

היערכות לקראת מתקפת סייבר Op-Israel 2024

- כל שנה, בתחילת אפריל (7.4), מתרחשת מתקפת סייבר המכונה #OP-Israel שנערכת על ידי אקטיביסטים מרחבי העולם כתגובה לסכסוך הישראלי-פלסטיני, כאשר היא משתמשת בפשעי סייבר ליצירת הד תקשורתי ולהפחדת הציבור הישראלי.
- כמו כן, כבר ביום שישי הקרוב (5.4), צפויות להתרחש מתקפות במסגרת יום ירושלים האירני - #OpJerusalem.
- על פי אינדיקציות שאנו מקבלים ממערכת המודיעין שלנו, ממערך הסייבר הלאומי ומגורמים שונים, נראה שחברות ישראליות רבות ממגזרים שונים כמו תחבורה, ממשלה, תשתיות ועוד, מופיעות ברשימת היעדים הפוטנציאליים של המתקפה.
- כידוע, ארגונים ישראליים מותקפים באופן קבוע גם בשגרה, ולא דורשת מאורע מיוחד או תאריך מסוים כדי להתרחש, אך כמות התקיפות הצפויה להתרחש במסגרת Op-Israel צפויה לשבור שיאים חדשים, על רקע המלחמה בעזה.
- עיקר ההתקפות הצפויות במסגרת הקמפיין מתאפיינות בהשחתה/השבתה של אתרי אינטרנט, חדירה למאגרי נתונים והדלפת מידע רגיש, גניבת מידע ממשתמשים באמצעות טכניקות פישינג שונות, תקיפות כופר, ניצול חולשות מוכרות חדשות וישנות, השתלטות על מערכות IOT של בתים חכמים, פריצת חשבונות בנק וכו'.
- מודעות מבוססת לאיומים ופעולות הכנה מקדימות להתגוננות מפני "הנורא מכל", עשויות לסייע למזער את פוטנציאל הנזק.

היערכות לקראת מתקפת סייבר Op-Israel 2024

- על מנת להישמר ולהיערך בצורה המיטבית ביותר כנגד מתקפות אלו, אנו ממליצים ליישם את ההנחיות הבאות:

- **בפן הארגוני:**

- עדכון התוכנות, האפליקציות ומערכות ההפעלה שברשותכם עשוי לעזור ולמזער למינימום את "משטח התקיפה" הקיים.
- סגירה מיידית של פגיעויות שכיחות המנוצלות לרעה – תוך מיקוד בחמש החולשות החמורות שנוצלו השנה לתקיפות סייבר בישראל.
- שימוש והגדרה במנגנון אימות רב-שלבי (MFA) לממשקי הניהול של האתר ושל כלל הממשקים החשופים לאינטרנט.
- חסימת מדינות עויינות בעלות פוטנציאל סיכון והטמעת מזהים זדוניים לניטור ולחסימה בכלל מנגנוני האבטחה של הארגון.
- טיוב והגדרה של מערכת ה-WAF, כולל מנגנוני Bot Mitigation, איזון עומסים (Load Balancer) וחיבור רכיבים לניטור במערכת ה-SIEM.
- הגדרה וניטור מוקפד על התרעות שמתקבלות ממערכת ה-EDR.
- תדרוך והגברת הערנות של עובדי הארגון מפני מתקפות פשינג אפשריות באמצעות המייל/רשתות חברתיות/SMS וכו'.
- ביצוע גיבוי offline של מידע רגיש ושל כל תוכן האתר, תוך בחינת שימוש בשירות Anti DDoS של ספקיות התקשורת.
- ממליצים להתעדכן באופן קבוע בחדשות סייבר עדכניות ובאזהרות הקשורות בקמפיין ולמלא אחר ההנחיות הנדרשות.

היערכות לקראת מתקפת סייבר Op-Israel 2024

■ בפן האישי:

- יש לוודא כי התוכנות, האפליקציות ומערכות ההפעלה מעודכנות עבור כלל המכשירים שבשימוש.
- יש לנקוט משנה זהירות מהודעות חשודות (SMS/דוא"ל/רשתות חברתיות) ולהימנע מפתיחת קבצים מצורפים או לחיצה על קישורים ממקורות לא ידועים. יש לאמת את פרטי השולח של כל הודעה שמתקבלת.
- הקפדה על שימוש בסיסמאות חזקות וייחודיות עבור כל חשבון ולאפשר אימות דו-שלבי במידת האפשר.
- הימנעות מפרסומות/תכנים ממומנים במדיה החברתית או הצעות חשודות שנראות טובות מכדי להיות אמיתיות.
- גבה באופן קבוע את הנתונים החשובים שלך למיקומים מאובטחים או לכוננים חיצוניים כדי להפחית את ההשפעה של התקפות פוטנציאליות כמו תוכנות כופר.
- מומלץ לאפשר סינון דואר אלקטרוני ותוכנות זיהוי ספאם כדי להפחית את הסבירות לקבלת הודעות דיג או קבצים מצורפים זדוניים.
- יש לוודא שימוש במערכות אנטי וירוס/חומת אש אמינות ומעודכנות לזיהוי ומניעת נזקות במכשירים האישיים.
- מומלץ לבדוק באופן שוטף ולדווח על כל פעילות חשודה בחשבונות האישיים (חשבון בנק, ארנקים דיגיטליים וכד') לספק השירות הרלוונטי או לגורמי האכיפה.
- ממליצים להתעדכן באופן קבוע בחדשות סייבר עדכניות ובאזהרות הקשורות בקמפיין ולמלא אחר ההנחיות הנדרשות.

היערכות לקראת מתקפת סייבר Op-Israel 2024

המלצות:

- אנו ממליצים לעקוב אחר ההנחיות המוזכרות ולהעבירן לכלל העובדים על מנת לשמור על אבטחתם מפני המתקפות הצפויות בשבוע הקרוב.
- ממליצים להישאר מעודכנים בחדשות הסייבר שמפורסמות על ידינו ועל ידי מערך הסייבר.

קישורים להרחבה:

- [מערך הסייבר הלאומי \(www.gov.il\)](http://www.gov.il)

