اتفاقية بودابست – دراسة حالة

الخلفية

**«ميدل أورث» (Middle Earth) دولة وهمية صغيرة نامية في أفريقيا، وهي مجاورة لدولتين أخريين هما «روهان» (Rohan) و «موردور» (Mordor). «ميدل أورث» دولة عضو في منظمة التجارة العالمية ومنظمة الأمم المتحدة، كما أنها دولة طرف في اتفاقية بودابست بشأن الجريمة الإلكترونية. ويعد البنك الوطني ل«ميدل أورث» (**MENB**) أكبر بنك في هذه الدولة ويتوفر على فروع في المنطقة ودوليا. "الميدل أورثية" هي اللغة الرسمية لهذه الدولة.**

**أنت موظف لدى سلطة لإنفاذ القانون في دولة "ميدل أورث" (**Middle Earth**)، أنت مسؤول عن التحقيق في الجرائم الإلكترونية في "ميدل أورث".**

الجزء 1 – القانون الموضوعي

تتلقى تقريرا من مصدر مجهول يفيد أن مجرمين على الفضاء الإلكتروني اخترقوا الخادوم الرئيسي للبنك الوطني ل"ميدل أورث" وأن هؤلاء المجرمين قاموا بتثبيت برمجية خبيثة تزيد من حجم مؤشر الفأرة والصورة الخلفية على جميع الكمبيوترات المرتبطة بالخادوم الرئيسي. ويقترح تحقيقك أن البرمجية الخبيثة تم إنشاؤها بواسطة مجموعة من القراصنة تدعى "DarkHacker" (القرصان الأسود).

وفي إطار تحقيقاتك، تحدد الموقع الإلكتروني الرسمي لـ"دارك هاكر" وهو [www.darkhacker.com](http://www.darkhacker.com). كما تلاحظ أن البرمجية المصممة أساسا لترجمة النصوص من اللغة الميدل أورثية إلى اللغة الإنجليزية معروضة للبيع على الموقع الإلكتروني، ولكن هذه البرمجية مسوقة أيضا على أنها تمكن من اختراق أجهزة الكمبيوتر.

فضلا عن ذلك، تكشف تحرياتك أن بيانات البصمات التي تمكن من النفاذ إلى الحواسيب والهواتف الذكية تباع أيضا على موقع [www.darkhacker.com](http://www.darkhacker.com). وفي محاولة لتحديد هوية الأفراد الذين يديرون "DarkHacker"، تطلق عملية سري وتقوم بشراء بيانات لبصمات الأصابع من موقع [www.darkhacker.com](http://www.darkhacker.com).

**الأسئلة:**

* ما هي الجريمة (الجرائم) الإلكترونية التي تم ارتكابها من خلال اختراق خادوم بنك "MENB" وتثبيت برمجية خبيثة عليه؟
* ما هي الجريمة (الجرائم) الإلكترونية التي يمكنك تحديدها على أنها ارتكبت من قبل "دارك هاكر" (DarkHacker)؟
* هل ارتكبت جريمة إلكترونية بشرائك لبيانات بصمات الأصابع من موقع قبل "دارك هاكر" (DarkHacker)؟

الجزء 2 – القانون الإجرائي

في إطار العملية السرية لشراء بيانات بصمات الأصابع من موقع "دارك هاكر"، يطلب منك إدخال عنوان البريد الإلكتروني الخاص بك لتلقي تعليمات الدفع. تتلقى بريدًا إلكترونيًا من حساب بريد إلكتروني [criminal@scammail.com](mailto:criminal@scammail.com) مع تعليمات للدفع باستخدام عملة بيتكوين.

يكشف تحقيقك الأولي أن مزود خدمة البريد الإلكتروني لعنوان البريد الإلكتروني [criminal@scammail.com](mailto:criminal@scammail.com) هو شركة "Scam Mail Inc" وتحدد موقعها الإلكتروني وهو [www.scammailinc.com](http://www.scammailinc.com). ومن خلال هذا الموقع، تعرف أن المقر الرئيسي للشركة ومركز بياناتها الوحيد يوجدان في "ميدل أورث". بالإضافة إلى ذلك، تعلم أن شركة " Scam Mail Inc." تحتفظ بالبيانات فقط لمدة 7 أيام، ويتم بعدها حذف جميع البيانات.

تفكر في استخدام عناوين البريد الإلكتروني لتحديد الأشخاص الذين يختفون وراء "دارك هاكر" (DarkHacker).

تحصل على معلومات عن أشخاص آخرين تم الاتصال بهم من خلال حساب البريد الإلكتروني [criminal@scammail.com](mailto:criminal@scammail.com)خلال الأيام السبعة الأخيرة.

**الأسئلة:**

* ما هي التدابير الأولية التي يجب اتخاذها لضمان عدم إبطال عملية التحقيق؟
* ما نوع المعلومات التي تحتاج إليها لتحديد هوية الشخص الذي يستخدم حساب البريد الإلكتروني [criminal@scammail.com](mailto:criminal@scammail.com)؟ كيف يمكنك الحصول على هذه المعلومات من شركة "Scam Mail Inc"؟
* كيف يمكنك الحصول على معلومات من شركة "Scam Mail Inc" عن أشخاص آخرين تم الاتصال بهم عبر criminal@scammail.com خلال الأيام السبعة الأخيرة؟

**الجزء الثالث – أشكال أخرى للتعاون**

بعد الدفع عبر استخدام عملة البيتكوين، تتلقى بريدا إلكترونيا آخر من حساب البريد الإلكتروني [fraud@hackmail.com](mailto:fraud@hackmail.com) مع مرفق ببيانات بصمات الأصابع.

تفكر مرة أخرى في استخدام عنوان البريد الإلكتروني لتحديد الأشخاص الذين يختفون وراء "دارك هاكر" (DarkHacker). ويكشف التحقيق الأولي أن شركة "Hack Mail Inc" (التي يوجد مقرها الرئيسي في موردور) لا تملك أي مكتب أو مراكز بيانات في "ميدل أورث"، لكنها نشرت مؤخرًا إعلانات بشأن خدماتها المجانية باللغة الميدل أورثية. وتخزن شركة "Hack Mail Inc" معلومات عن المشتركين في شكل بيانات كمبيوتر.

من جهة أخرى، تعلم أن عدة أشخاص في موردور اشتكوا على منتديات مختلفة من حوادث الاحتيال المزعوم ارتكابها من قِبل مستخدم حساب البريد الإلكتروني [fraud@hackmail.com](mailto:fraud@hackmail.com). ترغب في استخدام هذه الشكاوى كدليل في إجراءات لاحقة. بالإضافة إلى ذلك، تقوم بالاتصال بهؤلاء الأشخاص للحصول على معلومات وعبر هؤلاء الأشخاص عن استعدادهم على الموافقة لمنحك إمكانية النفاذ إلى حسابات البريد الإلكتروني ورسائل البريد الإلكتروني الخاصة بهم.

**الأسئلة:**

* ما نوع المعلومات التي ستحتاج إليها لتحديد هوية الشخص الذي يستخدم [fraud@hackmail.com؟](mailto:fraud@hackmail.com؟)
* ما هو أسرع إجراء للحصول على هذه المعلومات من شركة " Hack Mail Inc"؟
* ما هي الطريقة الأسرع للحصول على رسائل البريد الإلكتروني المرسلة من قبل مستخدم [fraud@hackmail.com](mailto:fraud@hackmail.com) إلى الضحايا في موردور؟

**الجزء الرابع – المساعدة القانونية المتبادلة**

في أعقاب تحليل المعلومات التي تلقيتها من شركتي Hack Mail Inc و Scam Mail Inc، نجحت في تحديد شخص واحد في مجموعة دارك هاكر، واسمه: بوريس سميث، وهو من مواطني "ميدل أورث".

تقوم باعتقال بوريس سميث في "ميدل أورث" ويفصح عن موقع نظام الكمبيوتر المستخدم من قبل "DarkHacker" في روهان. ونظرا لأن اعتقال بوريس لم يتم بشكل علني، يبدو أنه ليس هناك ما يدعو للاعتقاد بأن البيانات معرضة للضياع أو التعديل.

يخبرك سميث أن الحساب [fraud@hackmail.comاستُخدم](mailto:fraud@hackmail.comاستُخدم) للاتصال بعملاء آخرين في منتدى "DarkHacker". كما يخبرك بمعاملة واسعة النطاق لبيع رموز رقم التعريف الشخصي (PIN) لبطاقات ائتمان من المزمع تنفيذها في اليوم التالي على الساعة 17:00 باستخدام حساب البريد الإلكتروني نفسه.

**الأسئلة:**

* ما هي الإجراءات التي يمكنك اتخاذها لضمان أن شركة " Hack Mail Inc" تحفظ البيانات المتعلقة بحساب [fraud@hackmail.com](mailto:fraud@hackmail.com) ؟
* ما هي التدابير التي ينبغي أن تتخذها لتحديد هوية مزودي الخدمات الآخرين المشاركين في إرسال المراسلات ذات الصلة باحتيال "DarkHacker"؟
* ما هي التدابير التي يمكنك اتخاذها للحصول على بيانات الكمبيوتر من نظام كمبيوتر دارك هاكر "DarkHacker"؟
* ما هي التدابير التي يمكنك اتخاذها للتأكد من موقع زبون دارك هاكر "DarkHacker" الذي يخطط لشراء رموز رقم التعريف الشخصي لبطاقات الائتمان؟