payoff targets.	
A	Avenues of Approach	areas within the network which contain high profile, high value, or high payoff targets.	



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


IBM Security Framework
Governance, Risk and Compliance
Security Intelligence and Analytics
People
Data
Applications
Infrastructure
Advanced Security and Threat Research
Professional Services
Cloud and Managed Services
Software and Appliances



Intelligence • Integration • Expertise

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