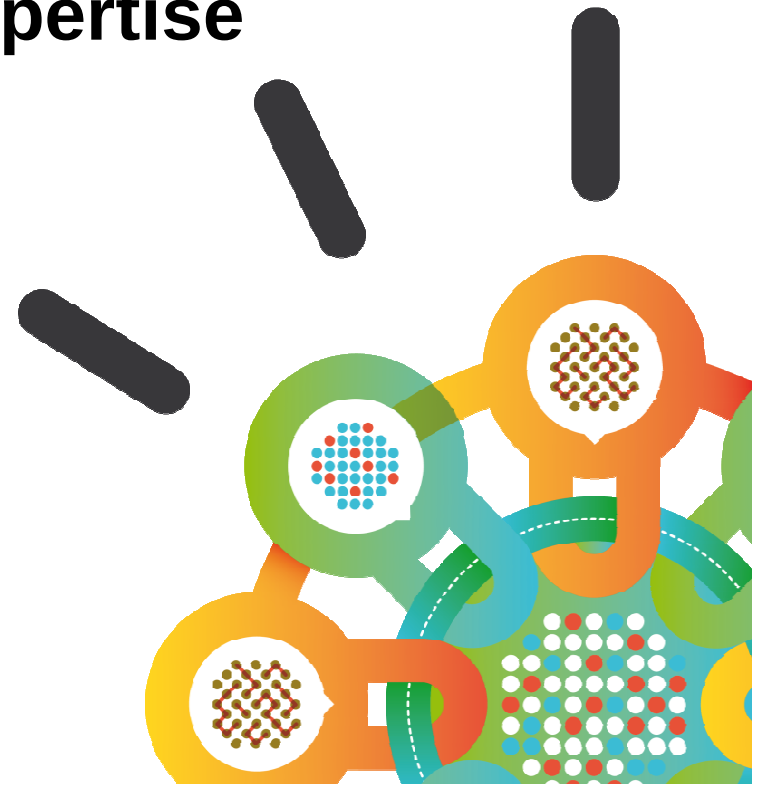
Security Intelligence.
Think Integrated.

IBM Security

Intelligence, Integration and Expertise

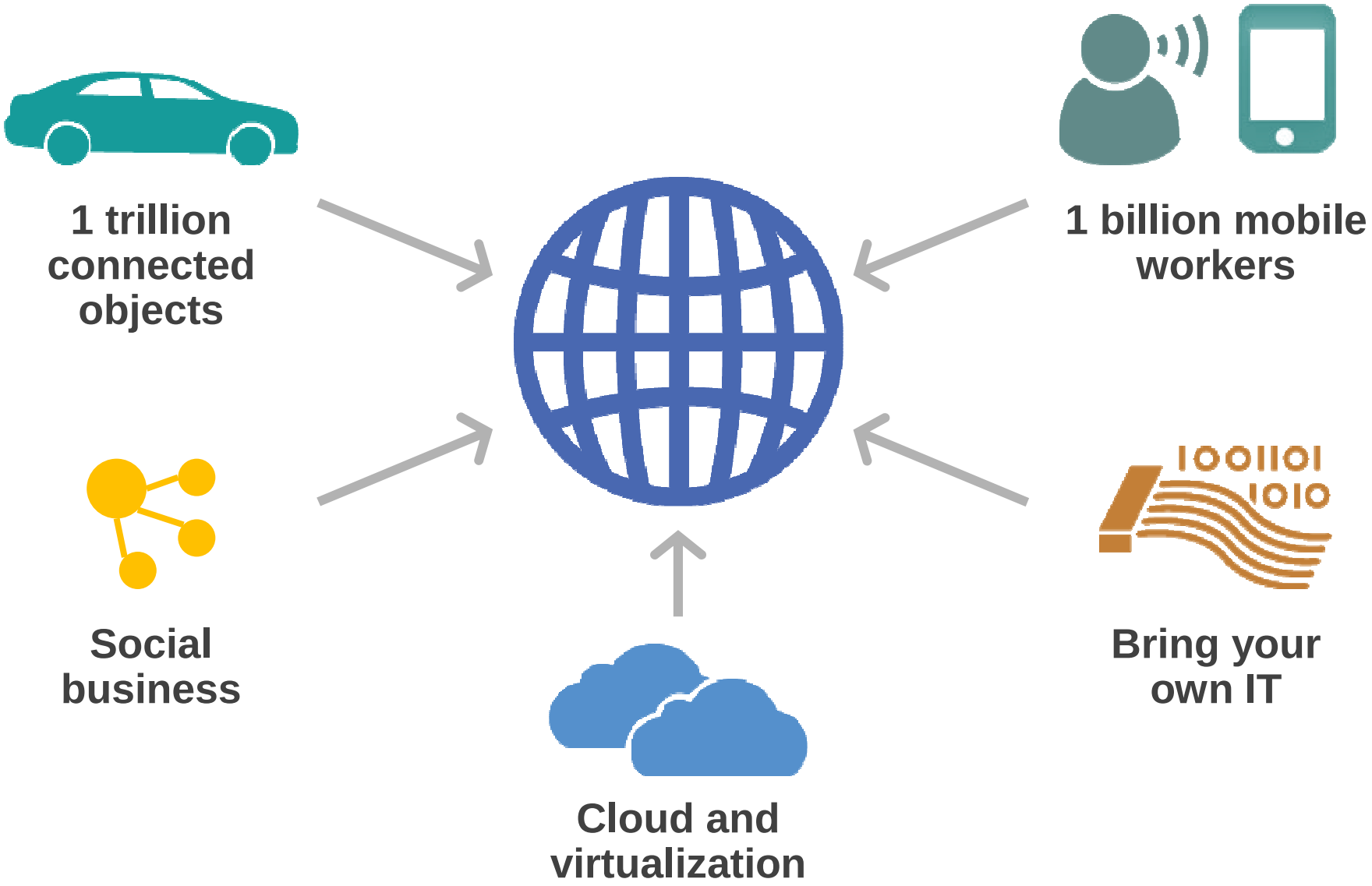


IBM Security Systems
May 2013

Agenda

- **Welcome and Introductions**
- Latest Security trends and 2012 X-Force Report
- Security Intelligence - Understanding your Organizational Security Posture
- Holistic approach to handling Advanced Persistent threats
- Break
- Managing Application Security
- From Identity & Access Management to Identity Intelligence
- Securing your Cloud
- IBM Global Financing

Innovative technology changes everything



Motivations and sophistication are rapidly evolving

National Security

Nation-state actors

Espionage, Activism

Competitors and Hacktivists

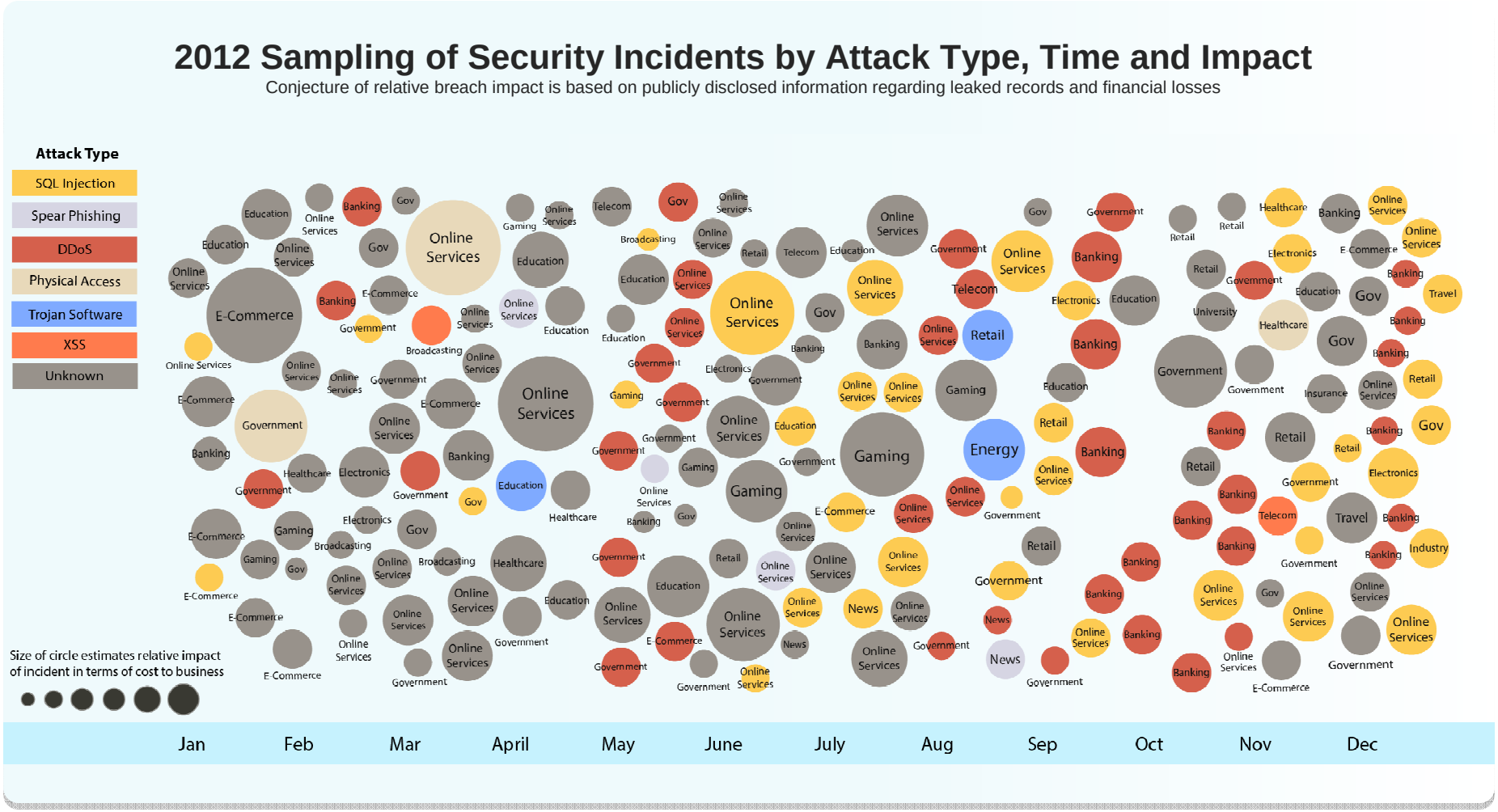
Monetary Gain

Organized crime

Revenge, Curiosity

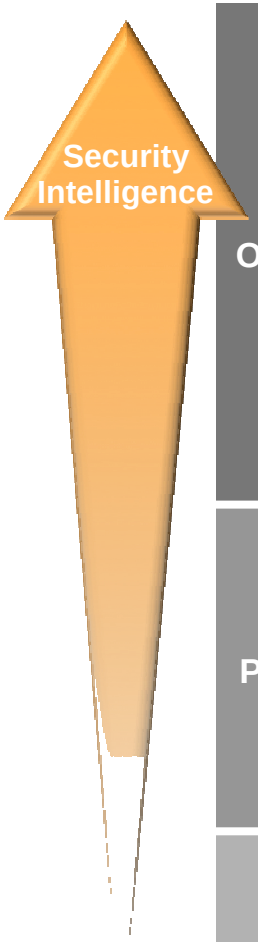
Insiders and Script-kiddies

IBM has tracked a massive rise in advanced and other attacks



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

Intelligent Enterprise Security Approach – Optimized Security



	People	Data	Applications	Infrastructure
	Security Intelligence: Flow analytics / predictive analytics Security information and event management Log management			
Optimized	Identity governance Fine-grained entitlements Privileged user management	Data governance Encryption key management	Fraud detection Hybrid scanning and correlation	Multi-faceted network protection Anomaly detection Hardened systems
Proficient	User provisioning Access management Strong authentication	Data masking / redaction Database activity monitoring Data loss prevention	Web application protection Source code scanning	Virtualization security Asset management Endpoint / network security management
Basic	Directory management	Encryption Database access control	Application scanning	Perimeter security Host security Anti-virus

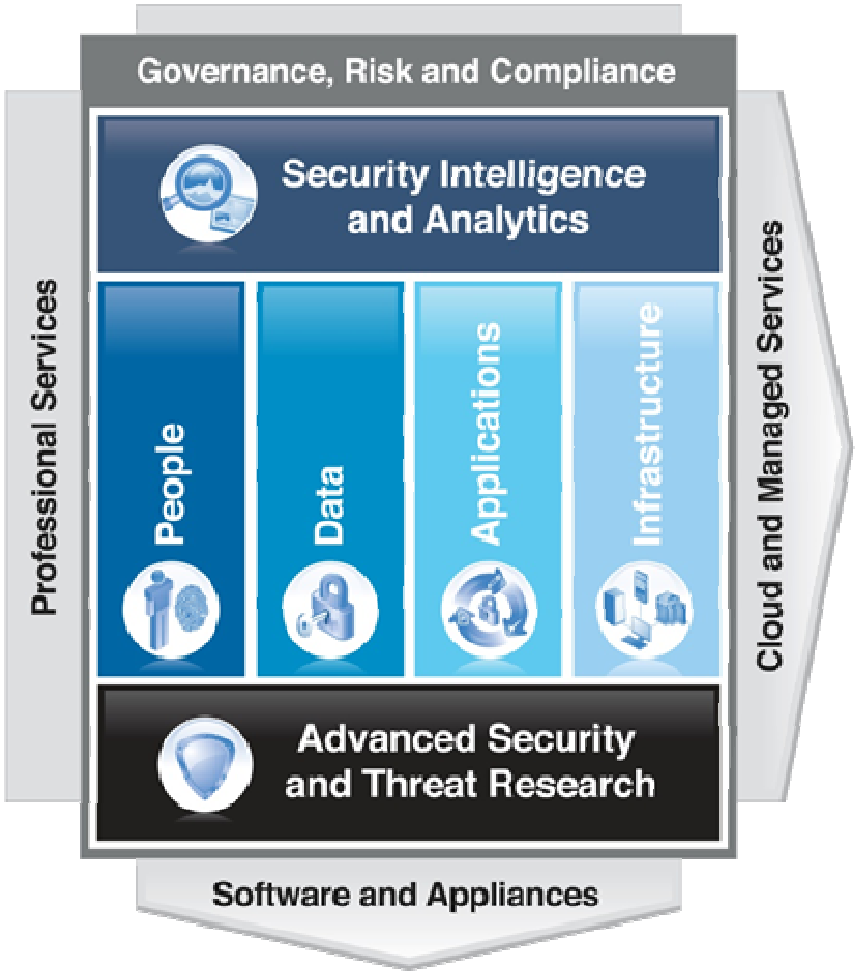
12-01

IBM delivers solutions across a security framework

Intelligence

Integration

Expertise



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.

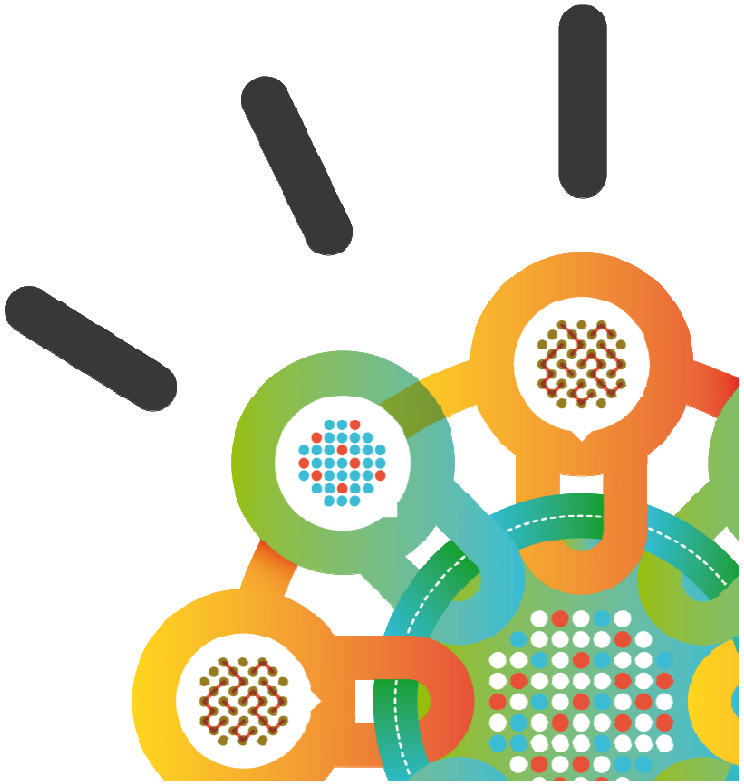
ibm.com/security

Agenda

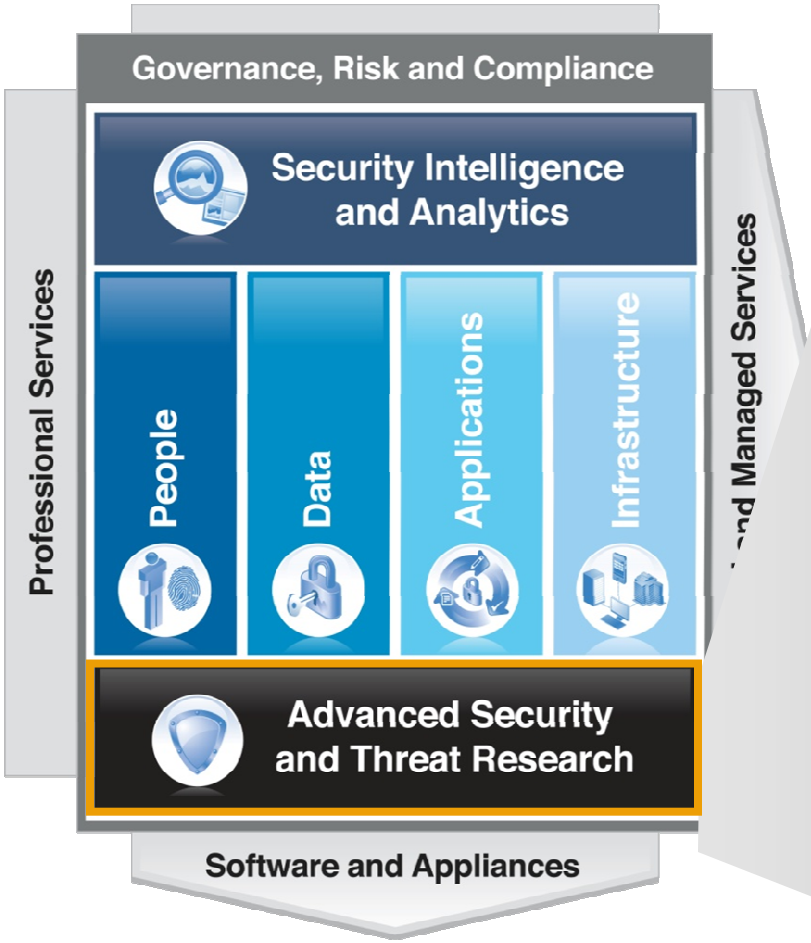
- Welcome and Introductions
- **Latest Security trends and 2012 X-Force Report**
- Security Intelligence - Understanding your Organizational Security Posture
- Holistic approach to handling Advanced Persistent threats
- Break
- Managing Application Security
- From Identity & Access Management to Identity Intelligence
- Securing your Cloud
- IBM Global Financing

Security Intelligence.
Think Integrated.

IBM X-Force 2012 Full-Year Trend and Risk Report



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

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

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

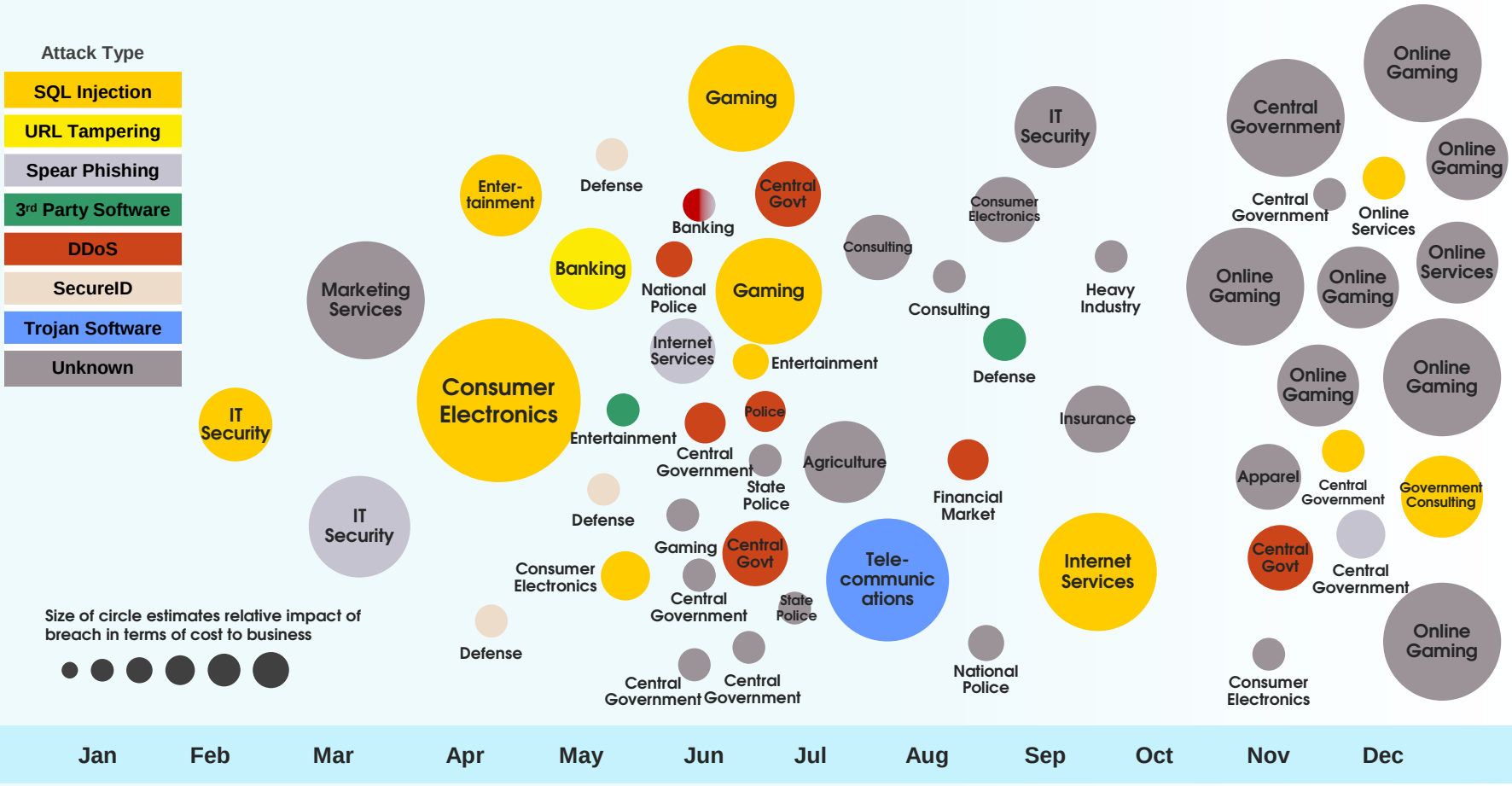
Emerging Trends

- 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"

2011 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

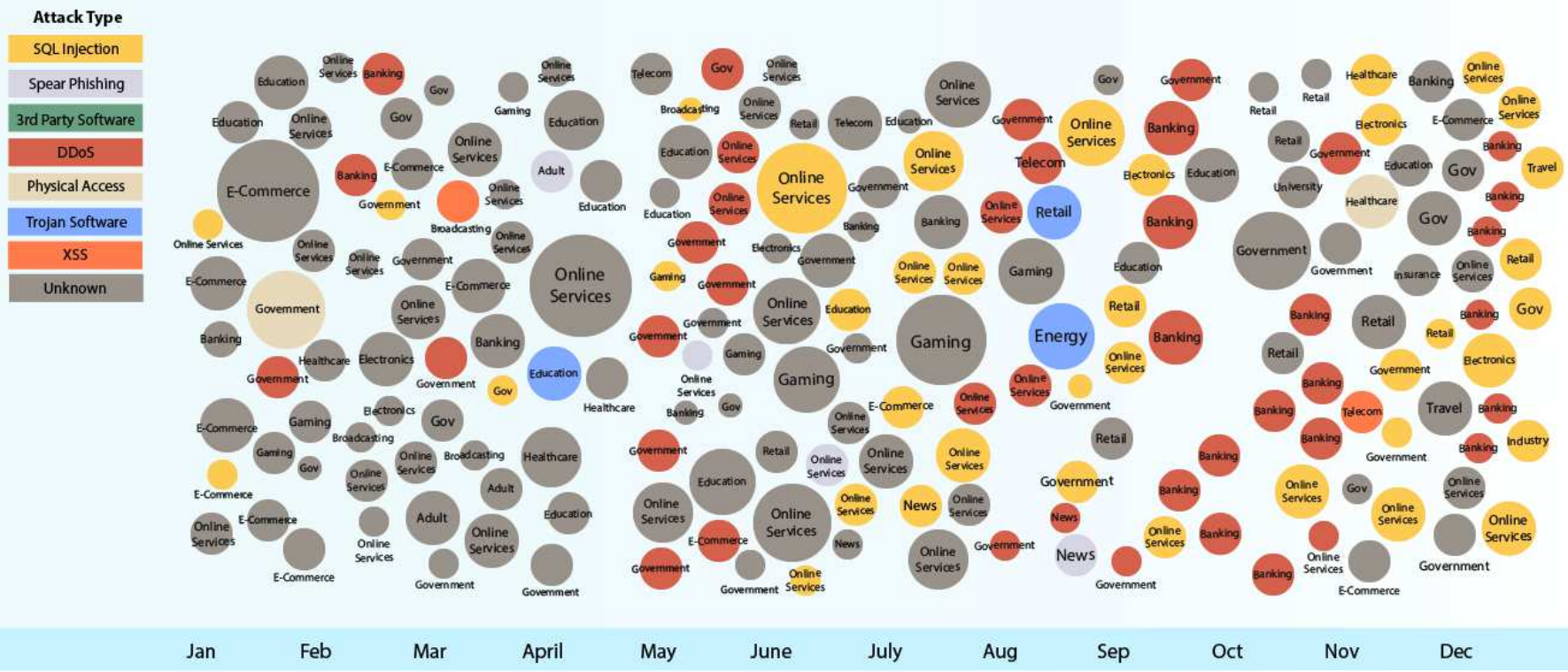


Source: IBM X-Force® Research 2011 Trend and Risk Report

2012: The explosion of breaches continues!

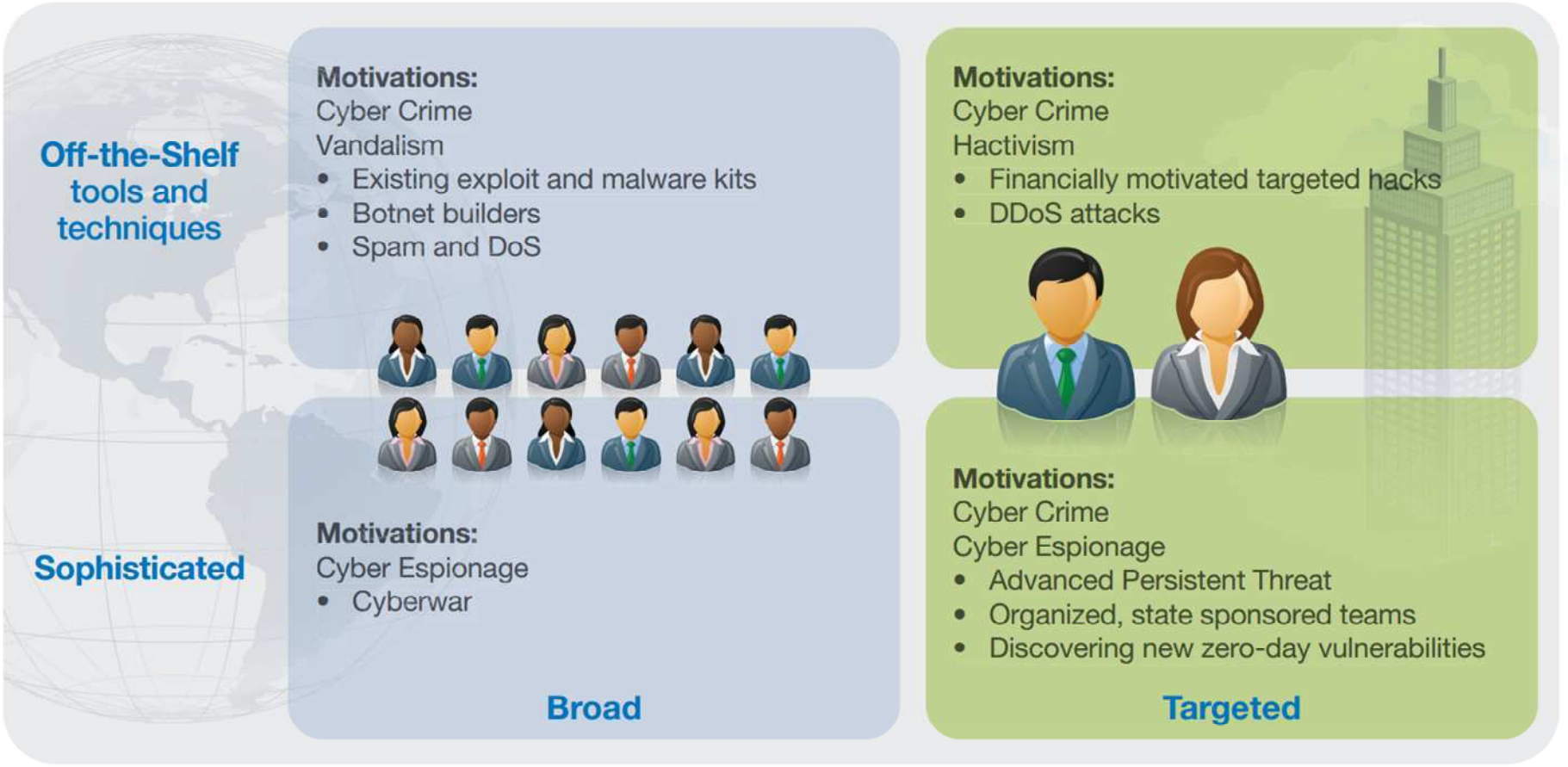
2012 Sampling of Security Incidents by Attack Type, Time and Impact

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

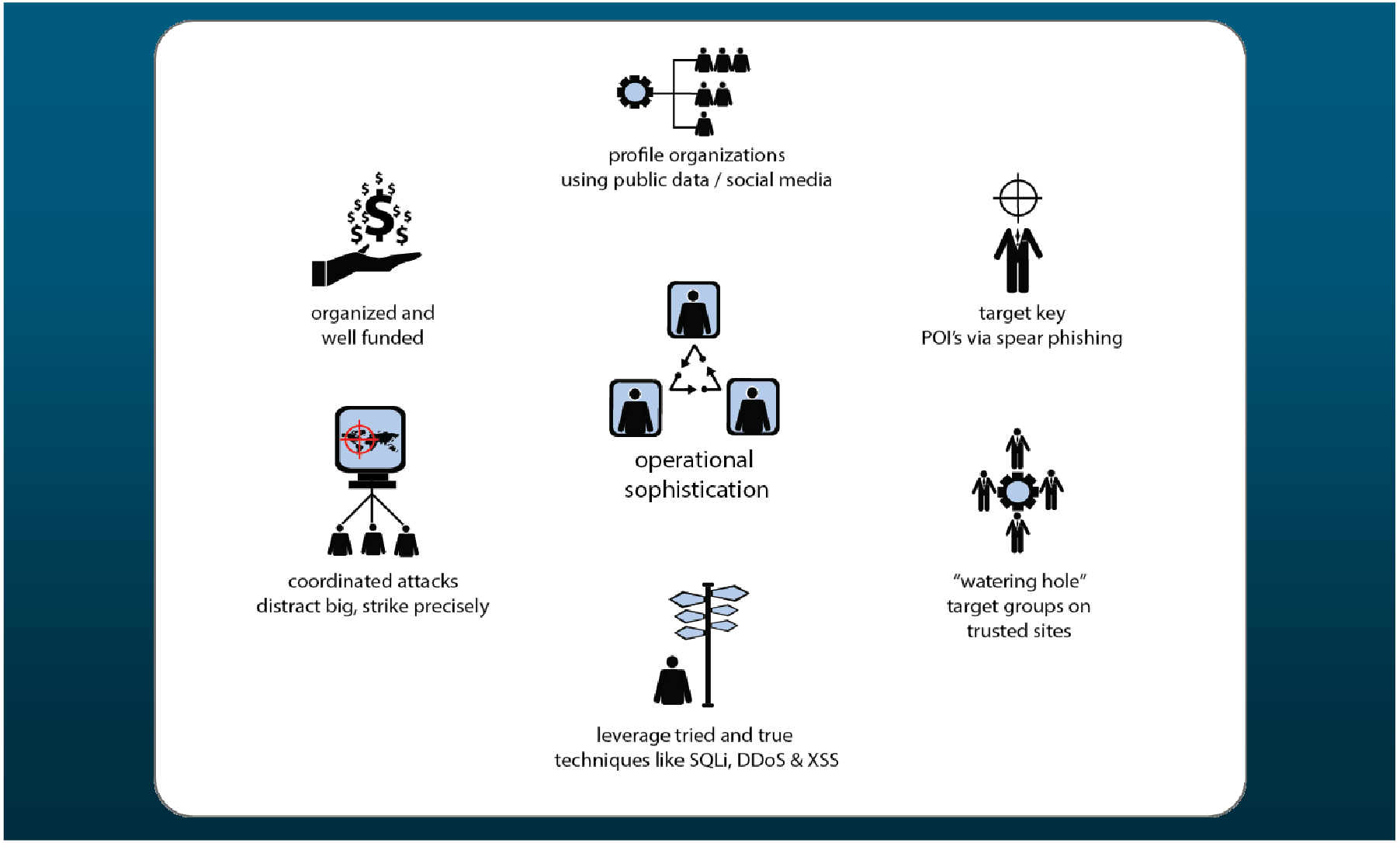


Majority of the security incidents disclosed in 2012 were carried out by attackers going after a broad target base while using off-the-shelf tools and techniques (top left)

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…

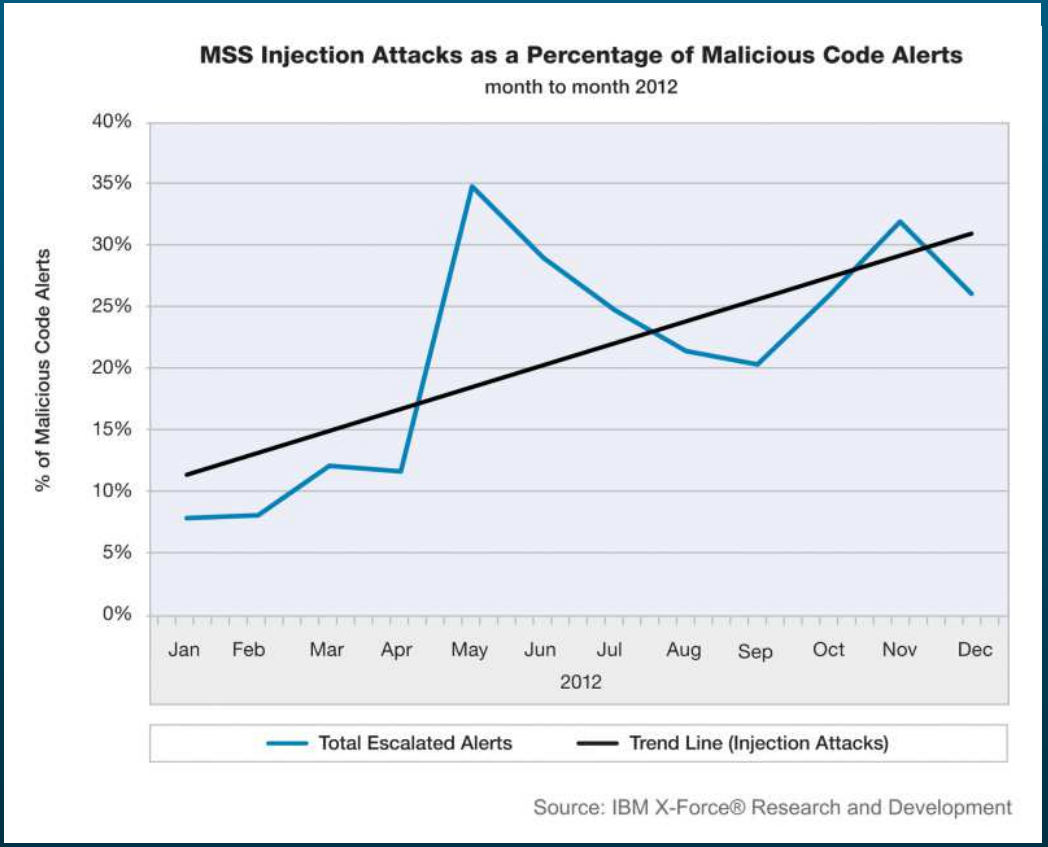
Operational sophistication, not always technology sophistication



Tried and true techniques - SQL and Command Injection attacks

Dramatic and sustained rise in SQL injection-based traffic

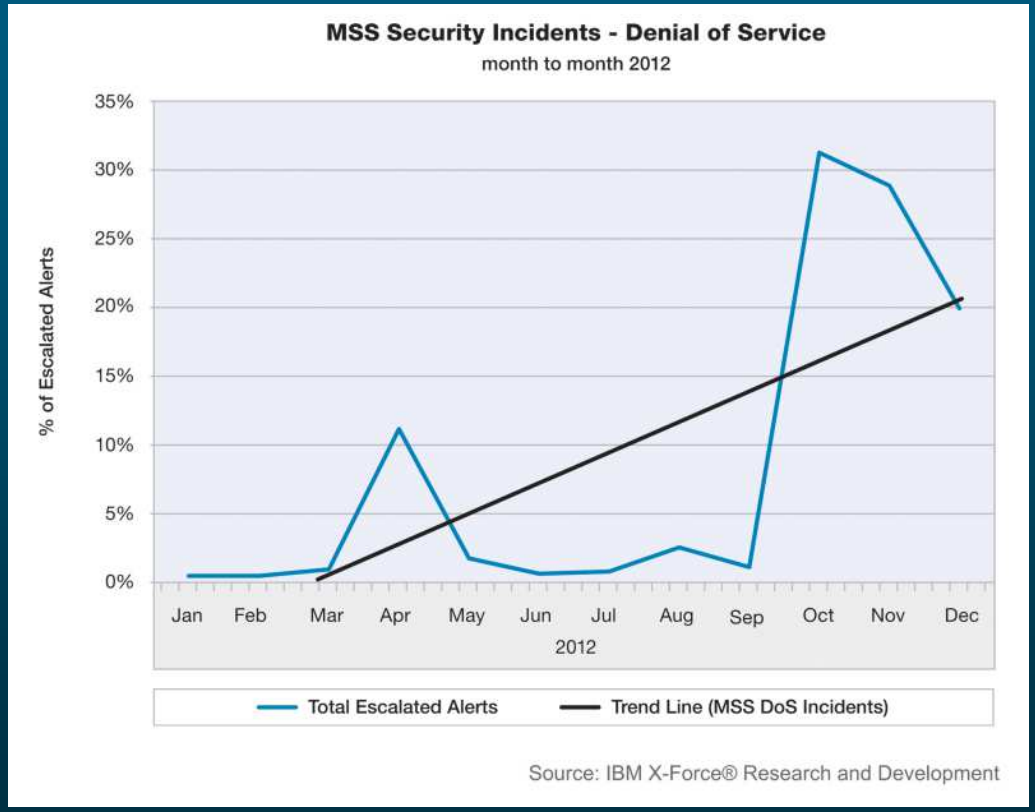
Alerts came from all industry sectors, with a bias toward banking and finance targets



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



Note: SA 2012 Cyber Threat Barometer reported that denial of service (DOS) attacks and the unavailability of ICT were cited as the highest potential cyber threats affecting the Finance and Government sectors and ranked highly for the Telecommunications sector in SA.

Tried and true techniques - Spear-phishing using social networks

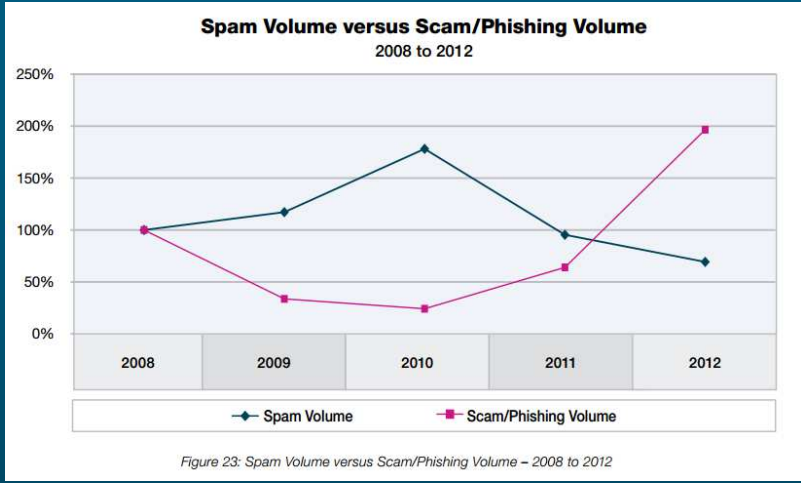


Figure 23: Spam Volume versus Scam/Phishing Volume – 2008 to 2012

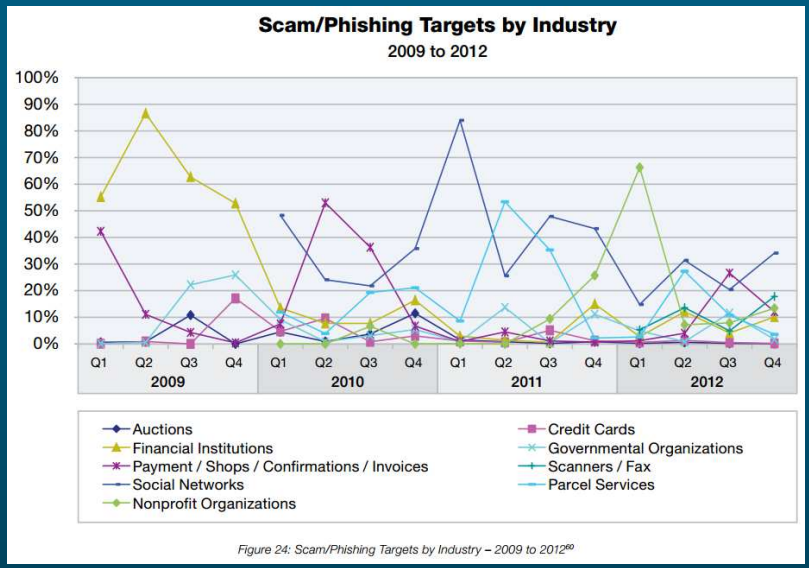


Figure 24: Scam/Phishing Targets by Industry – 2009 to 2012[60]

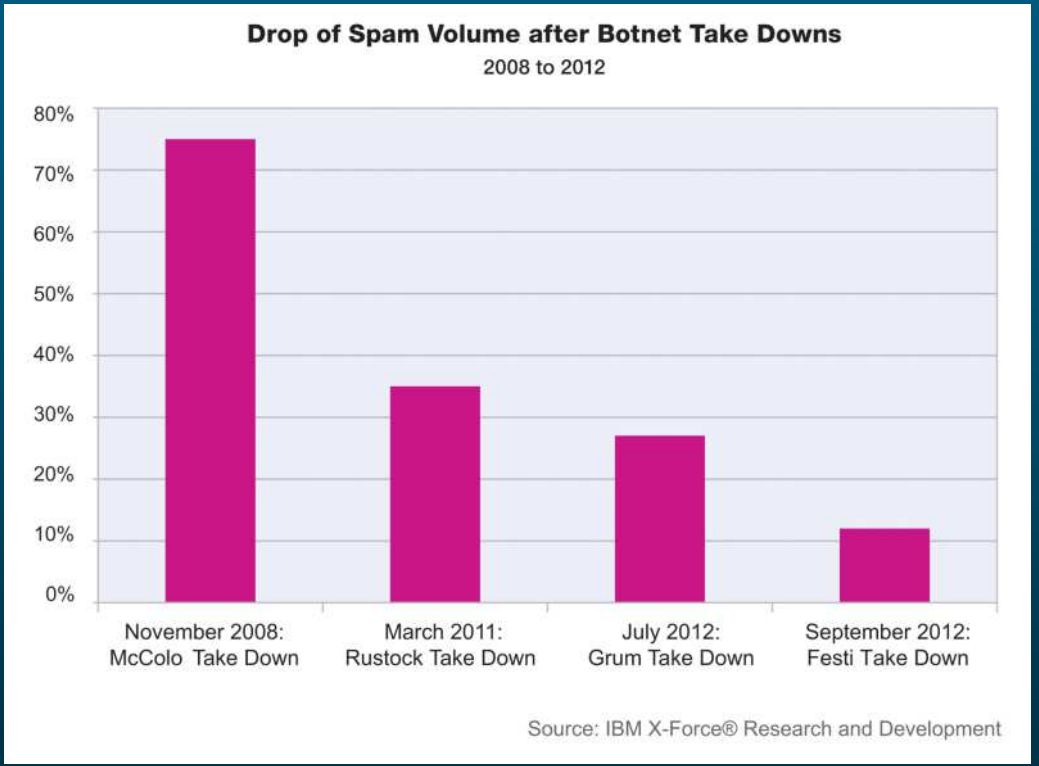
Overall spam volume continues to decline, but **spam containing malicious attachments is on the rise**

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

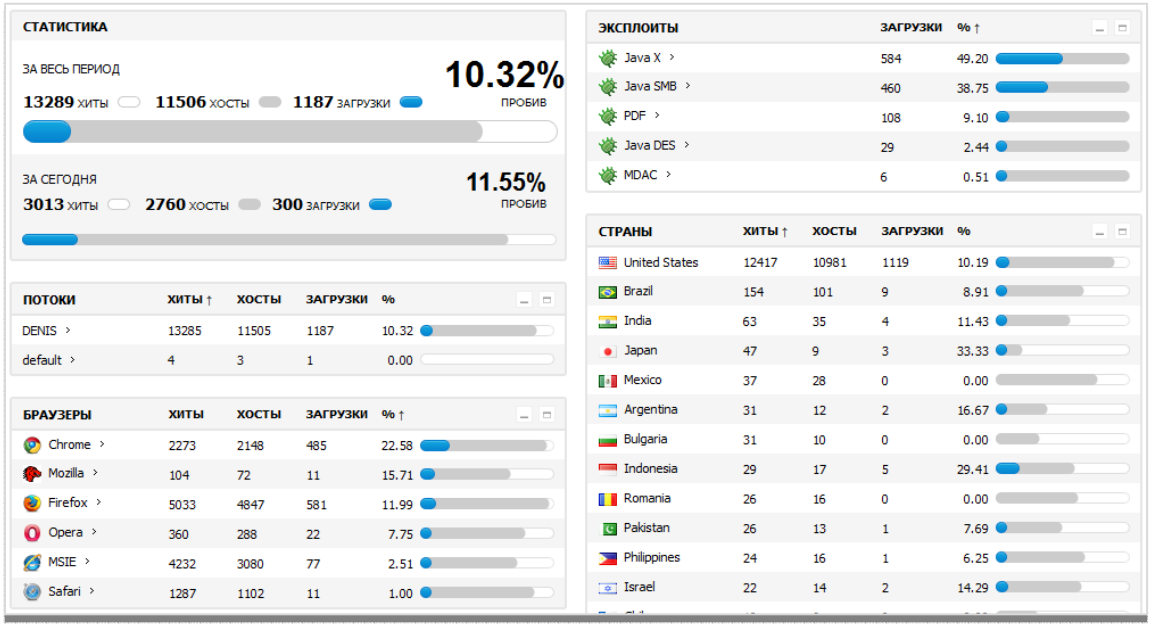


Why was Java one of 2012's hottest software targets?

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



СТАТИСТИКА

ЗА ВЕСЬ ПЕРИОД — 10.32% ПРОБИВ
13289 ХИТЫ | 11506 ХОСТЫ | 1187 ЗАГРУЗКИ

ЗА СЕГОДНЯ — 11.55% ПРОБИВ
3013 ХИТЫ | 2760 ХОСТЫ | 300 ЗАГРУЗКИ

ПОТОКИ

ПОТОКИ	ХИТЫ ↑	ХОСТЫ	ЗАГРУЗКИ	%
DENIS	13285	11505	1187	10.32
default	4	3	1	0.00

БРАУЗЕРЫ

БРАУЗЕРЫ	ХИТЫ	ХОСТЫ	ЗАГРУЗКИ	% ↑
Chrome	2273	2148	485	22.58
Mozilla	104	72	11	15.71
Firefox	5033	4847	581	11.99
Opera	360	288	22	7.75
MSIE	4232	3080	77	2.51
Safari	1287	1102	11	1.00

ЭКСПЛОИТЫ

ЭКСПЛОИТЫ	ЗАГРУЗКИ	% ↑
Java X	584	49.20
Java SMB	460	38.75
PDF	108	9.10
Java DES	29	2.44
MDAC	6	0.51

СТРАНЫ

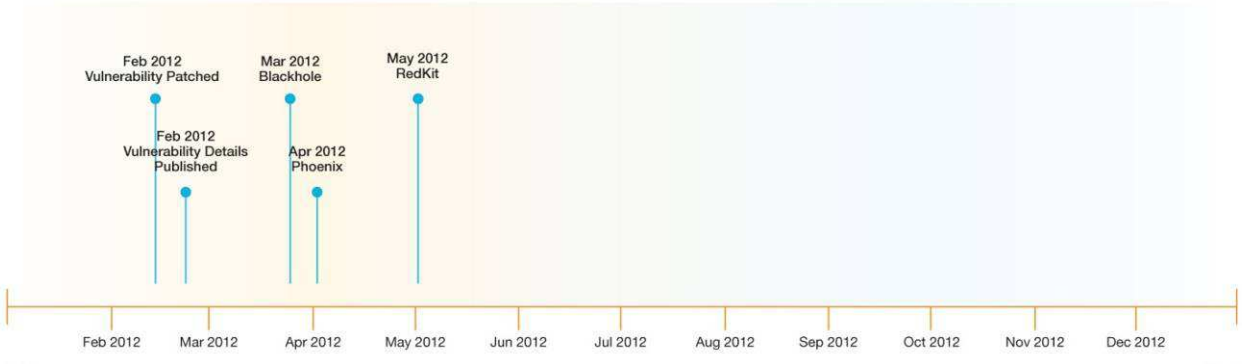
СТРАНЫ	ХИТЫ ↑	ХОСТЫ	ЗАГРУЗКИ	%
United States	12417	10981	1119	10.19
Brazil	154	101	9	8.91
India	63	35	4	11.43
Japan	47	9	3	33.33
Mexico	37	28	0	0.00
Argentina	31	12	2	16.67
Bulgaria	31	10	0	0.00
Indonesia	29	17	5	29.41
Romania	26	16	0	0.00
Pakistan	26	13	1	7.69
Philippines	24	16	1	6.25
Israel	22	14	2	14.29

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

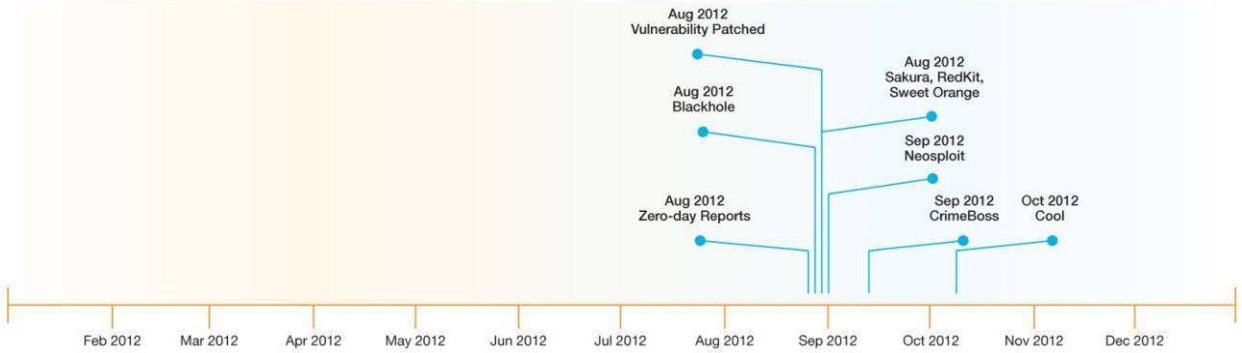
Within 2-3 months, 3-4 exploit kits will have a Java exploit integrated

CVE-2012-0507



CVE-2012-1723

CVE-2012-4681

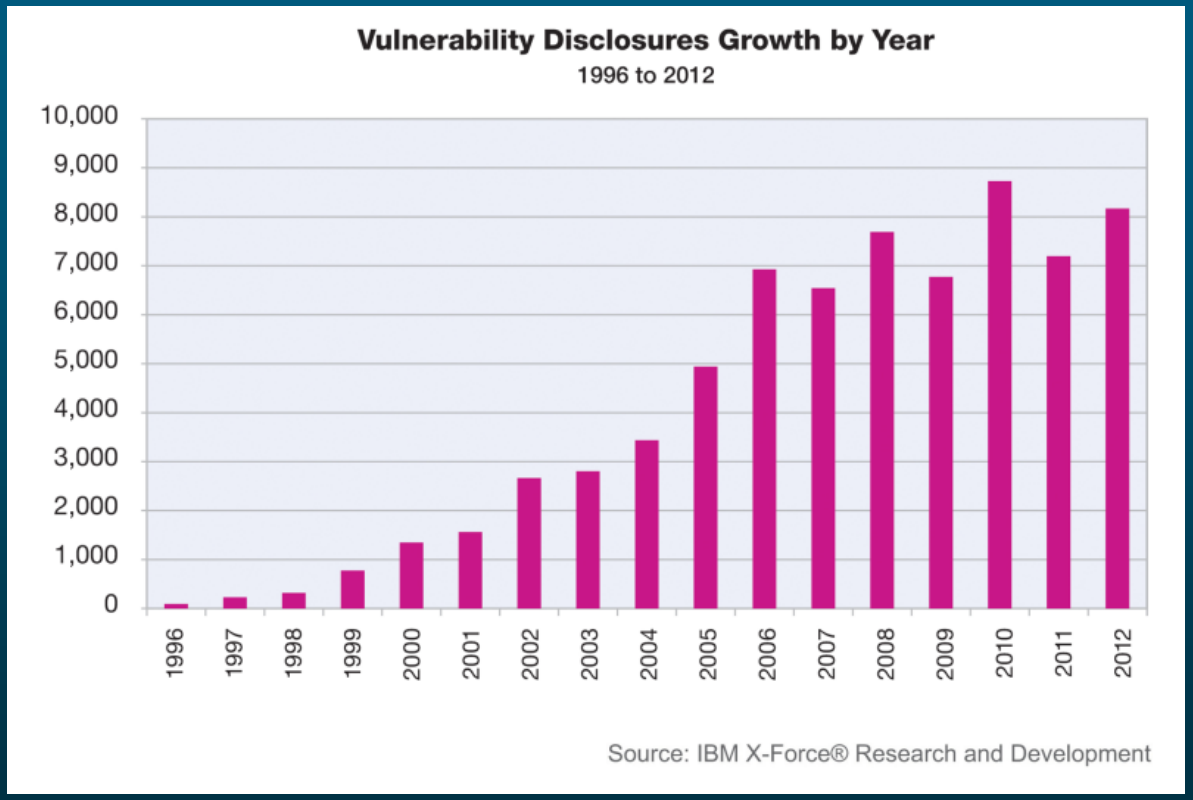


Software vulnerabilities - disclosures up in 2012

8,168

publicly disclosed vulnerabilities

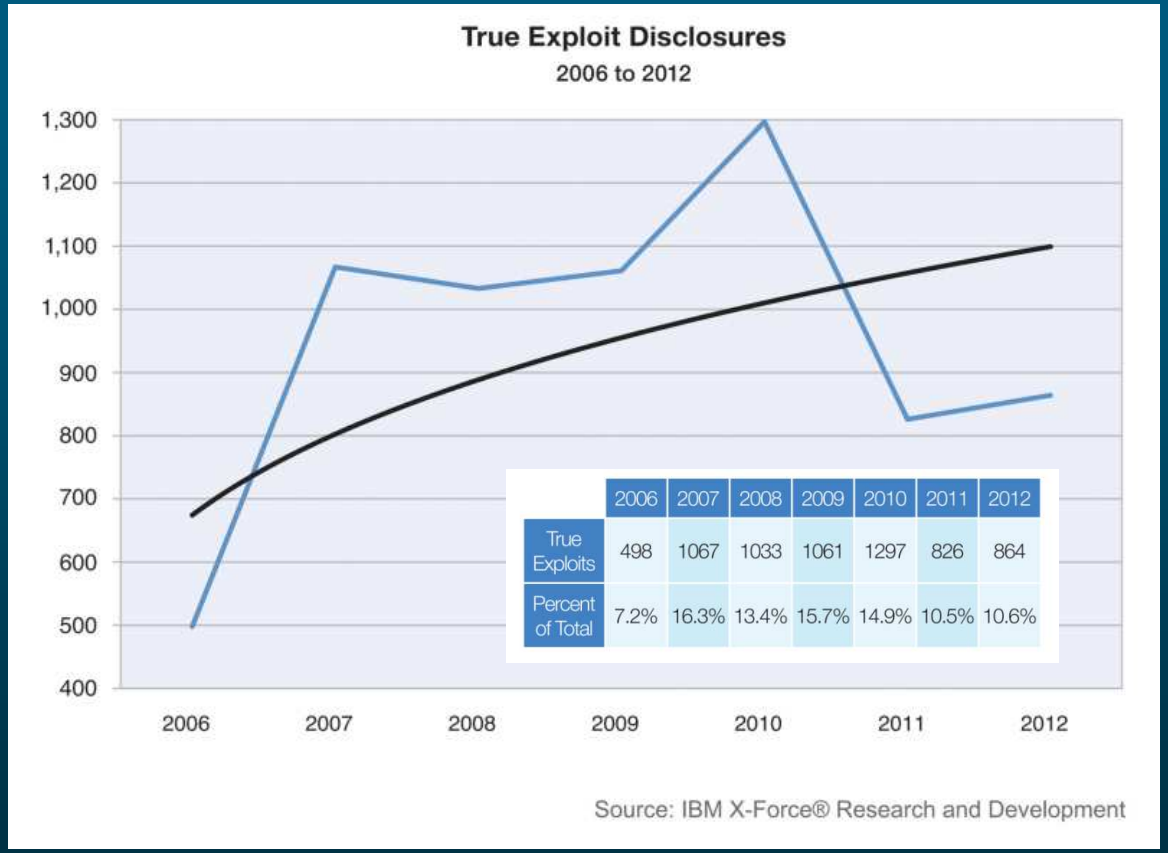
An increase of over 14% from 2011



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%

Source: IBM X-Force® Research and Development

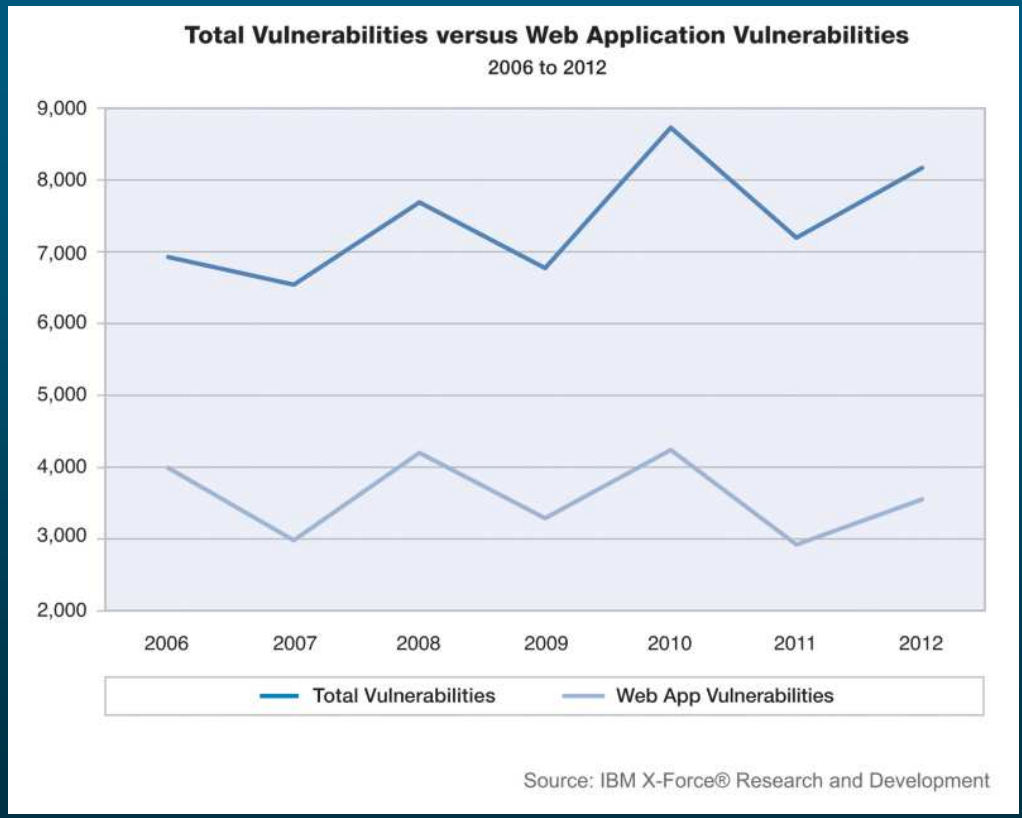
Web application vulnerabilities surge upward

14%

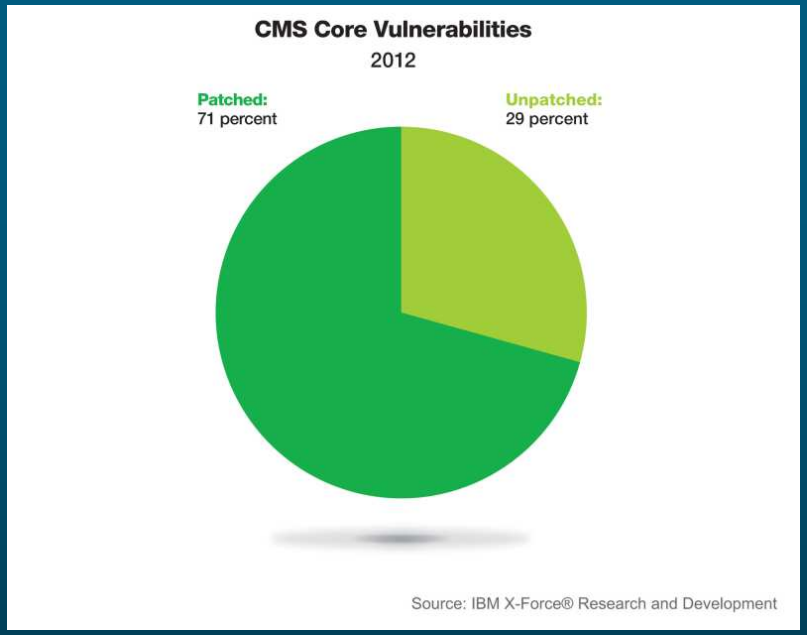
increase in web application vulnerabilities

Cross-site scripting represented

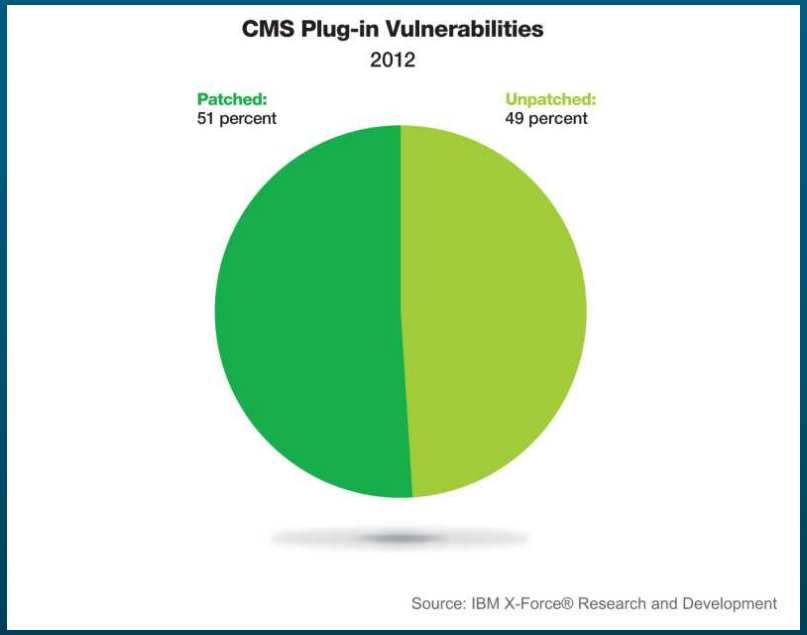
53%



Content Management Systems plug-ins provide soft target



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



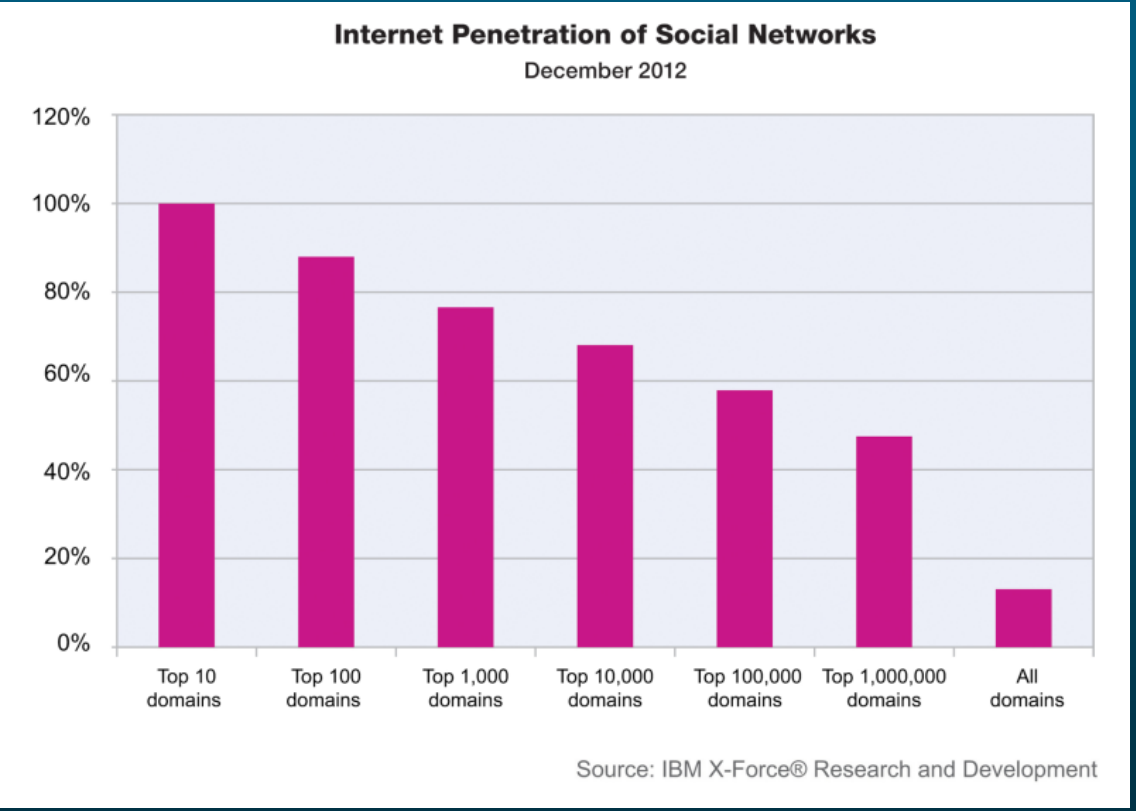
Compared to smaller organizations and individuals producing the add-ons and plug-ins

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)

Get Engaged with IBM X-Force Research and Development

Follow us at @ibmsecurity and @ibmxforce

Download X-Force security trend & risk reports
http://www-03.ibm.com/security/xforce/

Subscribe to X-Force alerts at http://iss.net/rss.php or X-Force Security Insights blog at http://www.ibm.com/blogs/xforce

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.

ibm.com/security

Agenda

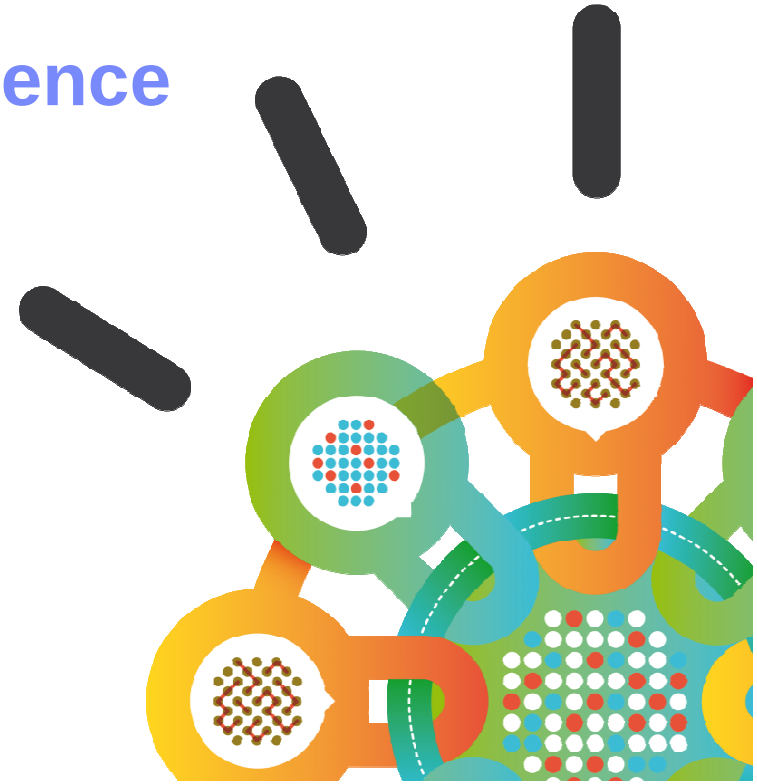
- Welcome and Introductions
- Latest Security trends and 2012 X-Force Report
- **Security Intelligence - Understanding your Organizational Security Posture**
- Holistic approach to handling Advanced Persistent threats
- Break
- Managing Application Security
- From Identity & Access Management to Identity Intelligence
- Securing your Cloud
- IBM Global Financing

Security Intelligence.
Think Integrated.

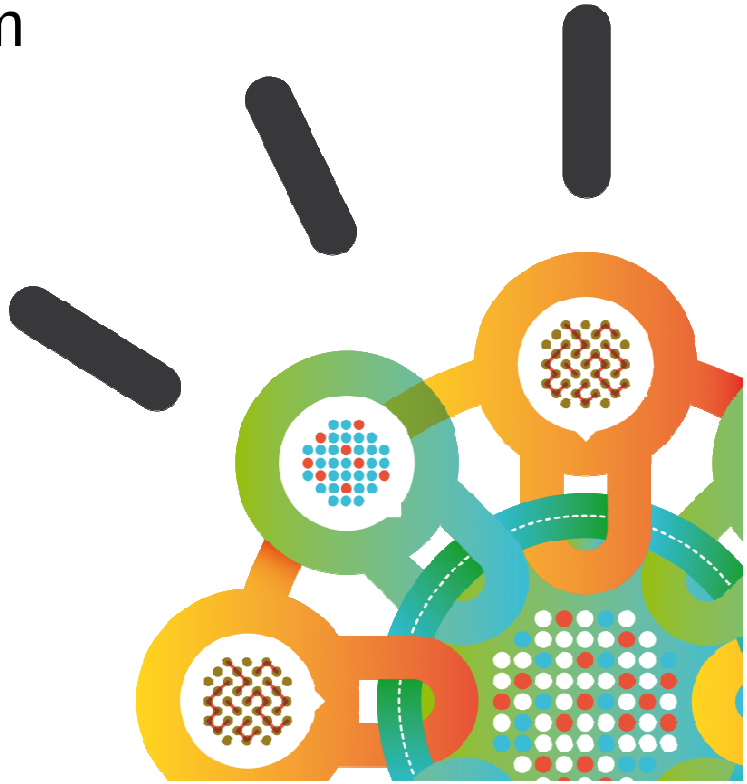
Understanding Your Organizational Security Posture

IBM QRadar Security Intelligence

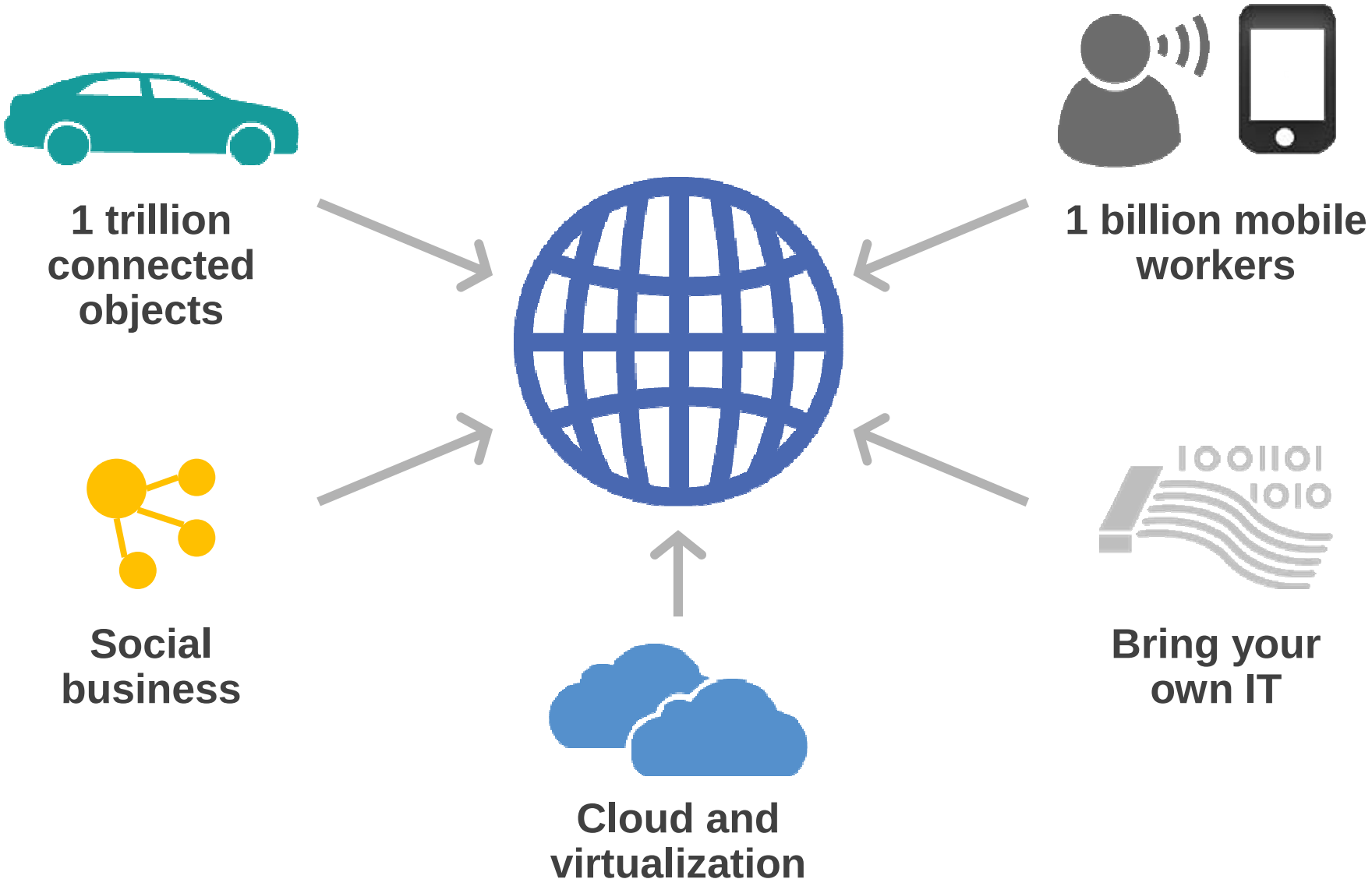
Jon Fraleigh
World Wide Sales Leader for QRadar
jfraleigh@us.ibm.com



- The IT security problem
- Security Intelligence defined
- QRadar Security Intelligence Platform
- QRadar Security use cases
- Case study examples



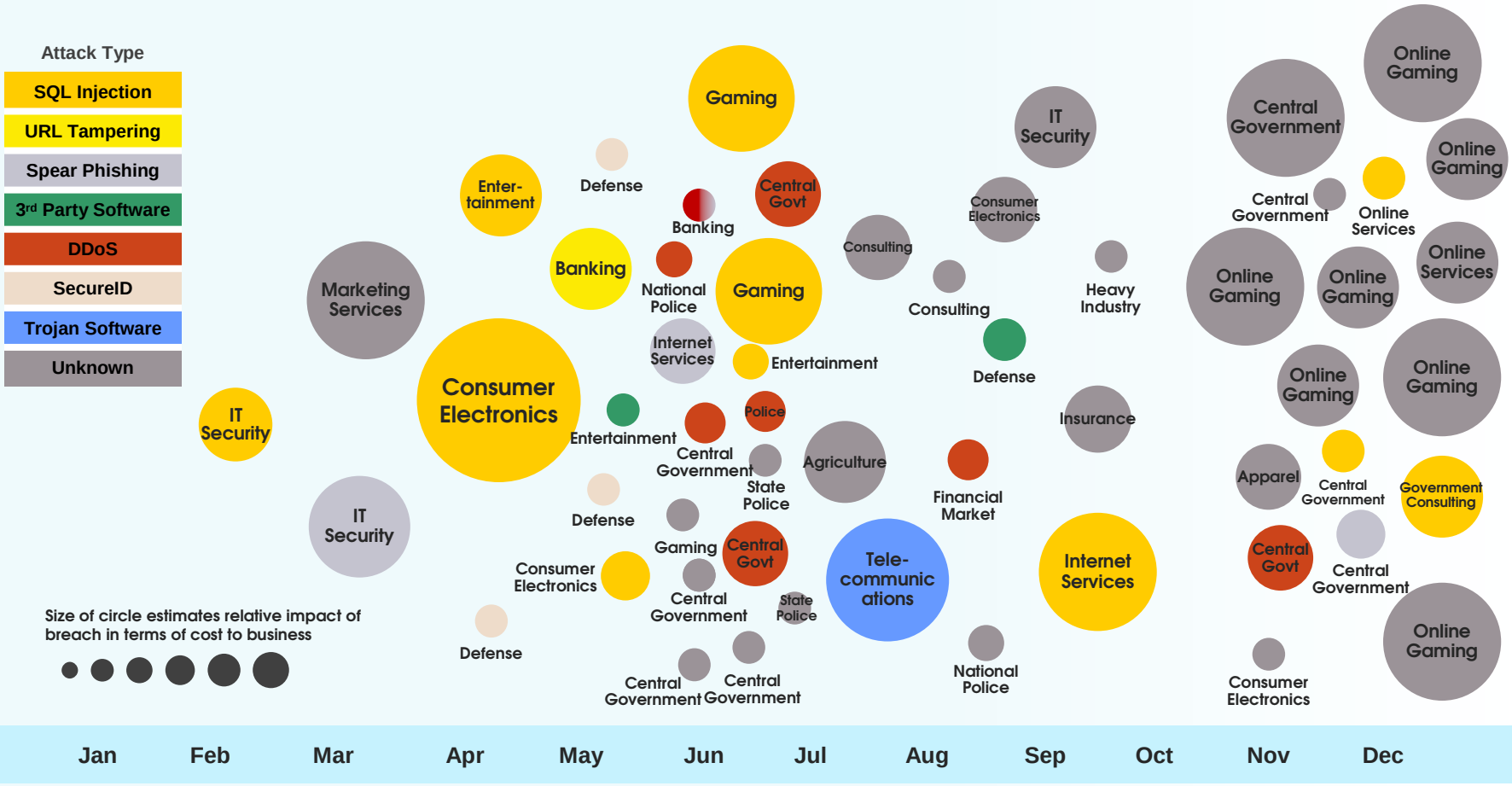
Innovative technology changes everything



2011: "The year of the targeted attack"

2011 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

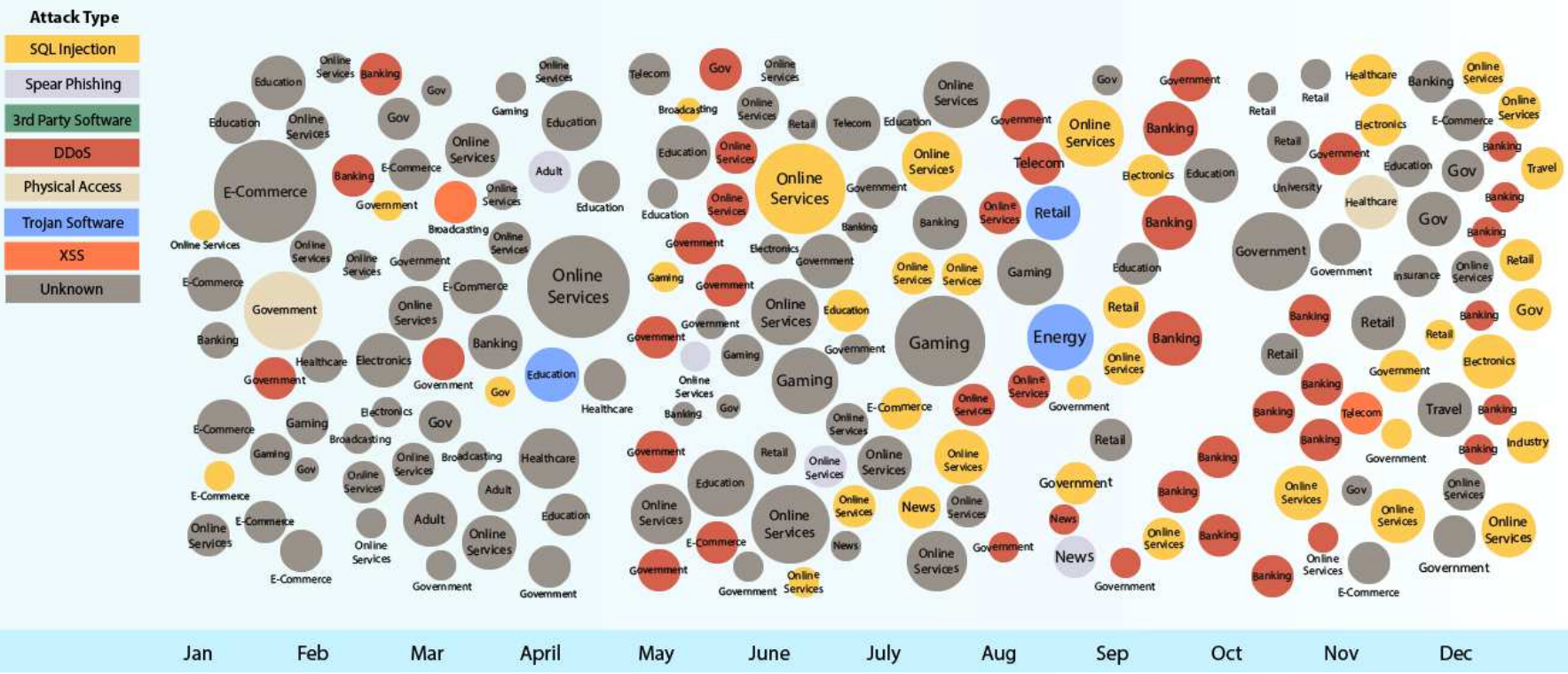


Source: IBM X-Force® Research 2011 Trend and Risk Report

2012: The explosion of breaches continues!

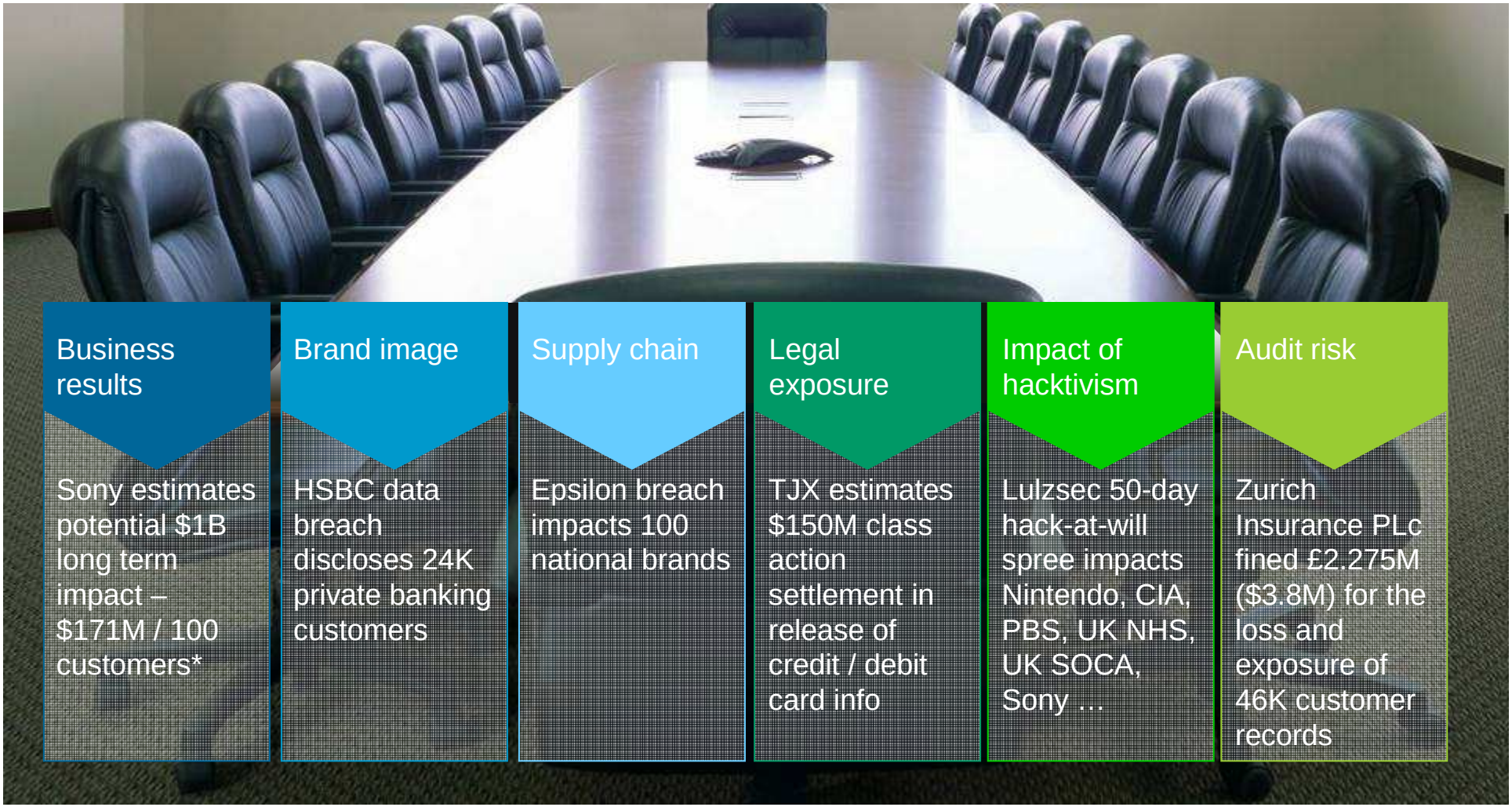
2012 Sampling of Security Incidents by Attack Type, Time and Impact

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

Propelling IT Security to a board room discussion



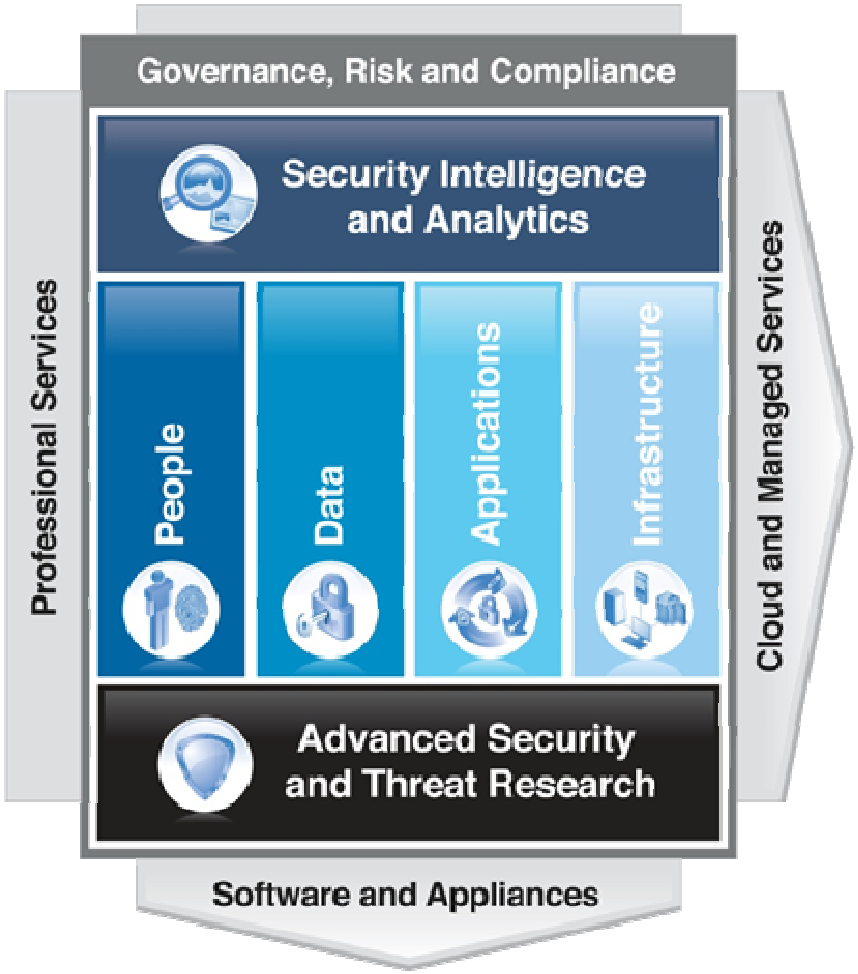
 *Sources for all breaches shown in speaker notes

IBM delivers solutions across a security framework

Intelligence

Integration

Expertise



Security Intelligence defined

What is Security Intelligence?

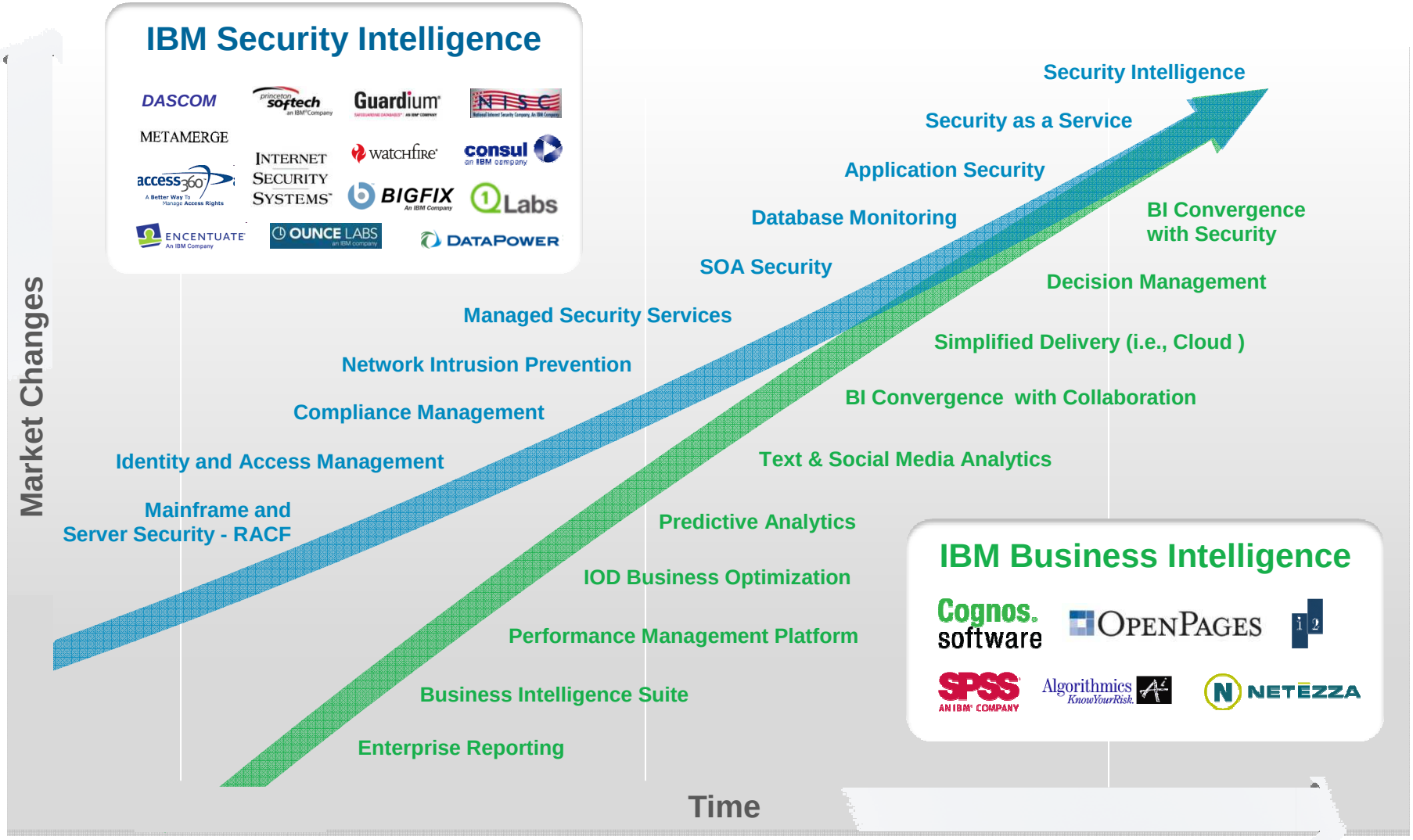
Security Intelligence

--noun

1. the real-time collection, normalization and analytics of the data generated by users, applications and infrastructure that impacts the IT security and risk posture of an enterprise

Security Intelligence provides actionable and comprehensive insight for managing risks and threats from protection and detection through remediation

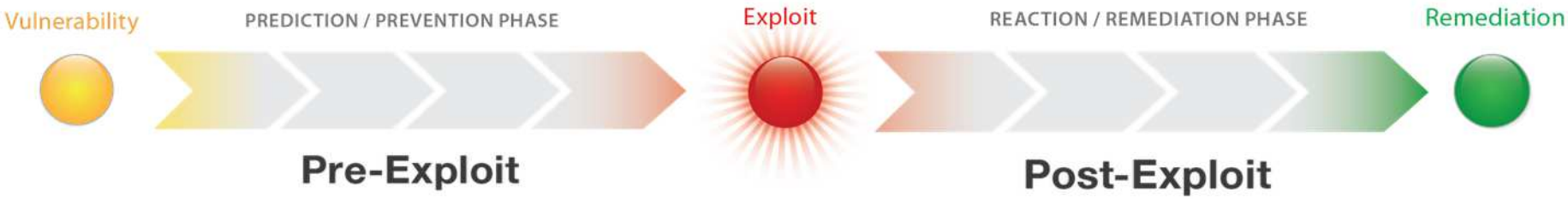
Security Intelligence & Business Intelligence offer insightful parallels



QRadar Security Intelligence Platform

Solutions for the full Security Intelligence timeline

What are the external and internal threats? → **Are we configured to protect against these threats?** → **What is happening right now?** → **What was the impact?**



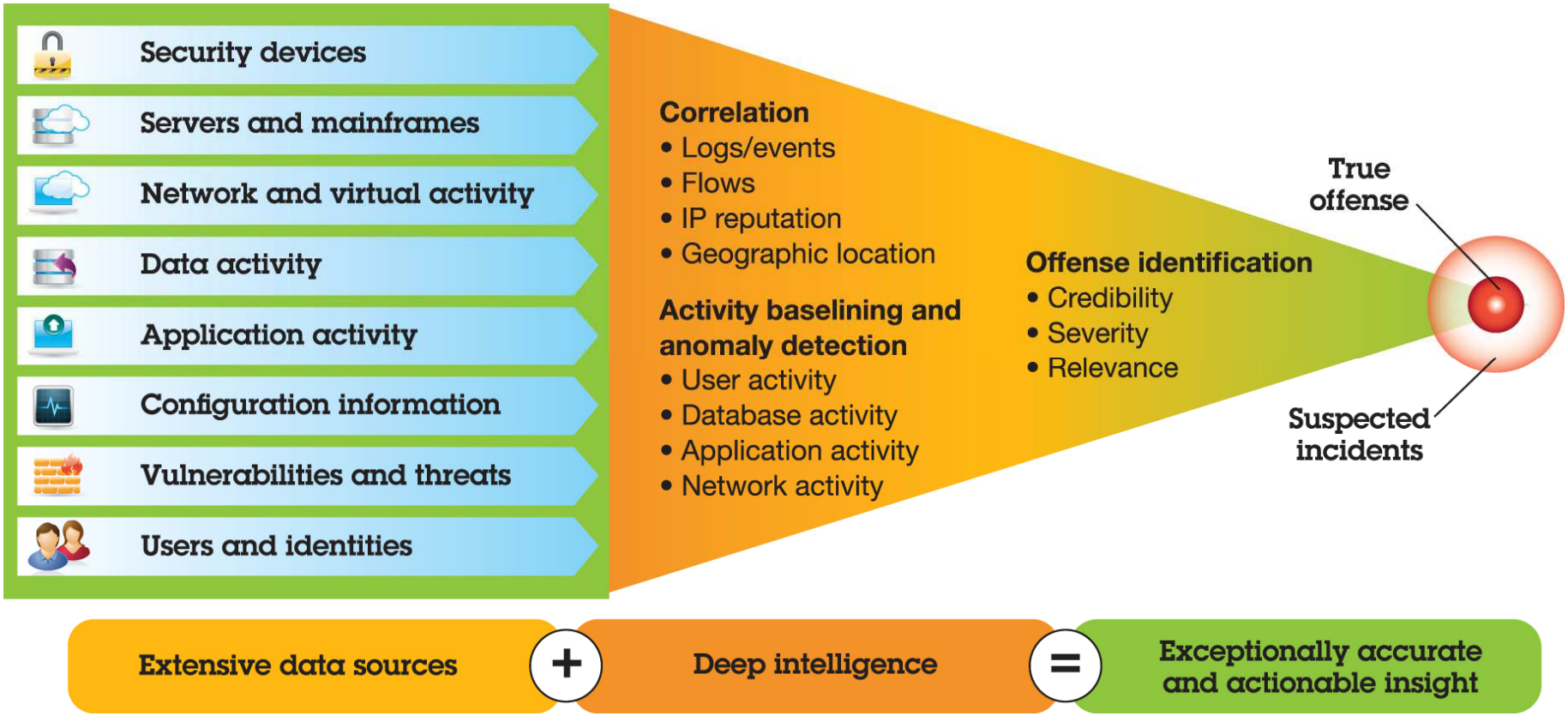
Prediction & Prevention

Risk Management. Vulnerability Management.
Configuration and Patch Management.
X-Force Research and Threat Intelligence.
Compliance Management.
Reporting and Scorecards.

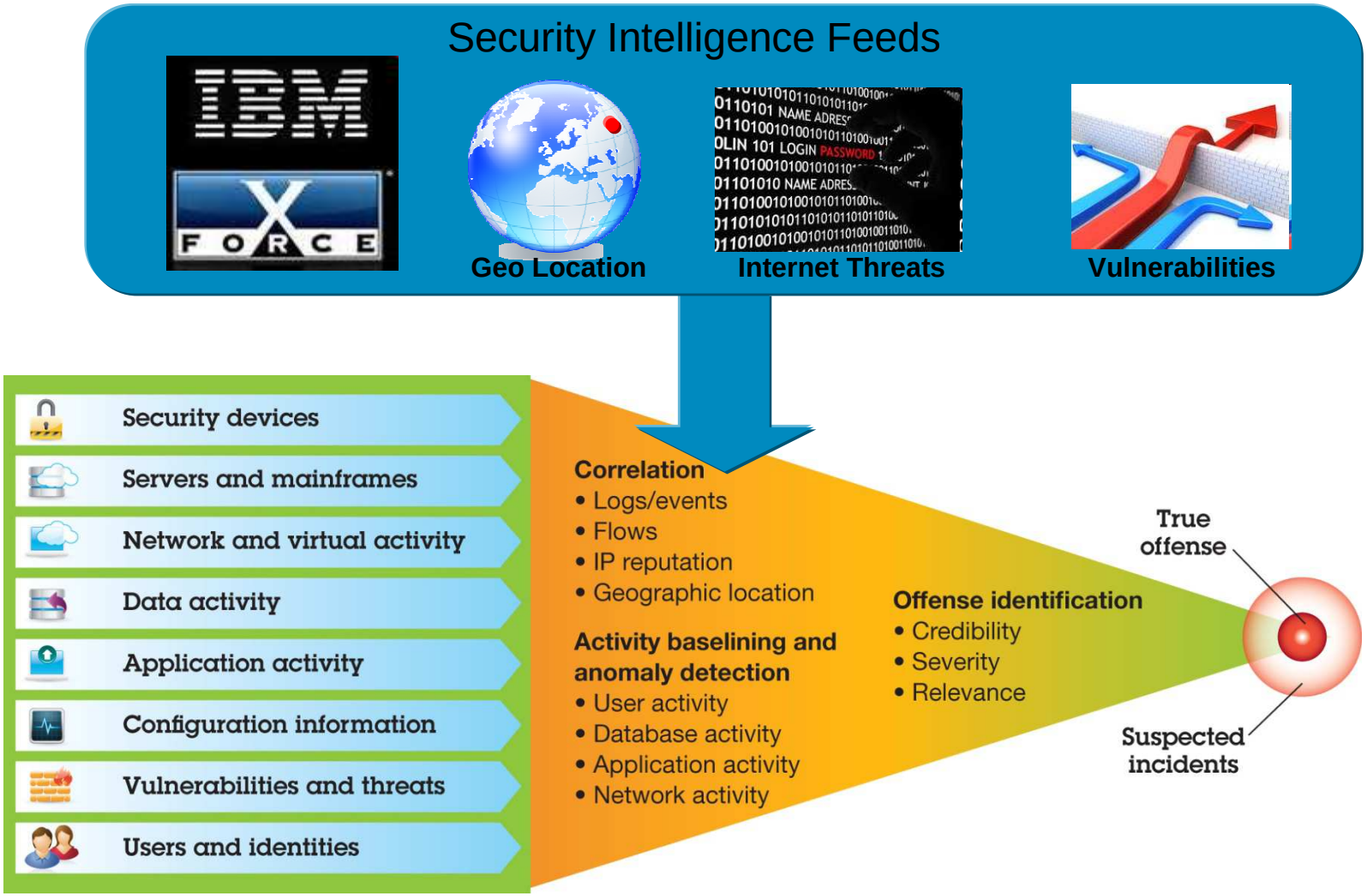
Reaction & Remediation

Network and Host Intrusion Prevention.
Network Anomaly Detection. Packet Forensics.
Database Activity Monitoring. Data Leak Prevention.
Security Information and Event Management.
Log Management. Incident Response.

Taking in data from wide spectrum of feeds



And continually adding context for increased accuracy



Deployed upon scalable appliance architecture

Log Management	QRadar® Log Manager 	• Turn-key log management and reporting • SME to Enterprise • Upgradeable to enterprise SIEM
SIEM	QRadar® SIEM 	• Log, flow, vulnerability & identity correlation • Sophisticated asset profiling • Offense management and workflow
Configuration & Vulnerability Management	QRadar® Risk Manager 	• Network security configuration monitoring • Vulnerability prioritization • Predictive threat modeling & simulation
Network Activity & Anomaly Detection	QRadar® SIEM  QRadar QFlow 	• Network analytics • Behavioral anomaly detection • Fully integrated in SIEM
Network and Application Visibility	QRadar QFlow  QRadar VFlow 	• Layer 7 application monitoring • Content capture for deep insight & forensics • Physical and virtual environments
Scale		• Event Processors • Network Activity Processors • High Availability & Disaster Recovery • Stackable Expansion

Using fully integrated architecture and interface

- Log Management
- SIEM
- Configuration & Vulnerability Management
- Network Activity & Anomaly Detection
- Network and Application Visibility

One Console Security

Built on a Single Data Architecture

QRadar's unique advantages

- Scalability for largest deployments, using an embedded database and unified data architecture
  - ➢ *Impact: QRadar supports your business needs at any scale*

- Real-time correlation and anomaly detection based on broadest set of contextual data
  - ➢ *Impact: More accurate threat detection, in real-time*

- Intelligent automation of data collection, asset discovery, asset profiling and more
  - ➢ *Impact: Reduced manual effort, fast time to value, lower-cost operation*

- Integrated flow analytics with Layer 7 content (application) visibility
  - ➢ *Impact: Superior situational awareness and threat identification*

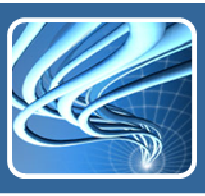
- Flexibility and ease of use enabling "mere mortals" to create and edit correlation rules, reports and dashboards
  - ➢ *Impact: Maximum insight, business agility and lower cost of ownership*

Security Intelligence Use Cases

Overview of use cases

Detecting threats

- Arm yourself with comprehensive security intelligence



Consolidating data silos

- Collect, correlate and report on data in one integrated solution

Detecting insider fraud

- Next-generation SIEM with identity correlation

Better predicting risks to your business

- Full life cycle of compliance and risk management for network and security infrastructures

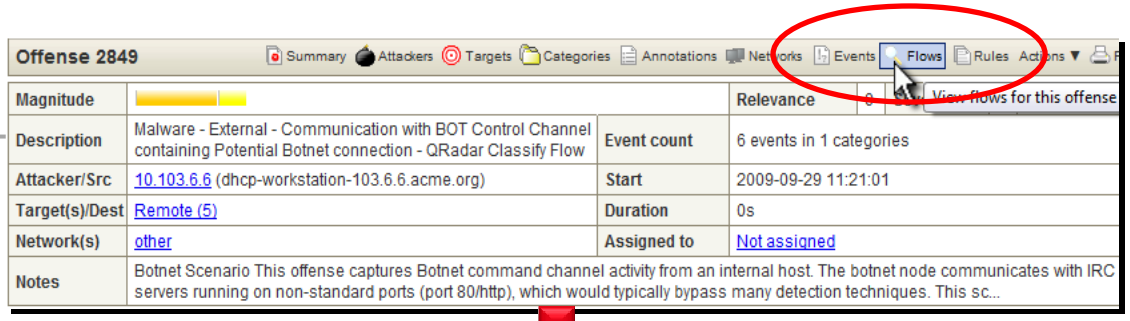
Addressing regulation mandates

- Automated data collection and configuration audits

Challenge 1: Detecting Threats

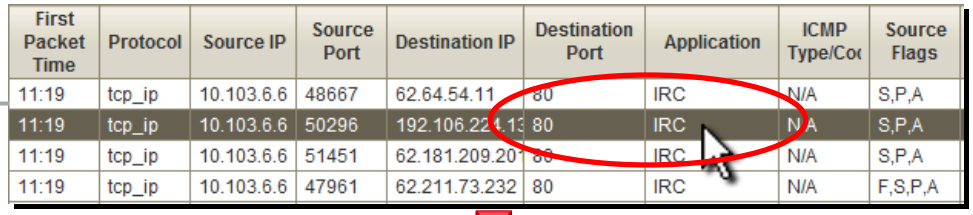
Potential Botnet Detected?

This is as far as traditional SIEM can go



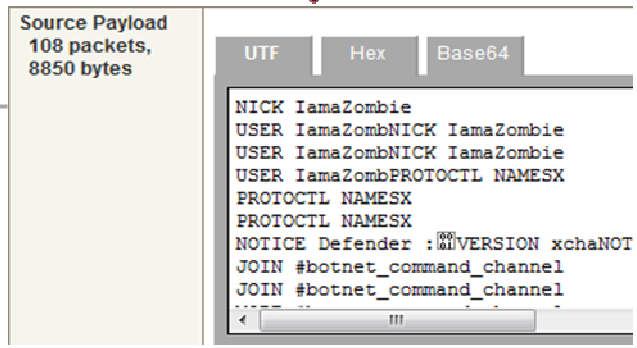
IRC on port 80?

IBM Security QRadar QFlow detects a covert channel



Irrefutable Botnet Communication

Layer 7 flow data contains botnet command control instructions



Application layer flow analysis can detect threats others miss

Challenge 2: Consolidating Data Silos

System Summary	
Current Flows Per Second	1.4M
Flows (Past 24 Hours)	1.3M
Current Events Per Second	17,384
New Events (Past 24 Hours)	677M
Updated Offenses (Past 24 Hours)	588
Data Reduction Ratio	1153571 : 1

Analyzing both flow and event data. Only IBM Security QRadar fully utilizes Layer 7 flows.

Reducing big data to manageable volumes

Advanced correlation for analytics across silos

Offense 160 Display ▼ Events Connections Flows View Attack Path Actions ▼ Print

Magnitude		Relevance 5	Severity 10 Credibility 8
Description	Destination Vulnerable to Detected Exploit preceded by Exploit/Malware Events Across Multiple Targets preceded by Aggressive Remote Scanner Detected	Offense Type	Source IP
		Event/Flow count	19984 events and 355 flows in 12 categories.
Source IP(s)	202.153.48.66	Start	2010-10-01 07:51:00
Destination IP(s)	Local (315)	Duration	2m 52s
Network(s)	Multiple (2)	Assigned to	Not assigned

Notes

Vulnerability Correlation Use Case
Illustrates a scenario involving correlation of vulnerability data with IDS alerts

An attacker originating from China (202.153.48.66) sweeps a subnet using the Conficker worm exploit (CVE 2008-4250).

The first systems scanned are not vulnerable, but the final system's asset profile has had vulnerability data imported from a Ne

Extensive Data Sources + Deep Intelligence = Exceptionally Accurate and Actionable Insight

Challenge 3: Detecting Insider Fraud

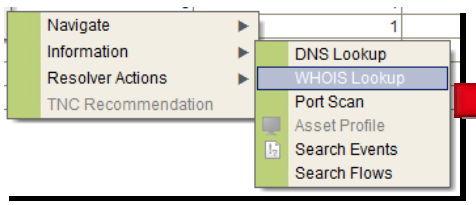
Potential Data Loss
Who? What? Where?

Magnitude	
Description	Potential Data Loss/Theft Detected
Attacker/Src	10.103.14.139 (dhcp-workstation-103.14.139.acme.org)
Target(s)/Dest	Local (2) Remote (1)
Network(s)	Multiple (3)
Notes	Data Loss Prevention Use Case. Demonstrates QRadar DL authentication ...

	Event Name	Source IP (Unique Count)	Log Source (Unique Count)	Username (Unique Count)	Category (Unique Count)
	Authentication Failed	10.103.14.139	OracleDbAudit @ 10.101.145.198	Multiple (2)	Misc Login Failed
	Misc Login Succeeded	10.103.14.139	OracleDbAudit @ 10.101.145.198	scott	Misc Login Succeeded
	DELETE failed	10.103.14.139	OracleDbAudit @ 10.101.145.198	scott	System Action Deny
	SELECT succeeded	10.103.14.139	OracleDbAudit @ 10.101.145.198	scott	System Action Allow
	Misc Logout	10.103.14.139	OracleDbAudit @ 10.101.145.198	scott	Misc Logout
	Suspicious Pattern Detec	10.103.14.139	Custom Rule Engine-8 :: qradar-vn	N/A	Suspicious Pattern Detected
	Remote Access Login Fa	10.103.14.139	Custom Rule Engine-8 :: qradar-vn	N/A	Remote Access Login Failed

Who?
An internal user

What?
Oracle data



QRadar Has Completed Your Request

Go to APNIC results

[Querying whois.arin.net]
[whois.arin.net]

OrgName: Google Inc.
OrgID: GOGL

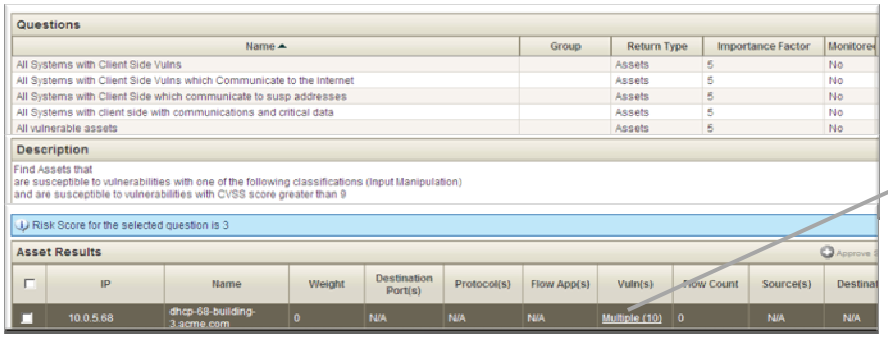
Where?
Gmail

Threat detection in the post-perimeter world

User anomaly detection and application level visibility are critical to identify inside threats

Challenge 4: Better Predicting Risks to Your Business

Assess assets with high-risk input manipulation vulnerabilities

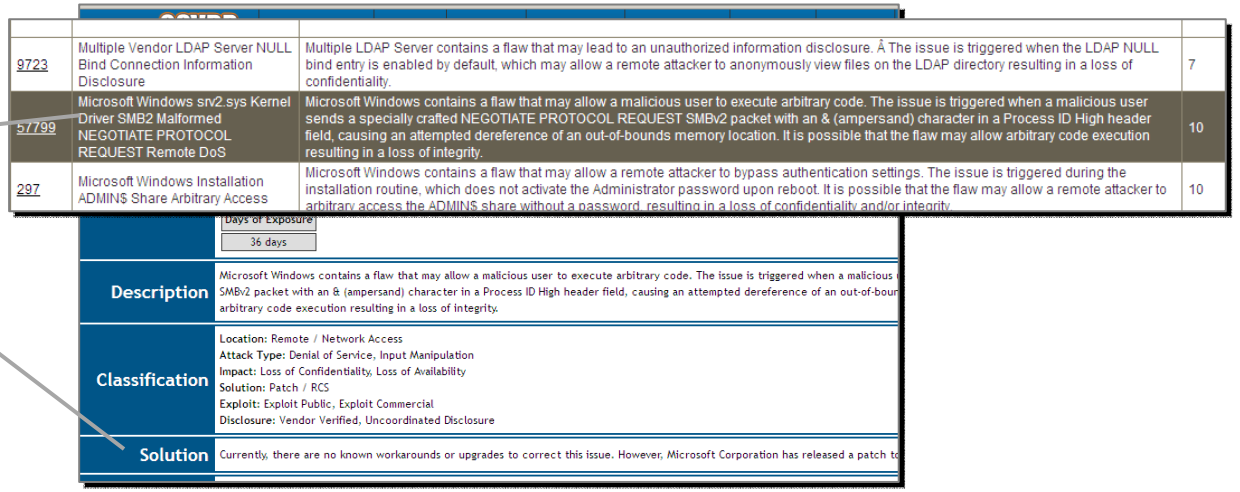


Which assets are affected?

How should I prioritize them?

What are the details?

Vulnerability details, ranked by risk score

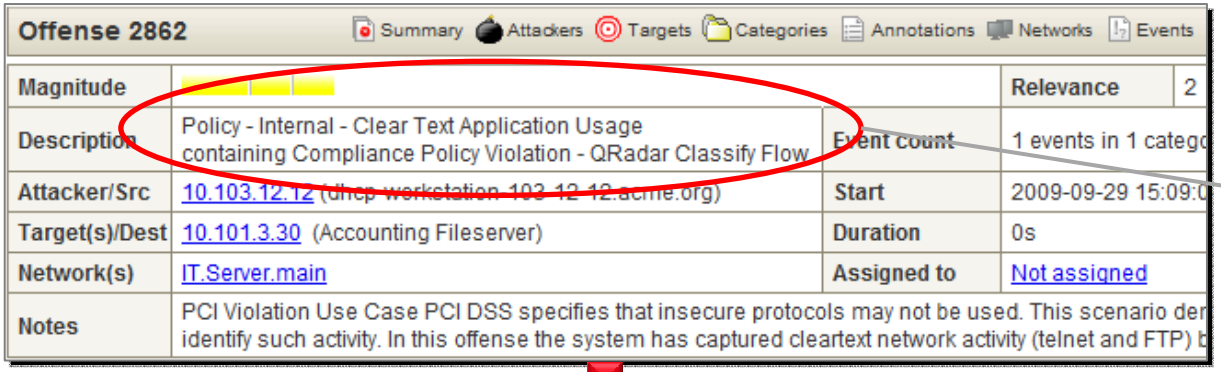


How do I remediate the vulnerability?

Pre-exploit Security Intelligence

Monitor the network for configuration and compliance risks, and prioritize them for mitigation

Challenge 5: Addressing Regulatory Mandates



PCI compliance at risk?

Real-time detection of possible violation

Event Name	Log Source	Source IP	Source Port	Destination IP	Destination Port
Compliance Policy Violation - C	Flow Classification Engine-5 :	10.103.12.12	1482	10.101.3.30	23

Unencrypted Traffic

IBM Security QRadar QFlow saw a cleartext service running on the Accounting server

PCI Requirement 4 states: Encrypt transmission of cardholder data across open, public networks

Compliance Simplified

Out-of-the-box support for major compliance and regulatory standards

Automated reports, pre-defined correlation rules and dashboards

QRadar customer case studies

Case study:
An international energy company reduces billions of events per day to find those that should be investigated

An international energy firm analyzes

2,000,000,000

events per day to find

20 – 25

potential offences to investigate

Business challenge:

- Reducing huge number of events to find the ones that need to be investigated
- Automating the process of analyzing security data

Solution: (QRadar SIEM, QFlow)

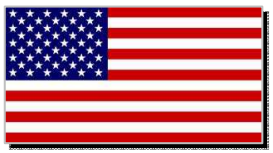
Real-time correlation of hundreds of data sources, anomaly detection to help identify “low and slow” threats, flexibility for easy customization and expansion

Security Intelligence and Analytics: A financial information provider hardens defenses against threats and fraud

Optimize risk management

Tracks 250 activity baselines dynamically adjusted over time

Saved 50-80% on staffing vs. alternative solutions



Business challenge:

- Detect wide range of security threats affecting public-facing Web applications
- Help identify subtle changes in user behavior that could indicate fraud or misuse

Solution: (QRadar SIEM, QFlow)

Real-time correlation of hundreds of data sources, anomaly detection to help identify “low and slow” threats, flexibility for easy customization and expansion

Case study:
A financial information provider hardens defenses against threats and fraud

A European Bank

250

activity baselines dynamically adjusted over time and saved on staffing versus alternative solutions

Business challenge:

- On-line banking system targeted
- DDOS attack, three times
- Had ‘security’ in place
- Early warning capability

Solution: (QRadar SIEM, QFlow)

Real-time correlation of hundreds of data sources, anomaly detection to help identify DDoS to “low and slow” threats.

Security Intelligence and Analytics: Growth markets payments processor achieves PCI compliance / exceeds regulatory mandates

Re-engineer profitable growth

Global electronic payments firm operates in 32 countries and processes over 2 billion transactions per year

Business challenge:

- Protect client data at the heart of this business
- PCI compliance for processing of >$25 billion in annual transactions
- Rapidly implement proven solution, 0 tolerance for delays or errors

Solution: (QRadar SIEM, IBM Security Network IPS)

- Integrated solution to provide visibility into PCI and data exposure risks
- Expert implementation services based on decades of financial industry experience
- Client passed PCI audit four weeks after purchase

Case study:
Fashion Designer uses compliance mandate to detect insider fraud & use evidence in court

Fashion Designer

Using deep forensic analysis, ability to detect insider fraud to be used in court

Business challenge:

- Employee
- Downloading information
- Erasing files
- Time stamped

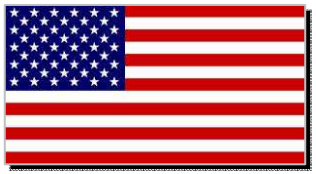
Solution: (QRadar SIEM)

Ability to detect who, what and how specific events occurred. Saving of raw files allowed for exact timings and application layer 7 provided methods used

Security Intelligence and Analytics: A credit card firm simplifies complexity, reduces costs and optimizes resources

Optimize risk management

50% reduction in cost of deployment, tuning and maintenance vs. competitor



Business challenge:

- 8-year old SIEM technology did not provide visibility into and protection from current threats
- High cost of tuning and maintenance of incumbent SIEM product

Solution: (QRadar SIEM)

Advanced security analytics engine for real-time threat detection and analysis

Scalable architecture to meet client's large data and infrastructure requirements

Next Steps

Download the Gartner SIEM Magic Quadrant Report: bit.ly/18Ff7TJ

Download the IBM Security QRadar SIEM datasheet: ibm.co/191DlYD

Read the Blog: blog.q1labs.com

Follow us on Twitter: @ibmsecurity

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.

ibm.com/security

Agenda

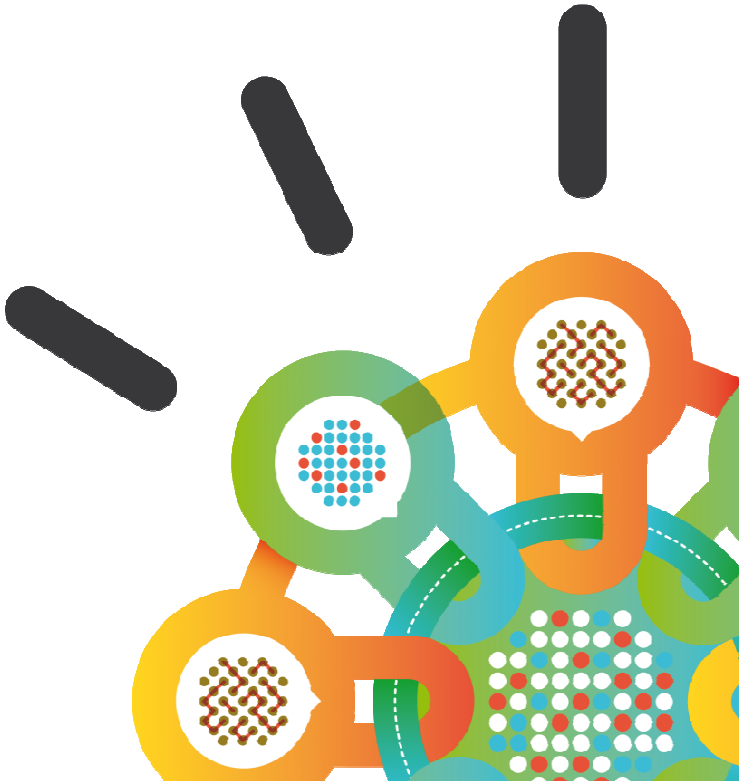
- Welcome and Introductions
- Latest Security trends and 2012 X-Force Report
- Security Intelligence - Understanding your Organizational Security Posture
- **Holistic approach to handling Advanced Persistent threats**
- Break
- Managing Application Security
- From Identity & Access Management to Identity Intelligence
- Securing your Cloud
- IBM Global Financing

Security Intelligence.
Think Integrated.

A Holistic Approach to Advanced Persistent Threats

How IBM is Helping Clients

May 2013



Agenda

The Challenge of Advanced Persistent Threats

IBM’s Comprehensive Security Portfolio

IBM’s Approach

137,400,000

…Number of cyber-attacks witnessed by IBM in 2012

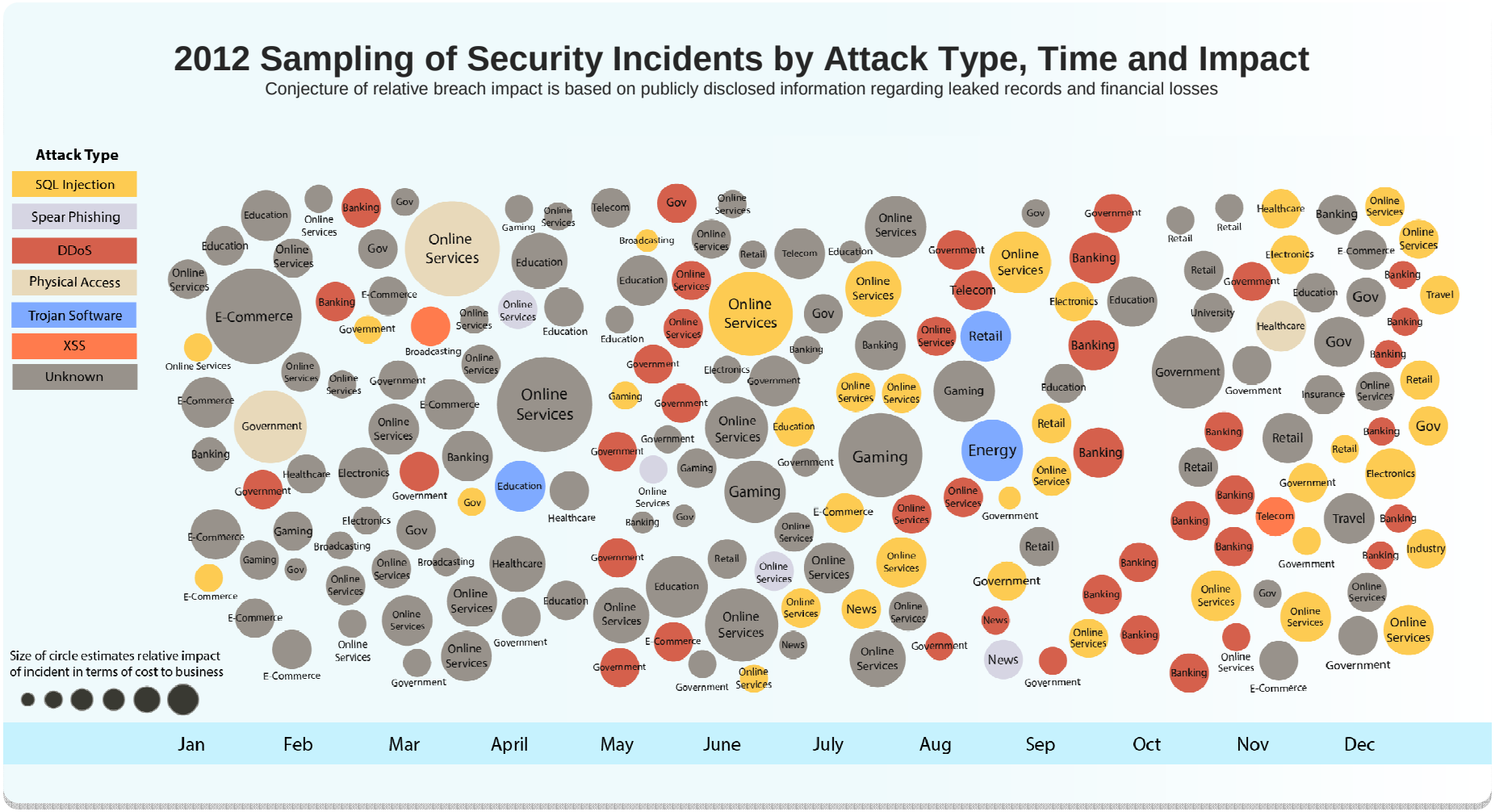
Most Attacked Industries

Industry	Average weekly attacks
Health and Social Services	10.1 million
Transportation	9.8 million
Hospitality	5.5 million
Finance and Insurance	3.6 million
Manufacturing	2.6 million

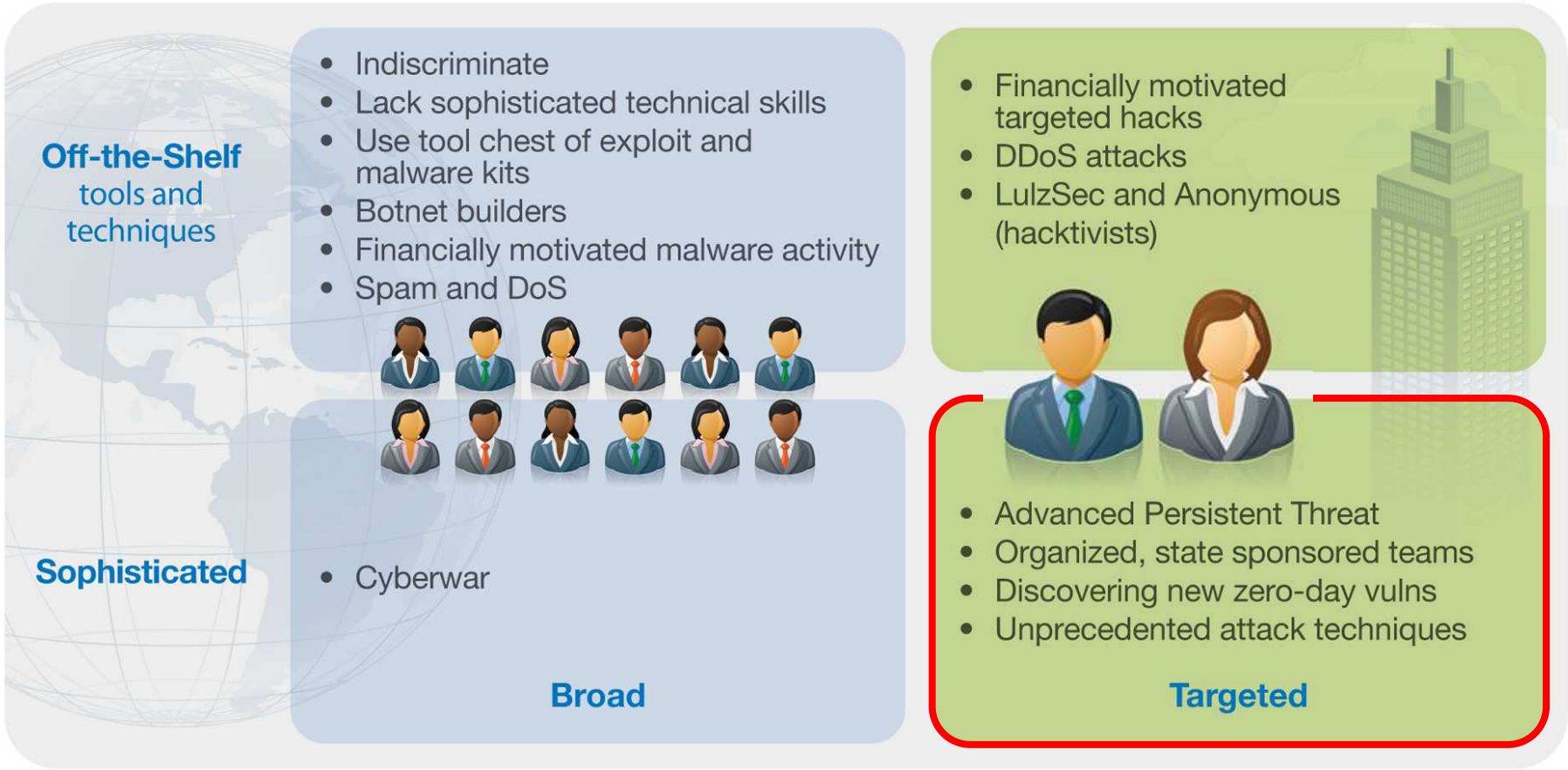
1.07

Incidents per
one million attacks[1]

IBM has tracked a massive rise in advanced and other attacks



Attackers are using sophisticated techniques to bypass defenses



"Advanced Persistent Threat" is the approach often used by State-Sponsored Entities

Source: IBM X-Force Research and Development

What's different about Advanced Persistent Threats?

Advanced

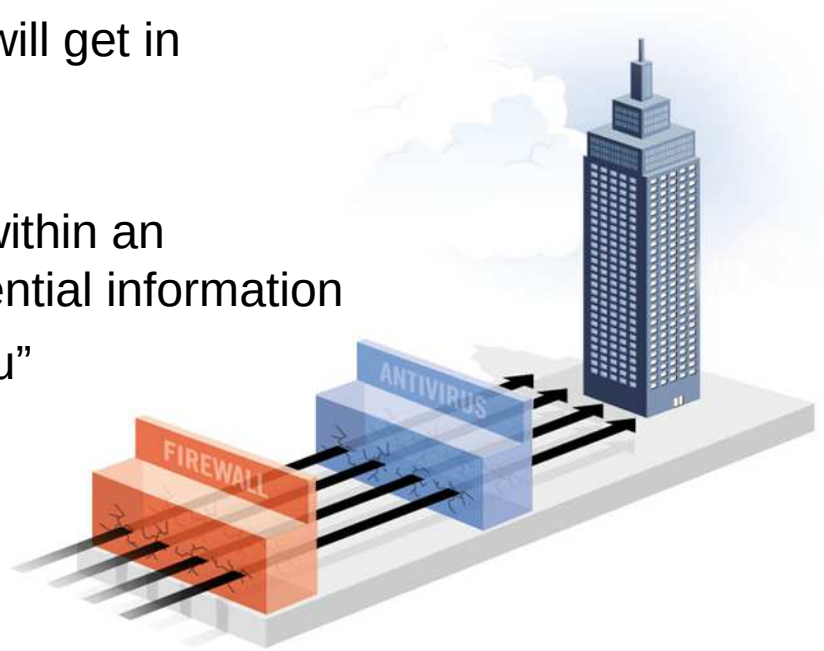
- Exploiting unreported (zero-day) vulnerabilities
- Advanced, custom malware is not detected by antivirus products
- Coordinated, well researched attacks using multiple vectors

Persistent

- Attacks last for months or years (average: 1 year; longest: 4.8 years)[1]
- Attackers are dedicated to the target – they will get in

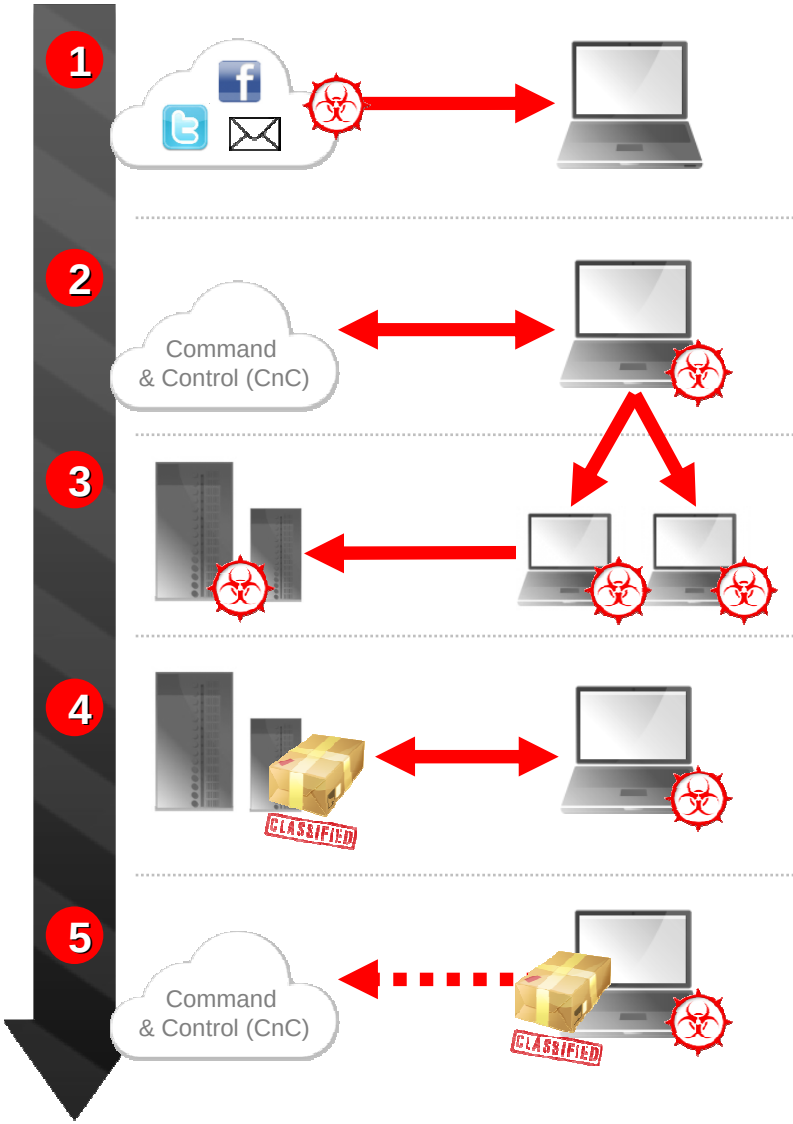
Threat

- Targeted at specific individuals and groups within an organization; aimed at compromising confidential information
- Not random attacks – they are "out to get you"



1) Source: http://intelreport.mandiant.com/Mandiant_APT1_Report.pdf

Attackers follow a 5-Stage attack chain



Break-in

Spear phishing and remote exploits to gain access

Latch-on

Malware and backdoors installed to establish a foothold

Expand

Reconnaissance and lateral movement to increase access and maintain a presence

Gather

Acquisition and aggregation of confidential data

Exfiltrate

Data exfiltration to external networks

IBM's unique approach to security

- Leader in security software and services – recognized by Gartner, Forrester and IDC
- Solutions deployed at the largest banks, retailers, and government agencies worldwide

Monitor

Big data **analytics** applied to security

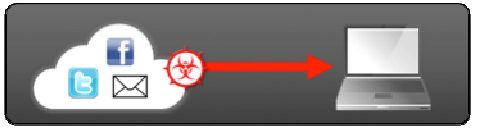
Control

Robust **controls** built into IT fabric, relying on leading IBM technologies across 12+ critical security domains

Apply Insight

World class **research** that finds threats before they impact you

Stage 1: Break-in



1 Break-in
2 Latch-on
3 Expand
4 Gather
5 Exfiltrate

Your Challenge

- Employees are always vulnerable to well-executed phishing attempts
- Even patched machines can be compromised by “zero-day attacks” that leverage previously unknown vulnerabilities
- Antivirus has proven to be largely ineffective against zero-day malware

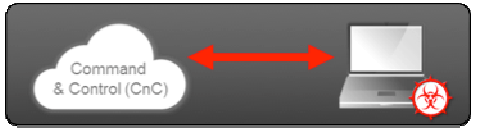
How IBM Can Help

- **IBM Security Network IPS** and **IBM Security Network Protection** help block zero-day exploits using advanced behavioral analysis, and block phishing and malware sites using a database of 13 billion URLs
- **IBM Endpoint Manager** helps limit attack surface by auditing and enforcing compliance with patch and configuration policies

Other Considerations

- Ask your endpoint protection (antivirus) vendor what they provide for advanced detection, and how they detect indicators of compromise
- Consider using a specialized malware detection solution
- Develop and implement a thorough employee education program

Stage 2: Latch-on



Your Challenge

- Once the attacker has breached your perimeter, they need to establish a communication channel back to “home” and create redundant ways to access your network

How IBM Can Help

- **IBM Security QRadar** continuously monitors the network and helps identify anomalous activity in terms of location, applications accessed, and more; logs network activity for future forensic investigations, to help determine extent of breach
- **IBM Security Network IPS** uses advanced behavioral analysis to detect subtle communications with malicious destinations

Other Considerations

- Ask your endpoint protection (antivirus) vendor what they are providing for advanced detection, including detecting indicators of compromise

Stage 3: Expand

1 Break-in
2 Latch-on
3 Expand
4 Gather
5 Exfiltrate

Your Challenge

- APTs usually don't infect the host containing target data; thus the attacker needs to find the target data and gain access to it
- They will perform reconnaissance to understand the network and identify high-value assets

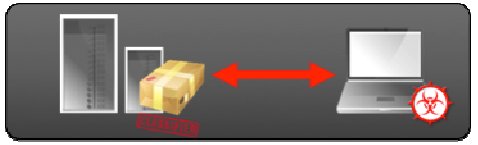
How IBM Can Help

- **IBM Security Privileged Identity Manager** helps lock down user accounts with access to high-value systems and data
- **IBM Security QRadar** uses out-of-the-box analytics to look for suspicious network probing – by correlating activity at big data scale
- **IBM Security Host Protection** helps identify suspicious system activity, and inspects and blocks malicious traffic – including connections to encrypted web applications
- **IBM Security AppScan** helps reduce the attack surface of enterprise applications by identifying and prioritizing application vulnerabilities

Other Considerations

- Proactively manage your access policies, grant the minimum rights required, and frequently review user access rights

Stage 4: Gather



1 Break-in
2 Latch-on
3 Expand
4 Gather
5 Exfiltrate

Your Challenge

- Once the attacker has compromised your users & gained access to sensitive data repositories, they explore what is available and begin copying target data

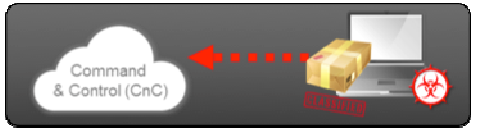
How IBM Can Help

- **IBM InfoSphere Guardium** continuously monitors databases and data warehouses to identify suspicious access and protect sensitive data
- **IBM Security Network IPS** helps block malicious behavior within (and beyond) the network
- **IBM Security Network Protection** controls application access at a granular user and application level
- **IBM Security Privileged Identity Manager** helps enforce access policies

Other Considerations

- Place extra controls and focus around your critical assets and data
- Encrypt & protect data in proportion to its value to you and attackers
- Implement an effective DLP (data loss prevention) strategy

Stage 5: Exfiltrate



1 Break-in
2 Latch-on
3 Expand
4 Gather
5 Exfiltrate

Your Challenge

- There are nearly unlimited ways to get acquired data off your network

How IBM Can Help

- **IBM X-Force Threat Intelligence** identifies malicious sites, to help block communications
- **IBM Security QRadar** uses X-Force data to detect traffic to suspect sites; performs activity baselining to help detect anomalous user behavior based on type of activity, volume of transfers, location, etc.
- **IBM Security Network IPS** helps stop encrypted traffic associated with suspicious entities, and sensitive data transmission (eg, credit card numbers)
- **IBM Security Network Protection** tracks and controls application usage in all directions to enforce policies and help prevent data loss

Other Considerations

- Push your Endpoint Protection, Network DLP and Network Security vendors to enhance their detection and blocking of suspicious data transmission

IBM's approach to defending against state-sponsored attacks

Network and Endpoint Security Use adaptive threat protection and endpoint management to reduce risks and fend off attacks

Network Security Use SIEM and adaptive threat protection to help identify and stop attackers from gaining a foothold

Secure Users Leverage strong identity management to enforce access policies and monitor for suspicious behavior

Data Security Embed security deep into data repositories with data activity monitoring; apply fine-grained access controls

Network Security Proactively monitor network traffic for common exfiltration tactics; block in real-time

Security Analytics Leverage Security Intelligence to correlate and analyze activity across the entire enterprise…

Extend with Big Data capabilities for analyzing unstructured data…

Utilize Emergency Response Services for breach or for assessment of risk

Security **Intelligence**. Think **Integrated**.

What to do if you have been breached

1. Call IBM Emergency Response Services (24x7):

The (cyber)storm is coming. ARE YOU READY?

Emergency? Call: (US) +1.888.241.9812 | (WW) +1.312.212.8034

Or get started with a **penetration test** or an **incident response plan**

2. Proactively assess risk and reduce future breach likelihood:

- Cyber Incident response training and simulated exercises to determine level of preparedness
- Incident Response Program gap assessment to ensure enterprise readiness and responsiveness when an incident occurs
- Active Threat Assessment as a preemptive service to determine weaknesses requiring remediation
- X-Force threat analysis service is available from IBM experts **24x7**

Key Features

24x7x365 Hotline for clients to call from anywhere worldwide for assistance if they believe they are experiencing an incident

Incident Case Managers who maintain calm, focus, and manage the incident and environment to completion and satisfaction

Advanced tools, expertise and scale for any platform, size client, and location worldwide

Globally collected intelligence applied to each engagement to improve outcomes and efficiencies

Unlimited emergency declarations

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.

ibm.com/security

Agenda

- Welcome and Introductions
- Latest Security trends and 2012 X-Force Report
- Security Intelligence - Understanding your Organizational Security Posture
- Holistic approach to handling Advanced Persistent threats
- **Break**
- Managing Application Security
- From Identity & Access Management to Identity Intelligence
- Securing your Cloud
- IBM Global Financing