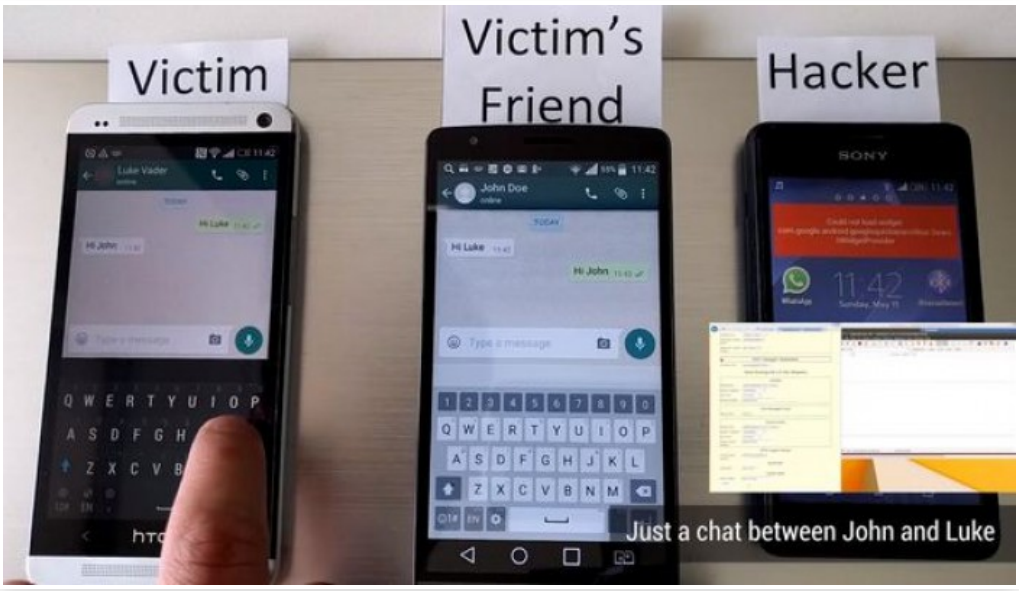
# كيف تمكن قراصنة من اختراق واتساب وتيليغرام؟




الأحد 5 يونيو 2016 02:06 م

تمكن قراصنة من استغلال ثغرة في نظام الاتصالات لاختراق تطبيقي واتساب وتيليغرام، مع أن الأخيرين يعدان من أكثر تطبيقات التراسل الفوري أمانًا بفضل تقنيات التشفير التي يعتمدانها.

ويروج تطبيقا واتساب وتيليغرام لنفسيهما على أنهما البديل الآمن للمكالمات الهاتفية، والرسائل النصية، والرسائل الإلكترونية، ولكن ذلك لا يمنع من اختراقهما إن اُستغلت ثغرات أخرى من خارجهما.

وتمكن قراصنة من ذلك بعد استغلال ثغرة أمنية في ما يُعرف بـ"نظام الإشارة رقم 7" Signaling System No 7، وهي شبكة عالمية من شركات الاتصالات تعمل كمُجمِّع مركزي يربط الشركات حول العالم.

وتقوم تطبيقات التراسل المشفرة عادةً بمنع المتطفلين الخارجيين من الوصول إلى رسائل المستخدمين بفضل تقنية التشفير "طرف إلى طرف" التي تخزن مفتاح إلغاء تشفير الرسائل على جهازي طرفي المحادثة فقط، أي أنه إن تمكن أحدهم من الوصول إلى الرسائل فلن يكون قادراً على قراءة الرسائل أو إلغاء تشفيرها.

ولكن بسبب الثغرة الموجودة في نظام الإشارة رقم SS7 7 تمكن قراصنة من اختراق تطبيقي واتساب وتيليغرام، وذلك من خلال إيهام شبكة الاتصالات بأن هاتف المهاجم يملك نفس رقم الضحية، ما يعني إمكانية إنشاء حساب على التطبيقين واستقبال الرمز السري الذي يُثبت أن هاتفه هو نفسه صاحب الحساب.

وبعد إتمام العملية، يصبح باستطاعة المهاجم التحكم بحساب الضحية، بما في ذلك القدرة على إرسال واستقبال الرسائل، فضلًا عن قراءتها.

أما عن سبب ترك ثغرات نظام SS7 دون إصلاح، فيعود إلى أن النظام شبكة من شركات الاتصالات حول العالم، ما يعني أن أيا من تلك الشركات تملك أو تتحكم بالنظام، لذا أي تغيير عليه يتطلب إجراءات معقدة.

ويُقال أيضًا إن وكالات الاستخبارات تقف عائقًا بين الثغرات وقدرات شركات الاتصالات على إصلاحها، فهي تستفيد منها في التجسس على المستخدمين في حال اعتماد التطبيقات لتقنيات تشفير معقدة.