SERVIÇO PÚBLICO FEDERAL
MJ - POLÍCIA FEDERAL
SUPERINTENDÊNCIA REGIONAL NO PARANÁ
Rua Profª. Sandália Monzon nº 210, Santa Cândida - Curitiba/PR - CEP 82.640-040 - fone: (41) 3251-7500

Ofício nº 5912/2017 - SR/PF/PR

Curitiba/PR, 26 de setembro de 2017.

Ao Excelentíssimo Senhor
Sergio Fernando Moro
Juiz Federal da 2ª Vara Federal Criminal de Curitiba
Av. Anita Garibaldi, 888, Ahú - Curitiba/PR
CEP 80.540-180

13ª VARA FEDERAL 27/09/17 16:27

Assunto: **Encaminha documento.**

Referência: **Ação Penal 5014170-93.2017.4.04.7000**

Senhor(a) Juiz(a),

Em atenção ao Ofício judicial 700003705400, relacionado à Ação Penal em referência (evento 577), encaminho a Vossa Excelência o Laudo nº 1837/2017-SETEC/DR/PF/PR com uma mídia embalada em saco plástico lacre nº 3119234.

Respeitosamente,

FELIPE EDUARDO HIDEO HAYASHI
Delegado de Polícia Federal
Classe Especial - Matrícula nº 16.027

Polícia Federal
Diretoria Técnico-Científica
Criminalística

Usuário: amanda.aac
(sair)

Recibo de Entrega

Movimentação

Origem: SETEC/SR/PF/PR - Setor Técnico-Científico
Destino: SR/PF/PR - Superintendência Regional de Polícia Federal no Paraná
Despacho: ENCAMINHO AO DPF HAYASHI OS ITENS RELACIONADOS ABAIXO REF AO MEMO 5905/2017-SR/PF/PR.
Data da movimentação: 18/09/2017 10:51:52
Procedimento de referência: Ação Penal 5014170-93.2017.4.04.7000/PR-SR/PF/PR
Registro de referência: 2809/2017-SETEC/SR/PF/PR

Conteúdo (02 itens)

Material 4169/2017-SETEC/SR/PF/PR
Data de registro: 03/08/2017
Tipo: Dispositivo de armazenamento computacional (Mídia ótica)
Finalidade: Exame
Número de itens: 1
Medida: 700 megabyte(s)
Descrição: 01 CD-R DA MARCA BEST WAY.
Lacre: 3119234

Laudo 1837/2017-SETEC/SR/PF/PR
Data de emissão: 11/09/2017
Classe: Laudo de Perícia Criminal Federal
Subclasse: Informática

Dossiê: D17-1763-SETEC/PR

Recebimento

Declaro ter conferido e recebido os itens relacionados.

Data: ____/____/_____

Assinatura: _____

Nome: _____

Matrícula: _____

Ao DPF Sch para encaminhamento ao Juízo da 13ª VF (Cumpra-se no expediente) 5014170-93.2017.4.04.7000).

26/9/17.

FELIPE EDUARDO HIDEO HAYASHI
Delegado de Polícia Federal
Chefe da DELECOR/PR

SERVIÇO PÚBLICO FEDERAL
MJSP - POLÍCIA FEDERAL
SUPERINTENDÊNCIA REGIONAL DE POLÍCIA FEDERAL NO PARANÁ
SETOR TÉCNICO-CIENTÍFICO

LAUDO Nº 1837/2017 – SETEC/SR/PF/PR

LAUDO DE PERÍCIA CRIMINAL FEDERAL

(INFORMÁTICA)

Em 11 de setembro de 2017, no SETOR TÉCNICO-CIENTÍFICO da Superintendência Regional de Polícia Federal no Paraná, designado pelo Chefe, Perito Criminal Federal FÁBIO AUGUSTO DA SILVA SALVADOR, o Perito Criminal Federal LUIS HENRIQUE BOGO elaborou o presente Laudo Pericial, no interesse da Ação Penal nº 5014170-93.2017.4.04.7000/PR-SR/PF/PR, a fim de atender a solicitação do Delegado de Polícia Federal FELIPE EDUARDO HIDEO HAYASHI, contida no Memorando nº 5905/2017-SR/PF/PR de 03/08/2017, registrado no Sistema de Criminalística sob o nº 2809/2017-SETEC/SR/PF/PR em 03/08/2017, descrevendo com verdade e com todas as circunstâncias tudo quanto possa interessar à Justiça e atendendo ao solicitado, abaixo transcrito:

> "[...] requisito seja verificada a possibilidade de acesso aos arquivos e a devolução dos mesmos sem criptografia **até o dia 14.08.2017**.".

I - MATERIAL

Este Laudo apresenta o resultado dos exames efetuados no material descrito na Tabela 1, o qual foi encaminhado através do Ofício nº 700003705400, da 13ª Vara Federal de Curitiba.

Tabela 1 – Informações sobre o material examinado.

SISCRIM Material nº 4169/2017-SETEC/SR/DPF/PR (Recebido em embalagem lacrada do SETEC/PR de nº 3119162)
Descrição
01 (uma) mídia óptica do tipo CD-R, marca BestWay, com capacidade nominal de 700 MB.

II - OBJETIVO

Este laudo pericial é realizado com a finalidade de descriptografar os arquivos

Visto

0036313317
Laudo 1837/17-SETEC/PR

747-A

contidos na mídia óptica encaminhada.

III - EXAME

A mídia óptica encaminhada contém dois arquivos, conforme apresentado na Tabela 2.

Tabela 2 – Arquivos presentes na mídia óptica.

Nome	Código hash (MD5)
CT Pentagram vs Cap Dupell - Schahin.pdf.pgp	f18d34239b3068113767a4d4686bd18d
CT Pentagram vs Casablanca - Schahin (com carta de aceite).pdf.pgp	d184736fe86289b7c6be413a448b02b2

Para a descriptografia dos arquivos listados na Tabela 2, faz-se necessário a utilização dos arquivos com as chaves públicas e privadas. Estes arquivos foram recebidos posteriormente, na data de 04/08/2017, através do encaminhamento de e-mail enviado pela Procuradoria da República do Paraná, totalizando 09 (nove). Os arquivos recebidos pelo e-mail são listados na Tabela 3.

Tabela 3 – Arquivos recebidos por e-mail.

Nome	Código hash (MD5)
pubring-bak-bak.pkr	bfc8a4cc861a3e190f4b0d76be536576
pubring-bak.pkr	bfc8a4cc861a3e190f4b0d76be536576
pubring.pkr	bfc8a4cc861a3e190f4b0d76be536576
pubringUP.pkr	bfc8a4cc861a3e190f4b0d76be536576
secring-bak-bak.skr	75fcc84af9e4d5758f340d54e7ad2413
secring-bak.skr	75fcc84af9e4d5758f340d54e7ad2413
secring-bakUP-bak.skr	75fcc84af9e4d5758f340d54e7ad2413
secring-bakUP.skr	75fcc84af9e4d5758f340d54e7ad2413
secring.skr	dab8a36682182693776aa584d45d2d6e

Os arquivos listados na Tabela 3 foram processados no cluster de alto desempenho disponível neste SETEC/PR. Esse equipamento efetua grande quantidade de cálculos matemáticos e possibilita, com a utilização de aplicativos específicos, a realização de ataques criptográficos[1] ou por força bruta[2] em arquivos cifrados. Foram realizados ataques de força bruta e com dicionários disponíveis no aplicativo de quebra de senhas. Estes ataques

[1] Ataque criptográfico é o método utilizado para atacar a segurança de um sistema de cifragem através de busca por vulnerabilidades no seu protocolo, algoritmo ou sistema de gerenciamento de chaves. Normalmente é mais rápido que o ataque por força bruta.

[2] Ataque por força bruta é a técnica criptográfica na qual são testadas todas as combinações possíveis para as senhas.

Visto

foram realizados por cerca de 8 dias, totalizando cerca de 810.000.000.000 (oitocentos e dez bilhões) de combinações, distribuídas entre todos os arquivos, porém sem sucesso.

IV - CONCLUSÃO

Conforme exposto na Seção III, foram realizados tentativas de quebras de senhas utilizando-se de dicionários disponíveis no aplicativo de quebra de senhas e com ataques por força bruta. Foram testadas, no total, cerca de 810.000.000.000 (oitocentos e dez bilhões), sem sucesso.

Tendo por bem esclarecido o assunto, o Perito devolve, com o Laudo, o material nº 4169/2017-SETEC/SR/PF/PR, lacrado em envelope de segurança sob o número 3119234.

Nada mais havendo a lavrar, o Perito Criminal encerra o presente laudo, abaixo assinado, elaborado em três páginas.

LUIS HENRIQUE BOGO
PERITO CRIMINAL FEDERAL

Visto