الرباط، 22 يونيو 2020

تقرير – استهداف صحفي مغربي بهجمات حقن شبكات الاتصالات باستخدام أدوات مجموعة "إن إس أو"

ملخص

- في أكتوبر/ تشرين الأول 2019، نشرت منظمة العفو الدولية أول تقرير عن استخدام برامج التجسس التي تنتجها شركة مجموعة "إن إس أو" الإسرائيلية ضد المدافعيْن الحقوقييْن المغربيين المعطي منجب وعبد الصادق البوشتاوي. من خلال تحقيقنا المستمر، حدد المختبر الأمني لمنظمة العفو الدولية أدلة مماثلة على استهداف **عمر راضي**، وهو ناشط وصحفي بارز من المغرب، في الفترة من يناير/كانون الثاني 2019 حتى نهاية يناير/كانون الثاني 2020.

- وكشفت الأدلة التي تم جمعها من خلال تحليلنا الفني لجهاز آي فون iPhone الخاص بعمر راضي عن آثار لنفس هجمات "حقن شبكات الاتصالات" التي وصفناها في تقريرنا السابق والتي تم استخدامها ضد المعطي منجب. وهذا يقدم دليلًا قوياً يربط هذه الهجمات بأدوات مجموعة "إن إس أو".

- وتتسم هذه النتائج بأهمية خاصة لأن عمر راضي تم استهدافه بعد ثلاثة أيام فقط من إصدار مجموعة "إن إس أو" لسياستها المتعلقة بحقوق الإنسان. وتواصلت هذه الهجمات بعد أن علمت الشركة بتقرير منظمة العفو الدولية الأول الذي قدم أدلة على وقوع الهجمات الموجهة في المغرب. وهكذا، يدل هذا التحقيق على استمرار تقاعس مجموعة "إن إس أو" في توخي الحرص الواجب إزاء حقوق الإنسان، وعدم فعالية سياستها الخاصة بحقوق الإنسان.

مقدمة

في أكتوبر 2019، نشرت منظمة العفو الدولية تقريراً بعنوان: "المغرب: استهداف المدافعين عن حقوق الإنسان ببرنامج تجسس تابع لمجموعة "إن إس أو"، حيث قمنا بتفصيل استهداف المدافعيْن عن حقوق الإنسان المغربيين المعطي منجب وعبد الصادق البوشتاوي،

20، زنقة ورغة، رقم 5، الطابق 2، أكدال – الرباط 20, Rue Ouargha, N. 5, 2ème étage, Agdal – Rabat 10080
+212 (0) 537 681 048 +212 (0) 537 686 648
admin-ma@amnesty.org www.amnesty.ma

باستخدام تكنولوجيا الرقابة التي تنتجها شركة مجموعة "إن إس إو". وفي هذا التقرير، تكشف منظمة العفو الدولية الآن أن **عمر راضي**، وهو مدافع بارز آخر عن حقوق الإنسان وصحفي من المغرب، تم استهدافه أيضاً باستخدام أدوات مجموعة إن إس أو.

لقد كثفت السلطات المغربية مؤخراً حملتها ضد المعارضة السلمية من خلال الاعتقالات التعسفية ومقاضاة الأفراد، بما في ذلك الصحفي عمر راضي، والبعض من مغني موسيقى الراب ومدوني يوتيوب، الذين استُهدف الكثير منهم لمجرد انتقادهم الملك أو مسؤولين آخرين. ومنذ نونبر 2019، وثقت منظمة العفو الدولية عشر حالات لنشطاء تم اعتقالهم بشكل غير قانوني ومقاضاتهم. اتُهم الأفراد العشرة بتهمة "إهانة" الموظفين العموميين أو المؤسسات العامة، الملك أو الملكية، وجميعها جرائم بموجب القانون الجنائي المغربي. وبين نونبر 2019 ومارس 2020، حُكم على جميع الأفراد والناشطين العشرة بالسجن مدد تتراوح بين أربعة أشهر مع وقف التنفيذ، وأربع سنوات. وقد دعت منظمة العفو الدولية السلطات المغربية إلى إسقاط التهم وإطلاق سراح المحكوم عليهم لممارستهم حقهم في حرية التعبير؛ وإلى إصلاح القانون الجنائي لإلغاء تجريم هذه الأشكال من التعبير المكفول بالقانون.

في 26 دجنبر 2019، اعتقلت السلطات المغربية راضي بسبب تغريدة نشرها في وقت سابق من ذلك العام، في أبريل ، وانتقدت النظام القضائي لتأييد الحكم ضد المحتجين من حركة الاحتجاج في 2017 في المنطقة الشمالية المغربية المعروفة باسم حراك الريف. بعد أيام قليلة من اعتقاله، أفرجت عنه محكمة الدار البيضاء إفراجاً مؤقتاً. لكن في 17 مارس، حكمت عليه محكمة في الدار البيضاء بالسجن أربعة أشهر مع وقف التنفيذ ودفع غرامة قدرها 500 درهم (52 دولاراً).

وعمر راضي هو صحفي استقصائي وناشط مغربي حاصل على جائزة، وعمل في العديد من وسائل الإعلام الوطنية والدولية، بما في ذلك راديو أتلانتيك Atlantic Radio، ومجلة تيلكيل TelQuel. وقام في عمله بالتحقيق في الصلات بين مصالح الشركات والمصالح السياسية في المغرب، وتطرق إلى قضايا الفساد وغيرها من قضايا انتهاكات حقوق الإنسان في المغرب، وكثيراً ما تناول استمرار الإفلات من العقاب، وغياب العدالة في البلاد.

أجرى مختبر الأمن التابع لمنظمة العفو الدولية تحليلاً تقنياً لهاتف عمر راضي، ووجد آثاراً تشير إلى أنه تعرض لنفس هجمات حقن شبكات الاتصالات التي رصدناها لأول مرة ضد المعطي منجب، ووصفناها في تقريرنا السابق. ومن خلال تحقيقنا تمكنا من التأكد من أن هاتفه كان مستهدفاً، ووضع تحت الرقابة خلال نفس الفترة التي حوكم فيها. وهذا يوضح كيف قد يضطر المدافعون عن حقوق الإنسان في كثير من الأحيان إلى مواجهة التحدي المزدوج للرقابة الرقمية إلى جانب أساليب أخرى للتجريم على أيدي السلطات المغربية مما يؤدي إلى تقلص مساحة المعارضة.

حقن شبكات الاتصالات، وأبراج اتصالات مارقة، ومجموعة "إن إس أو"

الافتقار إلى الشفافية حول صناعة الرقابة يجعل من الصعب معرفة الأدوات المستخدمة والمباعة والمشتراة والتي يساء استخدامها، وبالتالي يصعب على الضحايا والمراقبين السعي إلى إجراء المساءلة. وعلى الرغم من ذلك، فقد سلط بحثنا حتى الآن الضوء على كيفية تطور تكنولوجيا مجموعة "إن إس أو". حتى مطلع 2018، وُجد أن زبائن مجموعة "إن إس أو" يستخدمون بشكل رئيسي رسائل نصية قصيرة ورسائل واتساب من أجل خداع الأهداف ليفتحوا رابط خبيث، مما سيؤدي إلى استغلال وإصابة أجهزتهم المحمولة. وكما وثقنا في تقريرنا في أكتوبر 2019، لاحظت منظمة العفو الدولية أولاً أن المهاجمين يتبنون تقنيات جديدة لإيصال البرامج الضارة بشكل أشد خلسة وفعالية. فقد أصبح المهاجمون قادرين على تثبيت برامج التجسس دون الحاجة إلى أي تفاعل من قبل الهدف وذلك باستخدام ما نصفه بأنه "حقن شبكة الاتصالات".

في حين أن التقنيات السابقة تعتمد إلى حد ما على خداع المستخدم للقيام بخطوة ما، فإن حقن شبكة الاتصالات تسمح بإعادة التوجيه التلقائي وغير المرئي لمتصفحات وتطبيقات الأهداف إلى مواقع ضارة تحت سيطرة المهاجمين، غالبا ما تكون غير معروفة للضحية. وستعمل هذه المواقع على الاستفادة بشكل سريع من ثغرات البرامج من أجل اختراق الجهاز وإصابته.

وهذا ممكن فقط عندما يكون المهاجمون قادرين على الرصد والتحكم في حركة الهدف على الإنترنت. في كل من حالتي عمر والمعطي تم حقن شبكات الاتصالات أثناء استخدام اتصالهما بالإنترنت عبر الهاتف المحمول من خلال الجيل الرابع 4G/تطور طويل الأمد (LTE).

وهذا النوع من الهجوم ممكن باستخدام تقنيتين: نشر جهاز يشار إليه عادة باسم "برج اتصالات مارق" أو "ماسك هوية مشترك الهاتف المحمول الدولي - آي إم إس آي كاتشر - IMSI Catcher" أو "ستينغراي - stingray"؛ أو عن طريق الاستفادة من منفذ إلى البنية الأساسية الداخلية لمشغلي الهواتف المحمولة. ومن غير الواضح حالياً أي من هاتين التقنيتين تمّ استخدامها ضد عمر والمعطي.

ومع ذلك، تم وصف إمكانيات مجموعة "إن إس أو" في شن هجمات حقن شبكات الاتصالات بشكل موجز في وثيقة تحمل اسم "بيغاسوس - وصف المنتج" - يبدو أن مجموعة "إن إس أو" قد كتبتها - وتم العثور عليها في تسريب حصل في عام 2015 ل مصنّع برنامج التجسس الإيطالي المنافس، هاكينغ تيم Hacking Team. على وجه التحديد، في يناير 2020، أبلغت صحيفة بيزنيس إنسيدر Business Insider عن تكنولوجيا اعتراض الهاتف المحمول لمجموعة "إن إس أو" التي عرضتها خلال معرض ميليبول-Milipol، وهو فعالية ومعرض تجاري حول "الأمن الوطني" عقد في باريس في نونبر 2019.

حقوق الصورة: Becky Peterson/Business Insider

تعرض الصورة ما يبدو أنه نموذج لبرج الاتصالات المارق الذي تبيعه مجموعة "إن إس أو" - وهي أداة يمكن استخدامها في واحدة من التقنيتين اللتين تم تحديدهما أعلاه لإحداث هجوم حقن شبكة الاتصالات.

وتعمل هذه الأجهزة كمحطات قاعدي محمولة تنتحل صفة أبراج خلوية مشروعة من أجل خداع الهواتف في المنطقة المجاورة للاتصال بها، وتمكين المهاجم من التحكم بحركة بيانات الهاتف المحمول الذي تم اعتراضه. يبدو أن برج الاتصالات المارق في الصورة، يتألف من بطاقات مختلفة مكدسة أفقياً، ومن المرجح أنه على هذا النحو من أجل السماح للمشغلين بالاعتراض عبر نطاقات تردد متعددة لشبكات GSM (النظام العالمي للاتصالات المتنقلة)، والجيل الثالث 3G، وشبكات الجيل الرابع 4G ... إلى آخره. وكما بينت المحاكاة التي قامت بها مجموعة "إن إس أو" في كشكها في معرض ميليبول-Milipol ، هذه المعدات الإلكترونية يمكن أن تكون صغيرة للغاية، وبالتالي يمكن نقلها وإخفائها بسهولة في المركبات الصغيرة.

20، زنقة ورغة، رقم 5، الطابق 2، أكدال – الرباط 10080 20, Rue Ouargha, N. 5, 2ème étage, Agdal – Rabat
☎ +212 (0) 537 686 648 🖷 +212 (0) 537 681 048
admin-ma@amnesty.org www.amnesty.ma

وبدلاً من ذلك، يمكن للمهاجمين بالمثل اعتراض وقرصنة حركة بيانات الهواتف الذكية المستهدفة على الإنترنت، إذا تمكنوا من النفاذ إلى بنية مشغل الهاتف المحمول للضحية. في هذه الحالة، بدلاً من وضع برج الاتصالات المارق في المناطق المجاورة للهدف، فإن المهاجمين يعتمدون على البنية الأساسية الحالية للشبكة لمشغل الهاتف المحمول المستخدم من قبل الهدف.

وخلاصة القول، فإن الهجمات السابقة ضد المدافعين عن حقوق الإنسان التي وثقتها منظمة العفو الدولية في المغرب قد أثارت إمكانية استخدام أدوات مجموعة "إن إس أو" في هجمات حقن شبكة الاتصالات. ومن الواضح أيضاً من المعلومات المتاحة للجمهور أن مجموعة "إن إس أو" تبيع إمكانات حقن شبكة الاتصالات. وإن ذلك يعزز الأدلة التي تربط أدوات حقن الشبكات التابعة لمجموعة "إن إس أو" بهذا الهجوم، عندما يؤخذ مع الأدلة التقنية التي نوردها بالتفصيل في القسم التالي، والتي تظهر تداخلات في التوقيت، ومواد التحليل التقني المستعادة والبنى الأساسية للهجوم المرتبطة بهجمات الرقابة السابقة في المغرب باستخدام أدوات مجموعة "إن إس أو".

استهداف عمر راضي بحقن شبكة الاتصالات بين يناير/كانون الثاني 2019 ويناير 2020

أشار تحليلنا السابق لهاتف المعطي منجب إلى تنفيذ برامج ضارة عليه منذ أوائل عام 2018 وحتى يونيو 2019 على الأقل. في حين أنه تم استهدافه بين عامي 2017 و2018 من خلال رسائل نصية قصيرة تحمل روابط خبيثة مرتبطة بمجموعة "إن إس أو"، فقد وصفنا في تقريرنا الصادر في أكتوبر 2019 كيف يبدو أن هاتف المعطي منجب قد تعرض لعمليات إعادة توجيه ضارة أثناء تصفّحه الإنترنت باستخدام متصفح سفاري Safari. وقلنا إن عمليات إعادة التوجيه هذه كانت أعراضاً لهجمات حقن شبكة الاتصالات التي استغلت حركة انترنت غير مشفرة من أجل إجبار متصفح المعطي منجب على زيارة موقع استغلال، يقع في النطاق **free247downloads[.]com**، دون علمه.

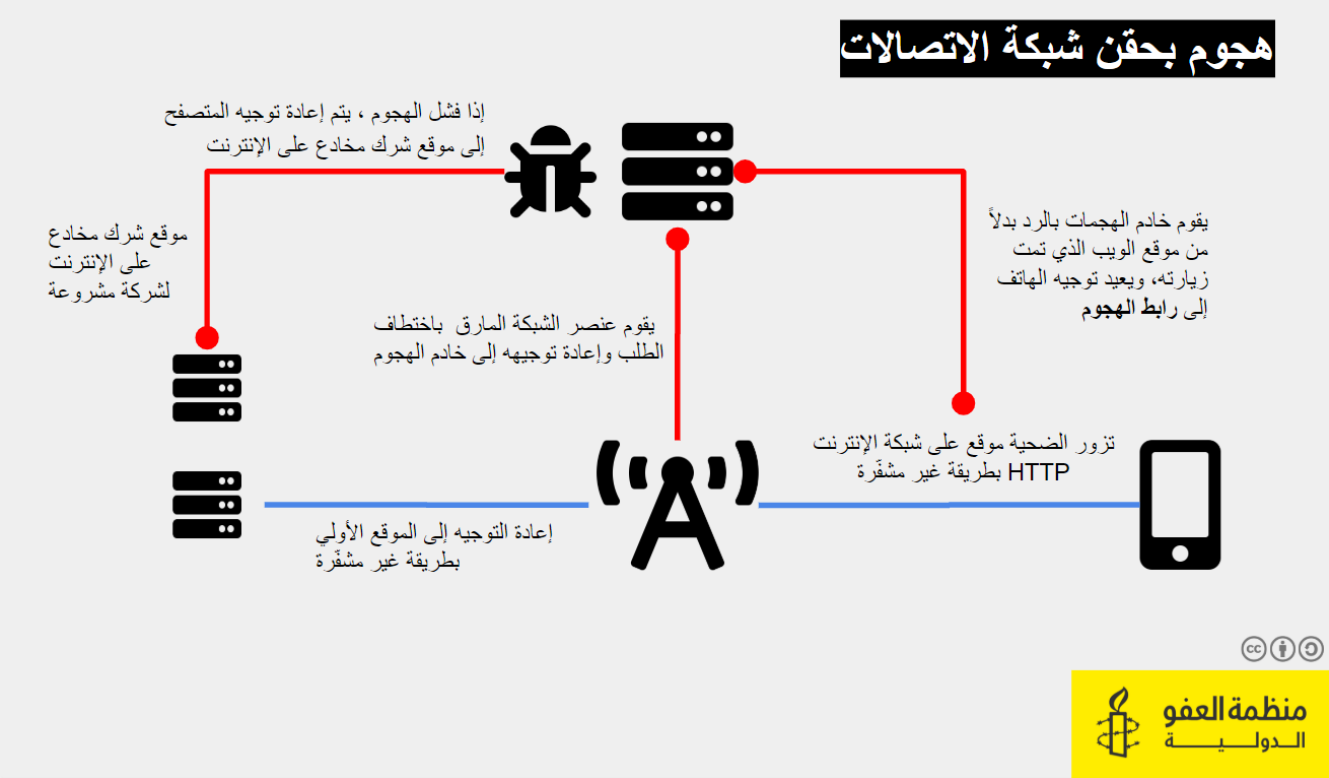
وأثناء تحليل هاتف آي فون عمر راضي، وجدنا أثاراً لنفس النطاق. تشير مواد التحليل التقني التي استخرجتها منظمة العفو الدولية من الجهاز إلى وقوع هجمات حقن الشبكة في 27 يناير و11 فبراير و13 شتنبر 2019.

بالإضافة إلى نفس موقع الاستغلال، حددنا نفس الأدلة على تنفيذ البرامج الضارة التي استعدناها من هاتف المعطي منجب في هاتف راضي أيضاً. وهذا يوفر لنا أدلة إضافية على أن نفس برنامج التجسس تم استخدامه في كلتا الحالتين، والذي نعتقد - على أساس تداخل البنية الأساسية في كلتا الحالتين وخصائص الروابط المستخدمة - أن يكون برنامج بيغاسوس التابع لمجموعة "إن إس أو".

ويسجل الجدول الزمني التالي التواريخ الرئيسية المرتبطة ببرامج التجسس الخاصة بمجموعة "إن إس أو" في المغرب. وتبين أدلة الفحص الجنائي التي تم استخراجها من كلا الهاتفين الصلات بين مختلف مراحل الهجمات.

✉ 20, Rue Ouargha, N. 5, 2ème étage, Agdal – Rabat 10080 ✉ 20، زنقة ورغة، رقم 5، الطابق 2، أكدال – الرباط
☎ +212 (0) 537 686 648 🖷 +212 (0) 537 681 048
admin-ma@amnesty.org www.amnesty.ma

فيما يلي، رسم يصور هجوم حقن شبكة الاتصالات على هاتف عمر لوحظ بينما كان يزور موقع على شبكة الانترنت بطريقة غير مشفرة (HTTP وليس HTTPS):



في 2 أكتوبر 2019، وكجزء من عملية النشر، قدمنا إلى مجموعة "إن إس أو" نسخة متقدمة من النتائج التي توصلنا إليها من تقريرنا "المغرب: استهداف المدافعين عن حقوق الإنسان ببرنامج تجسس تابع لمجموعة "إن إس أو"، وأعطيناهم فرصة للرد على ما كشف عنه التقرير. ووفقًا للبيانات التي جمعتها خدمة استطلاع على الإنترنت Censys.io، تم إغلاق البنية الأساسية التي يتحكم بها المهاجمون والمرتبطة بنطاقات فرعية لـ **free247downloads[.]com** بحلول 6 أكتوبر 2019، بعد التشغيل المتواصل تقريباً منذ ظهوره لأول مرة قبل عام، بعد أيام فقط من إخطار مجموعة "إن إس أو" بنتائجنا، ولكن قبل نشرنا التقرير في 10 أكتوبر 2019.

بالإضافة إلى ذلك، كشف تحليلنا لهاتف عمر عن آثار لحقن شبكة اتصالات مماثلة في فترة قريبة وهي 29 يناير 2020. وشملت هذه المحاولات الأخيرة اسم النطاق الجديد، الذي لم يتم الكشف عنه من قبل **urlpush[.]net**

تم تسجيل اسم النطاق *urlpush[.]net* في 6 نونبر 2019، بعد عدة أسابيع من نشرنا التقرير السابق، مما يشير إلى أن تقريرنا ربما دفع المهاجمين إلى تغيير البنية الأساسية للهجمات.

وخلاصة القول، في حين أن التوقيت يوحي بارتباط بمجموعة "إن إس أو"، فإن التفاصيل التقنية للهجمات، بما في ذلك أن كلا الموقعين يعيدان التوجيه إلى نفس الموقع، ويشنان الهجمات باستخدام العديد من مواد التنفيذ والفحص التقني المتطابقة، دليل قوي يربط أدوات مجموعة "إن إس أو" بالهجوم المستهدف على عمر راضي.

من يقف وراء هذه الهجمات؟

تدعي مجموعة "إن إس أو" أنها تبيع منتجاتها فقط إلى الأجهزة الحكومية. ووفقاً لموقع مجموعة "إن إس أو" على الإنترنت، *"أن منتجاتها تستخدم حصرياً من جانب أجهزة المخابرات وتنفيذ القانون لمكافحة الجريمة والإرهاب"*.

وفي تقريرها الصادر في شتنبر 2018، المعنون: "لعبة الغميضة تتبُّع عمليات برنامج بيغاسوس من شركة NSO في 45 دولة"، تحدد منظمة سيتزن لاب مشغلاً أطلق عليه اسم "أطلس ATLAS" يركز على المغرب. تشير أبحاثنا الخاصة إلى استمرار استخدام نفس البنية الأساسية للشبكة الضارة في الهجمات لتكون سمة كيان واحد وراء استخدام منتج مجموعة "إن إس أو" في المغرب. بالإضافة إلى ذلك، كما هو موضح سابقًا، فإن هجمات حقن شبكة الاتصالات التي وثقناها في المغرب، تتطلب إما القرب المادي من الأهداف أو القدرة على التأثير على مشغلي الهواتف المحمولة في البلاد التي لا يمكن أن تأذن بها سوى الحكومة. وبسبب هذا، واستمرار استهداف المدافعين المغاربة عن حقوق الإنسان، نعتقد أن السلطات المغربية هي المسؤولة عن هذه الهجمات.

لذلك، وعلى الرغم من الرقابة غير القانونية للمعطي منجب وعبد الصادق البوشتاوي التي كشفتها منظمة العفو الدولية، ووثقتها في أكتوبر 2019، نستنتج أن الحكومة المغربية ظلت على نحو نشط من عملاء مجموعة "إن إس أو" حتى يناير 2020 على الأقل، ولا تزال تستهدف المدافعين عن حقوق الإنسان بشكل غير قانوني، كما هو الحال في حالة عمر راضي.

وكل هذا يحدث في سياق يخضع فيه المدافعون عن حقوق الإنسان في المغرب للرقابة على نحو متزايد. كما يشير استمرار إساءة استخدام أدوات مجموعة "إن إس أو" في البلاد إلى تقاعس السلطات المغربية عن احترام وحماية الحق في حرية التعبير، وتكوين الجمعيات أو الانضمام إليها، والتجمع السلمي.

وبالإضافة إلى ذلك، وعلى الرغم من حالات عديدة من انتهاكات حقوق الإنسان، فإن الولايات القضائية المصدرة التي تمنح التراخيص لمجموعة "إن إس أو"، قد أخفقت في مسؤوليتها عن حماية حقوق الإنسان بعدم القيام بالتدقيق الكافي، وعدم رفض إعطاء الإذن بالتصدير عندما يكون هناك خطر كبير من إمكانية استخدام التصدير المشار إليه في انتهاك حقوق الإنسان.

وقد طلبنا من مجموعة "إن إس أو" الرد على المعلومات المفصلة التي كشف عنها هذا التقرير. ويرد ردها في مجمله في الملحق المرفق. كما كتبنا إلى الحكومة المغربية، إلا أننا لم نتلق رداً. لم تؤكد مجموعة "إن إس أو" أو تنفي ما إذا كانت السلطات المغربية تستخدم التكنولوجيا التي طوّرتها المجموعة وذكرت أنها ستراجع المعلومات المقدمة. وستتابع منظمة العفو الدولية الموضوع على ضوء الردّ الذي حصلت عليه.

وترد تفاصيل إضافية عن هذه الهجمات في *الملحق التقني* المرفق بهذا التقرير.

تقاعس مجموعة "إن إس أو" المتكرر عن التحقق من إساءة استخدام أدواتها

في أكتوبر 2019، رداً على تقريرنا بأن أدوات مجموعة "إن إس أو" قد استُخدمت لاستهداف المدافعين عن حقوق الإنسان بشكل غير قانوني في المغرب، أبلغت مجموعة "إن إس أو" منظمة العفو الدولية في رسالة بالتالي: *"تُطوّر منتجاتنا لمساعدة مجتمع الاستخبارات وإنفاذ القانون على إنقاذ حياة الناس. وهي ليست أدوات لمراقبة المعارضين أو نشطاء حقوق الإنسان. لهذا السبب فإن العقود مع جميع*

عملائنا تمكن من استخدام منتجاتنا فقط للأغراض المشروعة وهي منع الجريمة والإرهاب والتحقيق فيهما. وإذا اكتشفنا يوماً أن منتجاتنا قد أسيء استخدامها في خرق لمثل هذا العقد، فسوف نتخذ الإجراء المناسب".

وسألنا مجموعة "إن إس أو" عما إذا كانت قد اتخذت أي إجراء استجابة لتقريرنا السابق بما يحتويه من تفاصيل عن التحقيقات، ولماذا لم تنه عقدها مع السلطات المغربية، وعن تفاصيل أي إجراءات تخفيف الضرر قد تكون اتخذتها. لم تقم مجموعة "إن إس أو" بالإجابة بشكل محّدد على هذه الأسئلة في ردها، لأسباب تتعلق بالسرية حسبما وضّحت.

وعلى الرغم من هذه الادِّعاءات، يقدم هذا التقرير أدلة قوية على أن عمر راضي استُهدف بشكل غير قانوني باستخدام أدوات مجموعة "إن إس أو" في يناير 2020 وذلك بعد أن علمت مجموعة "إن إس أو" بالتحقيق الأول الذي أجرته منظمة العفو الدولية. وتستخدم أدوات الشركة لدعم جهود الحكومة المغربية من أجل اضطهاد الناس بسبب ممارستهم حرية التعبير، وقمع المعارضة.

وهذا يشير إلى أن مجموعة "إن إس أو"، خلافاً لمزاعمها، لم تتخذ إجراءات كافية لوقف استخدام أدواتها للرقابة غير المشروعة التي تستهدف المدافعين عن حقوق الإنسان في المغرب، على الرغم من علمها بأن ذلك كان يحدث. وهذا يدل على أن مجموعة "إن إس أو" لم تتوخى الحرص الواجب الكافي إزاء حقوق الإنسان من أجل منع الضرر أو التخفيف منه، ونتيجة لذلك لم تف بمسؤوليتها بموجب المعايير الدولية من أجل عدم المساهمة في انتهاكات حقوق الإنسان.

في فبراير 2019، دعمت شركة الأسهم الخاصة نوفابينا كابيتال Novalpina Capital، التي تتخذ من المملكة المتحدة مقراً لها، الاستحواذ الإداري على مجموعة "إن إس أو" وتمتلك نوفابينا كابيتال حصة مسيطرة من الشركة. في 10 شتنبر 2019، قالت نوفابينا كابيتال/مجموعة "إن إس أو" أنها ستنفذ سياسة حقوق الإنسان، وأن الشركة ستحكمها "لجنة الحوكمة والمخاطر والامتثال". وكما هو مفصل في هذا التقرير، بعد ثلاثة أيام فقط من هذا الإعلان، في 13 شتنبر 2019، تم استهداف عمر راضي. وهذا دليل آخر على وجود فجوة كبيرة بين سياسة الشركة المعلنة والممارسة الفعلية.

كيفية التحقق من وجود هجمات مماثلة على هاتف آي فون الخاص بك

إذا كنت مدافعاً مغربياً عن حقوق الإنسان ومستخدماً لهاتف آي فون، يمكنك اتباع الخطوات الموضحة في مقاطع الفيديو التالية للتحقق من وجود أدلة على هجمات مماثلة لتلك الموضحة في هذا التقرير:

انظر الفيديو على هذا الرابط - https://bit.ly/2ANS2qn

كيفية الحماية من هجمات حقن شبكة الاتصالات

نظرا لاعتماد المهاجمين على تحويل وجهة حركة الإنترنت على هاتفك المحمول ولكي تكون هذه العملية ناجحة، فإن المهاجمين بحاجة إلى فحص محتوى المواقع التي تزورها. وللقيام بذلك، يتم إنتظار زيارات HTTP غير المشفرة. في حين أن العديد من مواقع الإنترنت تتيح الآن استخدام تشفير النقل (المشار إليه بواسطة الروابط التي تبدأ بـ *https://* بدلاً من *http://*)، لا يزال العديد منها لا يتيح ذلك.

من الصعب التفطّن لهجمات حقن شبكة الاتصالات لأنها توفر أدلة بصرية قليلة جداً. عند استخدام أساليب أخرى لتوصيل برامج التجسس، مثل الروابط الخبيثة المرسلة عبر رسائل نصية قصيرة جذابة، قد يتنبه الشخص المستهدف، فيتجنب النقر. وعلى خلاف ذلك، يحدث هجوم حقن شبكة الاتصالات بشكل غير مرئي أثناء تصفّح الويب بشكل منتظم.

يمكن أن يساعد تجهيز هاتفك بشبكة خاصة افتراضية (VPN) ، لأنه من شأنه أن يحجب كل حركة المرور الواردة والصادرة، مما يمنع من التلاعب بها. ومع ذلك، فاختيار شبكة خاصة افتراضية جيدة أمر مهم. وتتوفر تطبيقات شبكات خاصة افتراضية ضارة أو مشكوك فيها على متاجر تطبيقات iOS وAndroid. تجنّب الشبكات الخاصة الافتراضية المجانية، لأنه من الأكثر ترجيحاً أن تستخدم بياناتك من أجل الربح، وتكون أقل احتراماً لحقك في الخصوصية.

تأكد دائماً من تنزيل آخر التحديثات لجهازك وللتطبيقات المثبتة. تقوم الشركات المصنعة للأجهزة والبرامج بإصدار تصحيحات أمنية بانتظام. قد يؤدي التأخير في التحديث إلى تعريض جهازك لخطر التعرض للهجوم دون داع.

20، زنقة ورغة، رقم 5، الطابق 2، أكدال – الرباط 10080 20, Rue Ouargha, N. 5, 2ème étage, Agdal – Rabat
☎ +212 (0) 537 686 648 🖷 +212 (0) 537 681 048
admin-ma@amnesty.org www.amnesty.ma

وتشير التقارير الأخيرة من الباحثين الأمنيين إلى أنه حتى المهاجمين المتقدمين يعانون من صعوبات متزايدة للحفاظ على النفاذ المستمر إلى جهاز محمول تم اختراقه. وإذا كان الأمر كذلك، فإن إعادة تشغيل الجهاز يعطّل الإصابة. لذلك، وكإجراء وقائي، قد ترغب في إطفاء هاتفك الذكي وإعادة تشغيله مرة أخرى من حين لآخر.

خاتمة

في أكتوبر 2019، قمنا بتوثيق الأدلة لأول مرة على استخدام أدوات مجموعة "إن إس أو" لاستهداف اثنين من المدافعين عن حقوق الإنسان المغاربة. كما استُهدف أحدهما، وهو المعطي منجب، باستخدام هجمات حقن شبكة الاتصالات. وقد اشتبهنا في أن هذه الهجمات كانت مرتبطة أيضًا بأدوات مجموعة "إن إس أو" وفي هذا التقرير، نورد بالتفصيل عملية الرقابة الموجهة غير القانونية لمدافع عن حقوق الإنسان مغربي آخر، وهو عمر راضي، بما في ذلك الأدلة التقنية القوية التي تربط أدوات مجموعة "إن إس أو" بهذا الهجوم.

فهذه الهجمات على المدافعين عن حقوق الإنسان هي جزء من حملة قمع متنامية للمعارضة السلمية في المغرب. يشير استمرار إساءة استخدام أدوات مجموعة "إن إس أو" في البلاد إلى تقاعس السلطات المغربية عن احترام وحماية الحق في حرية التعبير، وتكوين الجمعيات أو الانضمام إليها، والتجمع السلمي.

وبالإضافة إلى ذلك، فإن تقاعس مجموعة "إن إس أو" المتكرر عن اتخاذ إجراء بشأن إساءة استخدام السلطات المغربية لأدواتها، يشير إلى أنها أخفقت في تحمل مسؤولياتها في مجال حقوق الإنسان في عدم المساهمة في انتهاكات حقوق الإنسان، ولم تتوخى الحرص الواجب الكافية في مجال حقوق الإنسان من أجل التخفيف من الانتهاكات.

توصيات

ينبغي على السلطات المغربية والبلدان المصدرة تنفيذ إطار تنظيمي مناسب لحقوق الإنسان يحكم عمليا الرقابة. وإلى أن يتم تنفيذ مثل هذا الإطار، ينبغي فرض وقف اختياري لبيع ونقل واستخدام معدات المراقبة، على النحو الذي أوصى به المقرر الخاص للأمم المتحدة المعني بحرية التعبير، ديفيد كاي. وينبغي أن يشمل إطار حقوق الإنسان هذا، كحد أدنى، ما يلي:

إلى السلطات المغربية:

- الكشف عن معلومات حول جميع العقود السابقة أو الحالية أو المستقبلية مع شركات الرقابة الخاصة، بما في ذلك تلك المبرمة مع مجموعة "إن إس أو".
- وقف الرقابة غير القانونية للصحفيين والمدافعين عن حقوق الإنسان التي تنتهك الحق في الخصوصية، وحرية التعبير.
- ضمان التطبيق والتنفيذ الفعالين للمادة 24 من الدستور المغربي وقانون المسطرة الجنائية، الفصل 5 لضمان أن أي رقابة رقمية مرخصة من قبل السلطات القضائية المختصة مسبقاً.
- ضمان قيام النواب العامين واللجنة الوطنية لمراقبة حماية المعطيات ذات الطابع الشخصي بإجراء تحقيق مستقل وفعال في حالات الرقابة الرقمية الموجهة غير القانونية.

إلى الدول المُصدّرة:

- رفض التصريح بالتصدير عندما يكون هناك خطر كبير من إمكانية استخدام المواد المصدرة المعنية لانتهاك حقوق الإنسان.
- ضمان فحص كل تكنولوجيا ذات صلة قبل نقلها.

بالإضافة إلى ذلك، ينبغي على مجموعة **"إن إس أو" ونوفالبينا كابيتال** كحد أدنى:

- اتخاذ خطوات استباقية على وجه السرعة لضمان عدم تسببها أو مساهمتها في انتهاكات لحقوق الإنسان، والتصدي لأي انتهاكات لحقوق الإنسان عند وقوعها. ومن أجل الوفاء بتلك المسؤولية، يجب على مجموعة "إن إس أو" توخي الحرص الواجب الكافي إزاء حقوق الإنسان، واتخاذ خطوات لضمان عدم استمرار استهداف المدافعين عن حقوق الإنسان في المغرب بالرقابة غير القانونية.
- إنهاء أو تعليق عقدها مع السلطات المغربية.
- ضمان الشفافية فيما يخص حجم معدات الرقابة المنقولة وطبيعتها وقيمتها ووجهتها ومستخدميها النهائيين.

الملحق 1 ردّ مجموعة "إن إس أو" *

"لقد تلقينا رسالتكم المؤرخة 9 يونيو 2020، بشأن الاستهداف المزعوم لمدافع حقوقي من قبل السلطات في المغرب باستخدام التكنولوجيا التي طوّرناها. نظراً لقيود السرية المفصلة أدناه، لا يمكننا تأكيد أو نفي استخدام هذه السلطات للتكنولوجيا الخاصة بنا. ونقدر لفت انتباهنا إلى هذه القضية. تماشيا مع سياسة حقوق الإنسان لدينا، تأخذ مجموعة "إن إس أو" على عاتقها مسؤولية احترام حقوق الإنسان بجدية، وهي ملتزمة تماماً بتجنب التسبب في الآثار السلبية لحقوق الإنسان، أو المساهمة فيها، أو الارتباط بها ارتباطاً مباشراً.

ونشعر بقلق بالغ إزاء الادعاءات الواردة في رسالتكم، وسنراجع المعلومات الواردة فيها فوراً، ونبدأ التحقيق فيها إذا اقتضى الأمر. على الرغم من أنكم قدمتم معلومات معينة بشأن سوء الاستخدام المزعوم؛ فمن أجل التحقيق في القضية بدقة، إننا بحاجة إلى تفاصيل معينة، مثل رقم الهاتف أو اسم الفرد أو الـMSISDN (Mobile Station International Subscriber Directory Number) كما هو موضح في سياسة الإبلاغ عن المخالفات العامة. في حالة عدم وجود هذه المعلومات، سيتم تقييد استفساراتنا بشكل كبير. وإذا قدمتم بعض هذه المعلومات أو جميعها، فسيُسهل هذا بشكل كبير قدرتنا على تحديد ما إذا كانت منتجاتنا قد تم استخدامها بطريقة لا تتوافق مع سياساتنا، أو أي اتفاقيات تجارية قد تكون موجودة، أو المعايير الدولية، أو القوانين المحلية المعمول بها. ووفقًا لسياساتنا، سنحافظ على هذه المعلومات بسرية تامة، ولن نكشف عنها عدا ما هو مطلوب لإجراء تحقيق شامل.

وتطرح رسالتكم أيضاً عدة أسئلة تتعلق بأي علاقة قد تكون بين مجموعة "إن أس أو" والسلطات المغربية، والإجراءات التي اتخذناها بعد تقرير منظمة العفو الدولية حول سوء استخدام مزعوم لمنتجات "إن أس أو" من قبل تلك السلطات. في الوقت الذي نسعى فيه إلى أن نكون شفافين قدر الإمكان رداً على الادعاءات التي تفيد بإساءة استخدام منتجاتنا؛ فلأننا نقوم بتطوير وترخيص تكنولوجيا للدول وأجهزة الدولة للمساعدة في مكافحة الإرهاب والجرائم الخطيرة، والتهديدات للأمن القومي، نحن مُلزمون باحترام مخاوف سرية الدولة، ولا يمكننا الكشف عن هويات العملاء. ومع ذلك، فإن المراسلات المرفقة مع المقرر الخاص للأمم المتحدة ديفيد كاي تحتوي على وصف كامل لكيفية تعاملنا مع توخي العناية الواجبة بحقوق الإنسان، والإجراءات التي قد نطلبها في علاقات العملاء الفردية للتخفيف أو منع خطر الآثار على حقوق الإنسان، وخطوات التحقيق لدينا عندما نتلقى ادعاءات بشأن إساءة الاستخدام المحتملة، ومجموعة من

الردود عند تحديد سوء الاستخدام. ويمكننا أن نؤكد لكم أننا اتبعنا هذا النهج فيما يتعلق بتقريركم السابق، إلا أننا، وبسبب قيود السرية المذكورة أعلاه، لا يمكننا تقديم مزيد من التفاصيل.

ويحدونا الأمل في تزودينا بمزيد من التفاصيل، كما هو مذكور أعلاه، للسماح لنا بالتحقيق في الادعاءات المقلقة الموضحة في رسالتكم.
وتقبلوا بقبول فائق الاحترام والتقدير"

تشايم جيلفاند، مدير المطابقة والالتزام في مجموعة "إن إس أو"

* مترجم من الإنجليزية من طرف منظمة العفو الدولية

ملحق تقني

تم محو تاريخ تصفح سفاري الخاص بعمر راضي في مطلع أكتوبر 2019، مما ألغى سجلات عمليات إعادة توجيه متصفّح سفاري السابقة باستخدام free247downloads[.]com. ومع ذلك، تخلفت آثار إضافية على الجهاز تشير لنا توقيت هجمات حقن الشبكة ضده.

أدلة التحليل التقني لهجمات حقن شبكة الاتصالات

في 27 يناير 2019 تم إنشاء مجلّد الملفات مقترن بالنطاق:

private/var/mobile/Containers/Data/Application/4FC7C4F8-602A-4EA0-AF28-3264694AB07B/SystemData/com.apple.SafariViewService/Library/WebKit/WebsiteData/**https_skapth05c.get1tn0w.free247downloads.com_30874**/

ومن المثير للاهتمام أن مجلّد الملفات هذا يعمل كمخزن لتطبيق تويتر للجوال لنظام iOS. يشير اسم مجلد الملفات **"com.apple.SafariViewService"** إلى خدمة تحمل الاسم نفسه يوفرها نظام التشغيل والتي تسمح للتطبيقات الأخرى بالاستفادة من محرك متصفح سفاري لمعاينة مواقع الإنترنت بسهولة من داخل التطبيق. نعتقد أن وجود مجلّد الملفات "WebsiteData" للنطاق الضار *free247downloads[.]com* يشير إلى أن هجومًا بحقن الشبكة وقع أثناء استخدام عمر راضي لتطبيق تويتر، وبعد النقر على رابط يؤدي إلى موقع HTTP غير مشفر، تمت محاولة الاستغلال على هاتفه.

في 11 فبراير 2019، تم إنشاء مجلّد الملفات التالي:

private/var/mobile/Containers/Data/Application/AE2D9AEB-8935-408D-9499-023635ACA6E7/Library/WebKit/WebsiteData/IndexedDB/**https_d9z3sz93x5uei.dq3.get1tn0w.free247downloads.com_30897**/

يحتوي مجلّد الملفات هذا، الموجود داخل تخزين بيانات تطبيق سفاري، على العديد من قواعد بيانات اندكسد دي بي IndexedDB الفارغة التي تم إنشاؤها بعد زيارة النطاق الضار. في حين أن هذا التفصيل لم يدرج في تقريرنا السابق، كشف التحليلَ التقني الذي قمنا به لهاتف المعطي منجب أيضا ملفات اندكسد دي بي IndexedDB مماثلة. في حين أننا لم نتمكن من استعادة أي حمولة استغلال

(exploit payload)، فإننا نشتبه في أن إنشاء هذه الملفات قد يكون من أعراض نقاط الضعف المستخدمة ضد هاتفي عمر راضي والمعطي منجب في عام 2019.

ويبدو أن هجوم حقن شبكة الاتصالات هذا والاستغلال كانا ناجحين، وبعد ثوان قليلة تم تعديل الملف التالي:

```
/private/var/root/Library/Preferences/com.apple.CrashReporter.plist
```

في 13شتنبر 2019، نجح هجوم إضافي بحقن شبكة الاتصالات، وتم تنفيذ عمليات (processes)مشبوهة على الهاتف، وتم تعديل الملف التالي:

```
private/var/mobile/Library/Preferences/com.apple.softwareupdateservicesd.plist/
```

تم تعيين القيمة الواردة **SUAutomaticUpdateV2Enabled** إلى "كلا" *false*، مما يؤدي إلى تعطيل وظيفة التحديث التلقائي للهاتف وإبقائه على صيغة هشة.

تم إيقاف تشغيل خادم الأسماء (nameserver) بعد الاتصال بمجموعة "إن إس أو"

تم تحديد موقع خادم الأسماء المرتبط بالنطاقات الفرعية لحقن شبكة الاتصالات في **ns-get1tn0w.free247downloads[.]com** الذي يحمل عنوان بروتوكولات الإنترنت IP 35.180.42.148. تم تعيين عناوين بروتوكولات الإنترنت IP هذه إلى مركز بيانات Amazon Web Service- الموجود في فرنسا. وفقًا لبيانات Censys، ظل هذا الخاد يعمل من أكتوبر/تشرين الأول 2018 حتى تم إغلاقه في 4 أكتوبر/تشرين الأول أو 5 أكتوبر/تشرين الأول 2019:

```
[{"table":"20190929","ports":["53"],"tags":["dns"],"updated_at":"2019-09-29 13:22:40"}]
[{"table":"20190930","ports":["53"],"tags":["dns"],"updated_at":"2019-09-29 13:22:40"}]
[{"table":"20191001","ports":["53"],"tags":["dns"],"updated_at":"2019-09-29 13:22:40"}]
[{"table":"20191002","ports":["53"],"tags":["dns"],"updated_at":"2019-09-29 13:22:40"}]
[{"table":"20191003","ports":["53"],"tags":["dns"],"updated_at":"2019-10-03 06:47:28"}]
[{"table":"20191004","ports":["53"],"tags":["dns"],"updated_at":"2019-10-03 06:47:28"}]
[{"table":"20191005","ports":["53"],"tags":["dns"],"updated_at":"2019-10-03 06:47:28"}]
[{"table":"20191006"}]
```

حدث الإغلاق بعد وقت قصير من تقديمنا لإخطار مسبق بالنتائج التي توصلنا إليها من تقريرنا السابق "المغرب: استهداف المدافعين عن حقوق الإنسان ببرنامج تجسس تابع لمجموعة "إن إس أو" – NSO" إلى مجموعة "إن إس أو"" في 2 أكتوبر/تشرين الأول 2019. ولم يتم نشر التقرير قبل 10 أكتوبر/تشرين الأول.

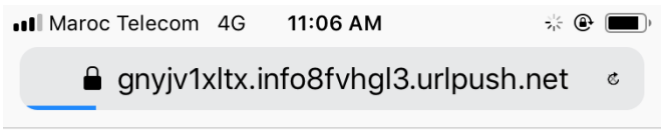
تم إنشاء بنية أساسية جديدة بعد عمليات الكشف التي قمنا بها

بعد أقل من شهر من نشر تقريرنا أنشئت بنية أساسية جديدة على النطاق **urlpush[.]net**، الذي اكتشفنا فيما بعد تورطه في هجمات حديثة لحقن شبكة الاتصالات ضد عمر راضي.

في 27 يناير 2020، أثناء زيارة رابط إلى موقع إخباري نقر عليه من تطبيق فيسبوك، تم قرصنة متصفح عمر وإعادة توجيهه أخيرًا في أقل من 3 مللي ثانية إلى خادم الاستغلال الجديد بنفس بنية عنوان URL التي لاحظناها سابقًا في عام 2019:

https://gnyjv1xltx.info8fvhgl3.**urlpush[.]net**:30875/zrnv5revj#0741964198279879192740015486227389198355567483259462

بسبب الاشتباه في هذا السلوك غير المعتاد، أخذ عمر راضي على الفور لقطة شاشة لمتصفح سفاري الخاص به محاولًا فتح الموقع الضار أثناء الاتصال بشبكة الجيل الرابع 4G:



وجرت محاولة ثانية لحقن شبكة الاتصالات واستغلالها في 29 يناير 2020. ويبدو أن هذا فشل، وأعاد توجيه المتصفح بدلاً من ذلك إلى موقع ويب لشركة مشروعة مقرها في فرنسا. لاحظنا أن هذا الموقع نفسه استخدم كشرك في الهجمات الفاشلة ضد المعطي منجب في عام 2019.

تم التعرف على ارتباط خادم الاسم للنطاقات الفرعية urlpush.net بعنوان بروتوكولات الإنترنت IP address 72.105.81.177. تم تعيين عنوان بروتوكولات الإنترنت IP هذا على أنه يتبع مزود الاستضافة لاينود - Linode المتواجد في ألمانيا.

انتهى./.

20، زنقة ورغة، رقم 5، الطابق 2، أكدال – الرباط 10080 20, Rue Ouargha, N. 5, 2ème étage, Agdal – Rabat
+212 (0) 537 681 048 +212 (0) 537 686 648
admin-ma@amnesty.org www.amnesty.ma