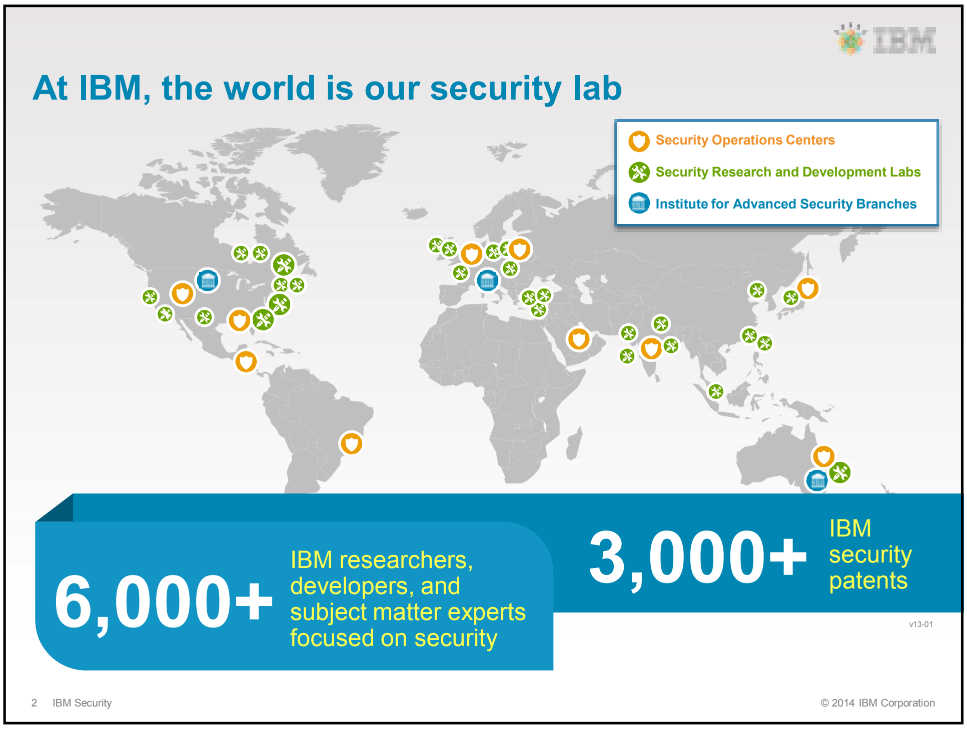
IBM

Security Intelligence.
Think Integrated.

IBM X-Force: The Emerging Threat Landscape

Michael Hamelin
Lead X-Force Security Architect
CTO Threat & Infrastructure, IBM Security Systems



IBM

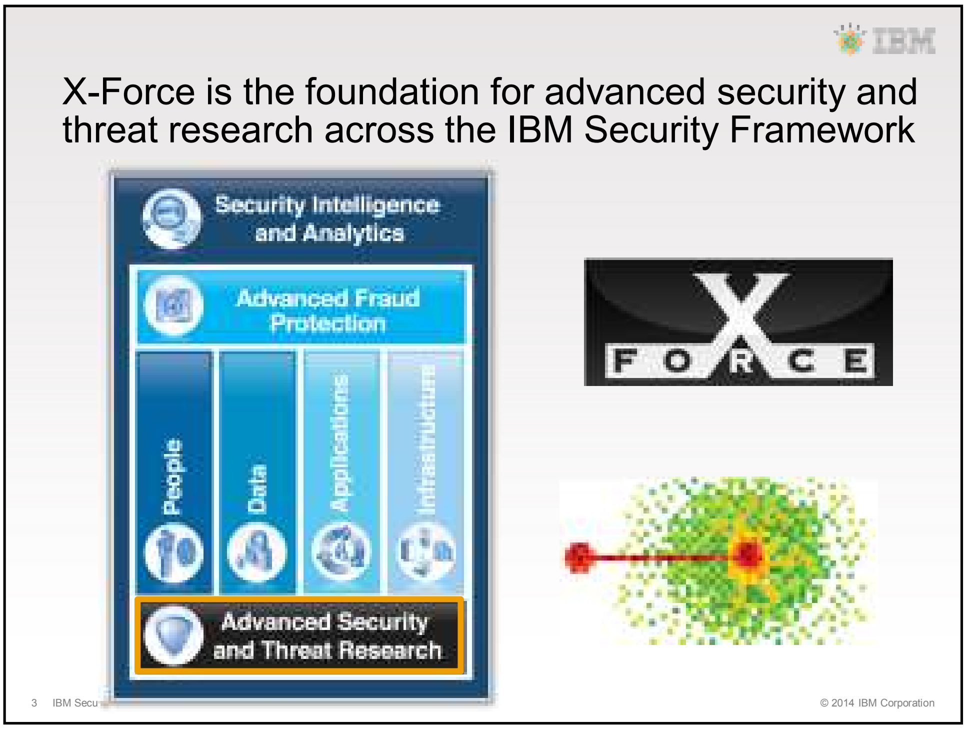
At IBM, the world is our security lab

Security Operations Centers
Security Research and Development Labs
Institute for Advanced Security Branches

6,000+ IBM researchers, developers, and subject matter experts focused on security

3,000+ IBM security patents

v13-01

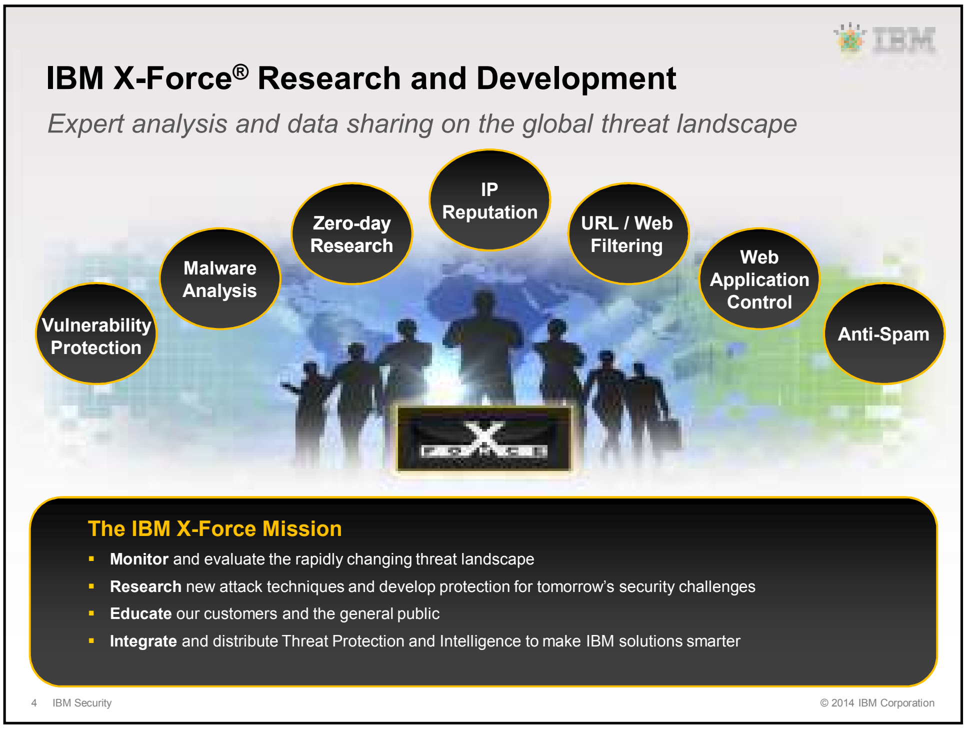


X-Force is the foundation for advanced security and threat research across the IBM Security Framework

Security Intelligence and Analytics
Advanced Fraud Protection
People
Data
Applications
Infrastructure
Advanced Security and Threat Research
X FORCE

3 IBM Secu

© 2014 IBM Corporation



IBM X-Force® Research and Development

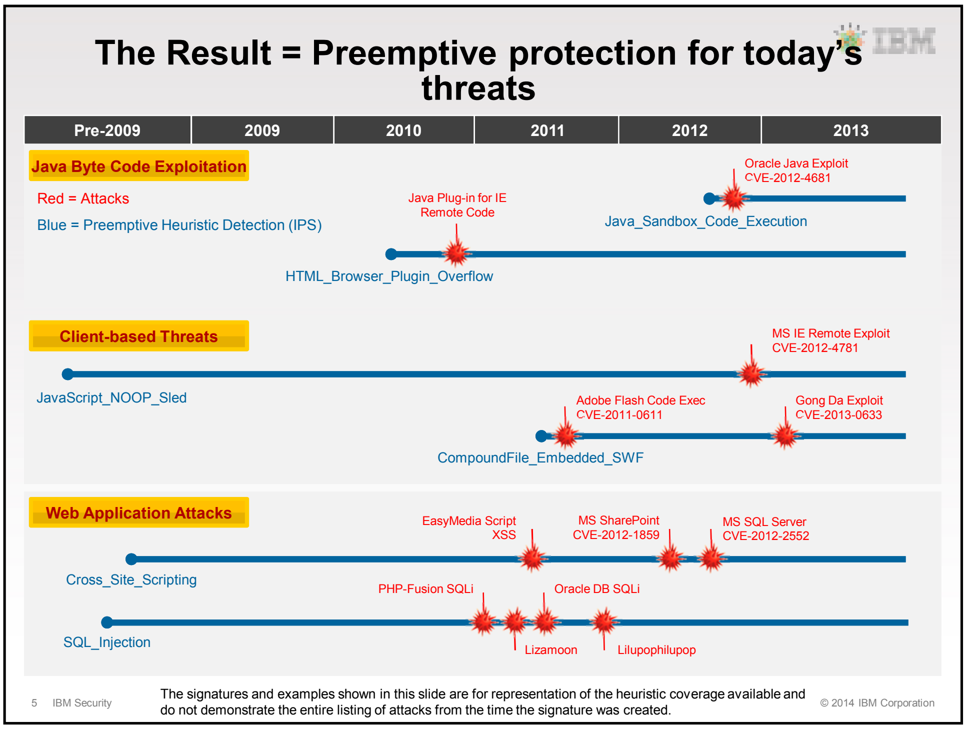
Expert analysis and data sharing on the global threat landscape

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

4 IBM Security

© 2014 IBM Corporation



The Result = Preemptive protection for today's threats

Pre-2009	2009	2010	2011	2012	2013

Java Byte Code Exploitation

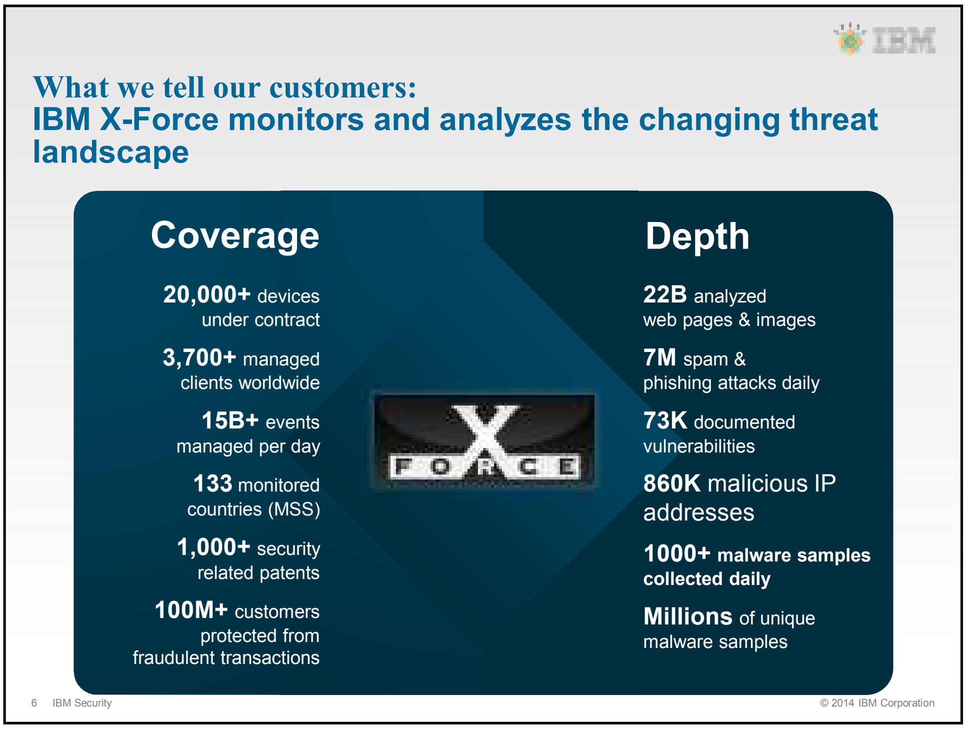
Red = Attacks

Blue = Preemptive Heuristic Detection (IPS)

Client-based Threats

Web Application Attacks

The signatures and examples shown in this slide are for representation of the heuristic coverage available and do not demonstrate the entire listing of attacks from the time the signature was created.



What we tell our customers:
IBM X-Force monitors and analyzes the changing threat landscape

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

100M+ customers protected from fraudulent transactions

Depth

22B analyzed web pages & images

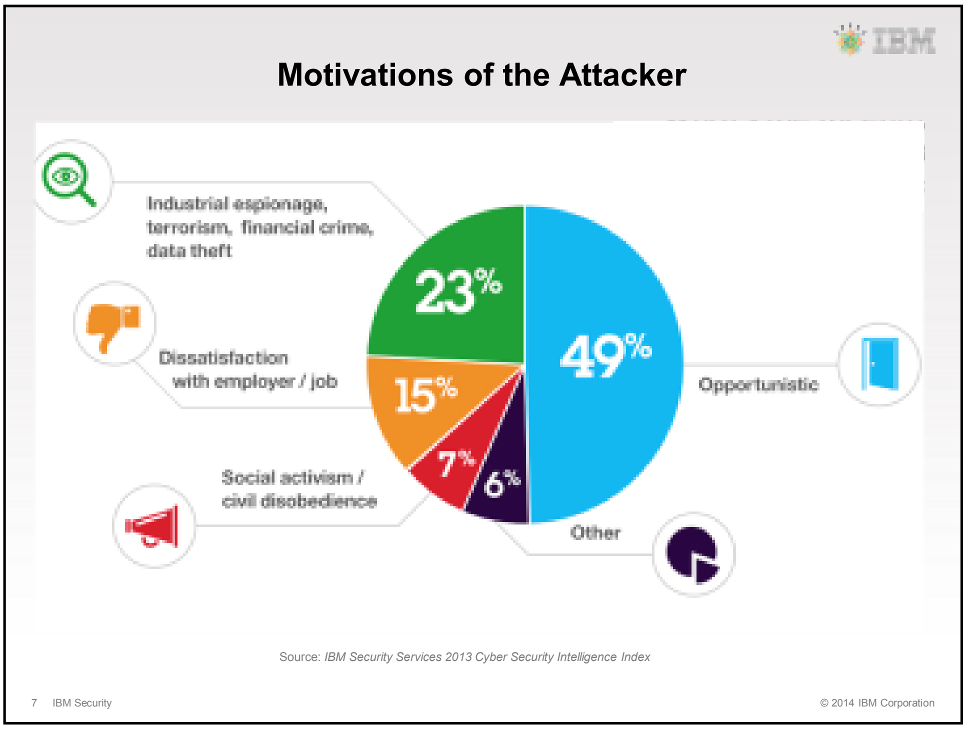
7M spam & phishing attacks daily

73K documented vulnerabilities

860K malicious IP addresses

1000+ malware samples collected daily

Millions of unique malware samples

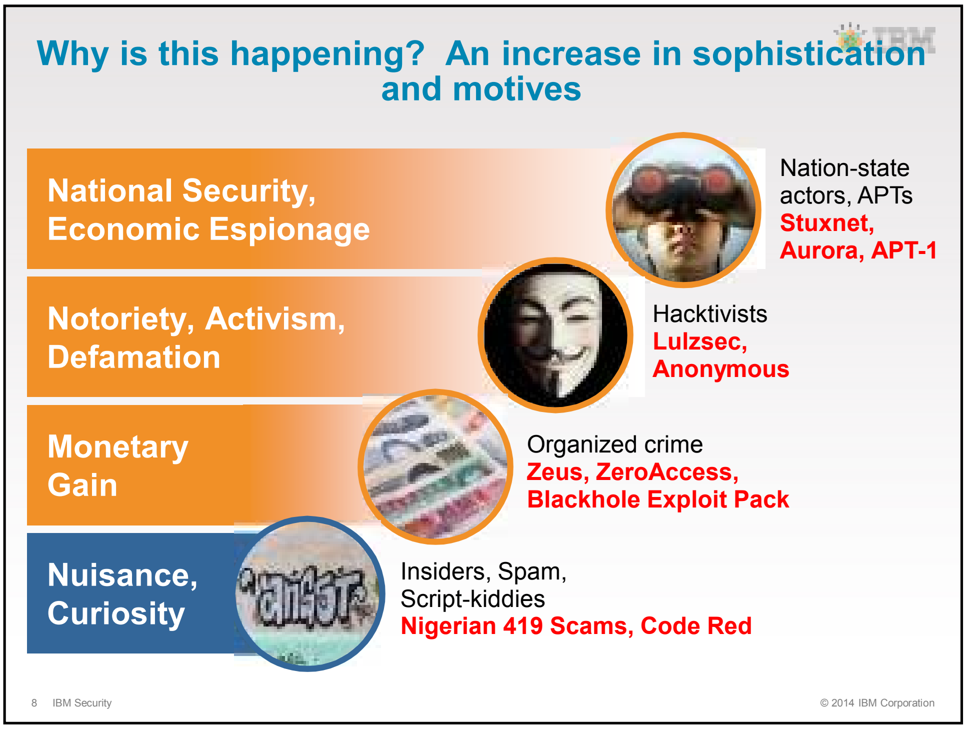


Motivations of the Attacker

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

7 IBM Security

© 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

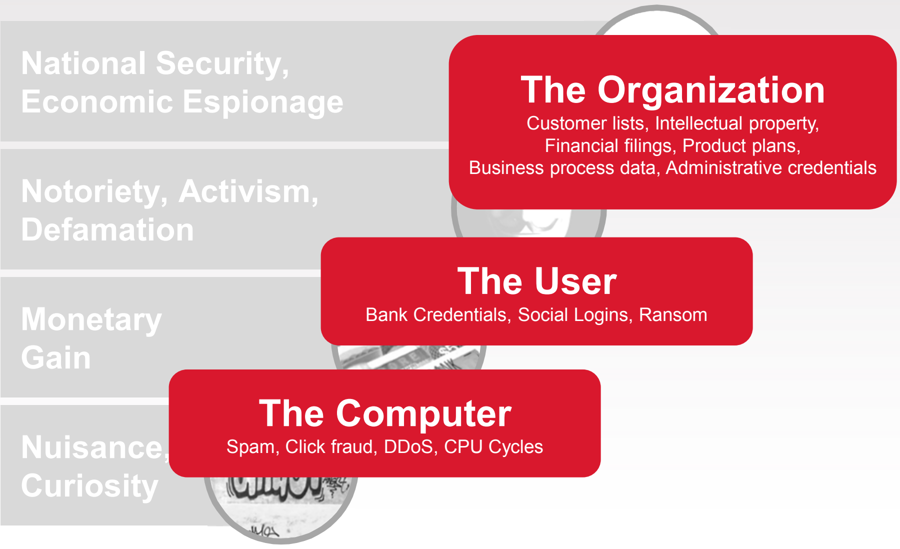
Nuisance, Curiosity

Insiders, Spam, Script-kiddies
Nigerian 419 Scams, Code Red

8 IBM Security

© 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

more than

half a billion records

of personally identifiable information (PII) were leaked in 2013

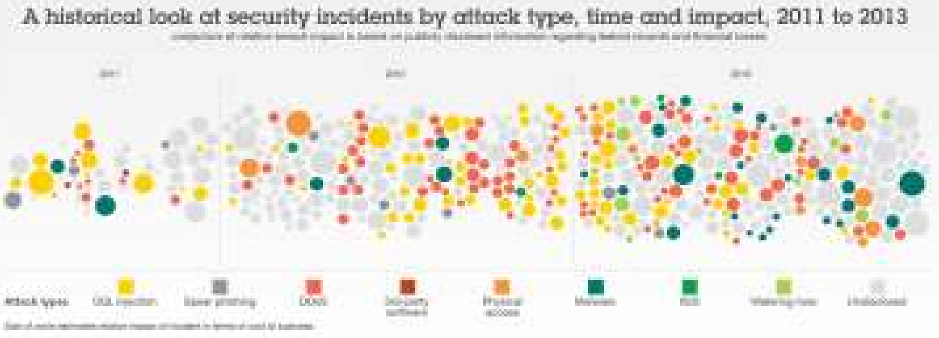
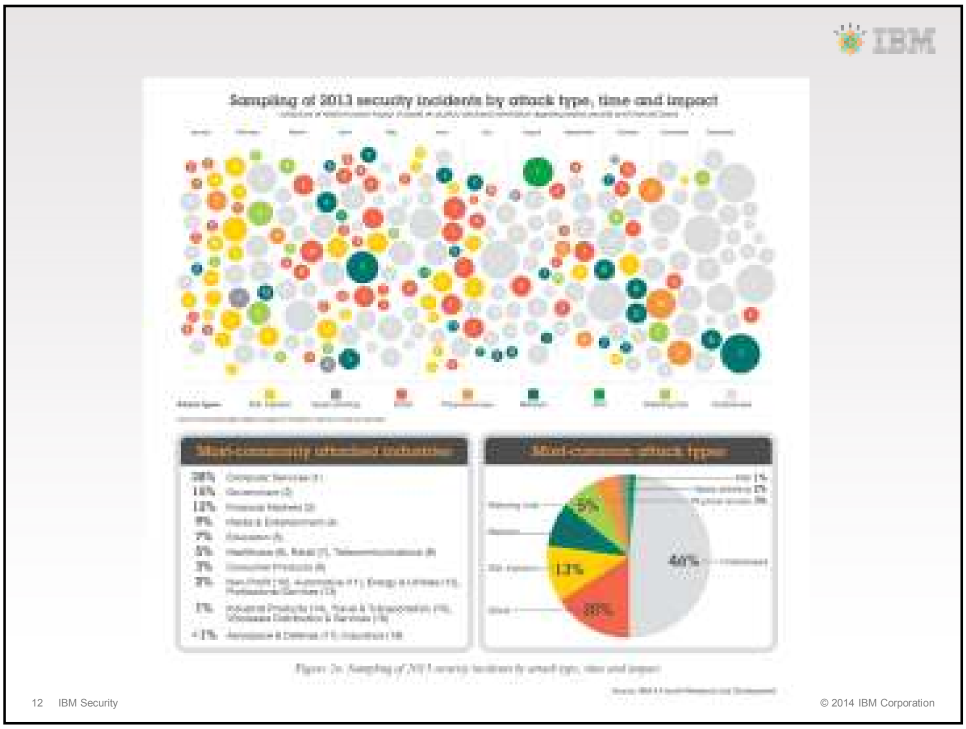


Figure 1. A historical look at security incidents by attack type, time and impact, 2011 to 2013

Source: IBM X-Force® Research and Development



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

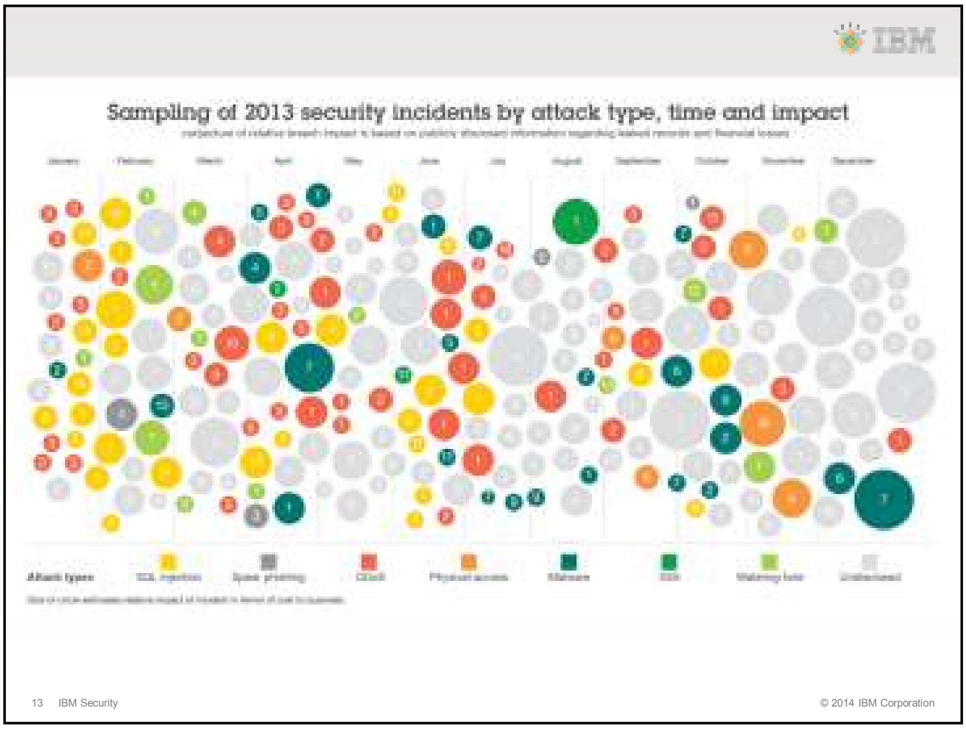
28%	Computer Services (1)
18%	Government (2)
12%	Financial Markets (3)
9%	Media & Entertainment (4)
7%	Education (5)
5%	Healthcare (6), Retail (7), Telecommunications (8)
3%	Consumer Products (9)
3%	Non-Profit (10), Automotive (11), Energy & Utilities (12), Professional Services (13)
1%	Industrial Products (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

12 IBM Security © 2014 IBM Corporation

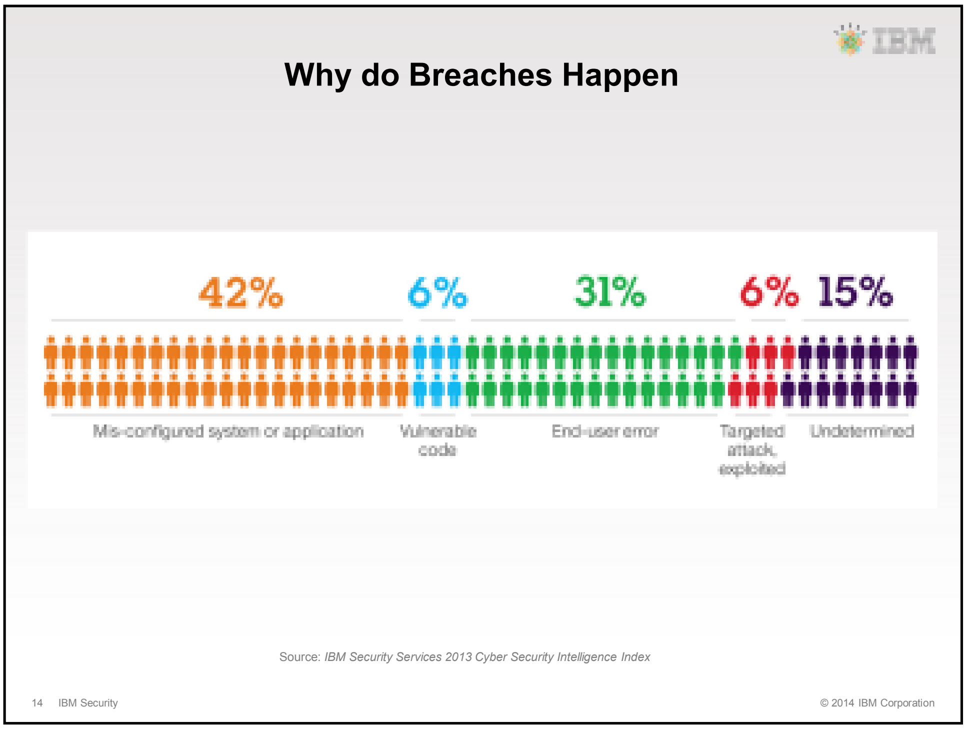


Sampling of 2013 security incidents by attack type, time and impact

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.

13 IBM Security © 2014 IBM Corporation

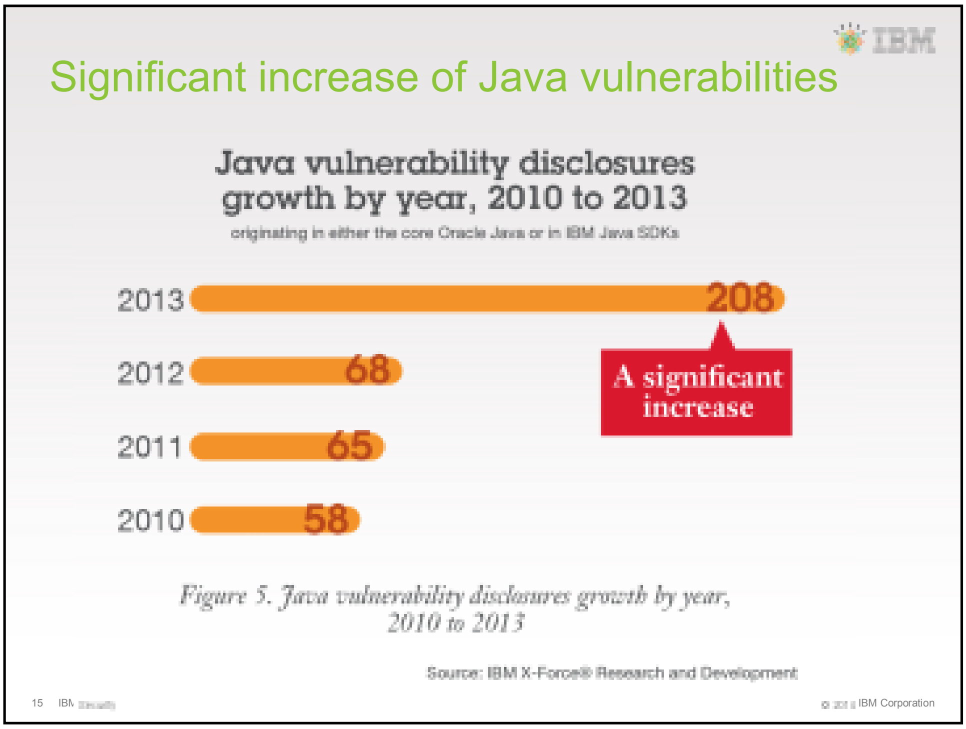


Why do Breaches Happen

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

14 IBM Security

© 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

15 IBM Security

© 2014 IBM Corporation

Weaponized content focused on end user apps

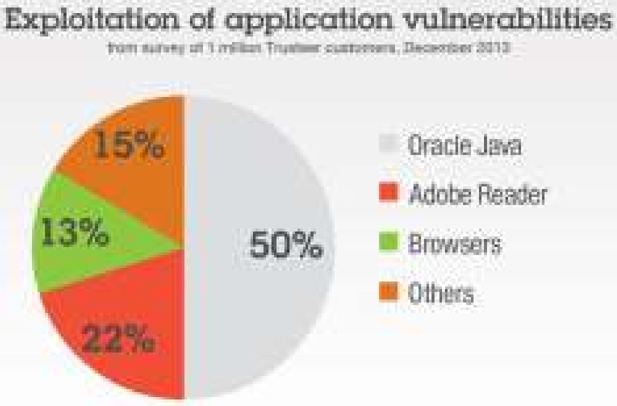


Figure 4. Exploitation of application vulnerabilities

Source: IBM X-Force® Research and Development

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

It’s just another business model

Bronze Edition

[illegible]

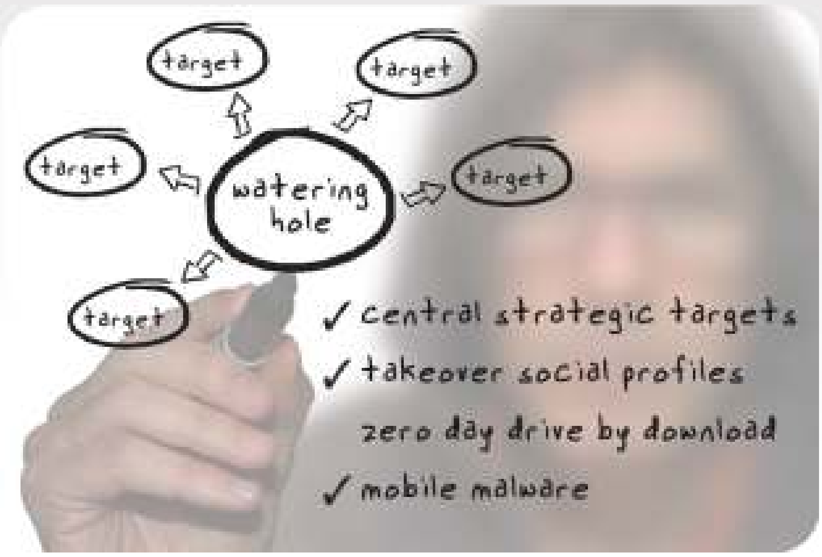
Silver Edition

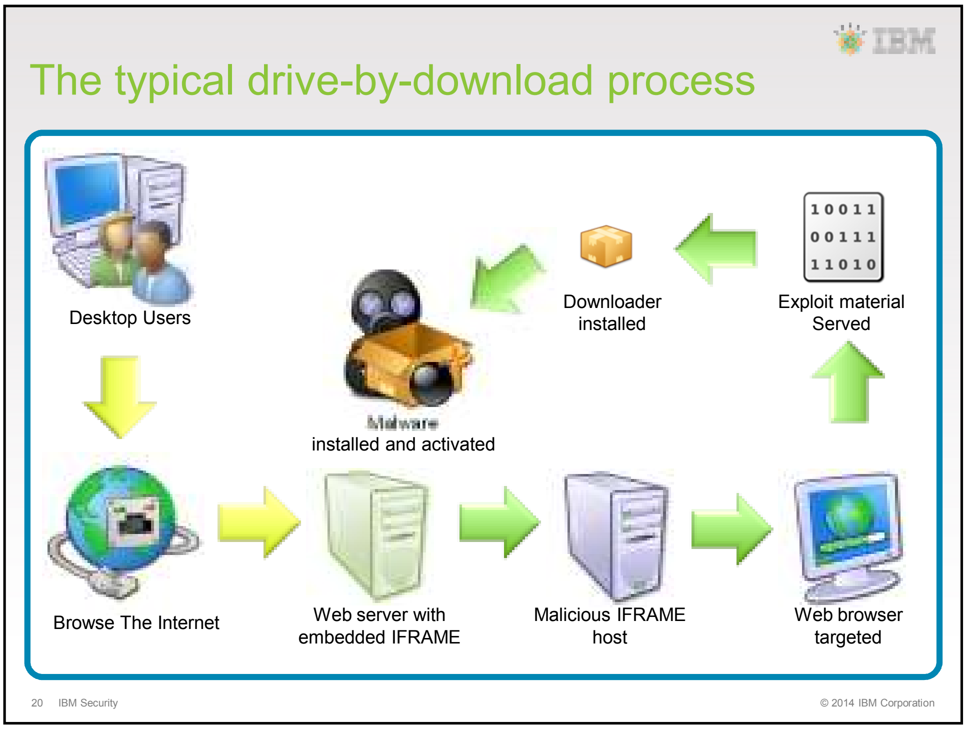
[illegible]

Gold Edition

[illegible]

Attackers optimize and refine target selection


target
target
target
watering hole
target
target
✓ central strategic targets
✓ takeover social profiles
zero day drive by download
✓ mobile malware



The typical drive-by-download process

Desktop Users

Browse The Internet

Web server with embedded IFRAME

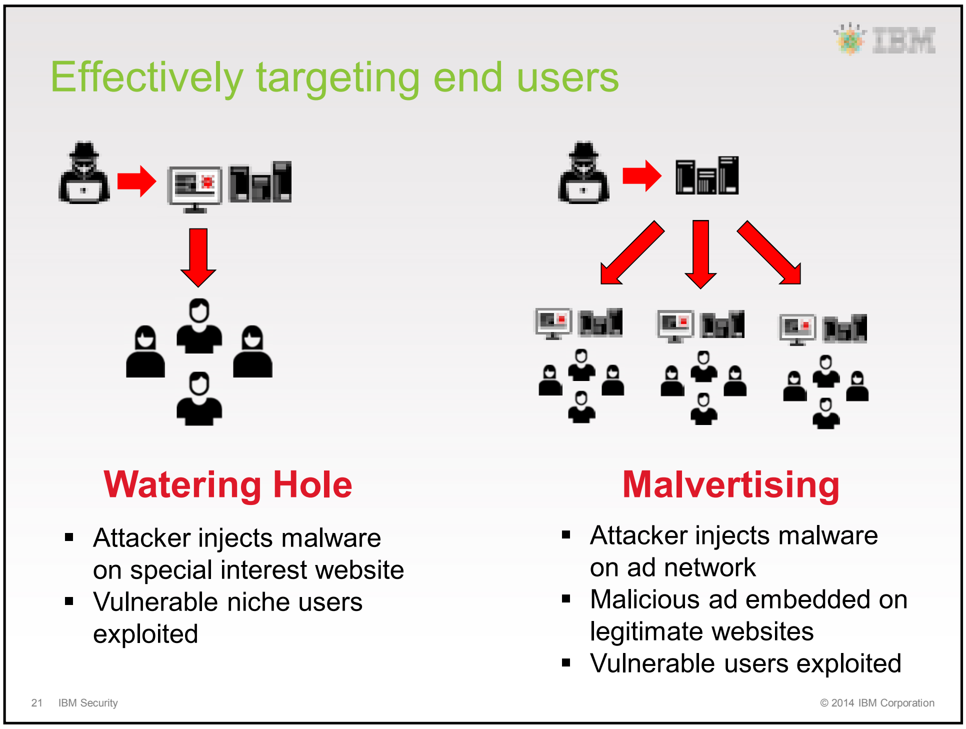
Malicious IFRAME host

Web browser targeted

Exploit material Served

Downloader installed

Malware installed and activated



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

Attackers exploit application vulnerabilities to access sensitive data.

50% of organizations underestimate the number of web applications they have deployed

Test and Remediate AppVulns

- Not testing puts the organization at risk of exposing valuable assets
- Broken authentication can result in take over of banking session and funds transfer as if the attacker were the legitimate user.

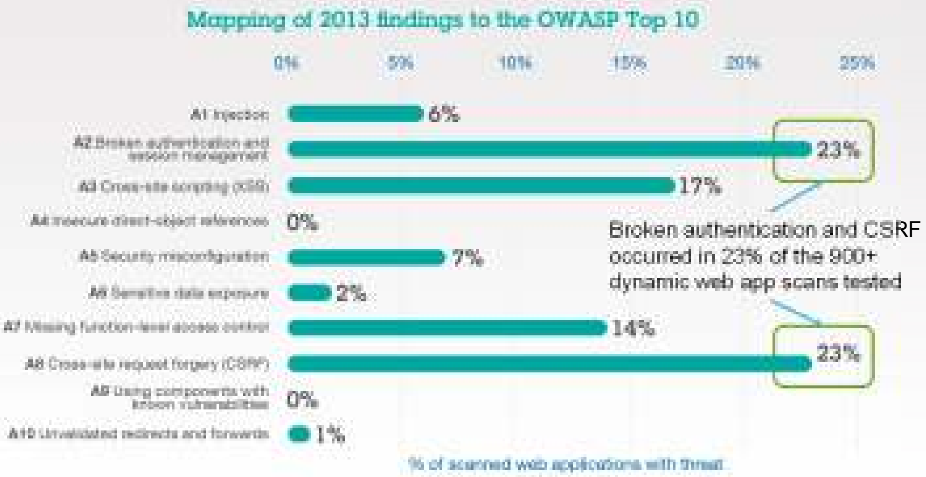
Protect Web Servers

- OpenSSL bug put a huge number of websites at risk for data leakage of private and critical information.
- Mitigating potential damages of breached user credentials, SSL certificates, and other sensitive information made cleanup a

Expect the Unexpected

- If your incident response is built around planning for the known situations, you're at a loss. Contents of random access memory (RAM) are now fair game, like data stored on the disk.

Underestimating web applications is not uncommon.

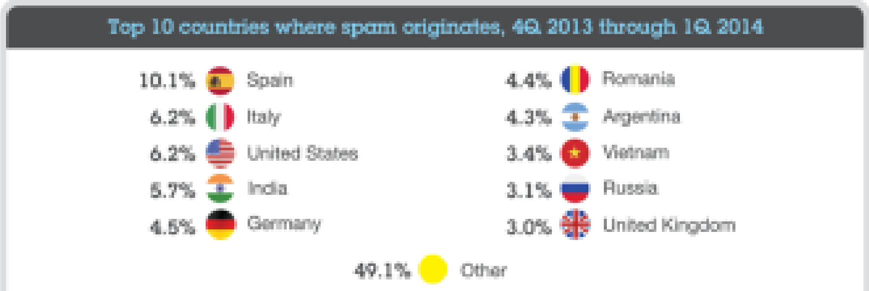


Broken authentication and CSRF occurred in 23% of the 900+ dynamic web app scans tested

Figure 1. Common vulnerabilities found occurring in web applications tested by the IBM Hosted Application Security Management (HASM) service, compared to the OWASP Top 10 for 2013

Spam continues to be a main channel of malware into company networks.

In March 2014, we saw the highest levels of spam measured during the last two and a half years.



Top 10 countries where spam originates, 4Q 2013 through 1Q 2014

10.1%	Spain	4.4%	Romania
6.2%	Italy	4.3%	Argentina
6.2%	United States	3.4%	Vietnam
5.7%	India	3.1%	Russia
4.5%	Germany	3.0%	United Kingdom
49.1%	Other		

Figure 3. The top 10 countries where spam originates, 4Q 2013 through 1Q 2014

Source: IBM X-Force® Research and Development

Attackers are recycling old image-spam techniques to test detection and exploit email inboxes.

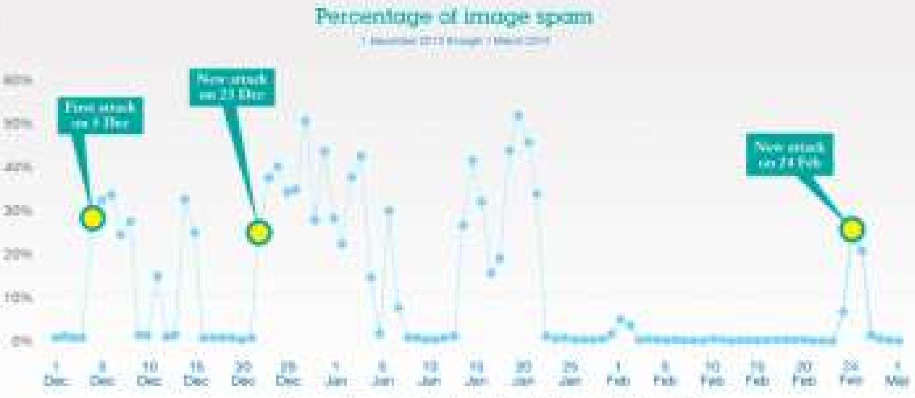


Figure 1. Percentage of image spam, 1 December 2013 through 1 March 2014

Source: IBM X-Force® Research and Development

Attackers are using doctor and medic .ru domains in these attacks.

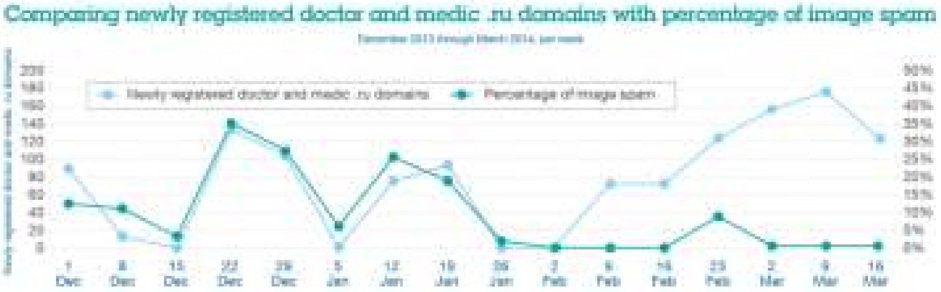


Figure 6. Comparing newly registered doctor and medic .ru domains with the percentage of image spam per week, December 2013 through March 2014

Source: IBM X-Force® Research and Development

Since the beginning of February 2014, spammers have used the domains they have purchased for other, non-image based types of spam.

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