Budapest Convention – Case Study

Background

Middle Earth is a small fictious developing country in Africa and a neighbor of two other countries, Rohan and Mordor. It is a member of the WTO, the UN and is a party to the Budapest Convention on Cybercrime. Middle Earth has traditionally been a centre of a thriving banking and finance industry. Its largest bank Middle Earth National Bank ("MENB") has several branches in the region and internationally. Middle Earthean is the official language of Middle Earth.

You are a law enforcement official of Middle Earth and are responsible for investigating cybercrimes in Middle Earth.

Part 1 - Substantive Law

You receive an anonymous report that cybercriminals have hacked into the main server of MENB. The cybercriminals have installed malware which randomly changes the size of the mouse cursor and the background wallpaper of all computers connected with the main server. Your investigation suggests that the malware was created by a group of hackers known as "DarkHacker".

As part of your investigation, you identify the official website of DarkHacker as www.darkhacker.com. You observe that software ostensibly designed for translating text Middle Earthean language to English is being sold on the website, but the software is marketed as also enabling hacking into computers..

Your investigation also reveals that fingerprint data that enables access to laptops and smartphones is being sold on www.darkhacker.com. In an attempt to identify the individuals operating DarkHacker, you conduct an undercover operation and purchase fingerprint data from www.darkhacker.com.

Questions:

- What cybercrime(s) was committed by hacking into and installing malware on the MENB server?
- What cybercrime(s) can you identify as being committed by DarkHacker?
- Did you commit a cybercrime offence by purchasing fingerprint data from DarkHacker?

Part 2 – Procedural Law

As part of the undercover operation to purchase fingerprint data from DarkHacker, you are prompted to enter your email address to receive payment instructions. You receive an email from an email account criminal@scammail.com with instructions on how to make the payment using Bitcoin.

Your initial investigation reveals that the email service provider for criminal@scammail.com is Scam Mail Inc. You identify its website as www.scammailinc.com. You learn from its website

Scam Mail Inc has its head office and only data center in Middle Earth. You also learn that Scam Mail Inc. only retains data for a period of 7 days after which all data is deleted.

You consider using the email addresses to identify the individuals behind DarkHacker.

You also consider obtaining details of other people contacted through the email account criminal@scammail.com in the last seven days.

Questions:

- What initial measures should you take to ensure that the investigation process is not frustrated?
- What kind of information would you need to identify the person using criminal@scammail.com? How can you obtain such information from Scam Mail Inc?
- How would you seek information from Scam Mail Inc regarding other persons contacted by criminal@scammail.com in the last seven days?

Part 3 – Other Forms of Cooperation

Upon making the payment through Bitcoin, you receive another email from an email account fraud@hackmail.com with the fingerprint data attached.

You again consider using the email address to identify the individuals behind DarkHacker. Your initial investigation reveals that Hack Mail Inc (headquarters in Mordor) does not have any office or data centers in Middle Earth but recently published advertisements regarding its free services in Middle Earthean language. Hack Mail Inc stores subscriber information in the form of computer data.

You learn of several persons in Mordor who have complained on different online forums of incidents of fraud allegedly perpetrated by the user of fraud@hackmail.com. You wish to use these complaints as evidence in subsequent proceedings. Moreover, you contact these persons for information and they are willing to consent to you accessing their email accounts and email messages.

Questions:

- What kind of information would you need to identify the person using fraud@hackmail.com?
- What is the most expeditious measure to obtain such information from Hack Mail Inc?
- What is the most expeditious way to obtain emails sent by user of fraud@hackmail.com to victims in Mordor?

Part 4 – Mutual Legal Assistance

Upon analysis of the information you received from Hack Mail Inc. and Scam Mail Inc., you identify one individual part of the DarkHacker group: Boris Smith, a Middle Earth national.

You arrest Boris Smith in Middle Earth and he discloses the location of the computer system being used by DarkHacker in Rohan. As the fact that Boris has been arrested is not public, there appears to be no reason to believe that the data in the DarkHacker computer system is vulnerable to loss or modification.

Smith informs you that the account fraud@hackmail.com was used to contact other DarkHacker agents. He also informs you of large scale transaction for the sale of Debit Card PIN codes planned to be undertaken the following day at 17:00 using the same email account.

- What measures can you take to ensure HackMail Inc. preserves data relating to the account fraud@hackmail.com?
- What measures should you take to identify other service providers involved transmitting communications related to the DarkHacker scam?
- What measures can you take to obtain computer data from the DarkHacker computer system?
- What measures can you take to ascertain the location of the DarkHacker customer who is planning to purchase Debit Card PIN codes?

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 ل"دارك هاكر" وهو 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. وفي محاولة لتحديد هوية الأفراد الذين يديرون "DarkHacker"، تطلق عملية سري وتقوم بشراء بيانات لبصمات الأصابع من موقع 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 مع تعليمات للدفع باستخدام عملة بيتكوين.

يكشف تحقيقك الأولي أن مزود خدمة البريد الإلكتروني لعنوان البريد الإلكتروني criminal@scammail.com هو شركة "Scam Mail Inc" وتحدد موقعها الإلكتروني وهو 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 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 ؟ 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 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. 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؟
- 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 إلى الضحايا في موردور؟

الجزء الرابع – المساعدة القانونية المتبادلة

في أعقاب تحليل المعلومات التي تلقيتها من شركتي Hack Mail Inc وScam 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.com استُخدم 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 ؟
- 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؟