

Anatomia de Ataques a Servidores SIP

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

jessen@cert.br, ceron@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

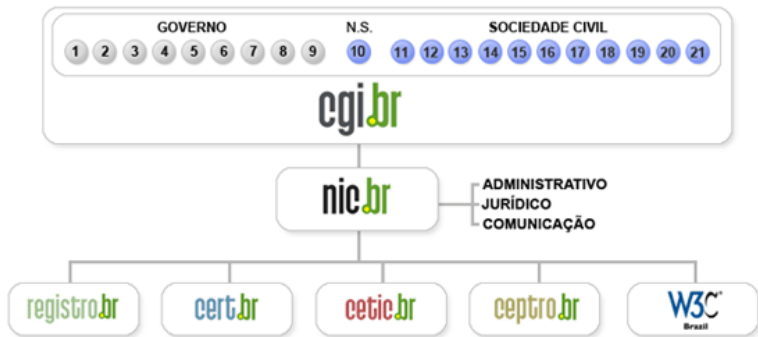


SEI Partner
Carnegie Mellon.



<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

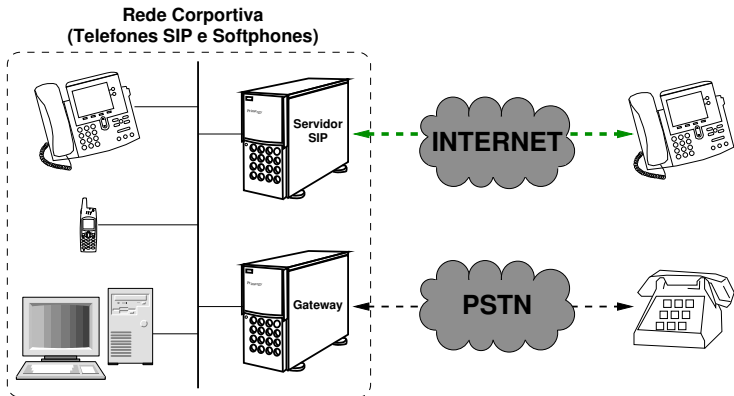
Conclusão

Recomendações

Referências

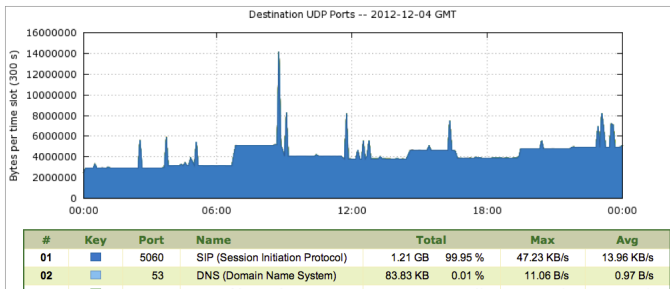
Motivação

- Popularização dos dispositivos SIP



Motivação (cont.)

- Alto volume de tráfego em nossos sensores (5060/UDP)
 - porta UDP mais sondada nos últimos 19 meses
- Ausência de detalhes do tráfego SIP
 - nível de aplicação



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.

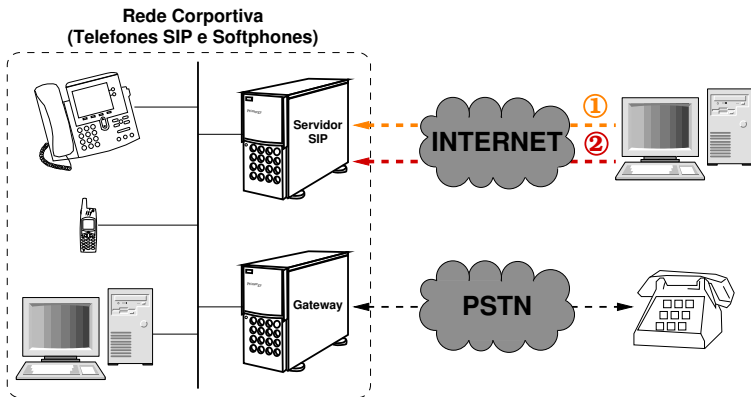
Implementação (cont.)

Logs do *software* implementado:

```
2013-04-29 12:21:48 +0000: sip-honeyd.pl[21131]: IP: 37.X.X.217,  
method: REGISTER, from: "101", to: "101", resp: 200, user-agent:  
"eyeBeam release 3006o stamp 17551"
```

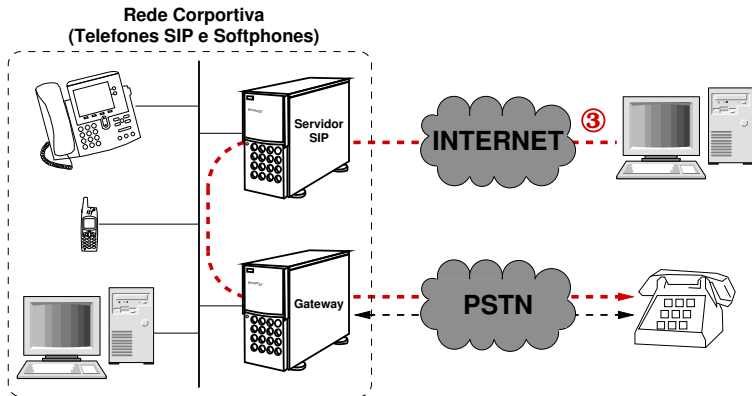
```
2013-04-29 12:22:40 +0000: sip-honeyd.pl[21131]: IP: 37.X.X.217,  
method: INVITE, from: "101", to: "00197259****839", resp: 403,  
user-agent: "eyeBeam release 3006o stamp 17551"
```

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 abuse 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 - Abril 2013

| | |
|----------------------|-------------|
| Mensagens REGISTER | 115.817.401 |
| Mensagens INVITE | 2.241.367 |
| IPs únicos | 13.443 |
| ASes únicos | 937 |
| Número total de dias | 589 |
| CCs únicos | 89 |

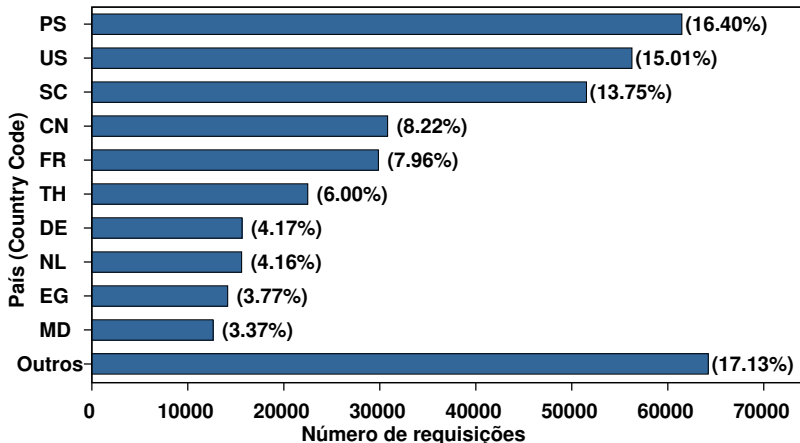
17.4 GB de dados (REGISTER + INVITE)

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 não foram exploradas
 - requisições a telefones internacionais

```
2013-04-29 12:22:40 +0000: sip-honeyd.pl[21131]: IP: 37.X.X.217,  
method: INVITE, from: "101", to: "00197259****839", resp: 403,  
user-agent: "eyeBeam release 3006o stamp 17551"
```

Análise dos Dados (cont.)

Identificar o destino das ligações

Redundância dos números solicitados:

```

2013-04-30 03:01:04 -0300: sip2db.pl [25198]:      00197259****839
2013-04-30 03:01:04 -0300: sip2db.pl [25198]:      0070097259****839
2013-04-30 03:01:04 -0300: sip2db.pl [25198]:      997259****839
2013-04-30 03:01:04 -0300: sip2db.pl [25198]:      1230097259****839
2013-04-30 03:01:04 -0300: sip2db.pl [25198]:      01397259****839
2013-04-30 03:01:04 -0300: sip2db.pl [25198]:      01597259****839
2013-04-30 03:01:04 -0300: sip2db.pl [25198]:      02197259****839
2013-04-30 03:01:04 -0300: sip2db.pl [25198]:      0072797259****839
2013-04-30 03:01:04 -0300: sip2db.pl [25198]:      01101197259****839
  
```

```

<-----|
Longest substring:  97259****839
  
```

```

97259****839|972|59****839|IL|Israel
  
```

```

biblioteca Number::Phone::Country
  
```

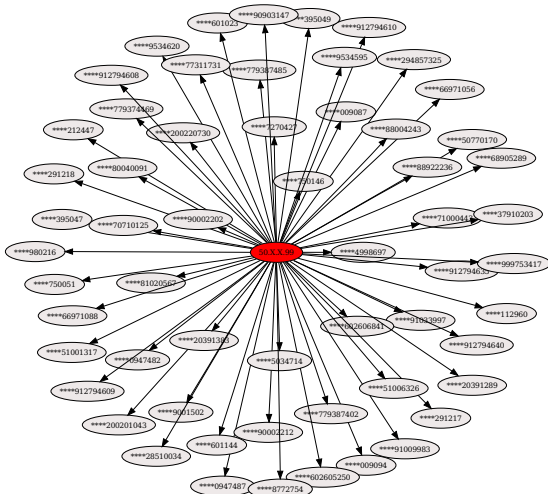

Análise das Ligações (cont.)

Tuplas mais frequentes observadas:

| IP | | DDI | Total | (%) |
|-----------|---|------------|--------------|------------|
| CZ | → | SC | 37128 | 9.90% |
| IL | → | PS | 23168 | 6.18% |
| RU | → | FR | 16197 | 4.32% |
| RU | → | PS | 14000 | 3.73% |
| CH | → | SC | 12709 | 3.39% |
| CZ | → | MD | 11603 | 3.09% |
| EG | → | EG | 8880 | 2.37% |
| GB | → | US | 8301 | 2.21% |
| IL | → | US | 8256 | 2.20% |
| IL | → | FR | 6291 | 1.67% |

Análise das Ligações (cont.)

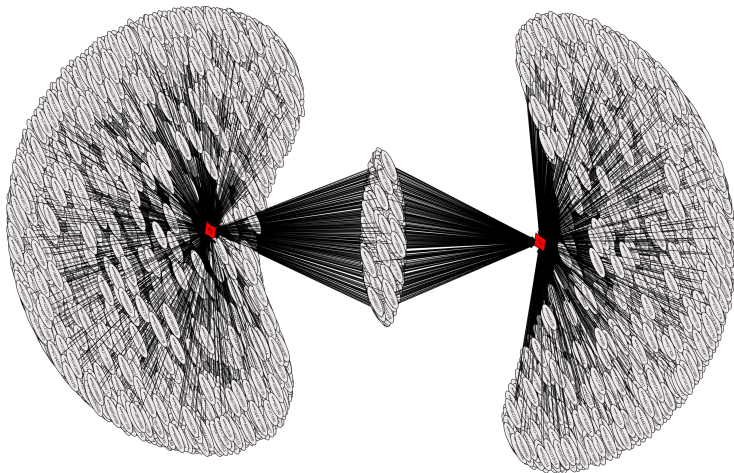
Números telefônicos solicitados pelo IP 50.X.X.99



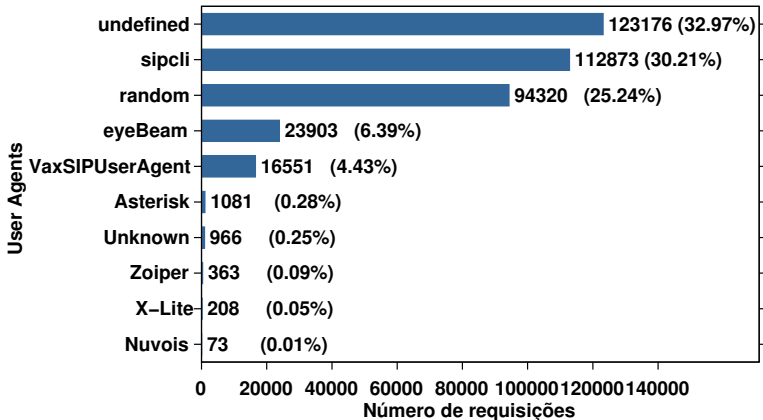
AlterGlow 1.6.2

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>