

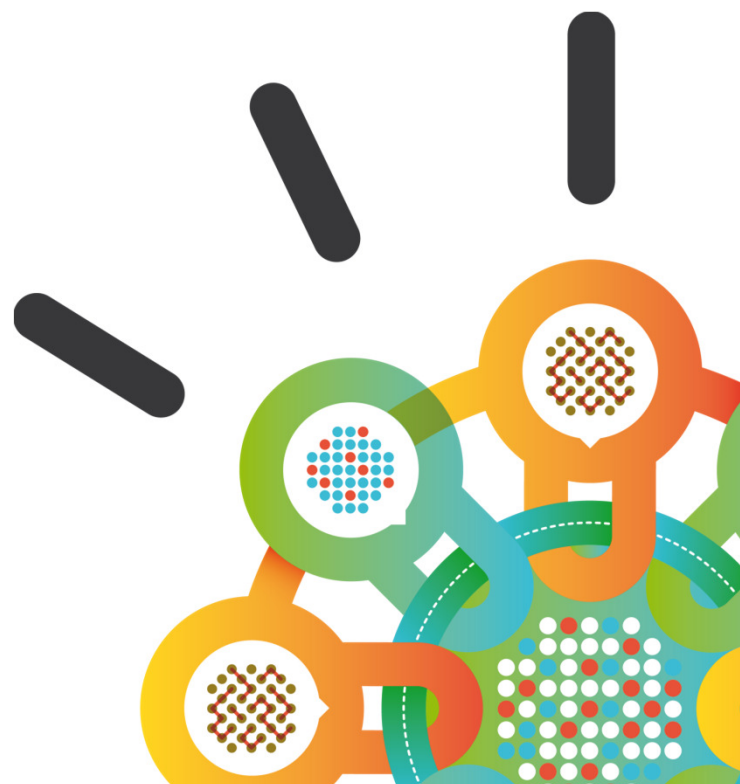
Security Intelligence.
Think Integrated.

Trends in the Threat Landscape

Thad Mann, CISM, CISSP, CeH, PMP

Cybersecurity Black Belt

tmann@us.ibm.com, 336-339-7206, October 2013



Several critical security business issues resonate consistently across senior management, and have become the top security focus issues

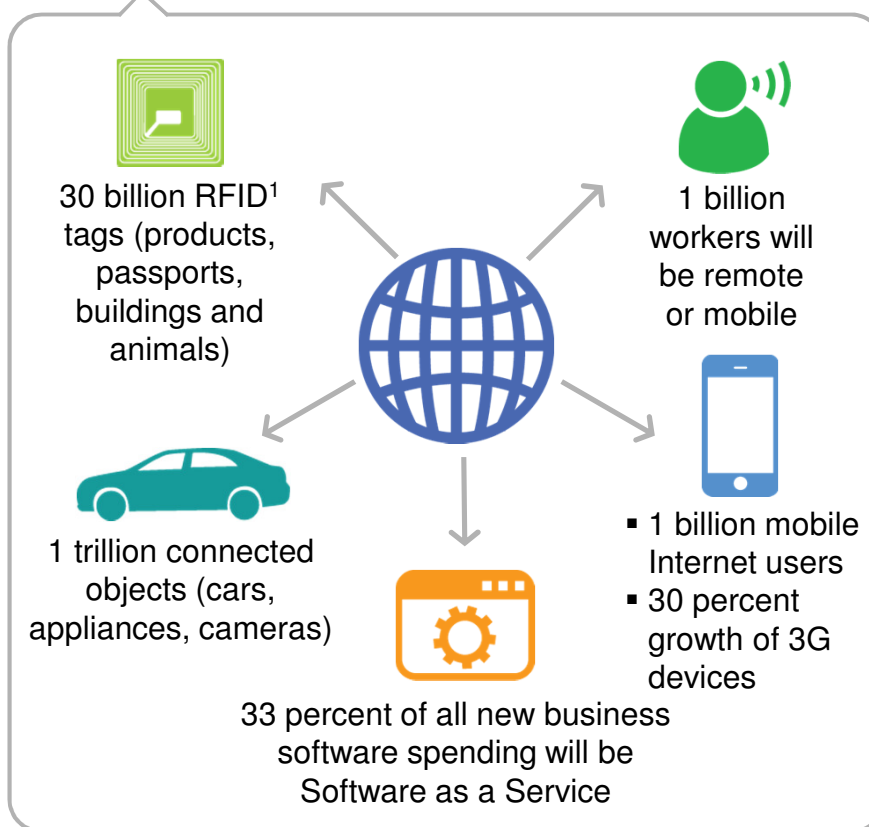
<p>Enable effective security</p> <p>The security investments need to support the business & IT requirements</p>	<p>Protect the Corporate & Brand image</p> <p>Avoid a breach that could have significant financial and brand impacts</p>	<p>Maximize security investment</p> <p>Ensure company is getting best bang for buck for security spend & integration with IT/Risk projects</p>	<p>Manage end to end security</p> <p>Leverage tools and technologies that enable limited staff to effectively address mobility & cloud</p>	<p>Develop & retain key security personnel</p> <p>Create optimal environment to secure company and build a program to acquire security talent</p>	<p>Leverage security across the business units</p> <p>Build a security DNA & culture that creates security approaches across the business units</p>
--	---	---	---	--	--

Vulnerabilities increase with emergence of new business models, new technologies and Big Data

Adopting new business models and embracing new technologies and data

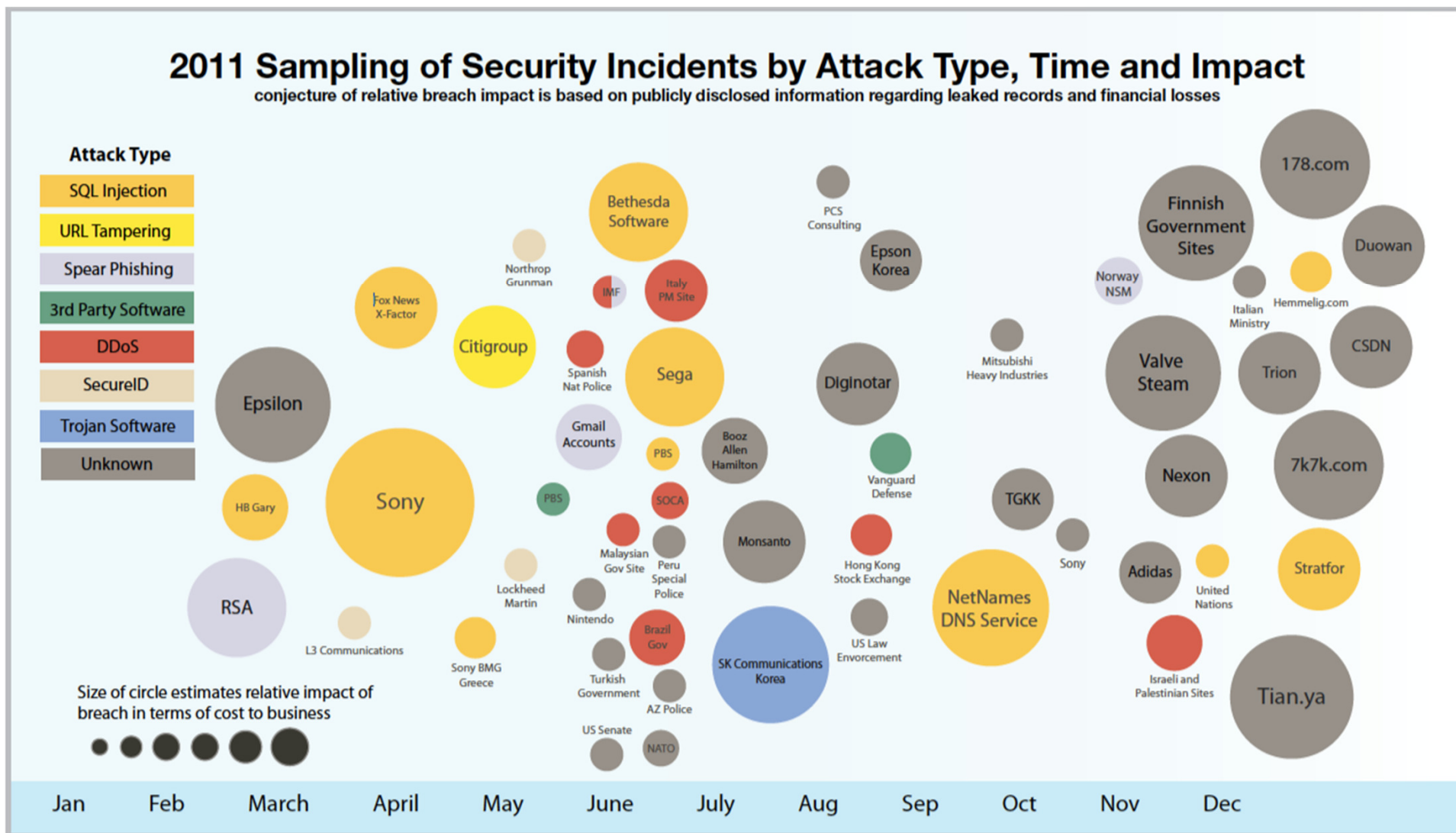


Exponentially growing and interconnected digital universe



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

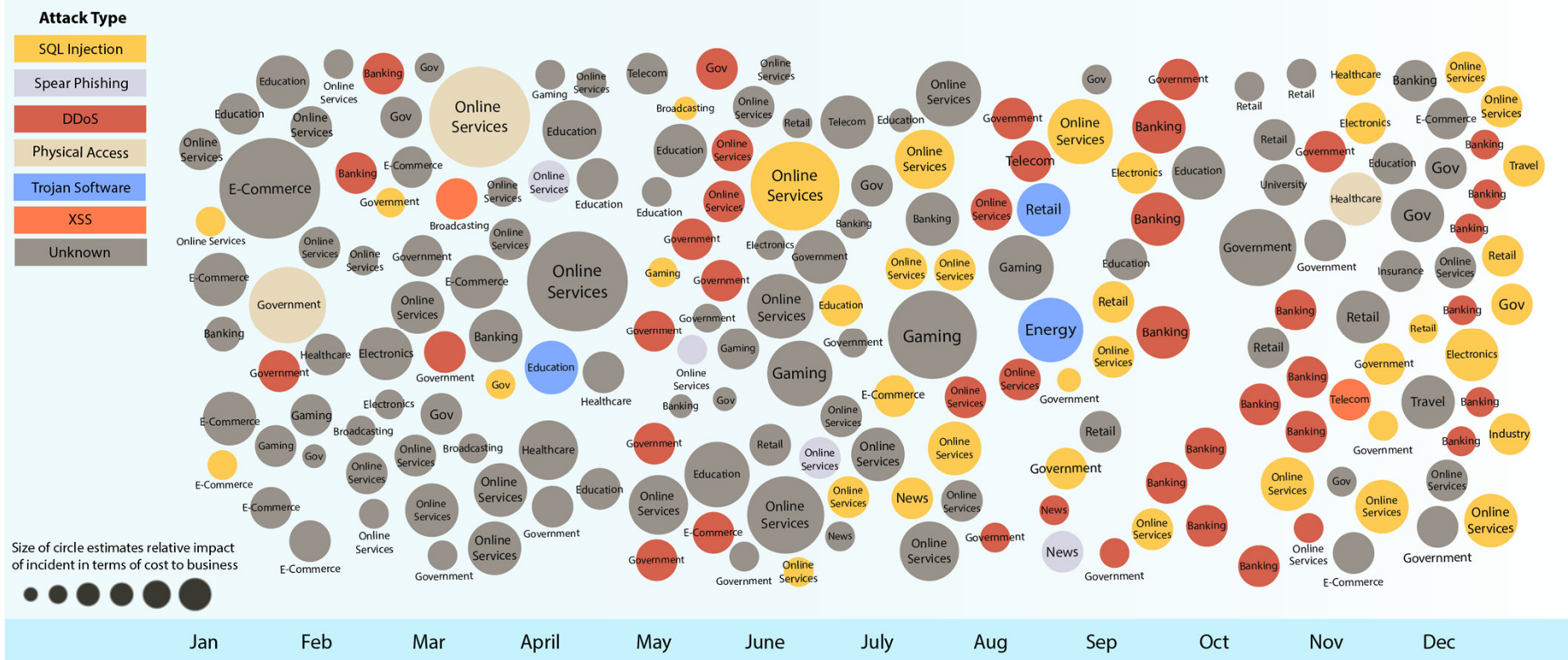
With targeted Attacks Shaking Businesses and Governments



IBM has tracked a massive rise in advanced and other attacks

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

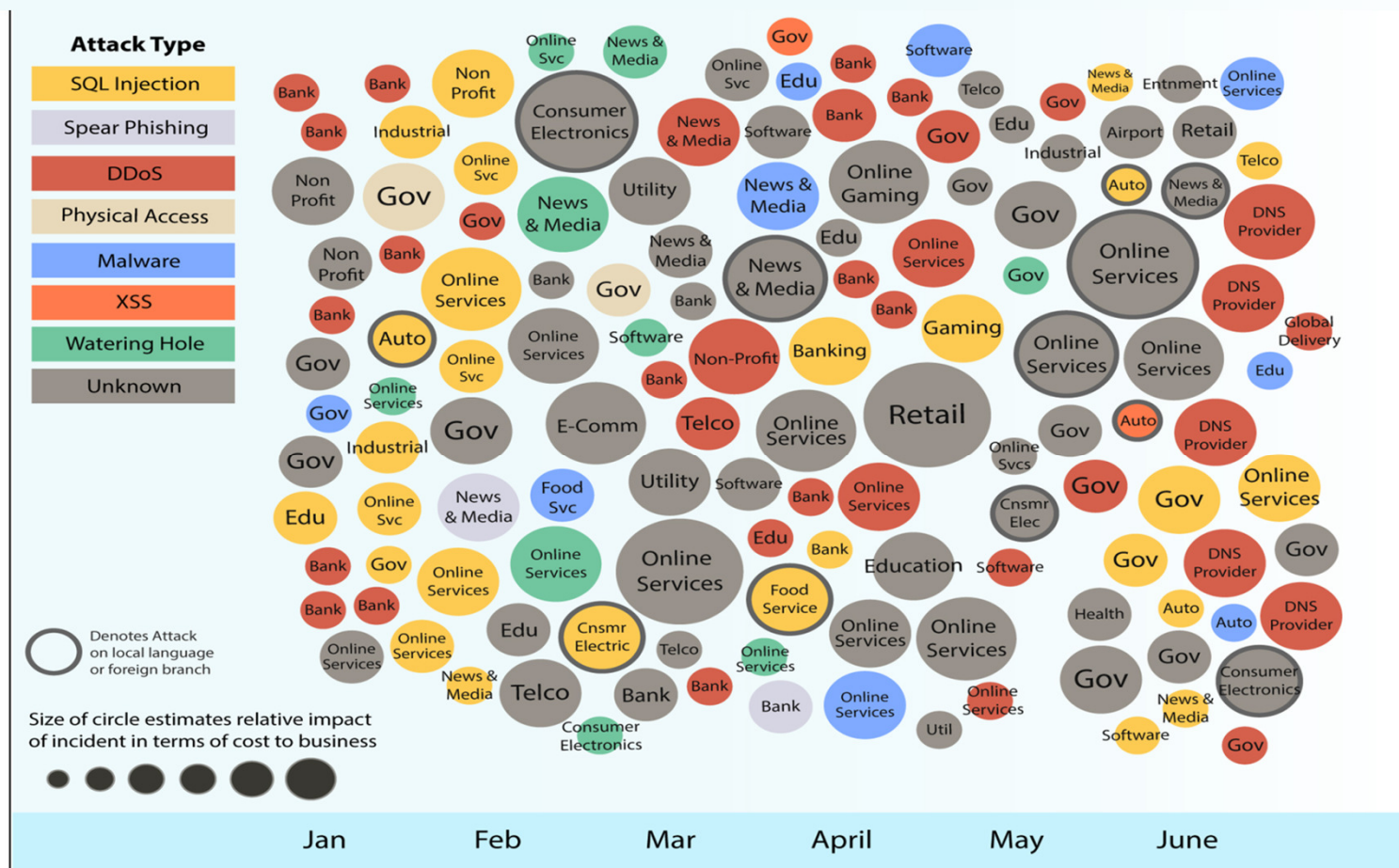
Conjecture of relative breach impact is based on publicly disclosed information regarding leaked records and financial losses



....there is no sign of the trend getting any better YTD 2013

2013 1H 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 2013 Trend and Risk Report

The *Average E&U Company* Faces Per Week

1,414,538

Security Attacks

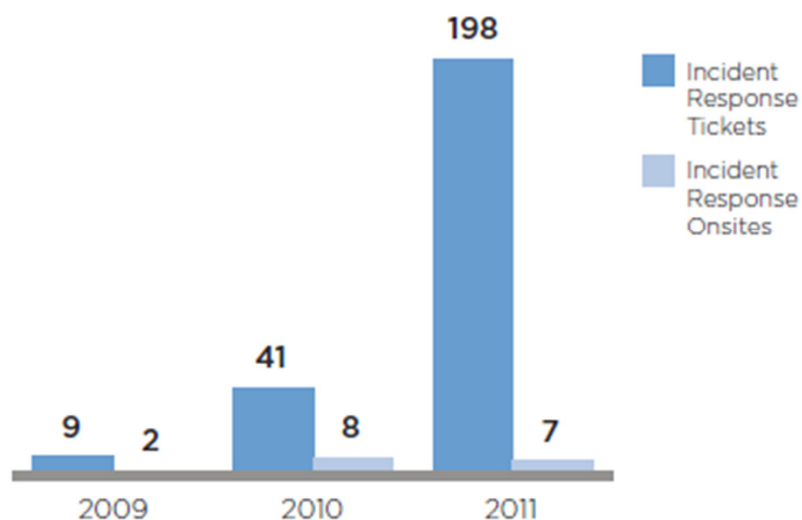
The *Average E&U Company* Faces Per Week

2.33

Security Incidents

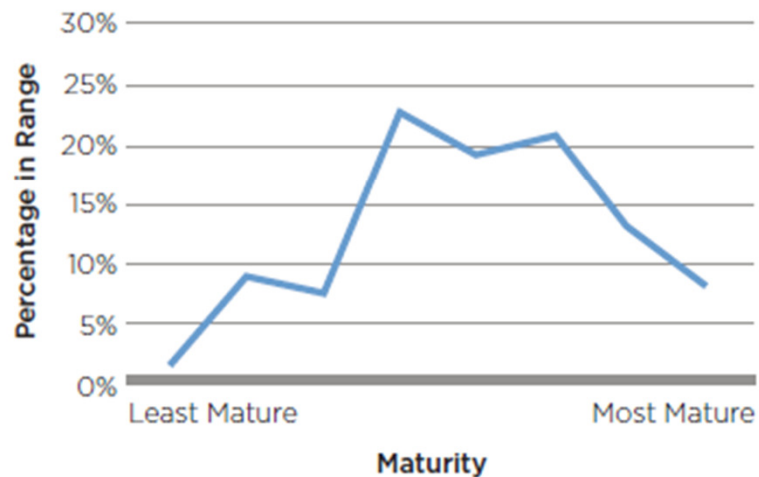
One of the 10 Security Imperatives in 2013: Upgrade Incident Response Capabilities to Prepare for Advanced Threats

ICS-CERT Incident Response Trends
Number of Attacks Reported and Requiring Onsite Help by US Critical Infrastructure Companies



Source: ICS-CERT Incident Response Summary Report, 2011.

Relative Maturity of IREC Members' Incident Response Processes
Percentage of Survey Respondents at Various Maturity Levels



n = 78.

Source: IREC Controls Maturity Benchmarking Service, 2009.

Most organizations have outdated incident response capabilities; increasingly sophisticated attacks require CISOs to revisit their processes.

Corporate Executive Board, Information Risk Executive Council Study, 2013 Security Outlook November 2012

Security skills are hard to attract and retain

58%

are unable to find people with the right skills

53%

complain of the inability to measure the effectiveness of their current security efforts

66%

struggle with an understaffed IT team

FORRESTER®

81% of chief information security officer functions are re-organizing or have been re-organized *within the last six months.*

Corporate Executive Board, Information Risk Executive Council Study, July 2012

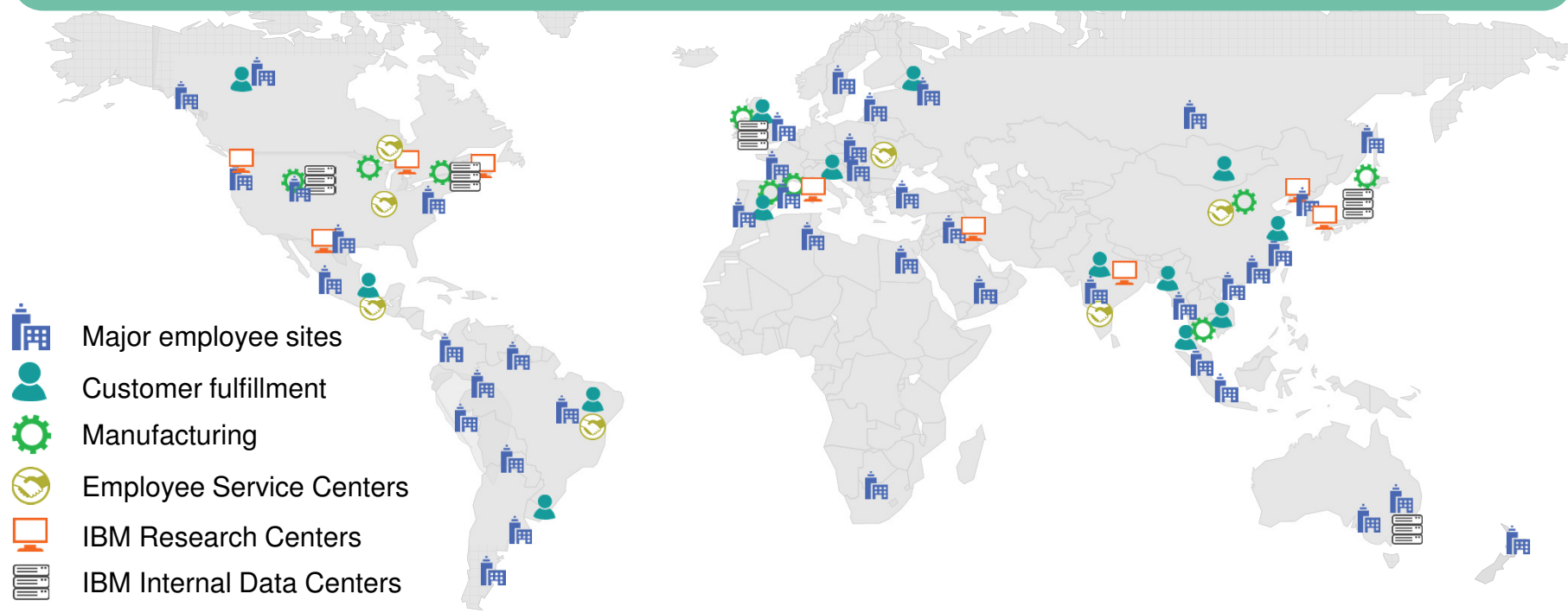


Threats & Vulnerabilities Research

IBM's approach to Cyber Security is based upon what we learn protecting our own multi-national enterprise and that of thousands of customers around the world

IBM has one of the largest, most complex internal IT infrastructures in the world

- 2,000-plus major sites
- 170-plus countries
- 400,000-plus employees
- About 200,000-plus contractors
- 800,000-plus traditional endpoints
- About 50 percent of employees are mobile



IBM provides unmatched global coverage and security awareness.



IBM Research

IBM Institute for Advanced Security
Enabling cybersecurity innovation and collaboration

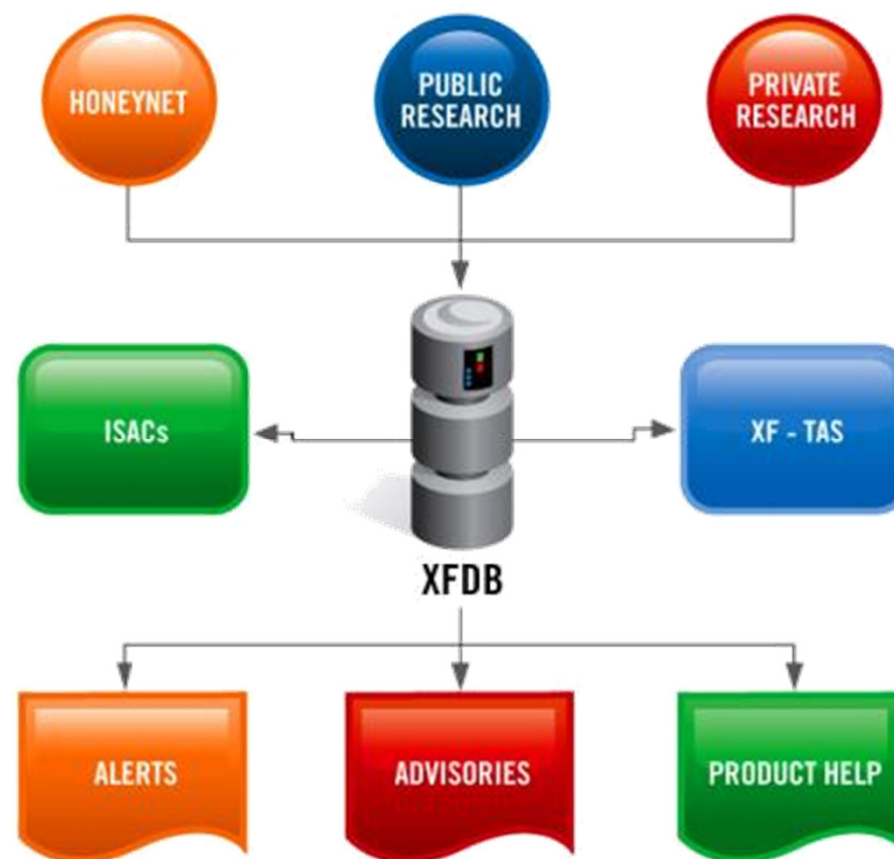
10B analyzed Web pages & images
150M intrusion attempts daily
40M spam & phishing attacks
70K documented vulnerabilities
 Millions of unique malware samples

World Wide Managed Security Services Coverage

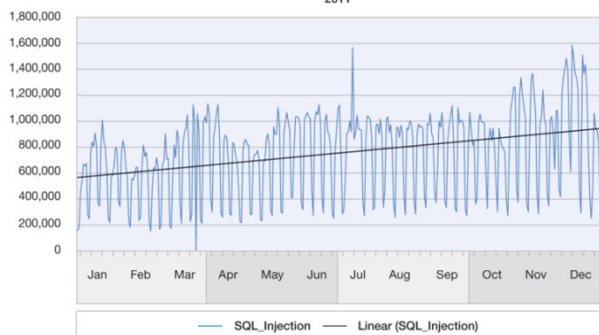
- 20,000+ devices under contract
- 3,300 GTS service delivery experts
- 3,700+ MSS clients worldwide
- 13B+ events managed per day
- 1,000+ security patents
- 133 monitored countries (MSS)

We analyze them all...

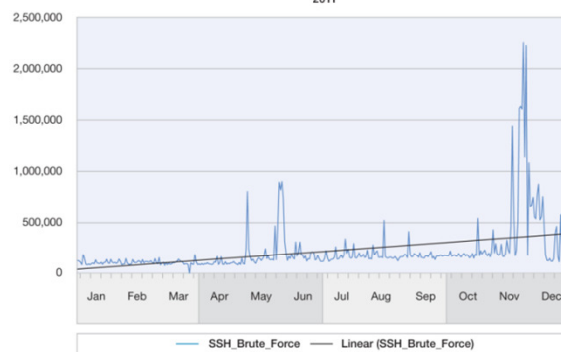
- Most comprehensive Vulnerability Database in the world
 - Over **70,000** unique vulnerabilities cataloged
 - Entries date back to the 1990's
- Updated daily by a dedicated research team
- The X-Force currently monitors over...
 - 8,000 Vendors
 - 17,000 Products
 - 40,000 Versions
 - 4,0000+ Clients
 - 13+ Billion events daily



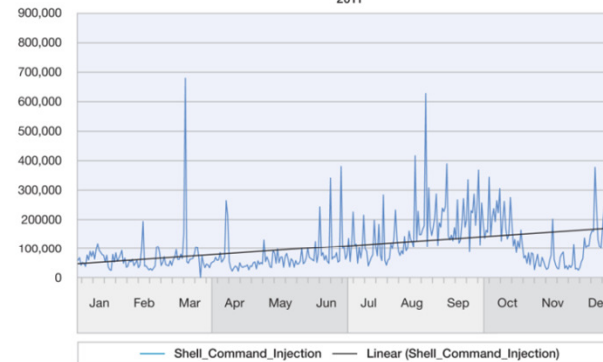
Top MSS High Volume Signatures and Trend Line – SQL_Injection
2011



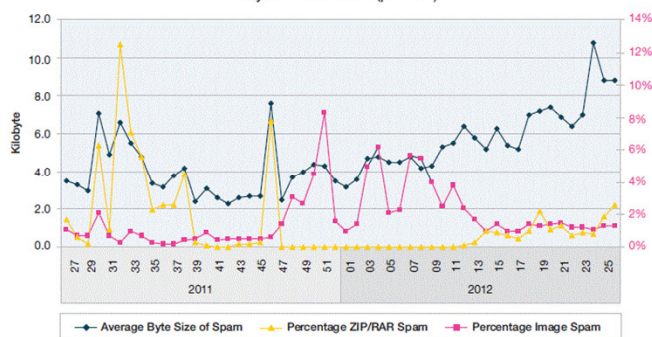
Top MSS High Volume Signatures and Trend Line – SSH_Brute_Force
2011



Top MSS High Volume Signatures and Trend Line – Shell_Command_Injection
2011

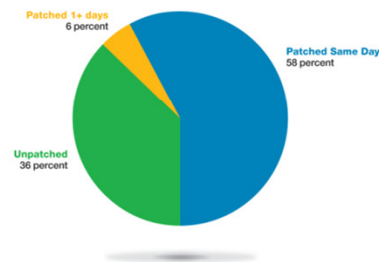


Average Byte Size of Spam versus Percentage of Image and ZIP/RAR Spam
July 2011 to June 2012 (per week)



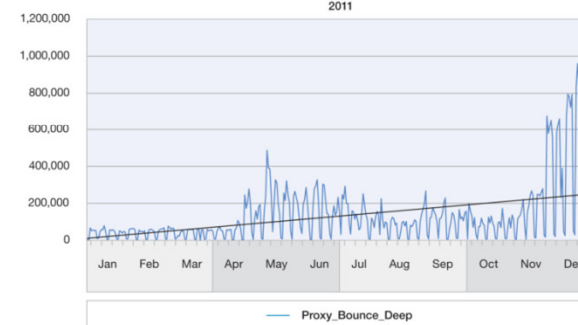
Source: IBM X-Force® Research and Development

Vendor Patch Timeline
2011

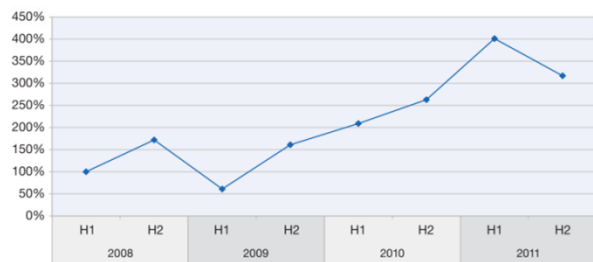


Source: IBM X-Force® Research and Development

Top MSS High Volume Signatures and Trend Line – Proxy_Bounce_Deep
2011

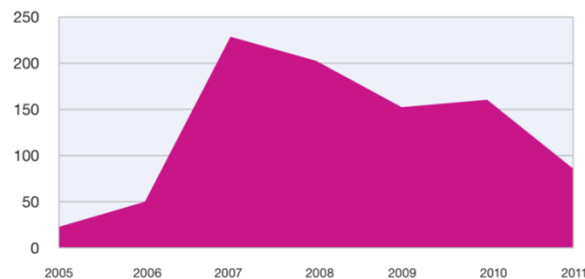


Volume of Newly Registered Anonymous Proxy Websites
2008 to 2011



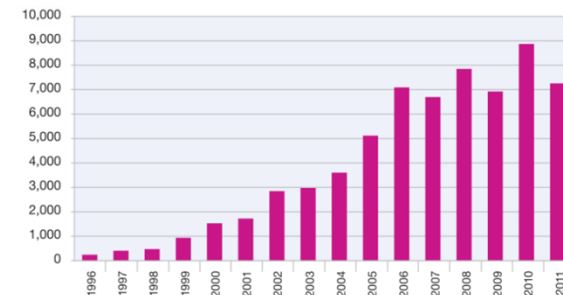
Source: IBM X-Force® Research and Development

Public Exploit Disclosures for Browser
2005-2011



Source: IBM X-Force® Research and Development

Vulnerability Disclosures Growth by Year
1996-2011



Source: IBM X-Force® Research and Development

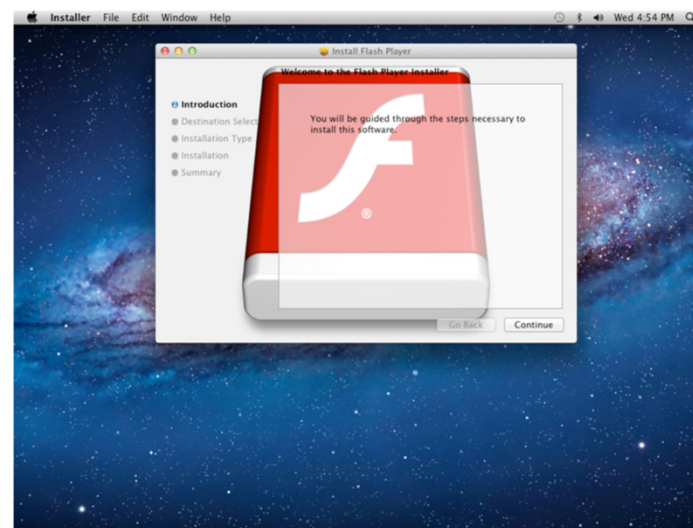
MAC malware

- Flashback
 - discovered September 2011 has seen the most activity in the Mac malware world.
 - Uses Java Exploit

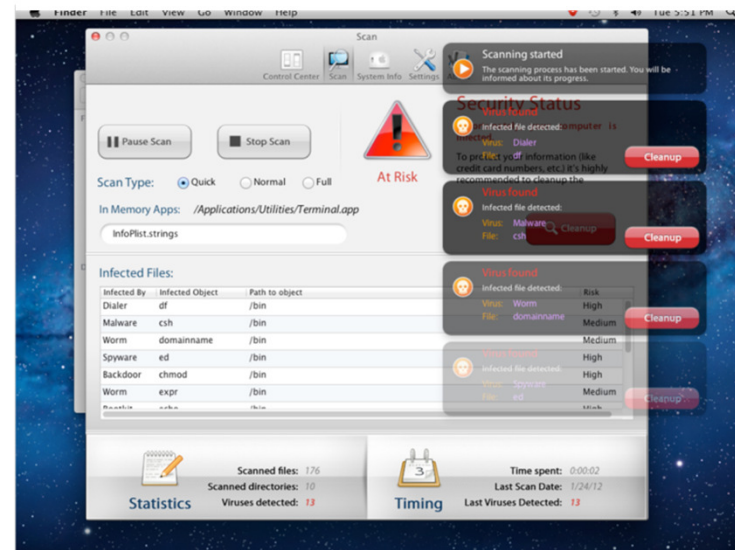
- APT
 - Tibet malware (March 2012); Java and Word Document exploits
 - SabPub backdoor (April 2012); Java exploit

- Crisis/Morcut (July 24, 2012)
 - Anti-reversing + Rootkit capabilities
 - Cross platform (Windows, OSX, VMWare?)
 - Not found in the wild (yet)

- Expect to see continued increase in number of Mac based malware with improved functionality



Source: IBM X-Force® Research and Development



Source: IBM X-Force® Research and Development

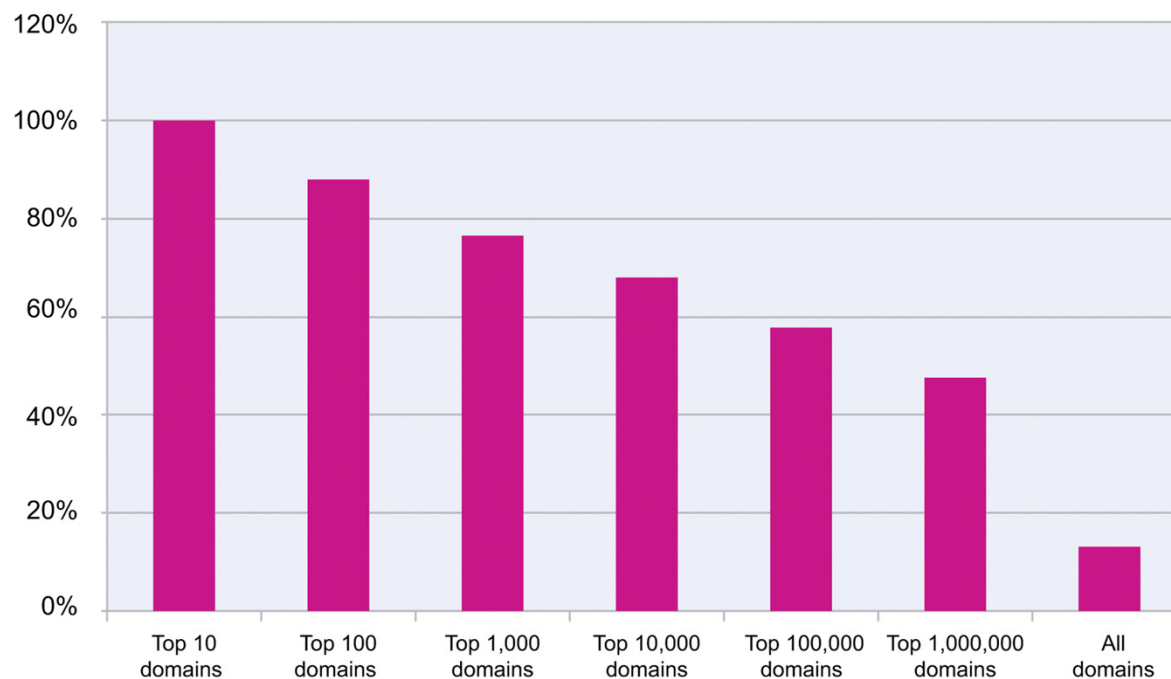
Social Networking – no longer a fringe pastime

Social Networks allow attackers to learn:

- Who works there?
- What are their titles?
- Create index cards with names and titles
- Who are their colleagues?
- Start to build an org chart
- What is their reporting structure?
- Who are their friends?
- What are they interested in?
- What are their work/personal email addresses?

Internet Penetration of Social Networks

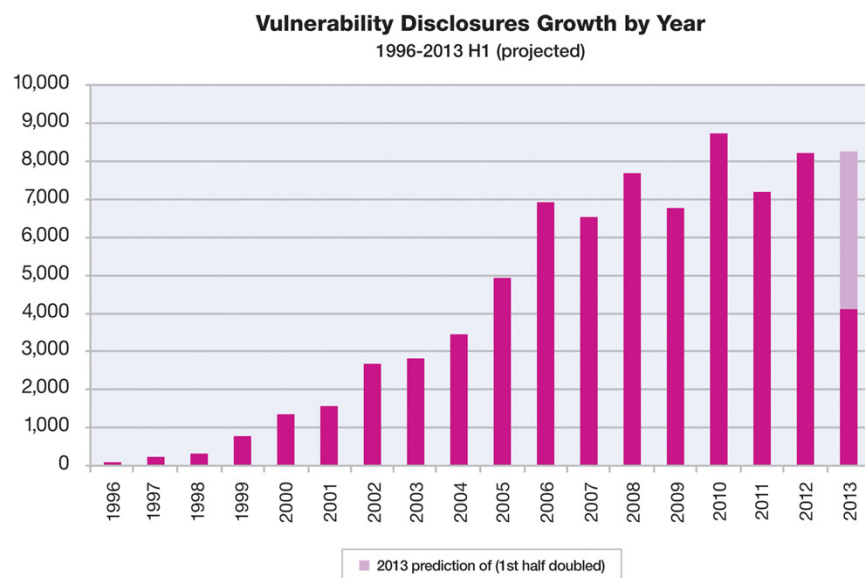
December 2012



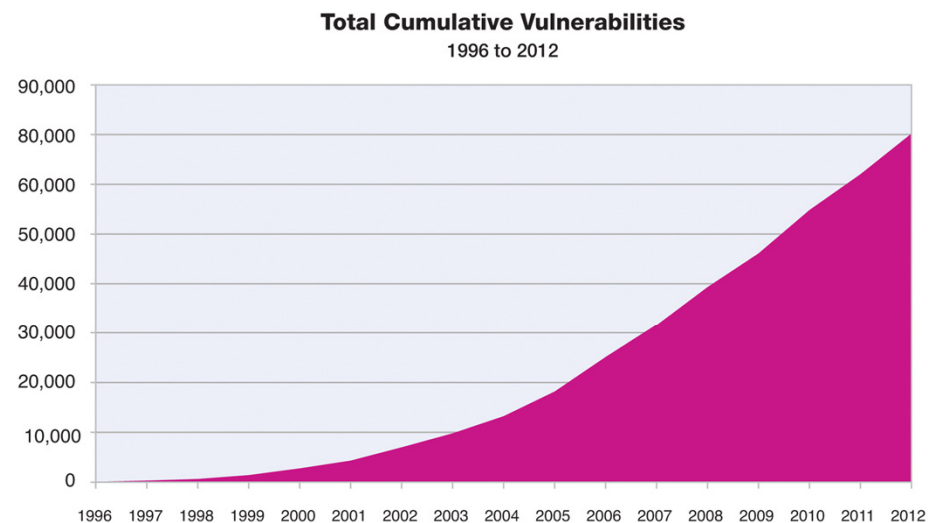
Source: IBM X-Force® Research and Development

Vulnerability disclosures up in 2012 and continuing to grow...

- 4,100 number of vulnerabilities (1H13)
- Total number of vulnerabilities is over 70,000 and growing!

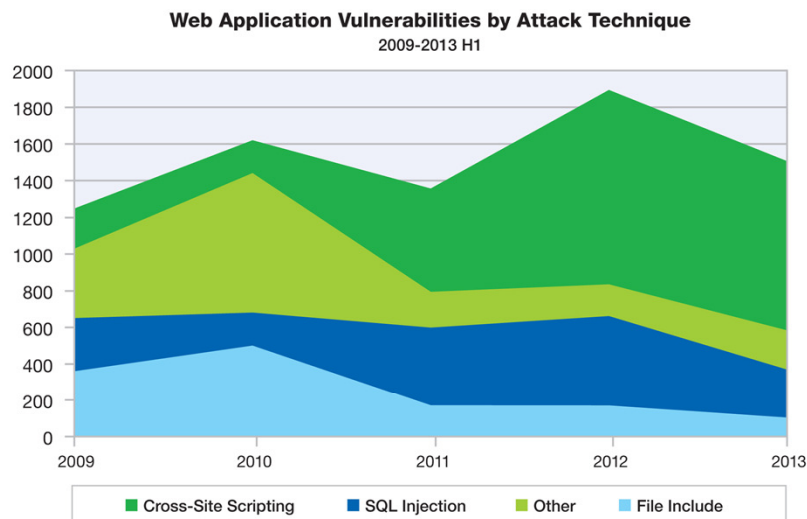


Source: IBM X-Force® Research and Development



Source: IBM X-Force® Research and Development

Vulnerabilities in Web Platforms, CMS and Plug-Ins

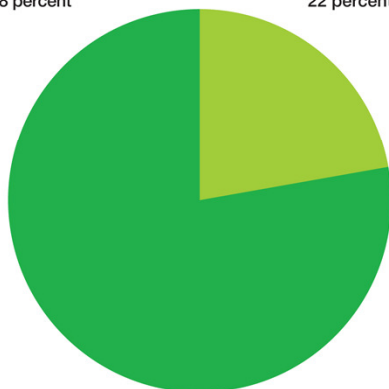


Source: IBM X-Force® Research and Development

CMS Core Vulnerabilities
2013 H1

Patched:
78 percent

Unpatched:
22 percent

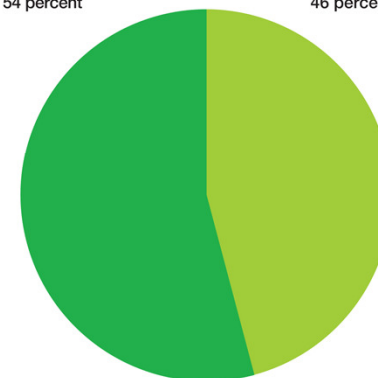


Source: IBM X-Force® Research and Development

CMS Plug-in Vulnerabilities
2013 H1

Patched:
54 percent

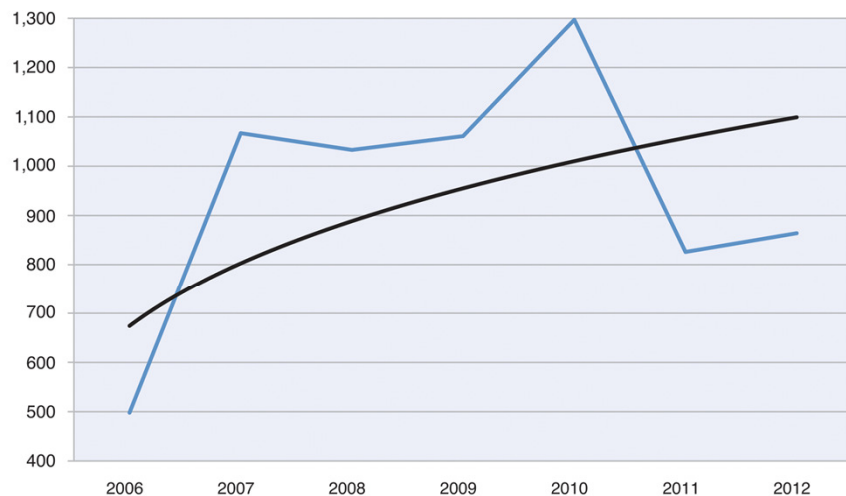
Unpatched:
46 percent



Source: IBM X-Force® Research and Development

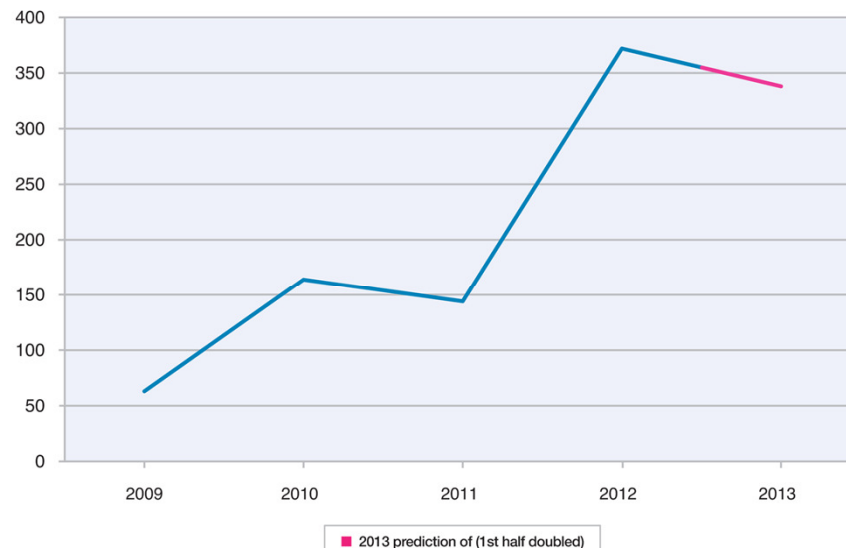
Public Exploit Disclosures

True Exploit Disclosures
2006 to 2012



Source: IBM X-Force® Research and Development

Total Mobile Vulnerabilities
2009-2013 H1



Source: IBM X-Force® Research and Development

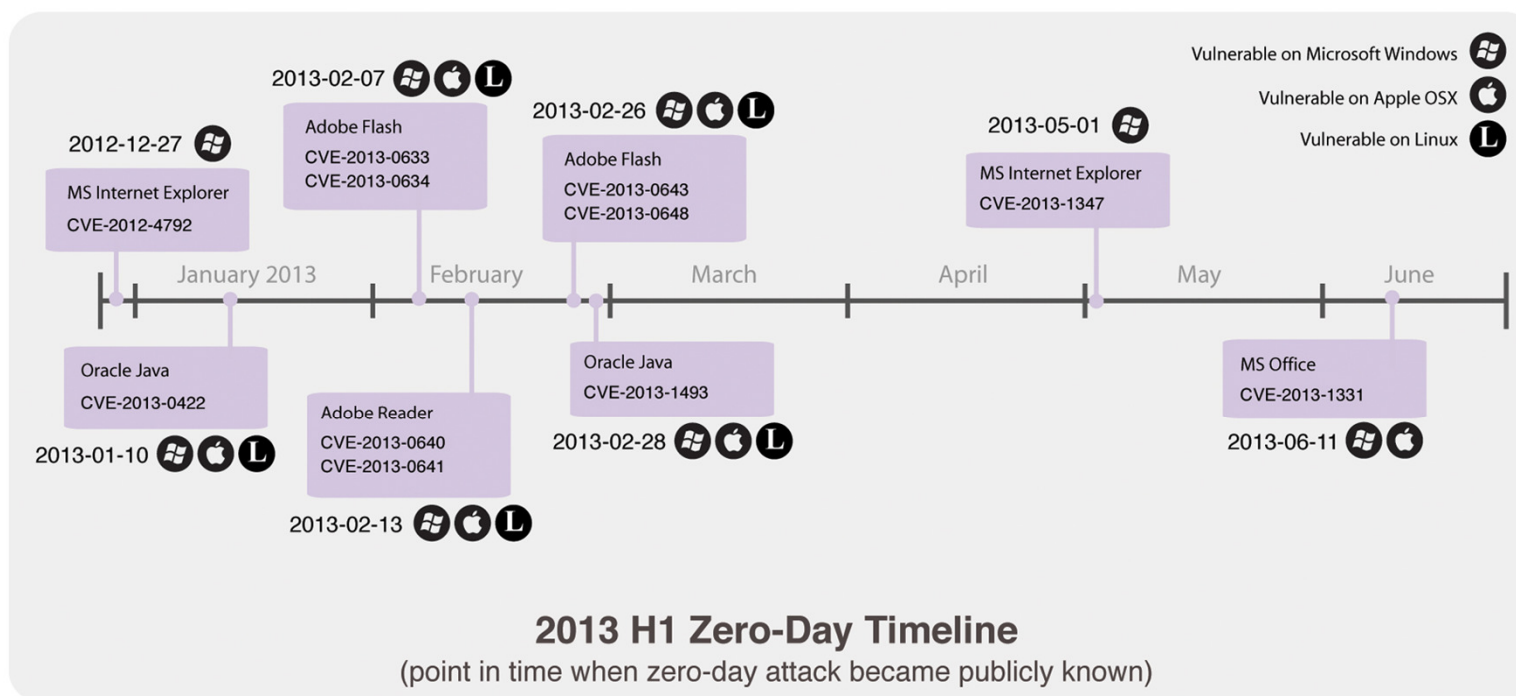
	2006	2007	2008	2009	2010	2011	2012
True Exploits	498	1067	1033	1061	1297	826	864
Percent of Total	7.2%	16.3%	13.4%	15.7%	14.9%	10.5%	10.6%

Mobile Exploits ~ 30%

Source: IBM X-Force® Research and Development

Zero Day Timeline

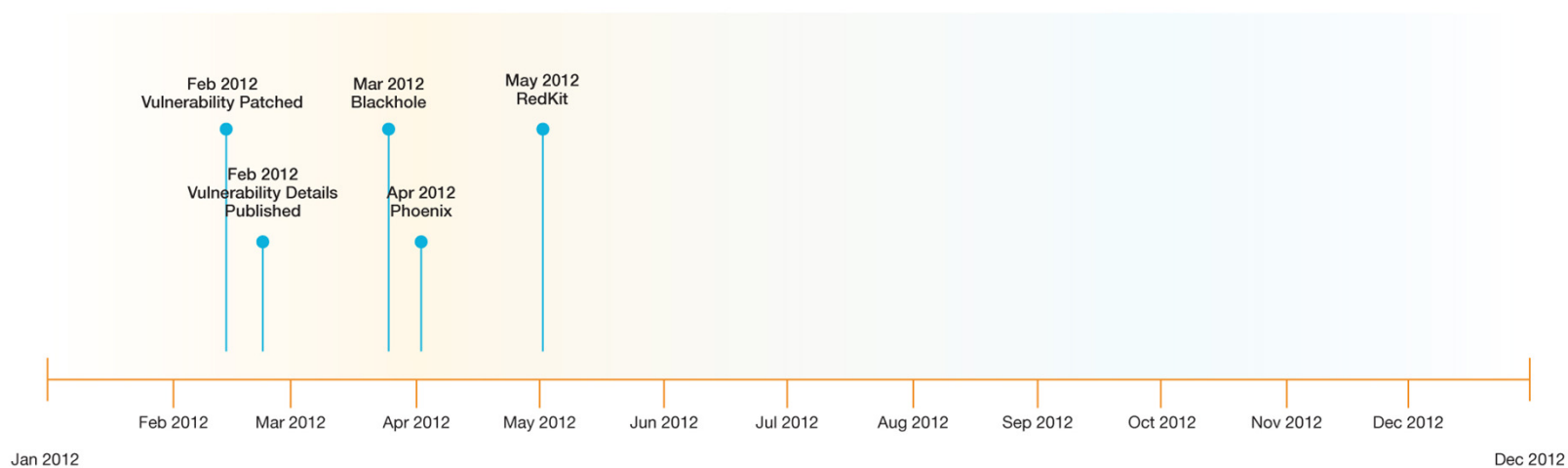
- IE, Java and Adobe
- Evolving from Spear Phishing to the Watering Hole



Source: IBM X-Force® Research and Development

CVE-2012-0507 Timeline

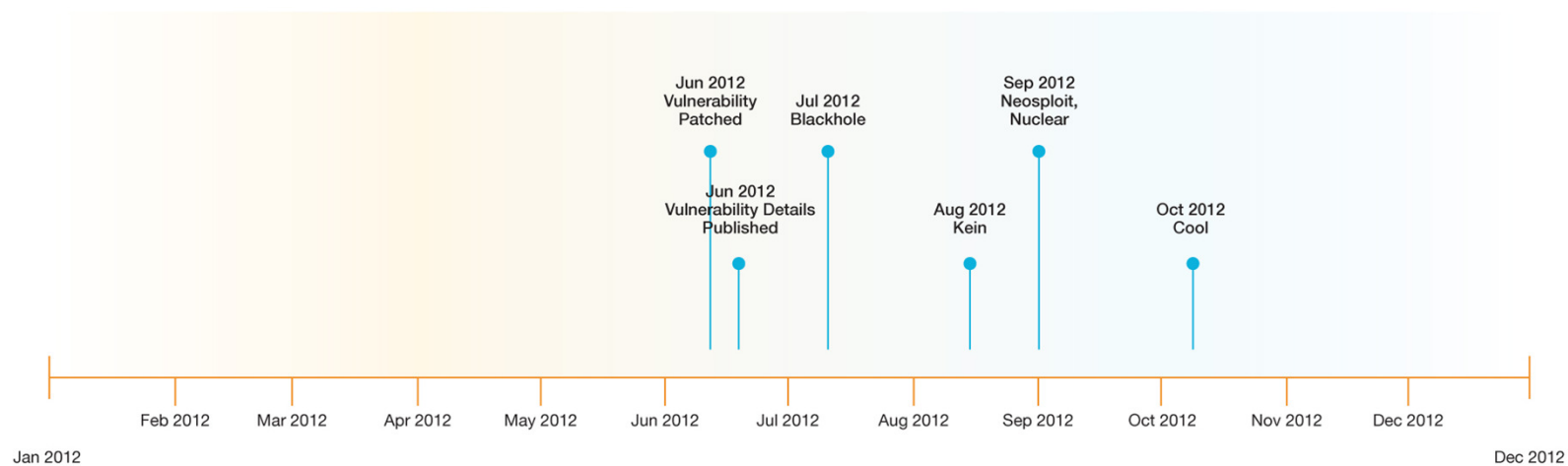
- Logical flaw in the handling of an array
- AtomicReferenceArray vulnerability



Source: IBM X-Force® Research and Development

CVE-2012-1723 Timeline

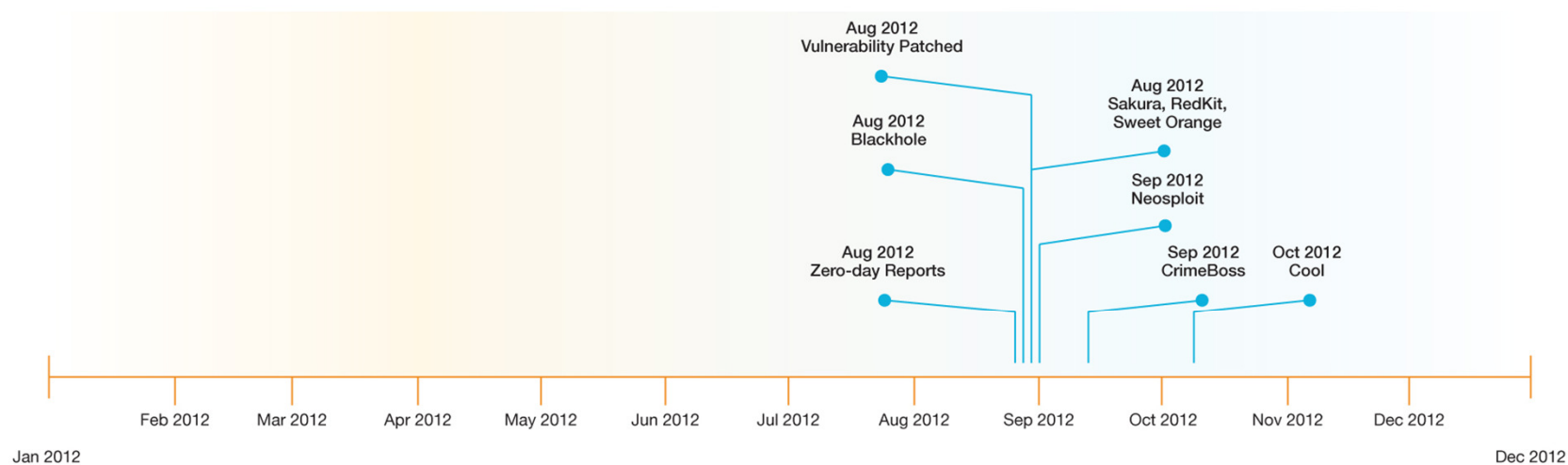
- Type-Confusion vulnerability in JRE



Source: IBM X-Force® Research and Development

CVE-2012-4681 Timeline

- Gondvv exploit
- Privilege escalation and bypass

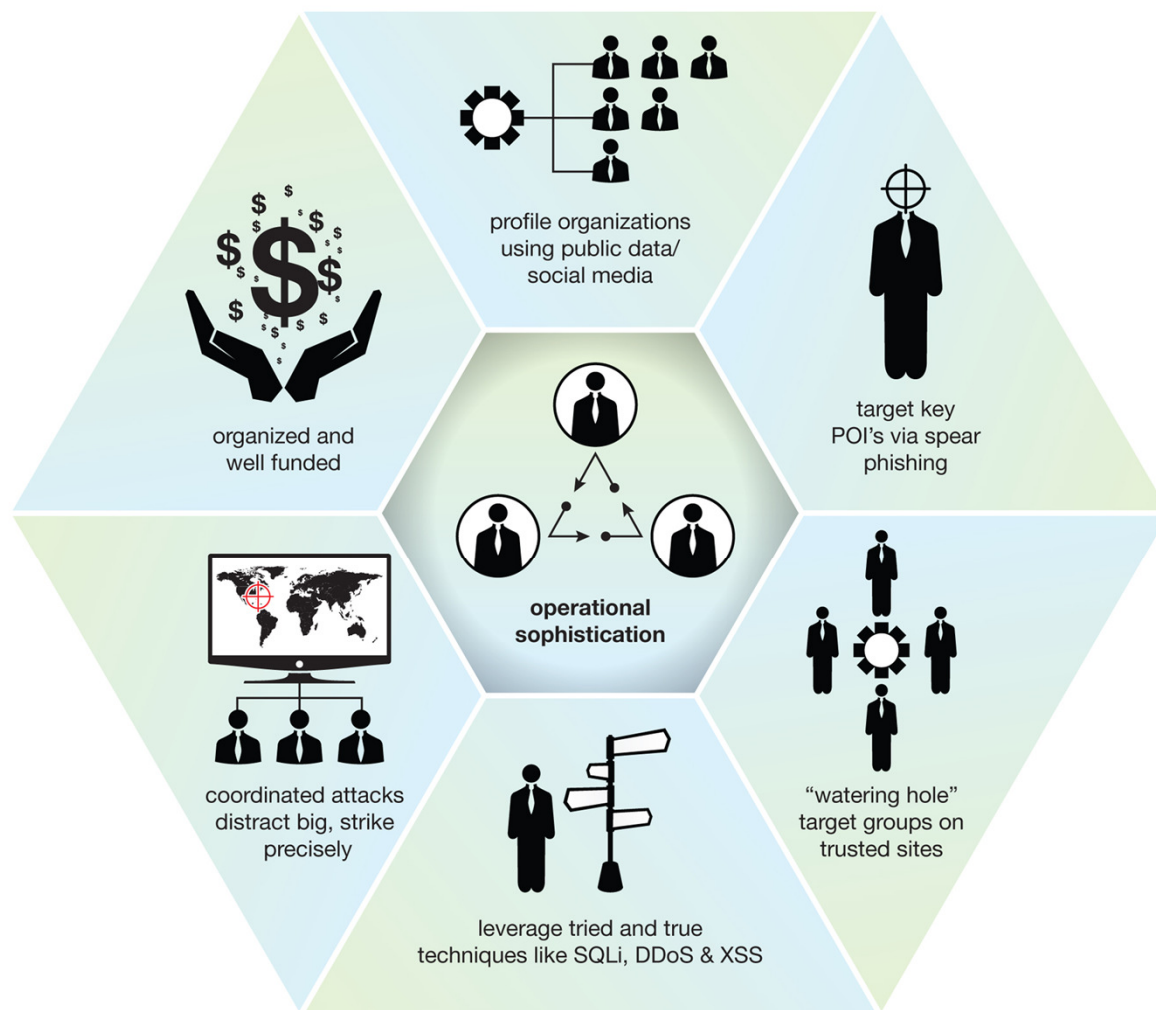


Source: IBM X-Force® Research and Development



How they do it

Operational sophistication is increasing...



Source: IBM X-Force® Research and Development

SQL Injection Attack Tools

地址: http://www.google.cn/search?as_q=inurl%3A.asp%3Fid%3D+and+intitle%3A%E5%85%AC%E5%8F%B8&complete=1&hl=zh-CN&newwindow=1&num=10 转到 停止 刷新 后退 前进

网页 图片 地图 资讯 视频 博客 更多 登录 信息

Google 高级搜索 搜索帮助 | Google

包含以下全部的字词 100 页结果

包含以下的完整字句

包含至少一个下列字词

小提示:

云南海泰贵金属是一家专业从事贵金属系列产品: 贵金属化合物、贵金属载体催化剂、贵金属催化传感器、贵金属半导体传感器、贵金属电镀的研发、生产, 含金、铂、钨、钼、...

www.cg160.com/userweb/company.asp?id=55442 - 22k - 网页快照 - 类似网页

扫描页面漏洞
 仅扫描地址栏
 停止扫描
 强行终止

安全漏洞 | 服务器错误

完整URL	响应时间	可利用度	确定漏洞方式	注入方式	注入类型	数据库	页面标题	错误指纹
http://www.cn/info.asp?id=6	1609	6	aND 8=8 + aND 8=3	AND	数字型	未探测	康馨催乳公司 催乳	
http://www.berstech.com/shownews.asp?	5281	5	aND 8=8 + aND 8=3	AND	数字型	未探测	中赢橡胶技术有限公司	
http://www.berstech.com/ProductShow.	6796	5	aND 8=8 + aND 8=3	AND	数字型	未探测	中赢橡胶技术有限公司	
http://www.u.com/sinonews/list.asp?i	438	7	aND 8=8 + aND 8=3	AND	数字型	未探测	江阴模塑集团有限公司	80040e21, :
http://www.gov.cn/qyml/corporation_y	2672	7	aND 8=8 + aND 8=3	AND	数字型	未探测	伟创力电子科技(上海)	80040e21, :
http://www.com/00new/list.asp?id=6	4610	5	aND 8=8 + aND 8=3	AND	数字型	未探测	上海假肢厂有限公司	
http://www.com.cn/products_list.as	4781	6	aND 8=8 + aND 8=3	AND	数字型	未探测	中怡数宽科技(苏州)	80040e21, :
http://www.ha.com/CN/show.asp?id=11	5078	1	aND8=8 + aND8=3	AND	数字型	未探测	浪莎针织有限公司	
http://dg.com/zfbz/zfnr.asp?id=78	515	5	XoR 8=3 + XoR 8=8	XOR	数字型	未探测	中国铁道东莞分公司-	

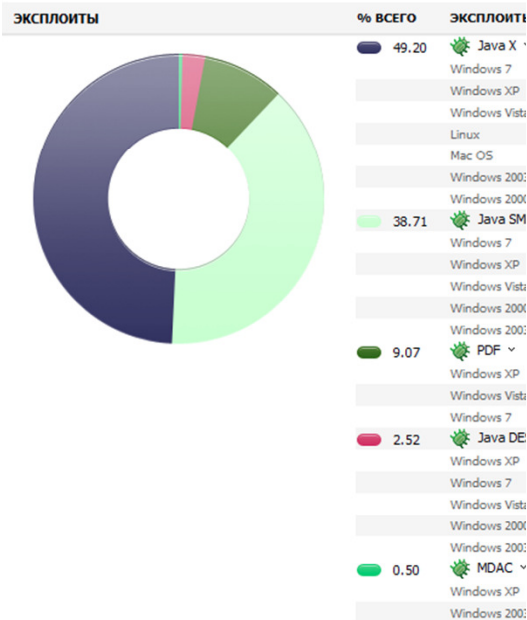
- * Automatic page-rank verification
- * Search engine integration for finding "vulnerable" sites
- * Prioritization of results based on probability for successful injection
- * Reverse domain name resolution
- * etc.

Forbes 2012 Vulnerability Price List

ADOBE READER	\$5,000-\$30,000
MAC OSX	\$20,000-\$50,000
ANDROID	\$30,000-\$60,000
FLASH OR JAVA BROWSER PLUG-INS	\$40,000-\$100,000
MICROSOFT WORD	\$50,000-\$100,000
WINDOWS	\$60,000-\$120,000
FIREFOX OR SAFARI	\$60,000-\$150,000
CHROME OR INTERNET EXPLORER	\$80,000-\$200,000
IOS	\$100,000-\$250,000

Source: <http://www.forbes.com/sites/andygreenberg/2012/03/23/shopping-for-zero-days-an-price-list-for-hackers-secret-software-exploits/>

Blackhole Crimeware



Blackhole Exploit Kit

- First appeared in August 2007
- Advertised as a “Systems for Network Testing”
- Protects itself with blacklists and integrated antivirus
- Comes in Russian or English
- Currently the most purchased exploit pack

Flexible Pricing Plan

• Purchase

- \$1500/annual
- \$1000/semi-annual
- \$700/quarterly

• Lease

- \$50/24 hours
- \$200/1 week
- \$300/2 weeks
- \$400/3 weeks
- \$500/month

*((\$35 domain name change fee if necessary)

Blackhole ^β СТАТИСТИКА ПОТОКИ ФАЙЛЫ БЕЗОПАСНОСТЬ НАСТРОЙКИ Выйти

Обновление: 5 сек.

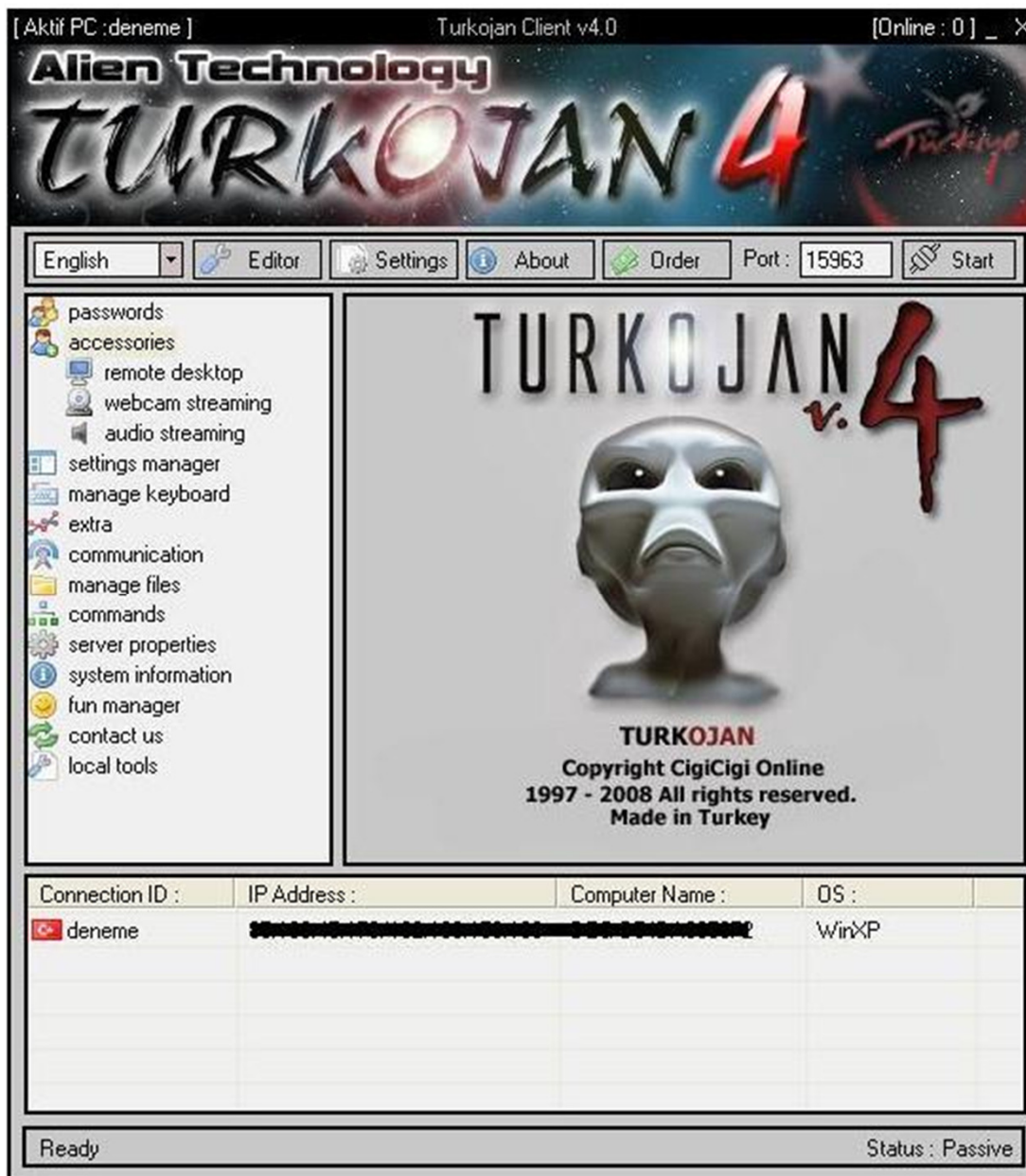
КАТЕГОРИИ	ЗАГРУЗКИ	% ↑
Java X >	584	49.20
Java SMB >	460	38.75
PDF >	108	9.10
Java DES >	29	2.44
MDAC >	6	0.51

ИД	ХИТЫ ↑	ХОСТЫ	ЗАГРУЗКИ	%
United States	12417	10981	1119	10.19
India	154	101	9	8.91
France	63	35	4	11.43
Japan	47	9	3	33.33
Germany	37	28	0	0.00
Spain	31	12	2	16.67
Italy	31	10	0	0.00
Indonesia	29	17	5	29.41
Ukraine	26	16	0	0.00
Russia	26	13	1	7.69
Canada	24	16	1	6.25
China	22	14	2	14.29
South Korea	19	6	0	0.00
Japan	18	15	0	0.00
Germany	18	11	0	0.00
Итого	327	222	41	18.55

Создать виджет

Trojan Creator Kits

- Constructor/Turkojan
- V.4 New features
 - Remote Desktop
 - Webcam Streaming
 - Audio Streaming
 - Remote passwords
 - MSN Sniffer
 - Remote Shell
 - Advanced File Manager
 - Online & Offline keylogger
 - Information about remote computer
 - Etc..



It's just business...



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 available with this version
- Realtime Screen viewing(controlling is disabled)
- Notifies chngements 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 chngements on clipboard and save them
- Technical support after installing software
- Viewing pictures without any download(Thumbnail Viewer)

Price : 249\$ (United State Dollar)



Who is doing it



Cybercrime is a **\$12.5 billion** global market

Source: <http://group-ib.com>

What's different about Advanced Persistent Threats?

Advanced

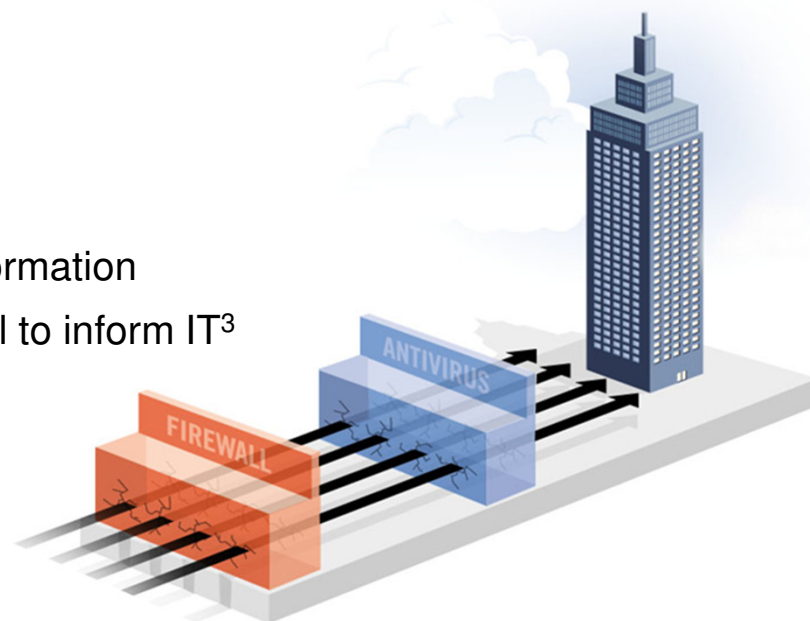
- Exploiting unreported (zero-day) vulnerabilities
- Advanced, custom malware is not detected by antivirus products
- Coordinated, well researched attacks using multiple vectors

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
- 210 day average from breach to detection²

Threat

- Targeted at specific individuals and groups within an organization; aimed at compromising confidential information
- 1 in 5 employees will open a suspicious email and fail to inform IT³
- Not random attacks – they are “out to get you”



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

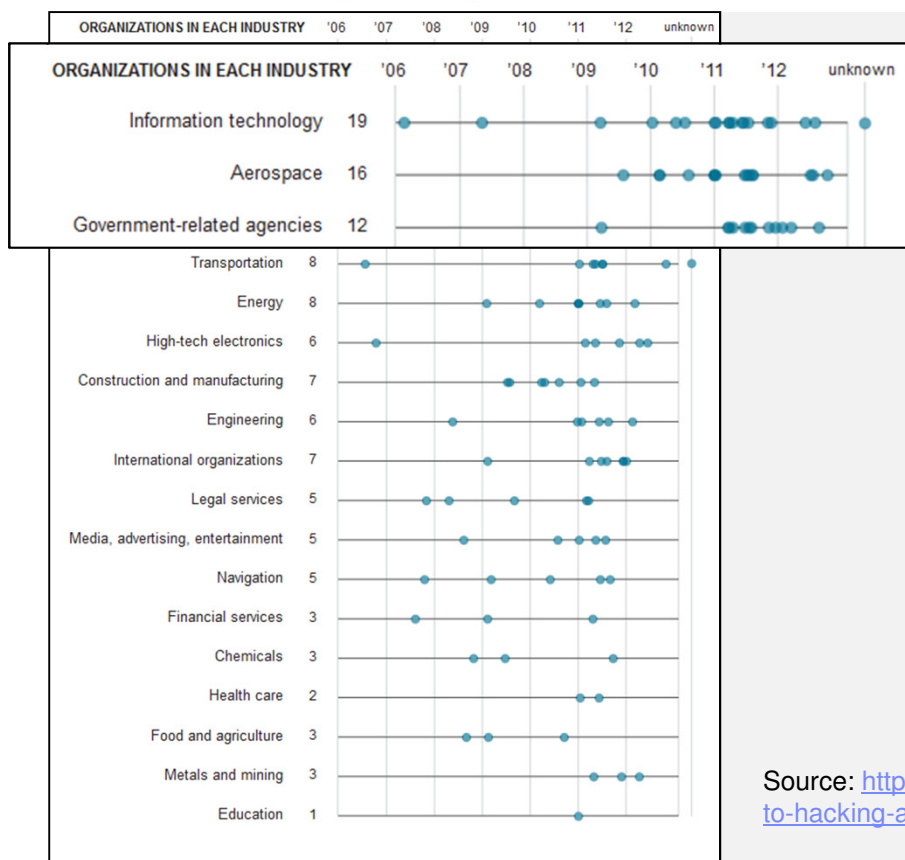
2) Source: 2013 Trustwave Global Security Report

3) Source: Courion Research, October 13, 2013

Today's News: NY Times publishes detailed account on state-sponsored attacks

The New York Times

Industries Targeted by the Hackers



“ A growing body of digital evidence leaves little doubt that an overwhelming percentage of the attacks on American corporations, organizations and government agencies originate in and around [one location]. ”

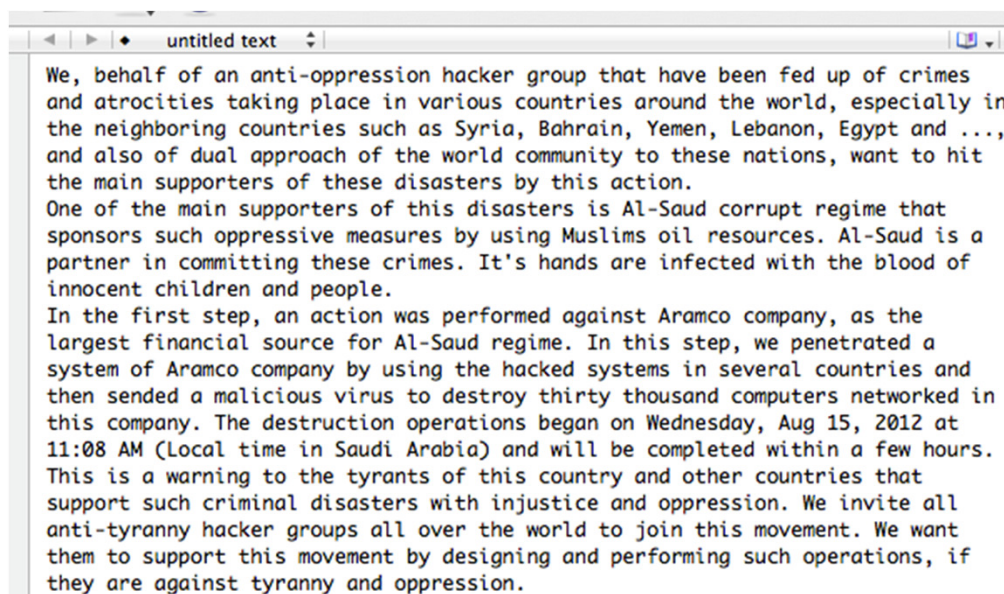
Source: <http://www.nytimes.com/2013/02/19/technology/chinas-army-is-seen-as-tied-to-hacking-against-us.html>

Famous APT Events...

- Operation Ababil - Iz Ad-Din al-Qassam cyber fighters
 - Three separate DDoS attackers
 - Targeting Major US Banks including J.P. Morgan Chase, Bank of America, US Bancorp, and PNC
- Moonlight Maze (1998-2001)
 - 3-year long campaign targeted against government systems
- Titan Rain (2003)
 - Targeted US Government and US Government contractors
- Ghostnet (2009)
 - Discovered in a 10 month investigation
- Operation Aurora
 - Targeted Fortune 100 companies
 - Moved APT to a marketing tool
- Night Dragon (2009-2010)
 - Targeted global energy
- StuxNet (Flame, Duqu, Gauss, Mini-Flame...)

Attacks on Aramco

- Highly sophisticated
- Likely government sponsored
- Infiltrated 30,000+ computers



We, behalf of an anti-oppression hacker group that have been fed up of crimes and atrocities taking place in various countries around the world, especially in the neighboring countries such as Syria, Bahrain, Yemen, Lebanon, Egypt and ..., and also of dual approach of the world community to these nations, want to hit the main supporters of these disasters by this action.

One of the main supporters of this disasters is Al-Saud corrupt regime that sponsors such oppressive measures by using Muslims oil resources. Al-Saud is a partner in committing these crimes. It's hands are infected with the blood of innocent children and people.

In the first step, an action was performed against Aramco company, as the largest financial source for Al-Saud regime. In this step, we penetrated a system of Aramco company by using the hacked systems in several countries and then sended a malicious virus to destroy thirty thousand computers networked in this company. The destruction operations began on Wednesday, Aug 15, 2012 at 11:08 AM (Local time in Saudi Arabia) and will be completed within a few hours.

This is a warning to the tyrants of this country and other countries that support such criminal disasters with injustice and oppression. We invite all anti-tyranny hacker groups all over the world to join this movement. We want them to support this movement by designing and performing such operations, if they are against tyranny and oppression.

Hactivists

- Definition:
 - Hactivist = Hacker Activist
 - The use of legal and/or illegal digital tools in pursuit of political ends
- Realities:
 - Membership amongst hactivist groups has grown rapidly over the past few years
 - Participation has become simplified via freely downloadable tools

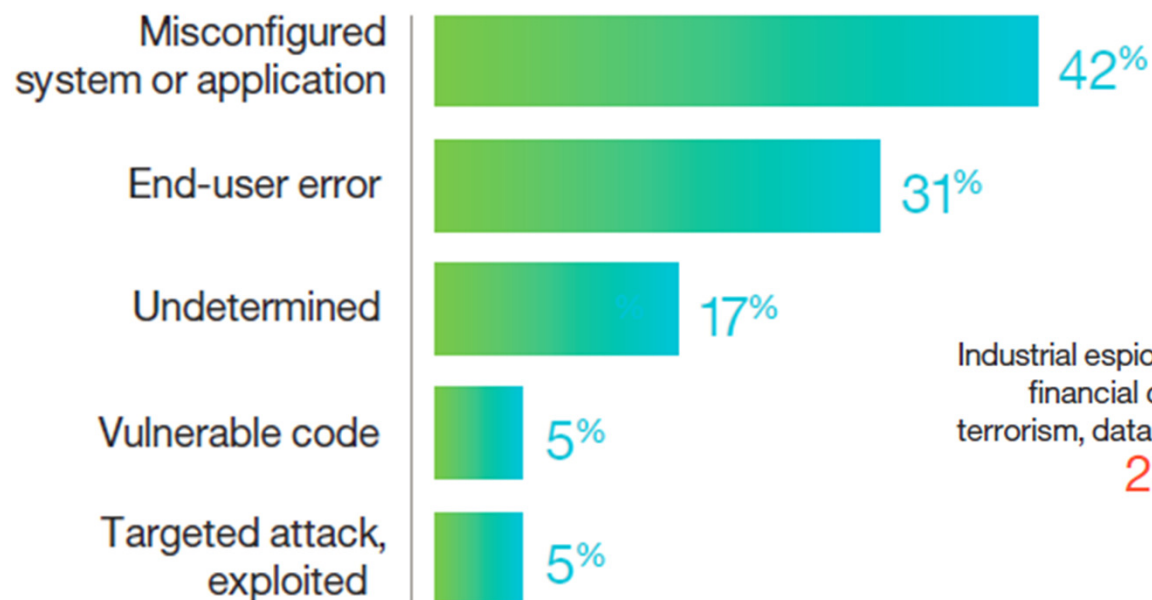


(UGNazi Hactivist Group Logo)

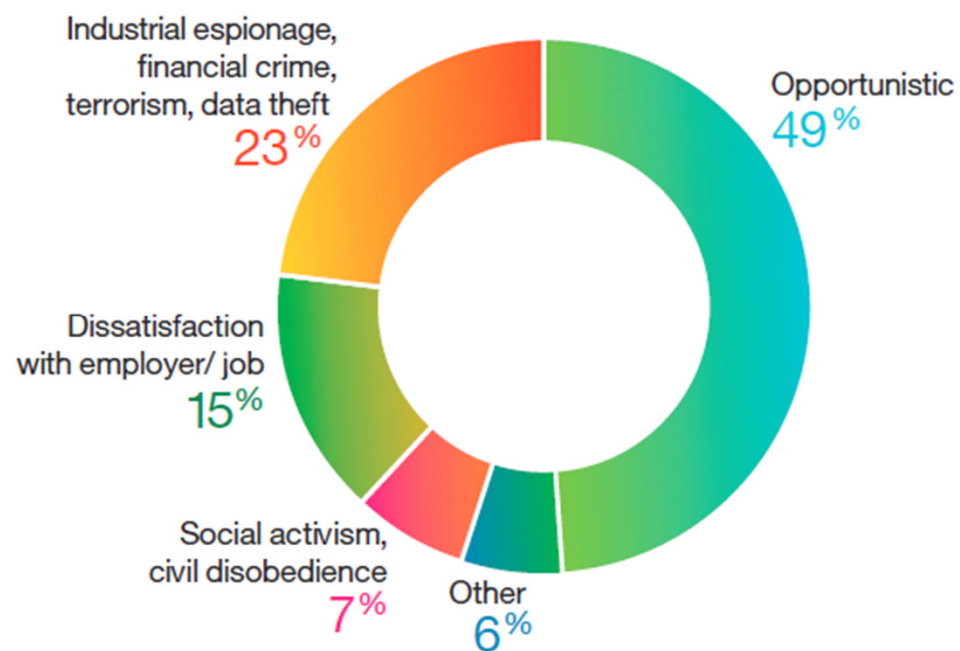
How to minimize the risk?

E&U Focus Areas

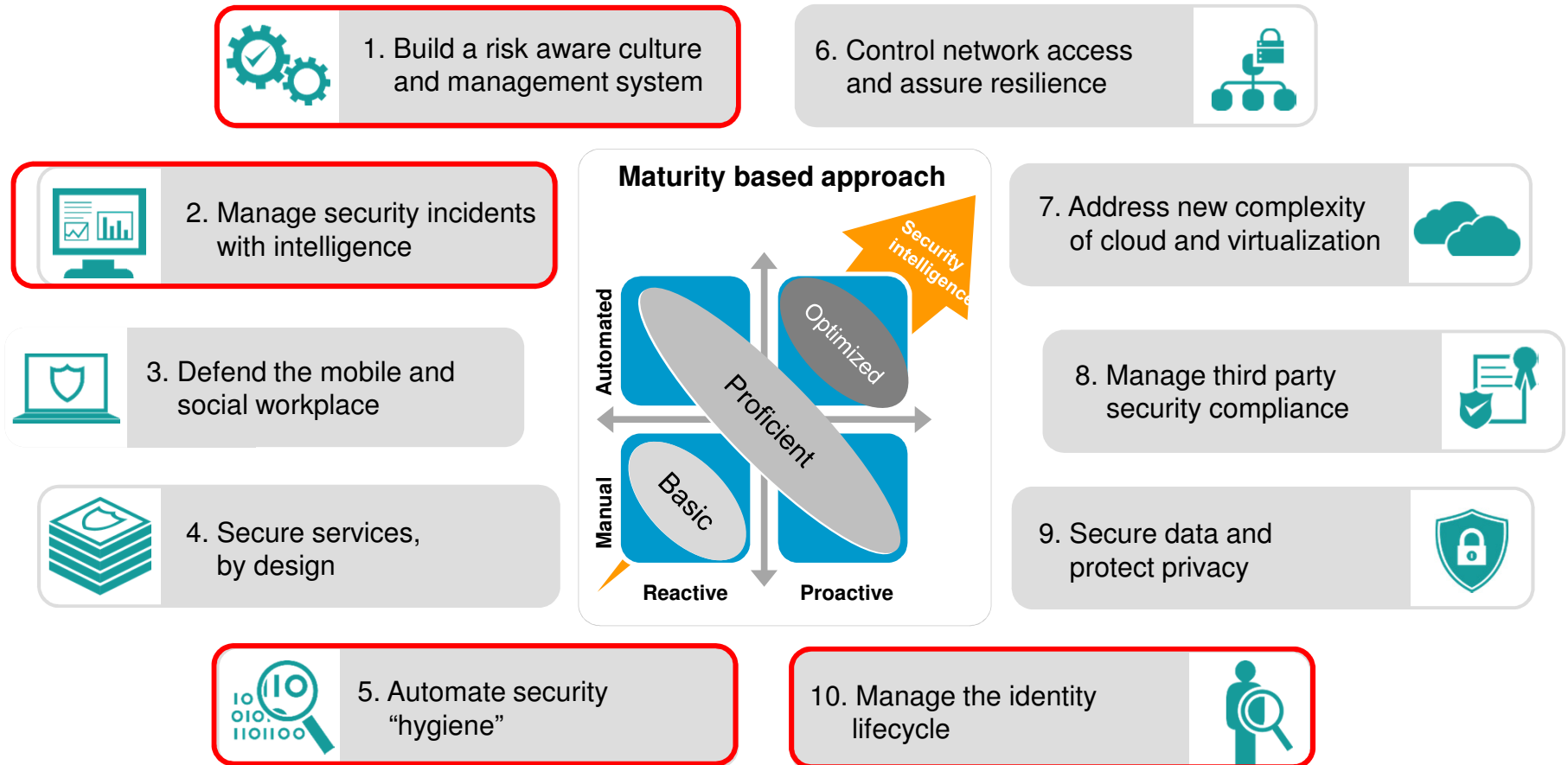
How breaches occur



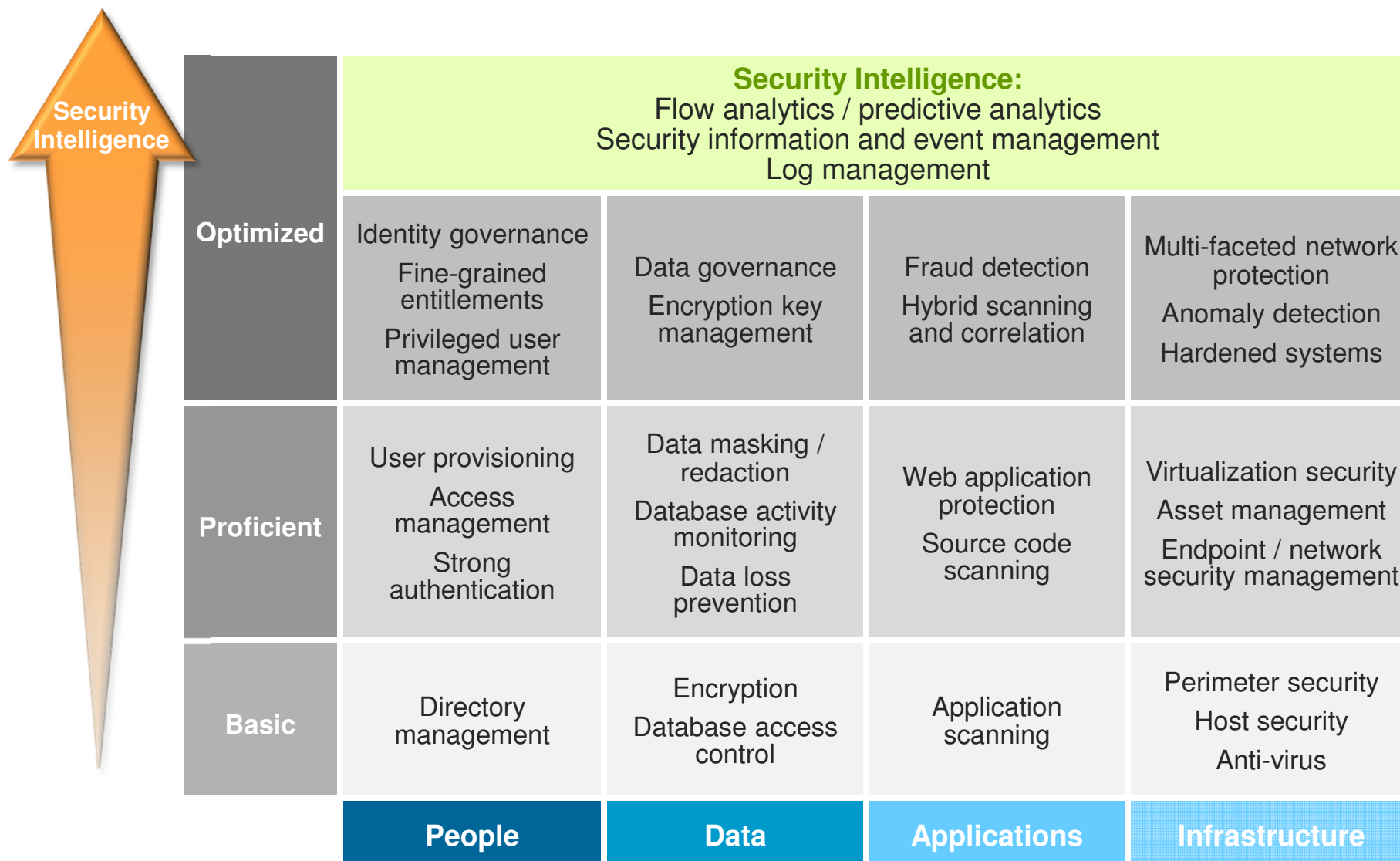
Attacker motivation



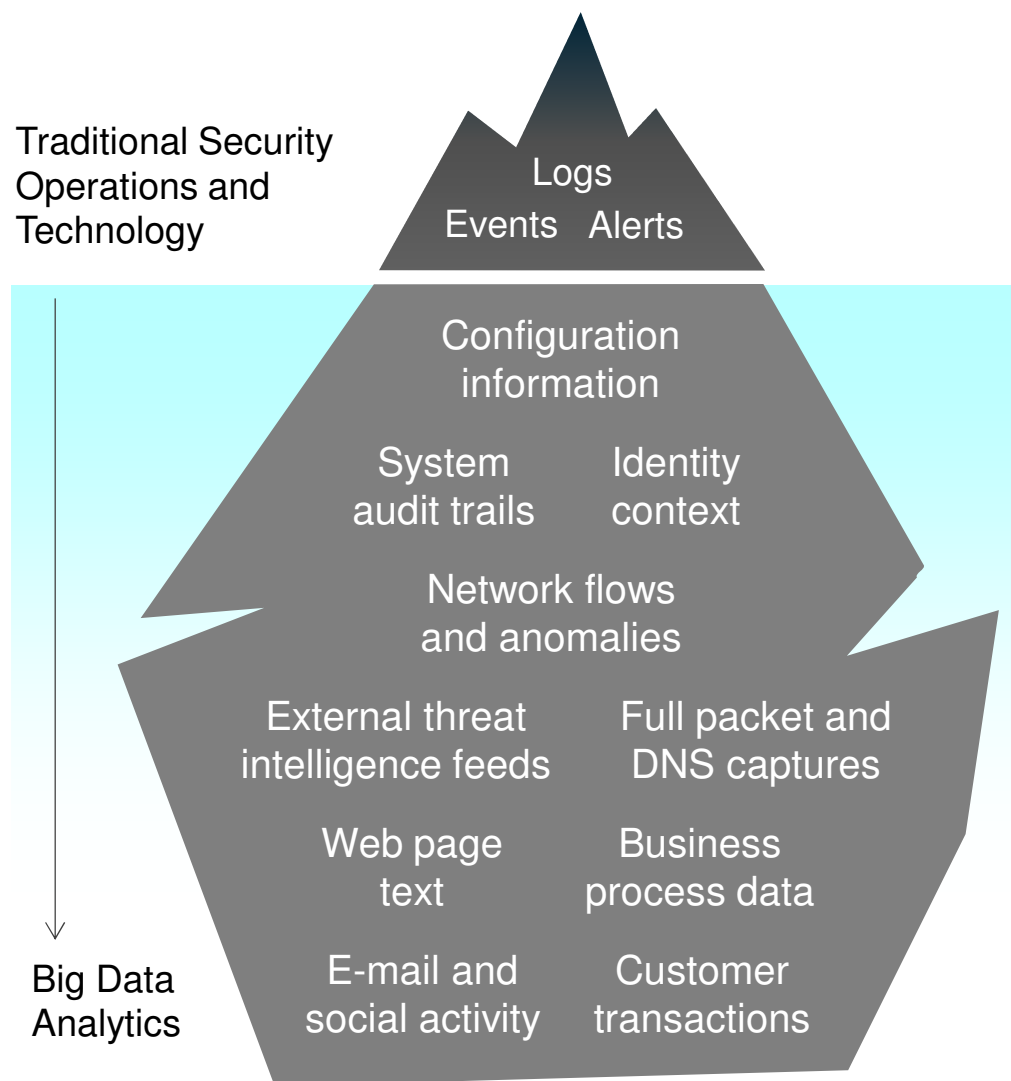
Essential Practices



Move to an optimized state across all security domains.



Extend Security Intelligence with complementary Big Data solutions



There is a growing need to identify and protect against these threats by building insights from broader data sets

1. Analyze a **variety** of non-traditional and unstructured datasets to improve security
2. Significantly increase the **volume** of data stored for forensics and historical security analysis
3. Visualize and query data in new ways
4. Integrate Big Data analysis with existing security operations

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>



Subscribe to X-Force alerts at
<http://iss.net/rss.php> or
Frequency X at

<http://blogs.iss.net/rss.php>



Attend in-person
events

<http://www.ibm.com/events/calendar/>



Join the Institute for
Advanced Security

www.instituteforadvancedsecurity.com

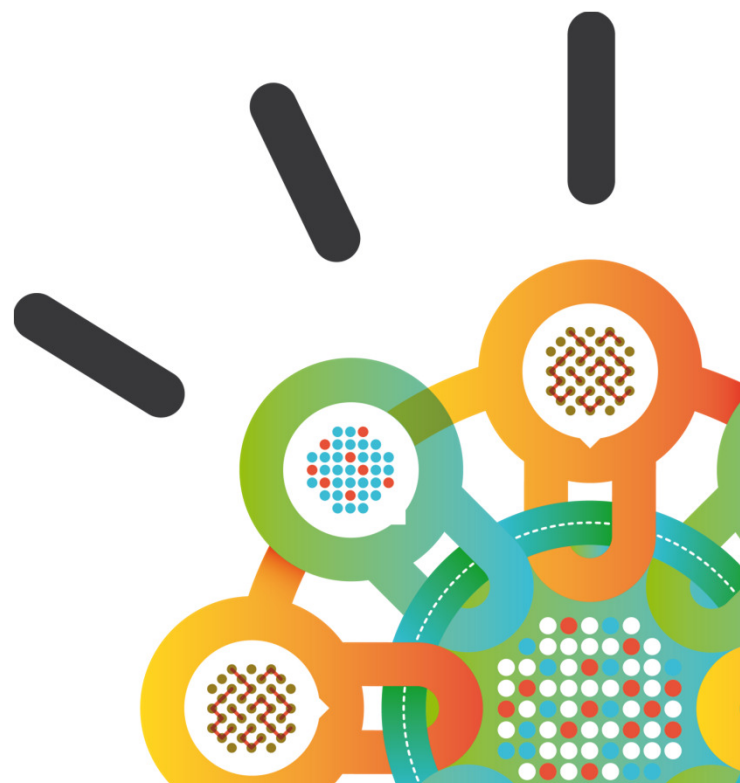


Subscribe to the security
channel for latest security
videos

www.youtube.com/ibmsecuritysolutions

Security Intelligence.
Think Integrated.

Thank You!



Why IBM?

Security is a top priority for IBM and significant investments have been made to enable us to continue leading in this space

- Over 100 researchers, representing 6 major research centers worldwide. Areas of research include:
 - Trusted platforms
 - Secure co-processors
 - Next-generation security analytics
 - Mobile computing
 - Biometrics
 - Security for cloud computing
 - Homomorphic encryption

- IBM has launched a *Cybersecurity Initiative* to build security skills
 - Working closely with over 80 universities worldwide
 - Supporting research efforts
 - Educating faculty members
 - Providing guest lectures and internships

“Looking ahead, we continue to invest to deliver innovations for the enterprise in key areas such as big data, mobile solutions, social business and security”

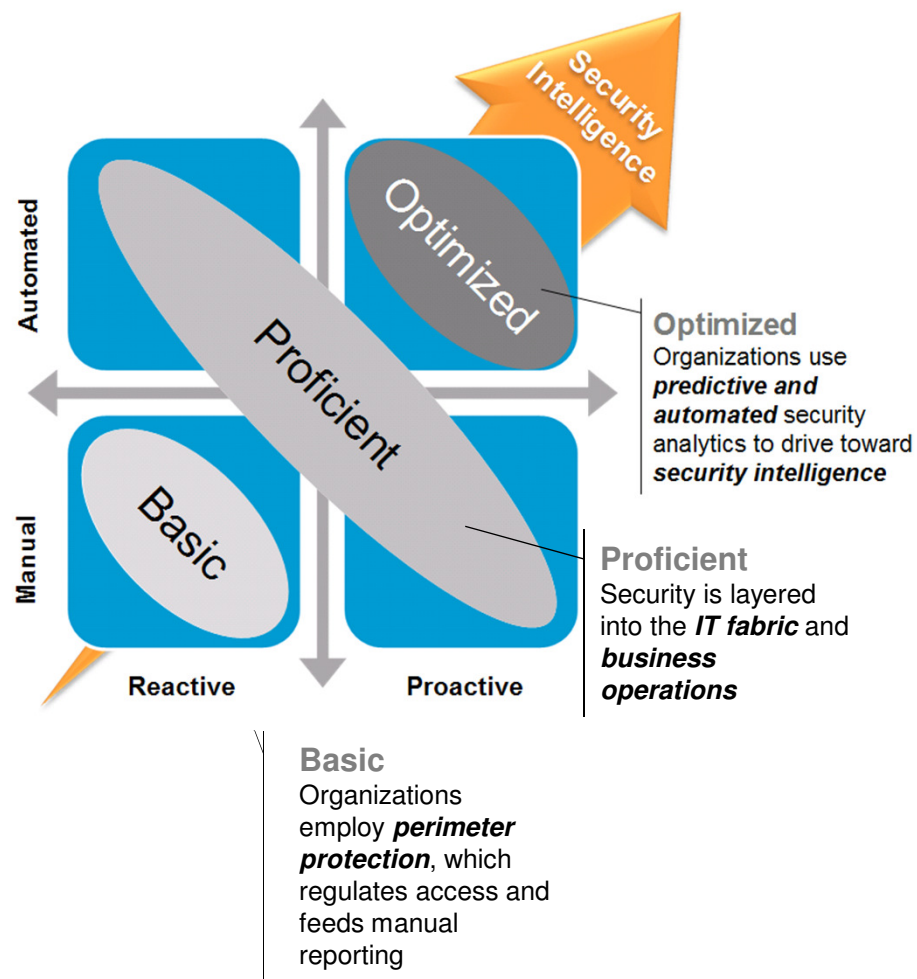
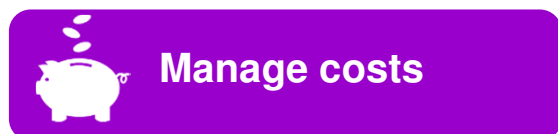
Ginny Rometty, CEO IBM, Jan 2013

IBM President and Chief Executive Officer Ginny Rometty, joined by Chairman Sam Palmisano, met with US President Barack Obama at the White House in early March, 2012. Rometty discussed issues including cybersecurity policy, and the global economic situation with President Obama and his senior economic team.



IBM has made significant investments, while leveraging our own global presence and experience, to help clients accomplish their business objectives and reach a more optimized security state

Client Business Objectives



IBM can provide unmatched global coverage and security awareness

4,300
Strategic outsourcing security delivery resources

1,200
Professional services security consultants

650
Field security specialists

400
Security operations analysts

10
Security research centers

10
Security operations centers

14
Security development labs



Security Solution Development Centers
 Security Operations Centers
 Institute for Advanced Security Branches
 Security Research Centers



IBM X-Force Expertise	Managed Services Excellence
<ul style="list-style-type: none"> 150M intrusion attempts daily 46,000 documented vulnerabilities 40M unique phishing / spam attacks Millions of unique malware samples Billions of analyzed web pages 1000+ security patents 	<ul style="list-style-type: none"> 20,000+ devices under contract 3,700+ MSS clients worldwide 15B+ events managed per day 133 monitored countries (MSS) Unique research and reports



Clients are asking IBM to expand the role we play with a their security program

Global Threat Operations Center

Security Governance

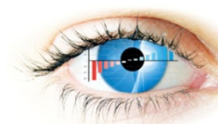
Advanced Threat Analysis Center

- Threat Intelligence Gathering
- Event and Vulnerability Analysis
- Impact Analysis
- Incident Management
- Investigations
- Enforcement Optimization
- Risk Assessments, Briefings, and Advisories



Hunter Team

- Penetration testing
 - Infrastructure
 - Application
 - Social
 - Phishing
- Awareness
- Attack modeling
- Assessments
- Ad-hoc projects



Security Operations Center

- Security Monitoring
- Incident Escalation and Response
- SIEM Intelligence Platform Administration
- Application & Device Management
- Configuration Management
- Policy Management



Security Intelligence Platform

- Aggregate security event, log and flow data
- Correlation, rules and feeds



IBM's X-Force organization is a unique capability that benefits our clients and is unmatched in the industry

IBM X-Force Research and Development

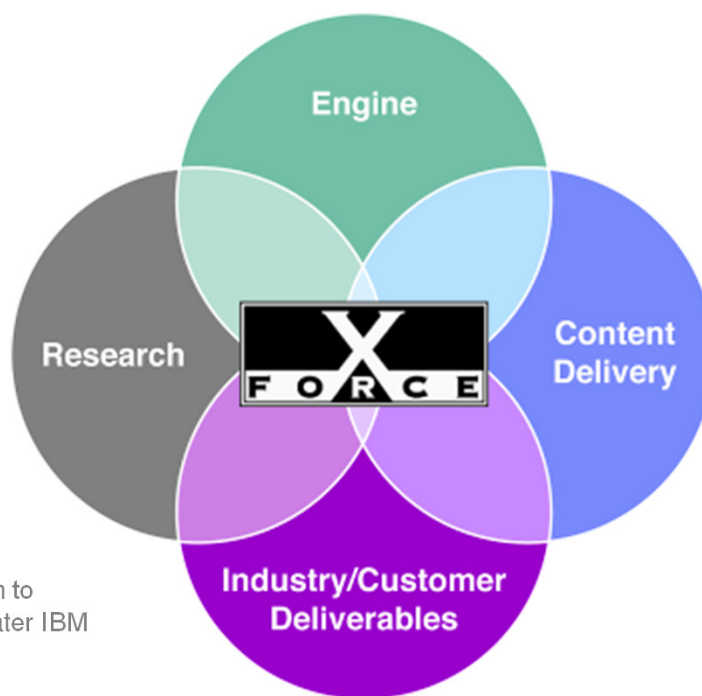
The world's leading enterprise security R&D organization

Engine

- Support content stream needs and capabilities
- Support requirements for engine enhancement
- Maintenance and tool development

Research

- Support content streams
- Expand current capabilities in research to provide industry knowledge to the greater IBM



Global security operations center (infrastructure monitoring)

Content Delivery

- Continue third party testing Dominance
- Execute to deliver new content streams for new engines

Industry/Customer Deliverables

- Blog, Marketing and Industry Speaking Engagements
- X-Force Database Vulnerability Tracking
- Trend Analysis and Security Analytics

X-Force Mission: To protect our customers from security threats on the Internet by developing a comprehensive knowledge of vulnerabilities and attack methodologies and applying that knowledge through effective protection technologies.

IBM Security Services Key Differentiators



Breadth of offerings

- Broadest security solution portfolio in the industry
- Professional and managed security services



Integrated solutions and services

- Families and bundles of integrated solutions
- Leveraging of services and data



Flexible options

- Solutions are standardized to provide economies of scale, but can be customized to meet unique requirements
- Remote delivery and on-premise delivery



Detailed threat and business analytics

- Latest threat and business analytics
- Integrated IBM X-Force® Security intelligence
- Work flow, ticketing, emergency response and forensics, and comprehensive reporting



Global delivery excellence

- Uniform delivery in hundreds of countries
- Global network of skilled consultants
- Certified delivery expertise around the world
- Standards-based delivery processes

Aligned to address our typical client challenges:



Manage costs



Reduce Risk

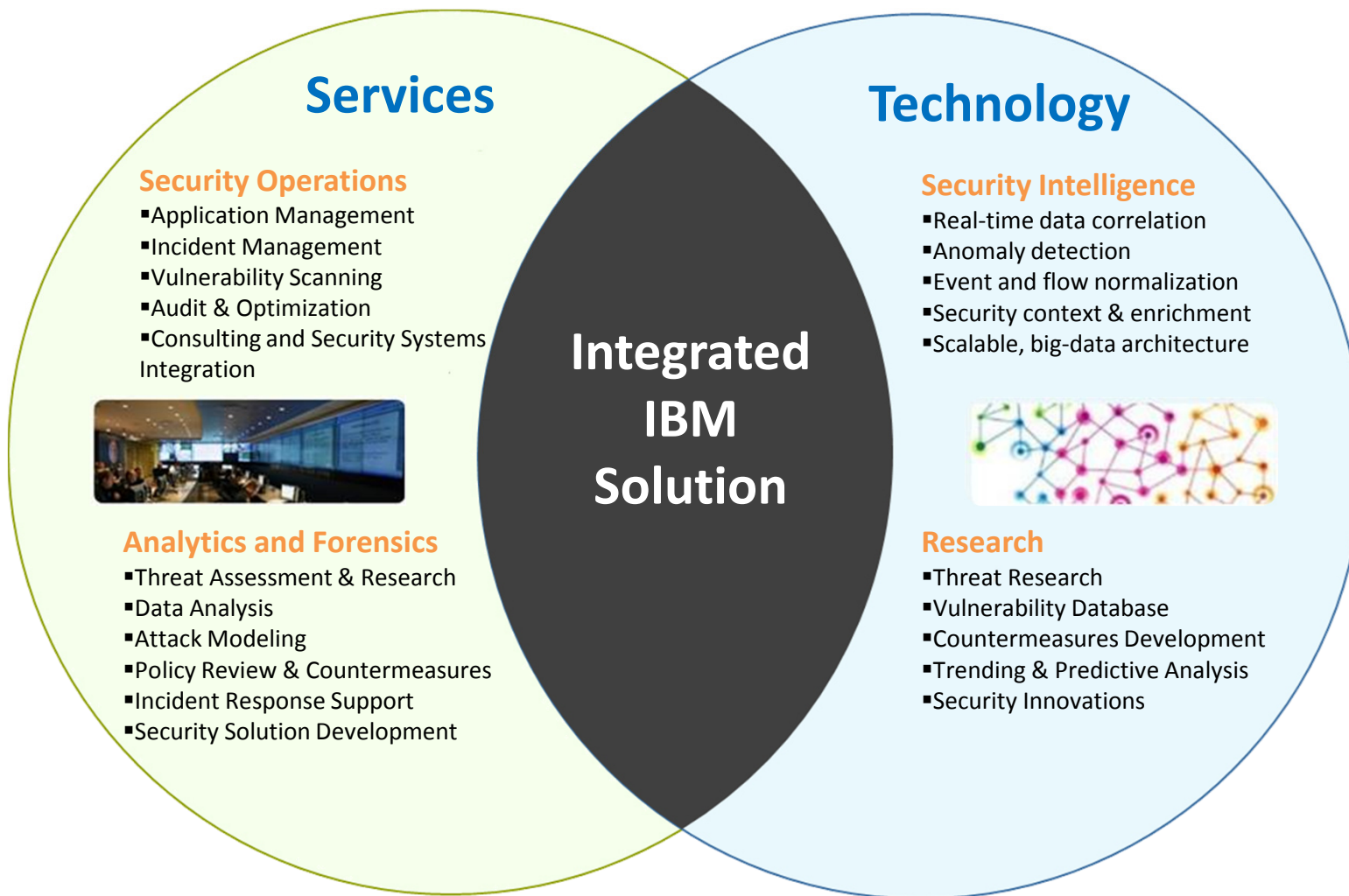


Enable business



Support compliance

Our clients tell us the power of IBM as a partner is realized when we leverage our security services, technology and research into an integrated IBM solution



The IBM Security Framework can help you with the challenges of cost, complexity and compliance

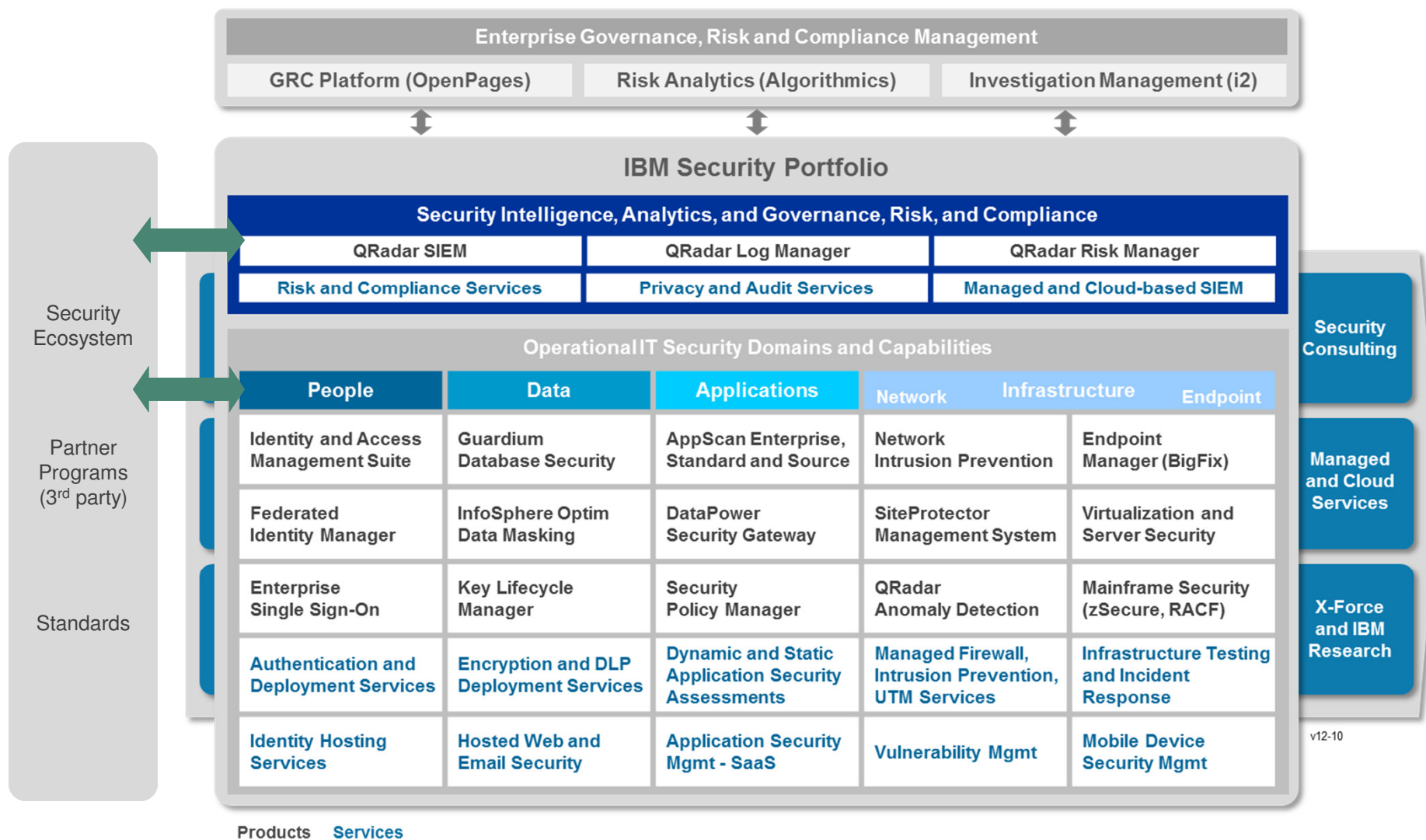


Designed to help:

- Enable innovation through security-rich, end-to-end infrastructure, platforms and services
- Reduce number and complexity of required security controls
- Reduce redundant security expenses
- Improve organizational and operational agility and resiliency
- Leverage industry expertise to help unify policy management
- Deliver needed visibility, control, security intelligence and automation

Capability: End-to-end security coverage

Bringing Products and Services together to deliver Solutions

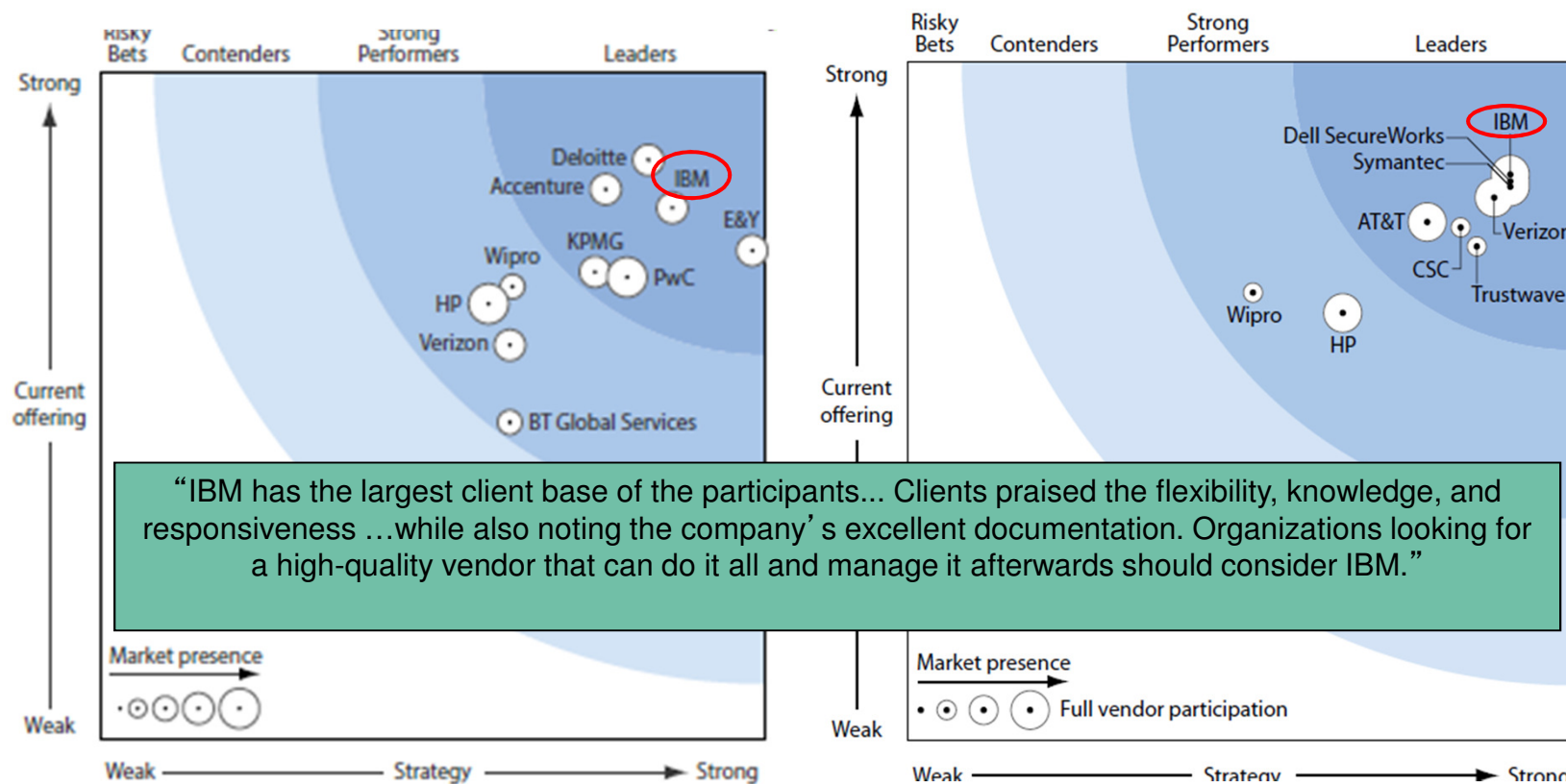


v12-10

And this experience has resulted in recognition from the marketplace

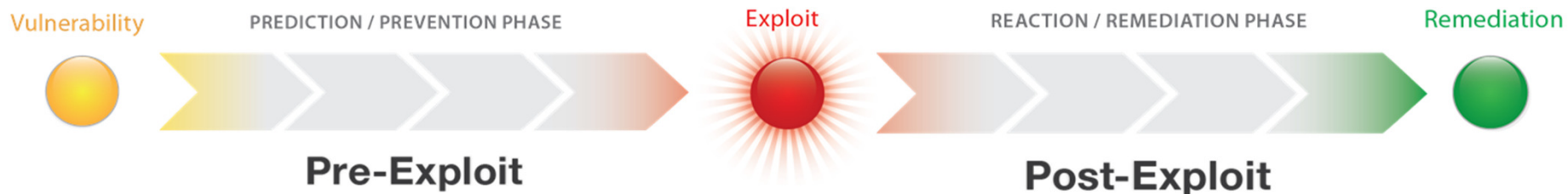
Security Consulting

Managed Security Services



Source: Forrester Research Inc. "Forrester Wave™": Information Security Consulting Services, Q1 2013". And Forester Wave: Managed Security Services providers Q1, 2012. Full report can be accessed at <http://www.ibm.com>

There is the need to address the full security intelligence timeline



Prediction & Prevention

Risk Management Vulnerability Management
 Configuration Monitoring
 IBM X-Force® Threat Intelligence
 Compliance Management
 Reporting and Scorecards

Reaction & Remediation

SIEM Log Management
 Incident Response
 Network Anomaly Detection Packet Forensics
 Database Activity Monitoring
 Data Loss Prevention



The security environment continues to be increasingly challenging with ever greater impact of incidents

The total number of attacks logged in the first eight months of 2012 by IBM's Cyber intelligence & Response Team is **40% higher** than attacks reported in all of 2011.

Threat	Profile Type	Share of Incidents	Attack Type
Advanced threat / mercenary	<ul style="list-style-type: none"> National governments Terrorist cells Crime Cartels 	23% ▲	<ul style="list-style-type: none"> Espionage Intellectual property theft Systems disruption Financial Crime
Insiders	<ul style="list-style-type: none"> Insiders - employees, contractors, outsourcers 	15% ▼	<ul style="list-style-type: none"> Financial Crime Intellectual Property Theft Unauthorized Access/
Hactivist	<ul style="list-style-type: none"> Social Activists 	7% ▲	<ul style="list-style-type: none"> Systems disruption Web defacement Information Disclosure
Opportunist	<ul style="list-style-type: none"> Worm and virus writers "Script Kiddies" 	49% ▼	<ul style="list-style-type: none"> Malware propagation Unauthorized Access Web defacement

Source: Government Accountability Office, Department of Homeland Security's Role in Critical Infrastructure Protection Cybersecurity, GAO-05-434; IBM CyberSecurity Intelligence & Response Team, September 2012



ibm.com/security

© **Copyright IBM Corporation 2012. 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.