كيف يخوض مرتزقة الإنترنت المعارك بالنيابة عن الحكومات الاستبدادية؟

كتبه نيويورك تايمز | 23 مارس ,2019

ترجمة وتحرير: نون بوست

كتب: مارك مازيتي، آدم غولدمان، رونين بيرغمان، نيكول بيرلروث

مضى الرجل المسؤول عن حملة المملكة العربية السعودية القاسية لخنق المعارضة رحلة البحث عن طرق للتجسس على الأشخاص الذين اعتبروا تهديدا للمملكة، وكان يعرف الوجهة المثلى لتحقيق ذلك، لينتهي به المطاف بالتفاوض مع شركة إسرائيلية سرية تقدم تكنولوجيا طورها عملاء المخابرات السابقون.

في أواخر سنة 2017، كان سعود القحطاني، الذي كان آنذاك كبير مستشاري ولي العهد السعودي، يعمل على تتبع المعارضين السعوديين في جميع أنحاء العالم، وذلك في إطار جهود المراقبة المكثفة التي أدت في النهاية إلى مقتل الصحفي جمال خاشقجي. وفي رسائل متبادلة مع موظفين من مجموعة "إن إس أو"، تحدث القحطاني عن خطط لاستخدام أدوات المراقبة الخاصة بها في جميع أنحاء الشرق الأوسط وأوروبا، على غرار تركيا وقطر أو فرنسا وبريطانيا.

في الوقت الحالي، يمكن لأصغر بلدان العالم شراء خدمات التجسس الرقمي مما يتيح لها إجراء عمليات معقدة مثل التنصت الإلكتروني أو التأثير على الحملات التي كانت ذات يوم حكرا على القوى الكبرى مثل الولايات المتحدة وروسيا

يمكن القول إن اعتماد المملكة العربية السعودية على شركة متمركزة في بلد كانت لها معه عداوات مستمرة على مدى قرون يقدم لمحة عن عصر جديد من حرب رقمية يحكمها عدد قليل من القواعد واقتصاد متنامٍ على نحو كبير. وتبلغ قيمة هذا المجال الاقتصادي حوالي 12 مليار دولار.

في الوقت الحالي، يمكن لأصغر بلدان العالم شراء خدمات التجسس الرقمي مما يتيح لها إجراء عمليات معقدة مثل التنصت الإلكتروني أو التأثير على الحملات التي كانت ذات يوم حكرا على القوى الكبرى مثل الولايات المتحدة وروسيا. ويمكن للشركات التي ترغب في الاطلاع على أسرار المنافسين، والأثرياء الذين يكنون حقدا تجاه أحد الخصوم، أن يقودوا حملات استخباراتية مقابل ثمن محدد يُدفع لقاء الحصول على أدوات وخدمات أشخاص تابعين لوكالة الأمن القومي أو الموساد.

تعتبر شركة "إن إس أو" ومنافستها "دارك ماتر" الإماراتية مثالا على انتشار عمليات التجسس بواسطة جهات خاصة. وبناء على المقابلات الصحفية مع المتسللين الإلكترونيين الحاليين والسابقين للحكومات والشركات الخاصة وغيرها، بالإضافة إلى مراجعة بعض الوثائق في هذا الغرض، تمكنت صحيفة "نيويورك تايمز" من الكشف عن المناوشات السرية في كنف هذا العالم المتنامي للمعارك الرقمية.

تحدث كبير المستشارين السابقين لولي العهد السعودي محمد بن سلمان عن استخدام منتجات مجموعة إن إس أو في الخارج كجزء من جهود المراقبة المكثفة

لم تُمكِّن هذه الشركات الحكومات من التجسس على المجرمين والتنظيمات الإرهابية وعصابات التجارة بالمخدرات واختراق حساباتهم فحسب، بل إن سطوتها امتدت في بعض الأحيان لتشمل التصرف حسب دوافع أكثر قتامة واستهداف الناشطين والصحفيين. وقد ساهم المجرمون الإلكترونيون الذين دربتهم وكالات التجسس بالولايات المتحدة في إثبات تورط بعض رجال الأعمال الأمريكيين وعدد من الناشطين الحقوقيين والإيقاع بهم. وقد سبق لمرتزقة الإنترنت العاملين مع "دارك ماتر" تحويل جهاز مراقبة الأطفال إلى أداة للتجسس.

في الوقت الحالي، يعمل العملاء الفدراليون على استجواب الموظفين الأمريكيين الحاليين والسابقين في شركة دارك ماتر فيما يتعلق باقترافهم جرائم إلكترونية، وذلك وفق معطيات أدلى بها أربعة أشخاص مطلعون على هذه التحقيقات. ونقلت وكالة "رويترز" للأنباء خبرا مفاده أن أحد الموظفين المتعاقدين مع الشركة الإماراتية أبلغ مكتب التحقيقات الفدرالي بأن هناك شكوك متزايدة حول نشاط الشركة، وهو ما قاد إلى تكثيف التحقيقات واتخاذها منحى جدي.

بلاك تيوب اكتسبت سمعة سيئة بعد أن استعان بها هارفي وينشتاين، مخرج الأفلام سيئ السمعة في هوليوود، لكشف بعض الحقائق والفضائح المتعلقة بمتَّهِميه

في الواقع، تتنافس كل من دارك ماتر وإن إس أو بشكل كبير مع بعضهما البعض، وهو ما يدفعهما إلى تقديم أجور عالية لأفضل المواهب في عالم القرصنة الرقمية من الولايات المتحدة و"إسرائيل" وغيرها من الدول، كما سبق لهما إغراء الموظفين وسرقتهم من الشركات المنافسة. ويعتبر الشرق الأوسط مركز هذه الحقبة الجديدة من التجسس الخاص، حيث تنشط شركة "بلاك تيوب" إلى جانب الشركتين الأخيرتين، وهي شركة خاصة يديرها أعضاء سابقون في الموساد الإسرائيلي وعناصر سابقون من المخابرات العسكرية الإسرائيلية.

والجدير بالذكر أن بلاك تيوب اكتسبت سمعة سيئة بعد أن استعان بها هارفي وينشتاين، مخرج الأفلام سيئ السمعة في هوليوود، لكشف بعض الحقائق والفضائح المتعلقة بمتَّهِميه. علاوة على ذلك، عملَت شركة بساي غروب الإسرائيلية المتخصصة في التلاعب بمواقع التواصل الاجتماعي لصالح رجال الأعمال الروس، كما قادت حملة ترامب سنة 2016 وفق خطة تتضمن بناء جيش من بوتات الإنترنت للتأثير على أصوات الناخبين الجمهوريين.

خلال السنة الماضية، عمد رجل الأعمال الأمريكي إليوت بروديدي إلى رفع دعوى قضائية ضد حكومة قطر وشركة في نيويورك يديرها عضو سابق في وكالة المخابرات المركزية، والتي تعرف باسم "غلوبال ريسك إدفايزورز". وترتكز هذه الدعوى على مساهمة الشركة في عملية أفضت إلى نشر الآلاف من رسائل البريد الإلكتروني الخاصة به إلى العامة، كما أفاد بروديدي بأن العملية كانت مدفوعة بالظروف الجيوسياسية الصعبة. وفي بداية ولاية ترامب، دفع البيت الأبيض إلى تبني سياسات مناهضة لقطر، وذلك في الوقت الذي كانت تستعد خلاله شركته إلى تلقي مئات الملايين من الدولارات بناء على عقود صادرة عن الإمارات العربية المتحدة.

لكن قوبلت دعوى بروديدي بالرفض، بيد أن الشكوك ازدادت حول ضلوع قطر في عمليات أخرى، بما في ذلك اختراق وتسريب رسائل البريد الإلكتروني الخاصة بيوسف العتيبة، السفير الإماراتي البارز في واشنطن. كما أن التوسع السريع لرقعة ساحة المعركة العالمية في مجال التقنيات العالية، والتي يتصادم بين حدودها جنود الجيوش الإلكترونية، أدى إلى ظهور تحذيرات من مستقبل فوضوي وخطير.

> تأسست شركة إن إس أو على يد صديقين درسا معا في المدرسة الثانوية في شمال "إسرائيل" وكانا يمتلكان فهما محدودا نسبيا لمجال الاختراق الإلكتروني

حيال هذا الشأن، أفاد مؤسس شركة "أدلومين" للأمن السيبراني وأحد المحققين الرئيسيين في قضية القرصنة الروسية سنة 2016 لموقع اللجنة الوطنية الديمقراطية بأنه: "حتى الدول الصغرى التي تمتلك ميزانيات منخفضة للغاية باتت قادرة على امتلاك قدرات هجومية أو شن هجمات عبر الإنترنت ضد الخصوم. وتلاحق كل من قطر والإمارات بعضهما بعضا، وهذه الحرب بينهما تزداد حدة. إن الحواجز التي تحول دون الولوج إلى هذا العالم باتت أضعف شيئًا فشيئًا".

ثغرة أمنية مستغَلّة

تأسست شركة إن إس أو على يد صديقين درسا معا في المدرسة الثانوية في شمال "إسرائيل" وكانا يمتلكان فهما محدودا نسبيا لمجال الاختراق الإلكتروني. وفي الوقت الحالي، تدير هذه الشركة عملياتها في ست قارات، ناهيك عن مساعدتها الحكومة السعودية في تعقب خصومها خارج المملكة، فضلا عن مد يد العون إلى المكسيكيين للإمساك بتجار المخدرات. وبالاعتماد على التكنولوجيا التي يطورها خريجون من وحدة 8200 التي تعادل وكالة الأمن القومي الأمريكي، أنشأ شليف خوليو وعمري لافي شركة خاصة سنة 2008، والتي سمحت لشركات الهاتف المحمول بالولوج إلى هواتف مستخدميها لصيانتها عن بعد.

امتدت هذه الخدمة وتطورت لتتخذ شكل خدمات تجسس في الدول الغربية، وتبادرت هذه الاستخدامات إلى مسامع أولئك الذين رأوا فيها فرصة ثمينة. وكان المسؤولون الأمريكيون والأوروبيون يحذرون من تطوير شركات مثل آبل وغوغل وفيسبوك وعملاقة التكنولوجيا الآخرين لتقنيات تتيح للمجرمين والإرهابيين التواصل عبر القنوات المشفرة غير القابلة للاختراق من قبل وكالات الاستخبارات وإنفاذ القانون، كما أطلقوا على هذه الظاهرة اسم "حلول الظلام".

> يمكن لهذه الأداة تنفيذ بعض الأمور التي قد تبدو جنونية، على غرار جمع كميات هائلة من البيانات التي يتعذر الوصول إليها من الهواتف الذكية دون ترك أي أثر

من جهتهما، قدم خوليو ولافي وسائل للالتفاف حول هذه المعضلة من خلال اختراق الهواتف المخصصة للقيام بالاتصالات بعد فك تشفير بياناتها. وبحلول سنة 2011، طورت شركة "إن إس أو" نموذجا أوليا، وهو عبارة عن أداة مراقبة متنقلة تسمى "بيغاسوس"، في إشارة إلى الحصان المجنح في الأساطير الإغريقية القديمة.

يمكن لهذه الأداة تنفيذ بعض الأمور التي قد تبدو جنونية، على غرار جمع كميات هائلة من البيانات التي يتعذر الوصول إليها من الهواتف الذكية دون ترك أي أثر، بما في ذلك المكالمات الهاتفية والنصوص ورسائل البريد الإلكتروني وجهات الاتصال والموقع وأي بيانات مرسلة عبر تطبيقات مثل فيسبوك وواتساب وسكايب. وخلال حديثها عن شركة "إن إس أو" ومنافسيها، صرحت آفي روسن، وهي متحدثة باسم شركة "كايميرا تيكنولوجيز" للأمن السيبراني عبر الإنترنت، بأنه: "بمجرد أن تلج هذه الشركات إلى هاتفك، سيصبح بإمكانهم امتلاكه".

عمري لافي على اليسار وشليف خوليو على اليمين، مؤسسا شركة إن إس أو واستخدما التكنولوجيا التي طورها خريجو وحدة 8200 الاستخباراتية، والتي تعادل وكالة الأمن القومي الأمريكية

سرعان ما حصلت الشركة على عميلها الأول المهتم بأداة "بيغاسوس" وهو حكومة المكسيك، وذلك في إطار حربها على عصابات تجارة المخدرات. ووفقا للرسائل الإلكترونية التي تلقتها صحيفة "نيويورك تايمز"، عملت إن إس أو على تثبيت أداة التجسس في ثلاث وكالات مكسيكية، وأشارت البيانات المستخرجة أن الشركة باعت الحكومة المكسيكية ما قيمته 15 مليون دولار من الأجهزة والبرامج. وظهر للعموم أن حكومة المكسيك كانت قد دفعت مبلغ 77 مليون دولار لتتبع تحركات مجموعة واسعة من الأهداف ومسح هواتفهم باستمرار.

كانت منتجات الشركة الإسرائيلية ذات أهمية كبرى في حرب المكسيك ضد عصابات تجارة المخدرات، وذلك وفقا لتصريحات بعض الأشخاص الذين كانوا على دراية بكيفية استخدام الحكومة المكسيكية لبيغاسوس، والذين وافقوا على الإفصاح عن المعلومات الاستخباراتية مقابل عدم الكشف عن هوياتهم. وأضاف هؤلاء المسؤولون أن بيغاسوس لعب دورا كبيرا في القبض على إل تشابو، ملك المخدرات الشهير الذي أدين الشهر الماضي في نيويورك وحُكم عليه بالسجن مدى الحياة في سجن شديد الحراسة.

> كانت الحكومة المكسيكية، عميل الشركة الإسرائيلية الأول، تستخدم أدوات القرصنة التي تتحصل عليها لأغراض أكثر سوداوية، وذلك كجزء من مجهوداته واسعة النطاق لمراقبة أداء الحكومة والمجال الصناعي

بعد فترة وجيزة، كانت شركة "إن إس أو" تبيع منتجاتها إلى حكومات من كافة أنحاء العالم، حيث كانت تتلقى طلبات من العديد من البلدان. وخلال المقابلات الشخصية التي أجرتها صحيفة "نيويورك تايمز"، صرح مسؤولو المخابرات الأوروبية وإنفاذ القانون أن منتجات إن إس أو وخاصة بيغاسوس ساعدت في تفكيك الخلايا الإرهابية ويسّرت التحقيقات في الجريمة المنظمة واختطاف الأطفال.

التجسس على المواطنين

كانت الحكومة المكسيكية، عميل الشركة الإسرائيلية الأول، تستخدم أدوات القرصنة التي تتحصل عليها لأغراض أكثر سوداوية، وذلك كجزء من مجهوداته واسعة النطاق لمراقبة أداء الحكومة والمجال الصناعي. بناء على ذلك، استخدمت السلطات المكسيكية هذه المنتجات لمراقبة ما لا يقل عن 24 صحفيا، ومنتقدي الحكومة والمحققين الدوليين الذين يبحثون في قضايا اختفاء 43 طالبا، لتشمل عمليات التجسس داعمي ضريبة الصودا في البلاد. وقد كانت هذه المعلومات نتاج تحقيقات صحيفة "نيويورك تايمز" والأبحاث التي أجرتها جامعة "تورنتو" الكندية.

تعرض الأشخاص المستهدفون من قبل الحكومة المكسيكية إلى دفق من الرسائل النصية المزعجة التي تحتوي على برامج ضارة. وتضمنت بعض الرسائل معلومات تخبر المستخدم بأن شريك حياته يخونه، أو أن أحد معارفه قد فارق الحياة. وفي إحدى هذه الحالات، لم يتمكن المسؤولون الحكوميون من التسلل إلى هاتف إحدى الصحفيات، وهو ما دفعهم إلى استهداف نجلها البالغ من العمر 16 سنة.

اعتبر المسؤولون المكسيكيون تكنولوجيا "إن إس أو" عاملا أساسيًا في المساعدة في تعقب وإلقاء القبض على ملك المخدرات إل تشابو

على الرغم من مزاعم شركة "إن إس أو" على أنها تبيع خدماتها خدمةً للتحقيقات الجنائية ومكافحة الإرهاب، لم يكن أي من المواطنين المكسيكيين الذين استُهدِفوا في عمليات التجسس مشتبها بهم في تحقيقات جنائية أو إرهابية. وفي بيان لها، أوردت الشركة أن "تقنياتنا ساهمت في وقف الجرائم الشريرة والهجمات الإرهابية القاتلة في جميع أنحاء العالم. نحن لا نتسامح مع سوء استخدام منتجاتنا، كما أننا نفحص ونراجع عقودنا بانتظام للتأكد من عدم استخدامها لأي غرض آخر عدا عن منع الإرهاب أو الجريمة أو التحقيق فيها".

أنشأت الشركة لجنة للأخلاقيات، التي تقرر ما إذا كان يمكنها بيع برامجها للتجسس إلى البلدان بناءً على سجلات حقوق الإنسان الخاصة بها، على غرار مؤشر رأس المال البشري التابع للبنك الدولي للتنمية، فضلا عن العديد من المؤشرات الأخرى. وقد أعلن موظفون حاليون وسابقون في الشركة الإسرائيلية أن شركتهم لن تبيع منتجاتها إلى تركيا بتعلة سجلها السيء في مجال حقوق الإنسان. في المقابل، تحتل تركيا مركزا أفضل من المكسيك والمملكة العربية السعودية عندما يتعلق الأمر بمؤشر البنك الدولي، لكن الشركة لا تزال تتعامل مع حكومتهما. من جهته، رفض متحدث باسم وزارة الدفاع الإسرائيلية، الملزمة بالتصريح بأي عقد توقعه "إن إس أو" مع أي حكومة أجنبية، الإجابة عن الأسئلة المتعلقة بالشركة.

> وقعت الشركة على أولى صفقاتها مع الإمارات العربية المتحدة سنة 2013. وفي غضون سنة واحدة، ضُبطت الحكومة الإماراتية وهي بصدد تثبيت برامج التجسس التابعة للشركة الإسرائيلية على هاتف الناشط البارز في مجال حقوق الإنسان، أحمد منصور

وتجدر الإشارة إلى أن إحدى الدعاوى القضائية زعمت أن السلطات السعودية استخدمت منتجات "إن إس أو" للتجسس على جمال خاشقجي، كاتب العمود في صحيفة "واشنطن بوست" الذي اغتاله العملاء السعوديون في قنصلية المملكة العربية السعودية في إسطنبول في مطلع شهر تشرين الأول/ أكتوبر الماضي. من جهتها، نفت الشركة الإسرائيلية هذا الاتهام، في حين ذكرت جامعة "تورنتو" أن العديد من اتصالات جمال خاشقجي مع الأشخاص المقربين منه كانت أهدافا لأدوات الاختراق التابعة لشركة "إن إس أو". ونظرا لعدم امتلاكهم حق الولوج إلى الأجهزة الخاصة بالصحفي السعودي المغتال، لم يؤكد الباحثون ما إذا كان هدفًا مباشرًا لمراقبة الشركة الإسرائيلية.

حتى في حالات سوء الاستخدام الصارخ، واصلت "إن إس أو" تجديد العقود مع عملائها الحكوميين. فعلى سبيل المثال، وقعت الشركة على أولى صفقاتها مع الإمارات العربية المتحدة سنة 2013. وفي غضون سنة واحدة، ضُبطت الحكومة الإماراتية وهي بصدد تثبيت برامج التجسس التابعة للشركة الإسرائيلية على هاتف الناشط البارز في مجال حقوق الإنسان، أحمد منصور.

بعد تلقيه وابلا من الرسائل النصية التي تحتوي على روابط مشبوهة، مرر منصور الرسائل إلى الباحثين في مجال الأمن، الذين توصلوا إلى أنها كانت برامج تابعة لشركة "إن إس أو" الهدف منها استغلال الثغرات الأمنية في برنامج آبل لاختراق هاتفه. وأضاف الباحثون أن ما صادفوه كان أكثر برامج الاختراق تطورا في عالم الهواتف الذكية.

لقد أجبر اكتشاف الثغرة الأمنية شركة آبل على إصدار تصحيح برمجي بصفة عاجلة، لكن ذلك لم يحل دون طرد منصور من وظيفته ومصادرة جواز سفره وسرقة سيارته واختراق بريده الإلكتروني وتعقب موقعه، فضلا عن إفراغ حسابه المصرفي الذي كان يحتوي على مبلغ 140 ألف دولار وتعرضه للضرب على يد غرباء في مناسبتين خلال أسبوع واحد. وفي المقابلة الصحفية التي أجراها قبل اعتقاله سنة 2017، أفاد أحمد منصور قائلا: "أنت تبدأ في الاعتقاد بأن كل خطوة تقوم بها مراقبة، وتبدأ عائلتك بالشعور بالذعر".

ضُبطت الحكومة الإماراتية وهي بصدد تثبيت برامج التجسس التابعة للشركة الإسرائيلية على هاتف الناشط البارز في مجال حقوق الإنسان، أحمد منصور

على الرغم من ضبط الإمارات العربية المتحدة وهي بصدد التجسس على الناشط الحقوقي، إلا أن بعض الفواتير المسربة أظهرت أن شركة "إن إس أو" واصلت بيع برامج التجسس وتقديم خدماتها إلى الإماراتيين مقابل ملايين الدولارات. ولاقى أحمد منصور حكما بالسجن لمدة 10 سنوات بسبب الإضرار بالوحدة الوطنية، كما سُجن في الحبس الانفرادي وتدهورت صحته بشكل ملحوظ. بالإضافة إلى ذلك، وردت العديد من التقارير الإخبارية حول البلدان التي تستخدم منتجات الشركة الإسرائيلية للتجسس على مواطنيها، وهو ما دفع الشركة إلى تغيير اسمها مؤقتا إلى "كيو". وعلى

الرغم من التغطية الإخبارية السيئة، استمرت قيمة "إن إس أو" في الارتفاع.

> أدى انتشار الشركات، التي تحاول تحقيق النجاح الذي حققته شركة "إن إس أو" ودخول المنافسة في سوق تصل قيمته إلى 12 مليار دولار من أجل تطوير برامج تجسس

في سنة 2013، اشترت شركة الأسهم الخاصة "فرانشيسكو بارتنرز" حصة نسبتها 70 بالمئة من شركة "إن إس أو" مقابل 130 مليون دولار. وخلال الشهر الماضي، جمع مؤسسو الشركة الإسرائيلية ما يكفي من المال لإعادة شراء حصة تمكنهم من الظفر بأغلبية أسهم الشركة مقابل مبلغ يقارب المليار دولار. ووفقا للسجلات الرسمية، دعمت شركة "نوفالبينا كابيتال" هذه الصفقة، مما جعل مستثمريها الرئيسيين، من قبيل صندوق معاشات موظفي ولاية أوريغون وصندوق الثروة السيادية في ألاسكا، جزءا من الشركة الإسرائيلية.

التجسس على الأمريكيين

أدى انتشار الشركات، التي تحاول تحقيق النجاح الذي حققته شركة "إن إس أو" ودخول المنافسة في سوق تصل قيمته إلى 12 مليار دولار من أجل تطوير برامج تجسس وفقا لتقديرات شركة "موديز"، إلى ظهور منافسة شرسة بين الشركات لتوظيف المحاربين الأمريكيين والإسرائيليين والروس القدامى في أكثر وكالات الاستخبارات تطورا في العالم. وكما يبدو، فإن هذه الشركات تسعى لصيد المواهب.

لكن في أواخر سنة 2017، أصبح المسؤولون التنفيذيون في شركة "إن إس أو" قلقين بشأن سلسلة من الاستقالات. وسرعان ما وجد المحققون الخاصون المشرفون على التحقيق أنفسهم في جزيرة قبرص المطلة على البحر الأبيض المتوسط لتعقب مجموعة من موظفي شركة "إن إس أو" السابقين الذين كانوا جميعهم من قدامى المحاربين في وحدة الاستخبارات الإسرائيلية 8200، وكانوا متجهين للعمل في مركز للأبحاث.

> كان للإماراتيين طموحات كبيرة وحاولوا دفع موظفي سايبر بوينت مرارًا وتكرارًا إلى تجاوز حدود الرخصة الأمريكية للشركة

كان المبنى مملوكًا لمؤسسة تابعة لشركة "دارك ماتر"، وهي شركة إماراتية استأجرت إسرائيليين بشكل سري لتطوير تكنولوجيات لصالح الإمارات العربية المتحدة من أجل شن هجمات إلكترونية ضد الأعداء المحتملين داخل وخارج البلاد. وتملك شركة دارك ماتر أيضًا مكاتب في برج يطل على الطريق السريع الذي يربط أبو ظبي بدبي، وهو المبنى ذاته الذي يضم وكالة الاستخبارات الأمريكية في الإمارات العربية المتحدة، وهو في الواقع الفرع الإماراتي لشركة "إن إس أو".

لم يكن ما حدث وليد الصدفة. فقد كانت دارك ماتر ذراع الدولة، التي عملت مباشرة مع عملاء المخابرات الإماراتيين في العديد من المهام مثل اختراق الوزارات الحكومية في كل من تركيا وقطر وإيران، بالإضافة إلى التجسس على المنشقين داخل الإمارات. وتعود أصول دارك ماتر إلى شركة أخرى، وهي شركة أمريكية تدعى سايبر بوينت، التي ظفرت قبل سنوات بعقود مع الإمارات العربية المتحدة للمساعدة في حمايتها من الهجمات الإلكترونية. وحصلت سايبر بوينت على ترخيص من الحكومة الأمريكية للعمل لدى الإماراتيين، وهي خطوة ضرورية تهدف إلى تنظيم تصدير الخدمات العسكرية والاستخبارية. وتجدر الإشارة إلى أن العديد من موظفي الشركة عملوا في مشاريع مهمة جدا لصالح وكالة الأمن القومي الأمريكي ووكالات الاستخبارات الأمريكية الأخرى.

في المقابل، كان للإماراتيين طموحات كبيرة وحاولوا دفع موظفي سايبر بوينت مرارًا وتكرارًا إلى تجاوز حدود الرخصة الأمريكية للشركة. لكن، رفضت الشركة طلبات عملاء المخابرات الإماراتيين لمحاولة كسر رموز التشفير وخرق مواقع الويب الموجودة على خوادم أمريكية، وهي عمليات كان من شأنها أن تتعارض مع القانون الأمريكي.

مثلت دارك ماتر ذراع الحكومة الإماراتية التي عملت مباشرة مع عملاء المخابرات في مهام متعددة بما في ذلك التجسس على المنشقين في البلاد

من هذا المنطلق، أسس الإماراتيون سنة 2015 شركة دارك ماتر، وهي شركة لا تلتزم بقانون الولايات المتحدة وجذبت ما لا يقل عن ستة موظفين أمريكيين في سايبر بوينت. في الواقع، أصبح مارك باير، الذي كان مسؤولا سابقا في وحدة وكالة الأمن القومي التي تنفذ عمليات هجومية إلكترونية

متطورة، أحد كبار المديرين التنفيذيين للشركة. علاوة على ذلك، جذبت الشركة العديد من الموظفين من الوكالات الأمريكية السابقة على غرار وكالة الأمن القومي الأمريكي ووكالة المخابرات المركزية. ووفقا لجدول الموظفين الذي تحصلت عليه صحيفة "ذي تايمز"، فإن بعضهم يحصل على رواتب تصل لمئات الآلاف من الدولارات سنويا.

في هذا السياق، قال جونستون، الخبير الأمني الذي كان يعمل في القيادة السيبرانية للجيش التي تعمل عن كثب مع الولايات المتحدة، في الوقت الذي كان يعمل فيه في المارينز: "كان من المفترض أنه عندما تغادر الولايات المتحدة، لن تقوم أبدًا بهذا النوع من العمل المسيء مرة أخرى. كان على وكالة الأمن القومي الأمريكي أن تعتبر أنه من مسؤولياتها ضمان عدم استخدام تقنيات القرصنة التي يتم تدريسها للموظفين ضد الولايات المتحدة".

> ، قال موظفون سابقون إن دارك ماتر استهدفت الناشط الحقوقي الإماراتي أحمد منصور، واخترقت جهاز مراقبة طفله للتنصت على عائلته

في الحقيقة، لم تردّ الشركة على طلب للتعليق، ورفض المتحدث باسم الحكومة الإماراتية الإدلاء بأي تصريح أيضا. وردا على سؤال حول ما إذا كانت الوزارة قد منحت ترخيصًا لعملاء المخابرات الإسرائيليين السابقين الذين يعملون لصالح شركة دارك ماتر، رفض كل من المتحدث باسم وزارة الدفاع الإسرائيلية ومحامي مارك باير التعليق.

حيال هذا الشأن، قال غريغ جوليان، المتحدث باسم وكالة الأمن القومي، إن الموظفين الحاليين والسابقين في وكالة التجسس يخضعون لالتزام مدى الحياة يقتضي حماية أسرار الولايات المتحدة. وأكد جوليان أنه يتعين عليهم أيضا الإبلاغ عند العمل مع الحكومات الأجنبية أو تمثيلها لمدة سنتين عقب مغادرتهم للوكالة. ووفقا لموظفين سابقين، اخترقت دارك ماتر، إلى جانب اختراقها لوزارات تابعة للحكومات الأجنبية، حسابات جي ميل وياهو وهوتميل أيضا. ويظهر عملاء الشركة كأصدقاء للأشخاص المستهدفين لاستدراجهم لفتح رسائل البريد الإلكتروني التي تحتوي على برامج ضارة.

في هذا الإطار، قال موظفون سابقون إن دارك ماتر استهدفت الناشط الحقوقي الإماراتي أحمد منصور، واخترقت جهاز مراقبة طفله للتنصت على عائلته. وفي عملية أخرى، لاحق عملاء الشركة روري دوناغي، الناشط البريطاني الذي ينتقد الحكومة الإماراتية وسجلها في مجال حقوق الإنسان، والذي كان أيضا هدفا لبرامج التجسس التابعة لشركة "إن إس أو". وقال موظف سابق إن شركة دارك ماتر استهدفت منظمة الأبحاث الكندية "سيتيزن لاب". وقد أعلمت شركة دارك ماتر الموظفين أن التجسس على المواطنين الأمريكيين أمر محظور، لكن ذلك التعهد لم يكن سوى حبر على ورق.

> وفقا لما أفاد به موظف ثان سابق، فإنه في حالات متكررة قامت مجموعة دارك ماتر بجمع معلومات عن الأميركيين، مضيفا أن معظم هذه الحالات شملت أمريكيين عملوا لصالح منظمات أجنبية، بما في ذلك منظمات حقوق الإنسان

خلال إحدى العمليات، التي لم يتم الإبلاغ عنها مسبقا، أطلق فرع تابع لدارك ماتر جهدا موسعا لاعتراض الاتصالات الخلوية في قطر. لكن في بعض الأحيان، وقع التقاط اتصالات تعود لمواطنين أمريكيين في شبكة المراقبة في أواخر سنة 2015. وقد صرح أحد الموظفين الأمريكيين الذي كان يعمل في المشروع أنه شارك رؤسائه في العمل هذه المخاوف، بما في ذلك موظف سابق في وكالة المخابرات المركزية المسؤول عن هذه الخطوة. مع ذلك، وقع الاستغناء عنه من المشروع، إلى جانب موظف آخر، وطُلب منه التوقيع على اتفاقية عدم الإفصاح.

وفقا لما أفاد به موظف ثان سابق، فإنه في حالات متكررة قامت مجموعة دارك ماتر بجمع معلومات عن الأميركيين، مضيفا أن معظم هذه الحالات شملت أمريكيين عملوا لصالح منظمات أجنبية، بما في ذلك منظمات حقوق الإنسان، التي استهدفتها هذه المجموعة لأنها كانت تنتقد الحكومة الإماراتية. ويقوم الموظفون التابعون لمجموعة "دارك ماتر" أحيانًا بجمع معلومات تتعلّق بجوازات السفر أو الطلبات المقدمة أو السير الذاتية الخاصة بالأمريكيين الذين تقدموا للعمل في هذه المنظمات. في هذا الخصوص، قال موظف سابق إن عملية جمع هذه المعلومات كانت عن غير قصد وقد حُذفت هذه السجلات من قواعد بيانات الشركة.

شارك موظفو "دارك ماتر" سابقًا في مشاريع شديدة السرية لصالح وكالة الأمن القومي، ووكالات استخبارات أمريكية أخرى

خلال سنة 2017، شرع قرصان حاسوب سابق تابع لوكالة الأمن القومي في تزويد عملاء مكتب التحقيقات الفيدرالي بمعلومات حول أنشطة الشركة، وفقًا لما جاء في تقرير أصدرته وكالة رويترز للأنباء. وكان لمجلة "فورين بوليسي" السبق في نشر تحقيق المكتب .من جهة أخرى، قالت المخبرة

لوري ستورود إنها أصبحت قلقة بشأن مراقبة الشركة للأمريكيين. وغادرت ستورود الشركة لاحقا مع العديد من الموظفين الآخرين لأنهم شكّكوا في حقيقة عدم استهداف "دارك ماتر" للمواطنين عن عمد. وسرعان ما شرع الموظفون في إيقاف الموظفين الأمريكيين في المطارات عند دخولهم الولايات المتحدة واستجوابهم بشأن عمليات مجموعة "دارك ماتر"، وفقًا لما ذكره موظفو الشركة السابقين.

مشاكل التكنولوجيا المتقدمة والبسيطة

تركز قضية وزارة العدل، التي يشرف عليها المدعون العامون في واشنطن، على الاحتيال عبر الإنترنت والنقل غير القانوني المحتمل لتكنولوجيا التجسس إلى بلد أجنبي. لكن، يواجه المدعون العامون رياحا معاكسة، بما في ذلك المخاوف الدبلوماسية المتعلقة بتعريض علاقة الولايات المتحدة بدولة الإمارات العربية المتحدة للخطر، التي تعد بلدا تربطه علاقات وثيقة بإدارة ترامب، ناهيك عن مخاوف بشأن كيفية متابعة القضية التي يمكن أن تكشف عن تفاصيل مربكة حول مدى التعاون بين شركة دارك ماتر ووكالات الاستخبارات الأمريكية.

> لا يمكن لهذه القواعد التصدي لمهارات القرصنة التي يمكن اكتسابها أمام كمبيوتر محمول، أو في وكالات الاستخبارات الأكثر تقدماً في العالم، وبيعها لأعلى مزايد

في الواقع، هناك حقيقة مفادها أن القوانين الأمريكية التي تحكم عصر الحرب الرقمية الجديد الحالي غامضة وغير ومؤهلة لمواجهة التطورات التكنولوجية السريعة. كما تهدف القواعد، التي تحكم ما يمكن لأفراد المخابرات الأمريكية والعسكريين تقديمه إلى الحكومات الأجنبية وما لا يمكنهم تقديمه، إلى التمكن من السيطرة على حرب القرن العشرين؛ على غرار بيع الصواريخ أو الطائرات في الخارج أو تدريب القوات الأجنبية على تكتيكات الجيش.

في المقابل، لا يمكن لهذه القواعد التصدي لمهارات القرصنة التي يمكن اكتسابها أمام كمبيوتر محمول، أو في وكالات الاستخبارات الأكثر تقدماً في العالم، وبيعها لأعلى مزايد. وفي هذا السياق، أفاد برايان بارثولومو، الباحث الأمني الرئيسي في شركة "كاسبرسكي لاب"، التي تعد إحدى الشركات الأمنية الرقمية أن "أسوأ أمر يحدث في الوقت الحالي هو أنه قد أصبح من السهل الحصول على الأسلحة". وأضاف بارثولومو قائلا: "لقد عملت مع الكثير من الجهات على الساحة الجديدة واكتشفت أن جميعهم لا يلعبون بالقواعد نفسها وما يحدث في الوقت الحالي يشبه وضع سلاح عسكري في يد شخص عادي".

المصدر: نيويورك تايمز

رابط المقال : https://www.noonpost.com/27079/