כלכליסט

מתקפת נוזקת הכופר WannaCry פגעה גם בישראל

מתקפת הסחיטה המקוונת הגיעה לארץ וככל הנראה פגעה במספר מצומצם של משתמשים. על אף שהיא השביתה בתי חולים, מערכי ייצור וזרעה בהלה ברחבי אירופה בסוף השבוע האחרון, התוקפים הרוויחו ממנה פחות מ-30 אלף דולר. מדוע הרווחים כה זעומים?

ניצן סדן ורפאל קאהאן 14.05.17 10:34

נוזקת הכופר WannaCry, שנוטרלה לאחר פגעה במחשבי משתמשים, בתי חולים ותשתיות ייצור באירופה במהלך סוף השבוע - חזרה לפעול. לפי מידע שהגיע לידי "כלכליסט" מחברת White Hat, גם בישראל נפגע מספר קטן מאוד של משתמשים - ככל הנראה עשרות בודדות.

קראו עוד בכלכליסט:

- בלוגר בריטי בן 22 הצליח לנטרל חלק ניכר ממתקפת הסייבר
- חברת החשמל והבנקים מוגנים ממתקפה. בתי החולים הם החוליה החלשה
- רשות הסייבר הלאומית: כך תתמודדו עם מתקפת הסייבר העולמית

פעילות הנוזקה נעצרה לאחר שבלוגר אבטחה רכש דומיינים בהם השתמשו מפעילי WannaCry והפעיל את מנגנון הניטרול האוטומטי שלה. ואולם, לפי שרון נימירובסקי מ-White Hat, התוקפים נטשו את הדומיין דרכו הועברה פקודת הניטרול ועדכנו את הקוד הזדוני - שנקרא כעת WannaCry 2.0.

על אף הצלחת התוקפים, הם לא יוכלו לפרוש לחיי עושר למרות שהנוזקה נשענת על גניבת כסף ישירות מהקורבן. קמפיין הכופר הגיע לפחות מחשבים משנדמה – ויצר אפקט בהלה בעיקר בשל העובדה שפגעה בבתי חולים בבריטניה ובתשתיות ייצור של חברות רכב אשר חשפו את דבר הפגיעה. בפועל, היתה זו מתקפת כופר גדולה למדי, אם כי היו בעבר מתקפות גדולות ממנה שגרמו לנזקים נרחבים בהרבה; בשורה התחתונה, המתקפה עשתה יותר רעש מנזק.

מתקפת הסייבר יצרה יותר בהלה מנזק צילום: איי פי

בריאן קרבס, ממומחי האבטחה המוערכים בעולם, תיאר בבלוג שלו את השתלשלות המתקפה ואסף נתונים לפיהם פושעי הסייבר ששיגרו את WannaCry הרוויחו כ-26,000 דולר ממנו. אמנם מדובר בסכום נאה, שלא הצריך מהם השקעה משמעותית - אך בהתחשב באפקט הציבורי של המתקפה, ניתן היה לחשוב כי התוקפים השיגו שלל גדול בהרבה. לפי דיווח של הניו יורק טיימס הנשען על שיעור הפקדות הביטקוין בחשבונות המקושרים למתקפה, הצליחו ההאקרים להרוויח 33,000 דולר.

לפי הערכת מומחי אבטחה, המבצע לא התמקד בבתי חולים, אך מדיניות אבטחת המידע של מוסדות אלה היתה כה רעועה שהם נפגעו בקלות. לפי הערכות, התוקפים הרוויחו מעט כסף

משום שמותקפים רבים לא הסכימו לשלם את הכופר. דרישת הכופר נמוכה יחסית, משום שהתוקפים רוצים להעלות את הסיכוי שהקורבן ישלם: אם הדרישה היתה לאלפי דולרים, יתכן שהיו המותקפים פונים למומחי אבטחה, מה שהיה מצמצם את הסיכוי לתשלום הכופר.

נוזקות הכופר אינן תופעה חדשה וקיימות כבר מספר שנים. למעשה, הן נהיות יותר פשוטות טכנית להפעלה ושליטה - תוך שרכיבי ההצפנה שלהן הופכים למורכבים ומתקדמים יותר. בכך, עולה הנגישות של כלי תקיפה זה עבור פושעי סייבר, ביניהם טירונים ובעלי ניסיון מוגבל. נוזקת כופר יכולה לעלות גם עשרות דולרים בודדים בשווקי נוזקות ברשת האפלה. אפילו תהליך סחיטת הקורבן והעברת הכספים הפכו לשירות מקוון לפושעים: האקרים יכולים לרשום את מבצע הכופר שלהם לשירות סליקה מאובטח וחשאי, שייקח עמלת שימוש אך יטפל בהעברת הכספים והמרתם בעת הצורך.