

«سيغنال» ملاذ أخير لمن يحرص على حماية أسراره

تطبيق مشفر غير قابل للاختراق بات مفضلاً لدى السياسيين ورجال المخابرات



في عالم مليء بالاختراقات للمعطيات والمحادثة الشخصية وحتى لقواعد البيانات الحكومية، فشلت تطبيقات متطورة مثل "واتساب" و"تليغرام" في كسب ثقة المستخدمين بعد كل ما جرى من فضائح دولية حول اختراقات مكنت البعض من التجسس حتى على محادثات سياسيين بارزين، فكان ذلك مؤثراً في محطات هامة من أهمها الانتخابات الرئاسية الأميركية التي فاز فيها الرئيس دونالد ترامب على حساب منافسته هيلاري كلينتون. وبات الجميع مؤخراً يميل إلى استعمال التطبيق الجديد "سيغنال" الذي يقول خبراء إنه غير قابل للاختراق وأنه أصبح التطبيق المفضل لدى السياسيين والأمنيين.

باريس - يميل العالم في القرن الحادي والعشرين إلى تحويل الحروب القادمة من ساحات الصراعات التقليدية والعسكرية إلى العالم الافتراضي، فمن يكسب الحرب السيبرانية يكسب حتماً مفاتيح موازين القوى ولذلك تكاد كل القوى العظمى للتسابق على إنتاج تطبيقات ذكية تكون عصية على الاختراق وأخرها تطبيق "سيغنال" المشفر والذي بات مفضلاً لدى أكبر الهياكل والمؤسسات الدولية.

في عالم مفتوح، تعدد الهيمنة السيبرانية أبرز ورقة بالإمكان لعبها لرسم ملامح الحروب القادمة وكل هذا دفع بشركات الذكاء الاصطناعي إلى البحث عن بدائل واستراتيجيات جديدة تعوض فشل تطبيقات ذكية كتطبيقي "واتساب" و"تليغرام" اللذين ثبت أنهما قابلان للاختراق.

في هذا السياق، بات الأشخاص الحريصون على سرية محادثاتهم المتبادلة عبر الإنترنت يميلون إلى تنزيل تطبيق الاتصال المشفر "سيغنال" الذي يعد حالياً الرائد في مجال الحفاظ على السرية ولو أنه لا يتجنب كل المشكلات الأمنية عبر الشبكة العنكبوتية. وفي الحرب السيبرانية تستخدم وسائل وأساليب قتال يمكن لها أن ترقى إلى مستوى النزاع المسلح أو تجرى في سباقه، ضمن المعنى المقصود في القانون الدولي الإنساني، حيث حصلت الكثير من الصوادر جراء هجمات سيبرانية استهدفت أجهزة كمبيوتر أو شبكات وقواعد بيانات تابعة لحكومات كثيرة أو شخصيات سياسية دولية بارزة.

تطبيق مثير

يتطلب الحفاظ على سرية المحادثات عبر الإنترنت حسن اختيار "أحدث" صيحات الموضة" ضمن التطبيقات المتوافرة، وهذا ينطبق على "سيغنال" الذي يزداد الاهتمام به ما يؤدي إلى نمو عدد مستخدميه.



في الواقع، يحل تطبيق "سيغنال" بديلاً عن خدمة الرسائل القصيرة على الهواتف الذكية، خصوصاً أنه يسمح بتشفير الرسائل "من بدايتها إلى نهايتها" مع ما تتضمنه من مكالمات صوتية ومقاطع فيديو، ما يجعله يكسب ثقة الأشخاص المهتمين بالحفاظ على سرية مكالماتهم وخصوصيتها، ومشاركي البيانات الحساسة أو القائمين على بعض الأسرار المهنية.

وفي فبراير الماضي، أوصت المفوضية الأوروبية فريقيا باستخدام هذا التطبيق للحفاظ على سرية ما تتبادله مع الأشخاص من خارج المنظمة. ويشير صحافي وكالات فرانس

برس إلى أن عدداً كبيراً من السياسيين يستخدمون هذا التطبيق، وبدرجة أقل بين المصادر القضائية والأمنية. وذكر في وقت سابق موقع "أي.تي" للأخبار التقنية أن تعليمات المفوضية الأوروبية ظهرت على لوحات الرسائل الداخلية في أوائل فبراير الماضي حيث تم إبلاغ الموظفين أنه تم اختيار "سيغنال" كتطبيق موثوق به للرسائل الفورية العامة، وذلك وفقاً لتقرير صحيفة "بوليتيكو" الأميركية. وأشارت الصحيفة، إلى أن "سيغنال" لن يُستخدم لجميع الاتصالات، بل سيتم استخدام رسائل البريد الإلكتروني المشفرة لإرسال المعلومات غير السرية ولكن الحساسة، في حين تستدعي المستندات السرية إجراءات أمنية أكثر صرامة، أما سيغنال فيستخدم في الاتصالات الخارجية بين الموظفين والأشخاص خارج المنظمة.

ويُفضل التطبيق من قبل ناشطي الخصوصية بسبب تشفيره الشامل وتقنية المصدر المفتوح. وقال بارت برينيل، خبير التشفير في جامعة لوفين "إن سيغنال يشبه تطبيق واتساب من فيسوك وتطبيق أي مسج من آبل، لكنه يعتمد على بروتوكول تشفير مبتكر للغاية، ويمكنك التحقق مما يحدث داخلياً لأنه مفتوح المصدر".

وجرى تطوير تطبيق سيغنال في عام 2013 من قبل ناشطي الخصوصية، وهو مدعوم من قبل مؤسسة غير ربحية تحظى بدعم من مؤسس تطبيق واتساب براين اکتون، الذي ترك الشركة في عام 2017 بعد مشاكل مع إدارة فيسوك.

ويعتبر خبراء الخصوصية أن التطبيق أكثر أماناً من التطبيقات الأخرى، ويوضح الموقع الإلكتروني للتطبيق "لا يمكننا قراءة رسائلك أو رؤية مكالماتك، ولا يستطيع أي شخص آخر ذلك".

ورغم أن تطبيق "واتساب" يعتمد على البروتوكول ذاته الذي يعتمد عليه سيغنال، والمعروف باسم "أوين ويسبر سيستمز" إلا أن المنصة الملوكة لفيسوك ليست مفتوحة المصدر، ويواجه تطبيق المراسلة الشهير وتليغرام، في الوقت نفسه، مخاوف مماثلة بنسب عدم وجود شفافية حول كيفية إنجاز التشفير الخاص به.

وتأتي هذه المبادرة لتعزيز معايير الأمن السيبراني لدى الاتحاد الأوروبي في الوقت الذي يحاول فيه الاتحاد الحفاظ على أمن اتصالاته في أعقاب

الاختراقات البارزة التي صدمت الدبلوماسيين والمسؤولين في بروكسل، بعد أن كانت سفارة الاتحاد الأوروبي في موسكو قد تعرضت في شهر يونيو 2018 إلى الاختراق وتمت سرقة معلومات من شبكتها.

وذكرت صحيفة "نيويورك تايمز" الأميركية حينها أن شبكة الاتصالات الدبلوماسية للاتحاد الأوروبي كانت مخترقة على مدار ثلاث سنوات بسبب الحماية السيئة، بشكل ملحوظ للاتصالات الرسمية. ولم يتوقف الأمر على المفوضية الأوروبية كمنظمة دولية، ولكن شمل مؤسسات أخرى حكومية على رأسها حزب المحافظين البريطاني الذي طالب أعضاءه والعالمون في مقر الحزب بعدم استخدام الواتساب نهائياً في تبادل المعلومات والرسائل بين الطرفين، وأيضاً أوصى باستخدام تطبيق "سيغنال" لخصوصيته العالية وقدرته على حماية كل التعاملات من خلاله، خاصة وأن هناك العديد من التسريبات لمعلومات مهمة تم تبادل إرسالها عن طريق تطبيق الفيسبوك، الذي ظل لفترة طويلة يحظى بثقة ملايين الزبائن بل احتفل منذ فترة قريبة بتخطي عدد مستخدميه حاجز الـ2 مليار مستخدم.

مخاطر التطبيقات الأخرى

تعتبر التطبيقات المنافسة لـ"سيغنال" مثل "تليغرام" و"واتساب" محفوفة بالمخاطر ولاسيما أن مصدر التشفير مملوك من جهة محدودة، حين لا يزال "سيغنال" حراً ولا يمكن اتهامه بالميل نحو بلد معين. ويقول عضو بارز في حزب "الجمهورية إلى الأمام" الذي أسسه الرئيس الفرنسي إيمانويل ماكرون إنه "بدأ بوصي باستعمال هذا التطبيق".

وبحسب الكثير من الخبراء، فإن "واتساب" لا يدعم خاصية تشفير الرسائل التي يتم تخزينها على أجهزة التواصل الذكية، ما يتيح لأي شخص إمكانية الوصول إلى رسائل أي جهة مرة واحدة في حالة استخدامه لنفس الجهاز.

وفي ما يتعلق بالبيانات الوصفية، فإن "واتساب" لا تزال عليه البيانات الوصفية غير مشفرة، وهو ما يُمثل خطورة كبيرة؛ حيث يعني هذا الأمر أن طريقة التشفير الآمن للبيانات الوصفية ليست قوية جداً.

ويجمع كثيرون على أن أسوأ ما في تطبيق "واتساب" هو أنه يخزن البيانات في غير مكانها ومن السهل الوصول إليها، وتكون مريثة لجميع التطبيقات. ورغم أن "واتساب" لا يستطيع الوصول إلى المحادثات أو الصور الخاصة، إلا أنه قادر على معرفة مع من يتكلم أي شخص، ويستطيع الوصول إلى دفتر العناوين الخاص بك، كما يمكنه مزامنة بياناتك مع الشركة الأم "فيسوك".



الأشخاص الحريصون على سرية محادثاتهم المتبادلة ومصطحاتهم الشخصية عبر الإنترنت باتوا يميلون إلى تنزيل تطبيق الاتصال المشفر «سيغنال»

ويجمع تطبيق "واتساب" الأميركي، أكثر من ملياري مستخدم ناشط حول العالم، فقد تعرض للكثير من عمليات القرصنة المدوية أبرزها حادثة اختراق هاتف صاحب شركة "أمازون" جيف بيزوس، فضلاً عن الانتقادات التي طالته منذ أن اشترته شركة "فيسبوك" في العام 2014.

أما بالنسبة إلى تطبيق "تليغرام" الروسي فقد تشوهت صورته بسبب استخدامه بشكل واسع من قبل الجهاديين وعلاقته المشبوهة نوعاً ما بالسلطة الروسية.

محبذ في الأوساط الأمنية

تعود أصول "سيغنال" إلى عام 2010، عندما قامت مجموعة "ويسبر سيستمز" الأميركية التي تضم باحثين في مجال الأمن عبر الأجهزة المحمولة، بإنشاء خدمة تبادل الرسائل "ريدفون". وبعد استحواد "تويتر" على الشركة في العام 2011 أسس أحد أعضاء المجموعة الأساسية، ماثيو روزنفلد (وهو من قرصنة الإنترنت ومعروف باسم موكسي مارلينسبايك) منظمة "أوبن ويسبر سيستمز" في سان فرانسيسكو لمواصلة تطوير تطبيق للرسائل المجانية.

أطلق "سيغنال" في عام 2015 بعدما مولته تبرعات، ومن دون أي حملة تسويقية، قبل أن يصبح هذا التطبيق المجاني شعبياً للغاية ولاسيما بين المخبين والصحافيين، ويعود الفضل في ذلك إلى الدعم الذي تلقاه من إدوارد سنودن الذي كشف

عن إجراءات أجهزة الاستخبارات الأميركية المتعلقة بمراقبة الاتصالات. ويقول خبير المعلوماتية باتيست روبرت "يعد هذا التطبيق من أكثر التطبيقات الموصى بها في الأوساط الأمنية. لقد تم التدقيق في تشفيراته من قبل طرف ثالث مرآت عديدة. ومن هنا اكتسب الثقة". ويقول الصحافي المتخصص بالأمن السيبراني داميان بانكال إنه أداة "ضرورية" لضمان أمن المحادثات خلال نقلها.

سيغنال يطيح بواتساب

في المقابل، يعتمد "سيغنال" كما مثله من تطبيقات الاتصال ("واتساب" و"تليغرام") على بنية مركزية من الخواديم التي يمكن أن تكون هدفاً للقرصنة والرقابة، فضلاً عن كونه يتطلب وجود رقم هاتف لبدء المحادثة ما يحول دون إمكانية إخفاء الهوية وكذلك التعرض للقرصنة.

وفي عام 2018، تلقت المنظمة هبة بقيمة 50 مليون دولار من براين اکتون، أحد مؤسسي "واتساب"، الذي كان غادر "فيسبوك" قبل أشهر، ليصبح أحد الرؤساء التنفيذيين في "مؤسسة سيغنال" مع هدف لاستقطاب "مليارات المستخدمين" الجدد.

ويسعى التطبيق إلى تسهيل طريقة استخدامه وزيادة شعبيته، لذلك أدخل إمكانية استعمال "الستيكر" وهي رسوم صغيرة يتم تبادلها ورسائل عابرة، فضلاً عن تشكيل مجموعات محادثة.

لا يعرف عدد مستخدمي "سيغنال"، إلا أن شركة "آب آني" المتخصصة بسوق التطبيقات تؤكد بأنه ينمو، إذ يحل في المرتبة 110 العالمية بين التطبيقات الاجتماعية، أما من ناحية تنزيله على الهواتف فهو يحل في المرتبة 59 في الولايات المتحدة والمرتبة 40 في فرنسا. وإلى حدود وقت غير بعيد كان تطبيق "سكايب" من أبرز التطبيقات المستخدمة في العالم للتواصل عبر الإنترنت بالصوت والفيديو والمحادثة الجماعية. لكن بحسب الخبراء منذ تلك شركة مايكروسوفت للتطبيق عام 2011 بـ8.5 مليون دولار والتغيرات التي أدخلتها عليه شعر المستخدمون أنه فقد الكثير من أدواته المجانية وكذلك شروط الحماية.

نفس الأمر ينطبق على تطبيق واتساب منذ أن أصبح تابعاً لـ"فيسبوك"، حيث أعرب كثيرون من الذين يهتمون بحماية خصوصيتهم بتسردون في استخدامه إمكانية التمتع والتتبع وأيضاً مشكلة حصر البيانات الخاصة والإعلانات غير المرغوب فيها التي ستدخل قريباً منصة "واتساب" وهم يبحثون عن أدوات بديلة مجانية.

كل هذه الإشكالات دفعت بكبرى الشركات إلى البحث عن برامج عديدة بديلة مجانية وتكون أكثر حماية ومنها "سيغنال" الذي ينصح باستعماله إدوارد سنودن وهو خبير أمريكي محترف في الإعلامية، وعمل سابقاً للولايات المتحدة.