القمع الرقمي عبر الحدود آخذ في الازدياد

كتبه ديفيد سيلفربيرغ | 13 يوليو ,2022

ترجمة وتحرير: نون بوست

اعتقد خطّاب الروحاني، وهو صحفي وناشط يمني المولد، أنه يمكنه الفرار من الاضطهاد الذي يعاني منه الصحفيون في الشرق الأوسط عندما غادر المنطقة. لكن الاضطهاد تبعه. بينما كان يدرس في واشنطن العاصمة في سنة 2015، نشر منشورات تندد بالانقلاب الحوثي الذي أطاح فيه فصيل مسلح بالحكومة اليمنية. ونتيجة لذلك، ألقِي القبض على والده لفترة وجيزة ثم على شقيقه.

عندما استقر خطّاب الروحاني في تورنتو اتخذت حياته منعطفًا مفاجئًا، إذ بدأ في تلقي رسائل على واتسآب من نساء لم يقابلهن من قبل تحثه على النقر على رابط. لم تبدو الرسائل التي تلقاها كأنها محاولات احتيال عادية بل تم تخصيصها، لأنها تضمنت معلومات أساسية حوله وأبدت تعليقات حول مقالات محددة كتبها أو الإشارة إلى المكان الذي كان يعيش فيه في اليمن.

اخترق قراصنة إنترنت مؤيدون للحوثيين صفحة فيسبوك التابعة لشبكته الإخبارية، التي تغطي انتهاكات حقوق الإنسان في اليمن، واستخدموها لنشر رسائل إيجابية حول الانقلاب باللغة العربية. يقول حيال هذا الشأن: "ما كان فظيعًا هو اعتقاد قرائنا أن هذه الرسائل منا". في النهاية، كان على فريقه حذف الصفحة بالكامل وإطلاق صفحة جديدة.

إن هذا النوع من التهديدات الإلكترونية غيّر منظور الروحاني للعالم وكذلك كيفية تفاعله مع الآخرين. وهو يوضح قائلًا: "لا أكتب جملًا كاملة على هاتفي عندما أراسل صديقًا أو زميلًا أو فردًا من العائلة" وإنما يستعمل الرموز، لأنه يفترض أن نشاطاته الهاتفية مراقبة بشكل مستمر من قبل

النظام الحوثي.

لكن خطّاب الروحاني ليس الشخص الوحيد الذي يعاني من هذا الأمر. في جميع أنحاء العالم، فر الناشطون من الدول الاستبدادية حفاظا على سلامتهم بيد أن التهديد يستمر في موطنهم الجديد، وإن كان في الفضاء الرقمي. وتشمل هذه التهديدات – التي يشار إليها بشكل عام على أنها القمع الرقمي العابر للحدود – هجمات التصيد الاحتيالي واختراقات برامج التجسس ذات النقرة الصفرية وعمليات إزالة صفحات مواقع التواصل الاجتماعي واختراق شرائح الهواتف النقالة والدعوات المزيفة للمؤتمرات.

في وقت سابق من هذا العام، وبينما تحتل التهديدات الجسدية ضد الناشطين عناوين الصحف، أُعتُقل – على سبيل المثال – خمسة مواطنين صينيين بتهمة التخطيط لهجمات ضد معارضين يعيشون في مدينة نيويورك. لكن المضايقات الرقمية التي يمكن إجراؤها بنقرة من زر الفأرة تحدث في غالبيتها خلف الكواليس، كما يبدو أن عددها في ارتفاع. أحصت "هندسة العلوم الجنائية الرقمية" وهي وكالة أبحاث يقع مقرها في لندن 326 حادثة قمع رقمي عابر للحدود ما بين 2019 و2021، مقارنة بـ 105 حوادث ما بين 2017 و2019.

تقول إيزابيل لينز، محللة الأبحاث في منظمة حقوق الإنسان "فريدوم هاوس"، إن أحد أسباب تزايد هذه الهجمات الإلكترونية يرجع إلى حقيقة أنها قد تكون أقل تكلفة بكثير من الهجمات الجسدية. وقد نشرت تقريرًا في شهر حزيران/ يونيو الماضي عن تكتيكات القمع المستخدمة ضد المعارضين الذين هاجروا إلى الولايات المتحدة. وتضيف قائلة: "إن هذه الهجمات "الرقمية" تحدث أكثر بكثير مما يعتقد الناس، ولها عواقب خطيرة على أولئك الذين يمارسون حياتهم العادية

وينخرطون في أعمالهم أو نشاطاتهم السياسية".

من الصعب تتبع النطاق الكامل للقمع الرقمي العابر للحدود لأنه لم يتم الإبلاغ عن العديد من الحوادث. تعمل بعض المؤسسات على إظهار مقدار الضرر الذي يمكن أن يُحدِثه – ومدى تهاون استجابة الحكومات وإنفاذ القانون. يتضمن تقرير صدر هذا العام عن "سيتيزن لاب"، وهي مجموعة بحثية في جامعة تورنتو، نتائج مقابلات مع أكثر من عشرة ناشطين فروا من أوطانهم للعيش في كندا.

وخلص التقرير إلى أن "الاستهداف الرقمي له تأثير خطير على رفاهية الضحايا، ويقوض قدرتهم على الانخراط في أعمال المناصرة العابرة للحدود، ويخرق الحقوق الجوهرية مثل الحق في الخصوصية وحرية التعبير والتجمع السلمي، كما يزيد من المخاطر الواقعة على عائلات وأصدقاء المستهدفين الذين يظلون داخل أوطانهم".

وتضم قائمة الدول التي حددها "سيتيزن لاب" على أنها من بين أكثر مرتكبي القمع الرقمي العابر للحدود شيوعًا، اليمن وأفغانستان والصين وإيران ورواندا وسوريا. وتقول نورة الجيزاوي، وهي مسؤولة الأبحاث في "سيتزن لاب" والمؤلفة المشاركة في التقرير، إن اختراقات البرمجيات ذات النقرة الصفرية، التي تسمح للمهاجم باختراق الهاتف أو الحاسوب حتى دون فتح أو النقر على رابط أو مرفق خبيث، هي الأكثر إثارة للقلق لأنه "يمكنها التهرب من ممارسات السلامة الرقمية".

في سنة 2021، استخدم المخترقون مثل هذه البرمجيات للتسلل وتركيب برامج التجسس على الهاتف الخلوي للناشطة السعودية في مجال حقوق المرأة لجين الهذلول، التي كانت تعيش في ذلك الوقت في كولومبيا البريطانية. وفي حالتها، ترك الجناة عن طريق الخطأ ملف صورة على هاتفها مما سمح للباحثين بتحديد مصدر البرمجة. أشار المخطط الرقمي إلى مجموعة "إن إس أو"، وهي شركة تكنولوجيا إسرائيلية تصدرت عناوين الصحف لبيع برامج التجسس للدول القومية الاستبدادية.

تهدف بعض أشكال القمع الرقمي إلى إذلال الأفراد والكشف عن معلوماتهم الخاصة. وقد اكتشفت إحدى المستجوبات في تقرير "سيتزن لاب"، التي انتقلت من الصين إلى كندا، أنه تم تداول صور عارية ملفقة لها بين الحاضرين في أحد المؤتمرات التي كانت تنوي حضورها. وقد نُشرت معلوماتها الشخصية في إعلانات إلكترونية تطلب خدمات جنسية.

ويشير التقرير إلى أن ضحايا هذا النوع من المضايقات يعانون من الكدر واضطراب القلق والخوف على سلامة أسرهم. وتقول المؤلفة المشاركة سيينا أنستيس، كبيرة المستشارين القانونيين في "سيتزن لاب": "هناك أيضًا اتجاه للتسليم بهذه الممارسات بين أولئك الذين استمروا في نشاطهم، وهو نابع من إدراكهم لحقيقة أن هذا النوع من الاستهداف سيستمر".

أصبح العديد من الناشطين مرتابين بشأن الرسائل التي يتلقونها. يولي المحامي العراقي كافيه شهروز، الذي يعيش في كندا ويمثّل المعارضين، كل بريد إلكتروني تدقيقًا خاصًا. يقول شهروز إنه تلقى ذات مرة رسالة ممن يفترض أنه منظم لمؤتمر لحقوق الإنسان في ألمانيا يدعوه فيها للتحدث ويطلب منه

ملء المعلومات الشخصية عبر رابط مقدم. وقد بحث أكثر عن المؤتمر واكتشف أنه لم تتم دعوته، مع أن البريد الإلكتروني بدى مخصصًا وذا طابع مهني كذلك.

يقول شهروز: "هذا أحد طرفي الخيط، وما قد يجعلك تنخدع بالنقر فوق الرابط. ولكن بعد ذلك، يتلقى الطرف الآخر رسائل تهديد حول عملي كناشط – أشياء مثل "نحن نعرف ما تفعله وسنتعامل معك لاحقًا"".

هناك القليل من الإنصاف القانوني. توضح أنستيس أن العديد من ضحايا هجمات برامج التجسس في المملكة المتحدة رفعوا "أو برفعون" دعاوى مدنية ضد مشغلي الدولة ومجموعة "إن إس أو". وتضيف أنه من المتوقع الطعن في مثل هذه القضايا، لأنها تركز بشكل عام على المطالبات المقدمة ضدّ شركات خارج نطاق اختصاص البلد المضيف.

في الولايات المتحدة، مثلا، هناك زخم متزايد وراء الدعوات المطالبة بمنع البرامج والأدوات التي تستغلها الأنظمة الاستبدادية. في سنة 2021، أدرجت وزارة التجارة الأمريكية العديد من شركات المراقبة على قائمة الكيانات لمتطلبات الترخيص الخاصة بها التي تقيد التجارة والأعمال التجارية التي تتنافى مع الأمن القومي أو مصالح السياسة الخارجية للولايات المتحدة. وتشمل الإضافات الجديدة للقائمة مجموعة "إن إس أو" وشركة "كانديرو"، وهي شركة لبرامج التجسس مقرها إسرائيل وتطور تكنولوجيا المراقبة والتجسس الإلكتروني للعملاء الحكوميين.

لكن هذا الإجراء لن يحمي الناشطين من التعرض للاضطهاد. قبل عشر سنوات، بدأت إليانا (وهو اسم مستعار لكندية سورية طلبت عدم الكشف عن هويتها) مشاركة قصص ضحايا نظام الأسد من خلال طرح قصص إخبارية عنهم لوسائل الإعلام المحلية مطبوعة وعبر الإنترنت. كما كرست وقتًا

لحشد تأييد الحكومة الكندية بشأن إعادة توطين العديد من اللاجئين السوريين الذين وصلوا إلى البلاد في سنة 2016.

ذكرت إليانا أنها تلقت رسائل منتظمة من غوغل يحذرها من أن أحدهم يحاول الولوج لحساب بريدها الإلكتروني. وجهت شكوكها نحو النظام السوري – لأنه لم يخطر في بالها أحد آخر. وكان مصدر قلقها الرئيسي هو سلامة الناشطين السوريين الذين تتواصل معهم: "كنت على علم بأنه إذا وقعت مثل تلك المعلومات في أيدي ديكتاتورية، فإنها قد تؤدي إلى تداعيات كارثية للغاية، بما في ذلك الاختطاف القسري والتعذيب والاغتيال".

اليوم، تقول إليانا إنها لم تعد اجتماعية كما كانت من قبل: "اعتدت على أن أكون منفتحة للغاية في تفاعلي مع الناس، لكني أدركت أنه يجب أن أكون أكثر حذرًا نظرًا لعدم قدرتي على التنبؤ بمن أو من أين سيأتي الأذى".

المصدر: تكنولوجي ريفيو

رابط المقال : https://www.noonpost.com/44630/