داخل فريق الاختراق السري للإمارات العربية المتحدة

كتبه 31 | roetrz يناير ,2019

ترجمة وتحرير نون بوست

كتب جويل شيكتمان وكريستوفر بنج

بعد أسبوعين من تركها منصب محللة استخبارات في وكالة الأمن القومي الأمريكية سنة 2014، كانت لوري ستراود تعمل في الشرق الأوسط مقرصنةً لصالح نظام ملكي عربي. وقد انضمت إلى بروجيكت رافن "Project Raven"، وهو فريق سري يضم أكثر من اثني عشر عميلا سابقا في المخابرات الأمريكية الذين وظفوا لمساعدة دولة الإمارات العربية المتحدة على المشاركة في مراقبة الحكومات الأخرى والميليشيات ونشطاء حقوق الإنسان الذين ينتقدون المملكة.

تستخدم ستراود وفريقها، الذي يعمل في قصر في أبوظبي يعرف باسم "الفيلا"، الأساليب التي تعلموها بعد عملهم لعقد من الزمن في مجتمع الاستخبارات في الولايات المتحدة، لمساعدة دولة الإمارات العربية المتحدة في اختراق الهواتف وأجهزة الكمبيوتر الخاصة بأعدائها.

في الواقع، عينت ستراود من قبل مقاول الأمن السيبراني في ولاية ماريلاند لمساعدة الإماراتيين على

إطلاق عمليات القرصنة. وخلال ثلاث سنوات، قدمت مردودا مبهرا في العمل. لكن سنة 2016، نقل الإماراتيون مشروع Raven إلى شركة أمن إلكتروني في الإمارات العربية المتحدة تدعى DarkMatter. وقبل فترة طويلة، قالت ستراود وغيرها من الأمريكيين المشاركين في هذا العمل إنهم رأوا المهمة تتجاوز الخطوط الحمراء؛ حيث استهدفت مواطنين أمريكيين لمراقبتهم.

وفي هذا الشأن قالت ستراود لرويترز "أعمل في وكالة استخبارات أجنبية تستهدف أشخاصا أمريكيين. أنا رسميا أمثل النوع السيء من الجواسيس". في الحقيقة، تكشف قصة "Project Raven" كيفية استخدام قراصنة الحكومة الأمريكية السابقين أحدث أدوات التجسس الإلكتروني نيابة عن خدمة استخبارات أجنبية تتجسس على نشطاء حقوق الإنسان والصحفيين والمنافسين السياسيين.

تظهر المقابلات مع تسعة من عملاء سابقين في Raven، بالإضافة إلى استعراض لآلاف الصفحات من وثائق المشاريع ورسائل البريد الإلكتروني، أن تقنيات المراقبة التي تدرسها وكالة الأمن القومي كانت أساسية في جهود الإمارات لرصد المعارضين. والجدير بالذكر أن المصادر التي قابلتهم وكالة رويترز لم يكونوا مواطنين إماراتيين.

بعد أن تركت لوري ستراود وظيفتها في وكالة الأمن القومي في عام 2014، أصبحت عميلة استخباراتية في دولة الإمارات العربية المتحدة. وقالت ستراود التي تعيش الآن في مكان غير معلوم في الولايات المتحدة إن البعثة تجاوزت الخطوط الحمراء عندما علمت أن وحدتها كانت تتجسس على الأمريكيين.

استخدم النشطاء ترسانة من الأدوات السيبرانية، بما في ذلك منصة تجسس متطورة تعرف باسم

كارما، حيث يقول موظفو Raven إنهم اخترقوا أجهزة آيفون المئات من النشطاء والزعماء السياسيين والإرهابيين المشتبه بهم. والجدير بالذكر أنه تم التطرق لموضوع الاختراق بواسطة أداة كارما في تقرير منفصل لوكالة رويترز اليوم.

في الحقيقة، رفض المتحدث باسم وكالة الأمن القومي والمتحدثة باسم شركة أبل والمتحدثة باسم وزارة الخارجية الإماراتية التعليق على موضوع "Raven". كما لم تستجب سفارة الإمارات العربية المتحدة في واشنطن والمتحدث باسم المجلس الوطني للإعلام لطلبات التعليق.

وقالت الإمارات العربية المتحدة إنها تواجه تهديدًا حقيقيًا من الجماعات المتطرفة وأنها تتعاون مع الولايات المتحدة لمكافحة الإرهاب. ويقول العاملون السابقون في "Raven" إن المشروع ساعد نسبيا في تفكيك شبكة تنظيم الدولة داخل الإمارات. فعندما قام أحد أفراد جماعة تنظيم الدولة بطعن أحد المعلمين في أبوظبي سنة 2015، يقول العاملون إن Raven قاد جهود الإمارات لتقييم ما إذا كانت هناك هجمات أخرى وشيكة.

سلطت تقارير مختلفة الضوء على سباق التسلح الإلكتروني الجاري في الشرق الأوسط، حيث تحاول الإمارات ودول أخرى أن تظفر بأسلحة التجسس والموظفين ذوي الكفاءات بشكل أسرع من منافسيها. ويعد التحقيق الذي تجريه رويترز أول من كشف عن وجود Raven، كما يوثق عمليات القرصنة التي تنفذها الدولة، والتي عادة ما تكون في كنف السرية وغير معترف بها أو غير معلن عنها.

توفر قصة Raven أيضًا نظرة جديدة حول الدور الذي تلعبه الدوائر الأمريكية السابقة في عمليات القرصنة الأجنبية. وداخل مجتمع الاستخبارات الأمريكية، يرى البعض أن العمل في خطة عميل في بلد آخر هو خيانة. وفي هذا الصدد، يقول بوب أندرسون، الذي عمل في منصب مدير تنفيذي لمدير مكتب التحقيقات الفدرالي حتى سنة 2015: "هناك التزام أخلاقي إذا كنت ضابط استخبارات سابق حيال التحول إلى أحد المرتزقة الفعليين لحكومة أجنبية".

وبينما يثير هذا النشاط معضلات أخلاقية، يقول محامو الأمن القومي الأمريكيون إن القوانين التي تتصدى لما يمكن أن يفعله مقاولو الاستخبارات الأمريكية في الخارج غامضة. وعلى الرغم من أنه من غير القانوني مشاركة المعلومات السرية، لا يوجد قانون محدد يحظر على المتعاقدين مشاركة معلومات عامة، مثل كيفية استهداف هدف باستخدام بريد إلكتروني محمّل بالفيروس.

ومع ذلك، فإن القواعد واضحة فيما يخص اختراق شبكات الولايات المتحدة أو التنصت على اتصالات الأمريكيين. وفي هذا الشأن قالت ريا سيرز، نائب مدير مساعد لشؤون السياسة في وكالة الأمن القومي، إن "الأمر غير قانوني للغاية".

كان اختراق الأميركيين سريا ومحكمًا حتى داخل Raven، خاصة مع تلك العمليات التي يقودها الإماراتيون. لكن تم تأكيد تقرير ستراود المتعلق باستهداف الأمريكيين من قبل أربعة عملاء سابقين آخرين وفي رسائل البريد الإلكتروني التي استعرضتها رويترز.

في الوقت الحالي، يقوم مكتب التحقيقات الفيدرالي بالتحقيق في ما إذا كان موظفو Raven

الأمريكيين قد سربوا تقنيات مراقبة أمريكية سرية، وإذا كانوا يستهدفون شبكات الكمبيوتر الأمريكية بشكل غير قانوني، وذلك وفقًا لموظفي Raven السابقين الذين قابلهم وكلاء إنفاذ القانون الفيدراليين. وحيال هذا الشأن قالت ستراود إنها تتعاون مع هذا التحقيق. ولم يتم تقديم أي اتهامات، ولا يمكن أن يظهر أي شيء من التحقيق. وقد رفضت المتحدثة باسم مكتب التحقيقات الفيدرالي التعليق.

البيان الأرجواني والبيان الأسود

في الواقع، تعد ستراود العاملة الوحيدة في Raven التي ترغب في ذكر اسمها في هذه القصة. وهناك ثماني عاملين آخرين تحدثوا عن تجاربهم ولكن بشرط عدم الكشف عن هويتهم. أمضت ستراود عقدًا في وكالة الأمن القومي؛ أولًا كعضو في الخدمة العسكرية من سنة 2003 إلى سنة 2009، وفي وقت لاحق كمتعهدة في الوكالة لمستشار التكنولوجيا العملاق بوز ألن هاملتون من سنة 2009 إلى سنة 2014. وكان اختصاصها يشمل البحث عن نقاط الضعف في أنظمة الكمبيوتر في الحكومات الأجنبية، مثل الصين، وتحليل البيانات التي ينبغي سرقتها.

خلال سنة 2013، تغيّر عالمها، حيث قالت ستراود إنه أثناء إقامتها في وكالة الأمن القومي في هاواي اتخذت قرارا مصيريا بإحضار فني لدى "ديل" الذي عمل في"الفيلا" لفريقها. كان هذا المقاول يدعى إدوارد سنودن.

وفي هذا الشأن تقول ستراود البالغة من العمر 37 سنة "كان سنودن عاملا سابقا لدى وكالة المخابرات المركزية، إنه شخص نظيف ومعروف". ومن ثم أضافت "كان شخصا مثاليا". وستقوم وكالة الأمن القومي وبوز ألن هاملتون بقبوله مما يخول له الوصول لأكثر المواد سرية.

بعد شهرين من انضمامه إلى مجموعة ستراود، هرب سنودن من الولايات المتحدة ونقل آلاف الصفحات من ملفات البرامج السرية إلى الصحفيين، موضحًا بالتفصيل برامج جمع البيانات الضخمة للوكالة. وفي حالة الغليان التي أعقبت ذلك، قالت ستراود إنه تم تشويه سمعة فريقها عن غير قصد لإتاحة أكبر اختراق أمني في تاريخ الوكالة. وفي هذا الشأن قالت "لقد تم تدمير سمعتنا".

تعرضت وكالة الأمن القومي للنقد بعد أن اتخذوا قرارا مصيريا خلال سنة 2013. بعد أشهر قليلة من توصية ستراود له بالعمل، سرب سنودن أسرار الأمن القومي للولايات المتحدة.

في أعقاب الفضيحة، عرض مارك باير، وهو زميل سابق في وكالة الأمن القومي في هاواي، على ستراود فرصة العمل لدى مقاول أمن سيبراني في أبوظبي يدعى سايبر بوينت. وفي أيار/ مايو 2014، اقتنصت ستراود هذه الفرصة وغادرت بوز ألن.

تأسس سايبر بوينت، وهو مقاول صغير للأمن السيبراني ومقره بالتيمور، من قبل رجل أعمال يدعى كارل غامتو خلال سنة 2009. وقد ضمت قائمة عملائه وزارة الدفاع الأمريكية، وحظيت أعمالها في الإمارات باهتمام إعلامي. وفي مقابلة أجريت معه، قال غامتو إن شركته لم تشارك في أي أعمال غير لائقة.

تحولت ستراود من موظفة حكومية إلى متعهدة لدى بوز وتقريبا بقيت مهامها هي ذاتها ولكن مع أجر أعلى. إن الحصول على وظيفة لدى سايبر بوينت لن يؤدي فقط إلى تحقيق حلم دائم بالانتشار في الشرق الأوسط وإنما في الحصول على راتب أعلى. ولقد تلقى العديد من المحللين، مثل ستراود، أجوراً تزيد على 200 ألف دولار سنوياً، وتلقى بعض المديرين رواتب وتعويضات تزيد على 400 ألف دولار.

لقد أدركت ستراود أن وظيفتها الجديدة ستنطوي على مهمة لمكافحة الإرهاب بالتعاون مع الإماراتيين، وهي حليف وثيق للولايات المتحدة في الحرب ضد تنظيم الدولة، ولكن هناك القليل من الأمور الأخرى التي سيكون عليها القيام بها.

ووفقا لستراود، أكد لها باير وبعض العاملين الآخرين في Raven أن جهاز الأمن القومي وافق على المشروع. مع السيرة الذاتية المثيرة للانتباه لباير، بما في ذلك إمضاء بعض الوقت في وحدة النخبة للقرصنة التابعة لجهاز الأمن القومي، كانت عملية الإقناع سهلة. تجدر الإشارة إلى أن باير لم يستجب للمكالمات الهاتفية المتعددة والرسائل النصية ورسائل البريد الإلكتروني والرسائل على وسائل التواصل الاجتماعي.

في عالم الاستخبارات المجزء والسري للغاية، ليس من غير المعتاد أن يحافظ الموظفون على المهمة وعميل من الموظفين المحتملين حتى يوقعوا على مستندات المحافظة على السرية والمرور بعملية إحاطة.

عندما جلبت ستراود إلى "فيلا" للمرة الأولى، في أيار/ مايو سنة 2014، مدتها إدارة Raven ببيانين منفصلتين متتاليتين. في البيان الأول، الذي عرف باسم "البيان الأرجواني" كشفت أنه قيل لها إن Raven سيقوم بمهمة دفاعية بحتة لحماية حكومة دولة الإمارات من المتسللين والتهديدات الأخرى. وبعد انتهاء الجلسة الإعلامية مباشرة، أكدت أنها أعلمت بأن تلك القصة كانت وهمية.

ومن ثم تلقت "البيان الأسود"، الذي اطلعت عليه رويترز. والذي جاء فيه أن "Raven" هو "الفرقة الهجومية والتشغيلية لهيئة الأمن الإلكتروني الوطنية ولن يتم الكشف عنها لعامة الناس". وبهذا الشكل، كانت هيئة الأمن الإلكتروني الوطنية، النسخة الإماراتية من جهاز الأمن القومي.

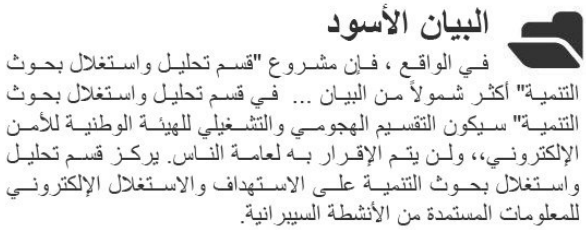
ستكون ستراود جزءًا من فريق Raven للتحليل والتطوير المستهدف، الذي يعمل على مساعدة الحكومة على التعرف على أعدائها عبر الإنترنت، واختراقهم، وجمع البيانات. وقد تم تقديم تلك الأهداف من قبل العميل، الهيئة الوطنية للأمن الإلكتروني، الذي يسمى الآن وكالة استخبارات الإشارات. وقالت ستراود إن لغة وسرية البيانات تعكسان عن كثب تجربتها في وكالة الأمن القومي، مما أعطاها إحساسا بالراحة.

كانت المعلومات التي حصل عليها Raven تغذي جهازًا أمنيًا أثار انتقادات دولية. وتجدر الإشارة هنا إلى أن الإمارات، وهي اتحاد غني يضم سبع إمارات يبلغ عدد سكانها تسع ملايين نسمة، حليف للجارة السعودية ومنافس لإيران.

الأرجواني والأسود

يتم تقديم البيانات باللونين الأرجواني والأسود بالتعاقب عند انضمام عملاء جدد إلى Raven في أبوظبي. وكان البيان الأول يستخدم بمثابة قصة تغطية إذا سئل عملاء عن العملية من قبل آخرين في الشركة المتعاقدة أو موظفي حكومة دولة الإمارات العربية المتحدة الذين ليس لديهم تصريح أمني لمعرفة الغرض الحقيقي من Raven.

وعموما، يعد قسم تحليل واستغلال بحوث التنمية الاسم الذي كانت الإمارات تملكه لمشروع Project Raven.



اتُهمت الإمارات العربية المتحدة بقمع حرية التعبير، واحتجاز المعارضين وغيرهم من الانتهاكات من قبل منظمات مثل هيومن رايتس ووتش. وتعليقا على ذلك، تقول الإمارات إنها تعمل عن كثب مع واشنطن لمحاربة التطرف "ما وراء ساحة المعركة" وتشجع الجهود المبذولة لمواجهة "الأسباب الجذرية" للعنف الراديكالي.

وقالت ستراود وثمانية آخرين من العاملين السابقين في Raven إن أهداف Raven ستشمل في نهاية المطاف المتشددين في اليمن والأعداء الأجانب مثل إيران وقطر وتركيا والأفراد الذين ينتقدون النظام الملكي. وقد تم التأكد من حساباتهم من خلال المئات من وثائق برنامج Raven التي استعرضتها رويترز.

وبموجب أوامر من حكومة الإمارات العربية المتحدة، قال نشطاء سابقون إن Raven سيراقب وسائل التواصل الاجتماعي ويستهدف الأشخاص الذين شعرت قوات الأمن أنهم أهانوا الحكومة. كما أضافت ستراود: "كان من الصعب المرور ببعض الأيام، مثلا عندما نستهدف طفلًا يبلغ من العمر 16 عامًا على تويتر. ولكن هذه مهمة استخباراتية، فأنت أحد عملاء المخابرات. أنا لم أقم بالتعامل مع الأمور بطريقة شخصية".

وقال الموظفون السابقون في شركة Raven إن الأمريكيين حددوا نقاط الضعف في أهداف مختارة أو طوروا أو اشتروا برمجيات لتنفيذ التدخلات وساعدوا في رصدها. ولكن، عادة ما يضغط أحد المشغلين الإماراتيين على الزر في أي هجوم. كان هذا الترتيب يهدف إلى إعطاء الأمريكيين "إنكارا" لطبيعة العمل، كما قال أعضاء سابقون في Raven.

استهداف جيرو وإيغرت

اكتشف ستراود أن البرنامج لم يكن يستهدف فقط الإرهابيين والوكالات الحكومية الأجنبية، ولكن أيضا المنشقين ونشطاء حقوق الإنسان الذين صنفهم الإماراتيون كأهداف أمنية وطنية. وفي أعقاب احتجاجات الربيع العربي والإطاحة بالرئيس المصري حسني مبارك سنة 2011، اعتبرت قوات الأمن الإماراتية أن المدافعين عن حقوق الإنسان يشكلون خطراً رئيسياً على "الاستقرار الوطني"، كما تظهر السجلات والمقابلات.

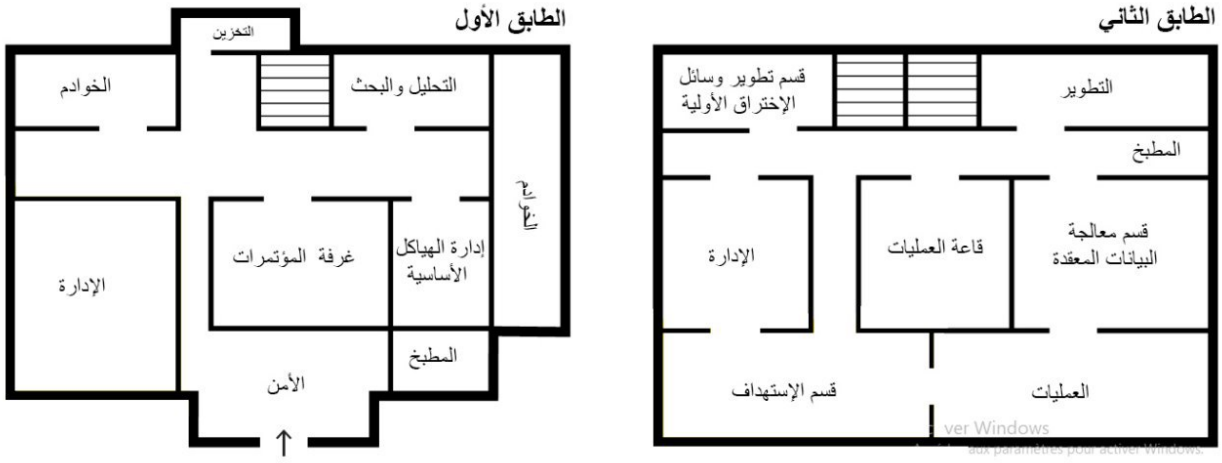
وفقا لعناصر ووثائق برنامج Raven السابقة، كان أحد الأهداف الرئيسية للبرنامج سنة 2012 هو روري دوناغي. كان دوناغي، البالغ من العمر 25 عامًا، صحفيًا وناشطًا بريطانيًا كتب مقالات تنتقد

سجل البلاد في مجال حقوق الإنسان. وخلال سنة 2012، كتب مقال رأي لصحيفة الغارديان ينتقد فيها القمع النشط لحكومة الإمارات العربية المتحدة ويحذر من أنه في حالة استمراره، فإن "من في السلطة يواجهون مستقبلاً مجهولاً".

قبل سنة2012، قال العاملون السابقون إن عملية جمع المعلومات في الإمارات العربية المتحدة قد اعتمدت إلى حد كبير على عملاء إماراتيين اقتحموا منازل الأهداف أثناء غيابهم ووضعوا برامج تجسس على أجهزة الكمبيوتر. ولكن مع قيام الأمريكيين بتأسيس Raven، فإن قرصنة دوناغي عن بعد قدمت للمقاولين فوزًا يمكنهم تقديمه إلى العميل.

داخل "الفيلا"

عمل العشرات من الموظفين الإماراتيين ومقاولي الأمن السيبراني الأميركيين في مشروع Project Raven، الذي كان مقره قصرا في أبوظبي. وتم تقسيم النشطاء إلى فرق تدعم كل منها مهمة اختراق الأهداف التي اختارتها قوات الأمن الإماراتية. وتطورت هذه العملية من قبل عملاء أمريكيين لديهم خلفية عميقة في الاستخبارات الأمريكية.



بسبب الحساسية من انتهاكات حقوق الإنسان وحرية الصحافة في الغرب، كانت العملية ضد ناشط صحافي بمثابة مقامرة. وجاء في وثائق برنامج سنة 2012 "إن المخاطر المحتملة على حكومة الإمارات العربية المتحدة والعلاقات الدبلوماسية مع القوى الغربية كبيرة إذا كان يمكن إرجاع العملية إلى الإمارات العربية المتحدة".

وقال أحد المرتزقة السيبرانيين: "من أجل الاقتراب من دوناغي، يجب على أحد عناصر Raven محاولة التقرب من الهدف من خلال تبني معتقدات مماثلة". كانوا يعتقدون أن دوناغي "غير قادر على مقاومة فكرة من هذا النوع".

وبصفته ناشطًا في مجال حقوق الإنسان، بعث عملاء Raven بالبريد الإلكتروني إلى دوناغي طالبين مساعدته "لجلب الأمل لأولئك الذين يعانون منذ مدة طويلة". وذلك مثل ما جاء في رسالة البريد الإلكتروني.

أقنع الناشط دوناغي بتنزيل البرامج التي ادعى أنها ستجعل الرسائل "صعبة التتبع". في الواقع، سمحت البرمجيات الخبيثة للإماراتيين بمراقبة حساب البريد الإلكتروني الخاص بدوناغي وتتبع عملية تصفحه للإنترنت باستمرار. وقالت ستراود إن مراقبة دوناغي، الذي حصل على الاسم الرمزي جيرو، استمرت في ظل ستراود وظلت أولوية قصوى بالنسبة إلى الإمارات لسنوات.

في نهاية المطاف، علم دوناغي أن بريده الإلكتروني قد تعرض للاختراق. وخلال سنة 2015، بعد تلقيه بريدًا إلكترونيًا آخر مريبًا، اتصل بباحث أمني في سيتيزن لاب، وهي مجموعة كندية متخصصة في حقوق الإنسان والخصوصية الرقمية، واكتشف أن المخترقين كانوا يحاولون لسنوات اختراق جهاز الكمبيوتر الخاص به.

ولدى الاتصال به عبر الهاتف من لندن، فإن دوناغي، الذي أصبح الآن طالبا في تخصص الدراسات العربية، عبر عن استغرابه من أنه كان يعتبر هدفا رئيسيا للأمن القومي على مدى خمس سنوات. وأكد دوناغي أنه تعرض للاستهداف باعتماد التقنيات التي تم وصفها في الوثائق.

وقال دوناغي: "أنا سعيد لأن شريكتي تجلس هنا بينما أنا أتحدث عبر الهاتف، لأنها لم تكن تصدق ذلك. ولدى إخباره بأن القراصنة كانوا مرتزقة أمريكيين يعملون لحساب الإمارات العربية المتحدة، فإن دوناغي الذي يحمل الجنسية البريطانية عبر عن استغرابه وامتعاضه من هذا الأمر وقال: "إن هذا بمثابة خيانة للرابط الذي يجمعنا."

أما ستراود فقد قالت إن الخلفية التي تأتي منها باعتبارها موظفة استخبارات جعلتها لا تنزعج من استهداف نشطاء حقوق الإنسان، طالما كانوا من غير الأمريكيين. حيث قالت: "نحن نعمل لحساب حكومة هذه البلاد، وهم لديهم أهداف استخباراتية محددة تختلف عن أهداف الولايات المتحدة، وهذا أمر مفهوم ونحن فقط نتعايش معه."

ويشار إلى أن الناشط الإماراتي المعروف أحمد منصور الذي أطلق عليه الإسم المشفر إيجرت (طائر البلشون)، كان هو أيضا هدفا آخر، بحسب ما أكده موظفون سابقون في فريق Raven. وعلى مدى سنوات، كان منصور ينتقد علنا الحرب التي تخوضها بلاده في اليمن، ومعاملة العمال المهاجرين واعتقال المعارضين السياسيين.

وفي أيلول/ سبتمبر 2013، عرض فريق Raven على مسؤولي الهيئة الوطنية للأمن الإلكتروني في الإمارات مواد تم أخذها من جهاز كمبيوتر منصور، وافتخروا بنجاحهم في جمع أدلة ضده. وقد تضمنت هذه المواد صورا تحتوي على مراسلات بريد إلكتروني ناقش فيها منصور مظاهرة قادمة ستتم أمام مقر المحكمة الفدرالية العليا في الإمارات، يحضرها أعضاء عائلات المعارضين المسجونين.

كما قال فريق Raven للأجهزة الأمنية الإماراتية أن منصور قام بتصوير محتجز زاره في سجنه، وهو ما يتعارض مع قوانين السجون، ثم حاول الفريق تدمير هذا الدليل الموجود على جهاز كمبيوتر منصور، وذلك بحسب عرض باستخدام برمجية باور بوينت اطلعت عليه وكالة رويترز.

تحت المراقبة: روري دوناغي على اليسار وأحمد منصور على اليمين كان يتم استهدافهما بشكل متواصل لمدة سنوات، من قبل موظفي الاستخبارات الأمريكية العاملين لحساب الإمارات.

وقد نشر مشروع سيتيزن لاب بحثا في 2016 يظهر فيه أن منصور ودوناغي كانا قد استهدفا على يد قراصنة، وقد رجحت تلك الأبحاث أن تكون الحكومة الإماراتية هي التي تقف وراء هذه العمليات. إلا أن الأدلة الملموسة حول المسؤول عن ذلك، والتفاصيل بشأن استخدام عملاء أمريكيين، وروايات الشهود العيان حول فريق القرصنة، كلها تنشر هنا لأول مرة.

ويشار إلى أن منصور تمت إدانته في محاكمة سرية في 2017 بتهمة المس من وحدة البلاد وتم الحكم عليه بالسجن عشر سنوات. وهو الآن يقبع في السجن الانفرادي، وقد تدهورت صحته بحسب ما أكده شخص مطلع على هذه المسألة.

أما زوجة منصور، وهي نادية، فهي تعيش في عزلة اجتماعية في أبوظبي. وجيرانها يتحاشون التواصل معها خوفا من مراقبة الأجهزة الأمنية. ويبدو أن هؤلاء كانوا على حق، إذ أنه بحلول حزيران/ يونيو 2017 كان فريق Raven قد تمكن من التسلل إلى هاتفها الجوال وقد أطلق عليه الإسم السري بيربل اغريت، (طائر البلشون البنفسجي)، بحسب وثائق البرنامج التي اطلعت عليها وكالة رويترز.

وللقيام بهذا الأمر، اعتمد فريق Raven على أداة اختراق جديدة وقوية تسمى كارما، وهي التي مكنت الموظفين من اختراق هواتف أيفون بعض المستخدمين في أنحاء العالم.

كما مكنت كارما أعضاء فريق Raven من الحصول على عناوين بريد إلكتروني، ومواقع ورسائل قصيرة وصور من أجهزة أيفون، وتم ذلك بكل بساطة عبر تحميل قوائم أرقام هؤلاء الأشخاص إلى

برمجيات معدة سلفا، وذلك بحسب ما أكده خمس موظفين سابقين في هذا المشروع. إلا أن رويترز لم تتمكن من التواصل مع زوجة منصور.

وكانت برمجية كارما قوية إلى درجة كبيرة، لأنها لم تكن تحتاج لأن يقوم الضحية المستهدف بالضغط على أي رابط أو تنزيل أي برمجية خبيثة. وقد فهم الموظفون أن هذه الأداة تعتمد على ثغرة سرية في برمجية "أي مساج" للرسائل القصيرة من شركة أبل.

وفي سنتي 2016 و2017، تم استخدام كارما ضد المئات من الأهداف في أنحاء الشرق الأوسط وأوروبا، من بينهم حكومات قطر واليمن وإيران وتركيا، بحسب ما أظهرته الوثائق. وقد استخدم فريق Raven برمجية كارما لاختراق جهاز أيفون يستخدمه أمير قطر، الشيخ تميم بن حمد آل ثاني، إلى جانب أجهزة مساعدين مقربين وشقيقه.

هذا ونشير إلى أن سفارة قطر في واشنطن لم تستجب لطلبنا للتعليق على هذا الأمر.

ما الذي كانت واشنطن تعرفه؟

يعتقد الموظفون السابقون في فريق Raven أنهم كانوا في الجانب الصحيح من القانون، لأنهم بحسب تأكيداتهم أخبرهم رؤسائهم المشرفون بأن هذه المهمة تحظى بدعم الحكومة الأمريكية.

رغم أن وكالة الأمن القومي لم تكن تتدخل في السير اليومي للعمليات، فإن الوكالة وافقت على هذا الأمر وكان يتم إطلاعها بشكل دوري على أنشطة فريق Raven، وهو ما أخبر به باير أعضاء الفريق، بحسب تأكيدهم.

إلا أن غامتو، مؤسس شركة سايبر بوينت للسلامة المعلوماتية، قال إن شركته لم تكن على علاقة بعمليات الاختراق، حيث قال غامتو في حوار معه عبر الهاتف: " لم نكن نقوم بعمليات هجومية. وإذا كان هنالك شخص يقوم بتصرف مارق، فإنه يؤلمني أن أفكر في أنه قام بهذا الأمر تحت راية شركتنا."

وعوضا عن ذلك، قال غامتو إن الشركة قامت بتدريب إماراتيين على الدفاع عن أنفسهم من خلال برنامج تم بالاتفاق مع وزير الداخلية الإماراتي. كما أن نظرة على الوثائق الداخلية لفريق Raven تظهر أن وصف غامتو للبرنامج على أنه "تقديم الاستشارات لوزير الداخلية حول الدفاع السيبراني"، تتطابق تماما مع القصة المظللة التي تم تلقينها لموظفي فريق Raven لتقديمها عندما يتم سؤالهم عن المشروع. كما تم إخبار موظفي Raven بأن يقولوا إنهم عملوا لفائدة مكتب تكنولوجيا المعلومات والعمل المشترك، بحسب ما هو مذكور في وثائق البرنامج.

المحاربون السيبرانيون في الولايات المتحدة: قبل الإنضمام لمشروع Raven في الإمارات، فإن الكثيرين من الموظفين عملوا مع وكالة الأمن القومي الأمريكية. وفي الصورة يظهر مقرها في فورت ميد في ماري لاند.

ويشار إلى أن تقديم معلومات دفاعية حساسة أو خدمات لحكومة أجنبية يتطلب في العادة تراخيص خاصة من وزارتي التجارة والخارجية. وكلا الوزارتين رفضتا التعليق على ما إذا كانت قد أصدرتا تراخيص من هذا النوع لشركة سايبر بوينت لعملياتها في الإمارات. كما أكدت الوزارتان أن مبادئ حقوق الإنسان تكون دائما منصوص عليها في مثل هذه التصاريح.

إلا أن اتفاقا مع سايبر بوينت تم توقيعه مع وزارة الخارجية في 2014 أظهر أن واشنطن فهمت أن المتعاقدين كانوا يساعدون على إطلاق عمليات مراقبة سيبرانية لفائدة الإمارات. وقد أوضحت وثائق الموافقة أن عقد سايبر بوينت ينص على العمل إلى جانب الهيئة الوطنية للأمن الإلكتروني، بغرض "حماية سيادة الإمارات عبر جمع المعلومات من أنظمة الاتصالات داخل وخارج الإمارات، وتحليل بيانات المراقبة."

وتنص إحدى الفقرات، في وثيقة موافقة وزارة الخارجية، على أن شركة سايبر بوينت ملزمة بالحصول على تصريح خاص من وكالة الأمن القومي قبل تقديم أي عروض توضيحية تتعلق باستغلال ومهاجمة شبكات الكمبيوتر. وقد حددت وكالة رويترز العشرات من هذه العروض التوضيحية التي قدمها فريق Raven للهيئة الوطنية للأمن الإلكتروني، وهي تصف عمليات ضد دوناغي ومنصور وآخرين. ومن غير الواضح ما إذا كانت وكالة الأمن القومي قد وافقت على عمليات رايفين ضد أهداف محددة.

وقد شدد الاتفاق على منع موظفي سايبر بوينت من استهداف مواطنين أو شركات أمريكية. وكجزء من الاتفاق، فقد تعهدت شركة سايبر بوينت بأن موظفيها وحتى الموظفين الإماراتيين الذين يعملون في المشروع لن يتم استخدامهم لاستغلال أشخاص أمريكيين (على سبيل المثال مواطنين أمريكيين، أوأجانب حاصلين على الإقامة الدائمة، أو شركات أمريكية) كما يمنع الإفصاح عن المعلومات المصنفة بأنها حصرية لدى الولايات المتحدة، والتكنولوجيات التي هي ملك للجيش، أو طرق الوكالات الاستخباراتية الأمريكية في جمع المعلومات كلها كانت ممنوعة.

وقد رفض غامتو مناقشة تفاصيل الاتفاق، وقال: "أفضل ما يمكنني فعله، وأقصى ما أعرفه، هو أننا قمنا بكل شيء كما هو مطلوب عندما تعلق الأمر بالقوانين والنظم الأمريكية. وقد وفرنا آليات للناس لكي يتوجهوا إلي مباشرة إذا شعروا بأن هنالك شيء يتم بشكل خاطئ" .

ونشير إلى أن المتحدث باسم وكالة الأمن القومي الأمريكية رفض التعليق على مشروع Raven. كما أن متحدثا باسم وزارة الخارجية رفض التعليق على هذا الاتفاق، إلا أنه قال إن مثل هذه التراخيص لا تسمح للناس بالتورط في انتهاكات لحقوق الإنسان.

وبحلول أواخر العام 2015، فإن بعض موظفي Raven قالوا إن مهماتهم أصبحت أكثر جرئة. على سبيل المثال، فإنهم عوضا عن أن يطلبوا منهم اختراق حسابات مستخدمين في منتدى إسلامي على الانترنت، كما كان الأمر سابقا، فإن هؤلاء المتعاقدين الأمريكيين طلب منهم صنع فيروسات كمبيوتر يمكنها إصابة كل شخص يزور ذلك الموقع الذي تم تحديده. مثل هذه العمليات الجماعية والعشوائية تهدد باكتساح الاتصالات بين المواطنين الأمريكيين، وهو ما يمثل تجاوزا للخطوط الحمراء، وهو أمر كان يعرفه هؤلاء جيدا منذ أيام عملهم في وكالة الأمن القومي.

يمنع أن القانون الأمريكي بشكل عام وكالة الأمن القومي ووكالة الاستخبارات المركزية، وبقية الوكالات الاستخبارتية من مراقبة المواطنين الأمريكيين. ومن خلال العمل مع المدراء، فإن ستراود ساهمت في وضع سياسة تحدد ما يجب فعله عندما يتمكن فريق رايفين من اختراق بيانات شخصية تعود لمواطنين أمريكيين. حيث أن الموظفين السابقين في وكالة الأمن القومي تمت توصيتهم بوضع تلك المواد ضمن الأشياء التي يجب حذفها. كما يتم أيضا إبلاغ موظفين آخرين في مشروع Raven حتى يتم إخراج أولئك الضحايا الأمريكيين من أي قوائم مستقبلية للمستهدفين.

ومع مرور الوقت، فقد لاحظت ستراود أن بيانات الأمريكيين التي تم وضعها ضمن قائمة الأشياء التي يجب حذفها كانت تظهر مرة بعد أخرى في قواعد البيانات التابعة للهيئة الوطنية للأمن الإلكتروني الإماراتية.

ورغم ذلك، فإن ستراود اعتبرت أن هذا العمل ممتع بالنسبة لها حيث تقول: "لقد كان أمرا لا يصدق لأنه لم تكن هنالك أي ضوابط مثلما كان عليه الأمر في وكالة الأمن القومي. لم تكن هنالك أشياء مزعجة مثل الشريط الأحمر، وكنت أشعر بأنني قمت بالكثير من العمل الجيد في مكافحة الإرهاب."

عندما تم تأسيس فريق Raven في 2009، كانت أبوظبي تتمتع بخبرة قليلة في المجال المعلوماتي. والفكرة الأصلية كانت تتمثل في الاعتماد على أمريكيين لتطوير وإدارة البرنامج لمدة خمس أو عشر سنوات إلى أن يتمكن موظفو الاستخبارات الإماراتية من اكتساب المهارات اللازمة لتولي الأمور، وذلك بحسب ما تظهره الوثائق

وبحلول العام 2013، كان عدد عناصر الفيلق الأمريكي الموجود في المهمة رايفين يتراوح بين 10 و20 شخصا، أي أنه أصبح يمثل الغالبية في عدد الموظفين في البرنامج.

وفي أواخر العام 2015، شهدت الفيلا (موقع إدارة العمليات) انتقالا في السيطرة بعد أن أصبح الإماراتيون أكثر انزعاجا من سيطرة الأجانب على برنامج للأمن القومي يخص بلادهم، بحسب ما ذكره موظف سابق. وقد أخبر مسؤولو وزارة الدفاع الإماراتية غامتو بأنهم أرادوا أن تتم إدارة مشروع Raven من قبل شركة محلية، تسمى DarkMatter.

وقد تم منح خيارين للأمريكيين المؤسسين لمشروع Raven: وهما الالتحاق بشركة DarkMatter أو التوجه للعودة نحو بلادهم.

قوة صاعدة: بعد سلسلة من الانتفاضات الشعبية التي هزت المنطقة في 2011، اتخذت الحكومة الإماراتية خطوات لتشديد المراقبة. وكان الهدف من إنشاء وكالة جديدة، وهي الهيئة الوطنية للأمن الإلكتروني كان يهدف لمساعدة النظام الحاكم على مراقبة التهديدات.

وقد غادر ما لا يقل عن ثمانية موظفين مشروع Raven خلال تلك الفترة الإنتقالية. وبعضهم قالوا أنهم غادروا بعد أن شعروا بعدم الإرتياح حيال التفسيرات الغامضة التي قدمها مدراء مشروع Raven عندما تم الضغط عليهم للقيام بعمليات مراقبة ضد أمريكيين آخرين.

وقد تم تأسيس شركة DarkMatter في 2014 على يد فيصل البنّاي الذي أسس أيضا أكسيوم، وهي واحدة من أكبر الشركات التي تبيع أجهزة الهاتف في المنطقة. وتقوم شركة DarkMatter بتعريف نفسها على أنها مطور ومجدد في مجال تكنولوجيا الدفاع السيبراني.

وقد ذكر تقرير لموقع انترسيبت في 2016 أن الشركة ساعدت الأجهزة الأمنية في الإمارات في عمليات مراقبة، وكانت تسعى لتوظيف خبراء أجانب في المجال السيبراني.

هذه الشركة الإماراتية التي تضم أكثر من 650 موظفا، تقر بشكل علني علاقتها التجارية المقربة من الحكومة الإماراتية، ولكنها تنفي أي تورط لها في جهود حكومية للقيام بعمليات اختراق. وقد تمت المحافظة على سرية الهدف الحقيقي من مشروع Raven وإخفائه على أغلب المدراء في شركة DarkMatter، بحسب ما قاله موظفون سابقون.

ويشار إلى أن شركة DarkMatter لم تستجب عن طلباتنا للتعليق. أما البناي وكريم صباغ، المدير الحالي للشركة، فإنهم رفضوا طلبنا للقيام بلقاءات معهم. كما أن المتحدثة باسم وزارة الشؤون الخارجية الإماراتية رفضت التعليق.

وتحت مظلة شركة DarkMatter واصل فريق Raven النشاط في أبوظبي انطلاقا من موقعه في الفيلا، إلا أن الضغوط تزايدت لجعل هذا المشروع أكثر جرئة.

وقبل أن يمر وقت طويل، تم منح مسؤولي الهيئة الوطنية للأمن الإلكتروني الإماراتي سيطرة أكبر على العمليات اليومية، بحسب ما أكده موظفون سابقون في Raven، وهو ما تسبب في كثير من الحالات في إبقاء المدراء الأمريكيين خارج الصورة. وبحلول منتصف 2016، بدأ الإماراتيون بجعل عدد متزايد من أقسام مشروع Raven مخفيا عن الأمريكيين الذين كانوا لا يزالون يقومون بالعمليات اليومية. وبعد وقت قصير تم إصدار قرار بتمكين إماراتيين فقط من الاطلاع على بعض الضحايا المستهدفين بعمليات الاختراق.

أسئلة مكتب التحقيقات الفيدرالي

بحلول سنة 2016، بدأ عملاء الإف بي آي بالتواصل مع موظفي DarkMatter الذين يعودون إلى الولايات المتحدة، لطرح أسئلة عليهم حول مشروع Raven، بحسب ما ذكره ثلاث موظفين سابقين.

وقد أراد مكتب التحقيقات الفيدرالي أن يعرف الآتي: "هل طلب منهم التجسس على أمريكيين؟ هل أن تقنيات جمع المعلومات الاستخباراتية الخاصة بالولايات المتحدة والتكنولوجيات المستخدمة انتهى بها الأمر إلى الوقوع بين يدي الإماراتيين؟"

وقد قام عميلان بالتواصل مع ستراود سنة 2016 في مطار دولس في فيرجينيا عندما كانت عائدة إلى الإمارات بعد زيارة إلى بلدها. وحينها قالت ستراود، التي كانت تخشى من أنها قد وضعت تحت مراقبة الإماراتيين هي أيضا، إنها قامت بالتخلص من محققي الإف بي آي، وقالت لهم أنها لن تخبرهم بأي شيء، بحسب روايتها.

وقد تمت ترقية ستراود ومنحها اطلاعا أكبر على قواعد البيانات الداخلية في مشروع Raven خلال العام الماضي. ومن خلال منصبها كمحللة رئيسية، فإن مهمتها تمثلت في التحقيق في حسابات الأشخاص المستهدفين، وتحديد نقاط الضعف التي يمكن استخدامها لاختراق بريدهم الالكتروني وبرمجيات تبادل الرسائل.

وقد تم تصنيف هذه الأهداف في قوائم مختلفة، بحسب البلاد. حيث أن الأهداف اليمنية كانت في قائمة بنية على سبيل المثال، والأهداف الإماراتية كانت ضمن قائمة رمادية.

وفي صبيحة أحد أيام ربيع 2017، بعد أن أنهت قائمتها للمستهدفين، قالت ستراود أنها بدأت تعمل على كومة أخرى من المهام غير المنجزة التي كان في الأصل موظفو الهيئة الوطنية للأمن المكلفين بها. فقد لاحظت أن صفحة من جواز سفر مواطن أمريكي كانت ضمن هذا النظام. وعندما أرسلت ستراود بريد إلكتروني إلى رؤسائها لتقديم شكوى، تم إخبارها بأن البيانات تم جمعها على وجه الخطأ وسيتم محوها وذلك بحسب بريد إلكتروني اطلعت عليه وكالة رويترز.

وبسبب شعورها بالقلق، بدأت ستراود في البحث في قائمة الأهداف التي كانت في العادة يقتصر الإطلاع عليها على الموظفين الإماراتيين، إلا أنها كانت لا تزال تمتلك التصريح للاطلاع عليها بفضل منصبها ككبيرة محللين. وقد شاهدت أن الأجهزة الأمنية طلبت القيام بعمليات مراقبة ضد أمريكيين اثنين آخرين.

وعندما تساءلت ستروا‌د حول ما يبدو أنه استهداف لمواطنين أمريكيين، تلقت توبيخا من زميل إماراتي لامها على دخولها لقائمة المستهدفين، بحسب ما تظهره المراسلة الإلكترونية. وقيل لها أن قائمة المستهدفين التي اطلعت عليها كان يفترض أن يتم العمل عليها من قبل "بعض الأشخاص"، وهي ليست واحدة منهم، بحسب ما كتبه لها الضابط الإماراتي.

وبعد أيام، قالت ستراود أنها اكتشفت بالمصادفة وجود ثلاث أسماء لأمريكيين آخرين في القائمة السرية للمستهدفين. هذه الأسماء كانت ضمن صنف لم تره من قبل، وهي القائمة البيضاء الخاصة بأصحاب الجنسية الأمريكية. وقالت ستراود أنها لاحظت خلالها أن مهنة هؤلاء كانت "صحفيين".

وحول ردة فعلها، أكدت ستراود أنها شعرت بألم في معدتها، وشعرت بالصدمة بعد أن تأكدت من أن هنالك قائمة بأكملها تم إفرادها للأمريكيين في هذا البرنامج.

وفي مناسبة أخرى أيضا، قالت ستراود أنها توجهت نحو المدير باير. وقد حاول هذا الأخير التقليل من أهمية مخاوفها وطلب منها تجاوز هذه المسألة وعدم الخوض فيها. إلا أنه أشار أيضا إلى أن أي

استهداف لمواطنين أمريكيين كان يفترض أن يتم من قبل الموظفين الأمريكيين في مشروع Raven، وهو ما أكدته ستراود وشخصان آخران اطلعا على فحوى هذا الحوار.

ويشار إلى أن رواية ستراود لهذه الأحداث أكدها أيضا أربع موظفون سابقون آخرون، إلى جانب المراسلات الإلكترونية التي اطلعت عليها وكالة رويترز.

وعندما أصرت ستراود على مواصلة طرح الأسئلة تم منحها عطلة من قبل رؤسائها في العمل، مع أخذ جواز سفرها وهواتفها، وتمت مرافقتها إلى خارج المبنى. وأكدت ستراود أن كل هذه الأمور حدثت بسرعة كبيرة لدرجة أنها لم تكن قادرة على تذكر أشخاص الصحفيين الأمريكين الثلاثة وباقي المواطنين الأمريكيين الذين اعترضتها أسماؤهم في الملفات. وهي تقول: "لقد شعرت حينها كما لو أني واحدة من المستهدفين في إطار الأمن القومي. لقد أصبحت عالقة في تلك البلاد، وأصبحت تحت المراقبة، وليس بإمكاني المغادرة."

وبعد شهرين، تم السماح لستراود بالعودة إلى الولايات المتحدة. وبعد وقت قصير من عودتها، تمكنت من الحصول على أرقام هواتف عملاء مكتب التحقيقات الفدرالي الذين كانوا قد اعترضوها لدى وجودها في المطار في وقت سابق.

وقالت ستراود لوكالة رويترز: "لا أعتقد أنه يفترض أن يقوم أمريكيون بهذا الأمر تجاه أمريكيين آخرين. أنا جاسوسة وأتفهم هذا الأمر، أنا عميلة استخبارات، ولكنني لست عميلة سيئة."

المصدر: رويترز

رابط المقال : https://www.noonpost.com/26395/