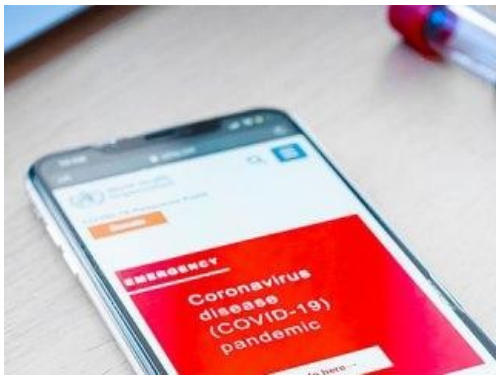
I NOSTRI DATI: un patrimonio da dover tutelare. SEMPRE!

Mentre “Immuni” fa il suo esordio sugli store di Apple e Google, una campagna di hacking che prova a sfruttare questo evento investe l’Italia. A renderlo noto è l’Agid-Cert, la struttura del governo che si occupa di cybersicurezza. Non si ha contezza, al momento, di quanti cittadini siano realmente coinvolti e a rischio. Ma la storia è abbastanza emblematica, e necessita di grande attenzione.



In sostanza, si tratta di una campagna di phishing – quindi attiva con le classiche mail-esca che puntano a ingannare chi le riceve – che prova a sfruttare l’esordio di Immuni, l’app per il contact tracing scelta dal governo italiano che proprio in queste ore è in fase di rilascio. All’interno della mail infetta, si prova a convincere l’utente a cliccare su un link che porta a un dominio creato ad arte per replicare i contenuti della Federazione Ordini Farmacisti Italiani (FOFI.it). In realtà basta un click per finire sul file eseguibile “Immuni.exe” che al suo interno contiene un malware chiamato FuckUnicorn.

È un virus di tipo ransomware – di quelli che bloccano i computer e chiedono un riscatto per sbloccarli – che una volta eseguito mostra una finta dashboard con i risultati della contaminazione da Covid-19. E mentre l’utente si trova davanti questa mappa, il malware provvede a cifrare i file presenti sul sistema Windows della vittima e a rinominarli assegnando l’estensione “.fuckunicornhtrhrtjrjy”. Alla fine dei giochi, sullo schermo compare il classico file di testo con le istruzioni per il riscatto, che ammonta a 300 euro in bitcoin per liberare i file cifrati, quindi il pc. Come nella maggior parte dei casi, quando c’è di mezzo un ransomware, pagare il riscatto è del tutto inutile. La transazione è protetta dall’anonimato tipico delle criptovalute. E mai nessun cybercriminale vi verrà in aiuto.

Fonte: Nòva Il Sole 24 Ore