סטודנטים בפקולטה למדעי המחשב בטכניון חשפו פרצת אבטחה בקורטנה – הסייעת הקולית של מיקרוסופט

מאת אבי בליזובסקי
חמישי, 14 יוני 2018 00:43

הסטודנטים רון מרקוביץ (משמאל) ויובל רון בפקולטה למדעי המחשב בטכניון. צילום : רמי שלוש, דוברות הטכניון

סטודנטים מהפקולטה למדעי המחשב בטכניון חשפו פרצת אבטחה בקורטנה – העוזרת האישית הווירטואלית של מיקרוסופט. הם יציגו את פרטי הפריצה ב- Hat Black- אחד מכנסי ההאקינג החשובים בעולם - לאחר שמיקרוסופט סיימה לתקן את הפרצה בעקבות הפרטים שקיבלה מהסטודנטים. קורטנה היא סייעת קולית המאפשרת למשתמשים להפעיל מחשבים, סמארטפונים ושעונים חכמים באמצעות דיבור. מערכת זאת, שבפיתוחה שותף גם מרכז הפיתוח של מיקרוסופט בישראל, נחשפה ב-2014 בכנס המפתחים של מיקרוסופט העולמית.

הסטודנטים רון מרקוביץ ויובל רון גילו את הפרצה בקורטנה במסגרת קורס "פרויקט באבטחת מידע" לתואר ראשון בפקולטה בהנחיית עמיחי שולמן ופרופ' אלי ביהם. הרעיון למתקפה על קורטנה החל משיחה של שולמן ובתו, שגם היא עוסקת באבטחת סייבר, על פריצה יצירתית למחשבים. בעקבות השיחה החלו שולמן ושותפו טל בארי לחשוב על אפשרויות שאינן דורשות כתיבת נוזקה (Malware), וכך הגיעו לרעיון של ניצול הממשק הקולי של מערכות ממוחשבות.

במשך הסמסטרים האחרונים עבדו כמה קבוצות סטודנטים בפקולטה למדעי המחשב בטכניון על פרויקטים בנושא של אבטחת סייעת קולית, ובסמסטר האחרון רשמו הסטודנטים מרקוביץ ורון הצלחה במתקפה על קורטנה. השניים הצליחו להשתלט על מחשב נעול ולהוריד אליו קובץ תוכנה חיצוני, וכך לשלוט בכל הפונקציות שלו. בעקבות ההצלחה הם דיווחו לחברת מיקרוסופט, שתיקנה את הפרצה האמורה. לדבריהם, "לא היינו מגיעים לפרויקט כזה, ובטח לא היינו מצליחים לזהות את פרצת האבטחה, בלי ההנחיה והכלים שקיבלנו בטכניון."

החדשנות בשיטת הפריצה שפיתחו מרקוביץ ורון טמונה בשימוש בממשק קולי כדי לעקוף מנגנוני אבטחה. שיטה זו מאפשרת ליזום התקפה ללא כל צורך בנוזקה. לדברי שולמן, זו כבר הפרצה השנייה המתגלה

מאת אבי בליזובסקי
חמישי, 14 יוני 2018 00:43

במסגרת המחקר. הפרצה הקודמת, שגם היא אפשרה השתלטות על מחשב נעול באמצעות פקודות קוליות, הוצגה בכנס של חברת קספרסקי בחודש מרץ 2018. לדברי שולמן, "הפרצה החדשה דרמטית אף יותר, ואני מעריך שקבוצות נוספות יציגו בסמסטר הנוכחי תוצאות משמעותיות בנוגע לסיכון הכרוך בשילוב של ממשק תפעול קולי במערכות מחשוב קלאסיות."

עמיחי שולמן השלים תואר ראשון ושני בפקולטה למדעי המחשב בטכניון ומאז משמש מנחה חיצוני בקורס זה במקביל לפעילותו העניפה בתעשייה. הוא שירת בחיל הקשר בתחום הגנת מערכות, הקים חברת סטארטאפ בתחום זה (Imperva) וכיום עובד כיועץ לחברות אבטחה. כמה מהפרויקטים שהנחה בטכניון זכו בפרסים יוקרתיים ואחד מהם התפרסם בניו יורק טיימס בדצמבר 2012; באותו פרויקט תקפו הסטודנטים 40 מוצרי אבטחה (אנטי-וירוס) באמצעות 82 וירוסים וגילו כי יעילות ההגנה של אותם מוצרים היא 5% בלבד. פרויקט אחר שזכה בתשומת לב (ובפרס אמדוקס לפרויקט הטוב ביותר) הראה כיצד ניתן לנצל את מנוע החיפוש גוגל כדי לתקוף בשיטתיות אתרים ברשת. תוצאות של פרויקטים נוספים, כגון ניתוח אבטחה של פרוטוקול HTTP/2 ומעקב אחרי פעילות של עברייני Phishing, הוצגו בכנסים בינלאומיים.

פרופ' אלי ביהם מכהן כראש מרכז המחקר לאבטחת סייבר ע"ש הירושי פוג'יווארה בטכניון. הוא מוביל את הוראת הקורסים בתחום הסייבר לרבות קורס הפרויקט באבטחת מידע, שבו מבצעים הסטודנטים מגוון רחב של פרויקטים בנושאים שונים של אבטחת מידע.

{loadposition content-related}

. הסטודנטים רון מרקוביץ (משמאל) ויובל רון בפקולטה למדעי המחשב בטכניון

צילום : רמי שלוש, דוברות הטכניון