هکرها از تلگرام به عنوان مرکزی برای فعالیت‌های مخرب استفاده می‌کنند - دیجیاتو

جواد تاجی | شنبه، ۰۴ اردیبهشت ۱۴۰۰

محققان امنیتی به این موضوع پی برده‌اند که محبوبیت تلگرام به عنوان یک پلتفرم پیام‌رسان با رمزگذاری سرتاسری، باعث محبوبیت آن میان هکرها هم شده است.

در گزارشی جدید، «عمر هافمن» از شرکت امنیت سایبری «چک پوینت» توضیح می‌دهد که تولیدکنندگان بدافزار برای فعالیت‌های مخرب خود بیش از پیش از تلگرام به عنوان یک سیستم فرماندهی و کنترل استفاده می‌کنند، زیرا این اپ در مقایسه با نرم‌افزارهای مخرب معمولی مبتنی بر وب مزایای بیشتری را در اختیار آن‌ها قرار می‌دهد.

تلگرام تنها ابزار رمزگذاری شده‌ای نیست که توسط عوامل این تهدیدها مورد استفاده قرار می‌گیرد. تحقیقات اخیر شرکت نرم‌افزاری «Sophos» نشان می‌دهد که آن‌ها به طور فزاینده‌ای برای جلوگیری از شناسایی به پروتکل‌های ارتباطی رمزگذاری شده و همچنین سرویس‌های ابری قانونی تغییر جهت می‌دهند.

هافمن در تجزیه و تحلیل خود عنوان کرده که «Massad» برای اولین بار در سال ۲۰۱۷ از تلگرام به عنوان سرور سیستم فرماندهی و کنترل استفاده کرده. گفته می‌شود که این گروه اولین افرادی بودند که برای انجام حملات خود به مزایای سرویس‌های پیام رسان پی برده بودند. به گفته هافمن، از آن زمان محققان ده‌ها نوع بدافزار مختلف را کشف کرده‌اند که برای انجام فعالیت‌های مخرب خود از تلگرام استفاده می‌کنند.

طی سه ماه گذشته، چک پوینت شاهد بیش از صد حمله بوده که با استفاده از یک تروجان از راه دور و چند منظوره جدید به نام «ToxicEye»، ایمیل‌های حاوی برنامه اجرایی مخرب را پخش کرده‌اند. همچنین از ToxicEye در محیط تلگرام برای برقراری ارتباط با سرور فرماندهی و کنترل و استخراج اطلاعات سرقت شده استفاده می‌شود.

تحلیل هافمن نشان می‌دهد که تولیدکنندگان بدافزارها از این تروجان در پوشش بات تلگرام استفاده می‌کنند و هنگام استفاده کاربر از این بات‌ها، مهاجم به گوشی یا رایانه او متصل می‌شود. این بات ظاهرا داده‌های کاربران را به سرقت می‌برد، صدا و ویدیو ضبط می‌کند و حتی شبیه باج‌افزارها، فایل‌ها را قفل می‌کند.

دیجیاتو