SENADO FEDERAL
Diretoria-Geral

Diretoria Geral
Folha:
Rubrica

Processo nº 00200.026985/2013-70
Processos apensos nºs 00200.027239/2013-01 e 00200.027193/2013-12

Brasília, 05 de dezembro de 2013.

Assunto: CPI-ESP – Requerimento nº 39/2013.

Excelentíssima Senhora Senadora Vanessa Grazziotin,

Considerando os termos do Requerimento nº 39 CPI-ESP, aprovado na 10ª reunião da Comissão Parlamentar de Inquérito da Espionagem, esta Diretoria-Geral encaminhou expediente ao Prodasen, à Secretaria de Polícia e à Secretaria de Infraestrutura com vistas à prestação das informações requeridas.

Encaminho o presente processo a Vossa Excelência para conhecimento das informações apostas nos autos relativas ao modo como se assegura a segurança das comunicações havidas no Senado Federal.

Respeitosamente,

ANTÔNIO HELDER MEDEIROS REBOUÇAS
Diretor-Geral

Subsecretaria de Apoio às Comissões Especiais e Parlamentares de Inquérito
Recebido em 09/12/2013
Às _____ horas.
Antônio Oscar Guimarães Lóssio
Secretário de Comissão

U:\Dger\Assessoria Técnica\2013\DESPACHOS\GABINETES - fabi

SENADO FEDERAL
Fl. nº 01
SSCEPI

SENADO FEDERAL
Diretoria-Geral

Diretoria Geral
Folha:

Memorando nº 116/2013-DGER

Brasília-DF, 04 de dezembro de 2013.

A Sua Excelência a Senhora
Senadora **VANESSA GRAZZIOTIN**

Assunto: Solicitação de informações sobre proteção das comunicações do Senado Federal, consoante o Requerimento nº 039/13 CPI-ESP.

Excelentíssima Sra. Senadora Vanessa Grazziotin,

Face à solicitação de informações sobre a proteção das comunicações do Senado Federal, nos termos do Requerimento nº 039/13 CPI-ESP, informo que esta Diretoria-Geral, mediante os Memorandos nºs 107, 108 e 109/2013 – DGER (cópias às fls. 4-6), já determinou às Secretarias competentes que respondam aos respectivos questionamentos.

Destarte, encaminho os autos a Vossa Excelência para conhecimento.

Respeitosamente,

ILANA TROMBKA
Diretora-Geral em exercício

U:\Dger\Assessoria Técnica\2013\Memorandos\Memorandos DGER – sergiovh

SENADO FEDERAL
Fl. nº
SSCEPI

SENADO FEDERAL
Diretoria-Geral

Memorando nº 107/2013 - DGER

Brasília, 08 de novembro de 2013.

A Sua Senhoria o Senhor
VICTOR GUIMARÃES VIEIRA
Diretor da Secretaria de Tecnologia da Informação - PRODASEN
Senado Federal

Assunto: Solicita a prestação de informações.

Senhor Diretor,

Considerando os termos do Requerimento nº 39 CPI-ESP, cópia anexa, aprovado na 10ª reunião da Comissão Parlamentar de Inquérito da Espionagem, realizada no dia 30 de outubro do corrente, encaminho a Vossa Senhoria a presente solicitação.

Tendo em vista a necessidade de a CPI da Espionagem conhecer como se assegura a segurança das comunicações havidas no Senado Federal, solicito a Vossa Senhoria que subsidie esta Diretoria-Geral, respondendo às questões que se encontrem dentro da esfera de competência dessa Secretaria.

Atenciosamente,

ANTÔNIO HELDER MEDEIROS REBOUÇAS
Diretor-Geral

U:\Dger\Assessoria Técnica\2013\MEMORANDOS\MEMORANDO DGER\SPOL – fabi

Memorando nº. 21/2013 – PRDSTI/GBPRD

Brasília-DF, 19 de novembro de 2013.

A Sua Senhoria o Senhor
ANTÔNIO HELDER MEDEIROS REBOUÇAS
Diretor-Geral do Senado Federal

Assunto: **CPI-ESP – Requerimento Nº 039/13.**

Senhor Diretor-Geral,

Em atendimento ao Memorando nº 107/2013-DGER, que trata da necessidade da CPI da Espionagem conhecer como se assegura a segurança das comunicações havidas no Senado Federal, encaminho as respostas às questões que se encontram dentro da esfera de competência desta Secretaria de Tecnologia da Informação – PRODASEN:

1) Que sistemas de proteção o Senado Federal utiliza para resguardar o sigilo das comunicações realizadas pelos seguintes meios:
Item c) mensagens eletrônicas pela internet (email).

O serviço de email eletrônico disponibilizado pelo Senado Federal é baseado em um conjunto de soluções, parte delas baseadas em software livre e parte baseada em soluções proprietárias.

No que tange ao resguardo do sigilo das comunicações, são utilizadas as seguintes medidas:

1) **Criptografia nas mensagens internas ao serviço de email:** As mensagens trocadas internamente são criptografadas durante todo o canal de comunicação, ou seja, entre o usuário que envia e o usuário que recebe, todo o trâmite da mensagem é feito de forma criptografada. Todavia, uma mensagem trocada entre um usuário interno ao serviço de correio do Senado e um usuário externo ao serviço, ou seja, que não possua caixa de correio nesse serviço, a mensagem trafega sem criptografia por exigência do próprio protocolo de troca de emails na internet conhecido como SMTP – *Simple Mail Tranfer Protocol*. Nesse último caso, para que o conteúdo da mensagem seja mantido seguro é necessário que o usuário interno ao Senado e o usuário externo acordem alguma forma de proteção do conteúdo, que poderá ser a aplicação de criptografia de chaves públicas por meio da utilização de uma infraestrutura de chaves públicas reconhecida pelos dois usuários, que poderia ser, por exemplo, a ICP-Brasil. Outra aplicação de criptografia também ocorre para a leitura dos emails, tanto por meio dos clientes

de email instalado nas estações de trabalho do Senado, como também pelo acesso feito à página da internet que disponibiliza o webmail;

2) **Antivírus de estações:** Os computadores do Senado Federal possuem um serviço de antivírus que protege as estações de trabalho de ameaças conhecidas como *malwares* (vírus, worms, cavalos de troias) que podem interagir com o serviço de email em nome do usuário;

3) **Antispam:** Antes de receber os emails provenientes da internet, ou seja, cuja origem seja em serviços de correio externos ao Senado Federal, todas as mensagens são filtradas por equipamentos conhecidos como antispam, cuja finalidade é identificar e bloquear mensagens que possam implicar em riscos para o serviço de correio eletrônico. Alguns exemplos de mensagens bloqueadas são as que contêm vírus e as caracterizadas como fraudulentas, que contém links para sites criados com a finalidade de obter informações dos usuários como senhas pessoais.

4) **Sistema de Prevenção de Intrusão (IPS)** - Trata-se de um equipamento cuja finalidade é avaliar todo o tráfego buscando identificar se o mesmo é algum ataque, e em caso positivo, realizar o bloqueio do mesmo.

5) **Firewall de rede** – Equipamento destinado a filtrar todo o tráfego de internet que chega e que sai, e aplica um conjunto de regras técnicas definindo que tipo de tráfego é autorizado. O tráfego não autorizado é bloqueado.

2) Como o Senado Federal resguarda a integridade das bases de dados do PRODASEN? Quais medidas de segurança são adotadas para defender os dados armazenados dos frequentes ataques enfrentados? Quais medidas de segurança são adotadas para defender os dados armazenados dos frequentes ataques enfrentados?

A integridade das bases de dados do PRODASEN e sua proteção contra os ataques enfrentados são garantidas por meio de várias medidas de segurança, quais sejam:

1) **Cópias de segurança:** Diversas rotinas de cópias de segurança (*backup*) são implementadas com a finalidade de viabilizar a restauração dos dados em momentos distintos;

2) **Controle de acesso:** o acesso aos dados é em sua maioria definido conforme a necessidade do gestor da informação, o qual determina quais os usuários devem ter permissões para acessar ou alterar esses dados;

3) **Redundância:** a maioria das bases de dados está mantida em equipamentos com redundância, a fim de permitir que o dado permaneça íntegro em caso de situações de falha de equipamentos;

4) **Antivírus de estações, antispam, Sistema de prevenção de Intrusão (IPS), Firewall de rede:** Conforme já apresentado no quesito anterior, esses dispositivos são independentes e têm função complementar em Segurança da Informação.

5) **Proteção física:** O datacenter do Senado protege os equipamentos quanto a intempéries físicas, com por exemplo: incêndios, inundações. O acesso a esse datacenter é controlado por guarda, e a autorização para entrada é feita mediante prévia autorização conforme norma da coordenação de infraestrutura de TI.

3) No sistema de proteção das comunicações do Senado Federal, quais as competências da Polícia Legislativa e do Prodasen?

De acordo com o Ato da Comissão Diretora nº 14, de 2013, as atribuições do Prodasen são as seguintes:
"Art. 264. À Secretaria de Tecnologia da Informação – PRODASEN compete prover, por meio de recursos próprios ou de terceiros, serviços, soluções, suporte e infraestrutura de tecnologia da informação; gerir a tecnologia da informação do Senado Federal; implementar a estratégia de tecnologia da informação; propor inovações nos processos finalísticos e de apoio do Senado, com uso de tecnologia da informação; propor padrões, normas, métodos e processos para uso da tecnologia da informação e monitorar sua aplicação; integrar iniciativas de adoção de novas soluções de tecnologia da informação por outras unidades da Casa; **gerir a segurança da informação do Senado no âmbito da tecnologia da informação**; gerenciar os riscos operacionais do Senado com origem em tecnologia da informação; e executar outras atividades correlatas." (grifo nosso).

Nesse sentido, no desenvolvimento dos processos de trabalho do Prodasen busca-se implementar a segurança da informação associando-a à questão tecnológica, seja por meio de dispositivos de proteção, como equipamentos, configurações ou softwares de segurança, seja no processo de desenvolvimento ou contratações de soluções.

Atenciosamente,

Victor Guimarães Vieira
Diretor do Prodasen

SENADO FEDERAL
Diretoria-Geral

Memorando nº 109/2013 - DGER

Brasília, 08 de novembro de 2013.

A Sua Senhoria o Senhor
PEDRO RICARDO ARAÚJO CARVALHO
Diretor da Secretaria de Polícia do Senado Federal
Senado Federal

Assunto: Solicita a prestação de informações.

Senhor Diretor,

Considerando os termos do Requerimento nº 39 CPI-ESP, cópia anexa, aprovado na 10ª reunião da Comissão Parlamentar de Inquérito da Espionagem, realizada no dia 30 de outubro do corrente, encaminho a Vossa Senhoria a presente solicitação.

Tendo em vista a necessidade de a CPI da Espionagem conhecer como se assegura a segurança das comunicações havidas no Senado Federal, solicito a Vossa Senhoria que subsidie esta Diretoria-Geral, respondendo às questões que se encontrem dentro da esfera de competência dessa Secretaria.

Atenciosamente,

ANTÔNIO HELDER MEDEIROS REBOUÇAS
Diretor-Geral

Praça dos Três Poderes | Senado Federal | Anexo I | 3º andar | CEP: 70165-900 | Brasília-DF
Telefone: +55 (61) 3303-4000 | Fax: +55 (61) 3303-4020 | dger@senado.gov.br

SENADO FEDERAL
Secretaria de Polícia

Memorando nº 086/2013 – SPOL

Brasília, 27 de novembro de 2013.

A Sua Senhoria o Senhor
ANTÔNIO HELDER MEDEIROS REBOUÇAS
Diretor-Geral
Senado Federal

Assunto: **Prestação de informações**

Senhor Diretor-Geral

No que tange as informações solicitadas por meio do Requerimento nº 39 CPI-ESP, cumpre-nos informar que:

Extrai-se do Ato da Comissão Diretora nº 14 de 2013 que a Secretaria de Polícia, a Secretaria de Tecnologia da Informação – PRODASEN e a Coordenação de Operações de Telecomunicações possuem atribuições relacionadas à proteção de dados e conhecimentos sensíveis ou sigilosos no âmbito do Senado Federal. A atuação destes órgãos, desde a vigência do referido Ato, é coordenada pelo Escritório Corporativo de Governança e Gestão Estratégica, chefiado por Diretor-Geral Adjunto, uma vez que o art 256 deste ato estabelece que:

> "Art. 256 Ao **Escritório Corporativo de Governança e Gestão Estratégica,** chefiado por Diretor-Geral Adjunto especialmente designado, compete **assessorar a administração, os colegiados e os órgãos** da Casa, bem como **coordenar as ações técnicas de governança corporativa**, exceto auditoria; governança de tecnologia da informação; **gestão de riscos organizacionais e segurança corporativa**; gesta o da estratégia

> organizacional, incluindo o planejamento estratégico com a coordenação técnica na formulação, desdobramento, monitoramento da execução e reavaliação da estratégia organizacional e respectivos objetivos e metas, e o assessoramento aos diversos órgãos da Casa na formulação, execução, monitoramento e revisão de planos setoriais; gestão estratégica de pessoas, incluindo gestão de competência e da cultura e clima organizacionais; gestão corporativa de portfólio, programas e projetos incluindo o gerenciamento do orçamento consolidado de projetos; gestão corporativa de processos e estrutura organizacionais incluindo o monitoramento e análise da maturidade, capacidade, eficiência, custos e desempenho dos processos críticos e estratégicos da organização bem como a análise e proposição de arquitetura, competências, organização e funcionamento da estrutura administrativa do Senado Federal; gestão corporativa do conhecimento organizacional; gestão corporativa da responsabilidade socioambiental e gestão corporativa da informação gerencial incluindo analise e consolidação de informações gerenciais da administração do Senado Federal." (grifo do autor)

Diante disso, pela disciplina desse ato, entendemos que o Escritório Corporativo de Governança e Gestão Estratégica, por coordenar tais atividades, é o órgão com melhores condições para prover com a amplitude e efetividade necessárias o requerimento da CPI-ESP.

Não obstante, em relação ao quesito três (3), informamos que à SPSF é atribuída a função de participar da elaboração, execução e gestão compartilhada da Política de Segurança Corporativa do Senado Federal, aprovada pelo Comitê de Governança Corporativa e Gestão Estratégica, e instituída pela Comissão Diretora do Senado Federal.

Além disso, são atribuições da Polícia Legislativa obter e analisar conhecimentos sobre fatos e situações de imediata ou potencial influência sobre o processo decisório e a atividade legislativa e sobre a salvaguarda e a segurança do

Senado Federal e seu patrimônio, membros, servidores e visitantes; desenvolver, em conjunto com a Secretaria de Tecnologia da Informação - PRODASEN (PRDSTI) e o Escritório Corporativo de Governança e Gestão Estratégica, planos e ações de segurança com vistas a preservar a integridade de dados e informações e a incrementar a segurança da instituição; e executar outras atividades correlatas.

Nesse ponto, cumpre-nos destacar que a doutrina policial aponta a Segurança Orgânica e a Análise de Risco como ramos da Segurança Passiva, que abarca as medidas passivas de prevenção e obstrução de ações intentadas por organizações ou pessoas em busca de dados ou conhecimentos sensíveis. A análise de risco, quando empregada sob essa ótica, permite uma visão técnica sobre a situação em que a unidade organizacional se encontra em relação à proteção dessas informações. A segurança orgânica, por sua vez, compreende 5 (cinco) dimensões da segurança, a saber: de Pessoal, da Documentação e do Material, da Informação, das Comunicações e Segurança das Áreas e Instalações.

Em linhas gerais, a Segurança de Pessoal está voltada a garantir a adoção de comportamentos adequados à proteção de dados ou conhecimentos sensíveis. A Segurança da Documentação e do Material, por sua vez, tem por objetivo a salvaguarda de dados ou conhecimentos sensíveis neles inseridos. A Segurança da Informação, por seu turno, compreende o conjunto de medidas voltadas a garantir a segurança das informações no âmbito da tecnologia da informação, diferenciando– se da denominada Segurança das Comunicações, que objetiva a proteção de dados e conhecimentos sensíveis durante os atos de transmissão e recepção. Por fim, a Segurança de Áreas e Instalações tem o escopo de salvaguardar os locais onde são elaborados, tratados, manuseados ou guardados dados ou conhecimentos sensíveis.

Diante das atribuições das diversas unidades do Senado Federal, esta Secretaria de Polícia Legislativa, por meio de seu Escritório Setorial de Gestão e de seus

outros serviços, sob a orientação técnica do Escritório Corporativo de Governança e Gestão Estratégica, participa de ações em todos os ramos da segurança orgânica.

Em relação ao âmbito da Segurança de Áreas e Instalações, esta Polícia Legislativa, imbuída em concretizar sua missão institucional, realiza a preservação das áreas e instalações físicas nas quais são armazenados ou manuseados dados e documentos sensíveis ou sigilosos. A título de exemplo elencam-se a proteção por pessoal qualificado 24 horas da Sala Cofre do PRODASEN e a da Comissão Parlamentar Mista de Inquérito instituída pelo Requerimento 1 de 19/04/2012, mais conhecida como CPMI – Vegas e Monte Carlo. No mais, atua na confecção de crachás identificadores que dão acesso às diversas áreas do Senado Federal com a observância de níveis de acesso.

No que diz respeito às ações em busca de uma adequada Segurança de Pessoal, esta Secretaria realizou palestras de conscientização sobre a importância da Segurança da Informação para servidores da Secretaria de Recursos Humanos, bem como participou do ciclo de palestras para novos servidores (promovido por aquela secretaria) com o mesmo objetivo. Idealizou, ainda, a recente Campanha de Segurança Corporativa realizada pela Secretaria de Comunicação Social e apoiada pelo PRODASEN e pelo Escritório Corporativo de Governança e Gestão Estratégica, a qual tinha como escopo, de uma maneira lúdica, introduzir conceitos e estimular a prática de procedimentos adequados a promover a segurança orgânica em todo o Senado Federal.

Ainda nessa linha, promove corriqueiramente o levantamento de informações de pessoas que possam causar comprometimento na segurança das informações. Esse tipo de levantamento, a título de exemplo, foi utilizado para subsidiar o Departamento de Polícia Federal com informações que possibilitaram operação conjunta de prevenção e detecção de possível fraude no último concurso para o provimento de cargos efetivos do Senado Federal, realizado em 2012.

No que tange à Segurança da Informação, desenvolvem-se, em conjunto com a Secretaria de Tecnologia da Informação – PRODASEN e com o Escritório Corporativo de Governança e Gestão Estratégica, planos e ações de segurança com vistas a preservar a integridade de dados e informações e a incrementar a segurança da instituição, além de realizar, em ação conjunta com a Secretaria de Tecnologia da Informação – PRODASEN, a detecção e remoção de dispositivos e programas relacionados à segurança da informação.

Exemplificam-se tais tipos de ações com os grupos que foram instituídos, em conjunto com o PRODASEN: o Grupo Técnico de Segurança da Informação e Comunicações; e o Grupo de Resposta a Incidentes. Tais equipes técnicas são compostas por servidores de ambas as Secretarias e objetivaram definir procedimentos entre esses dois órgãos para quando ocorrer algum incidente envolvendo a segurança da informação. Ademais, a Secretaria de Polícia participou dos grupos de trabalho instituídos pelo Escritório Corporativo de Governança e Gestão Estratégica, nos quais foram desenvolvidos alguns projetos, dentro os quais se destacam:

- Projeto regulamentando a Lei de Acesso a Informação no âmbito do Senado Federal, estipulando classificações e procedimentos específicos no trato com documentos materiais sensíveis e sigilosos;
- Projeto cujo escopo foi a definição de políticas e procedimentos integrados de Análise de Riscos no Senado Federal.

No que diz respeito à Segurança das Comunicações e da Segurança de Documentos e Materiais a atuação da Polícia Legislativa restringe-se ao âmbito *intra corporis*, apenas colaborando de maneira macro nestas espécies de segurança nos demais setores. Isso se deve a especificidade das ações relacionadas a estes tipos de segurança. Assim, a Polícia atua na orientação quanto às formas de proteção e não efetivamente na guarda das informações.

Ademais, no que tange ainda a Segurança Passiva, esta Secretaria elaborou, em 2011, Relatório de Vulnerabilidades e, em 2012, Relatório de Riscos acerca de vários aspectos da Segurança, dentre eles aqueles inerentes a Segurança Orgânica, do Senado Federal, os quais foram encaminhados à Diretoria Geral, a Primeira Secretaria e a Presidência.

Inobstante essas ações preventivas, a Secretaria desenvolve medidas ativas e reativas que visam corroborar a segurança das informações. Diante disso, realiza varreduras físicas e eletrônicas em ambientes sensíveis em busca de dispositivos eletrônicos, contando com o auxílio da Coordenação de Telecomunicações no que tange a busca em aparelhos telefônicos. Além disso, quando é detectado algum indício de violação de sigilo ocorrida nas dependências do Senado Federal, a SPSF instaura o competente inquérito policial com a finalidade de apurar a autoria e a materialidade do delito. A título de exemplo cita-se a investigação ocorrida em 2011, quando esta Secretaria investigou a violação de dados pessoais de servidores dessa Casa e identificou vulnerabilidades do sistema e o envolvimento de funcionários na conduta delituosa.

Diante do exposto, conclui-se que a Polícia do Senado, embora devesse integrar o Comitê de Governança, presta apoio e desenvolve ações nas mais diversas áreas da segurança orgânica, e que a gestão dessas é coordenada pelo Escritório Corporativo de Governança e Gestão Estratégica.

Respeitosamente,

PEDRO RICARDO ARAUJO CARVALHO
Diretor da Secretaria de Polícia do Senado Federal

SENADO FEDERAL
Diretoria-Geral

Memorando nº 108/2013 - DGER

Brasília, 08 de novembro de 2013.

A Sua Senhoria o Senhor
JORGE LUIZ ANDRÉ DE MELLO
Diretor da Secretaria de Infraestrutura
Senado Federal

Assunto: Solicita a prestação de informações.

Senhor Diretor,

Considerando os termos do Requerimento nº 39 CPI-ESP, cópia anexa, aprovado na 10ª reunião da Comissão Parlamentar de Inquérito da Espionagem, realizada no dia 30 de outubro do corrente, encaminho a Vossa Senhoria a presente solicitação.

Tendo em vista a necessidade de a CPI da Espionagem conhecer como se assegura a segurança das comunicações havidas no Senado Federal, solicito a Vossa Senhoria que subsidie esta Diretoria-Geral, respondendo às questões que se encontrem dentro da esfera de competência dessa Secretaria.

Atenciosamente,

ANTÔNIO HELDER MEDEIROS REBOUÇAS
Diretor-Geral

U:\Dger\Assessoria Técnica\2013\MEMORANDOS\MEMORANDO DGER\SPOL - fabi

SENADO FEDERAL
Secretaria de Infraestrutura – SINFRA

Mem. 00822/2013 – SINFRA

Em 12 de novembro de 2013.

À Coordenação de Operações de Telecomunicações,

Assunto: **Solicitação de informações acerca da segurança de telecomunicações no âmbito do Senado Federal**

Referência: Memorando n° 108/2013-DGER (00100.026743/2013-12);
Requerimento n° 39 CPI-ESP

1. Encaminho os documentos supracitados para atendimento, com a brevidade possível, à solicitação do Diretor Geral, mediante prestação das informações requeridas nas alíneas a e b, do item 1 do Requerimento n° 39 CPI-ESP.

Atenciosamente,

Jorge Luiz André de Mello
Diretor da SINFRA

Senado Federal – Praça dos Três Poderes – CEP 70165-900 – Brasília DF
Telefone: +55 (61) 3303-3441

fl. 02

SENADO FEDERAL
00100.026743/2013-12
DIR-GERAL

SENADO FEDERAL
Diretoria-Geral

Memorando nº 108/2013 - DGER

Brasília, 08 de novembro de 2013.

A Sua Senhoria o Senhor
JORGE LUIZ ANDRÉ DE MELLO
Diretor da Secretaria de Infraestrutura
Senado Federal

Assunto: Solicita a prestação de informações.

Senhor Diretor,

Considerando os termos do Requerimento nº 39 CPI-ESP, cópia anexa, aprovado na 10ª reunião da Comissão Parlamentar de Inquérito da Espionagem, realizada no dia 30 de outubro do corrente, encaminho a Vossa Senhoria a presente solicitação.

Tendo em vista a necessidade de a CPI da Espionagem conhecer como se assegura a segurança das comunicações havidas no Senado Federal, solicito a Vossa Senhoria que subsidie esta Diretoria-Geral, respondendo às questões que se encontrem dentro da esfera de competência dessa Secretaria.

Atenciosamente,

ANTÔNIO HELDER MEDEIROS REBOUÇAS
Diretor-Geral

U:\Dger\Assessoria Técnica\2013\MEMORANDOS\MEMORANDO DGER\SPOL – fabi

SENADO FEDERAL Fl. nº 12 SSCEPI

Fl. 06

SENADO FEDERAL

Secretaria de Infra Estrutura - SINFRA
Coordenação de Operações de Telecomunicações - COTELE
Serviço de Atendimento ao Usuário de Telecomunicações - SEAUTC

Memorando n.º 002/2013 – SEAUTC/COTELE/SINFRA
Origem: Memorando n.º 108/2013 - DGER

Brasília, 20 de novembro de 2013.

Assunto: **Solicitação de informações acerca dos procedimentos utilizados pelo Senado Federal para garantia da segurança das comunicações.**

Senhor Diretor da COTELE,

Conforme solicitação da Diretoria Geral do Senado Federal - DGER, por meio do ofício n.º 108/2013-DGER, que determinou que fossem respondidos os questionamentos contidos no ofício n.º 035/2013 – CPIDAESP e requerimento n.º 039/2013 da CPI-ESP, originários da "CPI da Espionagem", encaminhamos informações a respeito das características técnicas e medidas de segurança implementadas no sistema de telecomunicações do Senado Federal.

Sendo um sistema vital para o funcionamento do Senado e tendo em vista que as informações que transitam através dele são muitas vezes sigilosas e de importância nacional, a segurança das telecomunicações no Senado Federal sempre foi considerada prioridade por esta Coordenação de Operações de Telecomunicações - COTELE, o que levou à implementação de normas procedimentais e à instalação de equipamentos que buscam impedir a execução de grampos telefônicos e a sua dissimulação no sistema.

SENADO FEDERAL Fl. nº 13 SSCEPI

Fl._____

telefônico existente, o que, até a presente data, se mostrou suficientemente seguro, haja vista nunca ter ocorrido violação do sigilo das comunicações nas dependências desta Casa.

Apesar dos mecanismos e procedimentos existentes no Senado Federal buscando garantir a segurança das telecomunicações, essa segurança encontra fragilidade intransponível quando se origina ou se recebe chamadas de números particulares, haja vista que nesse momento a segurança das comunicações dependerá também da segurança implantada no terminal telefônico particular, sobre o qual o Senado não tem qualquer ingerência, podendo haver grampos nesses pontos.

Além disso, é importante ressaltar que não existe sistema totalmente seguro, haja vista que até os bancos, cujos prejuízos causados por ataques a seus sistemas podem ser imensos, não conseguem se proteger totalmente de acessos indevidos, estando o grau de segurança a ser implementado diretamente associado ao valor da informação que trafega no sistema.

Assim, quanto mais valiosa a informação, mais sofisticados serão os ataques aos sistemas de comunicação, demandando sistemas de segurança igualmente sofisticados e consequentemente caros.

Atualmente os mecanismos implantados no Senado Federal provêm um nível de segurança até então adequado às necessidades dessa Casa Legislativa, nunca tendo sido registrado qualquer tipo de violação em

suas instalações. Entretanto, como já dito, em telecomunicações não é suficiente a proteção de somente uma das pontas, haja vista que nenhuma medida de segurança adotada no Senado será efetiva se o outro lado da comunicação estiver desprotegido.

Cabe salientar que a segurança do sistema de telecomunicações está associada tanto aos mecanismos e procedimentos utilizados, quanto ao próprio desconhecimento por parte de terceiros dessas medidas. Dessa forma, alertamos que a divulgação das informações contidas neste documento pode vir a comprometer a segurança das comunicações do Senado Federal.

Respeitosamente,

ARÃO FERNANDES BULHÕES
Chefe do SEAUTC

Fl._____

1 – DA TELEFONIA FIXA

1.1 - CONFIGURAÇÃO ATUAL DO SISTEMA TELEFÔNICO DO SENADO FEDERAL.

Atualmente o Senado Federal conta com os seguintes PABX's:

- 01 (um) PABX Ericsson MX-ONE equipado com 3176 ramais digitais, 1472 ramais analógicos, 570 ramais IP, 300 licenças de *softphones* (BRIA), e 300 licenças para *smartphones* (AMC), conectando-se à central telefônica pública da Oi/Brasil Telecom por meio de 835 troncos digitais, utilizando fibras ópticas como meio de transmissão.
- 01 (um) módulo do PABX Ericsson MX-ONE equipado com 176 ramais digitais e 96 ramais analógicos, localizado na SQS 309, configurado como central independente e interligado ao Senado e à central pública por meio de fibra óptica, para atendimento aos Senadores em suas residências oficiais
- 01 (um) módulo do PABX Ericsson MX-ONE equipado com 16 ramais digitais, 16 ramais analógicos e 10 ramais sem fio, localizado na residência oficial do Presidente do Senado Federal, configurado como central independente e interligado ao Senado via enlace de rádio e à central pública por meio de fibra óptica.

Todos os PABX's que compõem o sistema de telecomunicações do Senado Federal também possuem interligação com a central telefônica pública por meio de cabo metálico, visando suprir possíveis falhas de comunicação que venham a ocorrer na interligação por meio de fibra óptica, sendo utilizados somente como mecanismo de contingência.

SENADO FEDERAL

Secretaria de Infra Estrutura - SINFRA
Coordenação de Operações de Telecomunicações - COTELE
Serviço de Atendimento ao Usuário de Telecomunicações - SEAUTC

A rede telefônica atual é composta de aproximadamente:

- 11.450 (onze mil, quatrocentos e cinquenta) pares metálicos de rede interna chegando ao DG principal (Unidade de Apoio VI – STELE), distribuídos por todo o complexo predial do SENADO;
- 980 (novecentos e oitenta) pares metálicos de rede externa interligando o DG principal às Concessionárias de Telecomunicações;
- 400 (quatrocentas) caixas de distribuição telefônica;
- 11 (onze) Distribuidores Gerais - DG's (STELE – Unidade de apoio VI, Centro de Transmissão do Colorado, Residências Oficiais – Asa Sul, Residência Oficial – Lago Sul, Anexo II – subsolo, Anexo I – Subsolo, SAMS – Unidade de Apoio IV, SEEP- Via N2, SEI – PRODASEN – Via N2, SETRAN – garagem externa, Interlegis – Via N2);
- sistemas de rede estruturada e convencional;
- galerias subterrâneas interligando diversas edificações;
- cabos CCI, CI e CTP-APL privativos do SENADO com capacidade variando de 01 (um) até 600 (seiscentos) pares;
- lances de cabos privativos do SENADO de até 1 (um) Km;
- emendas de cabos CI e CTP-APL (Raychem termocontráteis) em diversos tamanhos (utilizando conectores 3M e picabond);
- diversos tipos de blocos de conexão tais como blocos Krone de engate rápido, BLI, CooK B-303, Cook rotativo com corte, Cook rotativo sem corte.

Fl._____

- Proibição de instalação de extensões telefônicas em ramais analógicos e linhas diretas: Essa medida objetiva impedir que a conversação seja escutada em outro ponto do sistema, por meio de extensões, bem como dificultar a dissimulação de algum grampo no sistema telefônico, visto que o rigor da diretiva atual determina aos técnicos considerar qualquer tipo de extensão como procedimento extremamente irregular e suspeito, devendo, ao ser detectada, ser imediatamente informado à chefia superior para que promova a sua investigação de forma minuciosa.

- Utilização de ramais digitais com mecanismo de verificação da linha e codificação da conversação: Basicamente existem dois métodos de se tornar as comunicações seguras. O primeiro consiste em se impedir o acesso ao sinal transmitido por meio da implementação de barreiras físicas de segurança, tais como controle de acesso a ambientes, utilização de meios de transmissão confinados, etc. Já o segundo, consiste em garantir que mesmo tendo-se acesso ao sinal, que não seja possível extrair informações úteis do mesmo. A utilização de ramais digitais é um exemplo do segundo método. Mesmo que se consiga grampear um ramal digital, devido à informação que trafega do ramal até o PABX ser codificada, consistindo em uma transmissão de dados com protocolo proprietário (próprio do fabricante), não será possível compreender a conversação. A codificação existente não chega ao nível de segurança de uma criptografia, entretanto, é suficientemente segura para evitar os grampos normalmente utilizados. No Senado, além da codificação do sinal dos aparelhos digitais, existe um mecanismo que monitora a linha de forma a verificar alterações em suas características, promovendo o bloqueio do ramal caso essas características ultrapassem certos limites, sinalizando a possibilidade de existência de alguma escuta.

- - Utilização de ramais VoIP com criptografia: atualmente estão sendo testados e implantados gradualmente no Senado Federal ramais com tecnologia VoIP (*Voice Over Internet Protocol*), buscando permitir a utilização conjunta de infraestrutura de rede de dados já existente e a comunicação com custo reduzido através da Internet, bem como proporcionar maior segurança nas comunicações por meio de criptografia. Os ramais VoIP instalados no Senado formam, junto com os ramais *softphones* (BRIA) e os ramais *smartphones* (AMC), uma rede de comunicação mais segura, tendo em vista que a comunicação entre os ramais VoIP do Senado e os ramais BRIA e AMC, disponibilizados pelo Senado para utilização tanto em *notebooks/desktops* quanto *smartphones*, é feita por meio de criptografia. Infelizmente a qualidade da comunicação depende da rede de Internet que esteja disponível no local, o que tem limitado a disseminação de sua utilização, em especial em *smartphones*.

- Minimização da utilização de ramais analógicos e linhas diretas nos gabinetes parlamentares e na alta administração da Casa: Este item se justifica devido aos ramais analógicos e linhas diretas não serem tão seguros quanto os ramais digitais. Tanto os ramais analógicos quanto as linhas diretas não sofrem qualquer tipo de codificação, seguindo o padrão de comunicação pública definido pela Anatel e utilizado pelas prestadoras públicas de telefonia, de forma a poderem fazer uso de aparelhos telefônicos comuns, o que proporciona um custo de aquisição muito inferior ao dos ramais digitais, devendo ser empregados em áreas onde a segurança das comunicações não seja crucial. No caso das linhas diretas, a sua segurança é ainda inferior à dos ramais analógicos, visto que podem ser interceptadas em qualquer ponto da rede telefônica, desde a tomada onde se encontra conectado o aparelho telefônico até a central telefônica pública. Já no caso dos ramais analógicos, a única possibilidade de

Fl._____

interceptação dos mesmos seria necessariamente dentro do Senado Federal, que é um ambiente controlado com muito mais rigor que as redes telefônicas públicas, o que torna os ramais analógicos mais seguros que as linhas telefônicas normais, porém menos seguros que os ramais digitais.

- Bloqueio do envio da identificação do ramal nas ligações para fora do Senado Federal: Essa medida visa impedir a identificação do ramal do Senado que está originando a chamada, não sendo possível a sua identificação por meio de bina instalado no telefone recebedor. Todas as ligações efetuadas para fora do Senado são identificadas com um número único, que não está relacionado com o ramal originante. Dessa forma, mesmo que a tecnologia no futuro viabilize o grampeamento de entroncamentos digitais por meio de fibra-óptica, que é o caso do Senado, ainda assim não será possível saber qual ramal se estará grampeando, e, consequentemente, nem quem originou a ligação.

- Eliminação de troncos executivos, de forma que as chamadas executadas pelos ramais tomem alternadamente qualquer tronco livre de saída, não ficando associado o ramal ao tronco: Essa medida de segurança visa fazer com que as chamadas de saída tomem aleatoriamente qualquer tronco de saída que se encontre livre, impedindo que se saiba previamente por qual tronco a chamada sairá. No mesmo intuito do item anterior, mesmo que a tecnologia no futuro viabilize o grampeamento de entroncamentos digitais por meio de fibra-óptica, que é o caso do Senado, ainda assim não será possível saber qual ramal se estará grampeando, e, consequentemente, nem quem originou a ligação. Como já dito, existem dois métodos de se garantir a segurança das comunicações, sendo que o primeiro consiste em impedir o acesso ao sinal transmitido e o segundo em se garantir que não seja possível extrair informações úteis do sinal mesmo se tendo acesso a

Fl. 11

ele. Assim, a medida de segurança descrita no presente item, em conjunto com a citada no item anterior, busca aumentar a segurança das telecomunicações fazendo uso do segundo método.

- Identificação dos cabos de distribuição utilizando-se codificação própria: Todos os cabos que constituem a rede telefônica do Senado Federal são identificados de forma a permitir a sua manutenção quando necessário. Entretanto, a codificação utilizada segue padrão próprio do Senado, diferente dos utilizados pelas operadoras de telefonia fixa, de forma a dificultar a identificação por parte de pessoas não autorizadas. Tendo em vista a quantidade de cabos que compõem a rede telefônica, esta medida se apresenta como um incremento bastante eficaz na garantia de segurança de telecomunicações.

- Trancamento das caixas de passagem e de distribuição de rede telefônica: todas as caixas telefônicas existentes no complexo predial do Senado Federal são trancadas buscando dificultar o acesso por pessoas não autorizadas.

- Bloqueio no PABX da facilidade de intercalação: A facilidade de intercalação, disponível em várias centrais telefônicas, consiste em se permitir que alguns ramais, considerados de emergência, sejam acessados quando da eventualidade de emergência que o justifique. Esse aceso ao ramal poderá ser feito mesmo que já esteja em conversação, promovendo a quebra da segurança da comunicação. No Senado Federal esta facilidade se encontra bloqueada, não sendo permitida nem em casos de emergência, de modo a garantir que a intercalação nunca seja utilizada sob hipótese alguma.

SENADO FEDERAL Fl. nº 15 SGCEPI

Fl._____

- Minimização de mudanças no pessoal que presta serviço na área de telecomunicações: Um dos pontos de fragilidade na segurança é a substituição de pessoal que tem acesso aos sistemas de comunicação, incluindo-se nessa classe tanto o pessoal técnico, quanto o pessoal de manutenção predial e limpeza. Nesse sentido, a contratação de mão de obra externa para prestação de serviços, que ocorre por meio de licitação, é um dificultador da mantença da segurança, tendo em vista a real possibilidade de mudança total dos profissionais a cada licitação. Apesar da dificuldade relatada, intrínseca ao próprio processo licitatório, as empresas, de livre e espontânea vontade, têm optado por aproveitar a mão de obra especializada que já prestava o serviço, o que tem minimizado os riscos de quebra da segurança. Além, disso, todo o serviço a ser executado é registrado em ordens de serviço contendo dados que identificam o técnico, a data, o serviço executado e os locais acessados, o que facilita auditoria posterior caso necessário.

- Execução de varreduras sob demanda: A pedido de parlamentares são executadas varreduras no gabinete de modo a se verificar a existência de grampos telefônicos, bem como, por meio da Secretaria de Segurança Legislativa, a varredura de ambiente em busca de transmissores.

fl. 12

SENADO FEDERAL
Secretaria de Infraestrutura - SINFRA
Coordenação de Operações de Telecomunicações - COTELE
Serviço de Telecomunicações Móvel - SETEMO

Memorando n.º 241/2013 – SETEMO/COTELE/SINFRA
Origem: Memorando n.º 108/2013 – DGER

Brasília, 21 de novembro de 2013.

Assunto: **Solicitação de informações acerca dos procedimentos utilizados pelo Senado Federal para garantia da segurança das comunicações.**

Senhor Coordenador da COTELE,

Conforme solicitado no ofício n.º 108/2013 da Diretoria Geral do Senado Federal - DGER, para que fossem respondidos os questionamentos contidos no ofício n.º 035/2013 – CPIDAESP e requerimento n.º 039/2013 da CPI-ESP, originários da "CPI da Espionagem", temos a informar o que se segue;

Não existe sistema de proteção para resguardar o sigilo das comunicações realizadas pelo SMP (Serviço Móvel Pessoal) dos usuários do Senado Federal, que são executados pela Operadora contratada através de licitação, estando esta subordinada as Leis que regem o sigilo das comunicações, e ainda, ao contrato 133/2012 e seu aditivo, na Cláusula Terceira – Das Obrigações e Responsabilidades da Contratada, item XX, que determina, *"respeitar rigorosamente o dever de sigilo e confidencialidade das telecomunicações"*. Sendo este resguardo preventivo para a Prestadora.

Os aparelhos celulares utilizados são entregue em regime de comodato pela contratada e são os mesmos vendidos em seu portfólio.

Eu

SENADO FEDERAL Fl. nº 19 SSCEPI

SENADO FEDERAL

Secretaria de Infraestrutura - SINFRA
Coordenação de Operações de Telecomunicações - COTELE
Serviço de Telecomunicações Móvel - SETEMO

O Senado Federal adquiriu um sistema AMC (AAstra Mobile Client) que, **se utilizado no celular institucional, criptografa ligações entre celulares que utilizam o mesmo sistema e o PABX desta Casa Legislativa**, ainda assim, sua eficiência depende da velocidade de conexão à Internet.

Há alguns anos esta COTELE participou de comissão técnica com o objetivo de realizar estudos no sentido de verificar a viabilidade técnica e econômica da implantação de equipamentos de comunicação móvel com sistema de criptografia, tendo encontrado óbice na adoção desse tipo de sistema devido ao seu alto custo de aquisição e manutenção, bem como limitada utilização, haja vista que **a criptografia somente funcionaria entre os equipamentos adquiridos pelo Senado**, sendo que ligações para outros terminais móveis ou fixos estariam sem proteção.

De qualquer forma, esse tipo de solução encontra-se disponível no mercado, tendo já sido estudado pelas áreas técnicas, havendo possibilidade de sua aquisição caso esta Casa Legislativa delibere nesse sentido.

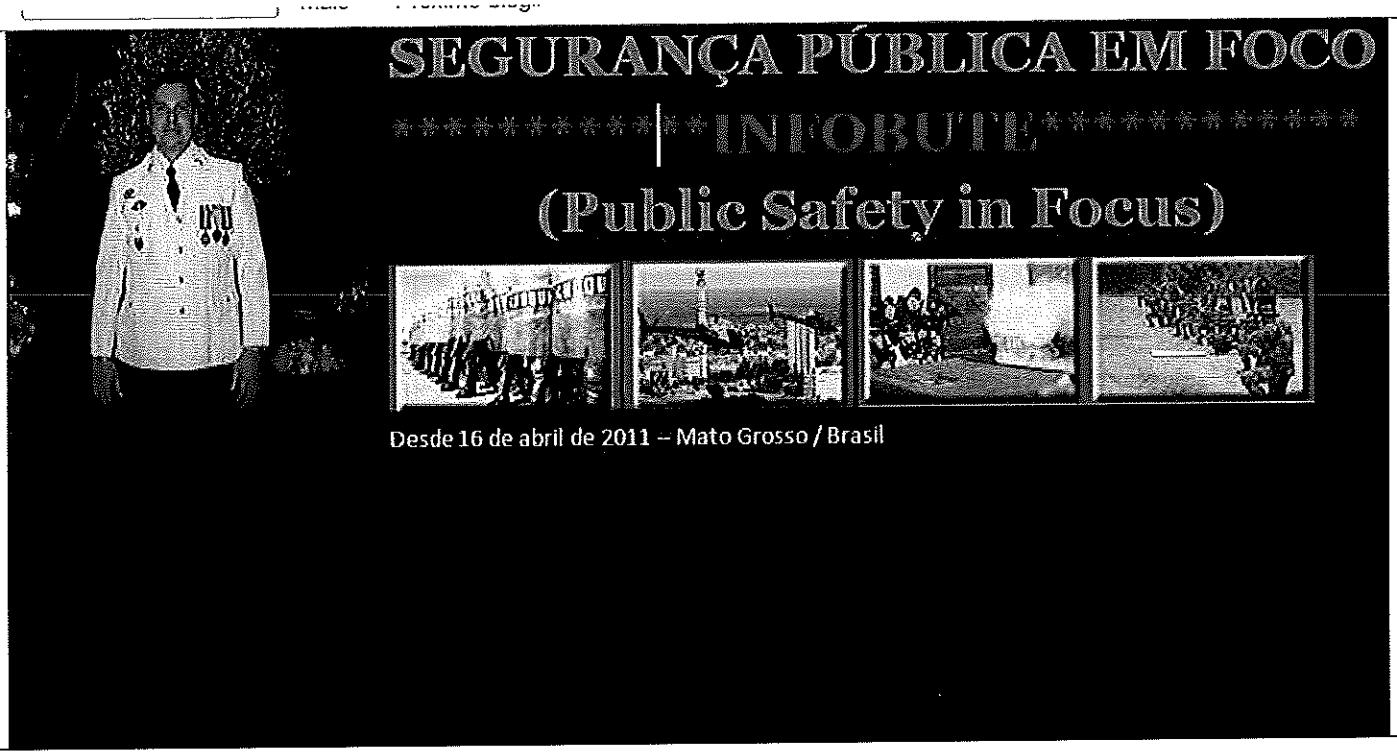
Para maior compreensão sobre a vulnerabilidade das comunicações móveis, anexamos alguns artigos publicados na Internet sobre o tema, com destaque para a matéria "Segurança em Foco", como também, anúncios oferecendo, a qualquer pessoa, equipamentos e software para escutas celulares.

Sem mais e a disposição,

Respeitosamente,

EURICO JACY KOPP AULER
Chefe do Serviço de Telecomunicações Móveis

Eu



terça-feira, 25 de setembro de 2012

GRAMPO: Com um telefone celular pode-se grampear conversas telefônicas, acessar dados de outros aparelhos e usar os celulares grampeados como microfones para escutas ambientais.

ATENÇÃO: Seu celular pode ser grampeado

Renata

Com apenas um celular nas mãos, o presidente da Companhia SecurStar, Wilfried Hafner, foi capaz de grampear conversas telefônicas, acessar dados de outros aparelhos e usar os celulares grampeados como microfones para escutas ambientais.

A demonstração foi feita a um público de agentes de inteligência de diversos órgãos como a Polícia Federal (PF), a Agência Brasileira de Inteligência (Abin), o Tribunal de Contas da União e a Corregedoria Geral da União, reunidos em seminário promovido nesta semana pela Comunidade de Inteligência Policial e Análise Evidencial (CIPAE).

Registre aqui seu e-mail e receba diariamente as postagens do Blog Segurança Pública em Foco

Email address... Submit

Total de visualizações - Desde 16Abr11

328060

Tradutor / Translate

inglês italiano espanhol

Quem sou eu

Alessandro Gonçalves Guimarães Ferreira

Visualizar meu perfil completo

Seguidores

Usando um vírus enviado por meio de SMS (mensagem de texto), Hafner pode grampear qualquer telefone celular ? basta possuir o número do aparelho. O programa espião chamado RexSpy foi desenvolvido por sua empresa para mostrar a vulnerabilidade do sistema de telefonia celular. De acordo com ele, versões similares do vírus circulam pela internet em comunidades de hackers, principalmente na China e Coréia do Sul.

Sua empresa, que trabalha no ramo de segurança de dados e produz software para criptografar ligações tornando-as seguras, identificou ataques de vírus similares ao RexSpy no Brasil. A primeira incidência se deu em agosto.

Ao receber o vírus, o telefone infectado sequer alerta para a chegada da mensagem. A partir de então, o "espião" passa a ter acesso a todos os dados do aparelho, como a agenda telefônica, mensagens de texto, fotos e vídeos. Além disso, o telefone que enviou o vírus recebe uma mensagem cada vez que o aparelho grampeado é usado, permitindo ouvir ou gravar as conversas realizadas.

Também sem deixar pistas, é possível que o "espião" use o celular infectado como microfone, ouvindo conversas de reuniões privadas, bastando que o aparelho infectado esteja no recinto. Todas as modalidades de grampo foram apresentadas durante o evento.

"Temos identificado o uso de vírus semelhantes ao RexSpy para espionagem industrial. A primeira vez que descobrimos uma tentativa de invasão foi em abril, na França. No Brasil, percebemos a tentativa em agosto", disse.

Questionado se este instrumento poderia estar sendo usado para grampear políticos no País, Hafner respondeu que "basta possuir o número do telefone".

Ele mostrou ainda a possibilidade de se adquirir pela internet um programa chamado FlexiSpy, que também permite o grampo de celulares, mas, diferente dos vírus similares ao RexSpy, é preciso instalá-lo diretamente no celular, o que dificulta seu uso. O produto pode ser adquirido por cerca de R$ 250 e, na maioria das vezes, tem sido usado, segundo a empresa, por mulheres que querem monitorar seus maridos.

Apesar do empecilho de instalação do FlexiSpy diretamente no celular a ser atacado, Hafner disse que vídeos e "ringtones" (sons para celular, como campainhas personalizadas) podem estar infectados e o usuário, sem perceber, acaba por instalar o programa.

Hafner disse que o vírus desenvolvido pela empresa, RexSpy, serve somente para demonstração e que, apesar da companhia já ter recebido inúmeras ofertas, ele jamais foi comercializado.

"É para uso interno, para demonstrarmos as falhas de segurança. O problema é que hackers já possuem tecnologia similar", pontuou.

Acesse o Artigo Original: www.uniblogbr.com/2012/09/atencao-seu-celular-pode-ser-grampeado.html#ixzz27PGh4Jgo

Postado por Alessandro Gonçalves Guimarães Ferreira às 21:52:00

Reações: engraçado (0) interessante (0) legal (0)

Nenhum comentário:

Postar um comentário

ORIGEM DOS VISITANTES

Arquivo do blog

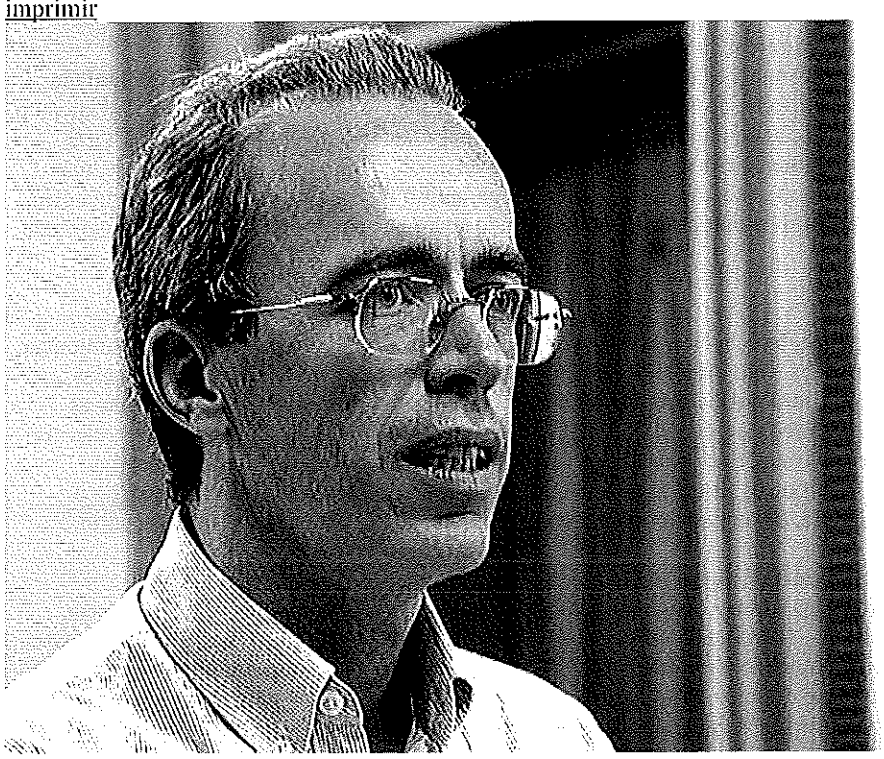
fls. 14

22/10/2011 07h13- Atualizado em 04/10/2013 15h56

Saiba mais sobre segurança da informação na comunicação sem fio

Da internet aos dispositivos móveis, especialista fala sobre atitudes seguras

imprimir



Marco Aurélio, professor da Faculdade de Engenharia Elétrica da Unicamp (Foto: Divulgação)

Se por um lado a comunicação sem fio trouxe benefícios importantes para a sociedade, por outro, ela levanta questões importantes sobre a segurança da informação. A internet passou a ser "desplugada", celulares e tablets expandiram o uso da rede para além da fronteira do uso doméstico, permitindo a troca de informações em praticamente qualquer lugar. Recursos como Wi-fi, Bluetooth e a conexão móvel à internet via modem são alguns dos pilares da mobilidade, porém possíveis portas de entrada para invasões. Para saber um pouco mais sobre a segurança na comunicação sem fio, o site do Globo Universidade conversou com o professor Marco Aurélio Henriques, da Faculdade de Engenharia Elétrica e de Computação da Universidade Estadual de Campinas (Unicamp / FEEC). Mestre e doutor em Engenharia da Computação pela Universidade de Chiba, no Japão, Marco Aurélio leciona a disciplina Segurança e Privacidade de Dados para alunos de pós-graduação da Unicamp. Nas linhas a seguir, confira como é possível se proteger das possíveis ameaças do meio eletrônico.

A comunicação sem fio é considerada segura atualmente?
- A questão se de ser segura, ou não, é muito relativa, além do que, por mais protegido que seja um meio, não há nada 100% confiável. Volta e meia, presenciamos invasões em sites importantes, como o da Nasa, ou de páginas de governo. Não existe segurança absoluta. Na telefonia celular, por exemplo, o sistema era muito mais vulnerável no início da década de 90, quando a rede era analógica. Naquela época, uma pessoa que tivesse um rádio FM multibanda poderia ouvir uma conversa. Com o advento da telefonia digital, a possibilidade de grampear uma conversa diminuiu muito, mas, mesmo assim, não é impossível fazer uma interceptação.

Da mesma forma que o celular ganhou novos recursos, aumentou também sua vulnerabilidade?
- É preciso lembrar que do sistema analógico para o digital, a segurança aumentou. Sendo assim, a partir de agora, é preciso ter conhecimento e equipamentos de ponta para burlar a segurança, como rádios digitais caros e sofisticados. No caso dos

celulares mais simples, sem recursos de transferência de dados, a única forma de a informação ser acessada por outro é através da antena, por ondas de rádio. Já os telefones mais sofisticados passaram a ter outras formas de comunicação, fora as redes das operadoras, como o Wi-fi e o Bluetooth, por exemplo. Se não tiver bem protegida, a rede sem fio passa a ser uma porta de entrada para invasões, possibilitando que uma pessoa se conecte ao seu celular e navegue por ele.

Pela própria natureza da comunicação sem fio, não é possível ter controle sobre a propagação do sinal da antena. Quando falamos ao telefone convencional, sabemos que a nossa voz passa por um cabo. Já na comunicação sem fio, a onda de rádio vai para tudo que é lado. Além disso, é preciso ter em mente que os telefones têm cada vez mais a característica de um computador.

Então, no caso dos aparelhos celulares, como se proteger de possíveis ameaças?
- O grande problema está na configuração. A grande maioria das pessoas compra um telefone e nem sabe que tem conexão Bluetooth e para que ela serve. Muitas vezes, o aparelho vem de fábrica com o Bluetooth ativado, permitindo que ele fique vulnerável a determinados tipos de invasão. Além disso, não adianta também o aparelho possuir recursos de criptografias se eles não são ativados pelo usuário. O mesmo se aplica em relação à conexão Wi-fi do celular. Se você não a está usando, é preciso mantê-la desligada.

Com relação ao uso da internet, como a comunicação sem fio pode ser segura?
- A melhor maneira de protegermos nossas informações é garantindo que essa comunicação por rádio seja criptografada, permitindo que só o destinatário, quando autorizado, possa decodificar a mensagem. No centro de computação da Unicamp, desenvolvemos um projeto que inclui a instalação de uma rede sem fio no campus Cidade Universitária Zeferino Vaz. Estamos implementando várias antenas no ambiente externo ao prédio da universidade, como as praças do campus, nas cantinas, ou seja, em locais em que há maior concentração de pessoas. Para garantir o mínimo de segurança, é obrigatório que os celulares e notebooks da comunidade universitária estejam configurados para que a comunicação seja criptografada e segura.

Como funciona a criptografia?
- Fazendo uma breve analogia, é como naquela brincadeira de criança, em que elas inventam um código para se comunicar, criando uma linguagem secreta entre os amigos, cujo princípio, por exemplo, pode ser a substituição de letras. Se elas escreverem uma carta seguindo essa lógica, outra pessoa simplesmente não entenderá o que está escrito lá, somente as pessoas que conhecem os parâmetros e requisitos para decodificá-la. Ou seja, criptografar é escrever de forma secreta. A criptografia é utilizada quando a troca de informações deve ser feita de forma segura, como em transações bancárias realizadas pela internet. Os navegadores já possuem sistemas de criptografias, que são ativados em sites seguros. Se o navegador não tiver algoritmos de criptografia, o computador do banco se recusa a "falar" com a máquina do usuário.

Com relação às transações bancárias na internet, como se proteger?
- Os servidores dos bancos são configurados para fazer com que as informações trocadas fiquem indecifráveis, ou seja, quando digitamos nossa senha, ela sai cifrada. O problema maior está no computador do usuário, que pode sofrer invasões. Muitas vezes, as pessoas recebem e-mails induzindo a clicar em links falsos, geralmente com programas maliciosos, cuja função principal é a de monitorar tudo o que é digitado no teclado. Esse monitoramento pode ser feito em celulares e computadores, e os dados coletados são transmitidos para outro site na internet.

Diante desse contexto, quais atitudes seguras os usuários podem adotar na internet?
- A primeira medida está em manter todos os softwares do computador atualizados, desde o sistema operacional e outros aplicativos ao próprio antivírus, reduzindo o número de vulnerabilidades. A outra medida é de caráter comportamental. A pessoa não pode acreditar em tudo que recebe na sua caixa de e-mails, mesmo que a mensagem pareça convincente. Na Unicamp, recebemos praticamente todos os dias e-mails falsos solicitando atualização de senhas. Para qualquer requisição de dados, incluindo nome completo e senha, é preciso que o usuário comprove por outros canais, como o telefone, por exemplo, se aquela solicitação é verdadeira. Além disso, existem alguns plug-ins para navegadores que detectam sites confiáveis.

O que é certificação digital?
- O certificado digital é uma espécie de documento eletrônico, emitido por uma autoridade certificadora confiável, uma espécie de cartório digital, que atrela uma senha especial, conhecida como chave pública, a uma determinada pessoa. O conteúdo de um certificado digital tem o nome do titular, a sua chave pública e o prazo de validade. As chaves de criptografia são números longos, com muitos dígitos, praticamente impossíveis de serem descobertas até mesmo por potentes computadores.

E na aviação, a comunicação sem fio é segura?
- Na aviação, a comunicação entre avião e torre é feita por rádio, que não tem proteção em criptografia, ou seja, qualquer pessoa com receptores FM multibanda podem ouvir essas transmissões. Entretanto, só é possível interferir nessa comunicação se for utilizado um transmissor, por isso que as rádios piratas próximas aos aeroportos são repreendidas, pois podem causar interferências. Além disso, hoje em dia, os aviões se comunicam constantemente com as fabricantes e com as torres de controle. Um caso recente dessa comunicação sem fio na aviação foi evidenciada no acidente com o avião da Air France, em 2009. Antes da queda, a aeronave emitiu para a fábrica da Airbus informações técnicas sobre o voo.

fl. 25

07/09/08 - 07h29- Atualizado em 07/09/08 - 07h49

Crise dos grampos impulsiona venda de aparelhos para fazer e bloquear escutas

Fabricantes e distribuidores oferecem equipamentos pela internet.
Celular antigrampo 'embaralha' dados de voz e impede escuta.

Maria Angélica Oliveira
Do G1, em São Paulo

clique para ampliar

Equipamentos para fazer grampos e contra espionagem são encontrados na internet (foto: Editoria de arte/G1)

Para além das altas esferas do poder, produtos que prometem fazer grampos telefônicos e equipamentos contra a espionagem estão cada vez mais populares.

A oferta de parafernálias para bisbilhotar ou para evitar ser bisbilhotado é grande e está disponível para todos os bolsos, gostos e necessidades.

Segundo empresas ouvidas pelo **G1**, as recentes denúncias de "arapongagem" envolvendo autoridades fazem as vendas crescerem.

Na semana passada, denúncias de que o presidente do Supremo Tribunal Federal (STF), Gilmar Mendes, foi grampeado fizeram com que o presidente Luiz Inácio Lula da Silva **afastasse temporariamente a cúpula da Agência Brasileira de Inteligência (Abin).**

Leia também:
Veja dicas para se prevenir de uma escuta ilegal
Relator de CPI quer proibir venda de aparelhos para grampo
Entenda a crise dos grampos ilegais

Pedido on-line

A lacuna na legislação – que não proíbe expressamente a comercialização de equipamentos que fazem escutas – deixa o território livre. As empresas que vendem equipamentos para grampos se respaldam na brecha existente. Afirmam que apenas vendem produtos e que não se responsabilizam pelo seu uso.

O acesso é fácil. Na internet, por exemplo, é possível encontrar microtransmissores do tamanho de uma moeda, canetas com microfone e transmissão por rádio e grampos telefônicos que podem ser instalados na tomada do aparelho. Os produtos, amadores, não chegam a custar R$ 50. Basta fazer o pedido on-line e esperar em casa.

Uma das fábricas de equipamentos para grampo, em Minas Gerais, quase não dá conta da demanda. "Trabalhamos aqui sem estoque. Tudo o que a gente produz está vendendo", diz o proprietário, um técnico em mecatrônica que começou a produzir os equipamentos por "hobby", chegou a exportar para a Argentina e agora vende, por mês, "algumas centenas" de produtos para escuta ambiental (que são escondidos em algum lugar) para todo o Brasil.

O analista de sistemas Vicente Levi Guedes, proprietário de um site de produtos eletrônicos, conta que chega a vender, mensalmente, cerca de 200 equipamentos para escuta. Ele diz que 40% das encomendas são de Brasília. "Não sei se é coincidência ou não", brinca.

Celular antigrampo

Na outra ponta, também é grande a oferta de produtos e serviços para quem quer evitar ser alvo de escutas. Os celulares antigrampo são a grande vedete do mercado. A tecnologia, no entanto, não está disponível para todos.

A "blindagem" no telefone celular é feita com a instalação de um software. O serviço chega a custar até cerca de R$ 3 mil por aparelho, segundo empresas ouvidas pelo **G1**. Mas há um detalhe: para funcionar, é preciso ter dois celulares com o software instalado, ou seja, o custo é em dobro.

SENADO FEDERAL Fl. nº 22 PSOL

O programa criptografa a voz, ou seja, "embaralha" os dados e faz com que eles não possam ser compreendidos por um espião que esteja escutando a conversa. No caso de um grampo, o que se ouve é apenas um ruído. A conversa só acontece porque os dois aparelhos emitem chaves que só são identificadas entre si. Essas chaves "decifram" o embaralhamento e jogam a voz, novamente, no alto falante do aparelho.

"As pessoas que detêm informações privilegiadas, importantes, acabam tendo que se proteger de alguma maneira. E a única maneira hoje conhecida, além de não falar, como disse nosso ministro, seria usar a criptografia", diz Marcelo Copeliovich, diretor da Gold Lock Brasil, empresa que instala o software antigrampo. Segundo ele, a procura aumentou cerca de 30% em relação ao ano passado.

"Quando aparece o tema grampo telefônico, a procura aumenta", conta Edison Santos, diretor comercial da CryptoCell, empresa que vende o software que criptografa a comunicação pelo celular e estima fechar o ano com um aumento de 60% nas vendas em relação a 2007.

Segundo ele, em busca do filão, duas operadoras já procuraram a empresa para analisar a viabilidade de oferecer o antigrampo como produto para o cliente. Há dois meses, a empresa resolveu baixar o valor do aparelho, que custava R$ 2,7 mil, para R$ 1.870.

Empresa 'aluga'

Para quem ainda considera o valor alto ou quer utilizar o antigrampo por um determinado período, há outras opções, como o "aluguel" do celular.

Na Secvoice, o cliente paga R$ 200 por mês para utilizar o software e pode interromper o serviço quando quiser. Ao contrário de outras empresas, nesse caso a tecnologia não é importada de países como Israel, origem de muitos desses programas, mas produzida no Brasil.

O proprietário da empresa e programador César Bremer Pinheiro diz que a quantidade de produtos para a bisbilhotice gerou uma "indústria do grampo". Há seis anos, ele percebeu a tendência quando procurava nichos ainda pouco explorados em tecnologia.

"Com a entrada dos primeiros palm tops, vi que poderia fazer criptografia de voz em equipamentos mais baratos", conta. Com o lançamento do novo produto, que utiliza **tecnologia 3G**, viu a procura triplicar no último mês.

Central antigrampo

Na Illix Tecnologia, o celular antigrampo é responsável por 40% das vendas. Adriana Gobbo, diretora da empresa, diz que o noticiário influencia a procura. "No caso Kroll, há uns cinco anos, teve um pico maior, cresceu bastante, mas depois normalizou."

Para quem também está preocupado com o telefone fixo, a empresa oferece uma "central antigrampo". Por R$ 700 por mês, o serviço não impede que o celular seja grampeado, mas promete detectar uma escuta.

O método consiste em monitorar a freqüência da linha. "Se a sua linha tiver algum problema, pode ser até uma pomba, um rato que roeu o fio da linha ou um grampo, vai haver uma variação de freqüência, o equipamento acusa isso e aí um técnico vai no local para verificar o que aconteceu", explica.

Pessoa física não compra

Além de o custo limitar as vendas, há outro fator impeditivo para uma popularização ainda maior do celular antigrampo.

Marcelo Copeliovich conta que o aparelho só é vendido para empresas e, antes de a venda se concretizar, é feita uma espécie de checagem do comprador. "A gente tenta fazer uma prévia na venda, verificar a empresa que está comprando, a situação cadastral", diz.

O objetivo é evitar que o celular antigrampo seja usado por criminosos ou por pessoas que possam ser alvo de ordens judiciais para escutas telefônicas, o que poderia gerar um impasse entre a operadora, que não irá conseguir obter os diálogos, a Justiça e a empresa que vendeu o software.

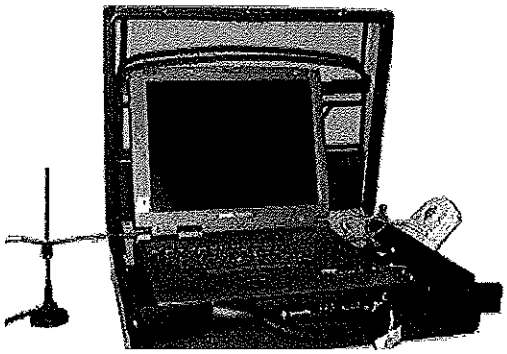
Pinheiro também afirma que vende o software apenas para empresas e para órgãos governamentais. Segundo ele, para fazer uma filtragem e evitar que o produto caia "na mão de qualquer pessoa".

"Não é interesse nosso o risco de ser usado por criminosos, traficantes de drogas. Se é uma pessoa jurídica, fica mais fácil tratar com ela, tem um endereço. Para uma pessoa física, teria que levantar a ficha cadastral na polícia e aí começa a entrar em uma

fl. 36

Quarta, 3 de setembro de 2008, 13h56 Atualizada às 14h12

Sites entregam equipamentos para grampo via Sedex



Diego Salmen

Os grampos telefônicos já renderam uma Comissão Parlamentar de Inquérito (CPI das Escutas Telefônica em Brasília e dor de cabeça a uma série de integrantes dos Três Poderes - sejam eles autores ou vítimas d supostos infortúnios.

Na terça-feira, 2, o ministro-chefe do Gabinete de Segurança Institucional da Presidência da Repúbli general Jorge Armando Felix, foi à comissão para rebater a acusação da revista *Veja* de que a Abin (Agên Brasileira de Inteligência) teria grampeado uma conversa entre o presidente do Supremo Tribunal Fede (STF), ministro Gilmar Mendes, e o senador Demóstenes Torres (DEM-GO).

A depender da disponibilidade de equipamentos para grampo na internet, os parlamentares da CPI terão l longo caminho pela frente. Uma rápida busca em sites de pesquisa mostra o quão diversificado é es segmento no mercado brasileiro. A venda dos aparelhos é legal; ao comprador, basta registrá-los na Poli Federal.

A Lei 9296 diz que "constitui crime realizar interceptação de comunicações telefônicas, de informática telemática, ou quebrar segredo da Justiça, sem autorização judicial ou com objetivos não autorizados em le A revisão da matéria está em discussão no Congresso Nacional.

Espião

De nome sugestivo, o site *A Casa do Espião* oferece aos internautas uma série de dispositivos para realização de grampos telefônicos. Há produtos em todas as faixas de preço.

De escutas por sinal UHF, a R$ 1.290,00, passando pelo kit transmissor de linha (R$ 3.400,00) ao celu *trapper*, que registra e transmite para outro telefone as conversas do "espionado". O preço é um pouco m salgado: R$ 10.780,00. Entrega expressa pelo correio.

Na *ItecDiffusion.com*, é possível encontrar outra versão do *trapper*: o chamado Celular Espião. O site anunc "Entregue este celular à pessoa que deseja vigiar e ouça todas as conversas a qualquer momento, qualquer lugar". Custam de R$ 1.800,00 a R$ 8.500,00,dependendo do modelo e das funções escolhidas - q vão da gravação de sons ambientes à interceptação de conversas e mensagens de SMS.

A entrega é feita pelos Correios, e o cliente mais apressado pode solicitá-la via Sedex. A propagan prossegue:

"Você tem suspeitas de alguém que convive com você? Tire essa dúvida imediatamente! Ideal para vigiar empregado, um colega de trabalho, as amizades de seus filhos ou as atividades de seu marido ou esposa".

Outros dispostivos podem ser encontrados em sites internacionais. No portal de leilões e compras online *Et*, é possível encontrar mecanismos de grampo via sinal FM por US$ 59,99. Basta instalar o mecanismo na lin a ser monitorada para as conversas serem transmitidas a qualquer aparelho de rádio num raio de até 3 metros.

A loja norte-americana *Amazon* vende o "Phone-007" por US$ 299,00. Descrição: "Parece e funciona como telefone comum, mas grava todas as ligações sem que o usuário saiba". Também serve como gravador som ambiente.

Maleta

Segundo informações da *Folha de S. Paulo*, o ministro da Defesa, Nelson Jobim, disse, em reunião no Palá do Planalto na segunda-feira, que a Abin adquiriu ilegalmente maletas de interceptação telefônica. revelação teria sido decisiva na atitude do presidente Lula de afastar a cúpula da agência. No site da empre *Ability BR*, o equipamento é anunciado assim:

"Estas maletas são ferramentas extremamente eficazes na investigação, permitindo ao operador - seja es um Policial ou membro do Ministério Público - a indispensável agilidade na realização de suas tarefas".

A página virtual não informa o preço do mecanismo (cerca de US$ 500 mil, segundo a *Folha de S. Paulo*). produto, segundo a empresa, é de uso "exclusivo do governo".

Terra Magazine

fl. 17

Busca no Site

Busca Avançada

CATEGORIAS

- DICAS UTEIS
- FRANQUIA
- CONSULTORIA
- 007 Celular Espião
- Ambiente Seguro Sala Protegida
- Analizador De Linha Telefonica L
- Automovel Video Gravador C/ Gps
- Binóculos Especiais
- Bloqueadores Diversos
- Camera Esportiva
- Câmera I.P e GSM ou 3G
- Cameras Especiais
- Caneta Filmadora
- Capa Bloqueaora De Sinal CelulaR
- Celular Espião
- Detector De Linha Telefonica Tra
- Detector De Onda Eletromagnetica
- Detector E Ident. De Cames
- Escutas Ambientes
- Espionagem Caneta Indutiva Bluto
- Finder Identif. Digitais
- Grampo deTelefone Fixo
- Gravador E Receptor D
- Gravadores Digitais De Audio
- Inspeção Visual Eletronica Digit
- Identificadores Diversos
- Jammer De Audi
- Maleta Escuta Celular Monitorame
- Maletas Especiais
- Micro Camera Gravador De DVR
- Micro Cameras Espiãs
- Microfones Especiais
- Modificador De Voz Para Celular
- Óculos Espião
- Oscor 5000 Contra Espionagem Omi

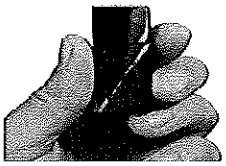
Home » Loja » Celular Espião »

R$ 1.300,00

Tweet

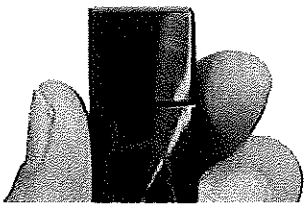
SENADO

SOFTWARE SPY PARA MONITORAR CELULAR



Clique para ampliar

Celular Spy é um software engenhoso e prudente sistema, que permite monitorar, rastrear e controlar o seu celular. Ele pode monitorar as mensagens de texto GSM, registros de chamadas, e-mails enviados e recebidos, bem como a localização geográfica do telefone. Celular Spy permite que você faça back-up do seu celular e terá um registro detalhado da sua atividade.



ATENDIMENTO VIA CHAT

Envie uma mensagem

CHAT - OFFLINE

Powered By: Crafty Syntax

SUAS COMPRAS

0 itens

ENTRAR

E-Mail:

Senha:

Entrar

Não tem Cadastro?
Clique aqui
Esqueceu sua Senha?

NOTIFICAÇÕES

Notifique-me de atualidades para **CELL PHONE RECON SPY**

INDIQUE

Indique esse produto para alguém que você conhece.

COMENTÁRIOS

Escreva um comentário neste produto!

ACEITAMOS

PayPal VERIFIED

PayPal

VISA

CONTATO VIA SKYPE

seuSkype

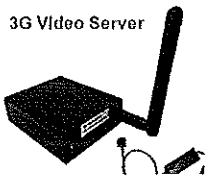
Ligue agora

SENADO FEDERAL Fl. nº 24 SSCEI

Pen Drives Espião
Ponto Eletronico
Produtos Profissionais
Radios
Rastreador Gsm / Gprs/ Gps Ultra
Relógio C/gravador Audio E Vídeo
Reversor Espião C/ Olho Mágico
Shot Gun Microfone Direcional De
Sistema De Gps Rastreamento C/ M
Sistema Digital Repetidor De Aud
Snake Fibra Ótica Ada
Software para computador
Software Para Celular
Telefone Modificador De Voz C/ 8
Ultra Mini Computador Wireles 4
LEGISLAÇÃO

LANÇAMENTOS

3G Video Server



INFORMAÇÕES

- Fale Conosco
- Como Comprar?
- Confirmar Pagamento
- Rastrear
- Mapa do Site
- Envio-Frete
- Condições de Uso
- Política Privacidade

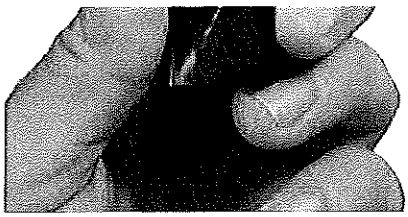
FAVORITOS

Adicionar aos Favoritos
Definir como Página Inicial

SEGURANÇA

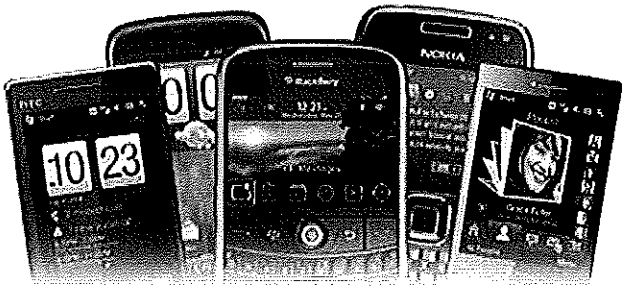
QUEM ESTÁ ONLINE?

No momento há
1 Visitante online.



Via Chat

Além do mais, o Cell Phone Spy utiliza rastreamento por GPS avançado, que vai identificar a localização exata do telefone através do Google Maps a cada 15 minutos. Se o telefone não está na visão direta de um satélite, a tecnologia GSM é usada para dar uma localização aproximada para o telefone dentro de um raio de 500 metros.



O software é simples de configurar e usar, tudo que você precisa fazer é instalar uma pequena aplicação no telefone, fornecer o número do telefone IMEI, e as informações serão exibidas na tela de seu PC, muito fácil de usar com painel de administração. Mesmo se os registros do Celular são excluídos, os dados ainda estarão disponíveis para visualização através da conta on-line segura.

LOJA DO DETETIVE
CELULARES spy cell

fl. 58

Uma compra dá acesso ilimitado ao software para cinco anos a contar da data de ativação, e inclui o armazenamento de dados ilimitado. Para mais informações sobre renovação após esse período, em contato com o local de compra. Por favor, note que

um serial key pode ser usada por apena sem um telefone e em um determinado momento, porém ele pode ser transferido para outros telefones após o uso. Você pode usar o software para monitorar o seu cônjuge, funcionários, e as crianças para a segurança da sua família.

LOJA DO DETETIVE
CELULARES spy cell

Smartphone Requisitos:

>> Compatível com Black Berry, Android, Windows Móbile e Symbian OS, incluindo os modelos da Samsung, Nokia, Motorola, HTC e muito mais
>> Compatível com T-Mobile, o Espírito, O2, Orange, Verizon, Alltel AT & T, e muitos mais.
>> Conexão com a Internet deve estar habilitado para software para trabalhar.

Para uma lista de aparelhos compatíveis consulte nosso suporte ou leia até o final da pagina.

suporte@lojadodtetive.com.br

11 41119661

Voce mesmo faz a instalação é muito simples.

LOJA DO DETETIVE
CELULARES spy cell

Compatibilidade:

Leia com atenção o seu computador e seu celular devem ter internet habilitadas para a instalação

O Celular Recon está disponível no sistema operacional a seguir:

Symbian OS 9.x Celular
Celular Recon é agora compatível com Symbian 9.x e

Celular Recon é agora compatível com Symbian 8.x 9.x 8.x dispositivos. O Symbian OS versão tem todas as funcionalidades da versão Windows Móbile, mas não registro de URL web visitadas.

Você deve ter uma ligação à Internet transportadora para que o software pode fazer upload de logs. Sua conta de telefone celular devem ter a Internet habilitado para o Celular software Recon pode carregar os logs para sua conta.

Nokia 3250, Nokia 5500, Nokia 5700

Nokia 6110, Nokia 6120, Nokia 6121, Nokia 6124, Nokia 6210

Nokia 6220, Nokia 6290, Nokia E50, Nokia E51, Nokia E60

Nokia E61, Nokia E61i, Nokia E62, Nokia E65, Nokia E66

Nokia E70, Nokia E71, Nokia E90, Nokia N71, Nokia N73

Nokia N73 ME, Nokia N75, Nokia N76, Nokia N77, Nokia N78

Nokia N80, Nokia N81, Nokia N81 8GB, Nokia N82, Nokia N91

Nokia N92, Nokia N93, Nokia N93i, Nokia N95, Nokia N95 8GB, Nokia N96

LG KS10, LG KT610

Samsung SGH-G810, Samsung SGH-i400, Samsung SGH-i450, Samsung SGH-i520, Samsung SGH-i550, Samsung SGH-i560

Tele móveis Windows Móbile 6.x
O Celular Recon O software é compatível com a maioria dos smartphones rodando o sistema operacional Windows Móbile. Uma lista parcial de telefones compatíveis é mostrado abaixo. Mesmo que você não vê o seu telefone nesta página, qualquer smartphone Windows Móbile com base conectividade com a Internet vai funcionar.

AT. & T Tilt

HP iPAQ 510

fl. 19

HP iPAQ 510

HTC TyTN II Mogul, HTC PPC6800, HTC, HTC Touch, HTC S621, Qtek S640, Qtek S710, Qtek S730, HTC Dash 3G, o ozônio HTC, HTC S740, HTC Shadow Hot Spot, HTC Snap

Motorola Moto Q 9m, Motorola Moto Q Global, Q9C Motorola, Motorola Q global, a Motorola Q 9c, 9m Motorola Q, Motorola Q 9h global

Samsung Ace, Samsung Black Jack II, Samsung SCH-i760, Samsung SPH-i325 ACE, Samsung Black Jack II SGH-i617, Samsung B7320 Omnia PRO, Jack Samsung (SGH-i637)

Shadow T-Mobile, T-Mobile Dash 6.0, T-Mobile Wing

Verizon SMT5800, Verizon XV6800, Verizon XV6900

Palm Treo 500v, 500w Palm Treo

Pantech Duo

Psion WPG2

Dopod C730

Exigências adicionais: Não há requisitos especiais para o Windows Móbile 6.x telefones. Sua conta de telefone celular deve ter uma opção de Internet para que o The Cell Phone software Recon pode carregar os logs para sua conta.

Windows Móbile 6.0 Pocket PC Professional
HP iPAQ 600/610, HP iPAQ 900/910

HTC Advantage X7501, HTC PPC6800 Mogul, HTC P3470, HTC P6500, HTC Tilt 8925/TyTN II, HTC Touch, HTC Touch Dual, HTC Fuze, HTC MAX 4G, 3G HTC Touch, HTC Touch Diamond, HTC Touch Diamond2, HTC Touch HD , HTC Touch Pro HTC Touch Pro2, HTC Touch Viva

LG MS20, LG MS25, LG Incite

Samsung SCH-i760, Samsung SGH-i780, Samsung Omnia SGH-i900, Samsung Omnia SCH-i910, Samsung SGH-i907 Epix, Samsung SCH-i770 Saga

T-Mobile Wing

Verizon XV6800, Verizon XV6900

Palm Treo 800w, Palm Treo Pro

Sony Ericsson XPERIA X1

Android Phones
Acer Liquid A1 1.6, Acer beTouch E110 1.5, Liquid Liquid Acer A1 (S100) 1.6, o Acer Liquid E 2.1, Liquid E Acer Ferrari 2.1, Acer Liquid Stream S110 2.1 com atualização para 2.2

Bluelans Sciphone 1,5 N19, N21 SciPhone Bluelans 1.6, Sciphone Comunicação Bluelans 1,5 N19, N21 SciPhone Comunicação Bluelans 1,6

Geek'sPhone Geek'sPhone 1.5 Cupcake, Geek'sPhone One

General Móbile General Móbile DSTL1 1,6 Imaginário

T-Mobile G1 (Era G1 na Polónia) 1.0 a 1.6, a T-Mobile G2 Touch, myTouch 3G da T-Mobile, T-Mobile Pulse (Huawei U8220, CHT8000 em Taiwa) 1.5 (2.1 beta), T-Mobile Vibrante

HTC Dream 1.0 a 2.1, o HTC Hero, 2.1, HTC Droid Eris, HTC Desire, HTC Legend, o HTC Magic, 1.5, 1.6, HTC Sapphire, HTC Tattoo (anteriormente Clique HTC) 1.6, 4G HTC Eco (Anteriormente HTC Supersonic) 2.1, HTC Paixão, Aria HTC (HTC Liberdade) 2.1, com interface HTC Sense, HTC Desire 2.1/2.2 com o HTC Sense UI,

HTC Droid Incredible (ADR6300) 2,1-2,2 com o HTC Sense UI, HTC Legend 2.1 com interface HTC Sense, Evo HTC 4G (anteriormente HTC Supersonic) (PC36100) 2.2 com interface HTC Sense, HTC Desire HD (HTC Ace) 2.2 com Sentido 2, myTouch 3G HTC Slide 2.1, com interface HTC Sense Espresso, HTC Wildfire 2.1, com interface HTC Sense, HTC Droid Incrível 2.1 (Éclair) com o HTC Sense UI

HT-03A DoCoMo no Japão

Google Nexus (2,1-2,2) codinome HTC Dragon

Huawei U8230 1,5

LG GW620 Eve (dublado GW620 Linkme para o mercado italiano) 1,5, LG GT540 Optimus (também

fl. 20

conhecido como o Swift GT540) 1.6, 2.0, 2.1 ou 2.2, dependendo da região, a LG KH5200 Andro-1 1.6, LG LU2300 Optimus Q 1.6, LG Ally VS740 (aka Aloha) 2.1, LG KU9500 Optimus Z (SU950) 2.1

GT540 Optimus Também conhecido como o GT540 Swift 1,6

Motorola Quench, a Motorola MB501 1.5 (expansível até 2,1), Backflip Motorola, Motorola MB300 1.5 (expansível até 2,1 em os EUA), Motorola Droid, Milestone 2,1, 1,6 Devour Motorola, o MOTO XT800 2.0, MOTO MT710 Ophone OS 1.5, da Motorola CLIQ, Motorola DEXT 1.5, da Motorola Charm 2,1 Éclair, a Motorola Quench, a Motorola CLIQ XT, Motorola Milestone Droid (Verizon) 2,0-2,2, Motorola Droid X 2.1 (2.2 atualizado esperado em setembro), a Motorola Droid 2, Motorola Milestone-2 2.2, da Motorola i1 1.5, da Motorola ME600 1.5 com Motoblur, Motorola Devour 1.6 com Motoblur, Motorola Milestone 2,1 XT701, XT720 Motorola, Motorola MOTOROI 2.1, da Motorola DEXT mundial MB200 1,5, 2,1 Defy Motorola, Motorola Flipout 2,1

Pentech Sirius Sky 2.1, Sirius Sky Pantech IM-A600S, Pantech IM A630K Izar Sirius, Sirius Vega Pantech IM-A650S

Grupo Samsung Samsung Behold II 1.5, o Samsung I7500 1.6, Samsung Galaxy, Samsung Moment 2.1, Galaxy A (ACS-M100S), Samsung i5700 1.6, 2.1, Samsung Spica, Samsung Galaxy Portal, Samsung i7500 Galaxy, Samsung M900 Moment (SPH-M900), Samsung i5700 Spica [75] (GT-i5700), Samsung i5800 Teos (GT-i5800), Samsung Galaxy A (ACS-M100S), Samsung I9000 Galaxy S, Samsung SCH-r880 Acclaim, a Samsung M910 interceptar, Samsung Moment II (M910)

Sony Ericsson XPERIA X10 1.6, Sony Ericsson XPERIA X10 Mini [mini X10 (E10i (UK))] 1.6 com Timescape UI, Sony Ericsson XPERIA X10 (X10i) 1.6 com Timescape UI (a ser atualizado para 2,1 no 4 ° trimestre 2010)

Spice CSL [14] 1.6

Dell Mini 3 (Mini 3i na China) 1,5

Garmin Garminfone 1,6

Highscreen PP5420

HKC Pearl, HKC Imobile v413

Huawei U8230

i-Mobile 6010

Kogan Technologies Agora Standard / Pro versão 1

Lenovo Ophone

QIGI i6

AT & T Captivate

Verizon Fascinate

Sprint 4G Epic [GT-I9000 (ACS-M110S (Coréia do Sul))]

Link ZTE

Nexian A980 (Journey)

Tiger Tiger G3 1,5

BlackBerry Celular
BlackBerry 8100, 8110, 8130, 8300, 8310, 8820, 8830, 8800, 8330, 8230, 8520, 8220, 8900, 9000 Bold, Tour 9630, Storm 9530, 9700, Pearl 8100, Pearl 8110, Pearl 8120, Pearl 8130, Pearl 9100, Pearl 8220 Flip, o Pearl Flip 8230, 88XX 8800, 8820 88XX, 88XX 8830, Curve 8300, Curve 8310, Curve 8320, Curve 8330, Curve 8350i, Curve 8900 (Javelin), Curve 8520 (Gemini) Curva 8530 (Áries), o Blackberry Curve 9300, Bold 9000, Bold 9650, 9700 Bold, Storm 9500, Storm 9530, Storm2 9520, Storm2 9550, Tour 9630, Torch 9800

Dúvidas contate nosso setor de suporte:

suporte@lojadodetetive.com.br

Peso: 1.00 Kg

Este produto foi adicionado em nosso catálogo em sábado 05 fevereiro, 2011.

Comentários | Voltar | Adicionar à Cesta

fl. 21

Vendo Equipamento Profissional Grampo Escuta Celular

R$ 22.500

Contatar

Área de Cobertura

Acre, Alagoas, Amapá, Amazonas, Bahia, Ceará, Distrito Federal, Espírito Santo, Estados Unidos, Goiás, Maranhão, Mato Grosso, Mato Grosso do Sul, Minas Gerais, Paraná, Paraíba, Pará, Pernambuco, Piauí, Rio Grande do Norte, Rio Grande do Sul, Rio de Janeiro, Rondônia, Roraima, Santa Catarina, Sergipe, São Paulo, Tocantins

Dados de contato

REINALDOMALEIRODACUNHA
Telefone: (00) 000000
Endereço: Alto Paraná, Paraná

dd

Vendo Equipamento
Intercepta GSM ,gravar,monitorar,escuta celular audio
e SMS Monitorar Grampear linhas de celular.(importado -Israel 100% digital.)
Apenas aconselhado para escuta e investigação de infidelidade conjugal,
comercial e ou empresarial,).operação fácil, manual em português
Funcionamento:
Basta plugar em qualquer notebook
ou PC normal (via USB) e inserir no Software
o número do "alvo" com DDD. e escolher a pasta
onde será gravado o audio
.(não requer conhecimentos técnicos)
sistema GSM(padrão ANATEL brasileiro),
(apenas uma linha simultanea)
Valor R$ 22.500,00

jggbggjjsuta cVendo EquipamentoIntercepte GSM ,gravar,monitorar,escuta celular audio e SMSMonitorar Grampear linhas de celular.(importado -Israel 100% digital.)Apenas aconselhado para escuta e investigação de infidelidade conjugal, comercial e ou empresarial,).operação fácil, manual em portuguêsFuncionamento:Basta plugar em qualquer notebookou PC normal (via USB) e inserir no Softwareo número do "alvo" com DDD. e escolher a pastaonde será gravado o audio oucópia dos SMS's.(não requer cotttnhecimentos técnicos)sistema GSM(padrão ANATEL brasileiro),cobre celular de DDD apenas local..o celular "alvo" tem queficar dentro da cidade ou regiao do mesmo código de área.não pega fora de seu DDD,Rastreia tb SMS's(apenas uma linha simultanea)Valor R$ 25.500,00CONTATO pelo email : metaltintas@terra.com.brVendo EquipamentoIntercepte GSM ,gravar,monitorar,escuta celular audio e SMSMonitorar Grampear linhas de celular.(importado -Israel 100% digital.)Apenas aconselhado para escuta e investigação de infidelidade conjugal, comercial e ou empresarial,).operação fácil, manual em portuguêsFuncionamento:Basta plugar em qualquer notebookou PC normal (via USB) e inserir no Softwareo número do "alvo" com DDD. e escolher a pastaonde será gravado o audio oucópia dos SMS's.(não requer conhecimentos técnicos)sistema GSM(padrão ANATEL brasileiro),cobre celular de DDD apenas local..o celular "alvo" tem queficar dentro da cidade ou regiao do mesmo código de área.não pega fora de seu DDD,Rastreia tb SMS's(apenas uma linha simultanea)Valor R$ 25.500,00CONTATO pelo email : metaltintas@terra.com.brelular

Perguntas ao vendedor.

Escreva sua pergunta ou repita a última realizada

caro amigo, é necessário estar próximo do celular no máximo quantos metros?

Basta estar no mesmo código de área ,não tem limite de metros. - Há 10 dias.

Amigo, boa tarde!!! Me responda, se este aparelho rastreia todo tipo de celular,inclusive Iphone!!! e todas operadoras!!! Tenho, interesse ok, pagamento á vistá!!! Grato, no seu aguardo,

Sim,qualquer op. e celular. - Há 13 dias.

Poderia estar num DDD e efetuar a monitoração de um celular em outro DDD? Por exemplo, monitorar um celular em outro estado?

Não - Há 20 dias.

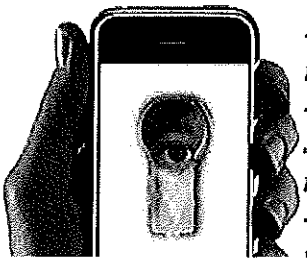
qual a forma de pagto?

10 % de sinal e o restante após receber. Envio por sedex ,sem adicional de frete ,um abraço. Enviado via MercadoLivre para Android - Há 22 dias.

fl. 22

Voltar para a lista | Serviços > Vestuário > Uniformes

Anúncio #520340187 Denunciar



Rastreador Celular Android Gsm Grampo Escuta Aplicativo

R$ 980

KOPP | Vender | Con

Contatar

Área de Cobertura

Acre, Alagoas, Amapá, Amazonas, Bahia, Ceará, Distrito Federal, Espírito Santo, Estados Unidos, Goiás, Maranhão, Mato Grosso, Mato Grosso do Sul, Minas Gerais, Paraná, Paraíba, Pará, Pernambuco, Piauí, Rio Grande do Norte, Rio Grande do Sul, Rio de Janeiro, Rondônia, Roraima, Santa Catarina, Sergipe, São Paulo, Tocantins

Dados de contato

REGINALAUCHERTREISDEH
Telefone: (00) 00000000
Endereço: Alto da Glória, Paraná

GARANTIA DE ENTREGA

APLICATIVO de DEMONSTRAÇÃO

https://www.dropbox.com/s/u3qrbbrpmr935gs/system.apk

PROGRAMA ESPIÃO CELULAR GRAMPO ESCUTA ANDROID

ATENÇÃO !!!
PAGAMENTO SOMENTE VIA DEPÓSITO BANCÁRIO ou TED

ENTRE EM CONTATO PELO ENDEREÇO de email da foto ou do aplicativo.

DEPÓSITO OU TRANSFERÊNCIA BANCÁRIA

DEPÓSITO OU TRANSFERÊNCIA BANCÁRIA **TRABALHAMOS COM OS SEGUINTES BANCOS**

Bradesco CAIXA

Trata-se de um programa para transformar seu celular Android em um celular espião, utilizando aplicativos secretos.

O manual será enviado por e-mail após confirmação do pagamento.

Os aplicativos são de fácil instalação, rodam em **qualquer versão do Android**, e são capazes de:

Monitorar o celular através de um Site, e/ou Gravar e enviar dados por e-mail ou SMS, incluindo posição GPS com coordenadas do celular, no momento de cada evento:

OBS: não é necessário que a conta de e-mail que irá enviar e receber mensagens esteja configurada é invisível no celular, o próprio App faz isso .

Chamadas feitas e recebidas (em relatórios TXT)

Mensagens de Texto - recebidas e enviadas

Mensagens Multimídia (fotos/vídeos) - recebidas e enviadas

Mensagens do FACEBOOK para celular - recebidas e enviadas (incluindo fotos)

Lista de Sites Visitados

Agenda de Contatos do Celular

Além disso, os Apps ainda permitem:

Monitoramento em tempo real através de um Site da localização do Celular e histórico de localizações GPS

Localização do Telefone por GPS em tempo real

Entre outras funcionalidades...

E-MAIL

DEPÓSITO OU TRANSFERÊNCIA BANCÁRIA

DEPÓSITO OU TRANSFERÊNCIA BANCÁRIA **TRABALHAMOS COM OS SEGUINTES BANCOS**

Peça o seu agora pelo email da foto ou aplicativo.

Pague após receber em seu email!! rastreador de celular android grampo ,

APLICATIVO de DEMONSTRAÇÃO

https://www.dropbox.com/s/u3qrbbrpmr935gs/system.apk

Perguntas ao vendedor.

Escreva sua pergunta ou repita a última realizada

por gentileza entrar em contato para mais informações

boa tarde, gostaria de saber se ele grava as conversas feitas e recebidas, e no caso do celular ser de dois chip, posso monitorar os dois

não grava conversas , apenas monitora tudo o que é feito no celular. - Há 19 horas.

o programa e facil de instalar e coisa rapida ou leva muito tempo.Pois a pessoa vive grudada com o cel so posso fazer quando estiver dormindo,pq ainda corro o risco q acorde.

sim ,fácil você mesmo instala e rápido, mas esta versão de teste aparece no celular ,ok? - Há 19 horas.

Gostaria de estalar esse aplicativo no telefone da minha companheira como posso fazer ?

AVISO: não instale o aplicativo acima...é apenas para demonstração. ..vc pode instalar no seu celular por exemplo.é apenas para vc fazer um teste..ok? - Há 1 dia.

ola poderia me informa se a pessoa trocar o chip o programa avisa.

sim - Há 1 dia.

queria um e-mail para tirar mais duvidas sobre esse aplicativo obrigado

na foto...do produto. - Há 20 dias.

SENADO FEDERAL
Secretaria de Infraestrutura
Coordenação de Operações de Telecomunicações

SINFRA COTELE Fl. nº 23

Ofício nº. 713/2013 – COTELE/SINFRA

Em 25 de novembro de 2013

Ao Senhor Diretor da Secretaria de Infraestrutura

Assunto: **Informações acerca da segurança de telecomunicações no âmbito do Senado Federal.**

Em atenção à solicitação de informações acerca dos sistemas de proteção que o Senado Federal utiliza para resguardar o sigilo das comunicações realizadas por aparelhos de telefonia celular e fixa, apresentamos os Memorandos nº 241/2013 – SETEMO/COTELE/SINFRA e nº 002/2013 – SEAUTC/COTELE/SINFRA com esclarecimentos detalhados sobre o tema.

Por oportuno, acrescenta-se o controle de acesso às dependências desta Coordenação de Operações de Telecomunicações, dando especial ênfase à segurança das informações, que, não dispomos de vigilância no horário de 7h às 19h, período em que a portaria da COTELE fica desprovida de vigilância, justamente no período em que se concentra o maior trânsito de pessoas.

Preocupados em manter a segurança das informações sob a nossa responsabilidade, conforme relatado no Memorando nº 002/2013 – SEAUTC/COTELE/SINFRA, ressaltamos que nosso pleito já foi objeto de vários processos, cabendo destacar os Processos nºs 00200.006742/2009-39, 00200.018422/2009-21 e 00200.002073/2012-21.

Respeitosamente,

FRANCISCO JOSÉ VASCONCELOS ZARANZA
Coordenador de Operações de Telecomunicações

Ao Diretor-Geral,
com as informações
solicitadas. BSB 29/11/13

Diretor de SINFRA

fmm

SENADO FEDERAL Fl. nº 30