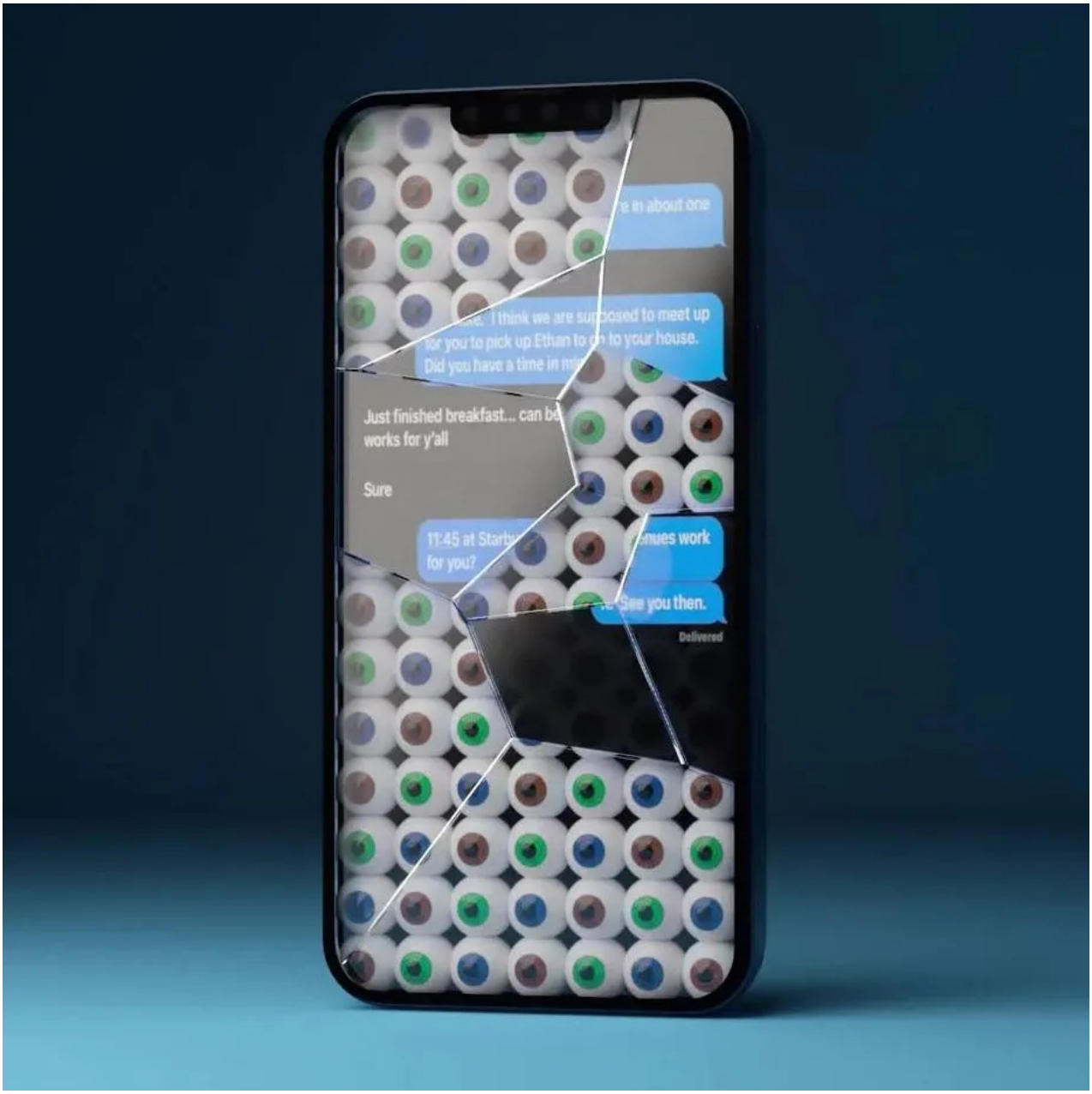
من داخل بيغاسوس وأخواتها.. قصة أشهر برامج التجسس التجارية



ترجمة وتحرير: نون بوست

يقع برلمان كتالونيا، المنطقة المتمتعة بالحكم الذاتي في إسبانيا، على أطراف المدينة القديمة في برشلونة على أطلال قلعة محصنة بناها الملك فيليب الخامس لمراقبة السكان المحليين الهائجين. بُنيت القلعة على أيدي مئات الكتالونيين عن طريق السُخرة، وما تبقى من هياكلها وحدائقها يستحضر بالنسبة للكثيرين منهم ذكريات القمع. واليوم، يؤيد غالبية البرلمانيين الكتالونيين استقلال المنطقة، وهو قرار اعتبرته الحكومة الإسبانية لا دستوريًا.

في سنة 2017، بينما كانت كتالونيا تستعد لإجراء استفتاء على الاستقلال اعتقلت الشرطة الإسبانية ما لا يقل عن 12 سياسيًا انفصاليًا. ويوم الاستفتاء، الذي حظي بتأييد 90 في المئة من الناخبين على الرغم من ضعف الإقبال، أدت مداهمات الشرطة لمراكز الاقتراع إلى إصابة مئات المدنيين. وفي الوقت

الحالي، يجتمع قادة حركة الاستقلال، الذين يعيش بعضهم في المنفى على امتداد أوروبا على انفراد ويتواصلون من خلال منصات الرسائل المشفرة.

بعد ظهر أحد أيام الشهر الماضي، التقى العضو المؤيد للاستقلال في البرلمان الأوروبي جوردي سولي بباحث الأمن الرقمي إليس كامبو في إحدى الغرف المزخرفة في البرلمان الكتالوني. سلّم سولي البالغ من العمر خمسة وأربعين عامًا هاتفه الخلوي "آيفون 8 بلس" الفضي، حيث كان يتلقى رسائل مشبوهة ويريد فحص الجهاز. وُلد كامبو ونشأ في كتالونيا وهو يدعم الاستقلال، وأمضى سنوات في العمل في شركتي "واتس آب" و"تليغرام" في سان فرانسيسكو، لكنه عاد مؤخرًا إلى وطنه الأم. والآن، يعمل كزميل في مؤسسة "سيتيزن لاب"، وهي مجموعة بحثية مقرها جامعة تورنتو تركز على انتهاكات حقوق الإنسان التي تخص التكنولوجيا المتقدمة.

في كتالونيا، جرى استهداف أكثر من 60 هاتفًا – مملوكًا لسياسيين ومحامين ونشطاء كتالونيين في إسبانيا وعبر أوروبا – باستخدام "بيغاسوس"

فحص كامبو سجلات نشاط هاتف سولي، بما في ذلك الأعطال التي تعرّض لها، ثم شغّل برنامجًا متخصصًا للبحث عن برامج التجسس المصمّمة للعمل بشكل غير مرئي. بحث كامبو عبر الهاتف عن أدلة على هجمات تتخذ أشكالًا مختلفة: وصل بعضها عبر "واتس آب" أو عبر خدمة الرسائل النصية القصيرة "إس إم إس" التي يبدو أنها تأتي من جهات اتصال معروفة؛ البعض يتطلب نقرة على رابط، والبعض الآخر يعمل بدون أي إجراء من قبل المستخدم.

حدّد كامبو إشعارًا واضحًا من وكالة الضمان الاجتماعي التابعة للحكومة الإسبانية استخدم نفس التصميم الخاص بالبرامج الضارة التي وجدتها "سيتيزن لاب" على الهواتف الأخرى. وأوضح كامبو: "بهذه الرسالة، استدلينا على أن هاتفك تعرّض للاختراق في وقت ما"، ثم اهتزّ هاتف سولي ليعطي "إشارة إيجابية" مؤكدًا هذا الأمر. وأضاف كامبو "هناك عمليتا اختراق مؤكدتان" منذ حزيران/ يونيو 2020، "في تلك الأيام، كان جهازك مُخترقًا، إذ سيطروا عليه وأمضوا على الأرجح عدة ساعات في التنزيل والاستماع والتسجيل".

استُهدف هاتف سولي ببرنامج التجسس "بيغاسوس"، المُصمّم من قبل شركة "إن إس أو غروب" الإسرائيلية، الذي يمكنه استخراج محتويات الهاتف وإتاحة الوصول إلى نصوصه وصوره أو تفعيل الكاميرا والميكروفون لتوفير المراقبة في الوقت المحدّد . على سبيل المثال، الاطّلاع على الاجتماعات السرية.

يعدّ برنامج "بيغاسوس" مفيدًا لجهات إنفاذ القانون التي تلاحق المجرمين أو للمستبدين الذين يتطلعون إلى قمع المعارضة على حد سواء. كان سولي قد تعرّض للقرصنة الإلكترونية في الأسابيع التي سبقت انضمامه إلى البرلمان الأوروبي، ليحل محل زميل كان مسجونًا بسبب أنشطته المؤيدة للاستقلال. أخبرني سولي: "كان هناك اضطهاد سياسي وقضائي واضح للناس والممثلين المنتخبين باستخدام هذه الأساليب القذرة".

نمت برامج التجسس التجارية إلى صناعة تقدّر قيمتها بنحو 12 مليار دولار، وفكرة أنها لا تخضع لقانون تنظيمي جعلها مثيرة للجدل بشكلٍ متزايد.

في كتالونيا، جرى استهداف أكثر من 60 هاتفًا – مملوكًا لسياسيين ومحامين ونشطاء كتالونيين في إسبانيا وعبر أوروبا – باستخدام "بيغاسوس". هذه أكبر مجموعة هجمات إلكترونية موثقة جنائيًا. ومن بين الضحايا ثلاثة أعضاء في البرلمان الأوروبي، من بينهم سولي. يعتقد السياسيون الكتالونيون أن الجناة المحتملين لحملة القرصنة هم مسؤولون إسبان، ويشير تحقيق "سيتيزن لاب" إلى أن الحكومة

الإسبانية استخدمت "بيغاسوس". أكد موظف سابق في "إن إس أو غروب" أن الشركة لديها حساب في إسبانيا. وسيتم الكشف عن نتائج تحقيق "سيتيزن لاب" لأول مرة في هذا المقال، إذ تحدّثتُ مع أكثر من 40 من الأفراد المستهدفين، وكشفت الأحاديث عن جو من الارتياب وانعدام الثقة. قال سولي إنّ "هذا النوع من المراقبة في البلدان الديمقراطية أمرٌ لا يُصدّق".

نمت برامج التجسس التجارية إلى صناعة تقدّر قيمتها بنحو 12 مليار دولار، وفكرة أنها لا تخضع لقانون تنظيمي جعلها مثيرة للجدل بشكلٍ متزايد. وفي السنوات الأخيرة، كشفت تحقيقات "سيتيزن لاب" ومنظمة العفو الدولية عن وجود "بيغاسوس" على هواتف السياسيين والنشطاء والمعارضين في ظل الأنظمة القمعية. وكشف تحقيق أجرته وكالة الأبحاث اللندنية "فورنسيك أركيتكشر" عن ارتباط "بيغاسوس" بـ 300 حالة عنف جسدي. وقد تم استخدامه لاستهداف أعضاء الحزب المعارض في رواندا والصحفيين الذين يفضحون الفساد في السلفادور.

"إن إس أو غروب" هي الشركة الأكثر نجاحًا وإثارةً للجدل والأكثر تأثيرًا من بين الشركات الإسرائيلية الناشئة التي جعلت من البلاد مركزًا لصناعة برامج التجسس

في المكسيك، تم العثور على "بيغاسوس" مثبّتًا على هواتف العديد من الأشخاص المقربين من الصحفي خافيير فالديز كارديناس، الذي قتل بعد تحقيق أجراه عن عصابات المخدرات. وفي الوقت الذي وافق فيه ولي العهد السعودي محمد بن سلمان على مقتل الصحفي جمال خاشقجي يُزعم أنه تم استخدام بيغاسوس لمراقبة الهواتف الخاصة بالدائرة المقرّبة من خاشقجي، مما سهّل عملية قتله في سنة 2018.

نفى بن سلمان تورطه في ذلك، وقالت شركة "إن إس أو" في بيانٍ لها: "لم تكن تقنيتنا مرتبطة بأي شكل من الأشكال بجريمة القتل البشعة". ولكن هناك أدلة على استخدام "بيغاسوس" في 45 دولة على الأقل، مع شراء برامج مماثلة من قبل وكالات إنفاذ القانون في الولايات المتحدة وأوروبا. وقد أخبرتني كريستين فلين جودوين، المديرة التنفيذية لشركة "مايكروسوفت" التي قادت جهود الشركة لمكافحة برامج التجسس، إنّ "السر الكبير والقذر هو أن جميع أنواع الحكومات تشتري هذه البرامج، ولا يقتصر الأمر فقط على الحكومات الاستبدادية".

ربما تكون "إن إس أو غروب" هي الشركة الأكثر نجاحًا وإثارةً للجدل والأكثر تأثيرًا من بين الشركات الإسرائيلية الناشئة التي جعلت من البلاد مركزًا لصناعة برامج التجسس. أجريتُ مقابلة لأول مرة مع الرئيس التنفيذي للشركة شاليف هوليو في سنة 2019، ومنذ ذلك الحين، تمكنتُ من الوصول إلى فريق الشركة ومكاتبها وتقنياتها، ووجدت أن الشركة تمر بحالة من التناقض والأزمات. وبينما يتحدّث مبرمجوها بفخر عن استخدام برامجهم في التحقيقات الجنائية – حيث تدعي الشركة أنها تبيع "بيغاسوس" فقط لوكالات إنفاذ القانون والاستخبارات – فإن التجسس والمساومة غير المشروعة من خلاله تزدهر على منصات التكنولوجيا.

بلغت قيمة الشركة أكثر من مليار دولار، لكنها الآن تكافح لسداد ديونها وتحارب مجموعة من داعمي الشركات، ووفقًا لمراقبي القطاع، فإن جهودها طويلة الأمد لبيع منتجاتها إلى سلطات إنفاذ القانون الأمريكية جزئيًا من خلال فرع أمريكي، وهو ويست بريدج تكنولوجي، متعثرة. وهي تواجه أيضًا العديد من الدعاوى القضائية في بلدان متعددة رفعتها كل من شركة ميتا (فيسبوك سابقًا) وآبل والأفراد الذين تم اختراق أجهزتهم من قبل "إن إس أو".

في بيان لها، قالت الشركة إنها "استهدفت من قبل عدد من منظمات الدعوة ذات الدافع السياسي، والعديد منها لديها تحيزات ضد إسرائيل"، وأضافت "لقد تعاونا بشكل متكرر مع التحقيقات الحكومية، حيث تكون المزاعم الموثوقة مستحقة، وتعلمنا من كل هذه النتائج والتقارير، وحسّنّا الإجراءات الوقائية

في تقنياتنا". وقد أخبرني هوليو "لم أتخيل أبدًا في حياتي أن هذه الشركة ستصبح مشهورة...لم أتصور أننا سننجح لهذا الحد. ولم أتخيل أنها ستكون مثيرة للجدل هكذا".

هوليو البالغ من العمر أربعين سنة، لديه مشية متثاقلة وملامح ممتلئة. وعادة ما يرتدي قمصانًا وسراويل جينز فضفاضة، وشعره في قصة قصيرة عملية. زرته الشهر الماضي في شقته المزدوجة في مبنى شاهق فاخر في بارك تزامريت، أفخم حي في تل أبيب حيث يعيش مع أطفاله الصغار الثلاث وزوجته أفيتال، الحامل في الرابع. هناك مسبح في الطابق العلوي من شقة هوليو، وفي الأسفل في غرفة المعيشة ذات الارتفاع المضاعف، آلة لعب أركيد المصممة خصيصًا والمليئة بالألعاب القديمة وتحمل صورة كرتونية له، مرتدي نظارات شمسية، جوار كلمة "هوليو" بحجم خط ثمانية كبير. تهتم أفيتال بالأطفال والتجديدات المتكررة ومجموعة دائمة التغير من الحيوانات الأليفة: يبقى الأرنب، لكن الببغاء لا يفعل. وتمتلك العائلة كلب بودل يدعى مارشميلو رينبو سبرينكل.

أسس كل من هوليو وعمري لافي ونيف كرمي مجموعة إن إس أو في 2010، مبتكرين اسمها من الأحرف الأولى من أسمائهم واستأجروا مساحة في حظيرة دجاج محولة في كيبوتس. تمتلك الشركة الآن حوالي 800 موظف، وأصبحت تقنياتها أداة رائدة لعمليات القرصنة التي ترعاها الدولة، وهي فعالة في الصراع بين القوى العظمى.

موظف في "إن إس أو": "نحن نسمع عن كل كل مكالمة يتم اختراقها في جميع أنحاء العالم، ونحصل على تقرير فوري"

خلص باحثوا "سيتزن لاب" إلى أنه في 7 تموز/ يوليو 2020، تم استخدام بيغاسوس لإصابة جهاز متصل بالشبكة في عنوان 10 شارع داونينغ، مكتب بوريس جونسون، رئيس وزراء المملكة المتحدة. وأكد مسؤول حكومي لي أنه تم اختراق الشبكة دون تحديد برنامج التجسس المستخدم. يتذكر جون سكوت رايلتون، الباحث الأقدم في سيتزن لاب، "عندما وجدنا الحالة رقم 10، اتسعت عيناي من الصدمة"، وأضاف بيل ماركزاك وهو باحث أقدم آخر هناك، "نشك في أن هذا يشمل تسربا للبيانات". أخبرني المسؤول أن المركز الوطني للأمن السيبراني، وهو فرع للمخابرات البريطانية، قد اختبر عدة هواتف في شارع داونينغ، بما في ذلك هاتف جونسون. وقال المسؤول إنه كان من الصعب إجراء بحث شامل للهواتف – "إنها مهمة صعبة للغاية"، ولم تتمكن الهيئة من تحديد مكان الجهاز المصاب. ولم يتم تحديد طبيعة البيانات التي تم أخذها.

اشتبهت مؤسسة "سيتزن لاب"، بناءً على الخوادم التي ارسلت البيانات لها، في أن الإمارات العربية المتحدة على الأرجح كانت وراء الاختراق. قال سكوت رايلتون: "كنت أعتقد أن الولايات المتحدة والمملكة المتحدة وقوى إلكترونية أخرى من الدرجة الأولى يتقدمون ببطء تجاه بيغاسوس لأنه لا يشكل تهديدًا مباشرًا لأمنهم القومي". وأضاف "أدركت أنني كنت مخطئًا: حتى المملكة المتحدة كانت تقلل من شأن تهديد بيغاسوس، وقد تم استهدافها بشكل مذهل".

لم تستجب الإمارات للطلبات المتكررة للتعليق، وأخبرني موظفو "إن إس أو" أن الشركة لم تكن على علم بالاختراق. قال أحدهم، "نحن نسمع عن كل كل مكالمة يتم اختراقها في جميع أنحاء العالم، ونحصل على تقرير فوري" – وهو بيان يتعارض مع حجج الشركة المتكررة بأنها لا تعلم الكثير حول أنشطة عملائها. وقد أضافت الشركة في بيانها أن "المعلومات التي أثيرت في الاستطلاع تشير إلى أن هذه المزاعم، مرة أخرى خاطئة ولا يمكن أن تكون مرتبطة بمنتجات إن إس أو لأسباب تكنولوجية وتعاقدية".

إن تأسيس قوانين صارمة حول من يمكنه استخدام برامج التجسس التجارية هو أمر معقد بسبب حقيقة أن هذه التكنولوجيا مقدمة كأداة للدبلوماسية، ويمكن أن تكون النتيجة فوضوية.

وفقًا لتحليل أجرته مؤسسة سيتزن لاب، تم اختراق الهواتف المتصلة بوزارة الخارجية باستخدام بيغاسوس في خمس حالات على الأقل، من تموز/ يوليو 2020 وحتى حزيران/ يونيو 2021. وأكد المسؤول الحكومي أنه تم الكشف عن دلائل القرصنة. ووفقًا لسيتزن لاب، أشارت خوادم الوجهة أن الهجمات مصدرها دول مثل الإمارات والهند وقبرص، علما بأن "المسؤولين في الهند وقبرص لم يستجيبوا لطلبات التعليق". بعد حوالي سنة من اختراق شارع داونينغ، كشفت محكمة بريطانية أن الإمارات استخدمت بيغاسوس للتجسس على الأميرة هيا، الزوجة السابقة للشيخ محمد بن راشد آل مكتوم حاكم دبي. كان مكتوم منخرطا في نزاع على الحضانة مع هيا، التي فرت مع طفليهما إلى المملكة المتحدة، كما تم استهداف محاميها البريطانيين. أخبرني مصدر متورط بشكل مباشر أن أحد المبلغين عن المخالفات اتصل بـ "إن إس أو" لتنبيهها إلى الهجوم الإلكتروني على هيا.

قامت الشركة بتجنيد شيري بلير، زوجة رئيس الوزراء السابق توني بلير ومستشارة إن إس أو، لإخطار محامي هيا. أخبرني هوليو: "لقد نبهنا الجميع في الوقت المناسب". بعد ذلك بوقت قصير، أغلقت الإمارات نظام بيغاسوس الخاص بها، وأعلنت إن إس أو أنها ستمنع برامجها من استهداف أرقام هواتف المملكة المتحدة، كما فعلت منذ فترة طويلة للأرقام الأمريكية.

في أماكن أخرى من أوروبا، ساهم بيغاسوس في سد الحاجة إلى هيئات إنفاذ القانون التي كانت تتمتع في السابق بقدرة محدودة على الاستخبارات الإلكترونية. حسب هوليو "جميع الحكومات في أوروبا تستخدم تقريبًا أدواتنا". وأضاف مسؤول استخباراتي إسرائيلي كبير سابق أن "إن إس أو تحتكر أوروبا". وقد اعترفت السلطات الألمانية والبولندية والمجرية باستخدام بيغاسوس. وتستخدمه كذلك سلطات إنفاذ القانون البلجيكية، رغم أنها لن تعترف بذلك. قال متحدث باسم الشرطة الفيدرالية البلجيكية إنها تحترم "الإطار القانوني لاستخدام الأساليب التطفلية في الحياة الخاصة". وأفاد مسؤول أقدم في إنفاذ القانون الأوروبي تستخدم وكالته بيغاسوس، بأنها ألقت نظرة من الداخل على المنظمات الإجرامية: "متى يريدون تخزين الغاز، والذهاب إلى المكان، ووضع المتفجرات؟" وأكد أن وكالته تستخدم بيغاسوس فقط كملاذ أخير، بموافقة المحكمة، لكنه اعترف، "إنه مثل السلاح... يحدث دائمًا أن يستخدمه فرد بطريقة خاطئة".

كانت الولايات المتحدة مستهلكًا وضحية لهذه التكنولوجيا. على الرغم من أن وكالة الأمن القومي ووكالة المخابرات المركزية لديها تقنيات المراقبة الخاصة بها، إلا أن المكاتب الحكومية الأخرى، بما في ذلك في الجيش ووزارة العدل، اشترت برامج تجسس من الشركات الخاصة، وذلك وفقًا لأشخاص متورطين في تلك المعاملات. وذكرت صحيفة "التايمز" أن مكتب التحقيقات الفيدرالي اشترى واختبر بيغاسوس في سنة 2019، ولكن الوكالة نفت توزيع التكنولوجيا.

إن تأسيس قوانين صارمة حول من يمكنه استخدام برامج التجسس التجارية هو أمر معقد بسبب حقيقة أن هذه التكنولوجيا مقدمة كأداة للدبلوماسية، ويمكن أن تكون النتيجة فوضوية. ذكرت صحيفة "التايمز" أن وكالة المخابرات المركزية دفعت لجيبوتي للحصول على بيغاسوس، كوسيلة لمحاربة الإرهاب. ووفقًا لتحقيق لم يتم الإبلاغ عنه سابقًا بواسطة "واتس آب"، فقد تم استخدام هذه التقنية أيضًا ضد أعضاء حكومة جيبوتي أنفسهم، بما في ذلك رئيس وزرائها، عبد القادر كامل محمد، ووزير داخليته حسن عمر.

ترى مجموعة "إن إس أو" نفسها على أنها نوع من تجار الأسلحة الذين يعملون في المجال بدون معايير ثابتة.

في السنة الماضية، ذكرت "صحيفة واشنطن" بوست وكشفت شركة آبل في ملف قانوني، أنه تم اختراق أجهزة آيفون الخاصة بـ 11 شخصًا يعملون لدى الحكومة الأمريكية في الخارج، وكثير منهم في سفارتها

في أوغندا، باستخدام بيغاسوس. علقت مجموعة إن إس أو، "بعد تحقيق إعلامي حول الحادث، أوقفت الشركة فورًا جميع العملاء ذوي الصلة المحتملة بهذه القضية، بسبب حدة المزاعم، وحتى قبل البدء بالتحقيق". وتحقق إدارة بايدن في استهداف إضافي للمسؤولين الأمريكيين، كما أطلقت مراجعة للتهديدات التي تشكلها أدوات القرصنة التجارية الأجنبية. أخبرني مسؤولو الإدارة أنهم يخططون لأخذ خطوات جديدة أكثر شراسة. وذكر أدريان واتسون، المتحدث باسم البيت الأبيض، أن الأهم هو "حظر الحكومة الأمريكية من شراء أو استخدام برامج تجسس تجارية أجنبية تشكل مخاطر على مكافحة التجسس أو أمن الحكومة الأمريكية أو تم إساءة استخدامها في الخارج".

في تشرين الثاني/ نوفمبر، أضافت وزارة التجارة مجموعة إن إس أو، إلى جانب العديد من صانعي برامج التجسس، لقائمة الكيانات الممنوعة من شراء تلك التقنيات من الشركات الأمريكية دون ترخيص.

كنت مع هوليو في نيويورك اليوم التالي. لم يعد بإمكان "إن إس أو" شراء أنظمة تشغيل ويندوز وآيفون وخوادم أمازون للتخزين على الشبكة – وهي أنواع المنتجات التي تستخدمها لإدراة أعمالها وبناء برامجها للتجسس. وقال لي "إنه أمر جسيم. نحن لم نبع أبدًا لأي دولة ليست حليفة للولايات المتحدة أو لإسرائيل. ولم نبع أبدًا لأي دولة لا تتعامل معها الولايات المتحدة". وأضاف هوليو: "إن الصفقات مع العملاء الأجانب تتطلب "موافقة مكتوبة مباشرة من حكومة إسرائيل".

أخبرتني إيفا غالبرين، مديرة الأمن السيبراني في مؤسسة الحدود الإلكترونية: "أعتقد أن القادة الأمريكيين لم يفهموا ذلك جيدًا، فهم دائما ما يتوقعون أن تقوم الحكومة الإسرائيلية بتضييق الخناق على مجموعة "إن إس أو" لهذا الغرض، في حين أنهم يقدمون في الواقع ما تطلبه الحكومة الإسرائيلية". وفي الشهر الماضي، ذكرت صحيفة "واشنطن بوست" أن إسرائيل منعت أوكرانيا من شراء بيغاسوس لعدم رغبتها في عزل روسيا. وقال هوليو: "لقد حصلنا على إذن من حكومة إسرائيل في كل ما نقوم به. وقد قام الأمريكيون ببناء آلية التنظيم بأكملها في إسرائيل".

ترى مجموعة "إن إس أو" نفسها على أنها نوع من تجار الأسلحة الذين يعملون في المجال بدون معايير ثابتة. وأضاف هوليو: "هناك اتفاقيات جنيف لاستخدام السلاح. وأؤمن بضرورة وجود اتفاقية للدول التي يجب أن تتفق فيما بينها على الاستخدام المناسب لمثل هذه الأدوات للحرب الإلكترونية". وفي ظل غياب التنظيم الدولي، تدور معركة بين الشركات الخاصة؛ فمن ناحية، هناك شركات مثل مجموعة "إن إس أو"؛ ومن ناحية أخرى، هناك المنصات التكنولوجية الرئيسية التي تثبت من خلالها هذه الشركات برامج التجسس الخاصة بها.

يوم الخميس الموافق لـ 2 أيار/ مايو 2019، كان مهندس البرمجيات كلوديو دان جورجي يعمل في المبنى العاشر في حرم فيسبوك في مينلو بارك، حيث كان يدير فريقًا من سبعة أشخاص مسؤولين عن البنية التحتية للاتصال الصوتي والفيديو في واتس آب. وقد ولد جورجي،الذي يبلغ من العمر خمسة وثلاثين سنة في رومانيا، بجسد نحيل وشعر داكن قصير. و قد استخدم خلال السنوات التسع التي قضاها في فيسبوك صورة احترافية يرتدي فيها سترة سوداء يبدو فيها مثل إليوت ألدرسون، بطل دراما القرصنة "السيد روبوت". يتكون المبنى العاشر من طابقين مع مساحات عمل مفتوحة وجدران ذات ألوان زاهية وألواح بيضاء، يعمل فيها مهندسون في العشرينات والثلاثينات من العمر، منحنين على لوحات المفاتيح. كما كُتبت كلمة "تركيز" على الحائط مختومة على قطع مغناطيسية متناثرة حول المكتب. وهو ما يتذكره جورجي قائلاً: "لطالما شعرت وكأنها كنيسة". ويُعتبر واتس آب، الذي اشتراه فيسبوك مقابل تسعة عشر مليار دولار في سنة 2014، تطبيق المراسلة الأكثر شعبية في العالم، مع حوالي ملياري مستخدم شهريًا.

قدّم فيسبوك المنصة التي تستخدم التشفير من البداية إلى النهاية كمنصة مثالية للاتصالات الحساسة؛

وفي الوقت الراهن استغرق فريق أمن الشركة أكثر من سنتين في محاولة لتعزيز أمن منتجاتها. ومن ضمن المهام كان هناك النظر في "إشارة الرسائل" التي يرسلها مستخدمو واتس آب تلقائيًا إلى خوادم الشركة من أجل بدء المكالمات. وفي ذلك المساء، تم تنبيه جورج إلى رسالة غير عادية، حيث يحتوي جزء من الرمز الذي كان يهدف إلى إملاء رنة الهاتف على رمز مع تعليمات غريبة لهاتف المستلم.

لطالما كانت الحالات الشاذة في نظام واسع مثل فيسبوك روتينية وغير ضارة. ويمكن أن يأتي الرمز غير المألوف من نسخة قديمة من البرنامج، أو يمكن أن يكون بمثابة اختبار ضغط يقوم به فريق ريد في فيسبوك الذي يجري هجمات محاكاة. ولكن مع البدء في فحص الرمز، أصبح المهندسون في المكاتب الدولية لفيسبوك قلقين. وقد أخبرني أوتو إيبلينج، الذي كان يعمل في فريق أمن فيسبوك في لندن، أن الرمز يبدو "مصقولا، ورائعا، ومثيرا للقلق". وفي صباح اليوم التالي بعد اكتشاف الرسالة، كتب خواكين مورينو جاريجو، وهو عضو آخر في فريق الأمن في لندن، عن نظام المراسلة الداخلية للشركة بالنظر لمدى تعقيد الرمز: "من المرجح أن المهاجم عثر على ثغرة أمنية".

غالبًا ما يصف المبرمجون الذين يعملون في قضايا الأمن عملهم من حيث نقاط الضعف واستغلالها. وقارن مهندس في شركة آبل، إيفان كرستيتش، هذا المفهوم بمشهد سرقة في فيلم "أوشن 12"، حيث ترقص شخصية في قاعة مليئة بأشعة الليزر التي تطلق إنذارات. وقال كرستيتش: "في هذا المشهد، تتمثل نقطة الضعف في وجود مسار عبر جميع أنواع الليزر، حيث يُمكن للشخص أن يعبر الغرفة. ولكن الاستغلال يكمن فعلا في أن شخصًا ما يجب أن يكون راقصًا دقيقًا بدرجة كافية ليكون قادرًا بالفعل على أداء تلك الرقصة".

أكثر شركات القرصنة التجارية شهرة في العالم غير محمية بشكل ملحوظ؛ ففي بعض الأحيان، كان هناك حارس أمن واحد.

بحلول وقت متأخر من يوم الأحد، أصبحت مجموعة من المهندسين الذين يعملون على حل المشكلة مقتنعين بأن الرمز كان استغلالا نشطا كان يهاجم نقاط الضعف في بنيتهم التحتية وهم يشاهدون ذلك. ويمكنهم رؤية أنه تم نسخ البيانات من هواتف المستخدمين. ويتذكر جورجي: "لقد كان الأمر مخيفًا، وكأن العالم يهتز نوعًا ما من تحتك، لأنك بنيت هذا الشيء الذي يستخدمه الكثير من الناس رغم هذا الخلل الكبير".

وبسرعة، قام المهندسون بتحديد طرق لمنع الرمز المسيء، لكنهم ناقشوا ما إذا كان عليهم فعل ذلك، قد يؤدي حظر الوصول إلى تنبيه المهاجمين، وربما يسمح لهم بمحو آثارهم قبل أن يتمكن المهندسون من التأكد من أن أي حل سيغلق جميع السبل الممكنة للهجوم. وقال إيبيلينج: "سيكون ذلك بمثابة مطاردة الأشباح". وقد كتب مهندس أمن واتس آب، أندري لابونتس، في رسالة داخلية: "اتخذنا قرارًا بعدم تنفيذ الإصلاح من جانب الخادم، لأننا لا نفهم السبب الجذري لتأثير المستخدمين وأرقام وتقنيات المهاجمين المحتملة الأخرى".

يوم الاثنين، في اجتماعات الأزمات مع كبير المسؤولين التنفيذيين في واتس آب، ويل كاثكارت، ورئيس الأمن في فيسبوك، أخبرت الشركة مهندسيها في جميع أنحاء العالم أن أمامهم 48 ساعة للتحقيق في المشكلة. وتذكر كاثكارت القلق قائلا: "ما هو حجم الضحايا؟ كم عدد الأشخاص الذين أصيبوا بهذا؟". وقررت قيادة الشركة عدم تبليغ سلطات إنفاذ القانون على الفور، خوفًا من أن يقوم المسؤولون الأمريكيون بإبلاغ المتسللين. وقال لي: "هناك خطر – قد تستهدف عميلا". (وقد كانت مخاوفهم صحيحة؛ فبعد أسابيع، ذكرت التايمز، بأن مكتب التحقيقات الفيدرالي استضاف مهندسي مجموعة "إن إس أو" في منشأة في نيوجيرسي، حيث اختبرت الوكالة برنامج بيغاسوس الذي اشترته). وقد نبه كاثكارت مارك زوكربيرغ، الذي اعتبر المشكلة "مروعة"، وضغط على الفريق للعمل بسرعة. أما بالنسبة لجورجي،

فقد كان يوم إثنين مرعبا، حيث استيقظ في الساعة السادسة صباحًا تقريبًا، ثم عمل حتى لم يعد بإمكانه البقاء مستيقظًا.

يقع مقر مجموعة "إن إس أو" في مبنى مكاتب من الزجاج والصلب في هرتسليا، وهي ضاحية خارج تل أبيب. وتعد المنطقة موطنا لمجموعة من شركات التكنولوجيا من قطاع الشركات الناشئة المزدهر في إسرائيل، حيث يبعد الشاطئ عشرين دقيقة سيرا على الأقدام. كما أن أكثر شركات القرصنة التجارية شهرة في العالم غير محمية بشكل ملحوظ؛ ففي بعض الأحيان، كان هناك حارس أمن واحد.

يجتمع المبرمجون الذين يرتدون أغطية للرأس في الطابق الرابع عشر من المبنى تحديدا في كافتيريا مجهزة بآلة إسبرسو وعصارة برتقال، أو يجلسون على شرفة تطل على البحر الأبيض المتوسط، حيث يوجد ملصق كتب عليه "كانت الحياة أسهل بكثير عندما كان التفاح والتوت مجرد فواكه". وتأخذك السلالم إلى مجموعات البرمجة المختلفة التي تمتلك كل منها مساحة ترفيهية خاصة بها، مع أرائك وبلاي ستيشن إس 5. كما يحب فريق بيغاسوس لعب لعبة كرة القدم "إلكترونيكس آرتس".

أخبرني الموظفون أن الشركة تحافظ على سرية تقنيتها من خلال قسم أمن المعلومات مع عشرات الخبراء. وذكر موظف سابق: "هناك قسم كبير جدًا في الشركة مسؤول عن التبييض، أود أن أقول إن كل اتصال بين الشبكة والعميل يعود الفضل فيه إلى مجموعة "إن إس أو". كما أنهم يشترون خوادم "في بي إن" حول العالم، ولديهم هذه البنية التحتية بأكملها التي أعدت بحيث لا يمكن تتبع أي اتصالات".

ابتكر فريق الأمان في شركة "فيسبوك" عملية مراوغة: سوف يحاكون جهازًا مخترقًا ليجعلوا خوادم "مجموعة إن إس أو" ترسل إليهم نسخة من الشيفرة. يقول جورجي: "لقد كان برنامجهم ذكيًا بدرجة كافية بحيث لم ينخدع بهذا الأمر".

رغم هذه الاحتياطات، تمكن مهندسو واتس آب من تتبع البيانات بما في ذلك مصدر الاختراق وعنوان بروتوكول الإنترنت وعناوين مرتبطة بالممتلكات وخدمات الويب التي تستخدمها مجموعة "إن إس أو". ويتذكر جورجي قائلاً: "لقد علمنا الآن أن أحد أكبر الجهات الفاعلة في مجال التهديد في العالم لديه برنامج يستهدف ثغرات واتس آب. ولقد كان الأمر مثيرا، لأنه من النادر جدًا التقاط بعض هذه الأشياء. لكن في الوقت نفسه، كان الأمر مخيفًا للغاية". بدأ الضحايا في الظهور. وكتب المهندس الأمني لابونتس في نظام الرسائل الخاص بالشركة: "من المرجح وجود صحفيين نشطاء في مجال حقوق الإنسان وآخرين على القائمة". (في النهاية، حدد الفريق حوالي 1400 من مستخدمي واتس آب الذين تم استهدافهم).

بحلول منتصف الأسبوع، كان حوالي ثلاثين شخصًا يعملون على حل المشكلة في تتابع على مدى 24 ساعة، بحيث تنام مجموعة بينما تتصل المجموعة الأخرى على الإنترنت. مددت شركة "فيسبوك" الموعد النهائي للفريق، وبدأوا في إجراء هندسة عكسية للشيفرة الخبيثة. يقول جورجي: "للأمانة إنه عمل رائع، أعني أنه عندما تنظر إليه يبدو كالسحر". وأضاف: "هؤلاء الناس أذكياء للغاية، أنا لا أتفق مع ما يفعلونه، لكن يا رجل هذا شيء معقد للغاية قاموا بإنشائه." حفّز البرنامج تشغيل مكالمتي فيديو في تعاقب وشيك، تنضم إحداهما إلى الأخرى مع إخفاء الشفرة الخبيثة في إعداداتهما. استغرقت العملية بضع ثوانٍ فقط، وحذفت أي إشعارات بعد ذلك مباشرة. استخدمت الشفرة تقنية تُعرف باسم "تجاوز سعة المخزن المؤقت"، وهي تحميل مساحة من الذاكرة على الجهاز ببيانات أكثر مما يمكن أن تستوعبه. يشرح جورجي ذلك قائلاً: "يبدو الأمر كما لو كنت تكتب على قطعة من الورق وتتجاوز الحدود. أنت تبدأ بالكتابة على أي سطح أليس كذلك؟ تبدأ الكتابة على الطاولة". يُمكّن تجاوز السعة البرنامج من الكتابة فوق أقسام الذاكرة المحيطة بحرية. يضيف جورجي: "يمكنك جعلها تفعل ما تريد."

لقد تحدثت مع نائب رئيس تطوير المنتجات في "مجموعة إن إس أو"، الذي طلبت مني الشركة تحديده فقط باسمه الأول عمر، الذي أشار دون سخرية واضحة إلى مخاوف تتعلق بالخصوصية. أخبرني عمر: "يمكن أن تجد الأركان والزوايا المظلمة التي تمكنك من القيام بشيء لم يقصده مصمم المنتج". وبمجرد السيطرة، تقوم الثغرة بتحميل المزيد من البرامج مما يسمح للمهاجم باستخراج البيانات أو تنشيط الكاميرا أو الميكروفون. كانت العملية بأكملها عبارة عن "نقرة صفرية" ولم تتطلب أي إجراء من مالك الهاتف.

تم تصميم البرنامج بواسطة مجموعة الأبحاث الأساسية التابعة "لمجموعة إن إس أو" والتي تتألف من العشرات من مطوري البرامج. قال عمر: "أنت تبحث عن حل سحري، عن ثغرة بسيطة يمكن أن تغطي أكبر عدد ممكن من الأجهزة المحمولة في جميع أنحاء العالم". أوضح جورجي: "يعتقد الكثير من الناس كما تعلمون أن جميع القراصنة مثل شخص واحد فقط متواجد في غرفة مظلمة يستعمل لوحة المفاتيح، أليس كذلك؟ لكن هذا ليس هو الواقع – هؤلاء الأشخاص مثل شركة تكنولوجيا أخرى".

قدمت شركات مثل "مايكروسوفت" و"غوغل" و"سيسكو" وغيرها موجزًا قانونيًا يدعم دعوى شركة "واتساب" ضد شركات التجسس

من الشائع لشركات التكنولوجيا أن توظف أشخاصًا لديهم معرفة مسبقة في القرصنة، وأن تقدم مكافآت للمبرمجين الخارجيين الذين يحددون نقاط الضعف في أنظمتهم. إن عنوان مقر شركة "فيسبوك" المميز هو طريق المخترق الأول. وغالبًا ما يصف زملاء المهندسين في "مجموعة إن إس أو" و"واتساب" الأقرب إلى البرمجة بأنهم انطوائيون ملتوون، ويشبهون النماذج الأصلية للقرصنة في الخيال. يقول عمر عن المبرمجين الذين يعملون على تطبيق "بيغاسوس": "إنهم أشخاص مميزون، بعضهم لا ينام لمدة يومين. ويصابون بالجنون عندما لا ينامون".

في وقت متأخر من الأسبوع، ابتكر فريق الأمان في شركة "فيسبوك" عملية مراوغة: سوف يحاكون جهازًا مخترقًا ليجعلوا خوادم "مجموعة إن إس أو" ترسل إليهم نسخة من الشيفرة. يقول جورجي: "لقد كان برنامجهم ذكيًا بدرجة كافية بحيث لم ينخدع بهذا الأمر، ولم نتمكن أبدًا من وضع أيدينا على ذلك".

قال عمر: "إنها لعبة قط وفأر"، رغم أن "مجموعة إن إس أو" تؤكد أن عملاءها يتحكمون في استخدام تطبيق "بيغاسوس" إلا أنها لا تجادل في دورها المباشر في هذه التبادلات. يقول هوليو: "يتم تصحيح الأمور كل يوم، وهذا هو العمل الروتيني هنا".

استقبل مستخدمو "واتساب" في بعض الأحيان مكالمات فائتة متكررة، ولكن لم يتم تثبيت الفيروس بنجاح. وبمجرد أن علم المهندسون بهذه الحوادث، تمكنوا من دراسة كيف بدا الأمر عندما فشل تطبيق "بيغاسوس". أخبرني جورجي في نهاية الأسبوع قائلاً: "قلنا حسنًا ليس لدينا فهم كامل في هذه المرحلة، لكنني أعتقد أننا التقطنا ما يكفي". في صباح يوم الجمعة، أخطر فيسبوك وزارة العدل، التي تنظر في قضية ضد "مجموعة إن إس أو". ثم قامت الشركة بتحديث خوادمها لحظر الشفرة الخبيثة. كتب جورجي في خدمة المراسلة الداخلية بعد ظهر ذلك اليوم: "جاهز للتشغيل". تم إنشاء الإصلاح ليبدو كأنه صيانة روتينية للخادم، حتى تستمر "مجموعة إن إس أو" في محاولة الهجمات وتزويد شركة "فيسبوك" بمزيد من البيانات.

ذكر مهندسو "فيسبوك" في اليوم التالي أن "مجموعة إن إس أو" بدأت في إرسال ما يشبه حزم البيانات الخادعة، التي تكهنوا بأنها وسيلة لتحديد ما إذا كانت أنشطة "مجموعة إن إس أو" قيد المراقبة. أخبرني جورجي في إحدى الحزم الخبيثة، أرسلوا بالفعل رابطًا لموقع "يوتيوب"، كنا جميعًا نضحك بجنون عندما رأينا محتوى الرابط". لقد كان الرابط يؤدي إلى فيديو موسيقي لأغنية ريك آستلي "لن أتخلى عنك

أبدأ" من سنة 1987. يعتبر إعداد كمين للأشخاص الذين لديهم رابط للأغنية أسلوبًا شائعًا في التصيّد يُعرف باسم "التصيّد المزيف". يتذكر أوتو إيبلينج ذلك قائلاً: "التصيّد المزيف هو، لا أعرف بالضبط، شيء قد يفعله زميلي بي وليس النوع من الأشخاص الذين قد ترعاهم الدولة". أخبرتني كاثكارت قائلة: "كانت هناك رسالة بداخلها. كانوا يقولون نحن نعرف ماذا فعلت نحن نراك." (يقول هوليو والعديد من موظفي "مجموعة إن إس أو" الآخرين إنهم لا يستطيعون تذكر "التصيّد المزيف" في تطبيق "واتساب".

في الأشهر التي تلت ذلك، بدأ تطبيق "واتساب" بإعلام المستخدمين الذين تم استهدافهم. وشملت القائمة العديد من المسؤولين الحكوميين، من بينهم سفير فرنسي واحد على الأقل ورئيس وزراء جيبوتي. تقول كاثكارت: " كما تعلمون، لم يكن هناك تداخل بين هذه القائمة وما شابه ذلك من التوعية المشروعة لإنفاذ القانون. يمكنك أن ترى أنه من الرائع وجود الكثير من البلدان في جميع أنحاء العالم. هذه ليست مجرد وكالة أو منظمة واحدة في بلد واحد تستهدف الأشخاص.". بدأ تطبيق "واتساب" أيضًا العمل مع "سيتيزن لاب" الذي حذّر الضحايا من خطر تعرضهم للاختراق مرة أخرى، وساعدهم على تأمين أجهزتهم. يقول جون سكوت رايلتون: "كان من المثير للاهتمام حقًا عدد الأشخاص الذين كانوا مستائين وحزينين، ولكنهم بشكل أعمق لم يتفاجؤوا، بل شعروا بالارتياح كما لو كانوا يحصلون على تشخيص لمرض غامض عانوا منه لسنوات عديدة".

يوجد خمسة أشخاص في المجموعة الأولية التي حددها تطبيق "واتساب" من كاتالونيا، بما في ذلك مشرعين منتخبين وناشط. أدرك كامبو، الباحث الأمني الكتالوني، أن القضايا "ربما كانت مجرد قمة جبل الجليد". وأضاف: "هذا عندما وجدت نفسي في تقاطع التكنولوجيا، وهو منتج ساهمت في بنائه كما بنيت بلدي الأم".

واصلت شركة "واتساب" مشاركة المعلومات مع وزارة العدل، وقد رفعت الشركة في ذلك الخريف دعوى قضائية ضد "مجموعة إن إس أو" في محكمة فيدرالية. أخبرتني كاثكارت أن "مجموعة إن إس أو" اخترقت أنظمتنا وألحقت بنا أضرارًا، ما أقصده ألن تفعل شيئًا حيال ذلك؟ لا، يجب أن تكون هناك عواقب".

باحثون من معمل الأبحاث للأمن السيبراني بشركة آبل: "تم اختراق هاتف الناشطة السعودية في مجال حقوق المرأة، لجين الهذلول، من خلال الرسائل الإلكترونية".

يقول هوليو "أتذكر أنه في يوم من الأيام رُفعت الدعوى القضائية، وأغلقوا حساب "فيسبوك" لموظفينا، وكان ذلك بمثابة حركة متنمرة للغاية من طرفهم". وأضاف مشيرًا إلى الفضائح المتعلقة بدور فيسبوك في المجتمع: "أعتقد أنه نفاق كبير". وقد دفعت "مجموعة إن إس أو" باتجاه رفض الدعوى بحجة أن عمل الشركة نيابة عن الحكومات يجب أن يمنحها نفس الحصانة من الدعاوى القضائية التي تتمتع بها تلك الحكومات. وقد رفضت المحاكم الأمريكية هذه الحجة حتى الآن.

لم يكن الموقف العدواني لشركة "واتساب" معتادًا بين شركات التكنولوجيا الكبرى، التي غالبًا ما تحجم عن لفت الانتباه إلى الحالات التي تعرضت فيها أنظمتها للاختراق. أشارت الدعوى إلى حدوث تحول، وقد أصبحت شركات التكنولوجيا الآن متحالفة بشكل علني ضد بائعي برامج التجسس. وقد وصف جورجي ذلك قائلاً: إنها "لحظة انفجار كل شيء".

قدمت شركات مثل "مايكروسوفت" و"غوغل" و"سيسكو" وغيرها موجزًا قانونيًا يدعم دعوى شركة "واتساب"، وقد ساعدت جودوين، المسؤولة التنفيذية في شركة "مايكروسوفت"، في توحيد تحالف من الشركات. وهي تقول "لم نتمكن من السماح "لمجموعة إن إس أو" أن تنتصر بحجة أن الحكومة تستخدم بكل بساطة منتجاتك وخدماتك، لذلك تحصل على حصانة سيادية مثلها، إنّ الأثر المضاعف لذلك سيكون خطيرًا للغاية."

يعتقد هوليو أنه عندما تستخدم الحكومات تطبيق "بيغاسوس"، فمن غير المرجح أن تعتمد على حاملي المنصات من أجل وصول أوسع إلى بيانات المستخدمين "عبر الباب الخلفي". وأعرب عن سخطه من الدعوى. وأخبرني "بدلاً من ذلك، كما نقول في الواقع – حسنًا شكرًا لكم – سوف يقوموا بمقاضاتنا، لا بأس فلنتقابل في المحكمة".

تمتلك شركة "مايكروسوفت" أيضًا فريق أمان يشارك في مكافحة القراصنة. ومع أن برنامج "بيغاسوس" ليس مصممًا لاستهداف المستخدمين من خلال منصات شركة "مايكروسوفت"، إلا أن أربعة أشخاص على الأقل في كتالونيا من مُشغلي برنامج "مايكروسوفت ويندوز" قد تعرضوا للهجوم بواسطة برامج التجسس التي صنعتها شركة "كانديرو"، وهي شركة ناشئة أسسها موظفون سابقون في "مجموعة إن إس أو"، (قال متحدث باسم شركة "كانديرو" إنها ترغم في أن يتم استخدام منتجاتها "لغرض وحيد وهو منع الجريمة والإرهاب).

في شهر شباط / فبراير 2021، وجدت "سيتزن لاب" دليلا على وجود اختراق نشط – وهو أمر نادر لبرامج التجسس من هذا الصنف – استهدف حاسوبًا محمولًا خاصًا يعود لجوان ماتامالا، وهو ناشط مرتبط ارتباطًا وثيقًا بالسياسيين الانفصاليين. وقد اتصل كامبو بماتامالا وأمره بتغليف الحاسوب المحمول بورق الألمنيوم، وهي طريقة مؤقتة لمنع البرامج الضارة من الاتصال بالخوادم. كانت "سيتزن لاب" قادرة على استخراج نسخة من برنامج التجسس، الذي أطلقت عليه شركة "مايكروسوفت" اسم "لسان الشياطين". أصدرت شركة "مايكروسوفت" بعد عدة أشهر تحديثات تحظر "لسان الشياطين" لمنعه من تنفيذ هجمات مستقبلية. وحسب جودوين فإن قائمة الناشطين والصحفيين المستهدفين بحلول ذلك الوقت "أصابتنا بالقشعريرة". تم استهداف ماتامالا أكثر من 16 مرة، وهو يقول "لا يزال لدي ورق الألمنيوم المخزن هنا، في حال اشتبهنا في وجود اختراق آخر".

في شهر تشرين الثاني/ نوفمبر الماضي، بعد أن تم استهداف مستخدمي هواتف "آيفون" من قبل "مجموعة إن إس أو"، رفعت شركة "آبل" دعوى قضائية خاصة بها، لكن "مجموعة إن إس أو" تقدمت بالتماس للرفض.

أخبرني المهندس إيفان كرستيتش أن "شركة آبل لا تؤمن بالدعاوى القضائية المزيفة، لقد كنا طوال هذا الوقت ننتظر الحجة القاطعة التي تسمح لنا برفع دعوى يمكن الفوز بها". أنشأت شركة آبل فريق تحرّي التهديدات منذ ما يقارب أربع سنوات. وحسب موظفين من آبل مكلفين بذلك العمل، فإن هذه الخطوة كانت استجابةً لانتشار برامج التجسس التي تطوّرها مجموعة "إن إس أو".

وقال أحد الموظفين إن شركة "إن إس أو" تمثل مصدر مشاكل، ولقد قمنا بإحباط "إن إس أو" عدة مرات حتى قبل أن تتداولها الأخبار، ففي سنة 2020، مع إطلاق برنامجها "آي أو إس 14"، قدمت آبل نظامًا يدعى "بلاستدور" قام بنقل معالجة الرسائل الإلكترونية – بما في ذلك أي رموز يحتمل أن تكون ضارة – إلى غرفة آلية متصلة ببقية نظام التشغيل خلال خط بيانات فردي ضيق فقط. لكن عمر، نائب رئيس "إن إس أو"، أخبرني: عادةً ما تحتوي الميزات الأحدث على بعض الثغرات في دروعها، ما يجعلها أسهل للاستهداف. واعترف كرستيتش: "لا زال هناك نوع من فتحة عين الإبرة".

وفي مارس 2021؛ تلقى فريق أمان آبل معلومة تفيد بأن أحد المتسللين نجح في إدخال الخيط لتلك الإبرة؛ فحتى الحرب الإلكترونية لها وكلاء مزدوجون. وقال شخص مطلع على إمكانيات فريق تحرّي التهديدات لدى آبل إن فريق الشركة يتلقى أحيانًا معلومات من مخبرين مرتبطين بمؤسسات برامج التجسس: "لقد أمضينا وقتًا طويلاً وبذلنا الكثير من الجهد في محاولة الوصول إلى مكان يمكننا فيه بالفعل معرفة شيء ما حول ما يحدث بعمق وراء الكواليس في بعض هذه الشركات".

(قال متحدث باسم شركة آبل إن شركة آبل لا تقوم "بتشغيل مصادر" داخل شركات برامج التجسس).

ويعتمد بائعو برامج التجسس أيضًا على جمع المعلومات الاستخبارية، مثل تأمين إصدارات تجريبية للبرامج، التي يستخدمونها لتصميم هجماتهم التالية.

أصبحت إسرائيل أكبر مصدر في العالم لتقنيات التجسس واختراق خصوصيات الدول والأفراد

قال لي عمر: "نحن نتبع المنشورات، ونتابع الإصدارات التجريبية لأي تطبيقات نستهدفها"، فيما اتصل باحثون من معمل الأبحاث للأمن السيبراني بشركة آبل: "تم اختراق هاتف الناشطة السعودية في مجال حقوق المرأة، لجين الهذلول، من خلال الرسائل الإلكترونية".

في وقت لاحق؛ كان معمل الأبحاث للأمن السيبراني قادر على إرسال نسخة إلى آبل من ثغرة اكتشفها الباحث بيل ماركزاك بعد شهور من التدقيق في هاتف الهذلول، والتي كانت قد أخفيت في ملف صور، فيما قال الشخص المطّلع على إمكانيات فريق تحرّي التهديدات لدى شركة آبل، أن استلام الملف، عبر قناة رقمية مشفرة، "نوعًا ما يشبه الحصول على شيء خطير يُعطى إليك في حقيبة، تقول لا تفتح إلا في معمل السلامة الحيوية المستوى 4"

واستغرق التحقيق الذي أجرته شركة آبل أسبوعًا وشارك فيه عشرات المهندسين في الولايات المتحدة وأوروبا، وخلصت الشركة إلى أن شركة "إن إس او" قد أدخلت تعليمات برمجية في ملفات "بي دي إف" من "أدوبي"، ثم خدعت نظامًا في الرسائل الالكترونية لقبول ملفات "بي دي إف" ومعالجتها خارج "بلاي ستور"، بينما قال المطّلع على إمكانيات فريق تحرّي التهديدات لدى آبل: "إنه خيال علمي محدود"، مضيفًا "عندما تقرأ التحليل، من الصعب تصديق ذلك."

ويدرس فريق البحث الأمني في غوغل مشروع "زيرو"، وهو أيضًا نسخة من الثغرة؛ حيث كتب لاحقًا في منشور له مدوّن: "نحن نقدر أن هذا هو أكثر الثغرات الفنية تطورًا التي رأيناها على الإطلاق"، مما يدل على أن القدرات التي تقدمها "إن إس أو" تنافس أولئك الذين كانوا يعتقدون سابقًا أنه لا يمكن الوصول إليه إلا في القليل من الدول القومية، ففي مكاتب "إن إس أو"؛ طبع المبرمجون في فريق أبحاث "كور" نسخة من المنشور وعلّقوه على الحائط.

لقد قامت آبل بإصدار تحديثات لمنصاتها التي جعلت هذا الاستغلال عديم الفائدة، فقد أخبرني كرستيتش أن هذه كانت "نقطة فخر" كبيرة، لكن عمر قال لي: "لقد رأينا مجيئها، فلقد كنا نعد الأيام حتى حدث ذلك، وأنه وآخرين في الشركة قالوا إن الثغرة التالية أمر حتمي، وأنه قد يكون هناك بعض الثغرات، وقد يستغرق الأمر أسبوعين للتوصل إليها مع الهدوء من جانبنا، وبعض الحلول البديلة".

وخلال مقابلات شخصية في مكاتب "إن إس أو" الشهر الماضي، تبادل الموظفون نظراتهم العصبية مع موظفي العلاقات العامة وهم يجيبون على أسئلة حول اعتبار وسط الفضائح والدعاوى القضائية والقوائم السوداء، فقد قال عمر:"لأكون صريحًا، ليس كل الوقت يكون المزاج حقًا جيد"، وادعى آخرون الولاء للشركة والإيمان بقوة أدواتها للقبض على المجرمين؛ حيث قال لي موظف سابق: "تمتلك الشركة سردًا قويًا للغاية بأنها تحاول البيع داخليًا للموظفين"، "إما أن تكون معهم أو تكون ضدهم".

وأصبحت إسرائيل أكبر مصدر في العالم لتقنيات التجسس واختراق خصوصيات الدول والأفراد، فقد قال لي مسؤول استخباراتي كبير سابق: "بسبب الخدمة الإجبارية، يمكننا تجنيد الأفضل".

يتمثل الحلم الأمريكي في التخرج من معهد ماساتشوستس للتكنولوجيا والعمل في شركة غوغل، في حين أن الحلم الإسرائيلي هو الانضمام إلى الوحدة 8200، وهي وحدة الاستخبارات العسكرية الإسرائيلية التي غالبًا ما يُنتدب بائعو برامج التجسس من خلالها. (هوليو، الذي يصف نفسه بأنه طالب عادي لم تكن نشأته "مليئه بالرفاهية"، يؤكد غالبًا أنه لم ينضم إلى الوحدة 8200). تاريخيًا، يُنظر إلى شركة " إن إس أو" على أنها فرصة عمل جذابة للمحاربين الشباب القدامى. لكن موظفا سابقا في "إن

إس أو"، الذي استقال بسبب قلقه من أن يكون برنامج بيغاسوس قد سهّل عمليّة قتل جمال خاشقجي، أخبرني أن الآخرين أصيبوا بخيبة أمل أيضًا. ذكر هذا الموظف: "قرر العديد من زملائي ترك الشركة في تلك المرحلة. كان هذا أحد الأحداث الرئيسية التي أعتقد أنها فتحت أعين العديد من الموظفين وجعلتهم يفهمون ما يجري". وفي السنوات القليلة الماضية، بدأ عدد الموظفين المستقيلين يتضاعف "مثل كرة الثلج". قال هوليو، ردًا على أسئلة حول مشاكل الشركة، "ما يقلقني هو ردود فعل الموظفين".

في سنة 2019، كانت "إن إس أو" مُثقلةً بمئات الملايين من الدولارات من الديون كجزء من صفقة شراء ذات رافعة مالية حصلت بموجبها شركة الأسهم الخاصة في لندن "نوفالبينا" على حصة سبعين في المئة. وفي الآونة الأخيرة، خفّضت شركة الخدمات المالية "موديز" التصنيف الائتماني لـ "إن إس أو" إلى "ضعيف"، ووصفتها بلومبيرغ بأنها أحد الأصول المتعثرة التي تجنبها تجار وول ستريت. استقال اثنان من كبار المديرين التنفيذيين في "إن إس إو"، وتدهورت العلاقات بين الشركة وداعميها. أدى الاقتتال الداخلي بين شركاء "نوفالبينا" إلى نقل التحكم بأصولها بما في ذلك "إن إس أو"، إلى شركة استشارية تدعى "مجموعة أبحاث بيركلي"، التي تعهدت بزيادة الرقابة.

لكن أحد المديرين التنفيذيين في مجموعة "بيركلي" زعم مؤخرًا أن التعاون مع هوليو أصبح "شبه معدوم". وأفادت وكالة "فرانس برس" بأن التوترات ظهرت لأن دائني شركة "إن إس أو " ضغطوا من أجل استمرار تدفق المبيعات إلى البلدان ذات السجلات المشبوهة في مجال حقوق الإنسان، في حين سعت مجموعة "بيركلي" إلى إيقافها مؤقتًا. وقال هوليو عن مجموعة "بيركلي": "لدينا بالفعل بعض الخلافات معهم فيما يتعلق بكيفية إدارة الأعمال".

أدت متاعب شركة "إن إس أو" إلى تعقيد تحالفها الوثيق مع إسرائيل. وأشار المسؤول الاستخباري الكبير السابق إلى أنه في الماضي، عندما رفضت وحدته الدول الأوروبية التي كانت تسعى إلى التعاون الاستخباراتي: "قال الموساد، إليك أفضل شيء قادم، وهي مجموعة "إن إس أو". العديد من الأشخاص المطلعين على هذه الصفقات قالوا إن السلطات الإسرائيلية قدمت القليل من القيود والتوجيهات الأخلاقية. وأضاف المسؤول السابق: "لم تكن الرقابة الإسرائيلية على الصادرات تعمل على أساس أخلاقي"، بل كانت تتعامل مع شيئين: أولا، المصلحة الوطنية الإسرائيلية، وثانيًا: السمعة"

ذكر الموظف السابق في الشركة أن الدولة "كانت مدركة جيدًا لإساءة الاستخدام، بل إنها تستخدمها كجزء من علاقاتها الدبلوماسية". من جهتها، أشارت وزارة الدفاع الإسرائيلية في بيان لها إلى أن "كل تقييم للترخيص يتم وفقًا لاعتبارات مختلفة بما في ذلك التصريح الأمني للمنتج وتقييم الدولة التي سيتم تسويق المنتج من أجلها. كانت القضايا المتعلّقة بحقوق الإنسان والسياسة والقضايا الأمنية هي التي وضعت شركة "إن إس أو" على القائمة السوداء، حيث سعى هوليو إلى تجنيد المسؤولين الإسرائيليين، بمن فيهم رئيس الوزراء نفتالي بينيت ووزير الدفاع بيني غانتس. قال لي: "لقد أرسلت رسالة. قلت ذلك كشركة منظمة، وكل ما طلبناه كان بإذن وسلطة من حكومة إسرائيل. لكن مسؤولا كبيرا في إدارة بايدن قال إن الإسرائيليين أثاروا "شكاوى بسيطة جدًا" حول القائمة السوداء. لم يعجبهم ذلك، لكن لم يكن لدينا فرصة أخرى".

في المجلس التشريعي الإسرائيلي، يقود السياسيون العرب حركة متواضعة لفحص علاقة الدولة بشركة "إن إس أو". أخبرني رئيس الحزب العربي سامي أبو شحادة: "حاولنا مناقشة هذا في الكنيست مرتين لإخبار السياسيين الإسرائيليين بأنهم يبيعون الموت للمجتمعات الضعيفة التي أوهنها الصراع، وأنتم تفعلون ذلك منذ فترة طويلة". وأضاف: "لم ينجح الأمر أبدًا، لأنهم، أخلاقيًا، لا يرون أي مشكلة في ذلك".

في الخريف الماضي، كشف تحقيق أجرته مجموعة المراقبة "فرونت لاين ديفندرز" عن وجود برنامج بيغاسوس على هواتف ستة نشطاء فلسطينيين – بما في ذلك أحد الذين تم إلغاء إقامتهم في القدس. جادل أبو شحادة بأن تاريخ تكنولوجيا برامج التجسس الإسرائيلية مرتبط بمراقبة المجتمعات الفلسطينية في الضفة الغربية والقدس الشرقية وغزة، قائلا "استخدموا الفلسطينيين كحقول تجارب لأدوات التجسس لفترة طويلة، ولم يكترث أحد لذلك". وردًا على سؤال حول استهداف الفلسطينيين، أجاب هوليو: "إذا استخدمت إسرائيل أدواتنا لمحاربة الجريمة والإرهاب، فسأكون فخورًا بذلك".

يعد مجال برامج التجسس مليئا بالمخترقين المحتالين المستعدين لاختراق جهاز لأي شخص يدفع لهم المال.

أقرّ هوليو: "أعلم أنه كان هناك سوء استخدام لهذه الأدوات، ومن الصعب علي أن أتعايش مع ذلك. ومن الواضح أنني أشعر بالأسف لذلك، وهذه هي المرة الأولى التي أفصح فيها عما يزعجني. رفضت الشركة تسعين عميًلا ومئات الملايين من الدولارات من الأعمال بدافع القلق بشأن احتمال إساءة استخدامها، لكنه من الصعب التحقق من مثل هذه الادعاءات". من جهته، صرّح مسؤول المخابرات الإسرائيلي السابق، الذي يعمل الآن في قطاع برامج التجسس بأن "شركة "إن إس أو" أرادت تقديمه كمثال أوروبي. لكن معظم أعمالهم مدعومة من السعودية".

ذكر موظف سابق كان على دراية بجهود مبيعات "إن إس أو"، "بالنسبة لدولة أوروبية، فإنهم سيتقاضون عشرة ملايين دولار. أما بالنسبة لبلد في الشرق الأوسط، يمكنهم دفع 250 مليونًا مقابل نفس المنتج". يبدو أن هذا يخلق حوافز فاسدة: "عندما أدركوا أن البرنامج تعرض لسوء استخدام في تلك البلدان التي باعوها إياه مقابل مبالغ ضخمة من المال، كان قرار إيقاف الخدمة عن ذلك البلد أكثر صعوبة بكثير".

عند سؤاله عن الانتهاكات الجسيمة المنسوبة إلى برنامج بيغاسوس، استشهد هوليو بحجة تقع في صميم دفاعه ضد شركتي واتساب وآبل:: "ليس لدينا ولوج إلى البيانات الموجودة على النظام وليس لدينا ضلوع في العملية بالإضافة إلى أننا لا نرى ما يفعله العملاء وليست لدينا وسيلة لرصد ذلك". قال مسؤولو الشركة إنه عندما يشتري عميل ما برنامج بيغاسوس، يسافر فريق من "إن إس أو" لتركيب شبكتين واحدة مخصصة للتخزين والأخرى لتشغيل البرنامج وبذلك يعمل النظام فقط مع اتصال محدود مع "إن إس أو" في اسرائيل.

لكن مهندسي "إن إس أو "يعترفون بأن هناك بعض المراقبة في الوقت الحالي للأنظمة بهدف منع التلاعب أو سرقة التكنولوجيا الخاصة بهم. وذكر موظف سابق تعليقًا على تأكيدات هوليو بأن الشركة ممنوعة من الناحية التقنية من الإشراف على النظام: "إنها كذبة". وأشار أيضًا إلى جهود الدعم والصيانة المرتبطة بالنفاذ عند بُعد من قبَل "إن إس أو" بإذن من العميل وإشراف مباشر منه.

وأضاف الموظف السابق "نعم، هناك نفاذ عن بُعد ويمكنهم رؤية كل ما يحدث. لديهم حق الاطلاع على قاعدة البيانات ولديهم إمكانية الوصول إلى جميع البيانات". وأخبرني مسؤول رفيع المستوى في إنفاذ القانون الأوروبي، بأنه يمكنهم الولوج إلى النظام عن بُعد عندما نسمح لهم بذلك.

يزعم المسؤولون التنفيذيون في "إن إس أو" أنهم يحاولون بناء حواجز حماية بعيدًا عن الرقابة. وقد روجوا لتنصيبهم لجنة امتثال وأخبروني بأنهم يحتفظون الآن بقائمة بالدول المصنفة حسب مخاطر سوء الاستخدام بناءً على مؤشرات حقوق الإنسان من فريدوم هاوس ومجموعات أخرى رفضوا الإفصاح عنها. تقول "إن إس أو" أيضًا إن أنظمة بيغاسوس تحتفظ بملف يسجل الأرقام المستهدفة لدى العملاء وبالتالي فإنهم ملزمون بموجب العقد بتسليم الملف عندما تفتح "إن إس أو" تحقيقًا.

أكد هوليو: "لم يحدث من قبل أن رفض أي عميل هذه الإجراءات". وتقول الشركة إنها تستطيع إيقاف الأنظمة عن بُعد، وقد فعلت ذلك سبع مرات في السنوات القليلة الماضية. وأشار هوليو إلى أن المنافسة مخيفة أكثر بكثير، موضحًا أن "الشركات في سنغافورة وقبرص وفي عدة أماكن أخرى تفتقر للتنظيم الحقيقي ويمكنها بيع منتجاتها لأي طرف".

يعد مجال برامج التجسس مليئا بالمخترقين المحتالين المستعدين لاختراق جهاز لأي شخص يدفع لهم المال. قال هوليو: "سيستحوذون على حاسوبك وهاتفك بالإضافة إلى حساب الجيميل الخاص بك". وأضاف هوليو "من الواضح أن هذا أمر غير قانوني لكنه أصبح شائعاً جدًا اليوم فضلاً عن أن تكلفته ليست باهظة. كما أن بعض الخدمات التكنولوجية التي تنافس "إن إس أو" مصدرها جهات فاعلة حكومية، بما في ذلك الصين وروسيا. ونجد اليوم أنه في الصين وإفريقيا تقدم الحكومة الصينية قدرات مشابهة تقريبًا لقدرات "إن إس أو".

وفقًا لتقرير صادر عن مؤسسة كارنيغي للسلام الدولي، تزود الصين 63 دولة بأجهزة مراقبة، ويتم هذا غالبًا من خلال شركات خاصة مرتبطة بالحكومة الصينية. قال لي هوليو: "لنقل إن "إن إس أو" لن تكون موجودة غدًا. لن يكون هناك فراغ. ماذا تعتقد سوف يحصل؟". تتنافس "إن إس أو" أيضًا مع الشركات الإسرائيلية. وشركات القرصنة الكبيرة مثل تلك الموجودة في كتالونيا تستخدم أدوات من عدة شركات في حملات القرصنة واسعة النطاق، والعديد من تلك الشركات أسسها أشخاص كانوا يعملون لدى "إن إس أو".

تأسست شركة "كانديرو" في سنة 2014 من قبل موظفين سابقين لدى "إن إس أو" وهما إيران شورر ويعقوب وايزمان. يوجد مزاعم أن الشركة مرتبطة بالهجمات الأخيرة على مواقع الويب في المملكة المتحدة والشرق الأوسط إلا أنها تنفي صلتها بالموضوع. وقد تم التعرف على برنامجها التجسسي في أجهزة مواطنين أتراك وفلسطينيين. لا تملك "كانديرو" موقع ويب واشتقت اسمها من اسم سمكة طفيلية تعيش في حوض نهر الأمازون، تعتاش على دماء الأسماك الكبيرة.

بعد عامين تأسست شركة جديدة اسمها "كوادريم" من قبل موظفين سابقين لدى "إن إس أو" وهما غاي جيفا ونمرود ريزينك. وعلى غرار "إن أس أو" تركز "كوادريم" على برمجيات الهواتف الذكية. وفي وقت سابق من هذه لسنة، ذكرت وكالة رويترز أن "كوادريم" استغلت نفس الثغرة الأمنية التي كانت تستخدمها "إن إس أو" للوصول إلى تطبيق "آي ميسج" الخاص بهواتف "آبل". يبدو أن شركة "كوادريم"، التي تقع مكاتبها في مكان مجهول في ضاحية رمات غان في تل أبيب، تشترك مع العديد من منافسيها في الاعتماد على الملاذات الضريبية التنظيمية. وحسب ما شاع، فإن برمجيتها الخبيثة الجديدة "رين" تعود ملكيتها لمنشأة "إن ريتش" التي تتخذ من قبرص مقراً لها. وحسب صحيفة "هآرتس"، فإن "كوادريم" من بين الشركات التي تعمل في المملكة العربية السعودية إلا أنه تعذر التواصل معها للتعليق على هذا الخبر.

تقدم شركات إسرائيلية أخرى نفسها على أنها ذات سمعة مقبولة مثل شركة "باراغون" التي تقوم بتسويق تقنيتها لمكاتب داخل الحكومة الأمريكية. تأسست "باراغون" في سنة 2018 على يد مسؤولين سابقين في المخابرات الإسرائيلية وتضم في مجلس إدارتها رئيس الوزراء السابق إيهود باراك. ولا تركز تقنية "باراغون" الرئيسية على التحكم الكامل بالهواتف وإنما فقط على اختراق أنظمة المراسلة المشفرة مثل "تليغرام" و"سيغنال".

أخبرني أحد المسؤولين التنفيذيين أن "باراغون" التزمت بالبيع لعدد محدد من البلدان التي لديها سجلات حقوق إنسان غير مثيرة للجدل نسبيًا: "استراتيجيتنا هي أن يكون لدينا قيم، وهو أمر يصب في اهتمامات السوق الأمريكية".

تواجه مجموعة "إن إس أو" أيضًا عواقب قانونية في المملكة المتحدة حيث أبلغ ثلاثة نشطاء مؤخرًا كلاً من الشركة وحكومتي السعودية والإمارات بأنهم بصدد التخطيط لمقاضاة تجاوزات مزعومة بحق "بيغاسوس".

يستعد المحامي غونزالو بوي الذي يمثل 19 شخصًا استهدفتهم برمجية "بيغاسوس" في كتالونيا لتقديم شكاوى جنائية للمحاكم في إسبانيا ودول أوروبية أخرى تطال كلاً من "إن إس أو" وهوليو وشركائه المؤسسين متهمًا إياهم بخرق القوانين المحلية وقوانين الاتحاد الأوروبي. مثل بوي السياسيين الكتالونيين في المنفى، بما في ذلك الرئيس السابق كارليس بويجديمونت.

ما بين شهري آذار/مارس وتشرين الأول/ أكتوبر 2020، كشف تحليل أجرته مؤسسة "سيتيزين لاب" أنه تم استهداف بوي 18 مرة بواسطة رسائل نصية تتنكر في شكل تحديثات من "تويتر" ومواقع إخبارية. وقد أدت إحدى هذه المحاولات إلى وصول "بيغاسوس" إلى جهاز بوي. يقول بوي إنه الآن يقضي جُلّ وقته خارج إسبانيا. وفي مقابلة أجريت معه مؤخرًا، تساءل متعجبًا: "كيف يمكنني الدفاع عن شخص ما، إذا كان الطرف الآخر يعرف بالضبط كل ما قلته لعميلي؟".

رفض هوليو الإشارة إلى عملاء محددين لكنه أفاد بأن استخدام إسبانيا للتكنولوجيا كان قانونيًا "إسبانيا لديها سيادة القانون بالتأكيد وإذا كان كل شيء قانونيًا وبموافقة المحكمة العليا أو بموافقة جميع الآليات القانونية، فلن يكون هناك مجال للعبث".

أخبرني بيري أراغون، الرئيس الحالي لكتالونيا: "نحن لسنا مجرمين، كل ما نريده من السلطات الإسبانية هو التحلي بالشفافية"، مع العلم أن أراغون هو واحد من بين ثلاثة أشخاص تم اختراق هواتفهم بواسطة "بيغاسوس".

شكّل البرلمان الأوروبي الشهر الفائت لجنة تحقيق للنظر في استخدام بيغاسوس في أوروبا. وذكرت وكالة "رويترز" الأسبوع الماضي أن كبار المسؤولين في المفوضية الأوروبية تم استهدافهم بواسطة برنامج التجسس التابع لشركة "إن إس أو". وستعقد اللجنة جلستها الأولى في 19 نيسان/ أبريل. ووصف بويجديمونت، أحد أعضاء اللجنة، أن أنشطة "إن إس أو" "تشكل تهديدًا ليس فقط لمصداقية الديمقراطية في إسبانيا، بل أيضا لمصداقية الديمقراطية الأوروبية بذاتها".

تواجه مجموعة "إن إس أو" أيضًا عواقب قانونية في المملكة المتحدة حيث أبلغ ثلاثة نشطاء مؤخرًا كلاً من الشركة وحكومتي المملكة العربية السعودية والإمارات العربية المتحدة بأنهم بصدد التخطيط لمقاضاة تجاوزات مزعومة بحق "بيغاسوس". وكان رد الشركة بأنه "لا يوجد أساس لهذه الإدعاءات".

تواصل "إن إس أو" الدفاع عن نفسها في دعوى واتس آب وقدمت هذا الشهر استئنافًا إلى المحكمة العليا الأمريكية. قال لي شموئيل صنراي المستشار العام لـ "إن إس أو": "إذا كان الأمر يتطلب المواجهة والتحدي فنحن جاهزون لذلك".

وقال محامو واتسآب إنهم واجهوا في معركتهم القضائية مع "إن إس أو" تكتيكات خفية، بما في ذلك حملة واضحة للتجسس على الخصوصيات.

كانت نيلسون كتومة على التعريف بنفسها ولكنها كانت حريصة جدًا على مقابلة مورنين لدرجة أنها اشترت له تذكرة طائرة من الدرجة الأولى من سان فرانسيسكو إلى نيويورك ودفعت ثمنها نقداً من خلال شركة "وورلد ترافل إكسبريس" وهي وكالة متخصصة في تنظيم رحلات إلى إسرائيل، إلا أن مورنين لم يستخدم التذكرة أبداً.

ولكن سرعان ما اختفى موقع شركة الأفلام الوثائقية العائدة لـ "نيلسون" من على شبكة الإنترنت، حيث كان مليئا بالصور الوهمية من أماكن أخرى على الإنترنت. وقامت "نيلسون" أيضاً بحذف ملفها

الشخصي من منصة لينكدإن. بعد عدة أشهر، اتصلت امرأة تدّعي أن اسمها أنستازيا تشيستياكوفا، وتعمل كوصية في موسكو لشخص ثري يُدعى بتراتشيستياكوفافيس ليبلانك، شريك كولي في قضية "واتس آب"، لطلب المشورة القانونية. أرسلت المرأة بريدًا صوتيًا وبريدًا إلكترونيًا ورسائل فيسبوك ولينكد إن. حدّدت مورنين صوتها على أنه ينتمي إلى نيلسون، وخلُصت شركة المحاماة في وقت لاحق إلى أن بريدها الإلكتروني ينتمي إلى نفس المجموعة الخاصة بعناوين P.I. مثل تلك التي أرسلها نيلسون، وأبلغ المحامون وزارة العدل بالحادثة.

كانت التكتيكات مماثلة لتلك التي استخدمتها شركة الاستخبارات الخاصة "بلاك كيوب"، التي يدير جزءًا كبيرًا منها ضباط سابقون في الموساد ووكالات استخبارات إسرائيلية أخرى، وهي معروفة باستخدام عملاء بهويات مزيفة. عملت الشركة نيابة عن مؤسّسها هارفي واينستين لتعقّب النساء اللاتي اتّهمنه بالاعتداء الجنسي. وفي الشهر الماضي، تلقّى ثلاثة من مسؤوليها أحكامًا بالسجن مع وقف التنفيذ بتهمة القرصنة وترويع المدعي العام لمكافحة الفساد في رومانيا.

استهداف "بيغاسوس" للفئات التي لا تُشكّل أهمية كبيرة ليس أمرًا مُستبعدًا.

ارتبطت "بلاك كيوب" بحالة أخرى على الأقل تتعلّق بمجموعة "إن إس أو غروب". ففي شباط/ فبراير 2019، ذكرت وكالة الأنباء الأمريكية "أسوشيتد برس" أن عملاء "بلاك كيوب" استهدفوا ثلاثة محامين قدّموا دعوى أخرى ضد شركة "إن إس أو غروب"، بالإضافة إلى صحفي مقيم في لندن يُغطّي القضية. ورفع المحامون – مازن مصري وعلاء محاجنة وكريستيانا ماركو – الذين مثّلوا الصحفيين والناشطين الذين تعرّضت هواتفهم للاختراق دعوى قضائية ضد "إن إس أو غروب" وشركة تابعة لها في إسرائيل وقبرص. وفي أواخر سنة 2018، تلقّى الثلاثة رسائل من أشخاص ادّعوا أنهم مرتبطون بشركة أو شخص ثري، ويقترحون بشكل متكرر عقد اجتماعات في لندن.

نفت شركة "إن إس أو غروب" الاستعانة بـ"بلاك كيوب" لاستهداف المعارضين. ومع ذلك، اتصل هوليو بي قائلاً: "بالنسبة للدعوى في قبرص، كان هناك تورط واحد لشركة "بلاك كيوب" لأن الدعوى القضائية "جاءت من العدم، وأريد أن أفهم حيثياتها". وأكد أنه لم يستأجر "بلاك كيوب" لدعاوى قضائية أخرى. ومن جهتها، رفضت "بلاك كيوب" التعليق على القضايا المُسندة إليها، ونفى مصدر مطّلع على الشركة أنها استهدفت محامي كولي.

حسب هوليو، يجب أن تتكيّف شركة "إن إس أو غروب" حاليًا مع الوضع الذي أصبح فيه منتجها الرئيسي رمزًا للقمع. وأضاف "لا أعرف ما إذا كنا سنكسب القضية، لكننا لن نستسلم". كان أحد الحلول هو توسيع خط الإنتاج. أطلعتني الشركة على أداة ذكاء اصطناعي تسمى "مايسترو" تقوم بفحص بيانات المراقبة، وتبني نماذج لعلاقات الأفراد والجداول الزمنية، وتنبّه سلطات إنفاذ القانون إلى الاختلافات الروتينية التي قد تكون نذيرًا للجريمة. أخبرني أحد مصمميها ليوز مايكلسون: "أنا متأكد من أن تلك الأداة ستكون الشيء الكبير التالي الذي سيصدر من "إن إس أو"، حيث سيتم تحويل كل نمط حياة إلى شعاع رياضي".

يُستخدم المنتج بالفعل من قبل مجموعة قليلة من الدول، وذكر هوليو أن البرنامج ساهم في نجاح عملية اعتقال بعد أن غيّر أحد المشتبه بهم في تحقيق إرهابي روتينه بمهارة. يبدو أن الشركة قد أولت القليل من الاهتمام لفكرة أن هذه الأداة أيضًا قد تثير الجدل. عندما سألتُ عما سيحدث إذا اعتقلت سلطات إنفاذ القانون شخصًا ما بناءً على . على سبيل المثال . رحلة بريئة إلى المتجر في منتصف الليل، قال مايكلسون: "يمكن أن تكون هناك إثباتات خاطئة". لكنه أضاف: "هذا الرجل الذي سيشتري الحليب في منتصف الليل موجود في النظام لسبب ما".

مع ذلك، فإن استهداف "بيغاسوس" للفئات التي لا تُشكّل أهمية كبيرة ليس أمرًا مُستبعدًا. ففي

الأسبوع الماضي، قرّر إليس كامبو فحص هاتفي والديه، العالمان اللذان لا يشاركان في الأنشطة السياسية، بحثًا عن برامج التجسس، واكتشف أن برنامج "بيغاسوس" كان مُثبّتًا على هاتف كليهما منذ أن زارهما خلال عطلة عيد الميلاد في سنة 2019.

أخبرني كامبو: "لم تعد فكرة أن أي شخص معرّض للاستهداف من قبل "بيغاسوس" مستبعدة". على هاتف والدته، الذي تم اختراقه ثماني مرات، وجد الباحثون نوعًا جديدًا من تقنية استغلال الضغط الصفري، التي هاجمت "آي مسج" ومحرك تصفح الويب لنظام "آي أو أس". لا يوجد دليل على أن أجهزة "آيفون" لا تزال عرضة لهذا الهجوم، الذي أطلق عليه "سيتيزن لاب" "هوميج". وعندما عُثر على الدليل، قال سكوت رايلتون لكامبو: "لن تصدّق هذا، لكن والدتك كانت الأولى في سلسلة من هجمات الاستغلال التي لم يتم اكتشافها من قبل".

وخلال زيارة حديثة لمكاتب "إن إس أو"، كانت النوافذ واللوحات البيضاء في جميع أنحاء المكان مليئة بالمخططات الانسيابية والرسومات المُرفقة بالنصوص العبرية والإنجليزية، التي تؤرخ لأفكار المنتجات ومآثرها. وعلى سبورة بيضاء، كانت هناك كلمة "حرب" مكتوبة بأحرف عبرية حمراء كبيرة ومُسطّرة بشدة.

المصدر: ذا نيويوركر

رابط المقال: https://www.noonpost.com/43901/