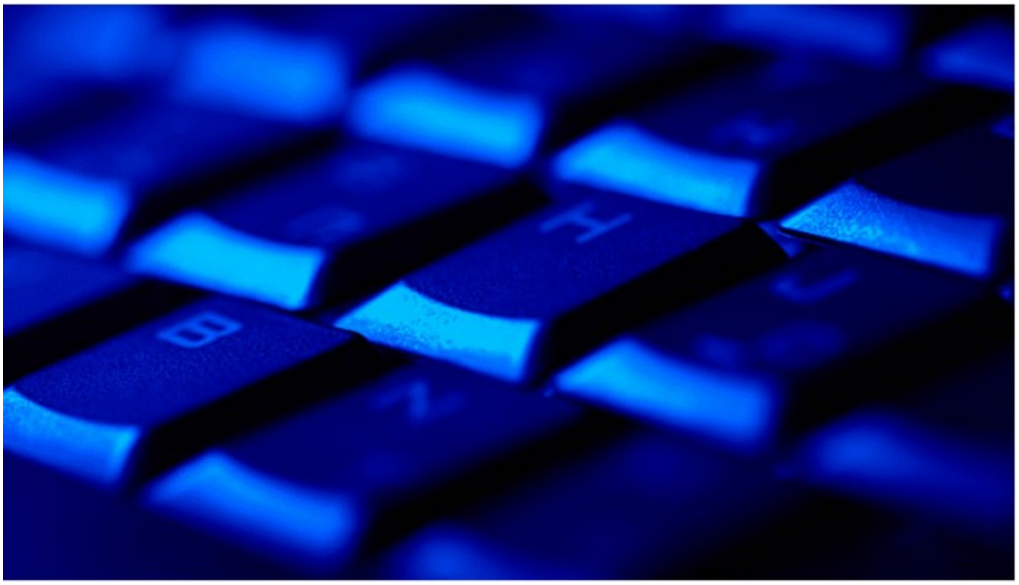
قراصنة يستغلون ثغرة أمنية في تطبيق تيليجرام لنشر برمجيات خبيثة



الاثنين 19 فبراير 2018 01:02 م

عثر باحثون في كاسبرسكي لاب على هجمات تُنفّذ عن طريق برمجية خبيثة جديدة من خلال استغلال ثغرة أمنية في تطبيق تيليجرام المكتبي، لم تكن معروفة من قبل.

واستغلّت الثغرة لإيصال برمجيات خبيثة متعددة الأغراض إلى أجهزة المستخدمين، والتي يمكن أن تستخدم إما كمدخل خلفي أو كأداة لإدخال برمجيات تعدين، اعتماداً على طبيعة عمل الحاسوب المصاب.

ووفقاً لبحث أجراه المختصون في كاسبرسكي لاب، تمّ استغلال الثغرة بنشاط منذ مارس 2017 من أجل التنقيب عن العملات الرقمية، مثل عملة مونيرو وزي كاش وغيرها.

وتشكّل خدمات التراسل والتواصل الاجتماعي منذ فترة طويلة جزءاً أساسياً من حياة الناس عبر الإنترنت، وهي مصممة لتيسير التواصل من أجل البقاء على اتصال مع الأصدقاء وأفراد العائلة، لكن يمكن لهذه الخدمات، في الوقت نفسه، أن تعقّد الأمور كثيراً إذا ما تعرّضت لهجمات إلكترونية.

على سبيل المثال، نشرت كاسبرسكي لاب الشهر الماضي تقريراً بحثياً عن البرمجية الخبيثة المتقدمة التي تستهدف الأجهزة النقالة، وهي تروجان القادرة على سرقة رسائل تطبيق واتساب.

وكشفت أحدث الأبحاث في هذا السياق أن خبراء تمكنوا من التعرّف على هجمات حقيقية تستغل ثغرة لم تكن معروفة سابقاً في الإصدار المكتبي من تطبيق تيليجرام للتراسل الفوري.

وتكمن الثغرة التي عُثر عليها في تيليجرام وفقاً للبحث، في معيار الترميز الموحّد RLO "الخاص بالكتابة من اليمين إلى اليسار"، والذي يُستخدم لترميز اللغات التي تُكتب من اليمين إلى اليسار، مثل اللغة العربية.

لكن مع ذلك، فإن هذا المعيار يمكن أيضاً أن يُستخدم من قبل منتجي البرمجيات الخبيثة لتضليل المستخدمين وحملهم على تنزيل ملفات خبيثة مقنَّعة، كالصور مثلاً.

واستخدم المهاجمون حرفاً مخفياً في اسم الملف من حروف معيار الترميز الموحّد، قام بعد الهجوم بعكس ترتيب الأحرف، ما منح الملف نفسه اسماً مختلفاً.

ونتيجة لذلك، قام المستخدمون بتنزيل برمجيات خبيثة خفية تم تثبيتها بعد ذلك على حواسيبهم، بغير عِلم منهم.

وقد سارعت كاسبرسكي لاب إلى إبلاغ القائمين على تيليجرام عن الثغرة، ولم يتمّ حتى الآن ملاحظة أي استغلال للثغرة في أي من منتجات التطبيق.

واستطاع خبراء كاسبرسكي لاب، خلال التحليلات التي أجروها، تحديد عدة سيناريوهات للهجمات التي شنها المخربون عبر استغلال الثغرة غير المعروفة، أولها استغلال الثغرة لإيصال برمجيات تعدين خبيثة يمكن أن تُحدث ضرراً كبيراً بالمستخدمين، إذ يخلق مجرمو الإنترنت أنواعاً مختلفة من العملات الرقمية، باستخدام قوة الحوسبة لجهاز الضحية.

وعلاوة على ذلك، عثر باحثو كاسبرسكي لاب عند تحليل الخوادم التي يستخدمها المجرمون، على محفوظات أرشيفية تحتوي على سجلات

من تطبيق تيليجرام مُحتفَظ بها محلياً بعد أن تمت سرقتها من الضحايا

أما ثاني تلك السيناريوهات، فكان تثبيت مدخل خلفي بعد الاستغلال الناجح للثغرة، يستخدم واجهة برمجة التطبيقات في التطبيق كبروتوكول للقيادة والتحكم، ما يمنح المتسللين القدرة على الوصول عن بعد إلى حاسوب الضحية

ويبدأ المدخل الخلفي العمل بصمت بعد التثبيت، ما يمنع من كشف المتسلل في الشبكة ويمكّنه من تنفيذ أوامر مختلفة تشمل تركيب مزيد من أدوات التجسس، وقد دلّت الأغراض المكتشفة خلال البحث على أن المخربين من أصل روسي

ودعا أليكسي فيرش، محلل البرمجيات الخبيثة في قسم أبحاث الهجمات الموجهة لدى كاسبرسكي لاب، مطوري التطبيقات إلى الاهتمام بتقديم الحماية المناسبة لمستخدمي تطبيقات التراسل الفوري كيلا تصبح أهدافاً سهلة للمجرمين، مشيراً إلى ما تتمتع به هذه التطبيقات من شعبية واسعة ورواج فائق، وأضاف: "وجدنا عدّة سيناريوهات حدثت في استغلال هذه الثغرة التي لم تكن معروفة في السابق، والتي تمّ عبرها إيصال برمجيات خبيثة عامة وأخرى للتجسس إلى أجهزة الضحايا، فضلاً عن استغلالها في إيصال برمجيات تعدين للتنقيب عن العملات الرقمية، والتي أصبحت توجهاً عالمياً شهدناه طوال العام الماضي، ونحن نعتقد كذلك بوجود طرق أخرى لاستغلال هذه الثغرة".

وتوصي كاسبرسكي لاب باتخاذ الاحتياطات التالية لحماية حواسيبهم من التعرض لأية إصابة:

عدم تنزيل ملفات غير معروفة من مصادر غير موثوق بها، وفتحها
تجنّب مشاركة أي معلومات شخصية حساسة في الرسائل الفورية
تثبيت حل أمني موثوق به لكشف جميع التهديدات المحتملة والحماية منها، بما يشمل برمجيات التعدين الخبيثة