/https://thehackernews.com

يوضح الباحثون كيفية اختراق أي حساب TikTok عن طريق إرسال الرسائل القصيرة

Mohit Kumar -January 08, 2020

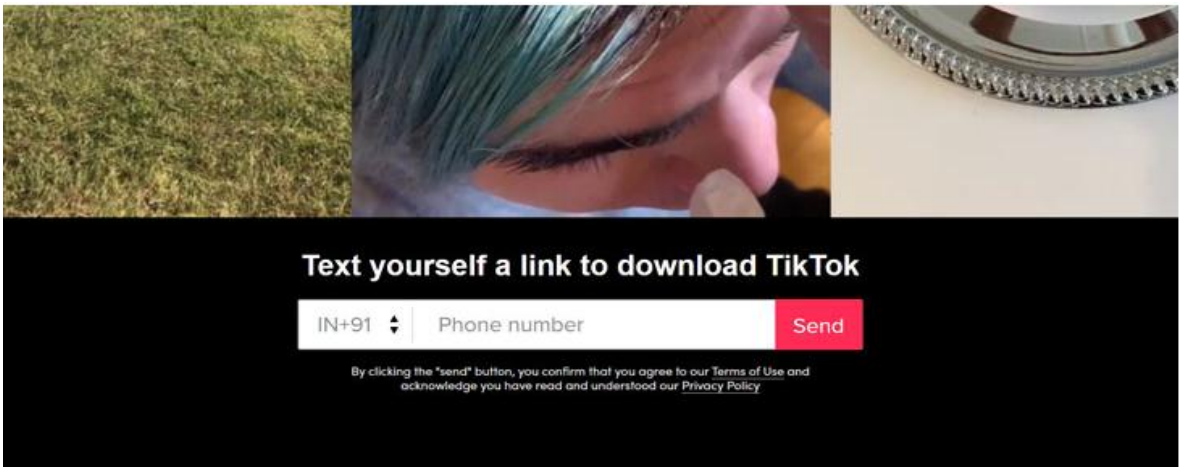
ترجمة وتنقيح – الباحث المهندس احمد الربيعي

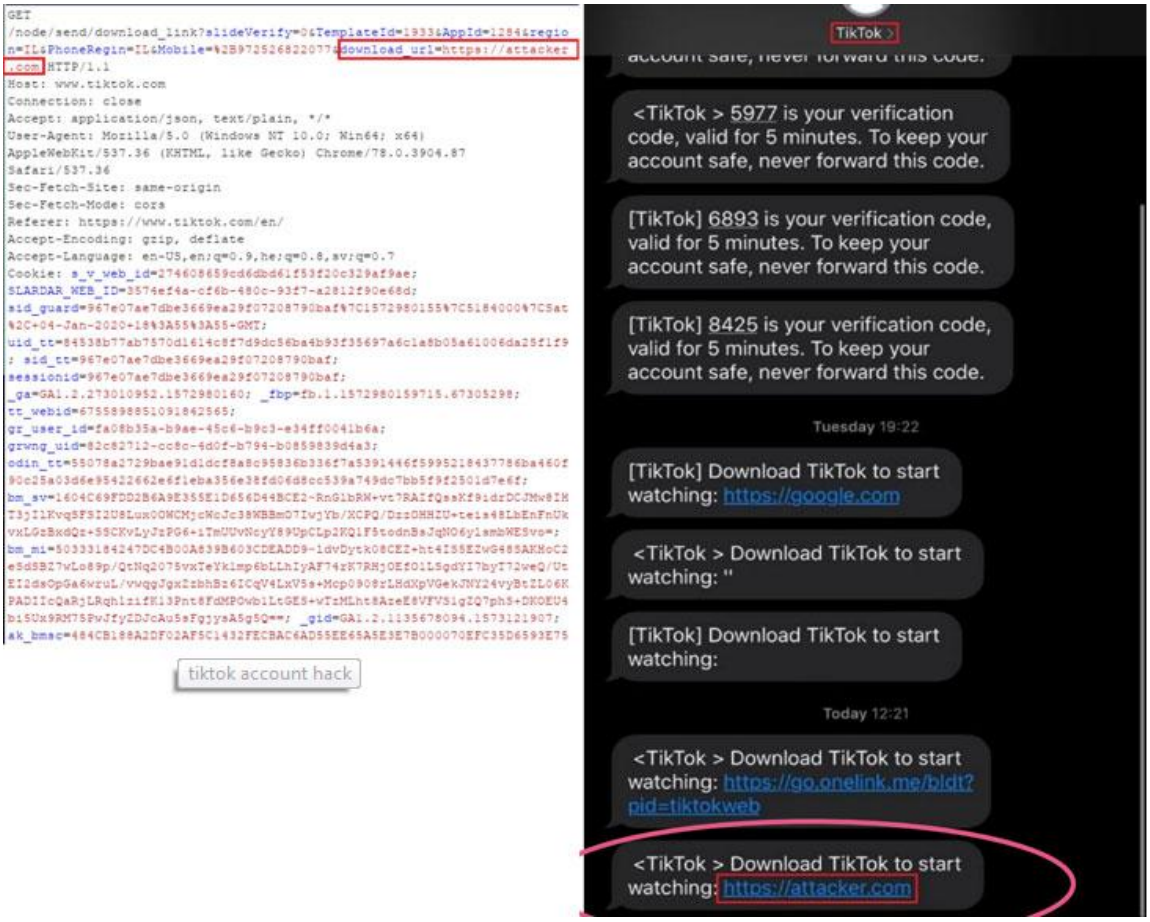
يخضع TikTok ، وهو ثالث أكثر التطبيقات التي تم تنزيلها في عام 2019 ، لتدقيق شديد على خصوصية المستخدمين ، مضافاً اليه فرض رقابة على المحتوى المثير للجدل من الناحية السياسية وعلى أسس تتعلق بالأمن القومي - لكنه لم ينته بعد ، حيث إن أمن مليارات مستخدمي TikTok أصبح الآن قيد السؤال. حيث احتوى التطبيق الصيني الشهير على خاصية مشاركة الفيديو ، الذي سمح بمشاركة بعض المقاطع الفيروسية التي تشتمل على ثغرات أمنية يحتمل أن تكون خطرة وتسمح للمهاجمين عن بعد باختطاف أي حساب مستخدم بمجرد معرفة رقم الهاتف المحمول للضحايا المستهدفين. وفي تقرير مشترك بشكل خاص مع The Hacker News ، كشف باحثون في الأمن السيبراني في Check Point أن هذه الثغرة تسمح للمهاجمين بتنفيذ التعليمات البرمجية الضارة عن بعد وتنفيذ الإجراءات غير المرغوب فيها نيابة عن الضحايا ودون موافقتهم .

تتضمن نقاط الضعف المبلغ عنها مشكلات منخفضة الخطورة مثل خداع روابط الرسائل النصية القصيرة (SMS link spoofing) وإعادة التوجيه المفتوح والبرمجة النصية عبر المواقع (XSS) والتي قد تتيح للمهاجم عن بعد القيام بهجمات عالية التأثير ، بما في ذلك:

١. حذف أي مقاطع فيديو من ملف TikTok الشخصي للضحايا
٢. تحميل مقاطع فيديو غير مصرح بها لملف TikTok الشخصي للضحايا
٣. اجعل مقاطع الفيديو الخاصة (المخفية) عامة المشاهدة
٤. كشف المعلومات الشخصية المحفوظة على الحساب ، مثل العناوين الخاصة ورسائل البريد الإلكتروني .

حيث يستفيد الهجوم من نظام الرسائل نصية الغير آمن والذي تقدمه TikTok على موقعها في الويب والذي يسمح للمستخدمين بإرسال رسالة إلى ارقام هواتفهم مع رابط لتنزيل تطبيق مشاركة الفيديو. ووفقًا للباحثين ، يمكن للمهاجم إرسال رسالة نصية قصيرة إلى أي رقم هاتف نيابة عن TikTok بعنوان URL معدّل للتنزيل إلى صفحة ضارة مصممة لتنفيذ التعليمات البرمجية على جهاز مستهدف مع تطبيق TikTok المثبت بالفعل. كما في الشكل التالي :





وعند دمجه مع إعادة التوجيه المفتوح ومشكلات البرمجة النصية عبر المواقع ، يمكن للهجوم أن يسمح للمتسللين بتنفيذ تعليمات JavaScript البرمجية نيابة عن الضحايا بمجرد أن ينقروا على الرابط الذي أرسله خادم TikTok عبر الرسائل القصيرة .تُعرف هذه التقنية عادةً باسم cross-site request forgery attack ، حيث يقوم المهاجمون بخداع المستخدمين المصادق عليهم لتنفيذ إجراء غير مرغوب فيه. وقد قال الباحثون : لقد أدركنا أنه بإمكاننا تنفيذ شفرة JavaScript وتنفيذ إجراءات نيابة عن الضحية ودون موافقته .

لقد قام Check Point بالإبلاغ عن هذه الثغرات الأمنية لدى ByteDance ، مطور TikTok في أواخر نوفمبر 2019 ، والذي قام بعدها بإصدار نسخة مصححة من تطبيقه المحمول في غضون شهر واحد لحماية مستخدميه من المتسللين. إذا كنت لا تشغل أحدث إصدار من TikTok المتاح في متاجر التطبيقات الرسمية لنظامي التشغيل Android و iOS ، يُنصح بتحديثه في أقرب وقت ممكن لتجنب هذه الهجمات .