# Chosen Brick: il malware iraniano che spia dissidenti e giornalisti nel mondo

Data: Invalid Date | Autore: Redazione


Un'operazione di **spionaggio informatico** su scala globale è stata smascherata dalle agenzie di **cybersicurezza** di **Regno Unito**, **Stati Uniti** e **Paesi Bassi**. Il software malevolo, denominato **CHOSEN BRICK**, è stato attribuito all'**intelligence iraniana** e sarebbe stato utilizzato per colpire **dissidenti**, **attivisti** e **giornalisti** in diverse aree del mondo.

## Un attacco mirato e subdolo

Secondo quanto riportato dalle autorità, gli hacker si sarebbero spacciati per **contatti affidabili** al fine di guadagnare la fiducia delle vittime. La tecnica principale è il **spear-phishing**, condotto attraverso piattaforme di messaggistica molto diffuse come **WhatsApp** e **Telegram**. In questo modo, gli aggressori inducevano le persone a scaricare **documenti falsi** che, una volta aperti, installavano il **malware** sui dispositivi.

## Le capacità del malware

Una volta installato, **CHOSEN BRICK** è in grado di **sottrarre e-mail**, **messaggi** e **contatti** dalla vittima. Inoltre, può acquisire **screenshot** dello schermo e attivare il **microfono** per captare conversazioni ambientali. Si tratta di un livello di intrusione che mette a serio rischio la **privacy** e la sicurezza dei bersagli, spesso figure critiche verso il regime iraniano.

## Implicazioni per la sicurezza internazionale

L'attribuzione ufficiale da parte di tre paesi occidentali rappresenta un passo importante nella lotta contro il **cyber-spionaggio** di matrice statale. Le autorità invitano i potenziali bersagli, in particolare **giornalisti**, **attivisti** e **dissidenti**, a prestare massima attenzione a messaggi sospetti e a non aprire file provenienti da fonti non verificate. La vicenda evidenzia ancora una volta come le **piattaforme di messaggistica** siano diventate un terreno fertile per operazioni di **guerra informatica**.