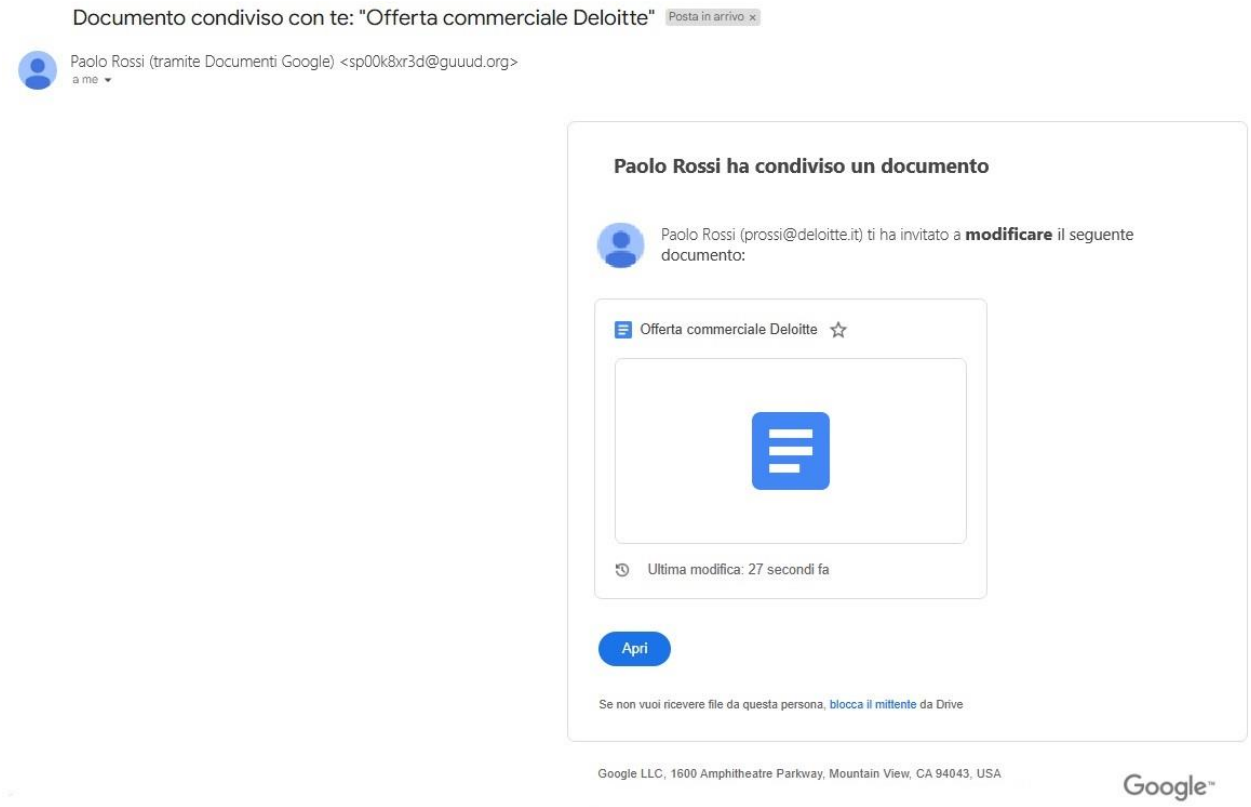
Ho costruito l'email di phishing facendo finta di essere uno dei venditori di Deloitte che condivide con altri collaboratori un'offerta commerciale.

Ho supposto che Deloitte utilizzi i Documenti di Google in condivisione come strumento di collaborazione aziendale, quindi è una prassi abbastanza frequente quella di ricevere questo tipo di email da parte dei colleghi.



Il tasto "Apri" fa partire il download di un file .doc contenente un ransomware che cripta tutti i file del PC della vittima e sostituisce lo sfondo del desktop con un messaggio che richiede il pagamento entro 30 giorni di 10 Ethereum sul portafoglio dell'attaccante altrimenti i file verranno distrutti.

Gli elementi che fanno capire che si tratta di una mail di phishing sono diversi:

Mittente della mail: il messaggio dovrebbe arrivare da una mail di Google che si occupa del servizio di condivisione documenti (in genere è drive-shares-dm-noreply@google.com) o quanto meno dovrebbe arrivare da prossi@deloitte.it, la mail del collega.
Immagine profilo: è sgranata e di solito un'azienda come Deloitte obbliga i dipendenti ad impostare una foto profilo o quanto meno imposta di default il proprio logo come avatar di tutti i profili dei dipendenti.

Font: non sono coerenti in tutto il corpo della mail, segno che sono state effettuate delle modifiche e non proviene dal sistema di Google.