

Cyberattacchi e frigoriferi hackerati, quali sono i rischi per gli elettrodomestici di casa?

Descrizione

default watermark

(Adnkronos) â?? Lâ??ondata di attacchi informatici che nella notte tra lâ??1 e il 2 novembre 2026 ha portato fino a 50 gradi i banchi frigo di mezza Europa ha reso i frigoriferi hackerati un rischio reale. Dopo la Francia, colpita a ottobre, sono stati presi di mira supermercati in Belgio, Svezia, Estonia, Irlanda e anche in Sicilia. Ma cosa rischia chi possiede un elettrodomestico connesso e come puÃ² difendersi? A rispondere Achiropita Cicala di Immobiliare.it. La tecnologia che regola a distanza i banchi frigo Ã¨ arrivata anche nelle case, dove un frigorifero smart, a prima vista un semplice elettrodomestico, funziona come un piccolo computer collegato al router. Rispetto a un pc riceve molta meno attenzione sul fronte della sicurezza, specie nei modelli economici, dove le difese vengono sacrificate al prezzo.

Quando un estraneo entra nel dispositivo, le conseguenze possono essere diverse. Furto delle credenziali: il frigorifero Ã¨ collegato al tuo account e, se usi la stessa password altrove, lâ??aggressore puÃ² provarla sulla posta o sui social; accesso al resto della rete: un elettrodomestico violato diventa una porta dâ??ingresso verso il tuo pc e le app bancarie; abitudini svelate ai ladri: consumi e routine programmate indicano gli orari in cui sei fuori casa; cibo a rischio: chi controlla lâ??app puÃ² modificare il raffreddamento e gli alimenti potrebbero perdere la catena del freddo; arruolamento in una botnet: il dispositivo entra in una rete di apparecchi infettati e usa la tua connessione per inviare spam. Sembra fantascienza, ma i frigoriferi hackerati e arruolati in una botnet esistono da oltre dieci anni, tanto che tra fine 2013 e inizio 2014 piÃ¹ di 100.000 dispositivi, tra cui un frigorifero, spedirono oltre 750.000 e-mail malevole allâ??insaputa dei proprietari.

La storia dei frigoriferi hackerati comincia quasi sempre con una scansione automatica di Internet, durante la quale alcuni programmi cercano dispositivi raggiungibili e ancora protetti dalle credenziali di fabbrica. Una volta individuato il bersaglio, lâ??aggressore prova le combinazioni piÃ¹ comuni oppure sfrutta una falla nota, corretta dal produttore ma mai aggiornata dal proprietario. A quel punto lâ??intruso non danneggia nulla, anzi usa le normali funzioni dellâ??app, come la temperatura, oppure rimane nascosto per spiare la rete. Nelle abitazioni il punto piÃ¹ fragile Ã¨ spesso il router, perchÃ© una

rete Wi-Fi con password debole consente a chiunque sia nei paraggi di intercettare i dati che lâ??elettrodomestico scambia con il cloud. Nel 2015 alcuni ricercatori lo dimostrarono con un frigorifero smart che, collegato al calendario di Google senza verificare i certificati di sicurezza, rivelava la password di gmail.

Oltre al router, Ã¨ sensibile anche lâ??account cloud del produttore, visto che con la sua password si comanda il frigorifero ovunque. Lo stesso router, poi, puÃ² esporre il frigorifero con lâ??UPnP, una funzione attiva di serie su molti modelli che lascia agli apparecchi di casa aprire da soli un passaggio verso internet, senza chiedere nulla. Per le app Ã¨ una comoditÃ , perchÃ© funzionano senza configurazioni manuali, perÃ² cosÃ¬ il frigorifero diventa raggiungibile anche da fuori casa.

La buona notizia Ã¨ che per mettere la cucina al riparo dai frigoriferi hackerati sono sufficienti pochi minuti. Cinque, secondo gli esperti, le cose da fare:

1) Cambiare la password di fabbrica: le combinazioni predefinite circolano online, perciÃ² sceglila lunga e diversa per ogni apparecchio.

default watermark

2) Creare una rete ospiti sul router: riservata agli elettrodomestici, impedisce che unâ??eventuale violazione raggiunga pc e smartphone.

3) Attivare gli aggiornamenti automatici: ogni nuova versione del firmware chiude vulnerabilitÃ giÃ scoperte.

4) Disattivare lâ??accesso remoto: se non comandi il frigorifero da fuori casa, spegni anche lâ??UPnP del router.

5) Controllare il supporto prima di comprare: verifica per quanti anni il produttore garantisce gli aggiornamenti di sicurezza. Sul supporto qualcosa si muove anche in Europa, perchÃ© il cyber resilience act dallâ??11 settembre 2026 obbliga i fabbricanti a segnalare entro 24 ore le vulnerabilitÃ sfruttate.

La casa meglio configurata puÃ² tradirsi per una distrazione, e molte intrusioni partono da lÃ¬: non comprare un frigorifero smart usato senza resettarlo: lâ??account del vecchio proprietario potrebbe rimanere collegato allâ??apparecchio; non accettare in blocco i termini dâ??uso: spesso autorizzano la cessione dei tuoi dati a terze parti; scollega ciÃ² che non usi: un forno connesso di cui ignori le funzioni smart moltiplica inutilmente le vie dâ??accesso; non sottovalutare i segnali anomali: una connessione lenta o temperature cambiate da sole possono indicare unâ??intrusione; blocca sempre lo smartphone: senza codice, chiunque lo prenda in mano ha le chiavi di tutti i dispositivi. Il telefono, in fondo, Ã¨ il telecomando della casa, e proteggerlo vale quanto chiudere a chiave la porta dâ??ingresso.

â??

cronaca

webinfo@adnkronos.com (Web Info)

Categoria

1. Comunicati

Tag

1. Ultimora

Data di creazione
Novembre 10, 2026
Autore
redazione

default watermark