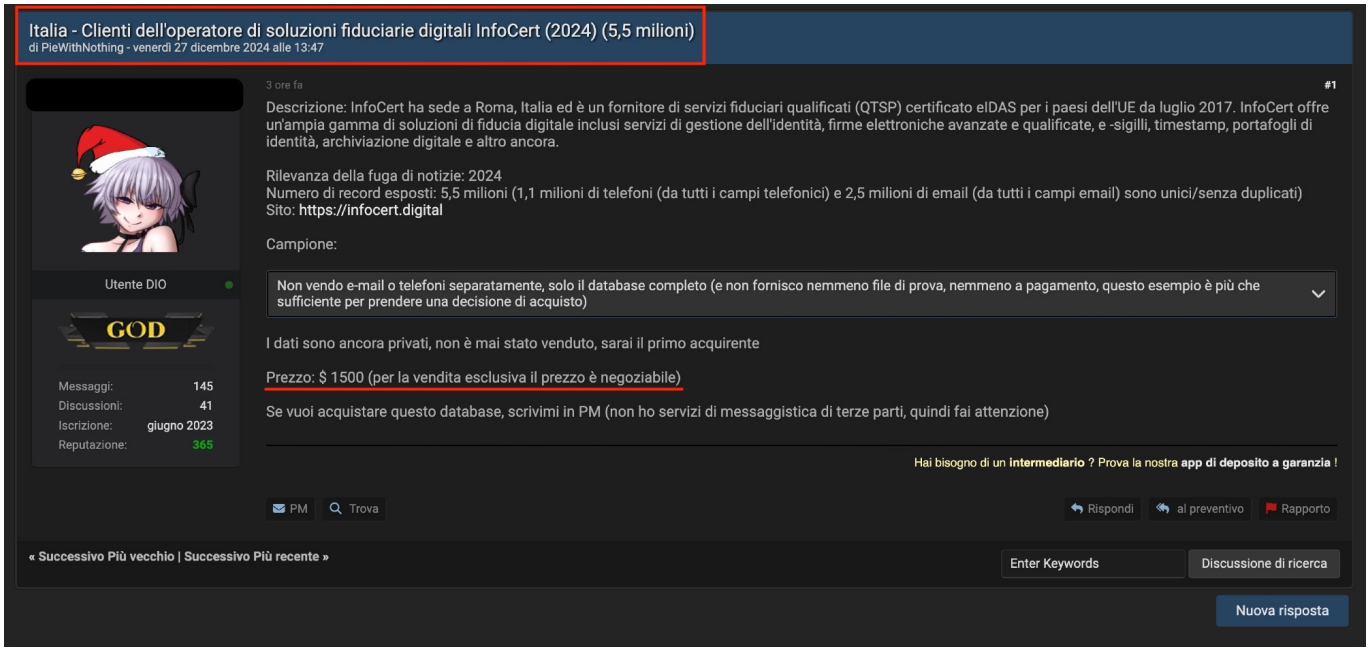
Hacker colpiscono InfoCert, azienda specializzata in SPID e identità digitali

InfoCert, una delle principali fornitrici europee di **identità digitali**, è caduta **vittima di un attacco hacker**, con i dati sottratti che sono ormai in vendita sul web. L'incidente rappresenta una potenziale violazione della sicurezza informatica e della privacy ed è stato individuato il **27 dicembre**. Tuttavia, non risulta che la società abbia ancora notificato formalmente l'accaduto al Garante della Privacy, il quale sarà chiamato a esaminare la vicenda per individuare eventuali criticità, negligenze e responsabilità.

La notizia dell'attacco è emersa inizialmente da un comunicato distribuito direttamente sul portale di InfoCert. La decisione di rendere pubblica l'informazione sembra essere stata dettata dalla necessità di rispondere alla circolazione delle notizie emerse sui siti di pirateria informatica, dove i dati rubati erano già stati resi disponibili. Nel comunicato, InfoCert ha confermato "la pubblicazione non autorizzata di **dati personali relativi a clienti censiti**". L'azienda ha dunque tenuto a precisare più volte che la violazione non è stata causata da falle interne, ma da **una vulnerabilità legata a un fornitore terzo**. In particolare, InfoCert ha sottolineato che l'attacco "non ha però compromesso l'integrità dei sistemi di InfoCert" e che "nessuna credenziale di accesso ai servizi InfoCert e/o password di accesso agli stessi è stata compromessa in tale attacco".

Questa precisazione potrebbe rappresentare un tentativo di rassicurare clienti e partner sul fatto che i servizi principali dell'azienda restano sicuri, tuttavia la compromissione di dati personali, **anche se indiretta**, costituirebbe comunque una violazione grave. Ancor più se si considera che la dichiarazione non trova pieno riscontro nelle comunicazioni espresse dagli hacker. Secondo un annuncio emerso su di un forum specializzato in fughe di dati, l'azienda subappaltante si sarebbe vista sottrarre **5,5 milioni di record**. Tra questi, **1,1 milioni di numeri telefonici e 2,5 milioni di email**, elementi che possono fare concretamente parte delle credenziali di accesso a SPID, PEC e la firma digitale, ovvero i servizi offerti da InfoCert. Complessivamente, si teorizza che il pacchetto dati contenga anche **nomi, cognomi, codici fiscali**, tutti trafugati da un archivio associabile al Ticketing System, una soluzione che viene tipicamente adoperata nel campo dell'assistenza ai clienti. Il tutto viene offerto sul banco in un singolo blocco, alla cifra di 1.500 dollari.

Hacker colpiscono InfoCert, azienda specializzata in SPID e identità digitali



In passato, InfoCert era già stata ritenuta **carente nel campo della sicurezza**. Il 9 maggio 2024, il Garante della Privacy aveva infatti emesso un provvedimento – in attesa del giudizio di opposizione – relativo a criticità riscontrate nel 2019 nella gestione delle caselle di posta elettronica certificata dell'Ordine degli Avvocati di Roma. Secondo quanto riportato dall'autorità, InfoCert non avrebbe adottato all'epoca le misure adeguate per garantire un trattamento dei dati conforme ai regolamenti europei.

InfoCert è classificata come Qualified Trust Service Provider (QTSP), ovvero una fornitrice di servizi fiduciari qualificati, ed è anche un Identity Provider di rilevanza internazionale. Che una realtà tanto accreditata sia stata coinvolta in una fuga di dati di tale portata solleva inevitabilmente riflessioni importanti sulla gestione dei dati sensibili da parte delle aziende. Tra gli aspetti da approfondire emergono la tendenza a subappaltare archivi delicati, la necessità di maggiore trasparenza nelle notifiche di incidenti e, soprattutto, la "responsabilizzazione" dei gestori nel caso di problemi, ancor più se si considera che simili problematiche non possono che ledere la fiducia del pubblico e danneggiare coloro che già si affidano a simili strumenti.

[di Walter Ferri]