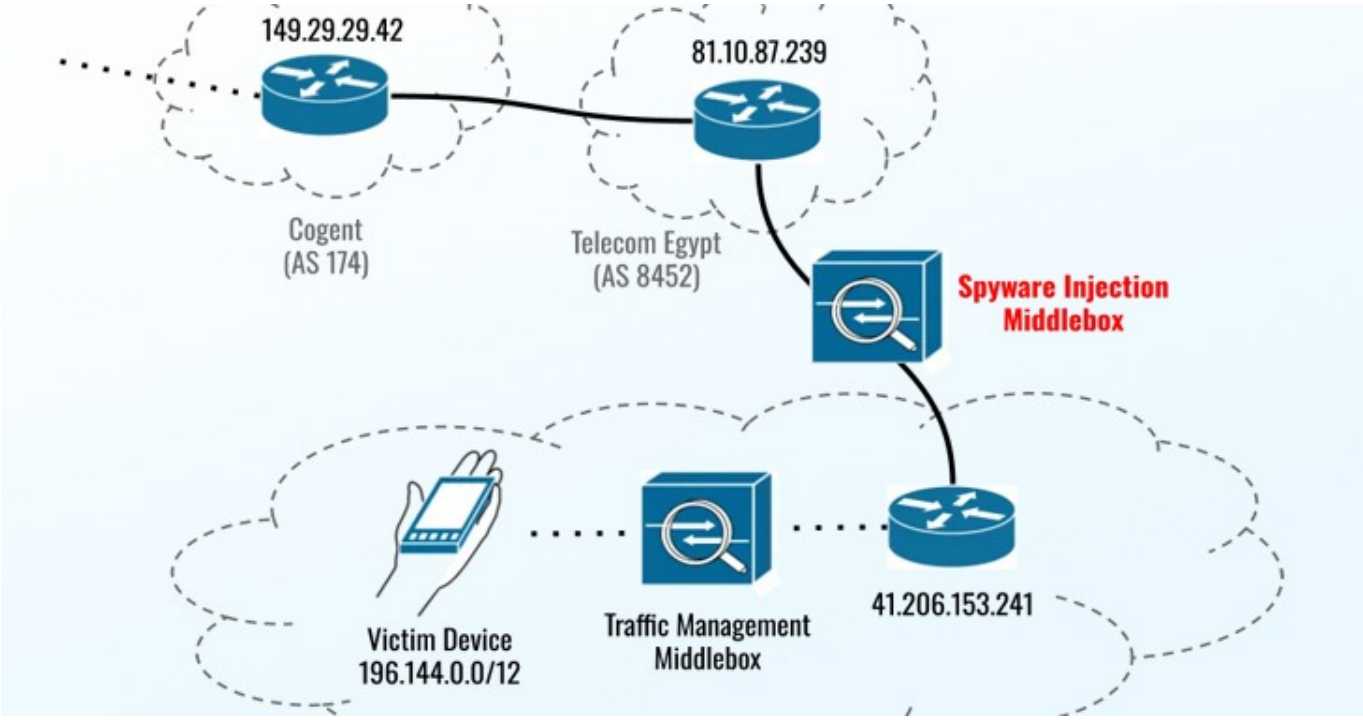
واشنطون بوست: برنامج التجسس بريداتور يستهدف مرشح رئاسي محتمل



نشرت صحيفة واشنطون بوست تقريراً أعدته إيفان هيل وجوزيف مين يسلط الضوء على محاولة التجسس على هاتف المرشح الرئاسي المحتمل أحمد طنطاوي باستغلال ثغرات يوم الصفر (الأخطاء الموجودة في البرنامج والتي تسمح بتنفيذ الأعمال الخبيثة سراً).

وقالت الصحيفة الأمريكية إن إن معارضًا مصريًا بارزًا يخطط لتحدي الرئيس عبد الفتاح السيسي في الانتخابات المتوقعة مطلع العام المقبل استُهدف بهجوم «يوم الصفر» لم يكن معروفًا من قبل في محاولة لإصابة هاتفه ببرامج تجسس بريداتور، وفقًا لبحث جديد أجرته جوجل و مختبر سيتزن لاب بجامعة تورنتو.

دفع اكتشاف الاستغلال لثغرة يوم الصفر، المصمم لتثبيت برنامج التجسس على أجهزة أي فون التي تعمل حتى بأحدث نظام تشغيل، شركة آبل إلى دفع تحديث الأمان للمستخدمين بعد ظهر يوم الخميس.

وقال مختبر سيتزن لاب إنه «يثق بشدة» في أن الحكومة المصرية مسؤولة عن محاولة القرصنة الفاشلة. واستهدف هذا الجهد النائب السابق في البرلمان أحمد الطنطاوي وتحدثت عنه لأول مرة مدى مصر، وهي مؤسسة إخبارية مصرية مستقلة. كان طنطاوي يعيش لفترة وجيزة في لبنان لكنه عاد إلى مصر في مايو.

تعتبر سمات يوم الصفر خطيرة وقيمة بشكل خاص لأنها تستفيد من الثغرات الأمنية التي لم تكتشف بعد. في هذه الحالة، لم يكن على طنطاوي النقر فوق أي شيء لإصابة هاتفه.

قال بيل ماركزاك، زميل أبحاث كبير في سيتزن لاب إن استغلال ثغرة يوم الصفر تلك، قادرة على تثبيت برامج تجسس على أحدث وأعظم أجهزة الأي فون.

وقال ماركزاك إنه بمجرد تثبيته على الهاتف، يمكن للبرنامج سرقة كلمات المرور وتسجيل نقرات المفاتيح وأخذ البيانات من تطبيقات مختلفة ونسخ رسائل الدردشة وتسجيل المكالمات، بما في ذلك تلك التي تجري داخل التطبيقات المشفرة.

مثل باعة برامج التجسس الراقية الأخرى، تقول سيتروكس إنها تبيع فقط البرنامج للوكالات الحكومية. ونظرًا لأن مصر عميل معروف لشركة بريديتور وأن إحدى محاولات الاختراق تمت بواسطة جهاز موجود فعليًا داخل مصر، قال مختبر سيتزن لاب إن لديه «ثقة عالية» في أن الحكومة المصرية مسؤولة عن الهجوم.

وأشارت الصحيفة إلى أن طنطاوي، الرئيس السابق لحزب الكرامة اليساري، منتقد صريح للحكومة المصرية. وفي مارس، أصبح أول سياسي يعلن عن خطط لتحدي السيسي للرئاسة.

رسائل مشبوهة

ونقلت الصحيفة عن طنطاوي قوله إنه أصبح قلقًا لأول مرة بشأن أمن هاتفه في منتصف سبتمبر بعد تلقي الرسائل المشبوهة التي تحتوي على روابط، وأن صديقًا نصحه بالاتصال بـ Lab Citizen حتى يمكن تحليل هاتفه.

ورفض ممثلو الحكومة المصرية التعليق أو لم يردوا على الفور على طلبات التعليق.

وفقًا لـ سيتزن لاب، تضمنت محاولات إصابة هاتف طنطاوي استخدام منتج يسمى باكيتلوجيك طورته ساندفين، وهي شركة معدات شبكات مقرها كندا. وفي عام 2017، استحوذت شركة فرانسيسكو بارتنرز على شركة ساندفين، وهي شركة أسهم خاصة تمتلك حتى عام 2019 أيضًا مجموعة إن أس أو جروب، الشركة المصنعة لبرامج التجسس بيجاسوس، والتي استخدمتها الحكومات للتجسس على الصحفيين والنشطاء والمعارضين السياسيين وغيرهم. ولم ترد ساندفين على طلبات التعليق.

وكتبت مجموعة تحليل التهديدات في جوجل: «هذه الحملة هي مثال آخر على الانتهاكات الناجمة عن انتشار بائعي المراقبة التجارية وخطرهم الجسيم على سلامة المستخدمين عبر الإنترنت».

محاولات عديدة

ولفتت الصحيفة إلى أن محاولات عديدة سعت لتثبيت بريديتور على هاتف طنطاوي بين مايو وسبتمبر، بعد أن أعلن عزمه الترشح للانتخابات، وفقًا لبحث سيتزن لاب. وبدءًا من مايو، تلقى طنطاوي رسائل نصية ورسائل على تطبيق واتساب مع روابط إلى صفحات الويب الخبيثة. ومن الواضح أنه لم ينقر عليها، بحسب الباحثين.

في أغسطس وسبتمبر، قال مختبر سيتزن لاب، تعرض طنطاوي لنوع أكثر خطورة من الهجوم يسمى حقن الشبكة، والذي لم يتطلب منه النقر فوق أي شيء. وفقًا لمجموعة تحليل التهديدات من جوجل، وقع هذا الهجوم عندما حاول طنطاوي زيارة صفحة ويب تحمل بادئة (http)، وعندما فعل ذلك، أعاد المخترق توجيهه إلى موقع إنتليكسا على الويب ثم إلى خادم قام بتنفيذ الاستغلال على هاتفه.

ووفقًا لتحليل سيتزن لاب، فقد فشل الاختراق لأن طنطاوي قام بتنشيط «وضع الإغلاق» من آبل، وهو إعداد حماية وفرته الشركة في عام 2022 يقلل من وظائف الهاتف ولكنه يمنع عديدًا من طرق الاختراق.

وأشارت الصحيفة إلى أن اختراق هاتف طنطاوي كان سيتطلب تثبيت باكيتلوجيك على شبكة فودافون، مزود الخدمة للشبكة التي يستخدمها طنطاوي. وفي حين لم يزعم مختبر سيتزن لاب أن شركة فودافون كانت متواطئة في الهجوم، قال ماركزاك إن الطريقة «الأسهل» لتثبيت باكيتلوجيك على شبكة فودافون سيكون بالتعاون مع الشبكة.

وقال «مصر غير معروفة بكونها حكومة ديمقراطية. يمكنك أن تتخيل أن الحكومة ستكون قادرة على ممارسة الضغط على الشركات للتعاون معها».

ولم ترد شركة فودافون مصر على طلبات للتعليق.

دوافع سياسية

وبحسب الصحيفة، فقد رفض طنطاوي إلقاء اللوم على الحكومة المصرية في الهجوم لكنه قال إنه يعتقد أنه استهدف بسبب أنشطته السياسية وتكهن

بأن محاولة القرصنة كانت تهدف إلى العثور على مواد «للتشهير» به.

وقال «ببساطة، لا يوجد شيء يمكن استخدامه لإحراجي، حتى مع عامين من الاختراق».

وقال طنطاوي إن الأسوأ من ذلك هو اعتقال الحكومة المصرية لأشخاص مختلفين مقربين منه. فقد اعتقلت السلطات ما لا يقل عن 35 متطوعًا لحملة طنطاوي في جميع أنحاء البلاد منذ أغسطس، وفقًا للمبادرة المصرية للحقوق الشخصية.