اتفاقية بودابست – دراسة حالة

الخلفية

**أنت موظف لدى سلطة لإنفاذ القانون في دولة "ميدل أورث" (**Middle Earth**)، وهو بلد وهمي صغير يجاور بلدين آخرين هما روهان وموردور. أنت مسؤول عن التحقيق في الجرائم الإلكترونية في "ميدل أورث".**

الجزء 1 – القانون الموضوعي

تتلقى تقريرا معلوماتيا يفيد أن محركات أقراص البيانات لأنظمة الكمبيوتر التابعة لمؤسسة مالية مشهورة قد تم اختراقها من قبل مجرمي الفضاء الإلكتروني غير معروفين وأنه قد تم تثبيت برمجية خبيثة تزيد من حجم مؤشر الفأرة على تلك الأنظمة. ويقترح تحقيقك أن البرمجية الخبيثة قد تم إنشاؤها بواسطة منتدى للقرصنة يدعى "DarkHacker" (القرصان الأسود).

وتكشف التحريات الموسعة أن برمجية الترجمة المصممة في المقام الأول للقرصنة في أجهزة الكمبيوتر تباع أيضًا من قِبل "DarkHacker" تحت شعار "اشتر برمجيتنا للترجمة وادعو أصدقاءك لتثبيتها – يمكنك النفاذ إلى أجهزة الكمبيوتر الخاصة بهم بدون حق!"

في محاولة لتحديد هوية الأفراد الذين يديرون "DarkHacker"، تنجح، في إطار عملية سرية، في الحصول على رموز النفاذ التي تمكن من الولوج إلى أنظمة الكمبيوتر.

**الأسئلة:**

* ما هي الجريمة (الجرائم) الإلكترونية التي تم ارتكابها بتثبيت البرمجية الخبيثة على أنظمة الكمبيوتر للمؤسسة المالية المشهورة؟
* ما هي الجريمة (الجرائم) الإلكترونية التي يمكنك تحديدها على أنها ارتكبت من قبل أشخاص على "DarkHacker"؟
* هل ارتكبت جريمة إلكترونية بحصولك على رموز النفاذ إلى أنظمة الكمبيوتر التابعة لـ"DarkHacker"؟

الجزء 2 – القانون الإجرائي

في إطار العملية السرية، تحصل على رموز النفاذ ومعلومات عن الدفع من وكيل "DarkHacker". تتلقى بريدًا إلكترونيًا من حساب بريد إلكتروني مدفوع [criminal@scammail.com](mailto:criminal@scammail.com) مع رابط التنزيل إلى رموز النفاذ.

يكشف تحقيقك الأولي أن مزود خدمة البريد الإلكتروني لعنوان البريد الإلكتروني [criminal@scammail.com](mailto:criminal@scammail.com) هو شركة "Scam Mail Inc"، التي يقع مقرها الرئيسي ومركز بياناتها الوحيد في "ميدل أورث".

تستخلص من الموقع الإلكتروني لشركة " Scam Mail Inc." أن الشركة تحتفظ بالبيانات فقط لمدة 7 أيام، ويتم بعدها حذف جميع البيانات.

تفكر في استخدام عناوين البريد الإلكتروني لتحديد وكيل "DarkHacker".

تشير المعلومات التي حصلت عليها أن حجم العمليات أكبر بكثير مما كان متوقعًا في البداية. تعتقد أنه من الضروري الآن الحصول على معلومات عن أشخاص مجهولين 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**

عند النقر على الرابط لتنزيل رمز النفاذ، تتلقى بريدا إلكترونيا آخر من حساب البريد الإلكتروني المجاني [fraud@hackmail.com](mailto:fraud@hackmail.com) مع معلومات البنك.

تفكر مرة أخرى في استخدام عنوان البريد الإلكتروني لتحديد وكيل " DarkHacker". يكشف 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 في "ميدل أورث" باللغة المحلية.

تخزن شركة "Hack Mail Inc" معلومات عن المشتركين في شكل بيانات الكمبيوتر.

فضلا عن ذلك، تعلم بشكل منفصل أن عدة أشخاص في موردور اشتكوا على منتديات عامة 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 وعبروا 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 الشخص الذي يستخدم [fraud@hackmail.com](mailto:fraud@hackmail.com) إلى مقدمي الشكاوى؟

**الجزء الرابع – المساعدة القانونية المتبادلة**

كنتيجة لتحليل البيانات التي تم الحصول عليها، نجحت في تحديد شخص واحد مسؤول عن بيع البيانات وتقديم الخدمات، 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 بوكلاء آخرين في منتدى "DarkHacker". كما يخبرك بمعاملة واسعة النطاق لبيع رموز رقم التعريف الشخصي (PIN) البنكي 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 الكمبيوتر "DarkHacker"؟
* ما هي التدابير التي يمكنك اتخاذها للتأكد من موقع زبون "DarkHacker" الذي يخطط لشراء رموز رقم التعريف الشخصي البنكية؟