Nexi e i database pubblicati su Pastebin, dubbi sul data-leak. La società, “Nessuna violazione informatica”

Ieri sera ***Pastebin***, popolare piattaforma di condivisione di codici sorgente, software, data set e altri contenuti a volte molto sensibili, mostrava al suo pubblico una serie di **elenchi di utenti** riferiti a **Nexi**. Elenchi completi di nomi e cognomi, indirizzi, codici fiscali, addirittura il numero del telefono personale. Insomma, veri e propri database completi di clienti del gigante dei pagamenti digitali in Italia, prova di un **attacco informatico** in piena regola.

> *https://t.co/XSImXbmMLA*
>
> *— Pawel ‘okno’ Zorzan Urban (@pawelzorzan) July 29, 2019*

Sul fatto si sta ovviamente cercando di fare luce, perché i dubbi sull’autenticità dell’attacco sono ancora molti. L’*ethical hacker* **Pawel Zorzan Urban** si è già messo al lavoro e ieri sera è stato tra i primi a far girare la notizia, rilanciando il messaggio dei presunti cyber criminali: “*Dati personali clienti Nexi Spa. Un saluto a Paolo Bertoluzzo, Luca Biancardi, Alessandro Cocciolo. Un abbraccio dagli schiavetti di Montefeltro*”.

Si tratta davvero della traccia di un attacco hacker?
Si tratta di ***data breach*** e ***data leak*** assieme? Quindi di sottrazione illecita e divulgazione non autorizzata di dati sensibili?

A giudicare dal messaggio, come ha anche suggerito Zorzan Urban, si potrebbe dedurre che l’attacco possa provenire

dall'interno, o che comunque sia un fatto nato e consumato dentro Nexi (Vendetta personale? Cliente insoddisfatto? Faida interna?).
Ci sono riferimenti a singole persone e a quello che pare "*un gruppo*" specifico di persone ("*gli schiavetti di Montefeltro*").
Su questo indagheranno Polizia Postale e la stessa società vittima dell'ipotetico attacco.

Al momento, a seguito dell'analisi condotta a caldo da Zorzan Urban, "*L'analisi delle prime porzioni di database ha portato ad un totale di 14.241 record privati esposti. 1.709 record comprendono numeri di cellulare associati a persone fisiche*".
Si parla di **diverse liste con migliaia di utenti, oltre 10.000 in totale** quelli che parrebbero coinvolti.

È anche vero, però, che nelle ultime ore, ulteriori indagini hanno portato ad un "*ridimensionamento*" dell'evento. Come ha scritto stamattina Simone Cosimi su *La Repubblica*: "*Ancora, potrebbe trattarsi di un sottoinsieme, cioè dei clienti di uno specifico servizio di Nexi, o più semplicemente di informazioni datate, visto che nel corso della notte diversi utenti hanno analizzato gli elenchi, che non contengono comunque informazioni finanziarie di alcun genere, e non sono riusciti a individuarsi*".

In base all'ultimo aggiornamento diffuso sulla pagina LinkedIn di Zorzan Urban, **sembra che i suddetti link incriminati siano scomparsi**: "*Aggiornamento ore 03:10 30 Luglio 2019 – Rimossi link da Pastebin*".

Stamattina, su TGCom24 è stata pubblicata la **notizia della denuncia di Nexi alle autorità** per "*presunto attacco hacker ai suoi danni, senza rilevare però alcuna violazione ai propri sistemi informatici e, soprattutto, alla sicurezza delle carte*

di pagamento da essa gestite”.
Sembrerebbe inoltre che Nexi abbia deciso di dare notizia del presunto attacco su un sito internet straniero, parlando di “*un post anonimo contenente una lista di circa 18mila nominativi corredati da dati personali di presunti clienti Nexi*“.
“In molti casi – secondo quanto dichiarato da Nexi e riportato dall’Ansa – *i dati anagrafici contenuti nel sito non trovavano corrispondenza con quelli contenuti nei propri sistemi informatici*”. Questo non ha impedito all’Azienda di “*diffidare immediatamente il sito internet che ha pubblicato i dati*”, che a sua volta li ha “*prontamente rimossi*”.

Nexi gestisce più di 41 milioni di carte di credito nel nostro Paese, attraverso 150 Istituti bancari partner (circa l’80% degli sportelli dell’interno sistema bancario nazionale), 1,4 milioni di terminali pos e 13.400 atm. Da aprile 2019 è una società quotata in Borsa.

> *Nexi e i database pubblicati su Pastebin, dubbi sul data-leak. La società, “Nessuna violazione informatica”*