עדכון חדשות סייבר יומי 22/05/2018

בארץ ובעולם

1. אוניברסיטת באפלו שבמדינת ניו יורק מדווחת כי פרטיהם של כ-2500 סטודנטים, בוגרים ועובדי סגל הודלפו כחלק מפריצה שחוותה האוניברסיטה. המידע שהודלף כולל שמות משתמשים וסיסמאות. טרם ידוע מי אחראי לפריצה זו (buffalo.edu ו-scmagazine).

2. גוגל תשלם 36,000 דולר לצעיר אשר חשף פגיעות ב-Google App Engine. היישום מאפשר לפתח יישומי אינטרנט. פגיעות זו הוגדרה כקריטית ואפשרה לתוקף להריץ קוד מרחוק (securityaffairs).

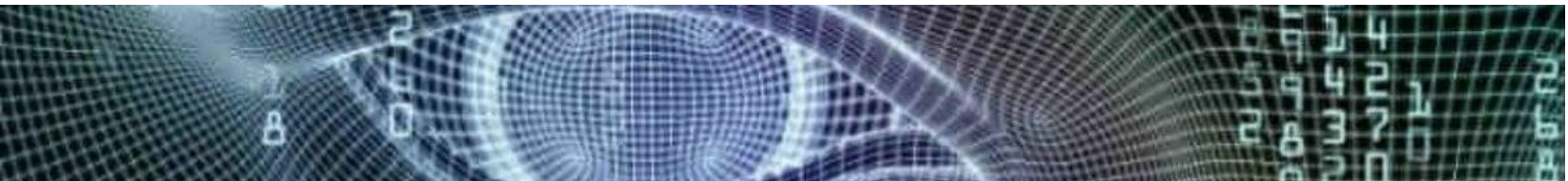
טכנולוגיה

3. מיקרוסופט וגוגל פועלות יחד כדי לתת מענה לפגיעות מעבדים חדשה. על פי דיווחים שונים, המענה לפגיעות זו יכלול עדכוני קושחה שעשויים להשפיע על ביצועי המעבד (theverge).

4. שרתי DNS מסוג Bind חשופים לפגיעות המאפשרת תקיפת מניעת שירות. ארגון Internet Systems Consortium (ISC) פרסם דרכי התמודדות (isc).

5. קבוצת התקיפה Team Sun הצליחה להסוות תוכנה זדונית במספר יישומים הנמצאים בחנות האפליקציות של גוגל. הקבוצה, שעיקר תקיפותיה הם נגד עריקים ועיתונאים צפון קוריאנים, פיתחה תוכנה זדונית אשר גונבת מידע אישי הנמצא במכשיר הסלולרי של הנתקף (mcafee).

6. חוקרי קספרסקי מדווחים על קמפיין נוסף של הפוגען הבנקאי Roaming Mantis. הפוגען עושה, בין היתר, שימוש בטכניקת DNS hijacking המפנה משתמשים לדפים מזויפים במגוון שפות, ביניהן עברית. אינדיקטורים רלוונטיים בקישור (securelist).



7. לפי דיווחים של חוקרי Malwarebytes, תוקפים ממשיכים לנצל את הפגיעות ב Drupal שפורסמה בחודש שעבר על מנת להתקין כורה מטבעות וירטואליים, כלים לניהול מרחוק ועוד. לדבריהם, 80% מהאתרים הפגיעים שימשו לכריית מטבעות וירטואליים. אינדיקטורים רלוונטיים בקישור (malwarebytes).