עדכון חדשות סייבר יומי – 03/01/18

בעולם

1. הממשל האמריקאי ממשיך לקדם את אימוץ מנגנון DMARC בדומיינים שלו. בחודשים האחרונים נרשם גידול משמעותי במספר הדומיינים של הממשל שאימצו את המנגנון, ובכירה ב-DHS הסבירה כי מנגנון זה יעיל בהגנה מפני התחזות וכי קריטי שתושבי ארה"ב ידעו שהודעת דוא"ל שהגיעה מהממשל היא אותנטית (infosecurity-magazine).

טכנולוגי

2. קיימות מספר אינדיקציות לכך שבהמשך החודש יפורסמו פרטים לגבי פגיעות קריטית בשבבים של חברת Intel. דווח כי הן מפתחי ה-kernel של Linux, והן חברת מיקרוסופט עובדים על עדכון תוכנה שיתקן את הפגיעות הנ"ל בחומרה. טרם נמסרו פרטים מדויקים לגבי אופי הפגיעות, אך דווח כי עדכון עלול לגרום להאטה משמעותית בביצועי מערכת ההפעלה של בין 5% ל-30% (the register, ו-siliconeangle).

3. חוקרים גילו כי ביותר מ-100 שירותים ששומרים מידע בציוד IoT, ישנן פגיעויות שתוקף יכול לנצלן כדי לגנוב מידע זה. התוקף יכול לגשת בין היתר למיקום הנוכחי, סוג המכשיר ומספר הטלפון (securityweek ו-trackmageddon).

4. נחשפה פגיעות בדפדפנים אשר שומרים את הסיסמאות לאתרים באופן אוטומטי. מדובר בדפדפנים Chrome, Firefox, Opera, Edge ועוד. דווח כי חברות פרסום הצליחו לנצל זאת כדי לעקוב אחר משתמשים (thehackernews).

5. עובד לשעבר ב-NSA ביצע הנדסה לאחור של תוכנת האנטי-וירוס של חברת קספרסקי והראה כיצד ניתן להפוך אותה לכלי חיפוש של מסמכים מסווגים במחשב עליו היא פועלת. העובד הראה כי התוכנה מייצרת חתימות אותן ניתן לשנות כדי לזהות מסמכים רגישים (nytimes).

6. מנגנון זיהוי הפנים במערכת Windows 10 ניתן למעקף על ידי הדפסת תמונה של המשתמש. כך גילו חוקרים בחברה הגרמנית SySS. לדברי החוקרים, פגיעות זו רלוונטית לרוב גרסאות המערכת (nakedsecurity).

7. בסוף דצמבר אותר גל חדש של הפצת פוגעני כופר באמצעות הבוטנט necurs. בוטנט זה ידוע בין היתר בהפצת הפוגענים Locky, Jaff, Trickbot, Dridex ועוד (securityaffairs).

8. לאחרונה פורסם עדכון אבטחה קריטי עבור הכלי phpMyadmin המשמש לניהול מאגרי MySQL. מצ"ב קישור לעדכון האבטחה (phpmyadmin).

עדכון זה ניתן כשירות למשרדי ממשלה ומבוסס על לקט פרסומים גלויים. הפרסומים מובאים בשם אומרים ואינם משקפים את עמדת הרשות ו/או פעולותיה.

Qualified by a Certificate Authority