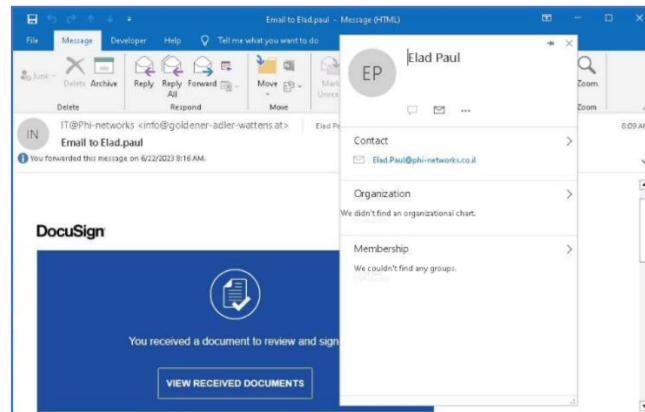


## בקשת תחקור

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:

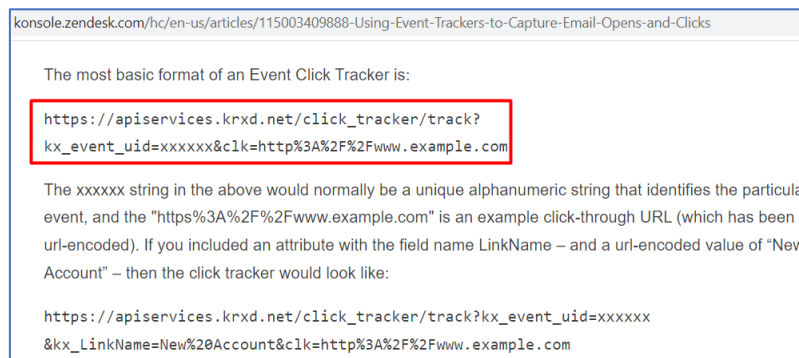
תחקור:

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 <sup>1</sup>zendesk 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. הדמיון מזהה כזדוני על ידי 5 מנועי אנטייורוס, מדובר בדומיין המכיל Subdomain רבים (מעל ל-5 אלף) ולכן נראה כי דומיין זה הינו שירות של Dyn dns (Dynamic DNS).

<sup>1</sup> <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 162.241.69.179. כתובת זו מכילה מספר תת דומיינים של sa[.]com כאשר חלק גדול מהם על פי PassiveTotal מקוטלג כפשינג.

Domain	IP Address	Category	Actions
vs6.digifeds.sa.com	2023-05-25	riskiq	
headwoop.sa.com	2023-02-26	riskiq	
vishako.sa.com	2023-05-25	riskiq	Blocklist Phishing Riskiq
aanfam.headwo.sa.com	2023-05-23	riskiq	Blocklist Phishing Riskiq
dekalb.headwo.sa.com	2023-05-24	riskiq	Blocklist Phishing Riskiq
wmpj.headwo.sa.com	2023-05-24	riskiq	Blocklist Phishing Riskiq
doyfowallaco.headwo.sa.com	2023-05-24	riskiq	Blocklist Phishing Riskiq
genesizret.headwo.sa.com	2023-05-24	riskiq	Blocklist Phishing Riskiq
ccdlc.headwo.sa.com	2023-05-25	riskiq	Blocklist Phishing Riskiq
ramlawj.headwo.sa.com	2023-05-24	riskiq	Blocklist Phishing Riskiq
shadelic.headwo.sa.com	2023-05-24	riskiq	Blocklist Phishing Riskiq
andersonlitfin.headwo.sa.com	2023-05-24	riskiq	Blocklist Phishing Riskiq
schraacke-associates.headwo.sa.com	2023-05-25	riskiq	Blocklist Phishing Riskiq
titandatacom.headwo.sa.com	2023-05-24	riskiq	Blocklist Phishing Riskiq
amerinoxprocessing.headwo.sa.com	2023-05-23	riskiq	Blocklist Phishing Riskiq
healybender.headwo.sa.com	2023-05-24	riskiq	Blocklist Phishing Riskiq
valortech.headwo.sa.com	2023-05-24	riskiq	Blocklist Phishing Riskiq

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

2 security vendors flagged this IP address as malicious

162.241.69.179 (162.241.69.0/24)  
AS 19871 (NETWORK-SOLUTIONS-HOSTING)

Community Score: 2 / 88

DETECTION DETAILS RELATIONS **COMMUNITY 1**

Contained in Graphs (1)

harvi **Redirectors to Phish**

לאחר ה-Redirect מועברים לדומיין הבא המשמש בהתקפה: Imogin[.]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 Imogin[.]restmaker[.]xyz ב-VirusTotal מראה מגוון סריקות של חברות שכלל הנראה כלפיהן בוצע פשינג זהה.

Scanned	Detections	Status	URL
2023-06-22	0 / 90	200	https://login.restmaker.xyz/?username=jj
2023-06-22	0 / 90	200	https://login.restmaker.xyz/?username=daniel@ayrton.ie
2023-06-22	0 / 90	200	https://login.restmaker.xyz/?username=jw@
2023-06-22	0 / 90	200	https://login.restmaker.xyz/?username=protecciondedatos@lavanguardia.es
2023-06-22	0 / 90	200	https://login.restmaker.xyz/?username=
2023-06-22	0 / 90	200	http://login.restmaker.xyz/?username=
2023-06-22	0 / 90	200	https://login.restmaker.xyz/?username=martin.adelhardt@leoni.com
2023-06-22	0 / 90	200	https://login.restmaker.xyz/?username=applicationprocessing@ucas.ac.uk
2023-06-22	0 / 90	200	https://login.restmaker.xyz/?username=florence.logan@communityfibre.co.uk
2023-06-22	0 / 90	200	https://login.restmaker.xyz/?
2023-06-22	0 / 90	200	https://login.restmaker.xyz/?username=5Vjmluium<uwfjW4lX8@j85JP
2023-06-22	0 / 90	200	http://login.restmaker.xyz/?username=mark.sanchez@moore.org&so_reload=true
2023-06-22	0 / 90	200	https://login.restmaker.xyz/?username=geoff.howard@cybg.com
2023-06-22	0 / 90	200	https://login.restmaker.xyz/?username=eric.kacal@totalenergies.com
2023-06-22	0 / 90	200	https://login.restmaker.xyz/?username=ryendlun@mnominds.com&so_reload=true
2023-06-22	0 / 90	200	https://login.restmaker.xyz/?username=jw@&so_reload=true
2023-06-22	0 / 90	200	https://login.restmaker.xyz/?username=olive.ojo@ncirl.ie%20Page%20URL
2023-06-22	0 / 90	200	https://login.restmaker.xyz/?username=mail.investigation@oerlikon.com
2023-06-22	0 / 90	200	https://login.restmaker.xyz/?username=5r*%m{w^A;RyXZ[S@
2023-06-21	0 / 90	200	https://login.restmaker.xyz/?username=gourav.sharma@wsp.com
2023-06-21	0 / 90	200	https://login.restmaker.xyz/?username=john.alves@mail.concordia.ca&so_reload=true
2023-06-21	0 / 90	200	https://login.restmaker.xyz/?username=dparsons@hubgroup.com
2023-06-21	0 / 90	200	https://login.restmaker.xyz/?username=carissam@sacredcircle.com
2023-06-21	0 / 90	200	https://login.restmaker.xyz/?
2023-06-19	0 / 90	200	https://login.restmaker.xyz/?Bw9WF=urw
2023-06-18	0 / 90	200	https://login.restmaker.xyz/?username=tara.mirchandani@sc.com
2023-06-16	0 / 90	200	https://login.restmaker.xyz/common/login

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

Search results (100 / 117, sorted by date, took 174ms)

URL	Age	Size	IPs
1. URL: login.restmaker.xyz/	5 minutes	255 KB	3 3 2
2. URL: login.restmaker.xyz/?username=martin.adelhardt@leoni.com	6 minutes	263 KB	5 4 2
3. URL: login.restmaker.xyz/?username=applicationprocessing@ucas.ac.uk	6 minutes	263 KB	5 4 2
4. URL: login.restmaker.xyz/?username=carly.degaute@nationalhighways.co.uk	11 minutes	263 KB	5 4 2
5. URL: login.restmaker.xyz/?username=carmen.tertre@tevaes.com	14 minutes	263 KB	5 4 2
6. URL: login.restmaker.xyz/?username=paz-@gmail.org.il	14 minutes	263 KB	5 4 2
7. URL: login.restmaker.xyz/?username=paz-@gmail.org.il	18 minutes	263 KB	5 4 2
8. URL: login.restmaker.xyz/?username=tami@har.law	20 minutes	263 KB	5 4 2
9. URL: login.restmaker.xyz/?username=kathy.ginzburg@mess-tech.co.il	30 minutes	263 KB	5 4 2

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

**Hotel Adler Betriebs GmbH (golden eagles)**  
 Owner of this company? [expand entry](#)

Innsbrucker Strasse 1  
 6112 Wattens

Tel.: 05224 52255  
 Fax: 05224 54471

Mail: [hotel@goldener-adler-wattens.at](mailto:hotel@goldener-adler-wattens.at)  
 Web: [www.goldener-adler-wattens.at](http://www.goldener-adler-wattens.at)

