‏יום ראשון, 03 ביולי 2016

- הודעה לעיתונות -

**דו"ח איומי יוני – עדכון מזויף למערכת חלונות מסתובב ברשת**

**זה היה חודש שוקק באיומים: עדכון חדש למערכת חלונות מתרוצץ שם בחוץ ואל תעזו להוריד אותו, הזכות לפרטיות נשללה מאתנו על ידי בית המשפט, תוכנות כופר חדשות הגיחו לרשת, תוכנות כופר וותיקות נתנו גז ווירוס פייסבוק אחד עשה בלגן שלם במדינת היהודים. דו"ח האיומים של חברת ESET לחודש יוני**

אף אחד לא אוהב לבהות במשך שעה ארוכה במחשב מבצע עדכונים, הספירה לאחור כאילו אף פעם לא נגמרת. יש משהו שאתם הרבה יותר לא תאהבו – מתיחות עדכון מחשב מזויפות!
האתר הבא – fakeupdate.net – מציע לכל דיכפין עדכונים מזויפים של מערכת ההפעלה ווינדוס, בגרסאות חדשות וישנות – XP, windows 98, Mac OSX, Vista, Windows בגרסאות 7,8,10 ואפילו לינוקס. כל אחד יכול להטמיע את דף עדכון המחשב בדפדפן של חבר שלא בידיעתו ולצפות במתיחה בהנאה רבה. למרבה המזל, מדובר רק במתיחה שאינה יכולה להזיק למחשב. למרות זאת, אם לוחצים על מקש ה-enter בעת ביצוע ה"עדכון" מתקבל מסך שגיאה מלחיץ.

**מצטערים, אין לכם זכות לפרטיות**

הפרטיות שלנו חשובה לנו מאוד, במיוחד כשאנחנו מבצעים פעולות רבות ואף פיננסיות באמצעות המחשב או הטלפון הנייד. מצד שני נדמה שאנחנו חיים בעולם שבו כל אחד חופשי לחטט בחייו של האחר, ואנחנו נותנים לאנשים לעשות זאת מרצוננו בשיתוף ברשתות החברתיות. שופט בווירג'יניה קבע כי עצם חיבור המחשב לרשת האינטרנט משמעותו שאתה לא יכול לצפות לפרטיות ולמעשה היא נשללת ממך לחלוטין.

שופט פדרלי במחוז המזרחי של וירג'ינה קבע כי כל המשתמש במחשב המחובר לאינטרנט לא צריך לדרוש כל זכות לפרטיות כי אין אבטחת מחשב יעילה דייה שיכולה לעצור האקרים. אז מה הוא בעצם מנסה לומר בזה – שאנחנו גם לא יכולים לצפות לפרטיות בבתינו כי פורצים יכולים בכל עת להיכנס אם הם רק מנסים לפרוץ את מנעול הדלת או את סורגי החלון? לדברי השופט, כן, כך בדיוק הדבר. אם יזדמן לכם לבקר בווירג'יניה דעו לכם שלא תהיה לכם שם כל זכות לפרטיות.

 **29.69% מאיומי הסייבר על ישראל בשבוע האחרון הם של לוקי**

תוכנת הכופר לוקי אינה מפסיקה להטיל את אימתה על הישראלים. תוכנת הכופר מצפינה קבצים במחשב הנגוע ודורשת תשלום כספי גבוה תמורת שחרורם. מעל ל-60% מהנוזקות המופעלות כיום בעולם, וכפועל יוצא בישראל, עלולות להסתיים במתקפת כופר. מתקפות אלה עושות שימוש בטכניקות הדבקה מתקדמות ולרוב גם מנצלות תמימות או חוסר מודעות מצד משתמשי הקצה כדי לייצר את פעולת ההדבקה הראשונית. לרוב מדובר בקבצים המצורפים להודעות דואר אלקטרוני המכילים קובץ ג'וואה סקריפט זדוני, שעובר מספר שינויים כדי לעבור מתחת לרדאר של תוכנות האבטחה הקיימות.

ניסיונות התקיפה כלפי ישראל רק מתגברים כאשר בשבוע האחרון שליש – 29.69% מהאיומים על ישראל זוהו כאיומים של תוכנת הכופר Locky. ההמלצה החמה ביותר היא לא לפתוח קבצים במיילים ממוענים שאינם מוכרים וכן לוודא שתוכנת האנטי וירוס נמצאת בגרסה המעודכנת ביותר שלה. חלק מתוכנות האנטי וירוס כבר יודעות לזהות את תוכנת הכופר הזו ולחסום את פעולתה במחשב. הכי חשוב שיהיה לכם גיבוי של כל החומר שיש על המחשב בכונן חיצוני שאינו מחובר למחשב.

 **וירוס הפייסבוק ששיגע את המדינה**

אתם בודקים את ההתראות בפייס, פעולה טבעית ושגרתית לחלוטין, ומסתקרנים למה חבר תייג אתכם או הגיב למשהו שכתבתם. ראו הוזהרתם: לחיצה על ההתראה מורידה באופן אוטומטי תוכנה מזיקה למחשב או לטלפון הנייד. מתקפת הווירוסים הזו השתוללה בזמן האחרון בפייסבוק כמו אש בשדה קוצים ופגעה במשתמשים ישראלים רבים.

השיטה שבה מופעל הווירוס אינה חדשה אבל המטרה שלה הפעם היא תוקפנית במיוחד – על ידי השתלת קובץ נוזקה אל המחשב של משתמש באמצעות לחיצה על התראה מאוד לא מחשידה "מישהו הגיב לפוסט שלך"/ "מישהו הזכיר אותך בהודעה". מיד עם הלחיצה יורד קובץ הווירוס אל המחשב אבל אל דאגה – כל עוד הוא לא הופעל המחשב אינו מצוי בסכנה. עם זאת, פתיחה של הווירוס תפעיל את הרעל הארסי שיש בו. בתחילה פורסם כי קובץ הנוזקה מכיל תוכנת כופר אבל כיום יודעים לומר כי הוא מכיל תוכנה המתקינה דפדפן מזויף שגונב פרטי גישה לחשבונות. הקובץ פוגע ופונה רק אל מחשבים ולא אל טלפונים ניידים.

**תוכנת הכופר CryptXXX תגנוב גם את הסיסמאות שלך**

הגרסה החדשה של תוכנת הכופר CryptXXX (3.100) זוהתה לראשונה ב-26 במאי על ידי חברת אבטחת המידע Proofpoint. היא כוללת שלל פיצ'רים חדשים ביניהם StillerX – מודול לגניבת סיסמאות שהופך את התוכנה לאחת מן המסוכנות ביותר ב"סצינת תוכנות הכופר". הפיצ'ר פועל באופן דיי דומה לתוכנות גניבת סיסמאות אחרות – מתקפה על בסיסי נתונים פנימיים ששמורים במערכת ההפעלה של המחשב ובדפדפני האינטרנט. כך הפיצ'ר מחלץ סיסמאות מוצפנות או לא מוצפנות ולאחר מכן שולח אותן לשרת מקוון.

המודול מסוגל לחדור לכל סוגי התוכנות: דפדפנים, מנהלי הורדות, שרתי מייל, תוכנות FTP, אפליקציות IM, אפליקציות פוקר, שרתי פרוקסי ו-VPN וסיסמאות שמאוחסנות בזיכרון המטמון או במנהל האישורים של מיקרוסופט.

משתמשים יכולים לזהות פגיעה של תוכנת הכופר crypXXX שמגיעה ביחד עם גונב הסיסמאות StillerX עם הימצאות של הקבצים: stiller.dll, stillerx.dll ו-stillerzzz.dll במערכת שלהם. מלבד היכולת לגנוב סיסמאות עבור התקפות סייבר עתידיות, תוכנת הכופר גם שינתה את אתר הפיענוח שלה לטובת מי שמעוניין לשלם את הכופר. האתר עבר מתיחת פנים וכולל גרפיקה חדשה.

כיצד ניתן להימנע מפגיעה של תוכנת הכופר? "גם תוכנת הכופר הזו יכולה להגיע אל הקורבנות בפתיחה תמימה של דואר אלקטרוני והורדת הקובץ הכלול בה", אומר אמיר כרמי מנהל טכנולוגיות ב-ESET ישראל. "כבר נתקלנו במקרים שבהם תוכנת האנטי וירוס זיהתה את הימצאות תוכנת הכופר וחסמה את הפעלתה על המחשב. בכל מקרה חשוב לשמור על ערנות בפתיחת קבצים מצורפים למיילים שאנחנו לא מצפים להם, או שמגיעים ממקורות שאיננו מכירים".

**אודות ESET**

ESET היא חברת אבטחת המידע החמישית בגודלה בעולם, בעלת ותק של 25 שנה בתחום פתרונות האבטחה במעל 200 מדיניות ברחבי העולם.

כחלוצת האנטי וירוס ,NOD32 ESET מפתחת ומייצרת פתרונות הגנה למגזר הפרטי והעסקי כאחד הכוללים הגנה מפני ווירוסים, מתקפות מקוונות, גניבת זהויות, הגנה על תשלומים ברשת, הצפנת מידע עסקי ועוד.

בין לקוחותינו ניתן למנות את בית חולים איכילוב, חברת דור אלון, רשת ארומה, חברת Cisco, קבוצת פוקס, משרדים ממשלתיים, עיריות, מוסדות חינוך, קופות חולים ועוד.

**למידע נוסף:**

ענבל סינגר

דוברת,ESET ישראל

inbal@eset.co.il

052-8272151