211783519, 323915363

מור משה ושי שלו

**Task 1 – OSINT**

**מבוא:**

בדו"ח זה מתועדים שלבי החקירה שביצענו באמצעות כלי OSINT על חברת Apple תוך התמקדות באיתור מידע ציבורי זמין. הדגש היה על שימוש בכלים מקוונים, חיפוש חופשי, וניתוח תוצאות רלוונטיות.

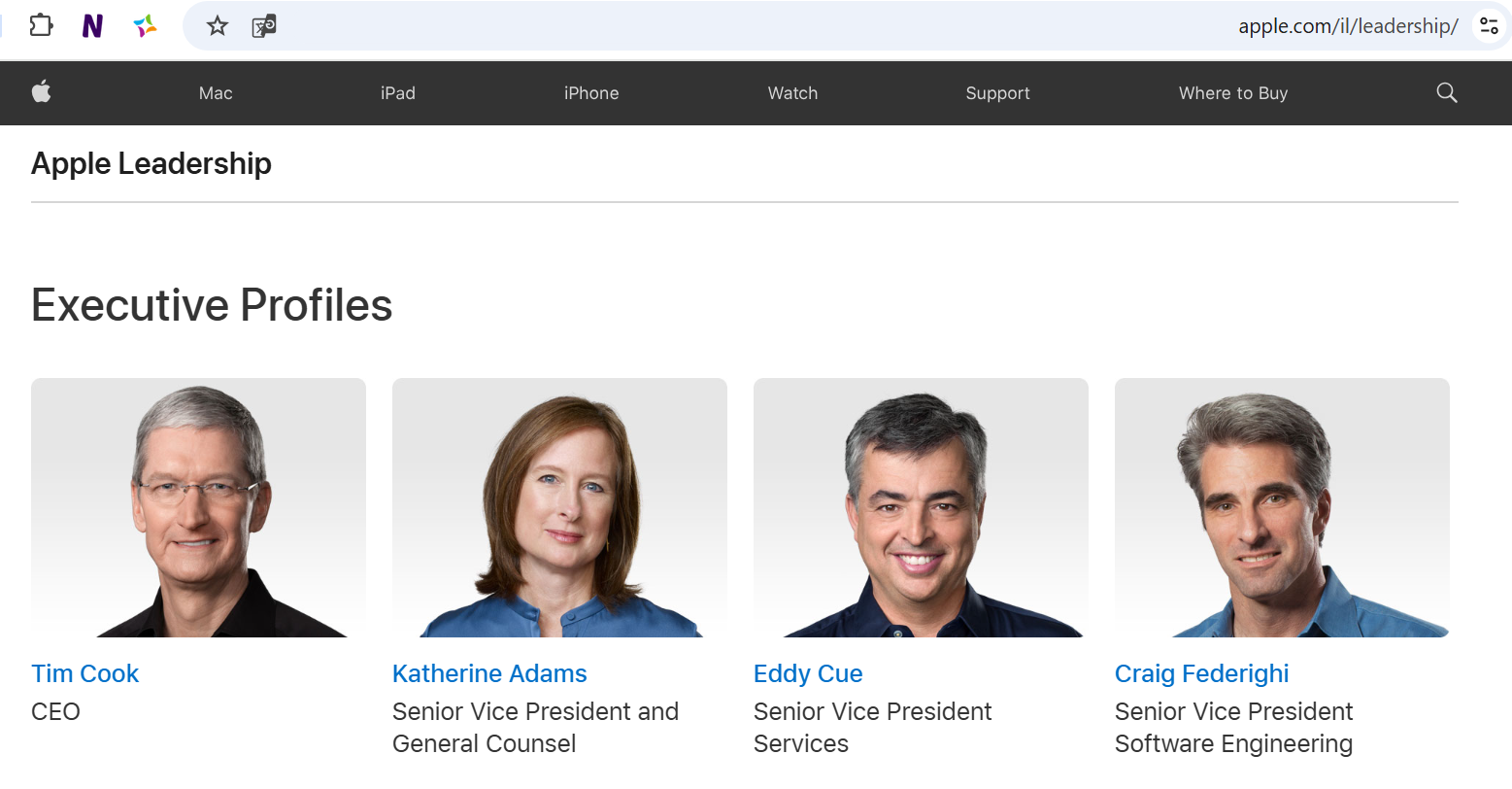
**יעד:**

1. השגת גישה לשרתים פנימיים.
2. איסוף מידע אישי של אנשי מפתח בחברה לצורך מתקפות ממוקדות

**Google Search:**

נכנסנו לאתר הרשמי של Apple

זיהינו את שמות אנשי ההנהלה הבכירים המפורטים באתר.



1. ביצענו חיפוש בגוגל על מנכ"ל החברה "Tim Cook"
   * מצאנו קישור לאתר [Business Roundtable](https://www.businessroundtable.org/members/tim-cook), שבו מופיע מידע על טים קוק כולל הפניות לפרופילי המדיה החברתי (לינקדאין, אינסטגרם, טוויטר, ופייסבוק).
2. תמונה שמכילה טקסט, צילום מסך, גופן

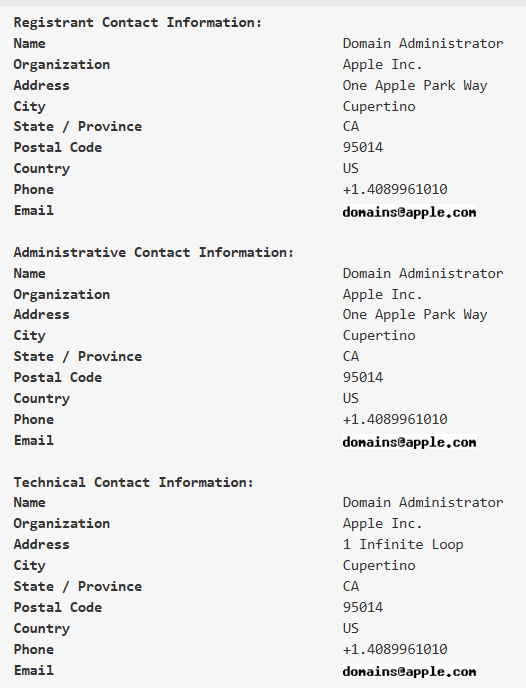
   התיאור נוצר באופן אוטומטיחיפשנו בגוגל את כתובתו של טים קוק.
   * מצאנו קישור לכתבה שמפרטת את כתובתו ומראה תמונות של הבית [Tim Cook House](https://www.squareyards.com/blog/tim-cook-house-celebhm).תמונה שמכילה טקסט, צילום מסך, בית

     התיאור נוצר באופן אוטומטיניתוח נוסף: זיהינו את שמות הרחובות באזור מגוריו באמצעות Google Maps, למרות שהבית עצמו מטושטש.



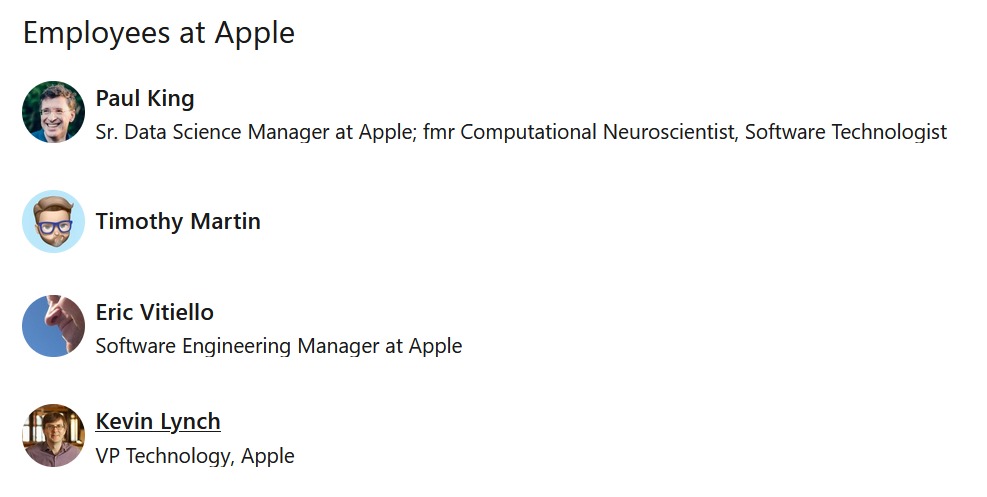
תמונה שמכילה טקסט, צילום מסך, מפה

התיאור נוצר באופן אוטומטי

**ניתוח דומיין באמצעות** [**WHOIS**](https://who.is/whois/apple.com)

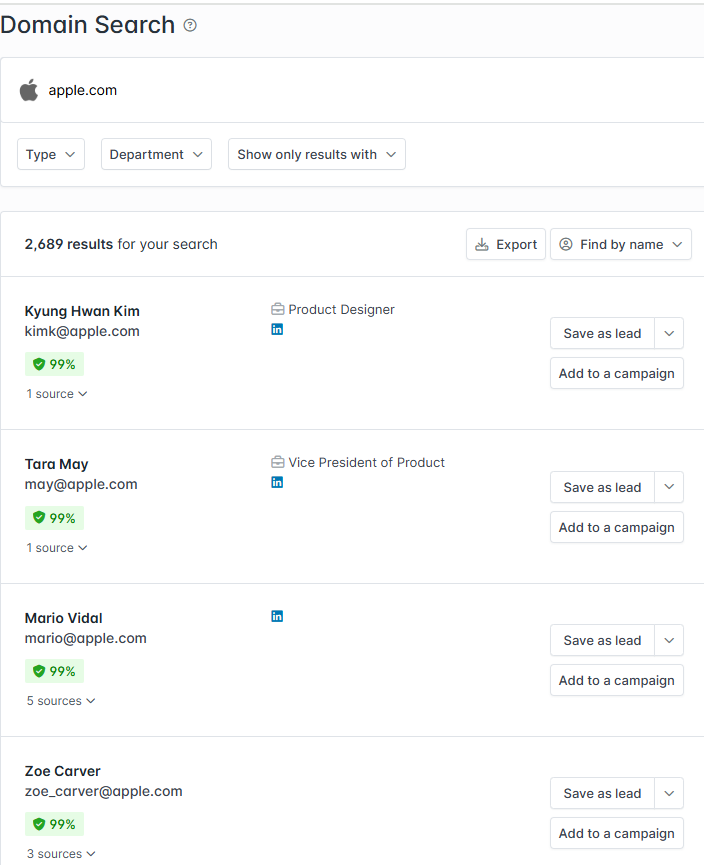
פרטי רישום הדומיין: בעלים, תאריכי רישום ותפוגה, שרתים ראשיים, ומיקום פיזי.

**לינקדין**:  
נכנסנו לפרופיל החברה Apple [בלינקדין](https://www.linkedin.com/company/apple/) וזיהינו רשימה של עובדים הפעילים ברשת.

* + ניתן להסיק מידע על מבנה החברה, תפקידים ופעילות עובדים.

**איתור כתובות מייל באמצעות Hunter.io**

* זיהינו תבניות של כתובות מייל בדומיין Apple:
  + אות ראשונה של השם הפרטי + שם משפחה מלא.
  + שם פרטי מלא + אות ראשונה של שם משפחה.
  + שם מלא.
  + כל כתובת מסתיימת [ב-@apple.com](mailto:ב-@apple.com).
* **תצפית מעניינת:**  
  חלק מהמידע שנמצא לא תאם את המסמך המקורי ממנו הוא לקוח, מה שמעלה שאלות לגבי אמינות המקור.

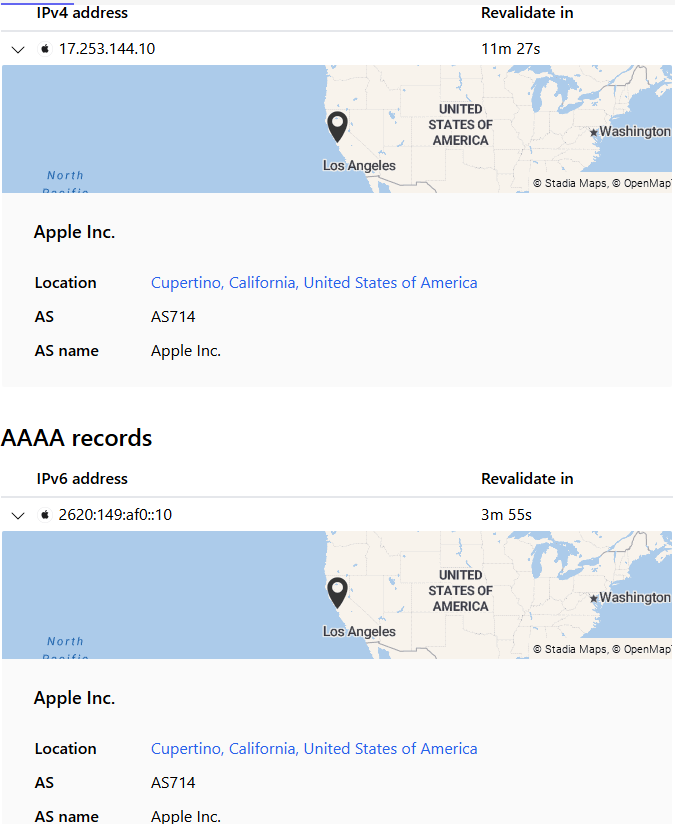


**מיפוי תשתיות רשת (Scanning)**

**שימוש ב-** [**NSLookup**](https://www.nslookup.io/domains/apple.com/dns-records/#google)

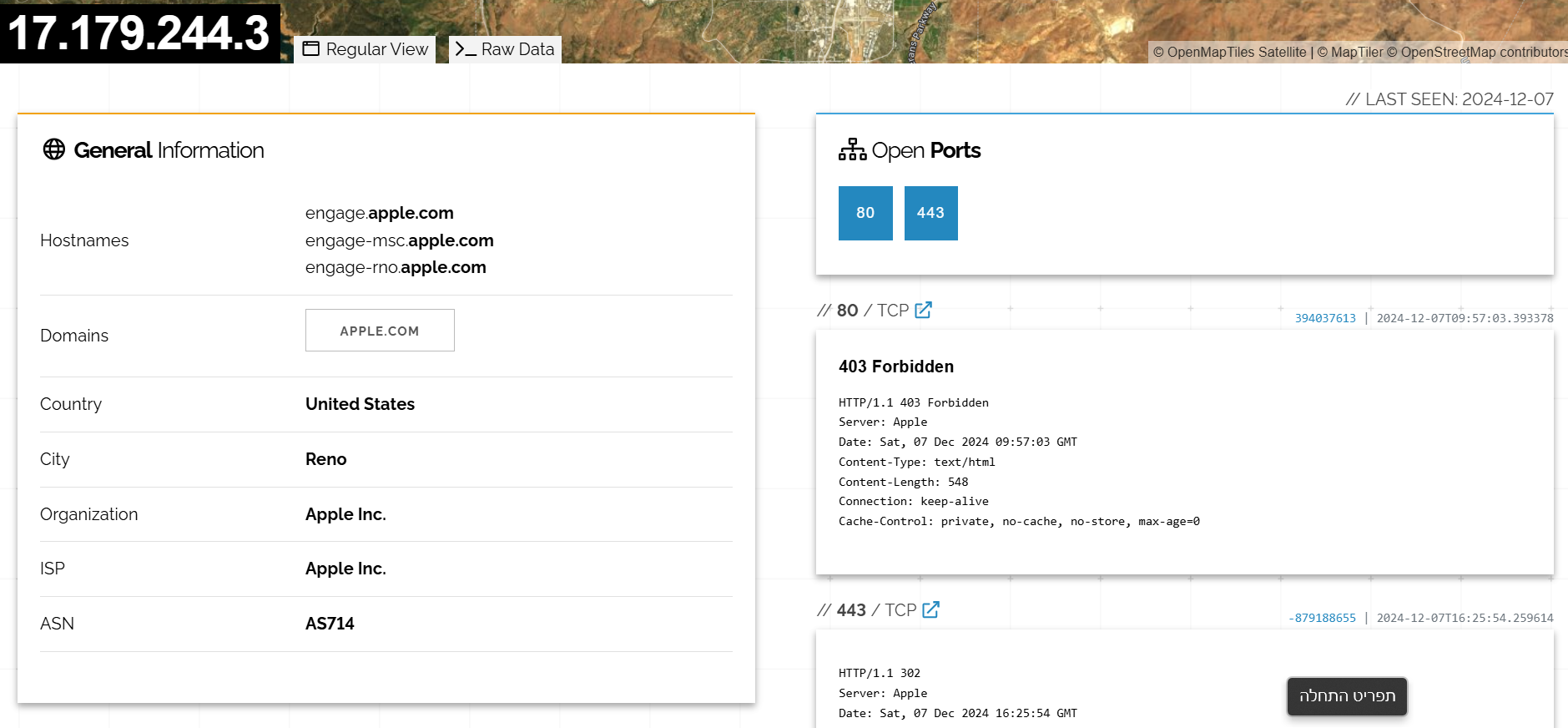
**ממצאים:**

* + הכתובות שנסרקו תאמו למידע שהתקבל מ- WHOIS ובנוסף קיבלנו מפה עם המיקום

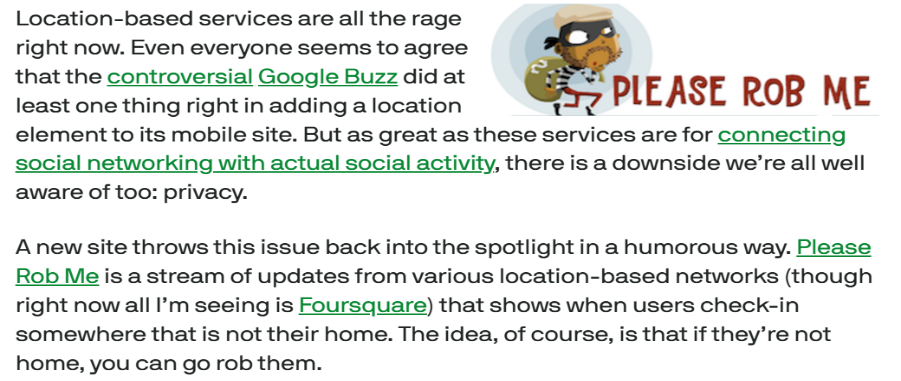


**סריקת רשת עם** [**SHODAN**](https://www.shodan.io/host/17.179.244.3)

* סרקנו כתובות IP הקשורות ל- Apple לאיתור שרתים חשופים, שירותים פתוחים ותצורה שגויה.
* **תובנות:** ניתוח שרתים ופורטים חשופים עשוי לחשוף חולשות אבטחה פוטנציאליות.

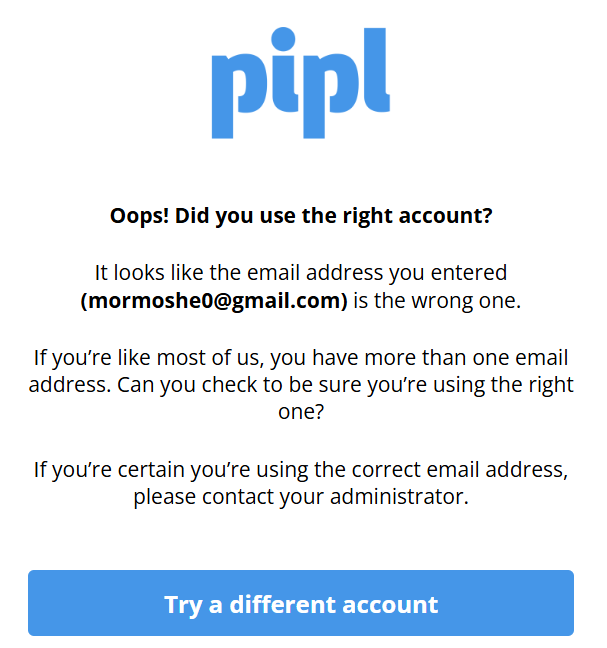
תמונה שמכילה טקסט, צילום מסך, גופן, מספר

התיאור נוצר באופן אוטומטי

**שלב 7: שימוש ב- please rob me**

ניסינו להשתמש באתר [Please Rob Me](https://pleaserobme.com) אחרי שהצלחנו לאתר את מגוריו אך האתר נחסם.



**שימוש ב-** [**pipl.com**](https://search.pipl.com/accounts/error_page_auth2/)

הגישה חסומה

**שימוש ב- Maltego**

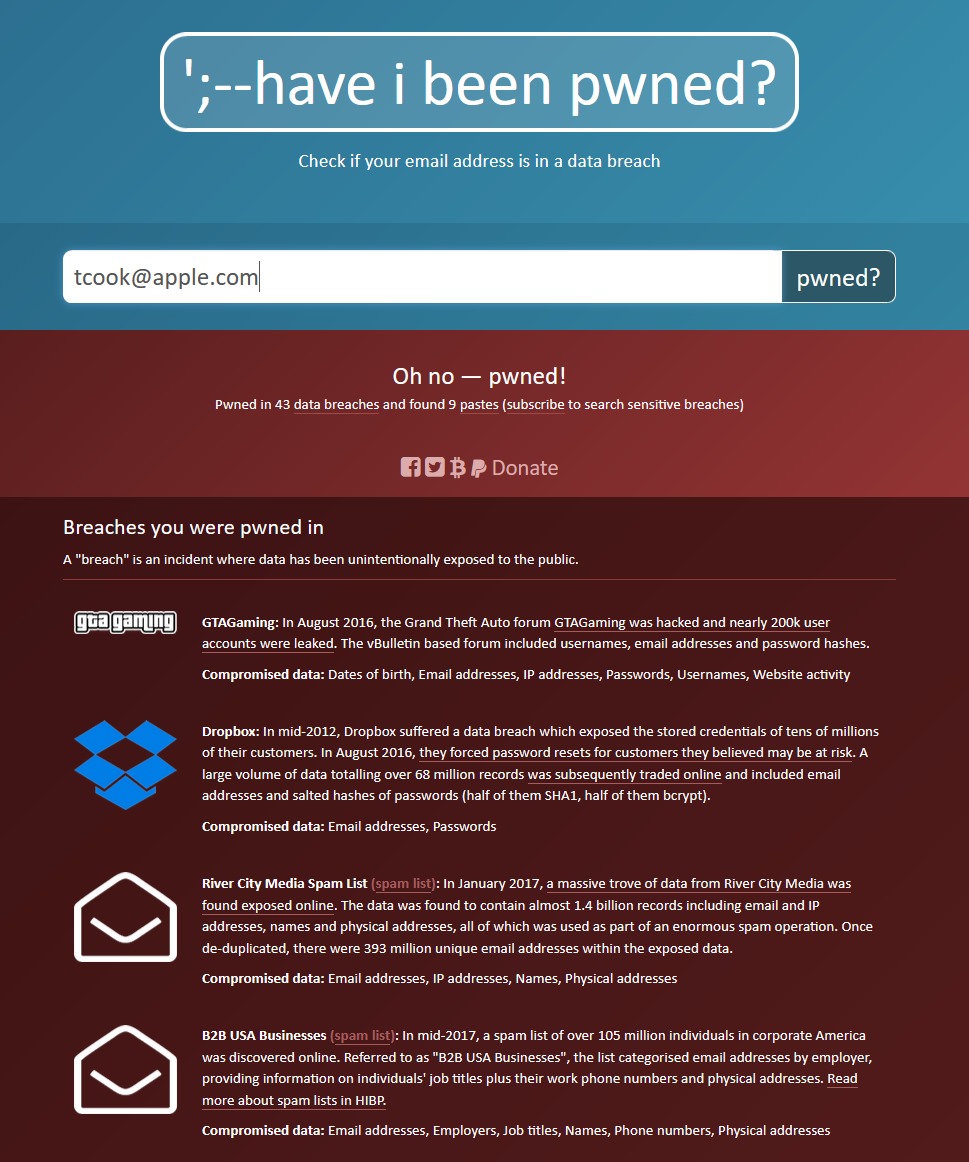
* השתמשנו בכלי לניתוח קשרים בין שמות, דומיינים, ואובייקטים נוספים הקשורים ל- apple.
* **תובנות:** מיפינו קשרים בין כתובות מייל וגורמים רשומים נוספים בדומיין apple.com

תמונה שמכילה טקסט, שרטוט, תרשים, ציור

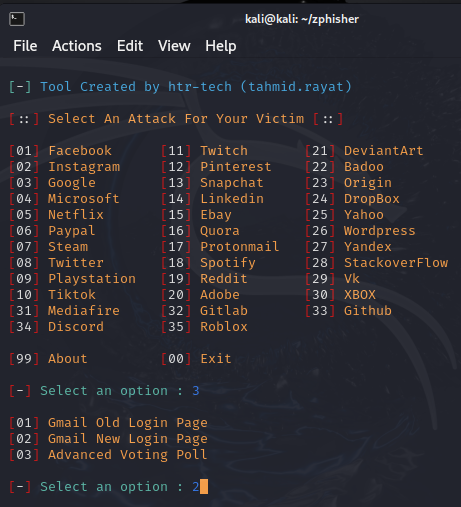
התיאור נוצר באופן אוטומטי

**בדיקת דליפות מידע עם** [**HaveIBeenPwned**](https://haveibeenpwned.com/)

* בדקנו האם כתובות מייל הקשורות ל- Apple נכללו במאגרים שהודלפו בעבר.



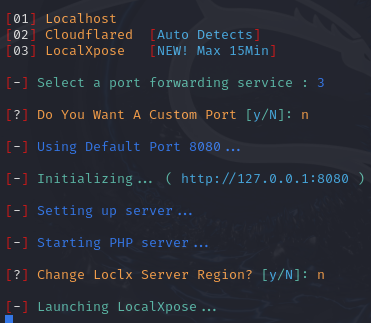
**חלק 2 – social engineering**

****

בחרנו להשתמש ב-ZPhisher, מכיוון שהוא כלי נוח וקל לתפעול

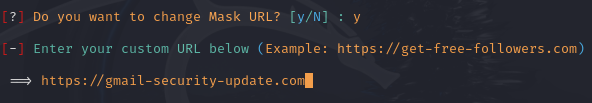
לאחר מכן, ניגשנו לתפריט ובחרנו את האפשרות להעתיק את עמוד ההתחברות של Gmail

בחרנו בשיטת התחברות המחקה דף חדש, על מנת שהדף לא ייראה חשוד למי שנכנס אליו.

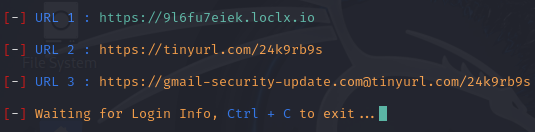
כאשר השתמשנו ב-localhost, הדף היה נגיש רק ברשת המקומית שלנו על מנת לשתף את דף הנחיתה עם אנשים מחוץ לרשת שלנו, השתמשנו ב-LocalXpose.

פורט ברירת המחדל הוא 8080

שינינו את כתובת ה-URL כדי שתיראה אמינה יותר.

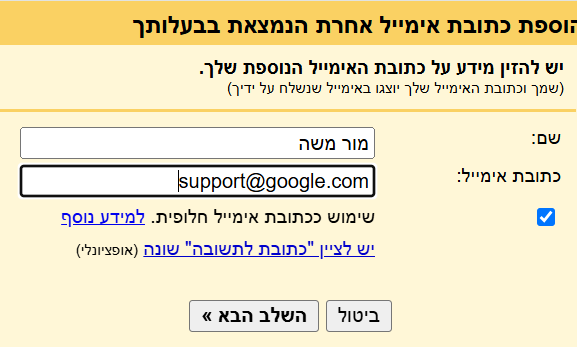


קיבלנו כתובת חדשה שהובילה לדף הנחיתה המועתק.



תמונה שמכילה טקסט, צילום מסך, גופן

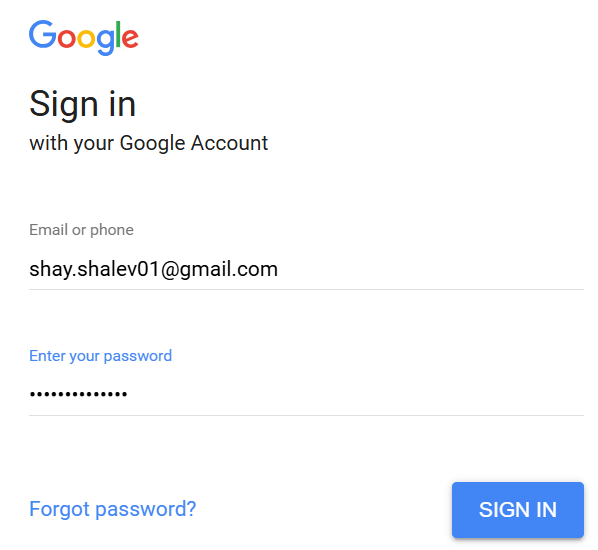
התיאור נוצר באופן אוטומטיבתוך הדף, המשתמש מתבקש לאשר את הביקור בדף המועתק.

תמונה שמכילה טקסט, צילום מסך, תוכנה

התיאור נוצר באופן אוטומטי

הגדרנו בשם השולח מייל שיראה אמין ככה שהצד המקבל ירצה לפתוח את הקישור ולהזין את הפרטים שלו.

המשתמש הזין את פרטי המייל שלו מקישור הURL שנשלח אליו במייל



וקיבלנו התראה לשם המשתמש והסיסמה שלו

ב- kali linux

תמונה שמכילה טקסט, צילום מסך, גופן

התיאור נוצר באופן אוטומטי