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 ישראליים כגון גופי ממשל, אקדמיה ומחקר במזרח התיכון. המערך משתמש בכלים מפיתוח עצמי ובכלי קוד פתוח בהם הוא מבצע שינויי קוד לצורך מטרותיו 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.

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