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 לשירותים או המוצרים המוצעים על ידם.

21 אוקטובר 2015

ח' חשון תשע"ו

סימוכין : י-ס- 155

הנדון: התרעה על פוגען Bedep

תיאור: לאחרונה אנו עדים לעלייה במספר התקיפות באמצעות Angler Exploit Kit אשר מובילות להורדה והתקנה של הפוגען הנ"ל. פוגען זה מנצל את הפלטפורמה הנתקפת על מנת לבצע "הונאת קליקים", או כפלטפורמה להורדה של פוגענים נוספים למחשב הנתקף.

למסמך זה מצורף קובץ IOC's

קישורים ומידע נוסף:

1. http://www.malware-traffic-analysis.net/2015/10/18/index.html
2. https://asert.arbornetworks.com/bedeps-dga-trading-foreign-exchange-for-malware-domains/
3. http://malware.dontneedcoffee.com/2015/01/unpatched-vulnerability-0day-in-flash.html
4. http://blog.trendmicro.com/trendlabs-security-intelligence/bedep-backdoors-brought-into-the-light-by-flash-zero-days/
5. http://www.trendmicro.com/vinfo/us/threat-encyclopedia/web-attack/148/putting-issues-of-bedep-to-bed

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.

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

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.