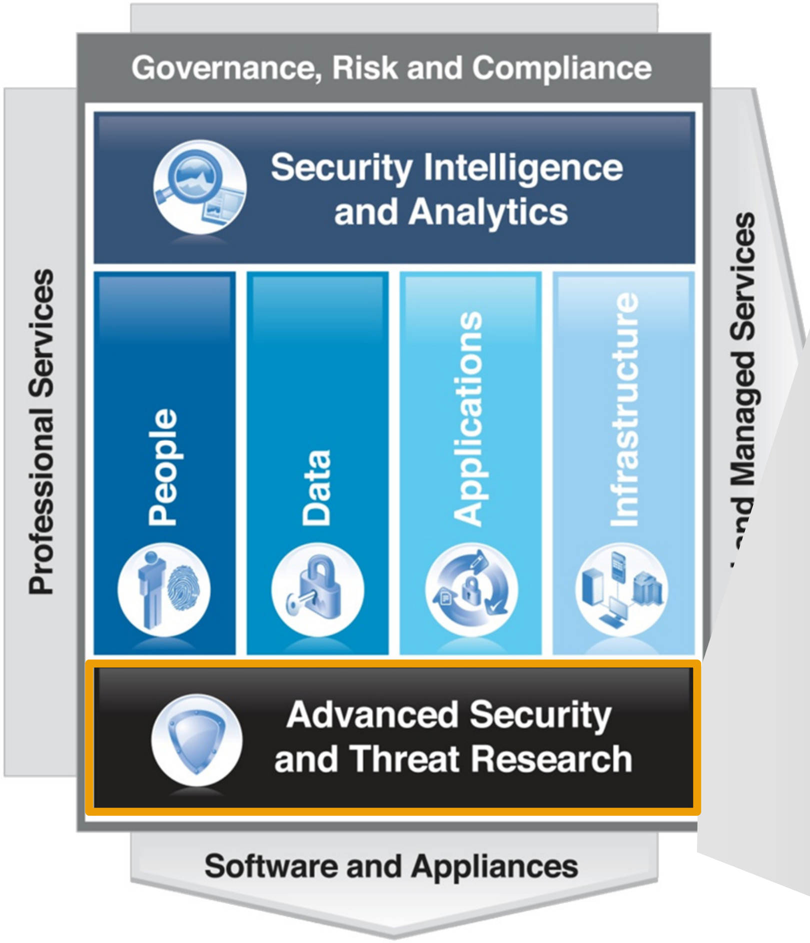
IBM SolutionsConnect 2013
Turning Opportunity into Outcomes.

# 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

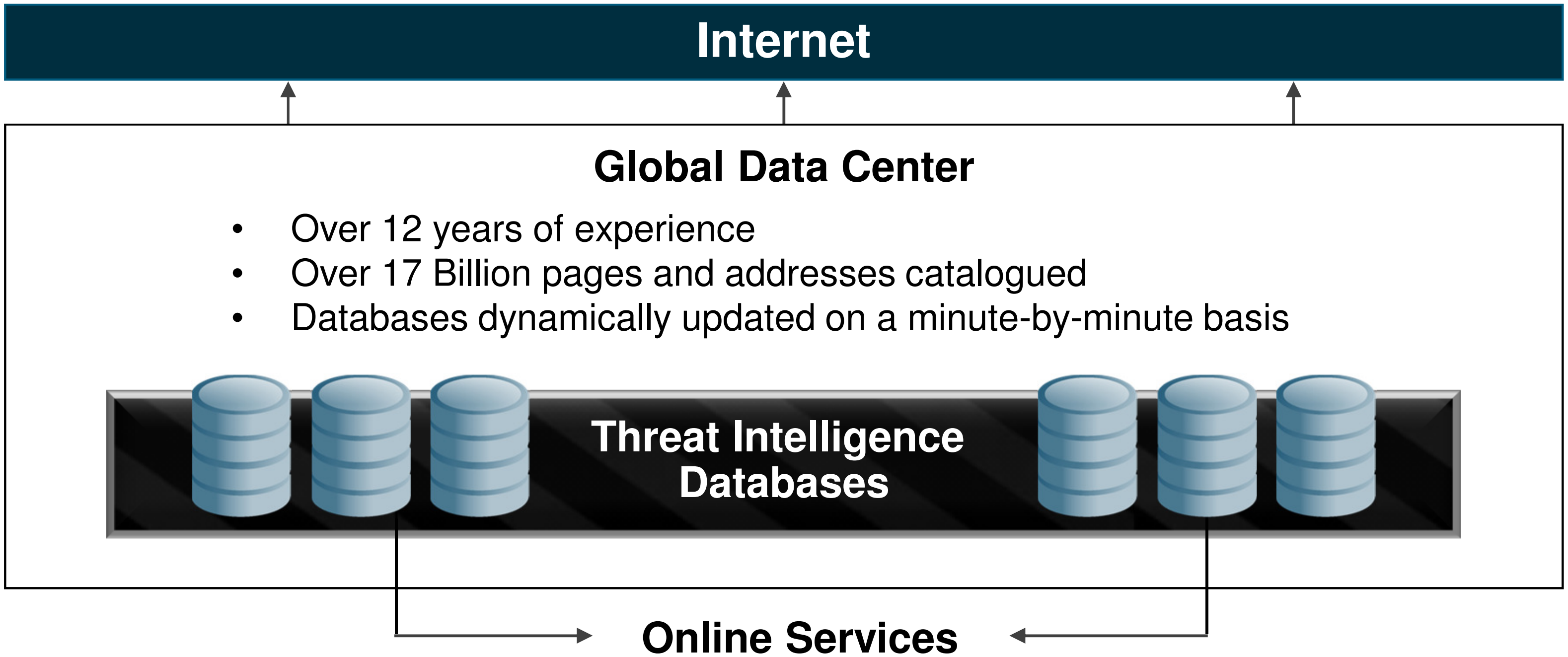

Governance, Risk and Compliance
Security Intelligence and Analytics
People
Data
Applications
Infrastructure
Advanced Security and Threat Research
Professional Services
nd Managed Services
Software and Appliances

X-FORCE

## 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

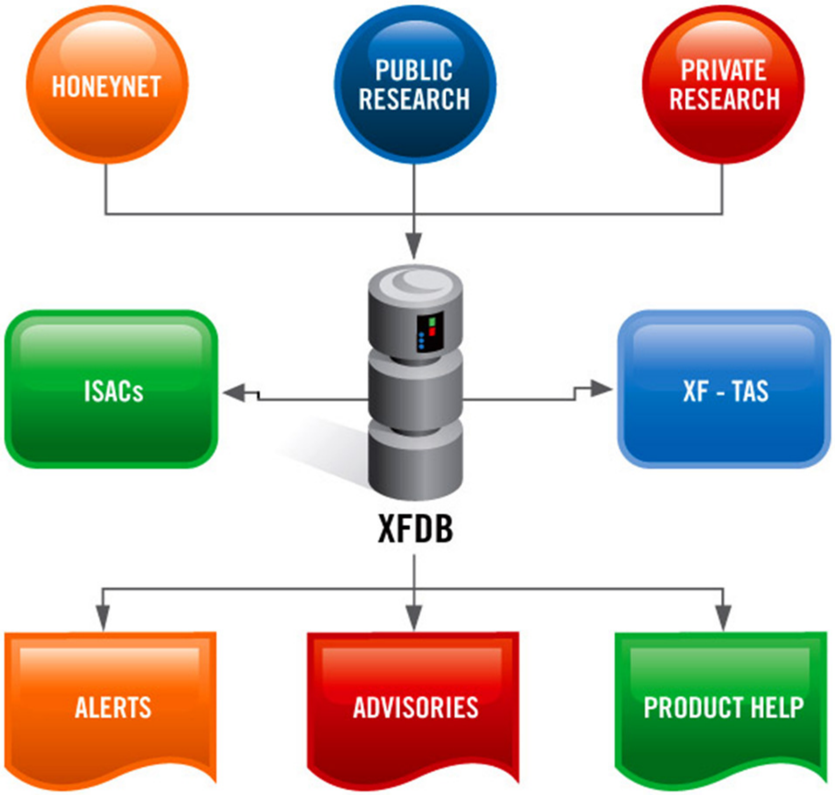
# **Research** - Analyzing all vulnerabilities - X-Force Database (XFDB)

## 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

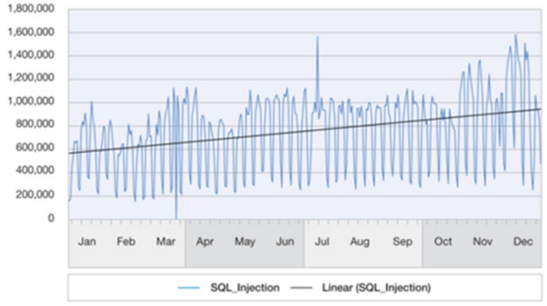
## Research also turns into innovative product "engines"

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



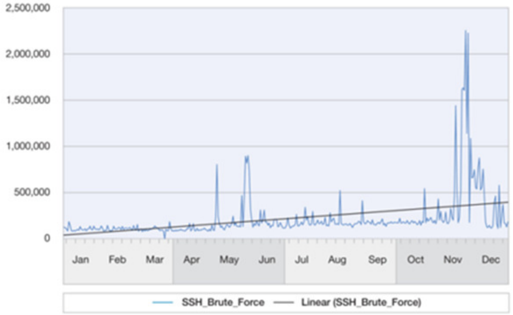
# **Educate** - unique "optics" on the latest security and risk trends

**Top MSS High Volume Signatures and Trend Line – SQL_Injection**
2011



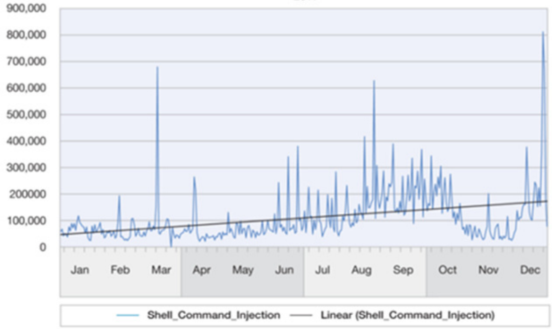
Source: IBM X-Force® Research and Development

**Top MSS High Volume Signatures and Trend Line – SSH_Brute_Force**
2011

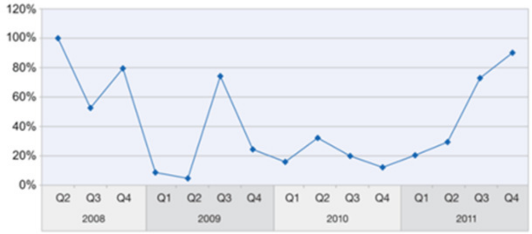


Source: IBM X-Force® Research and Development

**Top MSS High Volume Signatures and Trend Line – Shell_Command_Injection**
2011

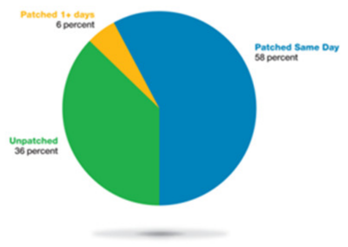


**Scam/Phishing Volume Over Time**
2008 Q2 to 2011 Q4



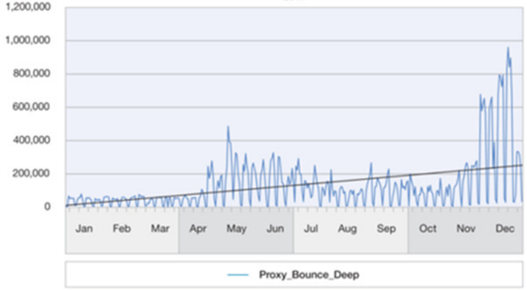
Source: IBM X-Force® Research and Development

**Vendor Patch Timeline**
2011

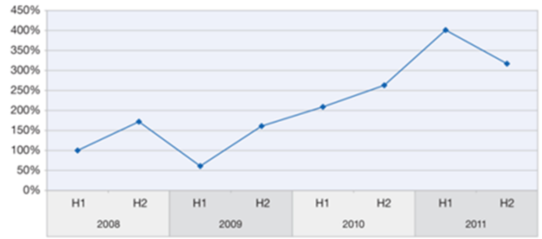


Source: IBM X-Force® Research and Development

**Top MSS High Volume Signatures and Trend Line – Proxy_Bounce_Deep**
2011

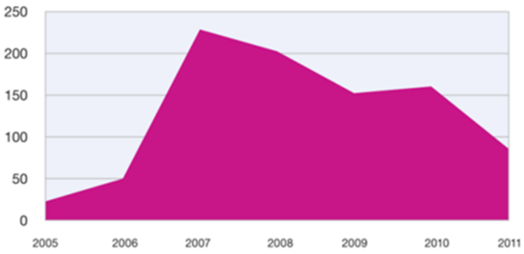


**Volume of Newly Registered Anonymous Proxy Websites**
2008 to 2011



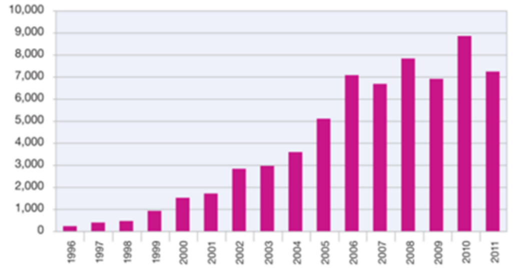
Source: IBM X-Force® Research and Development

**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

# What are we seeing?

IBM X-Force® 2012 Annual Trend and Risk Report

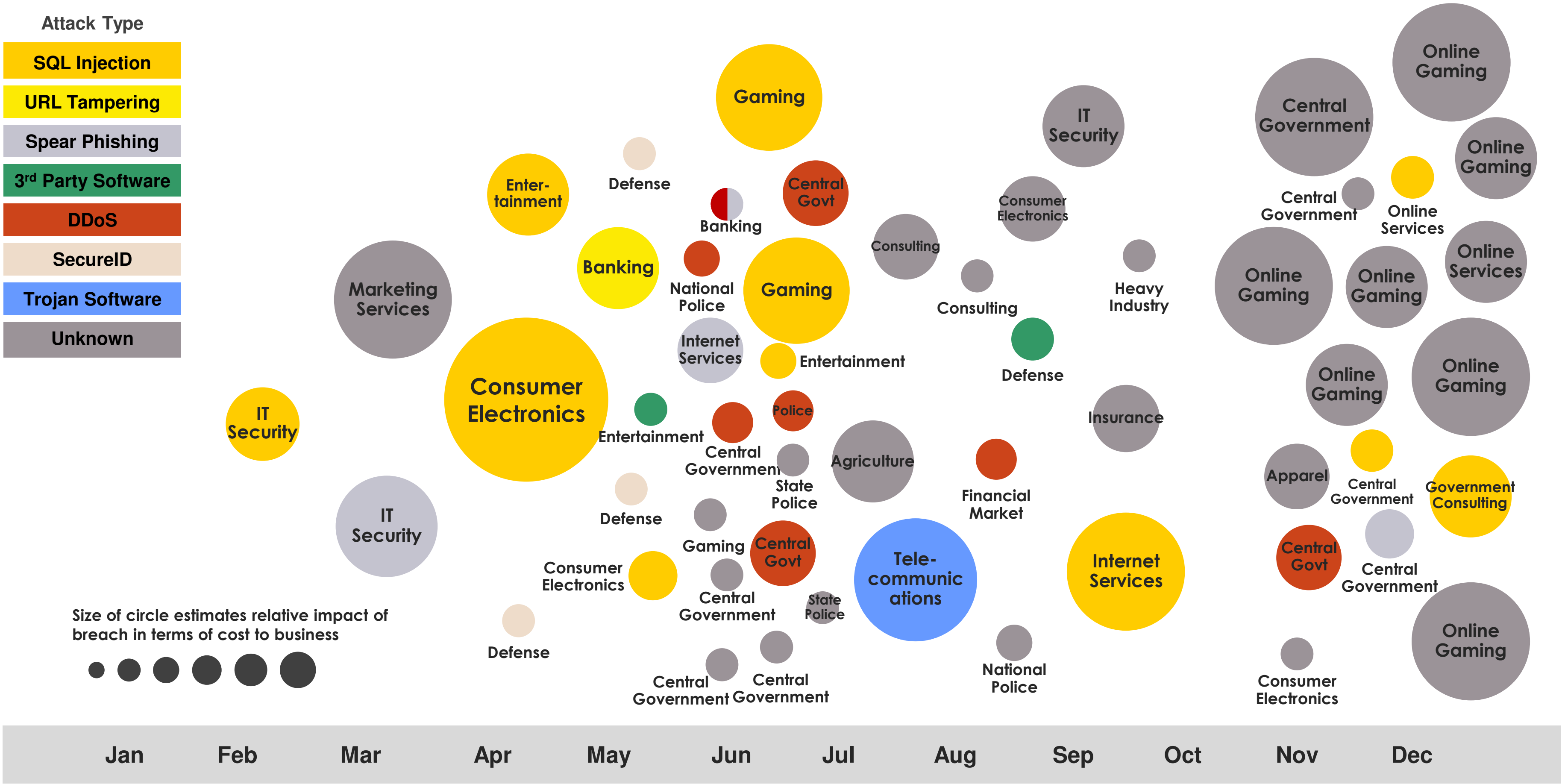
→Download and read about emerging security threats and trends.

**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*

# 2011: “The year of the targeted attack”

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

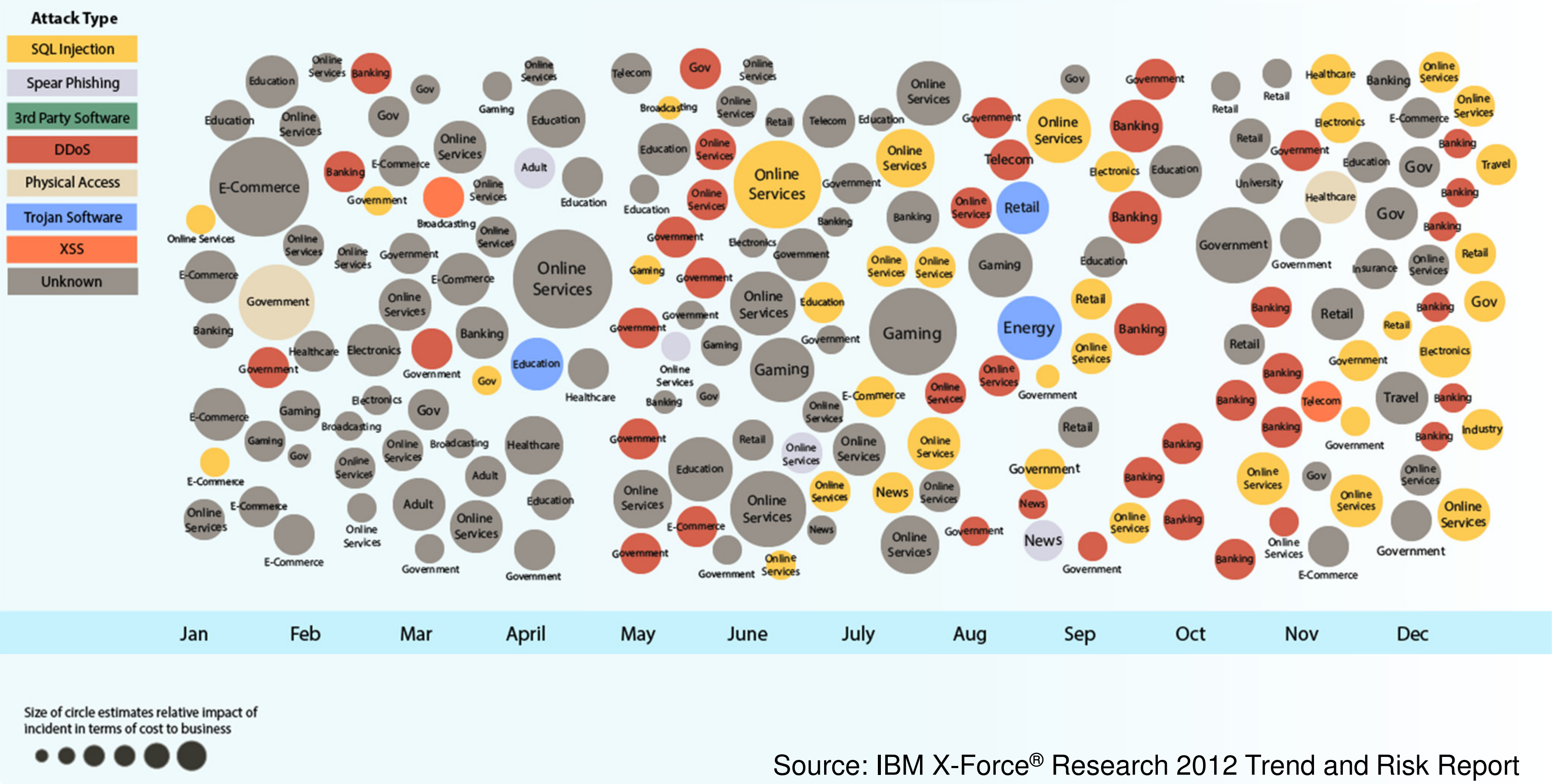


*Source: IBM X-Force® Research 2011 Trend and Risk Report*

# 2012: The explosion of breaches continues!

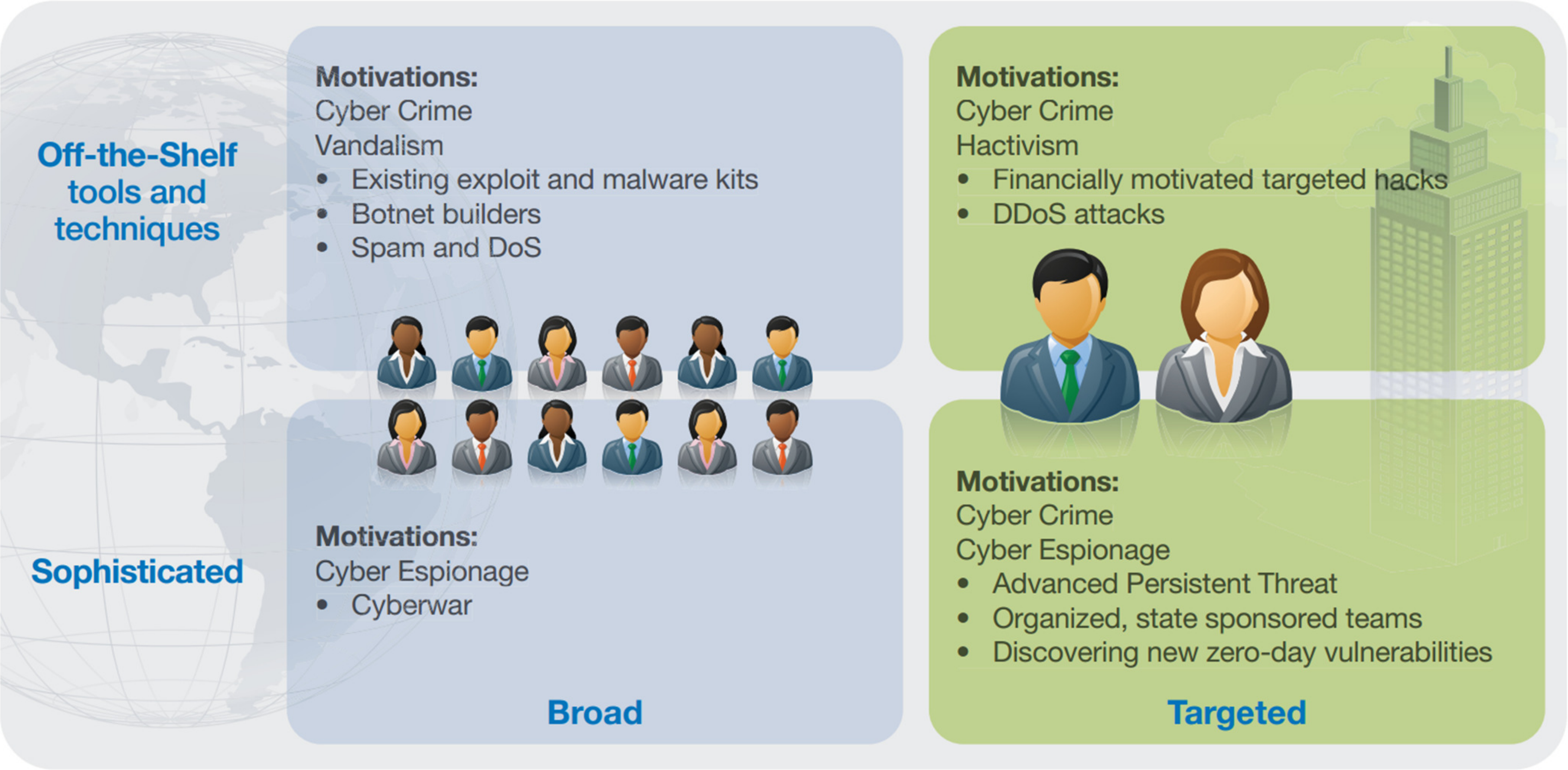
## 2012 Sampling of Security Incidents by Attack Type, Time and Impact

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



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

# Attacker types and motivations have not changed



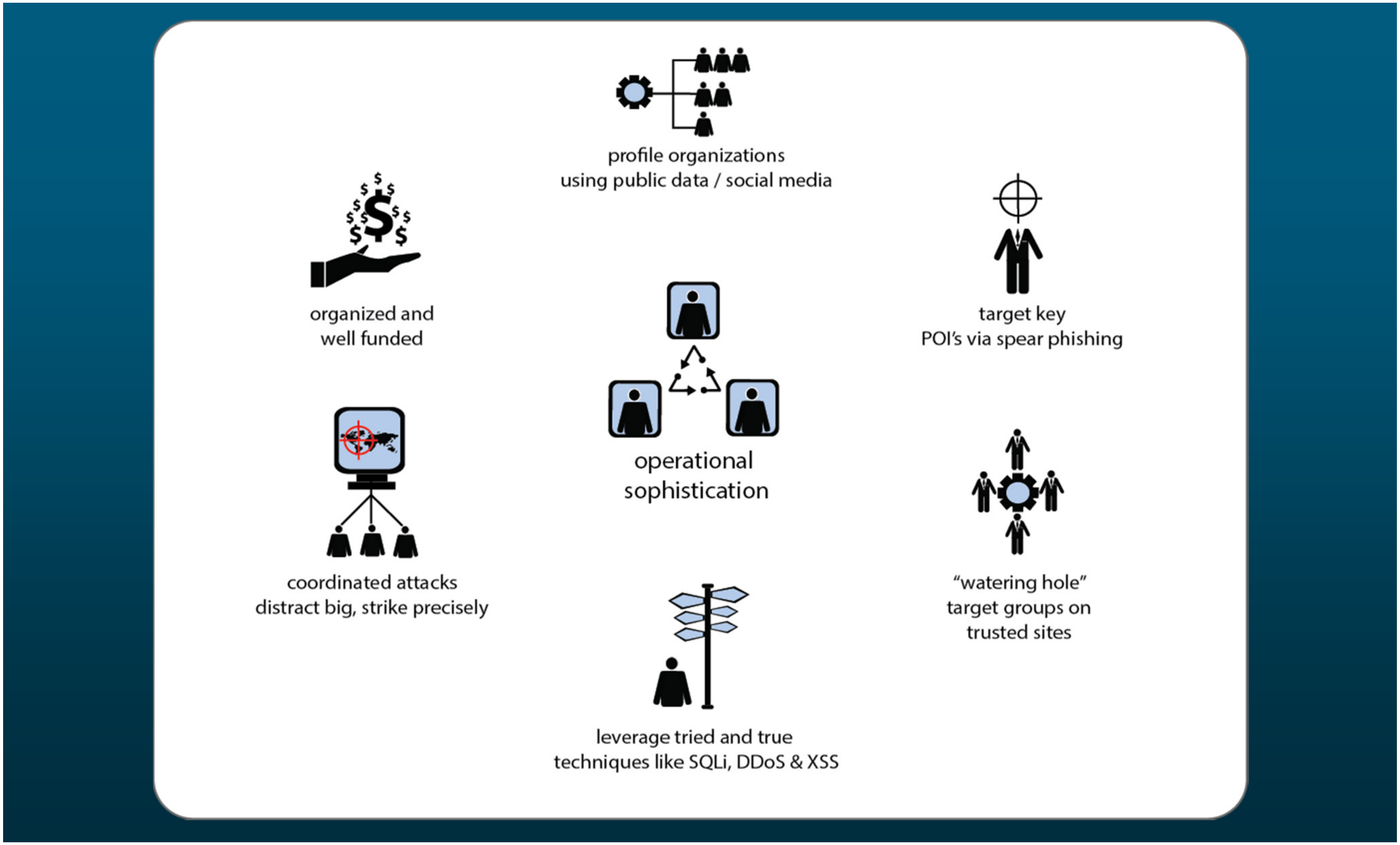
| | Broad | Targeted |
|---|---|---|
| Off-the-Shelf tools and techniques | **Motivations:**<br>Cyber Crime<br>Vandalism<br>• Existing exploit and malware kits<br>• Botnet builders<br>• Spam and DoS | **Motivations:**<br>Cyber Crime<br>Hactivism<br>• Financially motivated targeted hacks<br>• DDoS attacks |
| Sophisticated | **Motivations:**<br>Cyber Espionage<br>• Cyberwar | **Motivations:**<br>Cyber Crime<br>Cyber Espionage<br>• Advanced Persistent Threat<br>• Organized, state sponsored teams<br>• Discovering new zero-day vulnerabilities |

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

operational
sophistication

target key
POI's via spear phishing

coordinated attacks
distract big, strike precisely

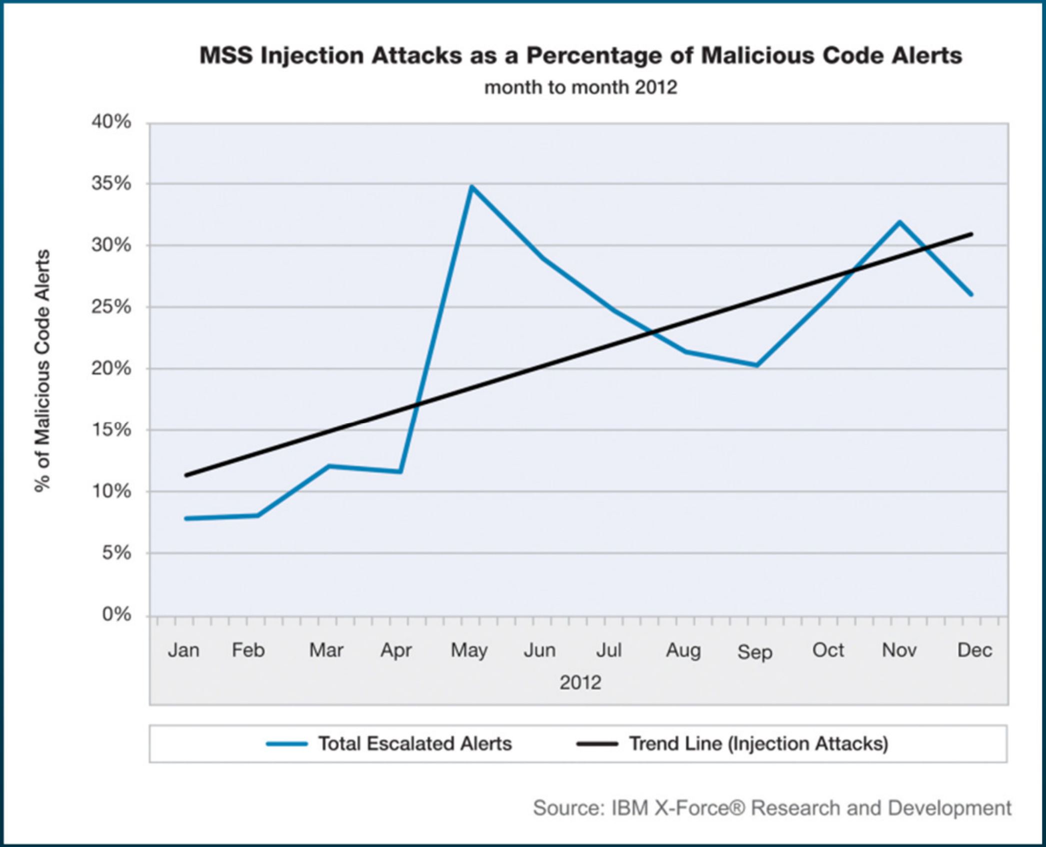
"watering hole"
target groups on
trusted sites

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

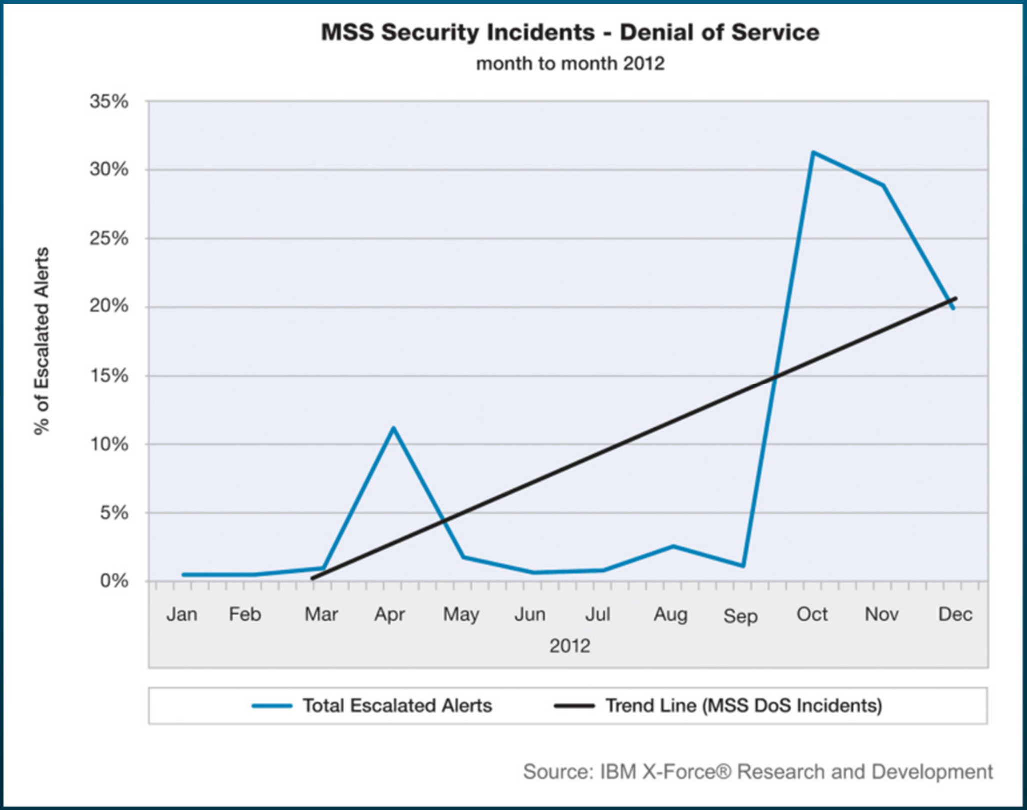


Source: IBM X-Force® Research and Development

# 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



Source: IBM X-Force® Research and Development

# Tried and true techniques - Spear-phishing against social networks

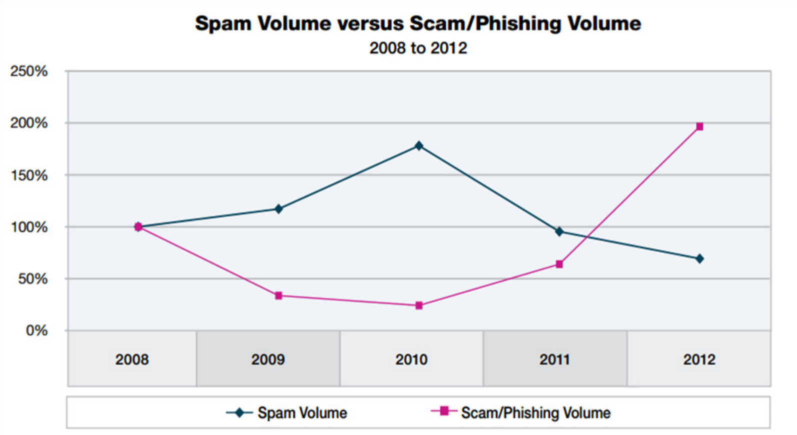


*Figure 23: Spam Volume versus Scam/Phishing Volume – 2008 to 2012*

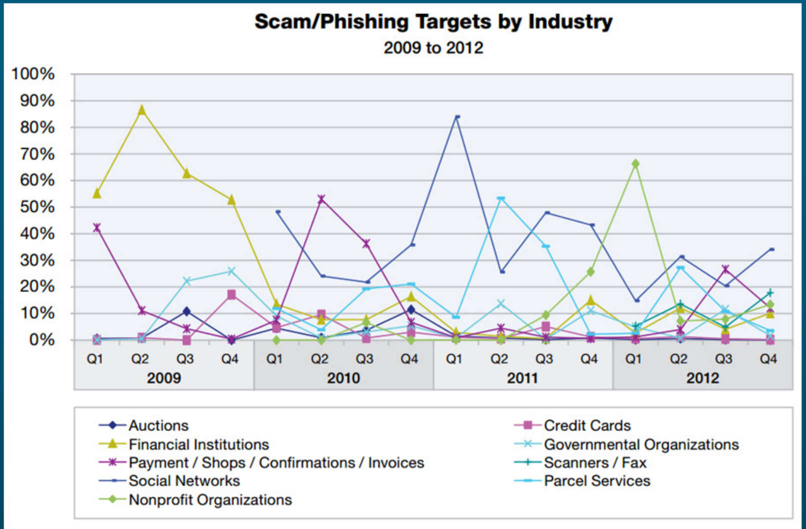


*Figure 24: Scam/Phishing Targets by Industry – 2009 to 2012*[60]

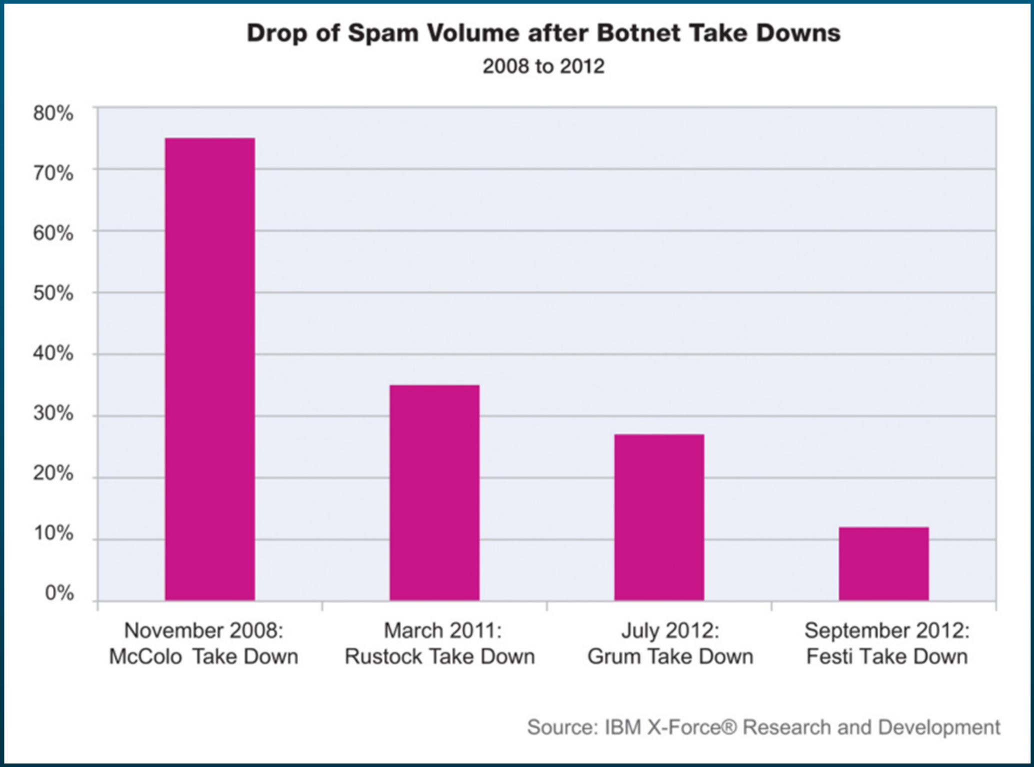
Overall spam volume continues to decline, but **spam containing malicious attachments is on the rise**

Scammers rotate the “carousel” of their targets – **focusing on social networks** in 2012

# Botnet Command & Control Server resiliency

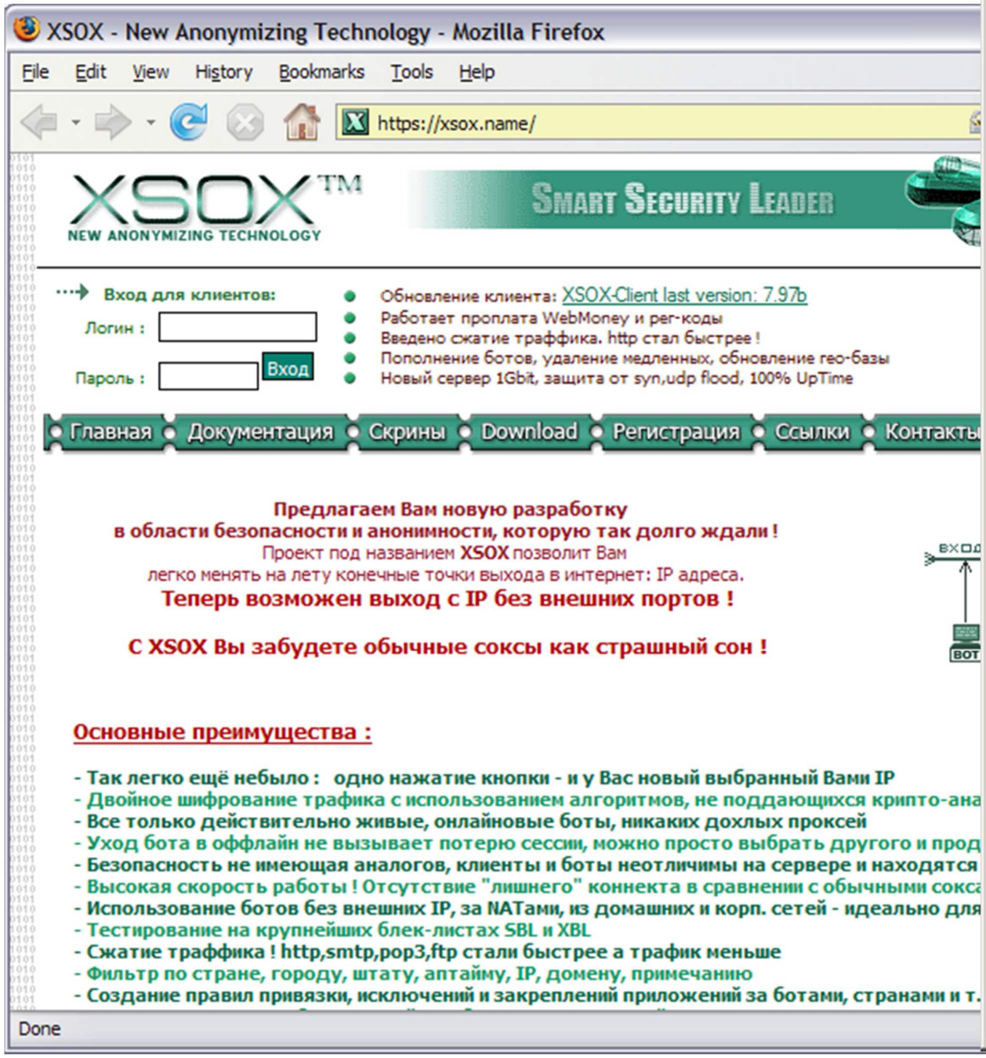
## Operational sophistication:

When botnet command and control servers are taken down, other readily available networks can be put into action



Source: IBM X-Force® Research and Development

# XSOX – Botnet Anonymizer



XSOX - New Anonymizing Technology - Mozilla Firefox

File Edit View History Bookmarks Tools Help
https://xsox.name/
XSOX™
NEW ANONYMIZING TECHNOLOGY
SMART SECURITY LEADER

Вход для клиентов:

Логин :

Пароль :

Вход

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

Главная Документация Скрины Download Регистрация Ссылки Контакты

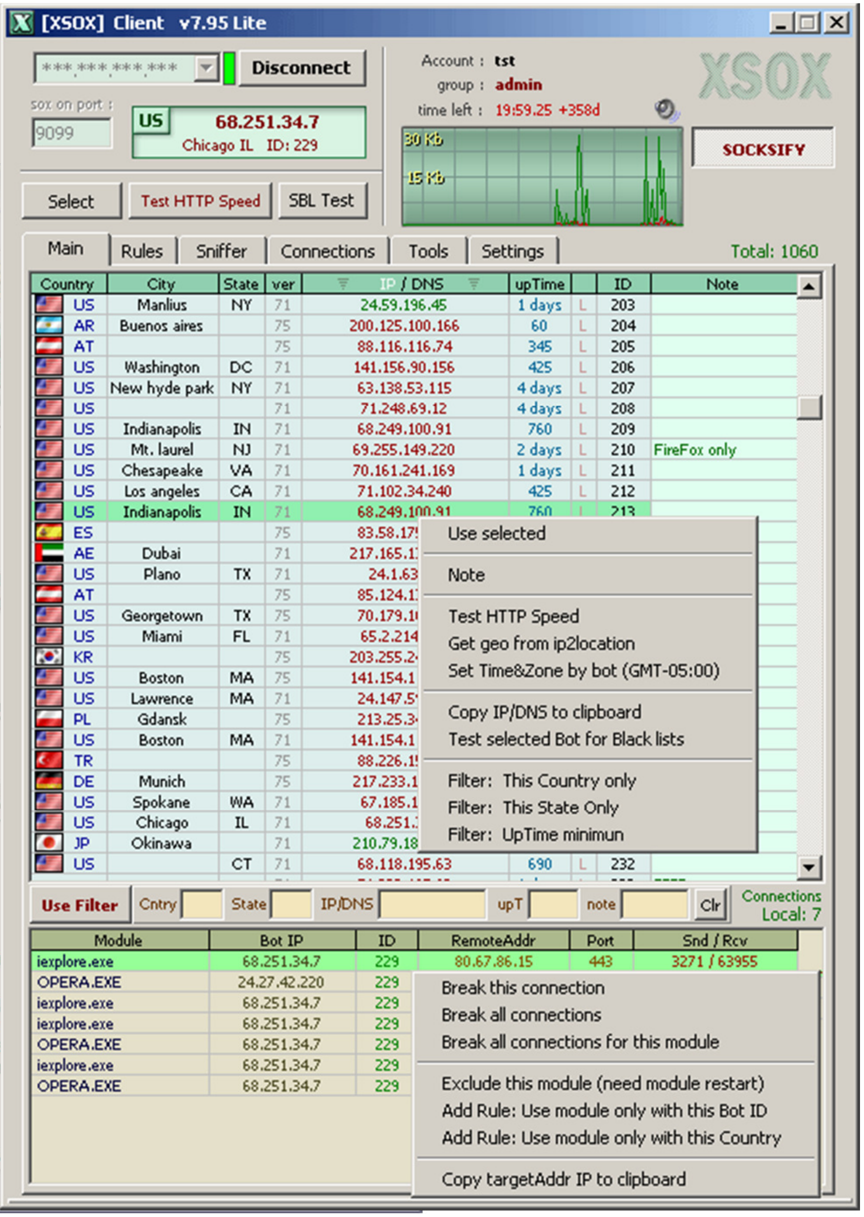
**Предлагаем Вам новую разработку**
**в области безопасности и анонимности, которую так долго ждали !**
Проект под названием **XSOX** позволит Вам
легко менять на лету конечные точки выхода в интернет: IP адреса.
**Теперь возможен выход с IP без внешних портов !**

**С XSOX Вы забудете обычные соксы как страшный сон !**

**Основные преимущества :**

- Так легко ещё небыло : одно нажатие кнопки - и у Вас новый выбранный Вами IP
- Двойное шифрование трафика с использованием алгоритмов, не поддающихся крипто-ана
- Все только действительно живые, онлайновые боты, никаких дохлых проксей
- Уход бота в оффлайн не вызывает потерю сессии, можно просто выбрать другого и прод
- Безопасность не имеющая аналогов, клиенты и боты неотличимы на сервере и находятся
- Высокая скорость работы ! Отсутствие "лишнего" коннекта в сравнении с обычными сокса
- Использование ботов без внешних IP, за NATами, из домашних и корп. сетей - идеально для
- Тестирование на крупнейших блек-листах SBL и XBL
- Сжатие траффика ! 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.

Done



[XSOX] Client v7.95 Lite

sox on port : 9099

US 68.251.34.7
Chicago IL ID: 229

Account : tst
group : admin
time left : 19:59.25 +358d

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 | 83.58.17 | | | | |
| AE | Dubai | | 71 | 217.165.1 | | | | |
| US | Plano | TX | 71 | 24.1.63 | | | | |
| AT | | | 75 | 85.124.1 | | | | |
| US | Georgetown | TX | 75 | 70.179.1 | | | | |
| 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 | 88.226.1 | | | | |
| 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 | |

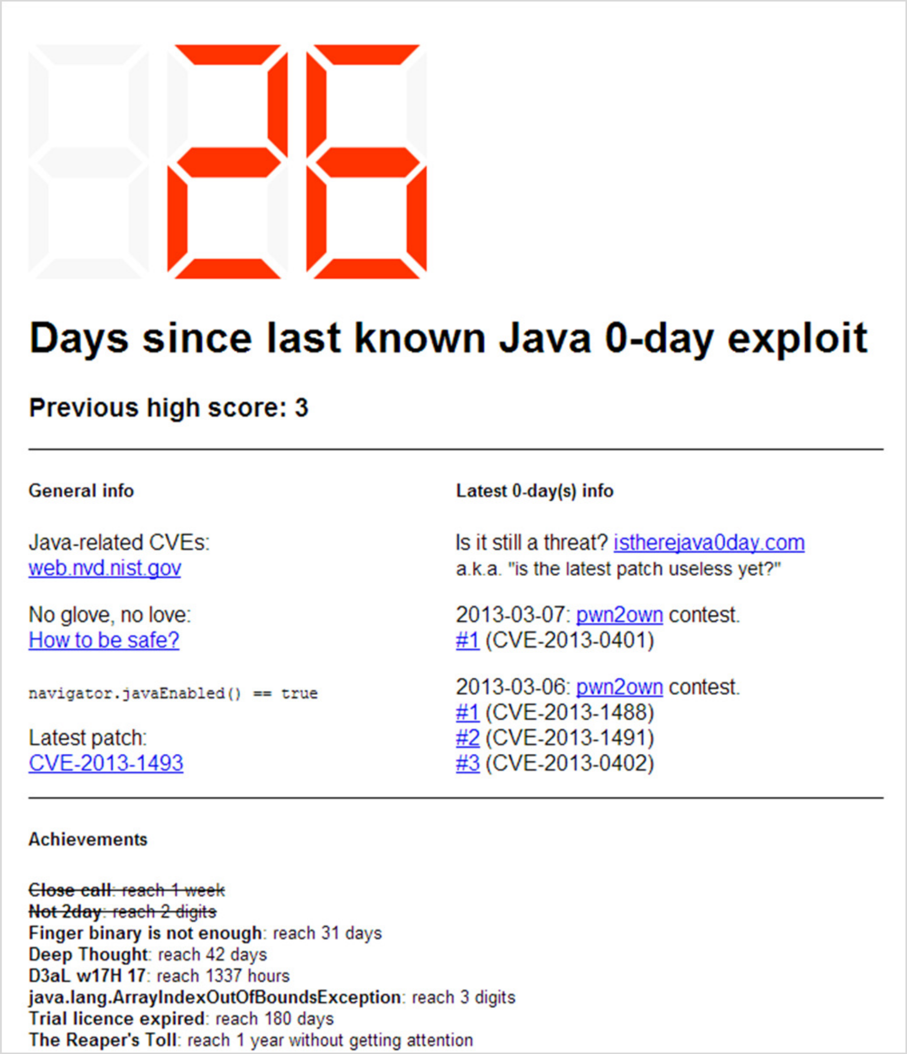
Connections Local: 7

| 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**

Java-related CVEs: web.nvd.nist.gov

No glove, no love: How to be safe?

`navigator.javaEnabled() == true`

Latest patch: CVE-2013-1493

**Latest 0-day(s) info**

Is it still a threat? istherejava0day.com
a.k.a. "is the latest patch useless yet?"

2013-03-07: pwn2own contest.
#1 (CVE-2013-0401)

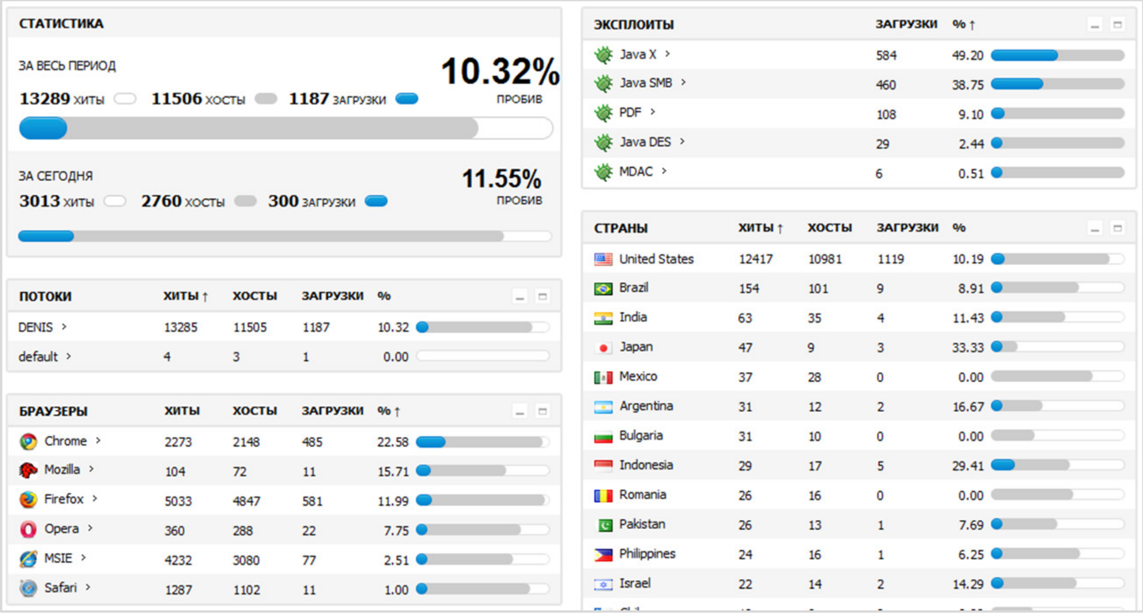
2013-03-06: pwn2own contest.
#1 (CVE-2013-1488)
#2 (CVE-2013-1491)
#3 (CVE-2013-0402)

**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



**СТАТИСТИКА**

ЗА ВЕСЬ ПЕРИОД

13289 хиты ○ 11506 хосты ● 1187 загрузки ● — 10.32% пробив

ЗА СЕГОДНЯ

3013 хиты ○ 2760 хосты ● 300 загрузки ● — 11.55% пробив

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

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

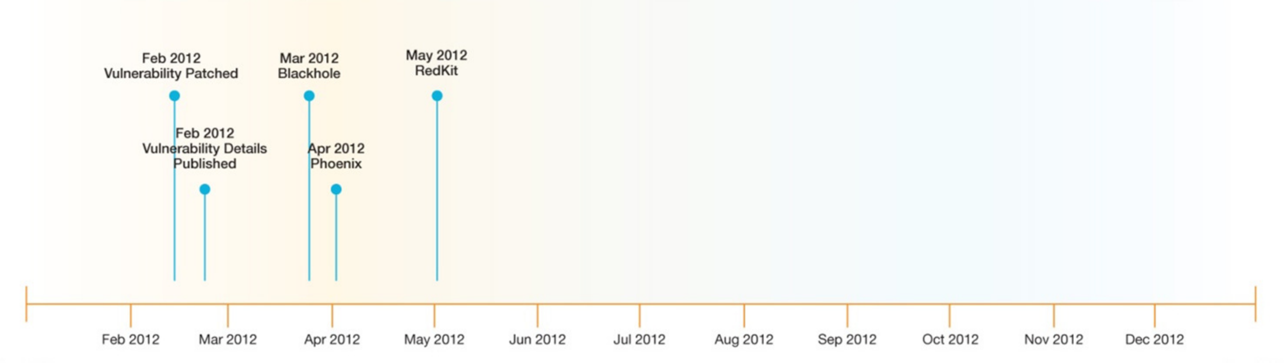
| СТРАНЫ | ХИТЫ ↑ | ХОСТЫ | ЗАГРУЗКИ | % |
|---|---|---|---|---|
| United States | 12417 | 10981 | 1119 | 10.19 |
| Brazil | 154 | 101 | 9 | 8.91 |
| India | 63 | 35 | 4 | 11.43 |
| Japan | 47 | 9 | 3 | 33.33 |
| Mexico | 37 | 28 | 0 | 0.00 |
| Argentina | 31 | 12 | 2 | 16.67 |
| Bulgaria | 31 | 10 | 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

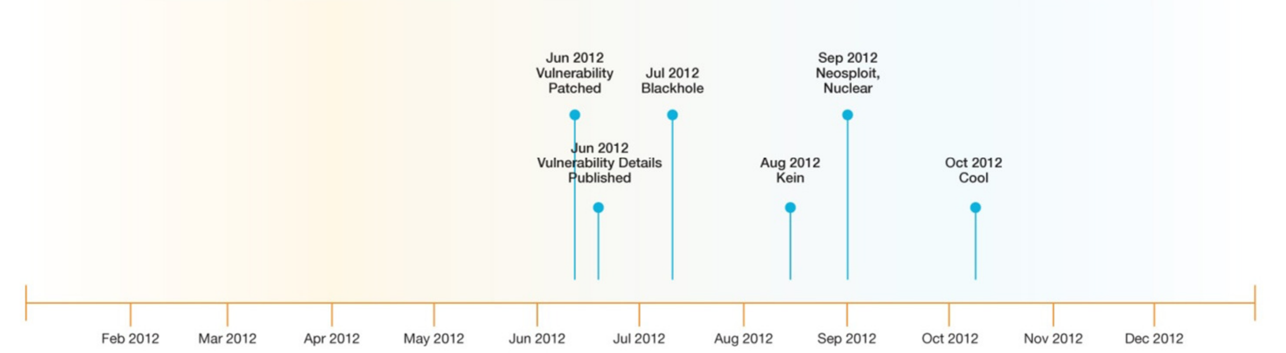
In 2012 we observed an upsurge in web browser exploit kit development and activity - the primary target of which are Java vulnerabilities

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

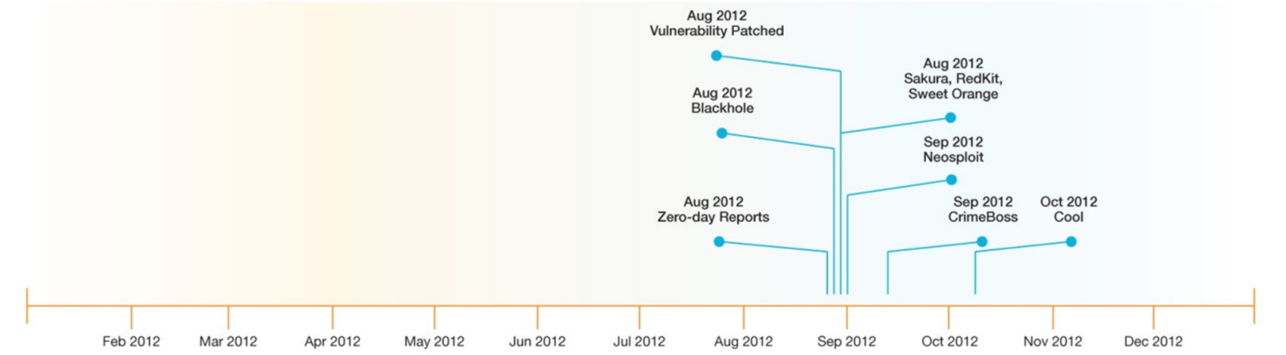
## CVE-2012 -0507



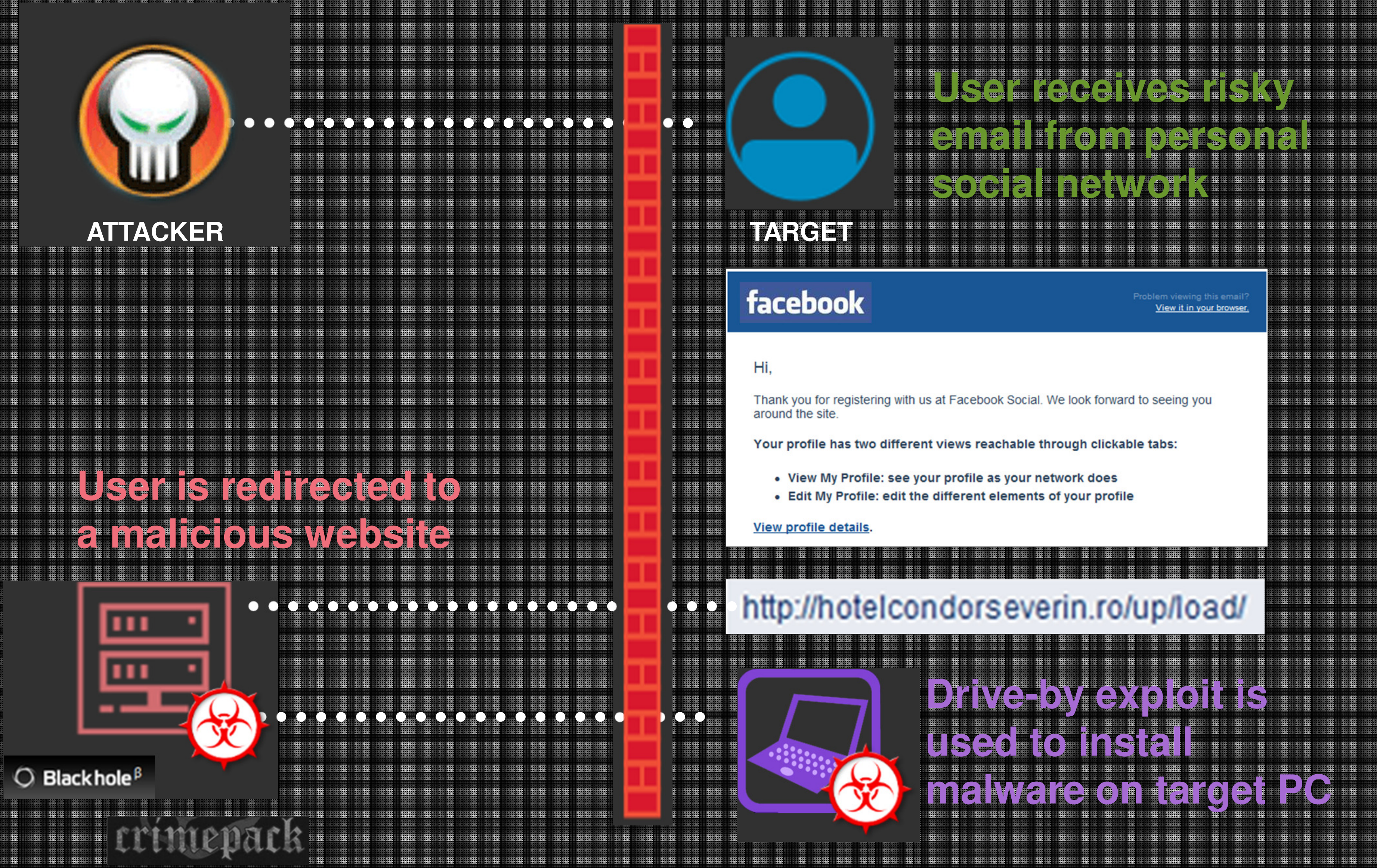
## CVE-2012 -1723



## CVE-2012 -4681



# Spear phishing and Exploit Kit Example



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**

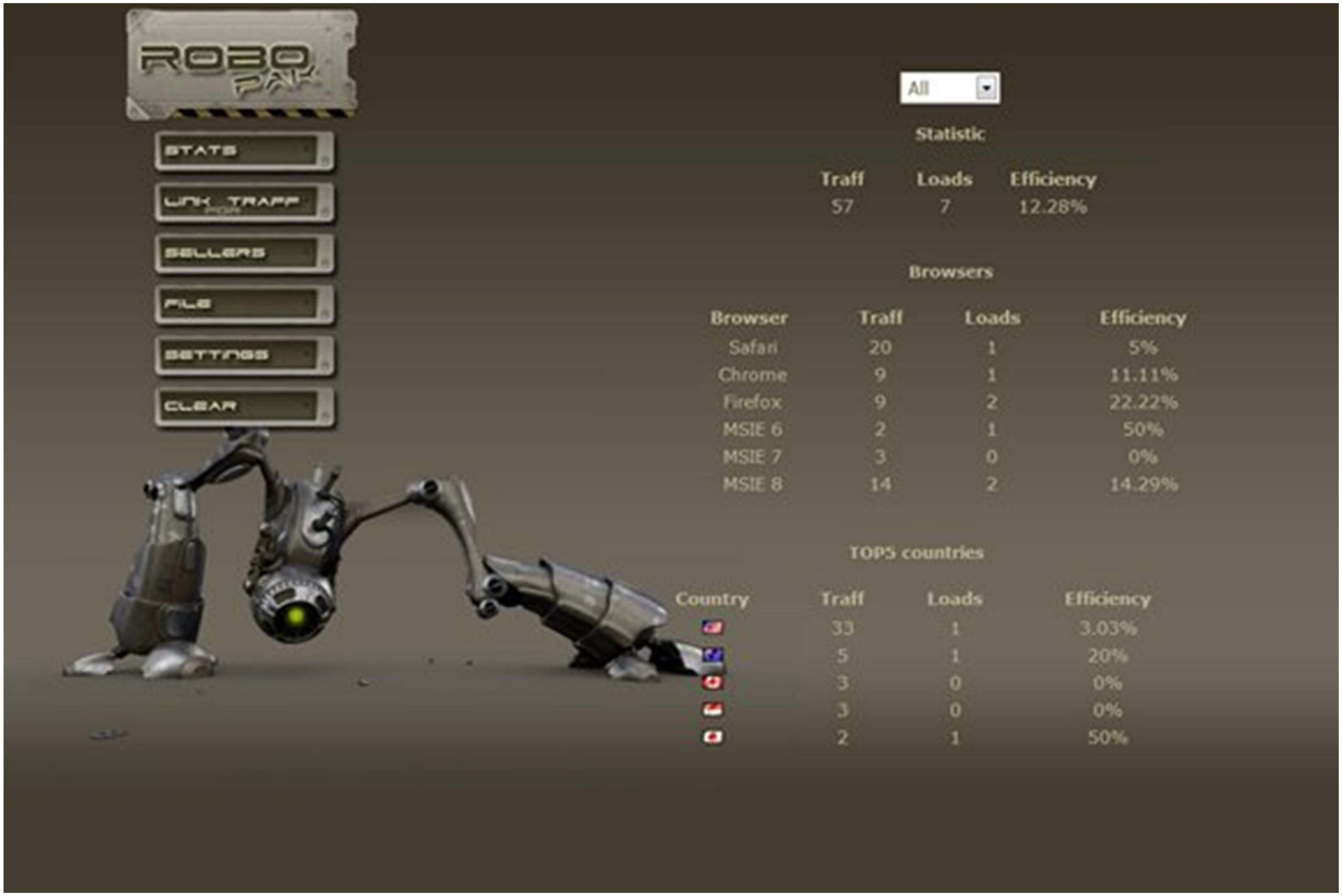
View profile details.

User is redirected to a malicious website

http://hotelcondorseverin.ro/up/load/

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

# Adversaries operate business too… Exploits as a Service



All

Statistic

| Traff | Loads | Efficiency |
|---|---|---|
| 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% |

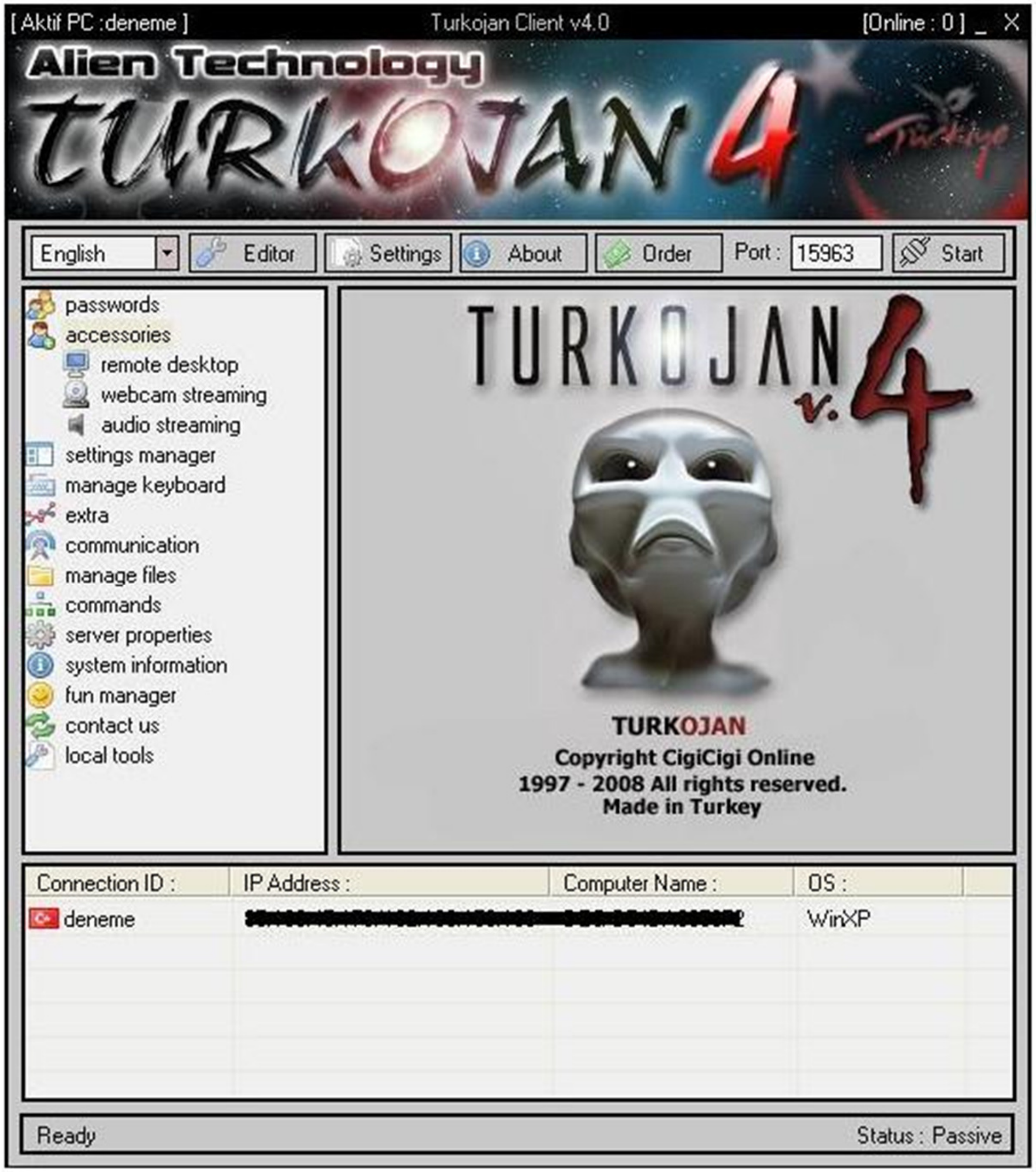
TOP5 countries

| 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..



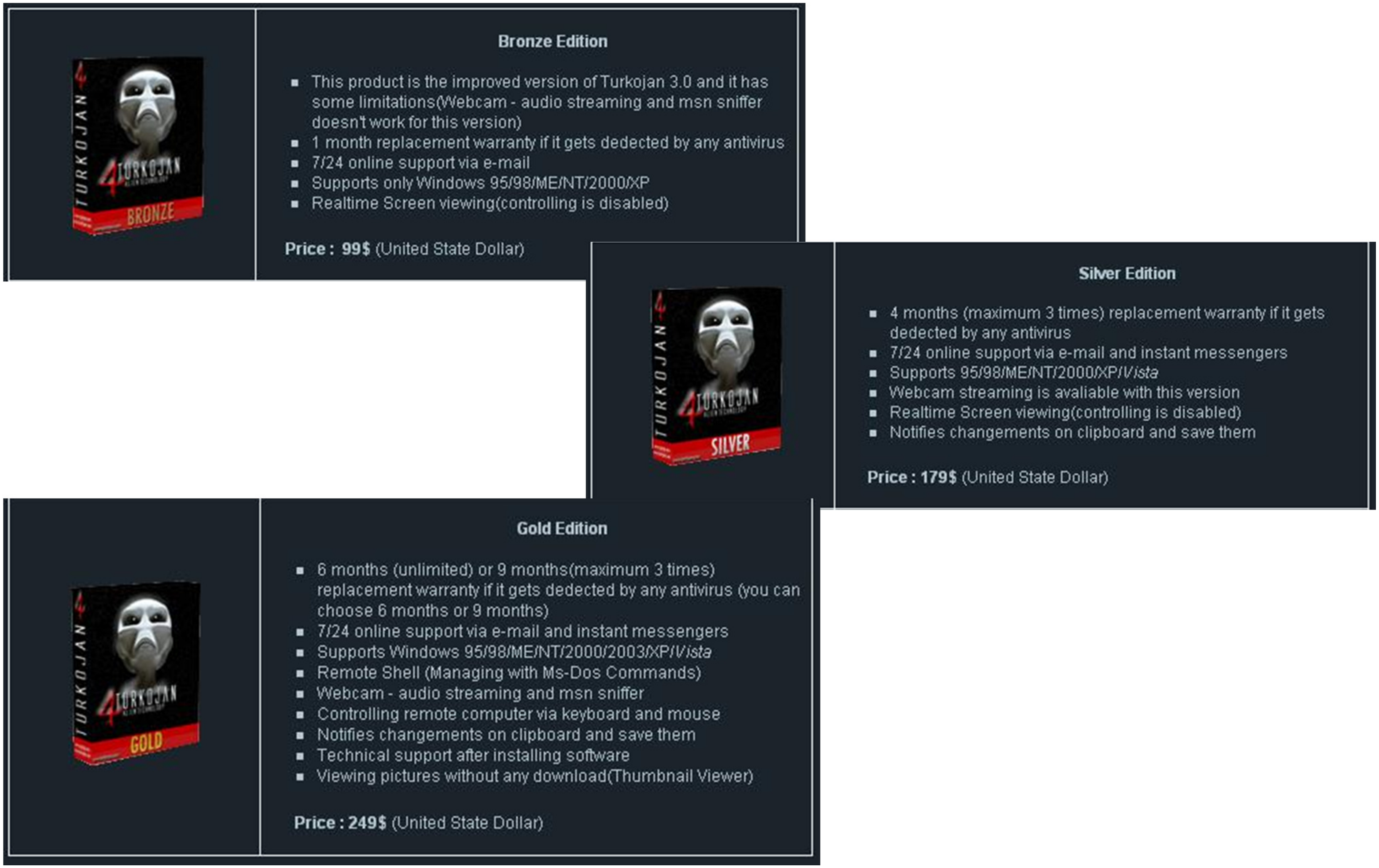
Port : 15963

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

| Connection ID : | IP Address : | Computer Name : | OS : |
|---|---|---|---|
| deneme | [redacted] | | 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**

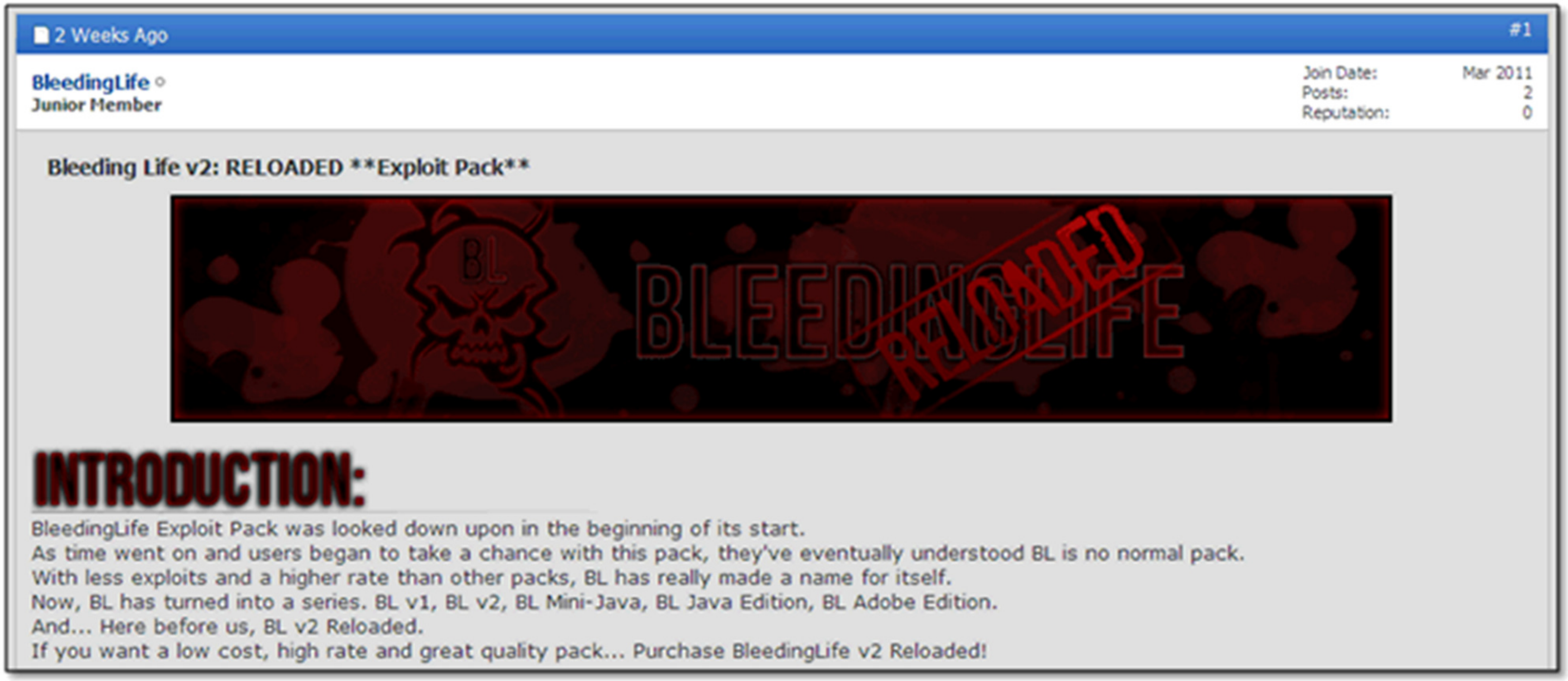
- 4 months (maximum 3 times) replacement warranty if it gets dedected by any antivirus
- 7/24 online support via e-mail and instant messengers
- Supports 95/98/ME/NT/2000/XP/*Vista*
- Webcam streaming is avaliable with this version
- Realtime Screen viewing(controlling is disabled)
- Notifies changements 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)



2 Weeks Ago #1

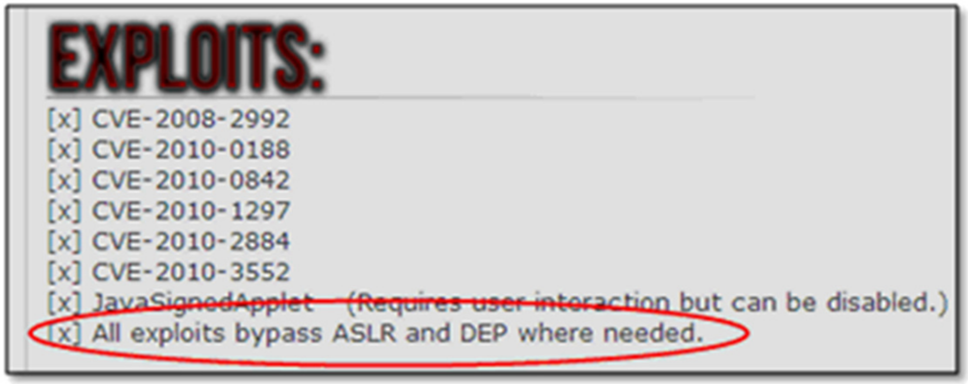
BleedingLife
Junior Member

| | |
|---|---|
| Join Date: | Mar 2011 |
| Posts: | 2 |
| Reputation: | 0 |

Bleeding Life v2: RELOADED **Exploit Pack**

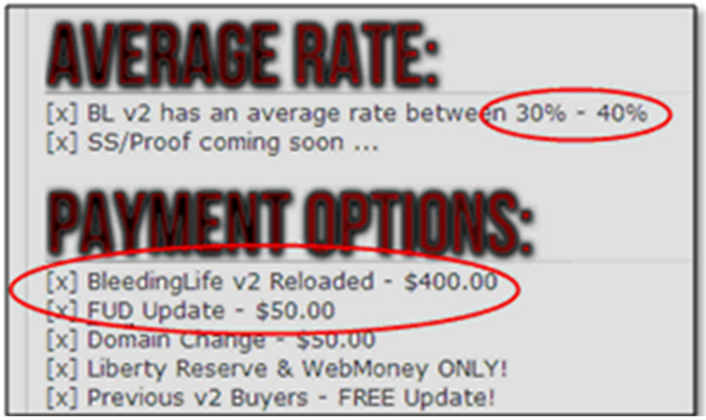
INTRODUCTION:

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:

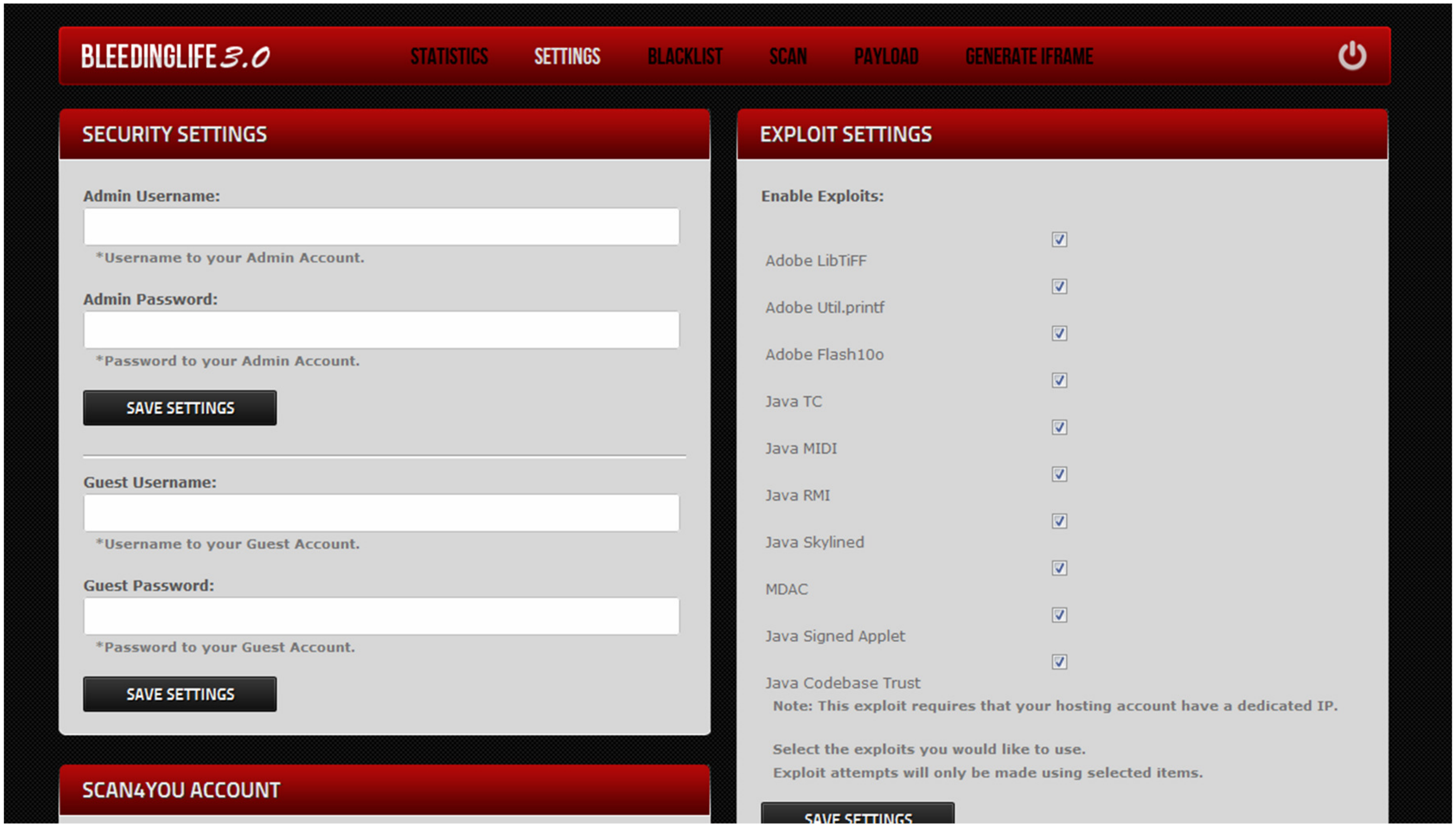
[x] BL v2 has an average rate between 30% - 40%
[x] SS/Proof coming soon ...

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



SECURITY SETTINGS

Admin Username:

*Username to your Admin Account.

Admin Password:

*Password to your Admin Account.

Guest Username:

*Username to your Guest Account.

Guest Password:

*Password to your Guest Account.

SCAN4YOU ACCOUNT

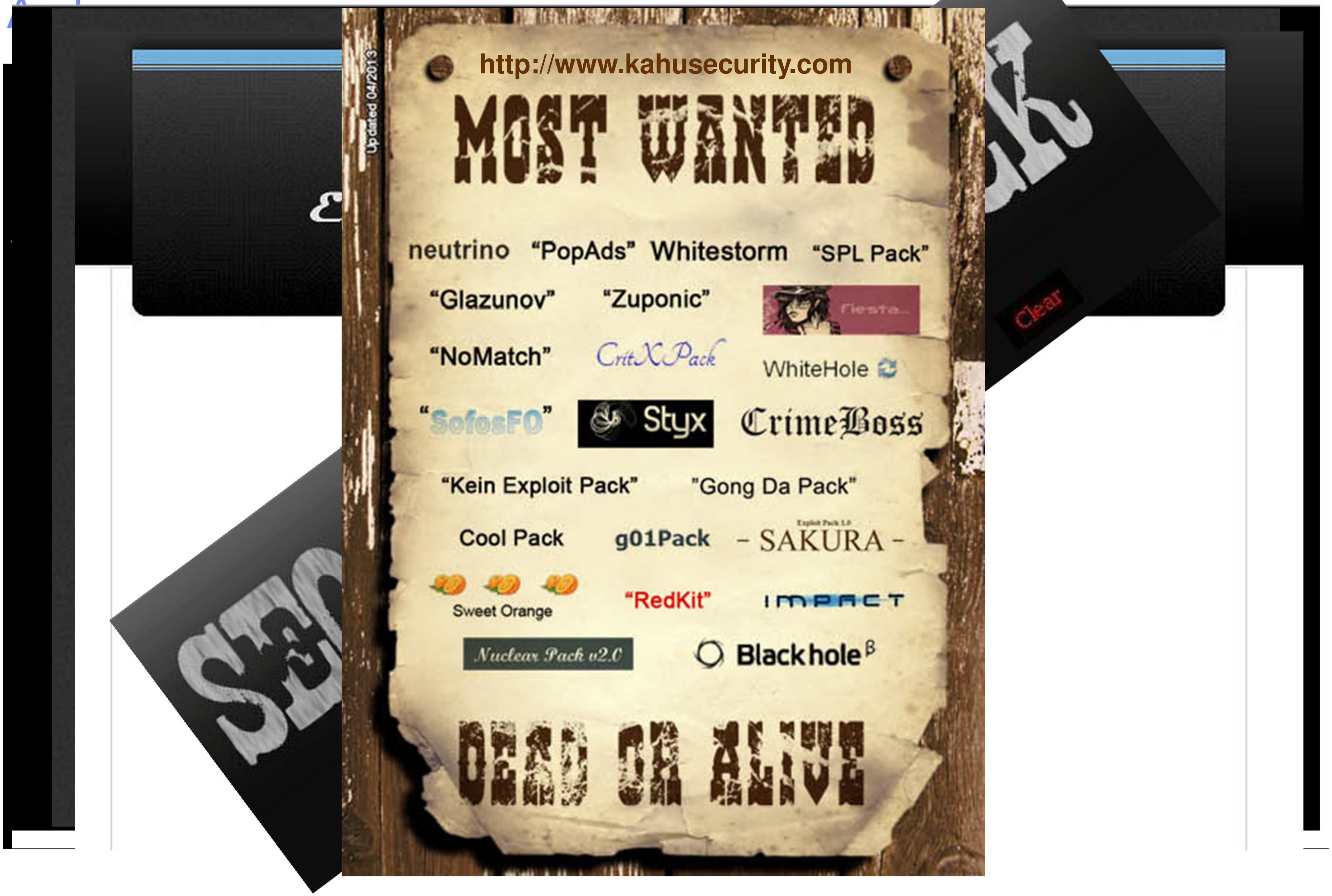
EXPLOIT SETTINGS

Enable Exploits:

- ☑ Adobe LibTiFF
- ☑ Adobe Util.printf
- ☑ Adobe Flash10o
- ☑ Java TC
- ☑ Java MIDI
- ☑ Java RMI
- ☑ Java Skylined
- ☑ MDAC
- ☑ Java Signed Applet
- ☑ Java Codebase Trust

Note: This exploit requires that your hosting account have a dedicated IP.

Select the exploits you would like to use.
Exploit attempts will only be made using selected items.

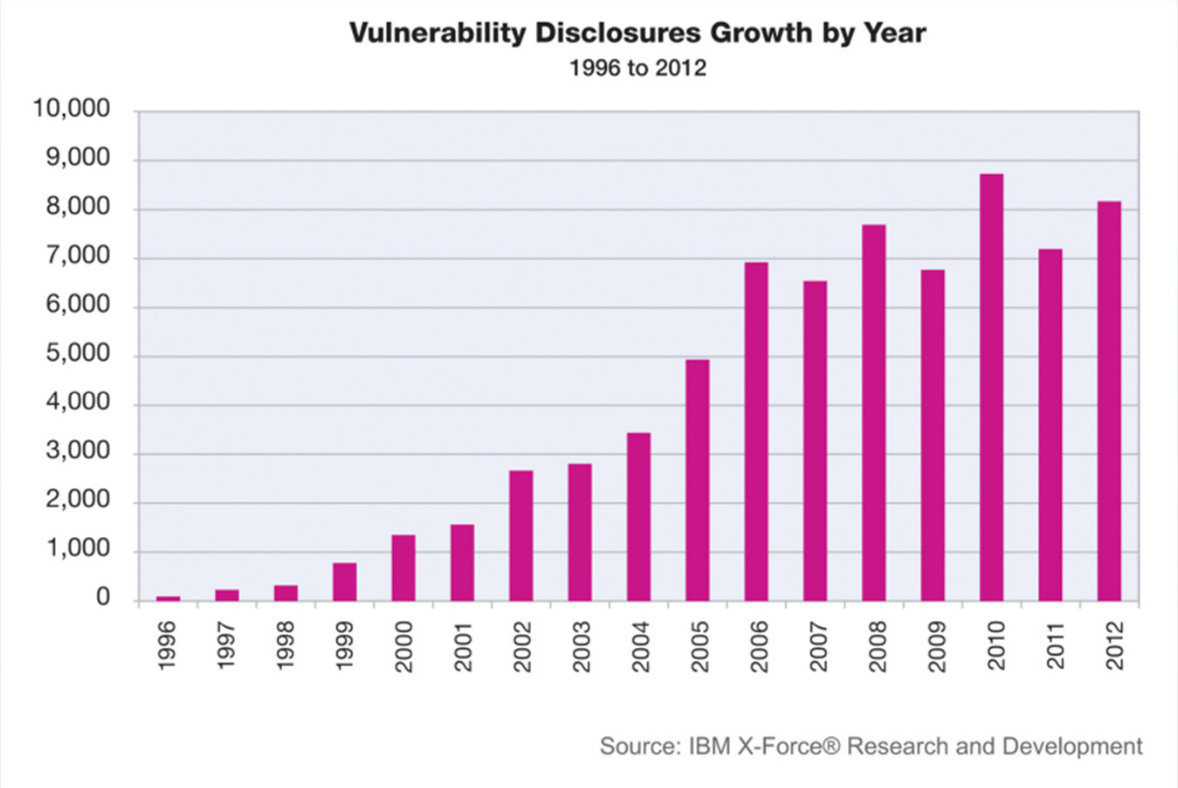

Updated 04/2013
http://www.kahusecurity.com
MOST WANTED
neutrino
"PopAds"
Whitestorm
"SPL Pack"
"Glazunov"
"Zuponic"
Fiesta
"NoMatch"
CritXPack
WhiteHole
"SofosFO"
Styx
CrimeBoss
"Kein Exploit Pack"
"Gong Da Pack"
Cool Pack
g01Pack
Exploit Pack 1.0
– SAKURA –
Sweet Orange
"RedKit"
IMPACT
Nuclear Pack v2.0
Blackhole β
DEAD OR ALIVE
Clear

# Software vulnerabilities - disclosures up in 2012

**8,168**

publicly disclosed vulnerabilities

An increase of over 14% from 2011

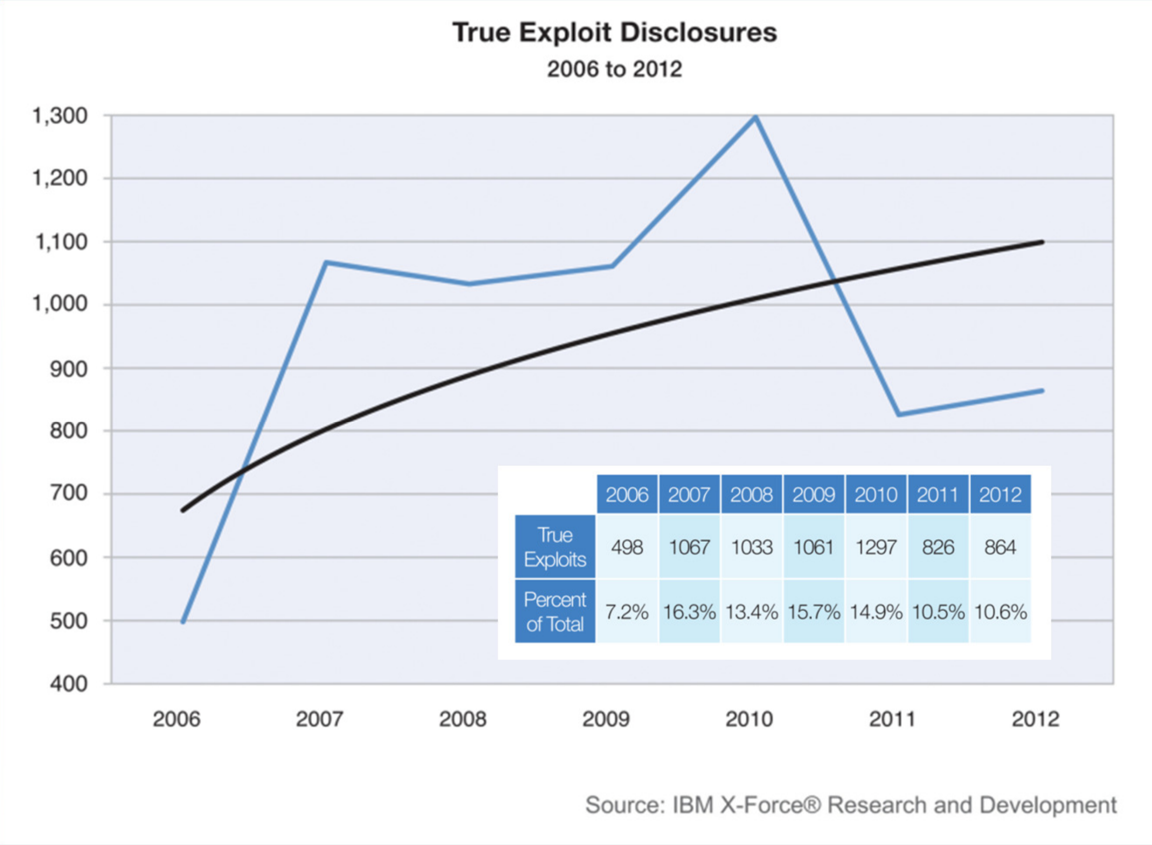


Source: IBM X-Force® Research and Development

# 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

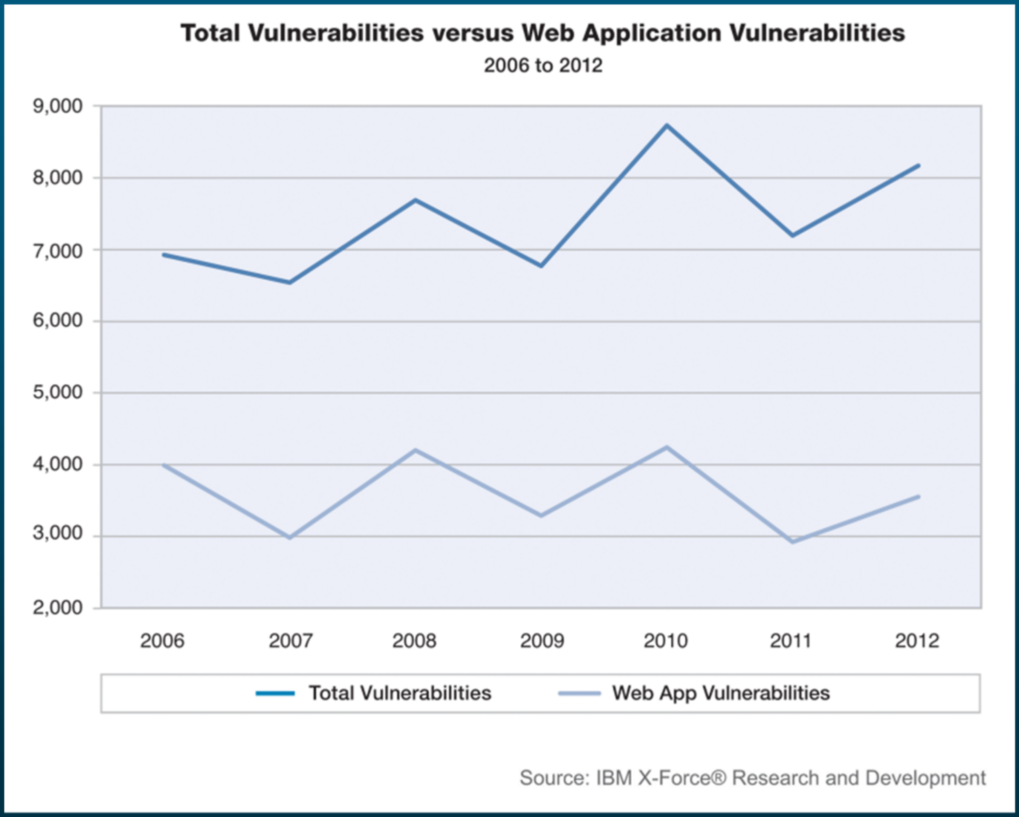
# Web application vulnerabilities surge upward

**14%**

increase in web application vulnerabilities

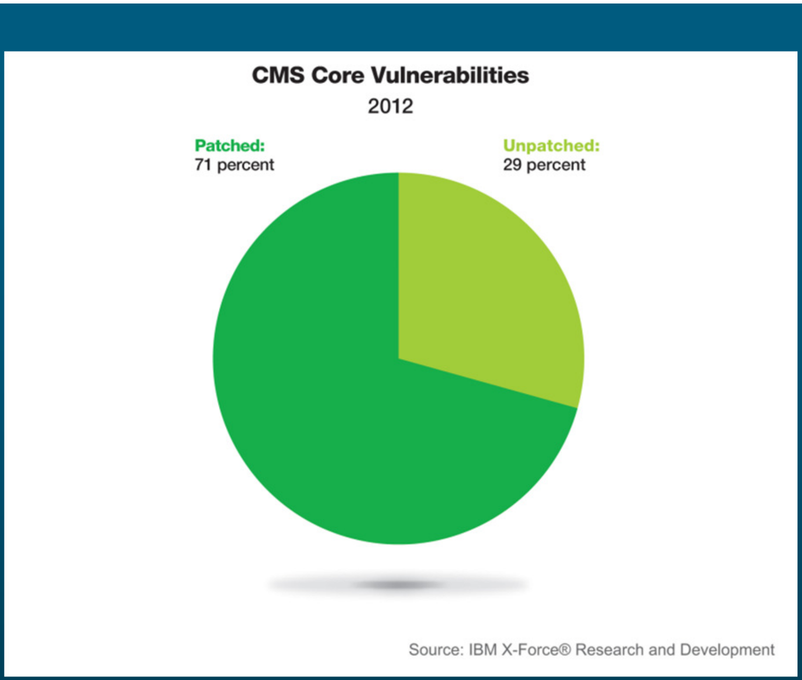
Cross-site scripting represented

**53%**

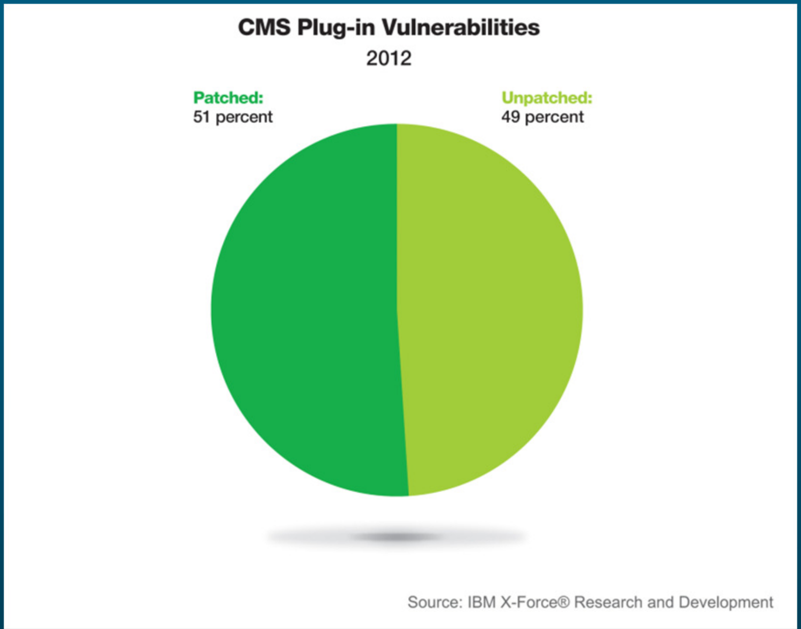


Source: IBM X-Force® Research and Development

# Content Management Systems plug-ins provide soft target



Source: IBM X-Force® Research and Development



Source: IBM X-Force® Research and Development

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

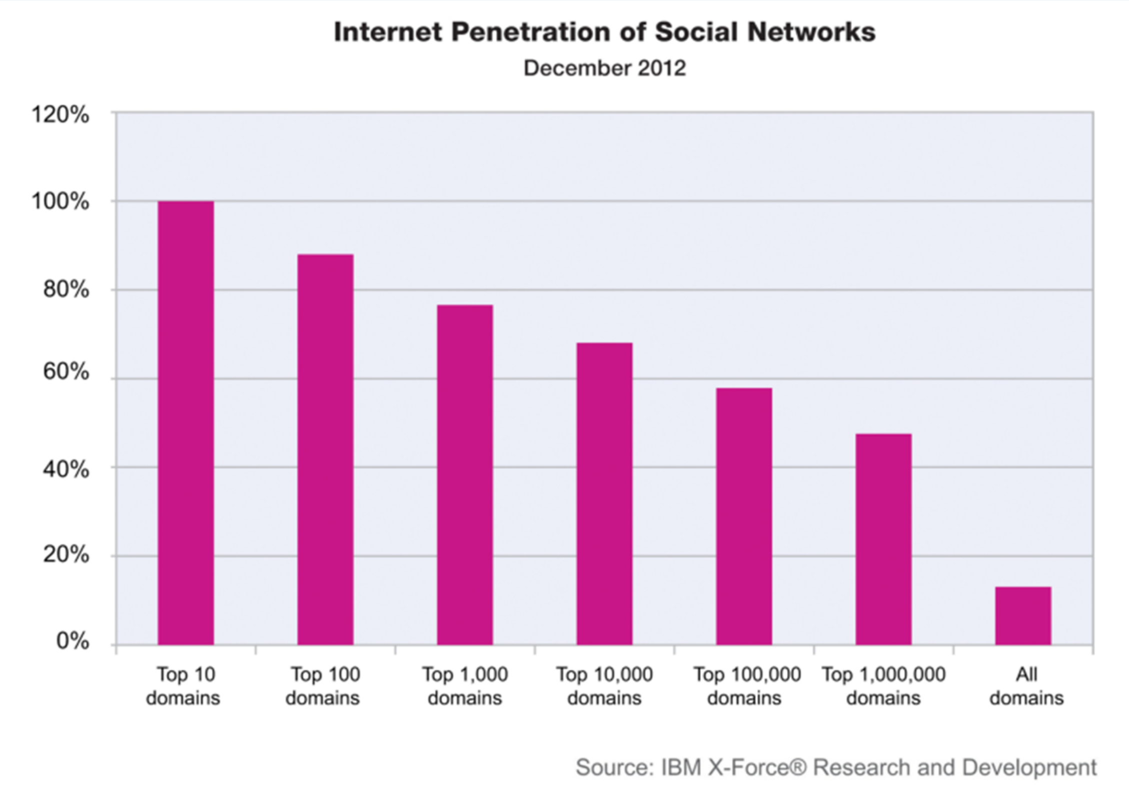
Compared to smaller organizations and individuals producing the add-ons and plug-ins

# Social Media and Intelligence Gathering

**50%**

of all websites connected to social media

Enhanced spear-phishing seemingly originating from trusted friends and co-workers



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

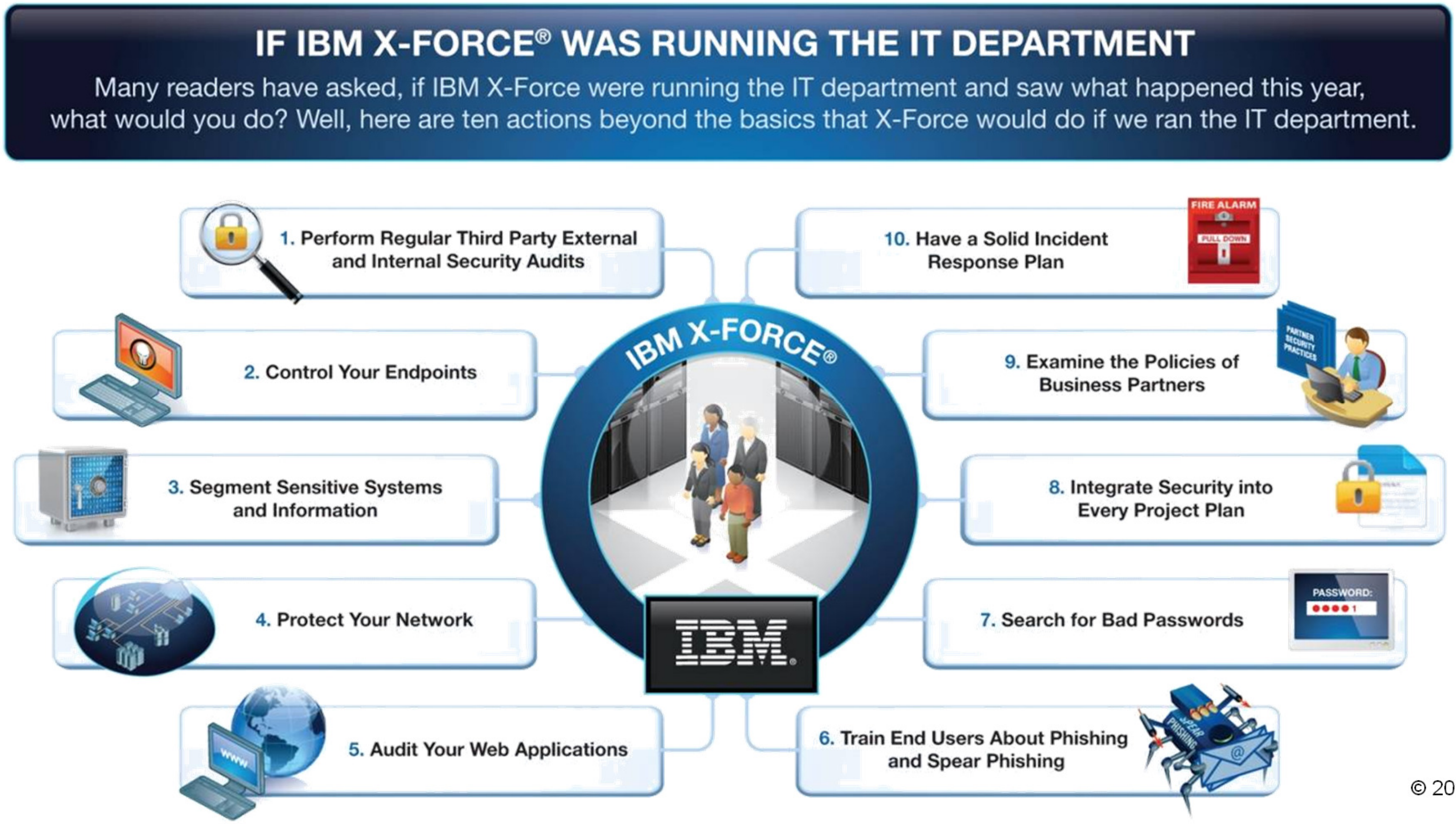
# Questions?

mochchakkeram
tesekkur
enkosi
najis
krap
leibh
Allahu
khob
chnorakaloutioun
gratias
nirringrazzjak
arigatô
cám
mananna
kiitos
deu
beacôp
dziękuję
ederim
edirem
didi
asko
maita
nanni
go
faafetai
kyay
grâces
grazzi
formal
mercé
mersi
thank
mèsi
grazie
pers
shukriya
bayarlalaa
singular
dankon
akpé
milesker
leat
mamnun
sah
faleminderit
bedankt
dank
graciñas
blagodaram
sagolun
grassie
agimus
dhanyavad
diakuiu
terima
kha
dhanyavaad
mauruuru
dakujem
sana
aabhar
much
sag
ago
hamnida
dhanyabaad
grandmercé
obrigado
dankie
danke
respectful
diolch
wel
po
pa
merci
akun
sobodi
gràcies
gracie
sheun
dhanyavadalu
díky
aabhari
rahmat
dankewol
ngiyabonga
dziakuju
blagodaria
olun
gracias
ni
je
tapadh
chai
kop
salamat
madloba
muchas
kasih
kié
ko
ačiū
misaotra
meharbani
ju
aguyjé
plural
mahalo
nižžik
murakoze
gratzias
familiar
aahe
hvala
fyri
khun
takk
obrigada
tänan
nandri
informal
saha
agat
raibh
asante
paldies
köszönöm
marahaba
efharisto
eskerrik
fiik
multumesc
Barak
maith
kam
chokrane
barkal
motashakkeram
dhanyavadagalu
lava
dieuf
děkuji
northern
djiere
danki
cóps
basque

ibm.com/security

# 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.

1. Perform Regular Third Party External and Internal Security Audits
2. Control Your Endpoints
3. Segment Sensitive Systems and Information
4. Protect Your Network
5. Audit Your Web Applications
6. Train End Users About Phishing and Spear Phishing
7. Search for Bad Passwords
8. Integrate Security into Every Project Plan
9. Examine the Policies of Business Partners
10. Have a Solid Incident Response Plan