Skyline International for human rights

خلال لقاء عقدته عبر صفحتها على فيسبوك

سكاي لاين تحذر من استمرار نشاط برامج التجسس على حياة ومعلومات الأفراد من الحكومات الديكتاتورية

ستوكهولم- أعربت مؤسسة سكاي لاين لحقوق الانسان عن قلقها ومخاوفها من استمرار الاستخدام التجاري لبرنامج التجسس بيغاسوس (Pegasus) ، الذي طورته شركة NSO الإسرائيلية، وفقًا للتحقيق الذي أجرته كلا من منظمة سيتزين لاب Citizen Lab ، ومنظمة فوربيدين ستوريز Forbidden Stories الفرنسية ، والذي خلص استخدام عدة دول وجهات تكنولوجيا الاختراق والولوج، لتسهيل الانتهاكات والجرائم ضد حرية التعبير وحقوق الإنسان بشكل لم يسبق له مثيل.

وأكدت المنظمة الحقوقية خلال بث مباشر عقدته بتاريخ 23 سبتمبر/ أيلول، عبر صفحتها على الفيسبوك على أن تقنية بيغاسوس كان من المفترض أن تكون لمحاربة الإرهاب، لكن أجهزة الاستخبارات استغلت هذه التقنية لاستهداف الآلاف من الصحفيين والنشطاء ورؤساء الدول وغيرهم من المهنيين وعائلاتهم في جميع أنحاء منطقة الشرق الأوسط وشمال إفريقيا.

وذكر مدير المؤسسة "دانيال ريفيرا" بأن " منظمته تؤمن بأنه من الأهمية بمكان منع هذه التكنولوجيا من الانتشار وتسويقها في جميع أنحاء العالم دون إطار قانوني واضح ينظم استخدامها. مشيرًا إلى أن منظمته قامت بأرسال رسائل مشتركة إلى مفوضية الأمم المتحدة السامية لحقوق الإنسان لإدانة تقنيات وبرنامج بيغاسوس، اضافة لحثها تلك الجهات على اتخاذ إجراءات ضد الدول التي استخدمت برامج التجسس الخاصة بشركة "NSO" لاختراق هواتف نشطاء حقوق الإنسان والصحفيين والأفراد.

بدأت "مروة فطافطة" مديرة السياسات في منظمة Access Now ، مداخلتها بشرح بدايات برنامج بيغاسوس وكيفية عمله. مشيرة إلى أن بيغاسوس هو برنامج تجسس طورته شركة NSOالاسرائيلية التي تم تأسيسها في عام 2010.

وأشارت إلى " قدرة هذا البرنامج على اختراق الهواتف وسرقة جميع المعلومات داخل الجهاز بما في ذلك: البريد الإلكتروني والرسائل والصور. بالإضافة إلى ذلك، يمكنه الوصول إلى الكاميرا والصوت، وغير ذلك من المهام الأخرى التي يمكن التحكم بها عن بُعد. بعد ذلك يتم أخذ كل هذه المعلومات وإرسالها إلى عميل له غرض من التجسس عليك. مؤكدة على أن " هذا البرنامج يحول الهاتف إلى جهاز تجسس."

وأوضحت مروة الطريقة التي يخترق بها هذا البرنامج الهاتف المراد اختراقه. حيث يتم ارسال رابط ضار على هيئة دعوة للشخص المستهدف ليتم الوصول الى جهازه. ومثال لذلك ما تعرض له الناشط الإماراتي في مجال حقوق الإنسان" أحمد منصور"، الذي تلقى رابطًا يُفترض أنه يحتوي على تحديثات وأخبار حول قضايا حقوق الإنسان في الإمارات العربية المتحدة وتم دعوته للنقر على الرابط لكن الرابط كان مجرد وسيله للاختراق. كما تلقى ناشط حقوقي سعودي في كندا رابطًا يبدو أنه اشعار تتبع لشحن DHL ، ولكن بمجرد النقر على الرابط ، تم اختراق جهازه.

ومع ذلك، هناك برنامج أو تقنية أخرى للتجسس على الجهاز دون الحاجة إلى قيام المستخدمين بأي شيء يُطلق عليها "النقر الصفري"، وفي هذه الحالة لا داعي لأي تفاعل مع مالك الجهاز حيث تستغل شركة NSO الثغرات الأمنية في جهاز الشخص المستهدف، لذلك بغض النظر عن مدى حرص الشخص، لا يوجد هناك أي شيء يمكنك القيام به لوقف هذا النوع من الهجوم.

كما أكدت مروة أنه " بعد التحقيق التي أجرته بعد المنظمات، يمكننا أن نستنتج أن بعض الحكومات الاستبدادية والديمقراطية على حد سواء استخدمت بيغاسوس لاستهداف النشطاء والمدافعين عن حقوق الإنسان والصحفيين والمحامين والجهات الفاعلة في المجتمع المدني. مشيرة إلى أن مجموعة NSO ادعت بيع تقنية بيغاسوس للحكومات التي عرفت عن نفسها بانها لا تنتهك حقوق الانسان، وأن الشركة الاسرائيلية وترفض بيعها للحكومات التي تفعل عكس ذلك ".

ومع ذلك، كشف التحقيق أن معظم عملاء مجموعة NSO، متهمون بارتكاب انتهاكات لحقوق الإنسان ، لا سيما عملائها في منطقة الشرق الأوسط وشمال إفريقيا: المغرب ، والإمارات، والسعودية، والبحرين ، على سبيل المثال لا الحصر. حيث استفادت شركة NSO، من انتهاكات حقوق الإنسان في جميع أنحاء العالم بسبب ضعف المساءلة والشفافية لعملياتها، حيث يمكن القول أن ما كشفه التحقيق ليس سوى غيض من فيض. إضافة إلى أنه، لم يتم معرفة جميع عملاء مجموعة NSO، والانتهاكات التي قاموا بها لحقوق الإنسان والأشخاص الذين استهدفوهم.

بدوره تحدث المدير التنفيذي لمركز الخليج لحقوق الإنسان، "خالد إبراهيم" عن التعاون بين مجموعة NSO والحكومات الاستبدادية في منطقة الشرق الأوسط وشمال إفريقيا. وأوضح تأثير ذلك على العمل السلمي والشرعي للمدافعين عن حقوق الإنسان وما يجب فعله لتعزيز حماية المدافعين عن حقوق الإنسان في مواجهة مثل هذا التعاون، مؤكدًا على أهمية هذه الحملة في إيقاف شركات مثل NSO الاسرائيلية وغيرها.

وأضاف "تؤثر هذه التكنولوجيا بشكل كبير على مجتمع المدافعين عن حقوق الإنسان في منطقة الشرق الأوسط وشمال إفريقيا. ومن الضروري وقف هذا التعاون بين شركة NSO والشركات الأخرى على حد سواء مع الحكومات القمعية في الشرق الأوسط وشمال إفريقيا وفي أماكن أخرى". ثم أضاف: "يعتبر الناشط الحقوقي أحمد منصور مثالا على استخدام هذه التكنولوجيا في منطقة الشرق الأوسط وشمال إفريقيا."

وأشار خالد في حديثه إلى اختراق هاتف النشاط الحقوقي "أحمد منصور" حيث قال " قامت عدة منظمات حقوقية مثل هيومن رايتس ووتش ومركز الخليج لحقوق الإنسان عام 2021 بإصدار تقرير بعنوان" الإمارات العربية المتحدة: ناشط حقوقي بارز معتقل في خطر "، جميعا نعلم أن أحمد منصور كان هناك ، وكان ضحية بيغاسوس، وأنه معتقل لمدة 10 سنوات استنادًا على العديد من التهم الملفقة له المتعلقة بأنشطته كمدافع عن حقوق الإنسان ، وتعاونه مع منظمات مثل منظمة العفو الدولية ، وهيومن رايتس ووتش ، ومركز الخليج لحقوق الإنسان وغيرها. كما نعلم أن الإمارات أنفقت الملايين للحصول على كل هذه المعلومات من منصور قبل اعتقاله في مارس 2017.

كما ذكر "خالد" أن برلمان الاتحاد الأوروبي أصدر مطالبةً في سبتمبر الماضي يطالب بالإفراج عن أحمد منصور. وأضاف، أن مركز الخليج لحقوق الإنسان يتعاون بشكل وثيق مع الاتحاد الأوروبي لمنع التعاون بين NSO وأعضاء الاتحاد الأوروبي.

وأشارت "مروة فطافطة" إلى أن " معظم الدول التي تستخدم هذه التكنولوجيا هي من دول الخليج ، مثل المملكة العربية السعودية والإمارات والبحرين. كما أن دول أخرى استخدمت هذه التكنولوجيا حديثا مثل عُمان، التي أصدرت تشريعًا العام الماضي يسمح لخدمة الأمن الداخلي بالوصول غير المحدود إلى أنشطة الإنترنت في البلاد، حيث تسيطر قوات الأمن العمانية على الإنترنت في بلادهم وتسمح الحكومة لخدمة الأمن الداخلي باستيراد معدات المراقبة الأكثر تطوراً والتكنولوجيا المتقدمة لمراقبة الأنشطة عبر الإنترنت في البلاد".

وأبرزت "فطافطة" إلى أن " من بين الأعمال الأخرى الناشئة عن هذه التقنية أن هذه البلدان يمكنها الآن تقديم بعض هذه الخدمات إلى البلدان الأخرى التي ليس لديها وصول أو موارد للحصول على هذه التكنولوجيا، ونشر استخدامها في كل ركن من أركان منطقة الشرق الأوسط وشمال إفريقيا".

تؤكد "سكاي لاين" على أن هناك تقنيات مراقبة ضخمة تعمل بالخفاء ، دون محاسبة ، وتحقق مكاسب وتشارك في انتهاكات حقوق الإنسان. فوفقًا لشركة مايكروسوفت، بلغ الانفاق على تقنيات وبرامج المراقبة اليوم بلغ ما قيمته 12 مليار دولار. على سبيل المثال، كانت الإمارات العربية المتحدة تستورد التقنيات والبرامج والمقاولين للعمل في مشاريع المراقبة ولم تكن تستهدف مواطنيها فحسب، بل أيضًا الشخصيات الأجنبية البارزة في القضية المعروفة اليوم باسم Tridentالتي لا يوجد الكثير من المعلومات حول هذا الموقع، لكن منظمة Access now وغيرها من المنظمات الأخرى تعمل على تسليط الضوء على العناصر النشطة لهذه الصناعة الناشئة.

تحدث "شريف منصور"، منسق الشرق الأوسط وشمال أفريقيا في لجنة حماية الصحفيين، عن أثر تقنية بيغاسوس وغيرها من تقنيات المراقبة على الصحفيين عبر الانترنت او في المنفى. كما قدم أمثلة على أولئك الذين يغطون قضايا الفساد في المغرب وتجربته الشخصية في توثيق تزوير الانتخابات في مصر.

سلط "منصور" الضوء على المغرب نظرا لتأثر العديد من الصحفيين فيها ببرامج التجسس والإجراءات القانونية والتكتيكات الأخرى، مثل حملات التشهير والاعتداءات الجسدية، ما أعاق قدرتهم على التحقيق في قضايا الفساد. وأكد "أن الخصوصية أمر بالغ الأهمية للشخص حتى يكون قادرا على القيام بعمله، وللاتصال بالمصادر ونشر المعلومات الهامة. وفقًا لبحث لجنة حماية الصحفيين، فإن الصحفيين الذين يعملون عبر الإنترنت وفي الخارج عادة معرضون بشكل خاص لهذه الهجمات".

ومثالا لذلك ما حدث مع "جمال خاشقجي" حيث تأثر أصدقائه وأفراد أسرته من التجسس قبل وبعد اغتياله. مؤكدًا على أن هذا الأمر تسبب في خسائر نفسية هائلة للضحايا الذين يسعون إلى المساءلة لأنهم يشعرون أن هذه التكنولوجيا تستهدفهم أيضًا. ونتيجة لذلك، أعرب العديد من الصحفيين عن قلقهم الكبير بشأن الافتقار إلى الخصوصية، وهم أكثر وعيًا بعملهم وما يكتبون، لكن من الممكن أن يصبحوا هدفا أيضا.

وأشار "شريف" إلى أنه وفقًا لتحقيقات لجنة حماية الصحفيين، فإن 17 دولة متورطة في عمليات اضطهاد لنشطاء في الخارج. على سبيل المثال، جمال خاشقجي الذي كان يعيش في تركيا والعديد من الأشخاص الآخرين أمثاله، الذين لم يتمكنوا من الاستمرار في النشر في بلدانهم بسبب إغلاق منشوراتهم، حيث كان الإنترنت مكانهم الوحيد لنشر أعمالهم. الأمر يتعلق بمتى تريد الدول بذل مجهود إضافي لملاحقة الصحفيين والنشطاء باستخدام تقنيات مثل بيغاسوس. واستكمل شريف حديثه قائلا: "لذلك يجب ألا يكون الرد محليًا أو إقليميًا بل دوليًا."

ثم أضاف شريف "هذا هو السبب الذي دفع لجنة حماية الصحفيين لإرسال توصية إلى الولايات المتحدة والاتحاد الأوروبي ومسؤولي الأمم المتحدة للعمل معًا. والآن لدينا 160 منظمة في جميع أنحاء العالم تدعو إلى وقف عمل خبراء برمجيات المراقبة. كما تدعم أيضا لجنة حماية الصحفيين الدعوى القضائية في الولايات المتحدة التي قدمتها WhatsApp وشركات أخرى لاستخدام NSO Group لتجسس وخرق الخصوصية في برامجهم".

أكد جميع المشاركين في البث على أنه تم استخدام تقنية التجسس "بيغاسوس" لتعزيز قمع الأصوات المعارضة خارج حدود الدول. ففي الوقت الحالي لا يستطيع الصحفيون الذين يعيشون في المنفى في منطقة الشرق الأوسط وشمال إفريقيا الشعور بالأمان كمنفيين حيث تعزز هذه التكنولوجيا الرقابة والقمع خارج حدود الأنظمة المعروفة بانتهاك حقوق الإنسان وحرية التعبير .

كما أجمع المشاركين على ضرورة وضع وسائل تحمي الأشخاص من مثل هذه التقنيات، وفي هذا السياق، قال "خالد ابراهيم" أنه من الضروري التأكد من عدم التجسس على هاتفك بمساعدة أحد خبراء تكنولوجيا المعلومات. كما أنه من المستحيل تقديم شكوى محلية حول هذا الأمر أو حماية الضحايا، لذلك من الضروري استخدام مفهوم الولاية القضائية الدولية ونقل القضية إلى المحاكم المعترف بها دوليًا، والتي يمكنها اتخاذ إجراءات قانونية على المستوى الدولي.

حيث شارك مركز الخليج لحقوق الإنسان، بالتعاون مع منظمات أخرى ، مؤخرًا في قضية قانونية مقدمة في فرنسا ضد مجموعة NSO وهناك المزيد من المنظمات التي تشارك في هذه الجهود لعزل الشركة الإسرائيلية، كما يجب على المزيد من المنظمات الدولية والدول ان تشارك في إيقاف مثل هذه التقنية.

وأشارت "مروة" إلى أن هناك عدة أمور يجب استكشافها لوقف عمل بيغاسوس. أولاً، نحتاج إلى إجراء تحقيق شامل وعالمي لفهم هذه التكنولوجيا ومدى انتشارها. نحتاج أيضًا إلى التفكير في سبل تنصف الضحايا.

أكدت سكاي لاين والمشاركين في البث على أهمية سن تشريعات دولية ووطنية لضمان قيام شركات مثل هذه بالتصريح عن عملائها وعملياتها وليتم أيضا أخذ أحكام حقوق الانسان بعين الاعتبار. ومع ذلك، يمكن القول بأن هذه التكنولوجيا بحكم تعريفها تنتهك حقوق الإنسان، ولا توجد وسيلة يمكن للدول أن تستخدم فيها بيغاسوس بشكل ايجابي دون انتهاك لاي حقوق.

هناك حاجة للتأكد من أن القوانين الوطنية تنظم استخدام مثل هذه البرامج أيضًا. لذلك فإن التقاضي هو وسيلة للاسمرار بملاحقة وايقاف عمل مثل هذه الشركات. وخلصت مروة الى أن " القضايا الرئيسية التي يجب التركيز عليها، المساءلة من خلال التقاضي، والتنظيم على الصعيدين العالمي والوطني، والرقابة الصارمة على صادرات برامج المراقبة."

واختتم "شريف" مداخلته بالتأكيد على " أنه من الأهمية معرفة أنه لا يوجد من هو في مأمن من هذه التكنولوجيا، فعلى الرغم من أن مجموعات NSO تدّعي أنه لا يمكن اختراق الهواتف الأمريكية، لا توجد طريقة لمعرفة ما إذا كان هذا صحيحًا. لذا، من المهم أن نتذكر أنه ليست الشركات الإسرائيلية هي من يستفيد ف حسب من تقنية بيغاسوس، بل الشركات الأوروبية والأمريكية، وكذلك الشركات الأخرى في إسرائيل.

وأشارت "سكاي لاين" إلى اتخاذ الاتحاد الأوروبي بعض تدابير المساءلة من خلال إنشاء بعض الرقابة المتخصصة على هذه البرنامج، ومن المتوقع أن تقوم الولايات المتحدة بنفس الشيء قريبا حيث كما يمكنها فرض ضوابط صارمة على شركاتها ستفعل نفس الشيء مع حلفائها الذين يبيعون ويستخدمون هذا البرنامج (المغرب، إسرائيل، السعودية، الإمارات العربية المتحدة). وبأن التحقيق في هذه الانتهاكات من قبل حكومة الولايات المتحدة والإبلاغ عنها سيساعد في تمكين عمل المجتمع المدني والجمهور العام بشأن هذه القضية.

واختتمت سكاي لاين لقائها بالتأكيد على أهمية الاستمرار في الضغط على الدول والمنظمات الدولية والجمهور لوقف تسويق هذا النوع من البرامج التي تنتهك بشكل صارخ حقوق الإنسان وحرية التعبير. مؤكدة على أن هذه التقنية تعمل على تسليح التكنولوجيا المدنية وتحويلها ضد مستخدميها، مما يتسبب في أضرار جسيمة لعمل الشخص المستهدف وحياته الخاصة وسمعته. كما أظهر المشاركين في البث مخاطر هذا البرنامج وبرمجته والاجراءات التي يجب اتخاذها لمنع انتشار برنامج التجسس هذا في جميع أنحاء العالم .