– RELAZIONE ATTACCO THETA –

Il 19/02/2025 ci siamo imbattuti in un file non autorizzato proveniente dalla rete esterna.
Si trattava di una cartella in formato **ZIP** e, una volta estratto il contenuto, abbiamo trovato al suo interno diversi script (alcuni scritti in linguaggio **Python**) e alcune foto criptate.

In uno di questi script **Python**, abbiamo trovato la prima password, utile per decriptare la prima foto. All'interno di essa era presente un indovinello, la cui soluzione ci ha permesso di ottenere la password necessaria per decriptare la seconda foto.

Successivamente, in ogni immagine, ci siamo imbattuti in nuovi indovinelli finalizzati a trovare la password per decriptare la foto successiva.

Arrivati all'ultima immagine, ci siamo ritrovati con **solo metà della password**, mentre l'altra metà era nascosta sotto forma di indovinello in uno degli script **Python**. Una volta decriptata, è apparso un messaggio da parte degli attaccanti che avvertiva dello svuotamento dei conti bancari di **THETA** e conteneva un link a un video su **YouTube**.

All'interno del video abbiamo trovato un'ulteriore password, che ci ha permesso di decriptare le restanti immagini contenute in un'altra cartella. Una volta decriptate queste ultime, è apparso un altro messaggio da parte degli attaccanti, accompagnato dall'immagine di una medaglia con la scritta **"THETA POWNED"**.

Già dal primo messaggio, abbiamo tempestivamente avvisato l'azienda **THETA** dell'accaduto. L'azienda, a sua volta, ha immediatamente contattato le autorità competenti, bloccando i movimenti bancari. Grazie a un'operazione internazionale di polizia, è stato possibile recuperare gran parte del denaro sottratto.