Milano, 13 marzo 2024 - Quante volte ci è capitato di usare un codice QR per iscriverci a una newsletter, per leggere la programmazione di un cinema o magari semplicemente per accedere al menu di un ristorante?

Dall’avvento della pandemia si sono moltiplicate le occasioni di utilizzo dei codici QR, grazie ai quali è possibile ottenere informazioni senza alcun contatto fisico; ma è proprio in virtù di tale diffusione che i criminali informatici hanno trovato uno strumento in più, efficace e temibilissimo, per sferrare i loro attacchi.

Secondo l’ultimo report trimestrale di Cisco Talos, la più grande organizzazione privata di intelligence al mondo dedicata alla cybersecurity, nel corso del 2023 è stato registrato un aumento significativo di attacchi phishing tramite la scansione di codici QR. Cisco Talos ha dovuto gestire una campagna di phishing che induceva le vittime a scansionare dei codici QR dannosi incorporati nelle e-mail, e che portavano i malcapitati all'esecuzione inconsapevole di malware.

Un altro tipo di attacco è invece l’invio di e-mail di spear-phishing a una persona fisica o a

un'organizzazione, mail contenenti codici QR che puntavano a false pagine di accesso a Microsoft Office 365 al fine di rubare le credenziali di accesso dell'utente. È quanto mai importante sottolineare che gli attacchi tramite codice QR sono particolarmente pericolosi, poiché utilizzano come vettore di attacco il dispositivo mobile della vittima, molto spesso dotato di minore protezione.

Come funzionano gli attacchi tramite codici QR?

Un attacco di phishing tradizionale prevede che la vittima apra un link o un allegato in modo da atterrare su una pagina controllata dall'aggressore. Di solito sono messaggi destinati a persone che hanno familiarità con l'utilizzo della posta elettronica e che normalmente aprono allegati o cliccano su un link.

Nel caso di attacchi tramite codice QR, l'hacker inserisce il codice nel corpo dell'e-mail con l'obiettivo di farlo scansionare tramite un'applicazione o tramite la fotocamera del dispositivo mobile. Una volta cliccato sul link malevolo, si apre una pagina di login sviluppata appositamente per rubare le credenziali, o un allegato che installa un malware sul dispositivo.

Perché sono così pericolosi?

Molti computer e dispositivi aziendali sono dotati di strumenti di sicurezza integrati, progettati per rilevare il phishing e impedire agli utenti di aprire link dannosi. Tuttavia, quando un utente utilizza un dispositivo personale, questi strumenti di difesa non sono più efficaci. Ciò accade perché i sistemi di sicurezza aziendali e di monitoraggio hanno meno controllo e visibilità sui dispositivi personali. Inoltre non tutte le soluzioni di sicurezza per la posta elettronica sono in grado di rilevare i codici QR dannosi.

Ma c'è di più. Con l'aumento del lavoro a distanza, un sempre maggior numero di dipendenti accede alle informazioni aziendali attraverso i dispositivi mobili. Secondo il recente report Not (Cyber) Safe for Work 2023, un'indagine quantitativa condotta dalla società di cybersecurity Agency, il 97% degli intervistati accede agli account di lavoro utilizzando dispositivi personali.

Come difendersi

Ecco alcuni consigli di Cisco Talos per difendersi dagli attacchi di phishing basati sui codici QR:

- implementare una piattaforma di gestione dei dispositivi mobili (MDM) o uno strumento di sicurezza mobile su tutti i dispositivi mobili non gestiti che hanno accesso alle informazioni aziendali;
- una soluzione di sicurezza sviluppata appositamente per le e-mail è in grado di rilevare questa tipologia di attacchi;
- la formazione degli utenti è fondamentale per prevenire gli attacchi di phishing basati sui codici QR. Le aziende devono assicurarsi che tutti i dipendenti siano istruiti sui pericoli degli attacchi di phishing e sul crescente utilizzo dei codici QR:
    - i codici QR dannosi utilizzano spesso un’immagine di scarsa qualità o possono apparire leggermente sfocati;
    - gli scanner di codici QR spesso forniscono un'anteprima del link a cui punta il codice, è molto importante prestare attenzione e visitare solo pagine web affidabili con URL riconoscibili;
    - le e-mail di phishing contengono spesso errori di battitura o grammaticali;
- l'utilizzo di strumenti di autenticazione a più fattori possono impedire il furto di credenziali, che spesso sono il punto di ingresso nei sistemi aziendali.