**Convenção de Budapeste – Estudo de caso**

**Enquadramento**

A Terra do Meio é um pequeno país em desenvolvimento fictício em África e vizinho de dois outros países, Rohan e Mordor. É membro da OMC e das Nações Unidas e é parte na Convenção de Budapeste sobre Cibercrime. A Terra do Meio tem sido tradicionalmente um centro de uma indústria bancária e financeira próspera. O seu maior banco, o Middle Earth National Bank (“MENB”), tem várias sucursais na região e a nível internacional. O Terra do Meio é a língua oficial do país.

É um agente responsável pela aplicação da lei da Terra do Meio, encarregado da investigação de cibercrimes no país.

**Parte 1 – Direito material:**

Recebe uma denúncia anónima de que criminosos informáticos piratearam o servidor principal do MENB. Os criminosos informáticos instalaram malware que altera aleatoriamente a dimensão do cursor do rato e o papel de fundo de todos os computadores ligados ao servidor principal. A sua investigação sugere que o malware foi criado por um grupo de piratas informáticos conhecido por “DarkHacker”.

No âmbito da sua investigação, identifica o site oficial do DarkHacker como www.darkhacker.com. Constata que o software aparentemente concebido para traduzir texto da língua da Terra do Meio para inglês está a ser vendido no site, mas é comercializado como permitindo também a piratear computadores.

A sua investigação revela igualmente que dados dactiloscópicos, que permitem o acesso a computadores portáteis e smartphones, estão a ser vendidos em [www.darkhacker.com](http://www.darkhacker.com). Na tentativa de identificar os indivíduos que operam o DarkHacker, realiza uma operação infiltrada e compra dados dactiloscópicos em www.darkhacker.com.

**Perguntas:**

* Que cibercrime(s) foi(ram) cometido(s) através da pirataria informática e da instalação do malware no servidor do MENB?
* Que cibercrime(s) pode identificar como tendo sido cometido(s) pelo DarkHacker?
* Cometeu uma infração de cibercrime ao adquirir dados dactiloscópicos ao DarkHacker?

**Parte 2 – Direito processual:**

No âmbito da operação infiltrada para adquirir dados dactiloscópicos ao DarkHacker, é-lhe solicitado que introduza o seu endereço de e-mail para receber instruções relativas ao pagamento. Recebe um e-mail de uma conta de e-mail [criminal@scammail.com](mailto:criminal@scammail.com) com instruções sobre como efetuar o pagamento usando bitcoin.

A sua investigação inicial revela que o fornecedor de serviços de e-mail de [criminal@scammail.com](mailto:criminal@scammail.com) é a Scam Mail Inc. Identifica o seu site como sendo [www.scammailinc.com](http://www.scammailinc.com). A partir do respetivo site, descobre que a Scam Mail Inc tem a sua sede social e o seu único centro de dados na Terra do Meio. Também descobre que a Scam Mail Inc. apenas conserva os dados durante um período de 7 dias após o qual todos os dados são apagados.

Pondera utilizar os endereços de e-mail para identificar os indivíduos que estão por trás do DarkHacker.

Considera também obter informações sobre outras pessoas contactadas através da conta de e-mail [criminal@scammail.com](mailto:criminal@scammail.com) nos últimos sete dias.

**Perguntas:**

* Que medidas iniciais deve tomar para garantir que o processo de investigação não é comprometido?
* Que tipo de informação necessitaria para identificar a pessoa que usa o e-mail [criminal@scammail.com](mailto:criminal@scammail.com)? Como obter essa informação da Scam Mail Inc?
* Como tentaria obter a informação da Scam Mail Inc relativamente a outras pessoas contactadas pelo e-mail [criminal@scammail.com](mailto:criminal@scammail.com) nos últimos sete dias?

**Parte 3 – Outras formas de cooperação**

Ao efetuar o pagamento usando bitcoin, recebe outro e-mail de uma conta de e-mail fraud@hackmail.com com os dados dactiloscópicos em anexo.

Mais uma vez, pondera utilizar os endereços de e-mail para identificar os indivíduos que estão por trás do DarkHacker. A sua investigação inicial revela que a Hack Mail Inc (com sede em Mordor) não tem qualquer escritório ou centros de dados na Terra do Meio, mas publicou recentemente anúncios sobre os seus serviços gratuitos na língua da Terra do Meio. A Hack Mail Inc armazena informação sobre os assinantes sob a forma de dados informáticos.

Tem conhecimento de várias pessoas em Mordor que se queixaram, em diferentes fóruns online, de incidentes de fraude alegadamente perpetrados pelo utilizador do e-mail [fraud@hackmail.com](mailto:fraud@hackmail.com). Deseja utilizar estas reclamações como prova em processos subsequentes. Além disso, contacta estas pessoas para obter informações e estas estão dispostas a consentir no acesso às suas contas e mensagens de e-mail.

**Perguntas:**

* Que tipo de informação necessitaria para identificar a pessoa que usa o e-mail [fraud@hackmail.com](mailto:fraud@hackmail.com)?
* Qual é a medida mais expedita para obter essa informação da Hack Mail Inc?
* Qual é a forma mais expedita de obter os e-mails enviados pelo utilizador do e-mail [fraud@hackmail.com](mailto:fraud@hackmail.com) às vítimas em Mordor?

**Parte 4 – Assistência jurídica mútua**

Após análise das informações que recebeu da Hack Mail Inc. e da Scam Mail Inc., identifica um indivíduo que faz parte do grupo DarkHacker: Boris Smith, cidadão da Terra do Meio.

Prende Boris Smith na Terra do Meio e ele divulga a localização do sistema informático que está a ser utilizado pelo DarkHacker em Rohan. Dado que a prisão de Boris não é pública, não parece existirem motivos para crer que os dados do sistema informático do DarkHacker sejam vulneráveis a perda ou alteração.

Boris informa-o de que a conta [fraud@hackmail.com](mailto:fraud@hackmail.com) foi utilizada para contactar outros agentes do DarkHacker. Informa-o igualmente sobre uma transação de grande escala de venda de códigos PIN de cartões de débito, prevista para o dia seguinte, às 17h00, utilizando a mesma conta de e-mail.

* Que medidas pode tomar para garantir que a Hack Mail Inc. preserva os dados relativos à conta de e-mail [fraud@hackmail.com](mailto:fraud@hackmail.com)?
* Que medidas deverá tomar para identificar outros fornecedores de serviços envolvidos na transmissão de comunicações relacionadas com a burla do DarkHacker?
* Que medidas pode tomar para obter dados informáticos do sistema informático do DarkHacker?
* Que medidas pode tomar para determinar a localização do cliente do DarkHacker que tenciona adquirir códigos PIN de cartões de débito?