גירסה 1.00 – 1.3.2001

וירוסים – סקירה קצרה

ניר אדר

הקדמה

אנשים רבים מכלילים וירוסים, סוסים טרוינים, פצצות לוגיות ועוד בהגדרה כוללנית של "וירוסים".
הגדרה זו מספקת קבוצות גדולות של אנשים, היודעים להשתמש במחשב ברמה בסיסית, ומשתמשים במחשב רק על מנת להפעיל תוכנות מסוימות כגון מעבד תמלילים וכדומה.
משתמשים מתקדמים יותר כבר מבינים שקיים הבדל בין ה"מזיקים" השונים.
במסמך זה אתמקד בוירוסים. אסביר מהו וירוס, כיצד נדבקים בוירוס, כדי מאתרים וירוסים ועוד.

מהו וירוס?

וירוס הוא תוכנה קטנה שיש לה היכולת להעתיק את עצמה על ידי הוספת הקוד שלה אל תוכניות מארחות ו/או איזורי מערכת. המשתמש בדרך כלל אינו מודע לפעולת השכפול של הוירוס, והוא נהיה מודע לקיומו רק כאשר הוירוס "מפעיל" את עצמו, שזה בד"כ מאוחר מדי עבור המשתמש.

כל וירוס מתנהג בדרך האופיינית לו. לכל וירוס יש מאפיינים המייחדים אותו.
הנה רשימה של מספר מאפיינים בהם וירוסים שונים אחד מהשני:

1. **גודל** – וירוס יכול להיות קטן, אפילו בגודל בתים ספורים, או יכול להיות גדול בהרבה. באופן כללי ניתן להגיד שוירוס קטן מאוד מהתוכנות אליהן הוא נדבק.

2. **שיטת ההדבקה** – וירוס יכול להדביק את התוכנות המארחות בצורות שונות:

- OVERWRITNG – הוירוס פשוט מחליף את התחלת התוכנית בקוד של עצמו. שיטה זו מיושמת על ידי וירוסים פרימיטיים, מכיוון ששיטה זו, למרות היותה קלה ליישום על ידי כותב הוירוס, מעוררת את חשדו של המשתמש. התוכנה המודבקת לא תוכל לעבוד יותר, ועל מנת לשחזרה יש להתקין אותה מחדש. שיטת הדבקה זו אינה משנה את גודלו של הקובץ המודבק.
- הוספה לסיום – שיטה זו מעט יותר מורכבת מהקודמת. הוירוס מוסיף עצמו לסוף הקובץ המודבק, ועורך את התחלת הקובץ כך שכאשר התוכנית רצה, היא קופצת להוראות המצויות בסוף הקובץ, היכן שהוירוס ממוקם, מבצעת אותן ואז חוזרת לתחילת הקובץ ומריצה את התוכנית כרגיל. עבור המשתמש, התוכנה תיראה כמתפקדת כרגיל. שיטת הדבקה זו גורמת לגודל הקבצים המודבקים לגדול.
- הדבקת דיסק – וירוסים אחרים מדביקים את הboot sector של הכונן או את הfat. זהו איזור ניתן להרצה בדיסק שרץ בצורה אוטומטית כל פעם שהמשתמש מעלה את המערכת דרך הכונן. על ידי הדבקת איזור זה, הוירוס נמצא בזיכרון ברגע שהמחשב עולה.

3. **TSR** – וירוס עלול להישאר בזיכרון. וירוסים הנמצאים בזיכרון בד"כ מדביקים כל תוכנה שהמשתמש מריץ. וירוסים שאינם נשארים בזיכרון מבצעים את פעולתם רק כאשר התוכנה המודבקת מורצת.

4. **STEALTH** – חלק מהוירוסים שנשארים בזיכרון יכולים להשתמש בשיטה המכונה STEALTH על מנת להתחמק מגילוי. הוירוסים מנטרים את פעולות המשתמש. כאשר המשתמש מבקש להציג קבצים, הם עלולים להסתיר קבצים וספריות מסויימים השייכים לוירוסים, או להציג את הגודל המקורי של הקבצים בזמן שהגודל שונה כבר על ידי הוירוס. על מנת לגלות וירוסים כאלו צריך להעלות את המערכת בעזרת דיסק נקי, ואז לראות את המצב האמיתי של הכונן הנגוע. וירוסים המדביקים את הboot sector יכולים להשתמש בטכניקה זו, ולעשות כך שכאשר המשתמש מבקש לראות את הboot sector, הוא יראה עותק של הboot sector המקורי, במקום את המודבק.

5. **זמן הפעולה והשפעתה** – תחום נוסף המבדיל בין הוירוסים הוא תנאי ההפעלה שלהם והפעולה שהם מבצעים. וירוסים מסוימים פועלים בתאריך קבוע מראש, אחרים כאשר תוכנה מסוימת רצה, אחרים יפעלו אחרי שהם הדביקו את כל הקבצים במערכת הודבקו וישנן עוד אפשרויות רבות. גם הפעולה של הוירוס יכולה להשתנות בין טווח רחב של אפשרויות. היא יכולה להיות לא מזיקה, כגון הצגת הודעה כלשהי על מסך המשתמש, או יכולה להשמיד לחלוטין את המידע בכונן הקשיח, או לבצע פעולות מזיקות אחרות. בתור משתמש, תמיד תרצה לאתר את הוירוס לפני שהוא יבצע את פעולתו.

איך ניתן להידבק בוירוס?

נושא זה הוא אחד מהנושאים המעורפלים לרוב המשתמשים. וירוס יכול להדביק את המערכת שלך רק בתנאי שאתה מריץ תוכנה הנגועה בוירוס, או מנסה להעלות את המערכת דרך דיסק נגוע. לא ניתן להידבק מוירוס על ידי צפייה בדיסק נגוע או בתוכנה נגוע. וירוס יכול להדביק כל סוג של קובץ הרצה, ביניהם EXE, COM, OVL, SYS, BIN ועוד. כמו כן הוא יכול להדביק את הfat או את הboot sector. אני מדגיש אחרי הסבר זה מספר נקודות:

1. כתבתי שעל ידי ניסיון להעלות את המערכת מדיסק נגוע המערכת יכולה להידבק. המערכת לא חייבת להעלות בהצלחה.
2. ניתן להידבק מוירוס כאשר מכניסים, למשל, דיסק לכונן התקליטורים במערכות Windows 9x או מתקדמות יותר, וזה מכיוון שקיים בWindows דבר הנקרא "Auto Run". האדם שהכין את הCD יכול לקבוע שתוכנה מסוימת תרוץ ברגע שהדיסק נכנס לכונן. אם תוכנה זו היא וירוס, המחשב יכול להידבק על ידי הכנסת הדיסק בלבד.

3. אינך יכול להידבק מקובץ המכיל נתונים, אלא במקרים בהם זהו קובץ הרצה ששונה שמו, ושתוכנה אחרת משנה שוב את שמו כך שניתן יהיה להריצו, או למשל קבצי נתונים כמו מסמכים של Word, המכילים אפשרות להוסיף בתוכם Macros, קטעי קוד בVisual Basic, שיכולים גם לרוץ כאשר המסמך עולה, ואז להדביק קבצים אחרים. (מה שעלול להעלות חרדות מסוימים אצל קוראי מסמך זה, לגבי הטרור שהוא כרגע מבצע במחשב שלהם ☺).

מהם הסימנים לכך שוירוס פעיל במערכת?

ישנם מספר דברים שעלולים לציין את העובדה שקיים וירוס במערכת:

1. גדילה לא מוסברת של גודל קבצי הרצה במערכת, עלולה לרמז על וירוס המוסיף עצמו לקבצים אלו.
2. תוכנות שעבדו בעבר מציגות כעת הודעות שגיאה, או מפסיקות לגמרי לעבוד. סימן זה עלול לרמז על וירוס שעשה Overwrite על קבצים אלו.
3. ירידה בזיכרון הפנוי של המערכת עלולה גם היא לציין קיומו של וירוס, הנשאר פעיל בזיכרון ומחכה כדי להדביק תוכנות.
4. שגיאות לא מוסברות כאשר מבצעים ScanDisk עלולות לרמז על וירוסים המסמנים את עצמם כאיזורים פגועים בכונן, על מנת שתוכנות לאיתור וירוסים לא יחפשו אותם במקומות אלו.
5. פניות לא מוסברות לכוננים – אם אור כונן הדיסקטים או הכונן הקשיח מתחיל לדלוק באופן פתאומי ללא סיבה, זה עלול לרמז על פעילות וירוס. יש לציין שלא תמיד אור הנדלק ללא סיבה מציין וירוס, מכיוון שwindows כותב קבצים לכונן מדי פעם, ובמקרה של דיסקט ייתכן שבהידלק האור עובד מידע מהcache של המחשב אל הכונן.
6. האטה של המערכת – אם המערכת מתחילה לפעול באיטיות, ותוכנות מתחילות לרוץ לאט יותר, יתכן שוירוס פעיל במערכת.

איך ניתן להתגונן מפני וירוסים?

הדרך הבטוחה ביותר לא להידבק בוירוסים היא לא להריץ שום תוכנה שאיננה מותקנת כבר במערכת, ולא לקבל דיסקטים השייכים לאיש מלבדך. לרוע המזל, רק לעיתים רחוקות שיטה זו מעשית. לכן, עלינו למצוא את האלטרנטיבות הבאות הטובות ביותר:

1. **גיבויים** – עשה גיבויים באופן קבוע של הקבצים החשובים במערכת. צא מתוך נקודת הנחה שבכל רגע אתה עלול לאבד את כל תוכן הכונן. האם יש לך גיבוי של רשימת הסיסמאות שלך? של רשימת הטלפונים שלך? רשימות כגון אלו הן קשות לשחזור במקרה של אובדן.

2. חשוב **לשמור דיסקט נגיע ומוגן** (write protected) של המערכת, על מנת שתהיה אפשרות לשחזר את המערכת במקרה של פגיעת וירוס. בזמן התקנת Windows, ניתנת לך האפשרות ליצור דיסקט הפעלה. כמו כן ניתן ליצור בעזרת windows דיסקט הפעלה במועד מאוחר יותר, דרך "לוח הבקרה".
3. **התעדכן בנוגע לוירוסים חדשים**, וכיצד הם עובדים. השתמש בידע זה על מנת לנקוט צעדים מונעים או צעדי טיפול במקרה של וירוס.
4. **תוכנות אנטי-וירוס** – ישנן לא מעט תוכנות אנטי וירוס טובות בשוק, היכולות לעזור באיתור והסרת וירוסים. קשה להצביע על התוכנה הטובה ביותר. בחר את האנטי וירוס המועדף עליך על ידי בדיקה של כמות וסוגי הוירוסים והמזיקים האחרים שהאנטי וירוס מגלה, וגם על פי התדירות בה האנטי וירוס מתעדכן. עדכונים לאנטי וירוס הם קריטיים על מנת לשמור את המערכת שלך כמה שיותר נקייה מוירוסים. ניתן להשתמש אף ביותר מתוכנת אנטי וירוס אחת, על מנת לסרוק את המערכת שלך עם סיכויים גדולים יותר לאיתור וירוסים. אפשרות זו עלולה לפעמים לגרום להתנגשות בין האנטי וירוסים השונים, המזהים לעיתים אחד את השני בתור וירוסים. פתרון לבעיה זו הוא להריץ כל פעם אנטי וירוס אחר. במערכת שלי מותקנים שני אנטי-וירוסים. אחד פעיל כל הזמן (אמור להיות פעיל כל הזמן אם נדייק) ואת השני אני מפעיל רק כאשר אני עושה סריקה של הכונן פעם בכמה זמן.