עדכון חדשות סייבר יומי 18/03/2018

בארץ ובעולם

1. רשויות האכיפה בפולין עצרו בסוף השבוע האחרון את יוצר פוגעני הכופרה Polski, Vortex ו-Flotera. מדובר באזרח פולני שמתגורר כיום בבלגיה והגיע לביקור מולדת. בתיאום עם רשויות האכיפה בבלגיה, החשוד נעצר והציוד שברשותו הוחרם. על פי הדיווח, באמצעות הציוד שהוחרם, הצליחו לשחזר את מפתחות ההצפנה של פוגענים אלו (bleeping computer).
2. תחרות ההאקינג Pwn2Own 2018 הסתיימה שלשום ובמסגרתה הוענקו 267 אלף דולר לחוקרים והאקרים שמצאו פרצות אבטחה, חלקן Zero Day. פגיעויות רבות שנמצאו בתחרות היו בדפדפנים שונים, ביניהם Safari, Firefox ו-Edge (eweek).

טכנולוגיה

3. חברת Check Point מדווחת על משפחת פוגענים לסמארטפונים שתקפו 5 מיליון מכשירים החל משנת 2016. משפחת הפוגענים מכונה RottenSys והיא מסווה את עצמה כאפליקציות לגיטימיות, ומופצת בין היתר באמצעות בוטנט (checkpoint).
4. חוקרים מ-MalwareHunterTeam חשפו פוגען כופרה חדש המכונה Zenis. הפוגען מצפין את הקבצים מהעמדה הנתקפת ובנוסף גם מוחק את הגיבויים הקיימים. טרם נחשף כיצד מופץ הפוגען. אינדיקטורים רלוונטיים מצורפים בקישור (bleeping computer).
5. נחשף וריאנט חדש של פוגען פיננסי למכשירי Android. הפוגען Fakebank מציג מסכי כניסה מזויפים על גבי אפליקציה לגיטימית ובכך גונב את פרטי המשתמשים. כמו כן, הפוגען מסוגל ליירט את השיחות ולהעבירן למספרים שהוגדרו מראש (symantec).
6. חוקרים מחברת Check Point מדווחים על פגיעות חדשה באפליקציה Google Chrome Remote Desktop בגרסתה למכשירי Mac. על פי הדיווח, במקרים בהם פתוחה גישה לאורח (Guest), תוקפים יכולים לנצל זאת כדי לעקוף את הסיסמה ולקבל גישה למידע (dailymail).
7. צוות של אקדמאים פיתח תוסף חדש ל-Chrome אשר מטרתו לחסום אפשרות של מתקפה באמצעות Java Script המיועדת להדליף מידע מהזיכרון. התוסף נקרא Chrome Zero והוא זמין ב-GitHub (bleeping computer).

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

עדכוני אבטחה

8. חברת VMware פרסמה עדכוני אבטחה למוצרים VMware Workstation Pro ו- VMware Fusion Pro. הפגיעויות שאותרו איפשרו מניעת שירות ודורגו כ-Important (vmware).

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