עדכון חדשות סייבר יומי 01/05/2018

בארץ ובעולם

1. חדשות CBS מדווחת כי בית ספר מחוזי במסצ'וסטס שילם 10,000 דולר על מנת לפענח קבצים שהוצפנו ע"י פוגען כופר. המחשבים הוצפנו ב-14 לאפריל, ולאחר משא ומתן עם התוקפים שולם הסכום, אך נכון למועד הדיווח הקבצים טרם פוענחו(cbsnews).

2. לפי דיווח של אתר חדשות סיני, עובדים בממשלת סין חשפו השבוע כי ביכולתה של הממשלה לגשת להודעות WeChat אשר נמחקו. WeChat היא רשת חברתית סינית והחברה העומדת מאחוריה, Tencent, יצאה בהצהרה כי היישום אינו מאחסן היסטוריית הודעות וכי כל המידע נמצא אצל המשתמש בלבד (bleepingcomputer).

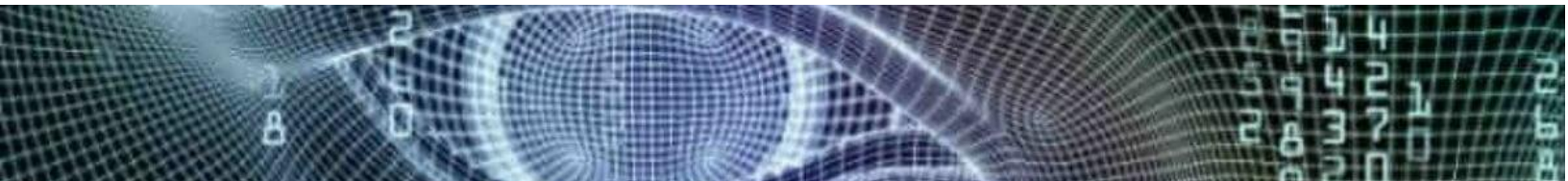
3. טוויטר חשפה השבוע כי היא מכרה נתונים לחוקר שעובד בשיתוף עם חברת Cambridge Analytica. דובר החברה אמר כי החוקר קיבל גישה חד פעמית לממשק API ולמדגם אקראי של ציוצים ציבוריים בשנת 2015 (threatpost).

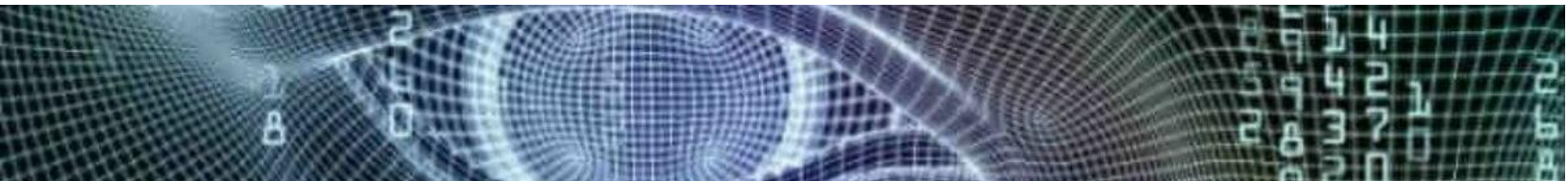
טכנולוגיה

4. חברת אבטחת המידע Sophos פרסמה דו"ח אודות פוגען הכופר SamSam אשר שב בגרסה חדשה הממוקדת לארגונים אשר סביר להניח ישלמו את סכום הכופר. הפוגען תר אחר פגיעויות ברשת או מבצע תקיפות Brute Force. לאחר שהוא מוצא וקטור כניסה, הוא מצפין את קבצי המשתמש ודורש כופר בעבור פענוחם. אינדיקטורים רלוונטים מצורפים בקישור(sophos).

5. בחודש אפריל פרסמה חברת Oracle עדכון אבטחה רבעוני אשר טיפל בין היתר בפגיעות שאיפשרה לתוקפים להריץ קוד מרחוק על שרת WebLogic ולקבל השתלטות מלאה. כעת, חוקר אבטחת מידע מחברת Alibaba מדווח כי נמצאו דרכים חדשות לעקוף את עדכון האבטחה ולנצל את הפגיעות. החוקר אף פרסם הוכחה בחשבון הטויטר שלו (thehackernews).

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



6. תוסף זדוני לדפדפן Chrome בשם FacexWorm מתפשט באמצעות קישור הנשלח ב-Facebook Messenger. התוסף הופץ לראשונה באמצעות הודעות ספאם עם קישור המובילות לדף המתחזה ל-YouTube ודורש התקנת תוסף מיוחד אשר גונב את נתוני הגישה של המשתמשים למגוון רחב של אתרים. אינדיקטורים רלוונטים מצורפים בקישור (trendmicro) .

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