هل هواتفنا المحمولة آمنة حقا؟

ترجمة وتحرير: نون بوست

تعتبر الشبكة الخلوية الأمريكية إحدى ضروريات المجتمع على غرار نظام الطرق السريعة وشبكات الكهرباء. في المقابل، لا تهدد نقاط الضعف في البنية التحتية للهواتف المحمولة، الخصوصية والأمان الشخصيين فحسب، بل تهدد كذلك أمن الدولة.

ووفقا لتقارير الاستخبارات، تنصت الجواسيس على محادثات الهاتف المحمول للرئيس دونالد ترامب من خلال استخدام أبراج خلوية وهمية في واشنطن لاعتراض المكالمات الهاتفية. وعلى الرغم من أن البنية التحتية للاتصالات الخلوية، التي تمثل المحور الأساسي للاتصالات الحديثة، والتجارة، والسلطة، تعتبر غير آمنة على الإطلاق، إلا أننا لا نحرك ساكنا من أجل إصلاحها.

تشمل أدوات التجسس، التي أصبحت في المتناول بشكل متزايد، أجهزة محاكاة المواقع الخلوية (المعروفة باسم العلامة التجارية "ستينغراي")، والتي تخدع الهواتف الخلوية للاتصال بها دون علم أصحابها

في حين يجب أن يتصدر هذا الخلل جدول أعمال الأمن السيبراني، غض صانعي السياسات وقادة الصناعة الطرف فيما يتعلق بهذا الأمر. وفي الوقت الذي لا يولي فيه المسؤولون الحكوميون أي أهمية لما يحصل، تبيع العديد من الشركات منتجات تسمح للمشترين باستغلال نقاط الضعف.

عموما، تشمل أدوات التجسس، التي أصبحت في المتناول بشكل متزايد، أجهزة محاكاة المواقع الخلوية (المعروفة باسم العلامة التجارية "ستينغراي")، والتي تخدع الهواتف الخلوية للاتصال بها دون

علم أصحابها. علاوة على ذلك، يمكن للبرامج المتطورة أن تستغل نقاط الضعف في المحرك الأساسي لنظام الهاتف العالمي (المعروف باسم "نظام التشوير رقم 7" أو "إس إس7") لتتبع مستخدمي الهواتف النقالة، واعتراض المكالمات والرسائل النصية، وتعطيل الاتصالات الهاتفية.

في الواقع، قد تنجر عن هذه الهجمات عواقب مالية حقيقية. فعلى سبيل المثال، استغل بعض المجرمين، خلال سنة 2017، نقاط الضعف في "نظام التشوير رقم 7" للاحتيال المالي عن طريق إعادة توجيه واعتراض الرسائل النصية التي تحتوي على كلمات السر، التي تعطى مرة واحدة لعملاء البنوك في ألمانيا. بعد ذلك، استغل المجرمون كلمات السر هذه لسرقة الأموال من حسابات هؤلاء الضحايا. لكن كيف وصلنا إلى هذا الوضع، وما الذي يجعل البنية التحتية الخلوية لدينا غير آمنة؟

يعتمد نظام الاتصالات المتنقلة الدولية على العديد من أجيال التكنولوجيا التي يزيد عمرها عن 40 سنة. لذلك، قد تكون بعض هذه التقنيات القديمة غير آمنة، لأنها لم تخضع للتدقيق المناسب، ولم تحض بالاهتمام اللازم لتأمينها بشكل صحيح. علاوة على ذلك، أنشأت البروتوكولات التي تشكل أسس نظام الاتصالات الخلوية اليوم، دون الحرص على تأمينها.

لقد ابتُكر "نظام التشوير رقم 7" سنة 1975، حيث لا يزال البروتوكول الذي تعتمده الشبكات الهاتفية في جميع أنحاء العالم للاتصال ببعضها البعض. وتجدر الإشارة إلى أنه تم إنشاء هذا البروتوكول على افتراض أن كل الأشخاص الذين سيتصلون بالشبكة هم مشغلو شبكات آمنة.

من الصعب على أحد تصور حجم العمق الذي ستؤول إليه التكنولوجيا الخلوية المترسخة في مجتمعنا، أو لأي مدى سيصبح استخدامها سهلا ومربحا

عندما أنشأ النظام لأول مرة، كانت تستخدمه 10 شركات فقط. أما في الوقت الراهن، فهناك المئات من الشركات في جميع أنحاء العالم المتصلة "بنظام التشوير رقم 7"، مما يزيد من احتمال تسريب أو بيع المستندات المضمنة في هذا النظام. فعلى سبيل المثال، يستطيع أي شخص الاتصال بشبكة "نظام التشوير رقم 7" واستغلاله لتتبع موقعك أو التنصت على مكالماتك الهاتفية. ومن جهة أخرى، يعاني أحدث بديل لهذا النظام، الذي يسمى "دييامتر"، من العديد من المشاكل ذاتها.

فضلا عن ذلك، اخترع بروتوكول آخر سنة 1991، أطلق عليه اسم "جي إس إم" أو النظام الموحد للاتصالات المتنقلة، الذي يسمح للهاتف المحمول الخاص بك بالاتصال ببرج الاتصالات لإجراء وتلقي المكالمات ونقل البيانات. لكن الجيل القديم من "جي إس إم" المعروف "بالجيل الثاني لشبكات الخلوي (2ج)"، لا يستطيع التأكد ما إذا كان البرج، الذي أنت على اتصال به، أصلي حقا، ما من شأنه أن يسهل على أي محتال خلق برج وهمي إما لتحديد موقعك أو للتنصت على مكالماتك.

لقد بدأت شركات النقل الجوي الكبرى بالفعل في تفكيك أنظمة الجيل الثاني (2 جي) من شبكات الاتصال. ويعد هذا الأمر بداية جيدة، حيث أن الأجيال الموالية للنظام الموحد للاتصالات المتنقلة (الجي إس أم)، على غرار الجيل الثالث (3 جي) والرابع (4 جي) والخامس (5 جي)، تساهم في حل العديد من مشاكل هذه الشركات. وعلى الرغم من ذلك، لا تزال أجهزة هواتفنا تستخدم الجيل الثاني إذ أن معظمها عاجز عن إبطال العمل بهذا النظام، الأمر الذي يجعلها عرضة للاختراقات. علاوة على ذلك، أظهرت الأبحاث أن كلا من الجيل الثالث والرابع وحتى الخامس تشوبهم بعض الثغرات التي من شأنها أن تسمح للأجيال الجديدة من تقنيات محاكاة مواقع الخلوي بمواصلة العمل.

من الصعب على أحد تصور حجم العمق الذي ستؤول إليه التكنولوجيا الخلوية المترسخة في مجتمعنا، أو لأي مدى سيصبح استخدامها سهلا ومربحا. وعلى العموم، تقوم شركات من الصين وروسيا وإسرائيل وغيرها من الشركات، بإنشاء أنظمة محاكاة مواقع الخلوي، فضلا عن كونها تؤمن الوصول إلى بروتوكولات

نظام تشوير الاتصالات الهاتفية "أس أس 7" بأسعار معقولة، حتى بالنسبة لأصغر المنظمات الإجرامية. وتجدر الإشارة إلى أنه أصبح من الأسهل إنشاء نظام محاكاة موقع خلوي في المنزل وبتكلفة منخفضة. وقد أدرك الجواسيس وعصابات المخدرات حول العالم مدى قوة هذه التقنيات التكنولوجية.

من المحتمل أن يعود التقصير في اتخاذ الإجراءات إلى أهمية المهمة، حيث توجد المئات من الشركات والهيئات الدولية المنضمة إلى الشبكة الخلوية

من جهتهم، تقاعس الخبراء وصناع القرار في هذا المجال، إلى حد هذه اللحظة، عن الحد من أنظمة محاكاة مواقع الخلوي فضلا عن هجمات نظام "الأس أس 7". وفي شأن ذي صلة، أرسل عضو مجلس الشيوخ الأمريكي رونالد لي ويدن، بصفته أحد المشرعين القلائل الذين تحدثوا عن هذه القضية، رسالة في آب/ أغسطس الماضي يشجع من خلالها وزارة العدل على أن تكون "صريحة تجاه المحاكم الفيدرالية حول الآثار المدمرة لأنظمة محاكاة مواقع الخلوي". وفي الواقع، لم ينشر أي رد على هذه الرسالة على الإطلاق.

من المحتمل أن يعود التقصير في اتخاذ الإجراءات إلى أهمية المهمة، حيث توجد المئات من الشركات والهيئات الدولية المنضمة إلى الشبكة الخلوية. وقد يكمن السبب الثاني في حقيقة أن وكالة المخابرات المركزية ووكالة تطبيق القانون تستفيدان من استغلال ثغرات هذه الأنظمة. في المقابل، تعتمد آليات تطبيق القانون على بعض الأدوات الأخرى الفعالة وغير المتاحة للمجرمين والجواسيس.

فعلى سبيل المثال، يمكن للشرطة التعامل بصفة مباشرة مع شركات الهاتف من خلال تقديم مذكرات تفتيش وإصدار أوامر متعلقة بالتنصت على المحادثات. وفي الحقيقة، لا تملك أية مؤسسة حكومية السلطة والموارد المالية اللازمة لمعالجة المشاكل. ومن جانبها، لم تعلن شركات كبرى على غرار "إيه تي آند تي" الأمريكية و"فيرايزون وايرلس"، إلى جانب شركتي "غوغل" و"آبل"، عن جهودها في هذا الإطار.

لابد من تغيير هذا الوضع من خلال توقف الشركات عن دعم التقنيات التكنولوجية غير الآمنة كنظام الجيل الثاني "2 جي". بالإضافة إلى ذلك، تحتاج الحكومة إلى تفويض رسمي يخوّل لها شراء الأجهزة، فقط من قبل الشركات التي أبطلت نظام "2 جي". في المقابل، يجب على الشركات التعاون مع خبراء الأمن السيبراني قصد تحديد معايير لحماية نظام "الأس أس 7".

كما يجب على الحكومة اقتناء الخدمات، من الشركات التي بإمكانها إثبات أن شبكاتها تنطبق على هذه المعايير. والجدير بالذكر أن العثور على حل لهذه المشكلة لا يقتصر على التنظيم المحلي فقط نظرا لأن نظام الاتصالات الخلوية يحتاج إلى تضافر جهود دولية. وفي الحقيقة، نحن لن نتسامح مع القيام بأعمال حفر في طرق السيارات السريعة أو حدوث عطل في خطوط الكهرباء. وينطبق الأمر ذاته على تأمين البنية الأساسية لشبكات الهاتف المحمول حيث يعتبر هذا الأمر ذو أهمية قصوى، ويجب على صناع القرار في هذا المجال، في جميع أنحاء العالم، العمل سوية من أجل تحقيق هذا الهدف المشترك.

المصدر: نيويورك تايمز