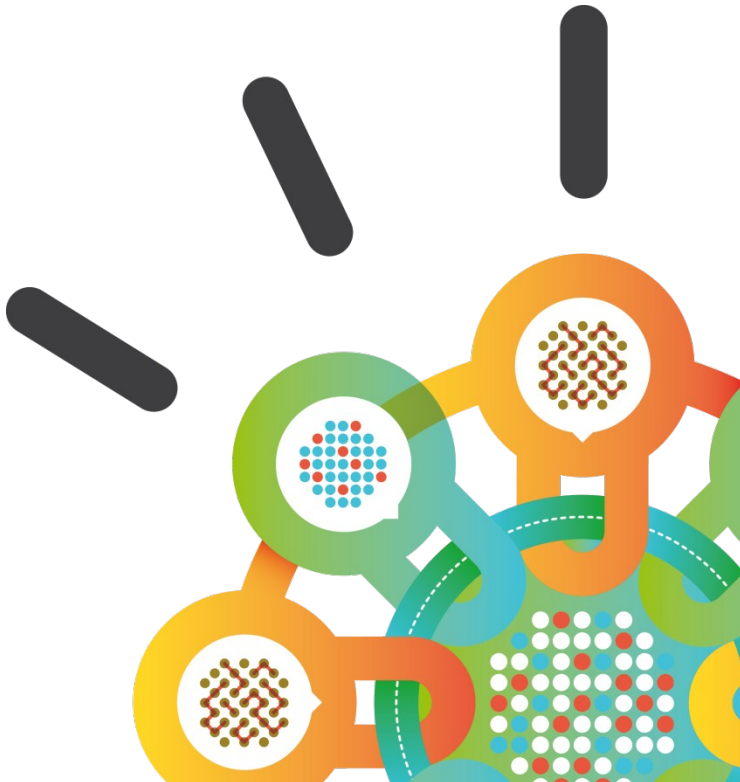
Security Intelligence.
Think Integrated.

Relatório Semestral de Tendências e Riscos IBM X-Force 2013

Novembro de 2013



O X-Force é a base para pesquisas avançadas de segurança e ameaças no Framework de Segurança IBM

X-FORCE

A missão do X-Force é:

- **Monitorar** e avaliar o panorama de mudanças rápidas de ameaças
- **Pesquisar** novas técnicas de ataque e desenvolver proteção para os desafios de segurança do futuro
- **Informar** nossos clientes e o público em geral

As equipes colaborativas da IBM monitoram e analisam o panorama de mudanças das ameaças

Cobertura

Mais de 20.000 dispositivos sob contrato

Mais de 3.700 clientes gerenciados no mundo todo

Mais de 15 bilhões de eventos gerenciados por dia

133 países monitorados (MSS)

Mais de 1.000 patentes relacionadas à segurança

IBM Research

Profundidade

20 bilhões de imagens e páginas da web analisadas

40 milhões de ataques de spam e phishing

76 mil vulnerabilidades documentadas

Bilhões de tentativas de invasão diariamente

Milhões de amostras exclusivas de malware

O Tema do relatório semestral de 2013:

Invasores Otimizam as Táticas

3 Capítulos do Relatório de Tendências

Ataques dirigidos e violação de dados

- Sofisticação operacional
- Ataques de "watering hole"
- Websites estrangeiros comprometidos
- Diversões de DDoS

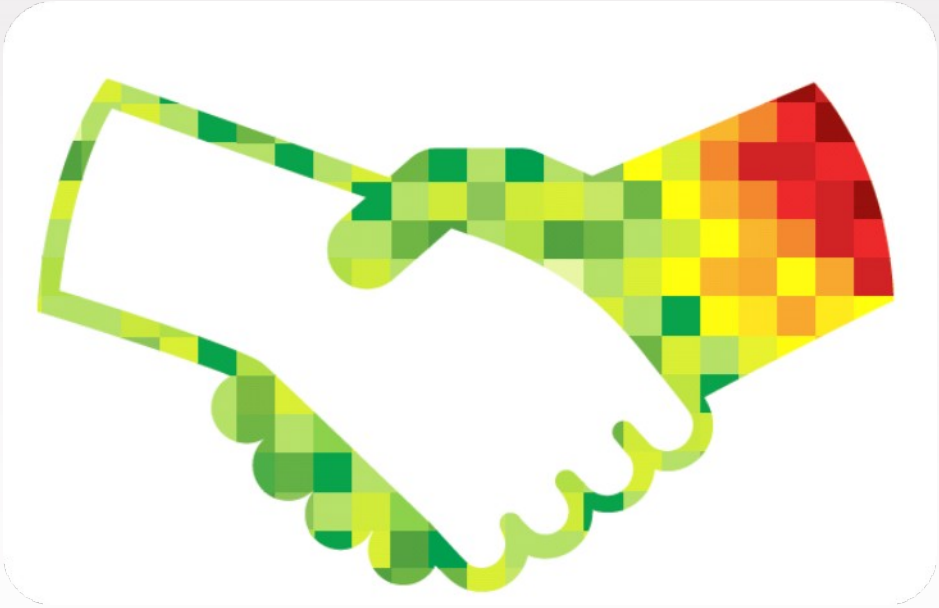
Social e Mobilidade

X-Force em Números

Explorando a confiança

Profissionais de segurança deveriam entender como os invasores estão tirando proveito da confiança em relacionamentos para:

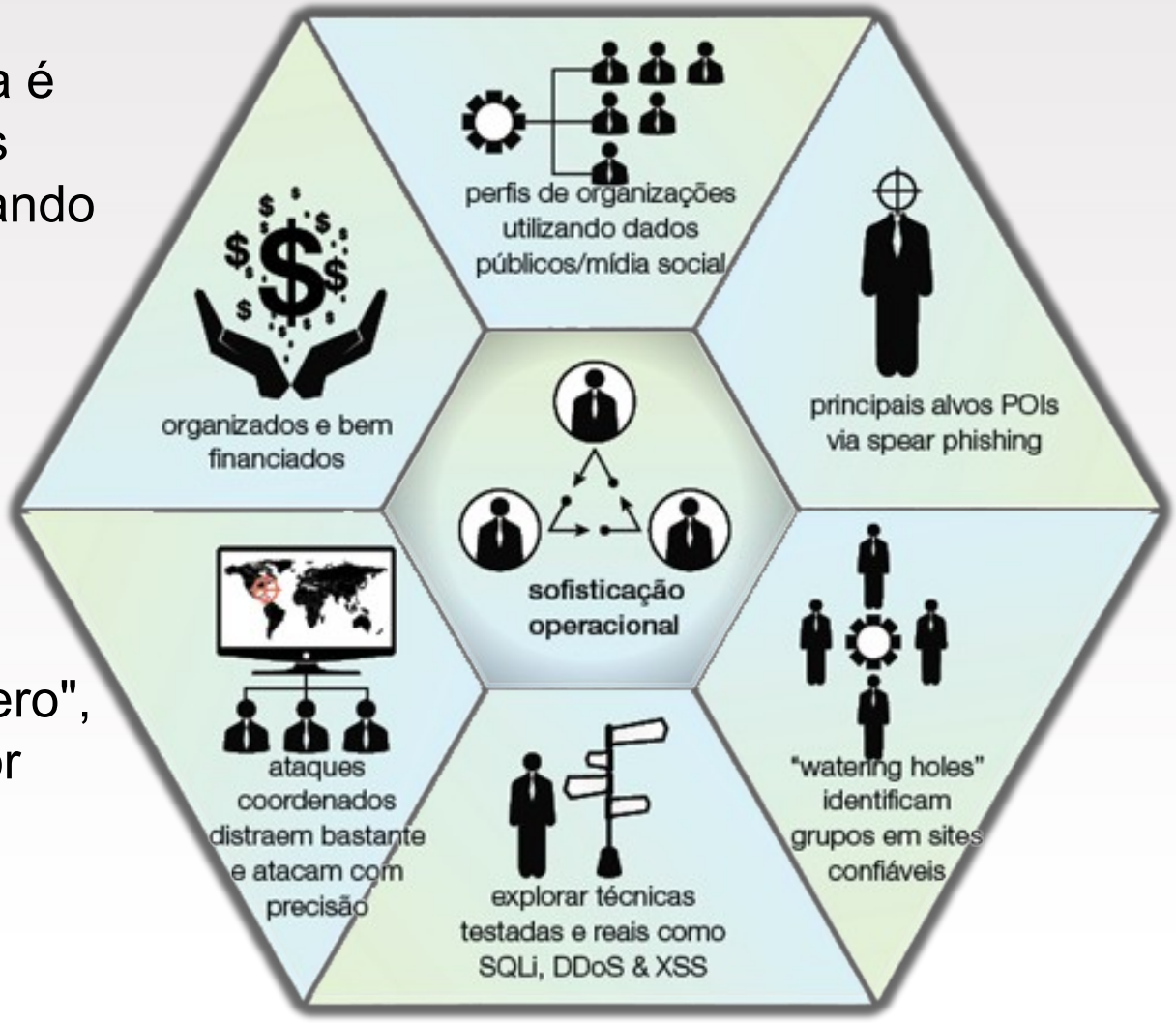
- Violar uma organização
- Visar grupos de usuários
- Criar métodos de diversão



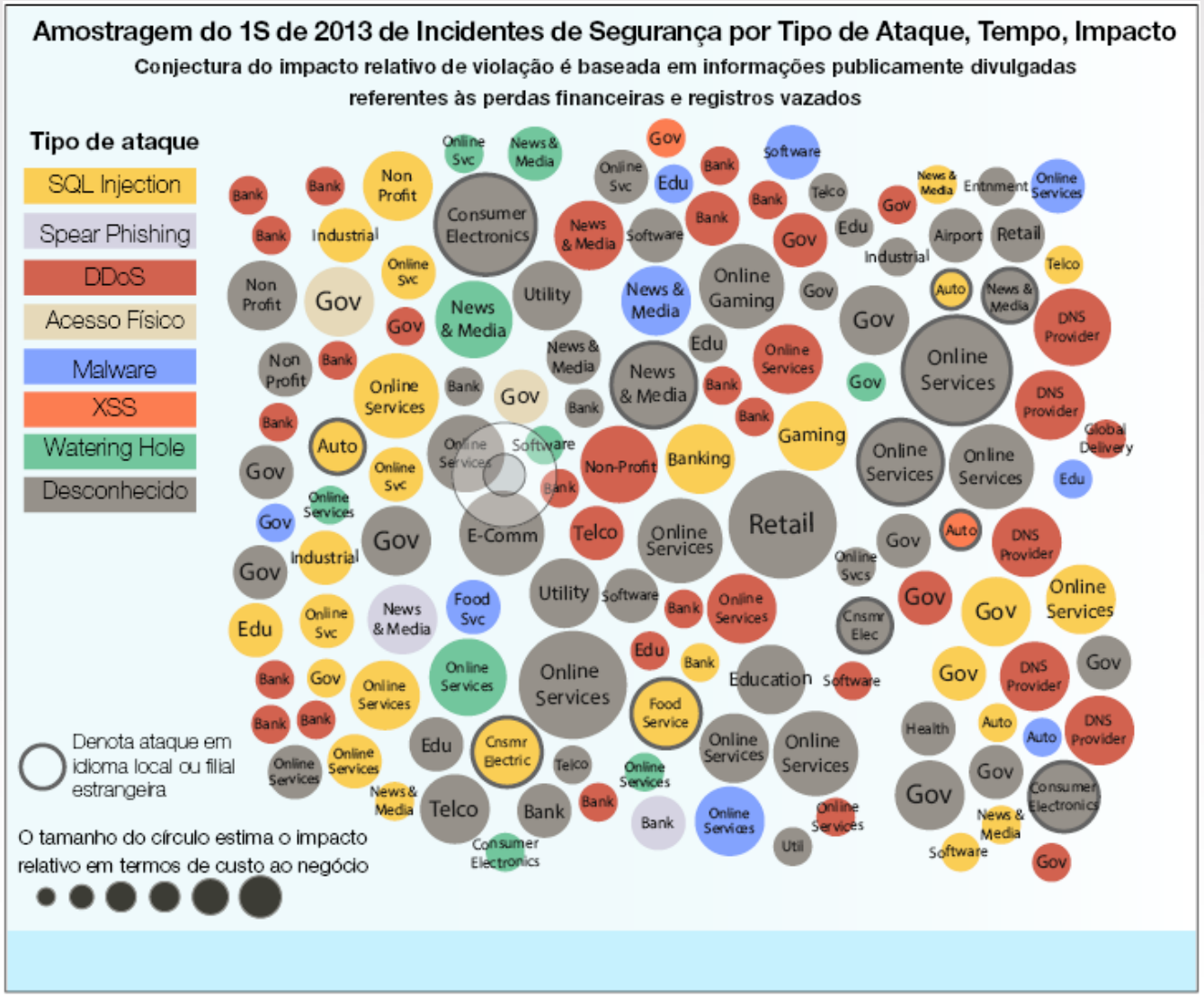
Sofisticação operacional

Exploração da confiança é um exemplo de como os invasores estão se tornando operacionalmente mais sofisticados para violar os alvos.

Muitas violações não são decorrentes de malware customizado e explorações do "dia-zero", os invasores buscam por caminhos de menor resistência

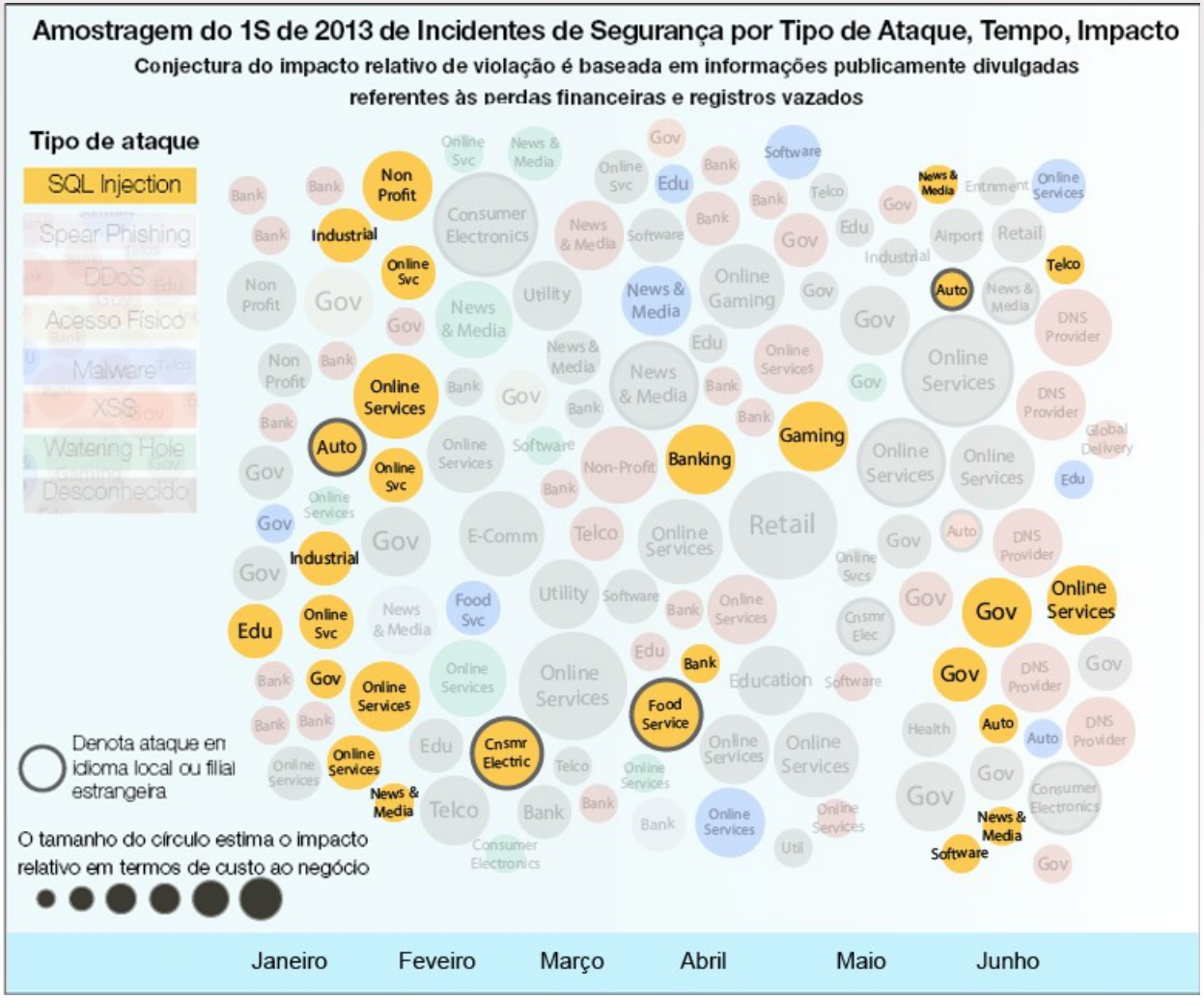


Incidentes de segurança no primeiro semestre de 2013



SQL Injection

ainda é confiável para a violação de banco de dados



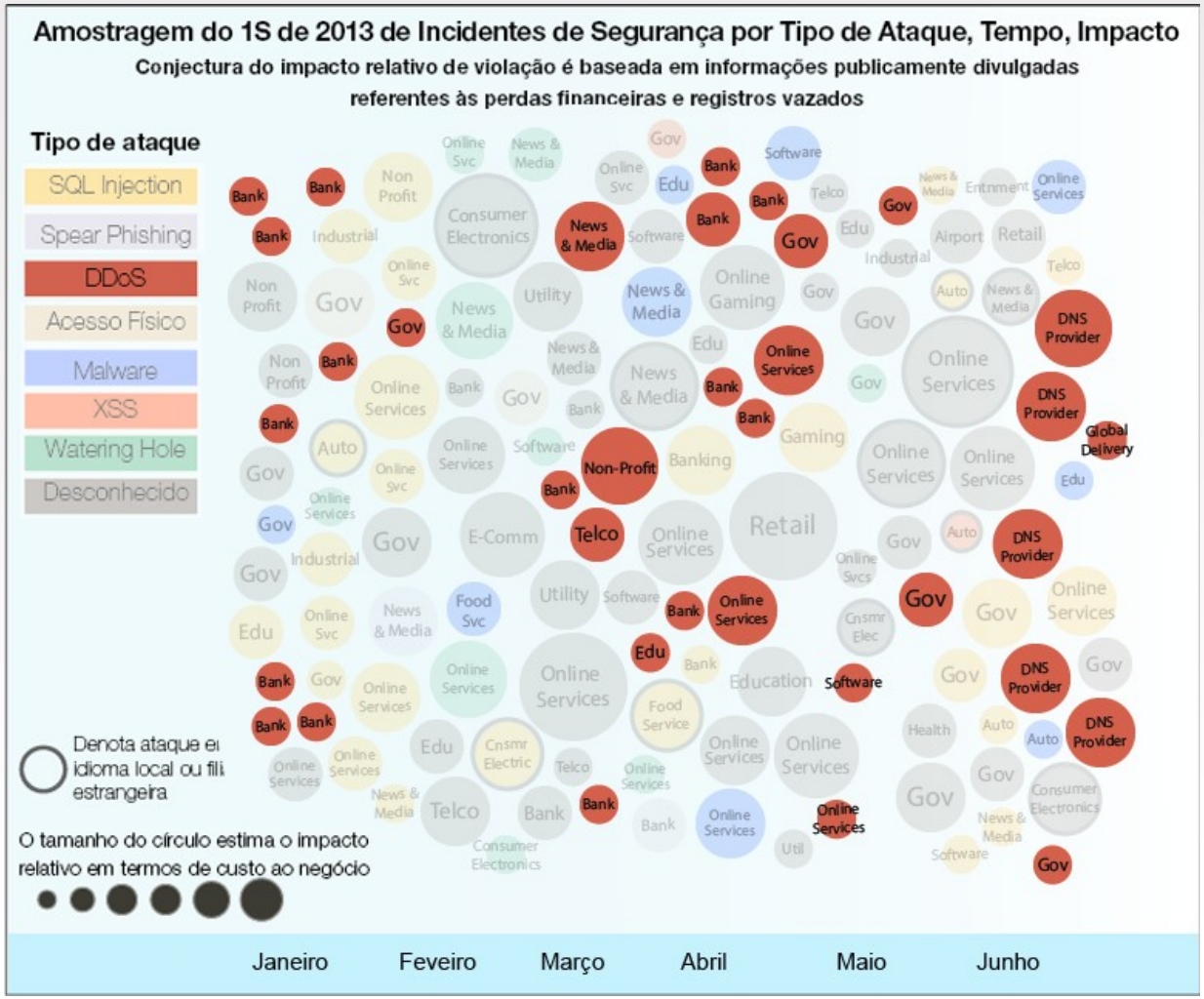
22% de violações rastreadas divulgadas

Baixo risco / alta recompensa

- **Instalações CMS antigas**
- **Plugins CMS**
- **Software de fórum**
- **Outros scripts populares de terceiros**

Ataques DDoS

continuam a interromper os negócios



Alto volume de tráfego de até

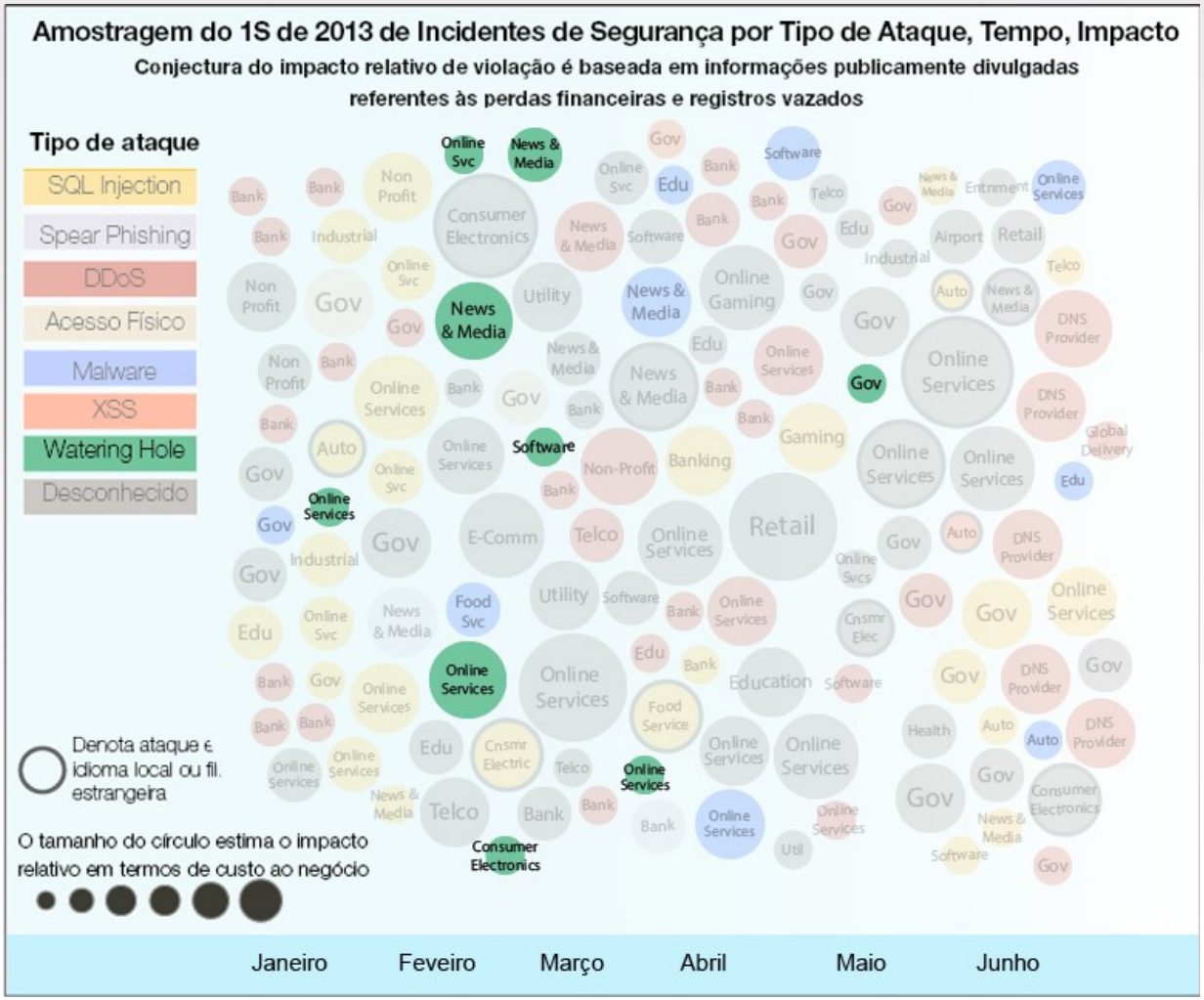
300Gbps

Segmentos afetados:

- **Bancário**
- **Governo**
- **Provedores de DNS**

"Watering Hole"

são ataques que comprometem a confiança do usuário final



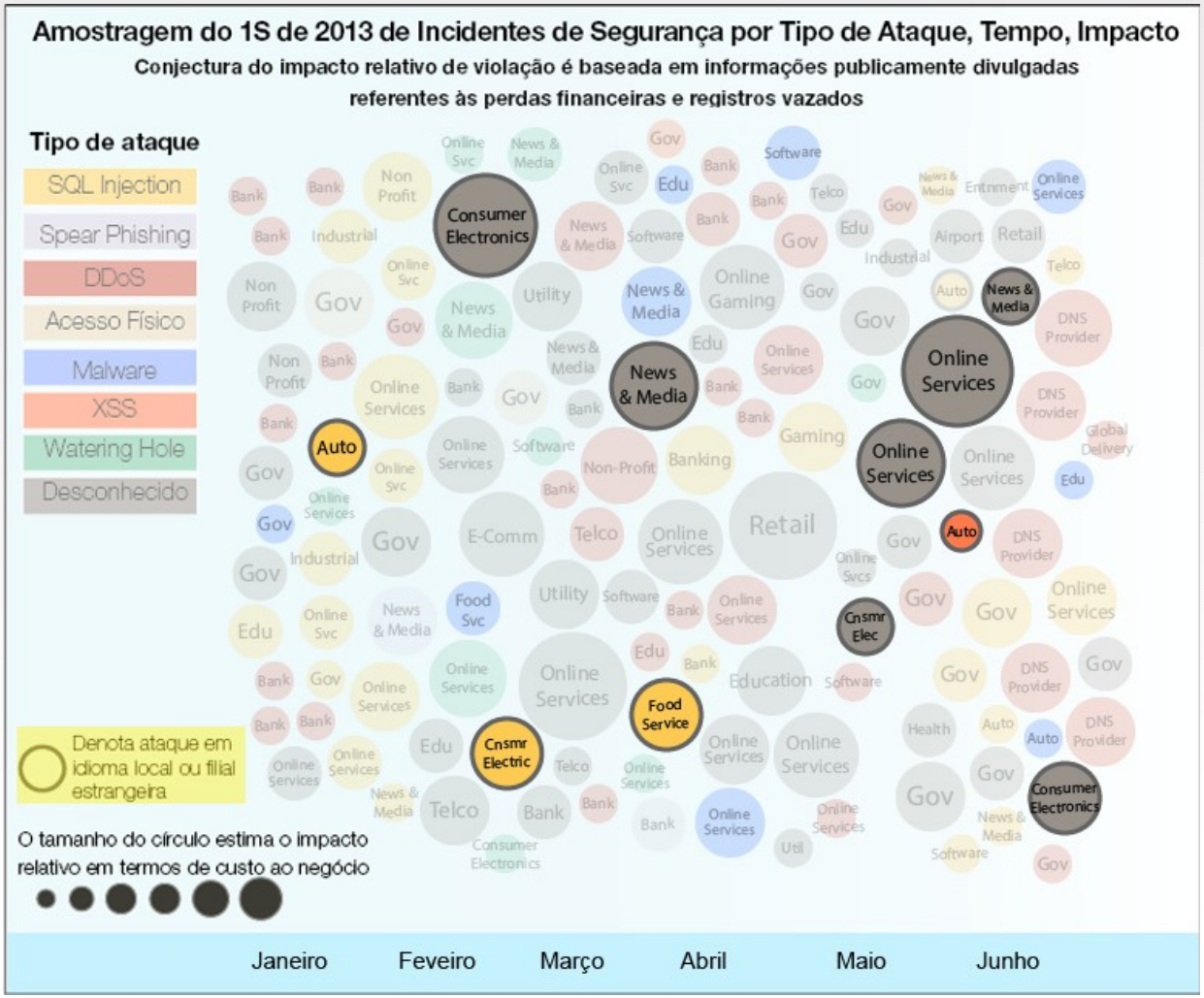
Corromper sites legítimos com exploração do "dia-zero"

Atingir Usuários Experientes

- **Desenvolvedores de empresas de tecnologia**
- **Funcionários do Governo**
- **Visitantes inocentes de sites confiáveis**

Websites não franqueados

(websites não franqueados) de filiais estrangeiras ou sites de idiomas locais denigrem marcas



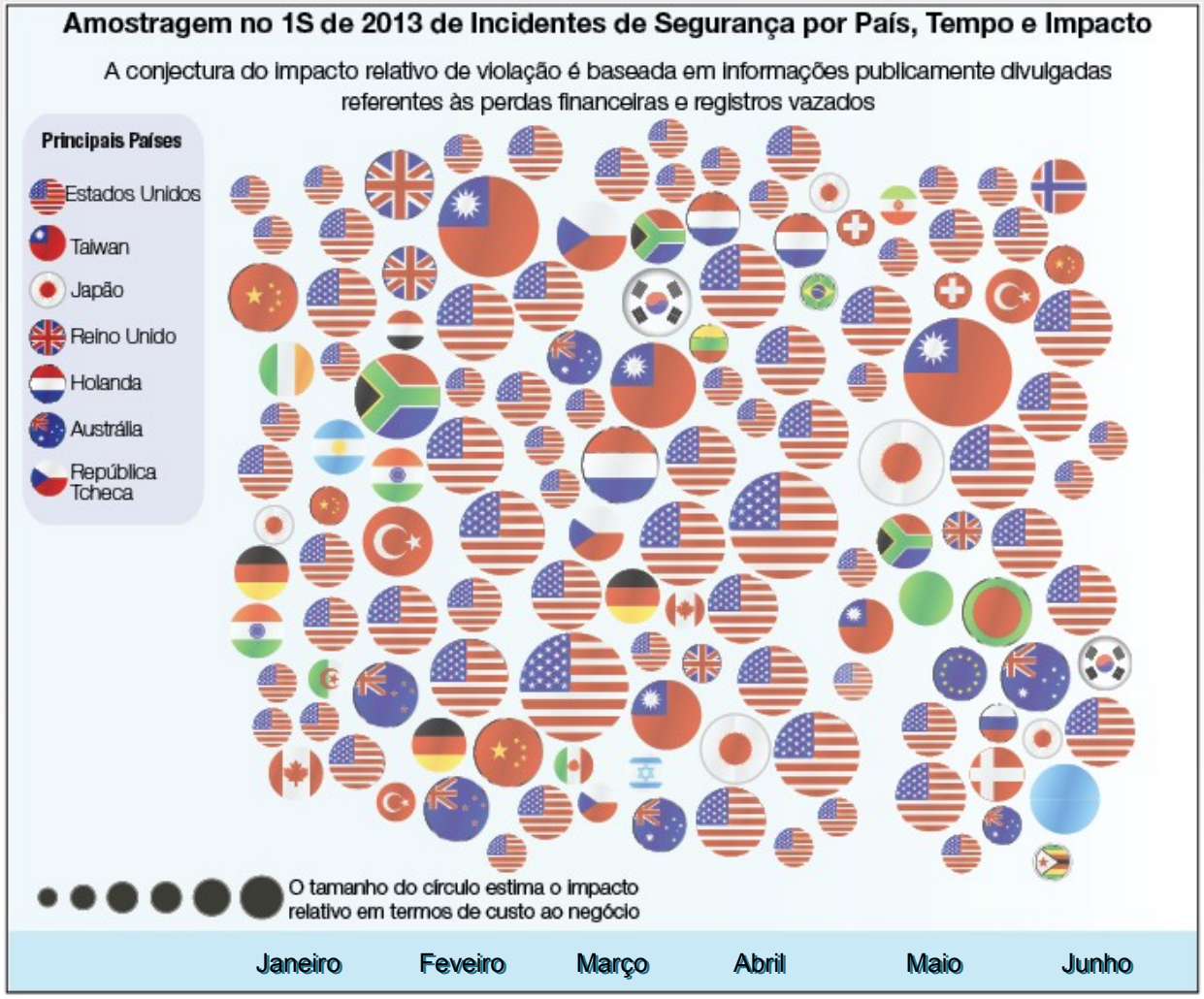
Marcas globais visadas em países estrangeiros fora da matriz

Invasores dependem de

- **Segurança mais baixa em sites de idioma local**
- **Microsites temporários que reúnem dados de usuários**
- **Denegrir marcas com caminho de menor resistência**

Incidentes por Localização

países mais impactados pelos incidentes de segurança



Os Estados Unidos divulgaram mais locais-alvo de violação

Taiwan foi o alvo em vários incidentes de segurança de filiais estrangeiras

3 Capítulos do Relatório de Tendências

Ataques dirigidos e violação de dados

Social e Mobilidade

- Visar usuários e abusar da confiança
- Impacto econômico e reputacional
- Mercado Negro das mídias sociais
- Avanços recentes em malware de Android

X-Force em Números

Mídia Social

tornou-se o novo "playground" para invasores

As Mídias Sociais são o principal alvo para ataques e os dispositivos móveis estão expandindo tais alvos

- Captação de inteligência pré-ataque
- Criminosos vendendo contas
- Campanhas atraindo o usuário a clicar em links maliciosos

Impacto Econômico e Reputacional

como a adoção generalizada promove tanto a pessoa quanto o negócio

Em vez de bloquear serviços, as organizações deveriam determinar como monitorar e reduzir os abusos destas plataformas

- As explorações das Mídias Sociais podem produzir impactos sobre a perda financeira e sobre a marca

- A defesa eficaz é a educação e a produção de suspeitas

Ameaças da Mobilidade

em qualquer lugar que vá, os invasores o seguirão

Crescimento excessivo do mercado para Android chama a atenção dos autores de malware

Alvos viáveis com mira especialmente em organizações específicas

ROI: Os autores de malwares estão redobrando esforços na criação de malwares que são mais resilientes e perigosos.

Avanços em Malware de Android

Chuli

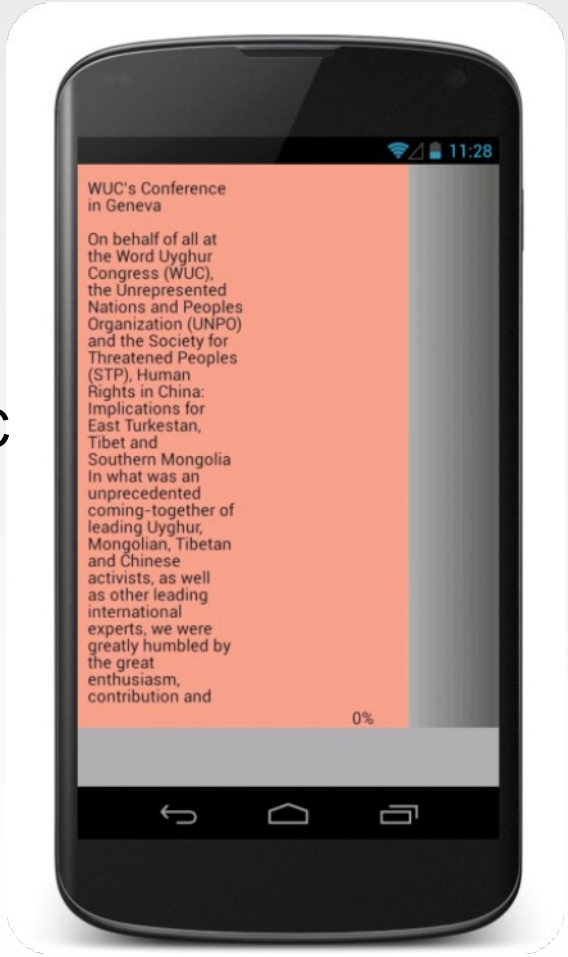
Ataque com alvos bastante específicos

- Lista de endereços comprometida
- Emails enviados aos alvos
- Vínculos com serviço SMS de Android
- Mensagens roteadas ao servidor remoto C&C

Obad

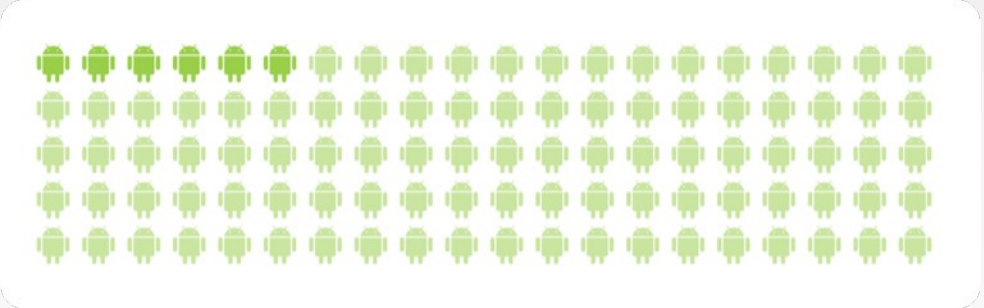
Difundido principalmente via spam de SMS

- Difusão por meio de Bluetooth
- Administração do dispositivo
- Técnicas de antianálise
- Ofuscação do código



O X-Force prevê que o número de aplicativos de malware de Android continue subindo

Grau de sofisticação
para este malware que, eventualmente, competirá com aqueles encontrados no malware de desktop



Aperfeiçoamentos de Segurança de Android
Dispositivos mais antigos estão mais em risco, com 6% executando a versão mais recente

A fragmentação de SO (Sistema Operacional) continuará como um problema

3 Capítulos do Relatório de Tendências

Ataques dirigidos e violação de dados

Social e Mobilidade

X-Force em Números

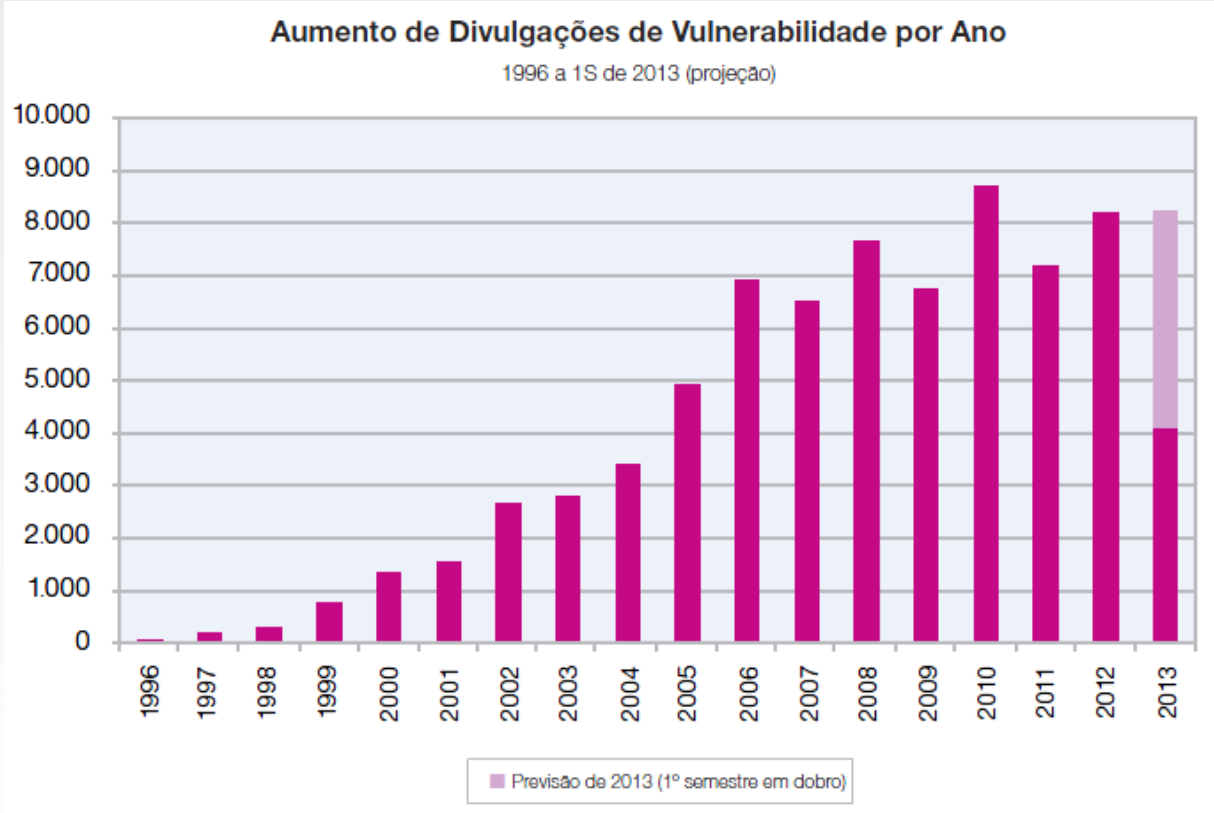
- Vulnerabilidades
- Explorações
- Tendências da Web
- Spam e Phishing

Divulgações de Vulnerabilidades

4.100

vulnerabilidades divulgadas publicamente

Se a tendência continuar, provavelmente, será a mesma que a de 2012



Fonte: IBM X-Force Research and Development

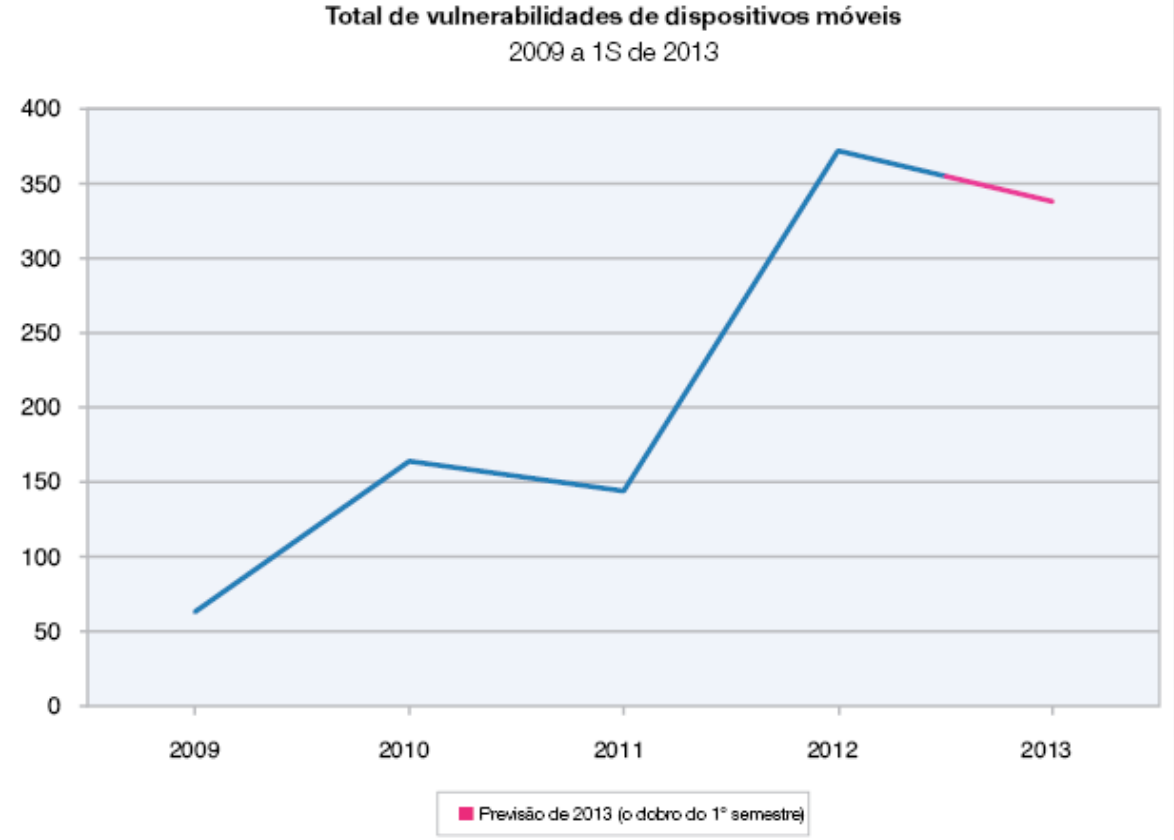
Vulnerabilidades afetando Software Móvel

Vulnerabilidades de dispositivos móveis

vêm aumentando desde 2009

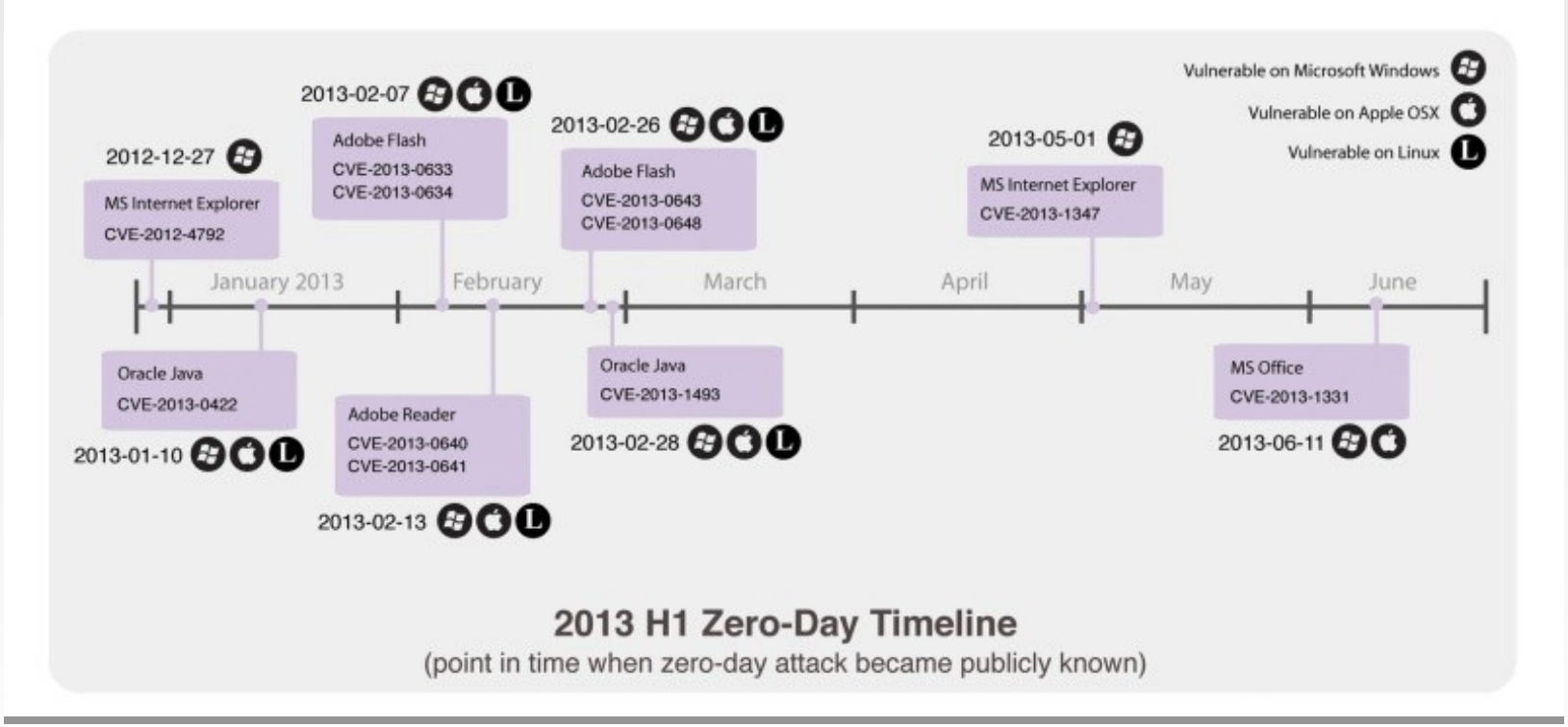
Embora ainda seja pequena a porcentagem total geral

Afetando tanto software de dispositivo móvel quanto de desktop



Fonte: IBM X-Force Research and Development

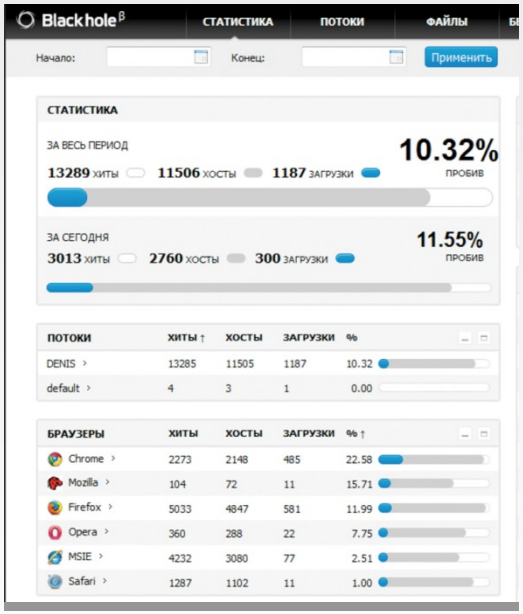
Vunerabilidades de "Dia-Zero"



80% do “dia-zero”

(80% das vulnerabilidades de "dia-zero") afetam Windows e OSX

Oracle Java, Adobe Flash e Microsoft IE
são cruciais para proteção e correção



Como fazer melhor:

- Reduza a superfície de ataque
- Atualize o software instalado
- Obtenha todas as informações sobre spear-phishing

Java

- "Dia-zero" rapidamente é utilizado nos kits de ferramentas de exploração
- Atualizações recentes permitem que "desabilite" o java
- Configurações de segurança padrão são agora "avançadas"

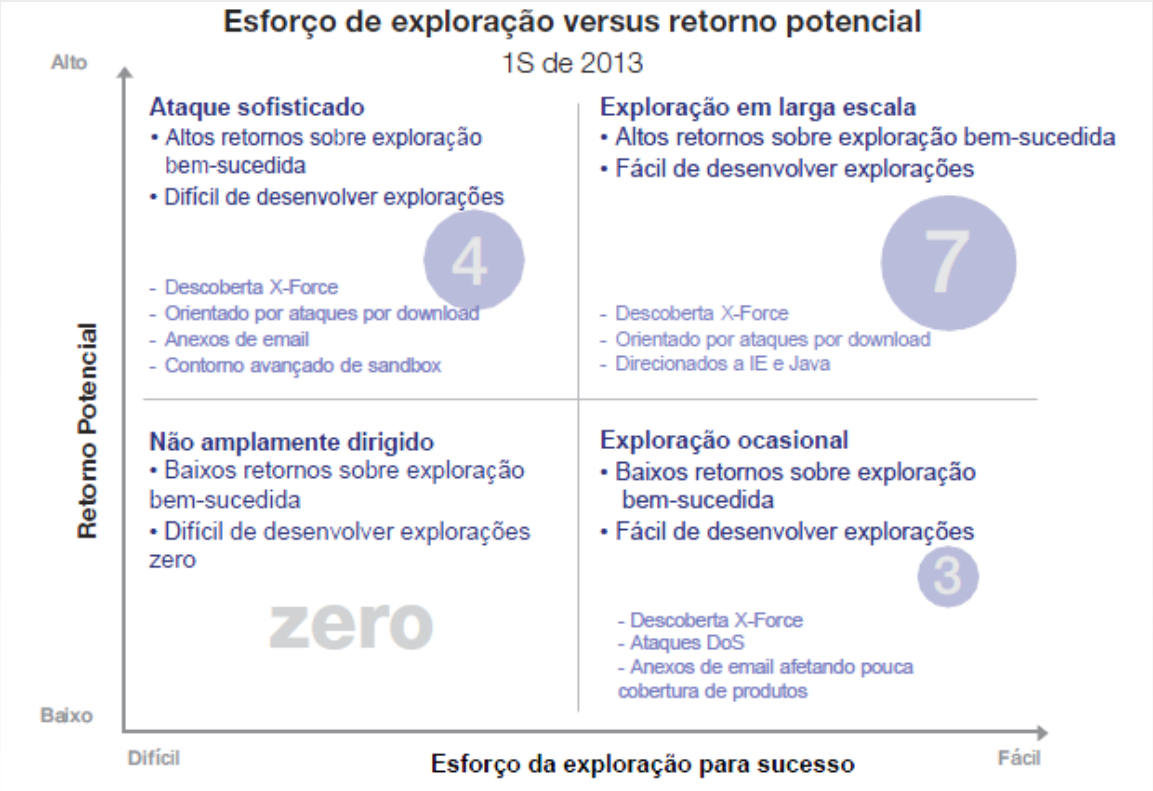
Adobe Flash

- Método mais comum de entrega, desde o sandbox Reader de 2010, é através de documentos MS Office

Microsoft Internet Explorer

- Ataques com alvos bastante específicos e técnica "water hole"

Esforço de Exploração versus Recompensa Potencial



Drive-by-downloads

IE e Java direcionados

Exploração fácil
com alto potencial de recompensa – ainda o ponto central

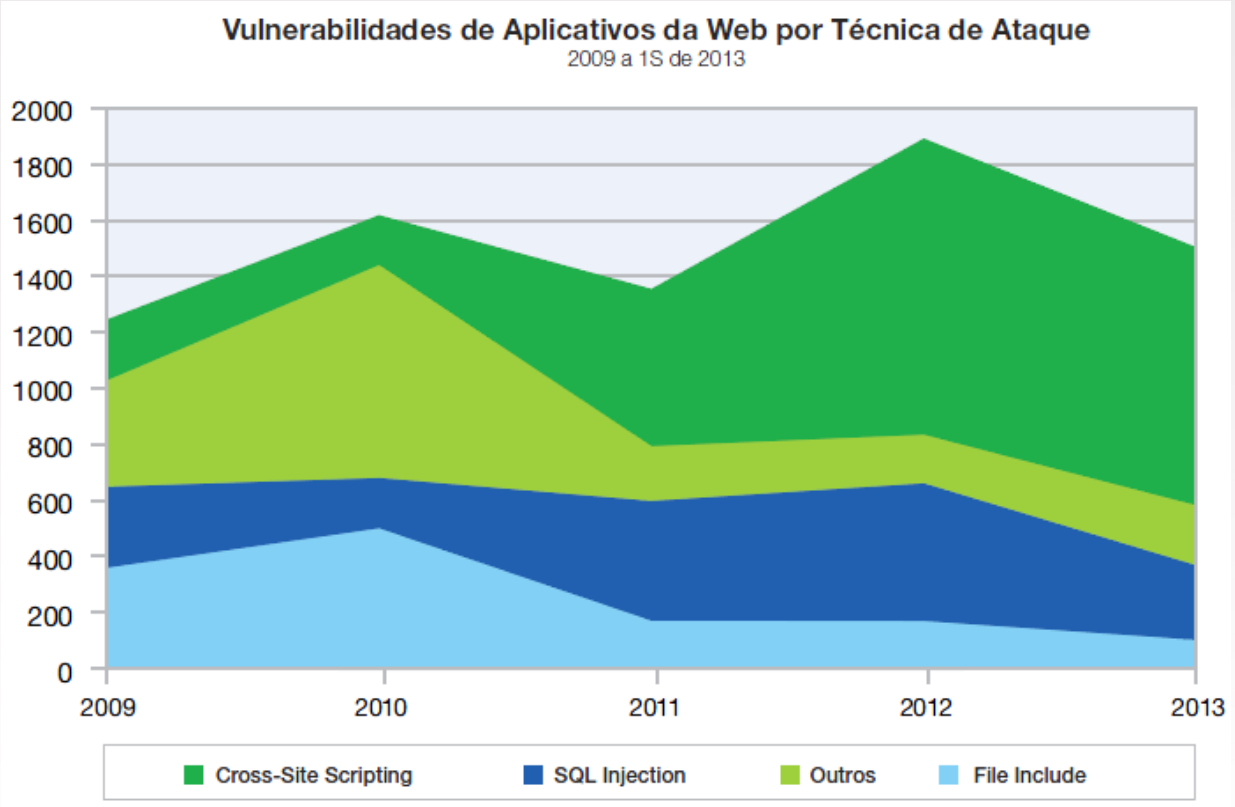
Fonte: IBM X-Force Research and Development

Vulnerabilidades em Aplicativos da Web

50%

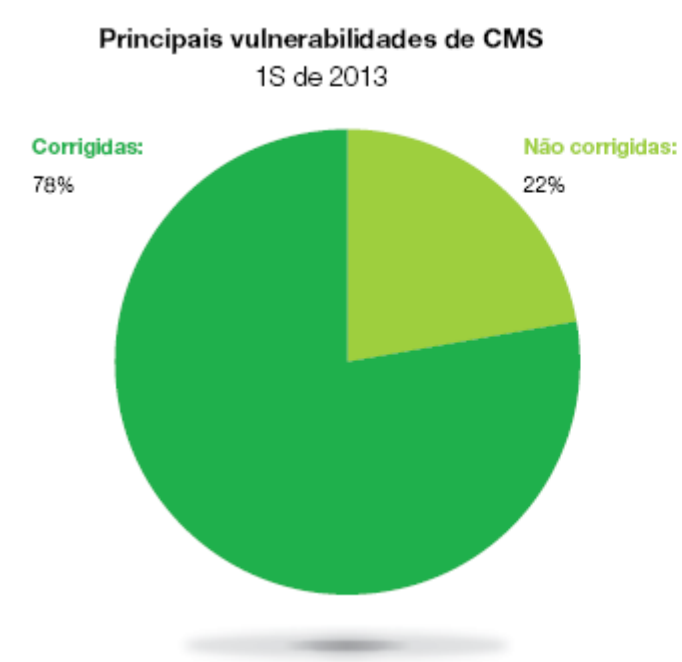
de todas as vulnerabilidades em aplicativos da web são de XSS

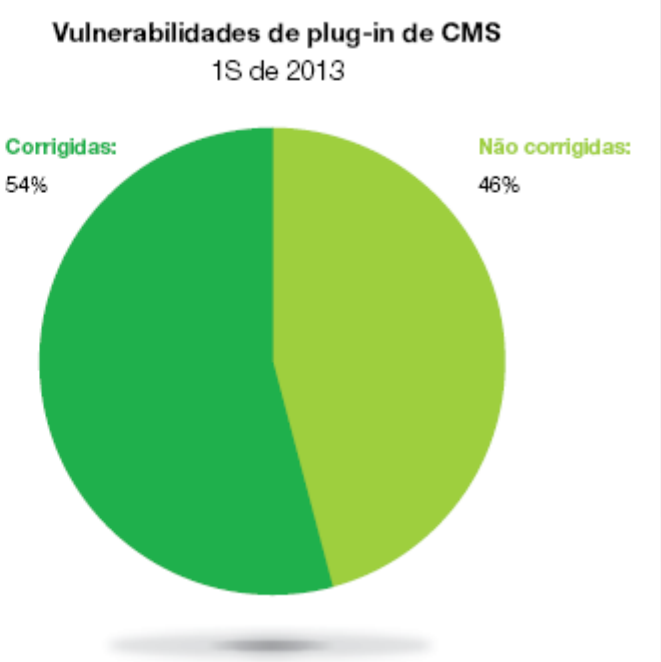
Redução relativa do total em comparação a 2012



Fonte: IBM X-Force Research and Development

Plug-ins do Sistema de Gerenciamento de Conteúdo continuam fornecendo alvos não tangíveis





Os invasores sabem que os fornecedores de CMS prontamente resolvem e corrigem suas exposições

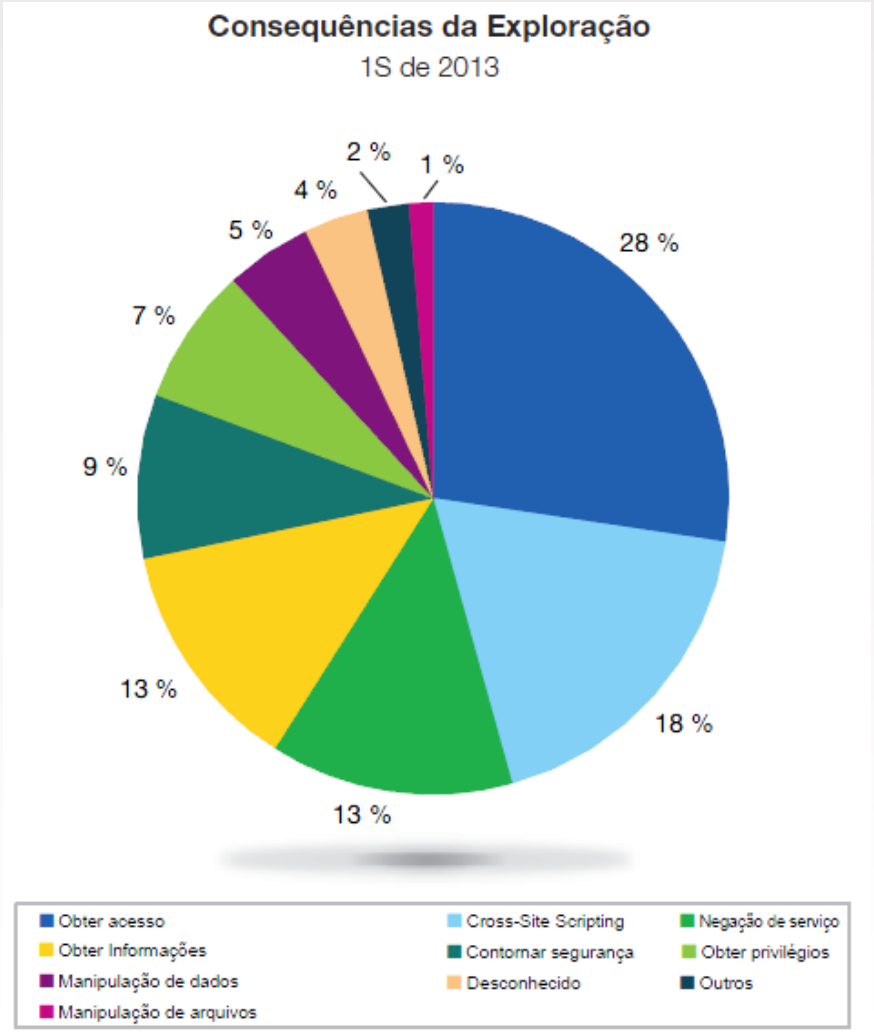
Comparado às organizações menores e pessoas que produzem plug-ins e complementos

Consequências da Exploração

28%

“obtem acesso”

Fornece ao invasor controle completo do sistema para roubar dados ou iniciar outros ataques



Fonte: IBM X-Force Research and Development

Alvos de Phishing e Fraudes

55%

são de links e anexos ruins

- Redes Sociais
- Pagamento / lojas
- Scanners / Fax

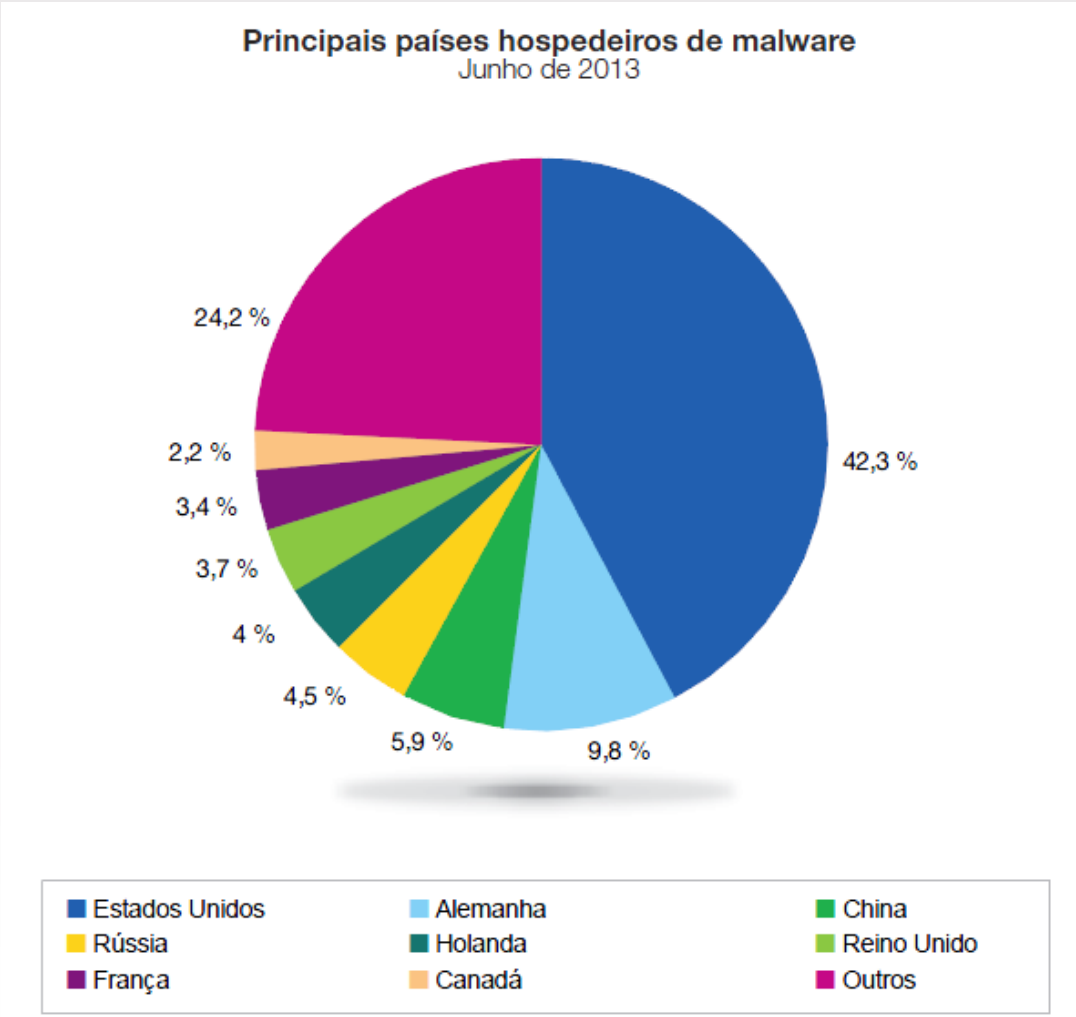
Fonte: IBM X-Force Research and Development

Hospedagem de malware

42%

são malwares distribuídos nos EUA

Alemanha em segundo com aproximadamente 10%



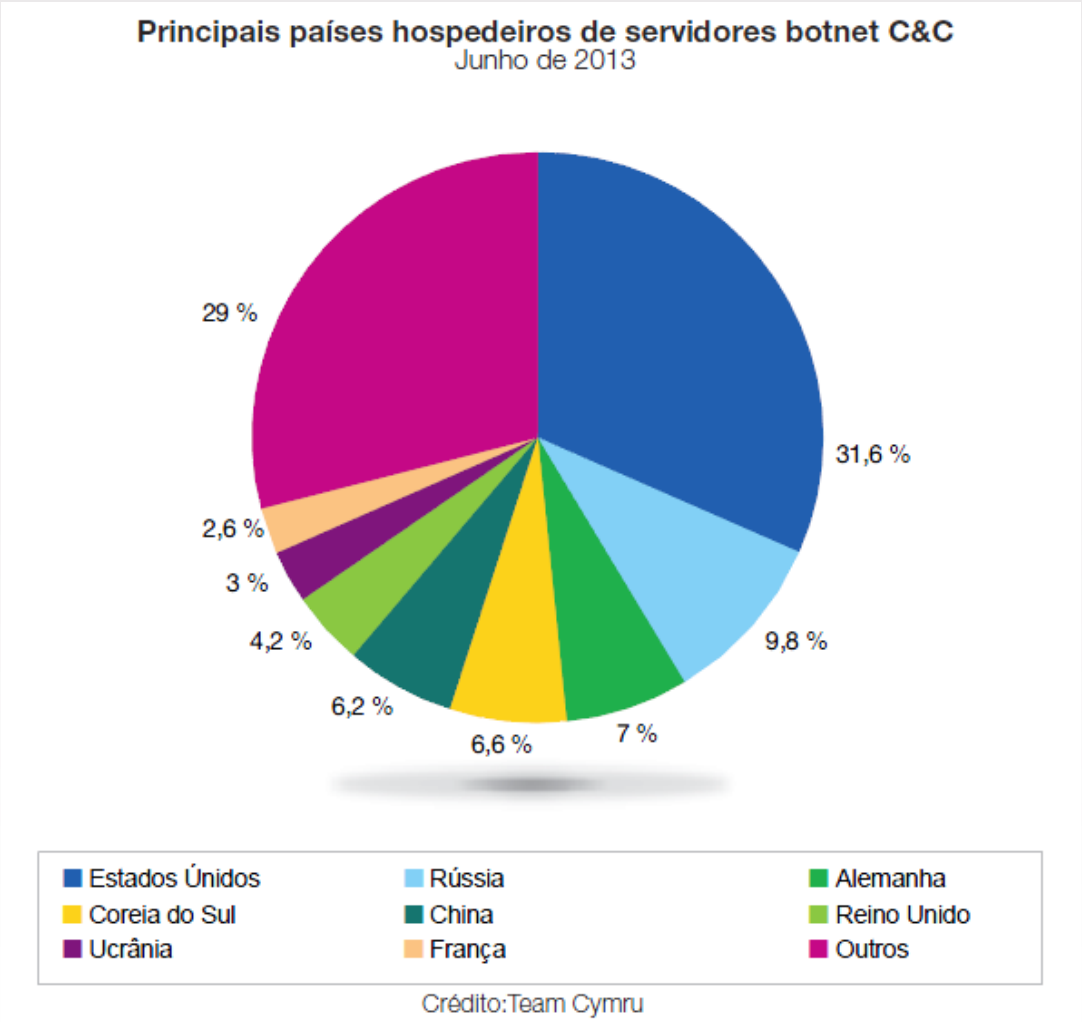
Fonte: IBM X-Force Research and Development

Controle de Hospedagem e Comando de Botnet

32%

são de servidores de botnet C&C nos EUA.

Rússia está em segundo com aproximadamente 10%



Fonte: IBM X-Force Research and Development

Principais conclusões para CISOs

Não se esqueça dos conceitos básicos
varredura, correção, configurações e senhas

Defesa Social necessita de Socialização
instruir usuários e produzir suspeitas

Desfragmente o seu Dispositivo Móvel
aplique constantemente atualizações e revise as políticas de BYOD

Otimize antes dos Invasores
identifique ativos problemáticos, analise comportamentos e localize anomalias

Declaração de Práticas Adequadas de Segurança: O sistema de segurança de TI envolve a proteção de sistemas e informações através de prevenção, detecção e resposta ao acesso incorreto de dentro e fora de sua empresa. O acesso incorreto pode resultar na alteração, destruição ou desapropriação de informações, ou pode resultar em danos ou uso impróprio de seus sistemas, inclusive para atacar terceiros. Nenhum produto ou sistema de TI deve ser considerado completamente seguro e nenhum produto único ou medida de segurança pode ser totalmente eficaz na prevenção de acesso incorreto. Os sistemas e produtos IBM foram projetados para fazer parte de uma abrangente abordagem de segurança, que necessariamente envolverá procedimentos operacionais adicionais e pode exigir que outros sistemas, produtos ou serviços se tornem mais efetivos. A IBM NÃO GARANTE QUE OS SISTEMAS E PRODUTOS SEJAM IMUNES À CONDUTA ILEGAL OU MALICIOSA DE QUALQUER PARTE.

Obrigado

www.ibm.com/security