

Sú smart hodinky naozaj bezpečné? V tomto newsletteri sa dozviete, aké hrozby môžu tieto zariadenia predstavovať, ako ovplyvňujú vaše dáta a čo môžete urobiť, aby ste sa pred nimi ochránili. Prezradíme vám aj praktické tipy, ako minimalizovať riziká a vyhnúť sa nepozorovaným útokom, ktoré môžu ohroziť vašu bezpečnosť.



Viete, ako sú na tom smart hodinky s bezpečnosťou?

Myslíte si, že vaše najcitlivejšie dáta sú v bezpečí vo "vzduchom oddelených" (air-gapped) systémoch? Mýlite sa! Výskumníci z Ben-Gurionovej univerzity odhalili šokujúci útok s názvom SmartAttack, ktorý dokáže obísť aj tie najprísnejšie bezpečnostné opatrenia a preniknúť do systémov, ktoré sú fyzicky odpojené od internetu.

Ako to funguje? Pripravte sa na prekvapenie!

SmartAttack využíva neuveriteľne sofistikovaný a nenápadný trik:

- **Neviditeľné signály:** Malvér nainštalovaný v cieľovom počítači s ochrannou vzduchovou medzerou dokáže kódovať citlivé dáta (heslá, šifrovacie kľúče, dokumenty) do ultrazvukových vln. Tieto zvuky sú pre ľudské uši úplne nepočuteľné (18-22 kHz) a prenášajú dáta pomocou špecifických frekvenčných párov.
- **Hodinky ako špión:** Ak sú vaše inteligentné hodinky infikované malvérom, ich vstavaný mikrofón dokáže nepretržite monitorovať akustické spektrum, zachytiť a dekódovať tieto nepočuteľné signály! Využívajú pritom pokročilé algoritmy ako rýchla Fourierova transformácia (FFT) a Kalmanovo filtrovanie na kompenzáciu pohybu zápästia.
- **Dáta unikajú:** Akonáhle hodinky dešifrujú ukradnuté informácie, okamžite ich pošlú útočníkovi cez svoje vlastné pripojenie – Wi-Fi, Bluetooth alebo mobilné dáta. Týmto sa elegantne obchádza ochrana vzduchovou medzerou, dokonca aj na vzdialenosti vyše šesť metrov!

Prečo sú smart hodinky taká hrozba?

Na rozdiel od smartfónov, inteligentné hodinky predstavujú oveľa väčšie riziko, pretože:

- **Sú vždy s nami:** Máme ich neustále na zápästí, čo zaručuje ich blízkosť k potenciálnym cieľom.
- **Sú nenápadné:** V citlivých a zabezpečených oblastiach sú smartfóny často zakázané, no inteligentné hodinky sú prehliadané a vnímané ako bežné príslušenstvo.
- **Sú efektívne:** Aj keď sa to zdá neuveriteľné, dokonca aj nízka prenosová rýchlosť (5 bitov za sekundu) stačí na exfiltráciu citlivých kľúčov či prihlasovacích údajov s takmer nulovou chybovosťou!

SmartAttack: Budíček pre každého z nás!

Kybernetické hrozby sa neustále vyvíjajú – je čas prehodnotiť bezpečnostné protokoly.

Čo môžeme urobiť?

Obmedziť nositeľné zariadenia – Smart hodinky a iné wearables nemajú čo robiť v citlivých priestoroch.

Monitorovať ultrazvuk – Špeciálne systémy dokážu odhaliť prenosy na ultrazvukových frekvenciách.

Zvýšiť fyzickú ochranu – Reprodukory a mikrofóny v kritických systémoch? Radšej nie.

Použiť rušiacie technológie – Ultrazvukové rušičky môžu byť ďalšou vrstvou obrany.

SmartAttack nám ukazuje, že aj teoretické útoky majú potenciál. Aj keď sú zložité, ponúkajú nové cesty k úniku dát. Budme o krok vpred. **Kyberbezpečnosť nie je len IT téma – týka sa nás všetkých.**

