# קמפיין דיוג שהסתיים בכופרה שהה כשנה על מחשבי משתמשים טרם הפעלתו

03/06/2026
י"ח סיון תשפ"ו

## [תקציר]

1. לאחרונה דווח למערך הסייבר הלאומי על מספר תקיפות כופרה כנגד ארגונים קטנים ומשתמשים פרטיים.
2. במהלך חקירת האירוע התברר כי הרקע לתקיפה היא הודעת דיוג שהופצה בדוא"ל לפני כשנה והתרעה לגביה פורסמה על ידי המערך.

## [פעולות מידיות לביצוע]

- להתרעה זו מצורף קובץ מזהים. מומלץ לנטרם בכל מערכות האבטחה הארגוניות הרלוונטיות.
- וודאו בהקדם האפשרי כי ברשותכם גיבויים תקינים ועיתיים של כל המידע החשוב לכם או לארגונכם.
- שימרו מספר גיבויים בשיטת 3-2-1: שלושה גיבויים שונים, באמצעות 2 שיטות גיבוי ו/או מדיה שונות, כאשר לפחות גיבוי אחד אינו מקוון או אף נשמר מחוץ לחצרי הארגון.

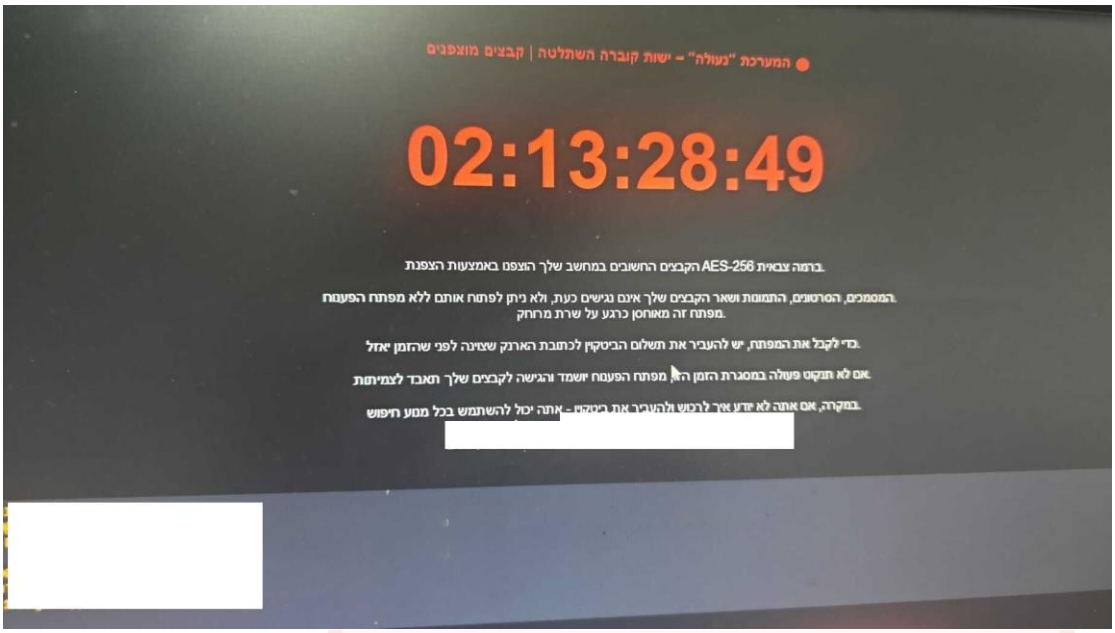
## [פרטים]

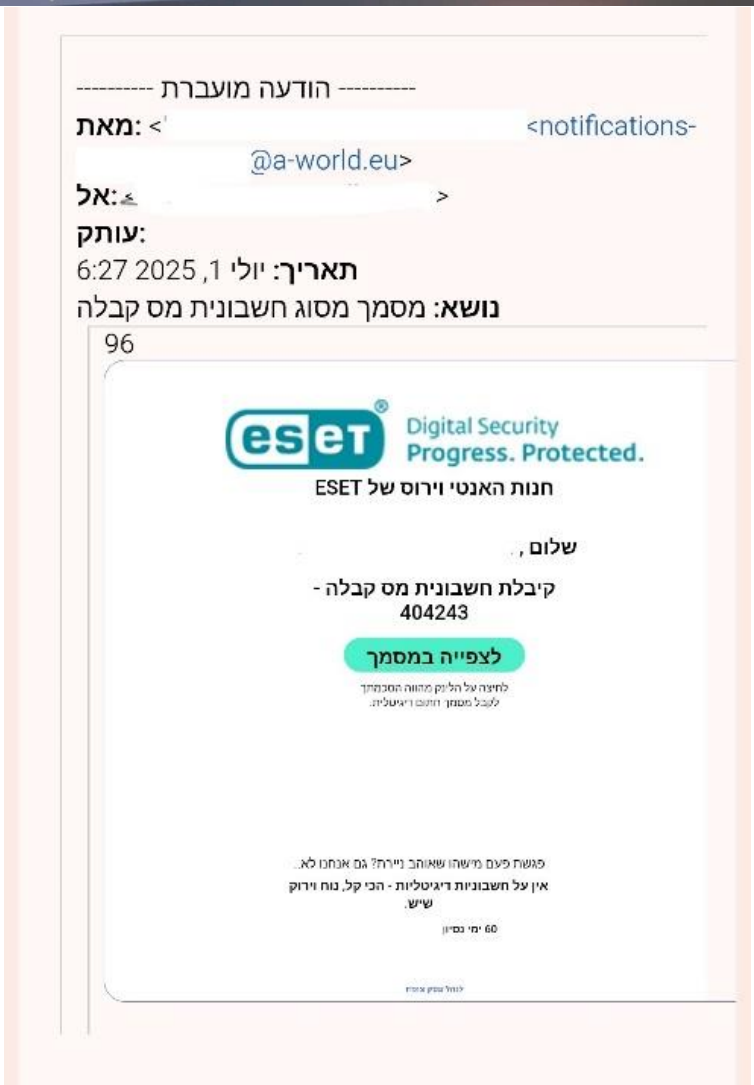
1. ממקרים שנבדקו במהלך החקירה עלה כי האחיזה הראשונית של התוקף בעמדה הושגה באמצעות הודעות דיוג שכללו קישור. ההודעות קשורות לקמפיין עבר שדווח על ידי המערך והתחזה להודעות מיצרן/מפיץ תוכנת ה-ESET AV. **ראו בקישור מס' 1 את ההתרעה שהוציא המערך בנדון ביולי 2025.**
2. דוגמה של הודעות שנשלחו בקמפיין הנ"ל, ניתן לראות בצילומי המסך להלן.
3. הפעלת הקישור על ידי המשתמש מתקינה בעמדה תוכנת RMM מסוג ScreenConnect. התוכנה מוגדרת מראש על ידי התוקף ליצור קשר עם שרת בשליטתו.
4. **יודגש כי התוכנות המצוינות לעיל הן לגיטימיות לחלוטין, ורק השימוש בהן או ההתחזות ליצרן/מפיץ אינה לגיטימית.**
5. במקרה זה, התוקף בחר שלא לממש מיידית התקפת כופרה על העמדות שהשיג אליהן גישה ראשונית, אלא המתין זמן רב יחסית, ובין התאריכים 24 ל-26 למאי 2026, הפעיל פוגען כופרה על העמדות. את בקשת הכופר ניתן לראות בצילומי המסך למטה.
6. בחקירה נמצא בין השאר קובץ המזוהה ככורה מטבעות וירטואליים (Crypto Miner) מסוג Monero, וייתכן כי התוקף ניצל את הזמן בין השגת האחיזה הראשונית בעמדה להצפנתה, לצורך כריית מטבעות מסוג זה.
7. בחלק מהמקרים ניסיון ההצפנה באמצעות הכופרה כשל ולא בוצעה הצפנה מלאה של הקבצים, כך שהמשתמשים הצליחו לשחזר אותם. לעומת זאת במקרים אחרים ההצפנה הצליחה, וחלק מהמשתמשים שלא גיבו את המידע נשארו ללא גישה לקבצים שלהם. נכון לכתיבת התרעה זו לא מוכרת אפשרות לשחזר הקבצים, אם כי אפשר ותימצא דרך לכך בעתיד.

## [דרכי התמודדות]

1. **וודאו בהקדם האפשרי כי ברשותכם גיבויים תקינים ועיתיים של כל המידע החשוב לכם או לארגונכם.**
2. **שימרו מספר גיבויים בשיטת 3-2-1: שלושה גיבויים שונים, באמצעות 2 שיטות גיבוי ו/או מדיה שונות, כאשר לפחות גיבוי אחד אינו מקוון או אף נשמר מחוץ לחצרי הארגון. יש לוודא באופן עיתי כי הנוהל והיכולת לשחזר מגיבוי - תקינים, ומוכרים למשתמשים ולמנהלנים.**
3. הימנעו מהפעלת קישורים או צרופות בהודעות (מייל, וואטסאפ, רשתות חברתיות, SMS או כל מנגנון תקשורת אחר) ממקורות שאינם מוכרים, ואף ממקורות מוכרים אם הנושא, התוכן או תזמון ההודעה נראים מוזרים, חשודים או לא סבירים. במקרים אלו יש לפנות לשולח **בערוץ תקשורת שונה** על מנת לוודא האם ההודעה אכן נשלחה ממנו.
4. וודאו כי לא מותקנות תוכנות לא מוכרות על המחשב שלכם. ארגונים – מומלץ לבחון האפשרות למימוש מנגנון מסוג Application Control השולט אילו תוכנות יכולות לפעול על מחשבי המשתמשים השונים.
5. התקינו תוכנות הגנה (AV/EDR) על מחשבי המשתמשים, נטרו התרעות שמגיעות מהן, והגיבו להן בהתאם לנהלי הארגון.
6. הגבילו גישה מרחוק אל מחשבי הארגון לכתובות ידועות, או השתמשו ב-VPN או ZTNA עם הצפנה והזדהות חזקה מתאימה.
7. להתרעה זו מצורף קובץ מזהים. מומלץ לנטרם בכל מערכות האבטחה הארגוניות הרלוונטיות. כן מומלץ לוודא כי המזהים מההתרעה בקישור מס' 1 גם הם מוגדרים במערכותיכם.
8. נבקש לעדכן את מערך הסייבר הלאומי בכל מקרה של זיהוי אחד או יותר ממזהים אלו במערכותיכם.
9. העבירו את כלל עובדי הארגון, **ובפרט מנהלנים**, **ועובדים הניגשים למערכות מרשת האינטרנט**, להזדהות חזקה העמידה בפני דיוג (Phishing Resistant MFA). ראו פרטים נוספים בקישורים
https://www.cisa.gov/sites/default/files/publications/fact-sheet-implementing-phishing-resistant-mfa-508c.pdf
https://learn.microsoft.com/en-us/security/zero-trust/sfi/phishing-resistant-mfa
10. וודאו כי כלל מערכות סינון הדוא"ל הארגוניות מוגדרות באופן המיטבי להתמודדות עם מתקפות דיוג.
11. וודאו כי כלל מערכות הארגון, ובפרט המערכות המוזכרות בסעיף הקודם, וכן שרתי הדוא"ל הארגוני ומערכות הקצה של המשתמשים, מעודכנות באופן עיתי עם עדכוני האבטחה העדכניים ביותר של היצרן.
12. **גם אם כעת אין אפשרות לשחזר את הקבצים המוצפנים באמצעות גיבוי או הפיכת ההצפנה, הימנעו מלפרמט את הדיסקים או לכתוב עליהם דבר. החליפו אותם בדיסקים חדשים והתקינו מחדש את המחשבים. את הדיסקים המוצפנים שמרו במקום בטוח למקרה שבעתיד תימצא דרך להפיכת ההצפנה.**

## צילומי מסך


המערכת "נעולה" – ישות קוברה השתלטה | קבצים מוצפנים
02:13:28:49
ברמה צבאית AES-256 הקבצים החשובים במחשב שלך הוצפנו באמצעות הצפנת
המסמכים, הסרטונים, התמונות ושאר הקבצים שלך אינם נגישים כעת, ולא ניתן לפתוח אותם ללא מפתח הפענוח
מפתח זה מאוחסן כרגע על שרת מרוחק
כדי לקבל את המפתח, יש להעביר את תשלום הביטקוין לכתובת הארנק שצוינה לפני שהזמן יאזל
אם לא תנקטו פעולה במסגרת הזמן הזה, מפתח הפענוח יושמד והגישה לקבצים שלך תאבד לצמיתות
במקרה, אם אתה לא יודע איך לרכוש ולהעביר את הביטקוין – אתה יכול להשתמש בכל ממע חיפוש


---------- הודעה מועברת ----------
מאת: <notifications-@a-world.eu>
אל: <
עותק:
תאריך: יולי 1, 2025 6:27
נושא: מסמך מסוג חשבונית מס קבלה
96
eset Digital Security Progress. Protected.
חנות האנטי וירוס של ESET
שלום ,
קיבלת חשבונית מס קבלה - 404243
לצפייה במסמך
לחיצה על הלינק מהווה הסכמתך לקבל מסמך חתום דיגיטלית
פגשת פעם מישהו שאוהב ניירת? גם אנחנו לא..
אין על חשבוניות דיגיטליות - הכי קל, נוח וירוק שיש.
60 ימי נסיון

---------- הודעה מועברת ----------
מאת: ESET HOME < @ertik.eu <mailto:r @ertik.eu> >
אל: @walla.com>
עותק:
תאריך: יוני 2, 2025 19:29
נושא: מסמך מסוג חשבונית מס קבלה מספר 409306

96
-->
<https:// s3-eu-west-1.amazonaws.com/6471.png?v=2>
חנות האנטי וירוס של ESET

שלום,

=

קיבלת חשבונית מס קבלה - 409306

לצפייה במסמך <https://postil.blog/InvoiceReceipt_409306>

לחיצה על הלינק מהווה הסכמתך
לקבל מסמך חתום דיגיטלית.

...פגשת פעם מישהו שאוהב ניירת? גם אנחנו לא

.אין על חשבוניות דיגיטליות - הכי קל, נוח וירוק שיש

ימי נסיון 60 <https://postil.blog/InvoiceReceipt_409306>

<https://postil.blog/InvoiceReceipt_409306>
<https://postil.blog/InvoiceReceipt_409306>

---------- הודעה מועברת ----------
מאת: <"notifications@ "< @a-world.eu <mailto:%22notifications@ a-world.eu> >
אל: < @walla.co.il>
עותק.
תאריך: יולי 1, 2025 9:54
נושא: מסמך מסוג חשבונית מס קבלה

96
<https:// s3-eu-west-1.amazonaws.com/6471.png?v=2>
חנות האנטי וירוס של ESET

שלום , @walla.co.il

קיבלת חשבונית מס קבלה - 404243

לצפייה במסמך <https://postil.ceo/InvoiceReceipt_404243>

לחיצה על הלינק מהווה הסכמתך
לקבל מסמך חתום דיגיטלית.

...פגשת פעם מישהו שאוהב ניירת? גם אנחנו לא

.אין על חשבוניות דיגיטליות - הכי קל, נוח וירוק שיש

ימי נסיון 60 <https://postil.ceo/InvoiceReceipt_404243>

<https://postil.ceo/InvoiceReceipt_404243>
<https://postil.ceo/InvoiceReceipt_404243>

## מקורות

1. https://www.gov.il/he/pages/alert_1883c
2. https://www.gov.il/he/pages/alert_1992
3. https://www.gov.il/he/pages/alert_1939
4. https://www.gov.il/he/pages/alert_1849
5. https://www.gov.il/he/pages/alert_1403