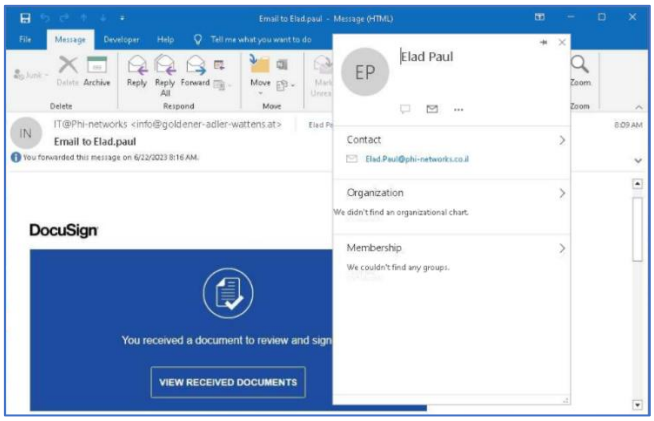
בקשת תחקור

שלום רב,
בהמשך לבקשת התחקור עבור מייל הפישינג שנשלח אליכם מאת info@goldener-adler-wattens[.]at, נראה כי מדובר בתקיפה רחבה כנגד מספר אירגונים כאשר חלקם מישראל, להלן מתואר מתווה התקיפה המפורט:

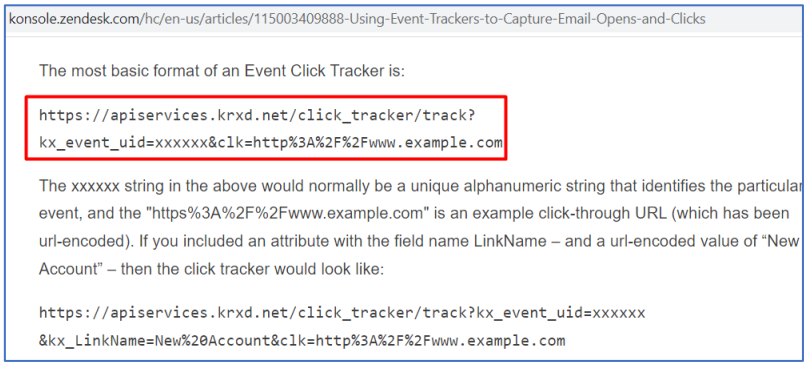
<u>תחקור:</u>

להלן דוגמה לאחד מקבצי הפישינג שנשלחו לאירגונים בישראל, קובץ המייל מתחזה ל-DocuSign.



המייל שמתקבל מכיל תמונה עם הכיתוב DocuSign המתחזה לשירות חתימה על קובץ.

בעת לחיצה על הקישור התוקף מקבל התרעה על כך שה-URL נלחץ וזאת באמצעות הדומיין apiservices[.]krxd[.]net/click_track. מדובר בדומיין שמטרתו לספק סטטיסטיקות פר לחיצה על קישור.



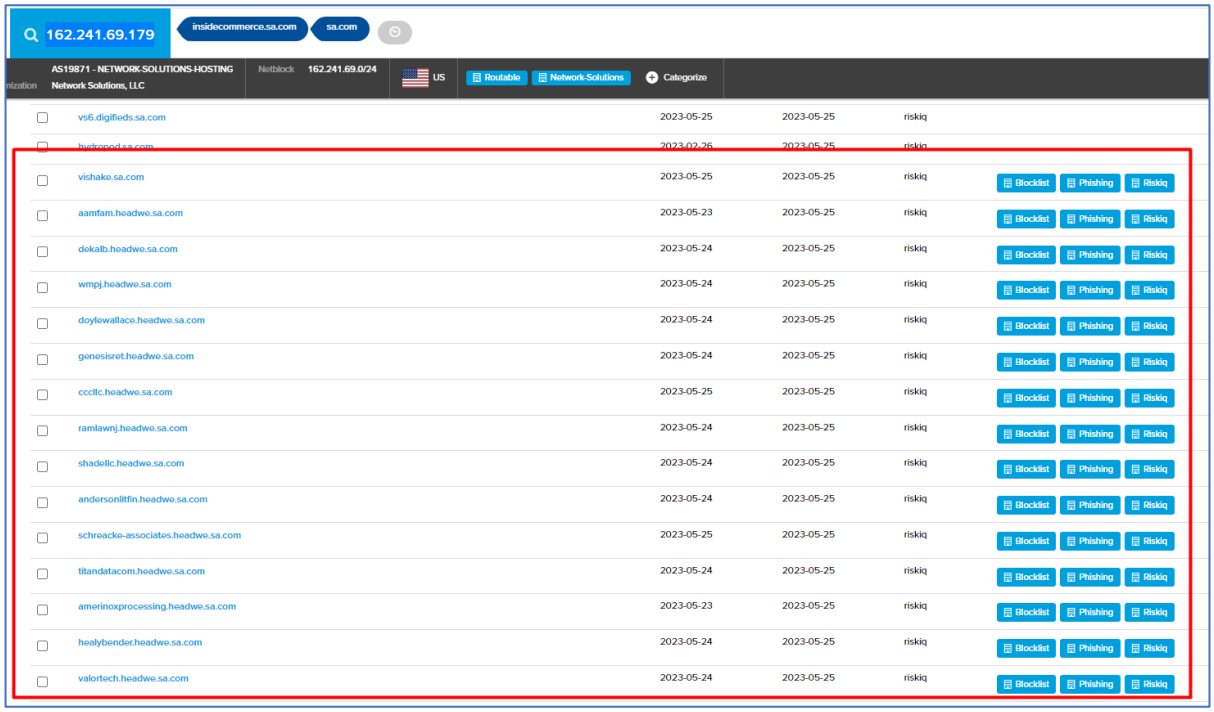
צילום מסך מתוך האתר zendex[1] המסביר לגבי השימוש ב-krxd[.]net.

לאחר מכן מועברים לדף המבצע Redirect וזאת ככל הנראה על מנת להימנע מגילוי כזדוני.

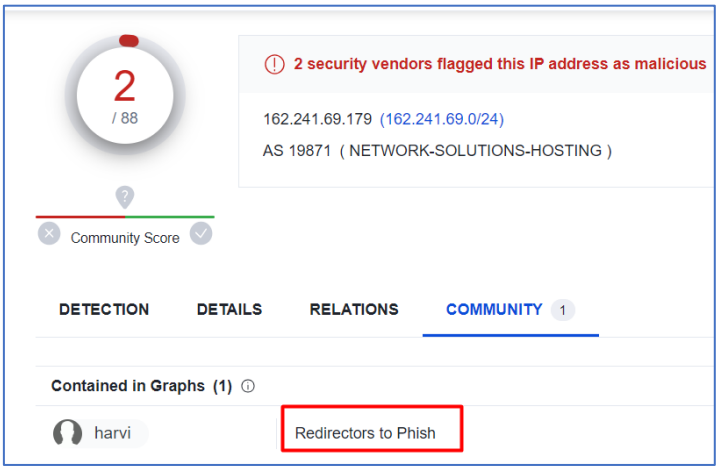
הדומיין המבצע את ה-Redirect הינו insidecommerce[.]sa[.]com.
הדמיין מזוהה כזדוני על יד 5 מנועי אנטיוירוס, מדובר בדומיין המכיל Subdomain רבים (מעל ל-5 אלף) ולכן נראה כי דומיין זה הינו שירות של Dyn dns (Dynamic DNS).

[1] https://konsole.zendesk.com/hc/en-us/articles/115003409888-Using-Event-Trackers-to-Capture-Email-Opens-and-Clicks

כתובת ה-IP אליה הדומיין מצביע היא 179[.]69[.]241[.]162. כתובת זו מכילה מספר תת דומיינים של sa[.]com כאשר חלק גדול מהם על פי PassiveTotal מקוטלג כפישינג.



כתובת זו מזוהה בקהילה של VirusTotal כ-Redirect של פישינג.



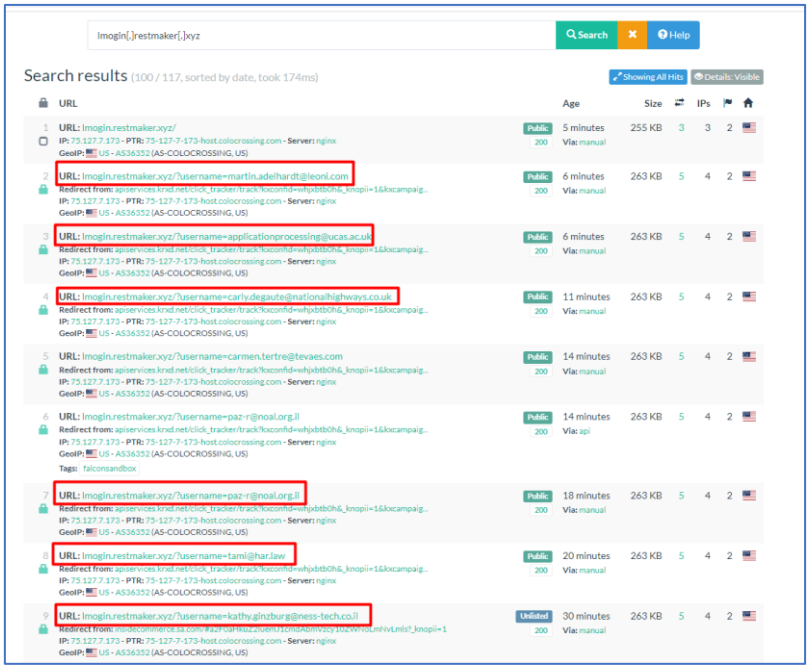
לאחר ה-Redirect מועברים לדומיין הבא המשמש בהתקפה: lmogin[.]restmaker[.]xyz.
הדומיין אינו מזוהה כזדוני כלל ב-VirusTotal (0 זיהויים) ונראה כי הוקם לראשונה לפני כשבוע.
אך, בעת גלישה לדומיין מקבלים התרעה מהדפדפן על כך שמדובר בדומיין זדוני.

הדף המוצג בסוף המתווה המוזכר לעיל הינו של Office365.
בדיקה של הדומיין restmaker[.]xyz ב-VirusTotal מראה מגוון סריקות של חברות שככל הנראה כלפיהן בוצע פישינג זהה.

URLs (27)

Scanned	Detections	Status	URL
2023-06-22	0 / 90	200	https://lmogin.restmaker.xyz/?username=jj
2023-06-22	0 / 90	200	https://lmogin.restmaker.xyz/?username=daniel@ayrton.ie
2023-06-22	0 / 90	200	https://lmogin.restmaker.xyz/?username=jw@
2023-06-22	0 / 90	200	https://lmogin.restmaker.xyz/?username=protecciondedatos@lavanguardia.es
2023-06-22	0 / 90	200	https://lmogin.restmaker.xyz/?username=
2023-06-22	0 / 90	200	http://lmogin.restmaker.xyz/?username=
2023-06-22	0 / 90	200	https://lmogin.restmaker.xyz/?username=martin.adelhardt@leoni.com
2023-06-22	0 / 90	200	https://lmogin.restmaker.xyz/?username=applicationprocessing@ucas.ac.uk
2023-06-22	0 / 90	200	https://lmogin.restmaker.xyz/?username=florence.logan@communityfibre.co.uk
2023-06-22	0 / 90	200	https://lmogin.restmaker.xyz/?
2023-06-22	0 / 90	200	https://lmogin.restmaker.xyz/?username=5jV]mMuium<uwf]W4[tX88@]85]P
2023-06-22	0 / 90	200	http://lmogin.restmaker.xyz/?username=mark.sanchez@moore.org&sso_reload=true
2023-06-22	0 / 90	200	https://lmogin.restmaker.xyz/?username=geoff.howard@cybg.com
2023-06-22	0 / 90	200	https://lmogin.restmaker.xyz/?username=eric.kacal@totalenergies.com
2023-06-22	0 / 90	200	https://lmogin.restmaker.xyz/?username=ryendluri@innominds.com&sso_reload=true
2023-06-22	0 / 90	200	https://lmogin.restmaker.xyz/?username=jw@&sso_reload=true
2023-06-22	0 / 90	200	https://lmogin.restmaker.xyz/?username=olive.ojo@ncirl.ie%20Page%20URL
2023-06-22	0 / 90	200	https://lmogin.restmaker.xyz/?username=mail.investigation@oerlikon.com
2023-06-22	0 / 90	200	https://lmogin.restmaker.xyz/?username=5r*&m{w^;RyXZ[S[@
2023-06-21	0 / 90	200	https://lmogin.restmaker.xyz/?username=gourav.sharma@wsp.com
2023-06-21	0 / 90	200	https://lmogin.restmaker.xyz/?username=john.alves@mail.concordia.ca&sso_reload=true
2023-06-21	0 / 90	200	https://lmogin.restmaker.xyz/?username=dparsons@hubgroup.com
2023-06-21	0 / 90	200	https://lmogin.restmaker.xyz/?username=carissam@sacredcircle.com
2023-06-21	0 / 90	200	https://lmogin.restmaker.xyz/
2023-06-19	0 / 90	200	https://lmogin.restmaker.xyz/?Bw9Wf=uwr
2023-06-18	0 / 90	200	https://lmogin.restmaker.xyz/?username=tara.mirchandani@sc.com
2023-06-16	0 / 90	200	https://lmogin.restmaker.xyz/common/login

סריקה של הדומיין restmaker[.]xyz ב-URLSCAN הראת כי ישנם סריקות רבות גם כן עבור חברות רבות שככל הנראה הותקפו באותו מתווה(חלקם מישראל).



הדומיין ממנו נשלח המייל פישינג כנגד מספר רב של אירגונים בארץ ובחו"ל הינו goldener-adler-wattens[.]at מדובר באתר של מלון Hotel Adler Betrieb שככל הנראה נפרץ בידי התוקף.