# Anatomia de ataques a servidores SIP

João M. Ceron, Klaus Steding-Jessen,
Cristine Hoepers

ceron@cert.br, jessen@cert.br, cristine@cert.br

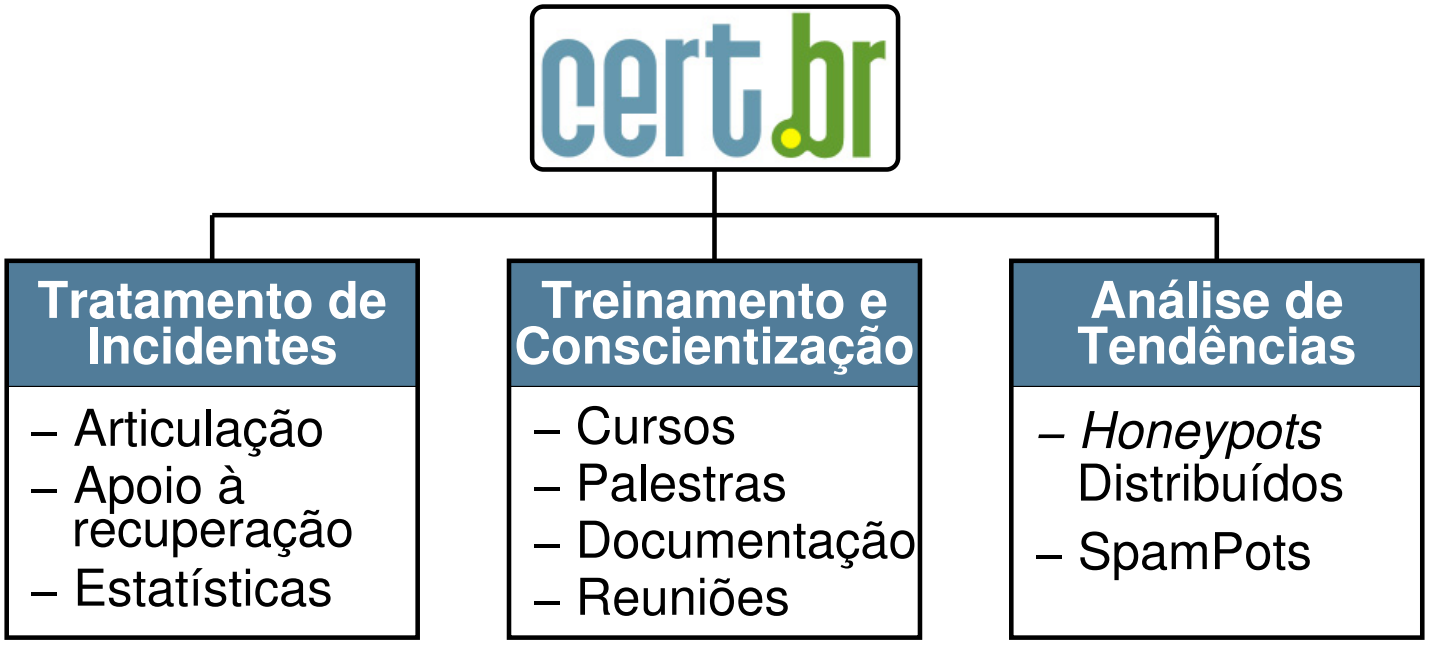
CERT.br – Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil

Núcleo de Informação e Coordenação do Ponto BR

Comitê Gestor da Internet no Brasil

# Sobre o CERT.br

Criado em 1997 como ponto focal nacional para tratar incidentes de segurança relacionados com as redes conectadas à Internet no Brasil




FIRST Improving Security Together MEMBER

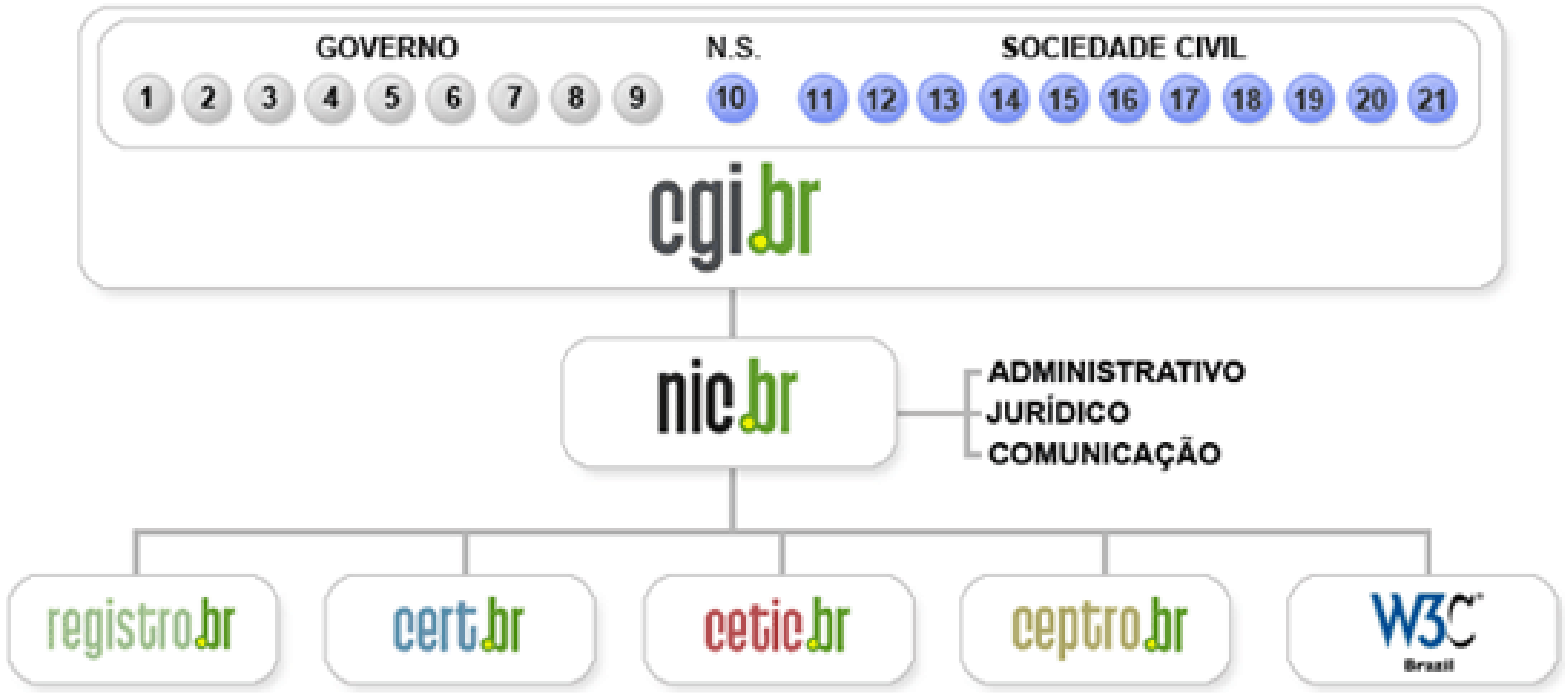
APWG RESEARCH PARTNER www.antiphishing.org

SEI Partner Carnegie Mellon

The Honeynet PROJECT

http://www.cert.br/sobre/

# Estrutura do CGI.br




01- Ministério da Ciência e Tecnologia
02- Ministério das Comunicações
03- Casa Civil da Presidência da República
04- Ministério do Planejamento, Orçamento e Gestão
05- Ministério do Desenvolvimento, Indústria e Comércio Exterior
06- Ministério da Defesa
07- Agência Nacional de Telecomunicações
08- Conselho Nacional de Desenvolvimento Científico e Tecnológico
09- Conselho Nacional de Secretários Estaduais para Assuntos de Ciência e Tecnologia

10- Notório Saber
11- Provedores de Acesso e Conteúdo
12- Provedores de Infra-estrutura de Telecomunicações
13- Indústria TICs (Tecnologia da Informação e Comunicação) e Software
14- Empresas Usuárias
15-18- Terceiro Setor
19-21- Academia

# Atribuições do CGI.br

Entre as diversas atribuições e responsabilidades definidas no Decreto Presidencial nº 4.829, destacam-se:

- a proposição de normas e procedimentos relativos à regulamentação das atividades na internet
- a recomendação de padrões e procedimentos técnicos operacionais para a internet no Brasil
- o estabelecimento de diretrizes estratégicas relacionadas ao uso e desenvolvimento da internet no Brasil
- **a promoção de estudos e padrões técnicos para a segurança das redes e serviços no país**
- a coordenação da atribuição de endereços internet (IPs) e do registro de nomes de domínios usando <.br>
- **a coleta, organização e disseminação de informações sobre os serviços internet, incluindo indicadores e estatísticas**

# Agenda

Motivação

Implementação

Análise dos Dados

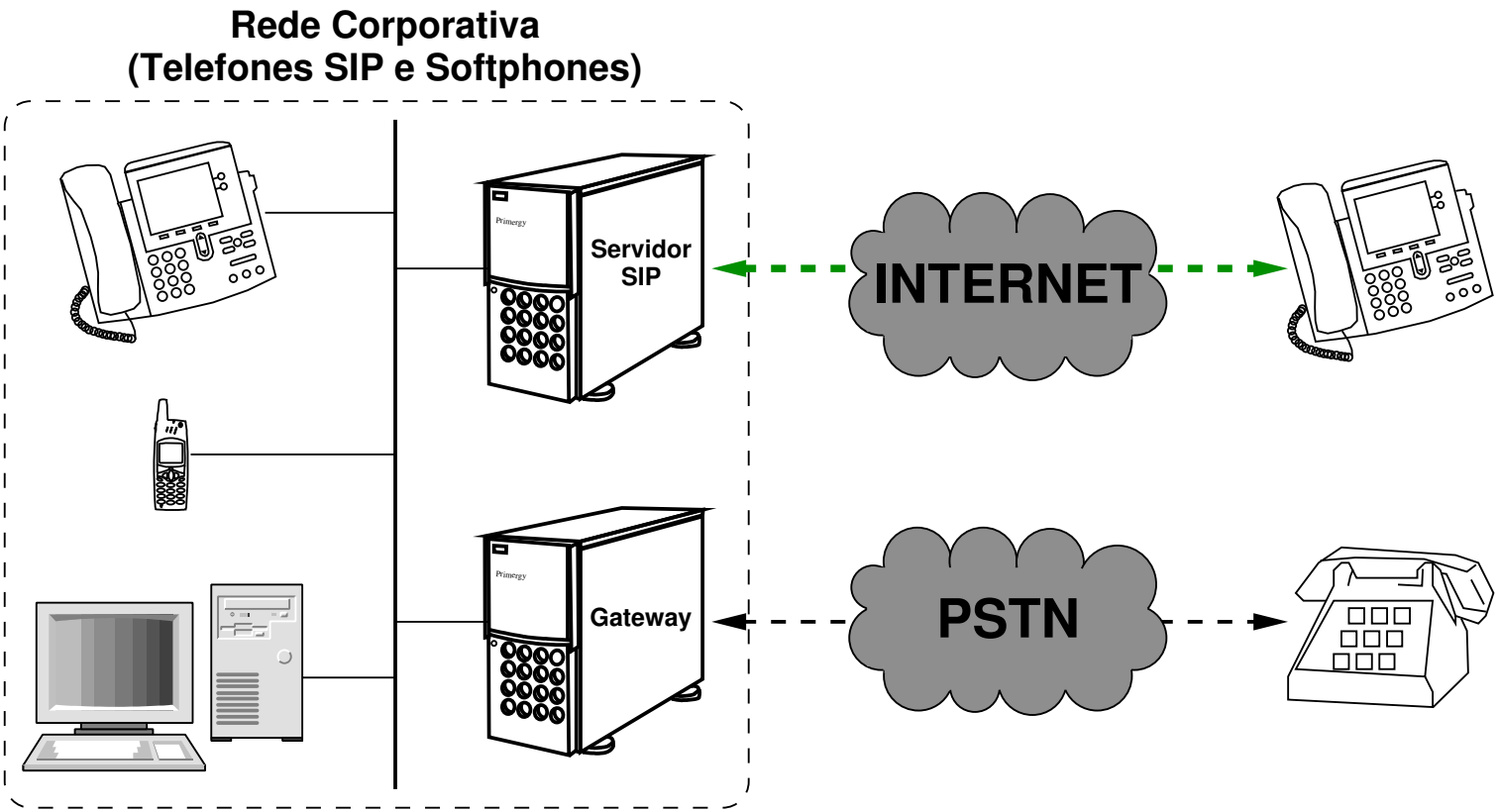
Conclusão

Recomendações

Referências

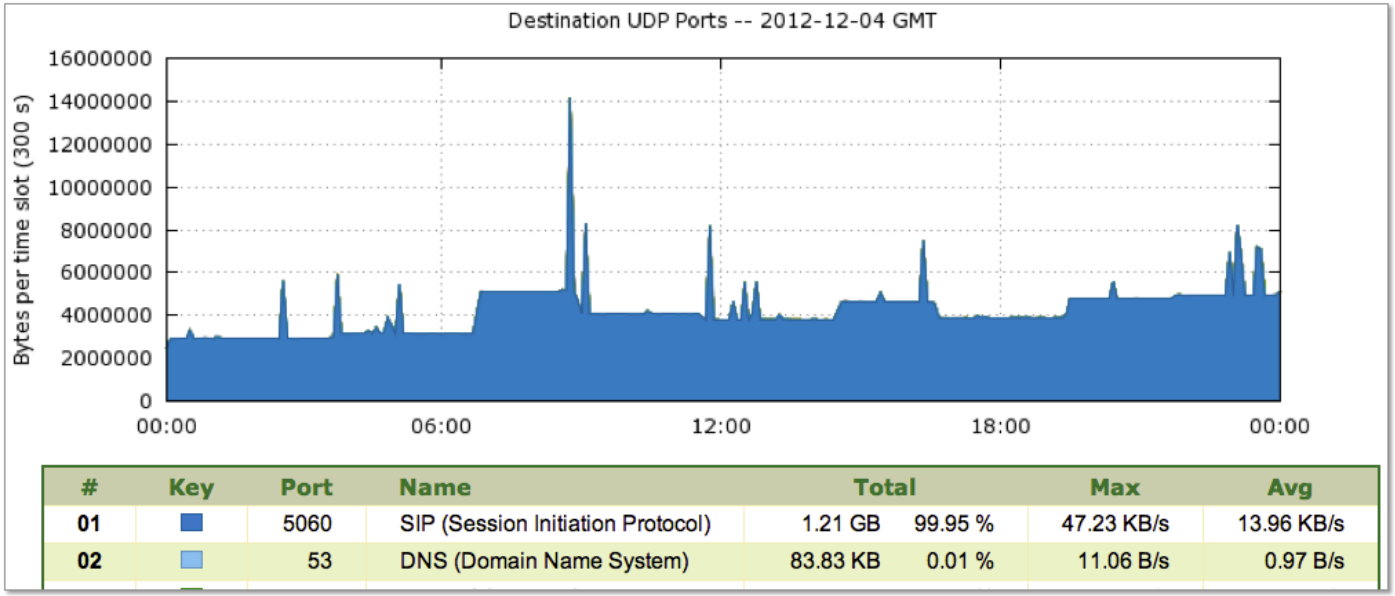
# Motivação

- Popularização dos dispositivos SIP



# Motivação (cont.)

- Alto volume de tráfego em nossos sensores (5060/UDP)
  - porta UDP mais sondada nos últimos 16 meses
- Ausência de detalhes do tráfego SIP
  - nível de aplicação




| # | Key | Port | Name | Total | | Max | Avg |
|---|---|---|---|---|---|---|---|
| 01 | | 5060 | SIP (Session Initiation Protocol) | 1.21 GB | 99.95 % | 47.23 KB/s | 13.96 KB/s |
| 02 | | 53 | DNS (Domain Name System) | 83.83 KB | 0.01 % | 11.06 B/s | 0.97 B/s |

# Implementação

Características do *software* implementado:

- escrito em Perl usando o pacote `Net::SIP`
  - módulo para Honeyd, instalado em 50+ sensores
- suporta os métodos `OPTIONS`, `REGISTER`, `INVITE`, etc.
- "ramais" são configuráveis, com ou sem senha, etc
- `INVITE` são respondidos com erros:
  - "Forbidden", "Request Timeout", "Temporarily Unavailable", "Busy Here", etc.
- áudio não é armazenado
  - questões de privacidade
  - SDP e RTP não são tratados
- logs com IP, método, número discado, *User Agent*, etc.

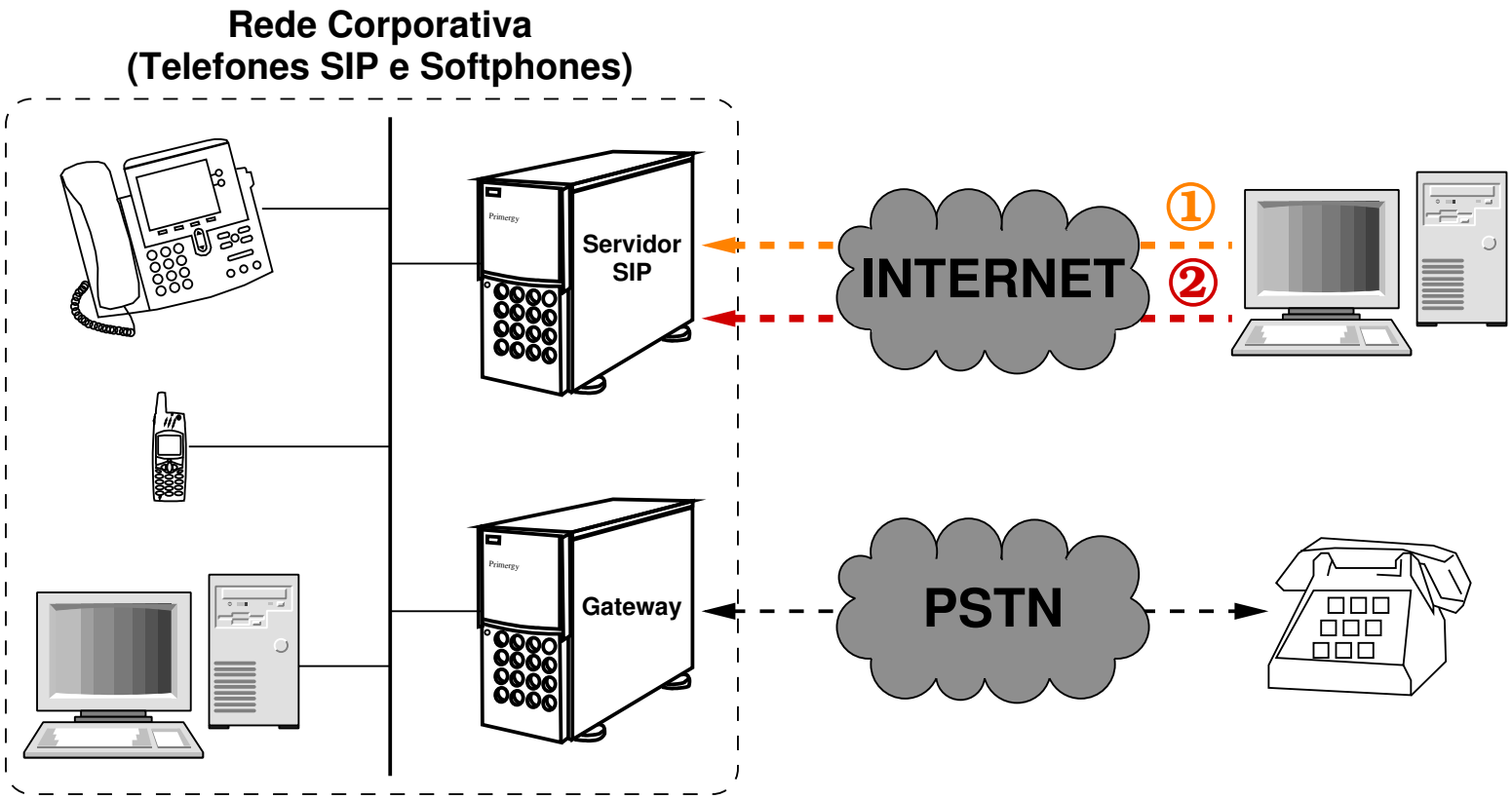
# Implementação (cont.)

Logs do *software* implementado:

```
2012-02-26 14:22:42 +0000: sip-honeyd.pl[729]: IP: 41.X.X.245,
method: REGISTER, from: "1234", to: "1234", resp: 200,
user-agent: "X-Lite release 1103d stamp 53117"

2012-02-26 14:22:44 +0000: sip-honeyd.pl[729]: IP: 41.X.X.245,
method: INVITE, from: "1234", to: "0015201*****194",
resp: 403, user-agent: "X-Lite release 1103d stamp 53117"
```

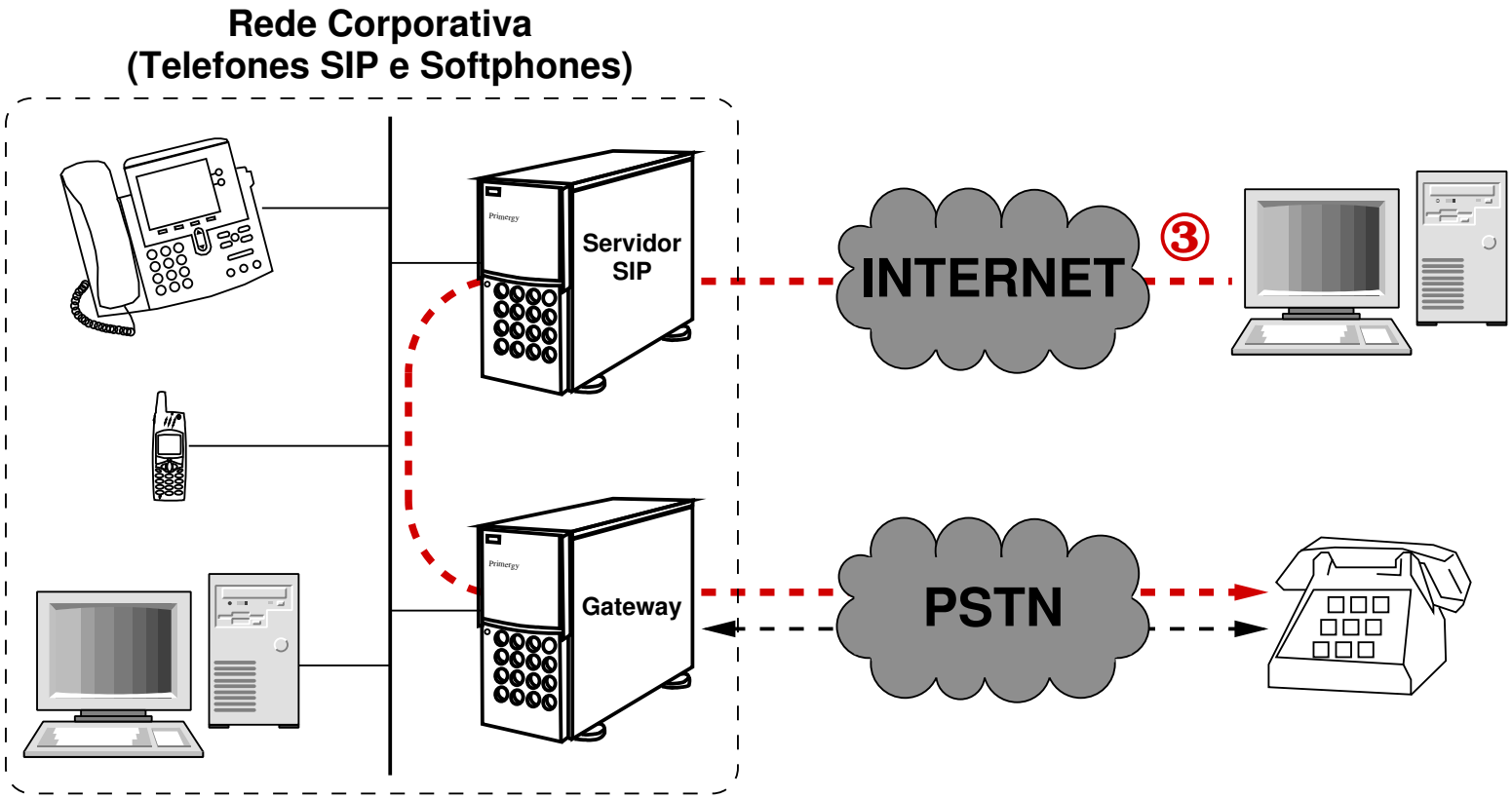
# Anatomia dos Abusos SIP




① Ferramentas automatizadas buscam por servidores SIP e mapeiam suas configurações

② Ferramentas automatizadas fazem ataques de força bruta em busca de ramais conhecidos e com senhas fáceis

# Anatomia dos Abusos SIP (cont.)




③ Atacante abusa servidores SIP para fazer ligações para telefones das redes fixas comutadas ou móveis

# Análise dos Dados Coletados

# Resumo dos dados coletados

- Período de coleta:
  - Setembro 2011 - Novembro 2012

| | |
|---|---|
| Mensagens `REGISTER` | 76.957.227 |
| Mensagens `INVITE` | 1.190.282 |
| IPs únicos | 9.295 |
| ASes únicos | 864 |
| Número total de dias | 435 |
| CCs únicos | 86 |

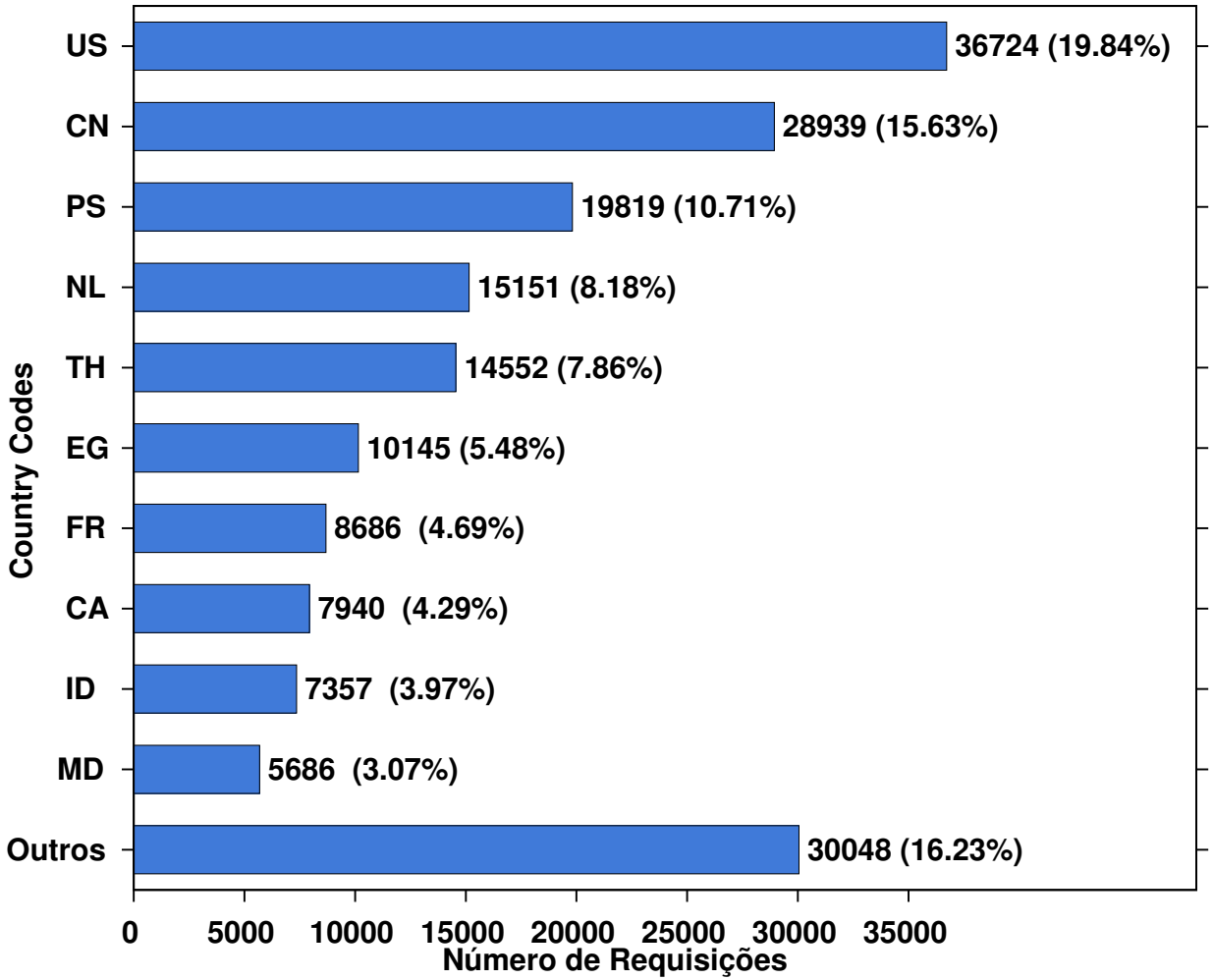
11.5 GB de dados (`REGISTER` + `INVITE`)

Mensagens `REGISTER`: no geral são varreduras de ferramentas automatizadas

Mensagens `INVITE`: na maioria *softphones* solicitando números telefônicos

# *Country Codes* de Origem

Considerando somente mensagens `INVITE`



# Análise dos Dados

- Abusos ao servidor SIP emulado
  - vulnerabilidades no servidor
  - requisições a telefones internacionais

```
2011-12-31 02:00:10 +0000: sip-honeyd.pl[30586]: IP: 188.X.X.85,
method: INVITE, from: "102", to: "90109725*****586",
resp: 0, user-agent: undefined
```

# Análise dos Dados (cont.)

## Identificar o destino das ligações

Redundância dos números solicitados:

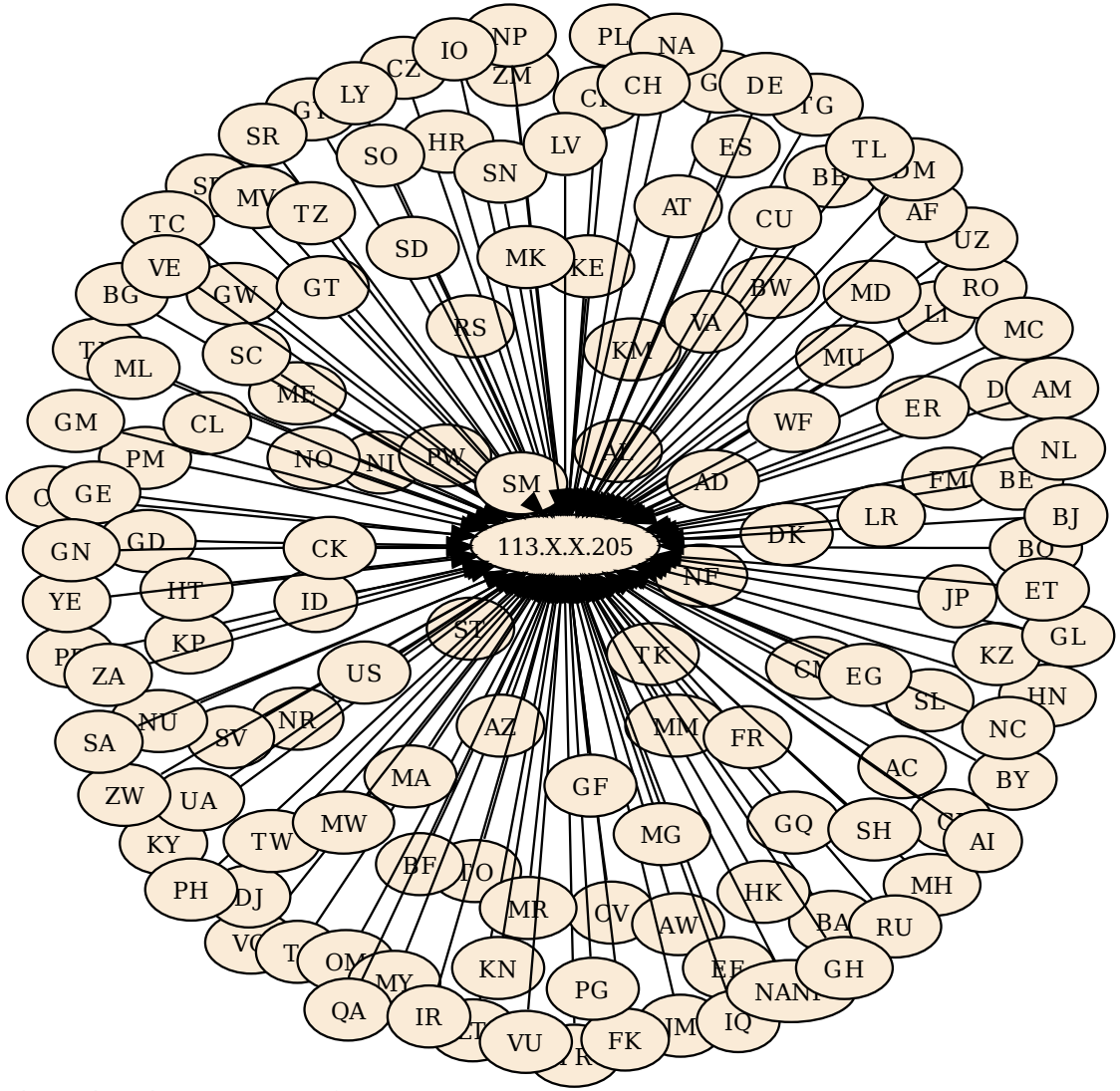
```
2011-09-26 19:21:55 -0300: sip2db.pl[9814]:  00149725*****586
2011-09-26 19:21:55 -0300: sip2db.pl[9814]: 000149725*****586
2011-09-26 19:21:55 -0300: sip2db.pl[9814]:  00159725*****586
2011-09-26 19:21:55 -0300: sip2db.pl[9814]:  00219725*****586
2011-09-26 19:21:55 -0300: sip2db.pl[9814]:  00219725*****586
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
```

# Análise das Ligações

Único IP realizou ligações para 144 países: possível **central telefônica**.






AfterGlow 1.6.2

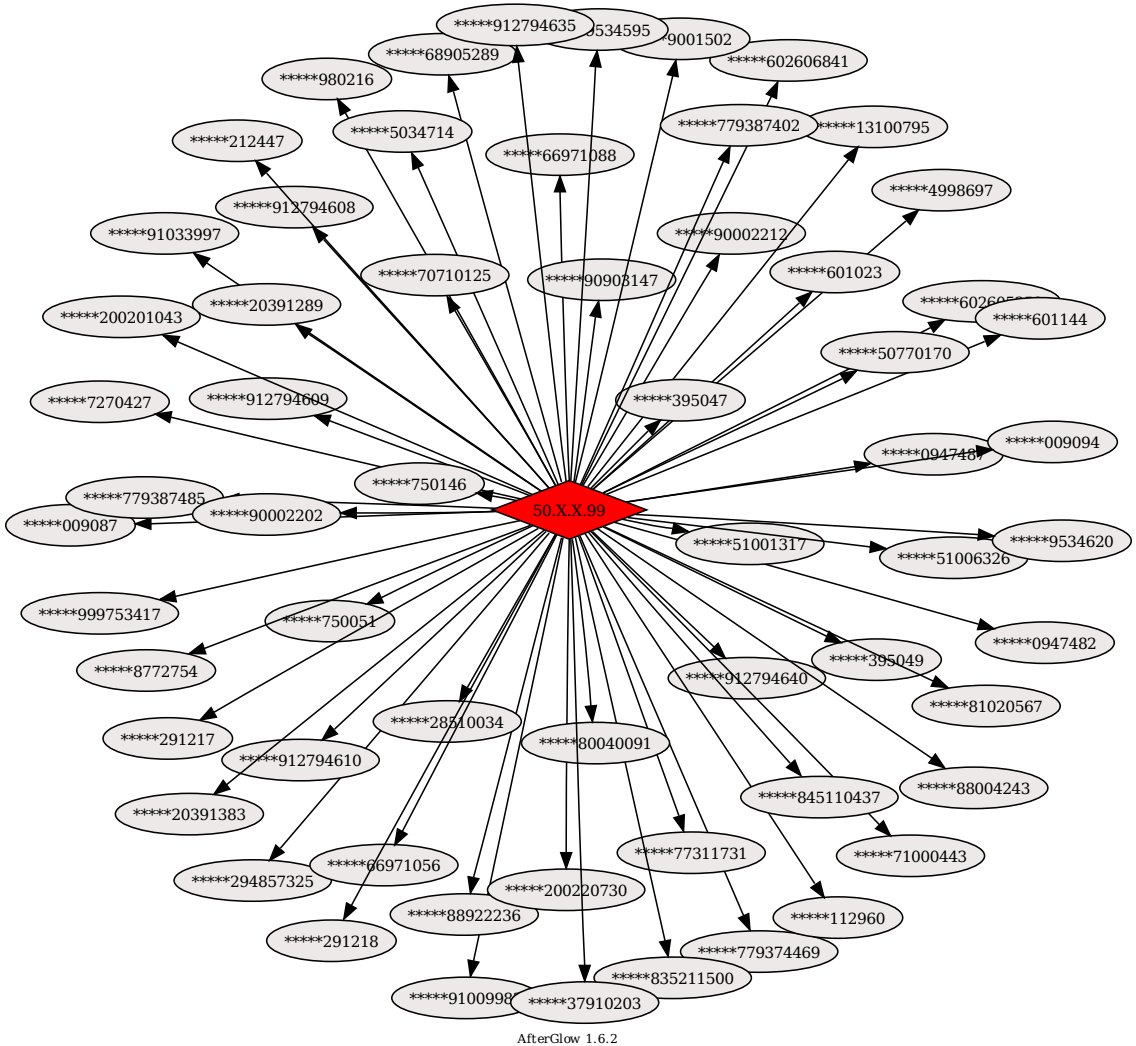
# Análise das Ligações (cont.)

Tuplas mais frequentes observadas:

| IP | | DDI | Total | (%) |
|---|---|---|---|---|
| PS | → | IL | 9910 | 5.19% |
| EG | → | EG | 7008 | 3.67% |
| MD | → | CZ | 5559 | 2.91% |
| US | → | CZ | 4535 | 2.37% |
| FR | → | RU | 4267 | 2.23% |
| US | → | IL | 3454 | 1.81% |
| PS | → | RU | 3449 | 1.80% |
| CA | → | Inter (0800) | 3296 | 1.72% |
| US | → | GB | 2038 | 1.06% |
| US | → | ZW | 1904 | 0.99% |

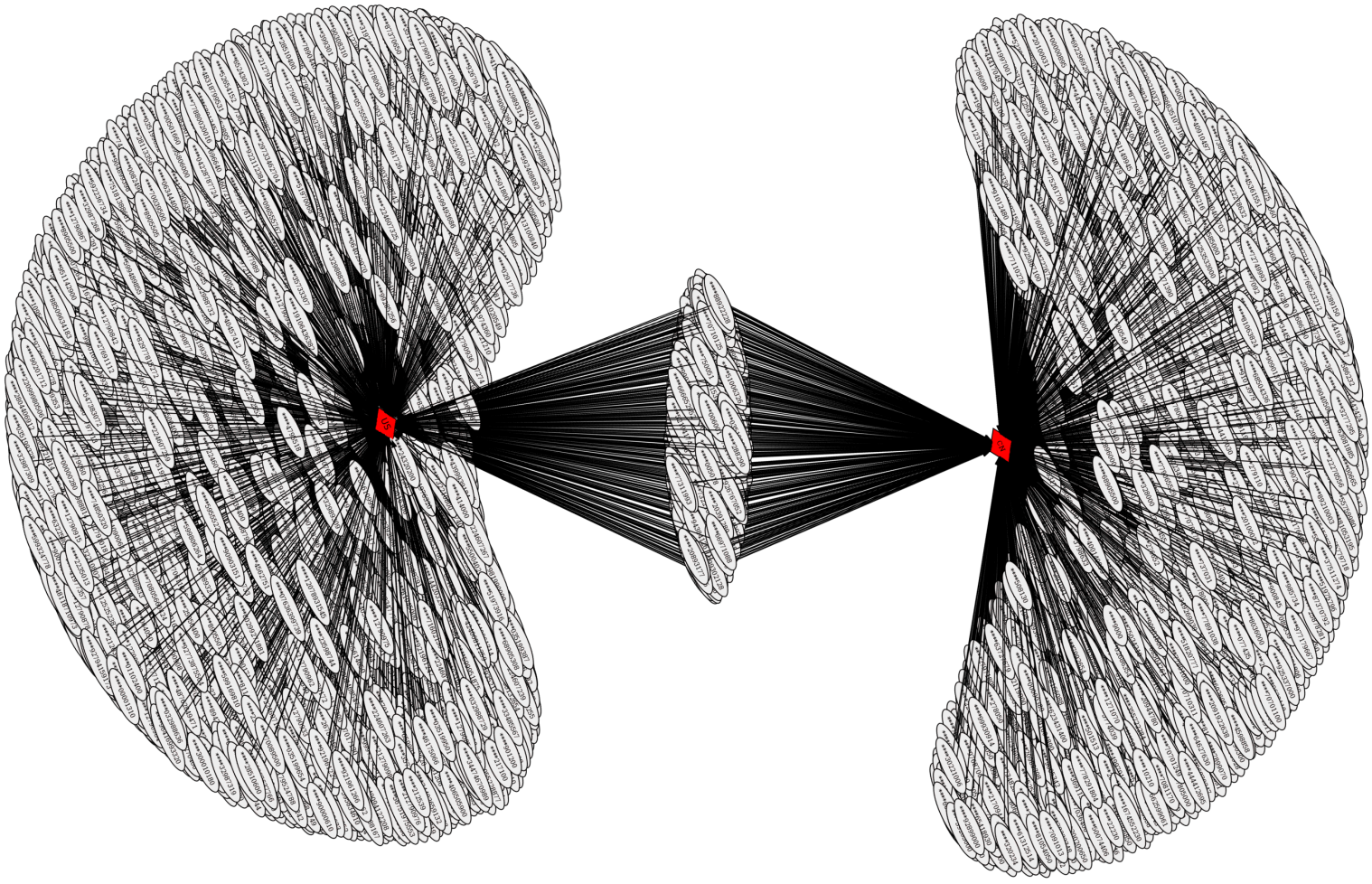
# Análise das Ligações (cont.)

## Números telefônicos solicitados pelo IP 50.X.X.99

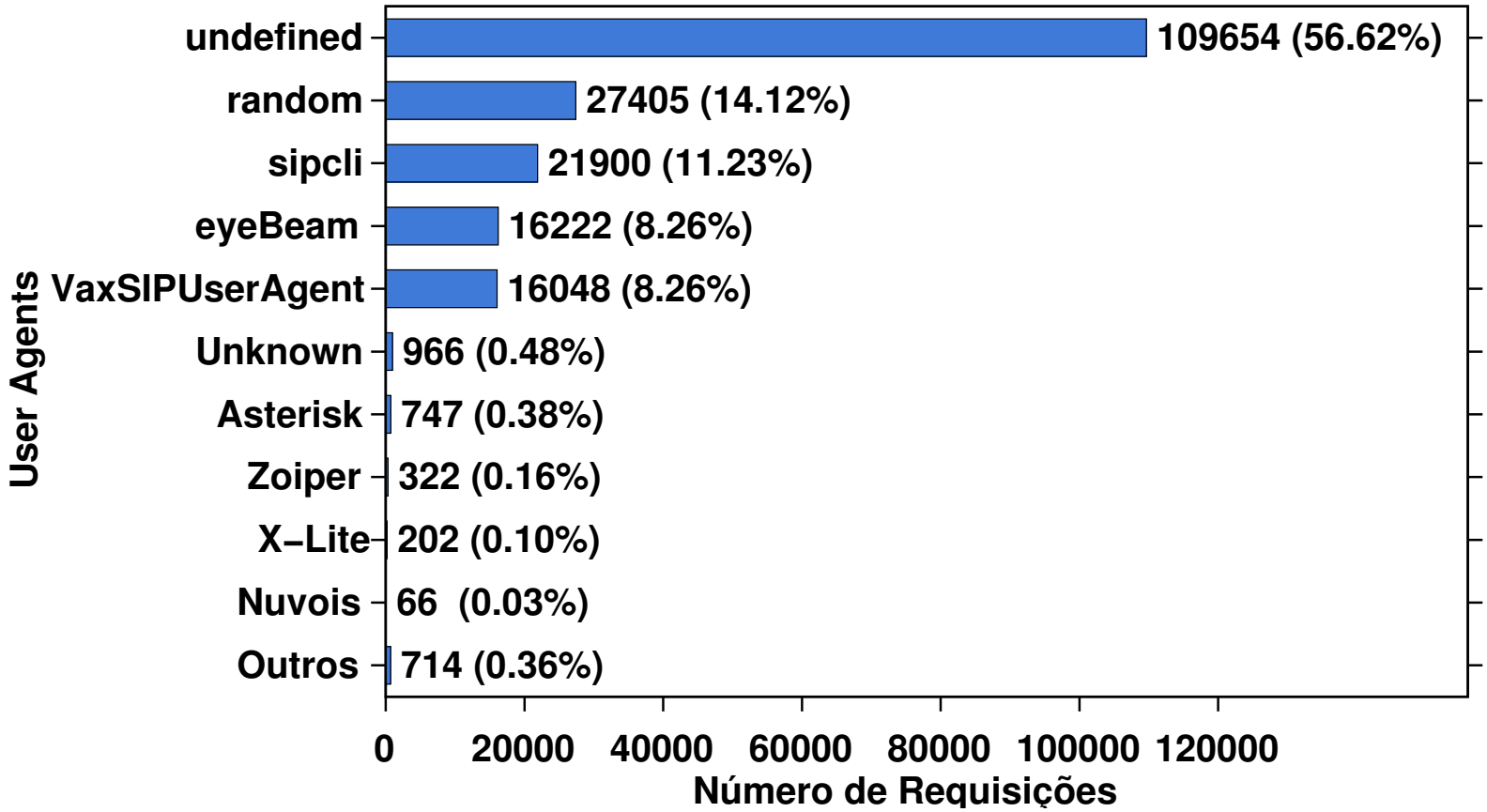


# Análise das Ligações (cont.)

Ligações com origem US vs CN:



# *User Agents* utilizados nas tentativas de ligações



# Conclusões

- Abusos objetivando ligações internacionais
- Ferramentas personalizadas
  - *User Agents* aparentemente modificados
- Números mais ligados sugerem fraudes
  - Bank of America e Citibank
  - Cartão pré-pago internacional
- Centrais telefônicas ou *proxies*
  - Mesmo IP e *User Agent*

# Recomendações

- Proteger o servidor SIP da Internet
- Usar senhas fortes
  - terminais VoIP e *softphones*
  - a senha é armazenada nos dispositivos, e pode ser longa e complexa
- Utilizar extensões com nomes não usuais
- Monitorar o uso do SIP na sua organização
  - Logs de acessos
  - Conta telefônicas procurando por ligações não usuais.

# Referências

- Comitê Gestor da Internet no Brasil – CGI.br
  http://www.cgi.br/
- CERT.br – Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil
  http://www.cert.br/
- Honeypots for Threats and Abuse passive Reconnaissance and information Gathering
  http://www.honeytarg.cert.br/
- Anatomy of SIP Attacks – Dezembro 2012 Usenix ;login: Magazine
  https://www.usenix.org/publications/login/december-2012-volume-37-number-6/anatomy-sip-attacks