



## עדכון חדשות סייבר יומי 22/01/18

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

### בעולם

1. תושב ניו מקסיקו בארה"ב הודה באשמה בגין עשרות תקיפות מניעת שירות (DDoS) שביצע נגד מעסיקו לשעבר, ארגונים מתחרים ורשויות אכיפת החוק. התקיפות נמשכו שנתיים, חלקן באמצעות שירותים המספקים תקיפות מסוג זה תמורת תשלום ([ibtimes](#))

### טכנולוגי

2. שירות הביטחון הפדרלי של רוסיה חשף פוגען חדש התוקף עמדות תדלוק בתחנות דלק. הפוגען מרמה את הלקוחות באמצעות מכירת חסר של עד 7%, לעומת הכמות המצוינת במונה המשאבה. ([RussiaBeyond](#)).

3. סוס טרואיני חדש בשם Evrial מסוגל לגנוב Cookies ונתוני גישה מהדפדפן. בנוסף, הפוגען מסייע לתוקף לגנוב מטבעות וירטואליים על ידי זיהוי ביצוע תשלום במטבע מסוג זה באמצעות מעקב אחר ה-Clipboard ("לוח הגזירה"), והחלפת הכתובות המיועדות לתשלום לכתובות בשליטת התוקף ([bleepingcomputer](#)).

4. חברת אבטחת המידע Pradeo מדווחת כי שלושה משחקי sonic של חברת Sega, המצויים בחנות של Google Play, אוספים מידע רב על המשתמשים. המידע מועבר בממוצע ל-11 שרתים מרוחקים, אשר 3 מהם אינם מורשים. למשחקים ישנם במצטבר מאות מיליוני הורדות על ידי משתמשים. על פי הדיווח, במשחקים נמצאו פגיעויות רבות ([pradeo](#)).

5. הפוגען הבנקאי drindex שב בגרסה חדשה, שבה הקישור להורדת הפוגען מתבצע באמצעות אתרי ftp. לאחר שהפוגען משיג גישה למחשב הקורבן, הוא גונב נתוני הזדהות לשירותים בנקאיים. אינדיקטורים רלוונטיים מצורפים בקישור ([forcepoint](#)).