PuntoSicuro

ARTICOLO DI PUNTOSICURO

Anno 28 - numero 6172 di Mercoledì 14 ottobre 2026

Attenzione ad usare reti Wi-Fi in alberghi e sale conferenze

Giunge dagli Stati Uniti la notizia che criminali informatici riescono a cambiare le impostazioni degli apparati Wi-Fi in luoghi pubblici per reindirizzare gli utenti a siti fraudolenti.

Questi attacchi sono cominciati a giugno di quest'anno e si sono allargati a macchia d'olio, colpendo organismi operanti in vari settori come i settori finanziari, i servizi professionali, la sanità, l'energia ed altre attività.

Una compagnia specializzata in analisi di frodi informatiche ha constatato come numerosi accessi Wi-Fi, in molte città degli Stati Uniti, nonché in altre regioni del mondo, come l'India e l'Arabia Saudita, sono stati compromessi da criminali informatici.

Poiché in genere queste reti Wi-Fi sono utilizzate in riunioni ed eventi di una certa rilevanza, la manomissione degli account Microsoft 365 può permettere agli attaccanti di accedere a informazioni sensibili dei soggetti attaccati.

Gli esperti hanno rilevato come questa tipologia di attacco prenda di mira numerosi contesti, a riprova del fatto che non sia un attacco mirato, ma un attacco a largo spettro.

Pubblicità

Secondo gli esperti è possibile che questa tipologia di attacco abbia avuto origine in Russia e da lì si sia propagata in altri paesi.

Una volta che l'attaccante acquisisce i livelli di accesso di un amministratore, egli può modificare le impostazioni DNS dell'accesso, per reindirizzare i soggetti che si collegano ad altri siti, sotto diretto controllo dell'attaccante informatico.

Gli investigatori hanno individuato con certezza almeno quattro diversi domini, che possono simulare domini legittimi:

m365-owa[.]com, owa-ms365[.]com, ms365-device[.]com, and ms365-live[.]com.

In alcuni casi, gli investigatori hanno rilevato come il flusso dei dati di autentica del collegamento viene reindirizzato ad un sito Microsoft, con un prompt. Quando l'utente approva il prompt, inconsciamente autorizza l'avvio di una sessione di collegamento, interamente gestita dall'attaccante.

Poiché siamo certi che molti dei nostri lettori, quando si trovano coinvolti in situazioni come quelle illustrate, potrebbero non effettuare accurati controlli circa la legittimità del collegamento Wi-Fi, abbiamo ritenuto opportuno divulgare questa importante notizia.

Adalberto Biasiotti


Licenza Creative Commons
I contenuti presenti sul sito PuntoSicuro non possono essere utilizzati al fine di addestrare sistemi di intelligenza artificiale.
