IT Security:
Current Landscape and 2012 Priorities

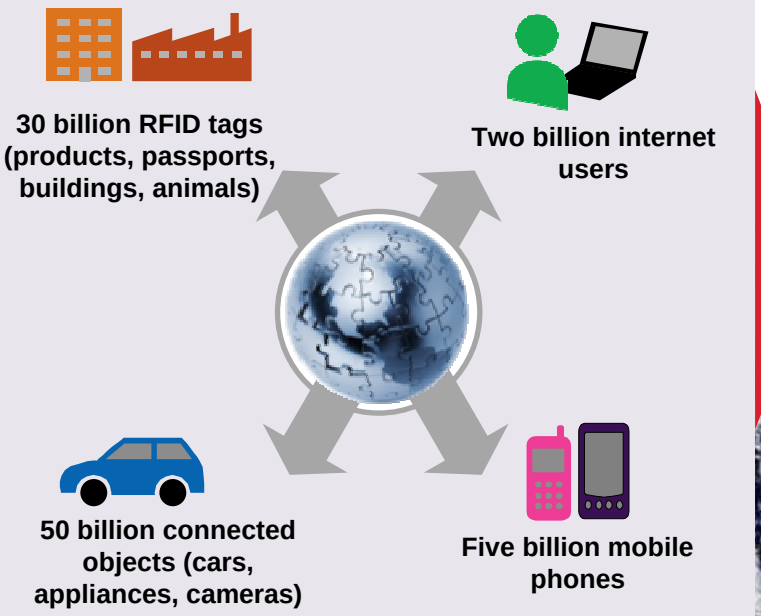
Venkatesh Sadayappan

Security Solutions Consultant,

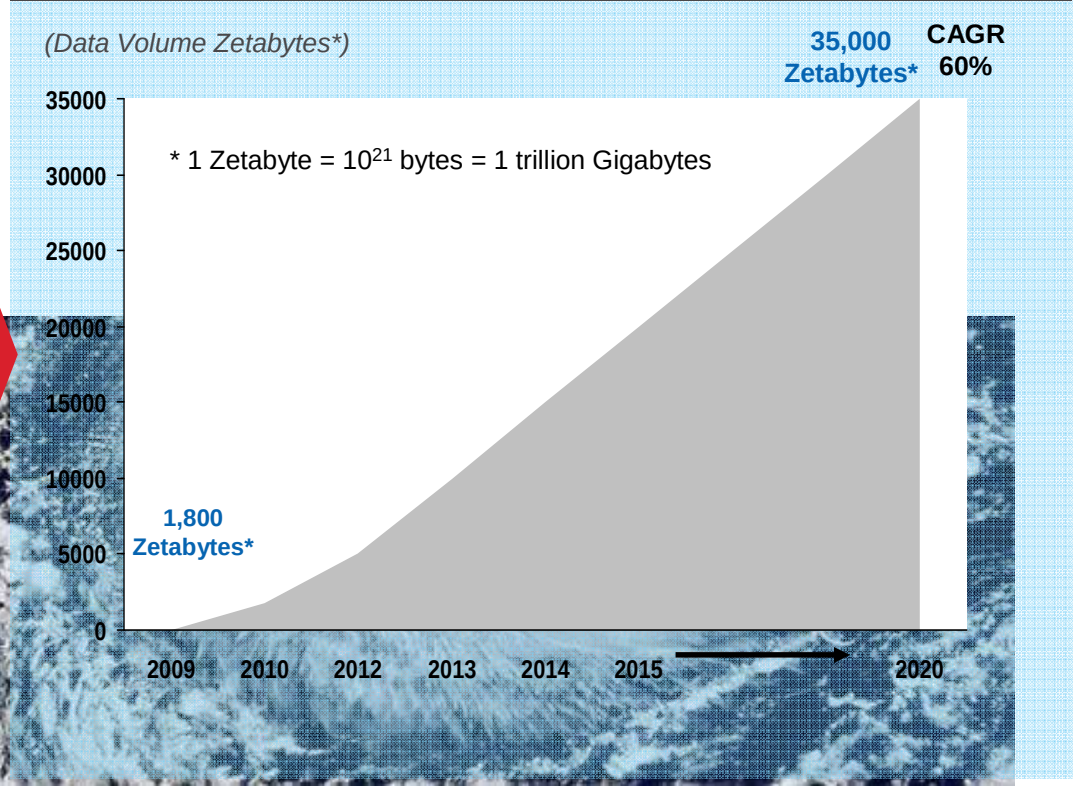
Security Tiger Team, IBM Worldwide

The world is becoming more digitized and interconnected

EXPLODING DIGITAL UNIVERSE



WORLDWIDE DATA VOLUMES PROJECTED TO INCREASE 29X OVER 10 YEARS



*Source: International Telecommunications Union. "Global Number of Internet Users, total and per 100 Inhabitants, 2000-2010." United Nations. http://www.itu.int/ITU-D/ict/statistics/material/excel/2010/Internet_users_00-10_2.xls; Ericsson. "More than 50 billion connected devices – taking connected devices to mass market and profitability." February 14, 2011. http://www.ericsson.com/news/110214_more_than_50_billion_244188811_c; IDC "Digital Universe Study," sponsored by EMC. May 2010

IBM Global Security Reach

9 Security Operations Centers + 9 Security Research Centers + 133 Monitored Countries + 20,000+ Devices under Contract + 3,700+ MSS Clients Worldwide + 21 Billion+ Events Per Day

IBM X-Force R&D - Unmatched Security Leadership

X-Force Research

14B analyzed Web pages & images

40M spam & phishing attacks

54K documented vulnerabilities

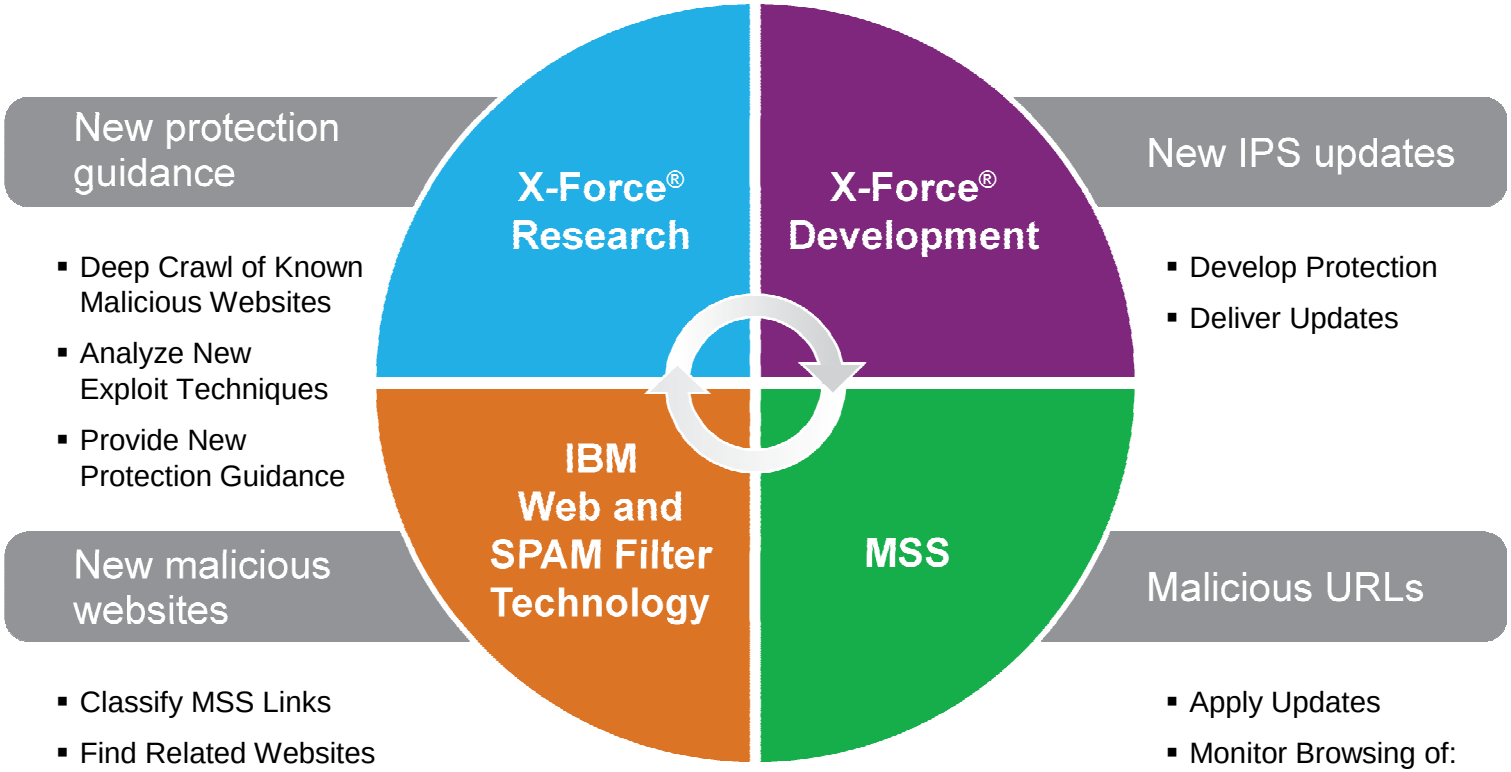
Billions of intrusion attempts daily

Millions of unique malware samples

Provides Specific Analysis of:

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

IBM X-Force web intelligence lifecycle



- Deep Crawl of Known Malicious Websites
- Analyze New Exploit Techniques
- Provide New Protection Guidance

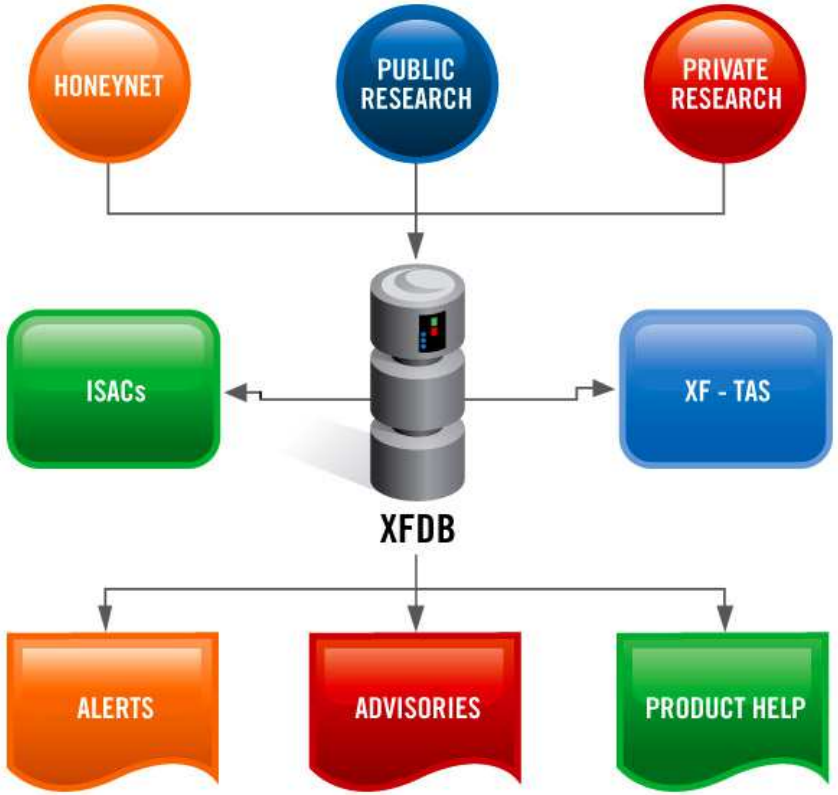
- Develop Protection
- Deliver Updates

- Classify MSS Links
- Find Related Websites (Deep Crawl)
- Search for Malware
- Find New Malicious Websites
- Block All Malicious Domains

- Apply Updates
- Monitor Browsing of:
  - Million of End-users
  - Thousands of Customers
  - Hundreds of Countries
- Block Malicious Links
- Send Links to X-Force

We analyze them all…

- Most comprehensive Vulnerability Database in the world
  - Over **50,000** unique vulnerabilities catalogued
  - Entries date back to the 1990's
- Updated daily by a dedicated research team
- The X-Force database currently tracks over...
  - 8000 Vendors
  - 17,000 Products
  - 40,000 Versions



Agenda

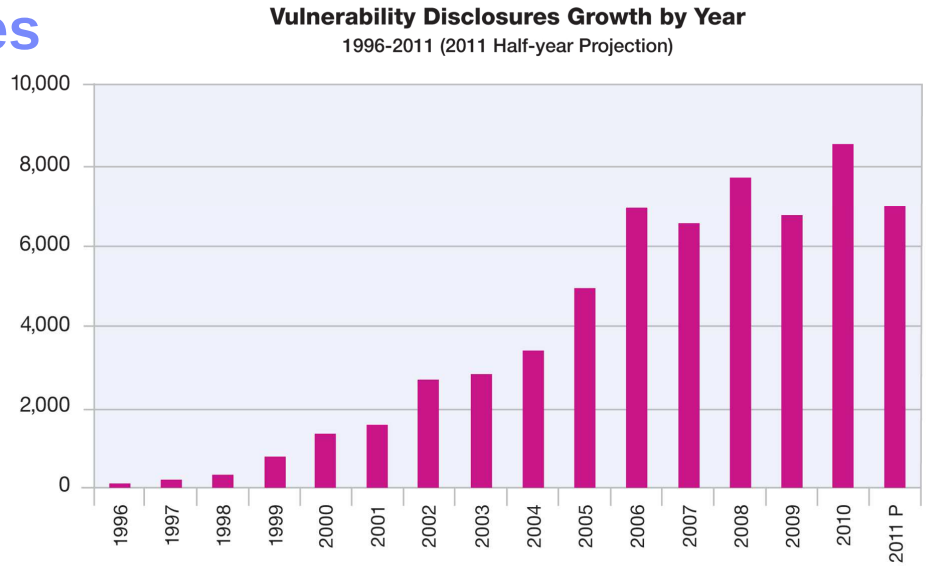
- Good news, we're making headway against threats and vulnerabilities

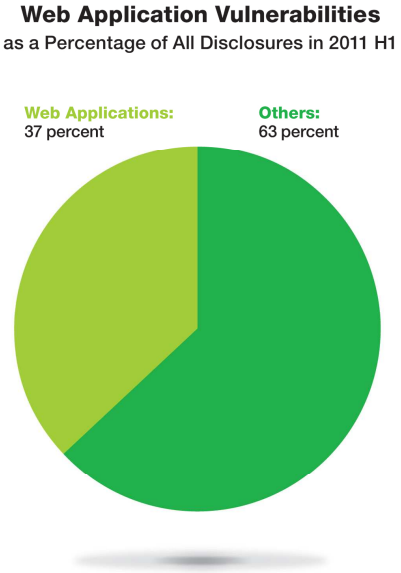
- Bad news, the landscape is becoming more complicated

- The Year of the Security Breach
  - Broadly targeted, financially motivated attacks
  - Advanced Persistent Threats
  - Hacktivism

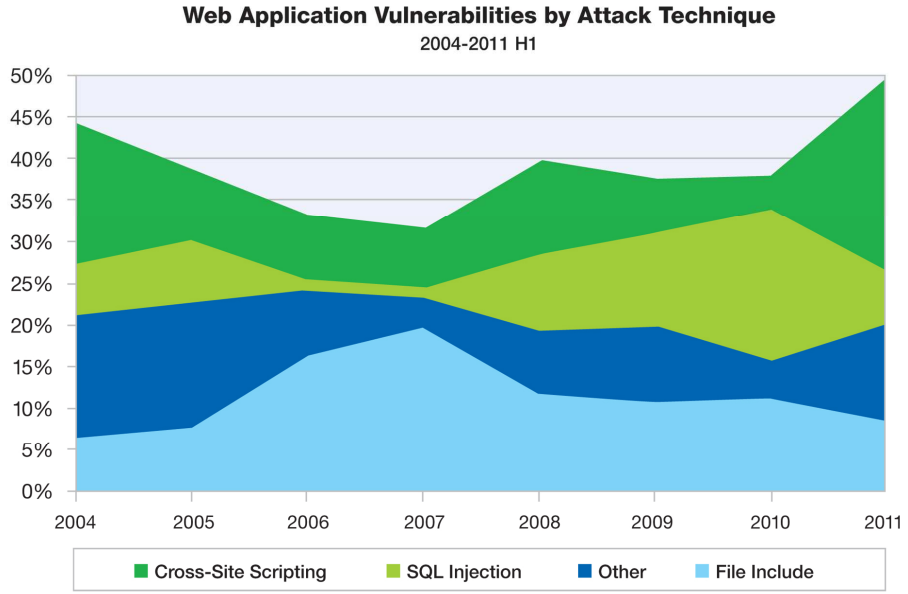
Decline in web vulnerabilities

- Total number of vulnerabilities decline — but it's cyclical
- Decline is in web application vulnerabilities





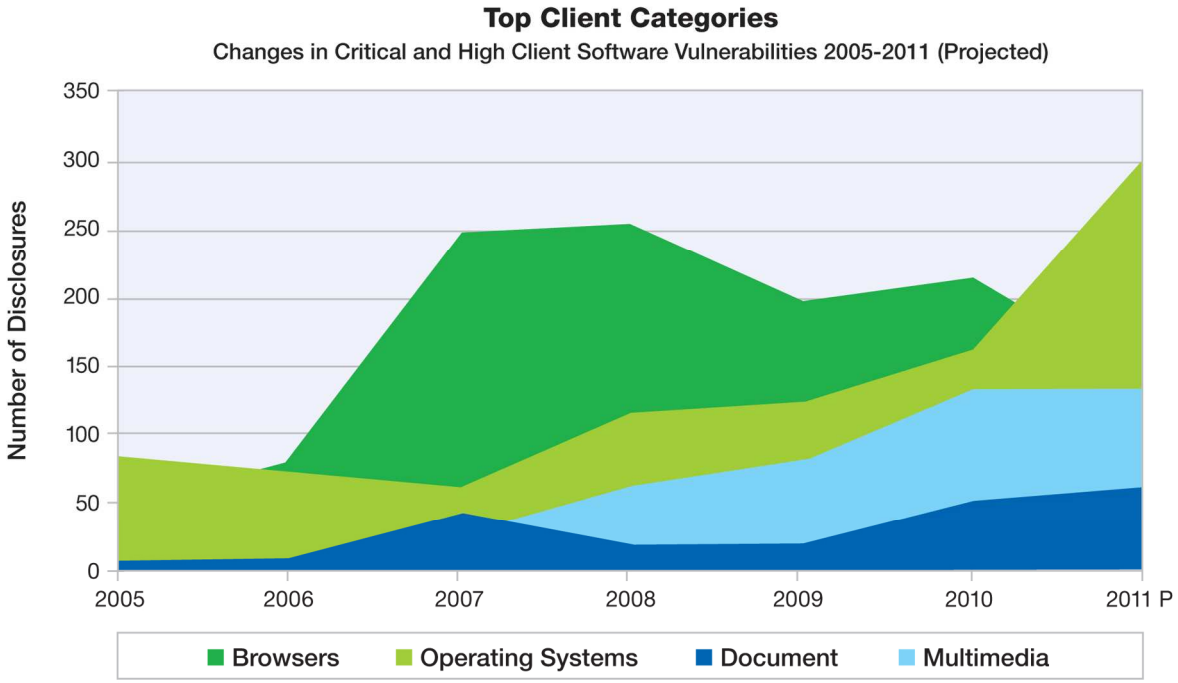
Source: IBM X-Force® Research and Development



Source: IBM X-Force® Research and Development

Exploiting other types of vulnerabilities more challenging

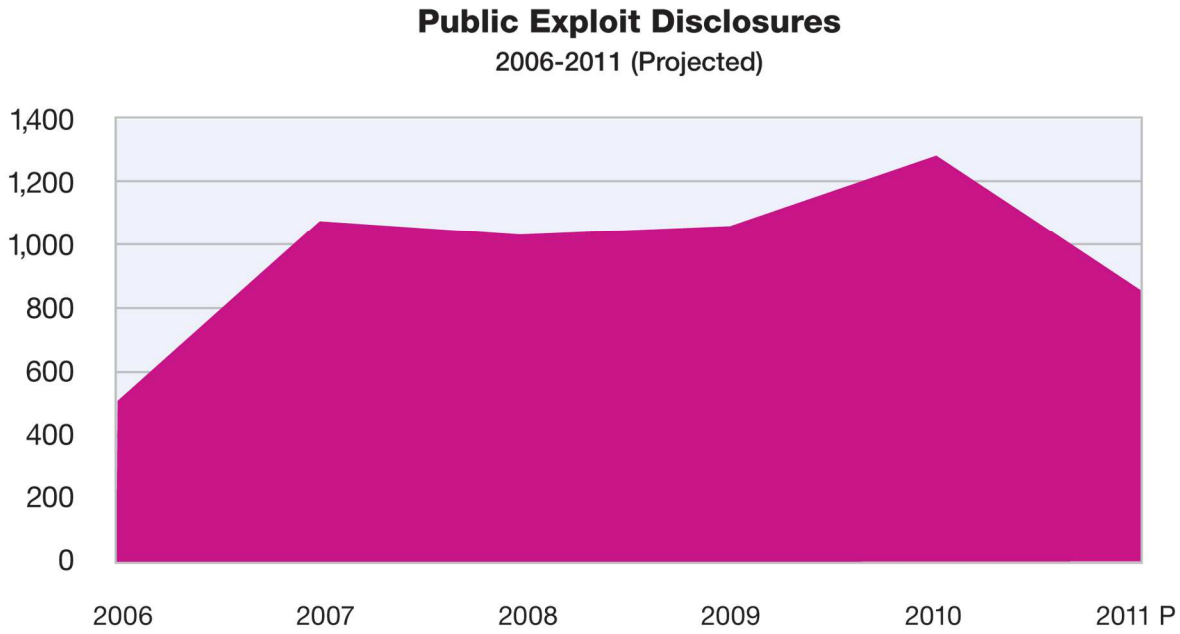
- High and critical OS disclosures exceed those in browsers
- However, advanced OS security features have made exploiting these vulnerabilities more challenging



Source: IBM X-Force® Research and Development

Public exploit disclosures decline

- Fewer exploits released in 2011
- Down as a percentage of vulnerabilities as well to 12%



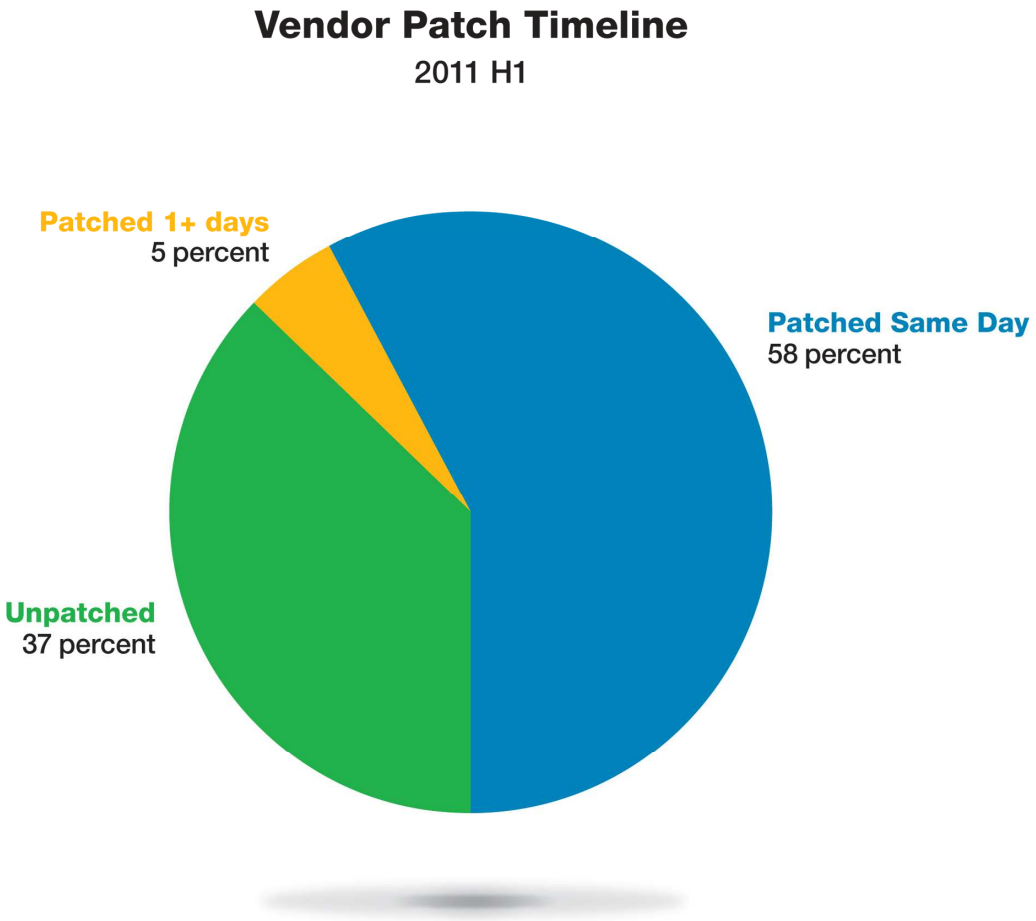
Source: IBM X-Force® Research and Development

True Exploits	2006	2007	2008	2009	2010	2011 Projected
Percentage of Total	7.3 percent	16.5 percent	13.4 percent	15.7 percent	14.9 percent	12.0 percent

Table 5: Public exploit disclosures – 2006-2011 (Projected)

Improvement in availability of Vendor Patches

- Significant improvement in unpatched vulnerabilities
- Hasn't dropped below 44% in over five years

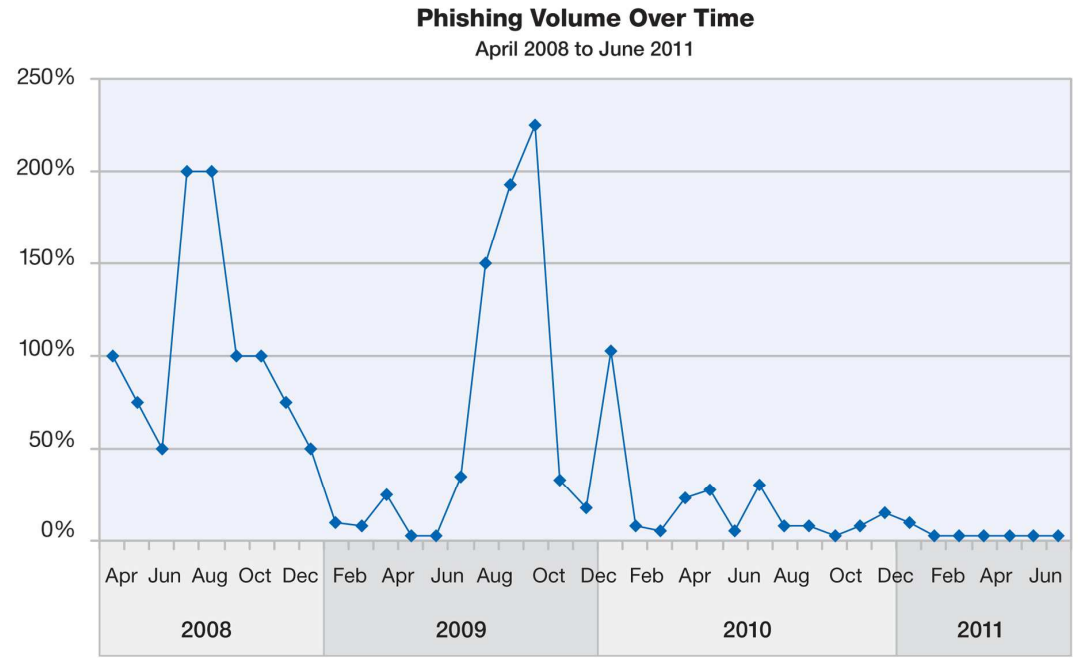


Source: IBM X-Force® Research and Development

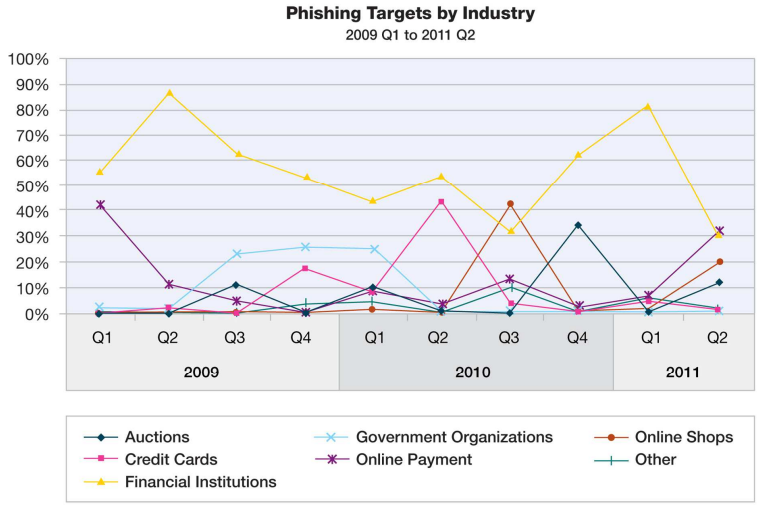
Goodbye to Phishing

- In 2011, spammers said goodbye to traditional email phishing. When looking at the percentage of spam that is phishing on a weekly basis we have measured less than 0.01 percent for every month.

- 80% still targeting financial institutions



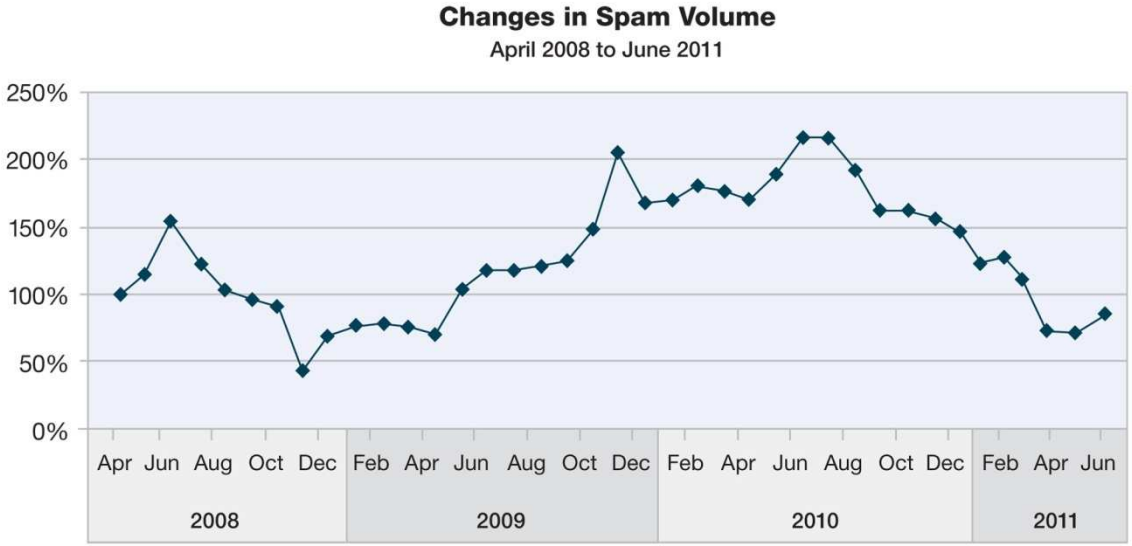
Source: IBM X-Force® Research and Development

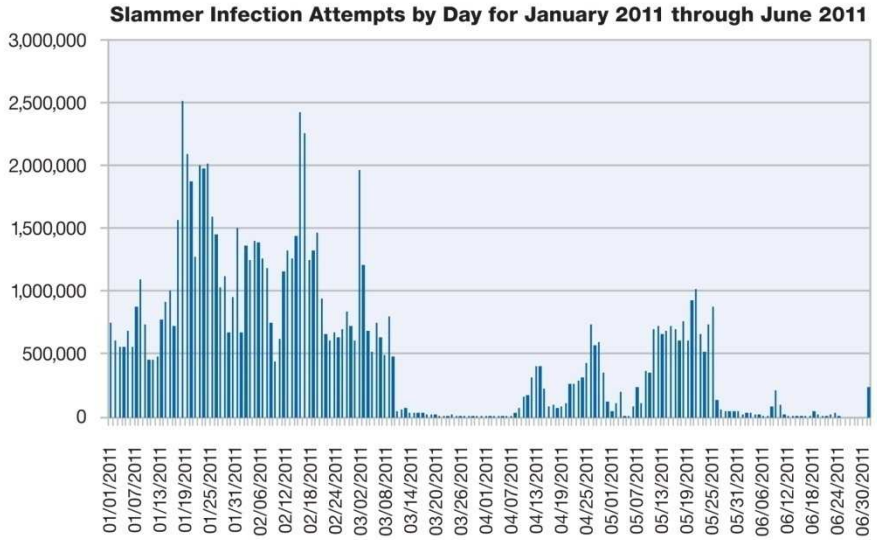


Source: IBM X-Force® Research and Development

Action taken against Bot Networks

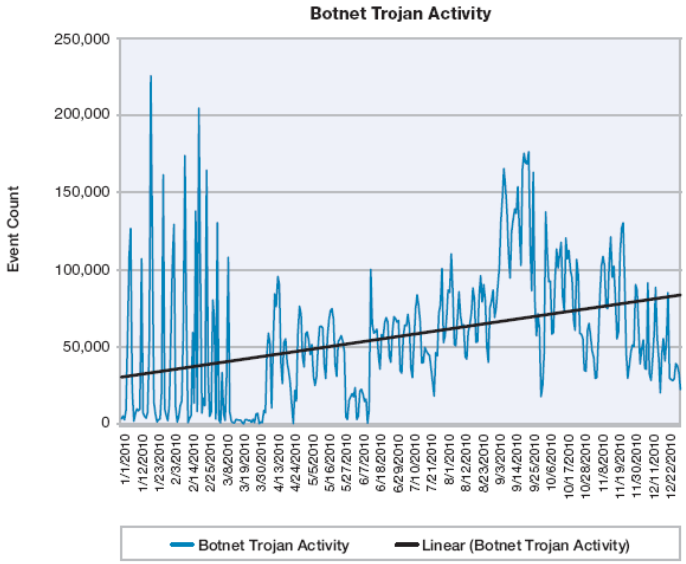
- Rustock Botnet Takedown early in 2011 caused significant spam volume decline.
- IBM Botnet C&C data from 2011 shows abrupt disappearance of Waledec.
- A number of other botnets have been taken out by vendors, researchers, and law enforcement.
- Mysterious disappearance of SQL Slammer





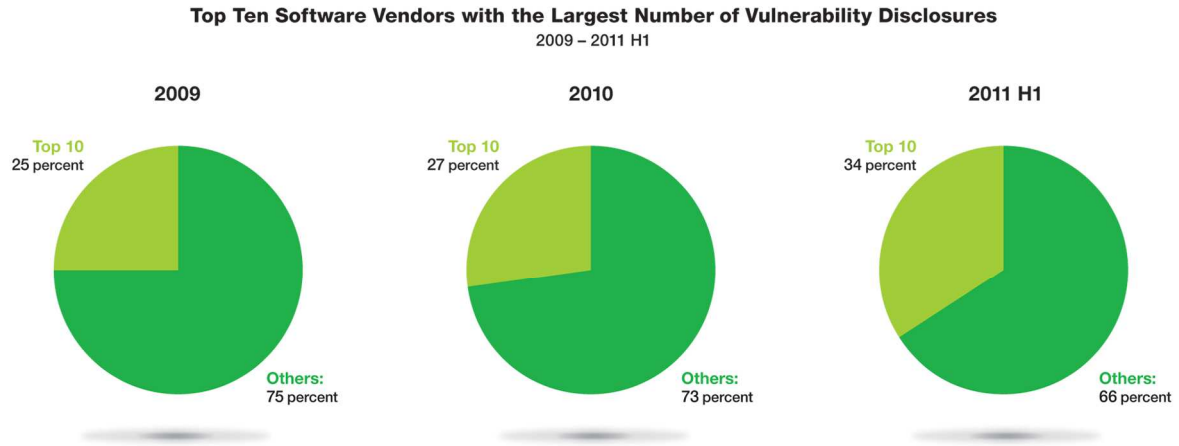
Source: IBM X-Force® Research and Development

Source: IBM X-Force® Research and Development



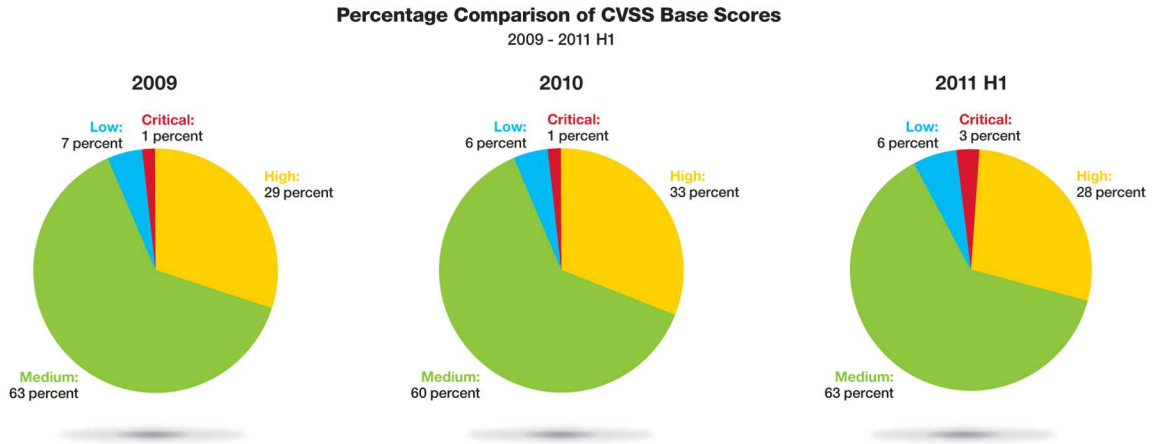
Critical vulnerabilities up

- Top 10 vendors a greater percentage



Source: IBM X-Force® Research and Development

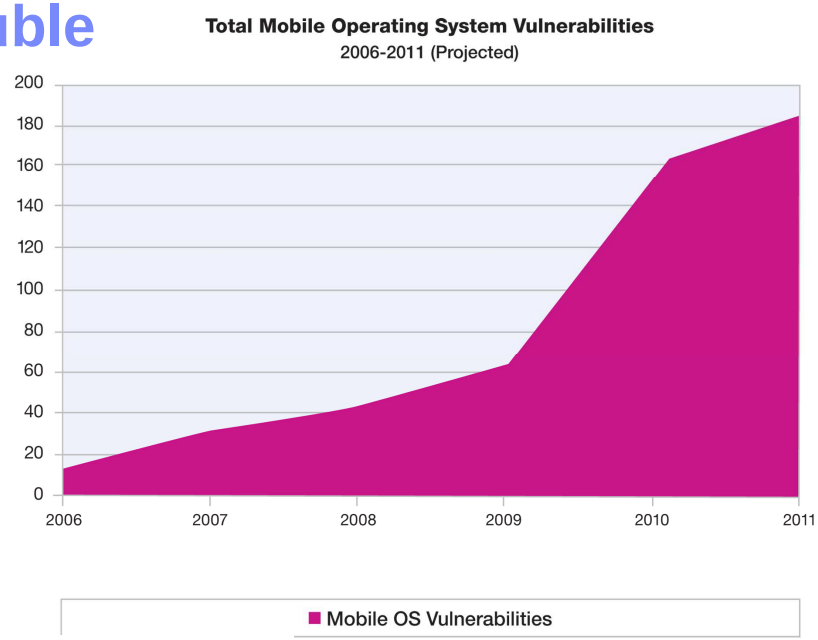
- Critical vulnerabilities triple as a percentage



Source: IBM X-Force® Research and Development

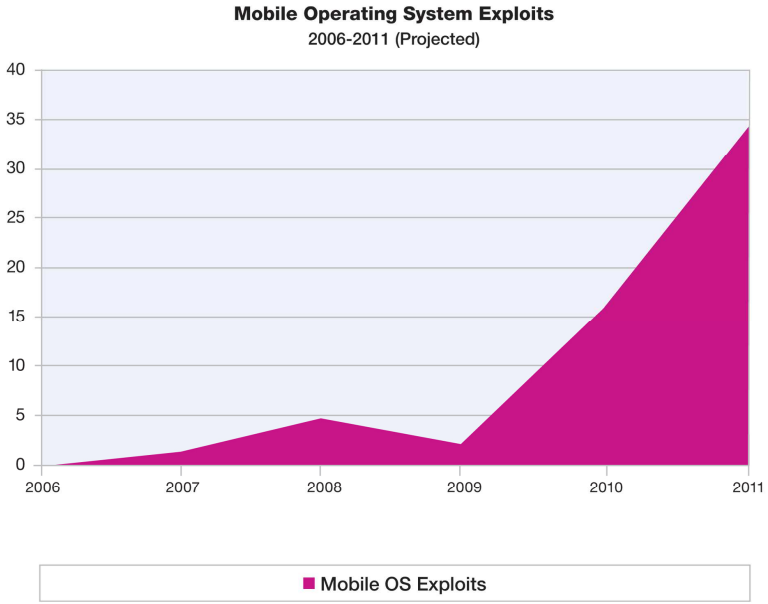
Mobile OS exploits projected to double

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



Source: IBM X-Force® Research and Development

- Attackers finally warming to the opportunities these devices represent



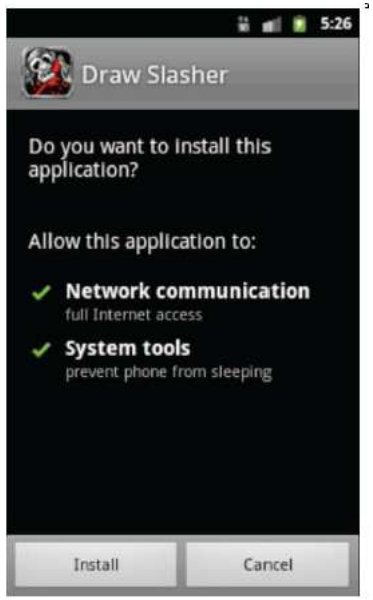
Source: IBM X-Force® Research and Development

COMPUTERWORLD
The voice of the ICT community

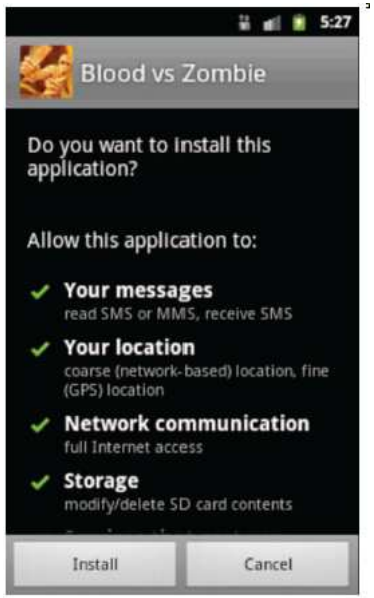
IBM X-Force: Mobile devices are a fast growing target of malware

Look for double the mobile exploits this year vs. 2010 and particularly watch out for mobile applications that are really malware, says IBM's X-Force security research team.

By Tim Greene, Framingham | Friday, 30 September, 2011



Draw Slasher, a legitimate game that requires minimal permissions

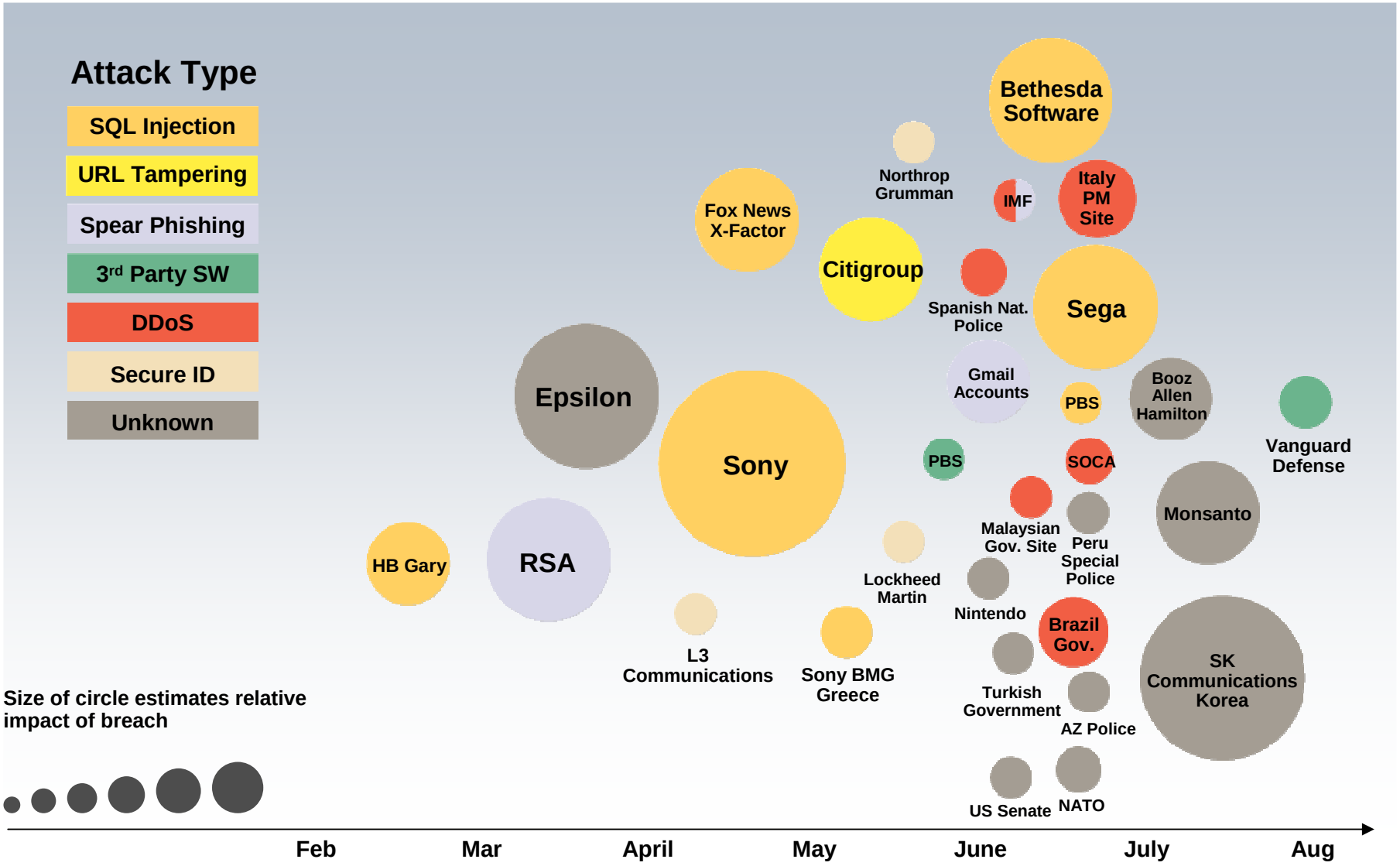


Blood versus Zombie, a malicious copy of Draw Slasher that contains more permissions than a game should need—including GPS[1] and SMS[2] access.

[1]GPS – Global Positioning System

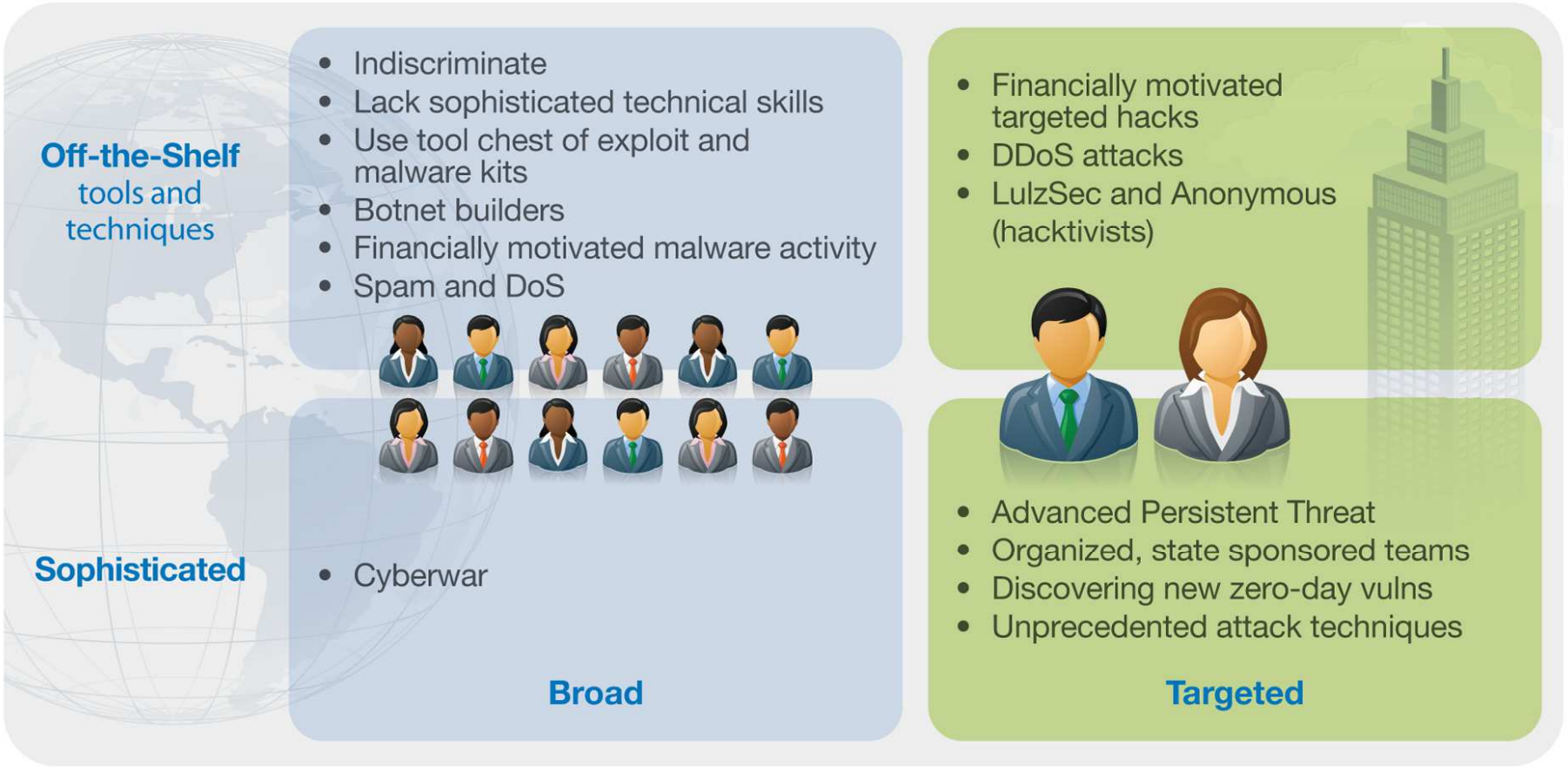
[2]SMS – Short Message Service

2011 – The Year of the Targeted Attack



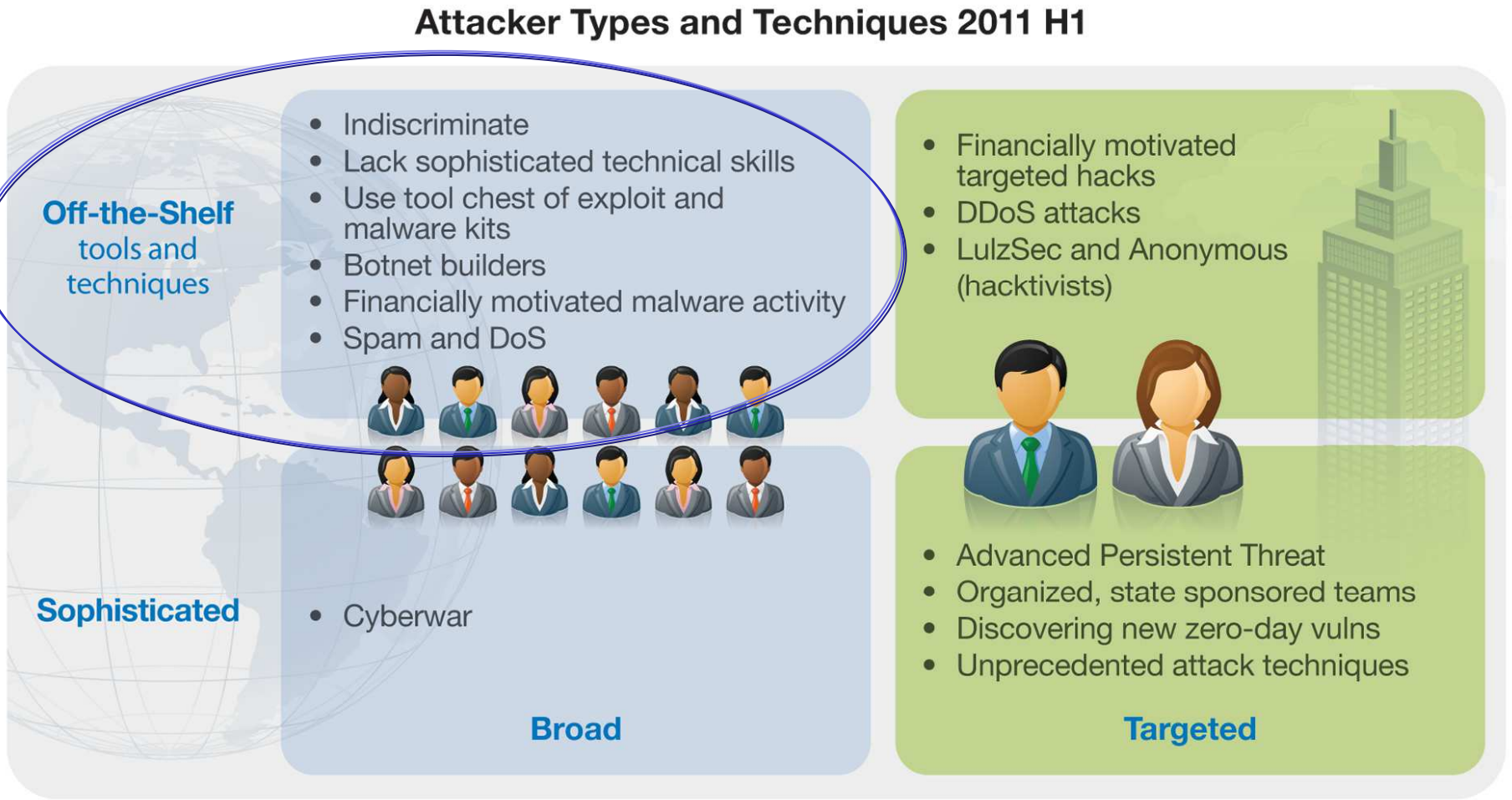
Who is attacking our networks?

Attacker Types and Techniques 2011 H1



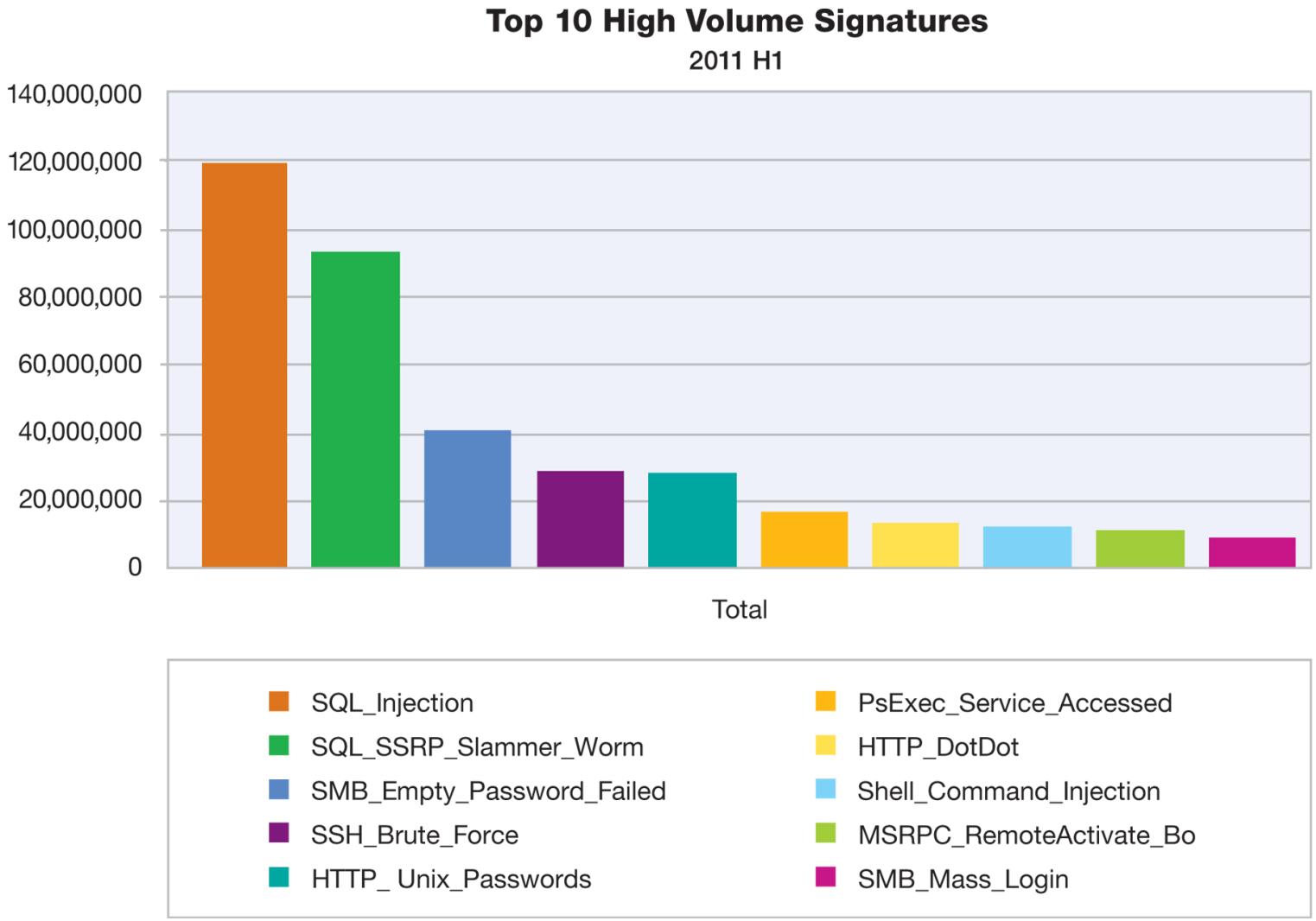
Source: IBM X-Force® Research and Development

Who is attacking our networks?



Source: IBM X-Force® Research and Development

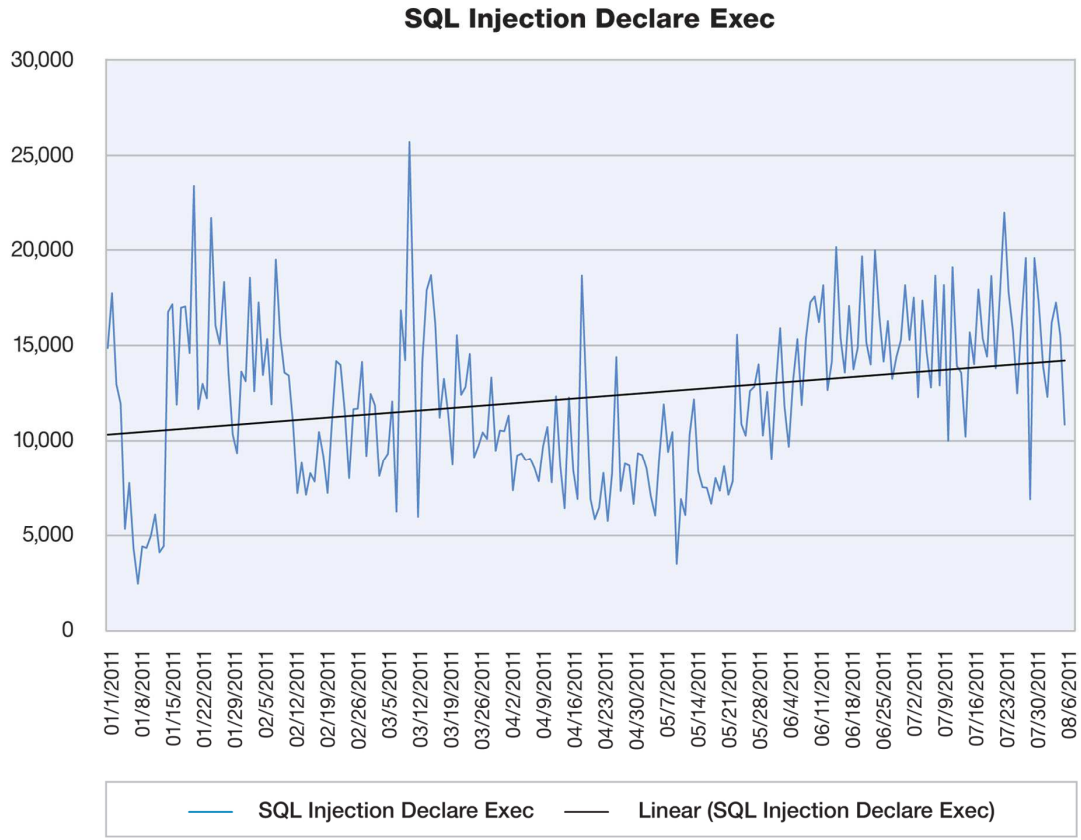
Highest volume signatures



Source: IBM X-Force® Research and Development

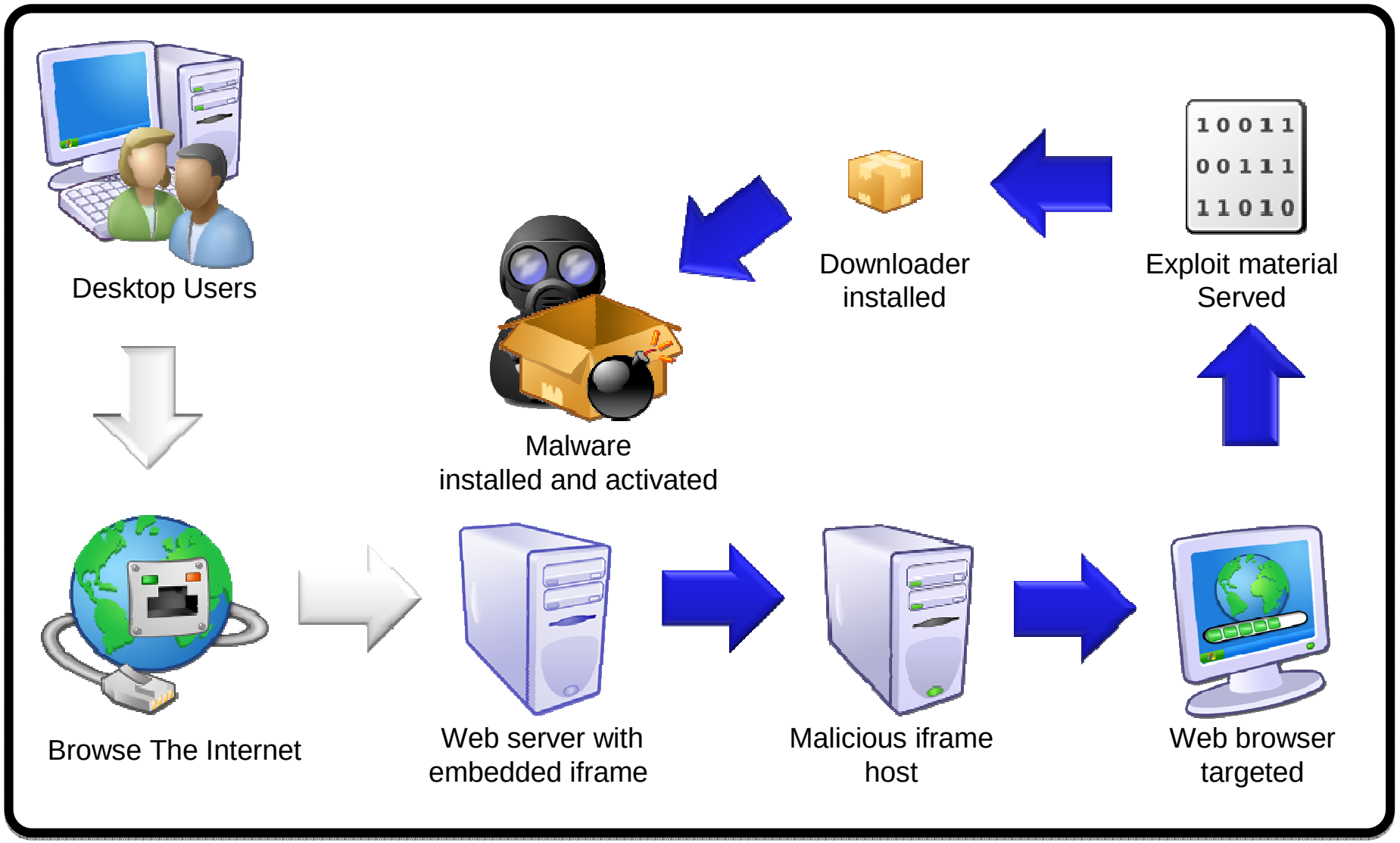
SQL Injection continues to be a favorite attack vector

- Attackers are analyzing Web applications to find SQL injection vulnerabilities they can exploit
- Once a vulnerable Web application has been identified, attackers use search engines to automate the process of finding target sites

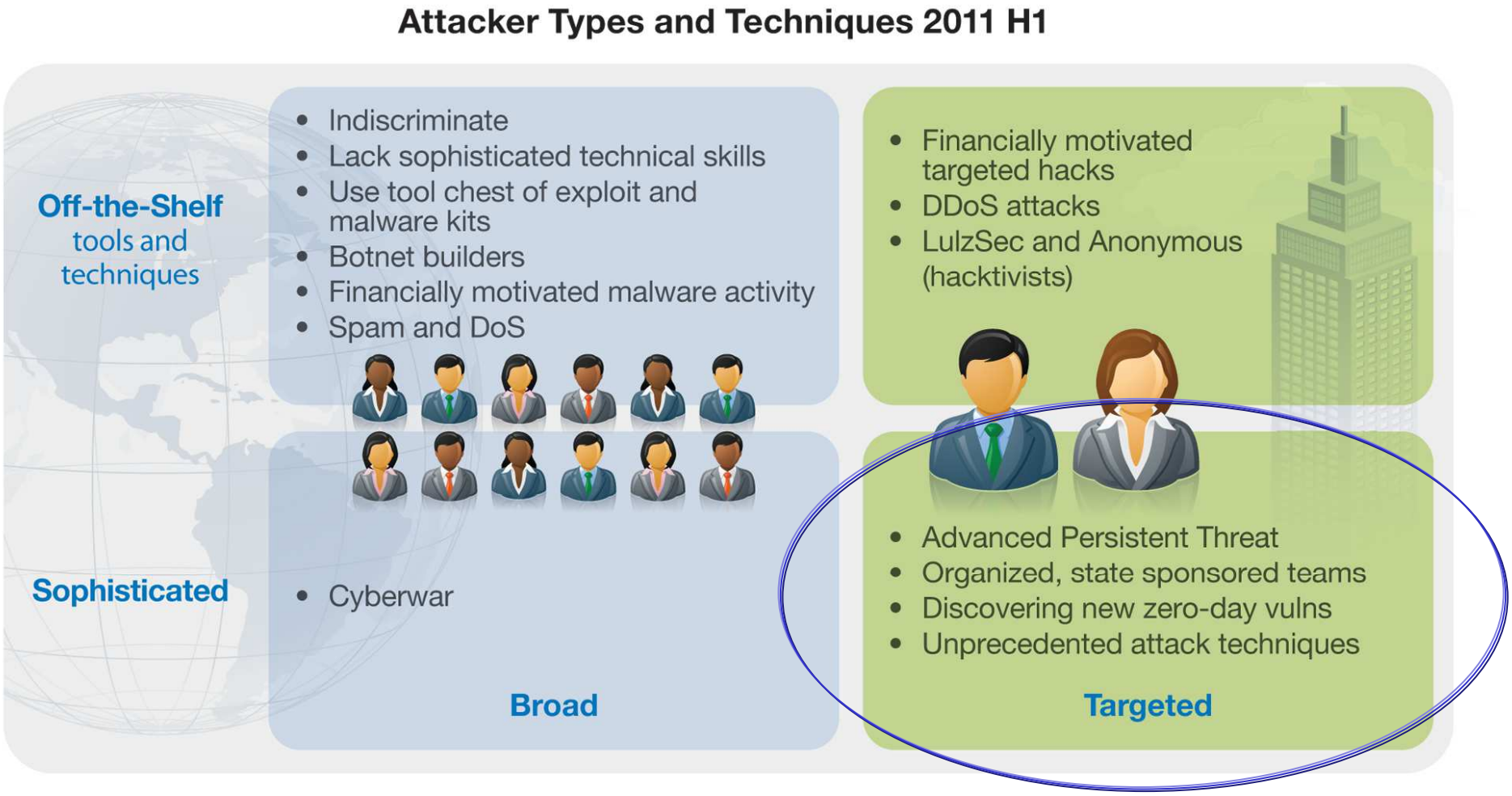


Source: IBM X-Force® Research and Development

The drive-by-download process



Who is attacking our networks?



Source: IBM X-Force® Research and Development

What is APT?

- **Advanced**
  - Using exploits for unreported vulnerabilities (zero day)
  - Advanced, custom malware that isn't detected by antivirus products
  - Coordinated attacks using a variety of vectors
- **Persistent**
  - Attacks lasting for months or years
  - Resistant to remediation attempts
  - Attackers are dedicated to the target – they WILL get in
- **Threat**
  - Targeted at specific individuals and groups within an organization, aimed at compromising confidential information
  - Not random attacks – they're actually "out to get you"

Internet Intelligence Collection

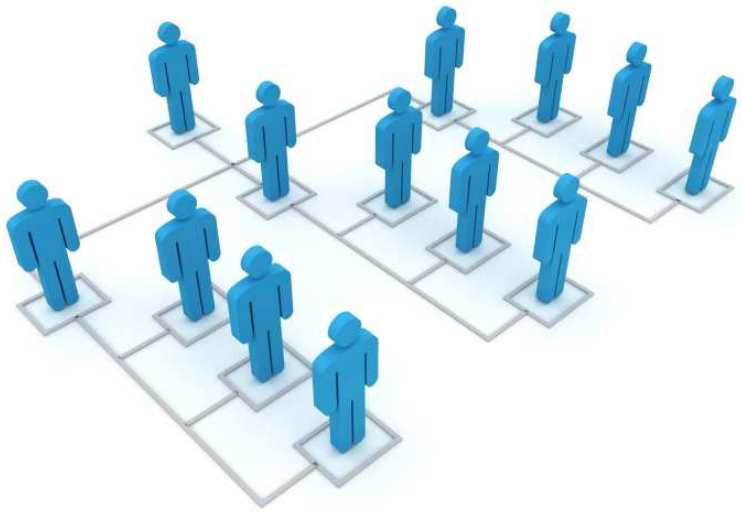
- Scan the corporate website, Google, and Google News
  - Who works there? What are their titles?
  - Write index cards with names and titles

- Search for Linkedin, Facebook, and Twitter Profiles
  - Who do these people work with?
  - Fill in blanks in the org chart

- Who works with the information we'd like to target?
  - What is their reporting structure?
  - Who are their friends?
  - What are they interested in?
  - What is their email address?

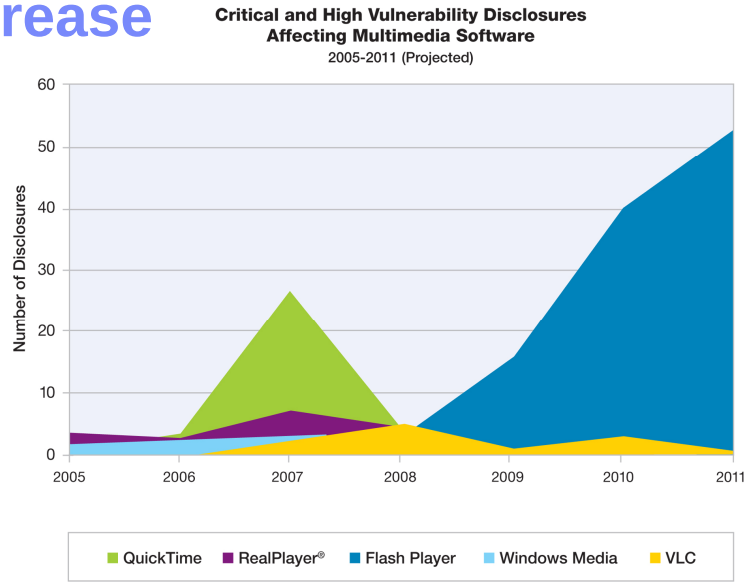
    At work?

    Personal email?

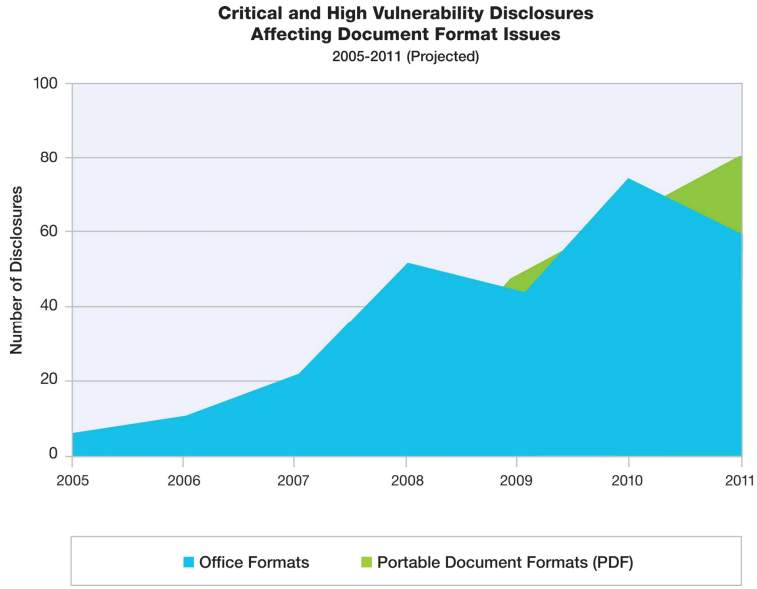


Multi-media & doc vulnerabilities increase

- Significant increases in both categories
- Attackers have zeroed in on software that consumers are running regardless of the browser
- Recent efforts to sandbox these applications are not perfect

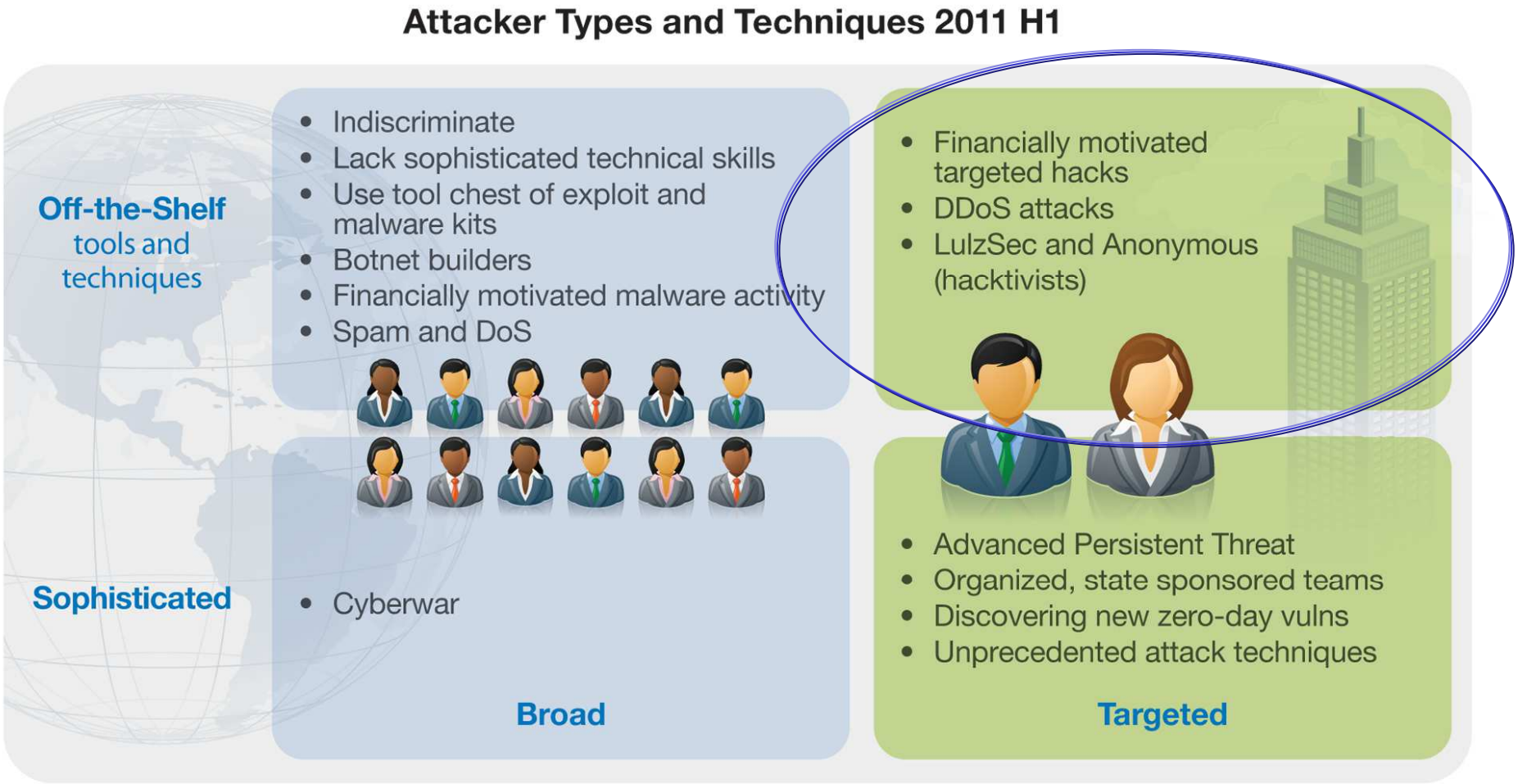


Source: IBM X-Force® Research and Development



Source: IBM X-Force® Research and Development

Who is attacking our networks?



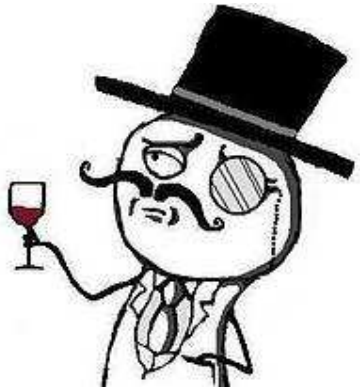
Source: IBM X-Force® Research and Development

Hacktivists are politically motivated

A member of Anonymous at the Occupy Wall Street protest in New York*

ANONYMOUS

One self-description is:
"We are Anonymous. We are Legion. We do not forgive. We do not forget. Expect us."**



Lulz Security logo

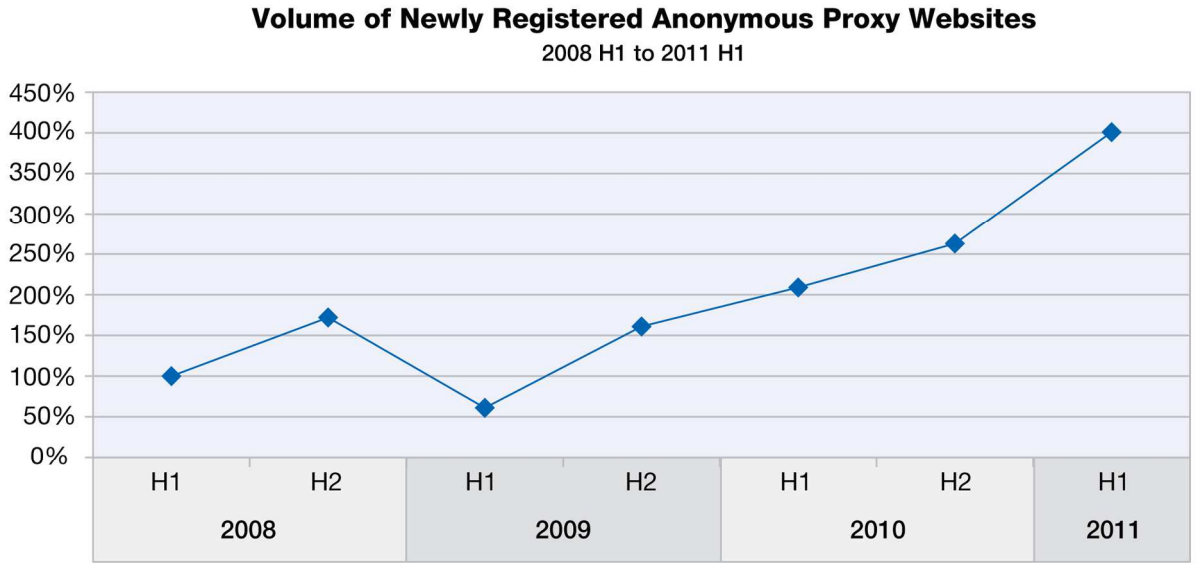
"The world's leaders in high-quality entertainment at your expense."

*Source: David Shankbone

**Source: Yale Law and Technology, November 9, 2009

Anonymous proxies on the rise

- About 4 times the amount from 3 years ago
- Some used to hide attacks, some used to evade censorship

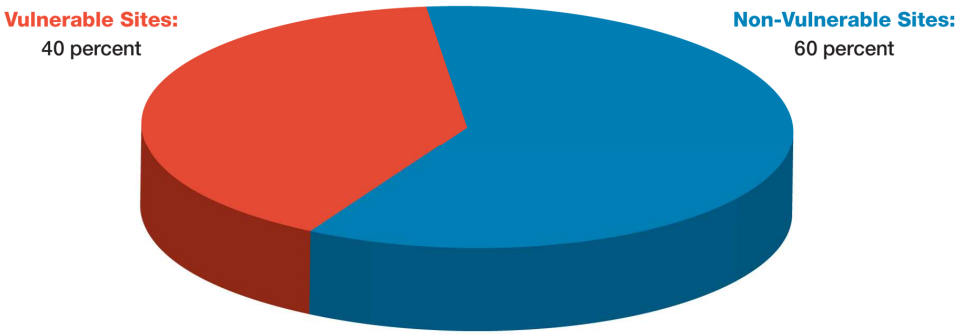


Source: IBM X-Force® Research and Development

Many major operations have important security blindspots

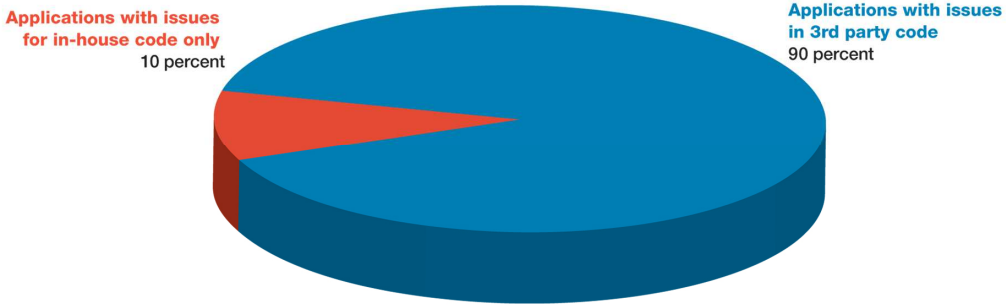
- IBM scanned 678 websites
  - Fortune 500 & 178 popular sites
- 40% contain client-side JavaScript vulnerabilities
- Third party code is primary culprit

Percentage of Vulnerable Websites



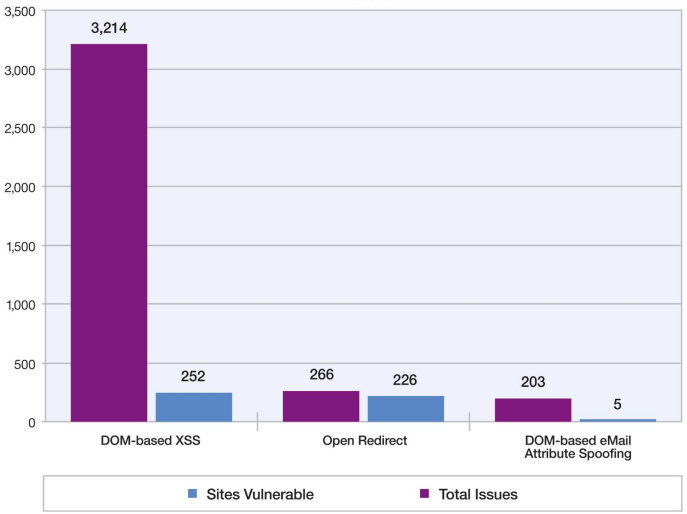
Source: IBM X-Force® Research and Development

Applications with Issues for In-house Code Only vs. Applications with Vulnerable 3rd Party Code



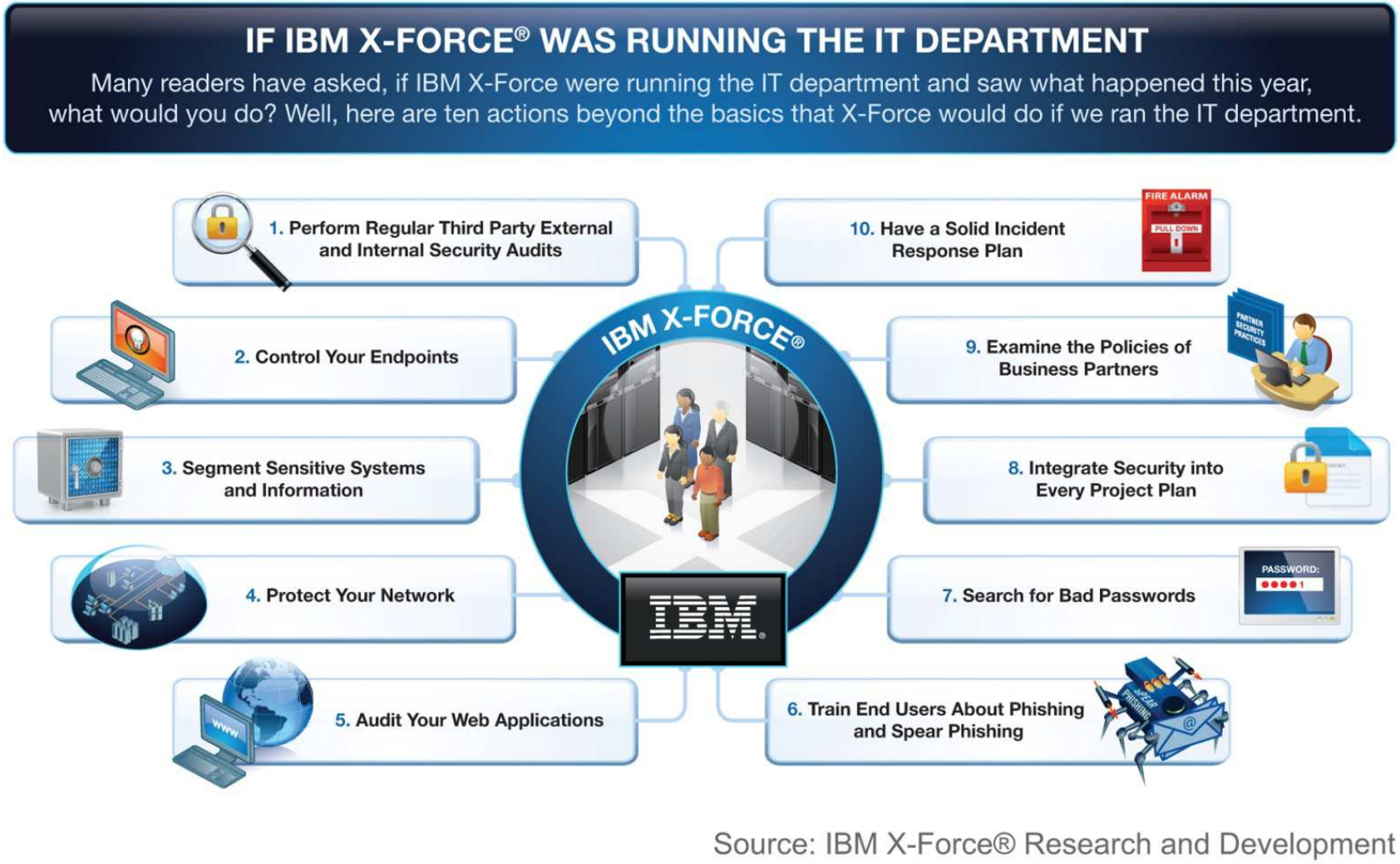
Source: IBM X-Force® Research and Development

Distribution of Client-Side Issue Types
2011 H1



Source: IBM X-Force® Research and Development

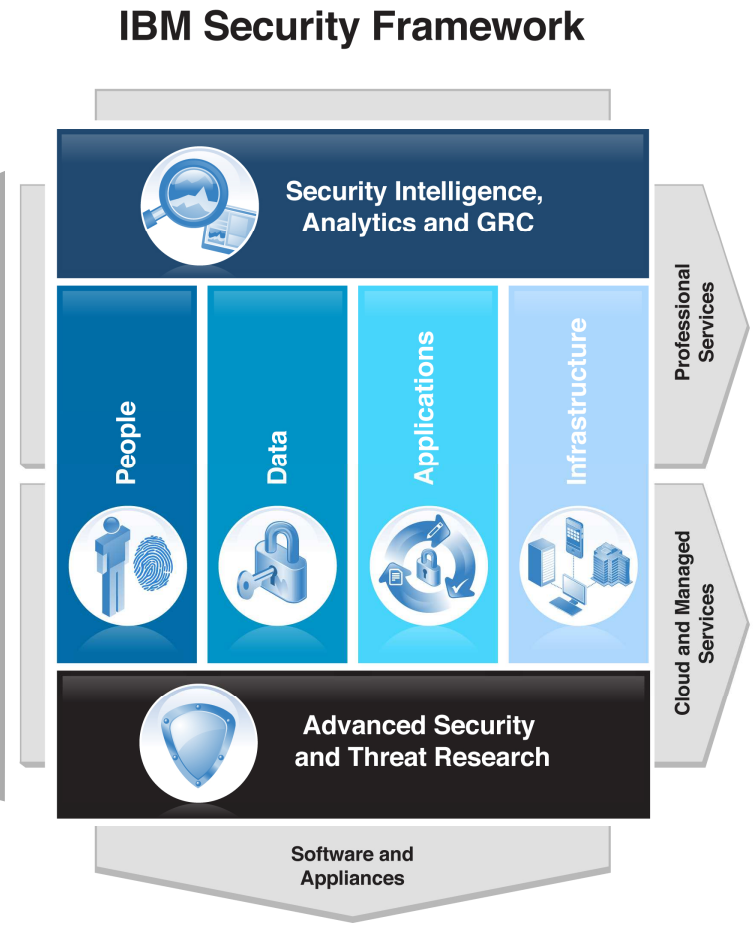
2012 Priorities and Next Steps



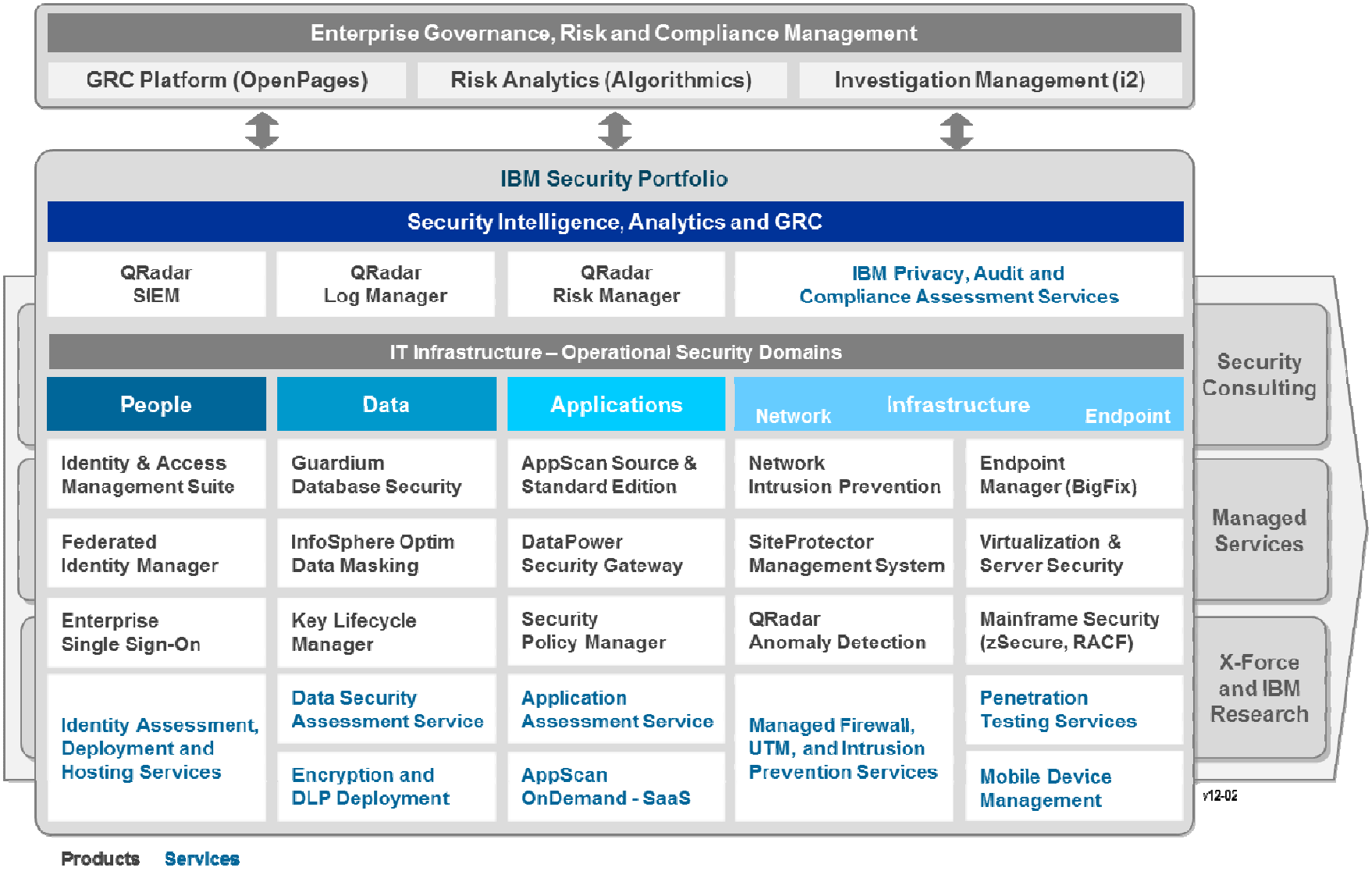
IBM Security Systems

IBM Security Systems

- Unique Security Framework
- $1.8B investment in innovative technologies
- 6K+ security engineers and consultants
- Largest vulnerability database
- Award-winning X-Force® research
- Analyst recognized Leadership in every segment



IBM Security Framework: Product, Services and Research



Thank you for your time today! Get engaged with IBM Security

Follow us at @ibmsecurity and @ibmxforce

Download X-Force security trend & risk reports

http://www.ibm.com/software/hk/security/threatlandscape.html

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

Thank You!

Venkatesh Sadayappan

venky.iss@in.ibm.com

+91-97420-00000