

18 דצמבר 2018  
י' טבת תשע"ט  
סימוכין : ב-ס-800

### קמפיין תקיפה גלובלי כנגד ארגונים ביטחוניים ותשתיות קריטיות

#### תקציר

לאחרונה דווח כי זוהה קמפיין תקיפה גלובלי כנגד ארגונים במגזרי ההגנה, האנרגיה, הגרעין, ושירותים פיננסיים. התקיפה בוצעה באמצעות קובץ וורד עם מקרו זדוני.

#### פרטים

על פי [הדיווח](#), הותקפו לפחות 87 ארגונים. התקיפה הוסוותה כניסיונות גיוס עובדים לתפקידים שונים. פתיחת קובץ הוורד הנגוע הפעילה מקרו אשר הזריק קוד זדוני לתוך הזיכרון שבשימוש תוכנת וורד. קוד זה שימש להורדת השלב השני של הפוגען, המשמש לאיסוף המידע על העמדה והמשתמש והעברתו לתוקף. מעבר לאיסוף מידע, הפוגען יכול גם להריץ פקודות שונות.

#### דרכי התמודדות

מצ"ב קובץ אינדיקטורים. מומלץ לנטרם במערכות הארגוניות. מומלץ לחזור ולהדגיש למשתמשים כי יש להפעיל שיקול דעת בנוגע לפתיחת צרופות או קישורים שהגיעו משולחים לא מוכרים או שהגיעו באופן בלתי צפוי אף משולחים מוכרים. מומלץ לפתוח קבצים מרשת האינטרנט רק כאשר הפעלת המקרו ב- Office מנוטרלת, ותחת Protected View בלבד. יש לנקוט במשנה זהירות אם מופיעות התרעות לגבי הצורך בנטרול אמצעי הגנה אלו.

לכל מידע נוסף ניתן לפנות אלינו. במידה שעלו ממצאים בבדיקתכם, נבקש לקבל היזון חוזר.

**הערה: שיתוף מידע עם ה-CERT הלאומי איננו מחליף חובת דיווח לגוף מנחה כלשהו, במידה שהתגלה צורך כזה**

בברכה,



**CERT-IL**

**טל: \*9344**

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