18 נובמבר 2015

ו' כסלו תשע"ו

סימוכין: י-ס- 160

הנדון: התרעה על פוגען "Brobot" and "Kamikaze/Toxin"

תיאור: לאחרונה התקבל ב - CERT הלאומי דיווח על הפוגענים "Brobot" ו - "Kamikaze/Toxin" המשמשים לתקיפת מניעת שרות מבוזרת (DDOS). הפוגענים הינם קוד PHP המושתל לתוך תיקייה נסתרת במערכות CMS של אתרי אינטרנט תוך שימוש בחולשות ידועות. מטרת הפוגענים היא להשתמש בשרת הנגוע לצורך ביצוע תקיפות DDOS על שרת צד ג'.

אינדיקטורים (IOC)

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

כלל המזהים שנצפו מצורפים כדבוקה.

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

במידה שבבדיקתכם 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: 03-7450801

team@cert.gov.il