تقرير جديد صادر عن المرصد المفتوح لاعتراض الشبكات و مؤسسة حرية الفكر والتعبير يعرض تفاصيل حالة الرقابة على الإنترنت في مصر

في العام الماضي، أمرت مصر بحجب 21 موقعًا إخباريًا. استجاب المرصد المفتوح لاعتراض الشبكات OONI، وهو مشروع لقياس الرقابة ضمن مشروع تور (Tor)، بنشر تقرير عن حجب 10 موقعا إعلاميا (على الأقل)، بما في ذلك مدى مصر والجزيرة. في محاولة لتحديد باقي المواقع المحجوبة ، قامت مؤسسة حرية الفكر والتعبير في مصر باستخدام اختبار المرصد OONI Probe عبر شبكات متعددة في مصر، ثم قامت المؤسسة بنشر تقريرين بحثين، كشفا عن حجب المئات من الروابط التي تجاوزت المواقع الإعلامية.

عملت المنظمتان معا واليوم ننشر تقريرا عن بحث مشترك حول الرقابة على الإنترنت في مصر، استنادًا إلى تحليلنا لقياسات شبكة OONI التي تم جمعها في الفترة ما بين يناير 2017 ومايو 2018.

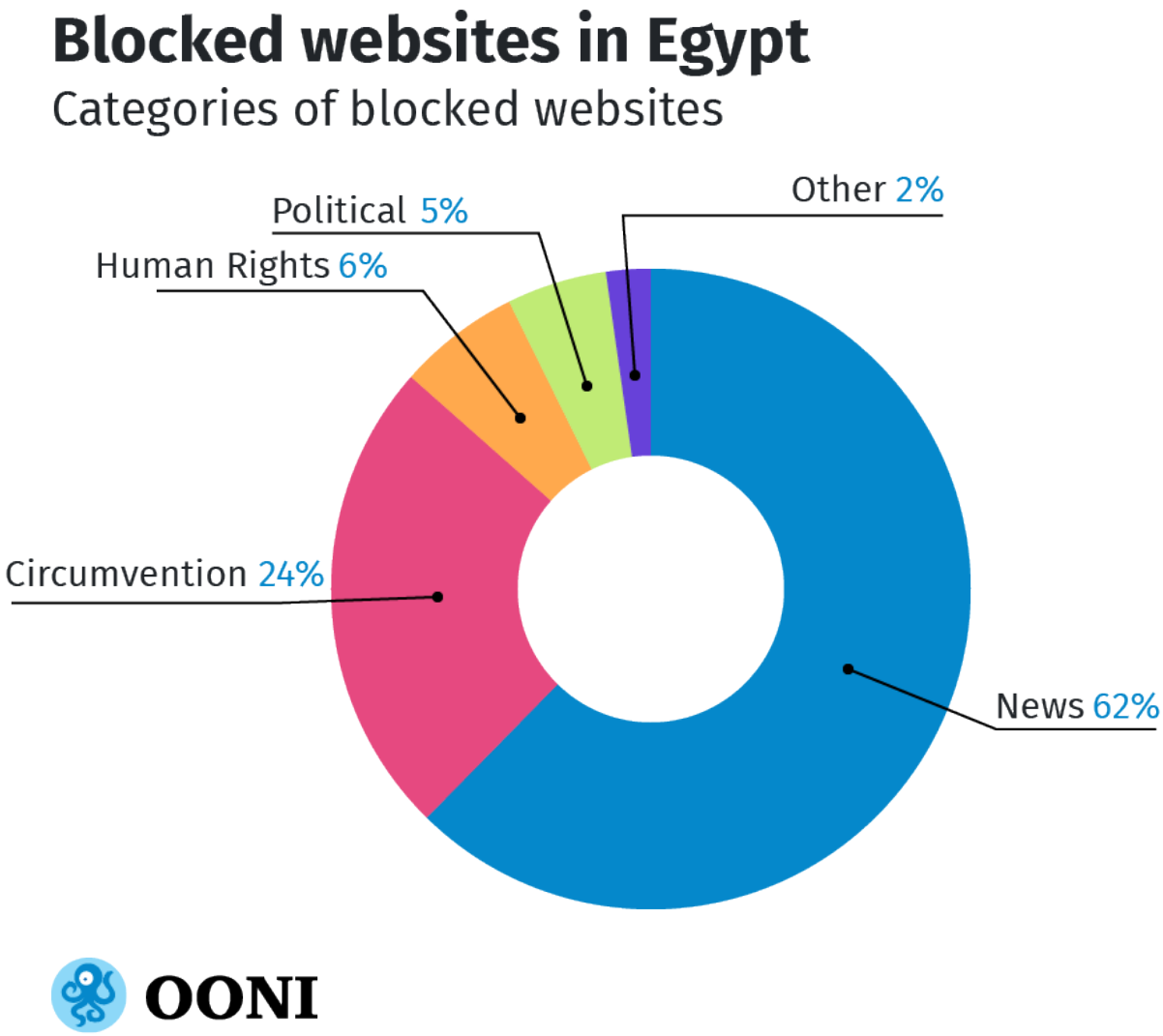
يمكن الاطلاع على بحثنا **هنا**. في هذه الورقة نعرض لبعض أهم النتائج.

انتشار الرقابة على الإعلام

رصدنا أكثر من 1000 رابط به اختلالا على الشبكة خلال فترة الاختبار، أظهر 178 منها بشكل ثابت نسبة عالية من حالات فشل الاتصال عبر HTTP، مما يشير بقوة إلى أنه تم حجبها. وبدلاً من استخدام صفحات تُخطر المستخدم بالحجب، يبدو أن مقدمي خدمات الإنترنت المصريين يقومون بمنع الوصول إلى المواقع المحجوبة باستخدام تقنيات التفتيش العميق (DPI) التي تُعيق.

في بعض الحالات، بدلاً من حقن RST، يقوم مقدمو خدمات الإنترنت بإسقاط الحزم، مما يشير إلى وجود تباين في قواعد التصفية. في حالات أخرى، يعترض مقدمو خدمة الإنترنت البيانات التي تستخدم بروتوكول التعمية (SSL)، والتي تمر بين نقطة اتصال كلاودفلير (Cloudflare) في القاهرة وخواديم مواقع (purevpn.com، psiphon.ca و ultrasawt.com) المُستضافة خارج مصر. تشير قياسات "فترة الاستجابة" (Latency) على مدار العام والنصف الماضي أيضًا إلى احتمال أن يكون مقدمو خدمة الإنترنت المصريون قد غيروا معدات و/أو تقنيات التصفية، نظرًا لأن الكشف القائم على فترة الاستجابة (Latency) لوجود صناديق وسيطة أصبح يُشكّل تحديا أكثر.

يوضح الرسم البياني أدناه أنواع المواقع التي أظهرت أكبر قدر من التشوهات الشبكية، وبالتالي يرجح أن تكون محجوبة.



المواقع المحجوبة في مصر
فئات المواقع المحجوبة: 62% مواقع إخبارية، 24% مواقع تجاوز الحجب، 6% مواقع ذات محتوى حقوقي، 5% مواقع ذات محتوى سياسي، 2% أخرى

يبدو أن أكثر من 100 رابط خاص بالمؤسسات الإعلامية قد حُجبت، على الرغم من أن السلطات المصرية أمرت فقط بحجب 21 موقعًا إخباريًا في العام الماضي. وتشمل هذه منافذ إخبارية مصرية (مثل مدى مصر و المصريون و مصر العربية و دبلي نيوز إيجبت)، بالإضافة إلى مواقع إعلامية دولية (مثل الجزيرة وهافينغتون بوست العربية). كما تم حجب العديد من المواقع الإخبارية التركية والإيرانية (مثل turkpress.co و alalam.ir)، مما يشير إلى أن قرارات الرقابة قد يكون وراءها مخاوف سياسية وأمنية. في محاولة للالتفاف على الرقابة، أنشأت بعض المؤسسات الإعلامية المصرية نطاقات بديلة، ولكن (في حالات قليلة) تم حجبها أيضا.

لدراسة تأثير مثل هذه، أجرت مؤسسة حرية الفكر والتعبير مقابلات مع موظفين يعملون مع بعض

المؤسسات الإعلامية المصرية التي حجبت مواقعها. وقد أفادوا بأن الرقابة كان لها تأثير شديد على عملهم. فبالإضافة إلى عدم قدرتهم النشر وفقدانهم لقطاع من جمهورهم كان للرقابة تأثير مالي عليهم ومنعت المصادر من التواصل مع الصحفيين. علّق عدد من المؤسسات الإعلامية المصرية عملها بالكامل، نتيجة لاستمرار الرقابة على الإنترنت.

يبدو أن العديد من المواقع الإلكترونية الأخرى، إضافة إلى المواقع الإعلامية، قد تم حجبها أيضًا. وتشمل هذه المواقع مواقع حقوق الإنسان (مثل هيومن رايتس ووتش، ومنظمة مراسلون بلا حدود، والشبكة العربية لمعلومات حقوق الإنسان، والمفوضية المصرية للحقوق والحريات، ومرصد صحفيون ضد التعذيب) والمواقع التي تعبر عن النقد السياسي (مثل حركة شباب 6 أبريل)، مما يطرح تساؤل ما إذا كانت قرارات الرقابة ذات دوافع سياسية.

تكتيكات "الدفاع في العمق" لفلترة الشبكة

ربما يكون خبراء الأمن على دراية بمفهوم "الدفاع في العمق"، الذي توضع فيه عدة طبقات من الطبقات الأمنية (الدفاع) في جميع مكونات نظام تكنولوجيا المعلومات. بشكل عام تهدف استراتيجية "الدفاع في العمق" إلى زيادة حماية النظام في حال إخفاق طبقة من طبقات الحماية أو استغلال ثغرة أمنية في إحداها.. في مصر، يبدو أن مقدمي خدمات الإنترنت يطبقون أساليب "الدفاع في العمق" لتصفية الشبكة من خلال إنشاء طبقات متعددة من الرقابة التي تجعل التحايل أكثر صعوبة.

يتضح ذلك بشكل خاص عند النظر في حجب موقع حزب الحرية والعدالة في مصر (FJP) يكشف اختبارنا أن إصدارات مختلفة من هذا الموقع http://www.fj-p.com و http://fj-p.com قد تم حجبها بواسطة اثنين من برمجيات الانترنت الوسيطة، وبذلك أضاف مقدمو خدمات الإنترنت المصريون طبقات إضافية من الرقابة، لضمان أن يتطلب تجاوزها جهدًا إضافيًا.

لم يقتصر الأمر على حجب العديد من مواقع أدوات الالتفاف على الحجب، (بما في ذلك torproject.org و psiphon.ca)، ولكن يبدو أن الوصول إلى شبكة Tor أصبح حجبوبا أيضا. تشير القياسات التي تم جمعها من Link Egypt (AS24863) و Telecom Egypt (AS8452) إلى أنه لا يمكن الوصول إلى شبكة Tor، حيث عجزت الاختبارات عن الاتصال مع شبكة تور Tor في غضون 300 ثانية. في الأشهر الأخيرة، أظهر أكثر من 460 قياسًا فشلا مستمرا في الاتصال بشبكة Tor. وبالمثل، فإن القياسات التي تم جمعها من اتصالات مصر (AS36992)، و موبينيل (AS37069) و فودافون (AS36935) تشير إلى أن الوصول إلى شبكة Tor محجوب. ومن المحتمل أن يكون انقطاع الاتصال من خلال حجب طلبات الاتصال ببعض خواديم تور.

كما يبدو أن تكتيكات "الدفاع في العمق" تطبق فيما يتعلق بحجب جسور تور، التي تمكن من الالتفاف على الرقابة على تور. يبدو أن فودافون تحجب obfs4 (الذي يُأتي كجزء من متصفح تور)، حيث أن جميع محاولات الاتصال كانت غير ناجحة (على الرغم من أنه لا يزال من غير الواضح ما إذا كانت الجسور الخاصة تعمل أم لا). تكشف جميع القياسات التي تم جمعها من الشركة المصرية للاتصالات أن obfs4 يعمل. وبالنظر إلى حجب موقع bridges.torproject.org، يمكن للمستخدمين بديلا عن ذلك الحصول على جسور تور عن طريق إرسال بريد إلكتروني إلى bridges@torproject.org (من حسابات Riseup أو Gmail أو Yahoo)

حملة إعلانية

في عام 2016، كشفت OONI أن الشركة المصرية للاتصالات المملوكة للدولة كانت تستخدم الفحص العميق للحزم (أو أدوات شبكات شبيهة) لاختراق اتصالات HTTP غير المعماة للمستخدمين وحقنها

ببرمجيات إعادة التوجيه إلى محتوى مدر للدخل، مثل الإعلانات بالعمولة. توسع مختبر Citizen Lab في هذا البحث، وحدّد استخدام أجهزة Sandvine PacketLogic وعمليات إعادة التوجيه التي تم حقنها بواسطة 17 جهة مقدمة لخدمة إنترنت (على الأقل) في مصر.

خلال العام الماضي، أظهرت مئات من قياسات شبكة OONI Probe (التي تم جمعها من ASNs متعددة) اختراق روابط HTTP غير المعماة وحقن عمليات إعادة التوجيه إلى الإعلانات بالعمولة وأكواد برمجية لتعدين العملات الرقمية المعماة (cryptocurrency). وقد تأثرت بذلك مجموعة واسعة من أنواع مختلفة من المواقع، بما في ذلك مواقع جمعية السجناء الفلسطينيين و مبادرات المرأة من أجل العدالة بين الجنسين، فضلا عن مواقع جماعات الميم والـ VPN والمواقع الإسرائيلية. حتى مواقع الأمم المتحدة، مثل un.org و ohchr.org، كانت من بين المواقع المتضررة من عمليات إعادة التوجيه للإعلانات.

التوسع في بحثنا

هذه الدراسة جزء من جهد مستمر لمراقبة الرقابة على الإنترنت في مصر وحول العالم. حيث أنه تم إجراء هذا البحث تم من خلال استخدام البرمجيات الحرة والمفتوحة المصدر، والمنهجيات المفتوحة والبيانات المفتوحة، فإنه يمكن إعادة إنتاجها والتوسع عنها.

يمكن لأي شخص تشغيل OONI Probe على Android و iOS و MacOS و Linux وعلى Raspberry Pis. عشرات الآلاف من مستخدمي OONI Probe من أكثر من 200 بلد يفعلون ذلك كل شهر. وبفضل تجاربهم، تم نشر ملايين من قياسات الشبكات، مما سلط الضوء على وسائل التحكم في المعلومات في جميع أنحاء العالم.

لكن نتائج الرقابة لا تثير الاهتمام إلا بقدر أنواع المواقع والخدمات التي يتم اختبارها. لذلك فإننا نشجع على المساهمة في مراجعة وخلق قوائم اختبار، للمساعدة في تطوير الأبحاث المستقبلية في مصر وخارجها.

لمعرفة المزيد حول هذه الدراسة، اقرأ التقرير الكامل **هنا**.