בס"ד

אירועי אבטחת מידע וסייבר מהעולם - פברואר 2015

אירועי אבטחת מידע וסייבר מרכזיים:

1. חברת **Anthem**, שהיא אחת מהחברות הגדולות בארה"ב בתחום ביטוחי הבריאות, מודיעה שמערכותיה נפרצו ופרטיהם של כ-**80,000,000** לקוחות, בהם גם פרטיו של מנכ"ל החברה נגנבו. הפרטים הכילו מידע אישי הכולל גם מספרי ביטוח לאומי (**SSN**) בהמשך פורסמו מספר דו"חות שלפיהם התקיפה בוצעה באמצעות הדבקת המחשבים בחברה בתוכנה זדונית דרך המייל. נטען שישנם הוכחות שמקור התקיפה הוא בגורמים ממשלתיים מסין.

2. **כל אתרי הממשל בדנמרק** הופלו למשך כ- **12 שעות** כתוצאה ממתקפת DDOS נרחבת. יום לאחר מכן פרסם משרד הפנים הודעה שהאתרים הותקפו בצורה נרחבת ומתואמת היטב.

3. האקר המכנה עצמו **Abdilo** הצליח לגנוב מידע אישי של כ- **60,000** סטודנטים מ**אוניברסיטת סידני** באמצעות מתקפת SQLi . הסטודנטים קיבלו הודעה מהאוניברסיטה שפרטיהם נגנבו ונמצאים בידיי פושעים.

4. הסוכנות האמריקאית לניהול הסכמים ביטחוניים (**DCMA**) האחראית על שירותי הניהול למשרד ההגנה האמריקאי. ספגה מתקפת סייבר מתקדמת שבה **מספר שרתים** הושבתו ומידע סודי הודלף מחוץ לרשתות המסווגות בדרגה גבוהה ביותר.

5. חברת **Uber** המציעה שירותי הסעות חברתיות בה כל נהג מן השורה הופך לנהג מונית בתשלום, דיווחה בסוף השבוע האחרון שמערכותיה נפרצו ופרטיהם של **50,000** נהגים לפחות נגנבו במהלך חודש מרץ . הפרטים כוללים מידע אישי ורשיונות נהיגה.

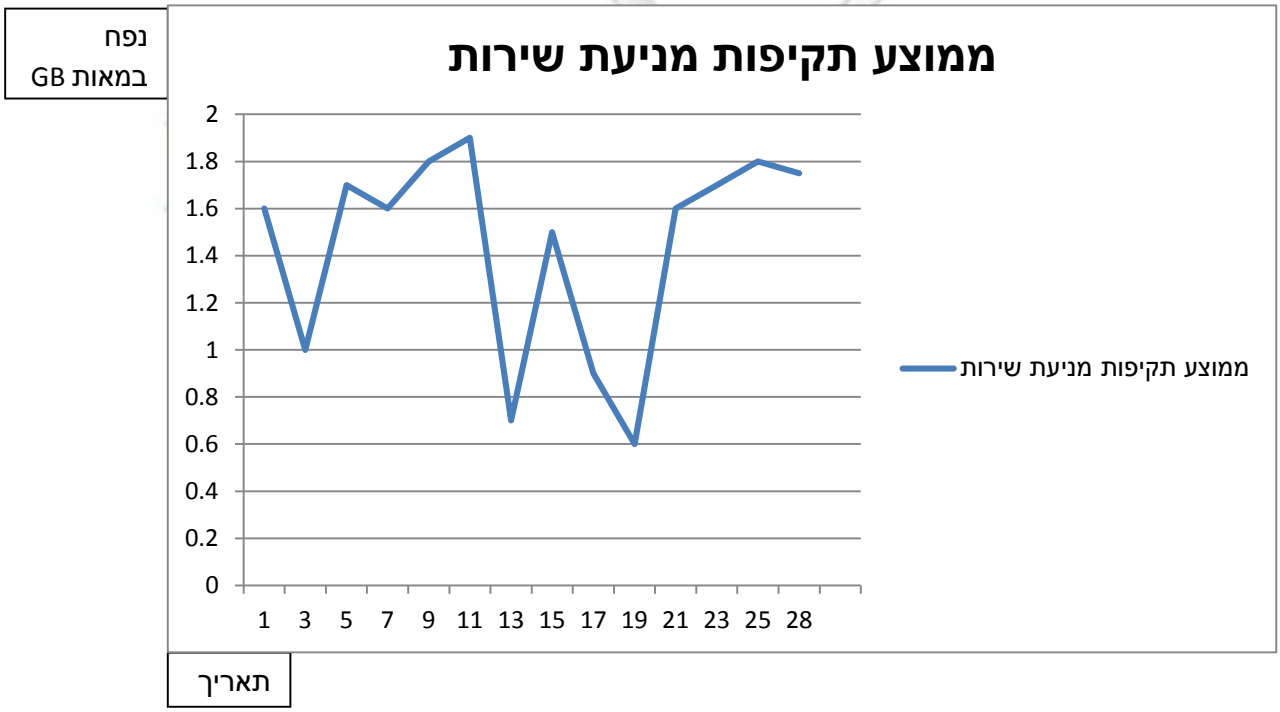
6. **האתר הרשמי של Lenovo** יצרנית המחשבים הענקית נפרץ ע"י האקרים המכנים עצמם **Lizard Squad** במתקפת DNS hijack. הפורצים שמו באתר **www.lenovo.com** תמונות של נער שצולם במצלמת האינטרנט שלו, כמו כן התקיפה איפשרה לתוקפים לגנוב מיילים מהחברה. הפריצה בוצעה כנראה כנקמה לפרשיית **Superfish** ע"י האקטיביסטים. בה נמצא כי מחשבים ניידים של החברה הגיעו עם תוכנה זדונית מותקנת מראש למטרות פירסום.

7. חברת אבטחת המידע **Sucuri** חושפת פגיעות המשפיעה על יותר מ- **1,000,000** אתרי **וורדפרס** ברחבי העולם. הפגיעות נמצאה בתוסף לניהול תוכן בשם Slimstat ומאפשרת לתוקפים לגנוב מידע רגיש הכולל סיסמאות ומפתחות הצפנה המשמשים לניהול האתרים.

כל המידע במסמך זה מסתמך על נתונים ממקורות רבים. תורגם ונערך ע"י **ליאור בן דוד**, החומר לשימוש והפצה חופשית בתקווה שתמצאו בו תועלת. לפירוט המקורות ומידע נוסף יש לפנות במייל : lior@lbd.co.il או בטלפון: 050-9969980 © LBD

תקיפות של השחתת אתרים (Deface)

תקיפות של מניעת שירות בעולם (DoS/DDoS)



כל המידע במסמך זה מסתמך על נתונים ממקורות רבים. תורגם ונערך ע"י **ליאור בן דוד**, החומר לשימוש והפצה חופשית בתקווה שתמצאו בו תועלת. לפירוט המקורות ומידע נוסף יש לפנות במייל : lior@lbd.co.il או בטלפון: 050-9969980 © LBD