"عصافير الأمن" إدارة يمولها السيسي.. نظام العسكر يتجسّس على المصريين

الجمعة 4 أكتوبر 2019 03:47 م

كتب: على حسن

نظامُ العسكر لم يكتفِ بالاعتقالات والقتل والتصفية والتشريد والتهجير، بل شرعن وقنَّن التجسس على المصريين، سواء عبر التليفون المحمول أو أجهزة الكمبيوتر أو الحسابات الخاصة على مواقع التواصل الاجتماعي.

وفى هذا السياق يسعى نظام الانقلاب الدموي إلى تحويل المصريين إلى "عصافير" مخبرين، حيث يُطالبهم بالإبلاغ عن أي شخص يُحرِّض على دولة العسكر أو يرفض الانقلاب، وخصّص مجلس وزراء الانقلاب رقمَ هاتفٍ على تطبيق "واتساب" يحمل اسم "واتساب مصر"، للإبلاغ عن "أية رسائل تحريضية أو أحداث شغب أو أعمال تخريبية" على حد زعمه.

انتهاكات العسكر تضمَّنت أيضًا تأسيس إدارة البحوث التقنية داخل جهاز المخابرات العامة، وشن هجمات إلكترونية تستهدف صحفيين وأكاديميين ومحامين وسياسيين ومعارضين وناشطين في مجال حقوق الإنسان.

كما كلَّف نظام الانقلاب إدارات الأمن في دواوين الوزارات والمديريات في مختلف المحافظات، وإدارات التفتيش في الهيئات القضائية، بمراقبة الصفحات الشخصية للموظفين والقضاة لاستخدامها في اصطياد العشرات منهم، وتحريك دعاوى تأديبية ضدهم أو إحالتهم للتحقيق.

ومن أبرز النماذج على هذه الحالة، صدور حكمٍ من المحكمة الإدارية، في يونيو 2018، بفصل علي أبو هميلة، مدير عام اتحاد الإذاعة والتلفزيون، من الخدمة نتيجة شكوى تقدّم بها أحد زملائه إلى إدارة أمن ماسبيرو ضده؛ لكتابته على صفحته الشخصية على موقع التواصل الاجتماعي "فيسبوك"، أن "تيران وصنافير مصرية ومن يقول غير ذلك خائن".

هجمات إلكترونية

شركة أمن إلكتروني إسرائيلية "تشيك بوينت" Check Point، كشفت عن سلسلة هجمات إلكترونية متطورة، شنّتها مخابرات العسكر ضد صحفيين وأكاديميين ومحامين وسياسيين وناشطين في مجال حقوق الإنسان.

ونقلت صحيفة "نيويورك تايمز"، عن الشركة، أنّ المهاجمين ثبّتوا البرامج على هواتف الضحايا، ما يسمح بقراءة ملفاتهم ورسائل البريد الإلكتروني، وتعقب مواقعهم، والتعرّف إلى من اتصلوا بهم، مشيرة إلى أنه أُلقي القبض على اثنين من الناشطين الذين استُهدفوا بالهجوم السيبراني، وفق الصحيفة، كجزء من حملة قمع الاحتجاجات المناهضة لنظام عبد الفتاح السيسي.

وأكدت "تشيك بوينت" أنّ الخادم المركزي المستخدم في الهجمات سُجِّل باسم وزارة الاتصالات المصرية، وأنّ الإحداثيات الجغرافية المضمّنة في أحد التطبيقات المستخدمة لتتبُّع الناشطين تتوافق مع مقرّ ما وصفته الصحيفة بـ"وكالة التجسس" الرئيسية في مصر، أي جهاز المخابرات العامة.

وأشارت إلى أنَّ الهجوم الإلكتروني بدأ عام 2016، وعدد الضحايا غير معروف، لكن نقطة التفتيش حددت 33 شخصًا، معظمهم من الشخصيات المعروفة في المجتمع المدني والمعارضة، الذين كانوا مستهدفين في جزء واحد من العملية.

وقالت الشركة: "اكتشفنا قائمة بالضحايا، من بينهم ناشطون سياسيون واجتماعيون اختيروا بعناية، وصحفيون بارزون، وأعضاء منظمات غير ربحية في مصر".

وأشارت إلى هجوم آخر، في أغسطس الماضي، كشف عن حملة مصرية "سرية" لدعم الجيش السوداني، باستخدام حسابات "مزيفة" على وسائل التواصل الاجتماعي.

تطبيقات خبيثة

وأوضحت الشركة أن الهجوم الذي استهدف الهواتف وحسابات البريد الإلكتروني للناشطين، استخدم مجموعة متغيرة من تطبيقات البرمجيات "الخبيثة" لخداع المستخدمين، لافتة إلى أن تطبيق Secure Mail أبلغ المستهدفين بأنّ حساباتهم قد اختُرِقَت، ثم استدرجهم إلى الكشف عن كلمات المرور الخاصة بهم. ووعد تطبيق آخر يدعى iLoud200% بمضاعفة حجم الهواتف المحمولة، لكنه بدلاً من ذلك أعطى المهاجمين حق الوصول إلى موقع الهاتف، حتى إذا أوقف المستخدم خدمات الموقع.

وقالت، إن أحد التطبيقات الأكثر تطورًا، IndexY، ادّعى أنّه تطبيق مجاني لتحديد المتصلين الوافدين، على غرار التطبيق الشهير Truecaller. لكن التطبيق نسخ أيضًا تفاصيل جميع المكالمات التي جرت على الهاتف إلى خادم يسيطر عليه المهاجمون، مع التركيز على اتصالات المستخدمين مع أطراف خارج مصر.

وأوضحت الشركة أنّه رغم المهارة والحيلة، إلا أنّ الجناة ارتكبوا عددا من الأخطاء التي سمحت لـ"تشيك بوينت" بتتبع منبع التطبيقات، مؤكدة أنّ جميع الصفحات والمواقع المستخدمة لتنفيذ الهجمات رُبطَت بعنوان IP خاص بشركة اتصالات روسية تدعى Marosnet، وخادم مركزي مسجل بـMCIT، في إشارة واضحة إلى وزارة الاتصالات في مصر.

ولفتت إلى انّ تطبيق iLoud200%، مثل معظم برامج تحديد الموقع الجغرافي، يحتوي على إحداثيات افتراضية، وتطابقت الاخيرة في التطبيق مع تلك الموجودة في مقرّ جهاز المخابرات العامة المصرية.

الخصوصية الدولية

وكشفت منظمة الخصوصية الدولية Privacy International، معلومات مثيرة عن عمل أجهزة الاستخبارات المصرية في التنصّت على المواطنين، من خلال تأسيس إدارة البحوث التقنية داخل جهاز المخابرات العامة، وأعدّت المنظمة، تقريرًا يتضمن تفاصيل طريقة عمل الإدارة.

وقالت، إن إدارة البحوث هي وحدة سريّة داخل "المخابرات العامة المصرية"، ولديها طموح كبير لشراء معدات التنصت وظلّ دورها قابعًا في الظلام.

وتؤكد أن إدارة البحوث التقنية تعد لاعبًا سريًّا أساسيًّا في عالم الاستخبارات المصري، لافتة إلى أن شركات غربية، منها مجموعة نوكيا/ سيمنز (NOKIA Group/Siemens) وهاكينج تيم (HACKING Team)، باعتا للإدارة تقنيات تنصّت متطورة.

وترصد المنظمة عددًا كبيرًا من وقائع القمع والقتل والتعذيب منذ حكم المجلس العسكري حتى الآن، لتؤكد أن "تأسيس ووجود وحدة استخبارات سرية كإدارة البحوث التقنية، يأتي متّسقًا مع نمط أوسع من القمع السياسي من طرف جهات أمنية لا تخضع للمحاسبة.

وبحسب المنظمة، تملك إدارة البحوث التقنية إمكانات تنصت واسعة النطاق. ويشمل ذلك وجود مركز لمراقبة الاتصالات، ونظام لإدارة اعتراض الاتصالات، وبرمجيات تجسس شديدة الاقتحام. ويظل غير واضح ما إذا كانت موازنة إدارة البحوث التقنية منفصلة عن موازنة المخابرات العامة، وإذا ما كانت التقنيات التي تشتريها إدارة البحوث التقنية تستخدمها أيضا المخابرات العامة.

وأشارت إلى أنَّ إدارة البحوث التقنية، مثل المخابرات العامة، تتمتع بموازنة مستقلة عن وزارتَي الدفاع والداخلية، مؤكدة أن إدارة البحوث لا يحاسبها إلا السيسي، وهو أيضًا مَن يخصص لها موازنة مباشرة غير معلنة.

أنظمة تجسس

وأكدت أن غرض الإدارة الجزئي هو أن تتجسس على موظفي الحكومة وعلى الخصوم المحتملين. ولا يظهر أي نص قانوني أو حتى قرار ينظم وجود وعمل إدارة البحوث التقنية.

وتوضح وثائق غير منشورة حصلت عليها المنظمة، عن أعمال شبكات "نوكيا/ سيمنز" في مصر، أنه في العام 2011 باعت شبكات "نوكيا/ سيمنز" شبكة "إكس 25" إلى إدارة البحوث التقنية، وهي تقنية قديمة تسمح بالوصول إلى الإنترنت عن طريق الاتصال الهاتفي. كما تسمح بالوصول إلى إحدى شبكات الإنترنت، حتى وإنْ أُغلقت البنية التحتية الرئيسية للإنترنت في البلاد، كما حدث أثناء ثورة يناير.

كما باعت شبكات "نوكيا سيمنز" إلى إدارة البحوث التقنية، نظام إدارة اعتراض الاتصالات، ومركز مراقبة شبكات الهواتف الثابتة والمحمولة. وتتيح هاتان التقنيتان إمكانات للتنصت الواسع، ما يمكّن حكومة العسكر من اعتراض الاتصالات الهاتفية.

وتضيف المنظمة أنّه باعتبار أن سجل مصر حافل في منظمة حقوق الإنسان، فمن المثير للقلق أن تحوز وحدة سرية كإدارة البحوث التقنية، والتي لا يظهر وجود أي نوع من الرقابة عليها أو المهام المحددة قانونيا لها، على إمكانات تنصت تمكّنها من مراقبة الاتصالات الهاتفية والإنترنت.

وتذكر أنّ مصر بالفعل لديها تاريخ في استخدام التنصت كوسيلة لنشر الخوف. فبعد تظاهرات 2011، بثّ برنامج تلفزيوني محتوى 29 محادثة هاتفية بين نشطاء معروفين ليقلل من مكانتهم في أعين الجمهور. ويلفت التقرير إلى أنّه تمّ تمرير محادثات ودردشات ناشطة عبر بريدها الإلكتروني مع شريكها أسفل باب بيتها، وذلك قبل استدعائها من قبل جهاز الأمن الوطني للاستجواب بفترة قصيرة.

وتوضح المنظمة أنّه في العام 2015، تورطت شركة هاكينج تيم في بيع أنظمة تجسس شديدة الاقتحام إلى حكومات قمعية. ومن إحدى هذه الأنظمة، برنامج خبيث يدعى "ريموت كونترول سيستم" (Remote Control System)، يسمح للمهاجم بالتحكّم الكامل في كمبيوتر المستهدَف. ويستطيع المهاجم عندها، مثلاً، أن يصل إلى أي محتوى مخزّن على الحاسوب، وأن يراقب استخدامه.

وظهر في التسريبات التي حصلت عليها المنظمة عقدان لإدارة البحوث التقنية: الأول مع وسيط يُعرف باسم "آي سكس" للاستشارات، وبعدها مع "سولف آي تي". أما العقد الثاني فكان مع مجموعة "جي إن إس آي"، وهي شركة تابعة لمجموعة منصور للأعمال، التي تمتلكها ثاني أغنى العائلات في مصر. وتقدم نفسها باعتبارها شركة توفر خدمات "تأمين المعلومات والتطبيقات والشبكات".

وكانت لإدارة البحوث التقنية طلبات خاصة من هاكينج تيم. فقد كشفت المراسلات مع "جي إن إس. آي"، عن أنّ إدارة البحوث التقنية أرادت استهداف هواتف آيفون، وحواسيب ماك من إنتاج شركة آبل، وكانت تخطط لاستهداف مستخدمي ويندوز. وطلبت أن تصمم شركة "هاكينج تيم" لها البرنامج الخبيث "ريموت كونترول سيستم"، الذي لا يستهدف فقط منتجات آبل. وبهذه الطريقة، تستطيع إدارة البحوث استهداف 25 نظامًا إلكترونيًّا.

قضايا بالجملة

فى سياق متصل، كشفت مصادر قضائية في محكمتي جنايات القاهرة والمنصورة عن أن الشهور الخمسة الماضية شهدت ارتفاعًا ملحوظًا في عدد القضايا المحالة من النيابة العامة بسبب ما ينشره الأفراد على مواقع التواصل الاجتماعي، وفي بعض الأحيان يؤاخذ المستخدمون على تعليقات يكتبها أصدقاؤهم أو معارفهم من خارج البلاد على صفحتهم الشخصية، وتعتبر النيابة مجرد نشرها على الصفحة والسكوت عليها مخالفة لقانون الجريمة الإلكترونية.

وأضافت المصادر أن هناك تعليمات من النائب العام السابق نبيل صادق، وأقر استمرارها النائب العام الجديد حمادة الصاوي، بفحص صفحات التواصل الاجتماعي الخاصة بالمتهمين في قضايا ذات طابع سياسي بشكل عام، وقضايا التظاهر والتحريض عليه بصفة خاصة.

وأكدت أنَّ هذه التعليمات لا تقتصر على الأخذ بنتيجة الفحص كقرينة أو دليل إضافي على ارتكاب الجريمة المنسوبة للمتهم، بل يجري استخدامها بهدف ضبط أي جرائم أخرى يكون المتهم قد ارتكبها بواسطة صفحاته الشخصية على تلك المواقع.