بسبب بن سلمان.. الأمم المتحدة تلاحقه وتحظره.. ما هي مشكلة "واتساب"؟

التغيير

لا تمر عدة أشهر إلا وتظهر فضيحة مدوية بخصوص اختراق تطبيق المراسلة الفوري "واتساب"، رغم أنه التطبيق الأكثر انتشاراً حول العالم بما يخص "الدردشة" على أجهزة الهاتف المحمول، حيث يستخدمه مليار ونصف مستخدم.

وبرزت أكثر فضائح "واتساب" بخصوص الاختراقات بعد أن حازته شركة "فيسبوك" (أبرز مواقع التواصل الاجتماعي)، منذ فبراير عام 2014، بمبلغ 19 مليار دولار.

ولا تطول الاختراقات المستخدمين العاديين لـ"واتساب" فقط؛ بل تعرض لها سياسيون ورجال أعمال بارزون، بالإضافة لصحفيين وناشطين في مجال حقوق الإنسان، الأمر الذي يثير المزيد من التخوفات حوله.

الأمم المتحدة لا تستخدمه

وفي ظل الاختراقات المتزايدة للتطبيق حظرت الأمم المتحدة على مسؤوليها استخدامه باعتباره تطبيقاً غير آمن؛ منذ أكثر من عام ونصف.

وقال فرحان حق، نائب المتحدث باسم الأمين العام للأمم المتحدة، الخميس (23 يناير 2020) إن العاملين بالهيئة الأممية لا يستخدمون تطبيق "واتساب" للتواصل؛ "لأنه غير مصنف كآلية آمنة".

وعندما سئل حق عما إذا كان الأمين العام للأمم المتحدة أنطونيو غوتيريش، قد اتصل بولي عهد آل سعود محمد بن سلمان، أو أي من قادة العالم الآخرين الذين يستخدمون واتساب، قال: "لقد صدرت تعليمات إلى كبار المسؤولين في الأمم المتحدة بعدم استخدام التطبيق؛ لأنه غير آمن".

وأضاف: "لذلك لا أعتقد أن الأمين العام يستخدمه"، مبيناً: إن "التوجيه بعدم استخدام واتساب قد أعطي لمسؤولي الأمم المتحدة، في يونيو من العام 2018".

اختراق هاتف بيزوس

ويعود كشف الأمم المتحدة عن ذلك بسبب معلومات تشير إلى تورط آل سعود في اختراق هاتف جيف بيزوس، مؤسس شركة "أمازون" ومالك صحيفة "واشنطن بوست" الأمريكية، عن طريق رسالة على تطبيق "واتساب".

وبدأت القصة في أبريل 2018، عندما حضر بيزوس حفل عشاء مع محمد بن سلمان، تبادلا خلاله أرقام الهواتف، وفي مايو منذ ذات العام تلقى بيزوس ملف فيديو مشفراً أُرسل من حساب الواتساب الشخصي لولي عهد آل سعود، تبعه بدء تسرّب كميات هائلة من البيانات من هاتف بيزوس.

بيزوس قال بعدها إنه تلقى رسائل واتساب من محمد بن سلمان تحتوي معلومات خاصة وسرية عن حياته الشخصية، بحسب ما نقلته وسائل إعلام، في الفترة بين نوفمبر 2018 وفبراير 2019، وهي الفترة التي تلت مقتل الصحفي السعودي جمال خاشقجي.

والتسريبات التي كُشف عنها هي رسائل وصور حميمية التقطت وجمعت، على مدار أربعة أشهر، لبيزوس وصديقته لورين سانشيز، وتسببت بالقضاء على زواجه الذي استمر 25 عاماً.

الأمر المثير أيضاً أن المحققين أغنيس كالامارد، مقررة الأمم المتحدة الخاصة بالإعدام خارج نطاق

القضاء، وديفيد كاي، مقرر الأمم المتحدة الخاص المعني بحرية التعبير، أصدرا بياناً، يوم الأربعاء (22 يناير 2020)، أشارا فيه إلى احتمالية تورط بن سلمان في عملية اختراق هاتف بيزوس، مشيرين إلى أن "تلك المزاعم تتطلب تحقيقاً فورياً من الولايات المتحدة وغيرها من السلطات المعنية".

وأوضح البيان أن "توقيت قرصنة هاتف بيزوس يدعم إجراء تحقيق عن مزاعم بأن بن سلمان أمر أو حرّض على قتل خاشقجي".

وأردف: "بينما كان مفترضاً أن يحقق آل سعود في مقتل خاشقجي كانت تستهدف سراً وعلانية جيف بيزوس"، مشيراً بالقول: "معلوماتنا تشير إلى احتمال تورط بن سلمان بمراقبة بيزوس للتأثير على صحيفة واشنطن بوست بشأن آل سعود".

ولفت إلى أن "البرنامج الذي استخدمه بن سلمان في قرصنة هاتف بيزوس هو برنامج (بيغاسوس) الإسرائيلي"، كاشفاً أن "الشهر الذي تم فيه اختراق هاتف بيزوس هو نفسه الذي اختُرقت فيه هواتف اثنين من المقربين لخاشقجي".

مدير الاتصالات في "واتساب"، كارل ووج، قال يوم الخميس (23 يناير 2020): إن "كل رسالة خاصة محمية بواسطة تشفير شامل للمساعدة في منع المتطفلين أو غيرهم من مشاهدة الدردشات".

وأردف: "تقنية التشفير التي طوّرناها تحظى بتقدير كبير من قبل خبراء الأمن، وهي أفضل المتاح في جميع أنحاء العالم".

هل المشكلة في "واتساب"؟

ولخبراء الأمن التقني حساسية مفرطة تجاه تطبيقات مثل "واتساب"؛ لما يحمل من ثغرات أمنية، وقد حذر منه محققون جنائيون ومواقع مختصة بأمن المعلومات بعد استحواذ "فيسبوك" عليه.

وفي مايو 2019، تحدثت صحيفة "فايننشال تايمز" الأمريكية عن وجود ثغرات أمنية في تطبيق "واتساب" تتيح للمخترق سرقة بيانات المستخدمين دون علمهم، ودون ترك أي بصمات خلفهم، وإن كانت الشركة قد عالجت تلك الثغرة على خوادمها بالإضافة للتطبيقات المستخدمة على الهواتف الذكية.

وأوضحت الصحيفة أنه "عثر على الثغرة في بروتوكول نقل البيانات المعروف اختصاراً بـ(SRTCP)، في الحزمة البرمجية الخاصّة بإجراء الاتصالات عبر شبكة الإنترنت (VOIP)، وهذا بعد اكتشاف محاولة فاشلة لاختراق أحد النُشطاء في مجال حقوق الإنسان، بتاريخ 12 مايو، لتبدأ التحرّيات فوراً لفهم آلية عمل هذه الثغرة".

ويؤكد خبراء في أمن المعلومات أن سياسة الخصوصية التي تعتمد عليها "فيسبوك" بالتعامل مع "واتساب" مشابهة لسياستها بعد الاستحواذ على تطبيق "إنستغرام"، الذي يتيح لها نقل المعلومات والبيانات من المستخدمين من "واتساب" إلى "فيسبوك"، ضمن ما يُعرف بـ"ميتا داتا".

كما أن "فيسبوك" لديها علاقات تعاون مع الأجهزة الاستخبارية، خاصة وكالة الأمن القومي الأمريكية، ومكاتب الاتصالات الحكومية في وكالة الاستخبارات البريطانية، بالإضافة لمذكرات تفاهم مع دولة الاحتلال الإسرائيلي.

زيادة الوعي الشخصي "ضرورة"

في المقابل قال مهندس البرمجيات عمار صرصر، في حديث مع "الخليج أونلاين": "لا أعتقد أن تطبيق واتساب أسهل اختراقاً من تطبيقات أخرى، ولكنه عادة يستعمل كأحد أهم وسائل خداع ضحايا الاستهداف بسبب انتشاره الكبير على جميع الأجهزة، فترسل من خلاله روابط ظاهرها بريء ولكن فتحها يؤدي إلى تثبيت برمجيات خبيثة في أجهزة المستخدمين".

وأضاف: "في 90% من حالات الاختراق يكون سبب الاختراق هو نقص وعي أو انتباه الضحية، فيضغط على روابط لا يعرف مصدرها، أو يحمّل تطبيقات من خارج متاجر التطبيقات الرسمية، وهذا لا يمكن منعه عبر أي تطبيق، لذا فإن زيادة الوعي الشخصي بأمن المعلومات يعتبر أهم وسيلة دفاعية".

ولفت الخبير البرمجي إلى أن "اختراق الجهاز سواء تم بسبب نقص وعي المستخدم، أو عبر استغلال ثغرات في واتساب أو تطبيقات أخرى، أو حتى في نظام التشغيل نفسه (iOS & Android)، فإنه لا شك يعتبر أمراً كارثياً؛ حيث يتمكن المخترق من الاطلاع على كافة معلومات الجهاز؛ من رسائل نصية، ومحادثات على وسائل التواصل الاجتماعي، وصور، وفيديوهات، وغيرها، كما يمكن تحميل كل هذه البيانات إلى جهاز المخترق، ومن ثم ستكون كل بيانات الضحية وخصوصيته في خطر".

وأكّد أن "جميع الشركات البرمجية تعمل على إغلاق الثغرات الأمنية التي تظهر في برمجياتها بشكل مستمر عن طريق التحديثات البرمجية للتطبيقات وأنظمة التشغيل، لذا ينصح دوماً بتحديث التطبيقات كافة -وخاصة واتساب- إلى أحدث نسخة".

وشدد "صرصر" على أنه "لا شك أن الواتساب ليس أكثر التطبيقات أمناً"، مقدماً نصيحة تتمثل بـ"استخدام بدائل أخرى خاصة في حالة وجود حوارات خاصة جداً وفيها معلومات حساسة، ومن أفضل بدائله تطبيق تلغرام".

واختتم حديثه قائلاً: "لا شيء يمكن أن يضر المستخدم أكثر من قلة علمه، لذا فإن زيادة ثقافة المستخدمين حول أمن المعلومات أصبحت ضرورة ملحة".

كيف يُخترق "واتساب"؟

ويتساءل الكثير عن إمكانية تجنّب الاختراق، أو كيف يحصل وتتم عبره السيطرة على الهاتف المحمول أو البيانات الموجودة فيه؟

فقد ذكرت مواقع التقنية أن هناك عدة طرق يمكن عبرها اختراق رسائل واتساب على أي هاتف محمول يعمل بأي نظام تشغيل؛ مثل "آندرويد"، أو "آي أو إس".

في عام 2016 شاركت فيسبوك بيانات المستخدمين بينها وبين "واتساب"، ولكن بعد رد الفعل العكسي لهذه الخطوة سمح التطبيق للمستخدمين بإلغاء الاشتراك في مشاركة البيانات، ولكن ذلك أتاح الوصول للبيانات الخاصة في التطبيق.

وفي يوليو 2019، اكتشف اختراق التطبيق عبر ملفات الوسائط، حيث يستفيد هذا الهجوم من طريقة تلقي التطبيقات لملفات الوسائط مثل الصور أو مقاطع الفيديو، وكتابة هذه الملفات على وحدة تخزين خارجية للجهاز، إذ يتم بتثبيت برمجية ضارة مخبأة داخل التطبيق.

وفي أغسطس 2019، كشف باحثو الأمن في شركة Point Check عن وجود ثغرات في واتساب تسمح للقراصنة باعتراض الرسائل المرسلة في المحادثات الخاصة والجماعية والتلاعب بها، وأن الشركة فشلت في معالجتها بالرغم من إبلاغها بها منذ عام.

وفي مايو 2019، قامت شركة "بيغاسوس" باختراق التطبيق عن طريق إجراء مكالمات صوتية عبر واتساب لأهدافهم، وحتى لو لم يستجب الهدف للمكالمة فقد يظل الهجوم فعالاً، وقد لا يدرك الهدف أن جهازه ثبتت عليه برمجيات تجسس.

في بداية شهر أكتوبر 2019، كُشف عن ثغرة أمنية في تطبيق واتساب تتيح للقراصنة الوصول إلى بيانات المستخدمين والتحكم فيها باستخدام صور GIF ضارة، حيث يعمل الاختراق من خلال الاستفادة من طريقة قيام واتساب بمعالجة الصور عندما يفتح المستخدم معرض الصور لإرسال ملف وسائط.