גירסה 1.00 – 31.12.2004

כיצד להגן על המחשב שלך מפני וירוסים

ניר אדר

Nir Adar

Email: underwar@hotmail.com

Home Page: http://underwar.livedns.co.il

אנא שלחו תיקונים והערות אל המחבר.

מסמך זה מציג מספר כללי אצבע ושיטות עבור משתמשי Windows כיצד להגן על המחשב שלהם מפני וירוסים ומזיקים אחרים.
בשם וירוסים נכלול במסמך זה גם טרוינים, spywares ומזיקים נוספים.

1. התקן עדכוני אבטחה

הרבה מהוירוסים הנפוצים כיום מתבססים על בעיות אבטחה המתגלות במערכות. הדבר הכי חשוב שניתן לעשות על מנת למנוע התקפות על המחשב הוא לעדכן את Windows כשיוצאים עדכוני אבטחה חדשים. כל מערכת Windows החדשות מאפשרות לבצע עדכון אוטומטי. מומלץ להעזר בו כדי להתקין, או לפחות להתריע, כאשר ישנם עדכונים חדשים.

2. שימוש באנטי וירוס, firewall ומוריד spywares

שימוש בכל אחת מתוכנות אלו באופן קבוע הוא חשוב למניעת וירוסים, ולא מומלץ לוותר על אף אחת מהן. עם זאת, יש לזכור כי העובדה שהן מותקנות על המחשב איננה מחליפה הגיון בריא. המחשב אינו מוגן לחלוטין בשום מקרה (וירוסים חדשים שעדיין לא הוספו לבסיס הנתונים של התוכנות, וירוסים המתקיפים את תוכנות ההגנה וכו').
יש לעדכן את קובץ החתימות של האנטי וירוס כל יום. אנטי וירוס שלא עודכן בשבועיים האחרונים – לא עוזר בכלל.
יש להשתמש ביותר ממוריד spywares אחד. שני המובילים – ad-aware ו-spy-sweeper, משלימים אחד את השני. במקרה אחד שראיתי – ad-aware מצא 20 adwares. לאחר מכן spy-sweeper מצא 20 נוספים. לפיכך – שימוש רק באחד מהם אינו נותן הגנה מושלמת.

3. גרום ל-Windows להציג תמיד את סיומת הקבצים

Windows, כברירת מחדל, מסתיר את סיומות הקבצים עבור קבצים מוכרים.
ניתן לאמר ל-Windows להציג תמיד את הסיומת. נעשה זאת דרך חלון Windows Explorer בתפריט Tools ← Folder Options ← View הורדת הסימון מ-" Hide extensions for known file types".

נשים לב שגם אחרי שנבצע פעולה זו, Windows מסתירה את הסיומות shs, pif ו-lnk.

כאשר נבוא להריץ קובץ, נסתכל על סוג הקובץ לפני שנריץ אותו.

הטבלה הבאה מרכזת סיומות חשובות של קבצים:

סיומת	תיאור
BAT	קובץ batch של DOS.
COM	קובץ הרצה (executable) של DOS.
CMD	קובץ batch של Windows 2000 (פרטים נוספים על הפורמט ניתן למצוא כאן: http://labmice.techtarget.com/articles/batchcmds.htm).
EXE	קובץ הרצה (executable) של DOS או Windows.
LNK	קובץ shortcut של Windows. מסמך נוסף באתר פרויקט UnderWarrior עוסק בסכנות שקובץ זה מציג.
MSI	קובץ התקנה של מיקרוסופט.
PIF	קיצור דרך לתוכנת DOS.
REG	קטע registry (ניתן לשתול אותו על ידי הפעלת הקובץ ב-registry המקומי).
SCR	שומר מסך (screen saver). זהו למעשה קובץ EXE ששינו לו את הסיומת.
VBS	סקריפט Visual Basic.
WS	קבצי Windows Script.

וירוסים יכולים להתחבא בכל אחד מסוגי קבצים אלו. אם מתקבל דואל המכיל קבצים עם הסיומות הנ"ל יש לפתוח אותו רק אם השולח ידוע, וכן אתם מצפים לקבל קובץ מסוג זה.

טריק נפוץ נוסף הינו ליצור קבצים עם רווחים רבים לפני הסיומת שלהם, לדוגמא:

```
mypicture.jpg                                    .exe
```

יש להזהר ולשים לב לסיומת האמיתית של הקובץ אותו מריצים.

4. השתמש בהגיון

הזהר ממלכודות ומאנשים המנסים להדביק אותך. זכור כי אימייל לא תמיד באמת מגיע מאיפה שרשום שהוא מגיע – אם הוא מכיל קובץ חשוד, ברר כי אכן האדם ממנו לכאורה הגיע המייל שלח לך אותו. לגבי צ'טים – בחורה השולחת לך "אוסף תמונות שלה" בתור קובץ EXE – זה משהו שראוי לחשוד בו.

כאשר אתה שולח אימיילים לאנשים אחרים, המכילים קבצים שעלולים להיות מסוכנים – זכור לכתוב, בנוסף לקובץ, מה הוא מכיל ולאשר כי אתה באמת זה ששלח אותו.

5. המנע מגלישה באתרים מפוקפקים

המנע מגלישה באתרים מפוקפקים, בייחוד כאלו שקיבלת את הכתובת שלהם דרך דואר זבל.
אתרים אלו מנסים לרוב להשתמש בפרצות, והם לרוב מנצלים פרצות חדשות עוד לפני שהעדכון המתקן אותן זמין.

6. גיבוי המידע

גבה את המידע במחשב באופן כמה שיותר יום יומי. במקרה של total lost של המחשב עקב התקפת וירוס, הנזק יהיה רק הזמן של התקנת התוכנות וטעינת הגיבוי. אם הנתונים אינם מגובים, יאבדו כל המסמכים שכתבת, הדואר שקיבלת, רשימת הסמאות שלך וכדומה.

EOF