

Crimes Cibernéticos

24/09/2015

FEBRABAN

Federação Brasileira de Bancos

Contexto

 Cenário – expansão dos meios digitais

 Volumes *Internet Banking*

Crimes Cibernéticos

 Principais tipos de crimes cibernéticos

 Como as fraudes acontecem

 Mecanismos de prevenção e combate

Gestão de Consequências

 Responsabilização e parcerias com Agentes Públicos

Contexto

 **Cenário – expansão dos meios digitais**

 *Volumes Internet Banking*

Crimes Cibernéticos

 Principais tipos de crimes cibernéticos

 Como as fraudes acontecem

 Mecanismos de prevenção e combate

Gestão de Consequências

 Responsabilização e parcerias com Agentes Públicos



Mais de 110 milhões acesso à internet

Fonte: Internet World Stats / 2014

O país que passa mais tempo conectado da América Latina

Fonte: comScore Media Metrix



Mais de 79 milhões acesso mobile

Fonte: Social Web Index / Jan 2015

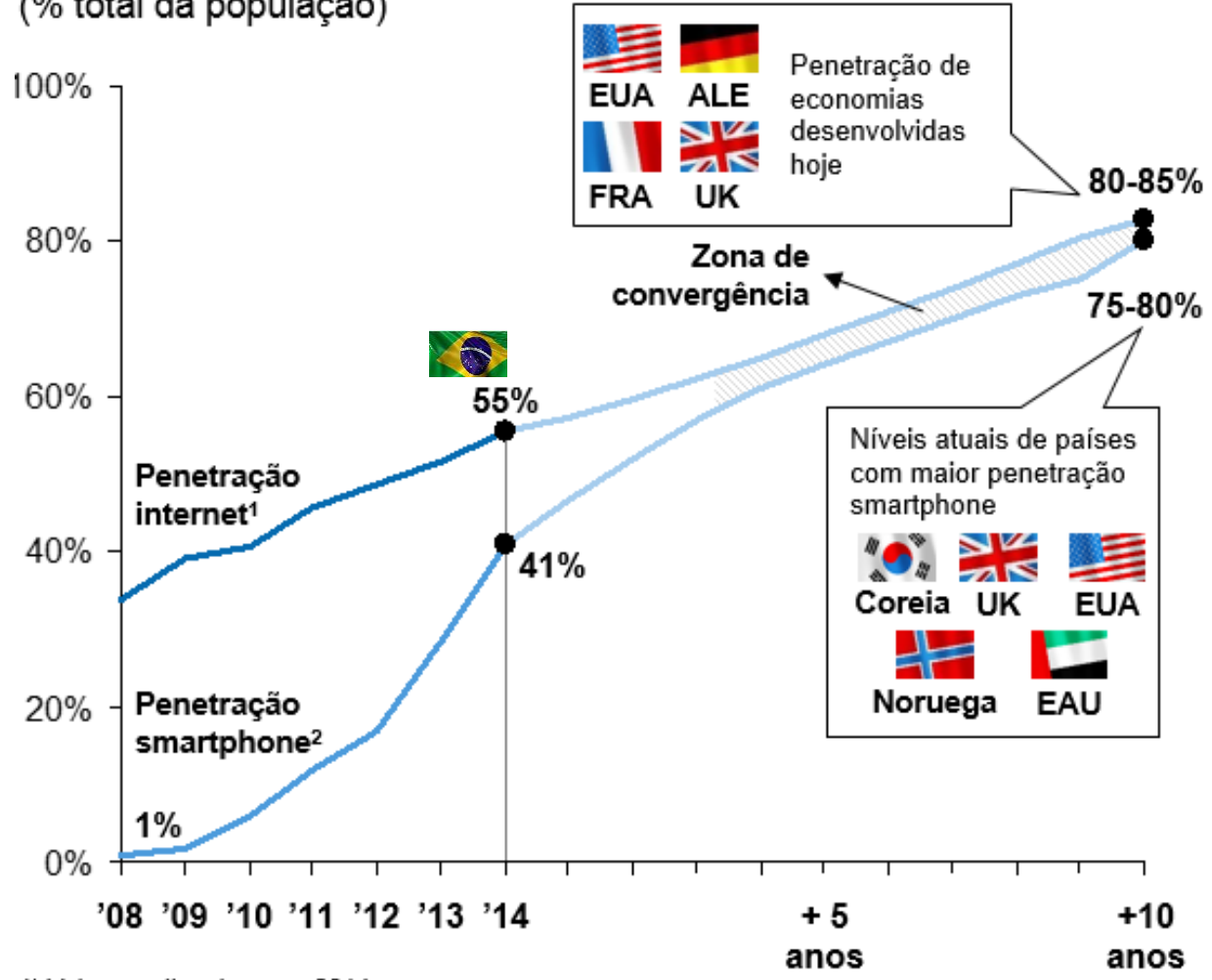
Mais de 1 celular por habitante no Brasil

Fonte: comScore Media Metrix

Expansão dos Meios Digitais no Brasil

Penetração de Acesso a Internet e Smartphones

(% total da população)



- Mais da metade da população (55%) tem acesso a internet, e a penetração de **smartphone continua apresentando crescimento importante, atingindo 41% em 7 anos**
- **Brasil pode atingir níveis de penetração de internet e smartphones de países desenvolvidos em até 10 anos**

1) Valores estimados para 2014

2) Considera a penetração de pessoas com acesso a smartphones

Fonte: Banco Mundial, International Telecommunication Union, World Telecommunication/CT, Cetic, IPC Target, Análises Strategy&

Contexto



Cenário – expansão dos meios digitais



Volumes *Internet Banking*

Crimes Cibernéticos



Principais tipos de crimes cibernéticos



Como as fraudes acontecem



Mecanismos de prevenção e combate

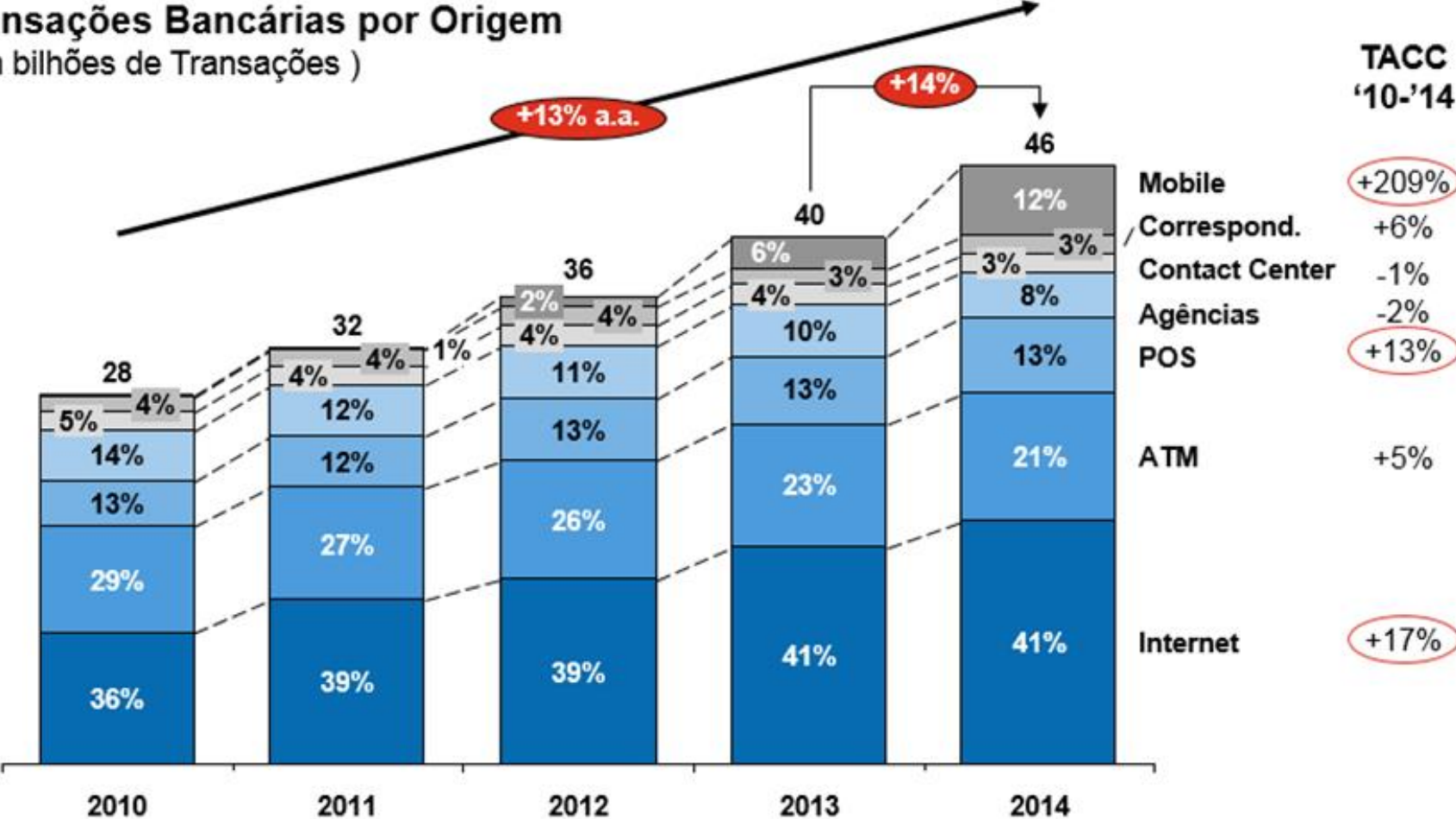
Gestão de Consequências



Responsabilização e parcerias com Agentes Públicos

Volumes Internet Banking

Transações Bancárias por Origem
(Em bilhões de Transações)



Fonte: Pesquisa FEBRABAN de Tecnologia Bancária 2014; Análises Strategy&

i Volume de contas e transações *i* Tipo de transação

Contexto

 Cenário – expansão dos meios digitais

 Volumes *Internet Banking*

Crimes Cibernéticos

 **Principais tipos de crimes cibernéticos**

 Como as fraudes acontecem

 Mecanismos de prevenção e combate

Gestão de Consequências

 Responsabilização e parcerias com Agentes Públicos

Principais Tipos de Crimes Cibernéticos

Ameaças

Fraudes financeiras

- Fraudes ocorrem na máquina do cliente.
- Métodos mais comuns (detalhamento a seguir):
 - *Man-in-the-middle*
 - *Man-in-the-browser*
 - Engenharia social

Ataques de indisponibilidade e contra a reputação (“Hacktivismo”)

- **Ataques de Negação de Serviço – DDoS (*Distributed Denial of Service*)**
 - Visam a indisponibilidade do serviço ao usuário.
- **Pichação – *Defacement***
 - Visam a alteração do conteúdo de um *site*.

Roubo ou vazamento de informações

- Tentativas de Invasão ao ambiente de empresas e Instituições Financeiras, com o objetivo de roubar informações.

Contexto

 Cenário – expansão dos meios digitais

 Volumes *Internet Banking*

Crimes Cibernéticos

 Principais tipos de crimes cibernéticos

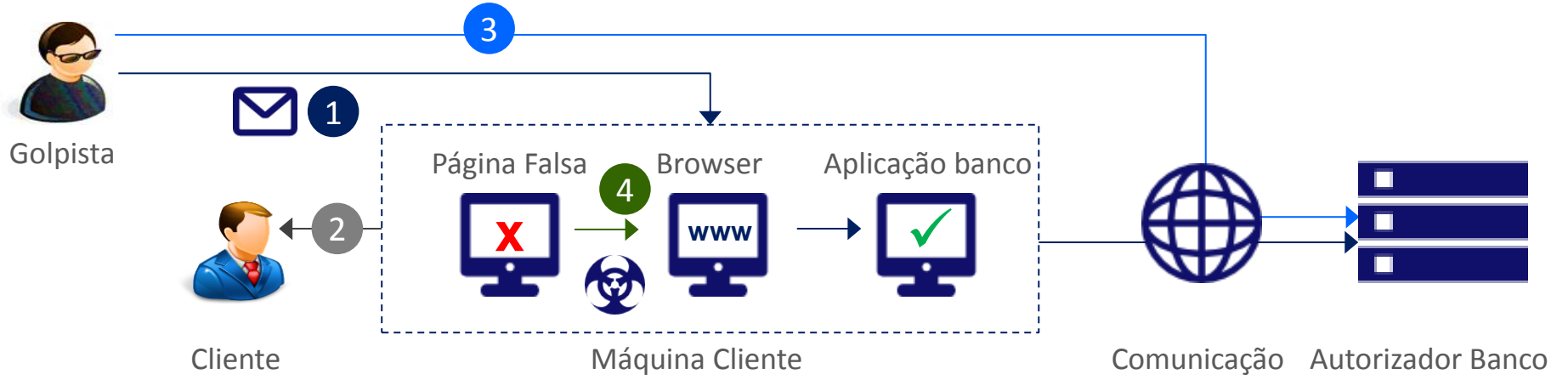
 **Como as fraudes acontecem**

 Mecanismos de prevenção e combate

Gestão de Consequências

 Responsabilização e parcerias com Agentes Públicos

Como as Fraudes Acontecem



1. Man-in-the-middle

1. Infecção

- Golpista envia *email* com programa malicioso
- Cliente abre email e executa *link* inadvertidamente
- *Malware* é instalado na máquina do cliente

2. Captura de informações

- Ao tentar acessar a aplicação do Banco, *malware* direciona o Cliente para página falsa
- Ele preenche seus dados pessoais e senhas nesta página
- Página redireciona as informações ao golpista

3. Execução

- De posse das informações do cliente, golpista acessa aplicação do Banco na sua máquina
- Golpista executa as transações a partir da sua máquina

4. Execução: Variante + Sofisticada

- Ao invés de enviar as informações do Cliente ao Golpista, *malware* abre a aplicação do Banco automaticamente
- *Malware* executa automaticamente as transações fraudulentas, a partir da máquina do Cliente.

Como as Fraudes Acontecem



Golpista



2. Man-in-the-browser

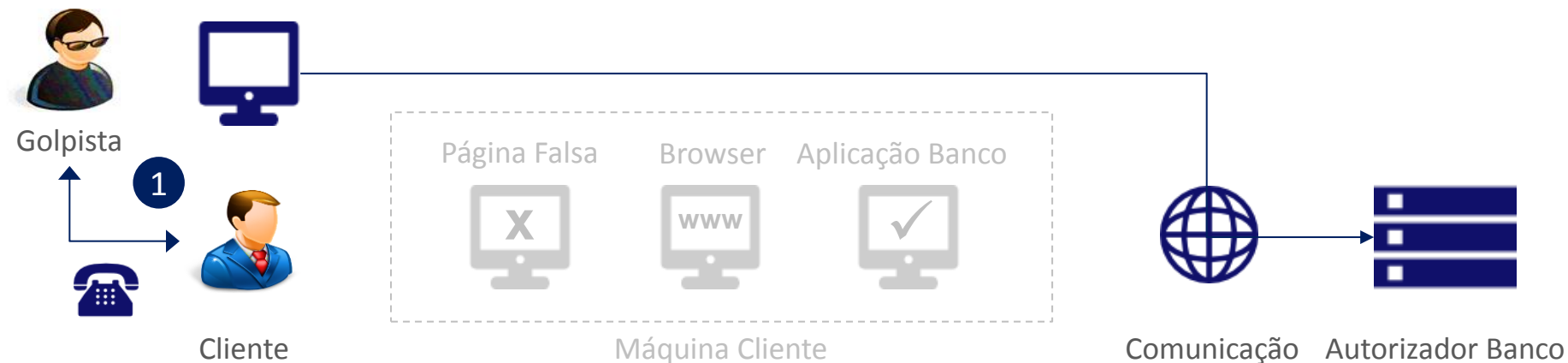
Infecção

- Golpista envia *email* com programa malicioso
- Cliente abre email e executa *link* inadvertidamente
- *Malware* é instalado na máquina do cliente

1. Execução (infecção permanece a mesma)

- Cliente acessa a aplicação verdadeira do Banco
- Quando o Cliente executa uma transação (por exemplo, pagamento de um boleto), *malware* é acionado e adultera as informações originais, substituindo-as por outras (por exemplo, adulteração de beneficiário e do valor)
- Banco recebe e processa a transação adulterada.

Como as Fraudes Acontecem



3. Engenharia Social

Infecção

- Golpista envia *email* com programa malicioso
- Cliente abre email e executa *link* inadvertidamente
- *Malware* é instalado na máquina do cliente

1. Execução (infecção permanece a mesma)

- De posse das informações pessoais e senhas, Golpista entra em contato com o cliente (por exemplo, por telefone), e solicita informações adicionais (por exemplo, código do Token)
- Após obter informações, Golpista executa fraude a partir da sua máquina.

Contexto

 Cenário – expansão dos meios digitais

 Volumes *Internet Banking*

Crimes Cibernéticos

 Principais tipos de crimes cibernéticos

 Como as fraudes acontecem

 **Mecanismos de prevenção e combate**

Gestão de Consequências

 Responsabilização e parcerias com Agentes Públicos

Mecanismos de Prevenção e Combate



1. Autenticação

Dispositivos Seguros de autenticação

- Senha Eletrônica (exclusiva para uso na internet)
- Senha do Cartão (para validação de transações realizadas)
- Teclado virtual
- Token / Bingocard
- Canal cruzado
- Confirmação de transações

Proteções continuamente testadas

Mecanismos de Prevenção e Combate



2. Preventivo

- Antecipação de riscos
- Plug-in
- Sistemas de proteção contra “malware” – anti-vírus
- Identificação de máquina

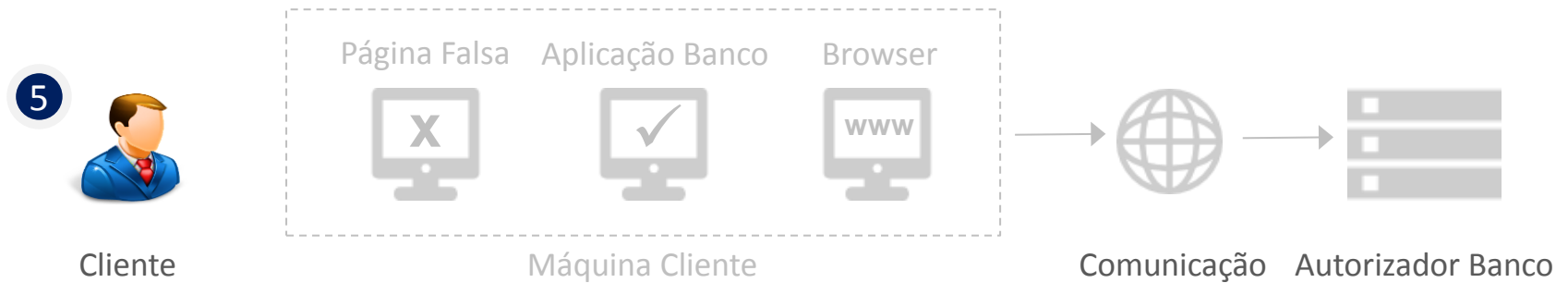
3. Proteção

- Criptografia

Proteções continuamente testadas

4. Processos

- Monitoramento e denúncia de páginas falsas
- Monitoramento de atipicidades (financeiras e comportamentais)
- Certificação Digital por institutos independentes
- Canais e acesso de confirmação de transações pelo cliente



5. Conscientização

Programas de comunicação e orientação aos clientes

- **Guia de segurança Febraban**

Recomendações aos clientes sobre a escolha da senha, uso da internet com segurança e recebimento de e-mails maliciosos.

- **Ações digitais**

Alerta aos clientes através das instituições financeiras, sobre os procedimentos de segurança, através de canais digitais como:

- Dia mundial da Internet Segura
- E-mail de orientação
- Pop-ups com dicas de segurança
- Homepage com orientações de segurança
- SMS de confirmação de transações
- Redes Sociais (facebook e twitter)

Contexto

 Cenário – expansão dos meios digitais

 Volumes *Internet Banking*

Crimes Cibernéticos

 Principais tipos de crimes cibernéticos

 Como as fraudes acontecem

 Mecanismos de prevenção e combate

Gestão de Consequências e Oportunidades

 Responsabilização e parcerias com Agentes Públicos

Ações

Responsabilização

- **Responsabilização de Beneficiários**
 - Identificação dos beneficiários de valores originados em fraudes
 - Encerramento da conta e adoção de medidas legais cabíveis

Parcerias com Órgãos Públicos

- **Oportunidades**
 - Reconhecimento da autenticação digital na formalização de contratações e movimentações financeiras eletrônicas
 - Impossibilidade de cancelamento das consequências das ocorrências de fraude (financeiras ou de regularização) envolvendo o pagamento de tributos Federais / Estaduais

Ações

Responsabilização

**Parcerias com Órgãos
Públicos**

- **Apuração de autoria**
 - Materialização de informações e evidências para suportar investigações policiais e detenções
- **Operações em parceria com a Polícia Federal**
 - **Operação Tentáculos:** compartilhamento de informações de fraude e beneficiários para correlação de eventos e identificação de autoria

OBRIGADO

FEBRABAN
Federação Brasileira de Bancos