עדכון חדשות סייבר יומי 28/02/2018

בארץ ובעולם

1. פגיעות באתר "קרנות השוטרים" אפשרה לזהות האם מספר תעודת זהות מסוים שייך לשוטר או מתנדב במשטרה. לפי הדיווח, לאחר פנייה של גופי תקשורת שונים, הפגיעות תוקנה (internet-israel).

טכנולוגיה

2. חוקרים מחברת אבטחת המידע Duo Labs, זיהו פגיעויות בפרוטוקול SAML, המשמש מערכות הזדהות רבות, כולל מערכות לזיהוי יחיד (Single Sign On – SSO). הפגיעות מאפשרת למשתמש מזוהה במערכת, להתחזות למשתמש אחר, ללא ידיעת הסיסמה של משתמש זה (duo).
3. מתקפות מניעת שירות מבוזרות, המבוססות על הגברת תעבורה (Amplification), ניתנות למימוש כאשר פרוטוקול מסוים, בתגובה לשאילתה או פניה קצרה יחסית, מחזיר תשובה ארוכה מאד. בדרך כלל מימוש תקיפה כזו יתבסס על פרוטוקול UDP, משום שבפרוטוקול זה קל לזייף את כתובת המקור. חברת Cloudflare דיווחה כי לאחרונה נצפתה עלייה משמעותית בניצול פרוטוקול בשם memcached (UDP/11211) המשמש למימוש Cache על גישות לשרתים, לביצוע תקיפות מסוג זה. (cloudflare).
4. לאחרונה זוהה פוגען חדש שתוקף מערכות הפעלה מסוג Android. הפוגען נפוץ בבריטניה ובסין והוא מופץ באמצעות אפליקציות מזויפות. בין יכולותיו: גניבת מידע מערכתי אודות המכשיר וכן גניבת קבצים השמורים בו, הקלטת אודיו ועוד (wandera).
5. ה-ICS CERT האמריקאי מדווח כי קיימות פגיעויות בציוד דימות המופעל באמצעות גרסאות שונות של תוכנת IntelliSpace Portal (ISP) מתוצרת חברת פיליפס. החברה מודעת לפגיעויות אלו ותפרסם עדכוני אבטחה עבורן (ics-cert).

*** עדכון זה ניתן כשירות ומבוסס על לקט פרסומים גלויים המובאים בשם אומרם ואינם משקפים את עמדת המערך ו/או פעולותיו. ***