TLP: CLEAR

RELATÓRIO DE PESQUISAS

Abuso de Infraestruturas SIP: A Porta 5060 como Entrada para Fraudes e Intrusões

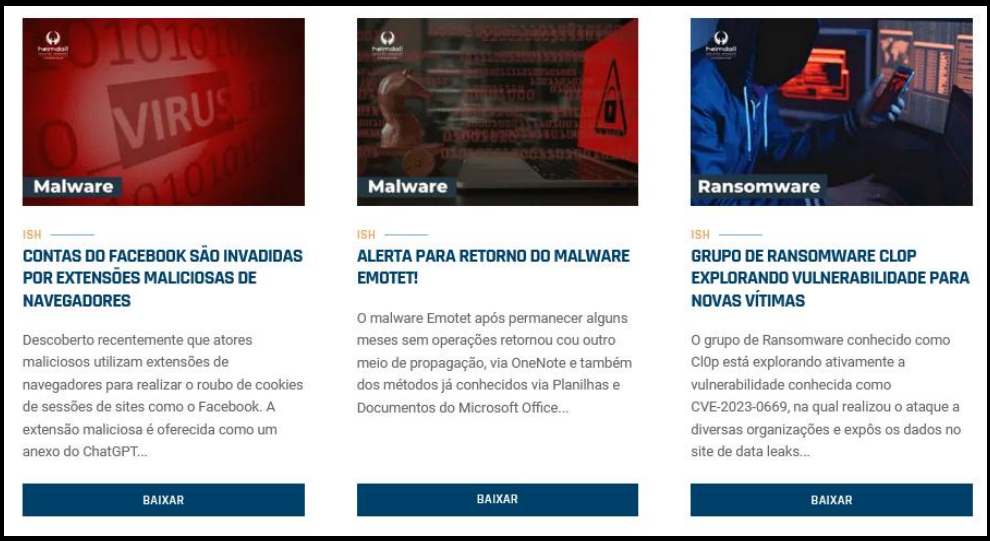
heimdall
security research

Acesse a nossa nova comunidade através do WhatsApp!

Heimdall Security Research

Acesse boletins diários sobre agentes de ameaças, *malwares*, indicadores de comprometimentos, TTPs e outras informações no *site* da ISH.

Boletins de Segurança – Heimdall



SUMÁRIO

LISTA DE TABELAS

LISTA DE FIGURAS

1 INTRODUÇÃO EXECUTIVA

Este relatório de segurança, desenvolvido pela equipe de inteligência **Heimdall da ISH Tecnologia**, tem como objetivo proporcionar uma compreensão aprofundada e um dimensionamento preciso das ameaças cibernéticas identificadas. O documento está estruturado em três níveis de abordagem: ***Estratégico***, ***Tático*** e ***Operacional***, garantindo uma visão completa e integrada das ameaças e ações recomendadas.

2 ESTRATÉGICO

2.1 INTRODUÇÃO SOBRE A AMEAÇA

A exposição indevida de serviços VoIP na Internet tem sido amplamente explorada por **grupos especializados em fraude financeira, extorsão e negação de serviço**, com foco principal em **IP-PBX corporativos, SBCs mal configurados e softswitches**.

A porta **5060/UDP e 5060/TCP** é utilizada por padrão pelo protocolo **SIP (Session Initiation Protocol)**, responsável por iniciar, manter e encerrar sessões de comunicação de voz e vídeo em ambientes VoIP. Devido à sua ampla utilização e à necessidade frequente de exposição externa para integração com operadoras, filiais e usuários remotos, serviços SIP tornam-se **alvos prioritários de campanhas automatizadas de exploração**.

Os ataques não exigem exploração de vulnerabilidades complexas. Na maioria dos casos, o comprometimento ocorre por meio de:

- Exposição direta do serviço SIP à Internet
- Credenciais fracas ou reutilizadas em ramais e troncos
- Falta de mecanismos de rate-limit e detecção de anomalias
- Dial plans permissivos permitindo chamadas internacionais ou premium

O vetor é altamente atrativo para criminosos devido ao **baixo custo operacional**, **alto grau de automação** e **retorno financeiro rápido**, principalmente por meio de **fraude de chamadas internacionais**, onde o prejuízo pode atingir dezenas ou centenas de milhares de reais em poucas horas.

Além do impacto financeiro, ataques contra SIP também são utilizados como:

- Vetor de **negação de serviço (DoS)** contra centrais telefônicas
- Meio para **interrupção de operações críticas** (call centers, hospitais, serviços públicos)
- Ferramenta de extorsão indireta, exigindo pagamento para cessar ataques

2.2 DISTRIBUIÇÃO MUNDIAL DE SIP 5060

Por meio de mecanismos de varredura de superfície de ataque como o Shodan, demonstra que **milhões de dispositivos permanecem expondo serviços SIP na porta 5060 diretamente à Internet**, distribuídos globalmente, com maior concentração em países com ampla adoção de VoIP corporativo e infraestrutura de telecom descentralizada. Essa exposição massiva evidencia que o protocolo SIP continua sendo um vetor altamente explorável em escala global, favorecendo campanhas automatizadas de varredura, enumeração e exploração conduzidas por atores financeiramente motivados. A ampla distribuição geográfica também contribui para a complexidade de mitigação, uma vez que ataques frequentemente se originam de múltiplas regiões e infraestruturas terceirizadas, dificultando bloqueios baseados exclusivamente em geolocalização ou reputação de IP.

Figura 1 – Distribuição global de dispositivos com serviço SIP (porta 5060) expostos na Internet.

2.3 Distribuição global de dispositivos com serviço SIP (porta 5060) expostos na Internet

A análise de dispositivos expostos no território nacional revela uma **concentração significativa de serviços SIP acessíveis publicamente em grandes centros urbanos e polos regionais**, com destaque para cidades como São Paulo, Montes Claros, Rio de Janeiro, Divinópolis e Brasília. Esse padrão indica que não apenas grandes capitais, mas também cidades de médio porte, apresentam elevada exposição de infraestruturas VoIP corporativas, sugerindo adoção ampla de IP-PBX em empresas, provedores regionais e instituições públicas. A presença desses serviços em regiões fora dos grandes centros reforça o caráter oportunista das campanhas de exploração, nas quais atacantes não realizam segmentação por setor ou porte organizacional, explorando qualquer ativo acessível que permita monetização por meio de fraude de tarifação, abuso de recursos de voz ou negação de serviço.

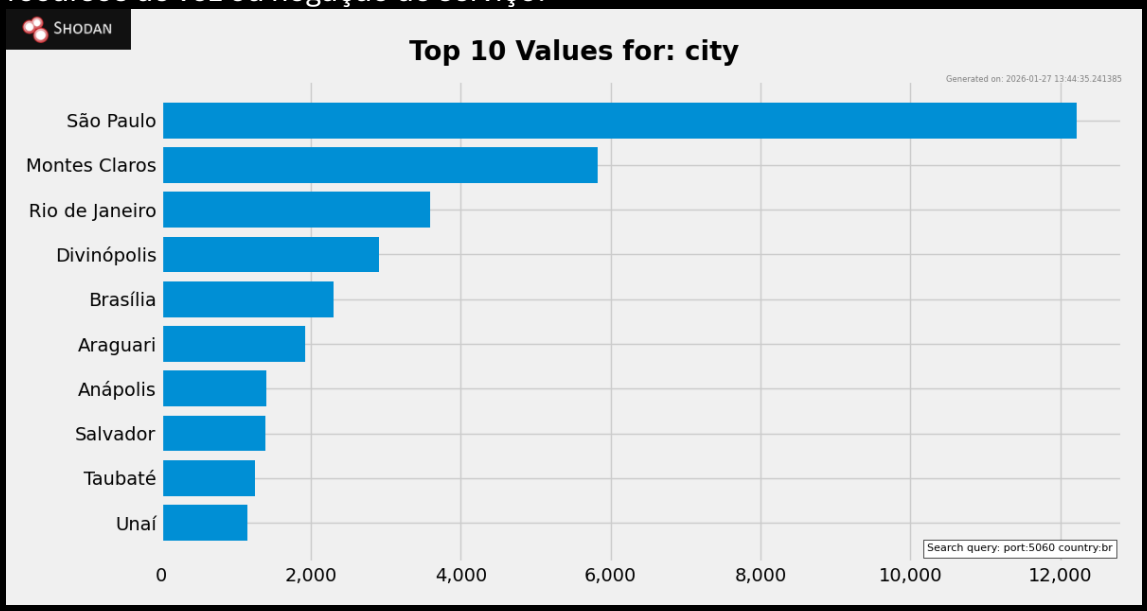


Figura 2– Distribuição geográfica de dispositivos com SIP (porta 5060) exposto no Brasil por cidade.

2.4 Vitimologia e Segmentos afetados

Principais segmentos impactados

- Empresas de médio e grande porte **com IP-PBX próprios**
- Provedores de telecom e VoIP
- Call centers e centrais de atendimento
- Instituições financeiras **com infraestrutura de voz integrada**
- Órgãos públicos e hospitais **com telefonia IP exposta**

Fatores de risco recorrentes

- PBX exposto diretamente sem SBC (Session Border Controller)
- Falta de controle de origem por IP (ACL)
- Uso de portas padrão (5060) sem segmentação

- Integração do PBX com Active Directory
- Ausência de monitoramento de custo e perfil de chamadas

Perfil das vítimas

As vítimas não são selecionadas de forma manual. O modelo é **oportunista e em larga escala**, onde sistemas expostos são automaticamente explorados. Organizações com **menor maturidade em segurança de telecom** tendem a sofrer recorrência de incidentes.

3 TÁTICO

3.1 MODELO DE NEGÓCIO DA AMEAÇA

O principal modelo de monetização associado à exploração da porta SIP 5060 é a **IRSF (International Revenue Share Fraud)**, na qual o atacante inicialmente compromete ramais ou troncos SIP por meio de força bruta, reutilização de credenciais ou falhas de configuração, passando então a realizar chamadas para destinos internacionais premium, de alto custo, nos quais parte da tarifa retorna aos grupos criminosos por meio de operadoras cúmplices ou serviços de *revenue sharing*. Além da IRSF, outros modelos de abuso são frequentemente observados, como a **revenda de acesso SIP comprometido para outros grupos criminosos**, permitindo que terceiros utilizem a infraestrutura da vítima para diferentes finalidades; **SPIT (Spam over Internet Telephony)**, utilizado em campanhas de golpe, engenharia social ou robocalls automatizados; **ataques de negação de serviço sob demanda**, nos quais floods de mensagens SIP (REGISTER, INVITE, OPTIONS) são utilizados para degradar ou interromper serviços de telefonia corporativa; e o **uso da infraestrutura comprometida como relay para outras campanhas**, funcionando como ponto intermediário para mascarar a origem de tráfego malicioso.

3.2 ANÁLISE DA KILL CHAIN DA AMEAÇA

3.3 RECONHECIMENTO E DESCOBERTA DE SUPERFÍCIE

Nesta fase, o ator realiza **varredura em larga escala da Internet** para identificar sistemas que expõem serviços SIP, principalmente na porta **5060/UDP e TCP**, além de portas alternativas configuradas por administradores. A descoberta ocorre por meio de *horizontal scanning* em blocos de IP, uso de motores de busca de ativos expostos (ex.: fingerprints de serviços VoIP) e varreduras distribuídas a partir de múltiplas origens para reduzir a eficácia de mecanismos de bloqueio baseados em IP.

Os atacantes utilizam mensagens SIP do tipo **OPTIONS, INVITE e REGISTER** para confirmar a presença do serviço, identificar respostas específicas do servidor e coletar informações de *banner grabbing* e headers SIP, permitindo o **fingerprinting do tipo de PBX, softswitch ou SBC**, bem como a versão do software, quando exposta. Em ambientes mal configurados, respostas distintas permitem inferir políticas de autenticação e existência de ramais válidos.

3.4 ENUMERAÇÃO E MAPEAMENTO LÓGICO DO AMBIENTE VOIP

Após a confirmação do serviço, o atacante passa para a **enumeração sistemática de ramais, contas SIP e troncos**, explorando diferenças sutis nas

respostas do servidor a mensagens REGISTER e INVITE. Essa etapa permite identificar:

- Extensões válidas
- Políticas de autenticação
- Restrições de origem e roteamento
- Comportamento do dial plan

Paralelamente, ocorre o **mapeamento da lógica de chamadas**, incluindo tentativas de discagem para diferentes prefixos, a fim de validar se há permissão para chamadas internacionais, destinos premium ou rotas específicas. Essa fase também permite avaliar se o ambiente possui mecanismos de rate limiting, CAPTCHA lógico ou bloqueio automático por falha de autenticação

3.5 Acesso Inicial e Comprometimento de Identidades SIP

Com ramais válidos identificados, o atacante inicia campanhas de **força bruta distribuída**, tentando combinações de senha, muitas vezes utilizando listas derivadas de vazamentos corporativos, padrões fracos (ex.: ramal = senha) ou credenciais padrão de fabricantes.

Em ambientes com falhas de configuração, o acesso também pode ocorrer por:

- Autenticação desabilitada em determinados troncos
- Regras permissivas de NAT e firewall
- Exposição administrativa do PBX via interfaces web integradas

Uma vez bem-sucedido, o atacante obtém **controle funcional sobre uma identidade SIP legítima**, permitindo registrar-se no servidor como se fosse um ramal corporativo válido.

3.6 Expansão de Capacidades e Preparação para Monetização

Após obter acesso, o atacante valida os **limites operacionais do ramal comprometido**, testando:

- Capacidade simultânea de chamadas
- Tipos de destino permitidos
- Horários e limiares de detecção

Essa fase é crítica para ajustar o volume e o ritmo das chamadas, evitando detecção precoce. Em alguns casos, ocorre a **alteração de parâmetros de roteamento ou criação de novos ramais**, quando há comprometimento administrativo do PBX, ampliando o acesso e reduzindo dependência de um único ponto comprometido.

O ambiente passa então a ser tratado como **infraestrutura operacional do grupo**, pronto para monetização contínua ou revenda.

3.7 Execução do Objetivo: Fraude, Abuso ou Ataque

Com a infraestrutura preparada, inicia-se a fase de impacto principal, que pode assumir múltiplas formas:

- IRSF (International Revenue Share Fraud): geração massiva de chamadas para destinos internacionais premium, geralmente concentradas em janelas noturnas ou fins de semana.
- SPIT e campanhas automatizadas de voz: uso do ramal para golpes telefônicos, engenharia social e robocalls.
- Ataques de negação de serviço: envio massivo de mensagens SIP ou saturação de canais, degradando a disponibilidade do serviço.

O volume de tráfego é ajustado dinamicamente para maximizar retorno financeiro antes que mecanismos de detecção sejam acionados.

3.8 Persistência e Resiliência Operacional

Para manter a operação, o atacante:

- Preserva credenciais válidas comprometidas
- Rotaciona IPs de origem para evitar bloqueios
- Alterna entre diferentes ramais e troncos
- Retorna periodicamente para testar se o acesso foi restaurado após mitigação

Em ambientes sem revisão completa de credenciais e sem mudança de dial plan, a reinfecção lógica é comum, com múltiplos episódios de fraude ocorrendo ao longo do tempo.

3.9 Impacto Organizacional

Os impactos observados incluem:

- Prejuízo financeiro direto elevado, frequentemente identificado apenas na fatura telefônica
- Interrupção de operações críticas, como atendimento ao cliente e suporte técnico
- Exaustão de recursos do PBX, levando a indisponibilidade total
- Risco reputacional, especialmente quando o ambiente é usado para golpes telefônicos

Potencial **pivot para outros sistemas internos**, quando o PBX possui integração com redes corporativa.

3.10 TABELA MITRE ATT&CK

Este tópico apresenta as Táticas, Técnicas e Procedimentos (TTPs) identificados nesta ameaça, conforme o framework MITRE ATT&CK, oferecendo uma visão tática detalhada sobre o comportamento do adversário. O objetivo é permitir o mapeamento das técnicas utilizadas pelos atacantes, facilitando a implementação de contramedidas eficazes e o aprimoramento das defesas de segurança.

Tática	Técnica	Detalhes
Reconhecimento	Active Scanning (T1595)	Varredura para identificar serviços SIP expostos (porta 5060/UDP/TCP) e endpoints.
Acesso Inicial	External Remote Services (T1133)	Uso do serviço SIP exposto como ponto de entrada (PBX/Proxy acessível externamente).
Credenciais	Brute Force (T1110)	Tentativas de senha em extensões/contas SIP; picos de REGISTER falhos.
Persistência	Valid Accounts (T1078)	Uso continuado de conta/ramal comprometido para originar chamadas.
Impacto	Network Denial of Service (T1498)	Flood de mensagens SIP ou exaustão de recursos do PBX/SBC (queda/degradação).

Tabela 1 – Tabela MITRE ATT&CK.

4 RECOMENDAÇÕES

São elencados abaixo pela ISH, medidas que poderão ser adotadas visando a mitigação da referida ameaça como por exemplo:

- **Não expor IP-PBX diretamente à Internet**, utilizando sempre um **Session Border Controller (SBC)** ou firewall de borda especializado para SIP.
- **Restringir acesso à porta 5060 por ACL**, permitindo apenas IPs e ASNs das operadoras, filiais e parceiros autorizados.
- **Migrar para SIP sobre TLS (porta 5061)** sempre que possível, reduzindo interceptação e abuso de sinalização.
- **Utilizar senhas fortes e únicas por ramal e tronco SIP**, eliminando credenciais padrão ou baseadas no número do ramal.
- **Habilitar bloqueio automático e rate limiting** para tentativas repetidas de REGISTER, INVITE e OPTIONS.
- **Bloquear chamadas internacionais e destinos premium por padrão**, liberando apenas para usuários que realmente necessitam.
- **Implementar alertas de anomalia de chamadas e custo**, especialmente fora do horário comercial.
- **Centralizar logs de PBX, SBC e firewall em SIEM**, com regras específicas para brute force e enumeração SIP.
- **Realizar varreduras periódicas de superfície externa (EASM)** para identificar serviços SIP expostos indevidamente.
- **Revisar dial plans e políticas de roteamento após qualquer incidente**, garantindo remoção de persistência lógica do atacante.

5 REFERÊNCIAS

- **Heimdall *by* ISH Tecnologia**
- **CTI Purple Team *by* ISH Tecnologia**
- **MITRE ATT&CK**

6 AUTORES

- **Thiago Cesar Maciel da Paixão – Threat Intelligence**

heimdall
security research
A DIVISION OF ISH