Vendesi auto, ma è una minaccia cyber per colpire diplomatici

La **Unit 42 di Palo Alto Networks** ha pubblicato una nuova ricerca su attori di minacce russi, associati al gruppo denominato *Fighting Ursa* (alias *APT 28*), che hanno utilizzato un annuncio di vendita di un veicolo come esca di phishing per distribuire il malware HeadLace. *Fighting Ursa (alias APT28, Fancy Bear e Sofacy)* è stato associato all'intelligence militare russa e classificato come minaccia persistente avanzata (APT).

I dettagli della campagna, iniziata nel marzo 2024, indicano che il gruppo ha preso di mira soprattutto figure diplomatiche, affidandosi a servizi pubblici e gratuiti per ospitare le varie fasi dell'attacco.

I temi del phishing che sfruttano veicoli in vendita sono utilizzati dagli attori russi da anni. Perché? Perché funzionano. Queste esche tendono a funzionare anche con i diplomatici, inducendo gli obiettivi a cliccare sul contenuto pericoloso. Il gruppo Fighting Ursa è noto perché ripropone tattiche di successo, anche sfruttando continuamente vulnerabilità note da 20 mesi, nonostante la loro copertura fosse già saltata.

Già nel 2023 Unit 42 aveva scoperto un altro gruppo di minacce, Cloaked Ursa (APT29), che riproponeva un annuncio di vendita di una BMW per colpire le missioni diplomatiche in Ucraina. Questa campagna non è direttamente collegata alla campagna Fighting Ursa, tuttavia, la somiglianza delle tattiche indica comportamenti noti.

Tutti i dettagli della campagna sono disponibili qui.

Leggi le altre notizie sull’home page di Key4biz

https://www.key4biz.it/vendesi-auto-ma-e-una-minaccia-cyber-per-colpire-diplomatici/500799/