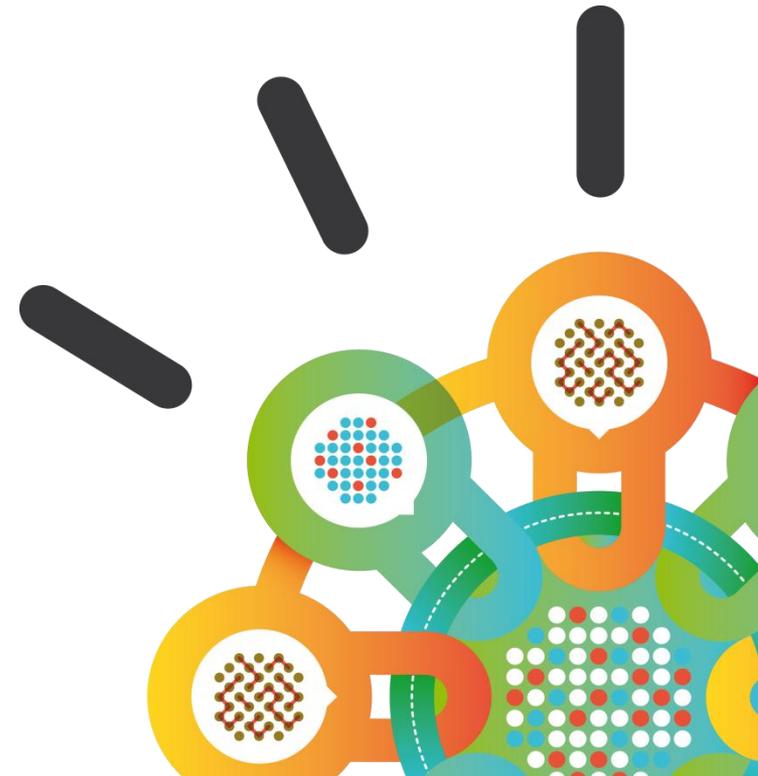


Security Intelligence.
Think Integrated.

IBM X-Force® 2012

Cyber Security Threat Landscape Highlights

Robert Freeman
Manager X-Force Research





IBM X-Force 2011 Trend and Risk Report Highlights

The mission of the IBM X-Force® research and development team is to:

- Research and evaluate threat and protection issues
- Deliver security protection for today's security problems
- Develop new technology for tomorrow's security challenges
- Educate the media and user communities



X-Force Research

- 14B** analyzed Web pages & images
- 40M** spam & phishing attacks
- 54K** documented vulnerabilities
- 13 billion** security events monitored daily

Provides Specific Analysis of:

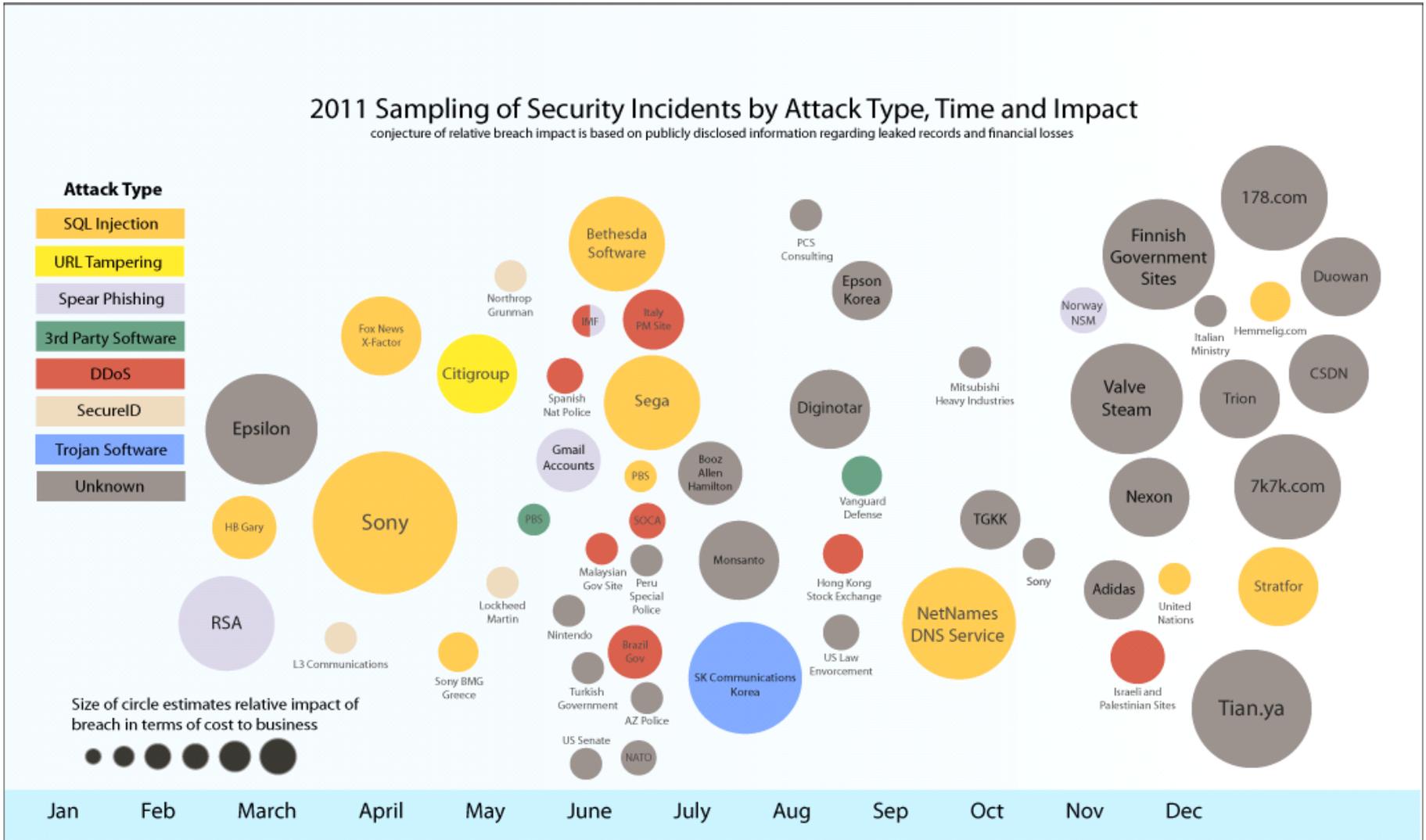
- Vulnerabilities & exploits
- Malicious/Unwanted websites
- Spam and phishing
- Malware
- Other emerging trends

In 2011:

- Reported 18 vulnerabilities
- Presented at 5 top conferences
- Authored 3 new heuristic engines

2011: Year of the Security Breach

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



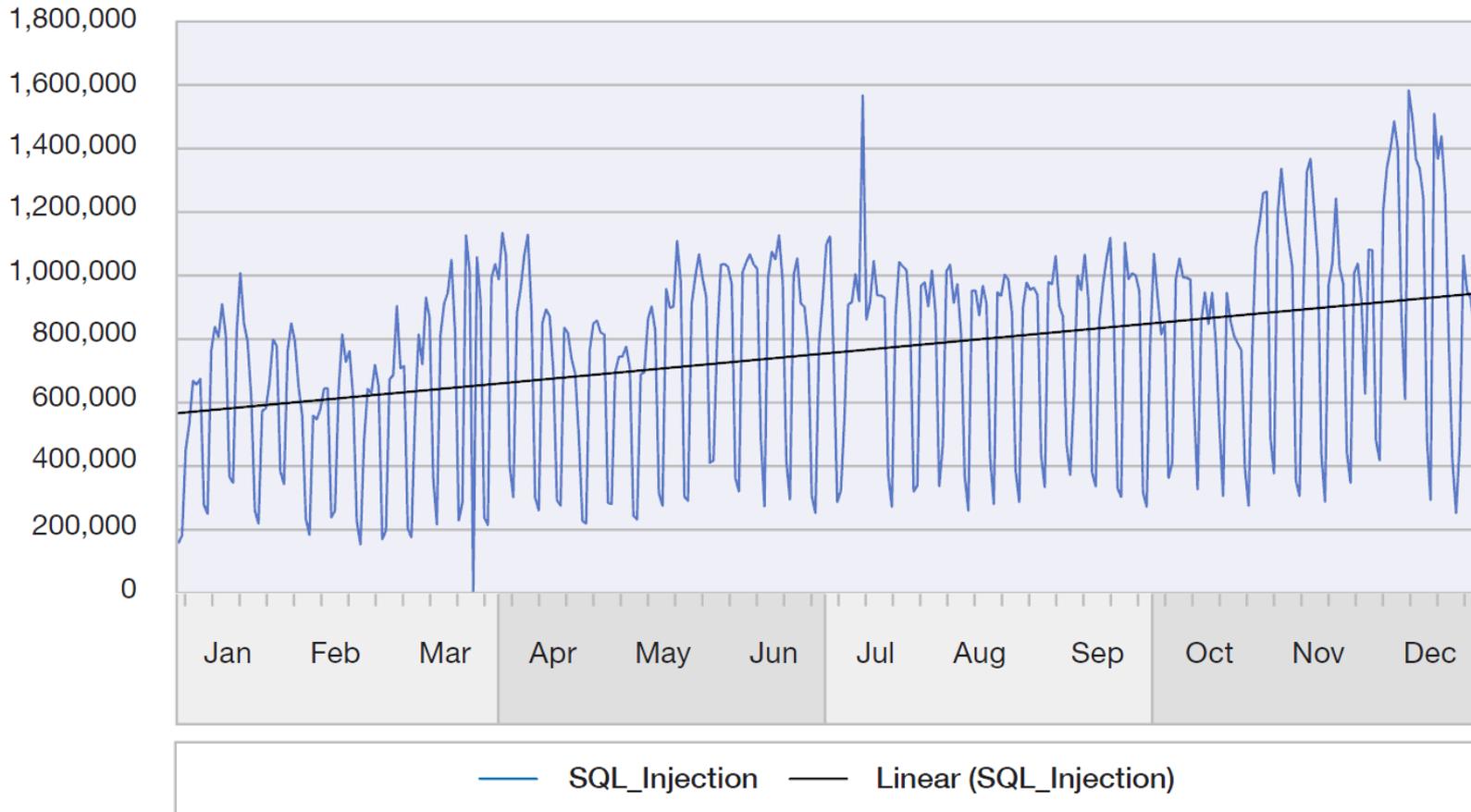


Highlights from the 2011 Trend Report

- **New Attack Activity**
 - Continued Trend with SQL Injection attacks
 - Rise in Shell Command Injection attacks
 - Spikes in SSH Brute Forcing
- Progress in Internet Security
- Interesting Developments

SQL Injection Attacks against Web Servers

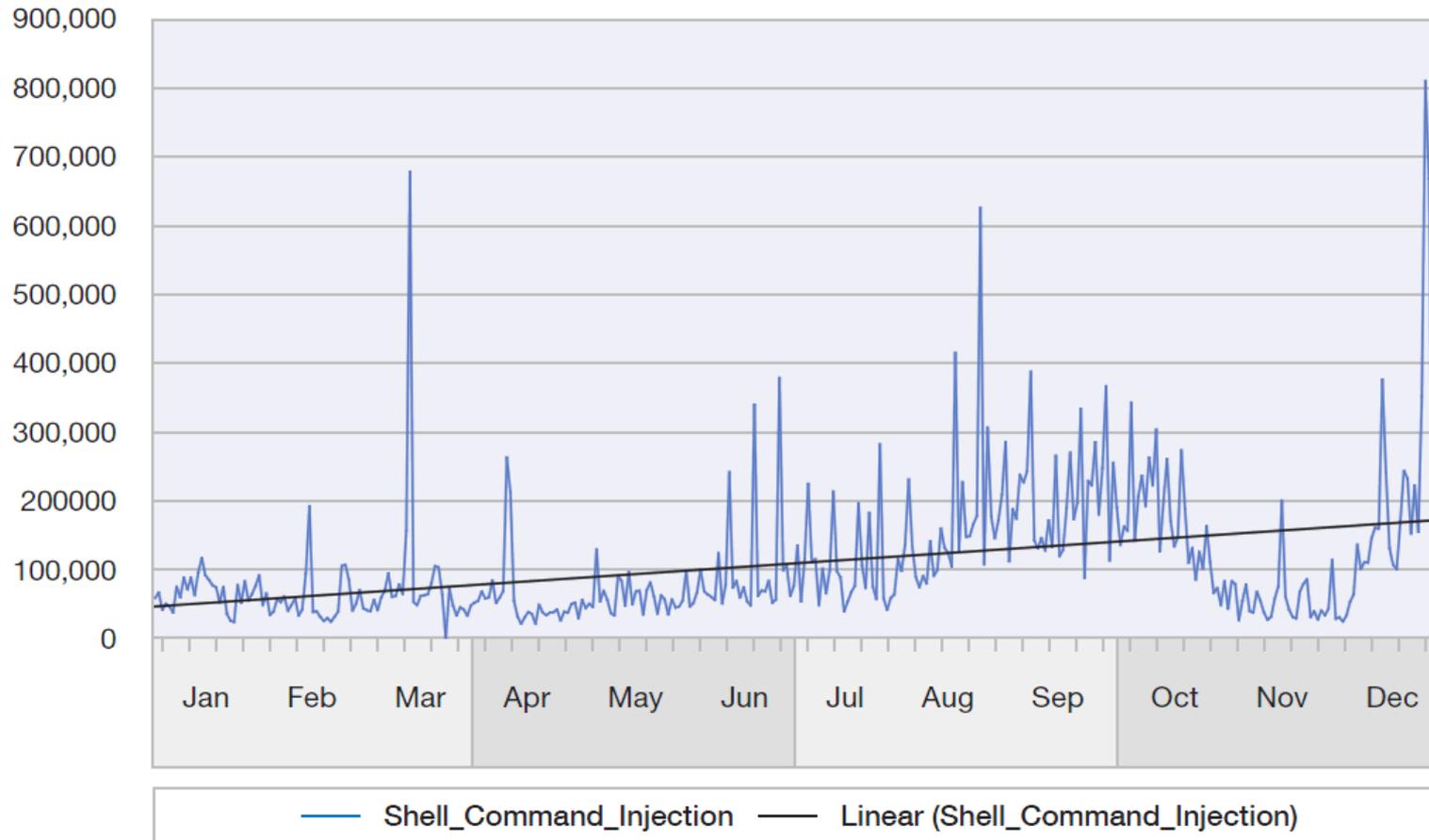
Top MSS High Volume Signatures and Trend Line – SQL_Injection
2011



Shell Command Injection Attacks

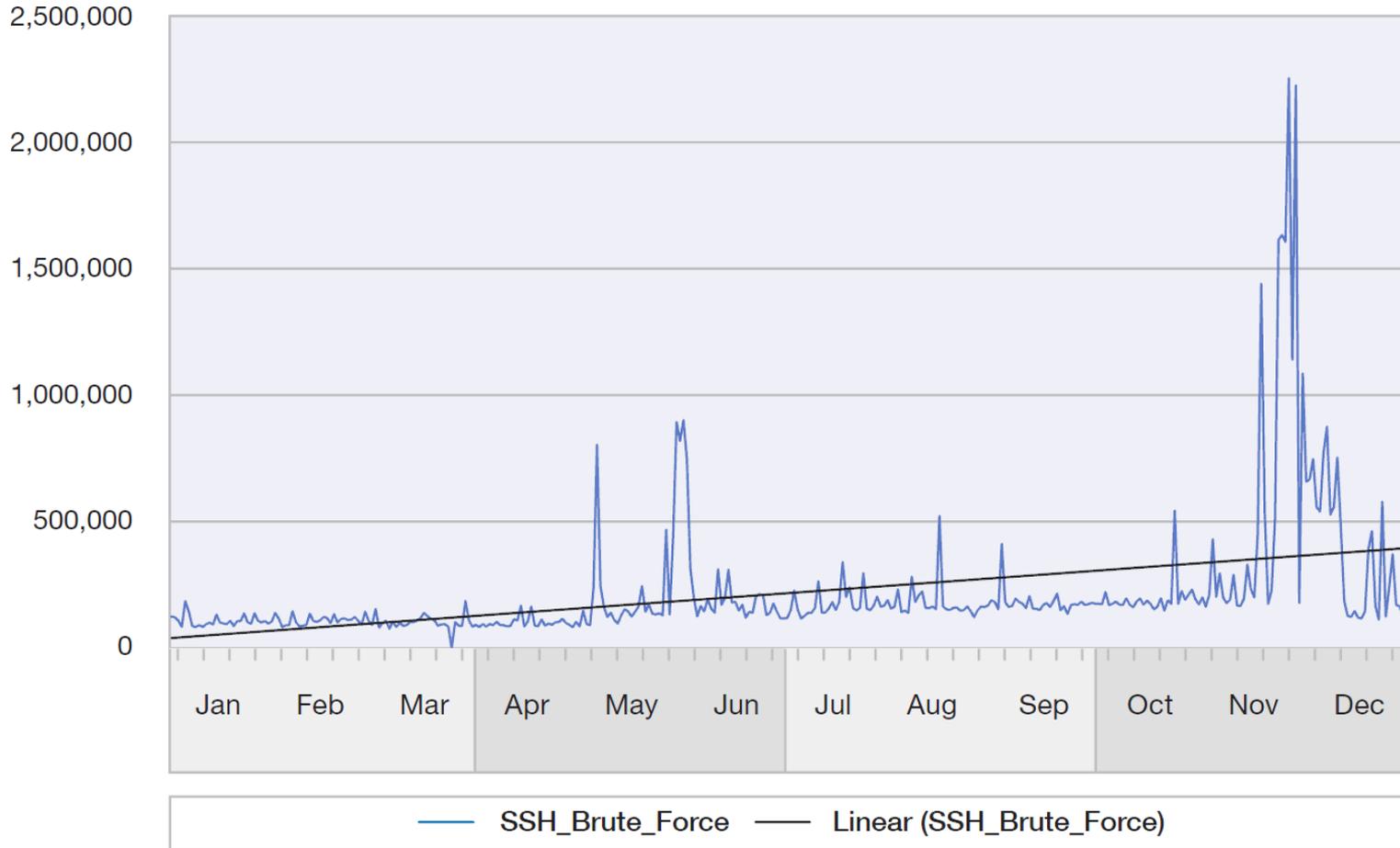
Top MSS High Volume Signatures and Trend Line –
Shell_Command_Injection

2011



SSH Brute Force Activity

Top MSS High Volume Signatures and Trend Line – SSH_Brute_Force
2011





Highlights from the 2011 Trend Report

- New Attack Activity
- Progress in Internet Security
- Interesting Developments



Progress in Internet Security

- Public exploits for browsers and document viewers decreased in 2011, whereas public exploits for multimedia renderers stayed the same.

- Sandboxes have seen success but are not bullet-proof.
 - CVE-2012-0724,-0725 – Flash for Chrome Sandbox Bypasses – X-Force Research
 - CVE-2011-1353 – Adobe Reader X Sandbox Bypass – X-Force Research

- Web app vulnerabilities declined from 49% of disclosures in 2010 to 41% in 2011
 - A large decline in new SQL Injection bugs, but SQL Injection rising as attack method

- Vendors continue to improve patching timeframes
 - 36% of vulns unpatched in 2011 versus ~50% a few years ago
 - 58% patched same day

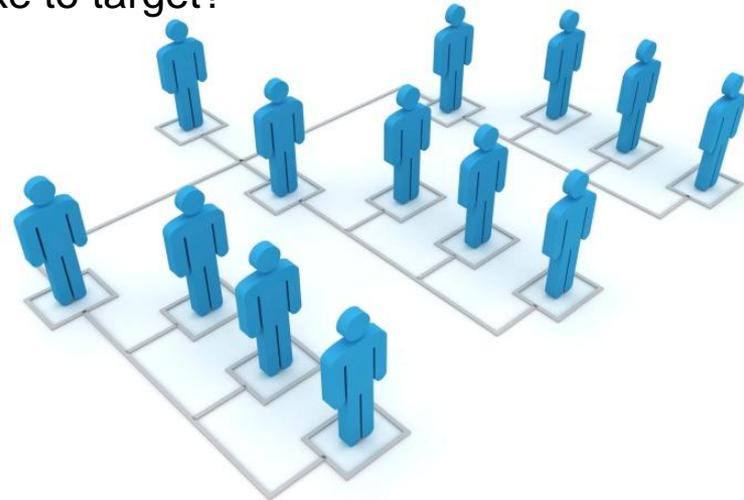


Highlights from the 2011 Trend Report

- New Attack Activity
- Progress in Internet Security
- **Interesting Developments**
 - **Social networking**
 - **Mobile exploit disclosures up**
 - **Anonymous proxies increase**
 - **Mac OS X Malware**

Social Networking – no longer a fringe pastime

- Attackers finding social networks ripe with valuable information they can mine to build intelligence about organizations and its staff:
 - Scan corporate websites, Google, Google News
 - Who works there? What are their titles?
 - Automating the process with tools and scripts
 - Search LinkedIn, Facebook, Twitter profiles
 - Who are their colleagues?
 - Start to build an org chart
 - Who works with the information the attacker would like to target?
 - What is their reporting structure?
 - Who are their friends?
 - What are they interested in?
 - What are their work/personal email addresses?
 - Can they leverage the developer API or ad network?





Mobile Numbers

Having your mobile number will help you log in from anywhere. Carrier charges may apply.

Mobile Numbers

- none -

[Add another](#)

Secret Questions (Required)

You must have two secret questions and answers.

Secret Question 1:

Your Answer:

Secret Question 2:

Your Answer:

- Select -

Who is your favorite author?

What is the last name of your best man at your wedding?

What is the last name of your maid of honor at your wedding?

What is the name of your favorite book?

What is the last name of your favorite musician?

Who is your all-time favorite movie character?

What was the make of your first car?

What was the make of your first motorcycle?

What was your first pet's name?

What is the name of your favorite sports team?

Where did you spend your childhood summers?

What was the last name of your favorite teacher?

What was the last name of your best childhood friend?

What was your favorite food as a child?

What was the last name of your first boss?

What is the name of the hospital where you were born?

What is your main frequent flier number?

What is the name of the street on which you grew up?

- Create your own question -

- Select -

Type your answer here

Secret Questions (Required)

You must have two secret questions and answers for future password reset attempts.

Secret Question 1:

Your Answer:

Secret Question 2:

Your Answer:

- Select -

- Select -

Where did you spend your honeymoon?

Where did you meet your spouse?

What is your oldest cousin's name?

What is your youngest child's nickname?

What is your oldest child's nickname?

What is the first name of your oldest niece?

What is the first name of your oldest nephew?

What is the first name of your favorite aunt?

What is the first name of your favorite uncle?

What town was your father born in?

What town was your mother born in?

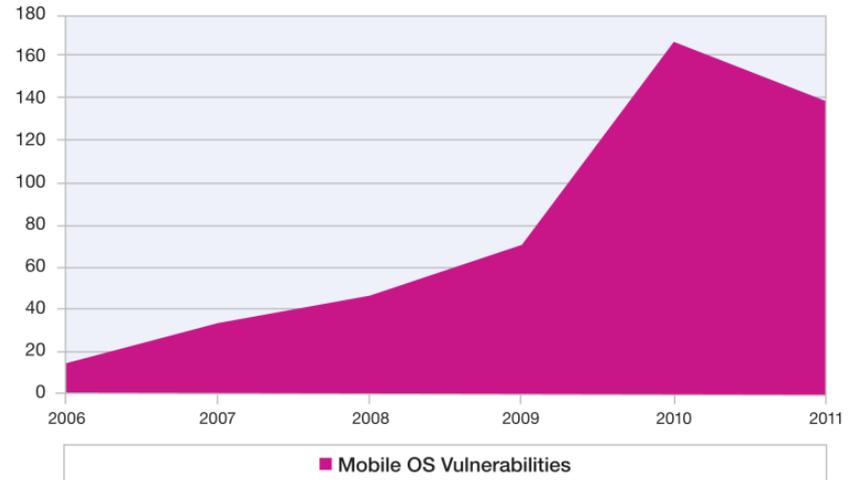
- Create your own question -

Mobile OS vulnerabilities & exploits

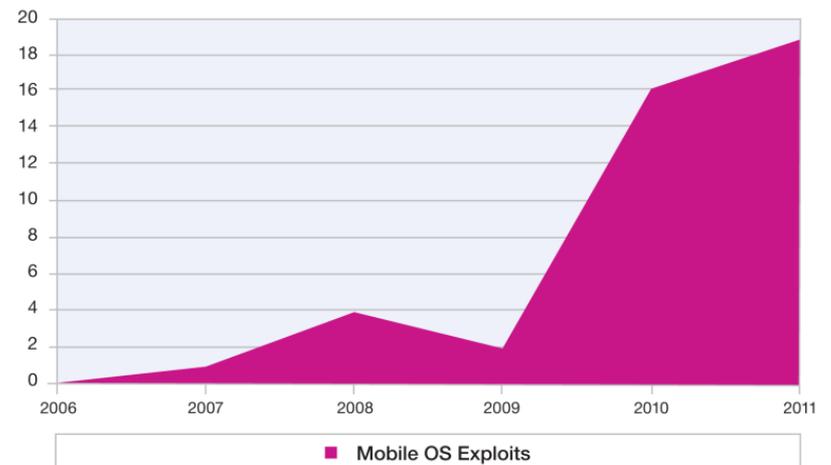
- Will 2012 be a ground-breaking year for mobile exploitation?
 - Half of the year is gone, but X-Force doubts it.

- Persistent rumors of in-the-wild exploitation of iOS despite majority of mobile attacks being phony Android apps.

Total Mobile Operating System Vulnerabilities
2006-2011



Mobile Operating System Exploits
2006-2011



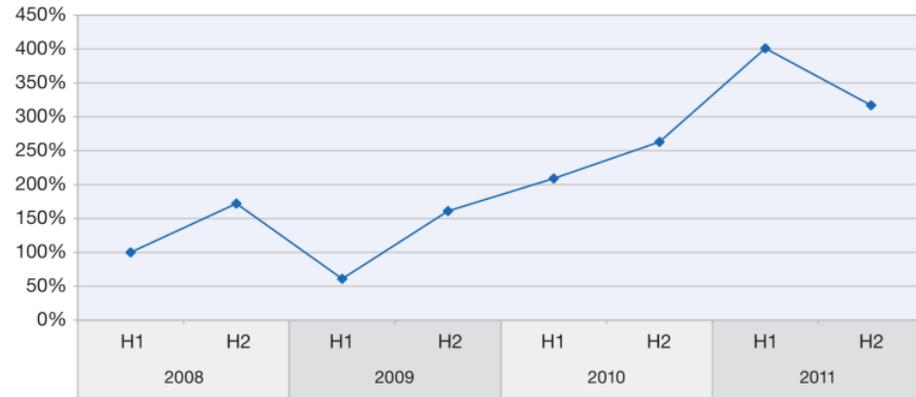
Anonymous HTTP proxies on the rise

- Approximately 4 times more anonymous proxies than seen 3 years ago
- Some used to hide attacks, others to evade censorship

Note: These proxies are not the highest anonymity proxies and services available.

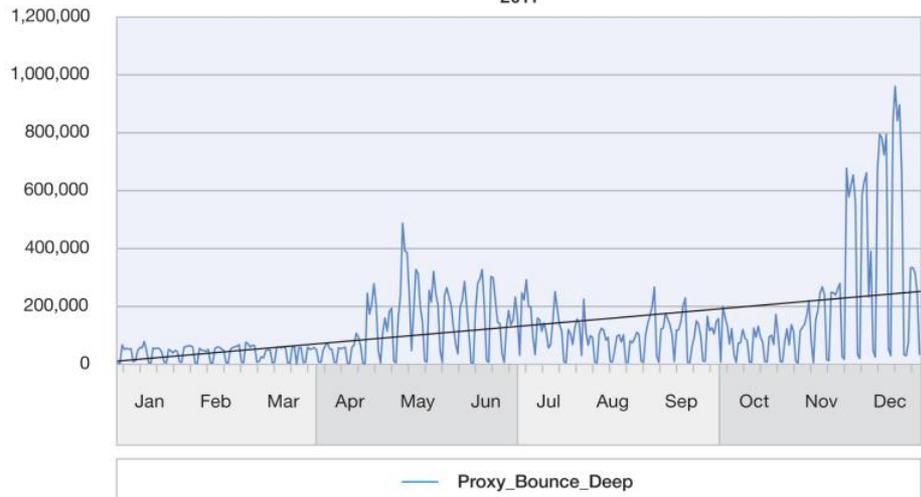
- Signature detects situations where clients are attempting to access websites through a chain of HTTP proxies
- Could represent
 - legitimate (paranoid) web surfing
 - attackers obfuscating the source address of launched attacks against web servers

Volume of Newly Registered Anonymous Proxy Websites
2008 to 2011



Source: IBM X-Force® Research and Development

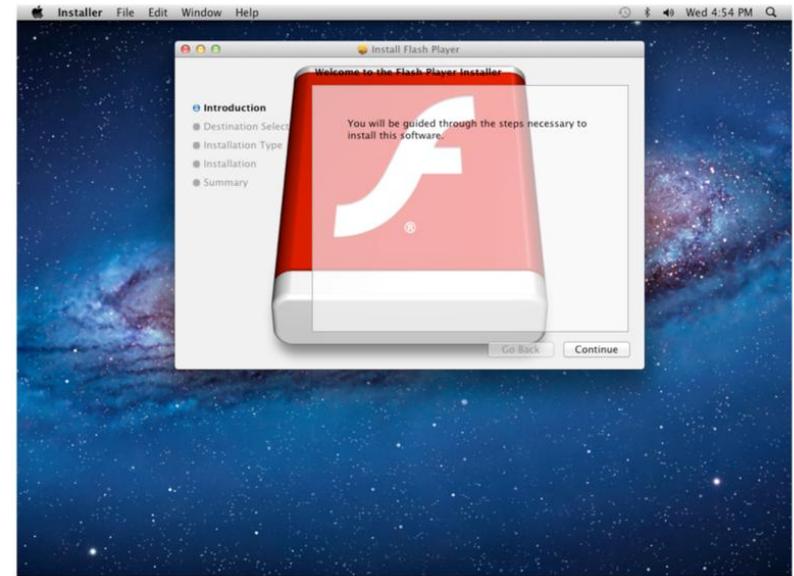
Top MSS High Volume Signatures and Trend Line – Proxy_Bounce_Deep
2011



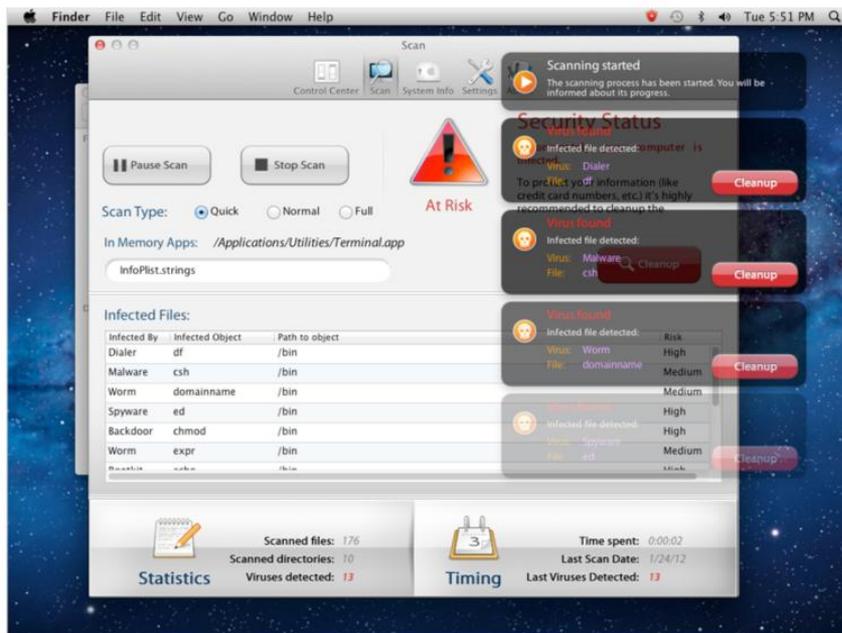
Source: IBM X-Force® Research and Development

Mac OSX malware

- 2011 has seen the most activity in the Mac malware world.
 - Not only in volume compared to previous years, but also in functionality.
- In 2011, we started seeing Mac malware with functionalities that we've only seen before in Windows® malware.



Source: IBM X-Force® Research and Development



Source: IBM X-Force® Research and Development

- MacDefender – Rogue AV
- Flashback – Backdoor Trojan
 - Added drive-by exploitation in 2012
- DevilRobber – Backdoor Trojan
 - Steals Keychain, Bitcoin Wallet,...

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
Frequency X at
<http://blogs.iss.net/rss.php>



Attend in-person
events
<http://www.ibm.com/events/calendar/>



Join the Institute for
Advanced Security
www.instituteforadvancedsecurity.com



Subscribe to the security
channel for latest security
videos
www.youtube.com/ibmsecuritysolutions



ibm.com/security