**שבוע הלאומי לבטיחות ברשת: חברת אימפרבה (imperva) חושפת את האתרים הישראליים שבסיכון הרב ביותר להונאת לקוחות**

**בין האתרים שבסיכון גבוה: אתרי מסחר, פיננסים ובריאות. התקפות אלו עלולות להוביל לגניבת כספים ופרטים אישיים רגישים**

בכל יום נעצרות מיליוני התקפות מסוגים שונים שעלולות לפגוע בזמינות האתרים ובמידע שהם מחזיקים על לקוחותיהם, כגון: פרטים אישיים, כתובות ופרטי תשלום. **לקראת שבוע הלאומי לבטיחות ברשת, קבוצת המחקר של חברת הסייבר אימפרבה (imperva) מתארת את הסכנות וחושפת את האתרים הישראליים שבסיכון הרב ביותר להונאת לקוחות.**

במסגרת זו, נאסף מידע הכולל פרטי התחברות של משתמשים ישראליים למערכות שונות, שהגיעו לתוקפים כתוצאה מנוזקות שהותקנו על מכשירים אלקטרוניים ומוצעים למכירה פומבית. נתונים אלה יכולים לאפשר לתוקפים להשתלט על חשבונות ולבצע בהם פעילויות לא מורשות כגון החלפת סיסמה והוצאת פרטים תשלום (כרטיסי אשראי).

מן הממצאים עולה כי, האתר שנמצא בסיכון הגבוה ביותר הוא alljobs עם 2,308 פרטים גנובים. מיד אחריו, ממוקמים אתרי המסחר שופרסל (1,925 סיסמאות) ויד2 (1,920 סיסמאות). במקום הרביעי ניצב אתר ישראכרט עם 1,213 סיסמאות גנובות ובמקום החמישי עמוד האזור האישי באתר האינטרנט של קופת החולים מכבי עם 1,076 סיסמאות.

בנוסף, נמצא כי ישנו גידול משמעותי (קרוב ל 100%) בסחר של פרטים אישיים אשר נגנבו ממשתמשים ישראלים, באמצעות תוכנות זדוניות, במהלך שלושת החודשים האחרונים. ככלל, כ-20% מניסיונות ההתאמתות לאתרים ישראלים (עמוד ה-Login) נעשים על ידי כלים זדוניים שבסבירות גבוהה מנסים לפרוץ לחשבונות משתמשים ולעשות בהם שימוש בלתי מורשה.

ישנן מספר שיטות להפחתת הסיכונים ברשת. ראשית, מידע רגיש נגנב על ידי תוכנות זדוניות שמותקנות על מחשבים אישיים במגוון שיטות. מומלץ להיות ערניים להודעות פישינג ולהימנע מהורדות לא חוקיות באופן כללי ובפרט מהורדות אפליקציות שלא מחנות האפליקציות הרשמית. בנוסף, יש להימנע משימוש חוזר באותה סיסמה במספר אתרים, להפעיל אימות שלבי בכל אתר או שירות המאפשר זאת, לדאוג שהדפדפן מעודכן בגרסה האחרונה של היצרן וכן בכל ניסיון התאמתות יש לוודא שהתקשורת מוצפנת (סימן מנעול) ושהאתר הוא הוא אכן האתר שאליו התכוונתם להגיע.

**נדב אביטל, ראש קבוצת המחקר באימפרבה:** ״פריצה לחשבונות אישיים יכולה להיעשות על ידי ניחוש מושכל של סיסמאות, שימוש בסיסמאות חוזרות משירותים שונים או על ידי גניבת סיסמאות מהמחשבים האישיים של המשתמשים. מהרגע שתוכנה זדונית מותקנת במחשב, ביכולתה לאתר כל ניסיון התאמתות לכל אתר ולשלוח את פרטי האימות לתוקף. מניתוח המידע שנגנב נמצאו פרטי משתמשים בבנקים הגדולים בישראל, רשתות סופרמרקט, אתרי מסחר פופולאריים וקופות חולים, שמעמידים את המשתמשים של אותם שירותים בסיכון גבוה לגניבת כספים, פרטי תשלום ונתוניים אישיים רגישים״.