گزارش خبر
NEWSREPORT

کد خبر: ۵۲۳۹۵۱
جمعه ۴ اردیبهشت ۱۴۰۵ ۱۳:۴۹

# از شایعه تا شکست: اثرات فاجعه‌بار انتشار ویدیوهای مسئولین

در عصر هوش مصنوعی، انتشار یک ویدیوی کوتاه، دیگر تنها یک پیام بصری نیست؛ بلکه یک بمب ساعتی اطلاعاتی است که می‌تواند مکان دقیق، زمان ضبط و حتی هویت تجهیزات را لو بدهد.  در این تحلیل، به سه لایه خطرناک امنیتی نهفته در ویدئوها می‌پردازیم که اغلب نادیده گرفته می‌شوند:<;br&#۴۷>

به گزارش شبکه خبری تعاون ، در عصر هوش مصنوعی، انتشار یک ویدیوی کوتاه، دیگر تنها یک پیام بصری نیست؛ بلکه یک بمب ساعتی اطلاعاتی است که می‌تواند مکان دقیق، زمان ضبط و حتی هویت تجهیزات را لو بدهد. در این تحلیل، به سه لایه خطرناک امنیتی نهفته در ویدئوها می‌پردازیم که اغلب نادیده گرفته می‌شوند:

جادوی بصری: مکان‌یابی با سایه و بازتاب

هوش مصنوعی با تحلیل «کرونولوکیشن» (زمان‌یابی) و زاویه سایه‌ها، می‌تواند زمان دقیق ضبط (حتی تا دقیقه) و عرض جغرافیایی را با خطای نزدیک به صفر محاسبه کند.

ژئولوکیشن: با بررسی پس‌زمینه و استفاده از مثلث‌بندی سه‌بعدی، موقعیت دوربین روی نقشه دقیقاً مشخص می‌شود.

استخراج اطلاعات خارج از کادر: سطوح براق (عینک، شیشه، قرنیه چشم) مانند آینه عمل کرده و تصویری از محیط پشت سر فرد را بازتاب می‌دهند که با پردازش تصویر، جزئیات کامل اتاق و افراد حاضر آشکار می‌شود.

شناسنامه مخفی: متادیتا و سیگنال‌های رادیویی

جمله معروفی در امنیت سایبری وجود دارد: «تصویر ممکن است دروغ بگوید، اما متادیتا هرگز دروغ نمی‌گوید.»

قالب EXIF: فایل‌های ویدئویی حاوی مختصات GPS دقیق، مدل گوشی، شماره سریال سنسور و زمان دقیق ضبط هستند که با یک کلیک ساده قابل استخراج‌اند.

هوش سیگنالی (TDOA): حتی ارسال ویدیو نیز ردپای دیجیتال دارد. سیستم‌های جاسوسی با تحلیل اختلاف زمان رسیدن سیگنال به آنتن‌ها، موقعیت فرد را با دقت چند متری ردیابی می‌کنند.

دکل‌های جعلی: دشمنان می‌توانند با استفاده از دستگاه‌هایی شبیه‌ساز دکل مخابراتی، گوشی فرد را فریب دهند تا به جای دکل واقعی، به دکل جاسوسی متصل شود. این کار نه‌تنها لو رفتن هویت و موقعیت را به همراه دارد، بلکه امکان تزریق بدافزارهای جاسوسی به دستگاه را نیز فراهم می‌کند.

تحلیل فرکانس برق: شبکه برق هر منطقه نوسانات فرکانسی منحصربه‌فردی دارد. میکروفون‌ها و دوربین‌ها این نوسانات (نویزهای نامحسوس) را ضبط می‌کنند که می‌تواند محل دقیق اتصال به شبکه توزیع برق را لو بدهد.

امضای صوتی: DNA محیطی حتی در سکوت مطلق، فیزیک محیط خیانت می‌کند.

اکو و بازتاب صوتی: هر اتاقی به دلیل ابعاد و جنس مصالح، امضای صوتی (اکو) منحصربه‌فردی دارد. هوش مصنوعی با حذف صدای گوینده و تحلیل بازتاب‌ها، می‌تواند تشخیص دهد فرد در یک آپارتمان مسکونی است یا یک سوله صنعتی.

نویزهای محیطی: صدای حشرات بومی، آژیرها، یا قطارهای خاص می‌تواند شعاع جست‌وجو را به یک شهر یا محله خاص محدود کند.

در عصر هوش مصنوعی امنیت به مدیریت هوشمند ردپای دیجیتال گره خورده است.