



## עדכון חדשות סייבר יומי 15/02/2018

### בארץ ובעולם

1. בכירים בקהיליית המודיעין האמריקאית מזהירים מפני רכישת מכשירים של החברות Huawei ו-ZTE הסיניות. במהלך שימוע שנתי בסנאט האמריקני אודות האיומים הגלובליים, טענו הבכירים כי קיימת בעייתיות גדולה בשימוש בציוד של חברות שקשורות קשר הדוק לממשל שאיננו שותף לערכים האמריקאיים. בנושא אחר, הבהירו הבכירים כי רוסיה מתכוונת להתערב בדרכים רבות בבחירות אמצע הקדנציה בארה"ב, שיתקיימו בסוף שנה זו.  
([cnn](#) ו-[cnbc](#)).

### טכנולוגיה

2. חוקרים זיהו בוטנט חדש התוקף ציוד IoT ומנצל שתי פגיעויות Backdoor, על מנת לעקוף FW, האחת בציוד של חברת Juniper והשנייה בנתבים של ZyXEL. הבוטנט המכונה DoubleDoor אינו מבצע פעילות זדונית בציוד הנתקף בשלב זה, מלבד הוספתו לרשת הבוט, ככל הנראה כהכנה לקראת תקיפה מאסיבית יותר בעתיד ([newskysecurity](#)).

3. אותר וריאנט חדש של הפוגען AndroRat התוקף מכשירים בעלי מערכת הפעלה מסוג Android. הפוגען מנצל פגיעות משנת 2016, המאפשרת תקיפה של גרסאות ישנות של Android, ומסווה את עצמו כאפליקציה לאופטימיזציה של המכשיר. אינדיקטורים רלוונטיים מצורפים בקישור ([trendmicro](#)).

4. דו"ח חדש מגלה כי מספר הפגיעויות הקריטיות שנתגלו במערכת ההפעלה Windows 10, גדלו ב-64% בשנת 2017 לעומת השנה הקודמת. ככלל, מספר הפגיעויות אשר דווחו למיקרוסופט בשנת 2013 לעומת 2017 גדל ב-111% וסך הפגיעויות שנמצאו בתוכנת Office גדל ב-89% ([businesswire](#) ו-[avecto](#)).





5. אינטל הודיעה כי היא מרחיבה את תוכנית איתור הפגיעויות במוצריה ( Bug Bounty Program), ומגדילה את הסכום הניתן למי שמוצא פגיעויות מסוג Side Channel Attack , כדוגמת Spectre ו-Meltdown. הסכום המעודכן עומד על 250 אלף דולר ([intel](#)).

6. חוקרים זיהו פגיעות קריטיות בתוכנת Skype אשר ניצולה עלול לאפשר השתלטות על המערכת המותקפת. על פי הדיווח, מיקרוסופט החליטה שלא להפיץ עדכון אבטחה, בשל השינויים הנרחבים הנדרשים ברכיב התוכנה הרלוונטי (מנגנון העדכון), והיא תיתן מענה לפגיעות רק בגרסה הבאה של התוכנה ([macobserver](#)).

