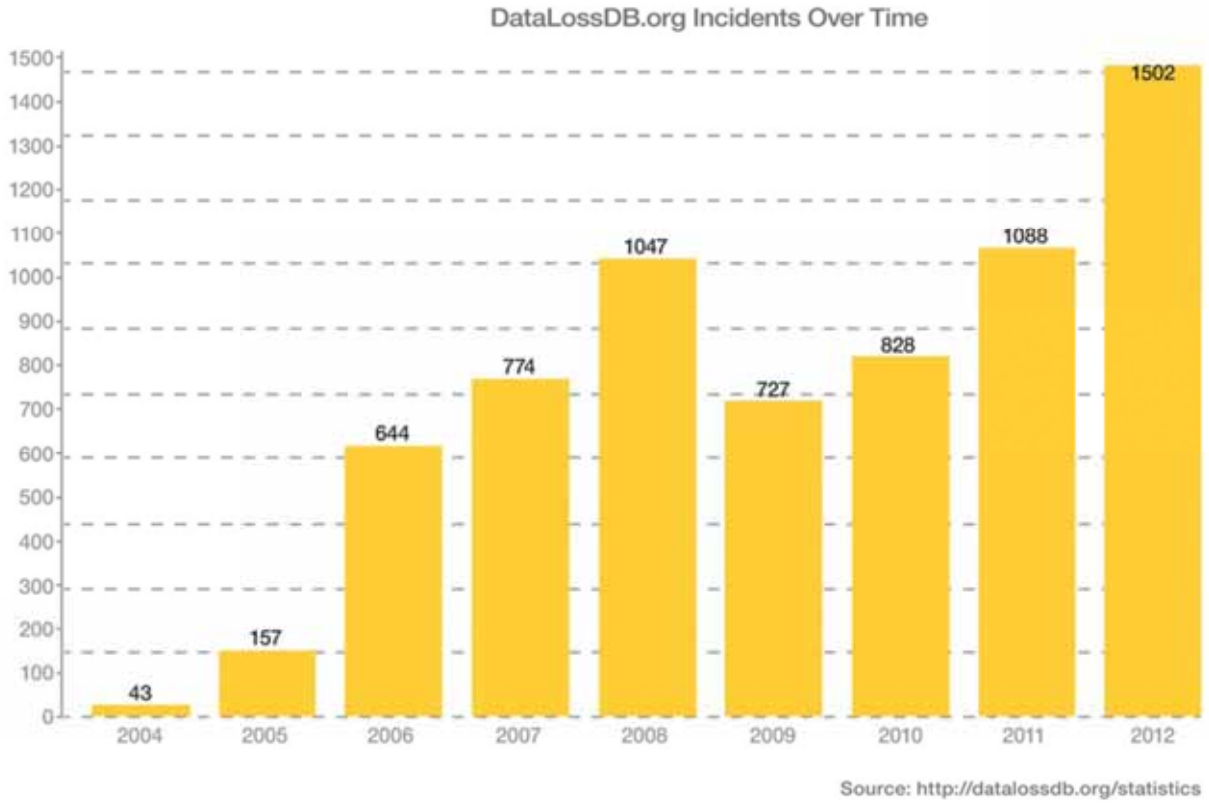
*Pedro Galvão, CISSP, CISA*
*Senior Managing Consultant, Security Services*

# Segurança da nova geração das TI

# Agenda

- Ambiente actual de segurança
- Tendências
  - Regulamento Europeu
  - Evolução do panorama de segurança
- Duas perguntas essenciais

2011 foi declarado com o ano do “Security Breach” dado o número elevado de intrusões com roubo de informação.
Em 2012 o número de incidentes deste género aumentou 40%.



# No inicio de 2010 a Google anunciou que tinha descoberto um ataque à sua rede com um nível de sofisticação muito elevado.

- O ataque decorreu durante vários meses sem ser detectado;
- O que a investigação identificou foi um tipo de ataque denonimado de Advanced Persistent Threat (APT).
- Um APT não usa necessariamente ferramentas ou tecnologias muito sofisticadas
- Usa sim, **processos operacionais muito sofisticados**
  - Vários elementos coordenados ao longo de um horizonte temporal longo (geralmente meses)
  - Acções pontuais, que encadeadas resultam no acesso a alvos específicos

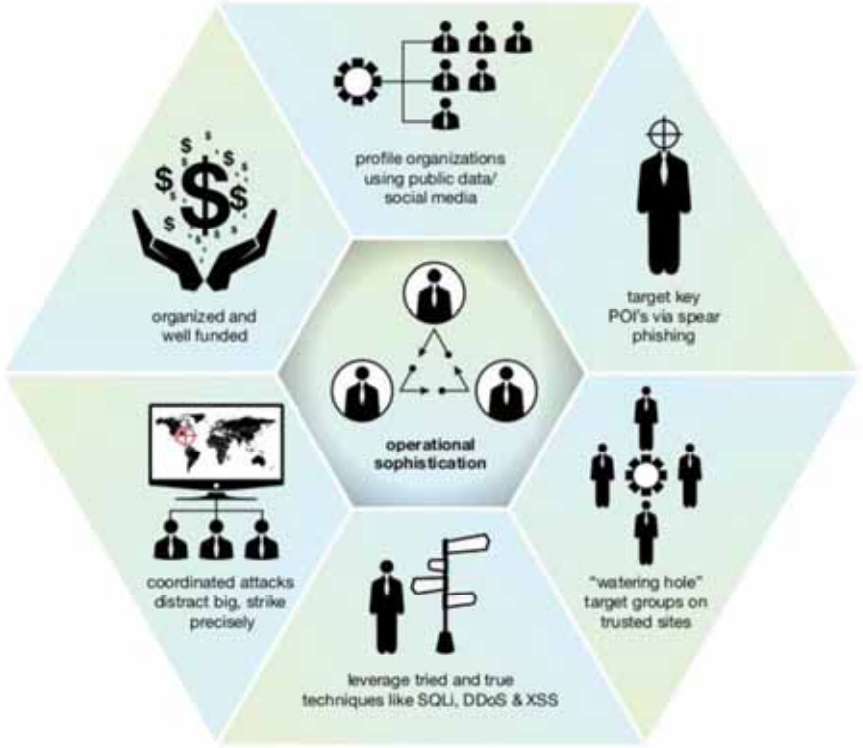
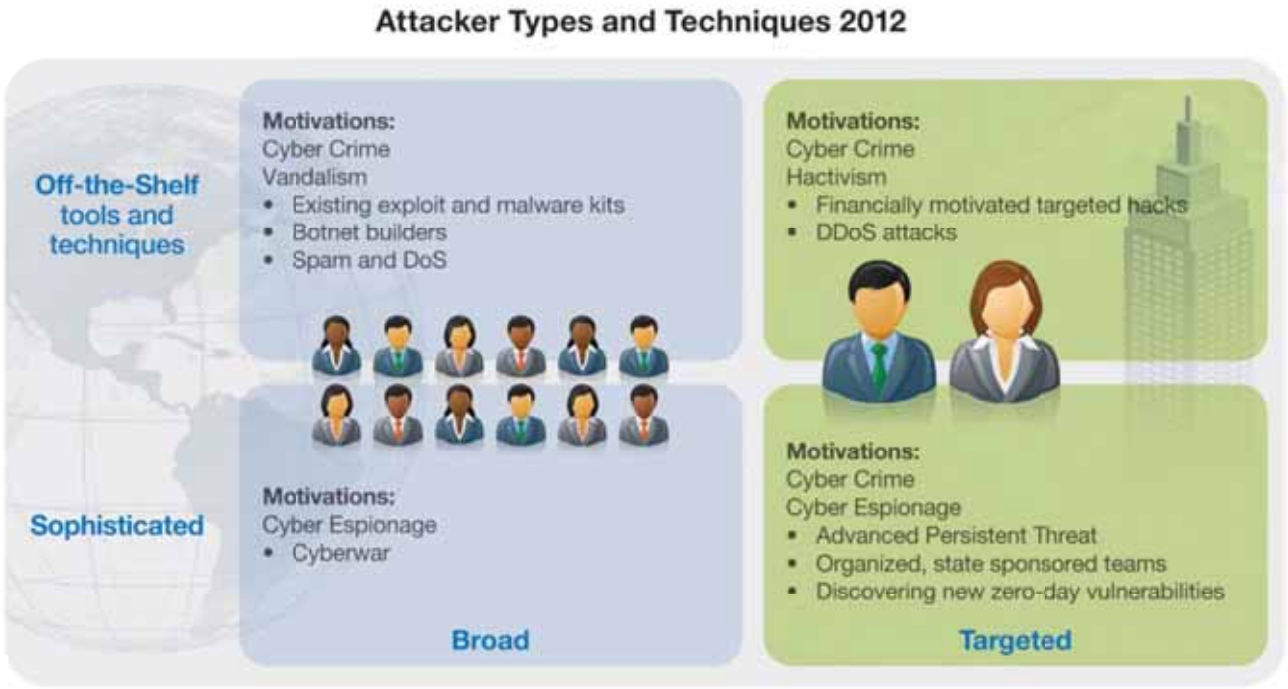


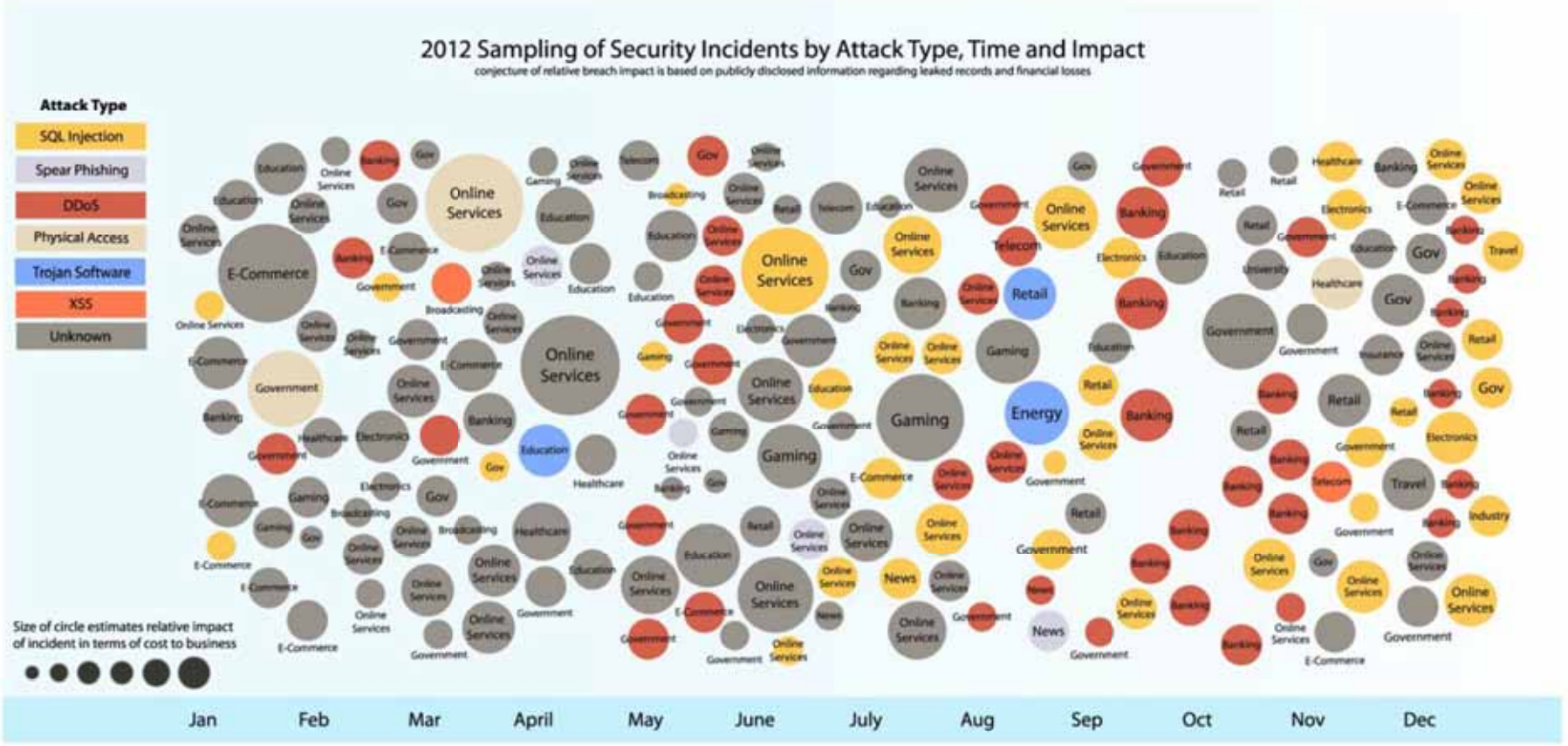

*Figure 1: 2013 Methods of Operational Sophistication*

# No entanto a maioria dos ataques continua a ter alvos generalizados e a usar ferramentas “off-the-shelf”.




Source: IBM X-Force® Research and Development

# As principais vulnerabilidades exploradas continuam a estar relacionadas com problemas no desenvolvimento de aplicações web (SQL Injection)...




Source: IBM X-Force® Research and Development

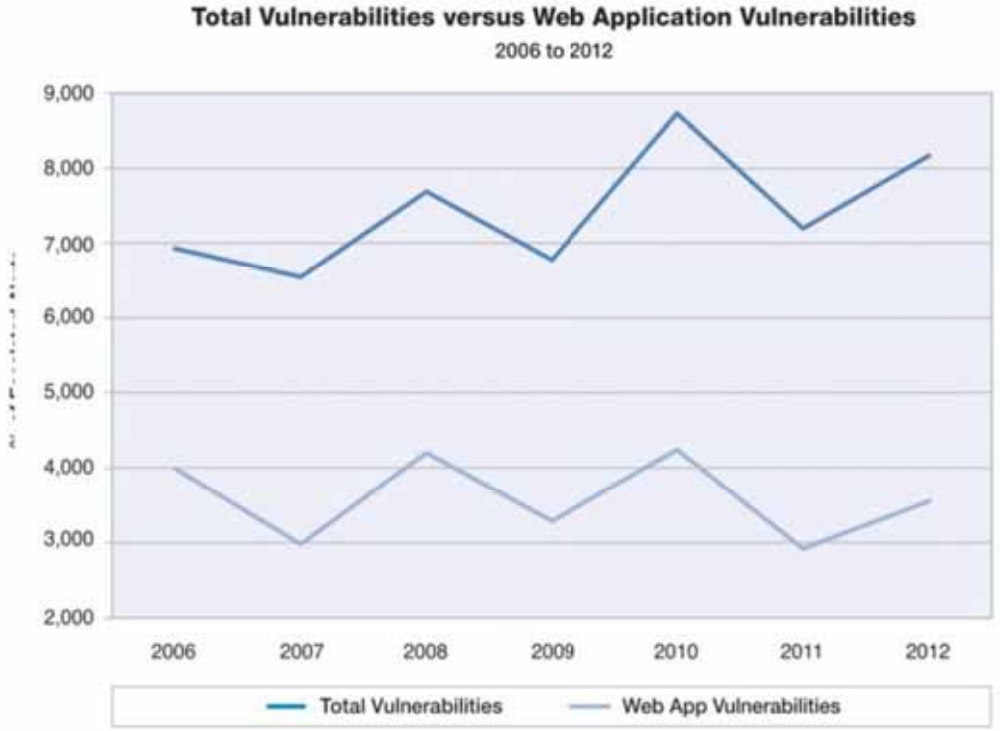
… e estas vulnerabilidades são exploradas para o primeiro passo de infecção – colocar conteúdos maliciosos nos sites ou influenciar utilizadores a visitar sites que confiem através de emails de SPAM.

**14%**

increase in
web application
vulnerabilities

Cross-site scripting
represented

**53%**



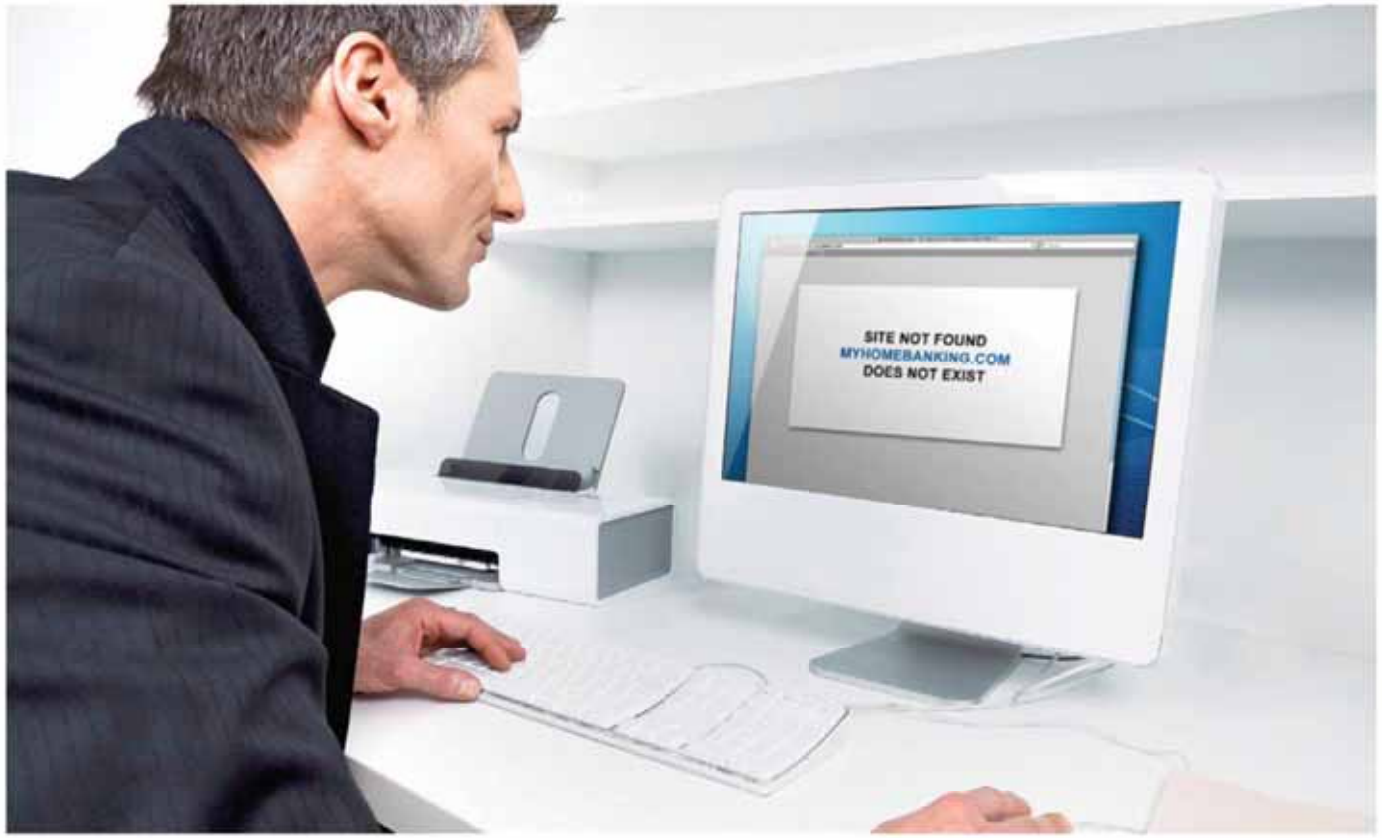

Source: IBM X-Force® Research and Development

# Outro vector que tem tido muita evolução são os ataques de Distributed Denial of Service.

Ataques deste género usam redes de milhares de computadores para "navegar" ao mesmo tempo para um alvo específico.

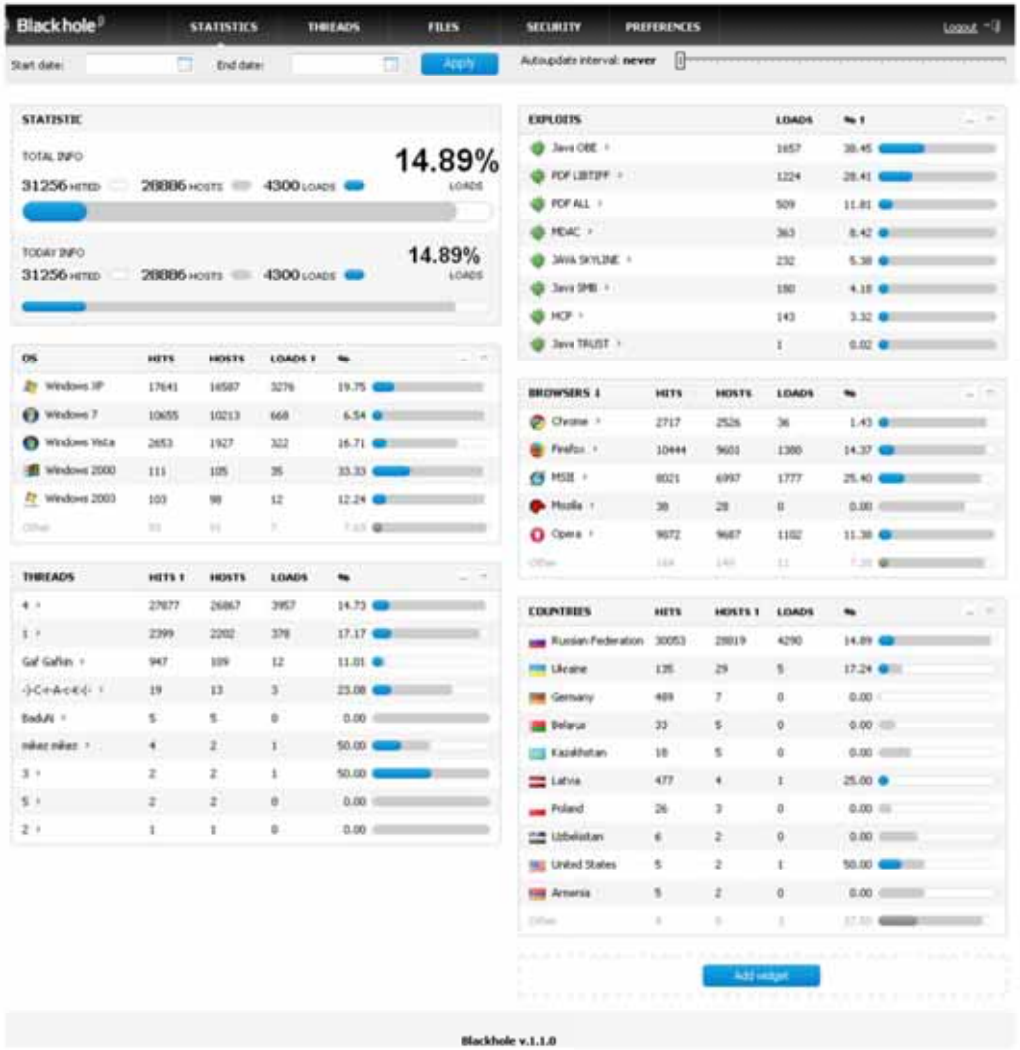
Tipicamente um ataque deste género consumia cerca de 10-15Gbps de largura de banda.

Em 2012 este tipo de ataque consumiu em média 60-70 Gbps e em alguns casos chegou a 200Gbps

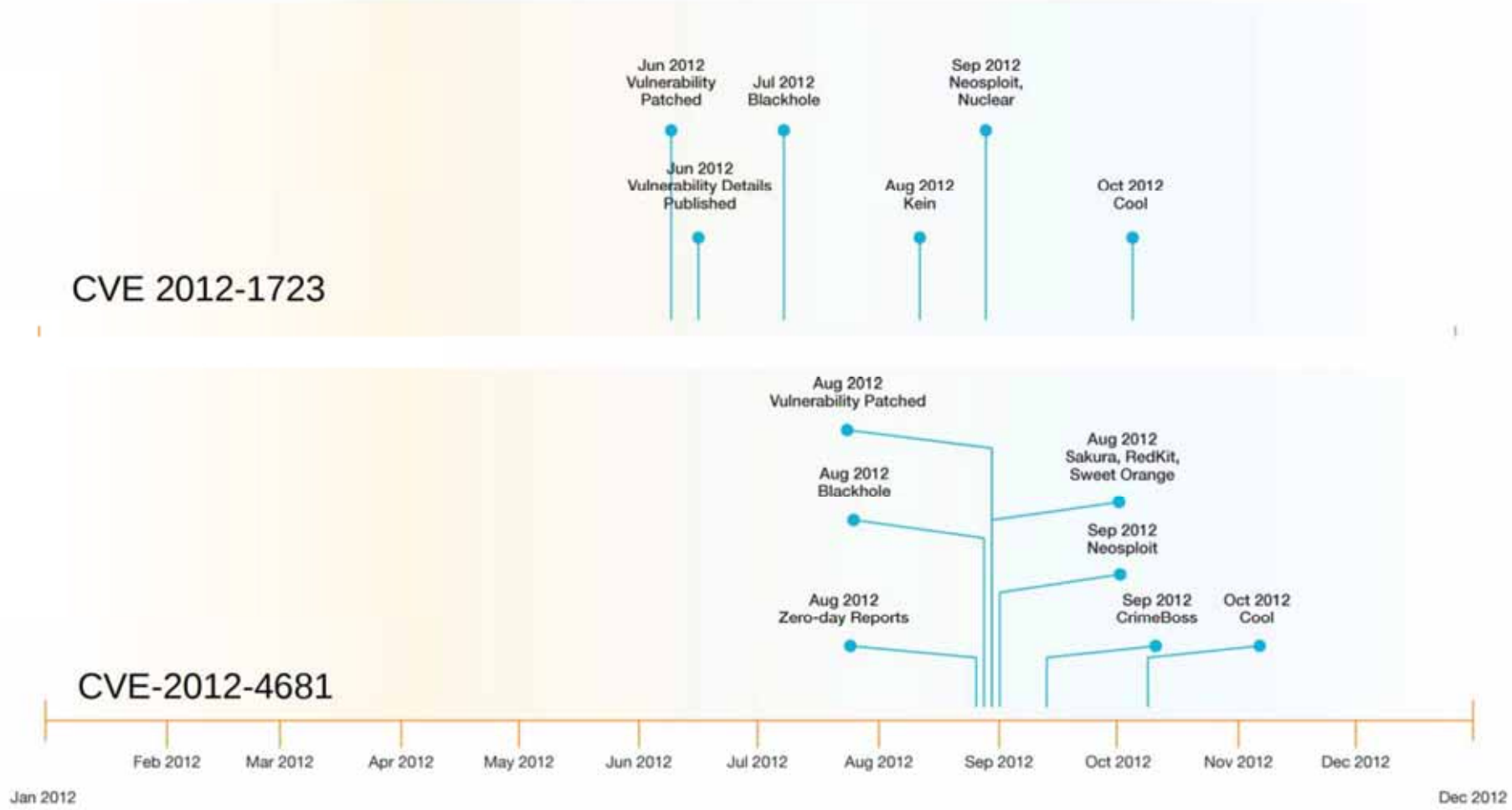


# Muitos dos ataques são automatizados recorrendo a ferramentas que se podem comprar na Internet.

- Blackhole
- Redkit
- Phoenix
- Kein
- Cool
- Neosploit
- Nuclear
- …

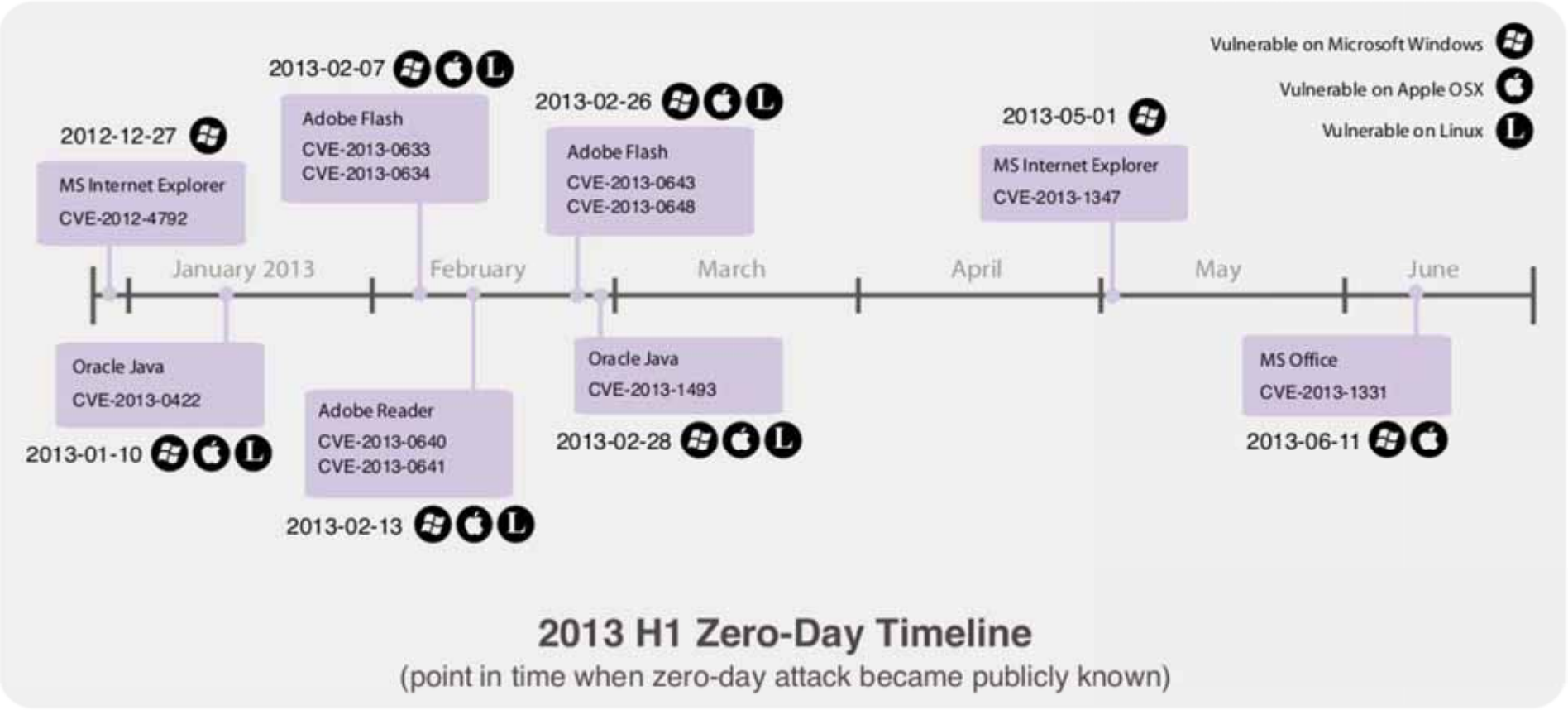


# Estas ferramentas têm suporte evolutivo, correctivo, e desenvolvimento activo, seguindo a evolução das vulnerabilidades.




Source: IBM X-Force® Research and Development

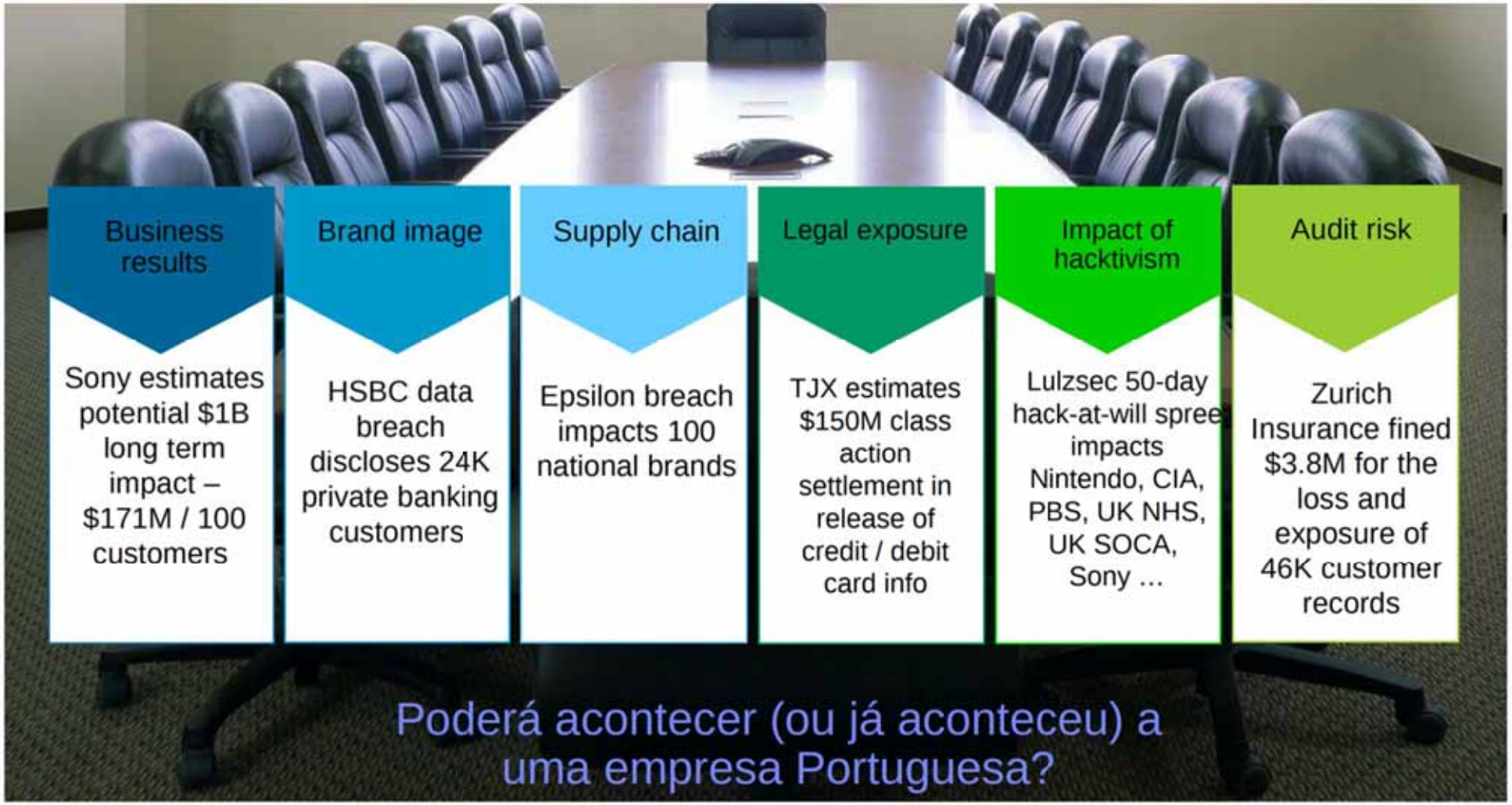
# Vulnerabilidades Zero-day na primeira metade de 2013




**2013 H1 Zero-Day Timeline**

(point in time when zero-day attack became publicly known)

# Consequências...



# "Lessons learned..."
# 10 medidas simples de protecção a implementar por todas as organizações

1. Realizar auditorias internas e externas numa base regular com foco em segurança;
2. Assegurar que os "endpoints" (Laptops, desktops, tablets, smartphones) são **controlados**;
3. Segmentar e isolar informação sensível;
4. Back to basics – assegurar que existem firewalls, antivirus e sistemas de prevenção de intrusões nos pontos e nos sistemas críticos;
5. Auditar aplicações web;
6. Sensibilizar utilizadores "safe computing"
7. Pesquisar todos os sistemas à procura de passwords fracas;
8. Integrar segurança em todos os projectos;
9. Rever / examinar as políticas e práticas de segurança dos parceiros de negócio;
10. Definir e implementar um plano de resposta a incidentes de segurança.

# Agenda

- Ambiente actual de segurança
- Tendências
  - Regulamento Europeu
  - Evolução do panorama de segurança
- Duas perguntas essenciais de segurança

# (Novo) Regulamento Europeu sobre protecção de dados pessoais

- Confere ao titular dos dados o direito de ser esquecido e ao apagamento dos dados
- Obriga o responsável pelo tratamento:
  - A informar terceiros a quem tenham sido transmitidos os dados para os apagar em caso de pedido do titular
  - A definir e implementar procedimentos e mecanismos para o exercicio dos direitos do titular (com prazos de execução)
  - A notificar violações de dados pessoais
  - A designar um delegado para protecção de dados na empresa

**Implicações**

1. Saber onde estão todos os dados pessoais e por onde passam
2. Assegurar que existem medidas de eliminação de dados em locais de passagem de dados
3. Assegurar que existe rastreabilidade (confiável) de acesso e de transmissão de dados
4. Definir e implementar procedimentos e mecanismos para lidar com todos os casos de uso relacionados
5. Definir e implementar procedimentos de gestão de incidentes de segurança
6. Assegurar a criação e a manutenção competências nesta área

# Tendencias (e necessidades) na gestão da segurança

- Aumento da eficiência operacional na gestão da segurança
  - Da mesma forma que os APTs se baseiam na eficiência de operações, a gestão da segurança tem de definir claramente as suas responsabilidades e delegar trabalho para optimizar resultados.
  - Está a haver um aumento na adopção de modelos de gestão externalizada para funções básicas de segurança (como a prevenção de intrusões e a gestão de firewalls).
- Aceleração da integração de funções
  - Para ser mais eficaz na detecção de situações de pré-incidente torna-se necessário retirar o isolamento muito comum da função de segurança – integrando ao nível da informação e dos processos a análise situacional de segurança
  - Traduz-se por exemplo em sistemas de recolha e de análise de logs que integrem a informação necessária para maior eficácia na interpretação do ambiente (Security Event Management e Centros de Operação Integrados).
- Foco nos processos de gestão de segurança e gestão de risco
  - Externalizar as actividades industrializáveis (gestão e monitorizaçãode segurança de sistemas, gestão de vulnerabilidades)
  - Concentrar esforços em explorar os resultados destas actividades através de processos ágeis e relevantes para a organização
  - Medir a eficácia e eficiência da segurança em termos de resultados práticos e deixar os cálculos complexos de ROI para segundo plano

# Duas perguntas essenciais

**1) Como é que nos prevenimos de ataques / acesso indevido na última semana, mês, trimestre?**

**2) Como é que estamos a preparar a nossa segurança para o próximo trimestre?**

# Centros de investigação e de operação de segurança da IBM


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