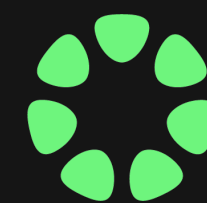


SABEU QUÈ SIGNIFICA "RECALL AI"?

- Es tracta d'una nova funció de Microsoft Windows que emmagatzema l'historial de l'escriptori de l'ordinador cada cinc segons a través d'una captura de pantalla automàtica gràcies a un sistema d'IA.
- El problema? Doncs que juntament amb la vigilància que això suposa per tota la nostra activitat d'escriptori (aquesta està arribant a límits impensables fa pocs anys), és un sistema que és fàcil d'abusar segons diversos pirates informàtics.
- https://www.wired.com/story/total-recall-windows-recall-ai/?utm_social-type=owned&mbid=social_twitter&utm_medium=social&utm_brand=wired&utm_source=twitter
- De fet, des que es va anunciar per primera vegada, les persones expertes en ciberseguretat han assenyalat que és relativament senzill instal·lar programari maliciós per accedir a l'historial complet de l'usuari i, és clar, l'anunci de *Recall* s'ha tornat en un nou malson.
- En aquest sentit, mentre l'empresa Microsoft es mostra segura de la seva fiabilitat, alguns pirates informàtics ja han demostrat a través d'una eina o prova de concepte anomenada #TotalRecall que es pot desviar immediatament tot l'historial de l'usuari registrat per la funció.
- A més, val a dir que malgrat que inicialment calia l'anomenada "escalada de privilegis" per accedir-hi totalment com "administradors", alguns investigadors (en aquest cas de Google) han trobat el mètode per accedir a totes les dades de *Recall* sense privilegis d'administrador.
- Per tant, ens trobem de nou davant d'un sistema d'IA de vigilància que no tan sols erosiona la privacitat sinó que es mostra clarament susceptible a problemes de seguretat, una recepta ideal per malmetre encara més la confiança dels usuaris.
- <https://www.wired.com/story/microsoft-windows-recall-privilege-escalation/>





- PD1: Finalment sembla que podem afegir que la funció de captura de pantalla silenciosa habilitada per IA en el sistema Windows de Microsoft es desactivarà de manera predeterminada quan es publiqui a finals de mes. Un nou episodi malentès del famós *Release Early and Release Often*.
- PD2: Pels que són curiosos amb el *RERO* i volen saber el que (realment) significa. És clar, molt aplicable en aquest context.
- <https://zhiminzhan.medium.com/release-early-release-often-clarified-e73fa8931e05>

