04-NOV-2026
da pag. 1-11 /foglio 1

il Giornale

Quotidiano - Dir. Resp.: Tommaso Cerno
Tiratura: 61128 Diffusione: 24512 Lettori: 279000 (Data Stampa 0006901)

DATA STAMPA
45° Anniversario

Data Stampa 0006901 Data Stampa 0006901

BLITZ COORDINATI IN UE

IL MANUALE BLOCCA-FRIGO

Basile e Sorbi

Pag. 10-11

Sul web la guida blocca-frigo E adesso si teme per le Poste

Il paradosso Il manuale per alterare le temperature circola in rete dall'inizio di agosto L'ipotesi della regia russa. L'agenzia Claroty: «Manomissioni possibili in soli 28 minuti»

La relazione, finita nelle mani degli hacker, è nata per denunciare le falle di sicurezza

Maria Sorbi

Cosa ci fa in rete il manuale tecnico che spiega come bloccare i frigoriferi dei supermercati? Circola da agosto e viene copiato e incollato da un gruppo di hacker all'altro. Sono le istruzioni per penetrare il sistema di sicurezza della grande distribuzione.

Un vademecum che spiega, passo per passo, come alterare le temperature e agire sulla catena del gelo. Titolo: «Bloccare il controller, scongelare gli alimenti: scoperta di vulnerabilità nei controller per refrigerazione Danfoss». In realtà il manuale nasce come alert per «tappare» le falle del sistema informatico e aumentare la protezione dei congelatori. Tutto comincia il 9 agosto, quando viene verificata la vulnerabilità dei sistemi di sicurezza. Viene scritta una relazione che evidentemente finisce nelle mani sbagliate. E quasi 3mila dispositivi non vengono aggiornati nei 63 giorni precedenti l'attacco in Francia. Qualcuno lo sa e sfrutta le maglie larghe del sistema per colpire gli impianti Danfoss e Dixell Xweb esposti su Internet, proprio quelli che le aziende rendono accessibili da remoto per «comodità di manutenzione».

Cosa significa tutto questo? Che probabilmente a colpire sono stati anche gruppi di hacker minori. A fare da «supervisori» sembra ci siano il gruppo Z Pentest e, anche stavolta, i filorussi di NoName057. Ma probabilmente le firme dei blitz sono molteplici vista la quantità di informazioni guida facili da reperire. Il vero problema non sono i pirati della rete ma i responsabili dei sistemi di sicurezza, che non aggiornano per tempo le protezioni. Se il sistema di scudo funzionasse davvero, la vulnerabilità verrebbe scoperta ben prima di un dossier.

Claroty, azienda di cybersecurity autrice della ricerca sulle falle del sistema informatico dei frigo, dichiara che, quando ci si è accorti della debolezza delle protezioni, era possibile «ottenere l'esecuzione di comandi in circa 28 minuti, con un costo di appena 6 dollari per l'utilizzo dell'AI». Di fatto, gli hacker arrivano con pochi passaggi all'interfaccia per la gestione degli impianti, modificano i parametri della temperatura e attivano la modalità di sbrinamento continuo. Niente malware, nessun ransomware, nessuna richiesta di riscatto. Solo il normale utilizzo delle funzioni che il produttore aveva programmato per gestire i frigoriferi.

Sugli attacchi indagano anche gli Stati Uniti, i primi a essere colpiti la scorsa estate. Già lo scorso dicembre i procuratori federali di Los Angeles hanno accusato una donna ucraina di far parte di un gruppo di hacker che nel 2024 ha messo fuori uso il sistema di refrigerazione di un impianto di lavorazione della carne, rovinando oltre 2mila libbre di carne. Ma se il settore alimentare è sull'attenti e si è mosso per proteggersi sia in Italia sia in Europa, in rete vengono annunciati nuovi obbiettivi. I NoName057 dichiarano di essere in possesso di dati sensibili rubati alle Poste. Per ora quelle francesi.





ARTICOLO NON CEDIBILE AD ALTRI AD USO ESCLUSIVO DEL CLIENTE CHE LO RICEVE - DS6901 - S.30524 - L.1992 - T.1748