1 INTRODUÇÃO

Operação Pombo – Uma abordagem Forense

Operação Pombo , fundamenta-se em procedimento investigatório criminal instaurado pelo MP-GAECO em 3 de maio de 2022, para apurar a relação ilícita de advogados com integrantes de facções criminosas que se encontram custodiados em estabelecimentos prisionais paraenses.

No decorrer de um ano, a investigação realizada no contexto da Operação Pombo conseguiu constatar a relação criminosa existente entre integrantes custodiados da facção Comando Vermelho e o advogado, o qual vinha funcionando como “mensageiro”, ao se utilizar de suas prerrogativas conferidas legalmente pelo exercício da advocacia (Lei nº 8.906/94) para servir de elo entre faccionados presos e faccionados soltos, repassando as informações obtidas por ocasião das visitas realizadas em estabelecimentos prisionais no Estado do Pará. Essas informações eram gravadas por Smartwatch e repassadas para os celulares dos advogados que estavam bloqueados com senhas pessoais. O trabalho do Núcleo de Fonética Forense e Extração de Dados da Polícia Científica do Pará, foi realizar o desbloqueio desses aparelhos, e em seguida realizar a extração dos dados dos mesmos para auxiliar nas investigações do MP-GAECO.

Operação Pombo

Polícia Científica tem atuação decisiva para a prisão de dois advogados

A Polícia Científica do Pará (PCEPA) foi determinante na Operação Pombo, realizada pelo Grupo de Atuação Especializada no Combate ao Crime Organizado (Gaeco), do Ministério Público do Pará (MPPA), em que foram detidos dois advogados acusados de serem informantes de membros de facções criminosas dentro das unidades prisionais do Estado. Eles visitavam os locais por meio das prerrogativas legais, uma vez que, exerciam a advocacia em favor dos internos.

Os peritos da Polícia Científica analisaram os aparelhos eletrônicos apreendidos com os advogados. Os equipamentos eram utilizados para gravar mensagens durante as visitas nas unidades prisionais. Eles também utilizavam uma agenda e bilhetes escritos à mão, repassados pelos advogados à integrantes da mesma facção dos internos que estão em liberdade.

Os aparelhos eletrônicos foram analisados pelo setor de extração de dados do Núcleo de Fonética Forense. Os celulares eram altamente criptografados, com senhas fortes e programa pago de bloqueio de aplicativos, porém, foram utilizadas técnicas forenses de tecnologia de quebra de senhas e, assim, os dados foram extraídos com sucesso pelos peritos. O laudo constatou que os áudios gravados eram transferidos nos aparelhos eram repassados para vários grupos de aplicativos de mensagem instantânea das facções.

Agencia Pará

https://www.agenciapara.com.br/noticia/37563

Jornal O Impacto

Polícia Científica tem atuação decisiva para a prisão de dois advogados
https://oimpacto.com.br/2022/06/03/policia-cientifica-tem-atuacao-decisiva-para-a-prisao-de-dois-advogados/

2 OBJETIVOS

A presente perícia teve por finalidade o desbloqueio, extração de dados tanto ativos, como a possível recuperação de informações que ora estivesse deletada pelos usuários dos aparelhos de telefonia celular.

E para finalizar, a análise desse conteúdo extraído com base na Requisição de Perícia em questão.

2 OBJETIVOS

Figura 1 – Frente do celular periciado

Fonte: Dos Autores (2022)

Figura 2 – Posterior do celular periciado

Fonte: Dos Autores (2022)

3 METODOLOGIA

A metodologia aplicada durante a perícia foi a seguinte:

- Caracterização do material encaminhado a exame pericial;
- Técnicas de desbloqueio, Bypass e Brutal Force (Força bruta);
- Extração/decodificação dos dados;
- Composição e redação do laudo pericial.

3 METODOLOGIA

Bypass - É o contorno de senha, onde a ferramenta forense não quebra, apenas contorna e coleta as informações do aparelho através de uma extração física, deixando a senha íntegra ainda no aparelho.

3 METODOLOGIA

Brutal Force (Força Bruta) - Um ataque de força bruta consiste em todo e qualquer método usado por um invasor para descobrir uma senha, uma chave criptográfica ou outro tipo de informação sigilosa, por meio de tentativa e erro. Como exemplo, pense em um cofre que exige uma combinação de quatro números como senha. Essa combinação pode ir de 0000 a 9999, portanto. Agora, imagine um ladrão tentando abrir esse cofre. Ele não consegue arrombar a porta, então decide testar todas as combinações possíveis (0000, 0001, 0002, 0003, …) até descobrir aquela que abre o cofre.

Podemos dizer que esse é um tipo ataque de força bruta. Rudimentar, trabalhoso e pouco eficiente, mas não deixa de ser interessante. Se não tiver sorte, o ladrão levará dias ou semanas tentando e errando até encontrar a combinação certa.

4 RESULTADOS E DISCUSSÃO

Com a ajuda da ferramenta forense **XRY** da **MSAB** (na época versão 10.0.1), foi realizado procedimento de ***BYPASS***, utilizando a técnica ***ADB (Android Debug Bright),*** onde se teve acesso a porta **5307** do aparelho de telefonia celular em questão, assim sendo, foi feito acesso a memória física do aparelho.

Em seguida foi feita o ataque por força bruta, conseguindo obter acesso a senha de desbloqueio do aparelho .

Figura 3 – Celular sendo periciado

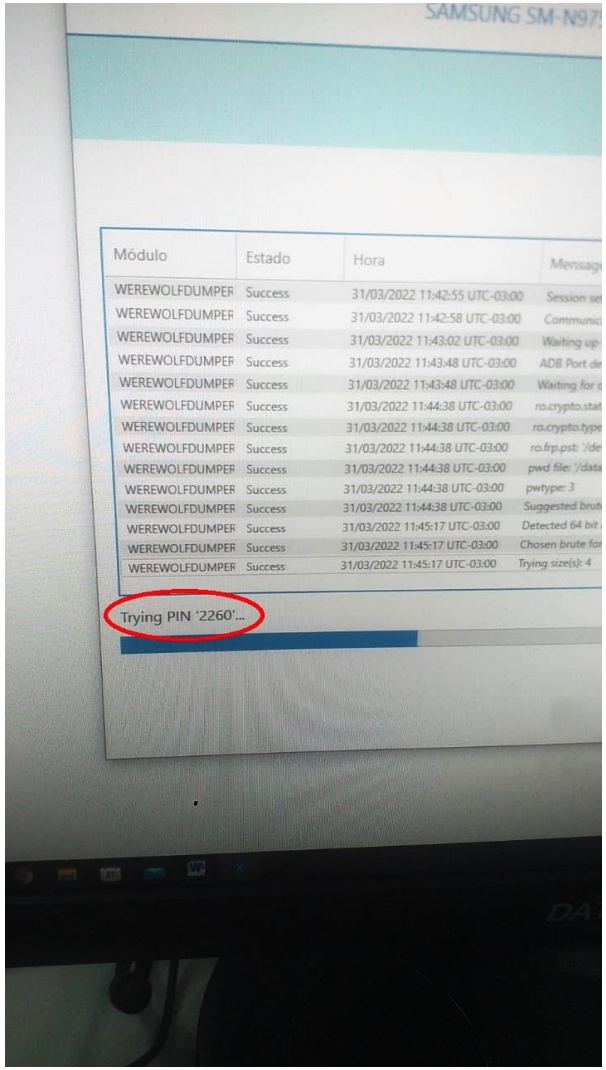
Fonte: Dos Autores (2022)

Figura 4 – Celular desbloqueado

Fonte: Dos Autores (2022)

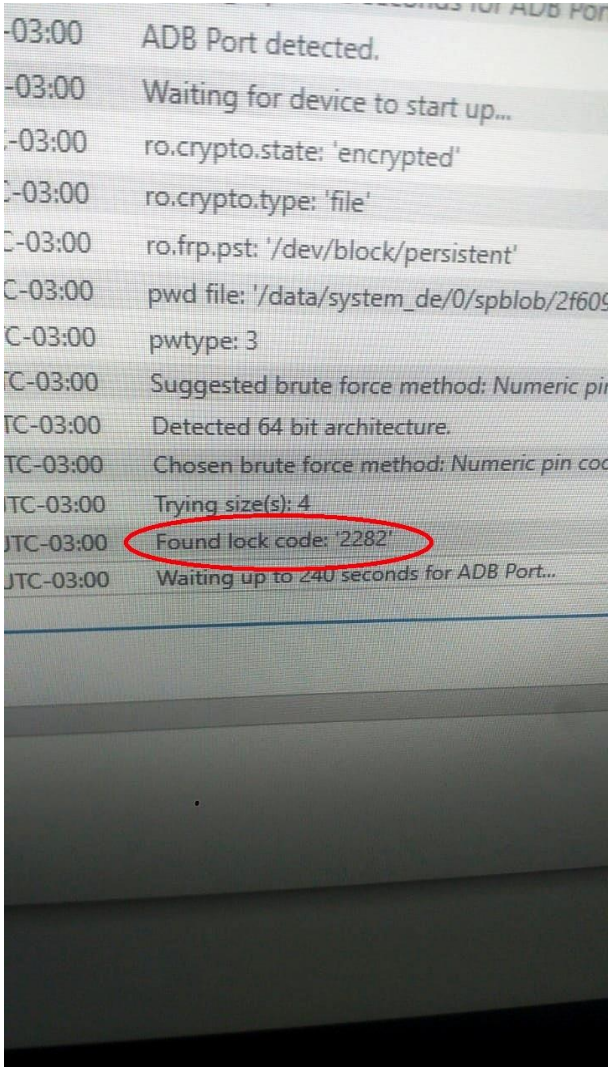
4 RESULTADOS E DISCUSSÃO

Figura 5 – Aplicação do método por Força Bruta



Fonte: Dos Autores (2022)

Figura 6 – Senha descoberta utilizando o método por força bruta



Fonte: Dos Autores (2022)

4 RESULTADOS E DISCUSSÃO

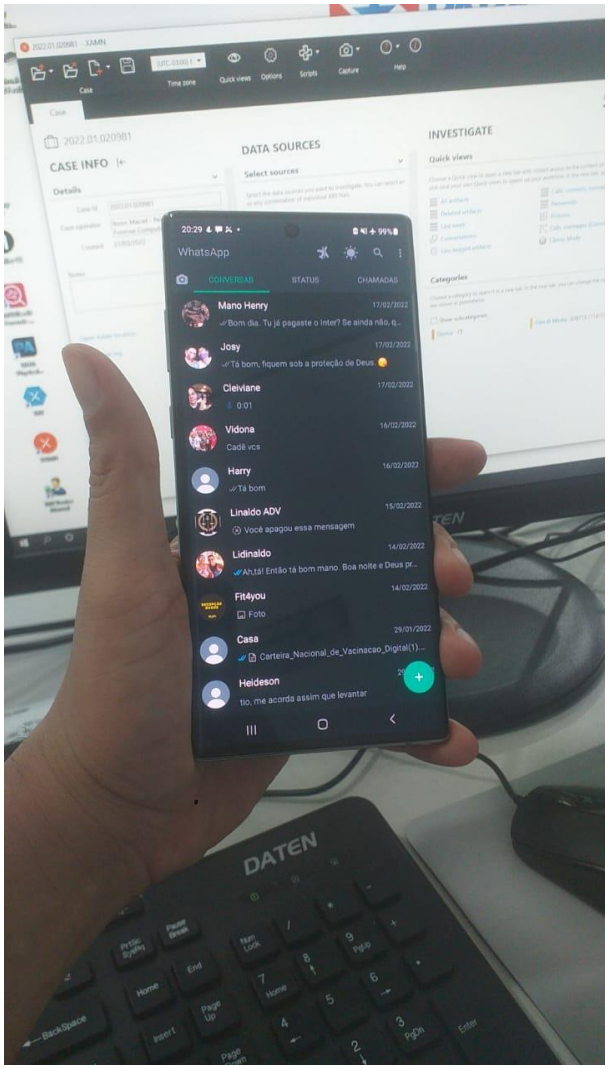
Após o desbloqueio dos aparelhos de telefonia celular, em um deles foram identificados 03 (três) tipos de aplicativo WhatsApp, o **WhtasApp normal**, o **WhatsApp Business** e o **YOWhatsApp**. Ambos os aplicativos estavam bloqueados pelo **App Locker (ver "Ilustração),** foi explorada uma vulnerabilidade do aplicativo, entrando no modo seguro do aparelho de telefonia celular, forçando a interrupção do aplicativo, e em seguida desinstalando o mesmo, normalizando assim o acesso aos aplicativos que estavam bloqueados no aparelho de telefonia celular.

4 RESULTADOS E DISCUSSÃO

Figura 7 – App Locker bloqueando os aplicativos do celular

Fonte: Dos Autores (2022)

Figura 8 – App Locker desinstalado no aparelho celular

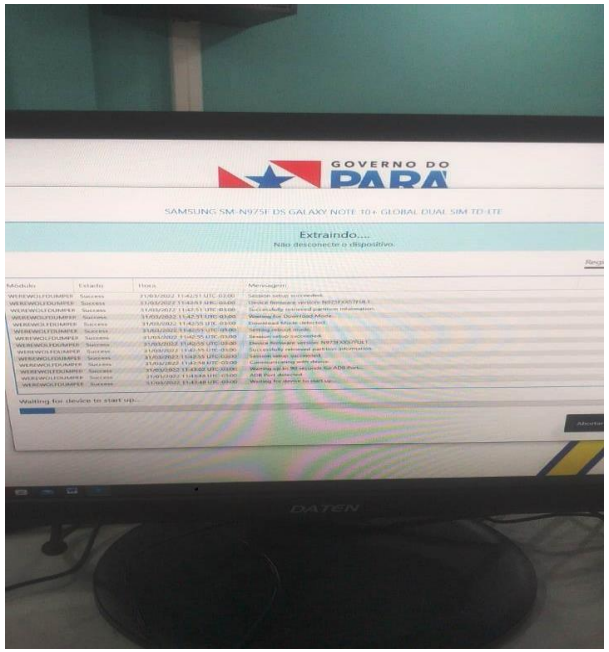


Fonte: Dos Autores (2022)

4 RESULTADOS E DISCUSSÃO

Em seguida, foi realizada a extração e decodificação dos dados armazenados nos aparelhos de telefonia celular utilizando-se a ferramenta forense **"XRY da MSAB" (na época versão 10.0.1)**. Com o procedimento foi possível obter arquivos de mensagens sms e de aplicativos, fotos, imagens, áudios, vídeos, documentos, localização GPS, histórico da web, lista de contatos e registro de chamadas.

Figura 9 – Extração sendo realizada pelo Software Forense XRY da MSAB



Fonte: Dos Autores (2022)

5 CONCLUSÃO

Com o desbloqueio, extração, análise do conteúdo e a confecção dos laudos pelo Núcleo de Fonética Forense e Extração de Dados da Polícia Científica do Pará, dos dois celulares dos advogados faccionados, a **"Operação Pombo"** do GAECO-MP que durava mais de um ano, foi deflagrada com sucesso!

6 AGRADECIMENTOS

Registramos nossos devidos agradecimentos a toda nossa **equipe** incansável do **Núcleo de Fonética Forense e extração de Dados**, ao nosso Coordenador Perito Criminal **Orley Cruz**, a toda equipe de **Peritos** e **Engenheiros** da **CEL – PCEPA**, todos os **Promotores** do **GAECO – MP**, toda diretoria da **ASPOP** e o Diretor Geral da PCEPA, Perito Criminal **Celso Mascarenhas**, pelo apoio incondicional e parceria nos trabalhos desenvolvidos por este setor de Fonética Forense e Extração de Dados.

REFERÊNCIAS

ELEOTÉRIO, Pedro; MACHADO, Márcio. **Desvendando a Computação Forense.** 1ª. ed. São Paulo: Novatec Editora, 2011.

FIGUEIREDO, Jorge; FRANÇA JUNIOR, Fausto. **Extração Forense avançada de dados em dispositivos móveis.** 1ª. ed. São Paulo: Brasport Editora, 2022.