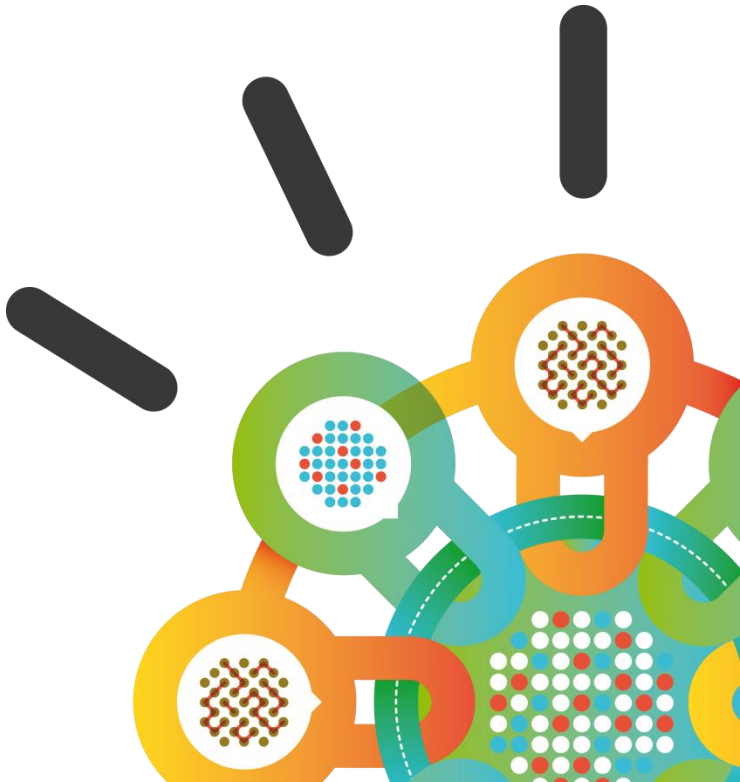
Security Intelligence.
Think Integrated.

# IBM X-Force: The Emerging Threat Landscape

Michael P. Hamelin
Lead X-Force Security Architect
IBM Security Systems




# IBM X-Force

is the foundation for advanced security and threat research across the IBM Security Framework.

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

| | |
|---|---|
| **Vulnerability Protection** | ➥ Reverse engineering and protection against more than **76K vulnerabilities** and **400 application protocols** housed in the X-Force Database |
| **IP Reputation** | ➥ Categorization more than **800K suspect IP addresses** into different categories including malware hosts, botnets, spam sources, and anonymous proxies |
| **Malware Analysis** | ➥ Analysis and defense of malware targeting financial institutions and customers leveraging a network of **30M endpoints** across the globe |
| **Web Application Control** | ➥ Identify and manage the capabilities of more than **2000 web and client applications** (e.g. Gmail or Skype) |
| **Web Application Protection** | ➥ Able to assess and remediate vulnerabilities in mission critical web applications |
| **URL/Web Filtering** | ➥ One of the world's largest URL databases containing categorized information on more than **22 billion** URLs |
| **Anti-Spam** | ➥ Detect spam using known signatures, discover new spam types automatically, **99.9% accurate**, near 0% over-blocking; monitoring of more than **7M spam & phishing attacks daily**. |

# IBM X-Force Threat Intelligence is a key differentiator for IBM Security Systems.

## Coverage

**20,000+** devices under contract

**3,700+** managed clients worldwide

**15B+** events managed per day

**133** monitored countries (MSS)

**1,000+** security related patents


## Depth

**22B** analyzed web pages & images

**7M** spam & phishing attacks daily

**73K** documented vulnerabilities

**Billions** of intrusion attempts daily

**Millions** of unique malware samples

More than

# half a billion records

of personally identifiable information (PII) were leaked in 2013.

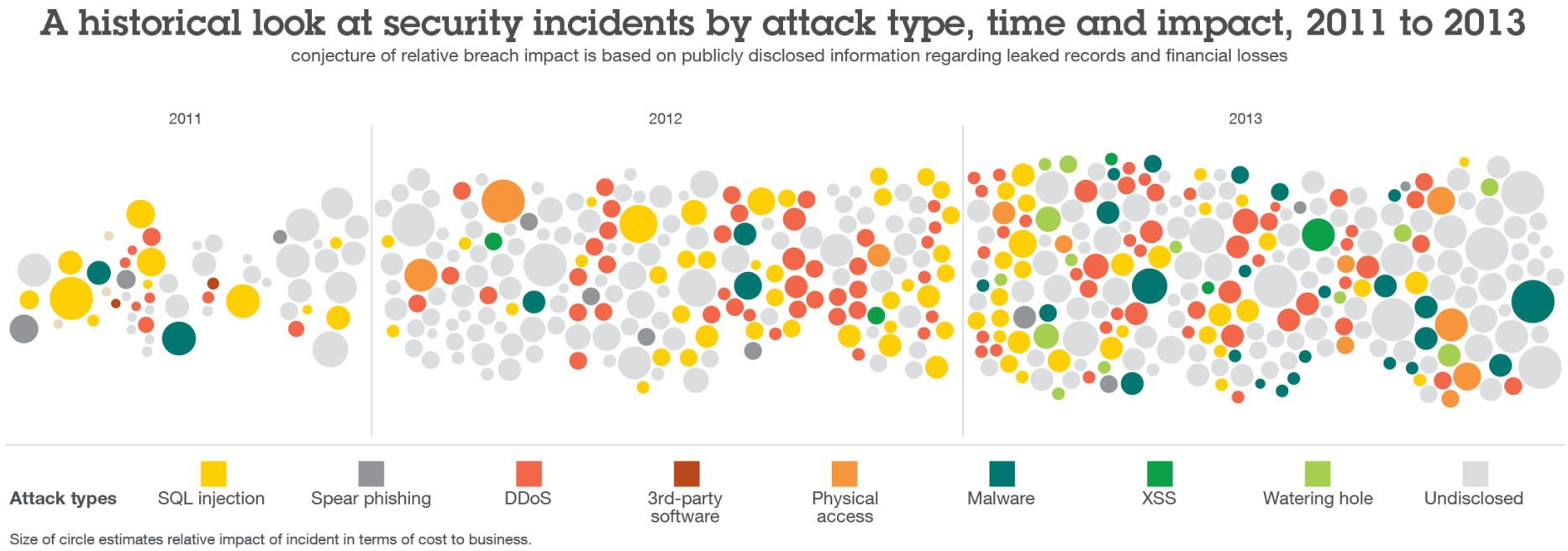



*Figure 1. A historical look at security incidents by attack type, time and impact, 2011 to 2013*

Source: IBM X-Force® Research and Development

Computer services, government and financial markets were the most attacked industries as

# attackers focused on central strategic targets.

## 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

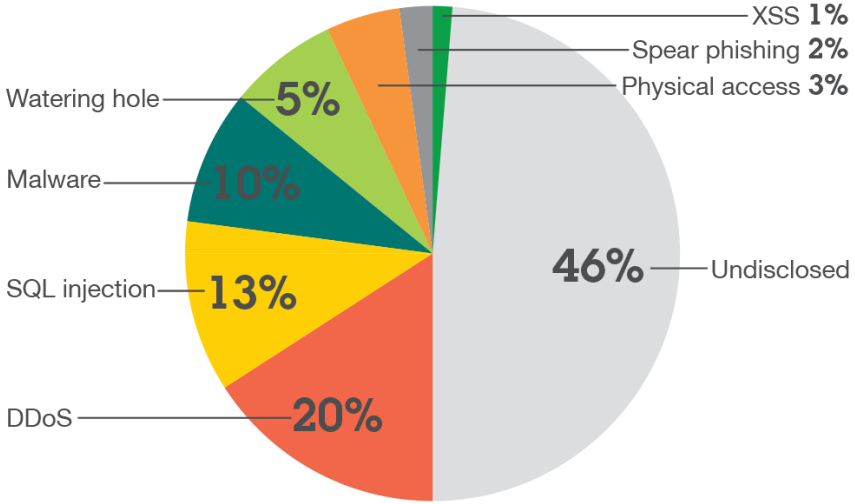



*Figure 2a. Sampling of 2013 security incidents by attack type, time and impact*

Source: IBM X-Force® Research and Development

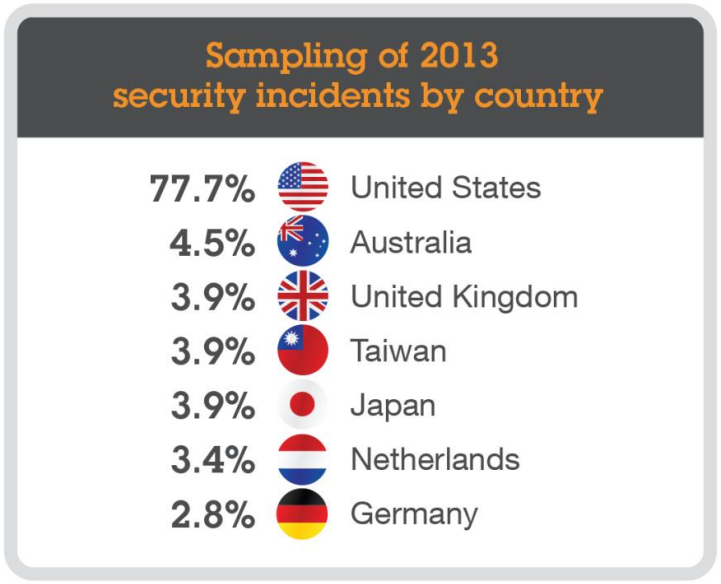



*Figure 3. Sampling of 2013 security incidents by country*

Aside from hard dollar value losses in fines and capital, breached companies will also suffer from a

**loss of intellectual property and customer trust.**

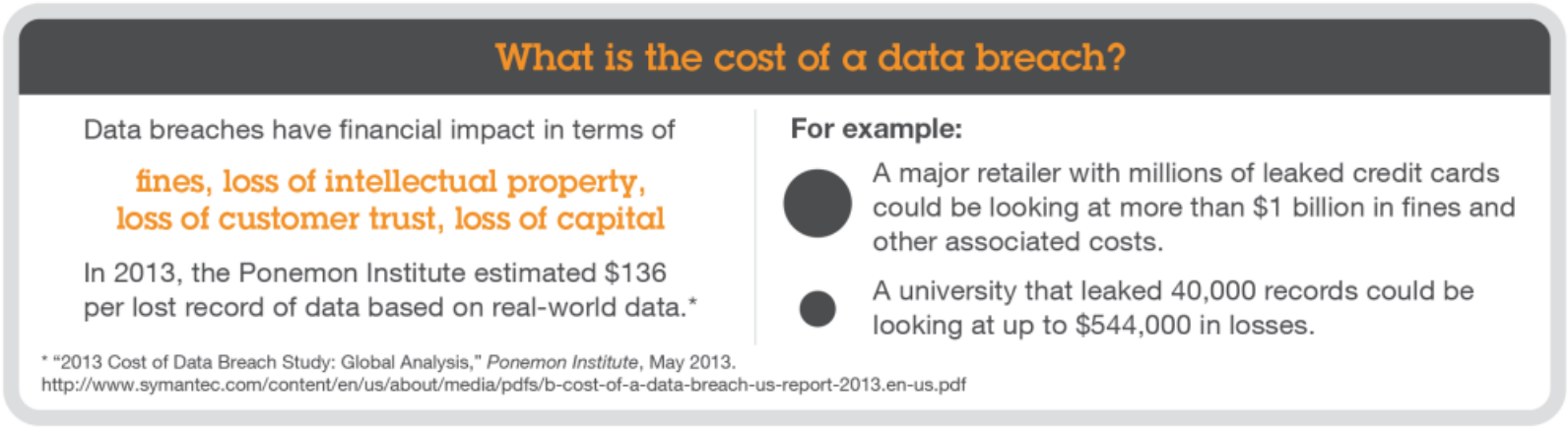



*Figure 2b. Sampling of 2013 security incidents by attack type, time and impact*

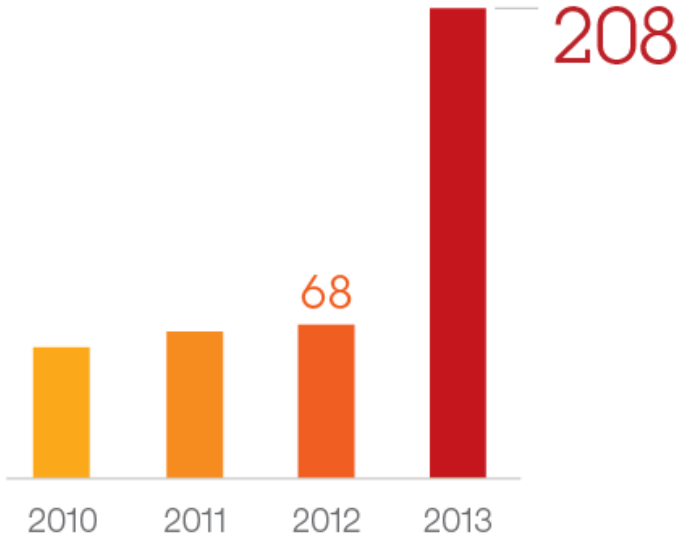
Source: IBM X-Force® Research and Development

Oracle Java™ Technology Edition is used in nearly every enterprise.

Explosive growth of **Java vulnerabilities**...

## Java vulnerability disclosures growth by year, 2010 to 2013

Originating in either the core Oracle Java or in IBM Runtime Environment, Java™ Technology Edition SDKs




Source: IBM X-Force Research & Development

## Exploitation of application vulnerabilities

from survey of 1 million Trusteer customers, December 2013

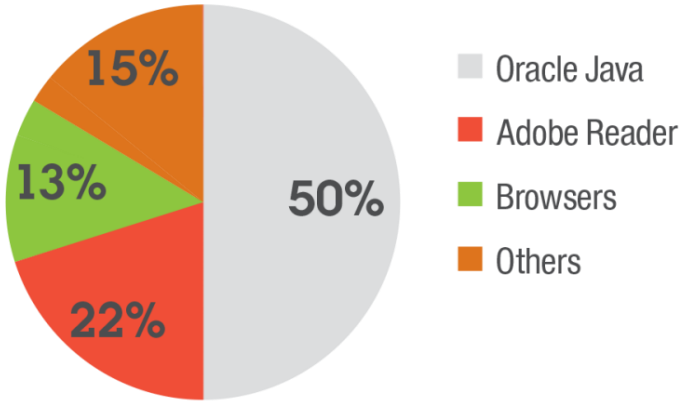



*Figure 4. Exploitation of application vulnerabilities*

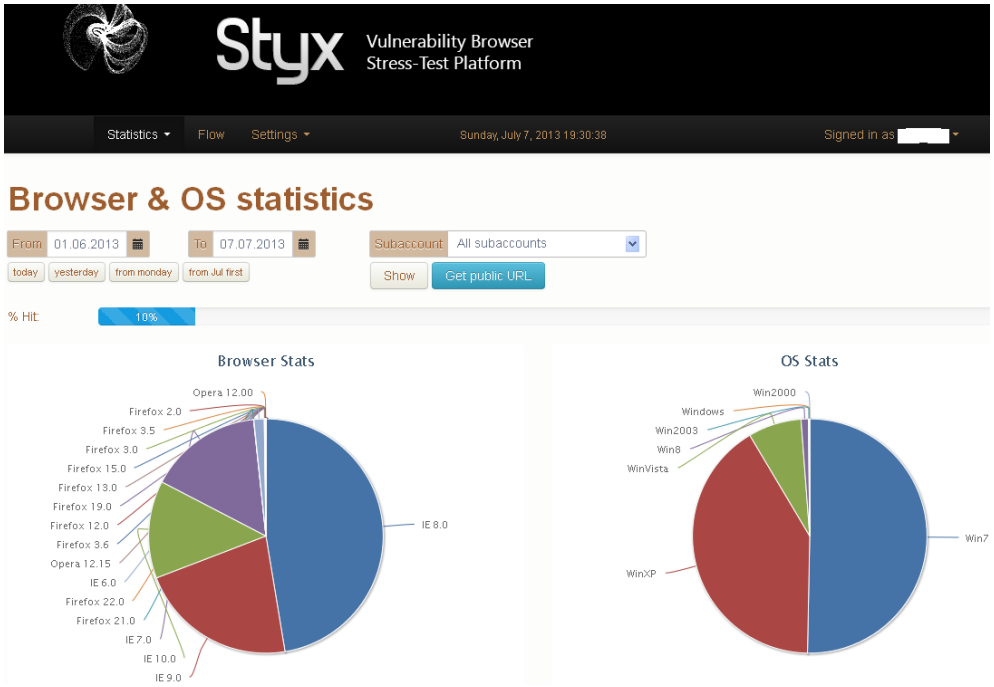
Source: IBM X-Force® Research and Development

… combined with a presence in every enterprise makes Java the **top target** for exploits.

Attackers are using **exploit kits** to deliver payloads.

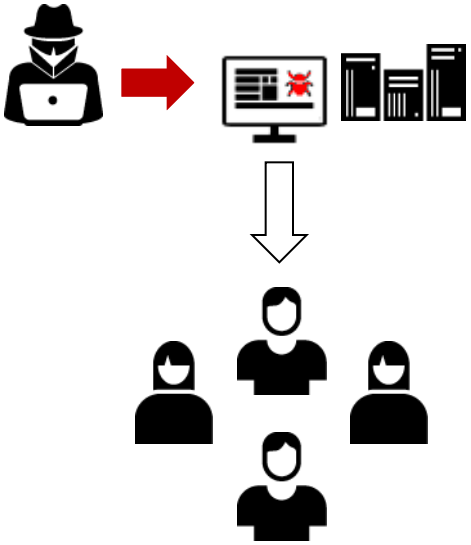
The **Blackhole Exploit Kit** was the most popular in 2013. The creator was arrested in October.

The **Styx Exploit Kit** is rising in popularity, successful in exploiting IE and Firefox on Windows platforms.

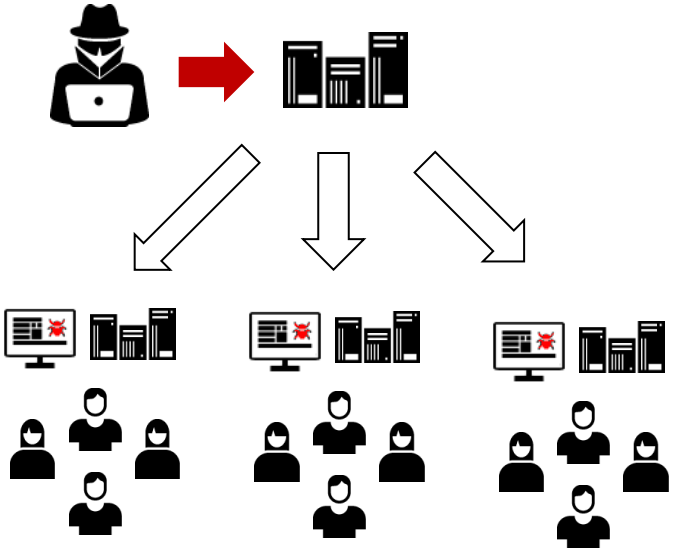
Attackers are effectively targeting end users with

# more sophisticated attacks.



## 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

Most successful Java exploits are **applicative**, exploiting vulnerabilities related to the **Java security manager** and bypassing native OS-level protections.

## Applicative exploits

- Difficult to defend
- Gain unrestricted privileges
- Bypass native OS-level protections

## Native exploits

- Buffer Overflow
- Illegal memory use
- Use-after-free

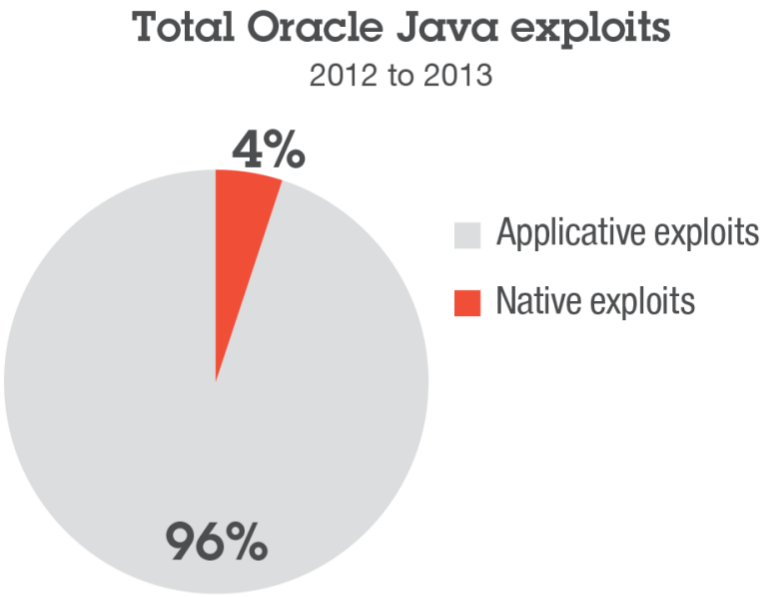



*Figure 6. Total Oracle Java expoits, 2012 to 2013*

Source: IBM X-Force® Research and Development

# The biggest risk to the enterprise isn't the data contained on **mobile devices** - it's the **credentials.**

## The real threats:

- Compromised credentials
- Personal information to further compromise social media accounts
- Rogue apps that are cracked and re-distributed

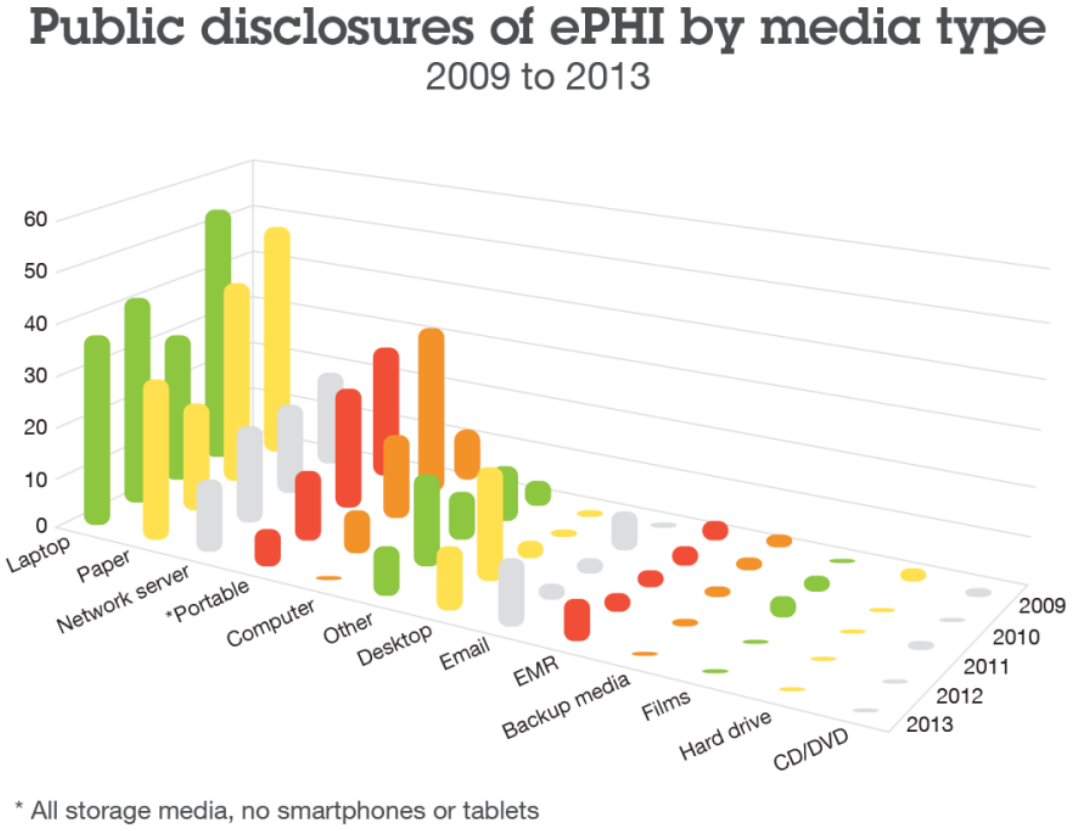



*Figure 7. Public disclosures of ePHI by media type, 2009 to 2013*

Source: IBM X-Force® Research and Development

Vulnerability disclosures leveled out in 2013, but attackers have

**plenty of older, unpatched systems to exploit.**

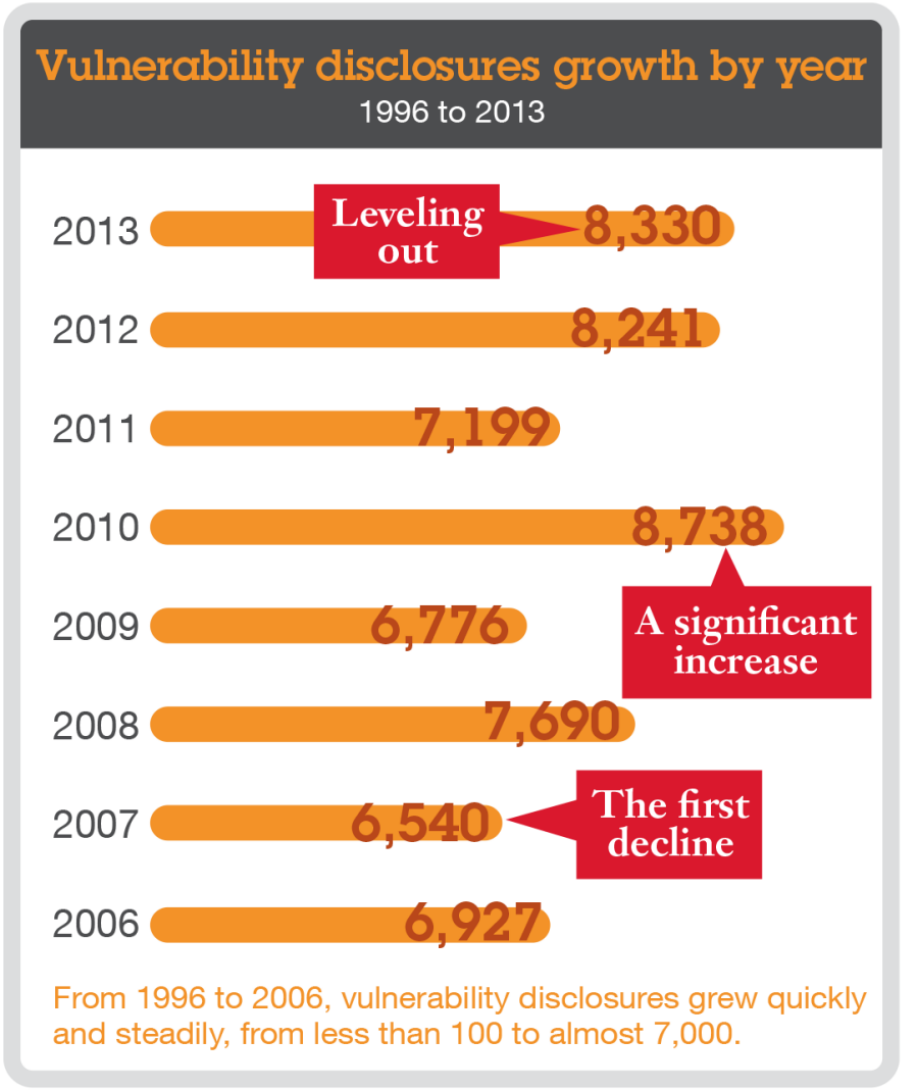



*Figure 8. Vulnerability disclosures growth by year, 1996 to 2013*

Source: IBM X-Force® Research and Development

# Declines in web application vulnerabilities

could indicate improvements in app authoring or patching practices.

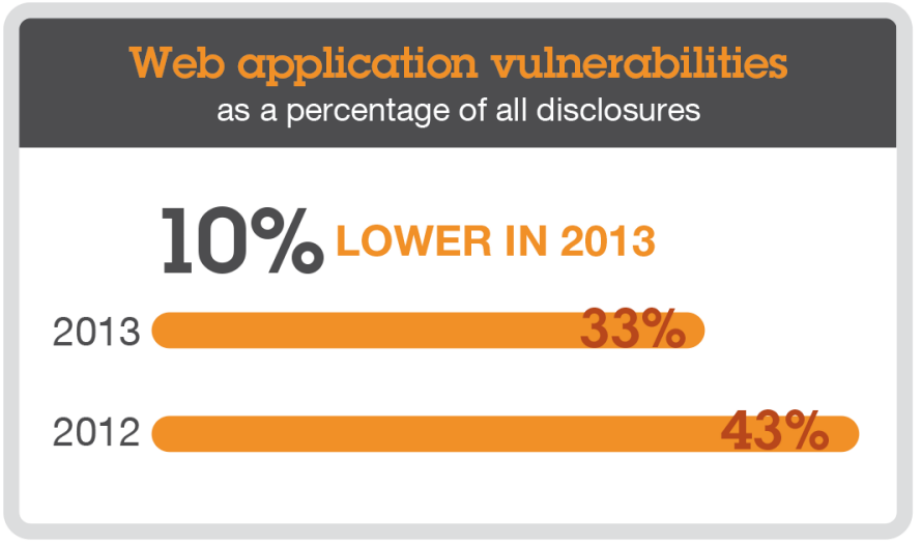



*Figure 9. Web application vulnerabilities as a percentage of all disclosures, 2012 to 2013*

Source: IBM X-Force® Research and Development

## Possible reasons:

- Software authors are doing a better job at writing secure web applications.
- CMS systems & plugins are maturing as older vulnerabilities are patched.

**And yet**… XSS and SQLi exploitation is still observed in high numbers.

Although declining as a portion of the total,

## XSS and SQLi attacks will continue

until the many thousands of websites running unpatched versions of their platform or framework are patched.

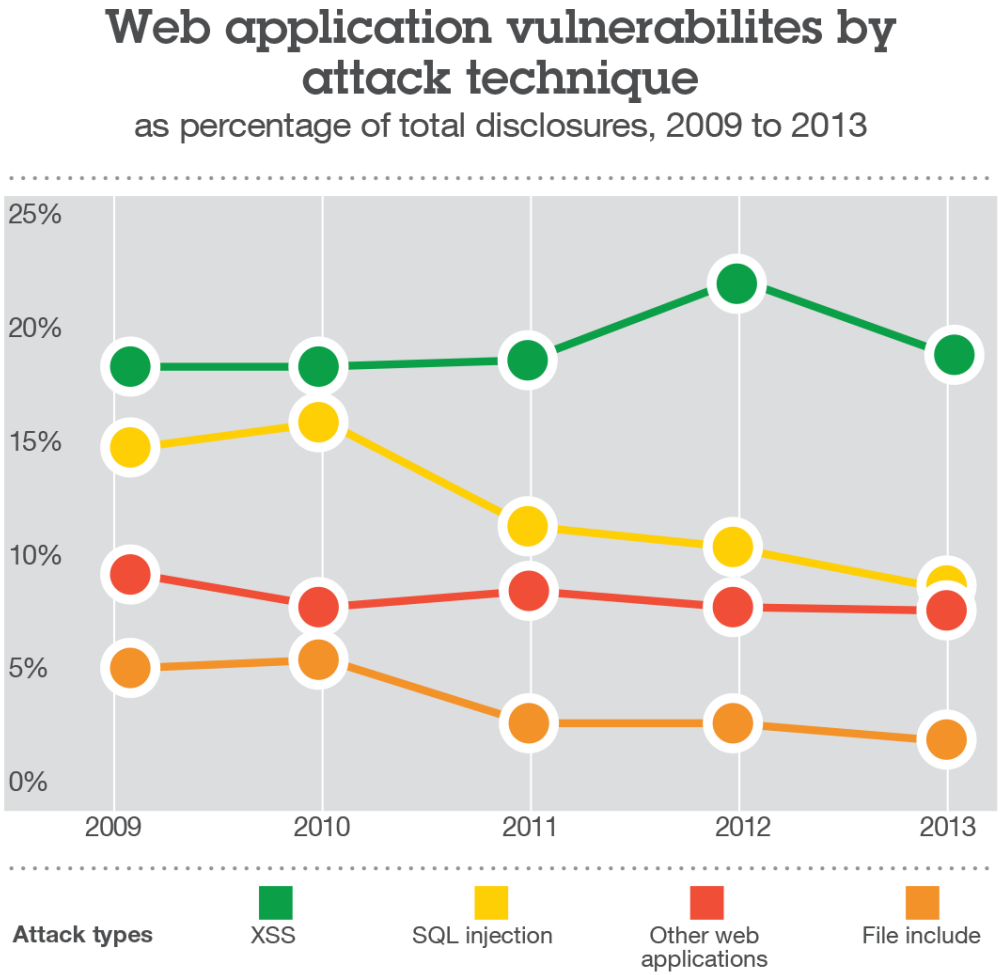



*Figure 11. Web application vulnerabilities by attack technique, 2009 to 2013*

Source: IBM X-Force® Research and Development

## Consequences of exploitation 2013

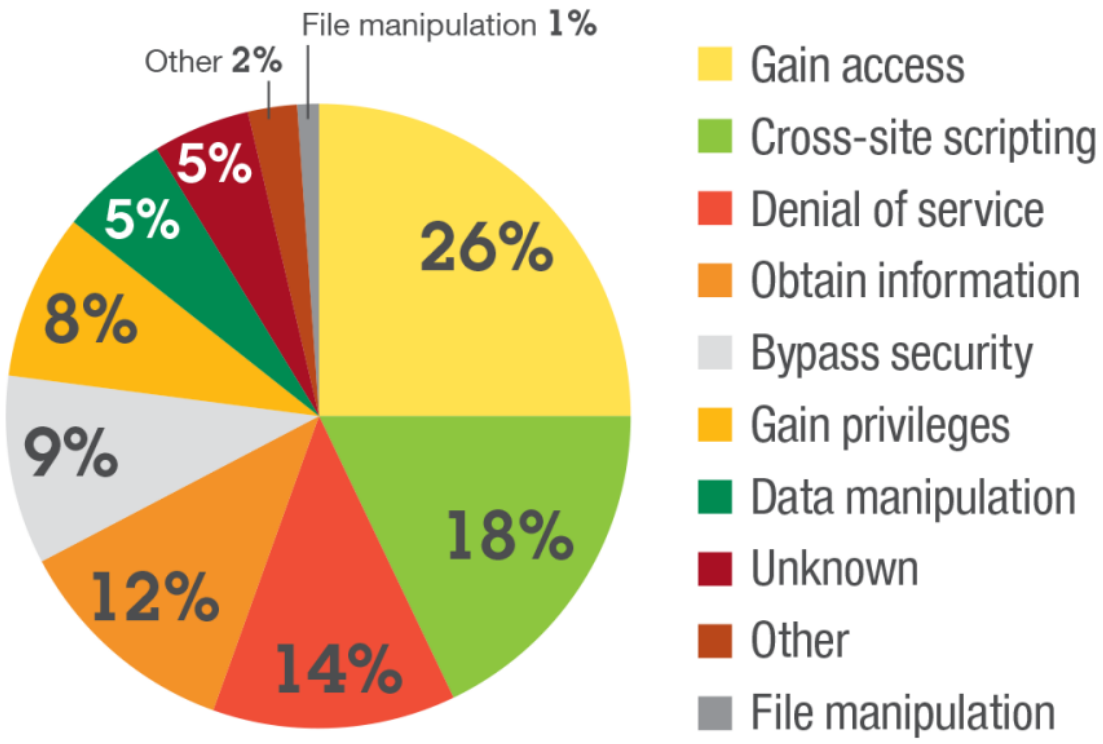



*Figure 12. Consequences of exploitation 2013*

Source: IBM X-Force® Research and Development

The top intended consequence for exploits was **gaining additional or unauthorized access.**

Major vendors continue to improve patching, so that the total amount of

unpatched vulnerabilities dropped 15%

last year.

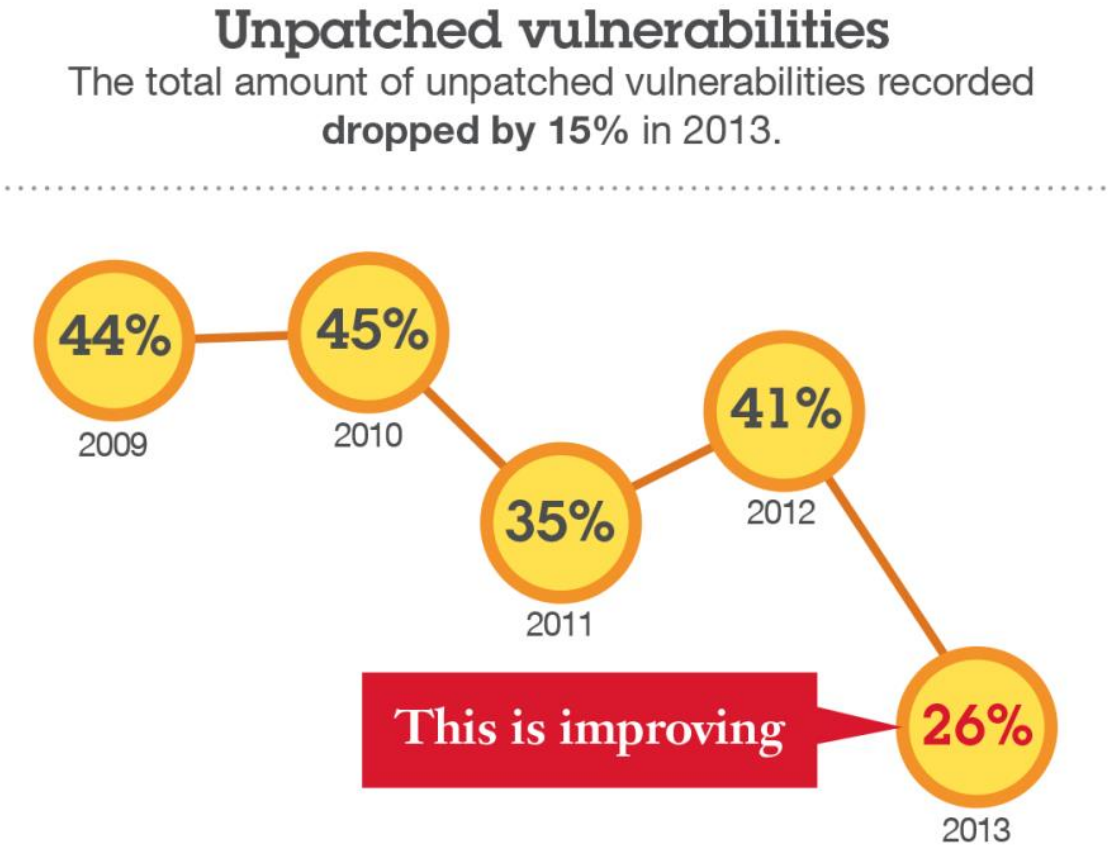



*Figure 10. Vendor patch rates of publicly disclosed vulnerabilities, 2009 to 2013*

Source: IBM X-Force® Research and Development

Reports of

# true exploits declined

to the lowest level in the past 5 years.

Two categories of exploits are tracked:

- *Exploits*: Proof-of-concept code
- *True Exploits*: Fully functional programs capable of attacks

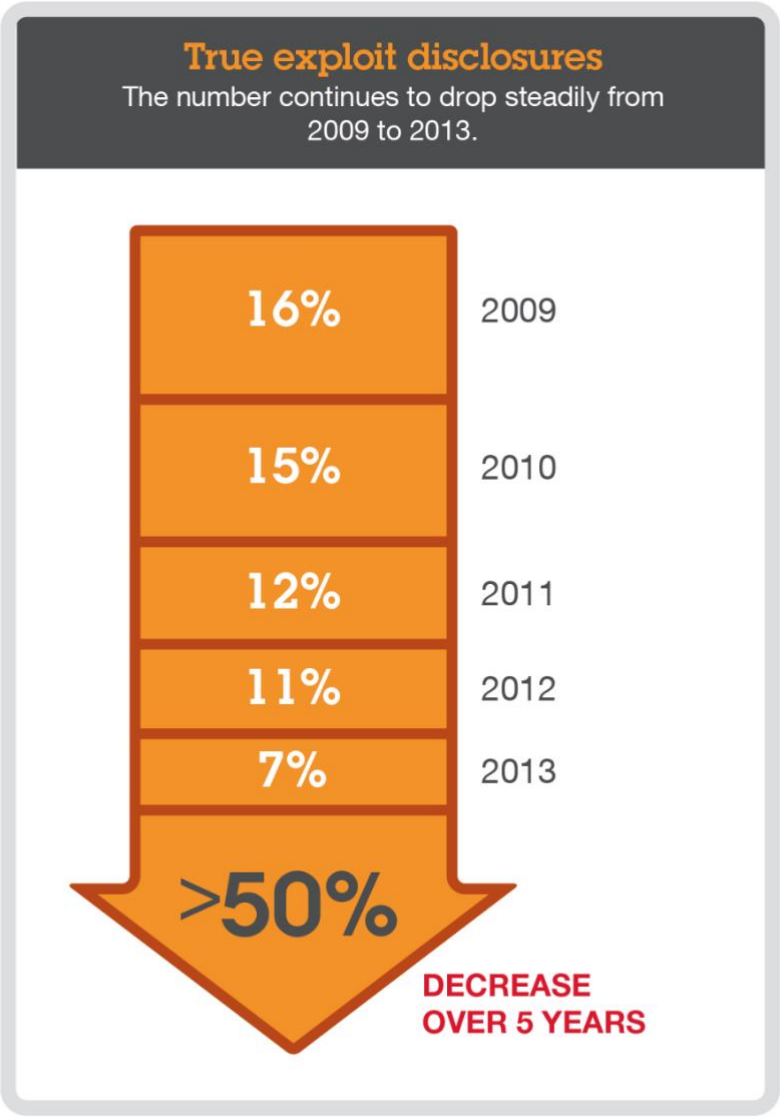



*Figure 13. True exploit disclosures, 2009 to 2013*

Source: IBM X-Force® Research and Development

# Connect with IBM X-Force Research & Development

Follow us at @ibmsecurity and @ibmxforce

Download IBM X-Force Threat Intelligence Quarterly Reports
http://www.ibm.com/security/xforce/

IBM X-Force Security Insights blog at
www.SecurityIntelligence.com/x-force

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**