martedì 7 gennaio 2025

PRATICA S5/L1

L’esercizio di oggi prevede una simulazione della fase di raccolta informazioni utilizzando dati pubblici su un target a scelta.
Lo scopo dell’esercizio è familiarizzare con i principali strumenti della fase di information gathering.

1. ***SELEZIONE DEL TARGET***

- Ho scelto come target **Revolut**, azienda innovativa nell’ambito tecnologico-finanziario che offre servizi bancari digitali.

2. ***RACCOLTA DELLE INFORMAZIONI CON GOOGLE***

- Per questa fase, ho utilizzato ricerche Google avanzate (**query**), applicando operatori specifici per ottenere informazioni mirate.

1. **site:revolut.com** per trovare informazioni di base sull’azienda.
2. **site:revolut.com “contacts”** per trovare informazioni sui contatti.
3. **filetype:pdf site:revolut.com financial report** per individuare report annuali finanziari e ottenere informazioni sul flusso di lavoro e di crescita.
4. **inurl:”privacy” site:revolut.com** per ottenere informazioni sulle politiche di sicurezza vigenti.
5. **site:revolut.com intext:”password”** per verificare la presenza di informazioni sensibili in chiaro.
6. **revolut “vulnerability report”** per ottenere informazioni su vulnerabilità esistenti o modalità di segnalazione.
7. **site:github.com Revolut** per ottenere eventuale codice sorgente o bug individuati dagli utenti.

8. **revolut site:shodan.io** per verificare eventuali dispositivi o sistemi esposti.
9. **revolut site:pastebin.com** per evidenziare fughe di dati.
10. **revolut feedback OR Revolut "negative reviews"** per ottenere informazioni sulla reputazione e sui problemi degli utenti.

3. *RISULTATI*

• Ho ottenuto diversi risultati per ognuna delle ricerche elencate sopra:

1. Informazioni di base sull'azienda come:
   - CEO, Nikolay Storonsky.
   - Fondazione, Luglio 2015.
   - Dipendenti, 7500.
   - Fatturato, 2,1 mld.
   - Sede principale, Londra

2. Non espongono numeri di telefono ma si affidano principalmente all'assistenza via chatbot.

3. Diversi PDF contenenti report annuali dove si espongono diverse figure interne in ruoli importanti dell'azienda, come analisi dei rischi. Comunicazioni sulla gestione dei flussi di lavoro per i vari dipartimenti.

4. Informativa sulla privacy appena aggiornata al 1 Gennaio 2025, che modifica la gestione dei dati degli utenti. Diversi post di Reddit di utenti che ritengono che la privacy policy sia poco chiara e accusano Revolut di obbligare il caricamento di informazioni non necessarie, il che potrebbe suggerire un uso imprudente degli ultimi.

5. Nessuna password di account esposta

6. Revolut utilizza un sistema basato su ricompense per ottenere informazioni sulle proprie vulnerabilità o bug da parte degli utenti esterni, promette ricompense in denaro non molto chiare..

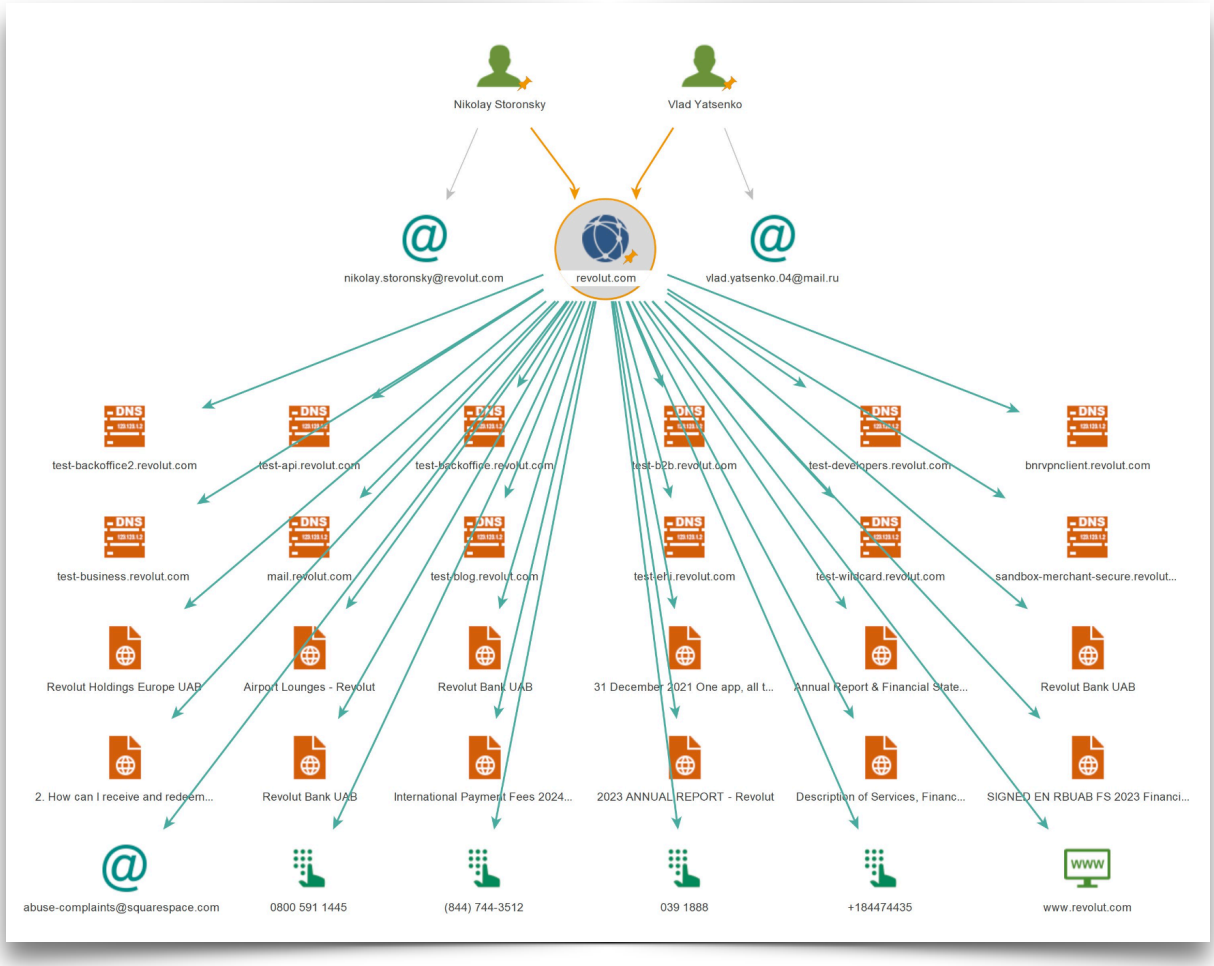
7. Sulla piattaforma Github nessun codice debole esposto.

8. shodan.io manifesta la presenza di diversi server, alcuni di questi lavorano con porta 80 aperta.

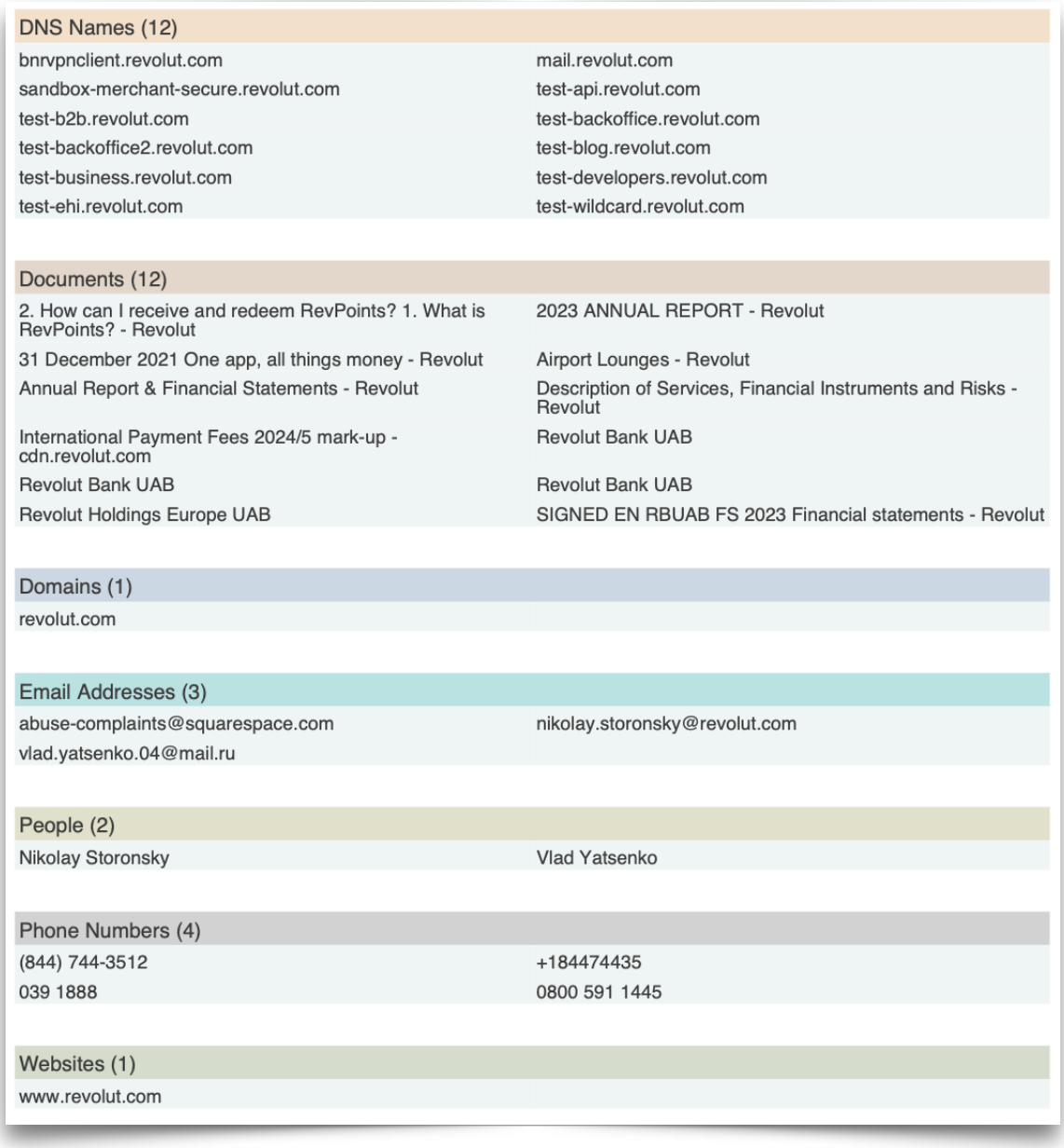
9. L'informazione più grave che ho trovato; su pastebin ci sono liste di carte di credito rilasciate da revolut delle quali si conosce ogni cosa, proprietario, numero, cvv, paese…

10. Le recensioni negative si basano su quanto discusso prima, ovvero di una policy poco chiara che addirittura sembra essere di difficile comprensione anche da parte dell'assistenza stessa.

- Ho inserito le informazioni ottenute su Maltego e ho ottenuto delle nuove informazioni come si vede dalla mappa:



Si notano **DNS**, **numeri di telefono** associati al dominio, **fondatori**, **indirizzi email dei fondatori**, **documenti.**



DNS Names (12)	
bnrvpnclient.revolut.com	mail.revolut.com
sandbox-merchant-secure.revolut.com	test-api.revolut.com
test-b2b.revolut.com	test-backoffice.revolut.com
test-backoffice2.revolut.com	test-blog.revolut.com
test-business.revolut.com	test-developers.revolut.com
test-ehi.revolut.com	test-wildcard.revolut.com

Documents (12)	
2. How can I receive and redeem RevPoints? 1. What is RevPoints? - Revolut	2023 ANNUAL REPORT - Revolut
31 December 2021 One app, all things money - Revolut	Airport Lounges - Revolut
Annual Report & Financial Statements - Revolut	Description of Services, Financial Instruments and Risks - Revolut
International Payment Fees 2024/5 mark-up - cdn.revolut.com	Revolut Bank UAB
Revolut Bank UAB	Revolut Bank UAB
Revolut Holdings Europe UAB	SIGNED EN RBUAB FS 2023 Financial statements - Revolut

Domains (1)
revolut.com

Email Addresses (3)	
abuse-complaints@squarespace.com	nikolay.storonsky@revolut.com
vlad.yatsenko.04@mail.ru	

People (2)	
Nikolay Storonsky	Vlad Yatsenko

Phone Numbers (4)	
(844) 744-3512	+184474435
039 1888	0800 591 1445

Websites (1)
www.revolut.com

CONCLUSIONI:

- Un esercizio davvero interessante che dimostra quanto sia a volte facile reperire delle informazioni, anche molto gravi come nel caso delle carte di credito rubate, sul web. Maltego è uno strumento davvero potente che facilita enormemente il processo di Information Gathering e aiuta a creare una mappa visiva e mentale che aiuta a seguire investigazioni molto vaste.