כלכליסט

שבת 10 ינואר

שלחו להדפסה
גודל פונט

טכנולוגי | אינטרנט

אתרי רפא"ל והתעשייה האווירית נפרצו

עשרות אלפי אתרים בעולם נפרצו, בהם אתרים של רפא"ל, התעשייה האווירית, אוניברסיטות תל אביב ובן גוריון. בחלק מהאתרים הושתל קוד זדוני. התעשייה האווירית: מדובר ברשת חיצונית שלא מכילה מידע מסווג

צמרת פרנט

05.10.08, 16:42

4 תגובות

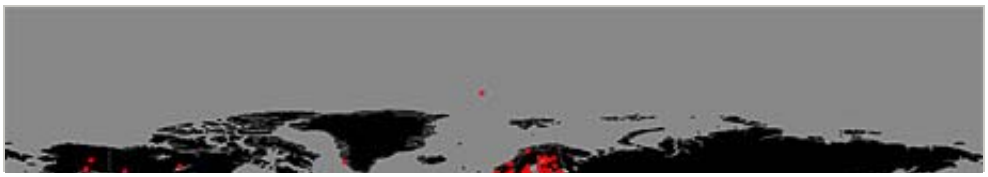
עשרות אלפי אתרי אינטרנט בארץ ובעולם נפרצו ובחלקם הושתל קוד זדוני שגרם להתקנת סוס טרויאני על מחשבי הגולשים שגלשו אליהם. כך לפי דיווח של חברת אלדין. צוות ממחלקת אבטחת המידע של חטיבת eSafe באלדין זיהה לפני כשבועיים שרת המכיל רשימה של יותר מ-200 אלף שמות משתמש וסיסמאות המאפשרים גישה לשרתי אינטרנט ב-86 מדינות בעולם. השרת שימש ככל הנראה שני ארגוני פשע מאירופה ומארה"ב.

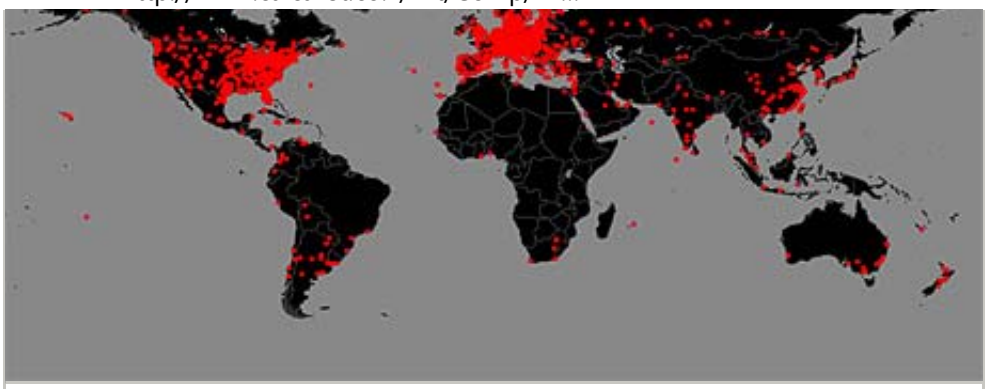
בין האתרים הישראלים שנפרצו – אתרים של התעשייה האווירית, רפא"ל, אוניברסיטת בן גוריון ואוניברסיטת תל אביב.

בחלק מהאתרים הושתל קוד שגרם להתקנת סוס טרויאני על מחשבי המשתמשים שגלשו לאתרים. הגולשים שנפגעו לא זיהו התנהלות חשודה באתרים, אך הסוס הטרויאני שהותקן על המחשבים איפשר להקליט שמות משתמש וסיסמאות באתרים כמו אתרי בנקים, חשבונות אימייל או חיבורים למקום העבודה.

האתרים הישראלים שנפגעו הם: אתר התעשייה האווירית, אתר רפא"ל, אתר אוניברסיטת בן גוריון, אתר אוניברסיטת תל אביב, Dsp.co.il, Solor2005.co.il, Bin.co.il, Shenkar.ac.il, Drp.co.il, Castik.co.il, Greenpages.co.il, Plasson.co.il, Derechhalev-israel.org, Denya.co.il, Opticom.co.il, Pioneer.co.il.

יפתח יאן עמית, ראש הצוות שגילה את הפריצה, אמר שהשרתים של רפא"ל והתעשייה האווירית נפרצו, אך לא הושתל בהם קוד זדוני שהשפיע על הגולשים. לדבריו, רפא"ל והתעשייה האווירית תיקנו את הפרצה, אך אוניברסיטת תל אביב ואוניברסיטת בן גוריון עדיין לא תיקנו אותה. עמית הוסיף כי באתר Greenpages.co.il עדיין מופעל סוס טרויאני. בחלק מהאתרים תוקנה הפרצה. לפי עמית, הפעילות הזדונית החלה בפברואר ונמשכה עד לימים האחרונים.





מפה של מיקום שרתי האינטרנט שנפגעו

הצוות של אלדין הצליח לנתח נתונים בשרת שאותר, ולחקור את הדרך שבה פועלים התוקפים באמצעות נתונים אלו ותוכנות ייעודיות שנמצאו בשרת. בעולם, בעיקר באירופה ובארצות הברית, נפרצו אתרים של חברות ענק וכן אתרים ממשלתיים, בהם למשל אתר של שירותי הדואר בארצות הברית (Usps.gov), אתר של ה-BBC, ושל ערוץ הטלוויזיה הצרפתי TF1.

אלדין הודיעה על הפריצה לארגונים בינלאומיים הנלחמים בפשיעה ממוחשבת וביניהם גם למשטרת ישראל (המפלג לעבירות מחשב) ומלמ"ב, האחראי על אבטחת מידע במערכת הביטחון בישראל. פעילות התיאום והדיווח הכלל עולמית נעשתה בשיתוף עם CERT - ארגון העל האחראי על אבטחת מידע באינטרנט.

מקור בכיר בהנהלת התעשייה האווירית אמר בתגובה: "האירוע ידוע לנו. מדובר ברשת חיצונית של התעשייה האווירית שלא מכילה כל מידע מסווג ואף על פי כן הנושא נבדק ומטופל בהתאם". גורם בכיר ברפא"ל מסר: "מדובר בפריצה לשרת חיצוני שאינו מכיל מסמכים מסווגים. כל המסמכים המסווגים נמצאים בשרת פנימי מאובטח. האירוע אותר וטופל".