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.

28 ינואר 2015

ח' בשבט תשע"ה

סימוכין : י-ס- 69

תקיפה נרחבת על יעדים בישראל במתווה שליחת דוא"ל המכיל צרופה נגועה

1. **ביממה האחרונה התקבלו ב- CERT הלאומי דיווחים אודות גלי תקיפה מרובים ובהיקף נרחב על ארגונים גדולים במשק הישראלי, באמצעות מתווה דוא"ל המכיל צרופה נגועה בפוגען** (פרטים מזהים מצורפים).
2. מבדיקה ראשונית אפשר ומדובר בגרסא של פוגען כופר (Ransomware) מסוג Crypto-locker, אשר מוכר כי תקף יעדים שונים בישראל במהלך החודש האחרון.
3. ברקע, המתיחות הביטחונית מאז ה-17 בינואר והחשש בעקבות האירועים האחרונים להתגברות תקיפות סייבר במרחב הסייבר הישראלי, מצד גורמים עוינים.
4. **לאור ניסיון העבר, מומלץ למקד מאמץ הגנתי מול תקיפות סייבר מסוגים שונים, לרבות:**

תקיפות מניעת שירות מבוזרת (DDOS), פוגענים למחיקות נתונים (Crypto-lockers/Wipers) **ברשתות ארגוניות, תקיפות והשחתות אתרים וסוגי תקיפות נוספים.**

דוגמה למתווה הדוא"ל

From: Mikaela Clayborne [mailto: adjourns@efleets.com]

Subject: RIMINI SAIL SRL

Content:

39, Viale Murano 47838 Riccione (RN)

Riccione

ITALY

Attachment: rimini_sail_srl.cab

צעדי הגנה מומלצים בסייבר

5. חסימת הודעות דוא"ל המכילות צרופות עם סיומות cab. ו- exe. (המתחזה ל-PDF, כמוכר מתקיפת Crypto-locker) בשרתי Mail Relay.
6. הגברת עירנות במערכות הניטור וההגנה (IDS, IPS) בהתאם למזהים המצורפים, ובכלל.

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.

7. הגברת עירנות בקרב עובדי הארגון מפני אפשרות לקבלת הודעות ממקורות בלתי-מזוהים, בדגש על המזהים הנ"ל.

8. **כחלק מקידום מאמצי ההגנה הלאומיים בסייבר, ה-CERT הלאומי מבקש להתעדכן בתמונת המצב במידה ומאותרות תקיפות סייבר חריגות במתווה המוזכר, וכן בכל מתווה אחר. בתוך כך, נשמח לשיתוף מידע אודות הממצאים הרלוונטיים ממערכות הניטור, הזיהוי והחקירה שברשותכם.**

9. **ה- CERT הלאומי עומד לרשותכם לטובת מתן מענה וסיוע בכל אירוע סייבר.**

הערה: שיתוף מידע עם ה- CERT הלאומי איננו תחליף לחובת הדיווח לגוף מנחה כלשהו, במידה והתגלה צורך לכך.

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.