MANDIANT
NOW PART OF Google Cloud

זיהוי קבצים אשר הועלו ל-Virus Total, ואשר ככל הנראה קשורים לארגון

1. במהלך בדיקות ניטור שגרתיות, איתרנו את המייל הבא, אשר עלה לסריקה ב-Virus Total ביולי 2022:
https://www.virustotal.com/gui/file/63bf4576413a8a6937b27bb75a3083b685e5f350c2a6ee9296ace3fb8ef21c01
2. על בסיס ניתוח הheader-ים של מייל זה, נראה כי הוא נשלח מהכתובת RoslanVo@soreq.gov[.]il לכתובת heaven.ferman@moondoo[.]org. הכתובת המקבלת הינה תיבת מייל חד-פעמית המונפקת על ידי השירות של minuteinbox[.]com. לתשומת ליבכם כי יתכן ופעולה זו ועומדת בסתירה למדיניות אבטחת המידע והוצאת חומרים מהארגון.
3. מבחינת תוכן, המייל ריק, אך פרטי ה-metadata ב-headerים של המייל חושפים את פרטי שרת המייל הפנימי של הארגון - bvmail01.bsoreq[.]net, את הכתובת החיצונית mailbox.soreq.gov[.]il וכתובת ה-IP המקושרת 212.150.66[.]166.

```
x-originating-ip: [192.168.22.1]
return-path: <RoslanVo@soreq.gov.il>
delivered-to: heaven.ferman@moondoo.org
received: from soreq.gov.il (mailbox.soreq.gov.il [212.150.66.166]) (using TLSv1.2 with cipher ECDHE-RSA-AES256-GCM-SHA384 (256/256 bits)) (No client
certificate requested) by www.minuteinbox.com (Postfix) with ESMTPS id A203742190 for <heaven.ferman@moondoo.org>
Mon, 11 Jul 2022 01:39:01 -0400 (EDT)
received: from mail.soreq.gov.il (unknown [192.168.64.127]) (using TLSv1.2 with cipher AES256-GCM-SHA384 (256/256 bits)) (No client certificate requested) by
Forcepoint Email with ESMTPS id 53863DE05BF525456B51 for <heaven.ferman@moondoo.org>
Mon, 11 Jul 2022 08:35:22 +0300 (IDT)
received: from bvmail01.bsoreq.net (192.168.64.127) by bvmail01.bsoreq.net (192.168.64.127) with Microsoft SMTP Server (version=TLS1_2,
cipher=TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256) id 15.1.2242.4
Mon, 11 Jul 2022 08:35:22 +0300
received: from bvmail01.bsoreq.net ([fe80::51be:1f3a:4f31:c899]) by bvmail01.bsoreq.net ([fe80::51be:1f3a:4f31:c899%3]) with mapi id 15.01.2242.004
from: "RoslanVo@soreq.gov.il" <RoslanVo@soreq.gov.il>
to: "heaven.ferman@moondoo.org" <heaven.ferman@moondoo.org>
subject: HELOO
thread-topic: HELOO
thread-index: AdiU6AK+XZ+rM+aXT7uNVWYNKsETIw==
date: Mon, 11 Jul 2022 05:35:21 +0000
message-id: <c513d55847f04aa5a57a0f1d4560f7b7@soreq.gov.il>
accept-language: en-US
content-language: en-US
```

4. ללא קשר לאירוע זה, זיהינו בעבר ב-Mandiant מיילים רגישים שעלו ל-VT, כאשר התרחיש הסביר ביותר לכך היה תוסף של VT לדפדפן, אשר היה המותקן על המחשב (השולח או המקבל). תוסף זה העלה, ללא ידיעת המשתמש, קבצים מהעמדה אשר אינם היו מוכרים ב-VT (על בסיס בדיקת hash).
5. מבדיקות נוספות, זיהינו כי המייל לעיל הועלה ל-VT בתאריך 11 ביולי 2022 ע"י סאבמיטר ישראלי במזהה f2aec1a1. באמצעות כלי מחקר פנימי שפותח ב- Mandiant, זיהינו כי משתמש זה פעיל ב-VT משנת 2016 והעלה עד כה בסה"כ 194 קבצים. על בסיס ניתוח קבצים נוספים שהועלו ל-VT ע"י סאבמיטר זה לאורך השנים, אנו מעריכים בסבירות גבוהה כי הינו קשור לארגון (לאחד הגופים).
6. ממעבר על רשימת הקבצים, נראה כי רוב מוחלט של הקבצים אינו זדוני, וכי מדובר בקבצים שונים – דרייברים של מערכות טכנולוגיות שונות, עדכונים של Windows ומוצרי אבטחה (Microsoft Defender, MacAfee), ברושורים ומסמכי הפעלה של מערכות שונות, PDFים של מחקרים שונים וכו'. להערכתנו, המשמעות המודיעינית הנובעת מכך היא פוטנציאל לחשיפת צי"ח, מערכות ייעודיות שהארגון משתמש בהם או מתעניין בהם (יעד להסתרה) וכדומה. רצינו להציף זאת לתשומת ליבכם, למקרה שמדיניות הארגון אוסרת על העלאת קבצים ל-VT.

דוגמאות לקבצים שעלו מהמשתמש:

שם הקובץ	Hash	תאריך העלאה	הערות
Terms-and-Conditions-Customers-English.pdf	aa2e15f9812d688380ef5b2576428b5c	23/03/22	קובץ T&C ללקוחות Rotem Industries Ltd.
MoravianCameraSDK.zip	e1e6e34e3fcfbb3e0c8d66e3393d40b5	08/12/21	קבצי פיתוח ודרייברים למצלמות Moravian
wat-2200mk-2-dimensions.pdf	f20951edaefe48ad8c1ec633369274b2	24/07/22	שרטוט של מצלמת Watec
Thorlabs.OpticalPowerMonitor.3.1.3780.521.zip	bbbdb6d2d6d41b91460604bf6bb67eb1	31/05/22	קבצי פיתוח של Thorlabs
opendicom-code-r134.zip	fd3a4936919098e419a37405a34e0585	03/03/22	קבצי פיתוח של MicroDicom
ESP301-Firmware-Installer-V1.1.1.zip	d0d9626237087342db5adbebe67171c0	22/12/22	קבצי התקנה של ציוד טכנולוגי של Newport
Workshop_v2_1_distribute.pdf	e2647029f91f6674d47618dcc813b90c	13/01/22	מצגת מסמינר LS-DYNA

<u>המלצות להמשך:</u>

- חידוד נהלים לעובדים בנוגע להעלאת חומר לאינטרנט ו/או ל-VT
- בחינת מחשבי האינטרנט בארגון לטובת זיהוי תוספי דפדפן של VT
- בחינת שרת המייל לזיהוי/חסימת מיילים הנשלחים לשירותי מייל חד-פעמיים, למשל על בסיס רשימה זו: https://gist.github.com/michenriksen/8710649
- במידת הצורך, בחינת שירות חלופי לסריקת קבצים (Sandbox / שירות אחר המאפשר סריקה פרטית)