

07 אוקטובר 2023  
כ"ב תשרי תשפ"ד  
סימוכין: ב-ס-1626

## מניעת תקיפות מניעת שירות מבוזרות (DDoS) כנגד ארגונים בישראל

### תקציר



1. כחלק מההיערכות הכללית במשק למצב המלחמה, צפויות להתבצע מתקפות מניעת שירות כנגד ארגונים שונים במשק.
2. מטרת מסמך זה, הכרת מאפייני התקיפה והמלצות להתגוננות מפניה.

### פרטים



1. מתקפת מניעת שירות מבוזרת (Distributed Denial of Service) הינה תקיפה בה התוקף מפעיל מספר רב של מקורות להעמסת התעבורה אל אתרי הארגון המותקף או שירות חיוני עליו נסמך הארגון (כגון DNS).
2. לתקיפה זו 2 סוגים עיקריים:
  1. תקיפת נפח (Volumetric) בה התוקף מציף את קווי התקשורת של הארגון בתעבורה לא רצויה.
  2. תקיפה אפליקטיבית בה התוקף מציף את שרתי הארגון בפניות הגוזלות מהם זמן עיבוד רב.
3. התוצאה מבחינת חווית המשתמש באתר היא שאתרי הארגון אינם נגישים, או שלוקח להם זמן רב מאד להגיב.

## דרכי התמודדות



1. התמודדות עם תקיפת מניעת שירות מבוצרת מחייבת בדרך כלל את הארגון לשתף פעולה עם גורמים המתמחים בכך, מאחר ולרוב רוחב הפס שהתוקפים יצליחו להעמיד לצורך התקיפה גדול מרוחב הפס של הארגון.
2. מומלץ לבחון שימוש בשירות Anti DDoS של ספקיות תקשורת/אינטרנט או חברות ייעודיות. מומלץ להתאים יחד עם הספק הרלוונטי את הטיפול לדרישות הארגון.
3. מומלץ לבחון חסימת תעבורה ממדינות בעלות פוטנציאל סיכון (על בסיס Geo Location). מומלץ לבצע את החסימה בשיתוף ספק התקשורת על מנת למנוע העמסת רוחב הפס בין הספק לארגון.
4. במקרים חריגים מומלץ להיעזר בספק/חברה לחסימה גורפת של תעבורה מחו"ל.
5. מומלץ שימוש והגדרת מערכת WAF כולל Bot Mitigation, זיהוי חתימה ייחודית של התקיפה, חסימתה וכד'.
6. מומלצת חסימה של כתובות הידועות כבעלות מוניטין בעייתי או עוין (על בסיס IP Reputation).
7. מומלץ זיהוי וחסימת כתובות של שירותים כגון TOR או Anonymizer המאפשרים גלישה אנונימית. מומלץ לבחון האם משתמשי הארגון משתמשים בשירותי VPN, ואם לא, להיערך לחסימתם במקרה הצורך.
8. מומלץ לבחון האפשרות להעברת האתר לענן במקרה הצורך.
9. מומלץ להכין אתר חלופי אליו תופנה התעבורה בעת הצורך.

## מקורות



1. [https://www.cisa.gov/sites/default/files/publications/understanding-and-responding-to-ddos-attacks\\_508c.pdf](https://www.cisa.gov/sites/default/files/publications/understanding-and-responding-to-ddos-attacks_508c.pdf)

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 לצורך הטמעתו.

