

מהם וירוסי מחשב:

וירוס מחשב הוא תוכנית מחשב קטנה אשר נכתבה כדי לשנות את דרך הפעולה של המחשב, מבלי ידיעתו ורשותו של משתמש המחשב. וירוס צריך לענות על שתי דרישות:

א. הוא חייב לדעת להפעיל את עצמו לבד. בד"כ ימקם את עצמו בנתיב החיפוש של תוכנה קיימת.

ב. הוא חייב לשכפל את עצמו. לדוגמא וירוס יכול להחליף קבצי הרצה אחרים עם עותק של הוירוס עצמו. הוירוסים תוקפים תחנות עבודה ושרתים בדיוק באותה מידה.

חלק מהוירוסים תוכנתו כדי לגרום נזק למחשב ע"י הריסת תוכנות מותקנות, כמו מחיקת קבצים או אף פירמוט מלא של הדיסק הקשיח. אחרים לכאורה לא גורמים נזק פרט לעובדה שהם מודיעים על הימצאותם בצורה של הצגת טקסט, וידאו או קול. אפילו וירוסים "שפירים" אלו יכולים לגרום בעיות למשתמש המחשב. הם תופסים מקום בזיכרון אשר נועד לשימוש של תוכנות אחרות, דבר היכול להוביל להתנהגות בלתי יציבה של המערכת או גם לקריסתה.

מבחינים בין חמישה סוגים של וירוסים:

א. קבצים נגועים בוירוסים – אלו קבצים אשר מדביקים קבצי תוכניות, בד"כ קבצי הרצה כמו EXE או COM. קבצים אלו יכולים להדביק קבצים אחרים כאשר הוירוס נמצא על דיסקט, על הדיסק הקשיח או על כונני רשת. רוב הוירוסים נשארים בזיכרון המחשב בצורה קבועה TSR.

ב. וירוסים של Boot Sector - אלו וירוסים אשר קושרים עצמם לחלק האחראי על העלאת המערכת בעת הפעלת המחשב, ויכולים להימצא על דיסקט ועל דיסק קשיח. וירוסים אלו הם שוכני זיכרון TSR. במקור וירוסים אלו נכתבו למערכת ההפעלה דוס הישנה, אך כל סוגי מערכות ההפעלה יכולים להידבק מוירוסים אלו. יש לציין כי ההידבקות שכיחה ומספיק להשתמש בדיסק חדש שאינו מוגן כתיבה במערכת שכבר הוירוס שוכן בזיכרון שלה בכדי להידבק.

ג. וירוסים של רשומת האיתחול הראשית (master boot record) - וירוסים אלו גם הם שוכני זיכרון. צורת ההדבקה שלהם זהה לזו של וירוסים מסוג BOOT SECTOR. ההבדל בין שני הסוגים הוא במיקום הקוד הויראלי. וירוסים אלו ברוב המקרים שומרים את הקוד הנכון של רשומת האיתחול הראשית במקום אחר, כך שלא ניתן להעלות את מערכת ההפעלה. יש כמובן גם הבדלים בטיפול, מכורח העובדה כי מערכות הפעלה שונות ניגשות בצורה שונה לקוד זה.

ד. וירוסים מרובי חלקים – וירוסים מסוג זה תוקפים גם את רשומות האיתחול וגם קבצי תוכניות. וירוסים אלו בד"כ קשים לתיקון.

ה. וירוסי מקרו – הם סוג של וירוסים אשר תוקפים קבצי נתונים. הם נפוצים ביותר ותיקונם אורך זמן רב. וירוסים אלו החלו להיות נפוצים יותר ויותר עם הפצתו של הוויז'ואל בייסיק בחבילת האופיס 97 של חברת מיקרוסופט. הם בד"כ מדביקים קבצי עיבוד תמלילים של WORD, גיליונות אלקטרוניים באקסל, מצגות פאוור פויינט ואף מסדי נתונים באקסס. מוטציות חדשות של הוירוסים יכולות להדביק תוכניות מסוגים שונים באותה שיטה.

מהם סוסים טרויאנים ?

סוסים טרויאנים הם קבצים אשר מתחזים לקבצים רצויים ולגיטימיים אך למעשה הם קטלניים. ההבחנה העיקרית בין סוס טרויאני לוירוס נעוצה בעובדה שסוסים טרויאנים אינם משכפלים את עצמם כמו וירוסים. בדומה לוירוס הם מכילים קוד קטלני אשר יכול לגרום בהפעלתו לאיבוד ואפילו גניבה של חומר מתוך המחשב עצמו. סוס טרויאני מגיע בד"כ בצורה של קובץ מצורף להודעת דואר אלקטרוני או בצורה של הורדת קובץ מאתר אינטרנט .

מהם תולעים (worms)?

בניגוד לוירוסים, תולעים הן תוכניות אשר משכפלות את עצמן ממערכת למערכת גם ללא שימוש בקובץ מארח (לרוב בצורת מאקרו). תולעים משחררות מסמך אשר כבר מכיל בתוכו תולעת מאקרו והמקארו עצמו יכול להפעיל שורה של פקודות אשר ימשיך להפיץ את עצמו באמצעים אחרים כמו תוכנת הדוא"ל. דוגמא נוספת - התולעת היא גם שרת שליחת דוא"ל SMTP SERVER עצמאי, וע"י כך מפיצה את עצמה.

מתיחות וירוסים:

מתיחות וירוסים הן בד"כ הודעות אשר נשלחות באמצעות הדואר האלקטרוני ומזהירות על סוג של וירוס , כמו

"אם אתה מקבל את ההודעה הזאת , אל תפתח אותה "

"מחק אותה " , " הוירוס ימחק את כל הדיסק הקשיח שלך "

אם אינכם בטוחים אם מדובר בוירוס או במתיחה , אל תפתחו את ההודעה במידה ומצורף לה קובץ מיחקו אותה מייד .

בוטים (spyware), פירסומות ותוכנות ריגול :

בוטים, פירסומות ותוכנות ריגול אינם וירוסים, אך יכולים להטריד רבות את המשתמש, מעמיסים על מערכת ההפעלה וברוב המקרים מאיטים אותה וגורמים לתופעות שונות ומוזרות. קל מאוד להידיבק בהן , והן מגיעות דרך אתרי אינטרנט שונים, אשר מריצים תסריטים שונים ללא ידיעת המשתמש. תסריטים אלו מתקינים תוכנות שלמות על המחשב ורצים ברקע. בין הסימפטומים: שינוי אתר הבית בדפדפן האינטרנט, התקנת גישה לספקי אינטרנט, ואף הקפצת תמונות פורנוגרפיות . בד"כ בוטים ותוכנות ריגול "מזהמות" את קובץ הרישום של מערכת ההפעלה חלונות. אמנם לא מדובר בוירוסים אך יש להתגונן בפניהם באותה מידה.

Key logger

או בתרגום חופשי "יומן-הקשות", הוא תהליך אשר מופעל בדכ' ע"י סוס טרויאני - התהליך מרגע שמופעל, מתעד את כל ההקשות שהתבצעו על המקלדת לקובץ טקסט פשוט. קובץ כזה יכול להכיל גם סיסמאות ומפתחות אשר משמשות לגישה לחומר רגיש כמו גישה לדואר אלקטרוני, גישה לחשבון הבנק דרך רשת האינטרנט וכד' במידה ואלו הוקלדו בזמן שהתהליך פעל. יומני הקשות כאלו בדכ' נשלחים בדואר אלקטרוני או דרך שרתי FTP, כחלק מתהליך הפעילות של הסוס הטרויאני. הטיפול ביומן-הקשות, הוא נספח לטיפול בירוס, סוס טרויאני, או Spyware ונוסף על הסרת הוירוס עצמו יש גם להסיר את הקובץ הרישום עצמו לפי סוג ההדבקה. לאחר הניקוי יש לשנות את כל הסיסמאות!

נכתב על-ידי עופר ארבלי