كيف التدوين مع الحفاظ على المجهولية؟

وضعت هذا الدليل التقني من وجهة نظر موظف يسعى إلى استقاء معلومات حول فضيحة شهد عليها في بلد يتسم فيه المس بهذا النوع من المشاكل بالخطورة. فلا تتوجه هذه النصائح إلى المتفوّقين في التشفير، وإنما إلى الأفراد الذين يقلقون بشأن أمنهم، ويرغبون في حماية حياتهم الخاصة في بلدان لا تحترم حرية التعبير. وتؤمن المقالة التي وضعتها المؤسسة الأمريكية المعنية بالدفاع عن الحريات الإلكترونية إلكترونيك فرونتيير فاوندايشن Electronic Frontier Foundation's (EFF) تحت عنوان "كيف التدوين بأمان؟" (http://www.eff.org/Privacy/Anonymity/blog-anonymously.php)، معلومات عملية إضافية عن هذا الموضوع.

الفهرس

عرض ساره
المرحلة الأولى : الأسماء المستعارة
المرحلة الثانية : أجهزة الكمبيوتر العامة
المرحلة الثالثة : المحوّلات
المرحلة الرابعة : المحوّلات في المرحلة الثانية. والآن، بات الأمر في غاية السرّية!
المرحلة الخامسة : توجيه أونيون onion routing بفضل نظام تور Tor
المرحلة السادسة : ميكسماستر Mixmaster وإنفيزيبلوغ Invisiblog و جي بي جي GPG
ما الذي يمكن كشفه؟ وما هي الحدود؟

عرض ساره

ساره محاسبة في إحدى الوزارات أدركت في أحد الأيام أن رئيسها الوزير يختلس أموالاً طائلة. لذا قررت أن تشهر هذا الجرم إلا أنها خشيت من أن تفقد عملها. فلا بدّ من أن تعرّض نفسها للتسريح إذا تحدثت إلى الوزير، مهما كانت الفرصة ضئيلة لتحصل على موعد منه. ونظراً إلى هذا الخطر الذي يحدق بها، ما كان منها إلا أن اتصلت بصحافي يعمل في صحيفة محلية ولكنه رفض مساعدتها لأنها لا تملك معلومات كافية ووثائق تثبت أقوالها.

قررت ساره إعداد مدوّنة لتكشف للعالم أجمعين ما يحصل في الوزارة. ولتحمي نفسها، أرادت التأكد من أنه ما من أحد يستطيع كشف هويتها. لذا، يفترض بها أن تبتكر مدوّنة تحافظ على المجهولية علماً بأنه يمكن اكتشاف هوية المدوّن بأسلوبين : من جهة، يستطيع المدوّن أن يكشف بنفسه عن هويته في محتوى المنشور. وعلى سبيل المثال، إذا قالت ساره: "أنا مساعدة رئيس المحاسبة في وزارة المناجم"، سيدرك قارئ المدوّنة فوراً هويتها. ومن جهة أخرى، يمكن استغلال المعلومات التي يقدّمها المتصفّح أو برامج البريد الإلكتروني. فيملك كل جهاز كمبيوتر يرتبط بالإنترنت أو يتشارك عنواناً شبكياً يتألف من سلسلة من أربعة أرقام بين 0 و255 تفصل نقاط ما بينها. مثلاً، 213.24.124.38. . وعندما تستخدم ساره وسيلة التصفّح لتسجل ملاحظة على مدوّنة الوزارة، يظهر عنوانها الشبكي في الرسالة.
ليس على مهندسي أجهزة الكمبيوتر إلا أن يبحثوا قليلاً ليكتشفوا هوية ساره بفضل العنوان الشبكي. أما إن اتصلت ساره بالإنترنت من جهازها، فيستطيع مزوّد خدمة الإنترنت أن يربط ما بين العنوان الشبكي المستخدم لعرض الرسائل ورقم هاتف ساره. وفي بعض البلدان، يضطر الوزير إلى طلب أمر قضائي ليحصل على هذه المعلومات في حين أنه لن يصعب عليه القيام بذلك في بلدان أخرى ولا سيما تلك التي تملك فيها الدولة مزوّدي الإنترنت.

تستطيع ساره اللجوء إلى عدة أساليب لتخفي هويتها على الإنترنت. وبشكل عام، ترتبط درجة الحماية بالجهد الذي هي مستعدة لتأمينه في سبيل أن تخفيه. وعلى كل الأفراد الذين يرغبون في استحداث مدوّنة بطريقة مجهولة، أن يقرروا إلى أي حد هم مستعدون لحماية هويتهم لأن بعض الأساليب تتطلب معلومات تقنية معمّقة وعملاً مضنياً.

المرحلة الأولى : الأسماء المستعارة

يتمثل أبسط السبل لتخفي ساره هويتها باستخدام حساب بريدي ومدوّنة مجانيين مؤسسين في الخارج (لا يشكل الحساب المدفوع للبريد الإلكتروني أو المدوّنة فكرة سديدة، لأن الدفع يسمح بالوصول إلى بطاقة ائتمان أو حساب جارٍ فيسهل اقتفاء أثر المدوّن). وتستطيع ساره انتحال صفة أخرى عبر ابتكار اسم مستعار تستخدمه في هذه الحسابات. وعندما تكتشف الوزارة مدوّنتها، تدرك أنه يعود إلى "مجهول" يتمثل عنوان بريده الإلكتروني بما يلي: « anonyme.blogger@hotmail.com ».

من بين مزوّدي حسابات البريد الإلكتروني المجانية:
هوتمايل Hotmail

ياهو Yahoo

هاشمايل Hushmail: هو بريد إلكتروني مجاني يؤمن حل تشفير

بعض أدوات التدوين:

بلوغسوم Blogsome: هو أداة مجانية للتدوين من وارلدبرس WorldPress

بلوغر Blogger

سيو بلوغ Seo Blog

لكن هذه الاستراتيجية تطرح مشكلة : عندما تستحدث ساره حساباً بريدياً أو مدوّنة، يسجل المزوّد الذي تستخدمه عنوانها الشبكي. إلا أنه في حال كان هذا العنوان يرتبط بمنزلها أو مكتبها، وفي حال كانت المؤسسة التي تتولى إدارة خدمة البريد الإلكتروني أو المدوّنة مجبرة على إفشاء معلوماتها، تستطيع الوزارة كشف هويتها، علماً بأنه ليس من السهل إجبار مزوّدي خدمات الويب على تقديم هذا النوع من المعلومات. فعلى سبيل المثال، لتدرك الوزارة أن ساره وقّعت عقداً مع هوتمايل Hotmail، ستضطر حتماً إلى اللجوء إلى حكم قضائي بالتعاون مع الوكالة الأمريكية لتطبيق القوانين. ولكن ساره لا تريد المجازفة في هذا الموضوع.

المرحلة الثانية : أجهزة الكمبيوتر العامة

تستطيع ساره أن تلجأ إلى أسلوب آخر لتخفي هويتها يتمثل باستخدام أجهزة كمبيوتر في مقهى إلكتروني أو مكتبة عامة يستعملها عدد كبير من الأفراد. إلا أن هذه الاستراتيجية لا تخلو من الشوائب. ففي حال تمكّن العاملون في المقهى الإلكتروني أو مختبر المعلوماتية الجامعي من ملاحظة هوية المستخدم وتحديد الساعة التي استخدم جهاز الكمبيوتر في خلالها، قد تكشف هوية ساره. ويجدر بها ألا ترسل الرسائل في منتصف الليل، عندما تكون وحدها في مختبر المعلوماتية لأن الحارس الليلي سيتذكّرها حتماً، كما يفترض بها أن تغيّر المقهى الإلكتروني باستمرار. فإذا اكتشفت الوزارة أن الرسائل تصدر دائماً من مقهى "شي جوجو" الواقع على الطريق العام، لا بدّ من أن ترسل أحداً للتحقق من هوية المرسل.

المرحلة الثالثة : المحوّلات المجهولة

ملّت ساره التوجه إلى "شي جوجو" كلما رغبت في تحديث مدوّنتها. وبمساعدة جارٍ لها، وضعت نظاماً يسمح لها بولوج الويب عبر جهاز الكمبيوتر الخاص بها باستخدام محوّل مجهول. ومنذ ذلك الحين، بات عنوان المحوّل الشبكي، وليس عنوان جهاز الكمبيوتر الشخصي، يظهر حين تستخدم بريدها الإلكتروني أو

مدوّنتها فيصعب على الوزارة اكتشافها.

في بادئ الأمر، تحصل على لائحة بالمحوّلات على الإنترنت عبر البحث عن "خادم محوّل" على غوغل Google. فتختار مثلاً محوّلاً من لائحة publicproxer.com مفضّلةً المحوّل الذي يحمل إشارة "مجهولية عالية" "High anonymity". ثم تدوّن عنوان المحوّل الشبكي ومحطته. (الرجاء مراجعة المقالة "ما السبل لتفادي الرقابة" في ما يتعلق بالمحوّلات).

من بين لوائح المحوّلات المعروفة:
- publicproxer.com : ينطوي على سلسلة من المحوّلات المجهولة والمعروفة.
- Samair (http://www.samair.ru/proxy/) : ينطوي على محوّلات مجهولة فضلاً عن معلومات عن محوّلات تتقبل نظام التشفير الذي يعتمد بروتوكول طبقة المقابس الآمنة SSL.
- قاعدة بيانات المحوّلات rosinstrument (http://tools.rosinstrument.com/proxy/): يشكل قاعدة بيانات حول المحوّلات.

ثم، تتوجه إلى قائمة "الخيارات" في المتصفّح لتقع على خيار في "عام" أو "شبكة" أو "أمن" يسمح لها بإدخال ثوابت المحوّل لولوج الإنترنت. (ينطوي المتصفّح فايرفوكس Firefox على هذا الخيار في "خيارات" و"عام" و"ثوابت الارتباط"). وبعد ذلك، تضغط على "تركيبة المحوّل لولوج الإنترنت، بين عنوان الخادم الشبكي والمحطة في القسمين "محوّل بروتوكول نقل النص التشعّبي http" و"محوّل بروتوكول طبقة المقابس الآمنة SSL". ومن ثم، تسجّل هذه الثوابت لتعمد إلى إعادة تشغيل المتصفّح وتتمكن من تصفّح الويب باستخدام محوّل مجهول.

لكنها لا تلبث أن تدرك أن الاتصال بالويب بطيء قليلاً لأنها مضطرة إلى القيام بدورة لتتمكن من تحميل كل صفحة. فبدلاً من أن تتصل مباشرة بهوتمايل Hotmail.com، تتصل أولاً بالمحوّل الذي يتصل بدوره بهوتمايل Hotmail. وعندما يرسل هوتمايل Hotmail صفحة إليها، يستلمها الخادم المحوّل أولاً ليرسلها إليها ثانياً. كذلك، تلاحظ أنها تواجه بعض المشاكل لولوج مواقع محددة على الويب ولا سيما تلك التي تفرض تسجّلها. ولكن أداة المدوّنة في هذه الحال لا تسجل عنوانها الشبكي!

فضلاً عن ذلك، تسمح المحوّلات للمستخدم بالاستمتاع: فإن توجهت إلى موقع إرسال البريد الإلكتروني الشهير noreply.org، يستقبلك بإعطائك عنوانك "أهلاً بك يا pool-151-203-182-

."212.wma.east.verizon.net 151.203.182.212

والآن، موعدنا مع anonymizer.com الذي يسمح بالإطلاع على صفحات محددة من الويب من خلال محوّل مجهول. فليس عليك إلا أن تطبع، في الخانة العليا من الجهة اليمنى، عنوان الموقع الإلكتروني http://www.noreply.org أو أن تضغط على الصلة http://anon.free.anonymizer.com/http://www.noreply.org ليظن noreply.com أنك تأتي من vortex.anonymizer.com (علماً بأن anonymizer هو وسيلة جيدة لاختبار المحوّلات من دون تغيير ثوابت المتصفّح إلا أن هذا الموقع لا يعمل مع خدمات الويب المتطورة مثل البريد الإلكتروني عبر الويب أو خوادم المدوّنات عبر الويب weblog).

في النهاية، ينبغي أن تتبع الإرشادات الآنفة الذكر لتتمكن من استخدام محوّل مجهول ومن ثم الانتقال إلى noreply.com لتكتشف كيف له أن يعرف من أين تأتي.

غير أن المحوّلات ليست بكاملة إذ تمنع بلدان كثيرة استعمال المحوّلات الشعبية لتتفادى لجوء مستخدمي الإنترنت إليها لولوج مواقع ممنوعة، فيضطر هؤلاء إلى تغيير المحوّل عندما تعطله السلطات. ولا شك في أنه من شأن هذه الإجراءات أن تتسبب بمضيعة للوقت. أما إذا كانت ساره الوحيدة التي تستخدم محوّلاً في بلدها فيمكنها أن تواجه مشكلة أخرى لا سيما إذا تمكّن المستخدم من بلوغ خادم محوّل واحد من المدوّنة وكانت الوزارة تملك الوسائل الضرورية للوصول إلى بيانات كل مزوّدي خدمة الإنترنت. ومع أن المسؤولين لا يستطيعون إثبات أن ساره قد استخدمت فعلاً المحوّل لتلج أداة مدوّنة، إلا أنهم يستطيعون أن يتحققوا من أنها مستخدمة الإنترنت الوحيدة التي استعملت هذا المحوّل. ومن الأفضل في هذه الحال أن تلجأ ساره إلى المحوّلات المشهورة في المنطقة التي تقطن فيها وتعمد إلى تغييرها باستمرار.

المرحلة الرابعة : المحوّلات، القسم الثاني. بات الأمر الآن بغاية السرّية!

بدأت ساره بالتساؤل ما قد يحصل في حال تمكّنت الوزارة من إقناع مشغّل المحوّل، بطريقة شرعية أو عبر رشوته، بالاحتفاظ بآثار مستخدميه كافة وتدوين المواقع التي يزورونها. إلا أنها تعتمد على مدير المحوّل ليحميها مع أنها لا تعرفه حتى! (في الواقع، قد لا يعرف مدير المحوّل أنها تمر عبره للاتصال بالشبكة لأنه غالباً ما يترك محوّله مفتوحاً بشكل عرضي).

لحسن الحظ أن لساره صديقاً في كندا وافق على مساعدتها على الحفاظ على مجهولية مدوّنتها خاصةً أن كندا أقل ميلاً من بلدها إلى فرض الرقابة على الإنترنت. فاتصلت به وطلبت منه تحميل نظام "سركمفنتور"

"Circumventor" (http://www.peacefire.org/circumventor/simple-circumventor-instructions.html) الذي يسمح لمستخدمه باستعمال جهاز الكمبيوتر كمحوّل لمستخدمين آخرين.

حمّل جيم، صديق ساره، هذا النظام من موقع peacefire.org وأنزله على ويندوز Windows علماً بأن هذه العملية ليست بسهلة البتة. فينبغي أن يبدأ بوضع Pearl ومن ثم OpenSA ليتمكن في النهاية من وضع Circumventor. ثم، يفترض به أن يترك جهاز الكمبيوتر متصلاً بالإنترنت بشكل مستمر ليسمح لساره باستخدامه كمحوّل من دون أن تضطر إلى طلب منه الاتصال كلما أرادت تصفّح الإنترنت على أن يتصل بها على هاتفها الخلوي ويعطيها عنوان الموقع الإلكتروني الذي تستطيع استعماله لتصفّح الويب أو مدوّنتها عبر استخدام المحوّل. وتتسم العملية بالسهولة لأن ساره تستخدم المحوّل من منزلها أو من مقهى إلكتروني من دون أن تبدّل أي ثابتة في نظامها.

لكن ساره لا تزال تواجه مشكلة كبيرة هي أن جهاز الكمبيوتر الخاص بصديقها غالباً ما يتوقف ليعيد التشغيل. وفي كل مرة، يعرض مقدّم خدمة الإنترنت عنواناً شبكياً جديداً لا تستطيع استخدام المحوّل من دون إدراكه. وفي كل مرة أيضاً، يضطر صديقها إلى الاتصال بها ليعطيها العنوان الجديد، وهذا مكلف ومزعج في آن. كذلك، تخشى ساره من أن يسلّم مقدّم خدمة الإنترنت للضغط الذي تمارسه الحكومة عليه كونها تستخدم العنوان نفسه لفترة طويلة.

المرحلة الخامسة : توجيه أونيون "onion routing" بواسطة نظام تور Tor

اقترح جيم على ساره أن تختبر نظام تور Tor الجديد نسبياً الذي يتمثل هدفه بالمحافظة على مجهوليتها فيما تتصفّح الإنترنت. ويعتمد توجيه أونيون على مبدأ الخوادم المحوّلة نفسه أي أن ساره تتصل بالإنترنت عبر المرور بجهاز كمبيوتر آخر كوسيط يبلغ مرحلة أبعد من التي بلغتها. وتجدر الإشارة إلى أن كل طلب يوضع في شبكة توجيه أونيون يمر بعدة أجهزة كمبيوتر يتراوح عددها بين 2 و20. فيصبح من الصعب معرفة أي جهاز كمبيوتر يصدر الطلب.

تخضع كل مرحلة من التوجيه لترقيم معيّن فيصعب على الحكومة اقتفاء أثر ساره. فضلاً عن ذلك، لا يعرف كل جهاز كمبيوتر في السلسلة إلا أقرب جيرانه أي أن الخادم ب يدرك أن الخادم أ أرسل إليه طلب ولوج صفحة الويب وأنه يمرر الطلب للموجه ج. إلا أن الطلب بحد ذاته مرقّم: فلا يدرك الموجه ب أي صفحة طلبتها ساره أو أي موجّه سيتولى تحميل الصفحة.

نظراً إلى تعقيد هذه التكنولوجيا، تفاجأت ساره من السهولة التي تمكنت فيها من تحميل تور Tor على نظامها (http://tor.eff.org/cvs/tor/doc/tor-doc-win32.html). ومن ثم، عمدت إلى تحميل بريفوكسي Privoxy وهو محوّل يعمل مع نظام تور Tor ويمحو كل الإعلانات التي تظهر على صفحات الويب. وبعد وضع البرنامج وإعادة تشغيل جهاز الكمبيوتر، توجهت ساره إلى noreply.com لتكتشف أن نظام تور Tor يغطيها. فظن موقع noreply.com أنها تتصل بالإنترنت من جامعة هارفرد Harvard. وعندما أعادت الكرّة، ظن noreply أنها تتصل من ألمانيا. فاستنتجت أن تور Tor يغيّر هويتها عند كل طلب، مما يساعدها على حماية مجهوليتها.

إلا أن هذه التكنولوجيا لا تعفيها من بعض التبعات الغريبة. فعندما تلج غوغل Google بالمرور بتور Tor، تتبدّل اللغة باستمرار! فيأتي البحث باللغة الإنكليزية ومن ثم اليابانية فالألمانية والهولندية في غضون بضع دقائق. فاستفادت ساره من هذا الوضع لتتعلم لغات جديدة في حين أن تبعات أخرى تقلقها. فهي تحبّذ مساعدة المعجم التعاوني ويكيبيديا Wikipedia ولكنها أدركت أنه يمنعها عن نشر المقالات عندما تمر عبر تور Tor الذي يواجه مشاكل المحوّلات الأخرى كافة. فيغدو تصفّح الإنترنت أكثر بطءاً مقارنةً بتصفّحه من دون محوّل. لذلك، تفضّل استخدام تور Tor وحسب عندما تنوي ولوج مواقع دقيقة المحتوى أو تدوين الملاحظات على مدوّنتها علماً بأنها لا تستطيع تسجيل تور Tor على جهاز كمبيوتر عام.

لكن الأمر المقلق هو أن تور Tor يتوقف أحياناً عن العمل! فيعمد مزوّد خدمة الإنترنت إلى تعطيل بعض الخوادم البدل التي يعتمد تور Tor عليها وقد تنتظر ساره طويلاً من دون أن تحصل على الصفحة المطلوبة عندما يحاول تور Tor استعمال موجّه معطّل.

المرحلة السادسة : ميكسماستر Mixmaster وإنفيزيبلوغ Invisiblog وجي بي جي GPG

تتساءل ساره ما إذا كان من حل لتتمكن من التدوين من دون استخدام خادم محوّل. وبعد أن أمضت فترة طويلة تناقش الموضوع مع فني في مجال المعلوماتية، بدأت تكتشف خياراً جديداً هو إنفيزيبلوغ Invisiblog الذي يشتمل على مجموعة من الأستراليين المجهولين تعرف بـــ "vigilant.tv" تدير هذا الموقع الموجّه إلى المشككين. إلا أنه يصعب التدوين على إنفيزيبلوغ Invisiblog عبر الويب كما يتم ذلك مع أدوات التدوين الأخرى لأنه يعتمد على استخدام بريد إلكتروني منظّم بطريقة خاصة وتوقيع مرقّم ابتكره نظام ميكسماستر MixMaster لإرسال البريد الإلكتروني.

بما أنه صعب على ساره فهم هذه الجملة الأخيرة، ما كان منها إلا أن لجأت إلى نظام السرية التامة

(Pretty Good Privacy) جي بي جي GPG وهو نظام تشفير بمفتاح عام. ويشكل الترقيم بمفتاح عام تقنية تسمح لك بإرسال رسائل إلى شخص فيما أنت متأكد من أنه الوحيد الذي سيتمكن من قراءتها من دون أن يضطر إلى مشاركتك مفتاحاً سرياً (مما قد يسمح لك بقراءة رسائل استلمها من أفراد آخرين). ويسمح الترقيم بمفتاح عام بتوقيع وثائق عبر استخدام توقيع رقمي يستحيل تقليده. فتبتكر مفتاحين تلجأ إليهما لتعرض الرسائل على المدوّنة ثم توقّعها بواسطة مفتاحها الخاص. أما إنفيزيبلوغ Invisiblog فيستخدم مفتاح ساره العام ليتأكد من أنها المرسلة الفعلية قبل أن يعرض الرسائل على مدوّنتها. (الرجاء مراجعة الفصل "كيف تحمي سرّية بريدك الإلكتروني" للإطلاع على تشفير البريد الإلكتروني).

وبعد الإنتهاء من هذه العملية، تنتقل إلى وضع نظام ميكسماستر MixMaster المجيب الذي يقوم بتشويش مصدر البريد الإلكتروني كونه يرسله من دون تحديد هوية المرسل، وذلك عبر تدمير كل المعلومات التي تسمح بتعرّف البريد الإلكتروني قبل إرساله إلى المرسل إليه. وباللجوء إلى سلسلة من هذا النظام تتراوح بين 2 و20 عنصراً، يصعب تحديد مصدر الرسالة الأصلي أو تسجيل معلومات تتعلق بمرسلها. وفي هذه الحال، من الضروري أن تنشئ ساره نظام ميكسماستر MixMaster عبر ترجمة الرمز المصدر وهو مشروع يحتاج إلى مساعدة تقنيين.

استعانت ساره بمفتاحها العام لترسل رسالة أولى من ميكسماستر MixMaster إلى إنفيزيبلوغ Invisiblog. فاستفاد إنفيزيبلوغ Invisiblog منها ليستحدث مدوّنة جديدة هي "invisiblog.com/ac4589d7001ac238 " علماً بأن هذه السلسلة من الأرقام تشكل البايتات الـــ 16 الأخيرة من مفتاح جي بي جي GPG. ومن ثم، تضمنت الرسائل اللاحقة التي أرسلتها إلى إنفيزيبلوغ Invisiblog عبر ميكسماستر MixMaster نصاً موقعاً بالمفتاح العام مع أن هذه العملية ليست بوسيلة سريعة بقدر المدوّنة المعتادة. فقد تستغرق الرسالة بين ساعتين ويومين لتصل إلى الخادم بسبب أنظمة إرسال البريد الإلكتروني الخاصة بميكسماستر MixMaster. إلا أنه يفترض بساره أن تنتبه ألا تلج المدوّنة كثيراً لأن أداة المدوّنة قد تسجّل عنوانها مؤكدة أنها كاتبتها. ولكنها تستطيع أن تطمئن إلى أن مالكي إنفيزيبلوغ Invisiblog يجهلون هويتها تماماً.

تتمثل مشكلة نظام إنفيزيبلوغ Invisiblog الكبرى في أن معظم الناس يعتبرونه معقّداً، كما أنه يصعب عليهم استخدام المفاتيح العامة والخاصة علماً بأن معظم أدوات الترقيم السهلة الاستخدام مثل سيفير Ciphire قد وضعت لمساعدة الأقل خبرةً في هذا المجال. والنتيجة هي أن عدداً قليلاً من الأفراد يستخدم

التشفير حتى بين الذين يحتاجون إليه فعلاً.

ملاحظة: يشكل ميكسماستر MixMaster تحدياً فعلياً بالنسبة إلى المستخدمين. أما مستخدمو ويندوز Windows فلا يستطيعون استعمال إلا نسخة نظام تشغيل القرص دوس DOS الأولى من برنامج التحميل. قمت بذلك ولكن يبدو أن البرنامج لا يعمل... أو لعل أنظمة إرسال البريد الإلكتروني تتبادل إرسال بريدي الإلكتروني في ما بينها. وعلى كل فرد يرغب في استخدام النسخة الجديدة، ولا سيما على لينوكس Linux أو ماك Mac، أن يترجم البرنامج بحد ذاته وهي مهمة يصعب على الخبراء تنفيذها. ومن البديهي أن يكون إنفيزيبلوغ Invisiblog أكثر إفادة إذا ما بدأ بقبول رسائل أنظمة إرسال البريد الإلكتروني مثل riot.eu.org. أما في الوقت الحاضر، فليس بعملي للأفراد الذين يحتاجون إليه.
يطرح التشفير مشكلة أخرى في البلدان التي تطبق فيها الحكومة سياسة قمعية. فإن اكتشف المسؤولون جهاز كمبيوتر ساره ومفتاحها الخاص، سيتأكدون من أنها كاتبة المدوّنة التي تثير الجدل. أما في البلدان التي لا يستخدم فيها الترقيم دائماً، قد تكتفي السلطات بمجرّد إرسال رسائل ميكسماستر MixMaster مرقّمة لتبدأ بمراقبة استخدام ساره للإنترنت.

ما الذي يمكن كشفه؟ ما هي الحدود؟

هل يعتبر الحل الذي اختارته ساره المتمثّل بتعلّم مبادئ التشفير وميكسماستر MixMaster الحل المناسب حكماً؟ هل يكفي الجمع ما بين المراحل الخمس لتأمين المجهولية لنشاطك؟ ما من إجابة وحيدة. فعندما يلتزم المرء المجهولية، ينبغي أن يأخذ شروط البلد والمهارة التقنية ومستوى التشكيك بعين الاعتبار. وإن كنت تملك الأسباب الوجيهة للاعتقاد بأن ما تعرضه يعرّضك للخطر وإن كنت تستطيع وضع نظام تور Tor، فلا تتردد أبداً عن القيام بذلك.

النصيحة الأخيرة، لا تنسَ أن توقّع رسائلك على المدوّنة باسم مستعار!

إيثان زوكرمان Ethan Zuckerman

إيثان زوكرمان Ethan Zuckerman هو طالب باحث في مركز بركمان Berkman للإنترنت في كلية الحقوق في جامعة هارفرد Harvard. ويدور بحثه حول العلاقات بين الصحافة المواطنية ووسائل الإعلام المألوفة ولا سيما في البلدان النامية. كذلك، هو مؤسس منظمة جيككوربس Geekcorps التي لا تبتغي الربح وتعمل على التقنيات التعليمية في البلدان النامية كما أنه أحد مؤسسي شركة تريبود Tripod.