THE JOURNALIST SURVIVAL GUIDE

ANANIMATEDVIDEOGUIDE

Samir Kassir eyes

الدرس ٨

كيف تحمي الكمبيوتر من القرصنة والبرمجيات الخبيثة

كيف تنعم باتّصال آمن

أهمية الاتصال الآمن

صحيحٌ أنّ تنزيل نظام التشغيل على جهاز الكمبيوتر الخاص بك خطوةٌ أولى وأساسية، لكنّ التأكّد من أنّ الاتصالات التي تجريها عبر جهازك تنتقل على نحو آمن أمرٌ لا يقلّ عنه أهميّةً. من هنا، سيبحث هذا الدرس في أساليب التحقّق من الاتصال الآمن عبر برنامج التصفّح، فضلاً عن كيفية استخدام تقنية اتّصال أكثر أماناً بالإنترنت، عن طريق خادم «بروكسي» يمكّن مستخدميه من الاتصال بدون الكشف عن هويّتهم، يُعرف باسم «تور».

بروتوكول نقل النصّ التشعبي الآمن (HTTPS)

ما هو بروتوكول نقل النصّ التشعبي الآمن؟

عندما تتّصل بموقع إلكتروني معيّن، فإنّك تجري هذا الاتصال عبر بروتوكول نقل النصّ التشعبي (HTTP)، وهو البروتوكول الذي تعتمده برامج التصفّح التي تسمح بإجراء هذا النوع من الاتصالات عادةً.

بعد ذلك، تُنقل المعلومات التي قمت بإرسالها ضمن نصّ عاديّ، كمن يرسل بطاقة بريدية تتضمّن معلومات شخصية مكشوفة على العلن. فيسهل على الأطراف الثالثة حينذاك قراءة البيانات التي يتمّ إرسالها وتلقيها عبر المواقع الإلكترونية، على غرار اسم المستخدم وكلمة السرّ.

لحلّ هذه المشكلة، تمّ ابتكار بروتوكول نقل النصّ التشعبي الآمن، وهدفه تأمين الاتصال المشفّر وتحديد خادم آمن لشبكة الإنترنت. من شأن هذا أن يغيّر طريقة اتّصالك، لكأنّك انتقلت من إرسال المعلومات عبر بطاقة بريدية إلى تدوينها ضمن رسالة في مغلّف مختوم.

ولا يخفى على أحد أنه من الممكن الاتصال على نحو آمن بمعظم المواقع الإلكترونية المهمّة، مثل «جيمايل»، إضافةً إلى برامج التواصل الاجتماعي التي تلاقي إقبالاً من الجمهور، على غرار «فايسبوك» و«تويتر». لكنّ هذا الاتصال الآمن لا يتوفّر، بالضرورة، بشكل تلقائي. لتشغيل بروتوكول HTTPS (أو طبقة المنفذ الآمن SSL، وهي طريقة أخرى لإجراء الاتصال الآمن تلقائياً)، يمكنك العودة إلى الإعدادات في البرامج المذكورة أعلاه. لكن، لتسهيل هذه العملية، يمكن إضافة ملحق «بروتوكول نقل النصّ التشعبي الآمن أينما كان» (HTTPS Everywhere) إلى متصفّح «فايرفوركس» أو «كروم» الذي سيقوم بالاسترداد التلقائي للمواقع الإلكترونية التي تزورها، بنسخة بروتوكول HTTPS، مثل فايسبوك وتويتر وغيرهما.

لكن تجدر الإشارة إلى أنّ هذا الملحق لن يتيح لك الاتصال بجميع المواقع الإلكترونية عبر بروتوكول HTTPS، بل بالمواقع التي تجيز إعداداتها استعمال كلا البروتوكولين (HTTP و HTTPS) فقط. لذا، من الضروري مراجعة شريط العناوين الإلكترونية في أعلى المتصفّح، للتأكّد من أنّ المواقع الإلكترونية حيث يجب أن تدرج معلومات هامّة (كعنوان البريد الإلكتروني، كلمة السرّ، معلومات عن بطاقة الائتمان إلخ.) مدعومة ببروتوكول HTTPS.

الشهادات

ما هي الشهادة؟

يمكن اعتبار الشهادة بمثابة بطاقة التعريف بموقع إلكتروني، كما إنها تضمن توافر معايير الأمن عند الاتصال عبر بروتوكول HTTPS. في بعض الأحيان، سيظهر لك متصفّح الويب رسالة إنذار تبيّن وجود مشكلة بالشهادة الرقمية الخاصة بالموقع. تهدف هذه الإنذارات إلى حمايتك من أيّة هجمات عبر الإنترنت؛ لذا نرجوك عدم تجاهلها. فإذا تجاهلت هذه الإنذارات أو تجاوزتها فعلاً، ستظلّ قادراً على زيارة الموقع الإلكتروني، لكنّ قدرة بروتوكول HTTPS على حماية اتّصالاتك ستغدو محدودة. في تلك الحالة، لن تكون زيارتك إلى الموقع أكثر أماناً من أيّ اتصال عادي تجريه عبر بروتوكول HTTP.

إذا وصلك إنذارٌ من هذا النوع، ينبغي أن تبادر إلى إبلاغ مسؤول الموقع الذي كنتَ تحاول زيارته، عن طريق رسالة إلكترونية، لتشجيعه على حلّ المشكلة.

إذا كنتَ تزور موقع HTTPS من إعداد شخص ما، كبعض أنواع خوادم «بروكسي الويب»، فقد تتلقّى إشعاراً بوجود خطأ ما. ومردّ ذلك إلى أنّ الشهادة «موقّعة ذاتياً»، مما يعني أنّ متصفّحك لا يستطيع الاستناد إلى أساس متين ليحدّد إنّ كان اتّصالك يتعرّض للعرقلة. في مثل هذه الحالات، لعلّك لن تملك خياراً آخر إلا قبول الشهادة الموقّعة ذاتياً، لا سيّما إذا كنتَ تريد زيارة الموقع المعنيّ فعلاً. لكن حاول التأكّد

عبر قناة أخرى، مثل البريد الإلكتروني أو التراسل الفوري، أنّ الشهادة هي تلك التي كنت تتوقّعها بعينها، أو تحقّق إن كانت هي نفسها عند استخدام وسيلة أخرى للاتصال بالإنترنت من جهاز كمبيوتر مختلف.
أما إذا تلقّيتَ إنذاراً بوجود خطأ عند استخدام بريد إلكتروني عادي، مثل «جيمايل» أو «فايسبوك»، فإياك والمضيّ قدماً!

التحايل

ما هو التحايل؟

التحايل هو طريقة للالتفاف على أيّ مصفيات يفرضها عليك مزوّد خدمة الإنترنت (ISP). يرتبط هذا الأمر بوجود خادم «بروكسي» واحد أو أكثر، مهمّته توجيه اتّصالك بالإنترنت عبر قناة خارجة عن سيطرة مزوّد خدمة الإنترنت، لتصلك بالموقع الإلكتروني الذي تريد زيارته.

أنواع أدوات التحايل

بروكسي الويب

«البروكسي» القائم على الويب هو خدمة تُدخل فيها الموقع الإلكتروني لبرنامج «بروكسي» معيّن تودّ استعماله ضمن شريط العناوين الإلكترونية، في أعلى المتصفّح، ومن ثم تُدخل، ضمن الموقع الإلكتروني، العنوان المصفّى الذي تريد زيارته. فيقوم «البروكسي» عندئذ بعرض المحتوى المطلوب ضمن صفحة إلكترونية خاصة به.

مع أنّ هذه الأنواع من خدمات «البروكسي» هي الأسهل استعمالاً، إلا أنها لا تنطبق إلا على نشاطاتك التي تستخدم فيها جهاز المتصفّح، وبالتالي فهي لا تجدي نفعاً مع زبائن الدردشة أو البريد الإلكتروني (عبر برامج «آوتلوك» أو «سكايب» أو غيرها). زد على ذلك أنّ برامج «البروكسي القائمة على الويب» لا تعتمد جميعها الاتّصال عبر بروتوكول HTTPS لتوجيه حركة الإنترنت الخاصة بك.
لكن لا بدّ من الإشارة إلى ضرورة عدم الوثوق بجميع برامج «البروكسي القائمة على الويب». ففي بعض الحالات، قد تعمد المجموعات التي ترغب في الاطلاع على معلومات خاصة بحسابات المستخدمين إلى إنشاء برامج «بروكسي قائمة على الويب»، مما يخوّلها معرفة كلّ النشاطات التي تقوم بها عبر الإنترنت. لذا، من الضروري أن تستخدم برامج وضعتها الشركات التي يمكن أن تثق بها.

الشبكات الخاصة الافتراضية (VPNs)

تستخدم الشبكة الخاصة الافتراضية خدمة الاتصال عبر بروتوكول HTTPS ، وهي تحمي كلّ حركة المرور التي تسيّرها بينك وبين جهاز كمبيوتر آخر داخل غطاء حماية. ولما كانت خدمات الشبكة الخاصة الافتراضية تحمي كلّ أنواع حركة الإنترنت، فيجوز استخدامها لحماية بيانات البريد الإلكتروني، والتراسل الفوري، وبرامج «بروتوكول الإنترنت الخاص بالتعليقات الصوتية» (VoIP) مثل «سكايب»، فضلاً عن أيّ خدمة إنترنت أخرى، ناهيك عن التصفّح عبر الإنترنت، جاعلةً من كلّ المعلومات التي تمرّ عبر غطاء الحماية غير مقروءة بالنسبة لأي شخص يمكن أن يصادفها.

إذا تكشّف غطاء الحماية هذا خارج المنطقة التي تكون فيها حركة الإنترنت مقيّدة، فمن الممكن أن يشكّل ذلك وسيلة تحايل فعّالة، بما أنّ الخادم/الكيان الذي يقوم بتصفية البيانات لن يلحظ إلا البيانات المشفّرة، وبالتالي لن يتمكّن من معرفة ما هي البيانات التي تمرّ تحت غطاء الحماية. وعلى غرار برنامج «البروكسي القائم على الويب»، من الضروري أن تثق بالجهة التي تزوّدك بالشبكة الخاصة الافتراضية. فبينما تتوفّر بعض الحلول المجانية مثل «بسيفون ٣» (Psiphon ٣) أو التجارية عبر «خدمة آمازون للإنترنت» (Amazon Web Services) وغيرها من مزوّدي خدمات الحوسبة السحابية، لا يخفى عليك أنّ هذه الخدمات ستتمكّن من رؤية المواقع الإلكترونية التي تزورها، حتى وإن كان مزوّد خدمة الإنترنت العاديّ لا يستطيع ذلك.

البروكسي السريّ

لعلّ أكثر أنواع «البروكسي» أماناً هو البروكسي السريّ الذي يحجب هوية متصفّح شبكة الإنترنت. وهو يوجّه الاتصال الذي تجريه بالإنترنت عبر سلسلة من ٣ خوادم «بروكسي» أو أكثر. ولعلّ أفضل هذه البرامج هو برنامج «تور».

يوجّه برنامج «تور»، عشوائياً، كلّ الاتصالات التي تجريها عبر شبكة من خوادم «البروكسي» المستقلة والمتطوّعة. فتكون كلّ حركة الإنترنت بين خوادم «تور» (أو الأجهزة المرحّلة) مشفّرة، كما يكون كلّ من هذه الأجهزة على علم فقط بعنوان بروتوكول الإنترنت (الآي. بي) للجهازين الآخرين- أي الجهاز الذي يسبقه مباشرة وذاك الذي يليه مباشرةً على طول السلسلة.
بفضل «تور»، يصبح من الصعب أن:

- يعرف مزوّد خدمة الإنترنت، أو أيّ مراقب محلي آخر، ما هو الموقع الإلكتروني الذي تريد زيارته أو ما هي المعلومات التي تقوم بإرسالها
- يعرف الموقعُ الإلكتروني الذي تريد زيارته من تكون (أو على الأقل يعرف عنوان بروتوكول الإنترنت الخاص بك)
- يعرف أيٌّ من الأجهزة المرحّلة المستقلة من تكون، أو أيّ موقع تريد زيارته، إما عن طريق تسجيل عنوان بروتوكول الإنترنت الخاص بك مباشرة وإما من خلال ربط عاداتك بتصفّح الإنترنت عبر مراقبة حركة استعمالك للإنترنت بشكل منتظم.

للمزيد من المعلومات حول كيفية تنزيل «تور» واستخدامه، يُرجى زيارة الموقع الإلكتروني التالي:
https://securityinabox.org/en/tor_main

إنتاج:
مركز الدفاع عن الحريات الإعلامية والثقافية «سكايز» – مؤسسة سمير قصير

تم إعداد محتوى الفيديو بمساعدة من:
فريق تكنولوجيا المعلومات والاتصالات في المعهد الديمقراطي الوطني للشؤون الدولية

المنتج التنفيذي: **مارون صفير**
تصميم وتحريك: **kook creative studio**

مستشار تقني: **أندرو كود**
ترجمة: **نور الأسعد**
صوت (عربي): **ريما خداج**
الصوت (انجليزي): **أندرو كود**
تسجيل الصوت: **Creative Impact**
موسيقى: **«Mining by Moonlight» by Kevin MacLeod**

تم تنفيذ هذا المشروع بفضل دعم **الصندوق الوطني للديمقراطية.**