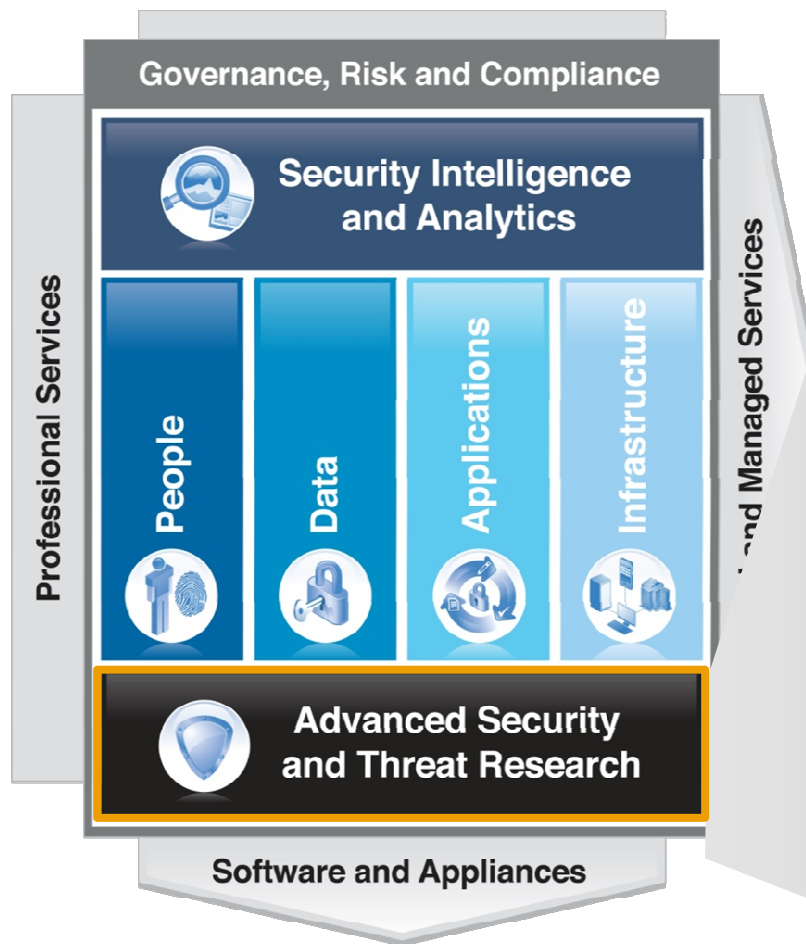# Today's Threat Landscape
Findings from the 2012 IBM X-Force Trend and Risk Report

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

Internet

Global Data Center
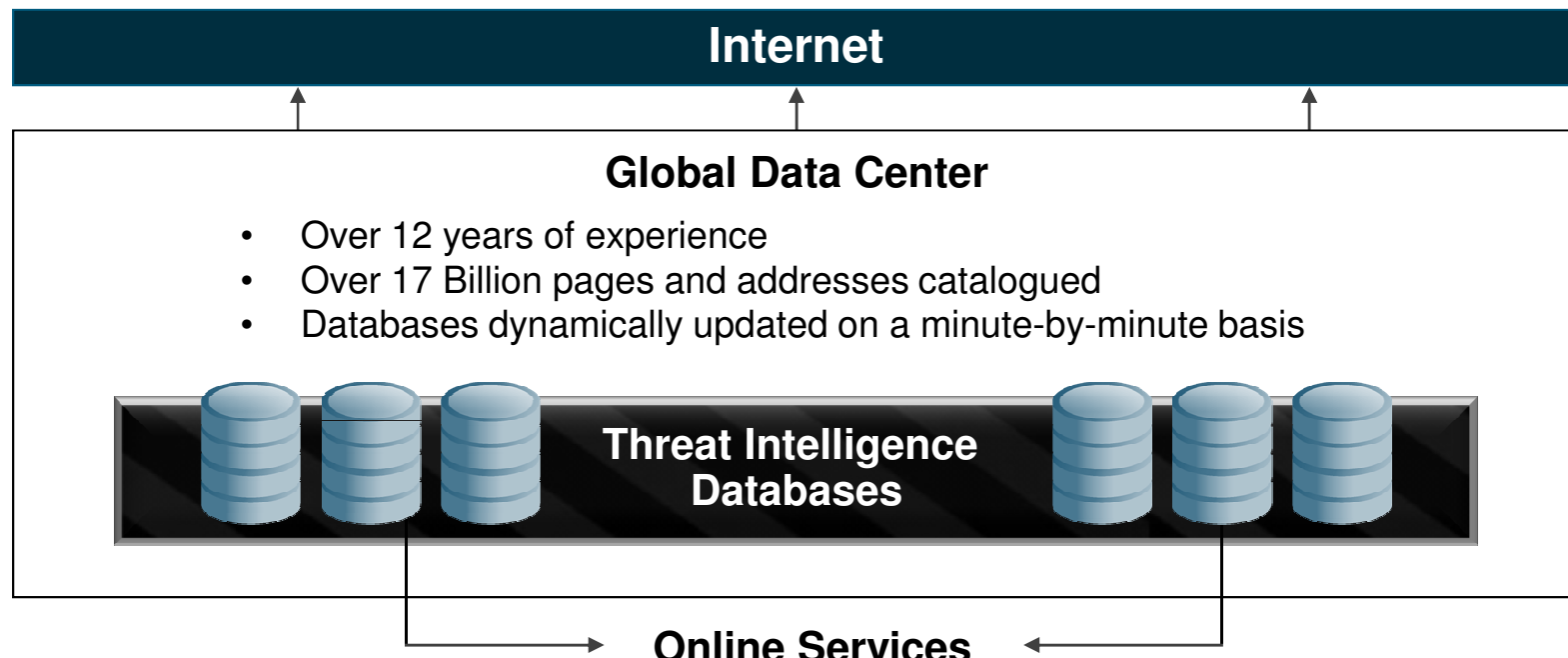
- Over 12 years of experience
- Over 17 Billion pages and addresses catalogued
- Databases dynamically updated on a minute-by-minute basis

Threat Intelligence Databases

Online Services
X-Force Threat Intelligence

Data capture

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

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

X FORCE

IBM Research

Depth

20B analyzed web pages & images

45M spam & phishing attacks

73K documented vulnerabilities

Billions of intrusion attempts daily

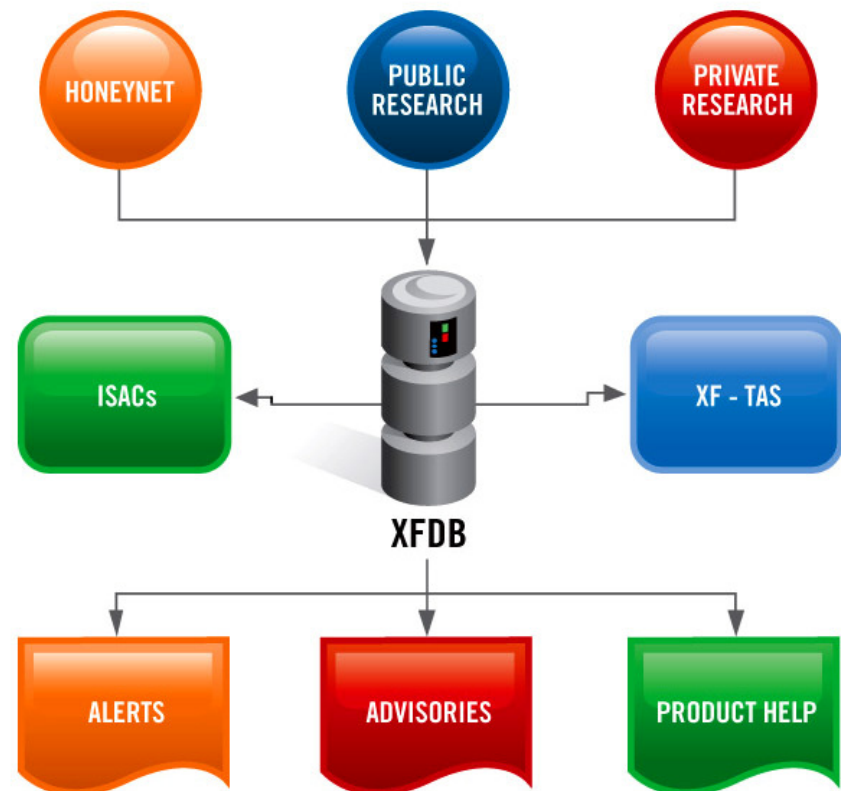**Millions** of unique malware samples

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

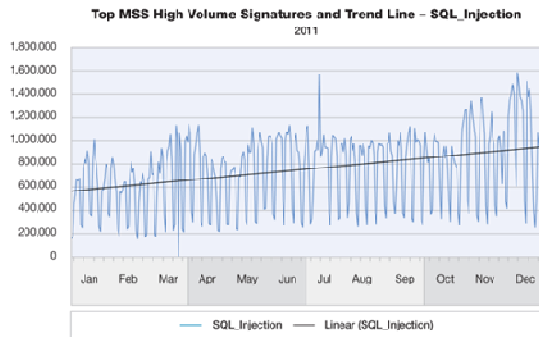## Most comprehensive Vulnerability Database in the world

– Updated daily by a dedicated research team

– Entries date back to the 1990's

– Over 80,000 unique vulnerabilities

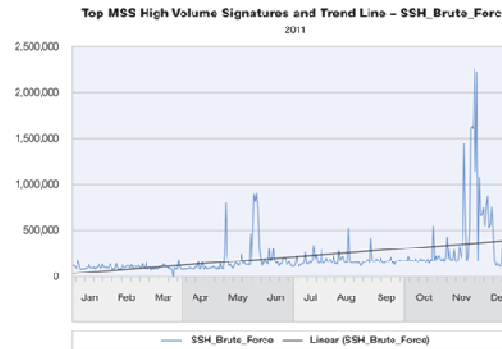## Research also turns into innovative product "engines"

– Protocol Analysis Module

– Shellcode Heuristics

– Web Injection Logic Engine
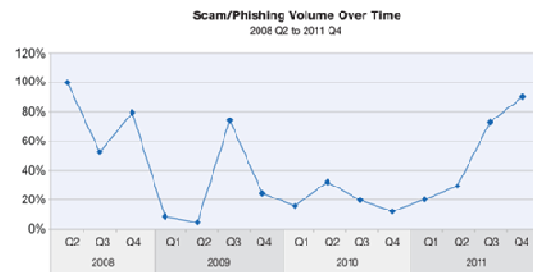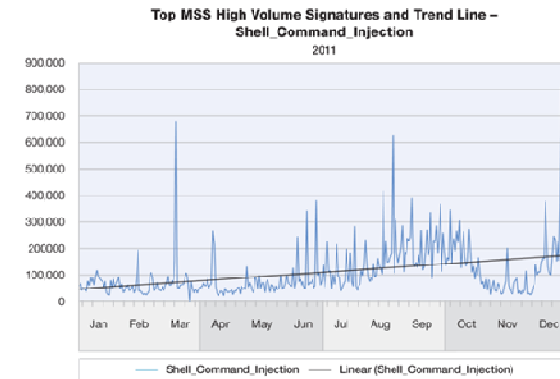
– Java and JavaScript Heuristics

HONEYNET

PUBLIC RESEARCH

PRIVATE RESEARCH

ISACs

XF - TAS

XFDB

ALERTS

ADVISORIES

PRODUCT HELP

Educate - unique "optics" on the latest security and risk trends
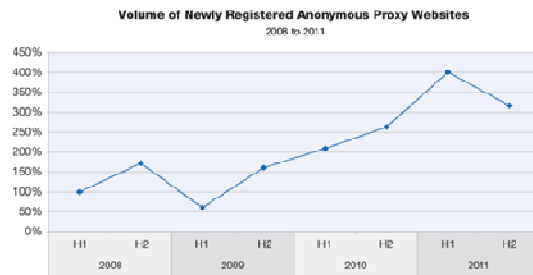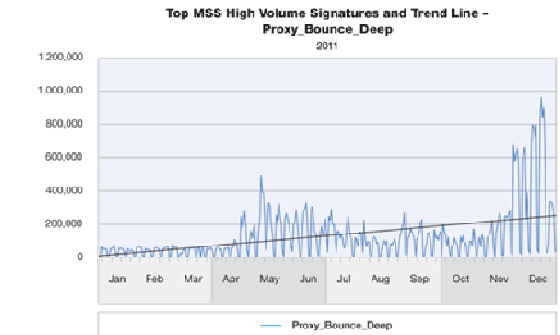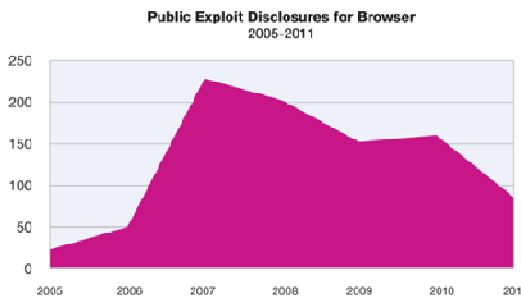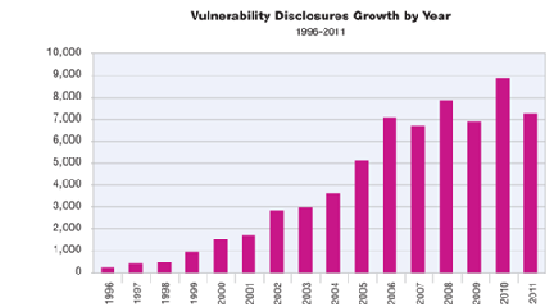
What are we seeing?

IBM X-Force® 2012 Annual Trend and Risk Report

→ Download and read about emerging security threats and trends.

X-FORCE

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!

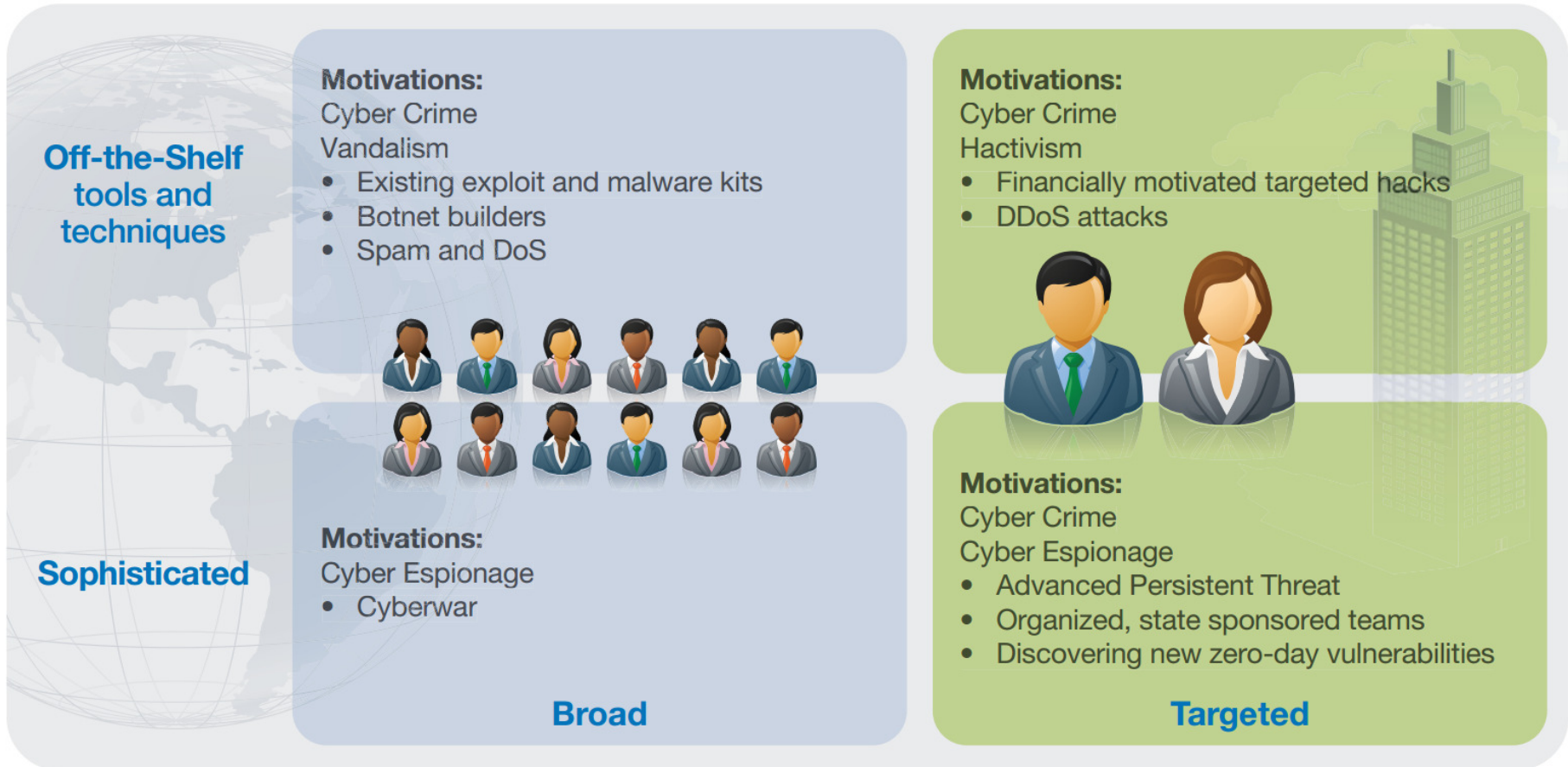## 2012 Sampling of Security Incidents by Attack Type, Time and Impact
Conjecture of relative breach impact is based on publicly disclosed information regarding leaked records and financial losses

Attack Type
- SQL Injection
- Spear Phishing
- 3rd Party Software
- DDoS
- Physical Access
- Trojan Software
- XSS
- Unknown

Jan | Feb | Mar | April | May | June | July | Aug | Sep | Oct | Nov | Dec

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

Off-the-Shelf tools and techniques

Motivations:
Cyber Crime
Vandalism
- Existing exploit and malware kits
- Botnet builders
- Spam and DoS

Motivations:
Cyber Crime
Hactivism
- Financially motivated targeted hacks
- DDoS attacks

Motivations:
Cyber Espionage
- Cyberwar

Motivations:
Cyber Crime
Cyber Espionage
- Advanced Persistent Threat
- Organized, state sponsored teams
- Discovering new zero-day vulnerabilities

Sophisticated
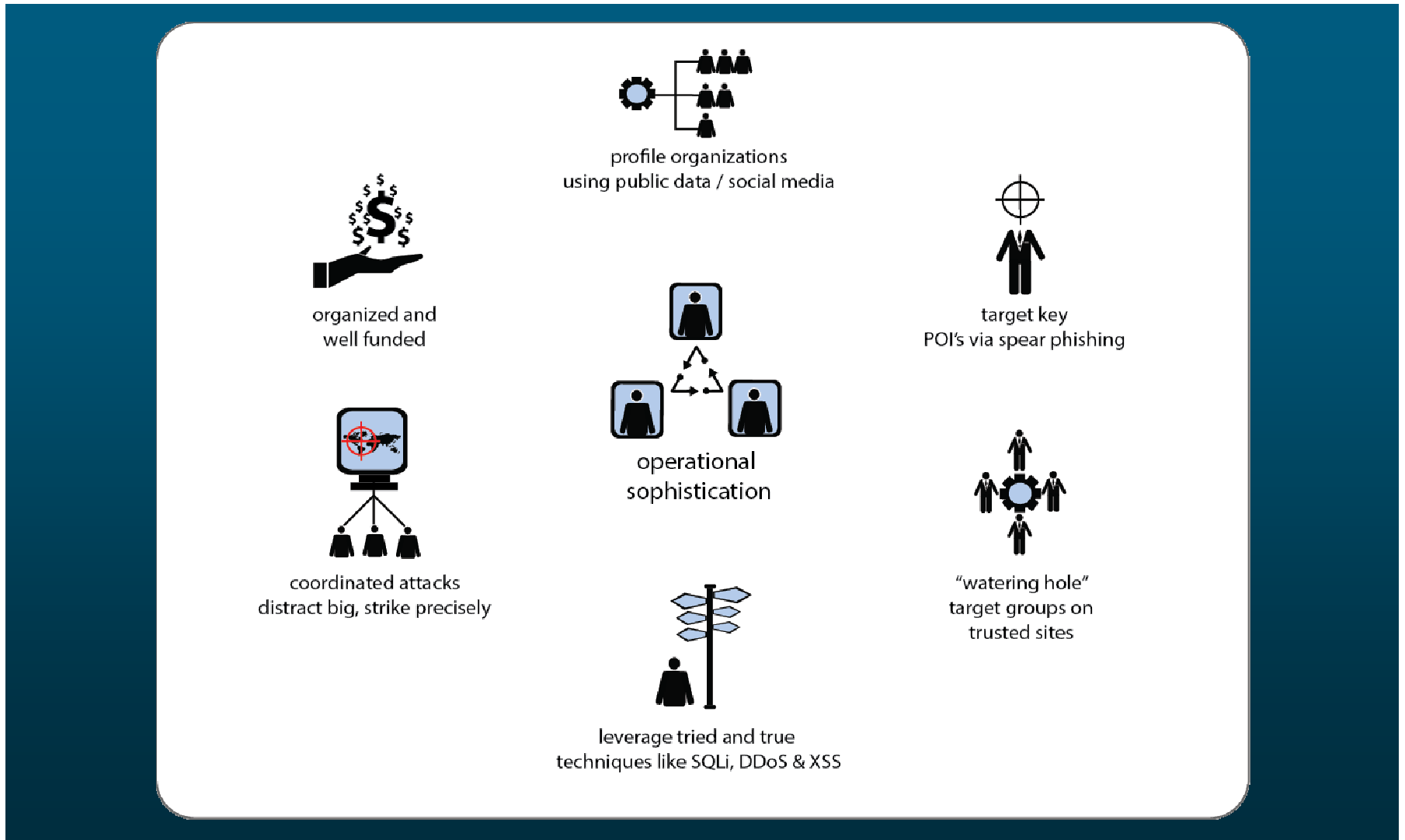
Broad

Targeted

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

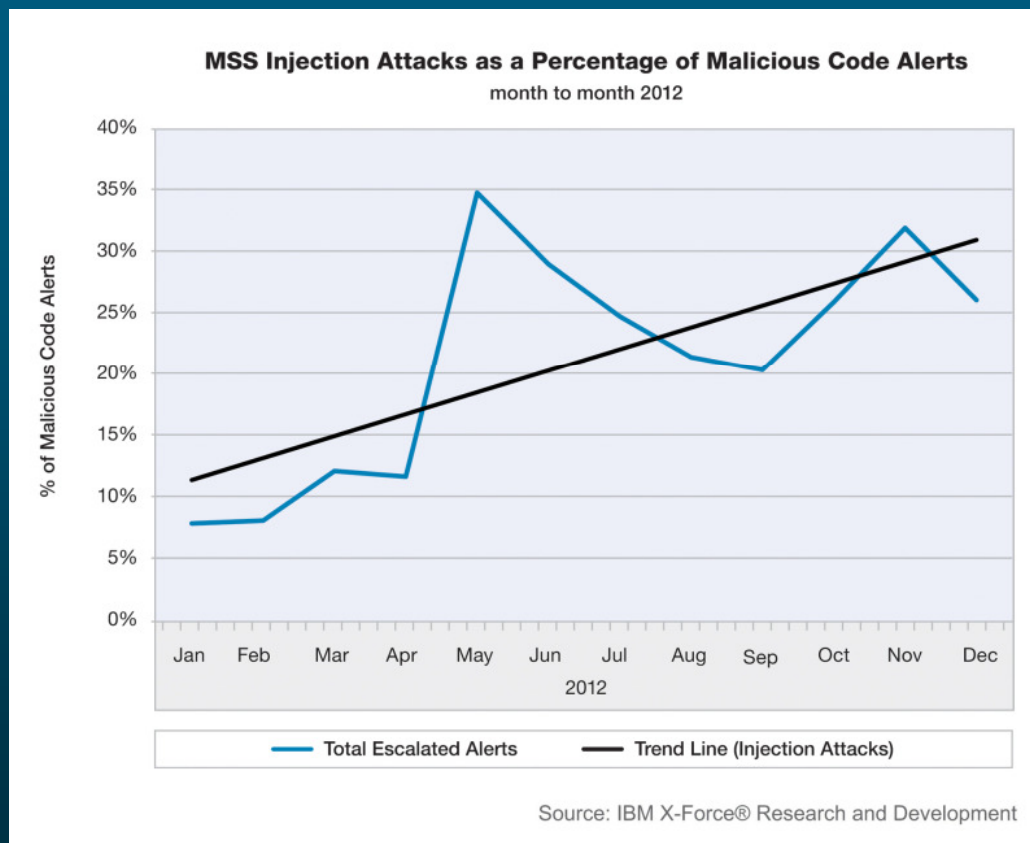Attackers are opportunistic, not all APTs and state-sponsored use exotic malware and zero-day vulnerabilities…

Operational sophistication, not always technology sophistication

profile organizations
using public data / social media

organized and
well funded

target key
POI's via spear phishing

operational
sophistication

coordinated attacks
distract big, strike precisely

"watering hole"
target groups on
trusted sites

leverage tried and true
techniques like SQLi, DDoS & XSS

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

MSS Injection Attacks as a Percentage of Malicious Code Alerts
month to month 2012

% of Malicious Code Alerts

40%
35%
30%
25%
20%
15%
10%
5%
0%

Jan Feb Mar Apr May Jun Jul Aug Sep Oct Nov Dec
2012

— Total Escalated Alerts   — Trend Line (Injection Attacks)

Source: IBM X-Force® Research and Development

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

MSS Security Incidents - Denial of Service
month to month 2012

Total Escalated Alerts — Trend Line (MSS DoS Incidents)

Source: IBM X-Force® Research and Development
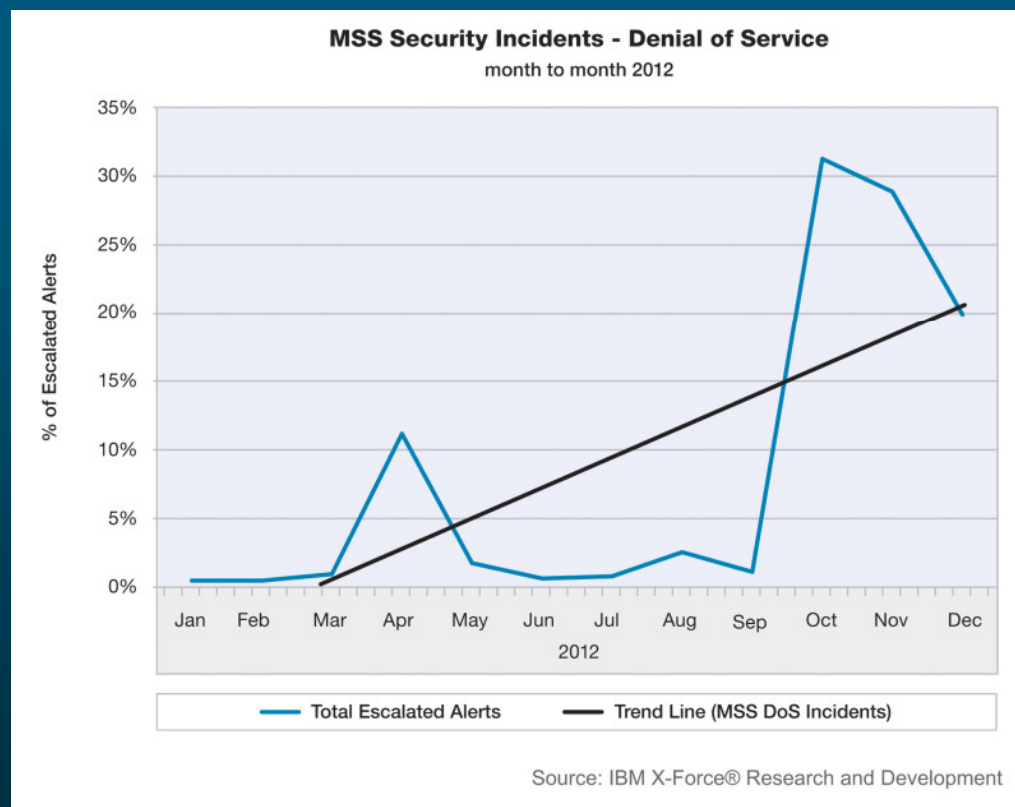
Tried and true techniques - Spear-phishing against social networks
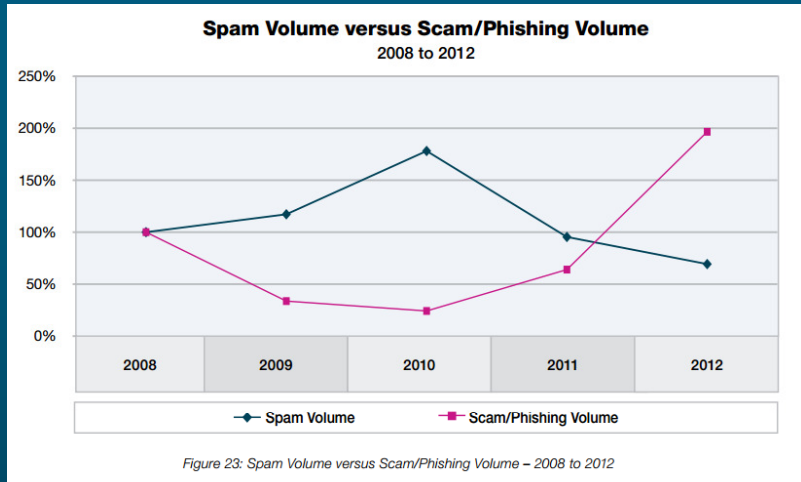
Figure 23: Spam Volume versus Scam/Phishing Volume – 2008 to 2012
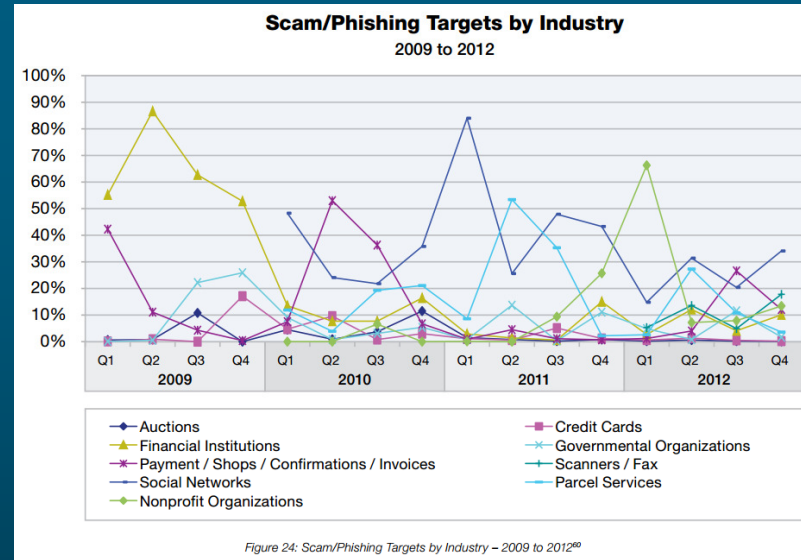
Figure 24: Scam/Phishing Targets by Industry – 2009 to 2012[60]

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

Drop of Spam Volume after Botnet Take Downs
2008 to 2012

Source: IBM X-Force® Research and Development

XSOX – Botnet Anonymizer

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

26

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)
navigator.javaEnabled() == true	2013-03-06: pwn2own contest. #1 (CVE-2013-1488)
Latest patch: CVE-2013-1493	#2 (CVE-2013-1491) #3 (CVE-2013-0402)

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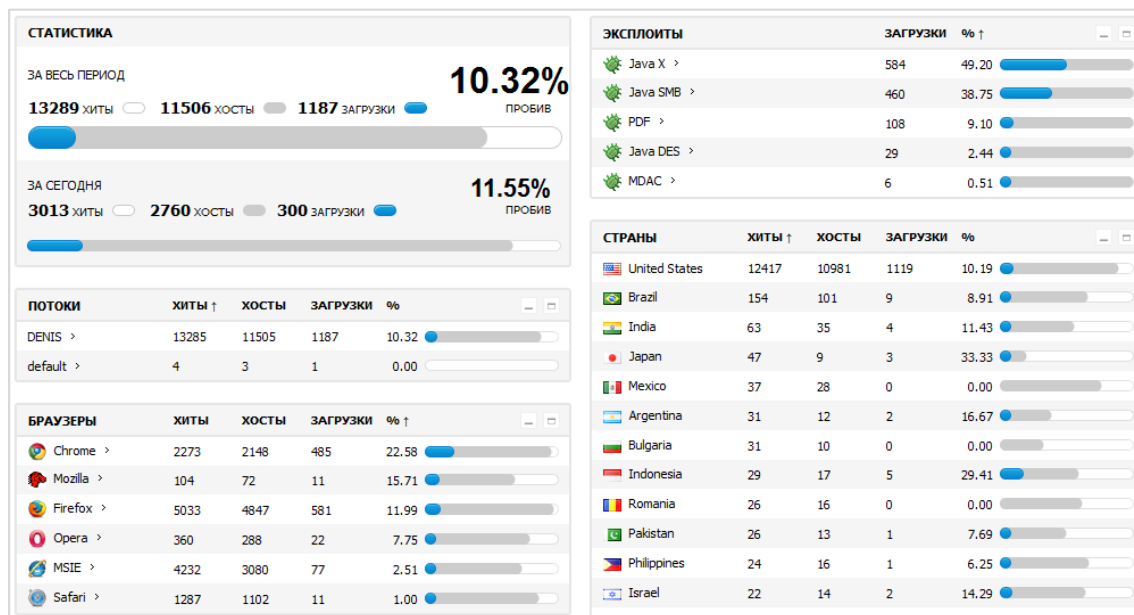
Web browser exploit kits - aka "exploit packs" - are built for one particular purpose: to install malware on end-user systems

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

Feb 2012
Vulnerability Patched

Feb 2012
Vulnerability Details
Published

Mar 2012
Blackhole

Apr 2012
Phoenix

May 2012
RedKit

Feb 2012   Mar 2012   Apr 2012   May 2012   Jun 2012   Jul 2012   Aug 2012   Sep 2012   Oct 2012   Nov 2012   Dec 2012

CVE-2012 -1723

Jun 2012
Vulnerability Patched

Jun 2012
Vulnerability Details
Published

Jul 2012
Blackhole

Aug 2012
Kein

Sep 2012
Neosploit,
Nuclear

Oct 2012
Cool

Feb 2012   Mar 2012   Apr 2012   May 2012   Jun 2012   Jul 2012   Aug 2012   Sep 2012   Oct 2012   Nov 2012   Dec 2012

CVE-2012 -4681

Aug 2012
Vulnerability Patched

Aug 2012
Blackhole

Aug 2012
Zero-day Reports

Aug 2012
Sakura, RedKit,
Sweet Orange

Sep 2012
Neosploit

Sep 2012
CrimeBoss

Oct 2012
Cool

Feb 2012   Mar 2012   Apr 2012   May 2012   Jun 2012   Jul 2012   Aug 2012   Sep 2012   Oct 2012   Nov 2012   Dec 2012

Spear phishing and Exploit Kit Example

ATTACKER

TARGET

User receives risky email from personal social network

facebook — Problem viewing this email? View it in your browser.

Hi,

Thank you for registering with us at Facebook Social. We look forward to seeing you around the site.

Your profile has two different views reachable through clickable tabs:

- View My Profile: see your profile as your network does
- Edit My Profile: edit the different elements of your profile

View profile details.

User is redirected to a malicious website

http://hotelcondorseverin.ro/up/load/
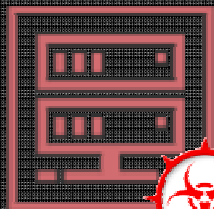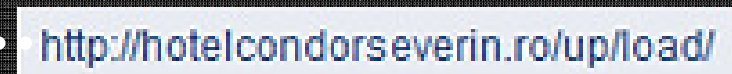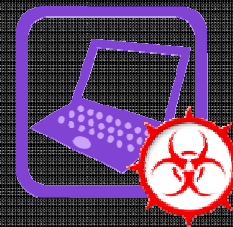
Drive-by exploit is used to install malware on target PC

Blackhole β

crimepack

Adversaries operate business too… Exploits as a Service

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

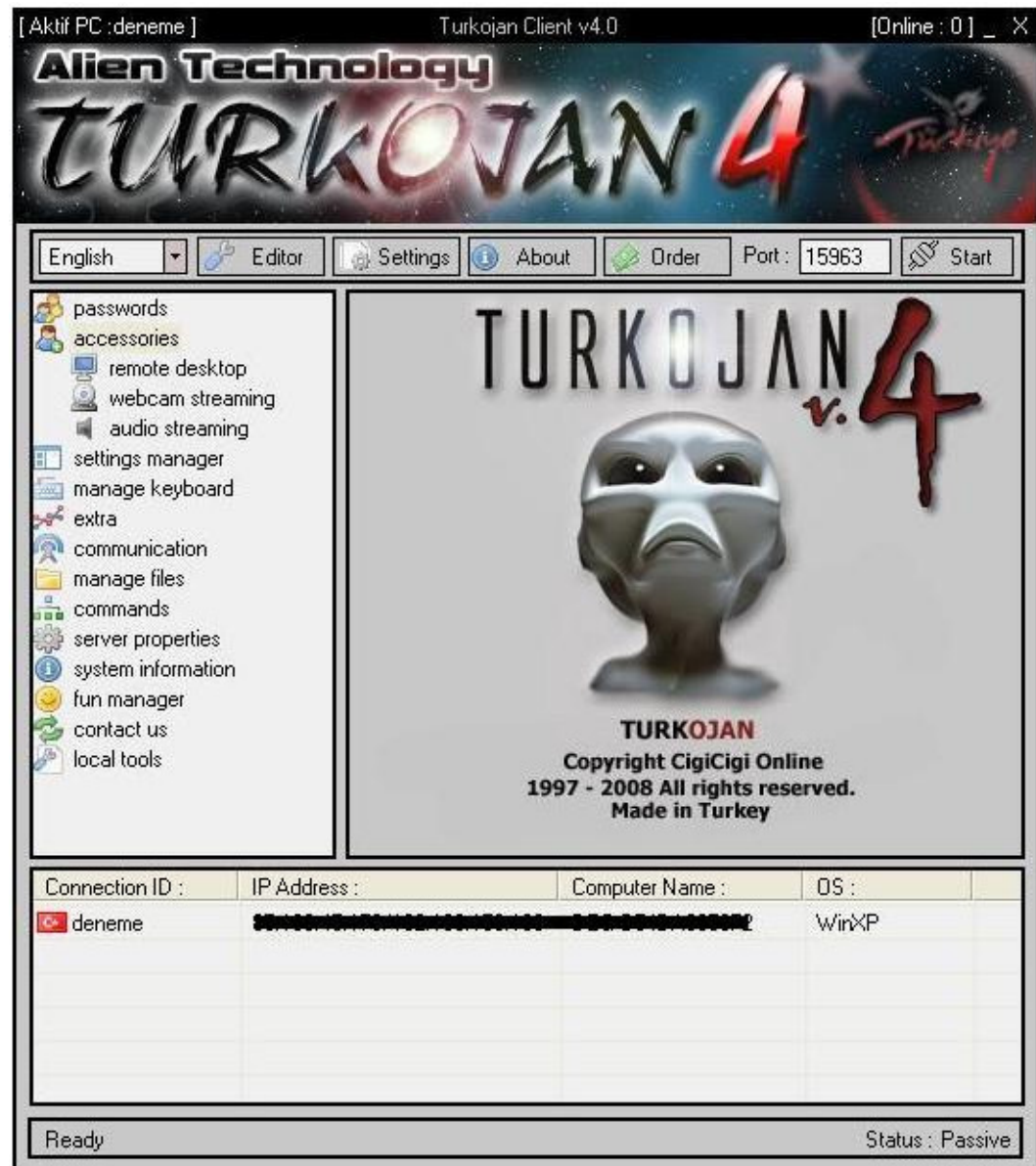✓ Information about remote computer

✓ Etc..

[Aktif PC :deneme]　　Turkojan Client v4.0　　[Online : 0] _ X

Alien Technology

TURKOJAN 4 Türkiye

English ▼ | 🔧 Editor | 🖳 Settings | ⓘ About | 📄 Order | Port : 15963 | 🔌 Start

- passwords
- accessories
  - 🖥 remote desktop
  - 🖵 webcam streaming
  - 🔊 audio streaming
- 📇 settings manager
- ⌨ manage keyboard
- ✂ extra
- 📡 communication
- 📁 manage files
- 🏢 commands
- ⚙ server properties
- ⓘ system information
- 😊 fun manager
- contact us
- local tools

TURKOJAN v.4
TURKOJAN
Copyright CigiCigi Online
1997 - 2008 All rights reserved.
Made in Turkey

Connection ID :	IP Address :	Computer Name :	OS :
🇹🇷 deneme	▬▬▬▬▬▬▬	▬▬▬▬▬▬▬	WinXP

Ready　　　　Status : Passive

Features, service levels, and technical support

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 95/90/ME/NT/2000/XP/Vista
- Webcam streaming is avaliable with this version
- Realtime Screen viewing(controlling is disabled)
- Notifies changements 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 changements on clipboard and save them
- Technical support after installing software
- Viewing pictures without any download(Thumbnail Viewer)

Price : **249$** (United State Dollar)

Threats   Operational Security   Emerging Trends   IBM

---

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
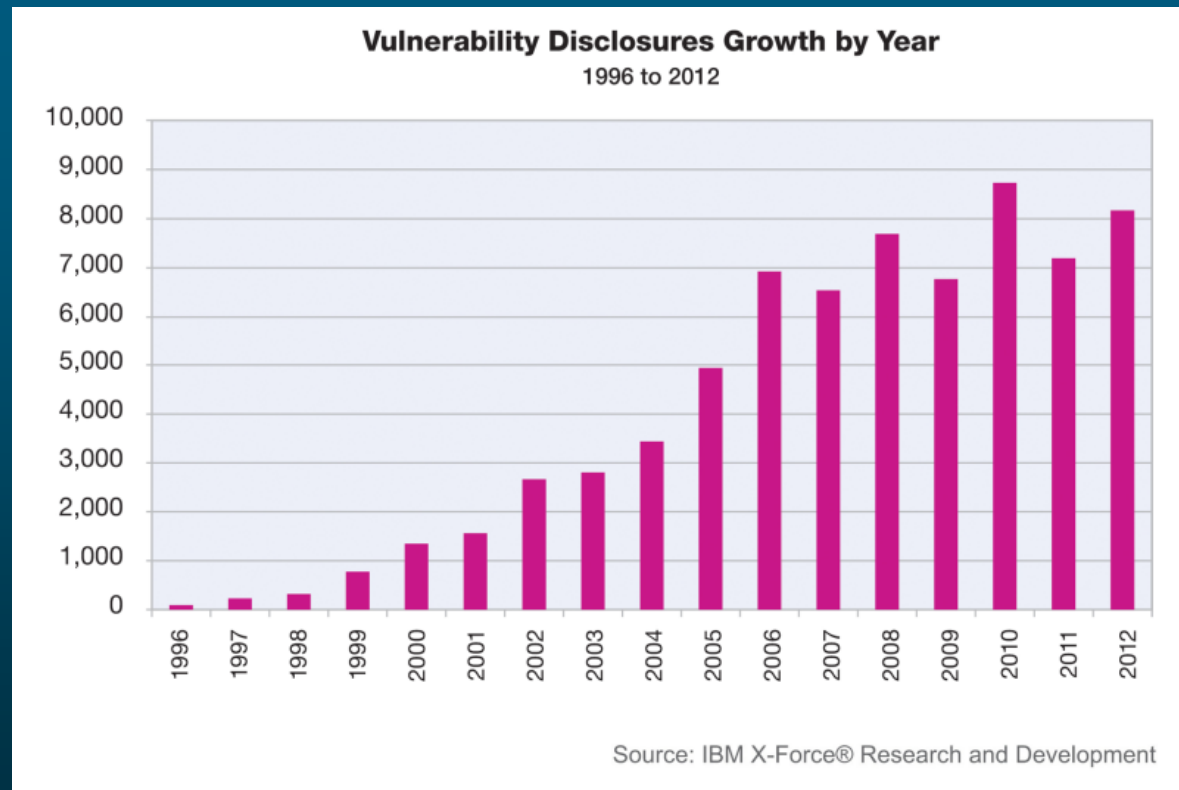✓ Ability to easily allow adding/removing of exploits

Software vulnerabilities - disclosures up in 2012

8,168

publicly
disclosed
vulnerabilities

An increase of
over 14% from
2011

Vulnerability Disclosures Growth by Year
1996 to 2012

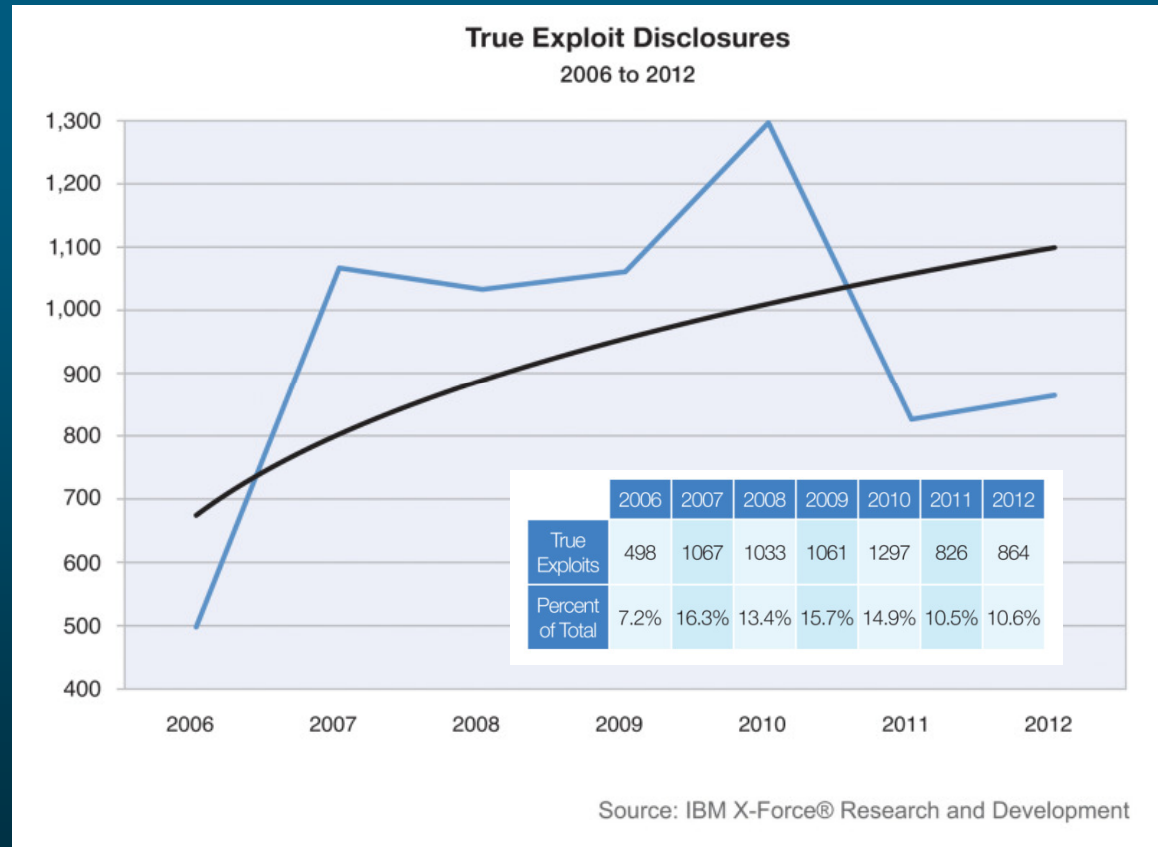| Year	
1996	~0
1997	~200
1998	~300
1999	~750
2000	~1,300
2001	~1,550
2002	~2,650
2003	~2,800
2004	~3,450
2005	~4,900
2006	~6,900
2007	~6,550
2008	~7,700
2009	~6,750
2010	~8,700
2011	~7,200
2012	~8,150

Source: IBM X-Force® Research and Development

Public exploit disclosures – not as many "true exploits"

Continued downward trend in percentage of public exploit disclosures to vulnerabilities
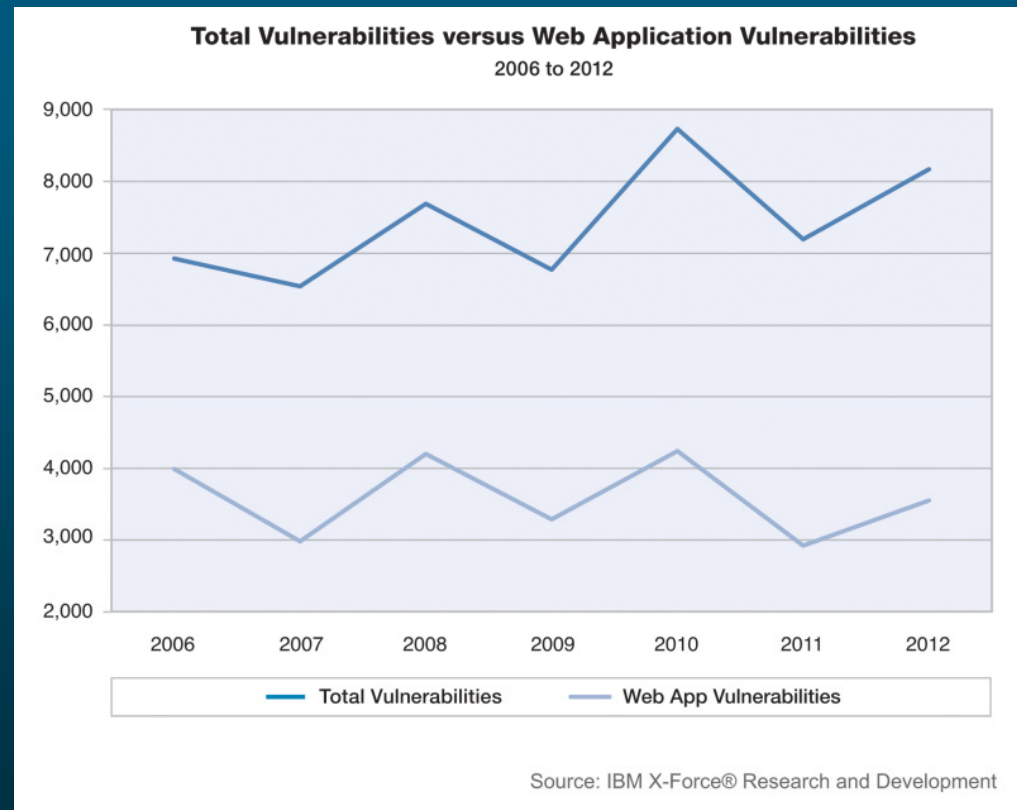
Slightly up in actual numbers compared to 2011

True Exploit Disclosures
2006 to 2012

	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%
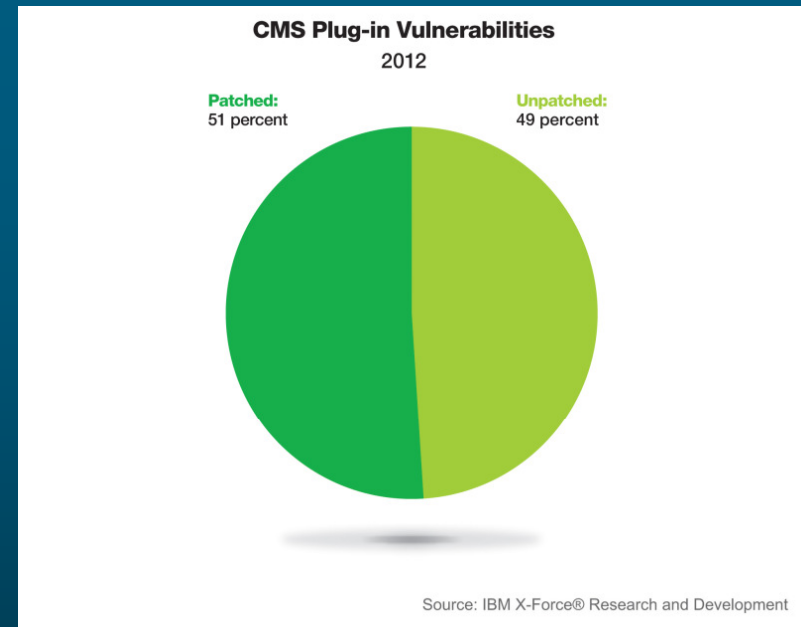
Total Vulnerabilities versus Web Application Vulnerabilities
2006 to 2012

Source: IBM X-Force® Research and Development

Content Management Systems plug-ins provide soft target

CMS Core Vulnerabilities
2012

Patched: 71 percent   Unpatched: 29 percent

Source: IBM X-Force® Research and Development

CMS Plug-in Vulnerabilities
2012

Patched: 51 percent   Unpatched: 49 percent

Source: IBM X-Force® Research and Development
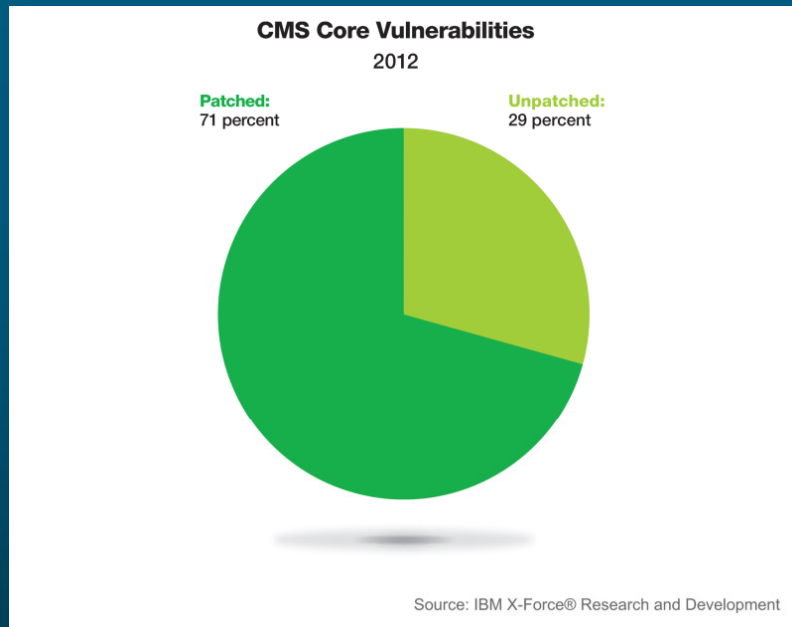
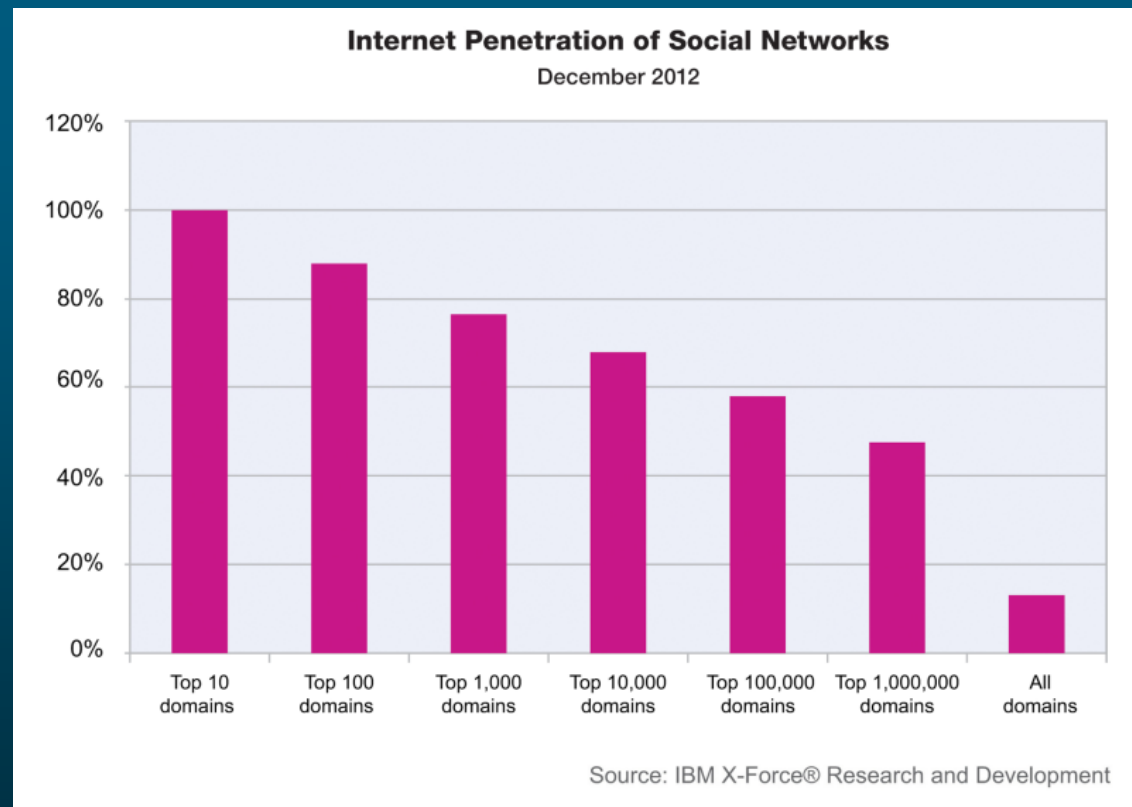Attackers know that CMS vendors more readily address and patch their exposures

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

Internet Penetration of Social Networks
December 2012

Source: IBM X-Force® Research and Development

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

Questions?

ibm.com/security
smartersecurity.nl

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?