

IBM SolutionsConnect 2013

Turning Opportunity into Outcomes.



Today's Threat Landscape

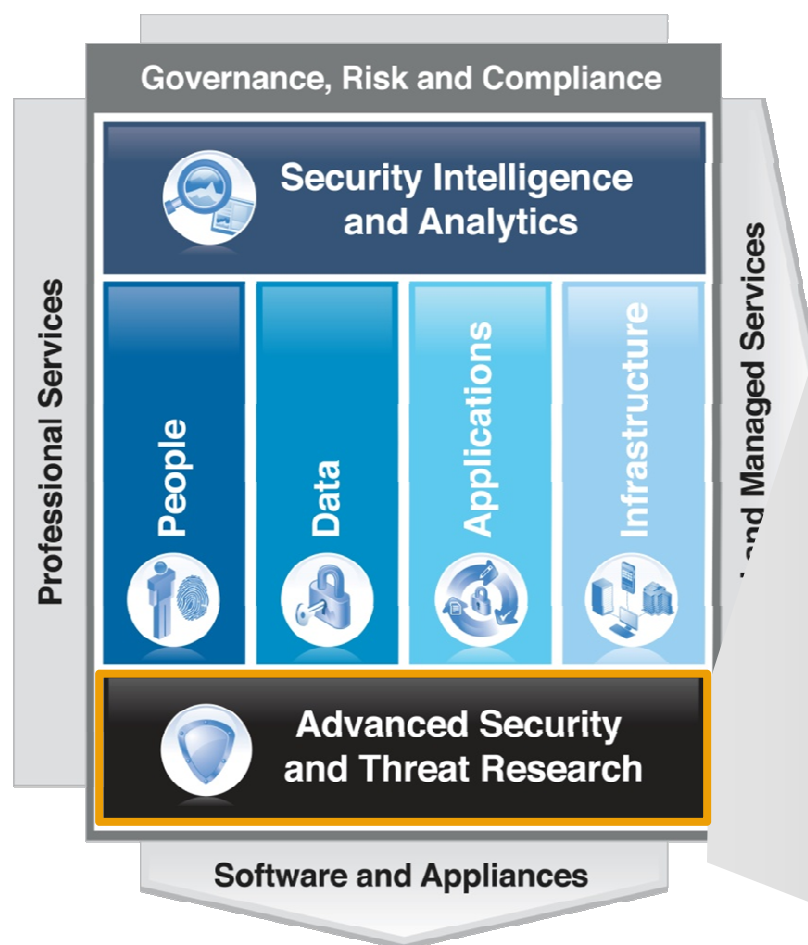
Findings from the 2012 IBM X-Force Trend and Risk Report

Leslie Horacek

X-Force Threat Response Manager



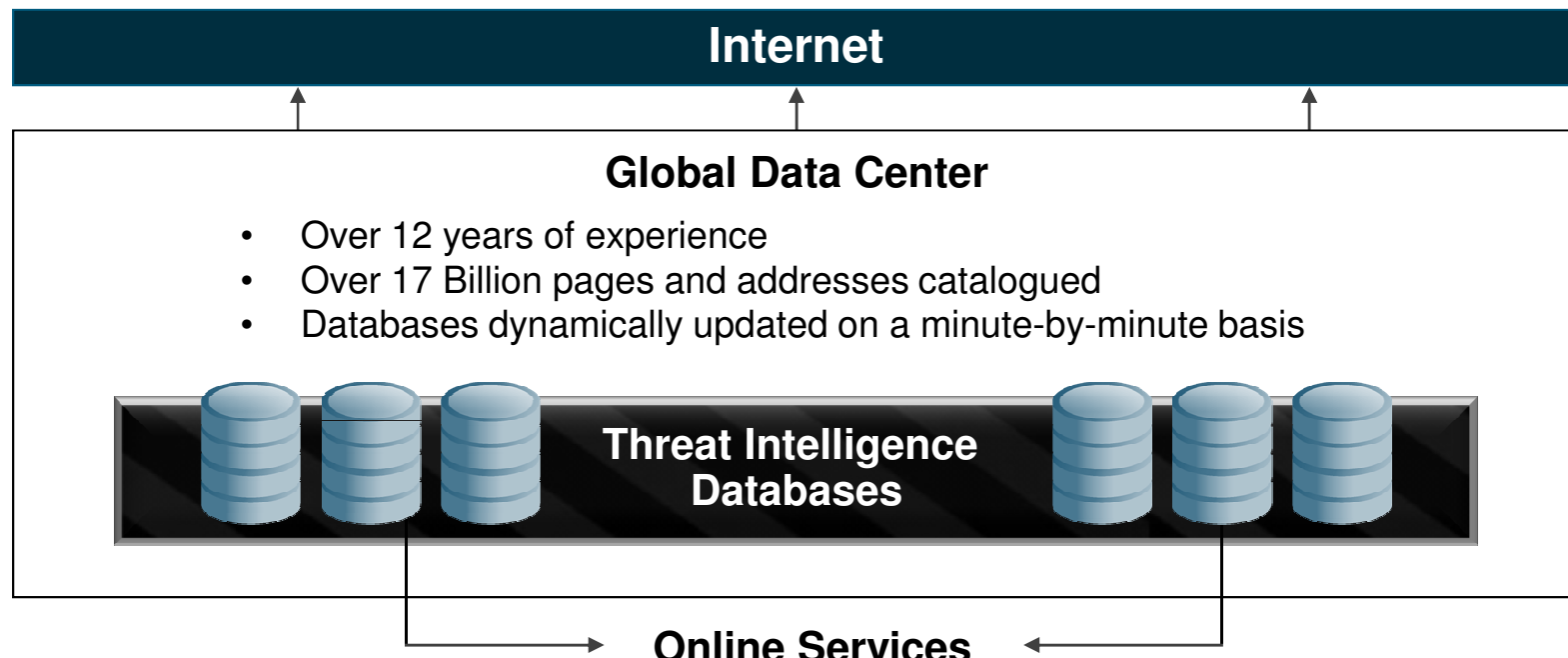
X-Force is the foundation for advanced security and threat research across the IBM Security Framework



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

Monitor - X-Force has the skills and infrastructure for collecting and analyzing changing threats



Data capture

- Crawler robots search the web in parallel
- Honeypots & darknets capture information
- Spamtraps obtain Spam IPs and samples

X-Force Threat Intelligence



Analysis

- Server clusters analyze the data acquired
- Insights for different threats are gleaned from the data and stored in an efficient manner

Monitor - Collaborative teams 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

20B analyzed
web pages & images

45M spam &
phishing attacks

73K documented
vulnerabilities

Billions of intrusion
attempts daily

Millions of unique
malware samples

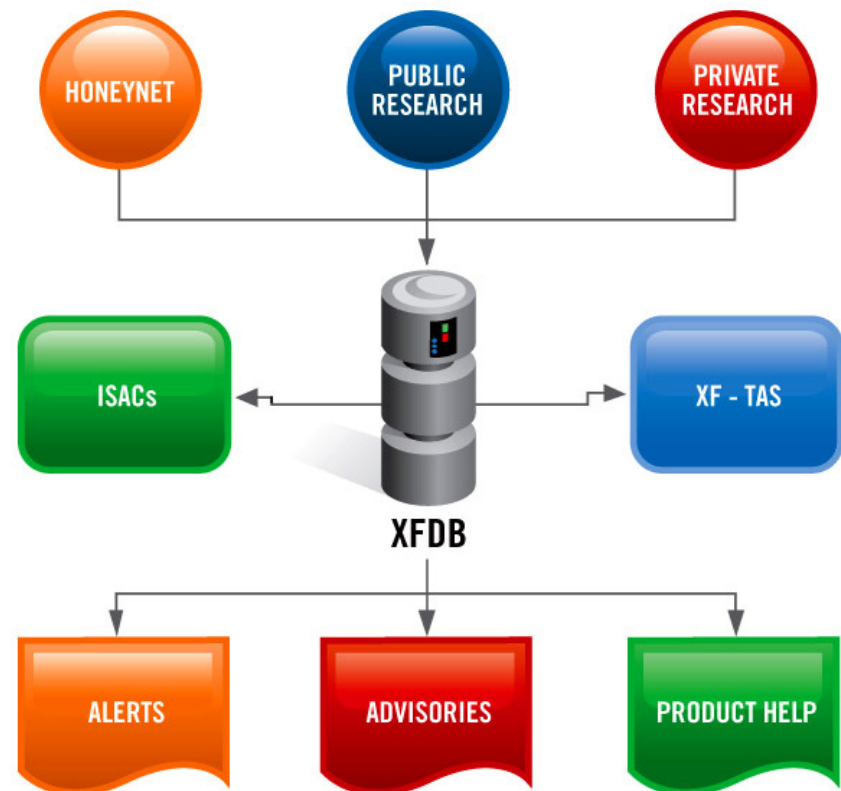
Research - Analyzing all vulnerabilities - X-Force Database (XFDB)

Most comprehensive Vulnerability Database in the world

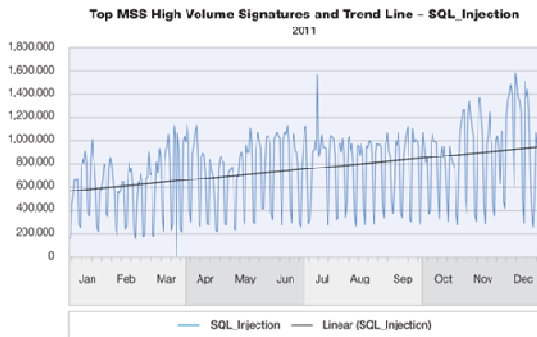
- Updated daily by a dedicated research team
- Entries date back to the 1990's
- Over 80,000 unique vulnerabilities

Research also turns into innovative product “engines”

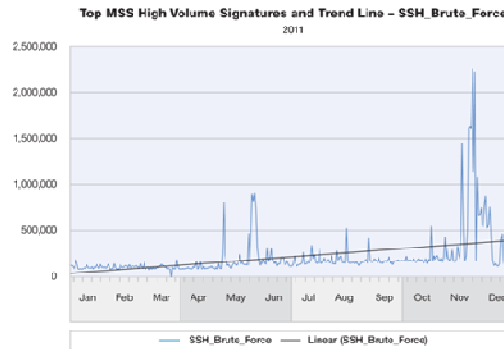
- Protocol Analysis Module
- Shellcode Heuristics
- Web Injection Logic Engine
- Java and JavaScript Heuristics



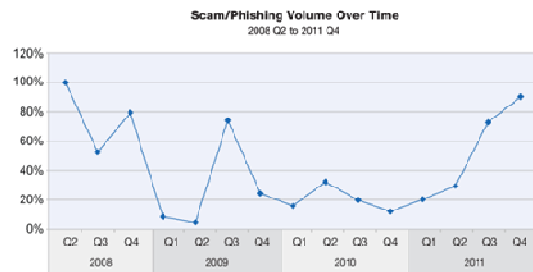
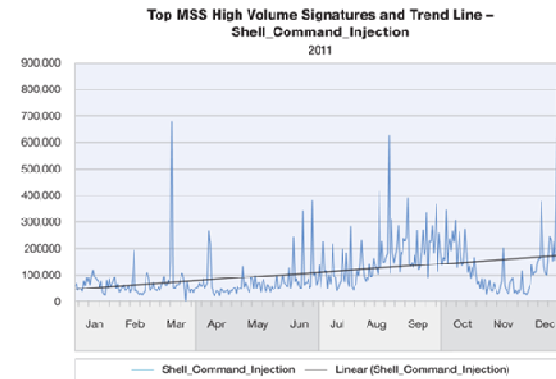
Educate - unique “optics” on the latest security and risk trends



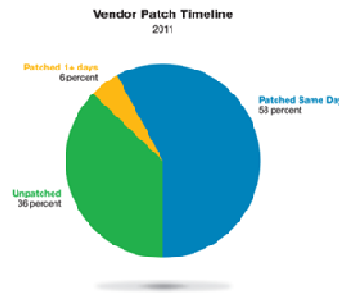
Source: IBM X-Force® Research and Development



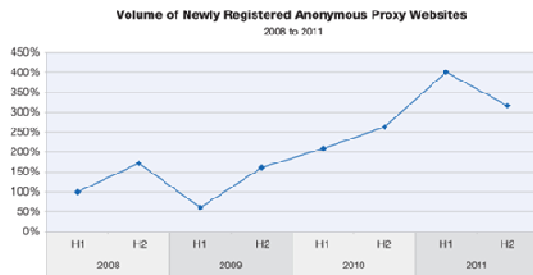
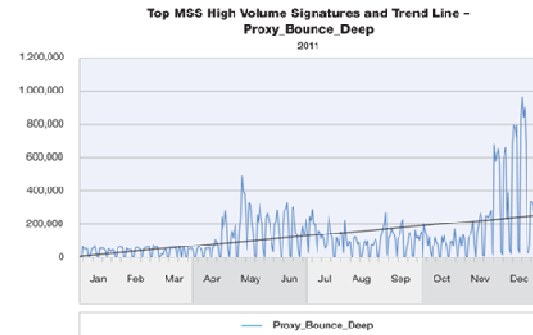
Source: IBM X-Force® Research and Development



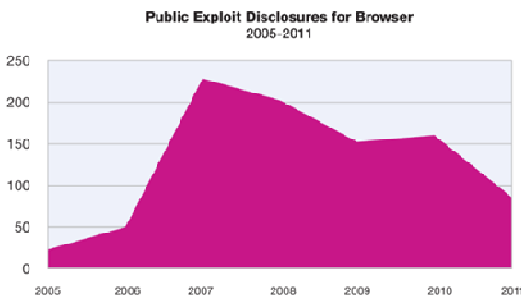
Source: IBM X-Force® Research and Development



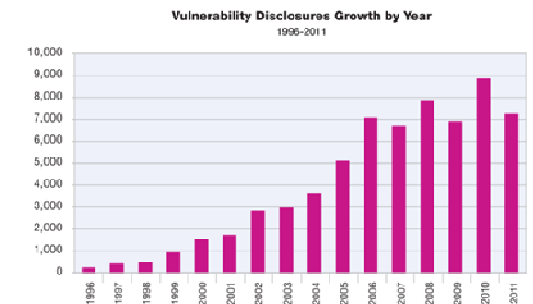
Source: IBM X-Force® Research and Development



Source: IBM X-Force® Research and Development



Source: IBM X-Force® Research and Development



Source: IBM X-Force® Research and Development

What are we seeing?

IBM X-Force® 2012 Annual Trend and Risk Report

→ Download and read about emerging security threats and trends.



**Annual Trend Report
gives an X-Force
view of the changing
threat landscape**

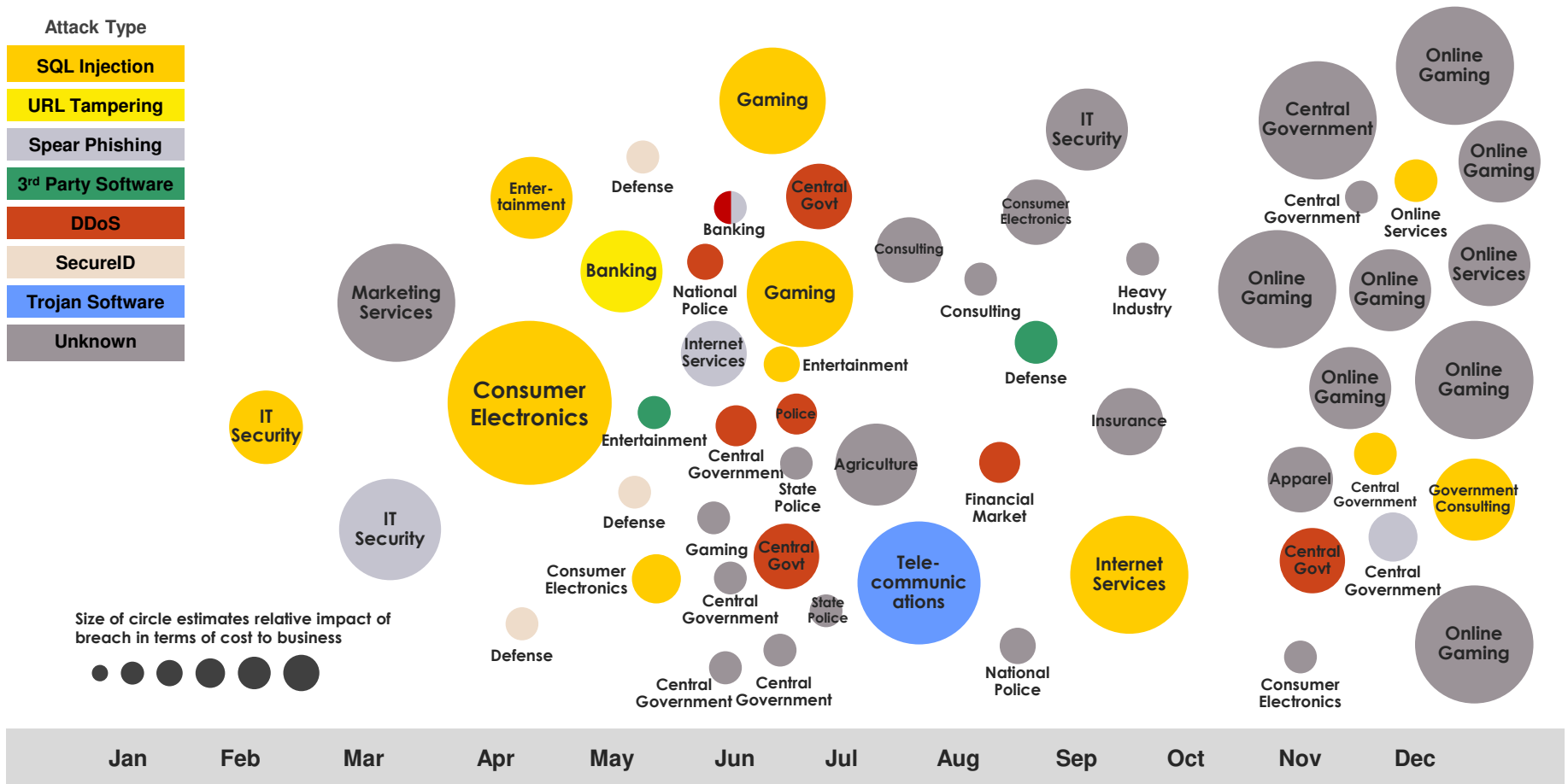
IBM X-Force 2012
Mid-year Trend and Risk Report
September 2012



IBM

2011: "The year of the targeted attack"

2011 Sampling of Security Incidents by Attack Type, Time and Impact

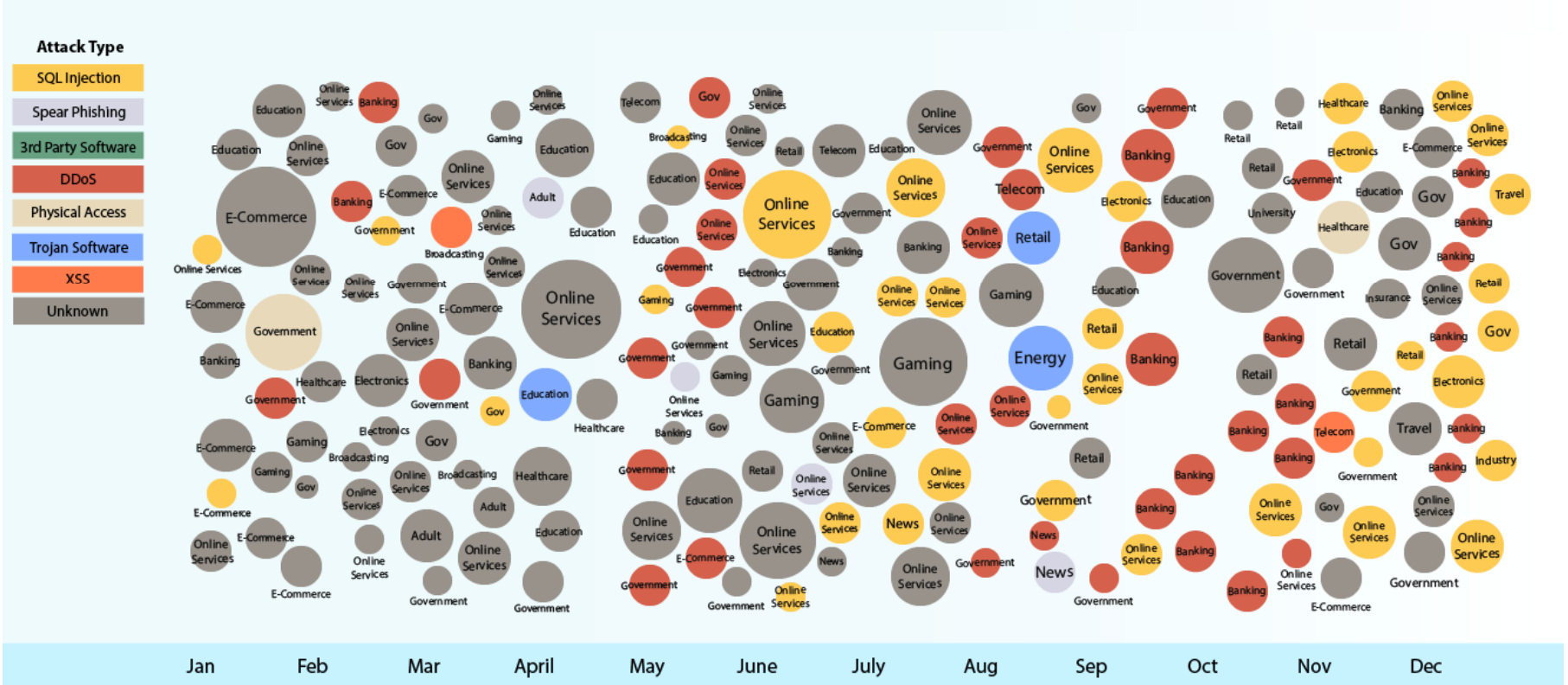


Source: IBM X-Force® Research 2011 Trend and Risk Report

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

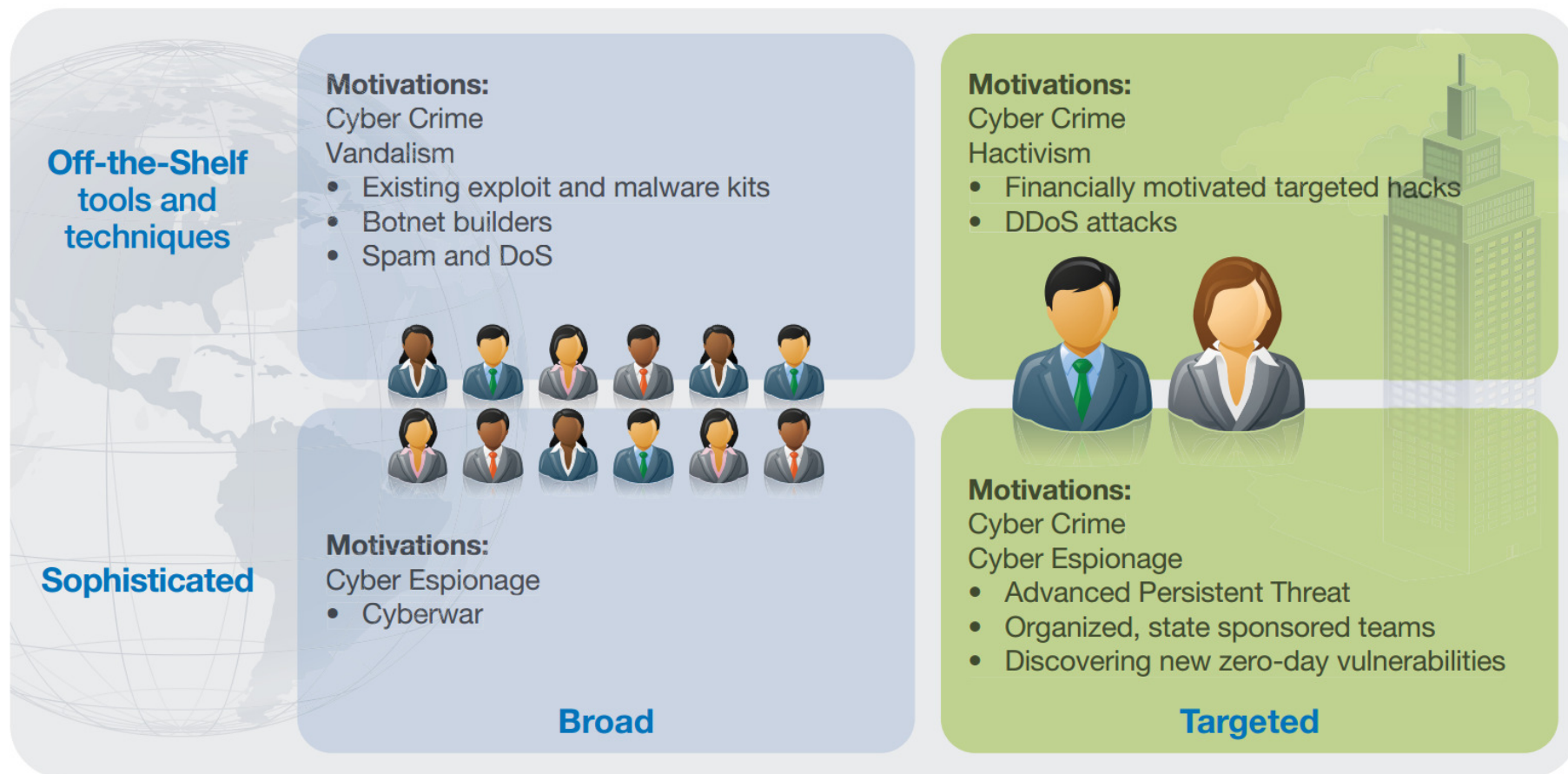


Size of circle estimates relative impact of incident in terms of cost to business



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

Attacker types and motivations have not changed

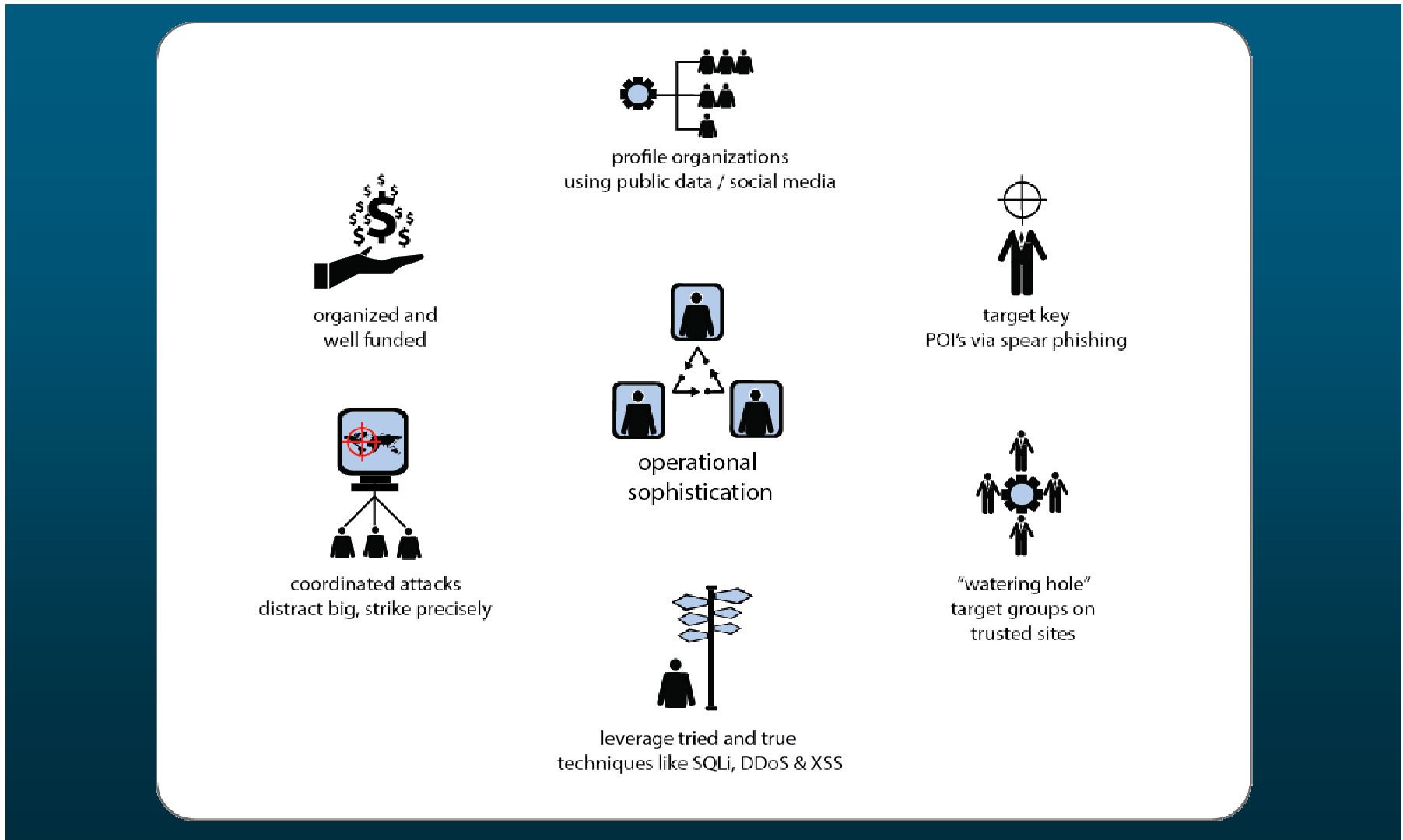


Majority of the security incidents disclosed in 2012 were carried out by attackers going after a broad target base while using off-the-shelf tools and techniques (top left)

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...

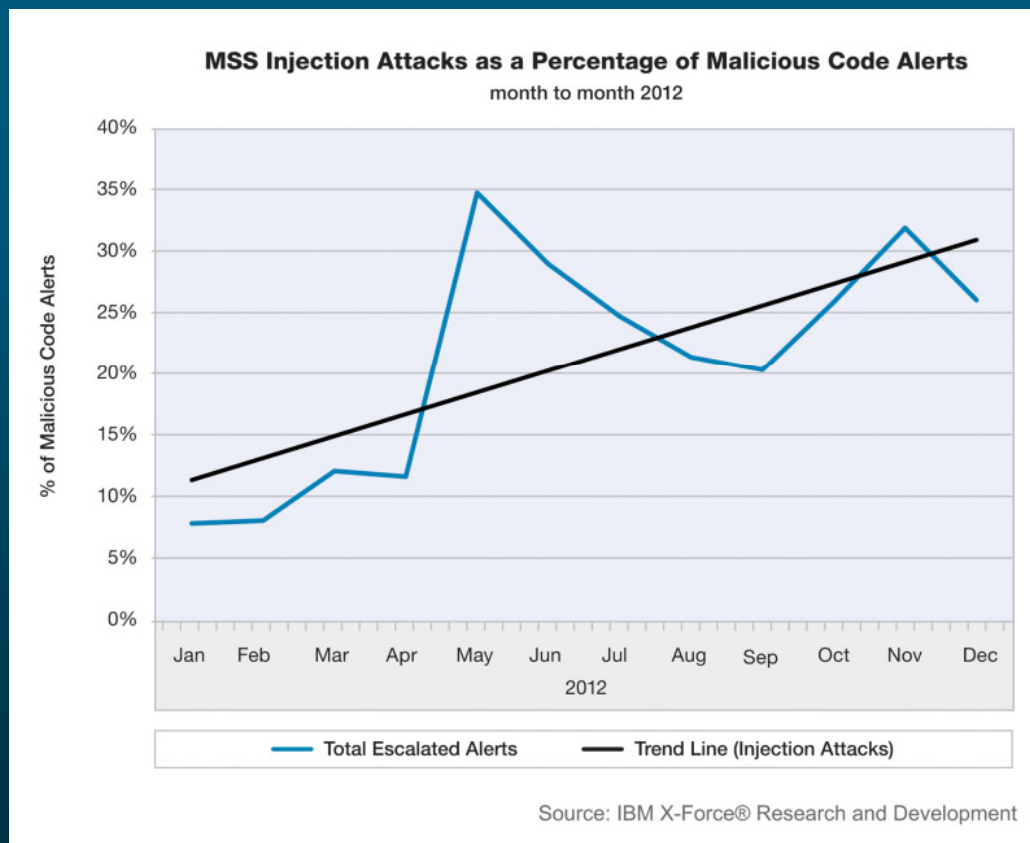
Operational sophistication, not always technology sophistication



Tried and true techniques - SQL and Command Injection attacks

Dramatic and sustained rise in SQL injection-based traffic

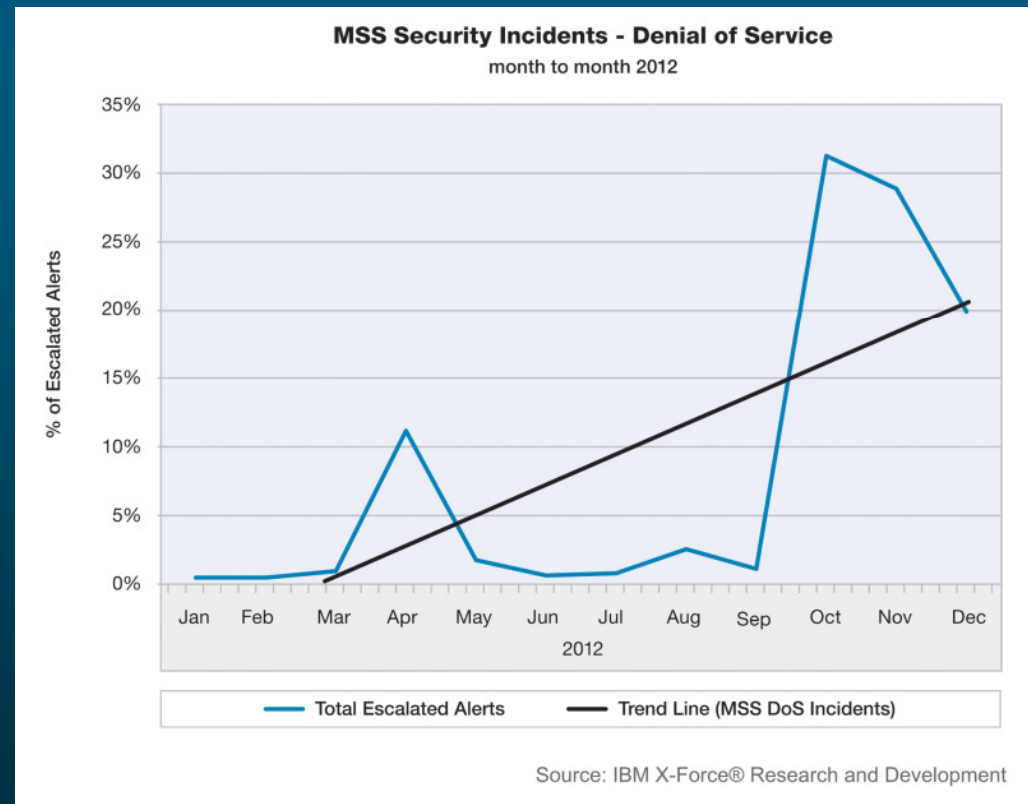
Alerts came from all industry sectors, with a bias toward banking and finance targets



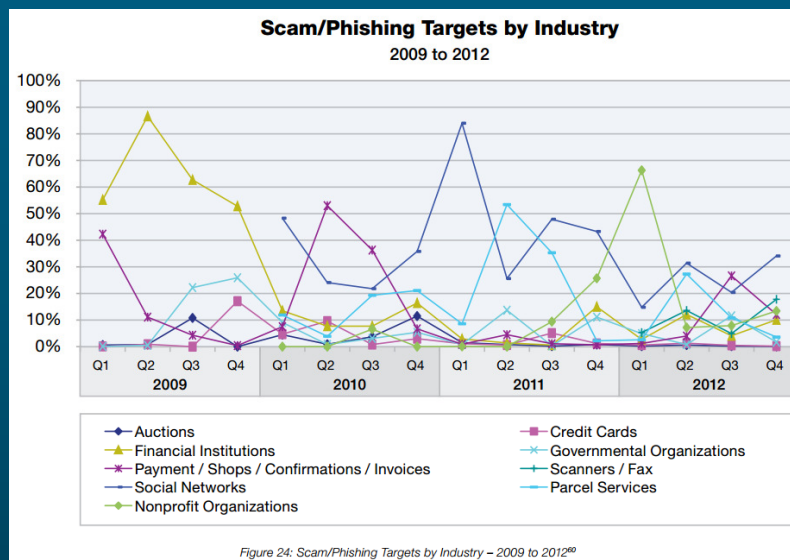
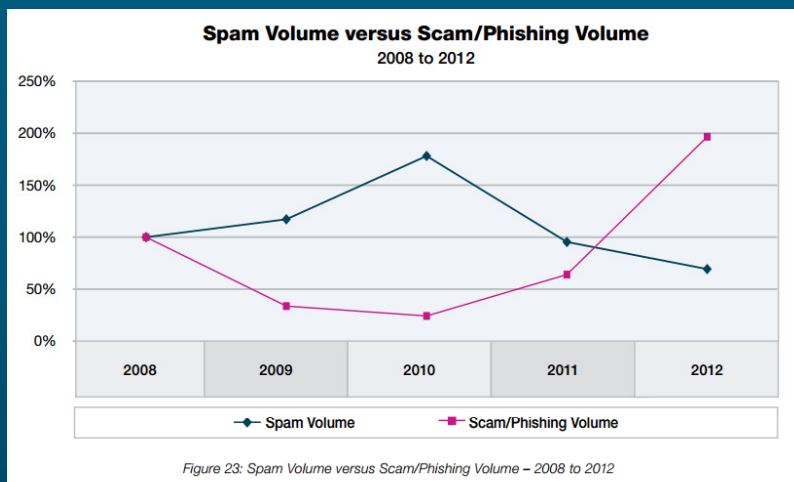
Tried and true techniques - Distributed Denial of Service (DDoS)

High profile DDoS attacks marked by a **significant increase in traffic volume**

Implementation of botnets on **compromised web servers** in high bandwidth data centers



Tried and true techniques - Spear-phishing against social networks



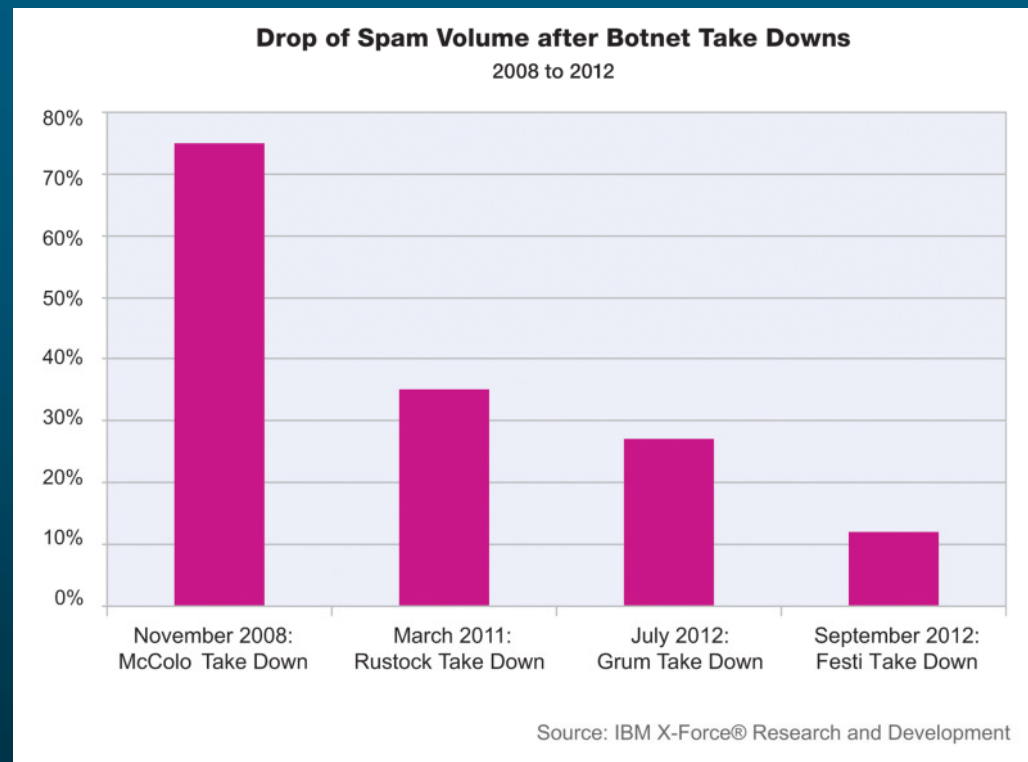
Overall spam volume continues to decline, but **spam containing malicious attachments is on the rise**

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



XSOX – Botnet Anonymizer

XSOX - New Anonymizing Technology - Mozilla Firefox

File Edit View History Bookmarks Tools Help

https://xsox.name/

XSOX™ SMART SECURITY LEADER
NEW ANONYMIZING TECHNOLOGY

Вход для клиентов:

Обновление клиента: XSOX-Client last version: 7.97b
 Работает проплата WebMoney и рег-коды
 Введено сжатие трафика. http стал быстрее!
 Пополнение ботов, удаление медленных, обновление гео-базы
 Новый сервер 1Gbit, защита от syn,udp flood, 100% UpTime

Логин: Пароль: **Вход**

Главная • Документация • Скринь • Download • Регистрация • Ссылки • Контакты

Предлагаем Вам новую разработку в области безопасности и анонимности, которую так долго ждали!
 Проект под названием XSOX позволит Вам легко менять на лету конечные точки выхода в интернет: IP адреса.
Теперь возможен выход с IP без внешних портов!

С XSOX Вы забудете обычные соксы как страшный сон!

Основные преимущества:

- Так легко ещё не было: одно нажатие кнопки - и у Вас новый выбранный Вами IP
- Двойное шифрование трафика с использованием алгоритмов, не поддающихся крипто-анализу
- Все только действительно живые, онлайн-боты, никаких дохлых проксей
- Уход бота в офлайн не вызывает потерю сессии, можно просто выбрать другого и продолжить работу
- Безопасность не имеющая аналогов, клиенты и боты неотличимы на сервере и находятся в одной сети
- Высокая скорость работы! Отсутствие "лишнего" коннекта в сравнении с обычными соксами
- Использование ботов без внешних IP, за NATами, из домашних и корп. сетей - идеально для анонимности
- Тестирование на крупнейших блек-листах SBL и XBL
- Сжатие трафика! http,smtp,pop3,ftp стали быстрее а трафик меньше
- Фильтр по стране, городу, штату, аптайму, IP, домену, примечанию
- Создание правил привязки, исключений и закреплений приложений за ботами, странами и т.д.

[XSOX] Client v7.95 Lite

Account: tst group: admin time left: 19:59:25 +358d

sox on port: 9099 **US 68.251.34.7** Chicago IL ID: 229

30 Kb 15 Kb **SOCKSIFY**

Select Test HTTP Speed SBL Test

Main Rules Sniffer Connections Tools Settings Total: 1060

Country	City	State	ver	IP / DNS	upTime	ID	Note
US	Manlius	NY	71	24.59.196.45	1 days	L 203	
AR	Buenos aires		75	200.125.100.166	60	L 204	
AT			75	88.116.116.74	345	L 205	
US	Washington	DC	71	141.156.90.156	425	L 206	
US	New hyde park	NY	71	63.138.53.115	4 days	L 207	
US			71	71.248.69.12	4 days	L 208	
US	Indianapolis	IN	71	68.249.100.91	760	L 209	
US	Mt. laurel	NJ	71	69.255.149.220	2 days	L 210	Firefox only
US	Chesapeake	VA	71	70.161.241.169	1 days	L 211	
US	Los angeles	CA	71	71.102.34.240	425	L 212	
US	Indianapolis	IN	71	68.249.100.91	760	L 213	
ES			75	83.58.171			
AE	Dubai		71	217.165.1			
US	Plano	TX	71	24.1.63			
AT			75	85.124.1			
US	Georgetown	TX	75	70.179.11			
US	Miami	FL	71	65.2.214			
KR			75	203.255.2			
US	Boston	MA	75	141.154.1			
US	Lawrence	MA	71	24.147.5			
PL	Gdansk		75	213.25.3			
US	Boston	MA	71	141.154.1			
TR			75	88.226.11			
DE	Munich		75	217.233.1			
US	Spokane	WA	71	67.185.1			
US	Chicago	IL	71	68.251.			
JP	Okinawa		71	210.79.18			
US		CT	71	68.118.195.63	690	L 232	

Use selected Note Test HTTP Speed Get geo from ip2location Set Time&Zone by bot (GMT-05:00) Copy IP/DNS to clipboard Test selected Bot for Black lists Filter: This Country only Filter: This State Only Filter: UpTime minimum

Use Filter Cntry State IP/DNS upT note Clr Connections Local: 7

Module	Bot IP	ID	RemoteAddr	Port	Snd / Rcv
iexplore.exe	68.251.34.7	229	80.67.86.15	443	3271 / 63955
OPERA.EXE	24.27.42.220	229			
iexplore.exe	68.251.34.7	229			
iexplore.exe	68.251.34.7	229			
OPERA.EXE	68.251.34.7	229			
iexplore.exe	68.251.34.7	229			
OPERA.EXE	68.251.34.7	229			

Break this connection Break all connections Break all connections for this module Exclude this module (need module restart) Add Rule: Use module only with this Bot ID Add Rule: Use module only with this Country Copy targetAddr IP to clipboard

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



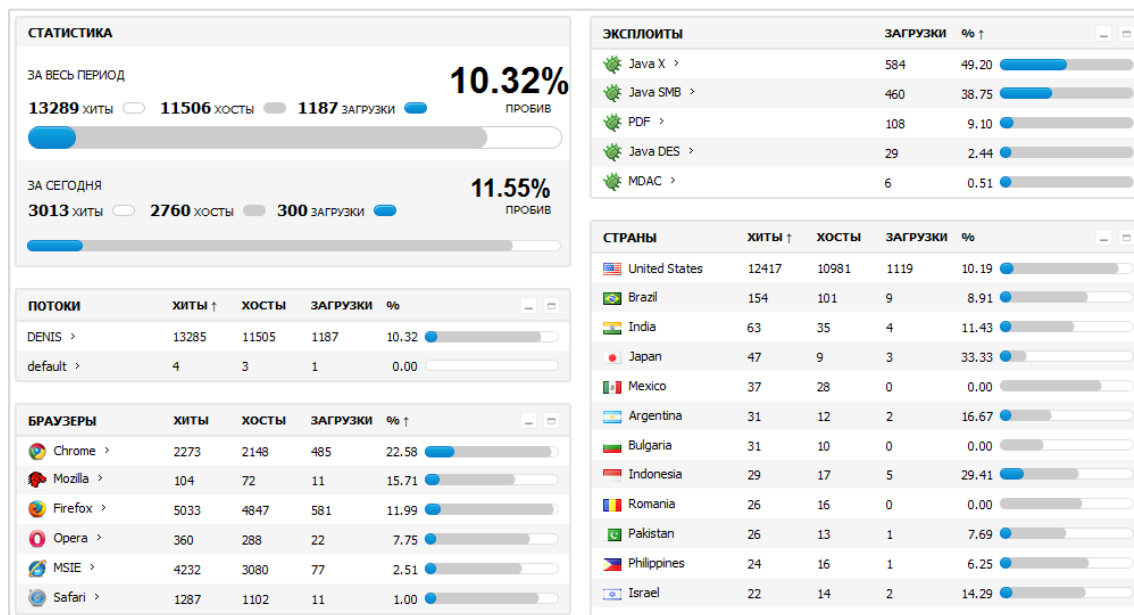
Days since last known Java 0-day exploit

Previous high score: 3

General info	Latest 0-day(s) info
Java-related CVEs: web.nvd.nist.gov	Is it still a threat? istherejava0day.com a.k.a. "is the latest patch useless yet?"
No glove, no love: How to be safe?	2013-03-07: pwn2own contest. #1 (CVE-2013-0401)
<pre>navigator.javaEnabled() == true</pre>	2013-03-06: pwn2own contest. #1 (CVE-2013-1488) #2 (CVE-2013-1491) #3 (CVE-2013-0402)
Latest patch: CVE-2013-1493	
Achievements	
Close call: reach 1 week Not 2day: reach 2 digits Finger binary is not enough: reach 31 days Deep Thought: reach 42 days D3aL w17H 17: reach 1337 hours java.lang.ArrayIndexOutOfBoundsException: reach 3 digits Trial licence expired: reach 180 days The Reaper's Toll: reach 1 year without getting attention	

<http://java-0day.com/>

As a result, exploit authors and toolkits favor Java

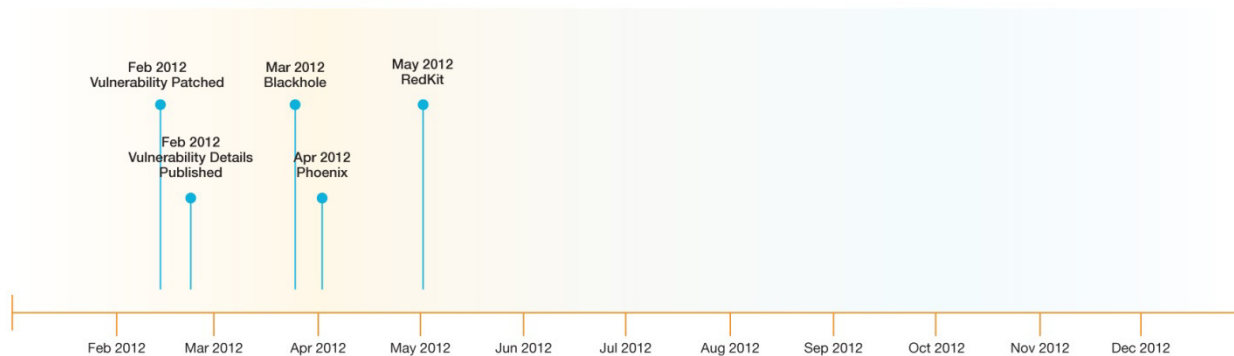


Web browser exploit kits - aka “exploit packs” - are built for one particular purpose: to install malware on end-user systems

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

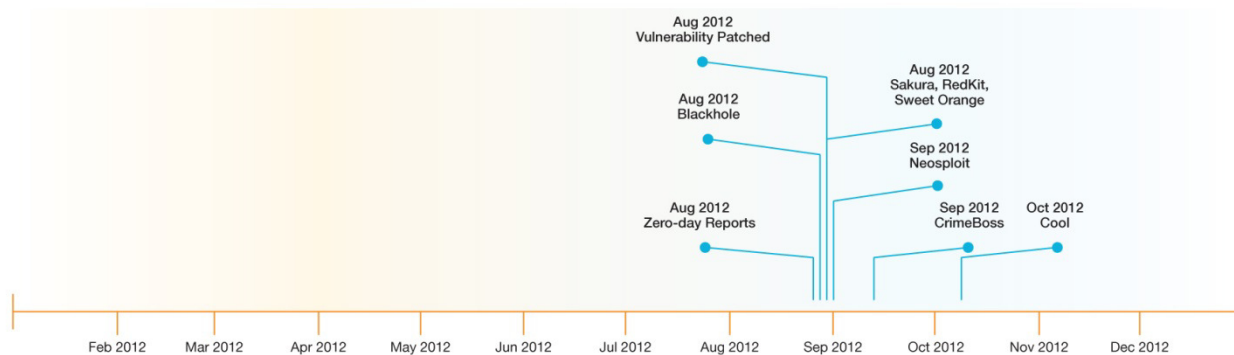
CVE-2012-0507



CVE-2012-1723



CVE-2012-4681



Spear phishing and Exploit Kit Example

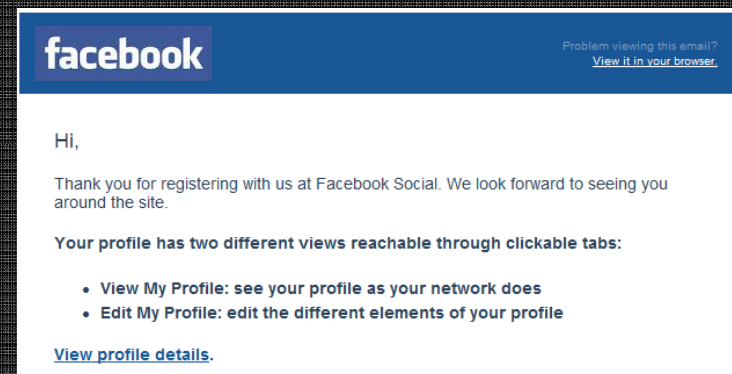


ATTACKER

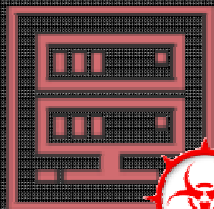
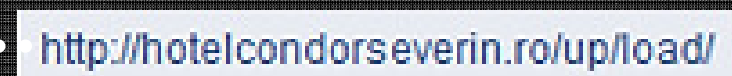


TARGET

User receives risky email from personal social network

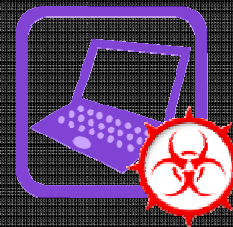


User is redirected to a malicious website



Blackhole^β

crimepack



Drive-by exploit is used to install malware on target PC

Adversaries operate business too... Exploits as a Service

The screenshot shows a dashboard titled 'ROBO ZAK' with a navigation menu on the left containing buttons for 'STATS', 'LINK TRAFF', 'SELLERS', 'FILE', 'SETTINGS', and 'CLEAR'. The main content area displays three data tables. At the bottom of the dashboard, there is a 3D rendering of a robot character.

Statistic

Statistic	Traff	Loads	Efficiency
All	57	7	12.28%

Browsers

Browser	Traff	Loads	Efficiency
Safari	20	1	5%
Chrome	9	1	11.11%
Firefox	9	2	22.22%
MSIE 6	2	1	50%
MSIE 7	3	0	0%
MSIE 8	14	2	14.29%

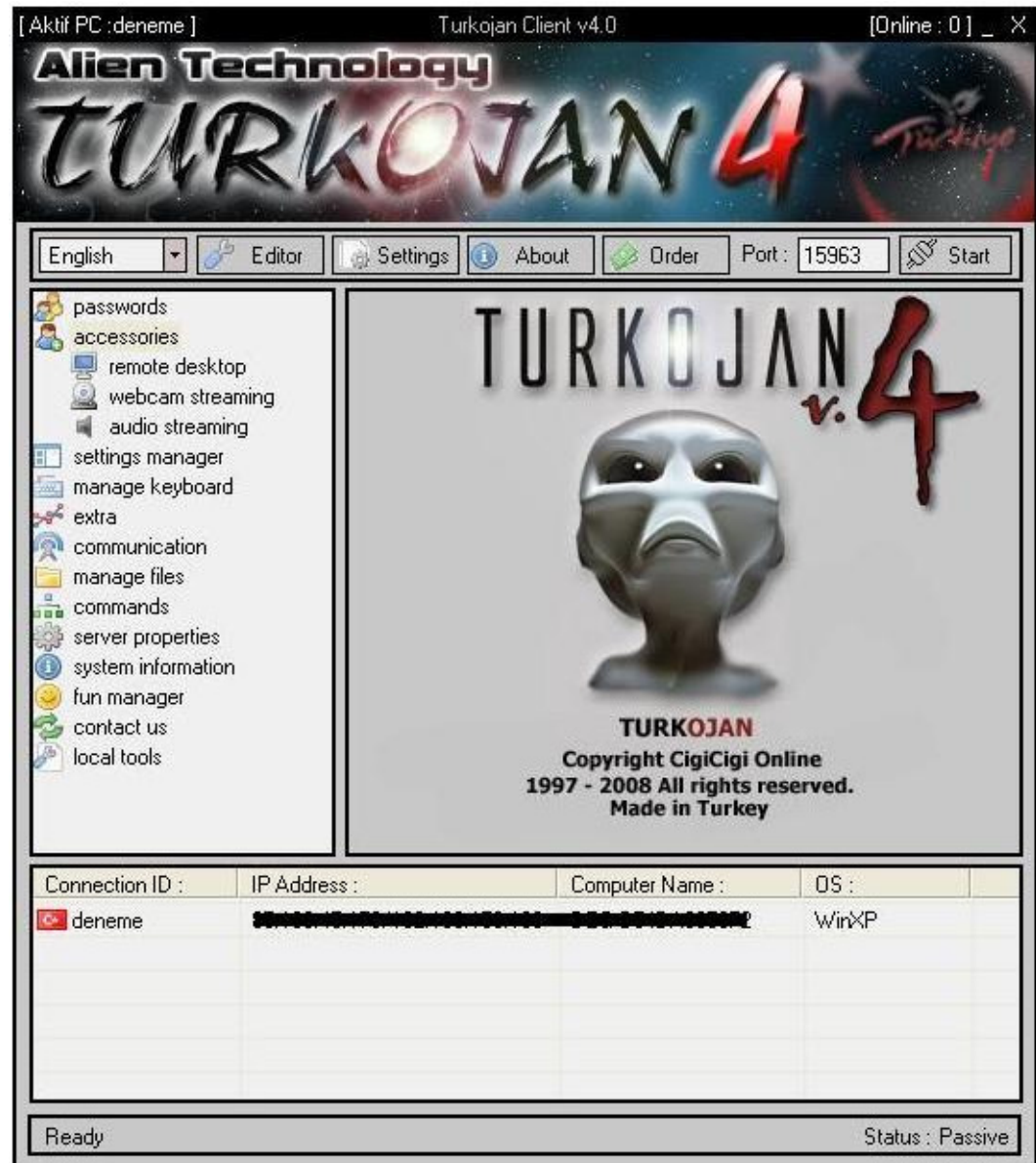
TOP3 countries

Country	Traff	Loads	Efficiency
	33	1	3.03%
	5	1	20%
	3	0	0%
	3	0	0%
	2	1	50%




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..



Features, service levels, and technical support

	<p style="text-align: center;">Bronze Edition</p> <ul style="list-style-type: none"> ■ 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) <p>Price : 99\$ (United State Dollar)</p>
	<p style="text-align: center;">Silver Edition</p> <ul style="list-style-type: none"> ■ 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 <p>Price : 179\$ (United State Dollar)</p>
	<p style="text-align: center;">Gold Edition</p> <ul style="list-style-type: none"> ■ 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) <p>Price : 249\$ (United State Dollar)</p>

2 Weeks Ago #1

BleedingLife ◦
Junior Member

Join Date: Mar 2011
Posts: 2
Reputation: 0

Bleeding Life v2: RELOADED **Exploit Pack**

INTRODUCTION:

BleedingLife Exploit Pack was looked down upon in the beginning of its start. As time went on and users began to take a chance with this pack, they've eventually understood BL is no normal pack. With less exploits and a higher rate than other packs, BL has really made a name for itself. Now, BL has turned into a series. BL v1, BL v2, BL Mini-Java, BL Java Edition, BL Adobe Edition. And... Here before us, BL v2 Reloaded. If you want a low cost, high rate and great quality pack... Purchase BleedingLife v2 Reloaded!

EXPLOITS:

- [x] CVE-2008-2992
- [x] CVE-2010-0188
- [x] CVE-2010-0842
- [x] CVE-2010-1297
- [x] CVE-2010-2884
- [x] CVE-2010-3552
- [x] JavaSignedApplet (Requires user interaction but can be disabled.)
- [x] All exploits bypass ASLR and DEP where needed.

AVERAGE RATE:

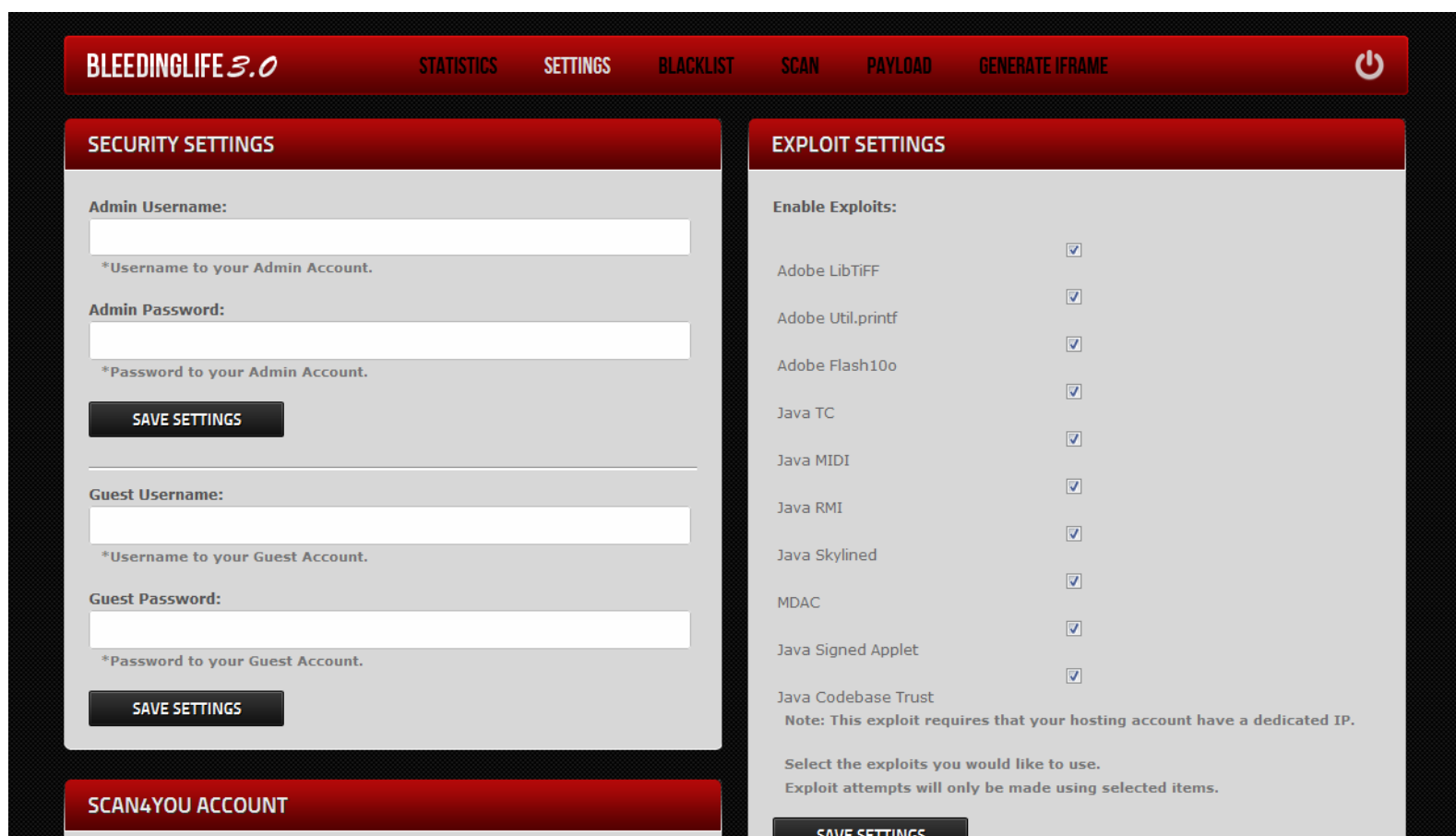
- [x] BL v2 has an average rate between 30% - 40%
- [x] SS/Proof coming soon ...

PAYMENT OPTIONS:

- [x] BleedingLife v2 Reloaded - \$400.00
- [x] FUD Update - \$50.00
- [x] Domain Change - \$50.00
- [x] Liberty Reserve & WebMoney ONLY!
- [x] Previous v2 Buyers - FREE Update!

But wait, there's more..... (Bleeding Life 3.0 now available)

- ✓ New Java and PDF exploits
- ✓ \$1000 for new customer, only \$250 for v2 customers
- ✓ Built-in scanner to scan for vulnerable IP's
- ✓ Ability to easily allow adding/removing of exploits



The screenshot displays the BleedingLife 3.0 web interface. The top navigation bar includes the product name 'BLEEDINGLIFE 3.0' and several menu items: STATISTICS, SETTINGS, BLACKLIST, SCAN, PAYLOAD, and GENERATE IFRAME. A power icon is located on the right side of the navigation bar.

The main content area is divided into two columns:

- SECURITY SETTINGS:** This section contains two sets of input fields. The first set is for 'Admin Username' and 'Admin Password', with a 'SAVE SETTINGS' button below. The second set is for 'Guest Username' and 'Guest Password', also with a 'SAVE SETTINGS' button below. Each input field has a small asterisk and a note indicating it's for the respective account.
- EXPLOIT SETTINGS:** This section is titled 'Enable Exploits:' and lists various exploit types, each with a checked checkbox. The list includes: Adobe LibTIFF, Adobe Util.printf, Adobe Flash10o, Java TC, Java MIDI, Java RMI, Java Skylined, MDAC, and Java Signed Applet. Below the list, there is a note: 'Note: This exploit requires that your hosting account have a dedicated IP.' and a final 'SAVE SETTINGS' button.



Software vulnerabilities - disclosures up in 2012

8,168

publicly
disclosed
vulnerabilities

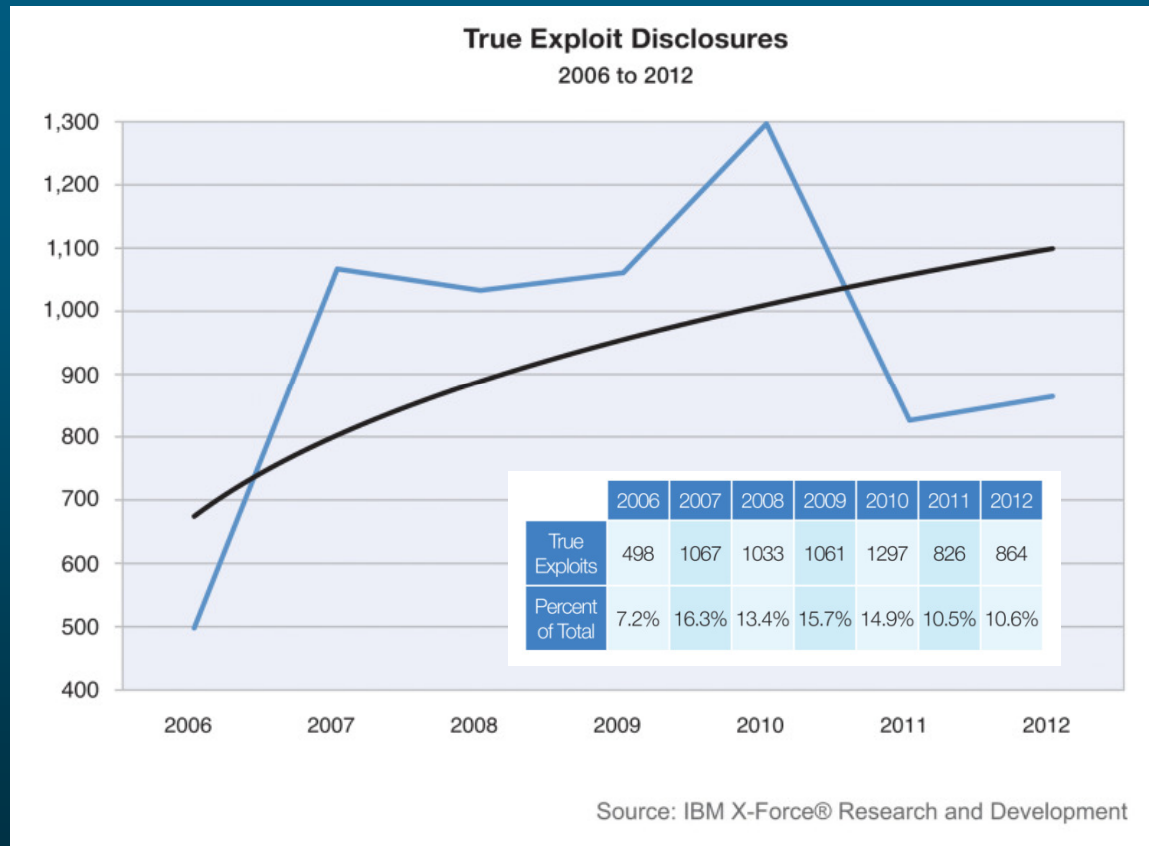
An increase of
over 14% from
2011



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



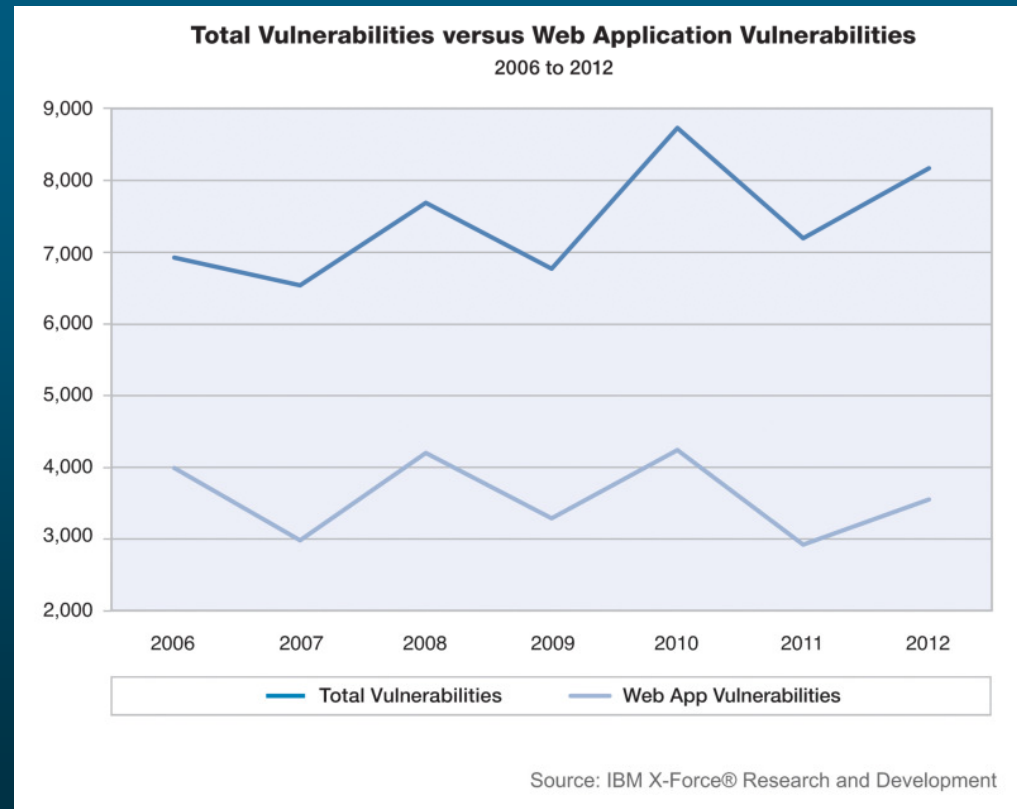
Web application vulnerabilities surge upward

14%

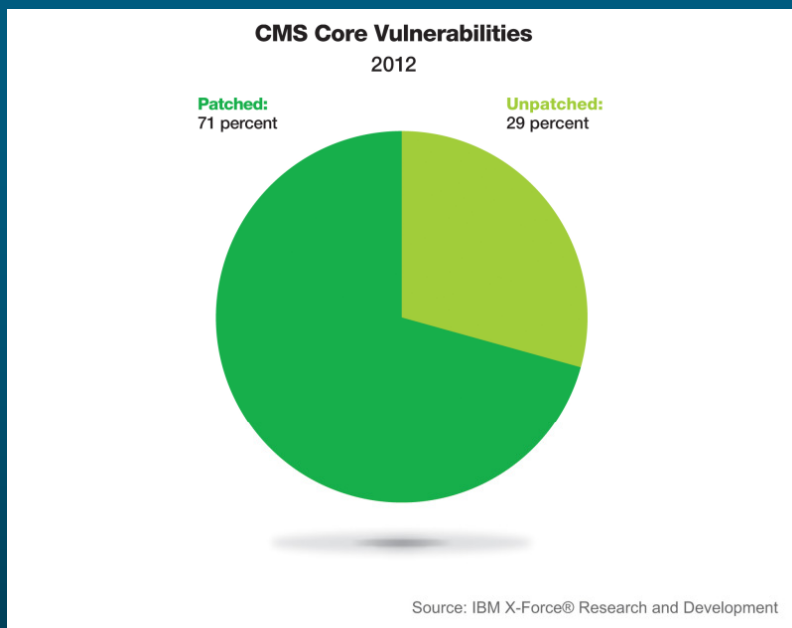
increase in
web application
vulnerabilities

Cross-site scripting
represented

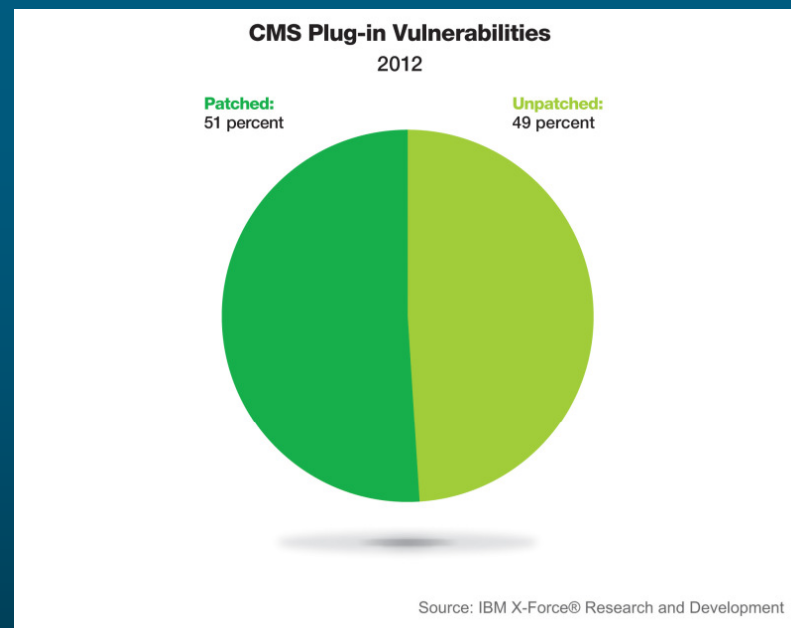
53%



Content Management Systems plug-ins provide soft target



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



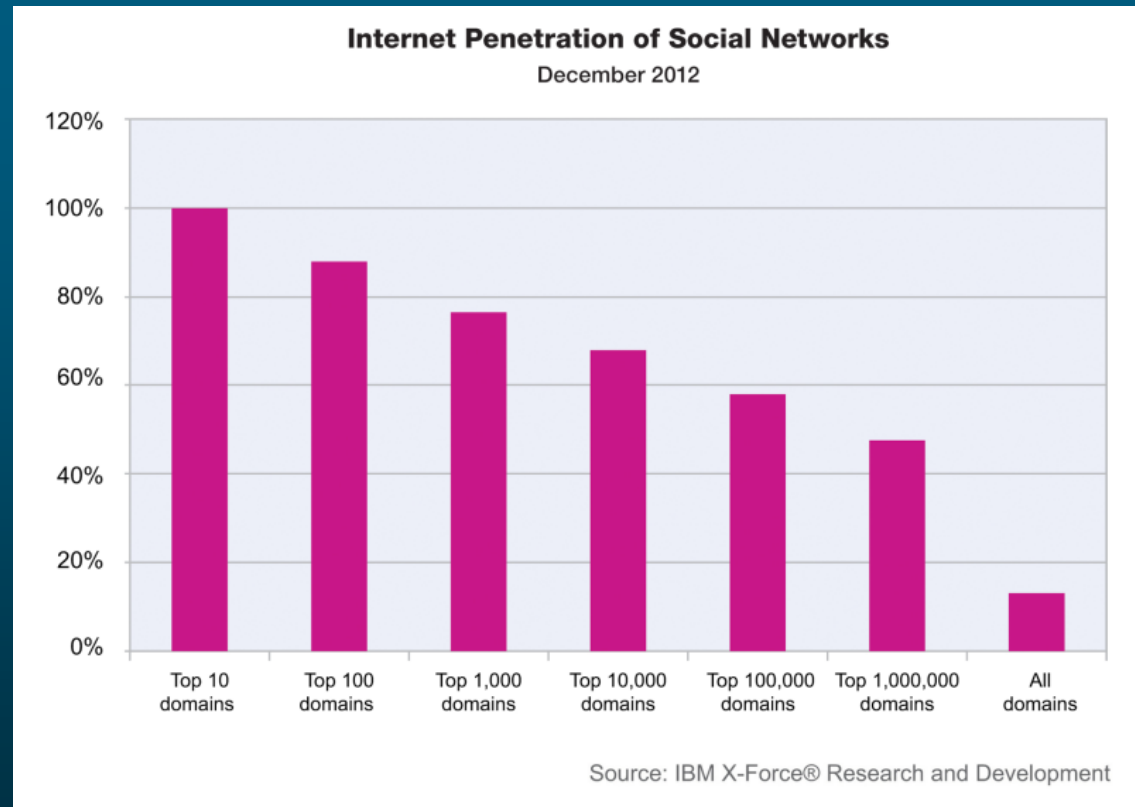
Compared to smaller organizations and individuals producing the add-ons and plug-ins

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)

Summary - 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

Get Engaged with IBM X-Force Research and Development



Follow us at @ibmsecurity
and @ibmxforce



Download X-Force
security trend & risk
reports

<http://www-935.ibm.com/services/us/iss/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>



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



ibm.com/security

© **Copyright IBM Corporation 2013. 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.

Not a technical problem, but a business challenge

- Many of the recent breaches could have been prevented
- Significant effort is required to inventory, identify, and close every vulnerability
- Financial & operational resistance is always encountered, so how much of an investment is enough?

IF IBM X-FORCE® WAS RUNNING THE IT DEPARTMENT

Many readers have asked, if IBM X-Force were running the IT department and saw what happened this year, what would you do? Well, here are ten actions beyond the basics that X-Force would do if we ran the IT department.

