עדכון חדשות סייבר יומי 10/05/2018

בארץ ובעולם

1. האקר פרץ ל-Bycyklen, רשת האופניים העירונית של קופנהגן, ומחק את מסד הנתונים של הארגון. הפריצה השביתה את גישת הציבור לאופניים במהלך סוף השבוע.
Bycyklen מדווחת כי לא נגנבו נתונים אודות המשתמשים, אך היא בכל זאת ממליצה להחליף את קוד ה-PIN ששימש את הלקוחות בהשכרת האופניים (cphpost ו-bycyklen)

טכנולוגיה

2. חוקרי אבטחת מידע מ-avanan הישראלית, חשפו פגיעות Zero Day המכונה baseStriker בפלטפורמת Office 365. לדבריהם, פגיעות זו מאפשרת לתוקפים לעקוף את כל מנגנוני האבטחה של מיקרוסופט. לפי החברה, עד כה תוקפים ניצלו פגיעות זו על מנת לשלוח הודעות דיוג, אך ביכולתם להפיץ גם פוגענים (avanan).

3. פוגען הכופר GandCrab שב בגרסה חדשה: הפוגען מחפש דפי אינטרנט בעלי פגיעויות ב-mysql, בעיקר אתרים של עסקים קטנים אשר אינם מודעים לפגיעויות על מנת שיוכל להצפינם.
GandCrab מופץ באמצעות הודעות דוא"ל המכילות קובץ zip או סקריפט הטוען מרחוק את הפוגען. אינדיקטורים רלוונטים בקישור (talos).

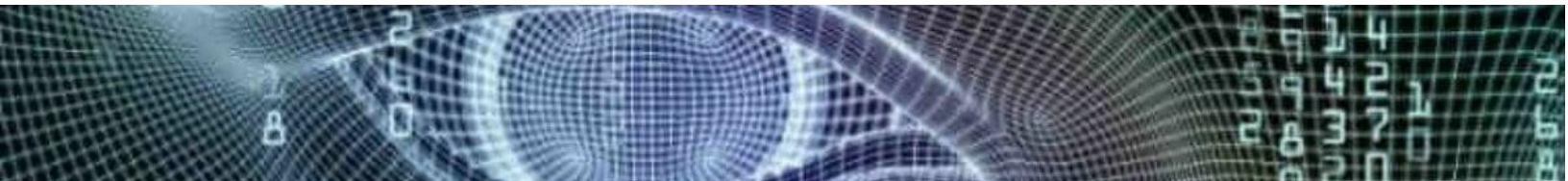
4. חברת CheckPoint פרסמה דו"ח רוחבי אודות השימוש ההולך וגובר ב-Telegram למטרות פשיעת סייבר. פושעים מנצלים את האפשרות להקים ערוצים (Channels) מאובטחים אשר נגישים יותר למשתמשים נוספים מאשר ה-Darknet, ובכך מרחיבים את מעגל הפשיעה האינטרנטית (checkpoint).

עדכוני אבטחה

5. גוגל הפיצה את עדכון האבטחה של מערכת אנדרואיד לחודש מאי, הכולל עדכון עבור פגיעות Meltdown (CVE-2017-5754). בנוסף, החברה מעדכנת גם פגיעויות ברכיבי NVIDIA ו-Qualcomm (source.android).

6. חוקרי אבטחה מחברת vpnMentor הוציאו עדכון אבטחה לא רשמי, אותו הם מכנים Antidote, לפגיעות בנתבים הביתיים של חברת Dasan (CVE-2018-10561 & CVE-2018-

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



10562). הפגיעות מאפשרת לתוקפים לעקוף את מנגנוני האימות ולהריץ קוד מרחוק. נתבים אלו נפוצים בעיקר במקסיקו, קזחסטן ו-ויאטנם (vpnmentor).

7. חברת LG תיקנה שתי פגיעויות חמורות במקלדת ברירת המחדל שלה שהשפיעו על כל המכשירים החכמים של החברה. הפגיעות מאפשרת לתוקף לבצע מתקפת MITM במהלך הורדת שפה חדשה למכשיר וקבלת הרשאות גבוהות (LGsecurity).

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