

[View the original article](#)

خبرهای کوتاه

آنتروپیک: هوش مصنوعی می‌تواند مانند کرم رایانه‌ای در دستگاه‌های هوشمند تکثیر شود

راديو فردا

۲۱/مهر/۱۴۰۵



شرکت هوش مصنوعی آنتروپیک هشدار داد که مدل‌های کوچک هوش مصنوعی ممکن است تنها چند ماه با دستیابی به توانایی تکثیر و گسترش خودکار میان دستگاه‌های متصل به اینترنت فاصله داشته باشند؛ قابلیتی که می‌تواند تهدید تازه‌ای برای امنیت سایبری ایجاد کند.

پژوهشگران آنتروپیک روز دوشنبه ۲۰ گفتند چنین برنامه‌هایی می‌توانند بدون دخالت انسان و بی‌نیاز از مراکز بزرگ پردازش داده، مانند کرم‌های رایانه‌ای از دستگاهی به دستگاه دیگر منتقل شوند و در شبکه‌ای از تلویزیون‌ها، دوربین‌ها و لوازم خانگی هوشمند که امنیت ضعیفی دارند گسترش یابند.

به گفته آن‌ها، مهار این برنامه‌ها پس از انتشار نیز دشوار خواهد بود، زیرا هیچ مرکز واحدی برای متوقف کردن فعالیتشان وجود نخواهد داشت.

ماه گذشته، داریو آمودئی، مدیرعامل آنتروپیک، گفته بود که طی یک سال آینده یا حتی زودتر، ممکن است هوشواره به مرحله‌ای برسد که با استفاده از یک «بات‌نت»، کل اینترنت را «گروگان» بگیرد؛ هشدارى که در جامعه کارشناسان امنیت سایبری، بحث‌های گسترده‌ای را رقم زد.

«بات‌نت‌ها»، شامل شبکه‌های بزرگی از تجهیزاتی هستند که از سوی اپراتورهای مخرب کنترل می‌شوند و از نخستین روزهای گسترش اینترنت فعال بوده و همچنان فعال هستند.

این شبکه‌ها عموماً شامل تجهیزات هوشمند یا سطح امنیتی پایین هستند؛ مثل تلویزیون‌های هوشمند اندروئیدی، دوربین‌های امنیتی و از این دست. هکرها از این تجهیزات برای فرستادن هرزنامه یا ویروس استفاده می‌کنند، یا با ایجاد ترافیک مصنوعی، شرکت‌های هدف را با اختلال مواجه می‌کنند.

بیانیه روز دوشنبه آنتروپیک، اولین تلاش برای توضیح روند عملی اجرای این موضوع بوده است.

بیشتر در این باره:

هوش مصنوعی کلود اطلاعات جعلی درباره یک پرونده
قتل به پلیس آمریکا ارسال کرد



بر این اساس، آزمایش‌های این شرکت نشان داده که یک عامل مخرب هوش مصنوعی می‌تواند توان محاسباتی تجهیزات هوشمند ارزان‌قیمت را در اختیار گرفته و با کنار هم گذاشتن آنها، دیگر مدل‌های هوش مصنوعی را اجرا کند. علاوه بر این، مدل‌ها توانستند با کپی‌کردن خود، در یک شبکه آزمایشی گسترش پیدا کنند.

آنتروپیک پیش‌بینی کرد که اگر مدل‌های کوچک هوش مصنوعی، با سرعت و شتاب کنونی به افزایش توان خود ادامه دهند، خواهند توانست تا پیش از پایان سال ۲۰۲۶، دو ماه و نیم دیگر، به توانایی لازم برای کپی‌سازی مستقل خود دست یابند.

این غول حوزه هوش مصنوعی همچنین هشدار داد که سیستم‌های آینده خواهند توانست تجهیزات قدرتمندتری، از جمله پردازنده‌های مراکز داده را هدف قرار دهند.

این مطلب بخشی از:

خبرهای کوتاه

بایگانی

دانش و فناوری

جهان