Anatomia de Abusos a Servidores SIP

João M. Ceron[1], **Klaus Steding-Jessen**[1], **Cristine Hoepers**[1]

[1]Centro de Estudos, Resposta e Tratamento de
Incidentes de Segurança no Brasil (CERT.br)
Núcleo de Informação e Coordenação do Ponto BR (NIC.br)
Comitê Gestor da Internet no Brasil (CGI.br)

{ceron,jessen,cristine}@cert.br

Resumo. *Serviços VoIP têm se popularizado nos últimos anos e, juntamente com sua popularização, tem crescido a quantidade de ataques a tais serviços. Boa parte destes ataques visam abusar a infraestrutura VoIP e utilizá-la de maneira indevida. Para aprimorar os atuais mecanismos de segurança é importante entender a dinâmica e as particularidades dos ataques. O presente trabalho apresenta uma análise das tentativas de abuso a serviços VoIP coletadas por uma rede de* honeypots *dispersos pelo território brasileiro. Por meio da análise de abusos direcionados a serviços emulados foi possível identificar motivações dos atacantes e quais medidas de segurança podem prevení-las.*

Abstract. *VoIP services have become increasingly popular in the past few years, as well as the amount of attacks to such services. Many of these attacks try to abuse the VoIP infrastructure and wrongfully use it. To improve current security mechanisms it is important to understand the dynamics and characteristics of those attacks. This paper presents an analysis of VoIP services abuse attempts collected by a network of honeypots deployed in Brazil. The analysis of the abuses lauched to the emulated services enabled to identify the abuses' characteristics and identify security measures which can prevent them.*

1. Introdução e Trabalhos Relacionados

A popularidade dos serviços VoIP (*Voice over* IP) teve um rápido crescimento nos últimos anos. Devido a características como flexibilidade e baixo custo, muitas organizações estão migrando dos sistemas telefônicos tradicionais (PABX – *Private Automatic Branch Exchange*) para implementações baseadas em VoIP. Esta ampla adoção de serviços VoIP vem contribuindo para torná-los mais atrativos aos atacantes, em especial os serviços implementados pelo protocolo SIP (*Session Initiation Protocol*) [IETF 2002, SANS 2013, CERT.br 2013b].

Um ataque a um serviço VoIP pode causar inúmeros prejuízos para uma instituição, como: indisponibilidade do sistema de telefonia; interceptação de conversas telefônicas; uso de ramais para engenharia social; ou utilização da central telefônica para efetuar ligações internacionais [El-moussa *et al.* 2010, Liu e Tu 2011, Ceron *et al.* 2012].

A comunidade de segurança tem demonstrado preocupação com relação à segurança de serviços VoIP, incluindo trabalhos que discutem fragilidades dos protocolos VoIP [Rezac *et al.* 2011, Keromytis 2010] e mecanismos de ataque [El-moussa *et al.* 2010]. Uma pesquisa apresentada por Valli [Valli 2010] é a que

mais se aproxima do trabalho proposto neste artigo, pois faz um estudo das sondagens a serviços VoIP implementados em um *honeypot*. Como limitações, o trabalho de Valli avalia apenas ataques direcionados a um único *honeypot*, e atêm-se a analisar as sondagens do ponto de vista de tráfego de rede e não estende a análise a mensagens do protocolo. Nosso trabalho, por outro lado, apresenta um estudo dos ataque SIP que vai além da camada de rede, analisando os ataques do ponto de vista da camada de aplicação.

Em aspectos fundamentais nosso estudo analisou características de ataques a centrais telefônicas SIP emuladas em um conjunto de sensores (cerca de 50 *honeypots*), observados num período de 589 dias, em redes exclusivamente brasileiras. Para captura dos dados foram desenvolvidos *softwares* que tratam mensagens do protocolo SIP, permitindo obter informações mais detalhadas dos ataques, como por exemplo, números telefônicos requisitados nos ataques.

O restante do trabalho está organizado da seguinte maneira. A seção 2 descreve características do protocolo SIP e conceitos relacionados à *honeypots*. Na Seção 3 é discutida uma visão do cenário de ataques a serviços VoIP baseados no protocolo SIP. A Seção 4 apresenta a implementação da solução desenvolvida. Os resultados são apresentados na seção 5, e na seção 6 são discutidas alguma recomendações de seguranças para proteger-se dos ataques identificados por nosso estudo. Por fim, as conclusões do trabalho são apresentadas na seção 7.

2. Contextualização Teórica

Esta seção busca relembrar conceitos básicos que são fundamentais para o entendimento deste trabalho. Para isso, na primeira subseção são apresentados elementos básicos do protocolo SIP e, na segunda subseção, o conceito de *honeypots* é discutido com o objetivo de contextualizar a parte analítica deste trabalho.

2.1. Protocolo SIP

O protocolo SIP (*Session Initiation Protocol*) é muito utilizado para a comunicação de voz sobre o protocolo IP [Rosenberg e Schulzrinne 2002]. Devido às características do protocolo, este vem sendo amplamente utilizado por boa parte dos fabricantes de dispositivos.

O SIP caracteriza-se por especificar um conjunto de regras para gerenciar sessões multimídia entre dispositivos de comunicação VoIP (telefones, sistemas de videoconferência, *softphone* e outros). Para isso, a arquitetura SIP define um conjunto de entidades funcionais: *User Agent* (UA), *SIP Proxy*, *SIP Registrar*, *SIP Redirect Server*, *Location Server* e *Media Gateway*.

A entidade definida como *User Agent* corresponde aos dispositivos que fazem a interface com o usuário do sistema, tipicamente um telefone VoIP ou um *softphone*. Já as entidades *SIP Proxy*, *Media Gateway*, *SIP Redirect Server* e *Location Server* são aplicações que permitem aos UAs estabelecer uma comunicação entre si. O *SIP Registrar*, por outro lado, é responsável por gerenciar o registro (autenticação) dos usuários na arquitetura. Atuando de forma complementar o *SIP Proxy* executa o roteamento das mensagens de controle e administração entre os dispositivos SIP [El-Sawda 2010].

As entidades SIP comunicam-se por meio de um conjunto de mensagens definidas pelo próprio protocolo. Diferentes métodos podem ser utilizados para a sinalização

de sessões: *REGISTER*: registra/autentica a localização do usuário; *OPTIONS*: solicita recursos disponíveis do servidor (*i.e* codificadores, métodos de autenticação); *INVITE*: inicializa uma sessão; *ACK*: confirma a inicialização da sessão; *CANCEL*: cancela uma sessão; *BYE*: finaliza uma sessão.

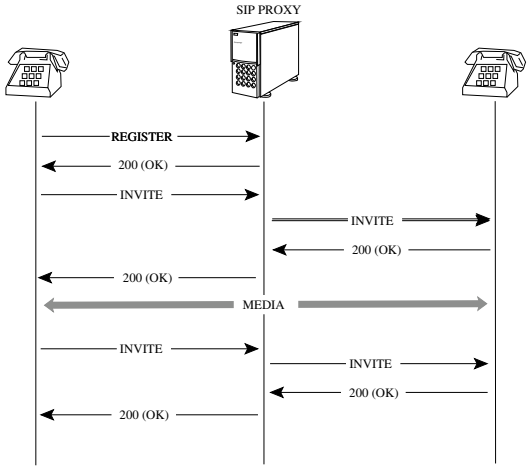


Figura 1. Mensagens SIP: Troca de mensagens entre dispositivos SIP.

O protocolo SIP especifica um conjunto de mensagens para a troca de informação entre as entidades. A troca de mensagens utiliza o modelo cliente-servidor – requisições e respostas – similar ao protocolo HTTP. Sendo assim, as mensagens são transmitidas em "texto claro" disponibilizando um "código" como resultado da operação realizada. Por exemplo, código 200 para sucesso (OK); código 401 acesso não autorizado; código 600 para ramal ocupado.

Uma comunicação típica é apresentada na Figura 1, onde é ilustrado um servidor "*SIP Proxy*" e dois telefones SIP. No momento que um cliente inicia uma ligação, uma solicitação *INVITE* é enviada diretamente para o IP do servidor (*SIP Proxy*). O servidor responde autorizando ou solicitando mais informações (autenticação). Uma vez que a ligação seja autorizada, é enviada uma mensagem de *INVITE* para o cliente final (destino da ligação). O destino da ligação aceita a ligação enviando uma mensagem (*ACK*). A origem confirma que recebeu o aceite e a partir desse ponto é estabelecida a troca de dados (conversação ponto-a-ponto). Por fim, uma mensagem *BYE* encerra a sessão terminado a comunicação entre as partes.

2.2. Honeypots

Um *honeypot* é um recurso computacional amplamente monitorado desenvolvido para ser sondado, atacado, ou comprometido [Provos e Holz 2008]. Por definição, todo tráfego destinado a um *honeypot* é malicioso, afinal não existe nenhum serviço legítimo sendo executado no mesmo. O valor de um *honeypot* está em obter informações de seu uso não autorizado por parte dos atacantes uma vez que é, em teoria, uma ferramenta de segurança isenta de falso-positivos.

O nível de informação sobre um ataque obtido nos acessos a um *honeypot* usualmente não pode ser obtido por outros dispositivos de segurança. Por exemplo, um *honeypot* pode registrar uma sessão interativa e, até mesmo, obter informações de sessões

criptográficas dos atacantes. Por meio de *honeypots* é possível entender o funcionamento de ataques, vetores de propagação, identificar varreduras, coletar artefatos entre outros.

Outros dispositivos de segurança, tais como os NIDS (*Network Intrusion Detection System*), requerem previamente assinaturas de tráfego malicioso para detectar uma atividade maliciosa. Os *honeypots*, por outro lado, podem detectar vulnerabilidades desconhecidas apenas observando as ações de um atacante ou *malware*. Um *honeypot* pode ser implementado de diversas maneiras e com diferentes níveis de complexidade. A literatura classifica os *honeypots* segundo a sua interação com os ataques recebidos [Provos e Holz 2008]:

> **Alta Interatividade:** são *honeypots* que fornecem um sistema real para o atacante interagir. Esses sistemas podem ser comprometidos completamente, permitindo a um atacante ter acesso total ao sistema e usá-lo para lançar ataques a terceiros. Muito embora seja possível obter informação com um maior nível de detalhamento, esse tipo de *honeypot* necessita de barreiras adicionais de segurança para impedir que os mesmos sejam utilizados em ataques a terceiros.
>
> **Baixa Interatividade:** são *honeypots* cujo nível de interação é limitado. Geralmente, são disponibilizados serviços emulados onde o atacante não acessa o sistema real, ou seja, os *honeypots* de baixa interatividade não podem ser efetivamente comprometidos. Mesmo sendo limitado, este tipo de *honeypot* é extremamente útil para obter informações detalhadas sobre o conteúdo de sondagens e varreduras de serviços, mas sem o risco de um comprometimento.

Os dois tipos de *honeypots* apresentam vantagens e desvantagens. Neste trabalho são utilizados *honeypots* de baixa interatividade para redução de riscos e também para adequar-se a já existente estrutura de monitoração utilizada.

O uso de *honeypots* para o estudo de atividades maliciosas é uma metodologia bastante consolidada. A bibliografia revela inúmeros trabalhos que valem-se de *honeypots* para investigar tendências de ataques e propor melhorias para ferramentas de segurança [Ceron *et al.* 2010, Santos *et al.* 2010, Hoepers *et al.* 2005].

3. O cenário de abusos a servidores SIP

Nos últimos anos a comunidade de segurança da informação vem notando um aumento significativo nas sondagens aos serviços VoIP, em especial varreduras destinadas à porta 5060/UDP, associada ao protocolo SIP [SANS 2013]. No Brasil, o CERT.br também vem observando um aumento no número de notificações relativas a varreduras com destino a esta porta [CERT.br 2013b]. Do mesmo modo, é possível observar nas estatísticas públicas do Projeto *Honeypots* Distribuídos [CERT.br 2013a] a mesma tendência, que mostra o protocolo SIP como um dos mais sondados nos *honeypots* do projeto.

Boa parte dessas varreduras são realizadas por ferramentas automatizadas que buscam enumerar serviços disponíveis em servidores VoIP. Entre as ferramentas disponíveis destaca-se o *SipVicious*, que, segundo a sua própria documentação, é um conjunto de ferramentas que podem ser utilizadas para auditar sistemas VoIP baseados em SIP [Sandro Gauci 2013]. Através dessa ferramenta um usuário pode realizar diversas ações, como por exemplo: varrer um bloco de endereçamento IP em busca de dispositivos

SIP acessíveis; identificar ramais ativos numa central telefônica; ou fazer força bruta em senhas de ramais.

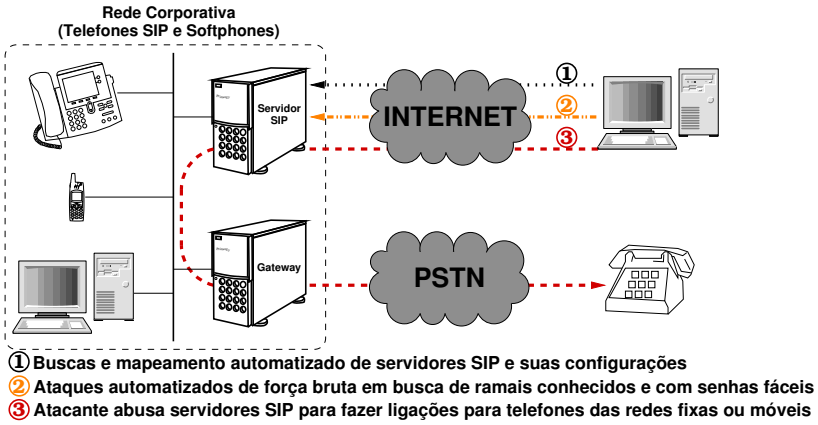


Figura 2. Anatomia de ataques aos servidores SIP.

Dentre os diversos tipos de ataque aos serviços SIP, um dos mais populares consiste no abuso a centrais telefônicas VoIP (Asterisk, FreeSwitch, entre outras). A grande maioria desses ataques apresentam um *modus operandi* muito similar entre si – vide Figura 2 – correspondendo às seguintes etapas:

1) **Enumeração**: busca por dispositivos com serviço SIP acessível e os inspeciona à procura de falhas de configuração. Nessa inspeção é possível identificar os ramais existentes no PABX e a respectiva configuração dos ramais.
2) **Força Bruta**: muitas vezes os ramais configurados num servidor PABX são acessíveis mediante senhas pré-configuradas. Para ter acesso ao sistema, é comum observar nesta etapa um processo automatizado de adivinhação dessas senhas (força bruta).
3) **Abuso**: após ter acesso a um ramal, o atacante realiza alguns testes para determinar a viabilidade do abuso da infraestrutura. Frequentemente o primeiro teste realizado é a verificação da possibilidade do sistema realizar ligações externas, em especial ligações internacionais sem restrição.

Estudos mostram que o abuso a centrais telefônicas em geral possui motivações financeiras [Sandro Gauci 2013]. Existem diferentes modelos de negócio, como por exemplo, o uso da central para realizar ligações internacionais de forma gratuita ou a revenda de serviços (sub-locação da central comprometida).

A fim de maximizar os ganhos financeiros, existem modelos de negócio que se valem de números telefônicos do tipo *premium*, um serviço oferecido por operadoras de telefonia com uma tarifa diferenciada. Nesse serviço é cobrada uma tarifa consideravelmente maior que a tarifa convencional, sendo que uma parte é transferida para o provedor do serviço como pagamento. No Brasil os números *premium* ficaram populares por conta de serviços como tele-amizade e horóscopo oferecidos com o prefixo *0900*. De forma simplificada, a operadora cobra um valor maior de tarifa pela ligação e uma parte do valor é transferida para o responsável pelo serviço *0900*. A utilização de telefones de terceiros para estabelecer ligações para números *premium* pode ser uma estratégia lucrativa para quem oferece o serviço.

A utilização de números *premium* em abusos SIP foi relatada em dezembro de 2010 quando uma quadrilha romena foi presa sob a acusação de ter causado um prejuízo de 11 milhões de euros abusando servidores SIP. A quadrilha realizou 1,5 milhão de ligações entre fevereiro e dezembro de 2010 [Silviu Bruma 2013].

4. Implementação

De forma a melhor compreender a natureza dos ataques e obter nível maior de detalhamento dos abusos destinados a servidores SIP foi desenvolvido um *software* específico que pudesse ser integrado à uma infraestrutura do Projeto *Honeypots* Distribuídos com cerca de 50 sensores baseados em *honeypots*.

O Projeto *Honeypots* Distribuídos é parte do honeyTARG Honeynet Project [CERT.br 2013a], mantido pelo CERT.br/NIC.br. Seu objetivo é aumentar a capacidade de detecção de incidentes, correlação de eventos e determinação de tendências de ataques no espaço Internet brasileiro. Atualmente o projeto conta com aproximadamente 50 *honeypots*, dispersos em 24 cidades e 12 estados brasileiros, coletando informações em redes parceiras, incluindo redes acadêmicas e comerciais.

Um módulo para o *software* Honeyd [Provos e Holz 2008] foi escrito para tratar as requisições do protocolo SIP que chegam até a porta 5060/UDP dos *honeypots* de forma a emular um serviço de central telefônica da família Asterisk [Asterisk 2013]. Como particularidade, a central telefônica emulada disponibiliza um número pré-definido de ramais protegidos através de uma senha de acesso de fácil adivinhação. Mesmo sem todas as funcionalidades de um servidor SIP implementadas, o *software* permite coletar as etapas iniciais de uma sessão SIP armazenando informações tais como origem do ataque e números telefônicos solicitados ao servidor. Por questões de privacidade os autores optaram por não gravar o áudio das seções, limitando-se à análise da sinalização SIP das tentativas de ligações. A implantação deste *software* no conjunto de *honeypots* nos possibilitou coletar e analisar uma quantidade significativa de dados (apresentados na seção 5).

O uso do *software* Dionaea [Baecher 2013] chegou a ser considerado pelos autores, mas necessitava-se um *software* que pudesse ser utilizado em conjunto com o Projeto Honeypots Distribuídos, que utiliza o Honeyd. Além disso, o suporte do Dionaea ao protocolo SIP não era suficientemente maduro quando do início deste trabalho.

```
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"
```

Listagem 1. Mensagens SIP coletadas por um *honeypot*.

Na Listagem 1 é apresentado um exemplo de uma conversação SIP coletada pelo módulo implementado, onde são apresentados dois métodos do protocolo SIP: *REGISTER* e *INVITE*, respectivamente. A mensagem *REGISTER* faz uma associação do usuário requisitante com o servidor SIP, necessária para estabelecer uma comunicação inicial. Já a mensagem *INVITE* inicializa uma ligação tendo como origem *101* (ramal existente na central telefônica) a um telefone externo "*00197259****839*" (números telefônicos obtidos nas tentativas de abuso foram sanitizados por questões de privacidade). Também

é possível identificar que a ligação aparenta ser iniciada a partir do aplicativo "*eyeBeam release 3006o stamp 17551*", segundo informação do *User Agent*.

Numa análise preliminar dos dados foi possível observar que as tentativas de abuso às centrais telefônicas apresentam um alto nível de redundância, ou seja, para aumentar as chances de sucesso, um número telefônico é solicitado de diferentes maneiras durante uma mesma seção de abuso (vide Listagem 2). Isto ocorre por conta de as centrais telefônicas poderem ser configuradas para realizar tanto ligações internas (ramais) quanto ligações externas (telefonia convencional). É comum, também, que cada central tenha uma configuração específica, como por exemplo, discar "*0*" para ligações externas, ou ainda discar "*0*" seguido da operadora de preferência. Os atacantes, por não saberem das configurações particulares de cada central telefônica, solicitam um mesmo número de diferentes maneiras.

```
2013-04-30 03:01:04 -0300: sip2db.pl:     00197259****839
2013-04-30 03:01:04 -0300: sip2db.pl:   00700197259****839
2013-04-30 03:01:04 -0300: sip2db.pl:       997259****839
2013-04-30 03:01:04 -0300: sip2db.pl:   12300197259****839
2013-04-30 03:01:04 -0300: sip2db.pl:     01397259****839
2013-04-30 03:01:04 -0300: sip2db.pl:     01597259****839
2013-04-30 03:01:04 -0300: sip2db.pl:     02197259****839
2013-04-30 03:01:04 -0300: sip2db.pl:   00727197259****839
2013-04-30 03:01:04 -0300: sip2db.pl:  01101197259****839
                                        <----------|
                     Máxima string comum:     97259****839
```

Listagem 2. Diferentes prefixos utilizados na solicitações de números telefônicos.

A Listagem 2 é um registro de um ataque coletado na nossa infraestrutura de *honeypots* onde podem-se identificar diversas variações para o mesmo número *97259****839*. É interessante observar os prefixos utilizados pelos atacantes, pois aparentemente eles têm conhecimento do sistema de telefonia brasileiro, incorporando os prefixos das operadoras nacionais em suas tentativas de abuso.

Para lidar com um alto nível de redundância foi desenvolvida uma heurística para identificar números de telefones discados e armazená-los de forma unificada. Em nossa heurística foram definidos dois níveis de redundância:

a) **Redundância intra-sessões**: identifica similaridades entre números solicitados numa mesma sessão (vide Listagem 2). Nesse exemplo, apesar de diversas tentativas diferentes de ligações , apenas uma sessão com o número "*97259****839*" será armazenada na base de dados.
b) **Redundância inter-sessões**: analisa similaridades entre números em diferentes sessões. Essa análise é útil para identificar abusos distribuídos – observadas em diferentes *honeypots* – mas com um padrão de similaridade.

O processo de unificação de ligações é realizado toda vez que uma nova sessão SIP é adicionada à base de dados. Dessa forma, diferentes sessões com números telefônicos semelhantes podem ter o campo "número telefônico" reescrito – como no exemplo de "*02197259****839*" para "97259****839" – tornando a base mais precisa para análise dos resultados.

5. Análise das tentativas de abusos

A análise dos resultados levou em conta todas as requisições que chegaram até os *honeypots* no período entre setembro de 2011 a abril de 2013. A Tabela 1 sumariza o volume de informações analisado.

Informação	Quantidade
Mensagens *REGISTER*	115.817.401
Mensagens *INVITE*	2.241.367
Mensagens "*INVITE*" unificadas	153.773
IPs únicos	13.443
ASes únicos	937
CCs únicos	89
Número total de dias	589

Tabela 1. Sumarização dos dados coletados.

A grande maioria dos ataques vistos foram mensagens do tipo *REGISTER*, oriundas de varreduras automatizadas. As mensagens *INVITE*, em menor volume, representam abusos a uma central telefônica, ou seja, são tentativas de ligações. Já as mensagens *INVITE* unificadas são aquelas que foram processadas segundo a heurística desenvolvida para evitar redundâncias (vide seção 4) e representam as tentativas de ligação, por sessão, para um único número. Também é possível observar a grande dispersão das origens dos ataques, ilustrada pela grande quantidade de países (CC) e sistemas autônomos (ASes) associados aos endereços IP de origem das conexões.

O escopo deste trabalho foi analisar a anatomia dos abusos aos serviços SIP, sendo assim, apenas as tentativas de ligações (mensagens do tipo *INVITE*) foram analisadas. Dessa forma, os resultados discutidos a seguir não levam em conta varreduras, mas sim ataques que necessariamente passaram pelas etapas descritas na seção 3 (Enumeração, Força Bruta e Abuso).

Inicialmente buscou-se observar como as tentativas de abuso a todos os *honeypots* comportavam-se na linha do tempo. Dessa forma seria possível esboçar possíveis sazonalidades e características na distribuição dos ataques. O comportamento é ilustrado no gráfico da Figura 3.

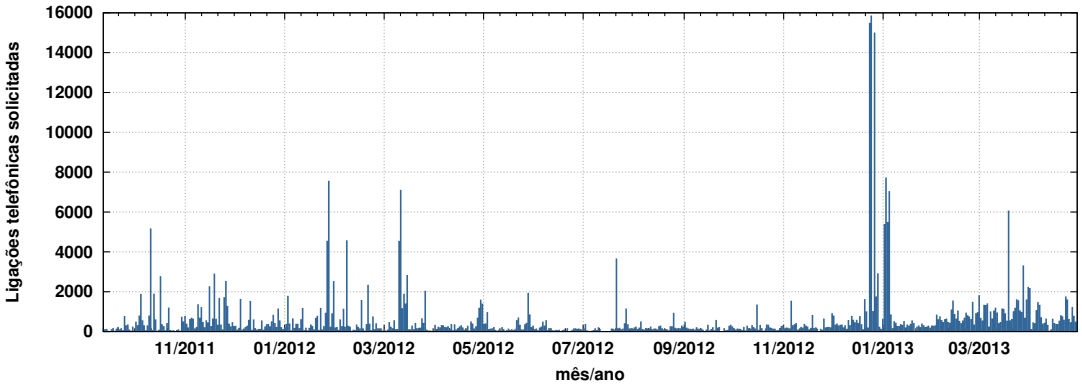
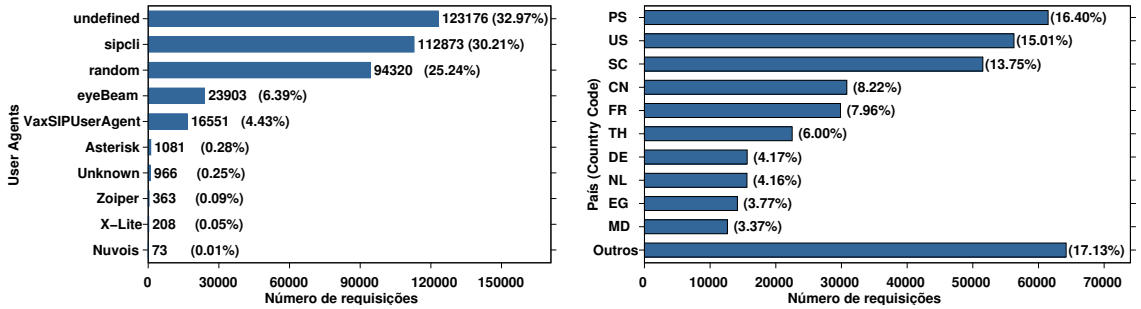


Figura 3. Total de ligações SIP solicitadas ao sistema de análise.

É fato que alguns *honeypots* são mais sondados que outros. Na Figura 3 pode-se visualizar alguns picos de solicitações. O maior pico (01/2013) corresponde a solicitações oriundas de apenas 2 IPs com origem na Tailândia. É importante também observar um sensível acréscimo nas tentativas no ano de 2013.

De forma complementar, analisar as características de cada tentativa de abuso pode nos revelar mais detalhes sobre o *modus operandi* dos ataques. O *User Agent*, por exemplo, é uma informação presente nas sondagens que permite identificar o equipamento ou *software* utilizado para gerar as requisições SIP. Conforme anteriormente exemplificado na Listagem 1, a informação do *User Agent* fornecida pelo dispositivo do atacante é coletada e armazenada na base de dados. Os *User Agents* mais observados nas tentativas nas tentativas de abuso são apresentados na Figura 4(a).

É interessante observar que o *User Agent* mais utilizado é "*undefined*" presente em 32.97% dos abusos coletados. Segundo a implementação da nossa ferramenta, quando o *User Agent* não é fornecido, a nossa ferramenta o armazena como *undefined*. A inexistência de *User Agent* na requisição não é um comportamento padrão de requisições legítimas. Esse comportamento sugere que a conexão está sendo realizada por uma ferramenta personalizada ou, ainda, uma ferramenta desenvolvida justamente para o propósito de abusar sistemas. O segundo *User Agent* mais observado é *sipcli* que corresponde a uma ferramenta de linha de comando para efetuar auditoria de sistemas, sugerindo um comportamento atípico. Como quinto *User Agent* mais frequente, observa-se o *VaxSIPUserAgent* correspondente a uma biblioteca para desenvolver aplicações SIP [VaxSoft 2013], o que também sugere a utilização de uma ferramenta personalizada. Os *User Agents* "*eyeBeam*", "*Zoiper*", "*Nuvois*" e "*X-Lite*" correspondem a *softphones* populares.



(a) Identificação do *User Agent* fornecida pelos clientes SIP que solicitaram ligações telefônicas.

(b) País de origem (baseado no IP de origem) das solicitações das ligações telefônicas.

Figura 4. Características dos abusos analisados.

Cabe destacar a existência de *User Agent* aparentemente aleatório. O *User Agent* fornecido era composto por 20 caracteres e para cada solicitação este era alterado aparentemente de forma aleatória (vide Listagem 3). Esse comportamento foi observado mesmo em requisições sequenciais oriundas de um mesmo IP. Tal característica possivelmente representa um *software* que busca evadir ferramentas que geram alertas baseados em assinaturas de *User Agents*.

```
2013-01-06 03:15:44 +0000: IP: 91.X.X.194 "UCB4ULAZsa3VWe8hY68a"
2013-01-06 03:15:44 +0000: IP: 91.X.X.194 "fD1tTwdaOzUzklECQGo0"
2013-01-06 03:15:44 +0000: IP: 91.X.X.194 "IqDbUvfmQ3ISyW7LZWEr"
2013-01-06 03:15:44 +0000: IP: 91.X.X.194 "lLhb4IZtNgA2FvkLoS9X"
2013-01-06 03:15:44 +0000: IP: 91.X.X.194 "HCfNq096O4tBo3DXmR99"
2013-01-06 03:15:44 +0000: IP: 91.X.X.194 "xEGJjYzLzF7nwwXBVAaG"
2013-01-06 03:15:44 +0000: IP: 91.X.X.194 "eqUpTTAD8jx4Qnmml85Y"
2013-01-06 03:15:45 +0000: IP: 91.X.X.194 "GDDvOyANwWOkMSbPy9ML"
2013-01-06 03:15:45 +0000: IP: 91.X.X.194 "QSLXOei4fooMt0gpw1bV"
```

Listagem 3. *User Agent* diferente em cada requisição.

Curiosamente o *User Agent Asterisk* também foi identificado nas sondagens. O *Asterisk* é um servidor VoIP, e não um *softphone* que realiza ligações. Esse comportamento pode indicar uma explícita modificação do *User Agent*, ou ainda que existam centrais telefônicas sendo abusadas de forma encadeada.

Além da análise do *User Agent*, buscou-se identificar em quantos *honeypots* um mesmo número telefônico foi requisitado. Esse parâmetro é importante para identificar a dispersão dos ataques na nossa rede de sensores. Constatou-se uma baixa dispersão das sondagens. Boa parte dos números telefônicos são observados em um pequeno número de *honeypots*, a maioria em apenas 1 único sensor. Esse fato vem levantar a hipótese de que a maioria dos números solicitados não se repetem com frequência.

Os abusos aos *honeypots* foram originados de diversos endereços IP. Observando o código do país – CC (*Country Code*, ISO 3166) – dos endereços foi possível identificar os países[1] que mais originaram requisições aos serviços emulados (vide Figura 4(b)). Dentre os principais países, chamam atenção os endereços IP da Palestina (PS), dos Estados Unidos da América (US) e das Ilhas Seicheles (SC), que são responsáveis por 45% das tentativas de ligações.

Ainda com relação à origem das tentativas de ligação a Tabela 2 apresenta característica dos 10 endereços IP que mais originaram abusos. Nessa tabela é possível observar: a quantidade (Quant.) de ligações telefônicas; endereço IP (sanitizado); país de origem; quantidade de DDIs únicos solicitados pelo IP; e por fim, a identificação do *User Agent*.

#	Quant.	IP	CC	DDIs	User Agent
01	19.562	113.X.X.205	CN	142	undefined
02	14.886	91.X.X.194	SC	45	random
03	11.511	83.X.X.16	NL	65	undefined
04	11.177	91.X.X.196	SC	19	random
05	11.003	91.X.X.195	SC	16	random
06	9.189	193.X.X.208	SC	42	random
07	7.566	71.X.X.9	US	66	VaxSIPUserAgent/3.0
08	7.486	50.X.X.99	US	28	undefined
09	6.943	194.X.X.36	MD	39	random
10	6.412	49.X.X.93	TH	39	undefined

Tabela 2. Principais endereços IP que originaram ligações.

Uma particularidade dos IPs que mais geraram abusos é o fato de que nenhum deles possuía *User Agents* comumente utilizados por *softphones* de ampla utilização. Os *User Agents undefined*, *VaxSIPUserAgent/3.0* e *random*, este previamente discutido na seção 5, não são esperados em conexões feitas a partir de clientes SIP. Além disso, observa-se que boa parte dos IPs solicitaram telefonemas para dezenas de DDIs.

Estas características dos IPs que geraram mais abusos sugerem que estes IPs podem ser centrais telefônicas clandestinas ou serviços de *proxy* utilizados para oferecer serviços de telefonia a custos reduzidos. O comportamento esperado de uma central telefônica ou *proxy* é uma grande dispersão dos números solicitados. Utilizando a ferramenta AfterGlow [AfterGlow 2013], que permite ilustrar um relacionamento entre entidades, foi possível evidenciar o comportamento de uma possível central telefônica. Na

[1]País de origem baseado na informação de alocação de IPs pelos Registros Regionais de Internet (RIRs).

Figura 5 são apresentados os *Country Codes* dos códigos DDI[2] dos números solicitados pelo IP mais observado em nossa análise. Este único IP tentou fazer ligações para números de 79 países diferentes. É importante ressaltar que todas estas tentativas utilizam o *User Agent* "*undefined*".

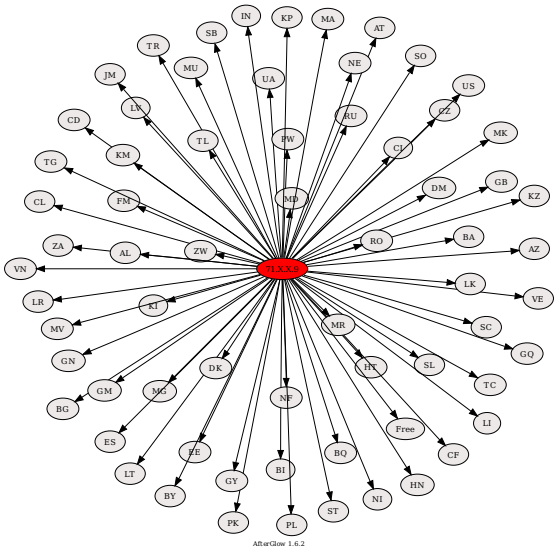


Figura 5. Códigos DDI identificados nas tentativas do IP 71.X.X.9.

Outra análise realizada foi com relação a quais números telefônicos foram solicitados aos nossos servidores emulados. Os números telefônicos mais solicitados aparentemente são de telefones móveis, de acordo com os prefixos. Além destes, alguns outros números frequentes puderam ser identificados através de pesquisas via mecanismos de busca na Internet. Os números telefônicos identificados foram classificados nas seguintes categorias:

- **Serviços financeiros** – como os serviços de atendimento ao cliente do *Bank of America* e *Citibank*.
- **Serviços de telefonia pré-pagos** – serviços de venda de cartões pré-pagos para ligações internacionais como Net2Phone.
- **Serviços de relacionamento** – serviços de atendimento a clientes de determinadas lojas *online*.

Chamou a atenção que o número mais solicitado de todos, com 6721 tentativas de ligação, é do "*Bank of America Credit Card Customer Service*". Fazendo uma análise mais aprofundada das origens destas tentativas verificou-se que apenas 9 endereços IP as originaram. Destes, 3 fazem parte da lista da Tabela 2 e todos os 9 possuem características que sugerem que sejam centrais clandestinas ou serviços de *proxy*.

6. Recomendações de Segurança

A análise dos dados coletados neste trabalho revelou características importantes do *modus operandi* utilizando pelos atacantes para abusar servidores SIP. Essa análise permitiu

[2]A determinação do CC em função do código DDI foi realizada utilizando-se a biblioteca Perl *Number::Phone::Country*.

mapear quais das falhas de configuração mais abusadas e quais práticas correntes de segurança dos serviços SIP [John Todd 2013] podem ser mais eficazes para impedir tais abusos.

Ficou evidente neste estudo que um serviço SIP disponível na rede sofre constantes varreduras e tentativas de abuso. Em aspectos gerais as sondagens visam identificar usuários que podem ter acesso ao sistema VoIP e, posteriormente, identificar as senhas dos seus respectivos ramais e então realizar ligações telefônicas. A maioria das sondagens poderiam ter sido evitadas seguindo uma ou mais das seguintes recomendações:

Usar senhas fortes – recomenda-se utilizar senhas longas e difíceis de serem adivinhadas. Boa parte dos dispositivos SIP requerem que a senha seja inserida apenas uma vez, dessa forma não existe necessidade de criar senhas de fácil memorização. A recomendação é a utilização de senhas longas e complexas, incluindo símbolo, números e letras maiúsculas e minúsculas.
Controlar o acesso aos ramais – é importante ser restritivo em termos de quais extensões (ramais) podem ser acessados a partir de um endereço IP externo. Nem todos os ramais necessitam estar acessível via Internet, por exemplo, ramais de teste e administração.
Criar nomes de usuários diferentes das extensões – os mecanismos automatizado de força bruta tentam nomes de usuários que correspondem aos números de ramais. Adicionalmente o uso de nomes de usuários menos óbvios dificultam o êxito de ataques de adivinhação baseados em dicionário.
Monitorar o uso de SIP na sua organização – monitorar não apenas os *logs* do servidor SIP é fundamental. Examinar a conta telefônicas em busca de ligações internacionais não usuais é uma maneira efetiva de detectar abusos.

É fundamental lembrar-se que a telefonia VoIP pode sofrer, num contexto amplo, aos mesmos ataques conhecidos da rede IP. Para isso, recomenda-se a segmentação da rede separando a rede de dados da rede de voz (VLANs). A utilização de mecanismos de segurança, como *firewall*, para uma proteção de perímetro deve ser considerada a fim de filtrar tráfego indesejado.

Por fim, ressalta-se a importância de manter os diferentes elementos da arquitetura SIP com as últimas correções de segurança. Ainda que não tenha sido o objetivo deste trabalho estudar as vulnerabilidades de *software*, é importante considerá-las como vetores de ataques. Falhas de segurança de *softphones*, *firmwares* dos dispositivos e *software* do PABX aumentam consideravelmente os ricos de comprometimento da estrutura SIP.

7. Conclusões e Trabalhos Futuros

Este trabalho coletou dados sobre as tentativas de abuso contra serviços VoIP, em especial aos serviços baseados no protocolo SIP, e analisou as características dos abusos realizados.

Foi possível constatar que ataques a serviços SIP estão ocorrendo de forma contínua e em grande volume no espaço da Internet brasileira. Uma importante contribuição deste trabalho foi a análise desses constantes ataques SIP de uma maneira que vai além da camada de rede, analisando os ataques do ponto de vista da camada de aplicação. Através da análise de mensagens do protocolo SIP foi possível demonstrar que existe um grande número de abusos cujo enfoque está na realização de ligações.

Uma parcela representativa dessas sondagens tem como objetivo abusar a infraestrutura para ligações internacionais. As ligações solicitadas não possuem um padrão claro, vão desde números comerciais, número de telefones móveis, serviços gratuitos e instituições financeiras. Com base nos dados observados não é possível afirmar com certeza as motivações dos abusos, mas é plausível levantar as seguintes hipóteses:

a) Revenda de serviços telefônicos VoIP por um preço mais atrativo valendo-se de centrais clandestinas ou comprometidas que abusaram serviços de terceiros;
b) Consulta de informações sensíveis de usuários, como dados de cartões de crédito ou saldo bancário de maneira anônima, através do abuso de centrais de terceiros;
c) Uso para realizar ligações pessoais sem custos e anônima;
d) Uso de ramais para ligações a números telefônicos do tipo *premium*.

Independente do uso, sabe-se que as centrais telefônicas baseadas em VoIP estão cada vez mais populares nas instituições. A análise dos resultados deste trabalho revelou a anatomia dos abusos, e com isso, identificar quais recomendações de segurança são essenciais para evitar os ataques identificados.

Como trabalhos futuros seria importante expandir este estudo para considerar os pontos não tratados neste trabalho, bem como ampliar e aprimorar a análise dos dados coletados. A emulação de diferentes centrais telefônicas nos sensores poderia revelar diferentes ataques. Da mesma forma, sabe-se que uma implementação mais completa das mensagens SIP poderia ser útil para tratar as limitações da central telefônica emulada, que interage de forma limitada com os atacantes. Do ponto de vista de análise seria importante incluir suporte para identificação de chamadas locais, pois atualmente considera-se a utilização de um código DDI em todas as solicitações.

Referências

AfterGlow (2013). AfterGlow – Link Graph Visualization. Disponível em: `http://afterglow.sourceforge.net/`.

Asterisk (2013). Asterisk – The Open Source Telephony Projects. Disponível em: `http://www.asterisk.org/`.

Baecher (2013). Dionaea. Disponível em: `http://dionaea.carnivore.it/`.

Ceron, J., Steding-Jessen, K., e Hoepers, C. (2012). Anatomy of SIP Attacks. *;login: USENIX*, 37(6).

Ceron, J., Tarouco, L., e Granville, L. (2010). Arquitetura baseada em assinaturas para mitigação de botnets. Em Duarte, O. C. M. B., editor, *Anais do X Simpósio Brasileiro em Segurança da Informação e de Sistemas Computacionais, SBSEG 2010*, Fortaleza, Brazil. Sociedade Brasileira de Computação (SBC).

CERT.br (2013a). CERT.br – Distributed Honeypots Project. Disponível em: `http://honeytarg.cert.br/honeypots/`.

CERT.br (2013b). Estatísticas do CERT.br – Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil. Disponível em: `http://cert.br/stats/`.

El-moussa, F., Mudhar, P., e Jones, A. (2010). Overview of sip attacks and countermeasures. Em *Information Security and Digital Forensics*, volume 41 of *Lecture Notes*

of the Institute for Computer Sciences, Social Informatics and Telecommunications Engineering, páginas 82–91. Springer Berlin Heidelberg.

El-Sawda, S. (2010). Sip seclite: Sip security solution all in one. *Journal of Next Generation Information Technology*, páginas 86–99.

Hoepers, C., Steding-Jessen, K., Cordeiro, L. E. R., e Chaves, M. H. P. C. (2005). A National Early Warning Capability Based on a Network of Distributed Honeypots. Em *Proceedings of the 17th Annual FIRST Conference on Computer Security Incident Handling*, Singapore.

IETF (2002). RFC3261 - SIP: Session Initiation Protocol. Technical report, IETF.

John Todd (2013). Seven steps to better SIP security. `http://blogs.digium.com/2009/03/28/sip-security/`.

Keromytis, A. D. (2010). Voice-over-IP security: Research and practice. *IEEE Security and Privacy*, 8(2):76–78.

Liu, X. e Tu, C. (2011). Research on security of voip network. Em Dai, M., editor, *Innovative Computing and Information*, volume 231 of *Communications in Computer and Information Science*, páginas 59–65. Springer Berlin Heidelberg.

Provos, N. e Holz, T. (2008). *Virtual Honeypots - From Botnet Tracking to Intrusion Detection*. Addison-Wesley.

Rezac, F., Voznak, M., Tomala, K., Rozhon, J., e Vychodil, J. (2011). Security analysis system to detect threats on a sip voip infrasctructure elements. *Advances in Electrical and Electronic Engineering*, 9(5).

Rosenberg, J. e Schulzrinne, H. (2002). Session initiation protocol (sip): Locating sip servers. RFC 3263, Internet Engineering Task Force.

Sandro Gauci (2013). SIPVicious - Tools for auditing SIP based VoIP systems. Disponível em: `http://blog.sipvicious.org/`.

SANS (2013). Internet Storm Center – Port Details: Port 5060. Disponível em: `https://isc.sans.edu/port.html`.

Santos, C., Bezerra, R., Ceron, J., Granville, L., e Rockenbach Tarouco, L. (2010). On using mashups for composing network management applications. *Communications Magazine, IEEE*, 48(12):112–122.

Silviu Bruma (2013). Adevarul - News in Bucharest. Disponível em: `http://www.adevarul.ro/locale/bucuresti/40_de_tineri_au_facut_11_milioane_de_euro_prin_telefonie_prin_internet_0_389961122.html`.

Valli, C. (2010). Developing voip honeypots: a preliminary investigation into malfeasant activity. *Journal of Digital Forensics, Security and Law 5(2)*, páginas 35–44.

VaxSoft (2013). Vaxvoip sip sdk. Disponível em: `http://www.vaxvoip.com/`.

