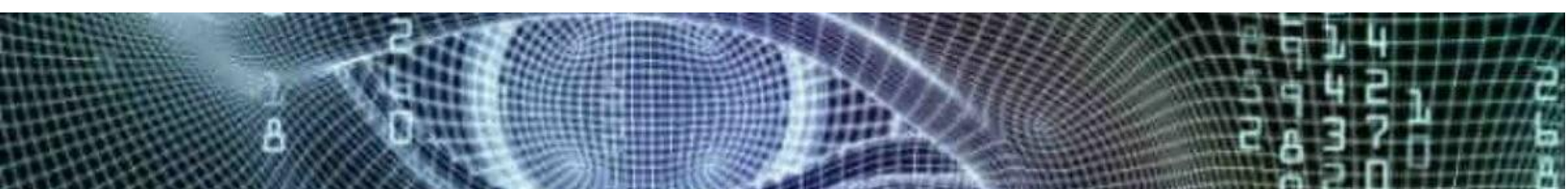
עדכון חדשות סייבר יומי 14/02/2018

בארץ ובעולם

1. פרטים נוספים על תקיפות הסייבר באולימפיאדת החורף בדרום קוריאה ממשיכים להתגלות: דגימות של הפוגען מאשרות כי מטרתו הייתה הרס ולא גניבת מידע, בדומה לתקיפת BadRabbit. הפוגען מוחק לוגים ו-Shadow Copies ומבצע תנועה רוחבית ברשת הנתקפת, באמצעות תוכנות לגיטימיות כדוגמת WMI ו-PsExec. אינדיקטורים רלוונטיים מצורפים בקישור (talos).

טכנולוגיה

2. חוקרי חברת McAfee זיהו קמפיין חדש של קבוצת התקיפה Lazarus המתמקד במשתמשי ביטקוין ובארגונים פיננסיים בינלאומיים. הקמפיין מבוסס על הודעות דוא"ל שהכילו פוגענים, אשר סרקו את העמדה הנתקפת בניסיון לאתר פעילות במטבע הוירטואלי. אינדיקטורים רלוונטיים מצורפים בקישור (McAfee).
3. קמפיין רחב היקף של הבוטנט Necurs מנסה לתקוף על רקע יום האהבה הבינלאומי. הקמפיין החל לפני כחודש וכלל כמה גלים שונים של הודעות דוא"ל הכוללות בתוכן מחמאות כביכול של השולחת לנמען, לאחר שצפתה בתמונותיו ברשתות חברתיות. ההודעות נשלחו למשתמשים ברשתות החברתיות פייסבוק ו-Badoo, רשת חברתית המתמקדת במציאת בני זוג ושידוכים (securityintelligence).
4. האקרים השתמשו בפגיעות Zero Day בתוכנת טלגרם למשתמשי Windows, על מנת להדביק אותם בפוגען לכריית מטבעות וירטואליים. הפגיעות הינה ב- RLO Unicode Character. אינדיקטורים רלוונטיים מצורפים בקישור (securelist).
5. ארה"ב זיהתה וריאנטים נוספים של פוגענים של תשתית Hidden Cobra המיוחסת לצפון קוריאה. שני הוראינטים מכונים Hardrain ו-Badcall. אינדיקטורים רלוונטיים מצורפים בקישורים (us-cert ו-us-cert).



עדכוני אבטחה

6. מיקרוסופט פרסמה 50 עדכוני אבטחה לחודש פברואר. העדכונים כוללים, בין היתר, פגיעויות קריטיות בתוכנת Outlook ובדפדפן Edge. מערך הסייבר הלאומי יפרסם בהמשך מסמך בנושא זה (microsoft).
7. בהמשך לעדכונים בעקבות דיווחים על פגיעויות Zero Day בתוכנת Flash שנוצלו על ידי גורמים ממדינות מזרח אסיה, Adobe פרסמה עדכוני אבטחה נוספים לתוכנות Acrobat, Reader ו-Experience Manager (adobe ו-adobe).