Security Intelligence.
Think Integrated.

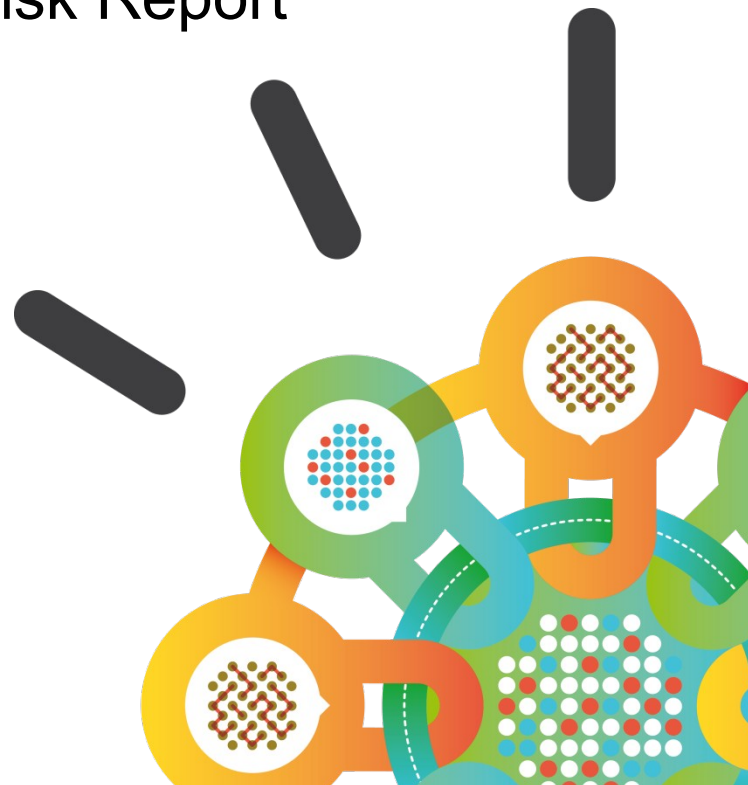
IBM Security Systems

IBM X-Force 2012 Annual Trend and Risk Report

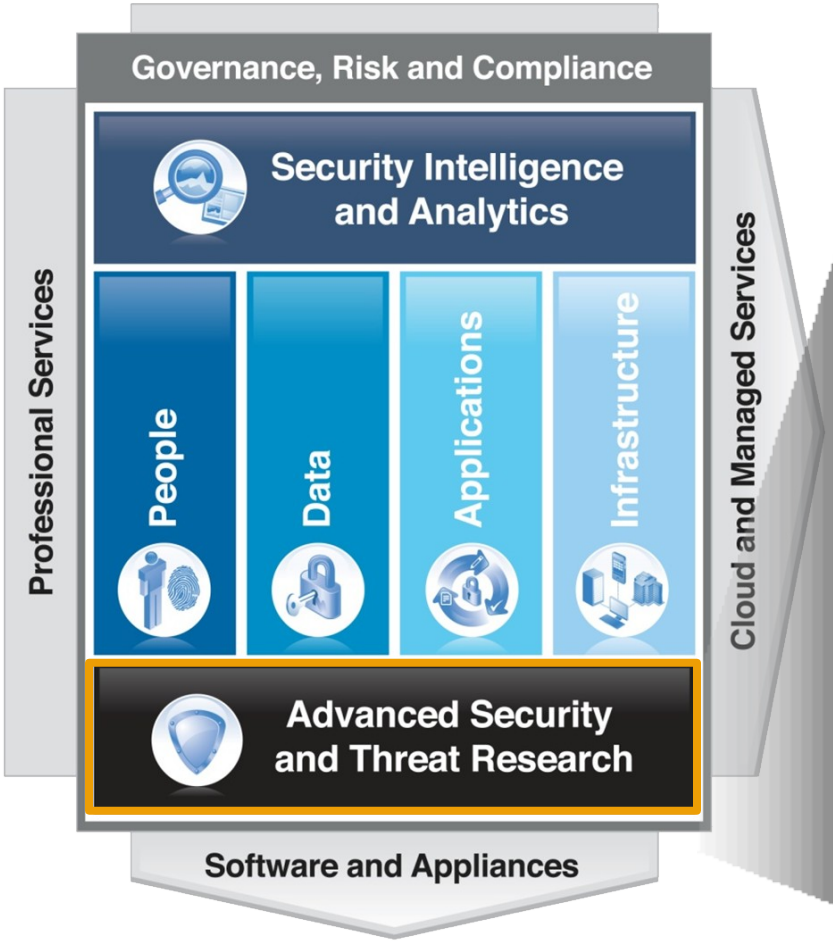
Simon Smith

simon.smith@uk.ibm.com

April 2013



X-Force is the foundation for advanced security and threat research across the IBM Security Framework



X-FORCE

The mission of X-Force is to:

- **Monitor** and evaluate the rapidly changing threat landscape
- **Research** new attack techniques and develop protection for tomorrow's security challenges
- **Educate** our customers and the general public

Collaborative IBM teams monitor and analyze the latest threats

Coverage

20,000+ devices under contract

3,700+ managed clients worldwide

13B+ events managed per day

133 monitored countries (MSS)

1,000+ security related patents

X-FORCE

IBM Research

Depth

17B analyzed web pages & images

40M spam & phishing attacks

80K documented vulnerabilities

Billions of intrusion attempts daily

Millions of unique malware samples

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

Threats and Activity

- 40% increase in breach events for 2012
- Sophistication is not always about technology
- SQL Injection, DDoS, Phishing activity increased from 2011
- Java means to infect as many systems as possible

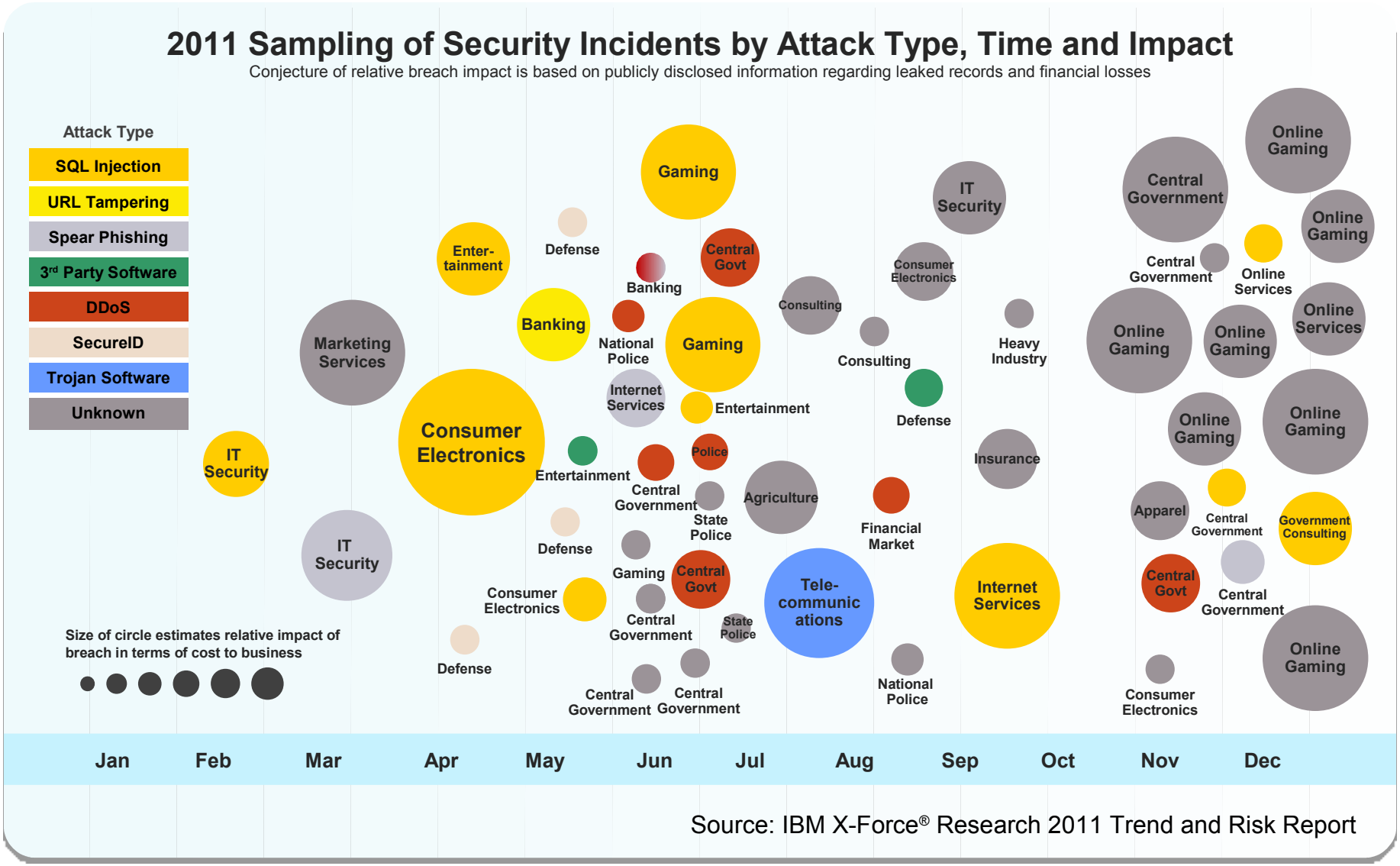
Operational Security

- Software vulnerability disclosures up in 2012
- Web application vulnerabilities surge upward
- XSS vulnerabilities highest ever seen at 53%
- Content Management Systems plug-ins provide soft target

Emerging Trends

- Social Media leveraged for enhanced spear-phishing techniques and intelligence gathering
- Mobile Security should be more secure than traditional user computing devices by 2014

2011: "The year of the targeted attack"

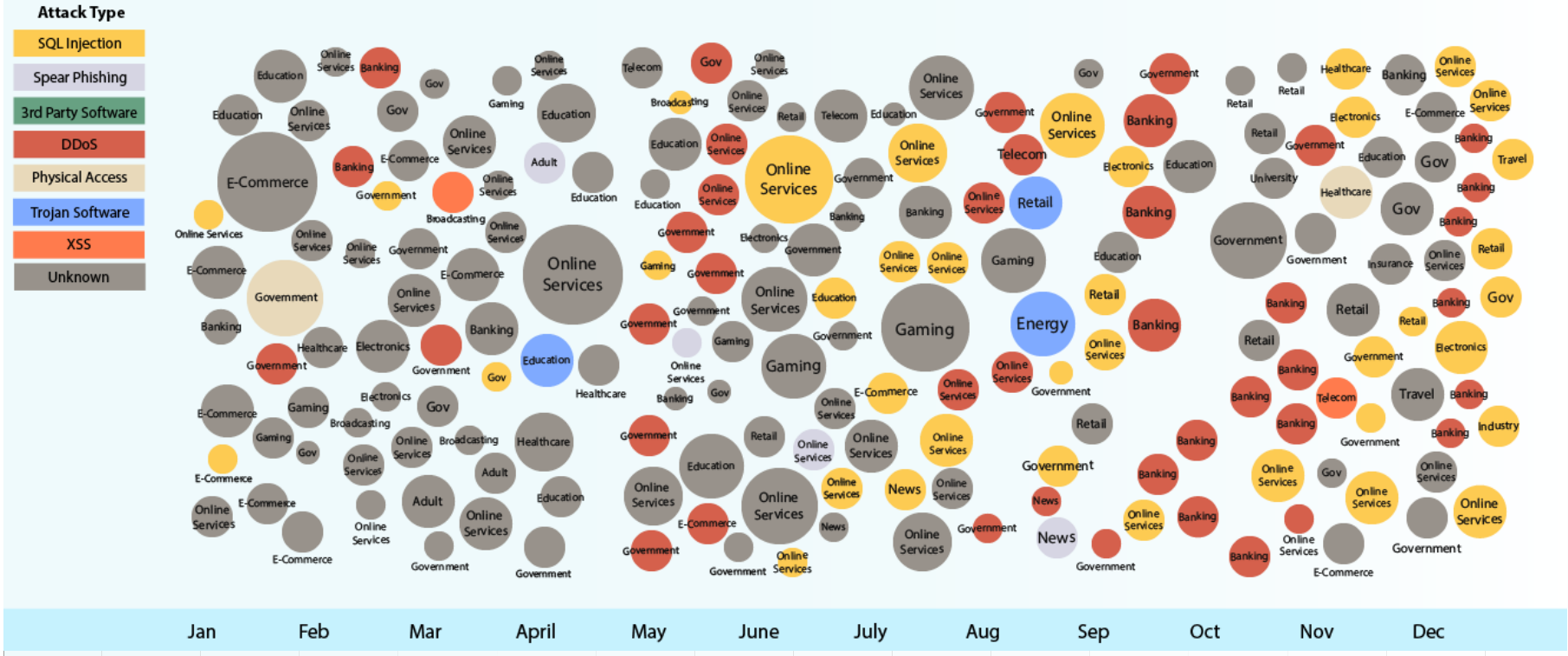


Source: IBM X-Force® Research 2011 Trend and Risk Report

2012: The explosion of breaches continues!

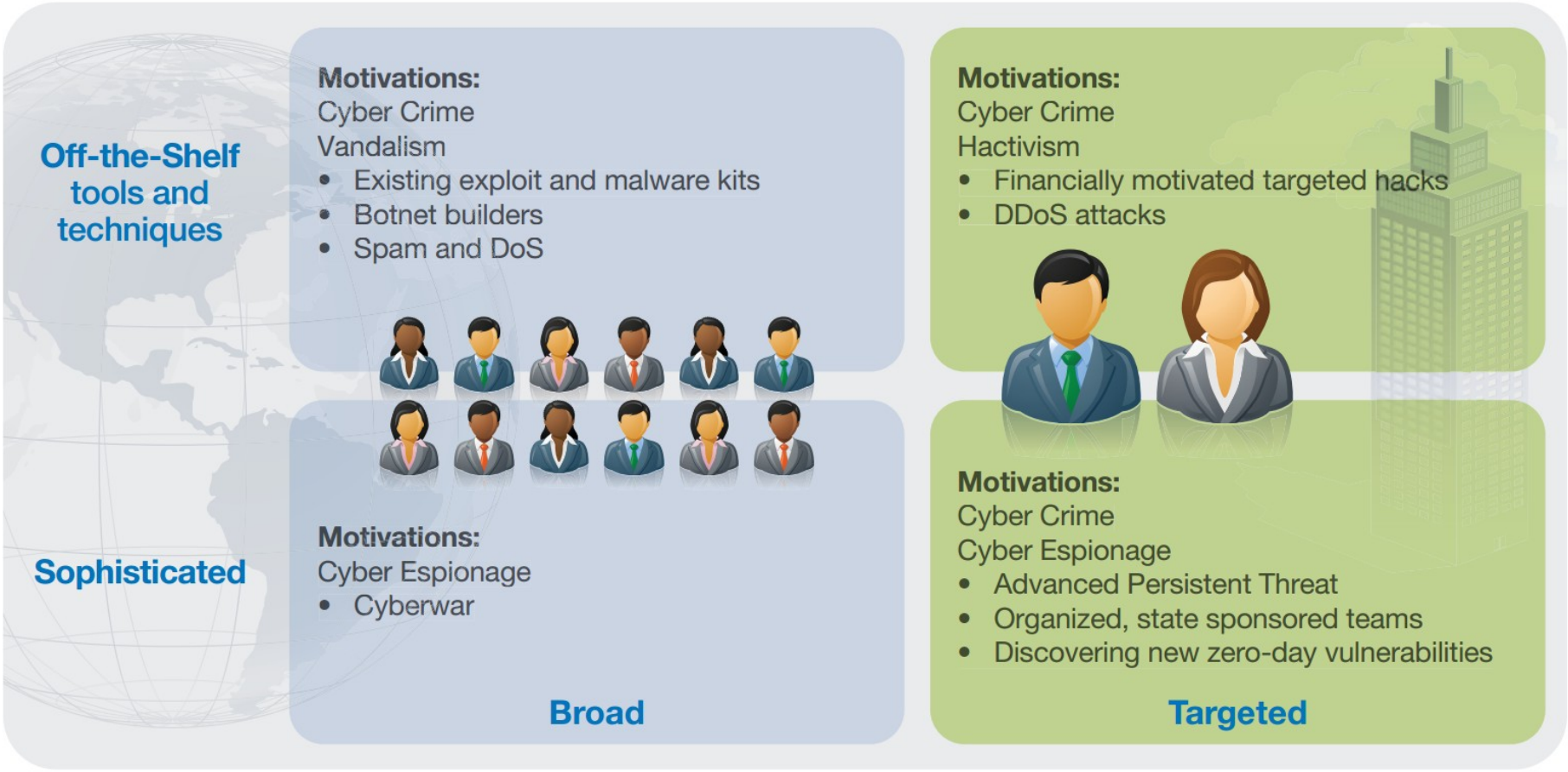
2012 Sampling of Security Incidents by Attack Type, Time and Impact

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



Source: IBM X-Force® Research 2012 Trend and Risk Report

Attacker types and motivations have not changed

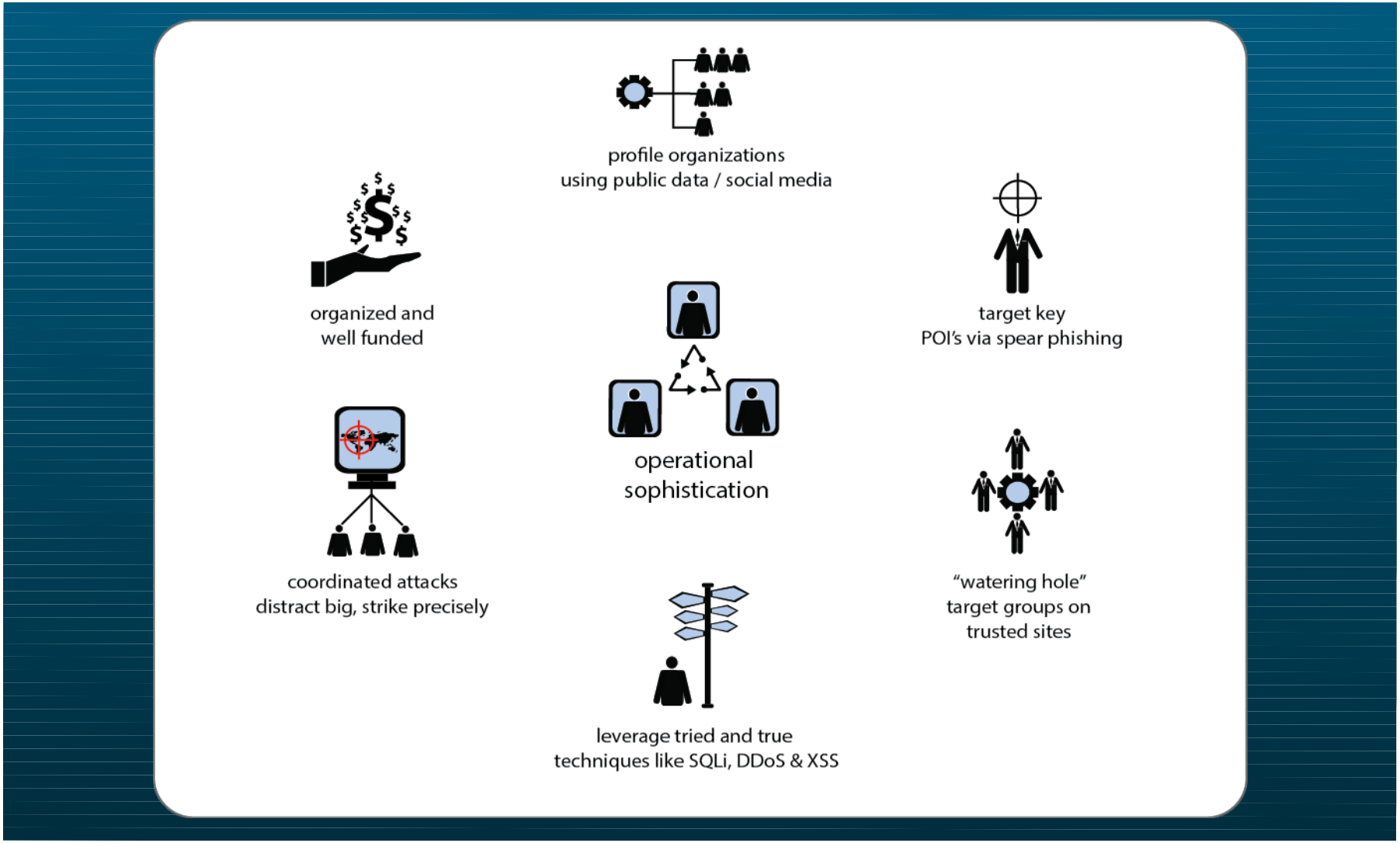


Majority of the security incidents disclosed in 2012 were carried out by attackers going after a broad target base while using off-the-shelf tools and techniques (top left)

SQL injection and DDoS continue to be tried-and-true methods of attack

Attackers are opportunistic, not all APTs and state-sponsored use exotic malware and zero-day vulnerabilities…

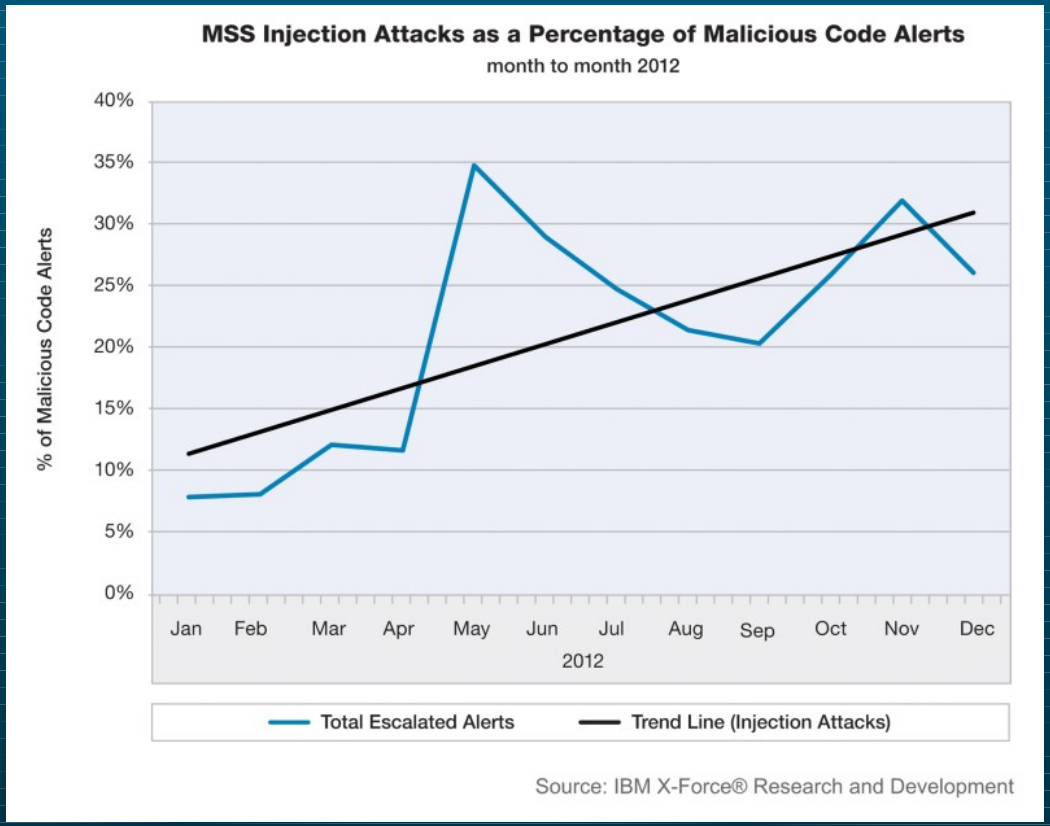
Operational sophistication, not always technology sophistication



Tried and true techniques - SQL and Command Injection attacks

Dramatic and sustained rise in SQL injection-based traffic

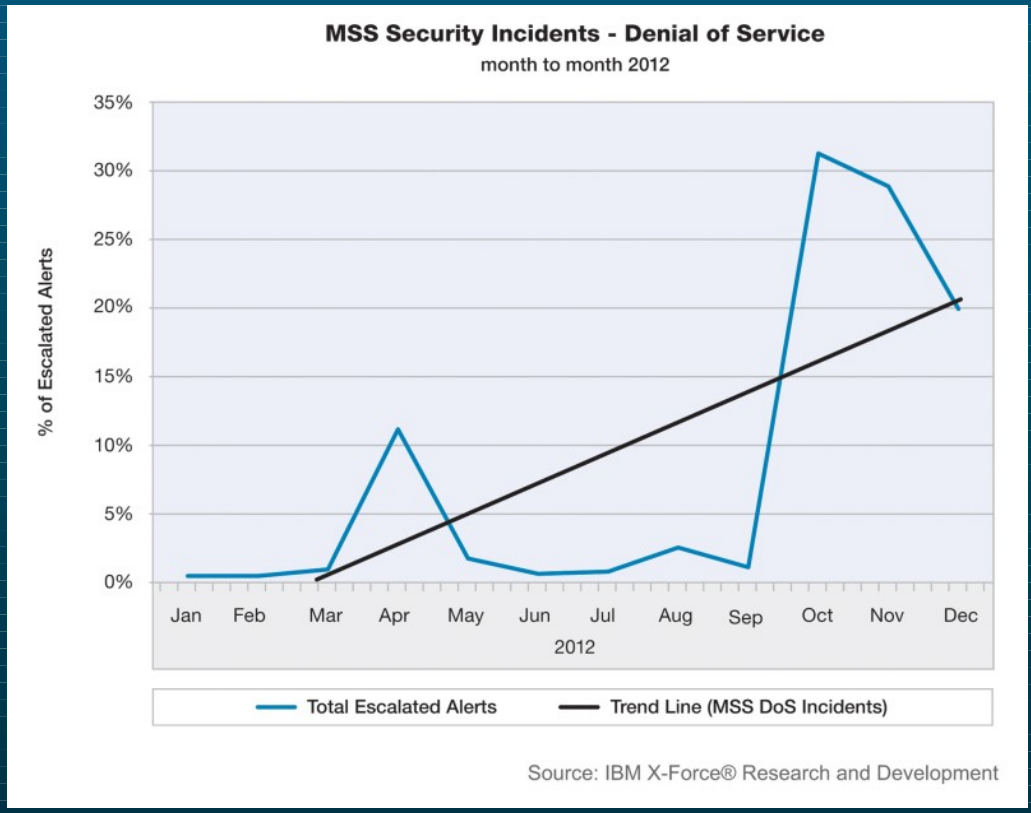
Alerts came from all industry sectors, with a bias toward banking and finance targets



Tried and true techniques - Distributed Denial of Service (DDoS)

High profile DDoS attacks marked by a **significant increase in traffic volume**

Implementation of botnets on **compromised web servers** in high bandwidth data centers



Tried and true techniques - Spear-phishing against social networks

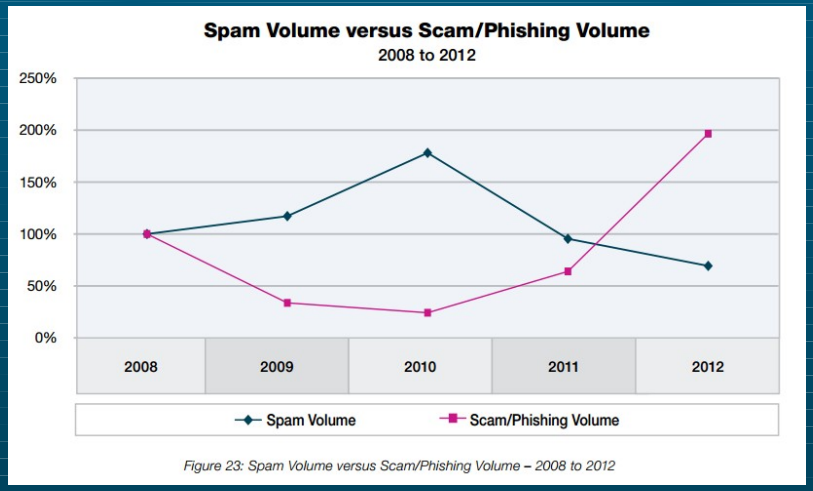


Figure 23: Spam Volume versus Scam/Phishing Volume – 2008 to 2012

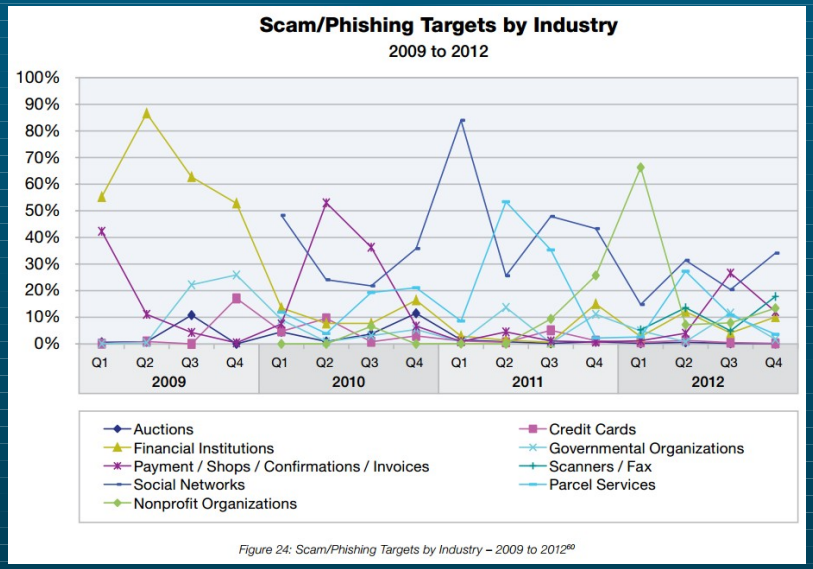


Figure 24: Scam/Phishing Targets by Industry – 2009 to 2012[60]

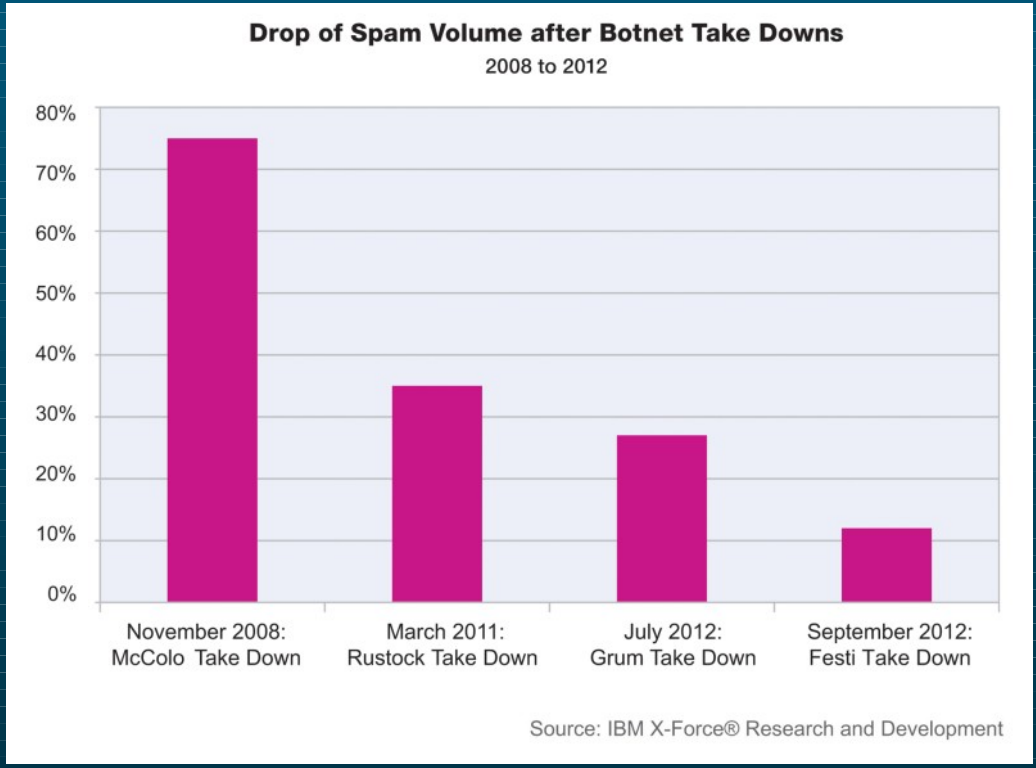
Overall spam volume continues to decline, but **spam containing malicious attachments is on the rise**

Scammers rotate the "carousel" of their targets – **focusing on social networks** in 2012

Botnet Command & Control Server resiliency

Operational sophistication:

When botnet command and control servers are taken down, other readily available networks can be put into action

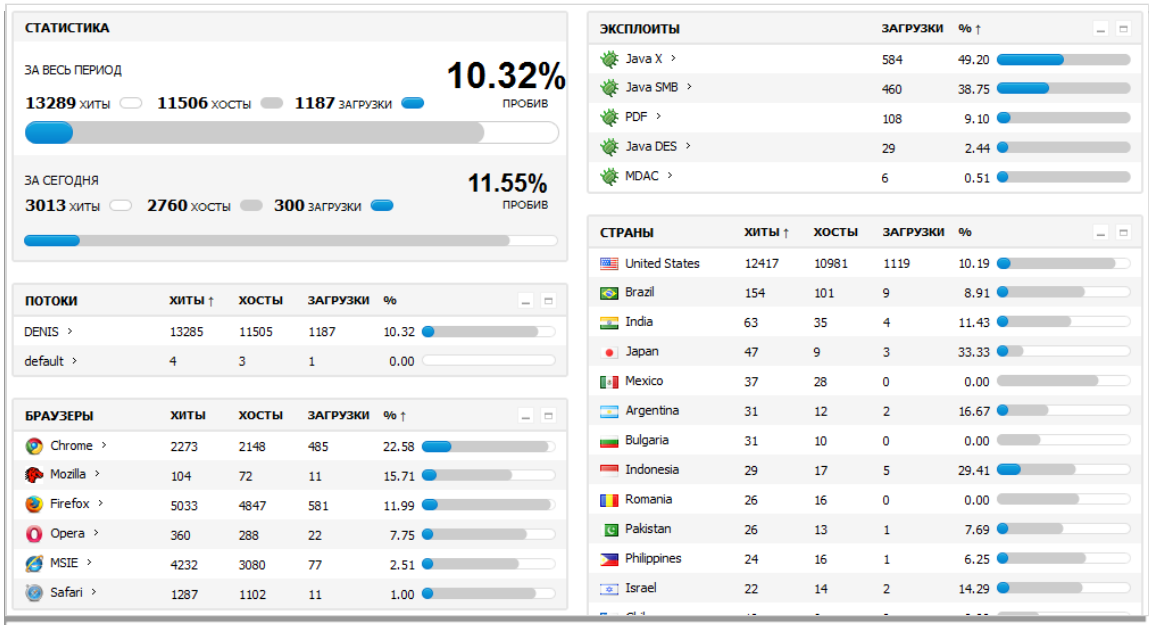


Why was Java one of 2012's hottest software targets?

1. Java is cross-platform
2. Exploits written for Java vulnerabilities are very reliable and do not need to circumvent mitigations in modern OSes
3. The Java plugin runs without a sandbox – making it easier to install persistent malware on the system

http://java-0day.com/

As a result, exploit authors and toolkits favor Java

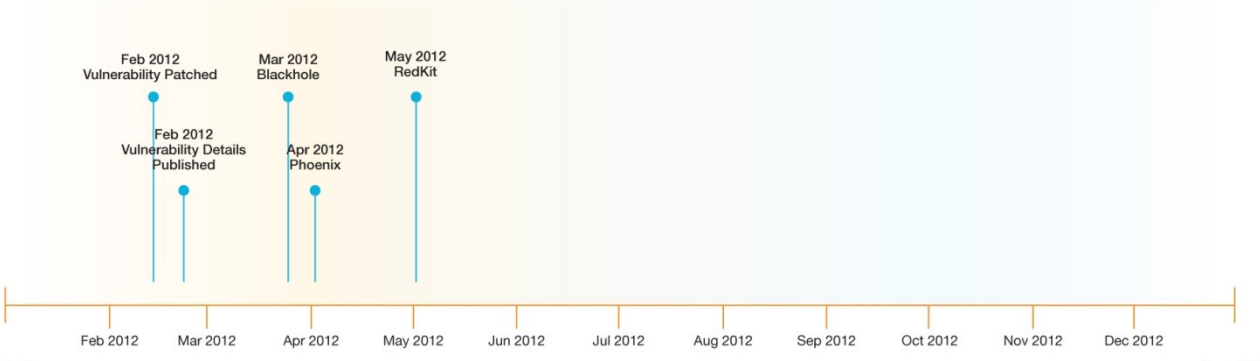


Web browser exploit kits - aka “exploit packs” - are built for one particular purpose: to install malware on end-user systems

In 2012 we observed an upsurge in web browser exploit kit development and activity -the primary target of which are Java vulnerabilities

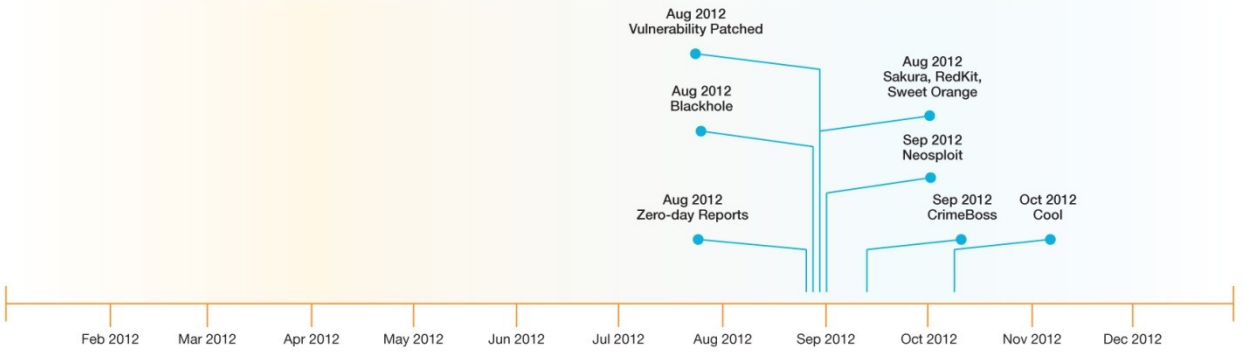
Within 2-3 months, 3-4 exploit kits will have a Java exploit integrated

CVE-2012-0507



CVE-2012-1723

CVE-2012-4681

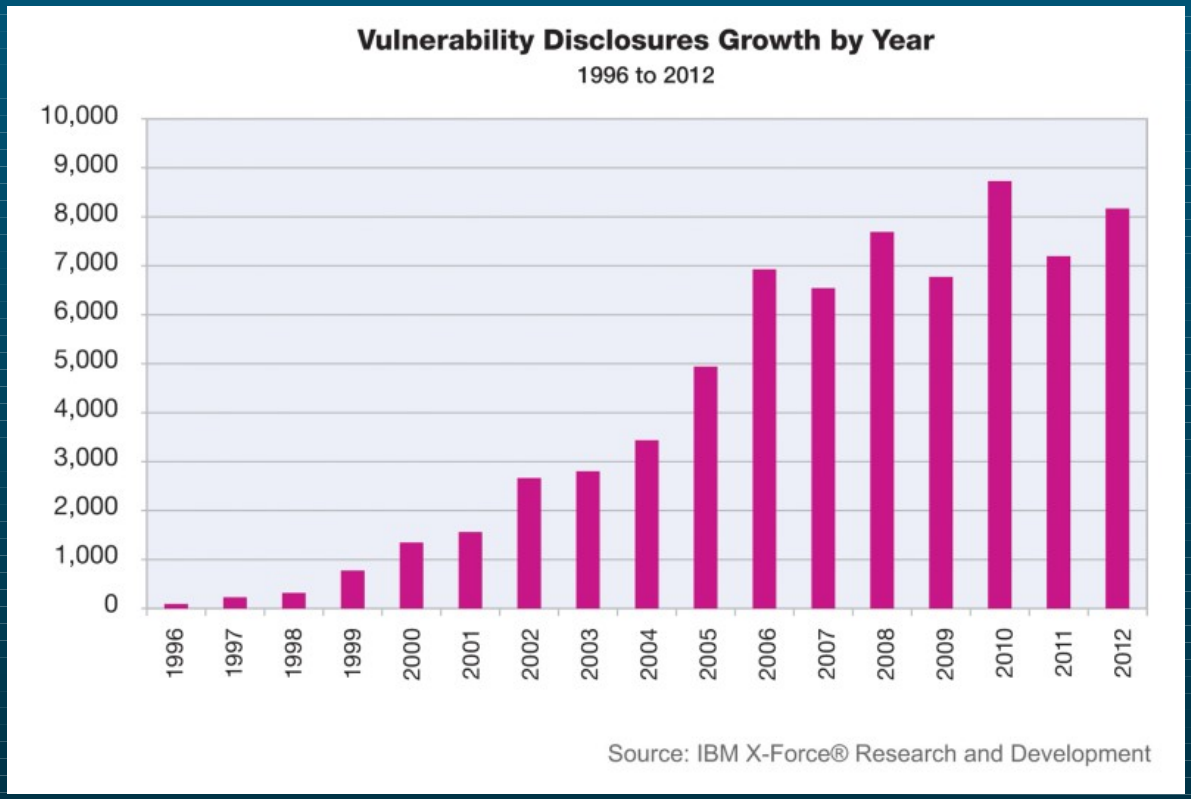


Software vulnerabilities - disclosures up in 2012

8,168

publicly disclosed vulnerabilities

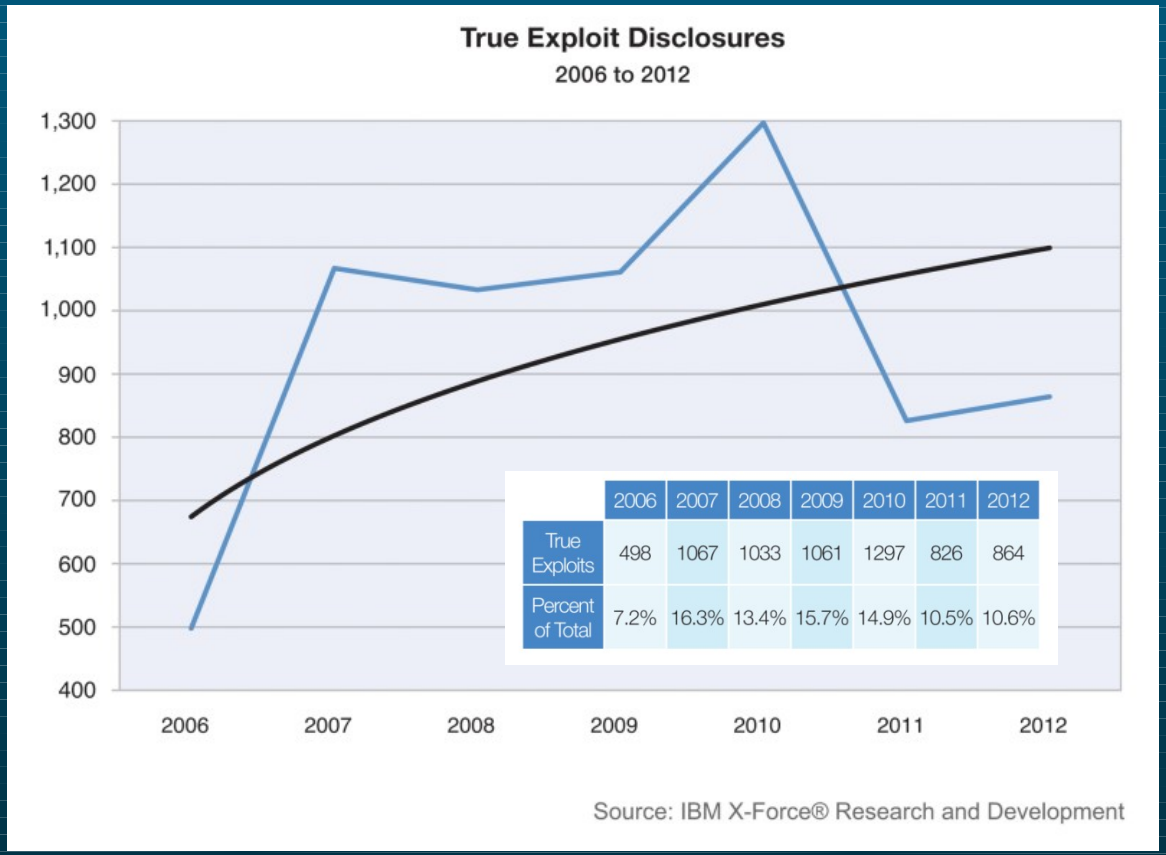
An increase of over 14% from 2011



Public exploit disclosures – not as many "true exploits"

Continued downward trend in percentage of public exploit disclosures to vulnerabilities

Slightly up in actual numbers compared to 2011



	2006	2007	2008	2009	2010	2011	2012
True Exploits	498	1067	1033	1061	1297	826	864
Percent of Total	7.2%	16.3%	13.4%	15.7%	14.9%	10.5%	10.6%

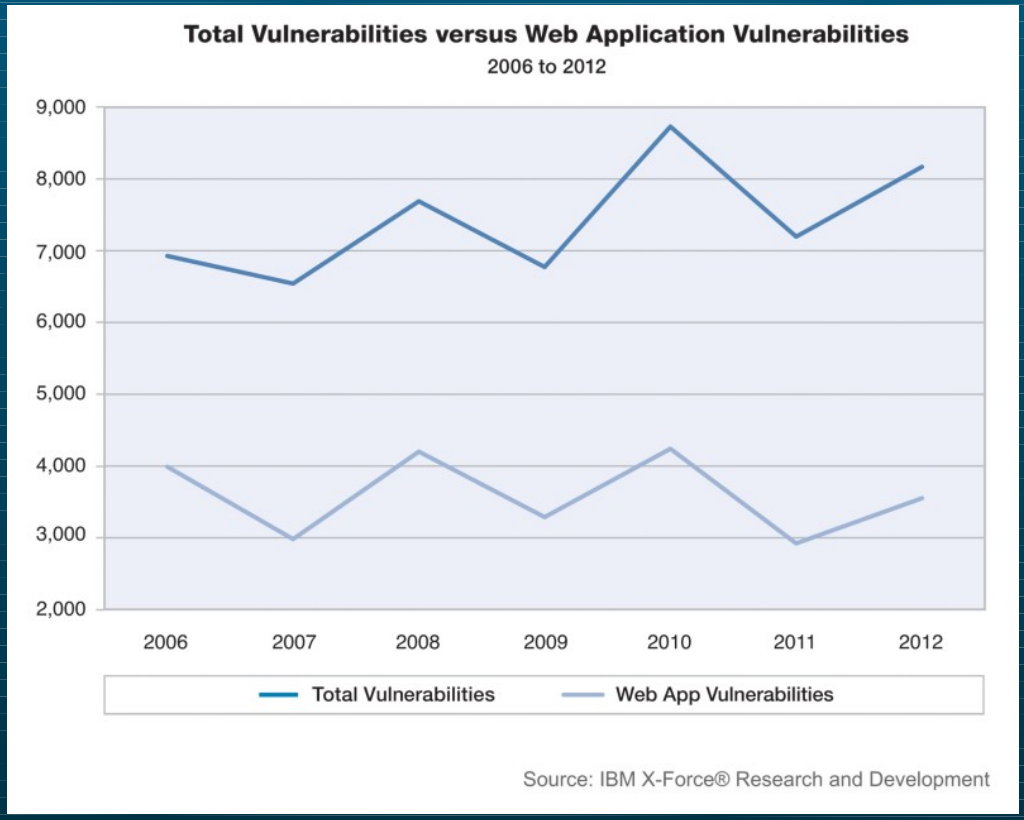
Web application vulnerabilities surge upward

14%

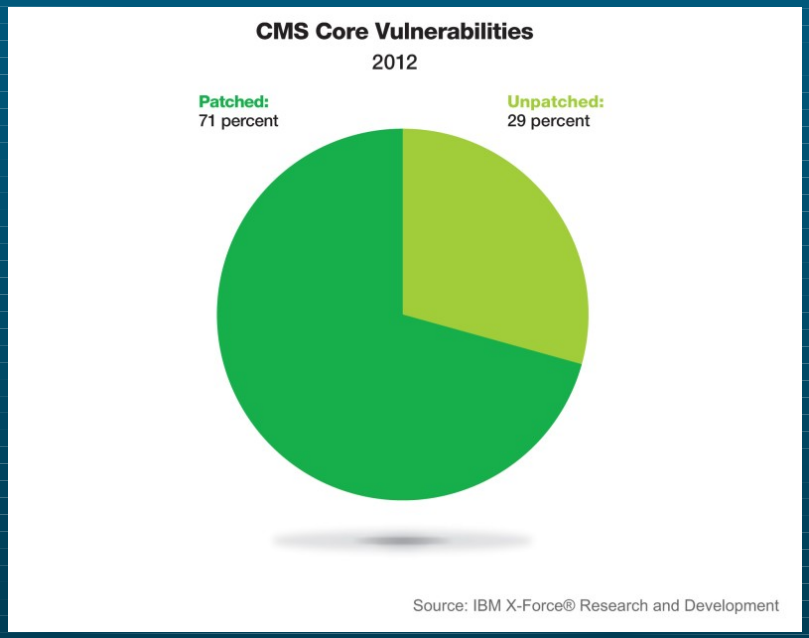
increase in web application vulnerabilities

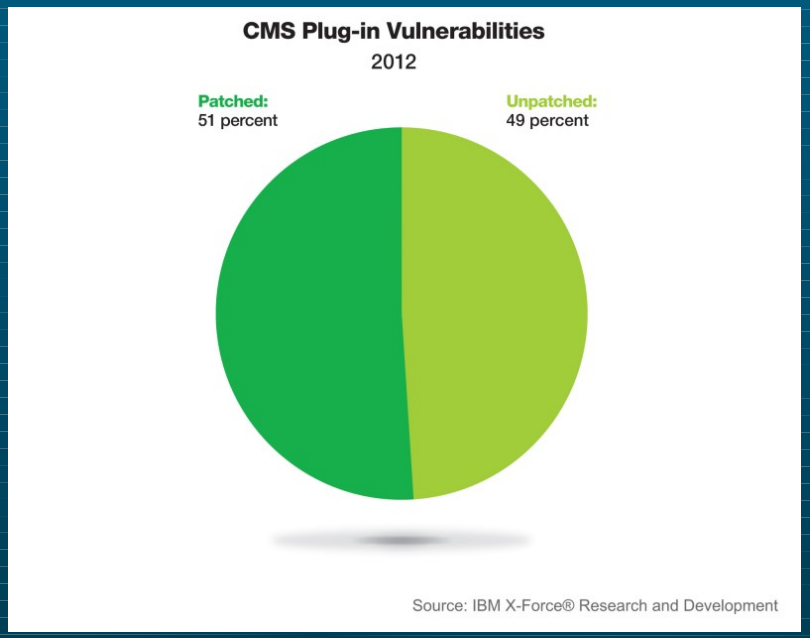
Cross-site scripting represented

53%



Content Management Systems plug-ins provide soft target





Attackers know that CMS vendors more readily address and patch their exposures

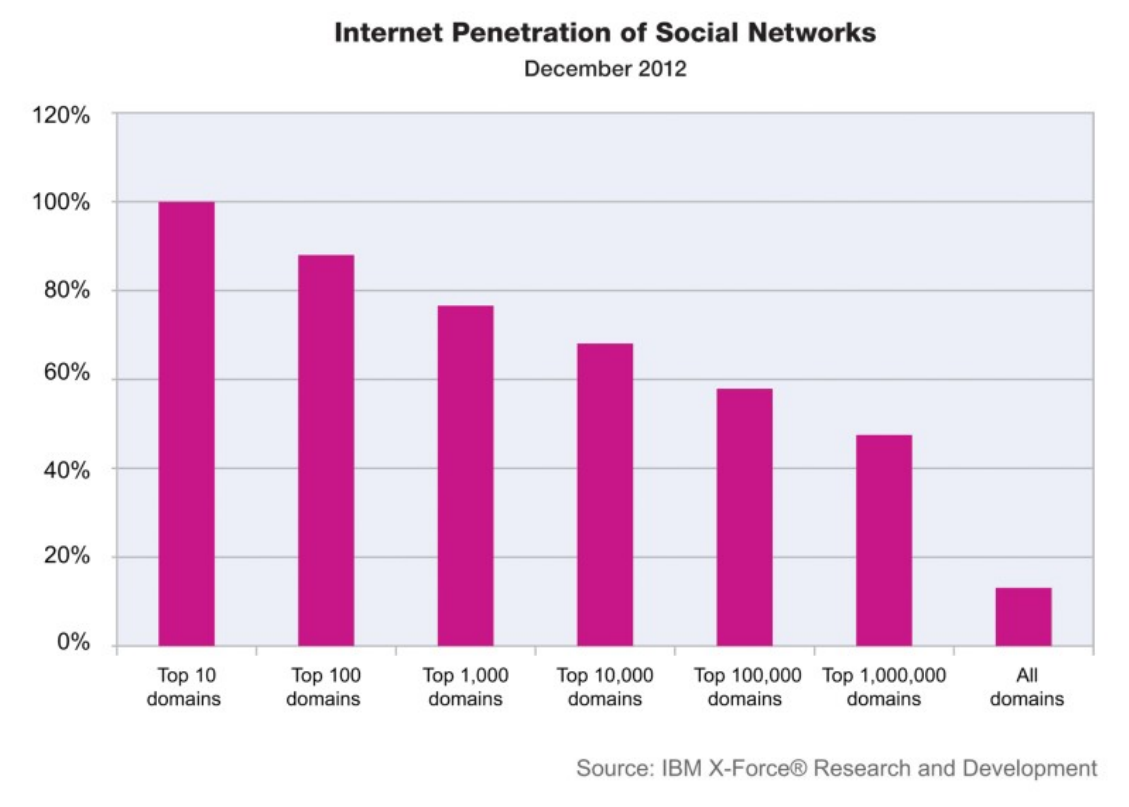
Compared to smaller organizations and individuals producing the add-ons and plug-ins

Social Media and Intelligence Gathering

50%

of all websites connected to social media

Enhanced spear-phishing seemingly originating from trusted friends and co-workers



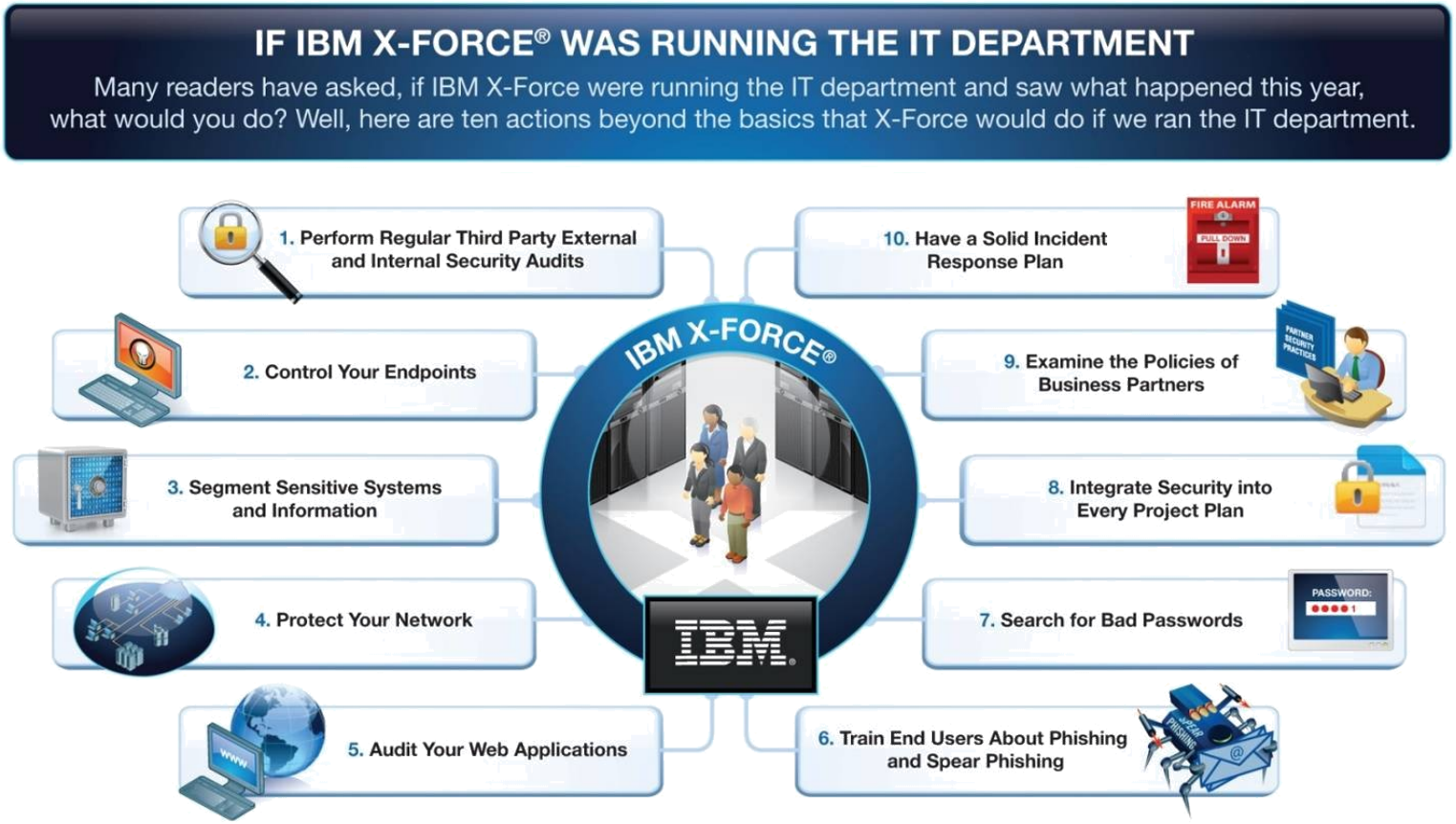
Mobile devices should be more secure in 2014

Mobile computing is becoming increasingly secure, based on technical controls occurring with security professionals and software development

- Separation of Personas & Roles
- Ability to Remotely Wipe Data
- Biocontextual Authentication
- Secure Mobile App Development
- Mobile Enterprise App Platform (MEAP)

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?



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