وظيفة استخباراتية جديدة لسعود القحطاني بدعم من الإمارات

التغيير

لا يزال دور سعود القحطاني، قائما داخل المملكة وخارجها، رغم جريمته البشعة بقتل وتقطيع الصحافي جمال خاشقجي داخل سفارة المملكة بمدينة إسطنبول التركية في أكتوبر 2018، وبإيعاز وإشراف محمد بن سلمان.

ومجددا يبرز حاليا اسم القحطاني مستشار ابن سلمان، بوظيفة ومهمة جديدة من قبل الأخير، وبتسهيل من دولة الإمارات العربية.

وأعلنت المجموعة 42 Group المرتبطة بالمخابرات الإماراتية عن اتفاق مع شركتي طيران ودفاع إسرائيليتين، مؤخرا، بزعم مواجهة فيروس كورونا، لكن قد يكون هناك أكثر مما تراه العين.

ووقعت مجموعتان دفاعيتان إسرائيليتان رئيسيتان صفقة تاريخية في 2 يوليو 2020 مع 42 Group ، وهي

شركة إماراتية للتكنولوجيا تصف نفسها بأنها متخصصة في الذكاء الاصطناعي ولكنها مرتبطة بالذكاء الإماراتي والشيخ طحنون بن زايد آل نهيان ، مستشار الأمن القومي الإماراتي.

ومن بين الموقعين الآخرين "رافائيل" لأنظمة الدفاع المتقدمة وصناعات الطيران الإسرائيلية، الذين يتعاونون للبحث وتطوير التكنولوجيا والحلول للتعامل مع Covid-19.

وتورطت المجموعة 42 (G42) مؤخرًا كمطور لـ ToTok، وهو تطبيق اتصال ومراسلة مجاني تم الكشف عنه على أنه "مستخدم من قبل حكومة دولة الإمارات العربية المتحدة في محاولة لتتبع كل محادثة، حركة، علاقة، موعد، صوت وصورة لمن يقومون بتثبيته".

الأهم من ذلك، أن المجموعة 42 مرتبطة بشكل مباشر بشركة Matter Dark ، وهي شركة تكنولوجية غامضة في الإمارات العربية المتحدة وظفت عملاء سابقين في وكالة الأمن القومي للتجسس على مئات الأهداف حول العالم. كانت المادة المظلمة نفسها متورطة في الحصول على Pegasus))، برنامج التجسس الإسرائيلي الذي طورته شركة Group NSO الإسرائيلية.

من خلال Matter Dark، لعبت الإمارات العربية المتحدة دورًا في بناء قدرات مملكة آل سعود على الإنترنت، وستقدم سعود القحطاني إلى مجموعة NSO الإسرائيلية من قبل الإمارات والتي توسطت في صفقة بين ممثلين عن MBS والمجموعة الإسرائيلية.

ونظرًا لأن إسرائيل تعتبر برنامج التجسس التابع لمجموعة NSO سلاحًا ، فإن الدعاوى القضائية ضد مجموعة NSO تشير إلى أنه كان يمكن بيعها فقط إلى المملكة والإمارات بموافقة صريحة من وزارة الدفاع الإسرائيلية.

في الصفقة، حصل نظام آل سعود على برنامج القرصنة Pegasus ، والذي استخدمته لاختراق هاتف الصحفي جمال خاشقجي قبل مقتله، بالإضافة إلى مجموعة واسعة من المنشقين والأعداء والمعارضين السياسيين.

وفي الوقت نفسه، تعد رافائيل وصناعات الطيران الإسرائيلية من مصنعي الأسلحة الرئيسيين الذين يزودون الجيش الإسرائيلي بالطائرات بدون طيار والذخائر ومعدات الاتصالات.

في حين أن مذكرة التفاهم G42 الموقعة مع مجموعتي الدفاع تشير إلى تفانيها في التحديات التي

يطرحها Covid-19 ، فإنها لا تحدد التركيز على الاتفاقية.

تجيب لا لكنها ،الإماراتية الصحة وزارة إشراف تحت Covid-19 لقاح تجارب إجراء عن ًحاليا مسؤولة G42 على ما تقدمه شركات الطيران والدفاع الإسرائيلية في صناعة الصحة.

ولا يزال شياو بنغ الرئيس التنفيذي الحالي لـ G42، يصف نفسه بأنه الرئيس التنفيذي لشركة Pegasus .الاثنين بين الروابط إنكار من الرغم على Dark Matter شركة وهي ،LLC

والأهم من ذلك، أنه تحت قيادة Xiao في 25 أبريل 2017، وقعت DarkMatter "مذكرة تفاهم استراتيجية عالمية" مع Huawei لأنظمة "Data Big" وحلول "المدينة الذكية".

ومع ذلك تم تأسيس قرب المجموعة 42 من المخابرات الإماراتية ، وسابقتها السابقة في تنفيذ مراقبة واسعة النطاق من خلال الشراكات مع الصين وإسرائيل.

وتبدو المخاوف الراهنة من أن عمليات نقل التكنولوجيا قد لا تمكنهم فقط من تتبع ومتابعة مرضى الإمارات في والاستخبارات المراقبة قدرات لتوسيع استخدامها ًأيضا ولكن ،المثال سبيل على Covid-19 ليست غير معقولة تمامًا.

وتتوالى التقارير عن استخدام نظام آل سعود أجهزة اختراق خارجية ضمن نهجه القائم على القرصنة والتجسس الالكتروني.

ونشر موقع "سيتيزين لاب" مركز أبحاث تابع لجامعة تورونتو، في كندا، تحقيقاً يكشف فيه عن تعرض هاتف رئيس مكتب صحيفة "نيويورك تايمز" في بيروت، بن هابارد، لهجوم سيبراني عبر برنامج تجسس يدعى "بيغاسوس" تنتجه مجموعة "NSO -إن إس أو" الإسرائيلية، وهي شركة متخصصة بتكنولوجيا المراقبة.

ويشير التحقيق إلى أن الرابط الذي أرسل إلى هاتف هابارد، مصدره موقع يستخدمه أحد مشغلي "بيغاسوس" يدعوه فريق التحقيق في "سيتيزين لاب" بـ"مملكة" (KINGDOM)، والذي يعتقد الفريق أنه مرتبط بنظام آل سعود.

ويظهر التحقيق أنه تم منذ عام 2016، توثيق استخدام "بيغاسوس" للتجسس على عدد من الصحافيين

والمدافعين في مجال حقوق الإنسان، والناشطين في المجتمع المدني.

أكدت تقارير سابقة صادرة عن "سيتيزان لاب" ومنظمة العفو الدولية، في عام 2018 أن المشغل "مملكة" كان يستهدف معارضين وناقدين للمملكة.

وسبق أن أكد تقرير نشرته منظمة العفو الدولية في 31 تموز/ يوليو عام 2018، أن أحد موظفي المنظمة قد تعرض لهجوم من قبل بيغاسوس، إلى جانب ناشط سعودي يعيش خارج المملكة، اتضح لاحقاً أنه يحيى العسيري المقيم في بريطانيا.

وفي تشرين الأول/ أكتوبر من العام ذاته، نشر "سيتيزين لاب" تقريراً يكشف تعرض المعارض السعودي المقيم في كندا، عمر عبد العزيز إلى هجوم عبر "بيغاسوس".

وكان عبدالعزيز، خلال هذه الفترة، على تواصل وثيق مع الصحافي السعودي جمال خاشقجي، الذي قتل في عام 2018 داخل سفارة بلاده في تركيا.

وبعد ذلك بأيام، نشر موقع "فوربز" تقريراً يكشف تعرض المعارض السعودي غانم الدوسري، بدوره، لاستهداف عبر "بيغاسوس". وفي حال قام هؤلاء بالضغط على الرابط الذين تلقوه، كان مشغل "مملكة" ليتمكن من مراقبة جميع اتصالاتهم ونشاطاتهم الهاتفية. وقام عبدالعزيز برفع دعوة ضد شركة "إن إس أو" في إسرائيل، فيما اختار الدوسري مملكة آل سعود هدفاً لدعوته التي رفعها من المملكة المتحدة.

أما بن هابارد، فكان، قبل أن يتم تعيينه رئيساً لمكتب "نيويورك تايمز" في بيروت، يركز في تغطياته على المملكة لا سيما نشاطات محمد بن سلمان.

وفي حزيران/يونيو عام 2018، تلقى هابارد رسالة إس إم إس على هاتفه من مرسل يدعى "أراب نيوز"، مضمونها رابط مرفق بعنوان: "بن هابارد وقصة الأسرة المالكة في الجزيرة العربية".

ويأخذ الرابط إلى موقع عنوانه "com.arabnews365". ويقول هابارد إنه لم يضغط على الرابط، ولم يتمكن "سيتيزن لاب" من معرفة ما إن كان قد تم اختراق هاتفه أم لا.

وتمكنت تحقيقات قام بها باحثون من "سيتيزين لاب" وغيرهم من تحديد 13 صحافيا وناشطا قد تم

استهدافهم جميعاً عبر بيغاسوس. ففي المكسيك وحدها، وثق المركز 9 صحافيين على الأقل.

وأشار المركز إلى أن ما يثير القلق، هو ارتباط هذه الهجمات السيبرانية بعمليات اغتيال. ويأخذ "سيتيزين لاب" من قضية خاشقجي مثالاً على ذلك، إذ يشير المركز إلى أنه تم قتل الصحافي السعودي، في اليوم الذي تلا نشر المركز للتقرير حول قضية التجسس على عمر عبد العزيز.

ويضيف تحقيق "سيتيزين لاب" أنهم تمكنوا من كشف أدلة على أن في الأسابيع التي سبقت اغتيال خاشقجي، كان أحد مشغلي "بيغاسوس" يرسل روابط باسم "واشنطن بوست". ويشير التحقيق إلى أنه أن تزامن الحدثين لا يعني ارتباطهما.

في هذه الأثناء قال خبراء إن نظام آل سعود متورط بشراء برامج التجسس التي يحتاجها لترسانتها من جهات خارجية، وهي نفس الطريقة التي يعتقد المحللون أن المملكة لجأت إليها لاختراق هاتف الملياردير الأمريكي جيف بيزوس.

وتقول أليزا سبنويس في تقرير نشره موقع "بلومبيرغ" إن عملية شراء الخدمات من جهات خارجية هي الوسيلة المفضلة في عملية التجسس الإلكتروني.

ففي الوقت الذي تحاول فيه دول مثل كوريا الشمالية والصين وروسيا الاستثمار في تطوير وتصميم أسلحة إلكترونية فإن المملكة لا تصممها ولكن تشتريها.