****

***דו"ח: מחקר מתקפת בית החולים***

1. **תיאור המתקפה שהתרחשה: הייתה פריצה לרשת המחשבים של בית החולים, מה שגרם לכך שאין גישה למידע רפואי אשר הכרחי לצורכי טיפול, התוקפים השתילו תוכנה זדונית במערכות בית החולים והם מחזיקים בהם תמורת כופר. התוקפים לקחו פרטיים אישיים של מטופלים**
2. **הממצאים שנמצאו:** נמצאו 5 קבצים מוצפנים**,** נמצא קובץ הנקרא keys, אשר ייתכן ומחזיק מפתחות בהן השתמשו להצפנת הקבצים.

**3. המידע שחולץ: 129 אימיילים של מטופלים, נמצאו בתוך 3 קבצים מתוך ה 5 המוצפנים, בשאר הקבצים לא היה טקסט שסימל משהו רלוונטי.**

**4. תיאור התהליכים הזדוניים: services.exe , explorer.exe , iexplore.exe , rundll32.exe**

**5. פירוט המתקפה שבוצעה: המתקפה שבוצעה היא flame. התוכנה הזדונית מחדירה חלקים שונים מהקוד שלה לשלושה שרשורים ומסתירה את פעולותיה מאחורי תהליכים רגילים ולגיטימיים נוסף על כך הוירוס מסוגל באופן מיידי לגנוב קבצים, לשמור צילומי מסך, לתעד הקשות על המקלדת, לחבל באמצעי אחסון, לשלוט בתעבורה ובקבצי מערכת, כאשר הוא מפיץ את עצמו באמצעות רשתות Wi-Fi, בלוטוס וחיבורי USB. כמו כן, במידה והושתל הוירוס במחשב אשר אליו מחובר מקרופון, הוא מסוגל להשתמש בו כאמצעי ציטוט ולשלוח תשדורות שמע מן הקורבן אל התוקף**

**6. היוזר החשוד בביצוע המתקפה: יאיר, מצאנו בקובץ לוג שכלל את שעות הפעילות שכל הפעולות החשודות התקיימו בחודש נובמבר בשעות הבוקר, ולפי תיאורו הוא זה שעבד בשעות המוקדמות של הבוקר בחודש נובמבר.**

**7. המלצות להתגוננות בעתיד מפני מתקפות דומות: אפשר להתקין תוכנות אנטי וירוס,** **התקנת תוכנת אנטי מאלוור חזקה ועדכנית וכדו' , נוסף על כך הייתי ממליצה לבית החולים לבדוק מדי פעם את קבצי ה log של המחשב ולבדוק אם מתקיימים שם תהליכים שנראים להם חשודים מהרגיל.**