فريق التحرير | نشر في ١٣ مارس ٢٠١٨,

كيف استغلت "المصرية للاتصالات" إنترنت الشعب لكسب الأموال؟

إذا استخدمت الإنترنت في زيارتك لمصر ووجدت أنك كلما زرت مواقع بعينها توجهك الشبكة لزيارة مواقع إعلانية لم ترغب في الأساس في زيارتها، أو مواقع لبرمجيات خبيثة واعتقدت حينها أن جهازك هو المصاب بالفيروسات ولا ضرر من الشبكة نفسها، في الواقع أثبتت لك جامعة تورونتو الكندية أنك على خطأ، وأن جهازك لم يكن مصابًا بالفيروسات، بل استخدمتك "المصرية للاتصالات" في وسيلة لتعدين العملات الرقمية وكسب الأموال.

في تحقيق عميق ومطوّل من مختبر بحثي "lab citizen" في جامعة تورنتو الكندية (مختبر متخصص في التركيز على البحث والتطوير والسياسة الإستراتيجية رفيعة المستوى والمشاركة القانونية في تقاطع تكنولوجيات المعلومات والاتصالات وحقوق الإنسان والأمن العالمي)، قام باكتشاف أجهزة تستخدمها شركة "المصرية للاتصالات" للتجسس وتحييد الأنشطة غير المرغوب فيها على شبكة الإنترنت وتعدين العملات الرقمية.

وجد البحث نتائج متشابهة من بحث شبكة الإنترنت المزودة إلى سوريا ومصر، التي أشارت إلى وجود الأجهزة المخصصة لفلترة البيانات على الإنترنت التي كانت قد استخدمتها الحكومة المصرية من قبل لحجب محتويات مواقع معينة في مصر، إلا أن نتائج مختبر بحث "lab citizen" كانت مختلفة هذه المرة، بعد اكتشافه أجهزة شركة "ساندفاين-بروكيرا" للتجسس وتحييد الأنشطة غير المرغوبة على شبكة الإنترنت.

تصمم شركة "ساندفاين" الكندية الأصل أمريكية الإدارة أجهزة ومنتجات تقنية مصممة خصيصًا للتحكم في شبكات الإنترنت واسعة النطاق، وذلك بحسب طلبات الحكومات التي تستعين بخدماتها، تكون من بين استخدامات تلك الأجهزة فلترة البيانات وإدارة مرور البيانات والتحكم بها على شبكة الإنترنت، والتحكم في حركة المرور في الإنترنت من تحليل بيانات معينة أو تسجيلها أو حظرها.

كيف استطاعت الشركة إعادة توجيه المستخدمين لصالح تعدين العملات الرقمية؟

تستخدم الحكومة الصينية والتركية والسورية أجهزة الشركة نفسها لأغراض مختلفة لمراقبة محتوى الإنترنت وحجب محتويات بعينها، أما عن الحكومة المصرية، فقد استغلت أجهزة "ساندفاين" هذه المرة من أجل كسب الأموال من تعدين العملات الرقمية، فقد نتج عن تتبع الباحثين في مختبر "سيتزين لاب" أن "المصرية للاتصالات" كانت تستخدم هيكلية أطلقت عليها اسم Adhose عبر أجهزة شبكية حاسوبية وبرامج إنترنت وسيطة middleboxes، وهي الأجهزة التي تُستخدم في التحكم في عملية نقل البيانات عبر الشبكة العنكبوتية.

باستخدام هيكلية Adhose استطاعت الشركة إعادة توجيه المستخدمين عن طريق نمطين:

النمط الأول يُدعى نمط الرش mode Spray الذي يعمل على تحويل زوار المواقع التي لا تخضع لبروتوكول الإنترنت الآمن (websites ssl non) بشكل جماعي إلى إعلانات قصيرة الزمن أو نصوص تعدين العملات الرقمية عند محاولة طلبهم موقعًا إلكترونيًا ما، ووُجد أن هذا النمط غير منتشر بشكل كبير مثلما ينتشر النمط الثاني.

تستخدم الشركة أجهزة وطرقًا غير قانونية لكي تقوم بالتعدين، حيث إنها تتحكم في عملية نقل البيانات كما تقوم بتوجيه المستخدمين إلى جهات معينة لتستفيد من ورائهم بصورة غير شرعية

أما عن النمط الثاني فهو نمط التنقيط mode Trickle الذي من خلاله يتم استهداف بعض موارد الجافا إسكريبت وإبطالها، بغاية حقن إعلانات تمكنهم من التعدين من خلال المستخدمين عن العملات المشفرة، حيث رجح الباحثون في تقريرهم أن هذا النمط مستخدم لجمع الأموال سرًا.

لا تشترط العُملات المشفرة فتح أي نوع من الحسابات، كل ما تحتاجه، هو تثبيت تطبيق خاص بالعُملة التي ترغب في استخدامها، يتولى هذا التطبيق مهمة (توليد عنوان) يتم استخدامه لإرسال واستقبال التحويلات

ذلك بالإضافة إلى وجود أجهزة "باكيت لوجيك ساندفاين" من الشركة نفسها، التي استخدمتها الحكومة المصرية في حجب أكثر من 400 موقع صحفي إلكتروني ومواقع ثقافية وعلمية حرة، بالإضافة إلى حجبها خدمات خاصة بالـ(VPN) التي تساعد المستخدمين على تخطي ذلك الحجب ولو جزئيًا.

لماذا يجب أن يخشى المصريون؟

تستخدم الشركة أجهزة وطرقًا غير قانونية لكي تقوم بالتعدين، حيث إنها تتحكم في عملية نقل البيانات كما تقوم بتوجيه المستخدمين إلى جهات معينة لتستفيد من ورائهم بصورة غير شرعية، وهو ما يزيد الطين بلة بالنسبة لوضع مصر من ناحية حرية استخدام الإنترنت، إذ أعربت الجهات العالمية عن قلقها من انحدار مرتبة مصر من حيث متوسط سرعة الإنترنت وحريته للشعب، كان من بينهم المندوب السامي للأمم المتحدة في جينيف حينما وصف سابقًا حجب المواقع في مصر بالمجزرة وإهانة لحرية التعبير.

تستخدم الحكومة الصينية والتركية والسورية أجهزة الشركة نفسها لأغراض مختلفة لمراقبة محتوى الإنترنت وحجب محتويات بعينها، أما عن الحكومة المصرية، فقد استغلت أجهزة "ساندفاين" هذه المرة من أجل كسب الأموال

المصرية للاتصالات تتحكم في حجم ونوع وكمية المعلومات التي يستخدمها المصريون على شبكة الإنترنت من خلال تلك الأجهزة، وبحسب ما ورد في تقرير مختبر بحث "سيتزين لاب" فإن هذا قد يظهر في بطء سرعة الإنترنت بشكل أكثر مما هي عليه في الأساس، بالإضافة إلى تعطل العديد من الأجهزة وانتهاك خصوصية بيانات المستخدمين بشكل غير قانوني.

هل هذه المرة الأولى؟

للحكومة المصرية تاريخ طويل في ابتياع أجهزة المراقبة بمختلف أنواعها، فلا تعد فضيحة مختبر "سيتزين لاب" جديدة على الحكومة المصرية، إلا أن هذه المرة حاولت الحكومة المصرية الانتفاع ماديًا من مراقبة المواطنين وضرب عصفورين بحجر واحد، ولكن هذه ليست المرة الأولى، في منتصف العام الماضي أهدت الإمارات للحكومة المصرية نظام مراقبة فرنسي من شركة "أماسيس" كأداة إلكترونية حديثة لقمع الشعوب، من شركة يلاحقها القضاء بتهمة بيع أجهزة إلكترونية لأنظمة ديكتاتورية.

يدعى نظام الرقابة "سيربر" الذي دفعت فيه الإمارات 10 ملايين يورو لإهدائه لمصر، أنه يوفر مراقبة حية للمستخدمين عبر أجهزتهم الإلكترونية ويمكن من معرفة المواقع التي يتم تصفحها، وتعقب المكالمات التليفونية والرسائل النصية والبريد الإلكتروني ومواقع التواصل الاجتماعي.

تخضع شركة "أمسيس" الفرنسية إلى تحقيق قضائي في فرنسا منذ العام 2011 لإمكانية تورّطها في أعمال التعذيب التي تعرض لها الناشطون في السجون الليبية

يعمل نظام "سيربر" على مستوى بلد بأكمله ويسمح بفرض عملية مراقبة واسعة النطاق على التحركات على الشبكة الدولية في البلد المعني، وحفظ البيانات الخاصة بالاتصالات بالشبكة بما في ذلك عناوين الشبكة أعماق ومراقبة التفتيش أي Deep Packet Inspection تسمى تقنية بفضل ذلك وكل IP الدولية والحصول على محتويات علب البريد الإلكتروني، الرسائل الفورية، شبكات التواصل الاجتماعي المختلف.

مصر تراقب المقيمين في المنازل أيضًا

في عام 2014 نشرت صحيفة "كريستيان ساينس مونيتور" تقريرًا بعنوان: "مصر تكثف مراقبة مواقع التواصل الاجتماعي بحجة مكافحة الإرهاب"، قالت فيه إن السلطات المصرية لن تكتفي فقط بمراقبة النشطاء الذين يدعون لمظاهرات ويخرجون في مظاهرات ضد النظام، ولكنها بدأت بـ"مراقبة المقيمين في منازلهم الذي ينشرون رأيهم على الإنترنت ويبدون إعجابهم بآراء الآخرين أيضًا".

ذكر التقرير أن لمصر تعاون مع 7 شركات أوروبية وأمريكية خبيرة في المراقبة والتجسس، من بينها شركة "جاما" الدولية في لندن و"فريق الهاكرز" في إيطاليا و"بلو كوت" في الولايات المتحدة الأمريكية و"ناروس سيستم" في "إسرائيل" و"سي إيجيبت" المصرية التابعة لشركة "بلو كوت" الأمريكية.

تراقب الحكومة المصرية الجماعات الإسلامية، وكل من له علاقة بالجماعات الإسلامية، وكل المعارضين من مختلف الأحزاب والتيارات بدعوى "محاربة الإرهاب"، بالإضافة إلى كل من له علاقة بمجتمعات المثليين جنسيًا ومجتمعات الدعارة بدعوى حماية "منظومة القيم والأخلاق" المصرية.

"اكتشاف أن وزارة الداخلية ليست منزّهة عن محاولة التجسس على الأفراد بعد اقتحام مقرات أمن الدولة عام 2011، حيث تتجسس عليهم في المحادثات والمراسلات الشخصية من خلال برامج الهواتف المحمولة والويب"

رامي رؤوف، باحث مصري في شؤون أمن المعلومات

كان قد ذكر التقرير كذلك أن شركة "سي إيجيبت" زودت جهاز "الأمن الوطني" – أمن الدولة سابقًا – بأنظمة تُزيد كفاءة الرقابة في العالم الافتراضي، مضيفًا أن الشركة تقوم بتدريب المسؤولين داخل الجهاز على التعامل مع تلك الأنظمة، لتطبيقها في رقابتهم على مواقع الإنترنت والمحادثات في موقعي فيس بوك وتويتر والمشاهدات في يوتيوب.

مصر ليست الدولة العربية الوحيدة التي تبتاع أجهزة المراقبة الإلكترونية لتقييد حرية الإنترنت، حيث تمتلأ قائمة الأنظمة التي تبتاع تلك الأجهزة من الشركات الأوروبية بما لا يقل عن 6 أنظمة عربية من بينها الإمارات والسودان والجزائر والسعودية.

رابط المقال: https://www.noonpost.com/22453/