**Despacho n.º 737/2019 – CHEFIA GAB/PGR**
(PGR-00311153/2019)

**Ref:** PGEA 1.00.000.010610/2019-84

Trata-se de procedimento instaurado no Gabinete da Procuradora-Geral da República com base em informações encaminhadas por membros das Forças-Tarefa Lava Jato do Rio de Janeiro e Curitiba, noticiando possíveis invasões de *hackers* a aplicativos instalados em aparelhos celulares funcionais.

Previamente a esta comunicação formal dos membros das Forças-Tarefas Lava Jato, a Secretaria de Tecnologia da Informação desta PGR já havia sido orientada a adotar as providências de apoio aos membros no sentido de se identificar as causas de possíveis ataques divulgados pela mídia e medidas a serem adotadas.

Com esta finalidade, foram produzidas uma Nota Explicativa e uma Cartilha de Informações já devidamente divulgadas a todos os membros a partir do dia 08 de maio de 2019.

Ultimadas as providências de instrução do Procedimento acima referido, o Sr. Secretário de Tecnologia da Informação e Comunicação e Secretária Adjunta encaminharam, nesta data, o Relatório Técnico nº 001/2019/STIC/SG, onde registram todas as diligências adotadas e sugestões para aprimoramento do sistema de segurança institucional, que estão assim sumariadas:

*"Sumário*

***2.9 Primeira reunião presencial na empresa Claro***
***2.10 Nova Nota Explicativa destacando o ataque por sequestro de ligações e SMS***
***2.11 Primeira resposta da Claro afastando violação de SS7***
***2.12 Solicitação de reunião com a Claro e com o MPF pela Polícia Federal***
***2.13 Reunião com a Polícia Federal, Claro e MPF afastando clonagem 2.14 Reunião com a procuradores da FT LJ em São Paulo***
***2.15 Envio de nova Nota ratificando medidas de segurança e orientando envio de evidências à STIC***
***2.16 Envio do Ofício nº 144/2019/STIC à Polícia Federal***
***2.17 Ataque ao Ministro e contato com o Ministério da Justiça***
***2.18 Reunião presencial com Polícia Federal, Ministério da Justiça e MPF***
***2.19 Segundo Ofício para a empresa Claro com números de telefone a serem analisados***
***2.20 Envio de informações sobre ataque à Polícia Federal***
***2.21 Pedido à Claro para resposta ao Ofício nº 149/2019/STIC e inclusão de novo número de telefone no levantamento .***
***2.22 Elaboração de Parecer técnico por peritos da SPPEA e da STIC***
***2.23 Pedido da Polícia Federal de Brasília para colaboração e apoio técnico do MPF***
***2.24 Resposta da Claro ao Ofício nº 149/2019/STIC***
***2.25 Envio das informações da resposta da Claro à Polícia Federal***
***2.26 Solicitação à Claro para informações sobre número de telefone que despertou suspeita e levantou nova hipótese***
***2.27 Nova reunião presencial com Polícia Federal e MPF***
***2.28 Envio do Ofício nº 155/2019/STIC à Polícia Federal***
***2.29 Desvendando o método de ataque***
***2.30 Validação de todo o ciclo do ataque e envio dessas informações à Polícia Federal***
***2.31 Pedido de cancelamento das caixas postais dos telefones institucionais***
***2.32 Desdobramento das investigações***
***3.CONCLUSÃO"***

A Secretaria de Tecnologia da Informação e Comunicação (STIC) apresentou a seguinte conclusão dos trabalhos realizados:

> *"3. Conclusão*
>
> *Em resposta à solicitação encaminhada pela Procuradora Geral da República Exma. Dra. Raquel Elias Dodge, foram registrados todos os eventos relevantes para afirmar que não foram encontrados elementos que indiquem que houve acesso indevido ou subtração de dados ou informações diretamente dos aparelhos celulares e demais dispositivos de acesso aos aplicativos Telegram ou WhatsApp dos membros do MPF noticiantes. Após uma série de reuniões, pesquisas e testes, envolvendo equipe técnica da STIC, operadoras de telefonia, Ministério da Justiça e Polícia Federal é possível afirmar que os ataques e comprometimentos ocorreram em soluções hospedadas e mantidas fora da infraestrutura do Ministério Público Federal. Em específico, os ataques visaram o sequestro das contas dos referidos aplicativos de mensageria, utilizando-se de vulnerabilidades de telecomunicação e configuração das caixas postais dos usuários, localizadas nas operadoras, quais sejam, a possibilidade de realização e recebimentos de ligações onde o número de origem é igual ao de destino (A=B) e essa condição ser suficiente para um acesso completo à caixa postal da vítima.*

*Como descrito anteriormente, desde o dia **8 de maio** a Secretaria de Tecnologia vem reiteradamente comunicando e recomendando medidas apropriadas e suficientes à segurança dos aparelhos telefônicos. Essas medidas foram, inclusive, repassadas e adotadas pelo Ministério da Justiça e Polícia Federal, com o intuito de conscientizar e proteger os seus membros.*

*Destaca-se que, ao habilitar a dupla verificação, o usuário deixa de estar vulnerável ao ataque porque o acesso ao código do Telegram ou WhatsApp não fornece elementos suficientes para o sequestro da conta, sendo necessário o fornecimento da senha cadastrada na dupla verificação. Além disso, com a implementação do pedido de cancelamento das caixas postais dos telefones institucionais dos membros do MPF eliminamos o alvo do ataque e, consequentemente, a vulnerabilidade explorada. Entretanto, há que se insistir que os aplicativos Telegram ou WhatsApp não devem ser utilizados para questões institucionais, e sim, o eSpace, solução parte do Serviço de Comunicação e Colaboração Unificada (UCC) licitada e adotada pelo órgão para tornar seguras as comunicações móveis e fixas, videoconferências e mensageria, utilizando-se de infraestrutura própria e criptografia baseada em certificados emitidos pelo MPF.*

*Por fim, apresentou-se nesse documento uma sequência cronológica de todos os fatos, diligências e providências adotadas, com o intuito de esclarecer os ataques, identificar seu método e ratificar a eficácia das medidas sugeridas. Evidenciou-se, também, não só o caráter colaborativo de todo esse levantamento, mas sobretudo, as relevantes contribuições do Ministério Público Federal com as investigações que visam identificar o autor dos ataques.*"

É o relatório.

Verifico que as providências necessárias para orientação, acompanhamento, adoção de medidas preventivas e de apoio material a membros do Ministério Público Federal e às investigações em curso foram adotadas e estão devidamente retratadas no Relatório acima.

A conclusão dos trabalhos técnicos desenvolvidos sob minha determinação afastou situação de fragilidade da segurança institucional do Ministério Público Federal e comprovou que nenhum sistema disponibilizado pelo Ministério Público da União foi alvo de invasões ou ataques cibernéticos de qualquer natureza.

Observo, no entanto, que há indicação técnica para adoção da solução *eSpace,* dispositivo que integra o serviço de comunicação e colaboração unificada, adotado pelo

Órgão para tornar seguras as comunicações móveis e fixas por videoconferência ou mensageria. Esta ferramenta utiliza infraestrutura própria e criptografia devidamente certificada pelo MPF.

Diante destas orientações técnicas e, considerando que a ferramenta *eSpace* já está disponibilizada aos membros e servidores do MPF, mas diante das informações ora apresentadas verifica-se a necessidade de elevar a segurança da comunicação institucional e, portanto, determino a elaboração de Portaria para definir a solução tecnológica acima referida como a ferramenta institucional para comunicação dos membros e servidores do MPF.

Brasília, 28 de junho de 2019.

Raquel Elias Ferreira Dodge
**Procuradora-Geral da República**