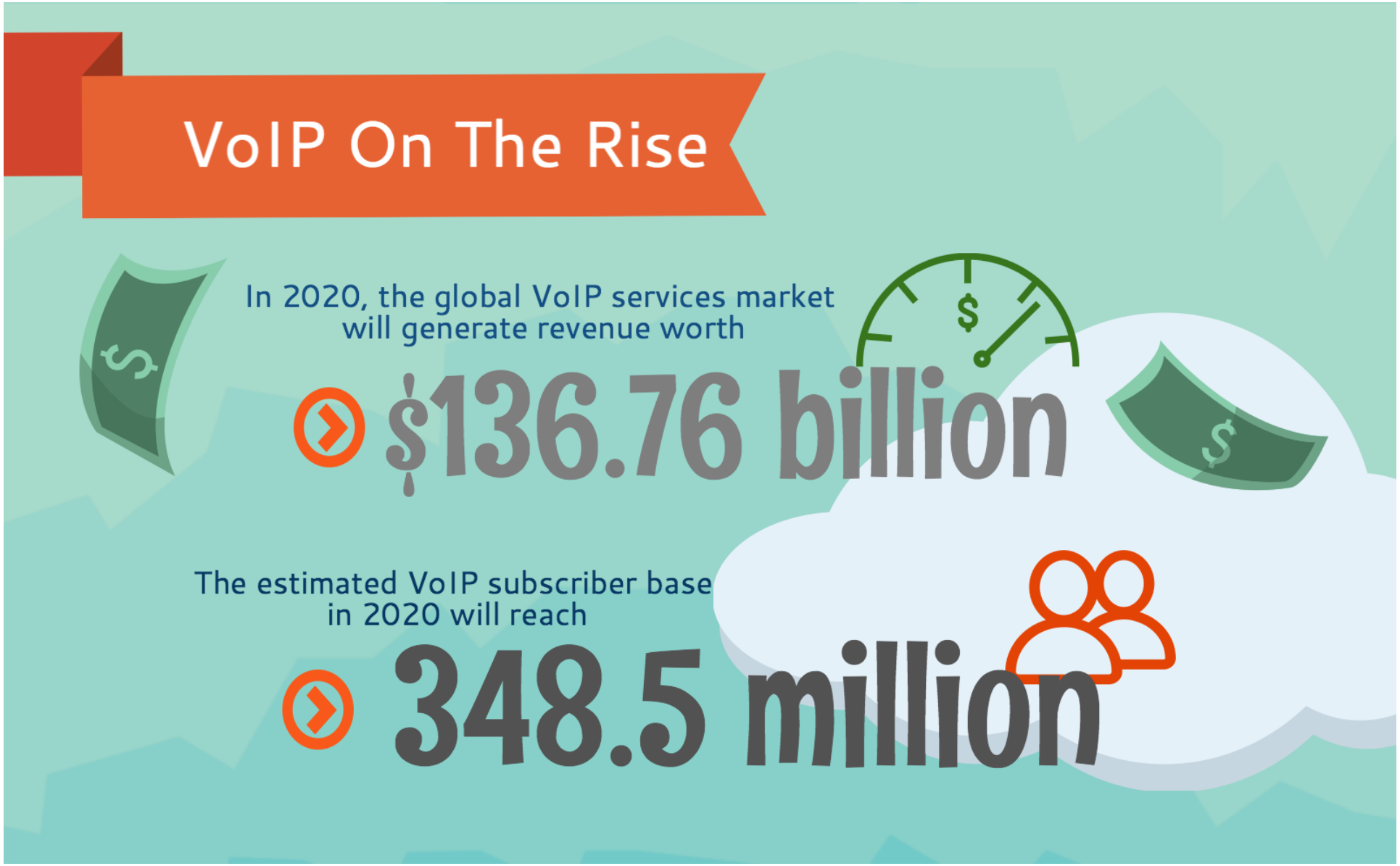
Fraude em Telefonia

Hermann Wecke

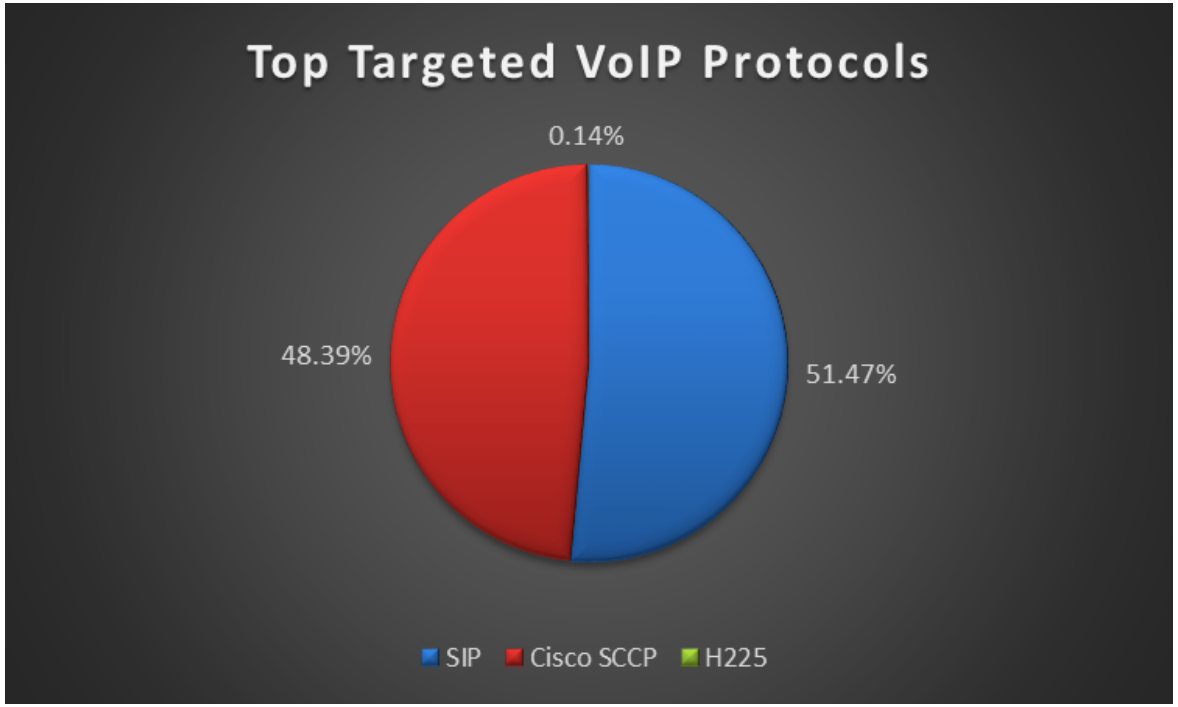
AVIVAVox



Fonte: Digium - Out/2015

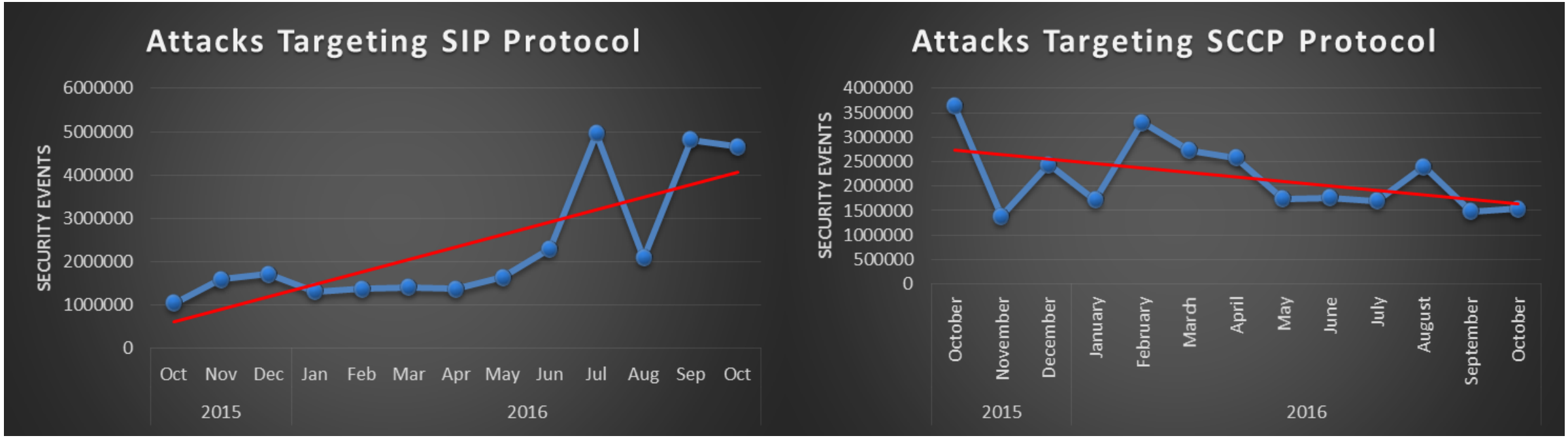
Ataques VoIP estão na moda

- Estudo da IBM mostra um aumento nos ataques contra serviços VoIP
- Do total de ataque, 51% são contra serviços SIP



Fonte: IBM Managed Security Services (Security Intelligence)

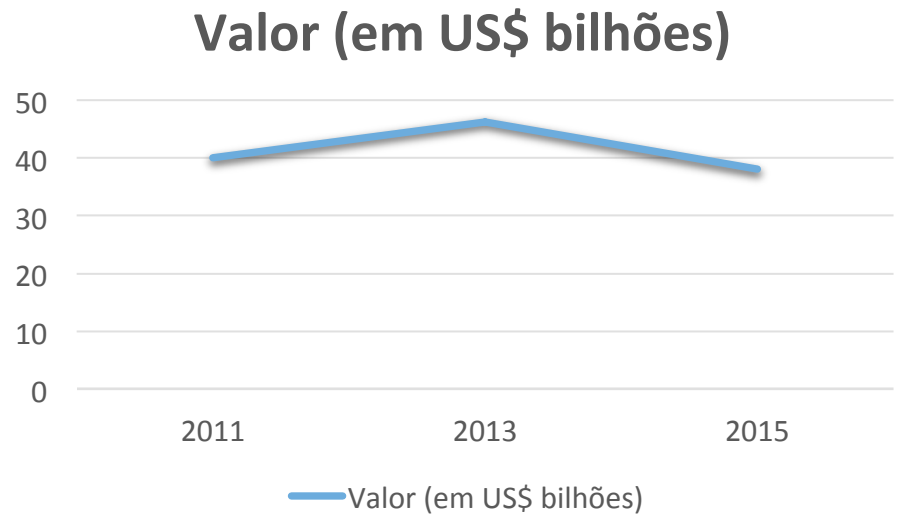
Ataques VoIP estão na moda



Fonte: IBM Managed Security Services (Security Intelligence)

Tamanho da Fraude

- US$ 38,1 bilhões em 2015
- US$ 46,3 bilhões em 2013
- US$ 40,1 bilhões em 2011



Fonte: CFCA – Communications Fraud Control Association – http://cfca.org/fraudlosssurvey

Tamanho da Fraude

- US$ 38,1 bilhões em 2015
  - Método:
    - US$ 3,93 bi – PBX
    - US$ 3,53 bi – IP PBX

Fonte: CFCA – Communications Fraud Control Association – http://cfca.org/fraudlosssurvey

Tamanho da Fraude

- US$ 38,1 bilhões em 2015
  - Método:
    - US$ 3,93 bi – PBX
    - US$ 3,53 bi – IP PBX
  - Tipo de Fraude:
    - US$ 10,76 bi – International Revenue Share Fraud (IRSF)
    - US$ 5,97 bi – Carrier Bypass (uso de serviços/equipamentos para evitar tarifação)
    - US$ 3,77 bi – Premium Rate Service

Fonte: CFCA – Communications Fraud Control Association – http://cfca.org/fraudlosssurvey

Anatomia da Fraude

International Revenue Share Fraud (IRSF)

- Scan para identificar servidor SIP
- Scan para identificar dialplan vulnerável
  - Incluindo todas as possíveis variações no dialplan, como o código de operadora de longa distância (CSP) e eventuais códigos de acesso da linha externa
- Confirmado o sucesso, testar novamente para uma rota possível de IRSF
- Inflar o valor da rota para valores absurdos (acima de US$ 5/minuto)
- Gerar tráfego até o limite do possível no servidor-vítima
- Correr para o banco e sacar o dinheiro

Anatomia da Fraude (IRSF)

Possíveis variações no dialplan

nic.br Núcleo de Informação e Coordenação do Ponto BR — cert.br 15 anos

Análise dos Dados (cont.)

Identificar o destino das ligações

Redundância dos números solicitados:

```
2011-09-26 19:21:55 -0300: sip2db.pl[9814]:  00149725*****586
2011-09-26 19:21:55 -0300: sip2db.pl[9814]: 000149725*****586
2011-09-26 19:21:55 -0300: sip2db.pl[9814]:  00159725*****586
2011-09-26 19:21:55 -0300: sip2db.pl[9814]:  00219725*****586
2011-09-26 19:21:55 -0300: sip2db.pl[9814]:  00219725*****586
2011-09-26 19:21:55 -0300: sip2db.pl[9814]:  00319725*****586
2011-09-26 19:21:55 -0300: sip2db.pl[9814]:      9725*****586
2011-09-26 19:21:55 -0300: sip2db.pl[9814]:  00219725*****586
                                             <----------|
                          Longest substring:      9725*****586

                          9725*****586|972|5*****586|IL|Israel

                             biblioteca Number::Phone::Country
```


cgi.br

International Revenue Share Fraud (IRSF)

28% OF THE GLOBAL FRAUD LOSSES CAN BE ATTRIBUTED TO IRSF.

THE AVERAGE LATENCY BETWEEN TEST CALLS AND THE ARTIFICIAL INFLATION OF TRAFFIC IN AN IRSF ATTACK 37 MINUTES

Fonte: fraudstrike.com

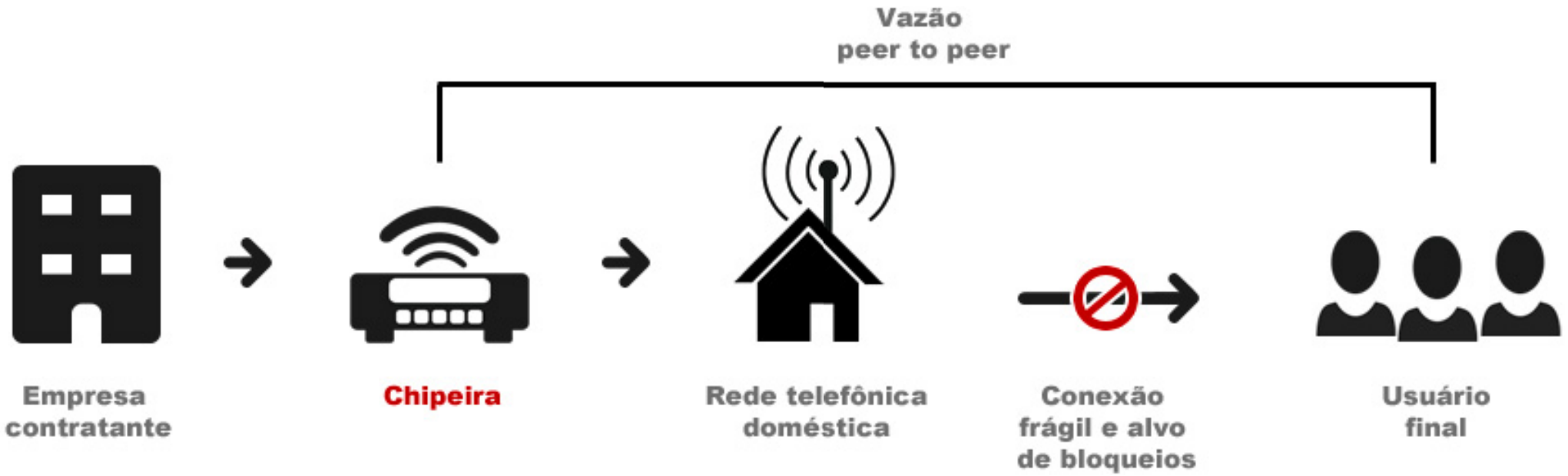
Tamanho da Fraude

- US$ 38,1 bilhões em 2015
  - Método:
    - US$ 3,93 bi – PBX
    - US$ 3,53 bi – IP PBX
  - Tipo de Fraude:
    - US$ 10,76 bi – International Revenue Share Fraud (IRSF)
    - US$ 5,97 bi – Carrier Bypass (uso de serviços/equipamentos para evitar tarifação)
    - US$ 3,77 bi – Premium Rate Service

Fonte: CFCA – Communications Fraud Control Association – http://cfca.org/fraudlosssurvey

Carrier Bypass

Carrier Bypass



SMS Pirata (“chipeira”)

Fonte: smspirata.com.br

Carrier Bypass

Tamanho da Fraude

- US$ 38,1 bilhões em 2015
  - Método:
    - US$ 3,93 bi – PBX
    - US$ 3,53 bi – IP PBX
  - Tipo de Fraude:
    - US$ 10,76 bi – International Revenue Share Fraud (IRSF)
    - US$ 5,97 bi – Carrier Bypass (uso de serviços/equipamentos para evitar tarifação)
    - US$ 3,77 bi – Premium Rate Service

Fonte: CFCA – Communications Fraud Control Association – http://cfca.org/fraudlosssurvey

Premium Rates

- Objetivo: Induzir o usuário a erro, orientando-o a ligar para um destino tarifado com um valor excessivo
- Diferente do IRSF, são serviços/destinos supostamente “legítimos”

Premium Rates

- Objetivo: Induzir o usuário a erro, orientando-o a ligar para um destino tarifado com um valor excessivo
- Diferente do IRSF, são serviços/destinos supostamente “legítimos”

Exemplos:

- Serviços 0900
- Telefones de suporte tarifado por chamada (comum no exterior)
- Assinaturas “forçadas” pelos fraudadores de serviços “premium” na telefonia celular, com conivência da operadora, com cobrança de valores extorsivos por semana (comum no Brasil, com celulares pré e pós pagos)

No Brasil, o serviço 0900 teve suas regras alteradas em Setembro/2016 pelo STJ, inibindo em parte a *“fraude característica”* do sistema.

Formas de ataque

Servidor

- Port Scan
- SIP Invite
- SIP Register
- Dialplan fraco/deficiente

Usuário

Formas de ataque

Servidor

- Port Scan
- SIP Invite
- SIP Register
- Dialplan fraco/deficiente

Usuário

- Furto de senha
- Reprogramação indevida
  - Destino Autorizado
  - Destino Indevido
- Senha default no telefone IP

Formas de ataque

Servidor

- Port Scan
- SIP Invite
- SIP Register
- Dialplan fraco/deficiente

Usuário

- Furto de senha
- Reprogramação indevida
  - Destino Autorizado
  - Destino Indevido
- Senha default no telefone IP
- Engenharia Social

Formas de ataque

Engenharia Social

- Golpes mais comuns:
  - “Oi Tio/Tia/Avô/Avó/Pai/Mãe”
  - Fui roubado
  - Sofri um acidente
  - Promoção “Caminhão do Gugu com patrocínio da ‘Nestrê’” (sic)
  - Aposentadoria (revisão), Montepio, Precatórios

- Voz ou SMS
  - Se for SMS, tentam “esconder” o telefone de origem junto do CSP

Formas de ataque

Servidor

- Port Scan
- SIP Invite
- SIP Register
- Dialplan fraco/deficiente

Usuário

- Furto de senha
- Reprogramação indevida
  - Destino Autorizado
  - Destino Indevido
- Senha default no telefone IP
- Engenharia Social
- Cold Call / Silent Call

Formas de ataque

Cold Call / Silent Call

- Utilizado para “varrer” um prefixo telefônico e identificar se o destino é voz, dados (modem), fax ou “linha morta”
- O resultado da varredura é vendido para golpistas

Formas de ataque

Cold Call / Silent Call

- Utilizado para “varrer” um prefixo telefônico e identificar se o destino é voz, dados (modem), fax ou “linha morta”
- O resultado da varredura é vendido para golpistas

NÃO CONFUNDIR com um servidor de chamada preditiva mal configurado!

Formas de ataque

Servidor

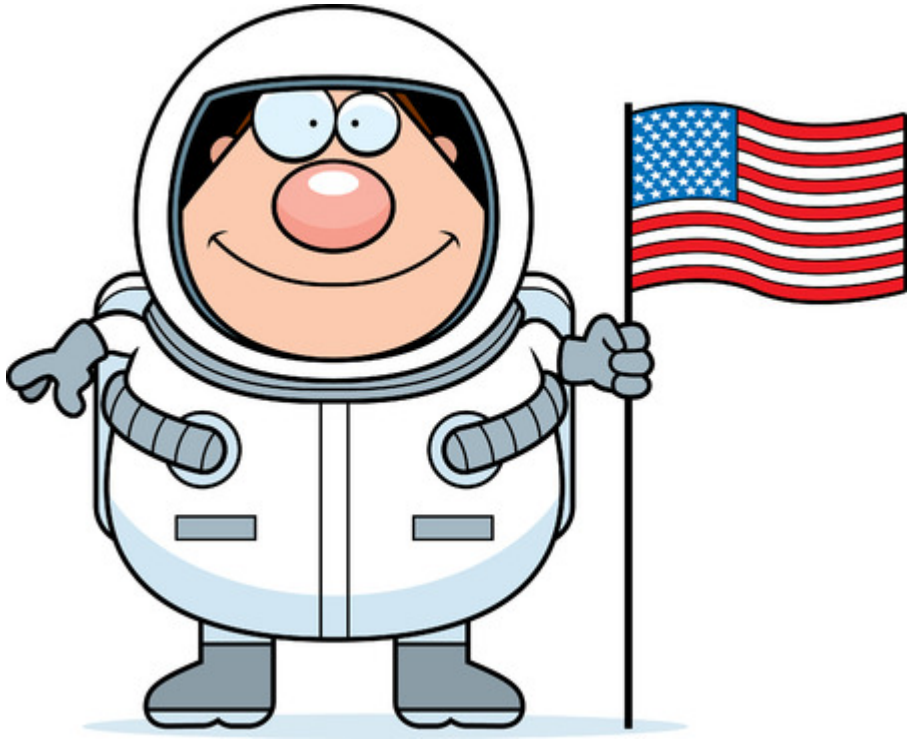
- Port Scan
- SIP Invite
- SIP Register
- Dialplan fraco/deficiente

Usuário

- Furto de senha
- Reprogramação indevida
  - Destino Autorizado
  - Destino Indevido
- Senha default no telefone IP
- Engenharia Social
- Cold / Silent Call
- Caller ID Spoofing

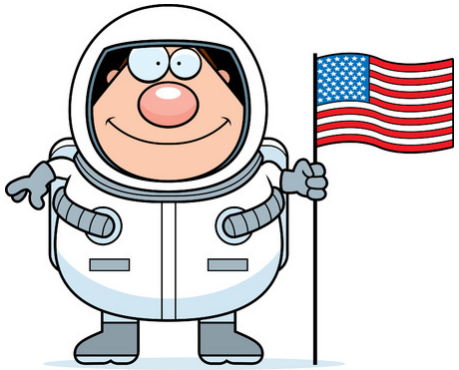
Formas de ataque

Caller ID Spoofing



Formas de ataque

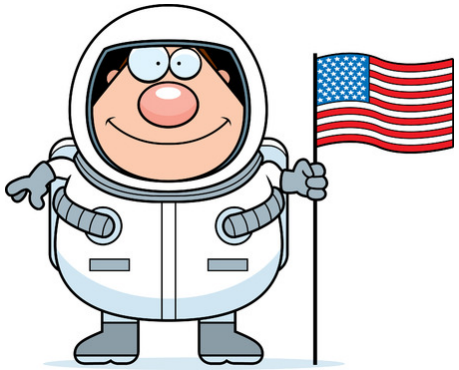
Caller ID Spoofing



- Muito comum nos EUA
  - Vastamente utilizado nos últimos anos para o scam da Receita Federal dos EUA (IRS)
  - Nada se cria, tudo se copia
    - Comum entre a comunidade latina, o golpe “sofri um acidente, preciso de dinheiro”
    - Estão usando o (número) de telefone da própria polícia da cidade, pedindo dinheiro para pagar a fiança
- Ainda engatinhando no Brasil, mas com grande potencial

Formas de ataque

Caller ID Spoofing



- Nos EUA, prática comum: alterar o número de origem para o mesmo código de área + prefixo do telefone da vítima
- Normalmente o telefone de origem (número que foi usado como origem da chamada) é válido e está ativo

- Chamadas de telemarketing, de cobrança ou não solicitadas para telefones celulares são punidas com multa de US$ 1.500 **por reclamação**
- SMS também é punido com o mesmo valor de multa

Formas de ataque

Caller ID Spoofing

Formas de ataque

Caller ID Spoofing

Caller ID Spoofing com o número do telefone da **SUA** agência bancária

Formas de ataque

Caller ID Spoofing

Caller ID Spoofing com o número do telefone da **SUA** agência bancária

- Prompts de voz roubados da URA do próprio banco
- Pede autenticação e validação do cartão de senhas

Medidas de Segurança

- Não permitir o acesso a partir da rede externa caso não seja necessário
- Caso seja realmente necessário o acesso, instalar o servidor IP PBX atrás de um SBC preferencialmente
- Não usar a porta padrão (SIP 5060, IAX 4569) – segurança por obscuridade... Eficácia questionável, mas retarda o ataque
- Se possível, usar VPN

Medidas de Segurança

- Não permitir o acesso a partir da rede externa caso não seja necessário
- Caso seja realmente necessário o acesso, instalar o servidor IP PBX atrás de um SBC preferencialmente
- Não usar a porta padrão (SIP 5060, IAX 4569) – segurança por obscuridade... Eficácia questionável, mas retarda o ataque
- Se possível, usar VPN

USE FAIL2BAN

Medidas de Segurança

Para sistemas de pequeno porte, o fail2ban é uma excelente alternativa.

- Dependendo das características do seu sistema, configurar a regra para que, em caso de falha, o IP seja bloqueado após “poucas” tentativas erradas de acesso
- Banir o IP “pelo resto da vida”

fail2ban.org

Medidas de Segurança

- Limitar o número de chamadas simultâneas do mesmo ramal
- Usar senhas fortes e aleatórias
- No Asterisk, não criar dialplans válidos debaixo do contexto [default]
- NUNCA usar dialplans genéricos/ilimitados

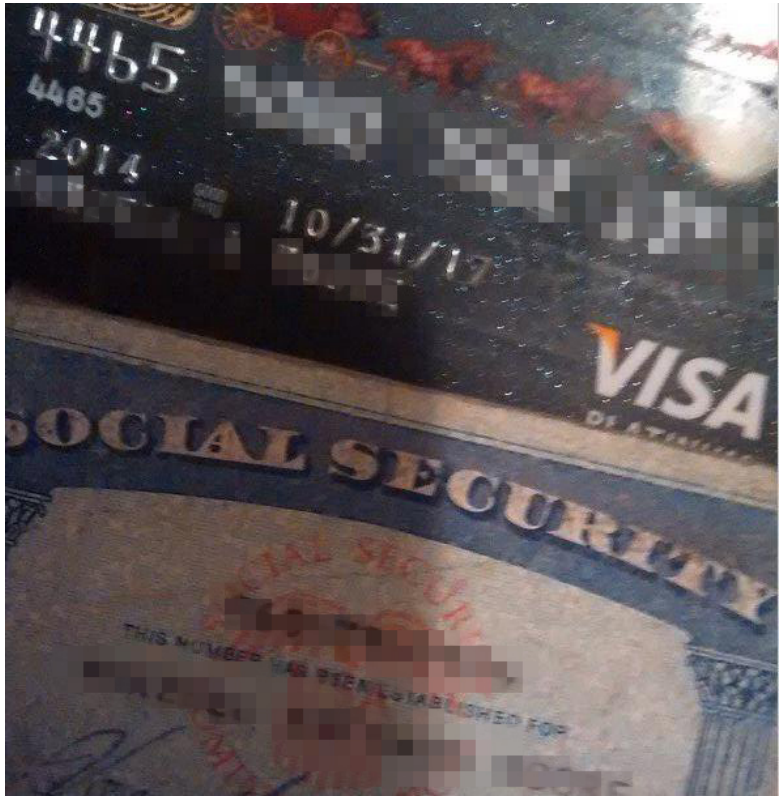
- No firewall, bloqueio por geolocalização do IP

- Preferencialmente, use contas pré-pagas nos provedores
- CONTROLE e valide sua fatura de serviços
- Monitore sua rede / verifique seu CDR

Medidas de Segurança

Exten => _X.,1,Dial(SIP/provedor/${EXTEN})

=



Recursos Adicionais

- Anatomia de ataques a servidores SIP - Klaus Steding-Jessen & João Ceron (GTS/20 - Dez/2012)
- FAIL2BAN – http://fail2ban.org
- CFCA – Communications Fraud Control Association – http://cfca.org
- Projeto “Quem Perturba” – Inércia Sensorial http://quemperturba.inerciasensorial.com.br
- openCNAM - https://opencnam.com

Fraude em Telefonia

Fraude em Telefonia

Hermann Wecke

AVIVAVox

hermann@gmail.com