BusinessConnect
A New Era of Smart

X-Force State of the Threat

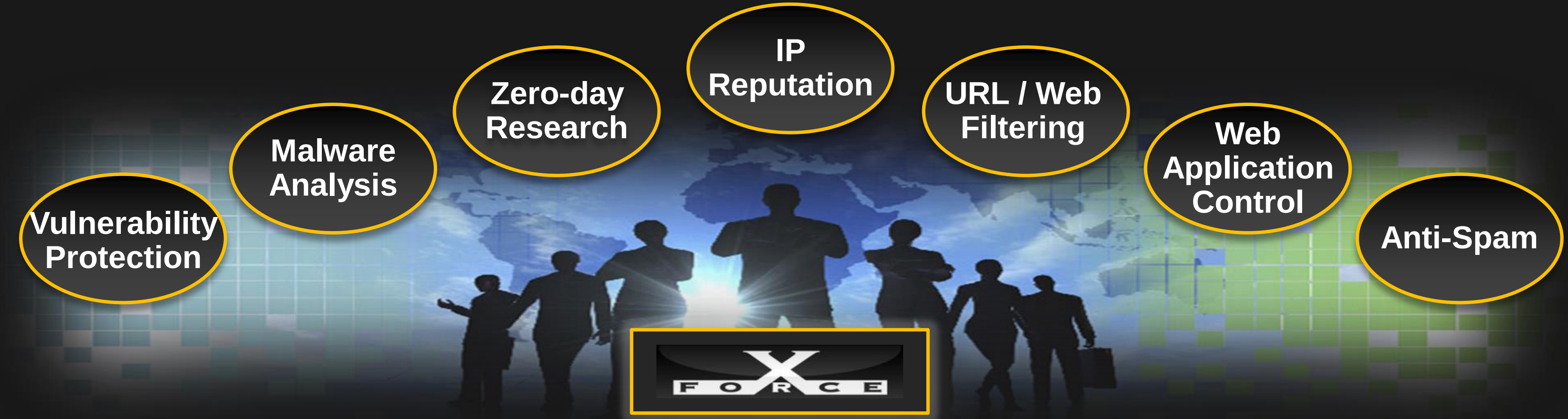
Michael Hamelin, Lead X-Force Security Architect

06/17/2014

© 2013 IBM Corporation

IBM X-Force® Research and Development

Expert analysis and data sharing on the global threat landscape



The IBM X-Force Mission

- **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
- **Integrate** and distribute Threat Protection and Intelligence to make IBM solutions smarter

© 2014 IBM Corporation

Collaboration with other IBM Security research groups

Global Technology Services (GTS)

- MSS Security Operations Centers (SOC)
- XF Threat Analysis Service (XFTAS)
- Cyber Index Report
- Emergency Response Services (ERS)

Improve security
IBM maintains the world's largest threat & vulnerability database

Reduce cost
Save up to 55% on information security management

Lower r
Reliable pr
guaranteed
level agree

Trusteer R&D

- Banking and Finance attacks
- APT and Advanced Malware
- 0day application exploits
- Spear-phishing attacks
- Data exfiltration

Trusteer
an IBM Company

X FORCE

AppScan R&D

- Joint research with Android exploitation
- App Vulns & Database collaborations

Evaluate IBM Security Appscan

→ Download trial

QRadar and other IBM products

- SIEM collaboration, integrated traffic analysis
- Identity & Access – Security Web Gateway Appliance (with PAM)
- IBM PSIRT – vulnerability discovery and coordination

© 2014 IBM Corporation

High profile breaches continue to make headlines

Bloomberg

Saudi Arabia Says Aramco Cyberattack Came From Foreign States

– Bloomberg, Dec 2012

InformationWeek

Lockheed Martin Suffers Massive Cyberattack

– InformationWeek, May 2011

theguardian

Facebook hacked in 'sophisticated attack'

– The Guardian, Feb 2013

The New York Times

RSA Faces Angry Users After Breach

– The New York Times, June 2011

THE WALL STREET JOURNAL.

Fed Acknowledges Cybersecurity Breach

– The Wall Street Journal, Feb 2013

THE WALL STREET JOURNAL.

NASDAQ Confirms Breach in Network

– The Wall Street Journal, Feb 2011

THE HUFFINGTON POST

Apple Hacked: Company Admits Development Website Was Breached

– Huffington Post, July 2013

CNN

South Carolina taxpayer server hacked, 3.6 million Social Security numbers compromised

– CNN, Oct 2012

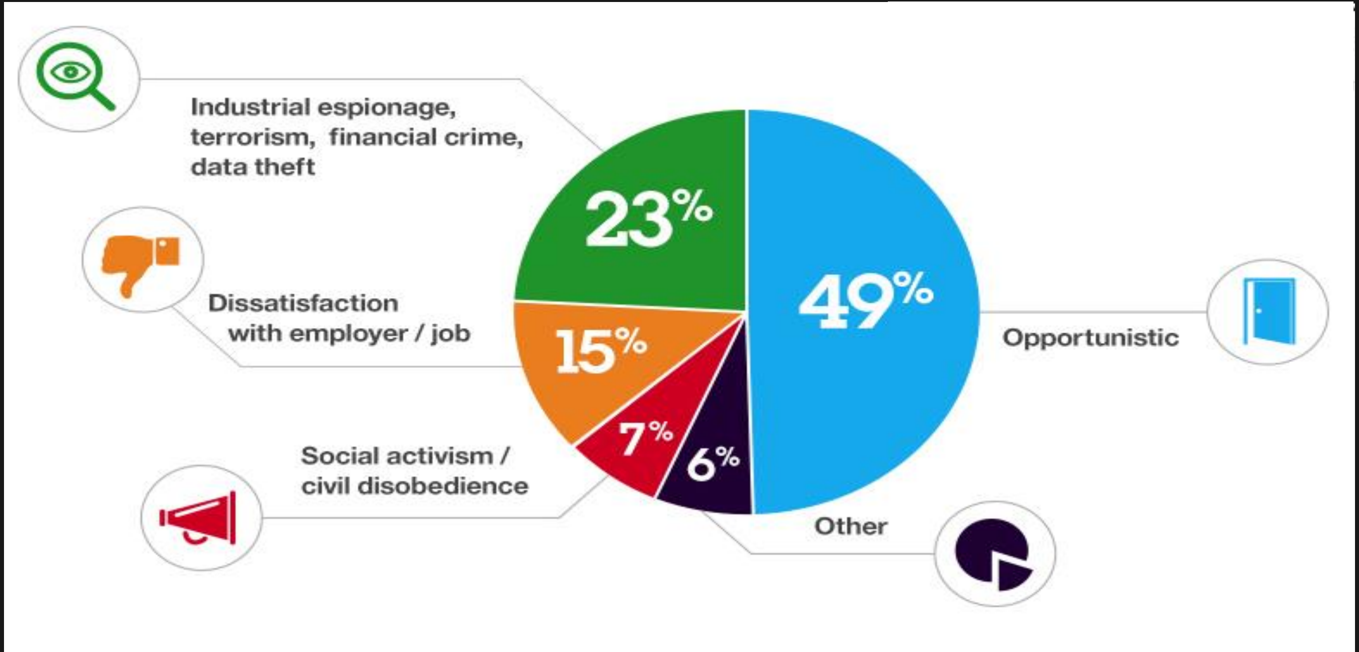
WIRED

Chinese hacking of US media is 'widespread phenomenon '

– Wired, Feb 2013

© 2014 IBM Corporation

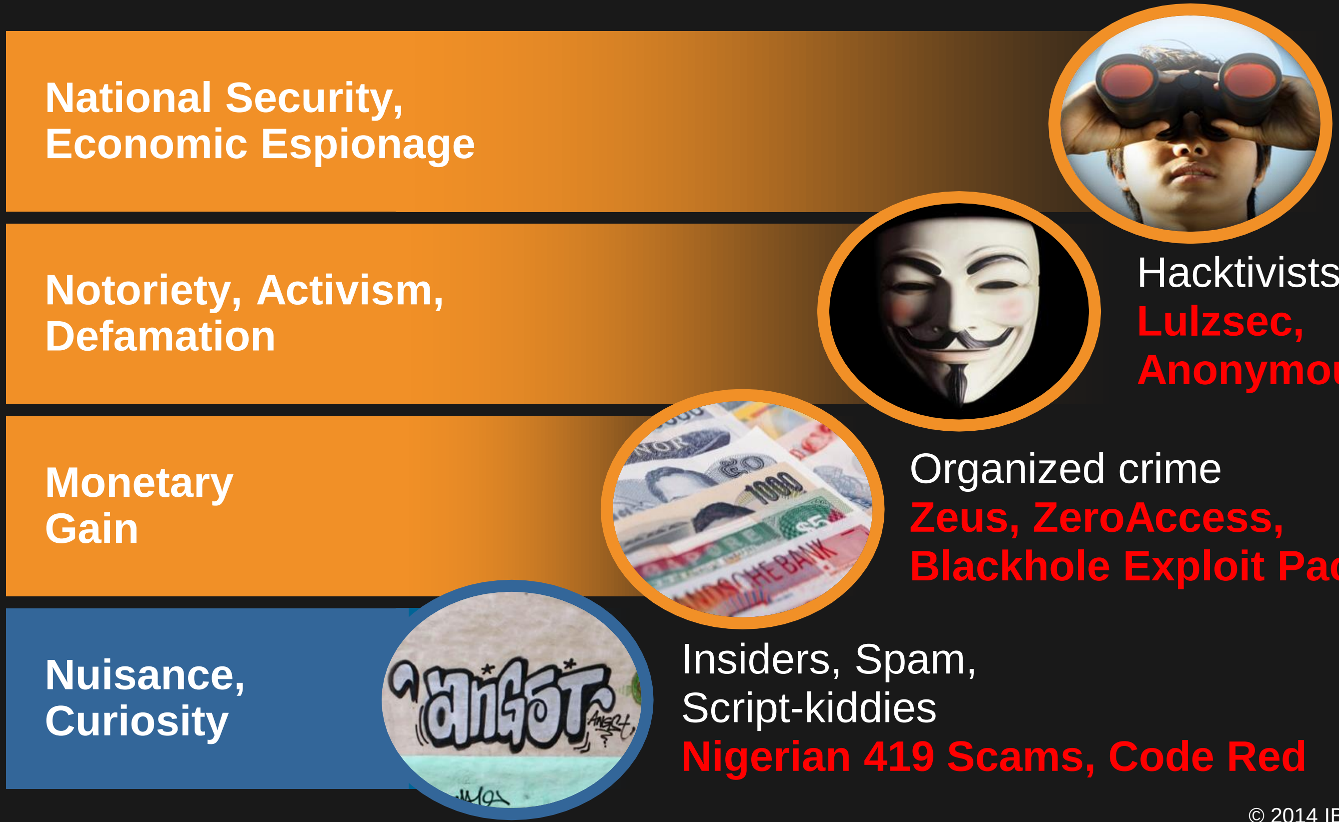
Motivations of the Attacker



Source: *IBM Security Services 2013 Cyber Security Intelligence Index*

© 2014 IBM Corporation

Why is this happening? An increase in sophistication and motives



National Security, Economic Espionage

Nation-state actors, APTs

Stuxnet, Aurora, APT-1

Notoriety, Activism, Defamation

Hacktivists

Lulzsec, Anonymous

Monetary Gain

Organized crime

Zeus, ZeroAccess, Blackhole Exploit Pack

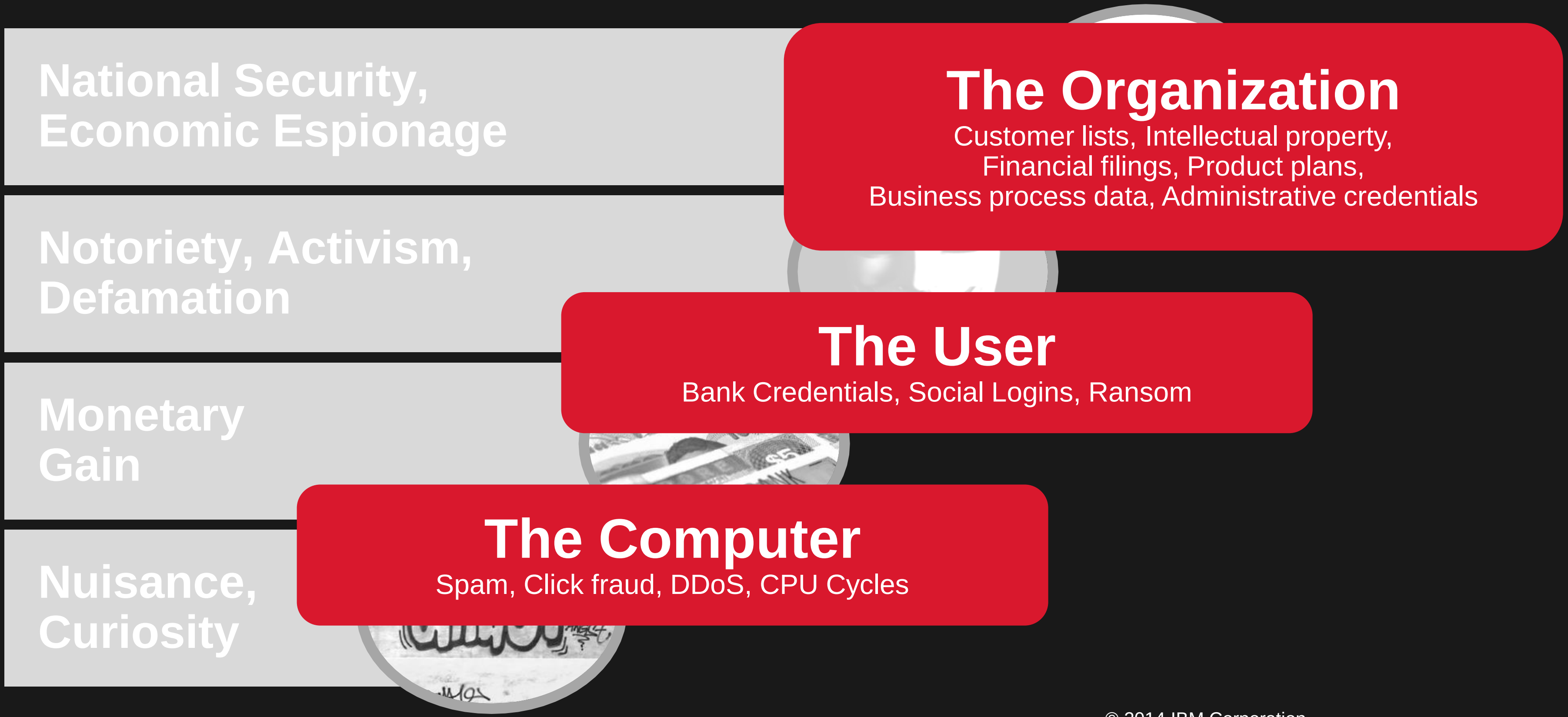
Nuisance, Curiosity

Insiders, Spam, Script-kiddies

Nigerian 419 Scams, Code Red

© 2014 IBM Corporation

The attack targets and vectors have also changed



National Security, Economic Espionage

Notoriety, Activism, Defamation

Monetary Gain

Nuisance, Curiosity

The Organization

Customer lists, Intellectual property, Financial filings, Product plans, Business process data, Administrative credentials

The User

Bank Credentials, Social Logins, Ransom

The Computer

Spam, Click fraud, DDoS, CPU Cycles

© 2014 IBM Corporation

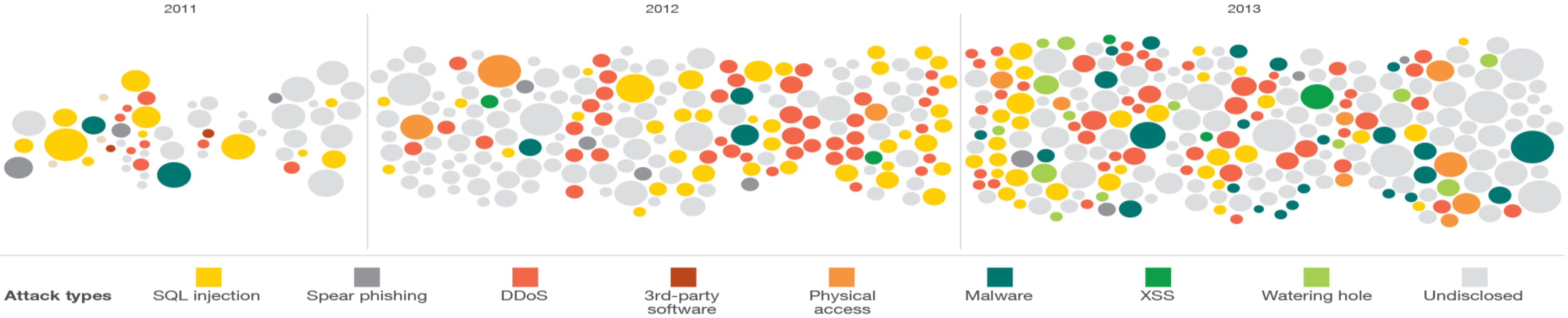
more than

half a billion records

of personally identifiable information (PII) were leaked in 2013

A historical look at security incidents by attack type, time and impact, 2011 to 2013

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



Size of circle estimates relative impact of incident in terms of cost to business.

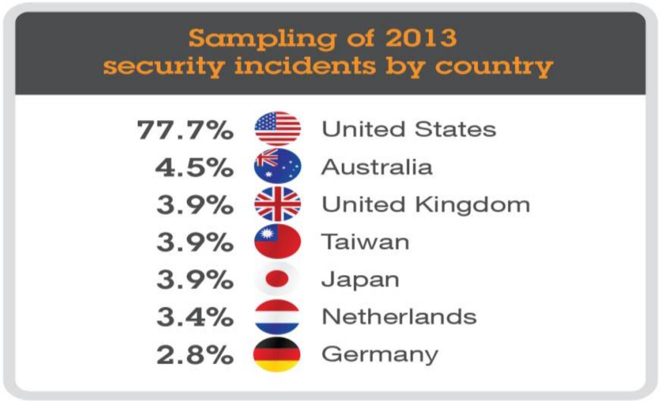
Figure 1. A historical look at security incidents by attack type, time and impact, 2011 to 2013

Source: IBM X-Force® Research and Development

What is the impact of a data breach

and

Where are customer’s most affected?

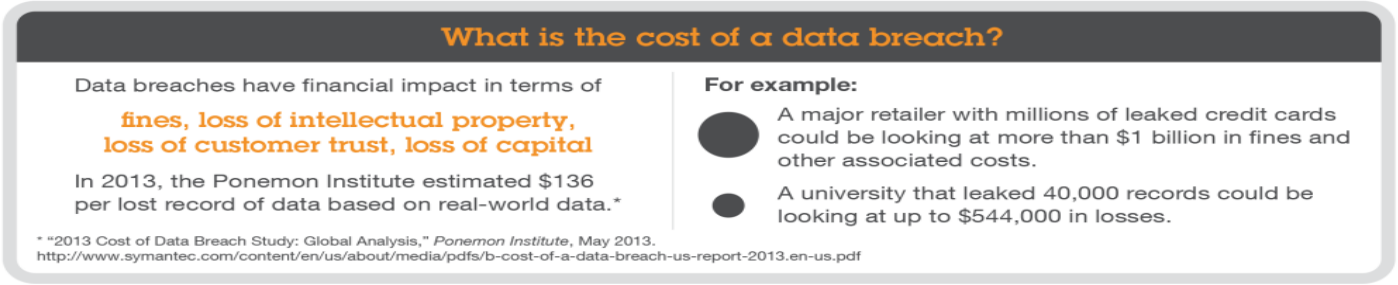


Sampling of 2013 security incidents by country

77.7%	United States
4.5%	Australia
3.9%	United Kingdom
3.9%	Taiwan
3.9%	Japan
3.4%	Netherlands
2.8%	Germany

Figure 3. Sampling of 2013 security incidents by country

Source: IBM X-Force® Research and Development



What is the cost of a data breach?

Data breaches have financial impact in terms of

fines, loss of intellectual property, loss of customer trust, loss of capital

In 2013, the Ponemon Institute estimated $136 per lost record of data based on real-world data.*

For example:

● A major retailer with millions of leaked credit cards could be looking at more than $1 billion in fines and other associated costs.

● A university that leaked 40,000 records could be looking at up to $544,000 in losses.

* “2013 Cost of Data Breach Study: Global Analysis,” *Ponemon Institute*, May 2013. http://www.symantec.com/content/en/us/about/media/pdfs/b-cost-of-a-data-breach-us-report-2013.en-us.pdf

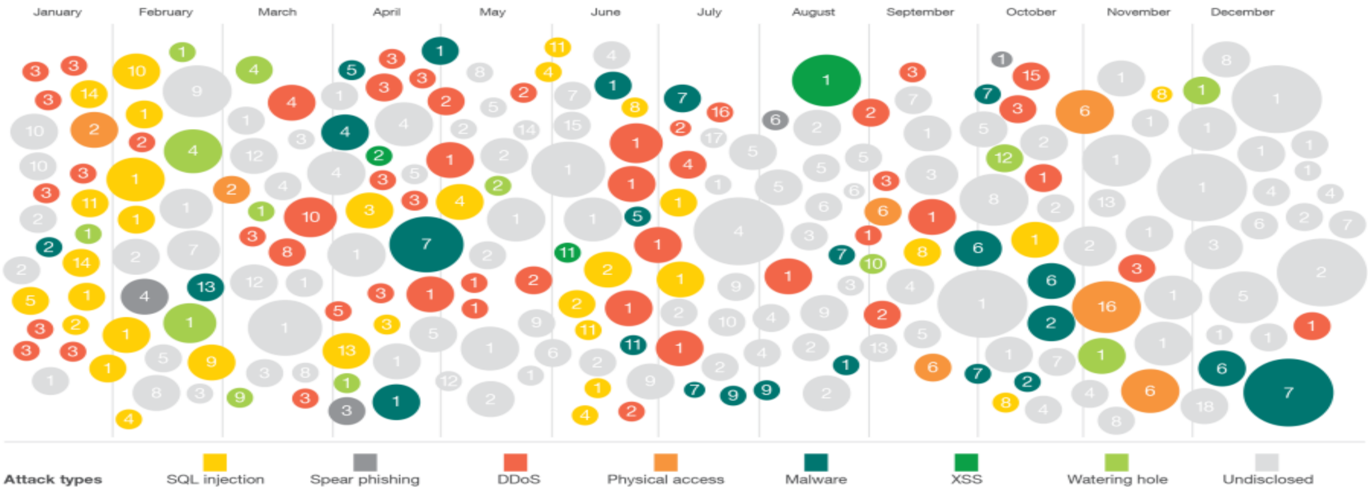
Figure 2b. Sampling of 2013 security incidents by attack type, time and impact

Source: IBM X-Force® Research and Development

© 2014 IBM Corporation

Sampling of 2013 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 incident in terms of cost to business.

Most-commonly attacked industries

28%	Computer Services (1)
15%	Government (2)
12%	Financial Markets (3)
9%	Media & Entertainment (4)
7%	Education (5)
5%	Healthcare (6), Retail (7), Telecommunications (8)
3%	Consumer Products (9)
2%	Non-Profit (10), Automotive (11), Energy & Utilities (12), Professional Services (13)
1%	Industrial Products (14), Travel & Transportation (15), Wholesale Distribution & Services (16)
<1%	Aerospace & Defense (17), Insurance (18)

Most-common attack types

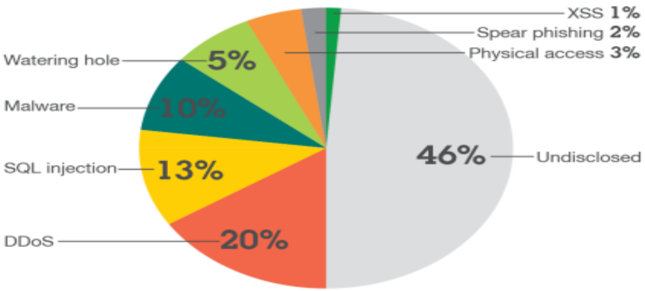
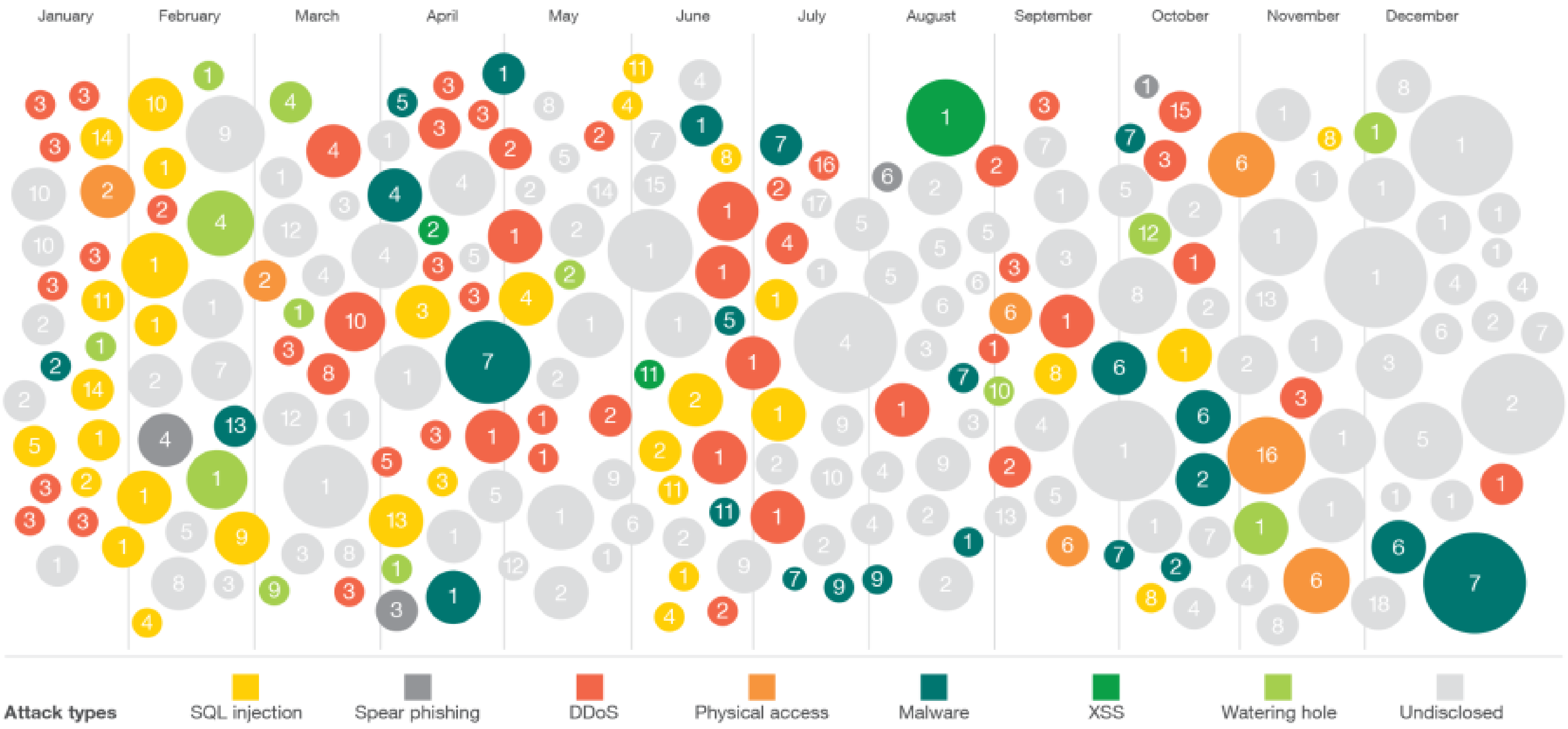


Figure 2a. Sampling of 2013 security incidents by attack type, time and impact

Source: IBM X-Force® Research and Development

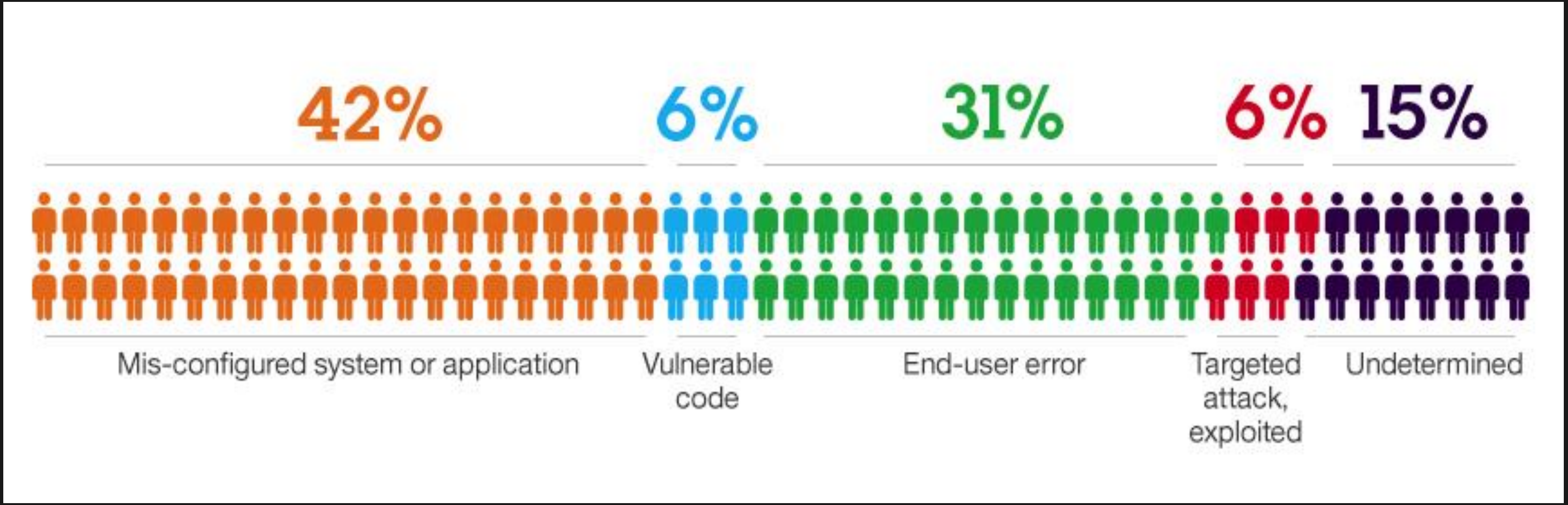
Sampling of 2013 security incidents by attack type, time and impact

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



Size of circle estimates relative impact of incident in terms of cost to business.

Why do Breaches Happen



Source: *IBM Security Services 2013 Cyber Security Intelligence Index*

© 2014 IBM Corporation

Significant increase of Java vulnerabilities

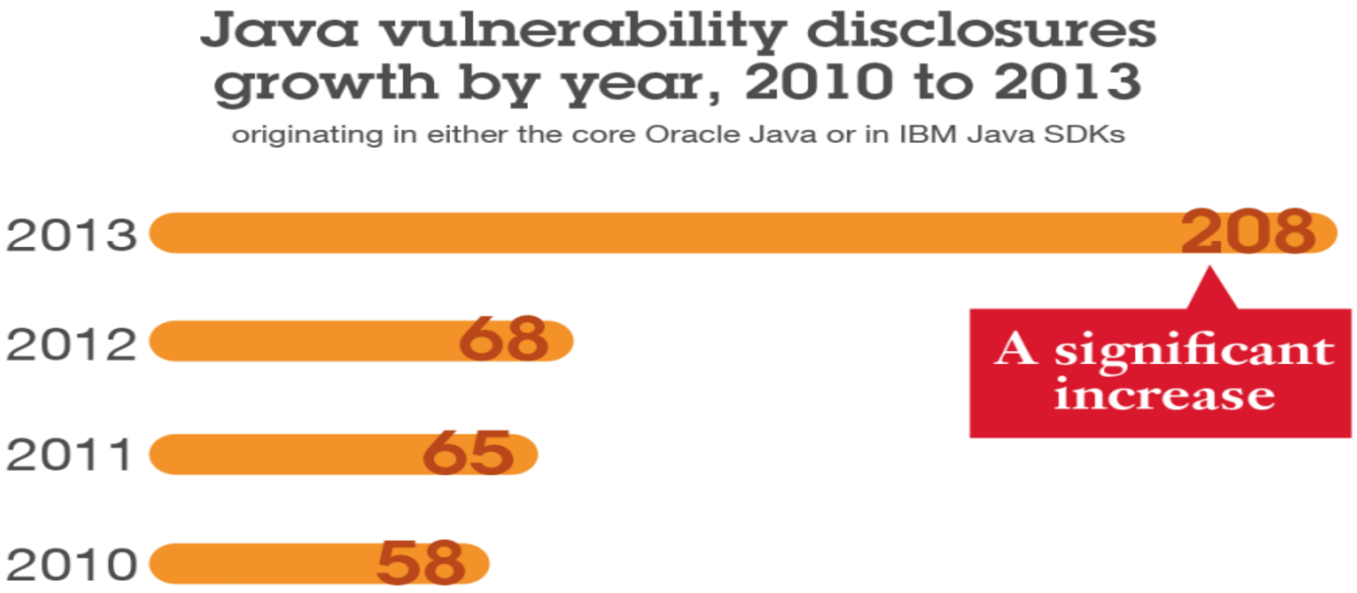


Figure 5. Java vulnerability disclosures growth by year, 2010 to 2013

Source: IBM X-Force® Research and Development

Weaponized content focused on end user apps

Exploitation of application vulnerabilities

from survey of 1 million Trusteer customers, December 2013

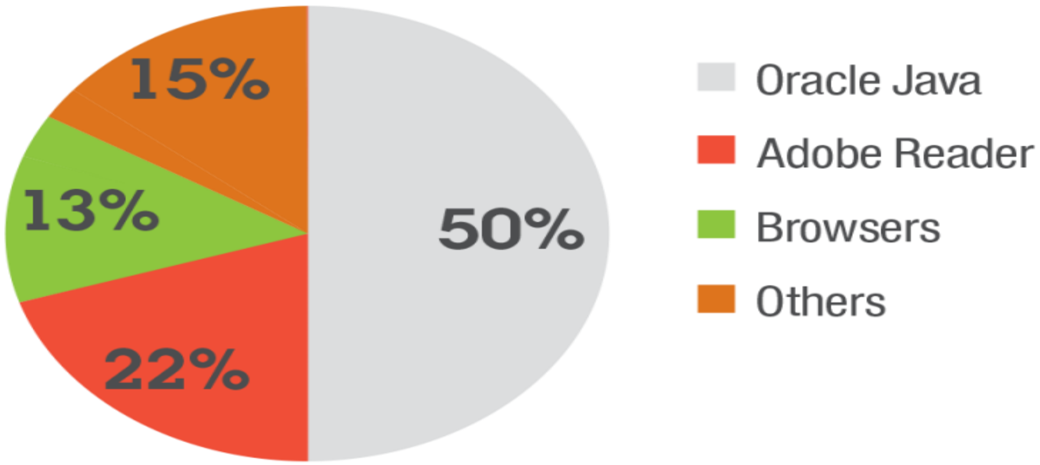


Figure 4. Exploitation of application vulnerabilities

Source: IBM X-Force® Research and Development

© 2014 IBM Corporation

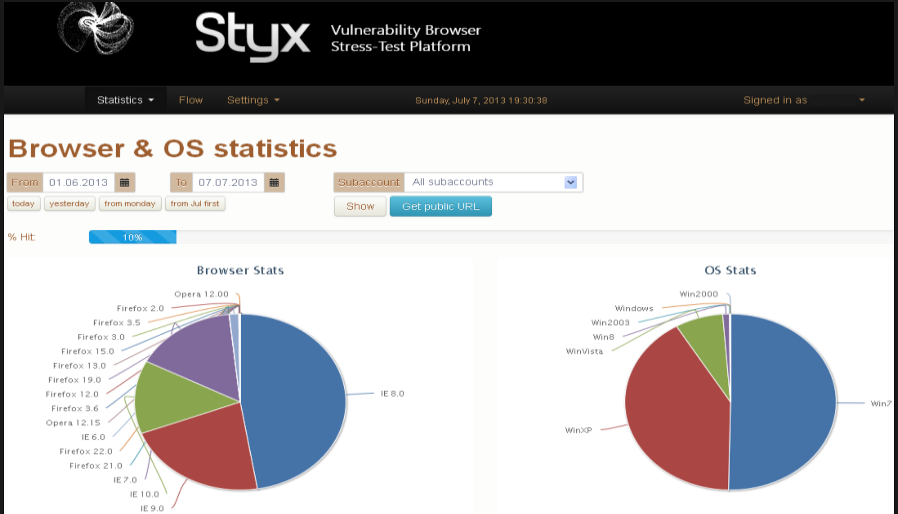
Attackers use exploit kits to deliver payloads

Blackhole Exploit Kit

- Most popular in 2013
- Creator arrested in October

Styx Exploit Kit

- Rising in popularity
- Successful in exploiting IE and Firefox on Windows


Styx Vulnerability Browser Stress-Test Platform

Sunday, July 7, 2013 19:30:38

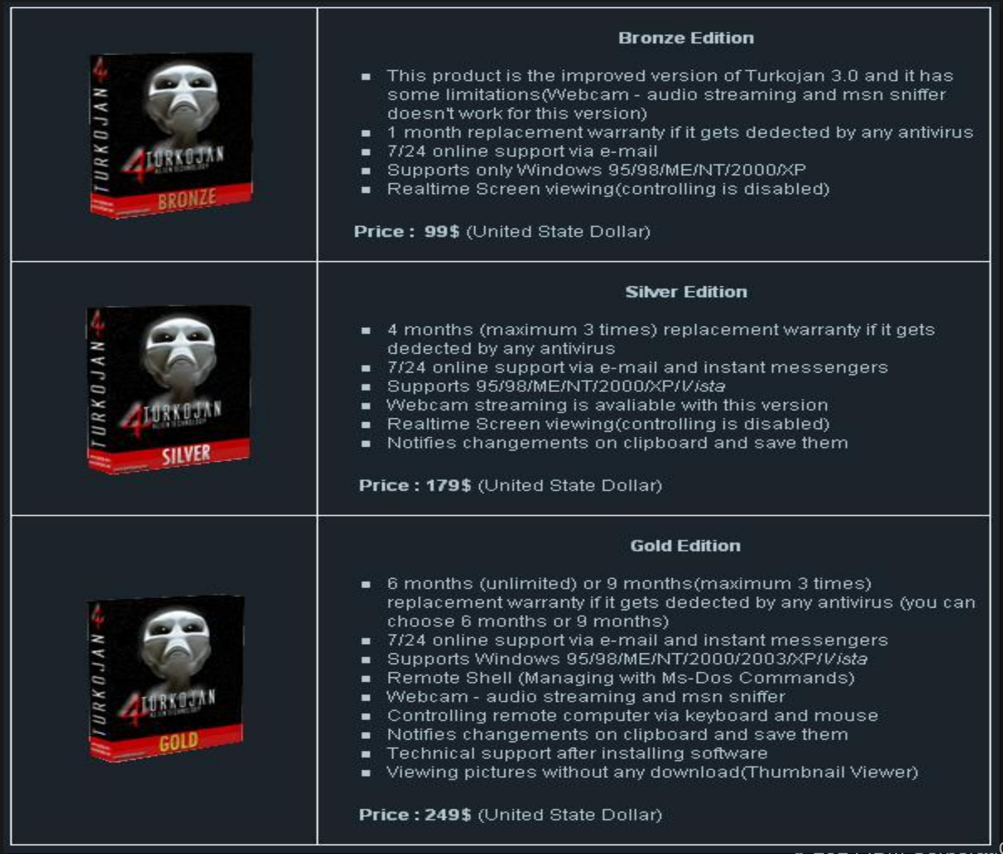
Browser & OS statistics

From 01.06.2013 To 07.07.2013 Subaccount All subaccounts

% Hit: 10%

© 2014 IBM Corporation

It’s just another business model



Bronze Edition

- This product is the improved version of Turkojan 3.0 and it has some limitations(Webcam - audio streaming and msn sniffer doesn't work for this version)
- 1 month replacement warranty if it gets dedected by any antivirus
- 7/24 online support via e-mail
- Supports only Windows 95/98/ME/NT/2000/XP
- Realtime Screen viewing(controlling is disabled)

Price : 99$ (United State Dollar)

Silver Edition

- 4 months (maximum 3 times) replacement warranty if it gets dedected by any antivirus
- 7/24 online support via e-mail and instant messengers
- Supports 95/98/ME/NT/2000/XP/*Vista*
- Webcam streaming is avaliable with this version
- Realtime Screen viewing(controlling is disabled)
- Notifies changements on clipboard and save them

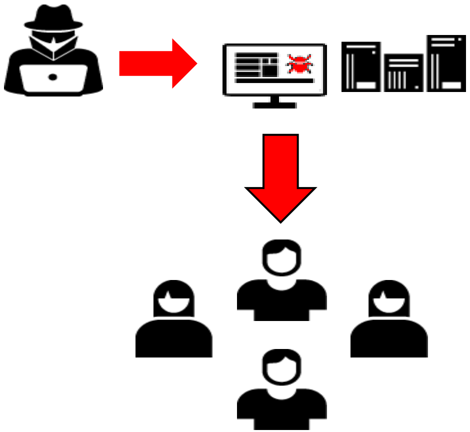
Price : 179$ (United State Dollar)

Gold Edition

- 6 months (unlimited) or 9 months(maximum 3 times) replacement warranty if it gets dedected by any antivirus (you can choose 6 months or 9 months)
- 7/24 online support via e-mail and instant messengers
- Supports Windows 95/98/ME/NT/2000/2003/XP/*Vista*
- Remote Shell (Managing with Ms-Dos Commands)
- Webcam - audio streaming and msn sniffer
- Controlling remote computer via keyboard and mouse
- Notifies changements on clipboard and save them
- Technical support after installing software
- Viewing pictures without any download(Thumbnail Viewer)

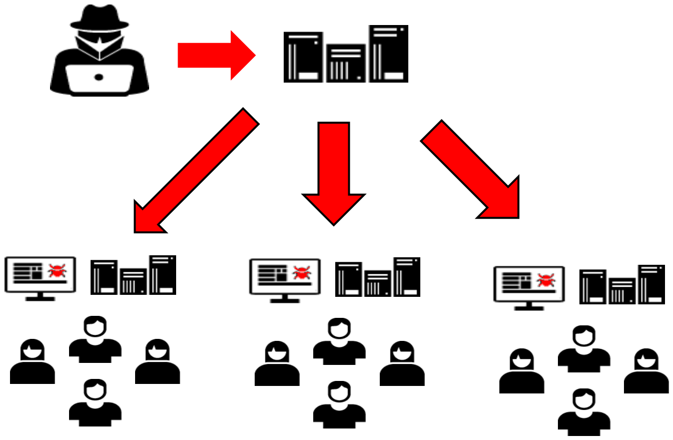
Price : 249$ (United State Dollar)

Effectively targeting end users



Watering Hole

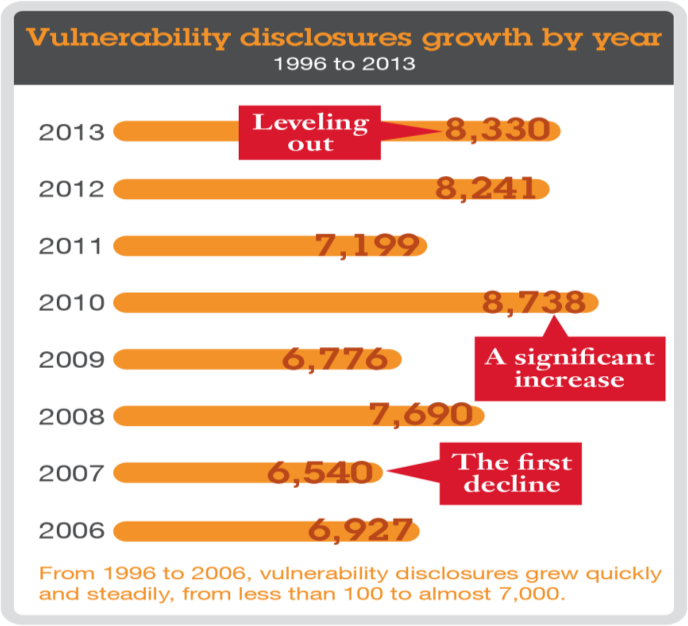
- Attacker injects malware on special interest website
- Vulnerable niche users exploited



Malvertising

- Attacker injects malware on ad network
- Malicious ad embedded on legitimate websites
- Vulnerable users exploited

Web app vulnerabilities: the dominant threat



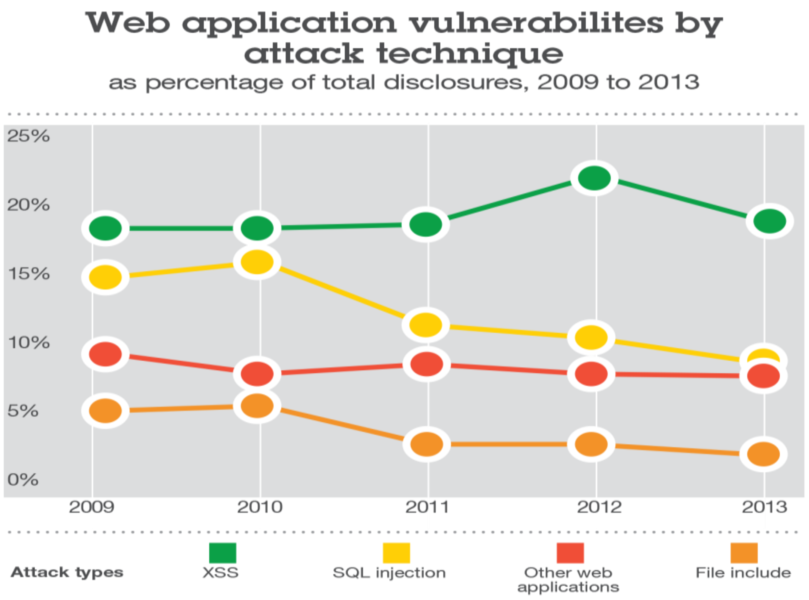
Vulnerability disclosures growth by year

1996 to 2013

From 1996 to 2006, vulnerability disclosures grew quickly and steadily, from less than 100 to almost 7,000.

Figure 8. Vulnerability disclosures growth by year, 1996 to 2013

Source: IBM X-Force® Research and Development



Web application vulnerabilites by attack technique

as percentage of total disclosures, 2009 to 2013

Figure 11. Web application vulnerabilities by attack technique, 2009 to 2013

Source: IBM X-Force® Research and Development

© 2014 IBM Corporation

Declines in key reporting – Web App Vulns

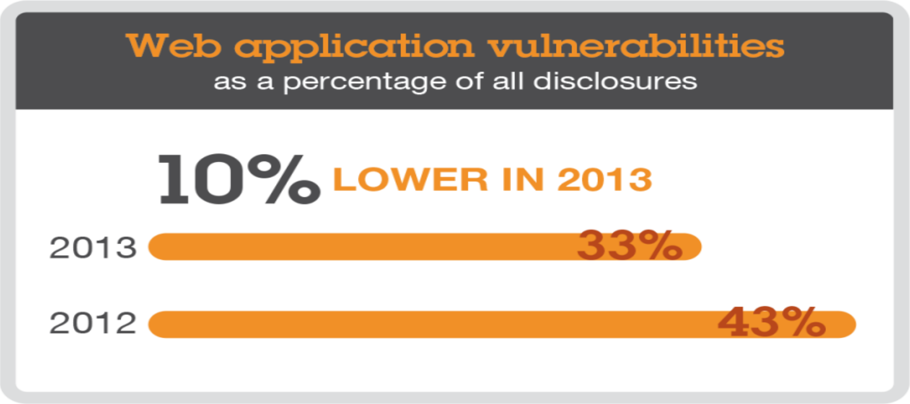


Figure 9. Web application vulnerabilities as a percentage of all disclosures, 2012 to 2013

Source: IBM X-Force® Research and Development

Could indicate…

- Better job at writing secure web applications
- CMS systems & plugins maturing as older vulns are patched

Attacks continue…

- XSS, SQLi exploitation still observed in high numbers

© 2014 IBM Corporation

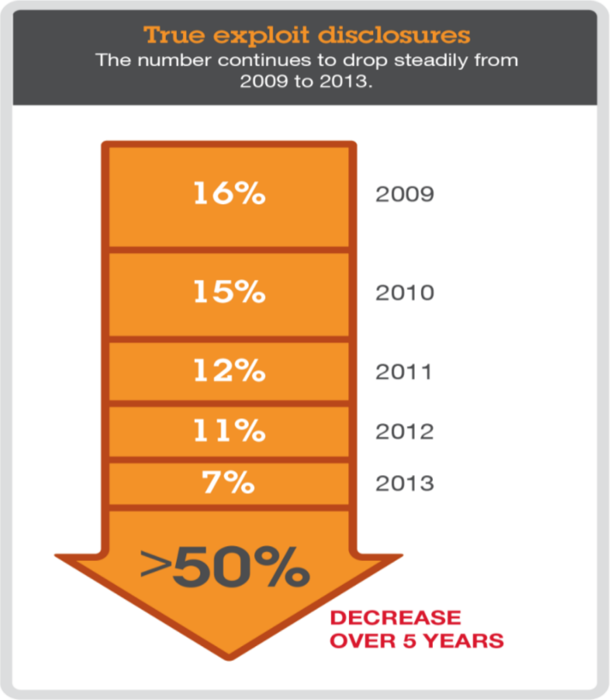
Declines in key reporting – True Exploits

Two Categories tracked

- Proof-of-concept code
- Fully functional programs capable of attacks are *true exploits*

Continue to decrease

- Lowest levels we’ve seen in past 5 years



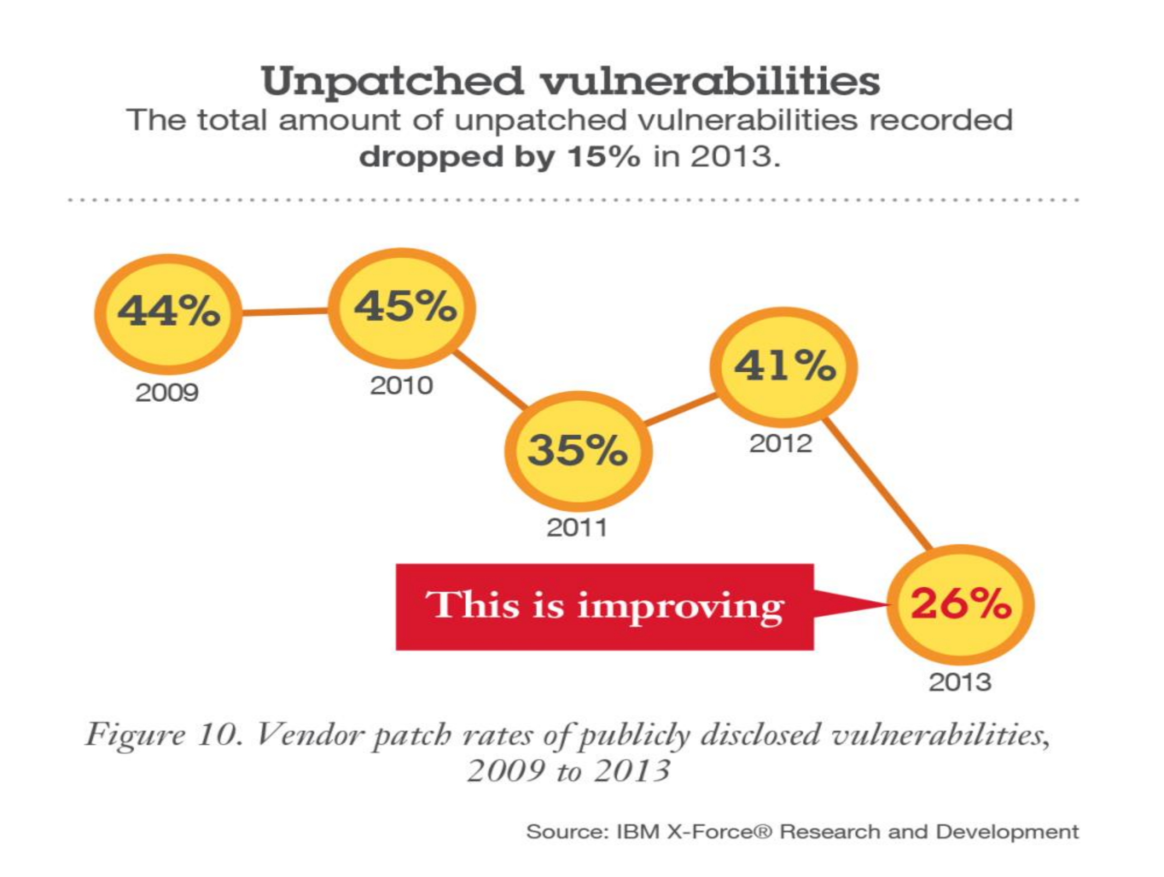
True exploit disclosures

The number continues to drop steadily from 2009 to 2013.

Figure 13. True exploit disclosures, 2009 to 2013

Source: IBM X-Force® Research and Development

Major vendors continue to improve patching



Unpatched vulnerabilities

The total amount of unpatched vulnerabilities recorded **dropped by 15%** in 2013.

Figure 10. Vendor patch rates of publicly disclosed vulnerabilities, 2009 to 2013

Source: IBM X-Force® Research and Development

Connect with IBM X-Force Research & Development

Follow us at @ibmsecurity and @ibmxforce

Download X-Force security trend & risk reports
http://www.ibm.com/security/xforce/

X-Force Security Insights blog at http://securityintelligence.com/xforce/

© 2014 IBM Corporation

Statement of Good Security Practices: IT system security involves protecting systems and information through prevention, detection and response to improper access from within and outside your enterprise. Improper access can result in information being altered, destroyed or misappropriated or can result in damage to or misuse of your systems, including to attack others. No IT system or product should be considered completely secure and no single product or security measure can be completely effective in preventing improper access. IBM systems and products are designed to be part of a comprehensive security approach, which will necessarily involve additional operational procedures, and may require other systems, products or services to be most effective. IBM DOES NOT WARRANT THAT SYSTEMS AND PRODUCTS ARE IMMUNE FROM THE MALICIOUS OR ILLEGAL CONDUCT OF ANY PARTY.

Thank You

www.ibm.com/security

© Copyright IBM Corporation 2014. All rights reserved. The information contained in these materials is provided for informational purposes only, and is provided AS IS without warranty of any kind, express or implied. IBM shall not be responsible for any damages arising out of the use of, or otherwise related to, these materials. Nothing contained in these materials is intended to, nor shall have the effect of, creating any warranties or representations from IBM or its suppliers or licensors, or altering the terms and conditions of the applicable license agreement governing the use of IBM software. References in these materials to IBM products, programs, or services do not imply that they will be available in all countries in which IBM operates. Product release dates and/or capabilities referenced in these materials may change at any time at IBM’s sole discretion based on market opportunities or other factors, and are not intended to be a commitment to future product or feature availability in any way. IBM, the IBM logo, and other IBM products and services are trademarks of the International Business Machines Corporation, in the United States, other countries or both. Other company, product, or service names may be trademarks or service marks of others.