



העדכון שלפניכם לוקט ועובד במסגרת פעילות ה-CERT הלאומי על בסיס מגוון מקורות רחב, כדי לרכז מידע רלוונטי ואקטואלי לעוסקים בתחום הגנת הסייבר. כפועל יוצא, ה-CERT הלאומי אינו יכול לערוב לחלוטין למידע המובא בעדכון או למסקנות המשתמעות ממנו, ואין באמור בעדכון משום המלצה לנקיטת פעולות כלשהן או לשינוי מדיניות אבטחה קיימת. אין באזכור חברות אבטחה או גורמים מסחריים אחרים משום הבעת עמדה או המלצה ביחס אליהם או לשיירותים או המוצרים המוצעים על ידם.

25 נובמבר 2015

י"ג כסלו תשע"ו

סימוכין: י-ס-162

## הנדון: התרעה על מערך התקיפה CopyKittens

### תיאור:

לאחרונה התקבל מידע ב-CERT הלאומי על מערך תקיפה בשם CopyKittens התוקף יעדים ישראלים כגון גופי ממשל, אקדמיה ומחקר במזרח התיכון. המערך משתמש בכלים מפיתוח עצמי ובכלי קוד פתוח בהם הוא מבצע שינויי קוד לצורך מטרתיו ופועל באמצעות תהליך תקיפה רב-שלבי שנועד להקטין את הסבירות לחשיפת פעילותו.

### תהליך התקיפה כולל את השלבים הבאים:

1. שליחת הודעת דוא"ל ייעודית לנתקפים (Spear Phishing) המכילה דבוקה זדונית. הפעלת הדבוקה מייצרת שני קבצים במחשב הקורבן:
  - א. קובץ PDF המשמש להתממת ההודעה.
  - ב. קובץ זדוני אשר ממשיך את תהליך ההדבקה.
2. יידוע התוקף על הצלחת ההדבקה באמצעות הורדת קובץ תמונה בסיומת png. משרת הפיקוד והשליטה (C&C) של התוקף.
3. בדיקת ריצה במכונה וירטואלית וב-Sandbox, על מנת לחמוק מחקירה בידי מומחי אבטחה.
4. במידה והבדיקה הינה חיובית, הפוגען יעדכן את התוקף על ניסיון החקירה, יפסיק את פעילותו וינסה למחוק את הקבצים הזמניים שיצר עד כה.
5. במידה והבדיקה הינה שלילית, הפוגען ימשיך בהדבקה ויזריק קוד זדוני המאפשר שליטה מרוחקת על מחשב הקורבן (RAT) לתהליך לגיטימי שרץ בזיכרון הווירטואלי של המחשב. הזלגת המידע ממחשב הקורבן לתוקפים יתבצע באמצעות פרוטוקול DNS.
6. ביצוע פעולות לשיפור שרידות:
  - א. רישום ל-Registry לצורך שרידות הפעלה מחדש.
  - ב. יצירת משימה מתוזמנת המבצעת מחדש את הזרקת הקוד הזדוני לתהליך בזיכרון בכל 20 דקות.

### אינדיקטורים (IOC)

(Indicators Of Compromise) - מאפיינים שנצפו ברשת או במערכת ההפעלה שעשויים להעיד על חדירה או פגיעה במערכות מחשב.

המזהים שנצפו מצורפים כדבוקה. תשומת לבכם כי היות ומערכי התקיפה הינם דינמיים, יתכן וחלק מהמזהים ששימשו לתקיפה בעבר לא ישמשו בהכרח לתקיפות נוספות.

ניתן לשתף מידע המסווג "ירוק" עם כל הגורמים העשויים לעשות בו שימוש מועיל. עם זאת, אין לשתפו בערוצים פומביים, דוגמת אתרי אינטרנט, רשתות חברתיות ואמצעי תקשורת המונים.



Prime Minister's Office  
National Cyber Event Readiness Team



משרד ראש הממשלה  
המרכז הלאומי להתמודדות עם איומי סייבר

TLP: ירוק  
- 2 -

### קישורים ומידע נוסף:

- <https://s3-eu-west-1.amazonaws.com/minervaresearchpublic/CopyKittens/CopyKittens.pdf>
- <http://www.clearskysec.com/report-the-copykittens-are-targeting-israelis/>

במידה שבבדיקתכם התגלה ממצא כלשהו נבקש לקבל היזון חוזר.  
לכל מידע נוסף ניתן לפנות אלינו .

**בברכה,**

**CERT-IL**

**טל: 03-7450801**

[team@cert.gov.il](mailto:team@cert.gov.il)

ניתן לשתף מידע המסווג "ירוק" עם כל הגורמים העשויים לעשות בו שימוש מועיל. עם זאת, אין לשתפו בערוצים פומביים, דוגמת אתרי אינטרנט, רשתות חברתיות ואמצעי תקשורת המונים.