الأنظمة الاستبدادية تحول الإنترنت إلى سلاح.. لكن ثمة أمل

كتبه مورغان ميكر | 25 ديسمبر ,2019

ترجمة وتحرير نون بوست

عندما اتُهم موظفان سابقان في تويتر بالتجسس لصالح المملكة العربية السعودية في نوفمبر 2019، سلطت القضية الضوء على الطرق الجديدة والمبتكرة التي تستخدم فيها الحكومات القمعية التكنولوجيا لإسكات المعارضة، فوفقًا لوزارة العدل الأمريكية قام الرجلان -وهما مواطنان أمريكيان سعوديان- بإرسال معلومات خاصة لأكثر من 6000 آلاف مستخدم من بينهم معارضين للنظام لمسؤول سعودي مقابل مئات آلاف الدولارات.

بالنسبة لغالبية الناس فقد أثارت تلك الأخبار مخاوفهم بشأن فشل الشركات مثل تويتر في الحفاظ على خصوصية معلومات المستخدم، لكن بالنسبة للنشطاء المعارضين للأنظمة القمعية، فخرق الخصوصية يثير مخاوفهم بأن تهدد تلك البيانات حياتهم إذا وقعت في أيدي الحكومة الخاطئة.

وفقًا لوثائق المحكمة فأحد الجاسوسين بإمكانه الوصول إلى معلومات "آي بي" المستخدمين -التي تكشف عن موقعهم- رغم عدم وجود أي غرض تجاري شرعي يسمح بالوصول بالوصول إلى حسابات المستخدمين.

يقول تويتر إنه قد غيّر من قواعده ويفرض الآن قيودًا على الوصول إلى المعلومات الحساسة للمستخدمين لتصبح متقصرة على مجموعة فقط من الموظفين المدربين والمحققين، لكن تلك القضية الاستثنائية لفتت الأنظار إلى كيفية استخدام الأنظمة الديكتاتورية للتكنولوجيا لسحق المعارضة.

لم تعد الأدوات الرقمية تشكل التهديد الوجودي الذي كانت عليه في بداية العقد، فبدلًا من ذلك يجب على نشطاء الديموقراطية التعامل مع جواسيس وسائل التواصل الاجتماعي وبرامج التجسس التي قد تخترق هواتفهم، ومتصيدو وسائل التواصل الاجتماعي الذين يقومون بمهاجمتهم، والدعايا الحكومية وحجب المواقع الإلكترونية ومراقبتها.

> يستخدم برنامج سايفون حوالي 5 إلى 6 مليون مستخدم في العراق وتركيا والسودان وأوغندا والبرازيل وفيتنام

في العام الماضي وصف مارك زوكربيرج مدير فيسبوك الأمن السيبراني بأنه "سباق تسلح" مع وجود ممثلين سيئين يتنافسون للتغلب على تكنولوجيا فيسبوك والفوز في سباق المعلومات، لكن عمالقة وسائل التواصل الاجتماعي لا يواجهون وحدهم هذا الاستبداد التكنولوجي المتزايد.

في ديسمبر 2018 سأم الرئيس السوداني عمر البشير من الاحتجاجات المتزايدة التي تطالب باستقالته، فحاول منع المحتجين من تنظيم المظاهرات عن طريق حجب منصات التواصل الاجتماعي في البلاد مثل تويتر وفيسبوك وانستغرام وواتساب، استمر الحجب 68 يوم وفقًا لمنظمة "نت بلوكس" التي تراقب حرية الإنترنت وأمن الشبكات.

لكن الناشط محمد أمين يقول إنه في ذلك الوقت استطاع الناس تجاوز الحجب باستخدام برامج الشبكات الافتراضية الخاص التي تقوم بإخفاء موقع المستخدم وتسمح له بالوصول إلى المواقع المحجوبة في بلده، يقول أمين: "كنت استخدم برنامج سايفون "Psiphon"، كان الأشهر في البلاد".

عندما أطلق مايكل هول برنامج "سايفون" من كندا عام 2006 كان معظم جمهوره من إيران والصين -أكثر دولتان تتمتعان برقابة عالية على الإنترنت-، يقول هول: "على مر السنين تطور الأمر بشكل كبير"، فاليوم يستخدم البرنامج حوالي 5 إلى 6 مليون مستخدم في العراق وتركيا والسودان وأوغندا والبرازيل وفيتنام.

يضيف هول: "في كل مكان في الشرق الأوسط وشمال إفريقيا هناك نوع من أنواع الحجب، إما لمواقع التواصل الاجتماعي، أو برامج المكالمات أو المواقع التقليدية"، وكلما تتحسن قدرة الحكومات في فرض الرقابة على الإنترنت تصبح مهمة هول أكثر صعوبة، فهو يعتقد أن الأنظمة القمعية تستخدم خوارزميات التعلم الآلي لتحصل على بصمات اتصال برامج "VPN" وتقوم بحجبهم.

فنقاط الوصول التي كانت تعمل جيدًا لعدة أشهر قد تتوقف فجأة، يقول هول: "أعتقد أن

الحكومات بدأت في تطبيق ونشر خوارزميات التعلم الآلي وبدأوا في إجراء البصمات على نطاق واسع غير مسبوق".

في بداية هذا العام؛ قامت الصين بتغريم رجل يدعى زو يونفينغ لاستخدامه تطبيق إزالة الحجب "Lantern"، وفي تركيا 2017 تعرض 75 ألف مواطن للاحتجاز أو الطرد من وظائفهم لوجود تطبيق الرسائل المشفرة "ByLock" على هواتفهم.

يقول الخبير الأمني توم لوينثال: "تصميم أشياء مخصصة للنشطاء أمر صعب، فعندما تصنع أداة لمجموعة مهددة، فإنك تخاطر بأن تُستخدم الأداة لإبراز ما يستحق الاهتمام به فقط".

بدأت بعض الشركات في محاولة إعادة تعريف طريقة وصول الناس إلى الإنترنت، اعتاد لوينثال على نصح النشطاء والصحفيين باستخدام أدوات تحميهم من التهديدات الإلكترونية وبدأ في العمل على متصفح " Brave"، أطلقت الشركة -ومقرها سانتا كلارا- متصفحًا يركز على الخصوصية في شهر نوفمبر وسوقت لنفسها كحل لأعطال الإنترنت التي تسببها "رأسمالية المراقبة".

> لا يوجد نظام مضمون تمامًا، لكن من الصعب تنظيم هجوم يستهدف أحد النشطاء عن طريق متصفح بريف

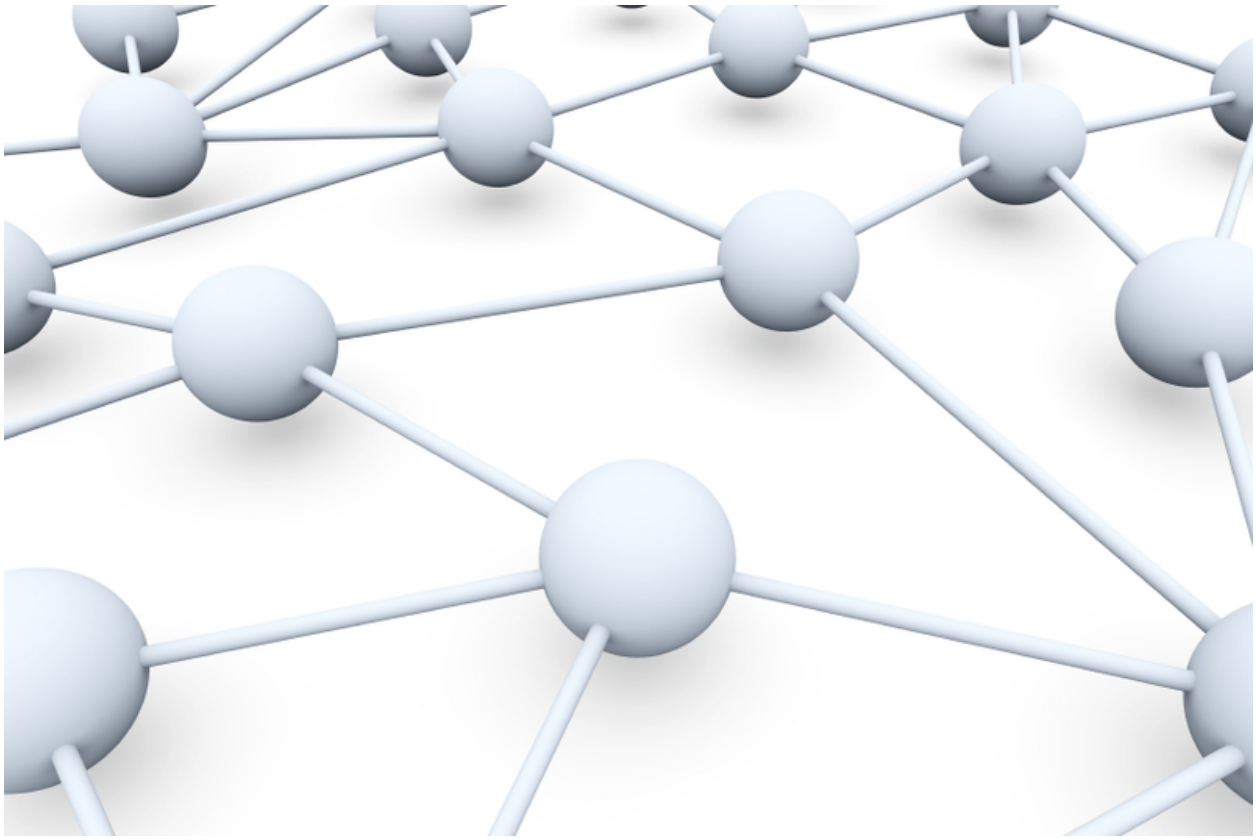
وفقًا للوينثال؛ فقد حاول متصفح بريف حجب المتتبعين واستخدام التصفح الآمن لحجب مواقع التصيد -وهي مواقع وهمية تخدع النشطاء لإدخال بريدهم الإلكتروني ورمز المرور فيتم اختراق حساباتهم، يضمن المتصفح مستوى عالٍ من الأمان والخصوصية حتى لا يتعرض أي شخص للخطر عندما يستخدم المنتج، سواء كان الدافع القلق من جمع الشركات للبيانات أو الاستهداف من قبل المراقبة الحكومية.

يضيف لوينثال: "لا يوجد نظام مضمون تمامًا، لكن من الصعب تنظيم هجوم يستهدف أحد النشطاء عن طريق متصفح بريف، ستحتاج حينها إلى رفع مستوى الهجوم واستخدام تقنيات باهظة وأكثر تطورًا، وبذلك فأنت تواجه خطرًا أكبر بكثير من مجرد القبض عليك"

تتجه بعض الحكومات لإغلاق الإنترنت لمواجهة الاحتجاجات السياسية، فوفقًا للمنظمة الحقوقية الرقمية " Access Now" يتعرض الإنترنت للإغلاق على مستوى محلي أو إقليمي أكثر من ذي قبل، فقد شهد العام الماضي 196 إغلاق مقارنة بـ106 عام 2017.

شهد شهر نوفمبر إغلاق واسع النطاق في إيران عقب اندلاع احتجاجات لمعارضة ارتفاع أسعار الوقود، يعتقد هول أن الإغلاق المتزايد للإنترنت دلالة على إحباط الحكومة، ويضيف: "أعتقد أن السبب وراء إغلاق الحكومة الإيرانية للإنترنت هو إدراكها لعدم قدرتها على منع أدوات مكافحة الرقابة".

وبغض النظر عن الدوافع، فالإغلاق قد يكون فعالًا ما لم يملك المستخدمين معرفة متقدمة للتحايل عليه، يقول أمير راشيسي -باحث في مركز نيويورك لحقوق الإنسان بإيران- أن أشخاص قليلون في إيران قادرون على الدخول إلى الإنترنت لكن هؤلاء الأشخاص تقنيون وليسوا أشخاصًا عاديين.



هناك تطبيق يسمى "Bridgefy" يستخدم تقنية دمج الشبكة ليستطيع المحتجون الاتصال بالإنترنت رغم انقطاعه، تقوم هذه التقنية بربط سلسلة من الأجهزة باستخدام البلوتوث والرسائل المشفرة التي يمكنها الاتصال مع جميع المستخدمين في السلسلة أو الدمج بين المستخدمين حتى يصلوا إلى المستلم المقصود.

انطلق التطبيق في 2015 ويحاول الآن ترخيص تقنيته لاستخدامها في التطبيقات الأخرى، يقول جورج ريبس المدير التنفيذي: "إذا قام تطبيق ما مثل أوبر بتبني تقنيتنا سيكون الناس حينها قادرون على استخدام أوبر دون إنترنت".

على كل حال تعتمد فكرة دمج الشبكات على عدد كبير من التنزيلات لتعمل على نطاق مدينة كاملة، ولا يمكن أن تكون المسافة بين كل رابط في السلسلة والذي يليه أكثر من 100 متر.

امتلك " Bridgefy" شبكة كافية لدعم متظاهري الديموقراطية في هونج كونج هذا الصيف ووصل إلى 96 ألف مستخدم في اليوم، فقد كان المتظاهرون يخشون من احتمالية إغلاق الإنترنت وكذلك من مراقبة الحكومة.

لا يحتاج التطبيق إلى التحقق من المستخدمين عن طريق أرقام هواتفهم، مما يعني أن المستخدمين

بإمكانهم اختيار أن يكونوا متخفيين تمامًا، لكن دور التطبيق في الاحتجاجات جعله هدفًا، فبعد فترة وجيزة من ارتفاع تنزيلاته تعرض موقعه للاختراق ويتم إعادة توجيه زواره لموقع مزيف.

وبينما تستمر الحكومات في التوسع في استخدام تقنياتها للسيطرة على الاتصالات وقمع المعارضة، فسوف تزداد الحاجة إلى المزيد من الأدوات المناسبة لمقاومتهم، يأمل لوينثال أن يكون هناك أدوات أكثر استدامة في المستقبل، ويضيف: "لا أعتقد أن أمان المجموعات المستضعفة يجب أن يبدأ وينتهي بمجرد أدوات، أشعر بالحرج والحزن لأننا نركز على الأدوات عند الحديث عن ضمان قيام النشطاء بعملهم دون الخوف من التعرض للقتل".

المصدر: ميديم

رابط المقال : https://www.noonpost.com/35369/