



OpJerusalem 2022 – סיכום פעילות

הבהרה



מסמך זה מופץ למשק בפרוטוקול-לבן TLP ומיועד לדרג הנהלה בארגונים. לאור מאפייני האירוע שבחלקו כלל מידע רגיש לא כל המידע מפורט בדוח זה, מידע ממוקד הועבר לגורמים הרלוונטיים וטופל בזמן אמת.

תקציר



1. קמפיין יום ירושלים האיראני, המוכר גם בכינויו OpJerusalem ו-AlqudsDay – מציין את הזדהות העם האיראני עם המאבק הפלסטיני.
2. הקמפיין מתקיים מדי שנה ביום שישי האחרון של חודש הרמדאן, ומתאפיין בהפגנות ברחבי איראן והרשות הפלסטינית, וכן בפעילות התקפית אנטי ישראלית במרחב הסייבר.
3. השנה הקמפיין היה צפוי להתחיל ב-29.04 ולהמשך מספר ימים לפני/אחרי.
4. בשנים עברו, התמקדו התקיפות בניסיונות להשחתת אתרים, ובניסיונות לגרימת נזק משמעותי ברשתות מידע ארגוניות.
5. מטרתו של מסמך זה הן לפרט את הפעילות שבוצעה בציר ההגנתי כנגד צעדי התוקפים ולגבש המלצות לקמפיינים הבאים.

ניתן לשותף מידע המסווג "לבן" עם כל קבוצת הנמענים, לרבות ערוצים פנימיים



רקע



1. מטרת הקמפיין: יצירת הד תקשורתי וקידום אג'נדה אנטי ישראלית, לעורר בהלה בקרב הציבור הישראלי, חשיפת מידע אישי, השחתת אתרים, פגיעה באמון הציבור ועוד.
2. שיטות תקיפה נפוצות:

- ניסיונות להתקפות מניעת שירות (DoS/DDos).
- ניסיונות לחדירה למאגרי נתונים והדלפת מידע.
- ניסיונות להדבקה בנוזקות כופרה (Ransomware).
- ניסיונות להשחתת אתרי אינטרנט (Defacement).
- ניסיונות לפריצה לשרתי ארגונים וחברות.

פעולות מקדימות שבוצעו



1. הפצת מסמך המלצות הגנה כללי למשק.
2. הרחבת קבוצת מובילי אבט"מ וסייבר וחברות IR.
3. הפצת פרסומי מודעות באתר המערך ורשתות חברתיות.
4. הכוונת מגזר חברות אירוח אתרים (Hosting) אודות פעילות תוקפים אל מול מרחב הסייבר הישראלי והפצת מסמך TOP7 המלצות ממוקדות.

ניתן לשתף מידע המסווג "לבן" עם כל קבוצת הנמענים, לרבות ערוצים פנימיים

השתלשלות האירועים**1. 16/4:**

- קבוצת DragonForce המלזית פרסמה בערוץ דיסקורד ייעודי כוונה לבצע DDoS מול מספר ארגונים, ביניהם אתרי השב"כ ואוניברסיטת תל אביב.
- כמו כן הקבוצה טענה שפרצה ללשכת שמאי המקרקעין והפיצה סרטון הממחיש גישה ל-DB.

2. 19/4:

- בפורום קבוצות תקיפה אינדונזיות פורסם כי יש כוונה לבצע מתקפת DDoS מול אתר idf.il.

3. 20/4:

- קבוצת ההאקרים Altahrea Team הודיעו כי החלו לתקוף את האתר של רשות שדות התעופה (ככל הנראה ניסיונות למניעת שירות).

4. 24/4:

- קבוצת Hackers Of Savior פרסמו אודות הקמת ערוץ גיבוי חדש בטלגרם.

5. 25/4:

- קבוצת Hackers Of Savior פרסמה סרטון הממחיש קבלת גישה למאגרי מידע של בנקים ישראלים הכוללים חשבונות של לקוחות.
- כמו כן שיגרו איומים לתקיפות סייבר נוספות במסגרת קמפיין יום ירושלים.
- חוקרי אבטחת מידע פרסמו דוח מפורט המציג כי הסרטון ערוך וכי לא התבצעה פריצה לרשתות הבנקים, מדובר בחלק מניסיונות ליצור רעש סביב אירועי יום קודס.

ניתן לשתף מידע המסווג "לבן" עם כל קבוצת הנמענים, לרבות ערוצים פנימיים

6. 27/4:

- קבוצת JE ARMY (צבא ירושלים) פרסמו כי הם הצליחו לחדור לשתיים מים באזור עוטף עזה – דיווח שהתברר בהמשך כמזויף.

7. 28/4:

- קבוצת Hackers Of Savior פרסמו כי הצליחו להשחית מספר אתרים ישראליים ההשחתות טופלו והאתרים חזרו לפעילות תוך פחות משעה.
- כמו כן הקבוצה פרסמה כי הצליחה להשתלט על מספר אתרים של ערוצי רדיו, אותר ווקטור התקיפה, טופל ע"י חברת הסטרימינג.

8. 29/4:

- DragonForce הודיעו כי הצליחו לגנוב סיסמאות ממשקי הניהול של כ-200 אתרים – טופל ע"י חברת בניית האתרים.

לסיכום – נראה כי גם השנה רוב קבוצות התקיפה התמקדו ב-Low Hanging Fruits – תקיפות פשוטות יחסית כגון השחתת אתרים ומניעת שירות, במטרה לגרום לנזק תודעתי והפחדה בקרב אזרחי מדינת ישראל. כמו כן רואים עלייה בפרסומים פיקטיביים.

המלצות לקמפיינים הבאים

1. הרחבה ושימור קבוצת שיתוף מידע משקי.
2. הפצת מסמכים ממוקדים וישימים למגזרים נוספים.
3. קידום הצטרפות של גופי המשק לסייברנט לטובת שיתוף מידע ופעולה בזמן אמת.
4. הפצה שוטפת של תוצרי מודעות לציבור ולארגונים.
5. הרחבת השיח השוטף עם CERTים בעולם לטובת קידום מהלכים אופרטיביים.
6. התמודדות יעילה מול תעמולה פיקטיבית.

ניתן לשותף מידע המסווג "לבן" עם כל קבוצת הנמענים, לרבות ערוצים פנימיים