Pulse

IBM SolutionsConnect 2013

2012 X-Force Annual Trend and Risk Report

Best practices X-Force would do if they were running your IT department

06/13/2013

IBM

Whois

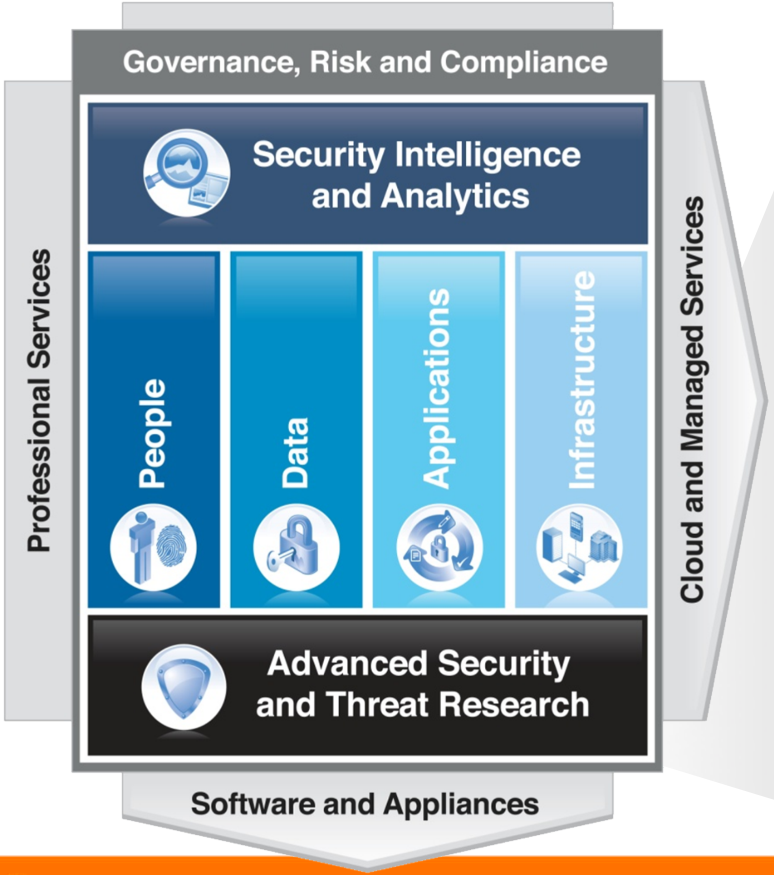
Michael Hamelin
X-Force Security Architect
CTO Office, IBM Security Systems
17 years experience in security

HackerJoe
Kenshoto founding member
Defcon CTF champion
Defcon CTF organizer, 4 years

in www.linkedin.com/in/hamelin/

@hackerjoe

X-Force is the foundation of the IBM Security Framework


Governance, Risk and Compliance
Security Intelligence and Analytics
People
Data
Applications
Infrastructure
Advanced Security and Threat Research
Professional Services
Cloud and 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

Collaborative IBM teams monitoring and analyzing

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

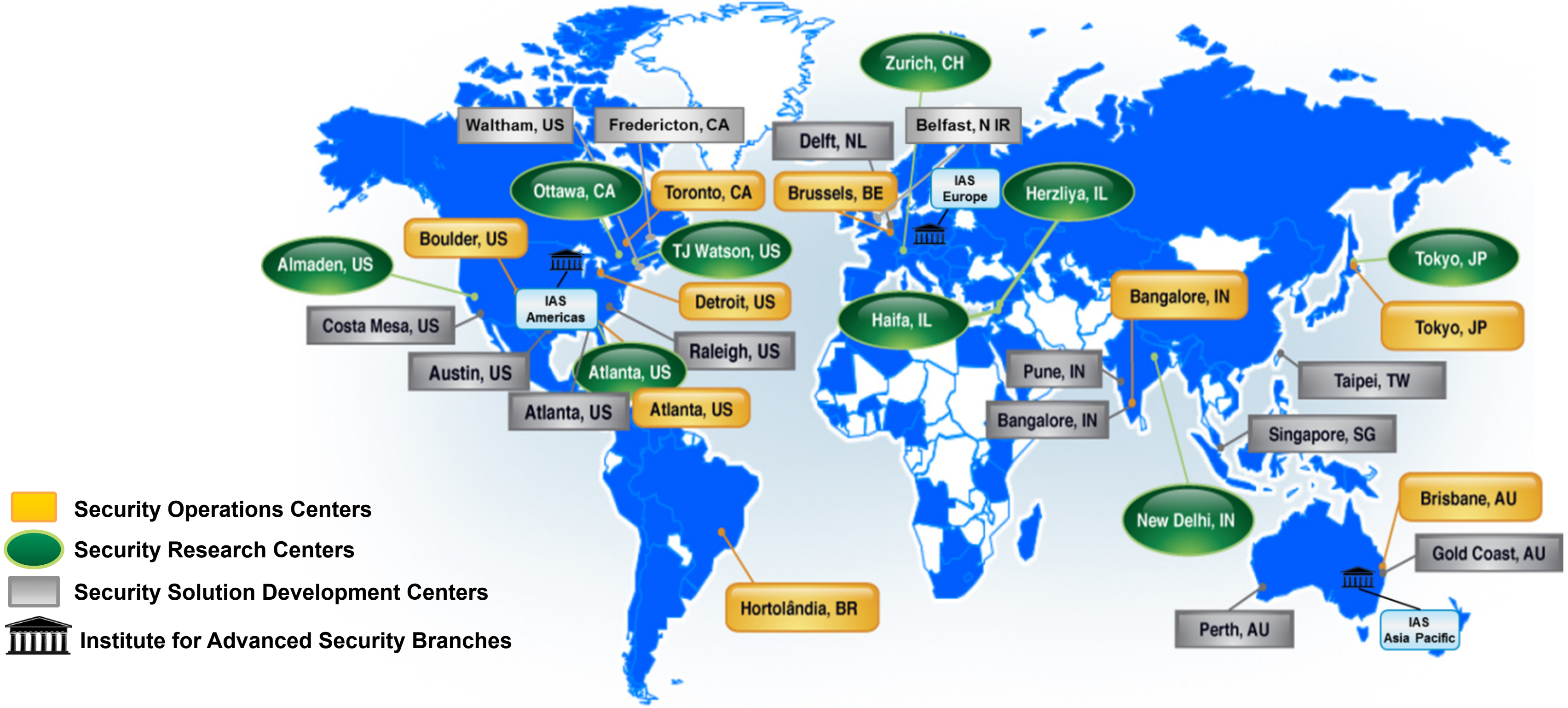
45M spam & phishing attacks

73K documented vulnerabilities

Billions of intrusion attempts daily

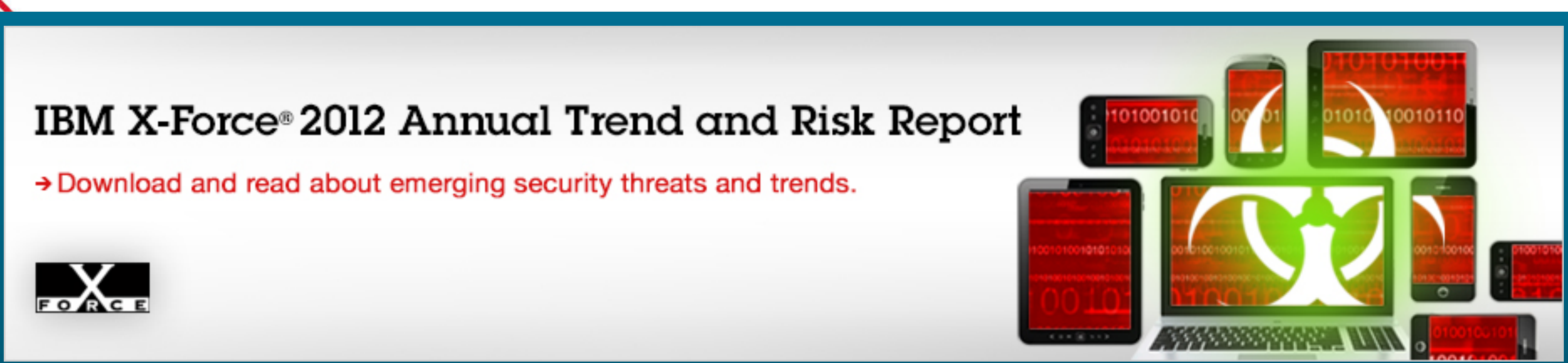
Millions of unique malware samples

The Global IBM Security Community



15,000 researchers, developers and subject matter experts working security initiatives worldwide

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

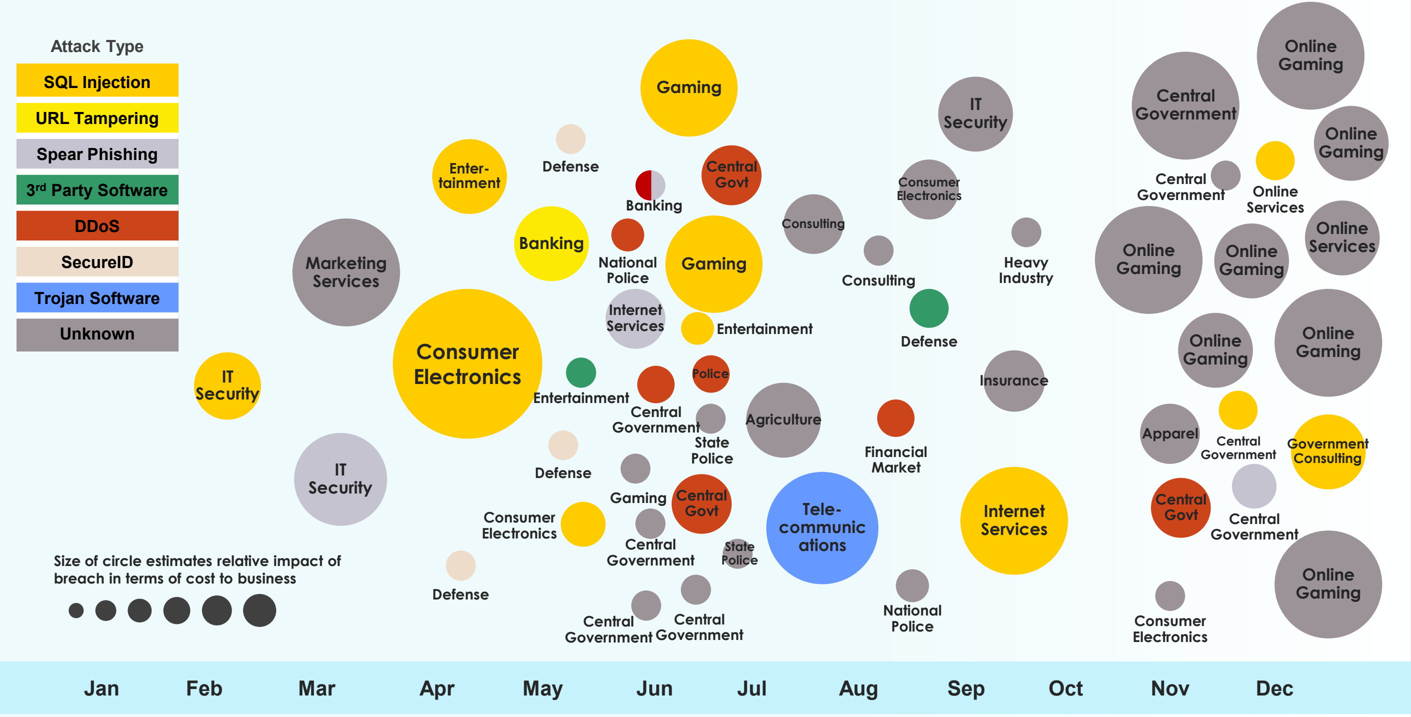
IBM X-Force 2012
Mid-year Trend and Risk Report

September 2012

2011: “The year of the targeted attack”

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

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



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

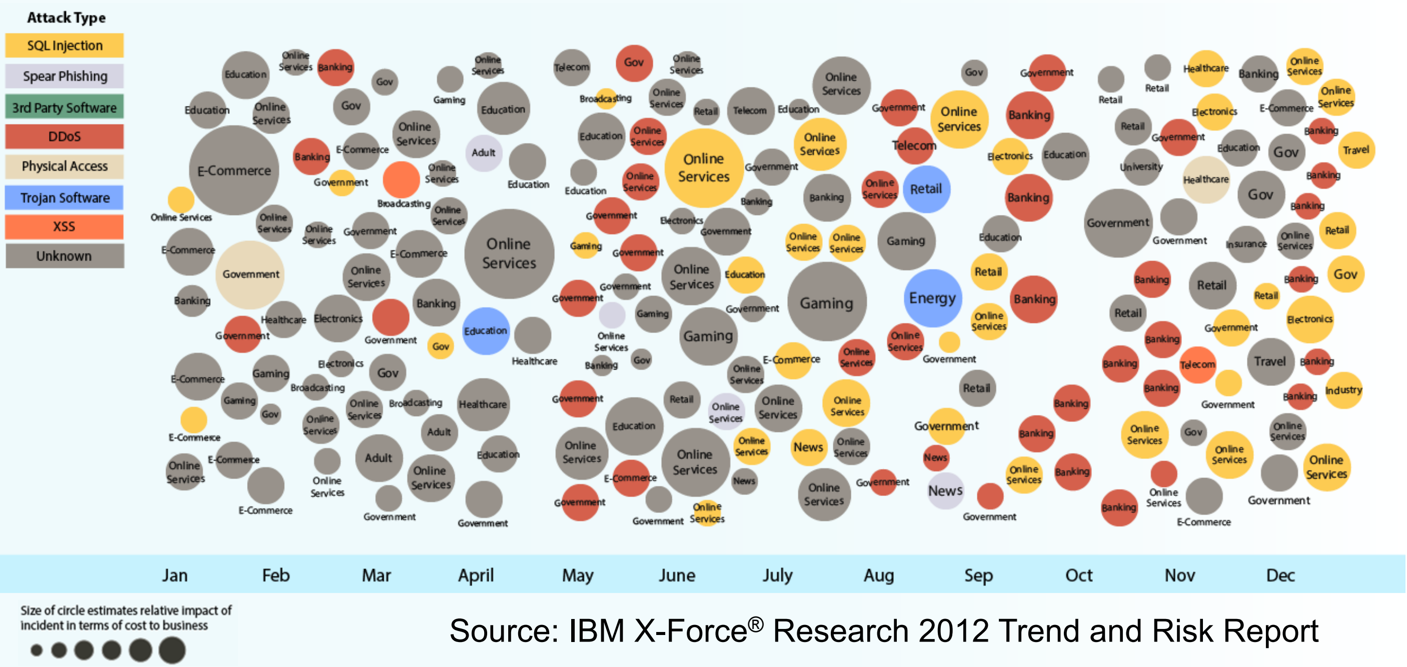
Pulse

IBM

2012: The explosion of breaches continues!

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

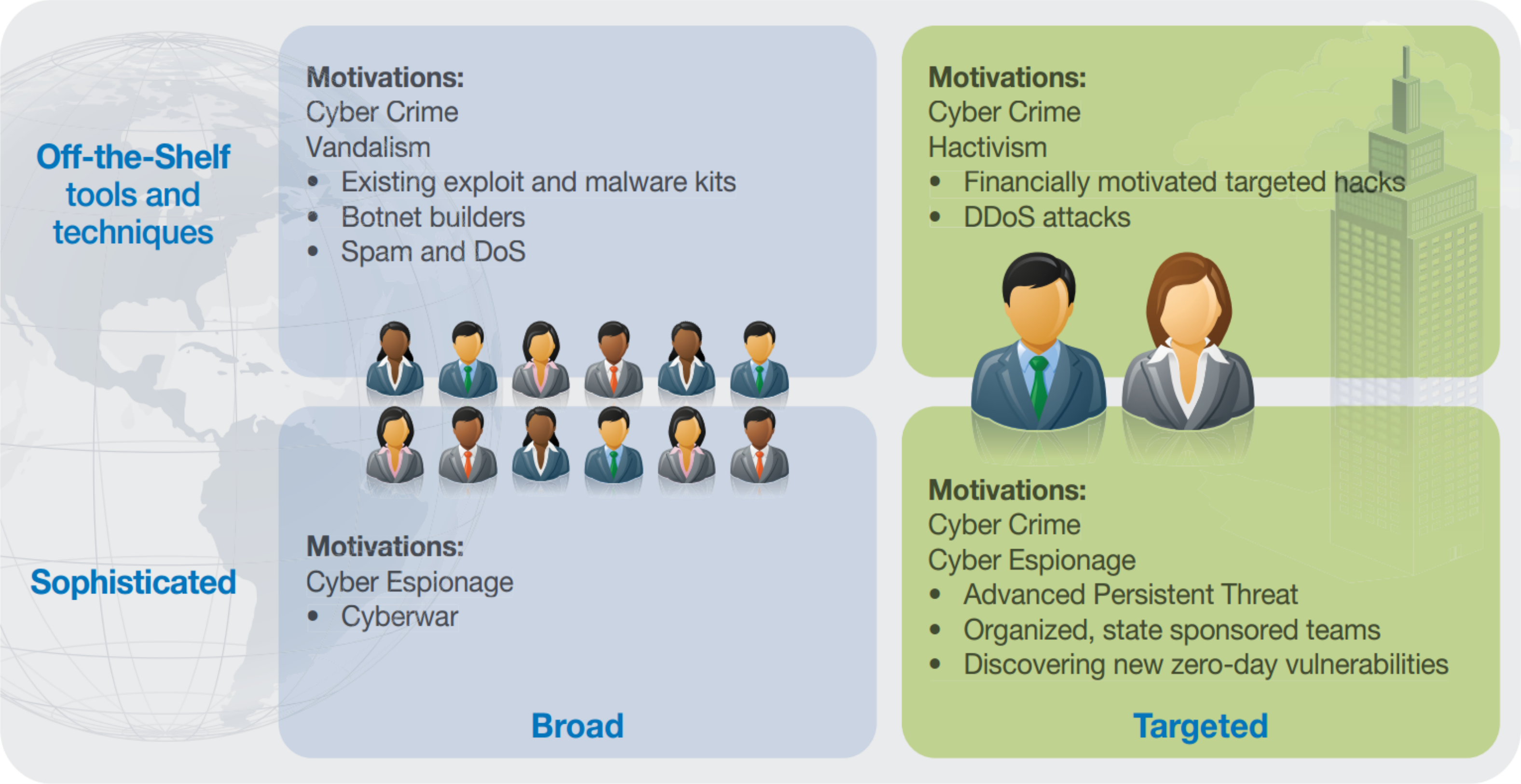
Conjecture of relative breach impact is based on publicly disclosed information regarding leaked records and financial losses



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

Pulse

Attacker motivations remain similar, although methods evolve



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

Sophisticated

Motivations:
Cyber Espionage

- Cyberwar

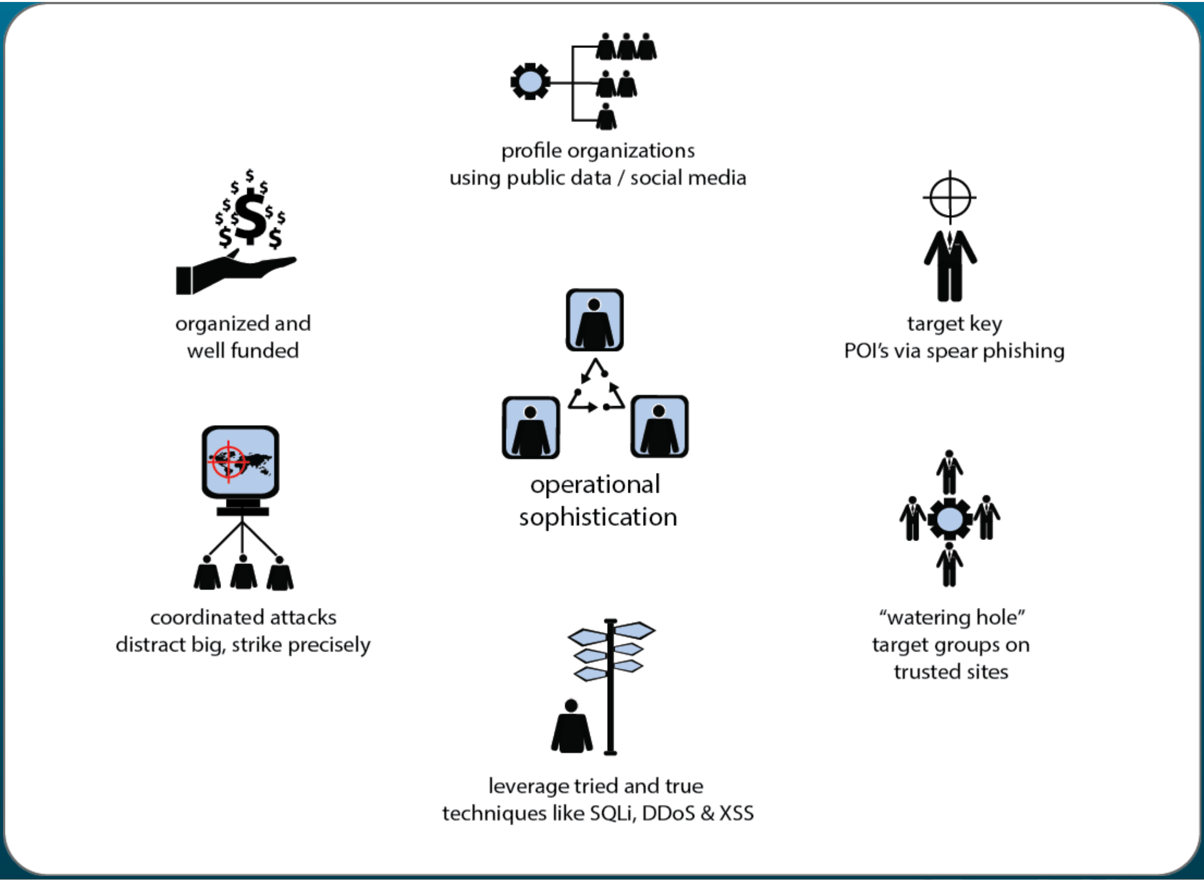
Motivations:
Cyber Crime
Cyber Espionage

- Advanced Persistent Threat
- Organized, state sponsored teams
- Discovering new zero-day vulnerabilities

Broad

Targeted

Operational sophistication, not always technical 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

Operational Sophistication – Current Events, Feb 2013

Hackers Steal $45 Million In 10 Hours

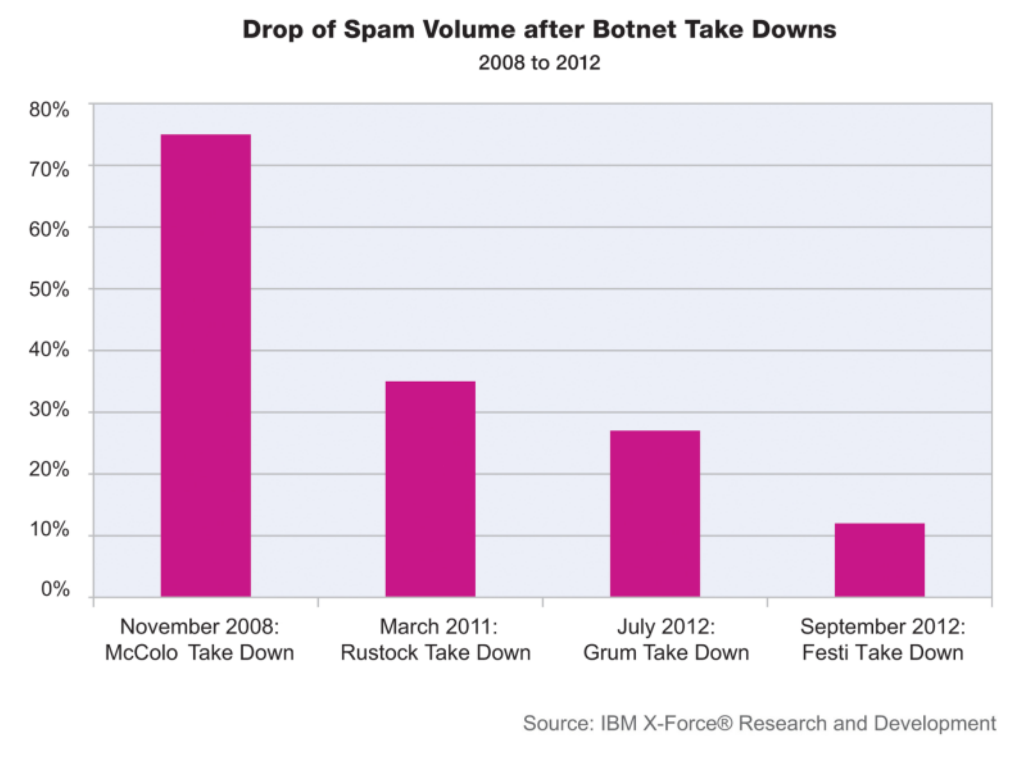
- Payment processor was compromised
- Targeted MC pre-paid cards
- Targeted Oman based Bank of Muscat
- 12 accounts were compromised
- Card limits removed, daily limits removed
- ‘Cashing Crews’ in 24 countries given ‘track data’
- 10 Hours time ran 36K ATM transactions

- Sophisticated structure of an organized crime enterprise

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

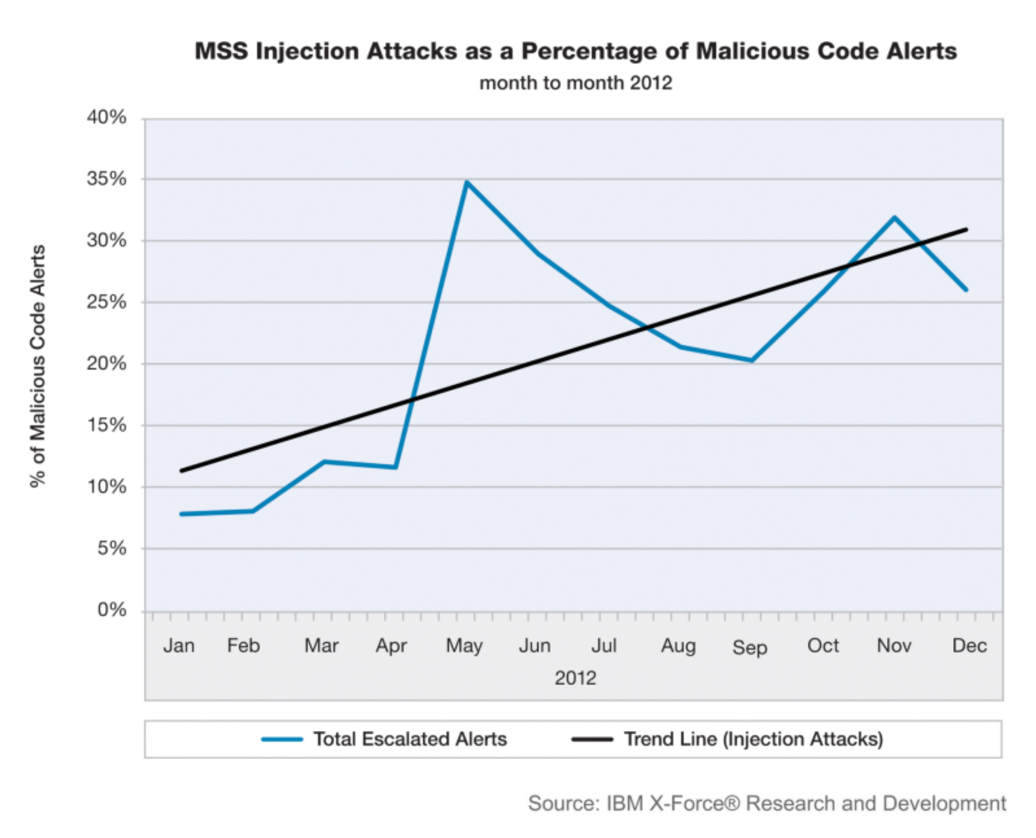


Source: IBM X-Force® Research and Development

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

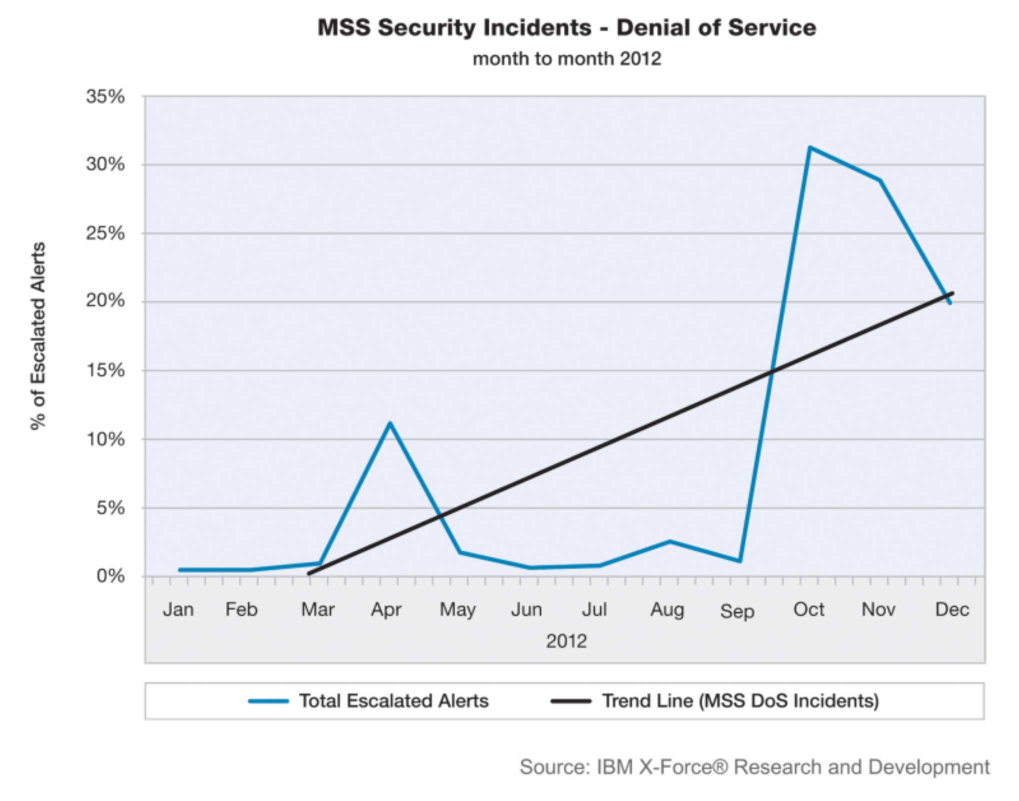


Source: IBM X-Force® Research and Development

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 using social networks

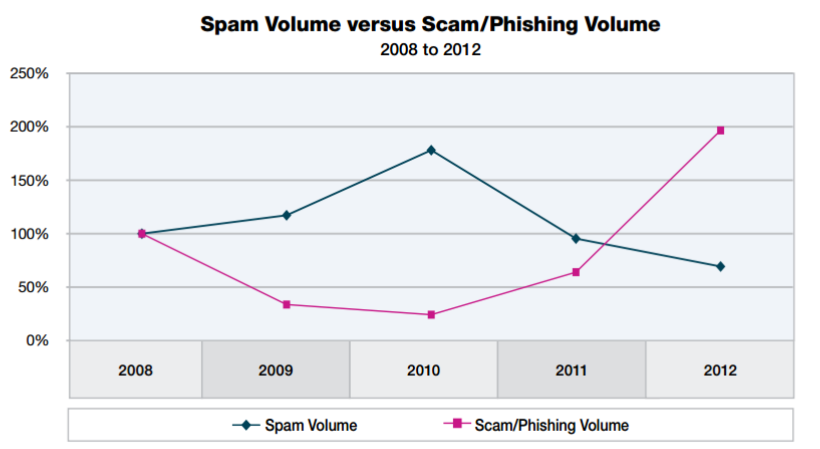


Figure 23: Spam Volume versus Scam/Phishing Volume – 2008 to 2012

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

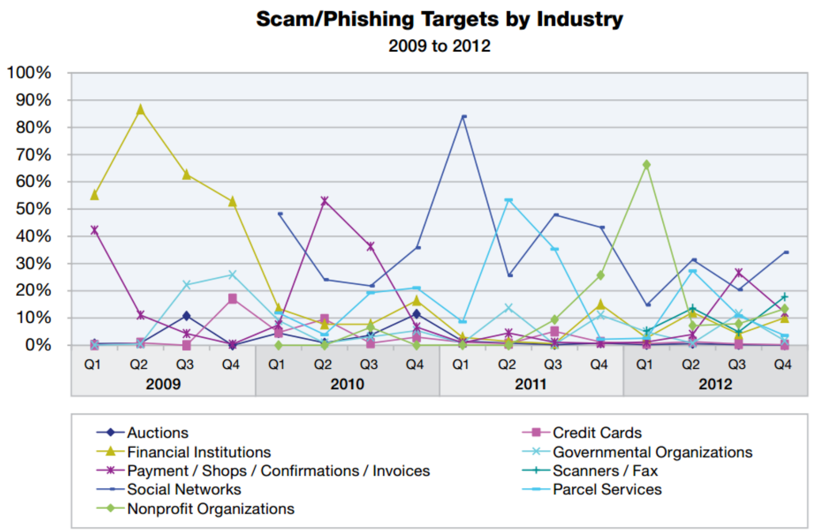


Figure 24: Scam/Phishing Targets by Industry – 2009 to 2012[60]

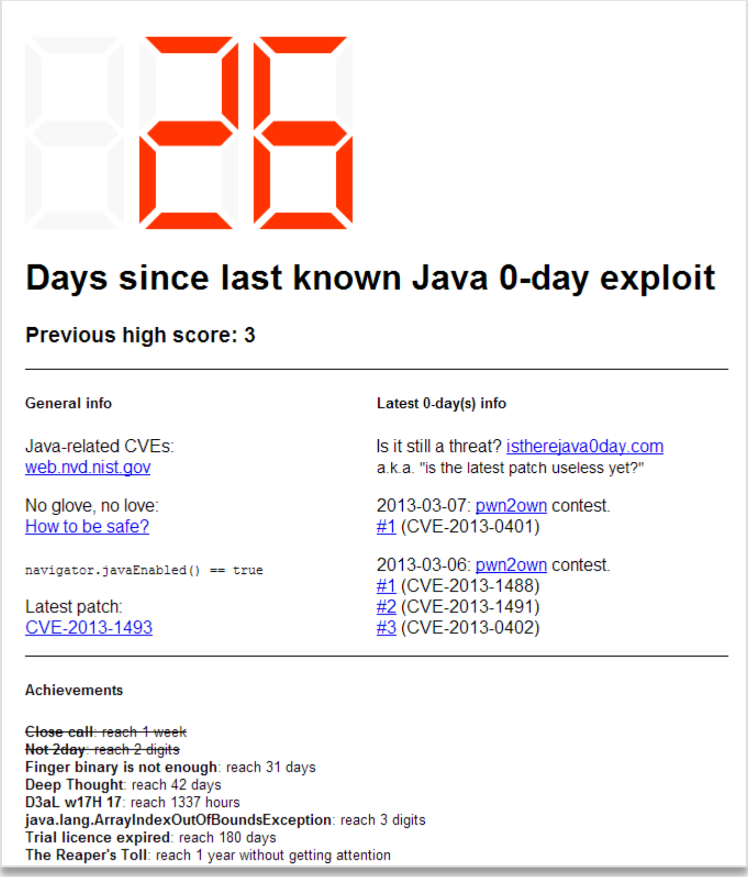
Scammers rotate the "carousel" of their targets – **focusing on social networks** in 2012

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

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)

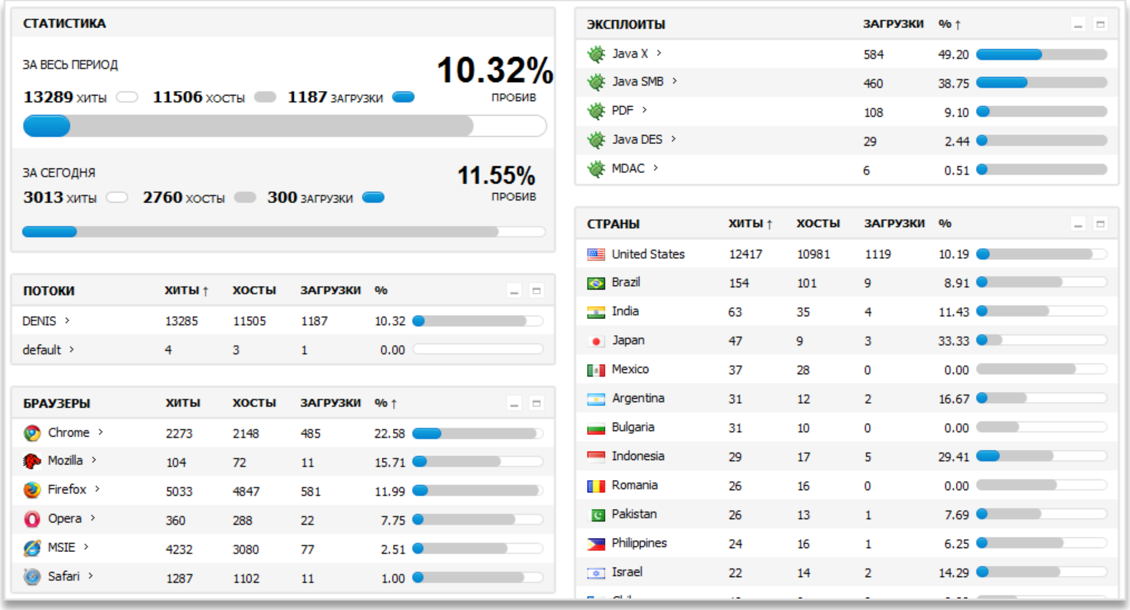
2013-03-06: pwn2own contest.
#1 (CVE-2013-1488)
#2 (CVE-2013-1491)
#3 (CVE-2013-0402)

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

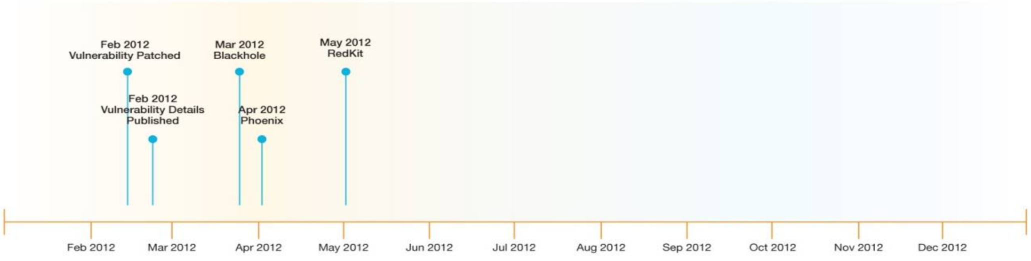
СТРАНЫ	ХИТЫ ↑	ХОСТЫ	ЗАГРУЗКИ	%
United States	12417	10981	1119	10.19
Brazil	154	101	9	8.91
India	63	35	4	11.43
Japan	47	9	3	33.33
Mexico	37	28	0	0.00
Argentina	31	12	2	16.67
Bulgaria	31	10	0	0.00
Indonesia	29	17	5	29.41
Romania	26	16	0	0.00
Pakistan	26	13	1	7.69
Philippines	24	16	1	6.25
Israel	22	14	2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

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

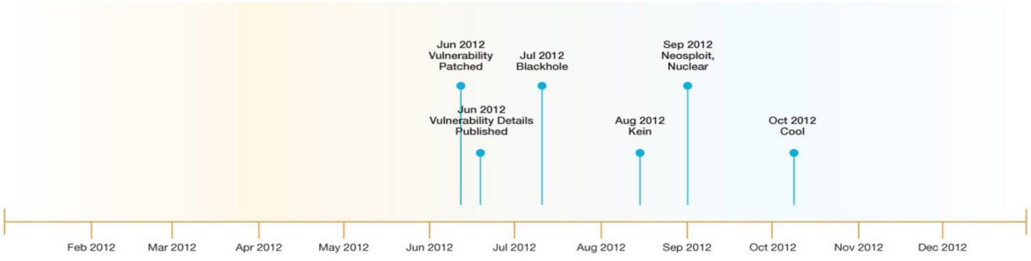
In 2012 we observed an upsurge in web browser exploit kit development and activity - the primary target of which are Java vulnerabilities

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

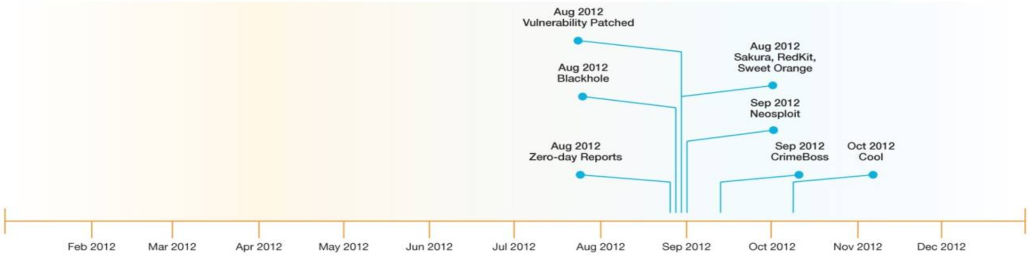
CVE-2012 -0507



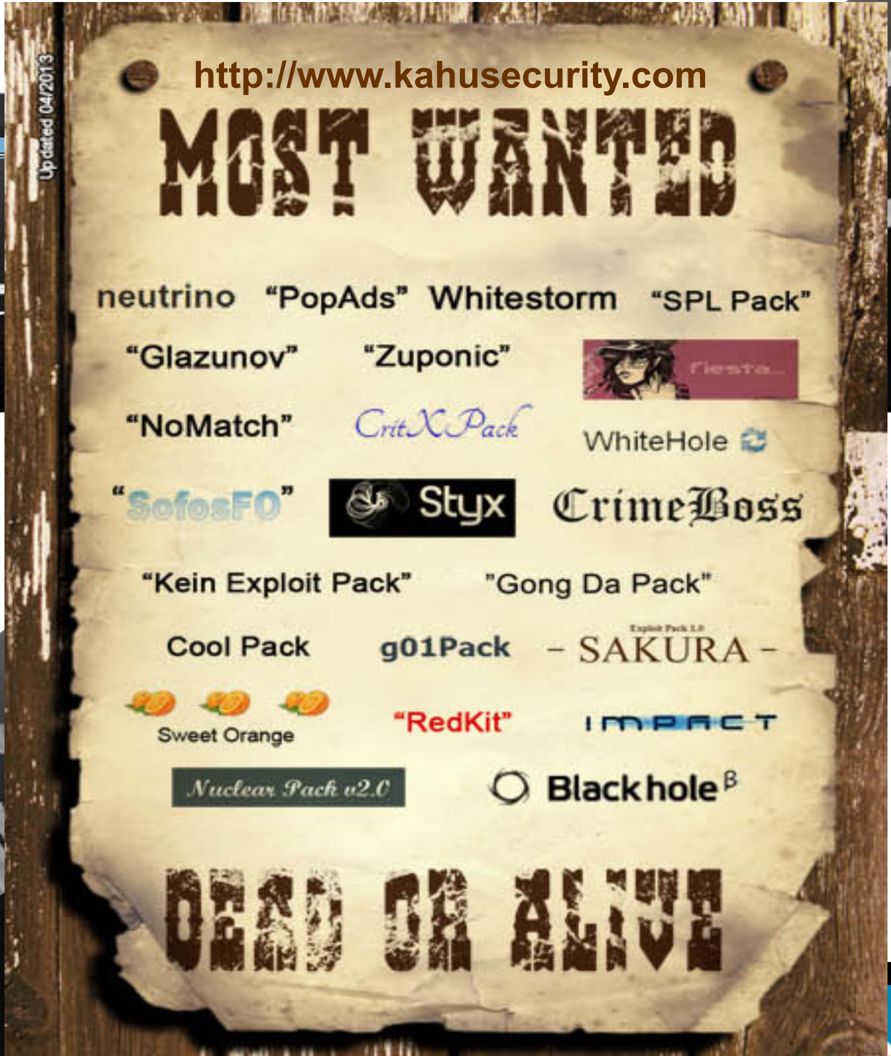
CVE-2012 -1723



CVE-2012 -4681



And more…



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”

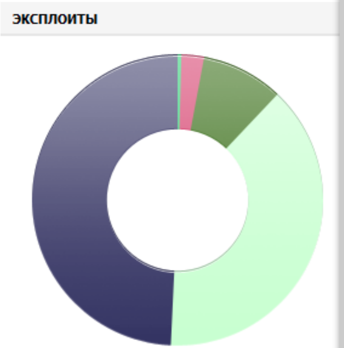
Cool Pack g01Pack Exploit Pack 1.0 – SAKURA –

Sweet Orange “RedKit” IMPACT

Nuclear Pack v2.0 Blackhole β

DEAD OR ALIVE

Blackhole Crimeware



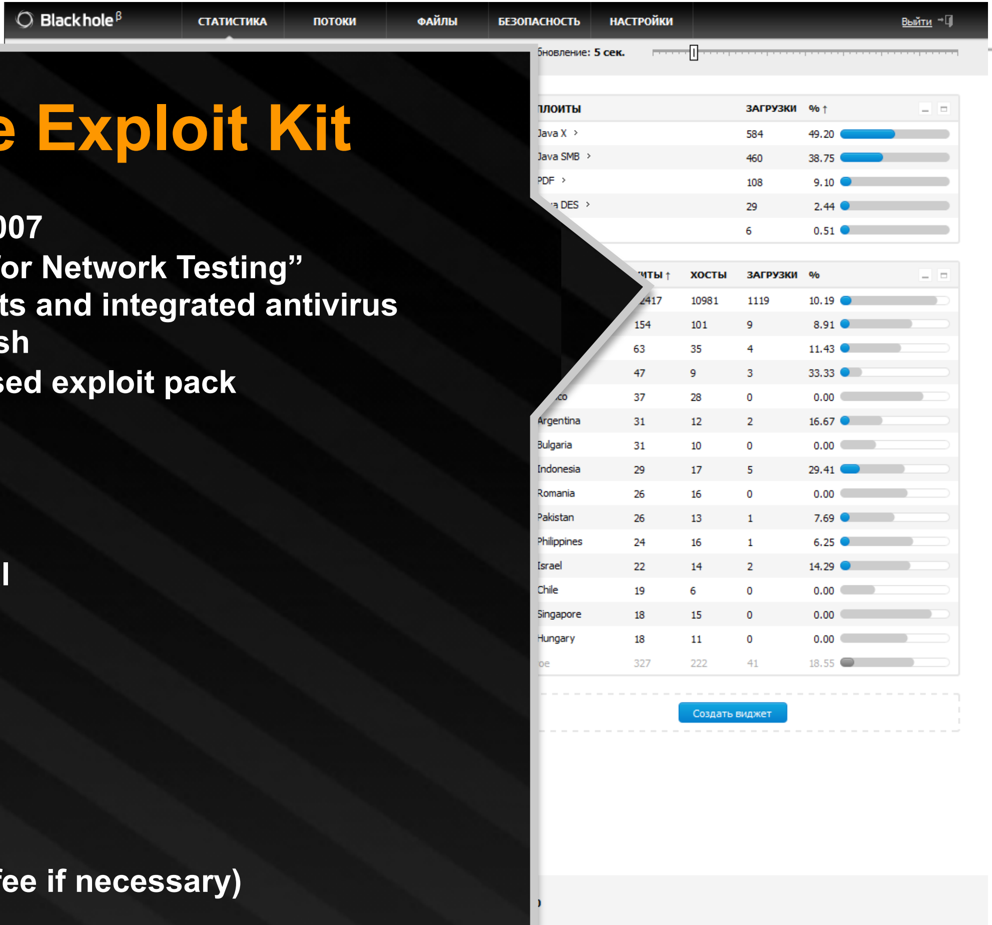
Blackhole Exploit Kit

–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)



бновление: **5 сек.**

ЛЛОИТЫ	ЗАГРУЗКИ	% ↑
Java X ›	584	49.20
Java SMB ›	460	38.75
PDF ›	108	9.10
a DES ›	29	2.44
	6	0.51

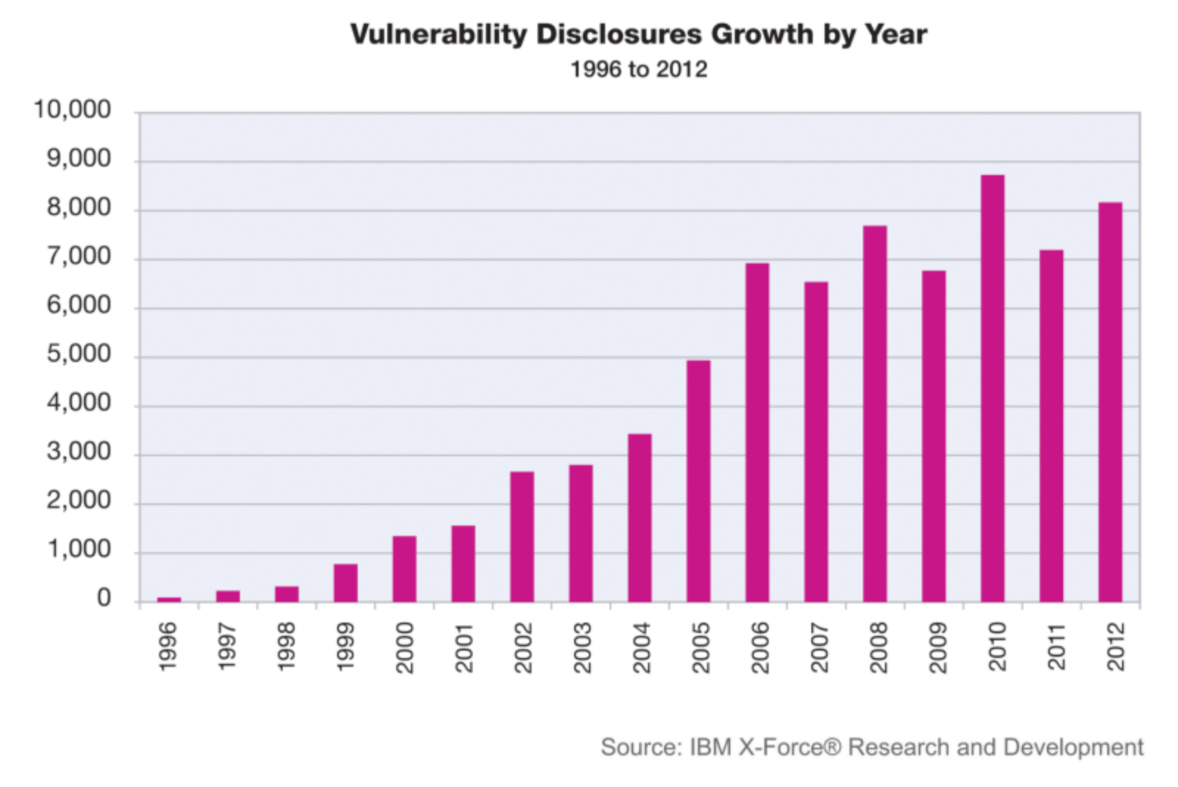
	ИТЫ ↑	ХОСТЫ	ЗАГРУЗКИ	%
	2417	10981	1119	10.19
	154	101	9	8.91
	63	35	4	11.43
	47	9	3	33.33
co	37	28	0	0.00
Argentina	31	12	2	16.67
Bulgaria	31	10	0	0.00
Indonesia	29	17	5	29.41
Romania	26	16	0	0.00
Pakistan	26	13	1	7.69
Philippines	24	16	1	6.25
Israel	22	14	2	14.29
Chile	19	6	0	0.00
Singapore	18	15	0	0.00
Hungary	18	11	0	0.00
oe	327	222	41	18.55

Software vulnerabilities - disclosures up in 2012

8,168

publicly disclosed vulnerabilities

An increase of over 14% from 2011

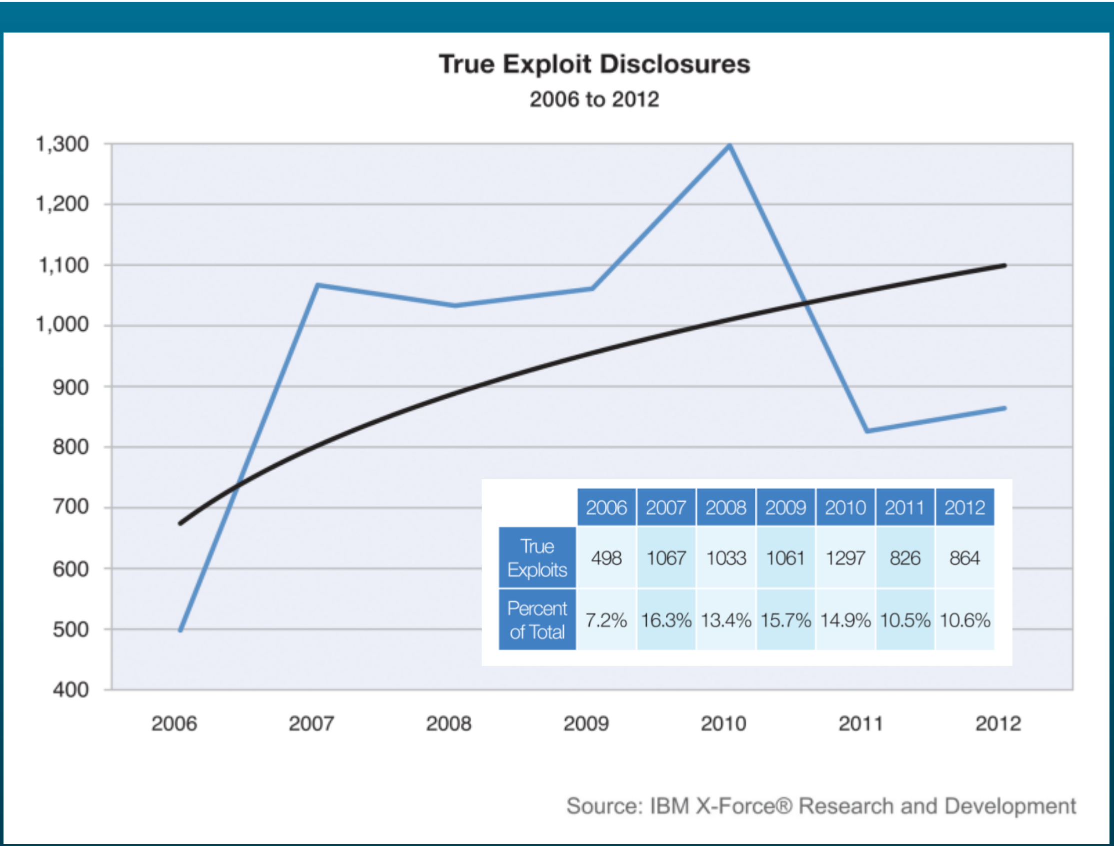


Source: IBM X-Force® Research and Development

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



	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

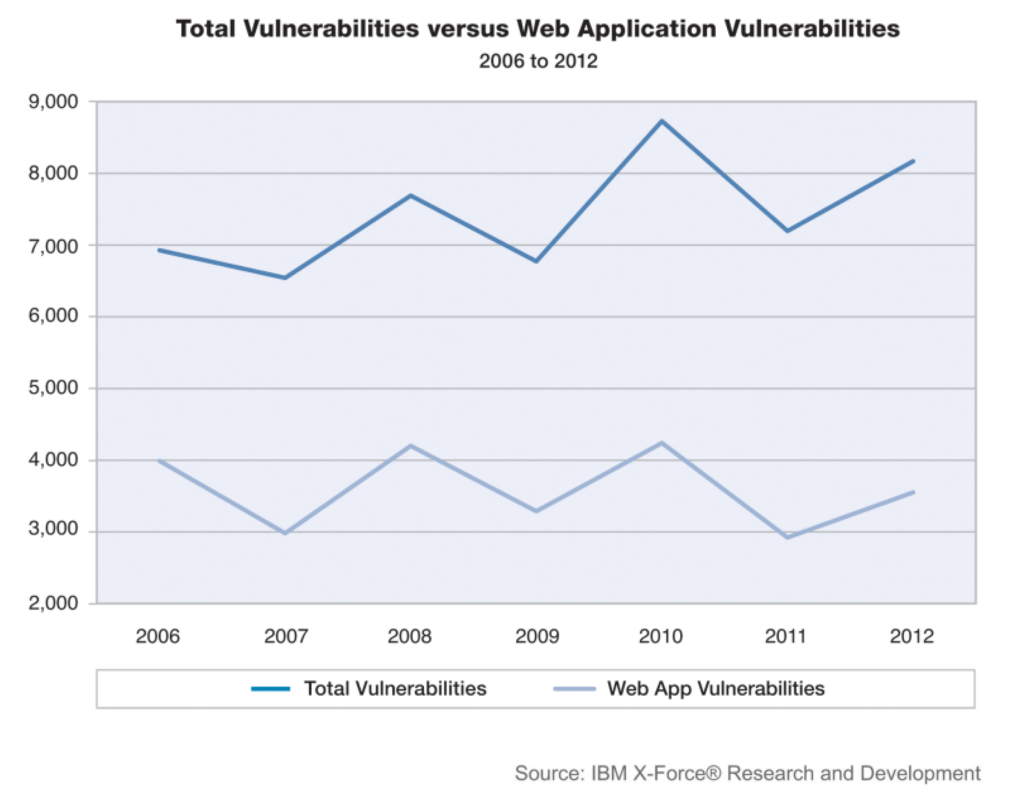
Web application vulnerabilities surge upward

14%

increase in
web application
vulnerabilities

Cross-site scripting
represented

53%



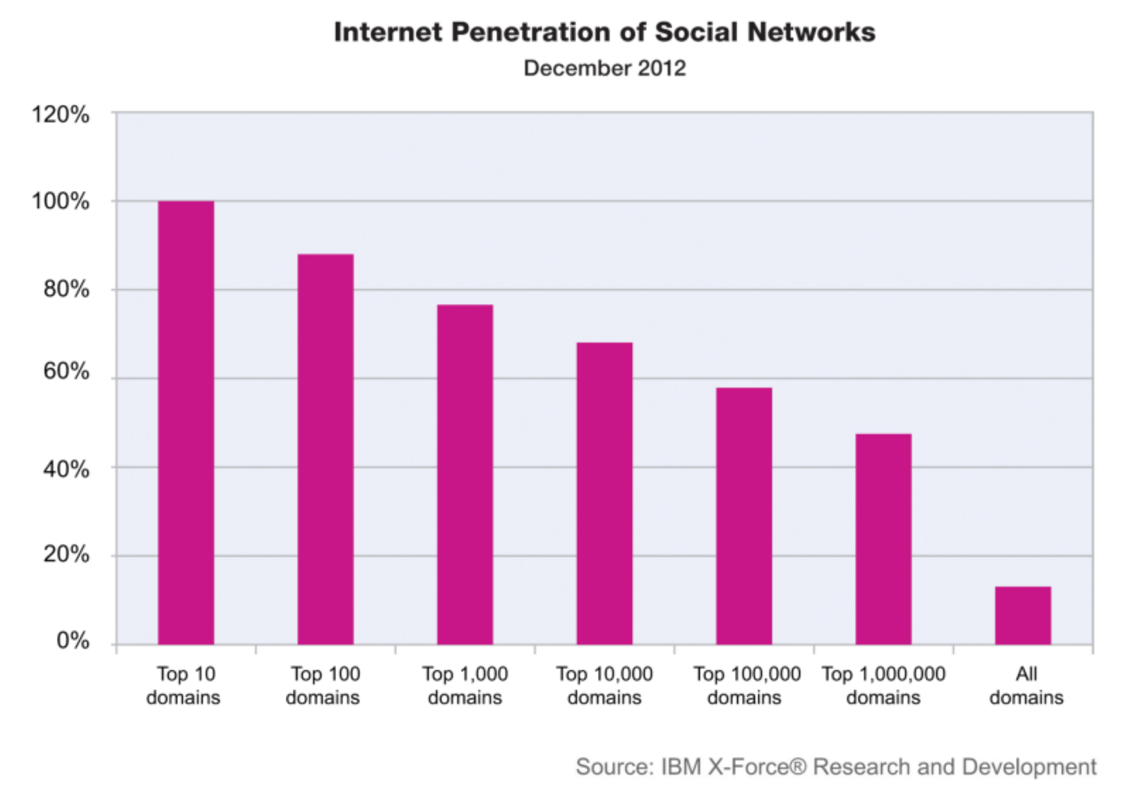
Source: IBM X-Force® Research and Development

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)

The 2012 IBM X-Force Trend And Risk Report highlights

Insecure infrastructure

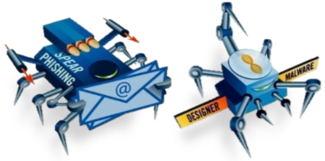
- Mutating threats and 0-day exploits
- Exploit kits: The Java Connection

Application threats

- Code injection attacks (SQLi, XSS)
- Vulnerable web plug-ins

Targeted attacks

- Social media and spear phishing
- Unknown threats and unusual activity

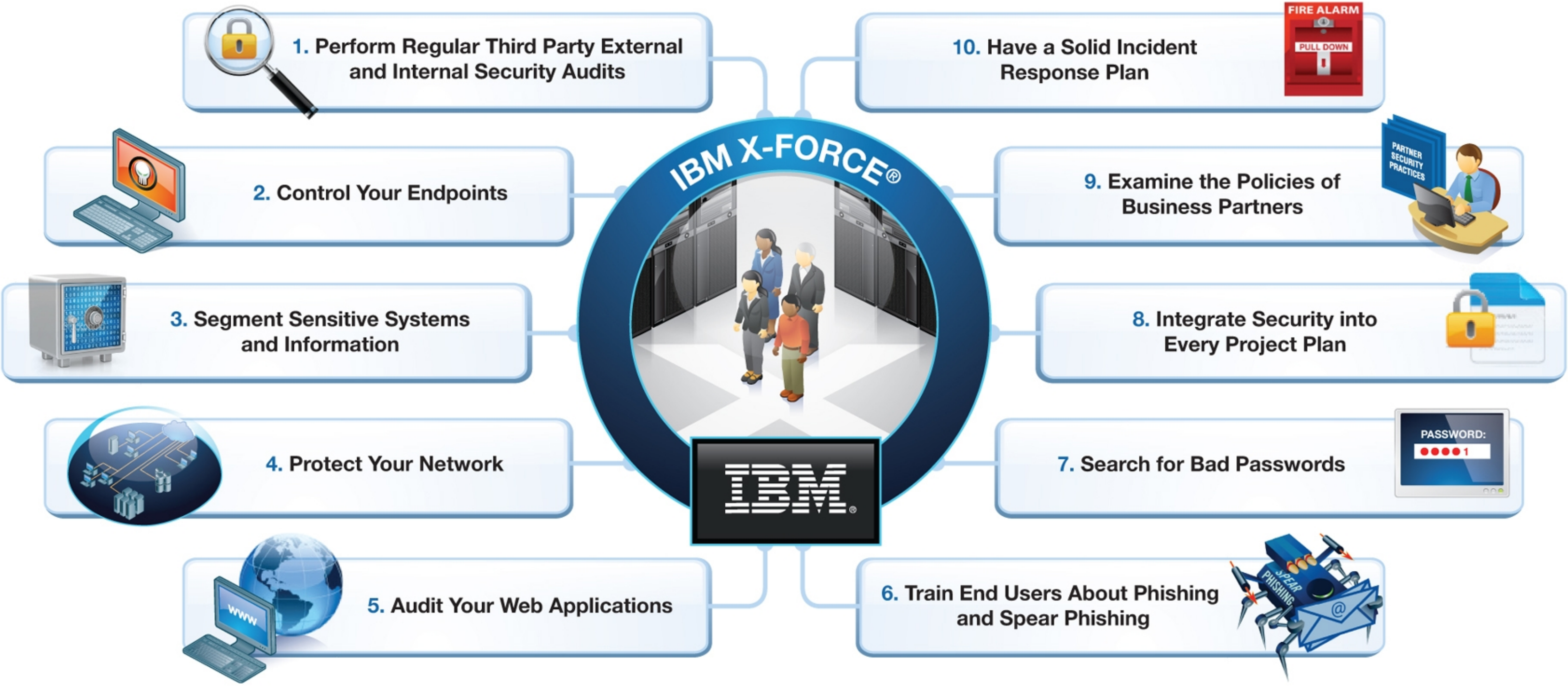


Mobile security

- BYOD and Mobile malware
- Mobile application vulnerabilities

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

Addressing the latest X-Force Trends…

Insecure Infrastructure

Mutating threats & 0-day exploits

- Attacks often leverage software vulnerabilities on operating systems, browsers, application software, etc.
- In 2012, we saw 8,168 publicly disclosed vulnerabilities - an increase of over 14% over 2011
- In some cases, vulnerabilities aren’t disclosed until after exploit code has been used successfully in the wild

IBM X-Force Recommendations

- ✓ Protect your network and the assets on your network such as servers, desktops and network infrastructure
- ✓ Focus on heuristic-based threat identification rather than simple signature detection
- ✓ Protect end users against exploits hidden in seemingly innocuous documents
- ✓ Limit employee access to malicious websites and other high risk areas
- ✓ Automate browser and endpoint software patching
- ✓ Perform regular user training on email phishing risks

Insecure Infrastructure

Exploit kits: The Java Connection

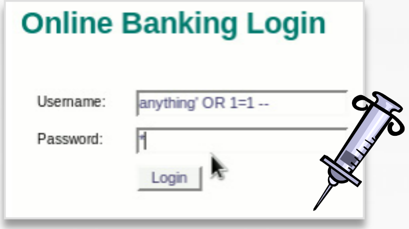
- Exploit kits are used to install malware on a large number of systems
- They continue to be popular because kits provide attackers a turnkey solution
- Java has become a key target for exploit kits because it' s cross-platform, ubiquitous and produces reliable exploits

IBM X-Force Recommendations

- ✓ Ensure your browser and browser plug-ins are up-to-date
- ✓ Uninstall browser plugins if not needed, to reduce attack surface
- ✓ Enable Click-to-Play to prevent drive-by or "silent" exploitation of browser plug-ins - by requiring an additional user interaction before a plugin can be activated
- ✓ Set security level of unsigned applications to High or Very High
- ✓ Deploy network-based protection that can inspect Java code for malicious activity
- ✓ Turn on IPS signatures designed to identify and block toolkit activity

Application Threats

Code injection attacks & vulnerable web plug-ins



Online Banking Login

Username: anything' OR 1=1 --

Password: '

- SQL injection continues to be one of the most popular points of entry for extracting data from a website
- Web app vulnerabilities also allow attackers to inject malicious scripts and files onto legitimate websites
- The high rate of vulnerable web applications and their plugins allow attackers to use automated scripts to scan the web for targets

IBM X-Force Recommendations

- ✓ Analyze applications before deployment, to identify security vulnerabilities
- ✓ Scan applications as early as possible in the development cycle, to reduce costs
- ✓ Remediate critical vulnerabilities, and validate by re-scanning
- ✓ Integrate scanning results with intrusion prevention, to block attacks before apps are updated
- ✓ Continuously monitor database activities to detect suspicious activity and respond in real-time
- ✓ Detect database vulnerabilities to prevent threats

Targeted Attacks

Social media & spear phishing

- One third of all web access is done on websites which allow users to submit content such as web applications and social media
- Individual employees who share personal details in their social profiles can be targeted for attacks
- Broadly targeted email scams and more personalized spear-phishing efforts continue to fool users

IBM X-Force Recommendations

- ✓ Conduct assessment of employee usage of social media and build policies to govern behavior
- ✓ Create awareness of how social media could affect an organization’s security
- ✓ Block access to potentially harmful or suspicious websites
- ✓ Limit actions against risky web applications – file uploads, data submissions, non-encrypted sites
- ✓ Utilize network security technology to scan for malicious links and files in email and web activity

Targeted Attacks

Unknown threats & unusual activity

- Advanced attacks don’t come with bells or blinking lights; they blend into your environment as much as possible
- Sophisticated adversaries sometimes use custom malware to only infect the target organization
- Custom malware may communicate over covert channels, using tunneled or proprietary protocols

IBM X-Force Recommendations

- ✓ Monitor user activity, especially for privileged users
- ✓ Monitor access to sensitive data - customer data, financial data, intellectual property, etc.
- ✓ Monitor outbound traffic to prevent data exfiltration
- ✓ Monitor geographic access and traffic
- ✓ Utilize threat intelligence in combination with anomaly detection
- ✓ Analyze network flows for greater insight into user & application behavior

Mobile Security

BYOD & mobile application vulnerabilities

- The security of enterprise information and data on employee-owned devices continues to be a challenge
- Popular mobile applications require extensive permissions – making users less vigilant towards risky behavior
- Mobile application vulnerabilities have become a primary attack vector for enterprises over the past few years

IBM X-Force Recommendations

- ✓ Protect against malware threats, exploits in vulnerable mobile apps and "jailbroken" mobile devices
- ✓ Remotely lock, locate and perform selective wipes when devices are lost, stolen or decommissioned
- ✓ Identify non-compliant mobile devices and take corrective actions
- ✓ Monitor unauthorized user access to the device, data, and back end corporate applications
- ✓ Identify vulnerabilities in Android and iOS applications by utilizing mobile source code scanning