فريق التحرير | نشر في ٢٢ يوليو ٢٠٢١,

"بيغاسوس": التكنولوجيا الإسرائيليّة سلعة للتجسس والجريمة لمن يدفع أكثر

في الأعوام العشرة الماضية، طفت على السطح عددٌ من وقائع "التسريب" المهمة، والتي كشفت، في كلّ مرة، بعضا من الجانب الآخر، غير المرئيّ، أو كما يقال "الكواليس" لكيفية إدارة الأمور، في السلطة والمال والأمن والعلاقات الخارجية، إقليميا وعالميا.

إلى جانب أمور مثل الطموح الشخصيّ الفرديّ أو النزعة الأخلاقية التي تدفع إلى إظهار الحقيقة أو حبّ المغامرة والسباحة ضد التيار؛ فقد لعبت ما تعرف بـ"الموادّ مفتوحة المصدر" والصحافة "الاستقصائية" دورا بارزا في عدد ليس هينا من مراحل الحصول على، أو نشر، هذه التسريبات، والتي يقول عنها رجال استخبارات إنها، أيّ الموادّ مفتوحة المصدر، تصل إلى أكثر من 90% من جملة النشاط التحليليّ لهذه الأجهزة المعلوماتيّة التي لا تترك شاردة أو واردة، إلا وقامت بحفظها وتفكيكها ثمّ محاولة ربطها بموادّ أخرى مشابهة، بغرض تكوين صورة مقاربة للواقع عن موضوع ما.

أهمّ القضايا التي ظهرت مؤخرا وتنتمي إلى هذا النوع من المعلومات الحساسة، كانت ما عرفت وقت ظهورها بتسريبات "ويكليكس"، والتي كان بطلها شخص يدعى "جوليان أسانغ"، إلى أن انفرط العقد بتسريبات إدوارد سنودن، ووثائق بنما، وصولا إلى رسائل بريد هيلاري كلينتون، والتي يربط بينها جميعا: الموثوقية العالية، والتفاصيل الدقيقة لمعلومات حساسة في ميادين غير تقليدية، مثل الدبلوماسية والأمن والمخابرات وصفقات السلاح والملاذات الضريبية.

غير أنه من الواضح، أنه قد انضمّ في الساعات الأخيرة إلى قضايا التسريبات تلك قضيةٌ جديدة، خطيرة، تنتمي إلى مجال "الأمن السايبرانيّ"، ذلك الحقل الرقميّ الجديد الذي بات يشغل اهتماما كبيرا على أجندة الدول والحكومات، حيث يبرز اسم دولة الاحتلال "إسرائيل" ودور برمجيّتها الخبيثة "بيغاسوس" في التجسس على نطاق واسع من الدول والشخصيات المرموقة عالميا، من خلال تقديم الدعم التقنيّ للجهات التي تدفع أكثر من أجل الحصول على تلك البرمجية، بغض النظر عن دوافع وسياقات

هذا الاستخدام.

بداية القصة

أبطال القضية الجديدة ليسوا من "الهاكر" أو من ذوي الطموح الشخصيّ النافذ، وإنما من خبراء الأمن الرقميّ والبحث الاستقصائيّ في منظمتين دوليّتين مرموقتين، هما منظمة العفو الدولية (قسم الأمن الرقميّ) ومؤسسة "Story Forbidden" الاستقصائية غير الهادفة للربح والتي يقع مقرها في باريس.

عكفت المنظمتان على تعقّب نشاط برمجية "بيغاسوس" الخبيثة، التي تنتجها شركة "إسرائيلية" أمنية يقوم عليها صفوة رجال الاستخبارات المتقاعدين أو المُحالين اختياريا للتقاعد من أجل التفرغ لأعمال خاصّة، وذلك بدايةً من ظهور تلك البرمجية عام 2016 وحتى يوليو/ تموز 2021.

ما دفع هاتين المنظمتين إلى التركيز على هذه الأداة وهذه الشركة تحديدا، أنه قد سبق إيجادُ دلائل على استخدامها في عدة دول من جهات مختلفة ضدّ نشطاء وعاملين في مجال حقوق الإنسان والمجتمع المدنيّ، ومن ذلك دلائل سابقة على استخدامها لتعقب الصحفيّ السعوديّ الذي جرى قتله لاحقا، جمال خاشقجي.

سلم القائمون على التحقيق نتائجه، بما في ذلك أرقام الهواتف المحتمل اختراقها، إلى 17 مؤسسة صحافية وإعلامية دولية، منها أرقام هواتف تخصّ عاملين في هذه المؤسسات بالفعل، مثل الغارديان وسي إن إن ورويترز وبلومبرغ وواشنطن بوست ونيويورك تايمز وفرانس برس والجزيرة

استطاع التحقيق أن يتوصل إلى نحو 50 ألف رقم هاتف، تعود معظمها إلى شخصياتٍ تسبب قلقا سياسيا واجتماعيا لحكوماتٍ قمعية في عدة دول، فضلا عن العثور على أرقام هواتف تخصّ شخصيات رفيعة كرؤوساء دول وحكومات، وعائلات مالكة، ودبلوماسيين، ورجال أمن واقتصاد.

ما يقوله التحقيق نصا إنه استطاع التأكد من استخدام هذه البرمجية الخبيثة التي تنتجها الشركة الإسرائيلية من أجل اختراق هواتف بعض الشخصيات التي جرى التعرف عليها، بطريقة أو بأخرى، في مرحلة لاحقة بعد الوصول إلى أرقام الهواتف، فيما يمكن الجزم أنّ بقية الأرقام الموجودة في القائمة موضوعةٌ على دائرة اهتمام عملاء هذه البرمجية؛ دون التأكد من نجاحها في اختراق خوادم هذه الشخصيات، وهو الأمر الذي قد يتطلب فحص هواتفهم للقطع بذلك.

سلم القائمون على التحقيق نتائجه، بما في ذلك أرقام الهواتف المحتمل اختراقها، إلى 17 مؤسسة صحافية وإعلامية دولية، منها أرقام هواتف تخصّ عاملين في هذه المؤسسات بالفعل، مثل الغارديان وسي إن إن ورويترز وبلومبرغ وواشنطن بوست ونيويورك تايمز وفرانس برس والجزيرة، وذلك لنشرها صحافيا يوم الأحد الماضي.

وفقا للنتائج الأولية للتحقيق، فإنّ العملاء الذين اشتروا هذه البرمجية من الشركة الإسرائيلية من أجل التجسس على شخصيات رفيعة أو نشطاء ومعارضين يقعون في نطاق واسع جغرافيا على مستوى العالم، على رأسه في الخليج العربيّ السعودية والإمارات والبحرين، وفي أوروبا أذربيجان والمجر، والهند وكازاخستان في قارة آسيا، إضافة إلى المكسيك في أمريكا الشمالية، والمغرب ورواندا في أفريقيا.

كيف تعمل البرمجية؟

رصد التحقيق أنّ البرمجية الخبيثة (بيغاسوس) قد طُورت من قبل القائمين عليها خلال الأعوام الخمسة الماضية، بحيث لا تقتصر طريقة عبورها إلى الهاتف الشخصيّ المستهدف على الطريقة التقليدية المعروفة باسم "التصيد الاحتياليّ"، والتي تقوم على إرسال رابط اختراق إلى الضحية عبر رسالة نصية أو رسالة بريد إلكتروني.

وإنما طور القائمون على هذه البرمجية أساليب الاختراق كي تشمل أيضا إلى جانب تلك الطريقة التقليدية التي قد تُجدي مع ضحايا معينين، طريقةً تعتمد على استغلال "الثغرات" الموجودة في أنظمة تشغيل هواتف أندرويد وآبل، والتي يُفترض أنّ الشركات المصنعة لهذه الأنظمة تسعى إلى تلافيها بصورة مستمرة من خلال التحديثات الدورية، وقد عُرفت هذه الطريقة باسم "الهجوم دون انتظار" (Zero Click – Zero Day).

بالإضافة إلى ذلك، طورت الشركة "الإسرائيلية" طرقا مكملة لضمان زيادة فرص احتمالية اختراق الهاتف المستهدف بنجاح، وذلك من خلال إمكان حقن البرمجية الخبيثة إلى هاتف الضحية من خلال "جهاز لاسلكي" يوضع بالقرب من هاتف الهدف، أو حتى يدويا حال نجح أحد الأشخاص في التعامل مع ذلك الهاتف المطلوب مباشرة.

بمجرد أن يتمّ الاختراق بنجاح، فإنّ البرمجية تنجح في التحكم في هاتف الضحية بشكل شبه كامل

ومع التركيز على تنويع طرق اختراق هواتف الضحايا، فإنّ القائمين على البرمجية دخلوا أيضا إلى حيز استخدام تطبيقات المراسلة المشهورة، مثل واتساب، كأدوات، يمكن من خلال اختراقها العبور إلى هواتف الضحايا، دون النقر على أيّ رابط، فقط تأتيك مكالمةٌ هاتفية من رقم غير معلوم في "واتساب"، وبمجرد نجاح البرمجية في عمل تلك المكالمة، يكون هاتفك قد تعرض للاختراق، حتى لو لم ترد على الاتصال، أو كما تقول الغارديان:"يفضلون الآن الهجمات التي لا تتطلب إرسال روابط بما يجعل الأمور أكثر تعقيدا".

وبمجرد أن يتمّ الاختراق بنجاح، فإنّ البرمجية تنجح في التحكم في هاتف الضحية بشكل شبه كامل، على سبيل المثال، يستطيع "بيغاسوس" النفاذ إلى الرسائل الخاصة، وتسجيل المكالمات الشخصية عبر الميكروفون، وفتح الكاميرا، وتعقب سجلّ تنقلات صاحب الهاتف، ومعرفة الأشخاص الذين التقى بهم.

الأدهى أنّ هذه البرمجية، باستثناء مؤشرات بسيطة يمكن لطبقة محدودة من المحترفين تتبعها، فإنها تستخدم حيلاً كثيرة كي لا يتمكن خبراء الأمن الرقمي من تعقبها، مثل استهداف الذاكرة المؤقتة بدلا من القرص الصلب، حتى يزول أي أثر للاختراق بمجرد غلق الهاتف، وهو ما يجعله "أقوى برنامج تجسس أنتجته شركةٌ خاصة"، كما وصفته الغارديان.

ما علاقة خاشقجي؟

لم يكن البحث وراء علاقة البرمجية الخبيثة بعملية اغتيال الصحفي السعودي جمال خاشقجي داخل قنصلية بلاده في إسطنبول أكتوبر/ تشرين 2018 دافعا أساسيا وراء إجراء ذلك التحقيق من قبل صناعه، ولكنّ تحليلا تاليا لبيانات أرقام بعض الهواتف الموجودة في القائمة كشف، أو أكد بالأحرى، وجود علاقة بين تلك البرمجية وعملية الاغتيال.

وفقا للبحث الاستقصائيّ فقد سلط عملاء لهذا المنتج هذه البرمجية على مجموعة من الأشخاص ذوي القرابة الشديدة بالضحية، في نطاق جغرافيّ من الولايات المتحدة الأمريكية إلى تركيا، قبل عملية التخلص منه، فيما يبدو أنها مساع مستمرة لعدة أعوام للتجسس عليه وتتبعه، هو ودائرته المقربة، قبل وبعد اغتياله.

وضاح خنفر، مدير عام شبكة الجزيرة سابقا وأحد أصدقاء الصحفي المغدور وواحد ممن وجدت أرقام هواتفهم في قائمة المخترَقين، علق على تلك التقارير قائلا إنه شعر أن هاتفه، أو هاتف السيدة چنكيز، خطيبة جمال، قد تعرض للاختراق، بعد اغتيال جمال خاشقجي

من بين المقربين من خاشقجي الذين وجدت أرقام هواتفهم في قائمة الـ50 ألف، زوجته، مضيفة

الطيران المصرية حنان العتر، والتي جرت محاولة اختراق هاتفها الذي يعمل بنظام "أندرويد" مرتين قبل اغتيال الصحفي السعودي، إحداهما في نوفمبر/ تشرين 2017، أي قبل نحو عام من الجريمة، والأخرى في أبريل/ نيسان 2018، وذلك عبر التقنية الأولى المعروفة بـ"التصيد الاحتيالي، بالإضافة إلى خطيبته، التي اخترق هاتفها "iOS" لأول مرة، وفقا للبحث، بعد 4 أيام من اغتياله، وما لا يقلّ عن 5 مرات في أيام لاحقة؛ دون معرفة البيانات المسروقة من تلك الهواتف.

ولكنّ وضاح خنفر، مدير عام شبكة الجزيرة سابقا وأحد أصدقاء الصحفي المغدور وواحد ممن وجدت أرقام هواتفهم في قائمة المخترَقين، علق على تلك التقارير قائلا إنه شعر أن هاتفه، أو هاتف السيدة چنكيز، خطيبة جمال، قد تعرض للاختراق، بعد اغتيال جمال خاشقچي، وذلك استنادا إلى معاينة تسريب رسائل خاصة دارت بينهما حول اختفائه بعد دخول القنصلية السعودية.

ليس معلوما ما إذا كان هاتف خاشقچي نفسه قد تعرض للاختراق أم لا؛ ولكنّ المؤكد أنه قد تركه لخطيبته قبل الولوج داخل القنصلية السعودية، والتي سلمته بدورها إلى السلطات التركية، التي قامت بالتحفظ عليه في إطار التحقيقات.

تأكيدا لما ورد في التحقيق عن تعرض عدد من الشخصيات التركية الرفيعة إلى محاولة الاختراق باستخدام هذه البرمجية عقب اغتيال خاشقچي، مثل الصحفي توران كشلاكچي والمدعي العام التركيّ عرفان فيدان؛ فإنّ ياسين أقطاي، مستشار الرئيس التركي رجب أردوغان، وأحد المدرجة أرقام هواتفهم في قوائم محاولات الاختراق، قال إنّ السلطات التركية قد أبلغته بالفعل بمحاولة أحدهم، لم تحدده، اختراق هاتفه الجديد من طراز "أبل"، ناصحةً إياه، على ضوء ذلك، باستبدال هذا الهاتف بآخر جديد، ضمن سلسلة توصيات تهدف لحماية أمانه الشخصي.

اللافت هنا فيما يخصّ تفاصيل اغتيال خاشقچي، أنه بالرغم من توقف السلطات التركية عن الإدلاء بأيّ مستجدات في التحقيق لأسباب كثيرة، سياسية تخص العلاقات السعودية التركية، وتقنية تخصّ مباشرة القضاء السعوديّ محاكمة وإدانة بعض المتورطين في الحادث، وعُرفية ترتبط بتخلي أولياء الدمّ، أبناء الضحية، عن متابعة القضية؛ فإنّ أطرافا أخرى، بخلاف السلطات التركية والجهات المعنية في الأمم المتحدة، لازالت تكشف مستجدات في القضية، بالاستعانة بالأدوات مفتوحة المصدر والصحافة الاستقصائية.

فقبل ما كشفه تحقيق "فوربايدن ستوري" ومنظمة العفو الدولية بمدة وجيزة، أزاح النقاب تحقيقٌ لموقع "ياهو نيوز" الأمريكي عن تفاصيل ترجح احتمالية ضلوع النظام المصري في عملية الاغتيال البشعة، من زاوية تدريب فريق الاغتيال السعودي (فرقة النمر) على يد عناصر أمنية مصرية، ومرور الطائرة السعودية على الأجواء المصرية قبل أن تحطّ في تركيا، من أجل الحصول على موادّ كيميائية ذات وظيفة مخدرة، ما دفع منظمات حقوقية إلى مطالبة الكونغرس الأمريكيّ بفتح هذا الموضوع مع المسؤولين المصريين، خلال زيارة مدير المخابرات العامة المصرية، عباس كامل، إلى واشنطن مؤخرا.

الدور المغربي

كما ذكرنا نقلا عن التحقيق، فإن عددا من الدول العربية ضالعةٌ في استخدام هذه البرمجية ضد عناصر مختلفة، كالسعوديّة والإمارات والبحرين والمغرب، كما أنّ عددا من الدول العربية وقع مسؤولوها تحت سطوة هذه الأداة المتطورة، مثل العراق، التي وجد رقم هاتف رئيسها برهم صالح ضمن قوائم المرصودين، ورئيس الوزراء المصري مصطفى مدبولي.

إلا أنّ ما أثار انتباهنا خلال قراءة التحقيق وربطه بتحقيقات أخرى سابقة، هو الدور المغربيّ المتشعّب في استخدام هذه الأداة "الإسرائيلية" على نطاق واسع ضدّ أهداف مختلفة، في الداخل والخارج، بعضها

قد تثير أزمات دبلوماسية للبلاد.

فوفقاً للبحث، فإنّ الرئيس الفرنسيّ إيمانويل ماكرون كان ضحيةً لمحاولة الاختراق، لا يُعلم نجاحها من عدمه، ولكن مَن مَن؟ من جهاز أمني حكومي تابع للدولة المغربية كما تقول نصا وسائل الإعلام الفرنسية، وهو ما دفع الرئاسة الفرنسية إلى اعتبار أنّ "هذا الأمر، سيكون له تداعيات خطيرة، حال ثبتت صحته".

يقول لوران ريشار مدير منظمة "Story Forbidden" شرحا لهذا الأمر:"وجدنا رقم هاتف ماكرون ضمن الأرقام التي تسعى البرمجية عبر زبائنها (في المغرب) إلى اختراقها، لكننا، بالطبع، لم نتمكن من إجراء تحقيق تقنيّ مباشر على هاتف الرئيس الفرنسي، ما يعني أنّ هذا لا يؤكد لنا ما إذا كان قد تعرض للتجسس أم لا، ولكن سواء قد تعرض لذلك من عدمه؛ فإن المؤكد أن هناك اهتماما بذلك".

وكان الخبير الرقمي المصريّ ضمن فريق عمل منظمة العفو الدولية، رامي رؤوف، قد علق على هذه التقارير التي تتحدث عن الدور المغربي في استخدام هذه البرمجية كاشفاً أنه عمل ضمن فريق تقني تابع للمنظمة، نجح، عام 2019، في الكشف عن خيوط استخدام النظام المغربي لهذه البرمجية من أجل استهداف مدافعين عن حقوق الإنسان.

وفقا لما كشفه رامي وفريقه في التحقيق، فإنّ "المعطي المنجب" الناشط المغربي في مجال حقوق الإنسان قد تعرض، وغيره، إلى محاولات اختراق، بالطريقة التقليدية التي تقوم على إرسال روابط ملوثة من خلال عناوين عن "تحديثات تضيف إمكانات جديدة في تطبيق تروكولر"، و"فضيحة أخلاقية داخل مقهى"، و"عريضة التوقيع على اعتبار القدس عاصمة فلسطين"، و"تحميل كتاب ترامب باللغة العربية".

كما اعتمد الزبون المغربي في حقن شبكات المحمول الخاصة بالنشطاء المستهدفين بالبرمجيّة الخبيثة، وفقا للتحقيق، على "اختطاف عنصر مارق لطلب البحث في محرك ياهو وإرساله إلى خادم الهجوم، كي يقوم ذلك الخادم بالرد بدلا من ياهو، وإعادة توجيه هاتف الضحية إلى رابط الهجوم".

التداعيات والنتائج

بعد نشر هذا التحقيق وانتشاره كالنار في الهشيم، ومطالبات حقوقية واسعة للشركة المنتجة للبرمجيّة بوقف التعاون مع الحكومات والأنظمة غير المضمون طرق استخدامها، قالت شركة "NSO" إن أدواتها الرقمية لا تباع إلا إلى جهات موثوقة، مثل أجهزة المخابرات الحكومية ووكالات إنفاذ القانون، لمنع الجرائم ومكافحة الإرهاب.

وكما نفت الشركة من قبل أيّ علاقة لها بحادث اغتيال خاشقجي، عاودت التأكيد على هذه المبدأ قائلة:"إن تقنياتنا لم تكن مرتبطة بأي شكل من الأشكال بالقتل الشنيع لخاشقجي"، وقد أفادت وسائل إعلام دولية بأنّ الشركة العبرية سوف توكل مكتب محاماة بريطاني مشهور، على صلة بعائلة توني بلير، من أجل الدفاع عنها إزاء هذه الحملة التي وصفتها الشركة، كما وصفها قادة عسكريون سابقون في جيش الاحتلال، مثل يائير غولان بأنها "ادعاءات زائفة لأغراض تجارية، هناك الكثير من الشركات الأخرى تبيع برمجيات مشابهة".

مع إقرار كلاوديو غوارنيري مدير المختبر التقنيّ لمنظمة لعفو الدولية بصعوبة كبح مثل الهجمات، فإنّ التوصيات التقليدية، وفقا لخبراء رقميين، قد تقلل من فرص حدوث هذه الاختراقات، مثل الابتعاد عن الروابط المشبوهة

من المفترض أن يحدث ما يشبه "الاستجواب" في لقاء بين وزير الصحة العبري ورئيس حزب "ميرتس" الذي يعد جزءا من الائتلاف الحاكم حاليا من جهة، وبين وزير الدفاع بيني غانتس من جهة أخرى، اليوم الخميس، بخصوص هذه الاتهامات، نظرا لكون الشركة مرخصةً من وزارة الدفاع، وذلك بعد مناداة

أصوات حزبية داخلية بما أسموه:"وقف بيع أسلحة محرمة إلى دول غير ديمقراطية".

فيما يخصّ الاستنتاجات، فإنّ أنييس كالامار، المسؤولة السابقة عن متابعة ملف التحقيق في اغتيال خاشقجي بالأمم المتحدة سابقا والأمين العام الحالي لمنظمة العفو الدولية، قد رجحت، أن تساهم السلطات التركية، في الكشف عن مزيد من المعلومات التي خلصت إليها تحقيقاتها من زاوية موضوع التحقيق؛ وذلك بعد كشف الجهات المعدة للتحقيق نيتها الإفصاح عن مزيد من هويات أصحاب أرقام الهواتف خلال الأيام المقبلة.

لم يكن خاشقجي وحده الذي تسببت هذه البرمجيات في المساعدة على التخلص منه، فوفقاً للتحقيق، فقد عُثِرَ من بين أرقام الهواتف، على رقم ناشط معارض للسلطات المكسيكية، توفيَ في جريمة قتل داخل مقر لغسيل السيارات، دون العثور على هاتفه الشخصي، الذي يُفترضُ أنه تعرض للاختراق.

وفقا لكتاب وصحافيين، فإنّ هذه القضية تسلط الضوء على عدة موضوعات متشابكة، من بينها: دور مجتمع استخبارات دولة الاحتلال بعد التقاعد، وماهية التقنية التي يروج الاحتلال إلى إمكان مشاركتها مع الدول الأخرى، وتطور أدوات تتبع الأنظمة العربية لخصومها السياسيين، وذلك بالأخصّ بعدما طلب مدير المخابرات المصري عباس كامل في زيارته الأخيرة إلى واشنطن الحصول على برمجيات متطورة تحت لافتة:"المساعدة في الحرب على الإرهاب".

ومع إقرار كلاوديو غوارنيري مدير المختبر التقنيّ لمنظمة لعفو الدولية بصعوبة كبح مثل الهجمات، فإنّ التوصيات التقليدية، وفقا لخبراء رقميين، قد تقلل من فرص حدوث هذه الاختراقات، مثل الابتعاد عن الروابط المشبوهة، والتحديث المستمر لنظم التشغيل وتطبيقات الهاتف، واستبدال الهاتف بآخر مختلف، حال التشكك في إمكان تسريب معلومات مهمة منه عبر اختراق خارجيّ.

رابط المقال: https://www.noonpost.com/41286/