23 אוגוסט 2020
ג' אלול תש"פ
סימוכין:ב-ס-1143

DNS Hijacking בנתבים ביתיים ובארגונים קטנים

תקציר

DNS Hijacking היא תקיפה המאפשרת לתוקף להפנות את תעבורת המשתמש לאתרים זדוניים.
מטרת מסמך זה, סקירת צורת תקיפה זו כאשר היא מופנית כנגד נתבים של משתמשים ביתיים וארגונים קטנים, וכיצד להתמודד עימה.

פרטים

1. ברשתות קטנות רבות (רשתות ביתיות או של ארגונים קטנים), הנתב האלחוטי המשמש לקישור לרשת האינטרנט מוגדר גם כשרת ה-DNS עבור משתמשי הרשת.
2. תוקף המשיג שליטה על הנתב, יכול לנצל שליטה זו על מנת להפנות תעבורת המשתמשים לאתרים זדוניים בשליטתו.
3. בדרך כלל הדבר יבוצע באמצעות הגדרת שרת DNS בשליטת התוקף כשרת המקבל פניות DNS מהנתב, בניגוד למצב הרגיל בו שרת ה-DNS של ספק האינטרנט, או שרת DNS חיצוני המופעל על ידי ספק מוכר, מוגדר כך.
4. הפניית התעבורה מאפשרת לתוקף מגוון רחב של אפשרויות תקיפה, החל מהצגת פרסומות תמורת תשלום, ועד להצגת אתרים מתחזים לאתרים בשימוש המשתמשים, כגון אתרי בנקים, לשם גניבת נתוני ההזדהות של המשתמשים.
5. השתלטות על הנתב עלולה גם להוות ראש גשר של התוקף לפעולות תקיפה ברשת הביתית או הארגונית.

6. לנושא חשיבות רבה לאור הגידול הניכר במשתמשים העובדים מהבית בשל מגפת הקורונה, ומשתמשים ברשת הביתית שלהם לגישה למערכות הארגוניות. בתקופה זו נצפתה עליה בהיקף התקיפות כנגד נתבים ביתיים.
7. התקיפה הראשונית כנגד הנתב מתבצעת לרוב באמצעות שימוש בסיסמת ברירת המחדל של היצרן, או עקב פגיעויות שלא עודכנו בתוכנת הנתב.

דרכי התמודדות

1. מומלץ לשנות את סיסמת ברירת המחדל של ממשק הניהול של הנתב.
2. מומלץ להגדיר בנתב חוקי Firewall המונעים גישה מרחוק אליו מרשת האינטרנט, ובפרט לממשק הניהול. אם קיים צורך עסקי לאפשר גישה כזו מרחוק, מומלץ להיעזר ב-VPN עם הצפנה והזדהות מתאימים.
3. מומלץ לנהל הנתב אך ורק מרשת מקומית בבית או בארגון, ולנטרל את האפשרות לנהלו מרשת האינטרנט.
4. מומלץ לוודא באופן עיתי כי הנתב מעודכן עם עדכוני האבטחה המפורסמים על ידי היצרן.
5. מומלץ לוודא באופן עיתי כי הנתב מצביע על שרת DNS המוכר למשתמש למשלוח שאילתות DNS, כגון שרת ה-DNS של ספק האינטרנט או שרת DNS חיצוני מוכר שנקבע על ידי המשתמש.
6. ראו גם פרסומי מערך הסייבר הלאומי בנושא הקשחת נתבים ביתיים בקישורים https://www.gov.il/he/departments/news/homerouter, https://www.gov.il/he/departments/general/router.

לכל מידע נוסף ניתן לפנות אלינו. במידה שעלו ממצאים בבדיקתכם, נבקש לקבל היזון חוזר.

מקורות

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.