**Convenio de Budapest – Estudio de caso**

**Antecedentes**

La Tierra Media es un pequeño país ficticio en desarrollo situado en África y vecino de otros dos países, Rohan y Mordor. Es miembro de la OMC, las Naciones Unidas y es parte en el Convenio de Budapest sobre la Ciberdelincuencia. La Tierra Media ha sido tradicionalmente un centro de una próspera industria bancaria y financiera. Su mayor banco, el Banco Nacional de la Tierra Media ("BNTM"), tiene varias sucursales en la región y a nivel internacional. El terrícola medio es el idioma oficial de la Tierra Media.

Usted es un oficial de las fuerzas del orden de la Tierra Media y es responsable de investigar los ciberdelitos en la Tierra Media.

**Parte 1 - Derecho sustantivo**

Recibe una notificación anónima de que unos ciberdelincuentes han jaqueado el servidor principal del BNTM. Los ciberdelincuentes han instalado un malware que cambia aleatoriamente el tamaño del cursor del ratón y el fondo de pantalla de todos los ordenadores conectados con el servidor principal. Su investigación sugiere que el malware fue creado por un grupo de piratas informáticos conocido como "DarkHacker".

Como parte de su investigación, identifica www.darkhacker.com como el sitio oficial de DarkHacker. Observa que en el sitio web se vende un software aparentemente diseñado para traducir textos de terrícola medio al inglés, pero que se comercializa como un programa que también permite jaquear ordenadores.

Su investigación también revela que en [www.darkhacker.com](http://www.darkhacker.com) se venden datos de huellas dactilares que permiten acceder a ordenadores portátiles y teléfonos inteligentes. En un intento de identificar a los individuos que están detrás de DarkHacker, lleva a cabo una operación encubierta y compra datos de huellas dactilares en www.darkhacker.com.

**Preguntas:**

* ¿Qué ciberdelitos se han cometido al jaquear e instalar malware en el servidor del BNTM?
* ¿Qué ciberdelitos cree que ha cometido DarkHacker?
* ¿Ha cometido usted un ciberdelito al comprar datos de huellas dactilares a DarkHacker?

**Parte 2 - Derecho procesal**

Como parte de la operación encubierta de compra de datos de huellas dactilares a DarkHacker, se le pide que introduzca su dirección de correo electrónico para recibir instrucciones de pago. Recibe un correo electrónico de la cuenta de correo electrónico [criminal@scammail.com](mailto:criminal@scammail.com) con instrucciones sobre cómo realizar el pago mediante Bitcoin.

Su investigación inicial revela que el proveedor de servicios de correo electrónico para [criminal@scammail.com](mailto:criminal@scammail.com) es Scam Mail Inc. El sitio web es [www.scammailinc.com](http://www.scammailinc.com). En dicho sitio web, averigua que Scam Mail Inc. tiene su oficina central y su único centro de datos en la Tierra Media. También averigua que Scam Mail Inc. solo conserva los datos durante un período de 7 días, tras el cual se procede a su eliminación.

Considera la posibilidad de utilizar las direcciones de correo electrónico para identificar a las personas que están detrás de DarkHacker.

También considera la posibilidad de obtener detalles de otras personas que han recibido un correo electrónico de [criminal@scammail.com](mailto:criminal@scammail.com) en los últimos siete días.

**Preguntas:**

* ¿Qué medidas iniciales debería tomar para asegurar que el proceso de investigación no se vea frustrado?
* ¿Qué tipo de información necesitaría para identificar a la persona que utiliza [criminal@scammail.com](mailto:criminal@scammail.com)? ¿Cómo puede obtener dicha información de Scam Mail Inc?
* ¿Cómo buscaría información en Scam Mail Inc sobre otras personas que han recibido un correo electrónico de [criminal@scammail.com](mailto:criminal@scammail.com) en los últimos siete días?

**Parte 3 - Otras formas de cooperación**

Tras realizar el pago mediante Bitcoin, recibe otro correo electrónico de fraud@hackmail.com con los datos de huella digital adjuntos.

Vuelve a considerar la posibilidad de utilizar la dirección de correo electrónico para identificar a los individuos que están detrás de DarkHacker. Su investigación inicial revela que Hack Mail Inc (con sede en Mordor) no tiene ninguna oficina o centro de datos en la Tierra Media, pero recientemente ha publicado anuncios sobre sus servicios gratuitos en el idioma de la Tierra Media. Hack Mail Inc almacena la información de los suscriptores en forma de datos informáticos.

Averigua que varias personas de Mordor se han quejado en diferentes foros en línea de incidentes de fraude supuestamente perpetrados por el usuario [fraud@hackmail.com](mailto:fraud@hackmail.com). Desea utilizar estas denuncias como prueba en un procedimiento posterior. Además, se pone en contacto con estas personas para pedirles información y ellas están dispuestas a consentir que acceda a sus cuentas y mensajes de correo electrónico.

**Preguntas:**

* ¿Qué tipo de información necesitaría para identificar a la persona que utiliza [fraud@hackmail.com](mailto:fraud@hackmail.com)?
* ¿Cuál es la medida más expeditiva para obtener dicha información de Hack Mail Inc?
* ¿Cuál es el modo más rápido de obtener los mensajes de correo electrónico que el usuario [fraud@hackmail.com](mailto:fraud@hackmail.com) ha enviado a sus víctimas de Mordor?

**Parte 4 – Asistencia judicial recíproca**

Tras analizar la información que ha recibido de Hack Mail Inc. y Scam Mail Inc., identifica a un individuo que forma parte del grupo DarkHacker: Boris Smith, un ciudadano de la Tierra Media.

Detiene a Boris Smith en la Tierra Media y este le revela la ubicación del sistema informático que DarkHacker está utilizando en Rohan. Como el hecho de que Boris haya sido detenido no es público, no parece haber ninguna razón para creer que los datos del sistema informático de DarkHacker sean vulnerables a pérdidas o modificaciones.

El señor Smith le informa de que la cuenta [fraud@hackmail.com](mailto:fraud@hackmail.com) se ha utilizado para contactar con otros agentes de DarkHacker. También le informa de una transacción a gran escala para la venta de códigos PIN de tarjetas de débito prevista para el día siguiente a las 17:00 horas utilizando la misma cuenta de correo electrónico.

* ¿Qué medidas puede tomar para asegurarse de que HackMail Inc. conserva los datos relativos a la cuenta [fraud@hackmail.com](mailto:fraud@hackmail.com)?
* ¿Qué medidas puede tomar para identificar a otros proveedores de servicios implicados en la transmisión de comunicaciones relacionadas con la estafa de DarkHacker?
* ¿Qué medidas puede tomar para obtener datos informáticos del sistema informático de DarkHacker?
* ¿Qué medidas puede tomar para averiguar la ubicación del cliente de DarkHacker que planea comprar códigos PIN de tarjetas de débito?