



SENADO FEDERAL

Diretoria Geral - DGER

Secretaria de Tecnologia da Informação - Prodases

DOCHSBC

Memorando nº 7/2016 - GBPRD

441

Brasília, 15 de março de 2016.

A Sua Excelência o Senhor
SENADOR PAULO ROCHA
 Presidente CPIHSBC
 Senado Federal

Assunto: **Análise de Dados - CPIHSBC.**

Em resposta ao Memorando nº 016/2016/CPIHSBC - Documento nº 031787/2016-07, venho informar a Vossa Excelência que no dia 08/03/2016 uma equipe técnica do Prodases compareceu à Coordenação de Comissões Especiais, Temporárias e Parlamentares de Inquérito - COCETI para analisar o conjunto de arquivos recebidos por aquela Coordenação. Nessa análise verificou-se a existência de duas imagens que, pelas características dos arquivos, indicam serem da mesma máquina. Tais imagens são compostas por duas partições cada: uma menor para a inicialização do sistema e outra maior supostamente contendo os dados. A partição menor contém apenas informações de sistema operacional para reinicialização da máquina, enquanto a partição maior não pode ter o seu conteúdo avaliado por estar cifrada. Esta partição possui um cabeçalho com metadados que sugerem o uso de whole-disk encryption (criptografia de todo o disco). Os mecanismos criptográficos utilizados – conjunto de técnicas desenvolvidas para garantir o sigilo dos dados deixando-os similares a um conjunto aleatório de bytes - não possuem registro público recente de ferramentas ou de tecnologias disponíveis capazes de decifrá-los, o que dificulta a recuperação da informação original.

No entanto, existe a possibilidade da utilização de hardware e software especializados que possam fazer esse trabalho. Estas ferramentas estão disponíveis em órgãos que tenham o estudo e a necessidade da quebra de algoritmos criptográficos como parte de sua atividade finalística. Tendo em vista a dificuldade matemática em diferenciar o conjunto dos dados cifrados de um conjunto qualquer de dados embaralhados, nem mesmo é possível garantir que a partição esteja criptografada, conforme sugerido em seu cabeçalho.



**SENADO FEDERAL**

Diretoria Geral - DGER

Secretaria de Tecnologia da Informação - Prodasen

Seja pela criptografia, seja pela utilização de alguma técnica de ocultação de dados, o Prodasen não dispõe de meios para decifrar o conjunto de dados recebidos. Dessa forma sugiro respeitosamente à Comissão Parlamentar de Inquérito verificar junto a órgãos especializados a possibilidade de apoio à análise dos referidos arquivos, tendo em vista a possibilidade de dispor de pessoas, software e hardware específicos e qualificados para tais tarefas.

Ressalto o compromisso do Prodasen em apoiar os trabalhos dessa Comissão junto à COCETI nas demais necessidades e estamos à disposição para maiores esclarecimentos.

Respeitosamente,

Alessandro Pereira de Albuquerque
Diretor do Prodasen

