עדכון חדשות סייבר יומי 28/01/18

עדכון זה ניתן כשירות ומבוסס על לקט פרסומים גלויים.

הפרסומים מובאים בשם אומרם ואינם משקפים את עמדת המערך ו/או פעולותיו.

בעולם

1. השירות החשאי האמריקאי החל להזהיר לאחרונה מוסדות פיננסיים מפני תקיפות מסוג JackPotting. בתקיפות אלו, פושעים מתקינים תוכנה ו/או חומרה זדונית על מכשיר כספומט וגורמים לו לפלוט כמויות גדולות של מזומנים, לפי פקודה. תקיפות מסוג זה מתקיימות מזה זמן באירופה ובאסיה, וכעת הגיעו גם לארה"ב. התקיפה מחייבת נגישות פיזית של התוקף למכשיר הכספומט (krebsonsecurity).

2. יו"ר ענקית הספנות Maersk חשף בפורום הכלכלי בדאבוס, כי בעקבות מתקפת NotPetya חברתו נאלצה להתקין מחדש אלפי שרתים, עשרות אלפי עמדות קצה וכ- 2500 יישומים. המשימה בוצעה תוך 10 ימים. הנזק נאמד בכ-300 מיליון דולר (scmagazine).

3. מטבעות וירטואליים בשווי מוערך של למעלה מחצי מיליארד דולר נגנבו מבורסת CoinCheck היפנית. טרם נמסרו פרטים נוספים אודות הגניבה (thehackernews).

טכנולוגי

4. חברת האבטחה Palo Alto חשפה קמפיין תקיפה חדש נגד אזרחים במזרח התיכון הנקרא "Top Hat". במסגרת הקמפיין, מופץ פוגען באמצעות מסמכים בערבית הקשורים לאירועים פוליטיים עכשוויים. אינדיקטורים רלוונטיים מצורפים בקישור (paloaltonetworks).

5. נחשף כלי חדש של קבוצת התקיפה Oilrig המכונה RGDoor. על פי הדיווח, מטרת כלי זה להוות גיבוי ל- Webshell TwoFace שבשימוש הקבוצה, למקרה שהארגון המותקף יצליח לזהותו ולהסירו. אינדיקטורים רלוונטיים מצורפים בקישור (paloaltonetworks).

6. תוקפים הצליחו לנצל את שירות הפרסומות DoubleClick של גוגל, כדי להפיץ סקריפט של coinhive וסקריפט נוסף לכריית מטבעות וירטואליים (trendmicro).

עדכוני אבטחה

7. Lenovo שחררה עדכון אבטחה קריטי למספר רב של דגמים בעלי מערכות הפעלה windows 7,8. הפגיעות ב- Fingerprint Manager pro מאפשרת קבלת גישה לנתונים רגישים (lenovo).

8. עדכון התוכנה האחרון למוצר anti-malware של חברת Malwarebytes גורם לצריכת זיכרון וכוח מעבד גבוהים מהרגיל. בחלק מן המקרים עדכון זה גורם לקריסת המחשב. החברה פרסמה הנחיות כיצד ניתן להתמודד עם מקרים אלו. (malwarebytes ו-bleepingcomputer)

כתובת לקבלת דואר: משרד ראש הממשלה, רח' קפלן 3, ירושלים
טלפון 03-7450811, פקס 03-7450822