11 יוני 2018
כ"ח סיוון תשע"ח
סימוכין: ב-ס-635

קבצי אקסל עם סיומת IQY משמשים לתקיפת עמדות קצה

תקציר

קבצי אקסל מסוג Excel Web Query (.iqy), מצורפים להודעות דוא"ל הנשלחות על ידי הבוטנט Necurs.

הפעלת הקבצים על ידי המשתמש, למרות הודעות האזהרה של התוכנה, תביא להורדת פוגען מהרשת ולתקיפת העמדה.

פרטים

פורמט קובץ IQY מאפשר להוריד תוכן ישירות מרשת האינטרנט לתוך תוכנת אקסל.

מאחר והפורמט הינו של קובץ טקסט פשוט, מערכות AV אינן מזהות אותו בדרך כלל כאיום, אינן חוסמות את הקובץ ומאפשרות לו להגיע אל הנמען.

פתיחת הקובץ המצורף לקמפיין התקיפה, תביא להרצת קוד אשר יתקין פוגען מסוג RAT על העמדה.

הבוטנט Necurs שיגר בתקופה האחרונה מספר קמפיינים של תקיפה המבוססים על שימוש בקובץ מסוג זה.

דרכי התמודדות

מומלץ לצפות בקבצי Office שמקורם באינטרנט רק כאשר Protected View מופעל ופונקציית ה-Macros מנוטרלת.

אין להתעלם מהודעות אזהרה של התוכנה, ואין לנטרל מנגנוני הגנה, גם אם ההודעות ו/או המידע בקבצים מציעים לעשות זאת.

יש להפעיל שיקול דעת לגבי פתיחת הודעות, הפעלת צרופות או לחיצה על לינקים בהודעות בלתי-צפויות המגיעות מרשת האינטרנט, גם אם מקור ההודעה מוכר. במקרה של ספק, מומלץ להימנע מפתיחת ההודעה ולבדוק מול הגורם השולח האם אכן שלח אלינו הודעה.

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

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

בברכה,
CERT-IL
טל: 9344*
team@cert.gov.il