

الإمارات العربية المتحدة تستخدم الأسلحة السيبرانية للتجسس على أجهزة آيفون خصومها

كتبه 31 | roetrz يناير, 2019



ترجمة وتحرير نون بوست

كتب جويل شيكتمان وكريستوفر بنج

اخترق فريق من قدماء عملاء المخابرات الأمريكية يعملون لحساب دولة الإمارات العربية المتحدة أجهزة آيفون تابعة لنشطاء معارضين وخصومها من القادة الأجانب بمساعدة أداة تجسس متطورة تسمى "كارما"، وذلك في إطار حملة تعكس كيفية تطور الأسلحة الإلكترونية القوية خارج نطاق القوى العظمى في العالم وبين أيدي الدول الأصغر.

بداية من سنة 2016، سمحت هذه الأداة السيبرانية للدولة الخليجية الصغيرة بمراقبة مئات الأهداف بداية من أمير قطر ومسؤول تركي رفيع المستوى وصولاً إلى ناشطة حقوقية حائزة على جائزة نوبل للسلام في اليمن، وذلك وفقاً لخمسة عناصر سابقين ووثائق البرامج التي استعرضتها

رويترز مع العلم أن المصادر التي أجرت معهم رويترز الحوارات لم يكونوا مواطنين إماراتيين.

استُخدمت أداة التجسس “كارما” من قبل وحدة العمليات السبيرانية الهجومية في أبوظبي المؤلفة من مسؤولي الأمن الإماراتيين وقدماء عملاء المخابرات الأمريكية الذين يعملون كمقاولين لصالح أجهزة الاستخبارات الإماراتية. ولم يتم الإبلاغ سابقاً عن وجود هذه الأداة وعن وحدة القرصنة أيضاً، التي تحمل اسم “Project Raven”. وسيتم التطرق إلى أنشطة هذه الوحدة في قصة منفصلة من المقرر أن تنشرها رويترز اليوم.

وصف العاملون السابقون في وحدة القرصنة “كارما” بأنها أداة يمكن أن تسمح بإمكانية الوصول إلى هواتف آيفون ببساطة عن بعد، عن طريق تحميل أرقام الهواتف أو حسابات البريد الإلكتروني في نظام الاستهداف الآلي. ولكن لهذه الأداة حدود، فهي لا تعمل على أجهزة أندرويد ولا تعترض المكالمات الهاتفية. ومع ذلك، كان أداء هذه الأداة قويا حيث أنه على خلاف العديد من الأجهزة لا تحتاج كارما الى أن ينقر الهدف على رابط مُرسل إلى آيفون.

بين سنتي 2016 و2017، تم استخدام كارما للحصول على صور ورسائل البريد الإلكتروني والرسائل النصية ومعلومات تحديد الموقع من أجهزة الآيفون المستهدفة. وساعدت هذه التقنية المخترقين على الحصول على كلمات المرور المحفوظة، التي يمكن استخدامها للتدخلات الأخرى. وليس من المعروف ما إذا كانت أداة كارما مستخدمة إلى الآن. كما قال أحد العناصر السابقين أنه بنهاية سنة 2017 جعلت التحديثات الأمنية لبرامج آبل التي تقدمها شركة آبل أداة كارما أقل فعالية.



أمير قطر الشيخ تميم بن حمد آل ثاني من بين الشخصيات السياسية التي تراقبها الإمارات

في مقابلة لها مع وكالة "رويترز" للأخبار، تحدثت لوري ستراود، إحدى العاملات السابقات في وحدة "Raven" التي كانت تعمل سابقاً في وكالة الأمن القومي الأمريكية، عن الإثارة التي شعرت بها عندما تعرفت على أداة كارما سنة 2016. وقالت ستراود: "لقد شعرنا بالحماس بشأن امتلاك هذه التقنية التي اشتريناها حديثاً بين أيدينا. لقد أمدتنا بقائمة كبيرة من الأهداف التي بحوزتها أجهزة آيفون في ذلك الوقت. لقد كان الأمر شبيها بعيد الميلاد".

يأتي الكشف عن أداة كارما ووحدة Raven وسط سباق محموم في مجال التسليح السيبراني بين متسابقين مثل قطر والمملكة العربية السعودية والإمارات العربية المتحدة، الذين يتنافسون على أدوات القرصنة والموارد البشرية الأكثر تطوراً. ووفقاً للمختصين في الحروب الإلكترونية، بإمكان أداة تجسس مثل "كارما" اختراق المئات من أجهزة الآيفون في وقت واحد وتحديد مواقعها والصور والرسائل المطلوبة بشكل كبير.

في هذا الصدد، قال مايكل دانييل، وهو مسؤول سابق في إدارة الأمن السيبراني في البيت الأبيض في عهد الرئيس أوباما، إنه يعتقد أن 10 دول فقط مثل روسيا والصين والولايات المتحدة وأقرب حلفائها قادرين على تطوير مثل هذه الأسلحة. من جانب آخر، قال باتريك واردل، الباحث السابق في وكالة الأمن القومي وخبير آبل في مجال الأمن، إن أداة كارما وتقنيات التجسس المماثلة جعلت الأجهزة الشخصية مثل آيفون "أكثر الأهداف استقطاباً". وتجدر الإشارة إلى أن المتحدث باسم وزارة الخارجية الإماراتية وشركة آبل رفضا التعليق على هذه المسألة.

خلل في نظام الرسائل الخاص بآبل

قال مطلعون على وحدة Raven إن كارما تسمح للمشغلين بجمع الأدلة على عشرات الأهداف، انطلاقاً من الناشطين المعارضين للحكومة وصولاً إلى المنافسين الإقليميين بما في ذلك قطر والمعارضين الإيديولوجيين للإمارات وحركة الإخوان المسلمين. علاوة على ذلك، سمحت هذه الأداة بإجراء المساومات وحتى الوصول إلى صور جنسية للأشخاص المستهدفين. وقد تم وصف المواد المتحصل عليها بالتفصيل لوكالة "رويترز" لكن المرسلين لم يقوموا بفحصها. وتظن الوكالة أنه ليس هناك أي دليل على أن الإمارات العربية المتحدة قد سربت هذه المواد المتحصل عليها عن طريق كارما.

لقد كان أغلب العاملين في وحدة Raven من قدامى الموظفين في المخابرات الأمريكية، الذين كانوا يتقاضون رواتبهم من خلال إحدى شركات الأمن السيبراني الإماراتية التي تدعى "DarkMatter"، وذلك حسب ما تبينه الوثائق التي استعرضتها "رويترز". ولم تستجب الشركة للعديد من رسائل البريد الإلكتروني والمكالمات الهاتفية للتعليق، كما رفضت وكالة الأمن القومي التعليق على "Project Raven". وقال العاملون السابقون في الوحدة إن حكومة الإمارات اشترت أداة كارما من أحد الوكلاء خارج البلاد. ولم تستطع رويترز تحديد مصدر صنع هذه الأداة.

في الحقيقة، استطاع العاملون السابقون في الوحدة استخدام أداة كارما من خلال إدراج أهداف جديدة كل يوم في نظام لا يحتاج أي معلومات بعد تحديد الهدف. لكن مستخدمي الأداة لم يستطيعوا فهم التفاصيل التقنية المتعلقة بكيفية استغلال ثغرات آبل. وقال أشخاص على دراية بفن التجسس الإلكتروني إن هذا أمر مألوف في وكالة المخابرات، حيث يجهل المشغلون معظم ما يعرفه المهندسون الفعليون للأداة عن كيفية عمل السلاح.

قال ثلاثة موظفين سابقين إنهم فهموا أن كارما تعتمد، جزئياً على الأقل، على خلل موجود في نظام التراسل الخاص بآبل iMessage، الذي يسمح بزراعة البرامج الضارة على الهاتف من خلال iMessage، حتى لو لم يستخدم مالك الهاتف هذا البرنامج؛ مما يمكن المتسللين من إنشاء اتصال مع الأداة. ولا تحتاج أداة كارما إلا لإرسال الرسالة النصية إلى الهدف، ولا يطلب المخترق أي تدخل من جانب المتلقي، ومع ذلك لم يستطع مستخدمو هذه الأداة من تحديد كيفية عمل الثغرة الأمنية.

في الواقع، أكد شخص لديه معرفة مباشرة بصفحة بيع أداة كارما للإماراتيين من وكيل خارجي، حوزته لتفاصيل على قدرتها واستغلالها لثغرة في iMessage. وقد نجح فريق Raven في اختراق حسابات المئات من الشخصيات السياسية البارزة في الشرق الأوسط والناشطين في جميع أنحاء المنطقة، وفي بعض الحالات في أوروبا، وذلك وفقاً لعناصر سابقين في وحدة Raven ووثائق سابقة.

استهداف “المرأة الحديدية” في اليمن

سنة 2017، على سبيل المثال، تم استخدام أداة كارما لاختراق جهاز آيفون تابع لأمير قطر الشيخ تميم بن حمد آل ثاني، بالإضافة إلى أجهزة نائب رئيس الوزراء السابق محمد شيمشيك، ورئيس الشؤون الخارجية العماني يوسف بن علوي بن عبد الله. ولكن لم يتم تحديد المواد التي تم الاستيلاء عليها من أجهزتهم.

خيال هذا الشأن، قال شيمشيك، الذي تنحى عن منصبه في يوليو/ تموز الماضي، لوكالة “رويترز” إن التطفل الإلكتروني على هاتفه كان “مروعاً ومزعجاً للغاية”. في المقابل، لم ترد سفارات واشنطن في قطر وعمان وتركيا على رسائل البريد الإلكتروني والمكالمات المتعددة التي تطلب التعليق على استهداف الشخصيات السياسية في بلدانهم.



تم وضع توكل كرمان، قائدة مظاهرات الربيع العربي في اليمن، تحت المراقبة من قبل الإمارات، وقد تمكنت وحدة Raven من اختراق هاتفها الآيفون سنة 2017.

اخترقت وحدة Raven هاتف توكل كرمان، وهي ناشطة في مجال حقوق الإنسان تُعرف باسم المرأة الحديدية في اليمن. وأبلغت كرمان "رويترز" أنها استهدفت وقالت إنها تعتقد أنها اختيرت بسبب قيادتها لاحتجاجات الربيع العربي التي اندلعت في أنحاء المنطقة سنة 2011 وأدت إلى الإطاحة بالرئيس المصري حسني مبارك.

في سياق متصل، أضافت كرمان أنها تلقت على مدى سنوات إخطارات متكررة من حساباتها على وسائل التواصل الاجتماعي تحذر من أنها تعرضت للقرصنة. قد صُدمت عند معرفة أن الأمريكيين ساعدوا الحكومة الإماراتية في مراقبتها. علاوة على ذلك، قالت توكل كرمان إنه "من المتوقع أن يعمل الأمريكيون على حماية المدافعين عن حقوق الإنسان ويزودوهم بكل وسائل الحماية والأدوات الأمنية، وألا تكون أداة في أيادي الطغاة للتجسس على النشطاء وتمكينهم من قمع شعوبهم".

المصدر: رويترز

رابط المقال : <https://www.noonpost.com/26394/>