

כ"ח אדר ה'תשפ"ג

21 מרץ 2023

# המלצות הגנה לארגונים ואזרחים – Oplrael

רקע



קמפיין Oplrael הינו קמפיין התקפי אנטי-ישראלי מתואם במרחב הסייבר, הנערך מדי שנה ב-7 באפריל, ובימים לפניו ואחריו, במטרה להסב נזק למשק הישראלי. הקמפיין מזוהה עם ארגון אנונימוס (Anonymous), ובאופן עקבי משתתפים בו האקטיביסטים וקבוצות תקיפה פרו-פלסטיניים. ה-CERT הלאומי מנהל פעילות פרואקטיבית לאורך השנה לצורך מוכנות מיטבית למבצע, בדגש על קבוצות ושחקנים המעוניינים לקחת בו חלק, כלי תקיפה, שיטות ומתווי תקיפה ויעדים פוטנציאליים. על פי רוב, פשעי הסייבר שהן יוזמות במהלך פעילותן מיועדים ליצירת הד תקשורת, ניסיון להפחדת הציבור והעברת מסרים פוליטיים.

עיקר ההתקפות במסגרת הקמפיין מתאפיינות בהשחתות אתרים, מתקפות למניעת שירות, חדירה למאגרי נתונים והדלפת מידע, גניבת מידע אודות משתמשים, הדלפת נתונים חוזרים מתקיפות קודמות, תקיפות כופר, ניצול חולשות ברכיבי IOT לתקיפות מניעת שירות מבוזרות ועוד.

בעקבות זאת מערך הסייבר הלאומי גיבש מסמך המלצות להעלאת החוסן מפני איומי סייבר אצל כלל הארגונים והאזרחים.

המלצות הגנה ליישום



## 1. עדכוני אבטחה –

1.1. סגירה בהקדם האפשרי של פגיעויות שכיחות המנוצלות לרעה. בהקשר זה מומלץ לעקוב אחר התרעות המתפרסמות באתר מערך הסייבר ואף להתמקד ב**חמש החולשות החמורות** שנוצלו השנה לתקיפות סייבר בישראל.

1.2. הסרה של רכיבי תוכנה ללא תמיכת יצרן מלאה (EOL) דוגמת Windows XP, 7, Vista וכדומה.

## 2. אתר האינטרנט –

2.1. שימוש והגדרת מערכת ה-WAF להפעלת Bot Mitigation, זיהוי חתימה ייחודית של התקיפה, חסימתה וכד'.

2.2. ביצוע גיבוי offline לתוכן האתר וכלל המידע הרלוונטי.

2.3. הגבלת גישה לממשקי הניהול של האתר באמצעות MFA.

2.4. בחינה כי האתר פותח בהתאם לעקרונות פיתוח מאובטח מקובלים

2.5. ווידוא עדכניות כלל הרכיבים באתר, לרבות ספריות קוד פתוח (Open Source) פגיעות.

2.6. בחינת שימוש בשירות Anti DDoS של ספקיות התקשורת.

## 3. הגנה מפני תקיפת DoS/DDoS על אתר האינטרנט –

3.1. שימוש והגדרת מערכת WAF כולל Bot Mitigation, זיהוי חתימה ייחודית של התקיפה, חסימתה וכד'.

3.2. בחינת האפשרות לביצוע פעולות כגון:

3.2.1. חסימת תעבורה ממדינות בעלות פוטנציאל סיכון (על בסיס Geo Location).

3.2.2. במקרים חריגים של תקיפה מחו"ל - חסימה גורפת של פניות מחו"ל.

3.2.3. חסימה ב-FireWall של כתובות הידועות כבעלות מוניטין בעייתי או עוין (על בסיס IP Reputation).

3.2.4. זיהוי וחסימת כתובות של שירותים כגון TOR או Anonymizer המאפשרים גלישה אנונימית.

3.2.5. העברת האתר לענן במידת הצורך.

שיתוף מידע עם ה-CERT הלאומי אינו מחליף חובת דיווח לגוף מנחה כלשהו, ככל שחלה על הגוף חובה כזו. המידע נמסר כפי שהוא (as is), השימוש בו הוא באחריות המשתמש ומומלץ להיעזר באיש מקצוע בעל הכשרה מתאימה לצרכי הטמעתו.

