

# איך לכתוב וירוס ללינוקס

## או למה לינוקס יותר בטוחה, בלי קשר לשכיחות

### שחר שמש, יועץ קוד פתוח וחבר בוועד עמותת "המקור"

אחת לכמה ימים מתפרסמת עוד הודעה בעיתון המזהירה את המשתמשים מעוד תולעת המדביקה את מערכות חלונות השונות ומתפשטת הלאה. בכל פעם שכתבה מעין זו מתפרסמת בעיתון מקוון, מיד יש מספר מגיבים שאומרים "תתקינו לינוקס". ראויות לציון במיוחד התגובות לכתבה ב-YNet על [Sober.A](#). במקרה זה התפתח הדיון בין המגיבים לגבי האם, אילו תהפוך לינוקס למערכת הפעלה נפוצה, יהיו גם לה וירוסים. כדי לחקור נושא זה, בואו ננסה לכתוב ביחד וירוס ללינוקס.

## מכשול מס' 1 – הפתיון

בניגוד למה שמקובל לטעון ביחס לחלונות, רוב הוירוסים לחלונות אינם נובעים מחורי אבטחה במערכת עצמה. למעט יוצאי דופן בולטים כמו Blaster ו-Slammer-1, כמעט כל התולעים המודרניות, החל מ-Melisa הזכור לרע, ועד ל-Sober.A העדכני, פועלות ע"י מה שמכונה "הנדסת אנושית" (Human Engineering). טכניקה זו כוללת רכיב מטעה באימייל שיגרום לאנשים להריץ את הקוד הזדוני, מתוך צפיה למצוא משהו אחר. הטכניקות כוללות כותרות מושכות (מישהו זוכר את "I love you"?), התחזות לעדכוני אבטחה, ועכשיו האשמה שנדבקתם בוירוס. רכיב מרכזי בכל מנגנון הטעיה הינו הקלות שבה הקורבן יכול להריץ קוד שנשלח אליו. ככל שתהליך ההדבקה עצמו דורש מהקורבן יותר שלבים, כך גדל הסיכוי שההדבקה תכשל.

וכאן אנו נתקלים במכשול הראשון – בניגוד לצפיה ב-PDF או ראיית סרט שנשלח אלינו בלינוקס, פעולות שמתבצעות בדומה לצורה שמתבצעות בחלונות, לא מייד לקחת תוכנה שנשלחה אלינו ולהריץ אותה. הסיבה להבדל נעוצה בעובדה שמערכות Unix מחליטות אם קובץ הוא בר הרצה לא על סמך שמו, אלא על סמך ההרשאות שלו במערכת הקבצים. הרשאות אילו אינן מלוות את הקובץ בעוברו בדוא"ל. במילים אחרות – לא ניתן לשלוח קובץ כך שהקלקה עליו תוביל להרצתו ממילא, גם לא אם הוא וירוס.

ניתן, לכאורה, לשלוח את הקובץ מכווץ בצורה שכן תשמר את ההרשאות שלו. גם אם נעשה זאת, אולם, חסר שלב חשוב ביותר בתהליך – איך לגרום לקורבן להריץ את הקובץ מבלי שיבין שזה מה שהוא עושה. אנחנו רואים שכבר בשלב הראשון של תכנון הוירוס שלנו ללינוקס נתקלנו בבעיה שלחלוטין לא קל לעקוף אותה.

## מכשול 2 – ההדבקה

בואו נניח שמצאנו דרך פלאית לעקוף את הבעיה הראשונה. לכאורה, בשלב זה אנחנו יכולים לעשות על המחשב את כל מה שהמשתמש הלגיטימי של אותו המחשב יכול לעשות.

בפועל, אנחנו מגלים שהמצב מעט יותר מסובך. ראשית – אנחנו לא יכולים להיות בטוחים באיזו מערכת הקורבן שלנו משתמש. בניגוד לחלונות, בה ניתן להניח

שהדפדפן הוא אקספלורר, מערכת הדוא"ל היא Outlook או Outlook express, והסביבה היא חלונות, בלינוקס קיימות מספר חלופות בשימוש נפוץ לכל אחת מהמטלות הנ"ל. הדבר גורם לכך שהרבה יותר קשה (אף כי לא בלתי אפשרי) לנו לדעת איך אנחנו צריכים לפעול כדי להמנע מגילוי, וכדי להשיג את התוצאות.

בנוסף לכך, משתמש לינוקס טיפוסי אינו מחובר למחשב עם משתמש בעל הרשאות לעשות נזקים למחשב. במערכת חלונות כולם מנהלים הסיבה היא שאם אינכם מחוברים בהרשאות מנהל, לא ניתן להריץ את רוב התוכנות. בלינוקס מקובל שלא להתחבר כמנהל, וכל התוכנות זמינות ועובדות. כתוצאה מכך, אין כמעט משתמש לינוקס שגולש באינטרנט או קורא דוא"ל בעודו מחובר כמנהל. במילים אחרות – גם אם הצלחנו להדביק את המשתמש, עדיין איננו יכולים להדביק את המחשב כולו. נוכל לשלוח דואר ולהפיץ את הווירוס הלאה, אבל נזקים מקומיים ייצטרכו להיות מוגבלים למסמכים ולמידע, ללא יכולת לגעת בתוכנות.

### **מכשול 3 – ההסרה**

זה לא סוד. כדי שהווירוס שלנו יהיה מוצלח, צריך להיות קשה להסיר אותו. המגבלה של ההדבקה מהסעיף הקודם נעשית פתאום לבעיה אמיתית. כל שצריך לעשות כדי להסיר את הווירוס שלנו הוא להתחבר למחשב כמנהל, להרוג את כל המשימות שהמשתמש שהודבק מריץ (כדי שהווירוס לא יהיה בזיכרון), ולתת למשתמש ספרית בית נקיה חדשה. הפעולה דורשת כחצי דקת עבודה, אינה דורשת אנטי וירוס, ואינה תלויה בוירוס הספציפי. ניתן אפילו לתת למשתמש גישה לקבצים מהספרייה הישנה, כדי שיוכל להעביר את המידע, אם הווירוס לא הרס אותו.

### **מסקנות**

אנחנו רואים שכתובת וירוסים לחלונות הינה משימה קלה לאין שיעור יותר מאשר כתיבת וירוסים ללינוקס. כל סיבות הנ"ל הן סיבות טכנולוגיות ותרבותיות, ואינן קשורות למידת השכיחות של המערכות. אין הדבר אומר שמדי פעם לא יוצו וירוסים שיצליחו להתגבר, בהפצה מסויימת, בגרסאות מסויימות, במקרים מסויימים, על המכשולים הנ"ל. נסיון העבר מראה שגם כאשר זה קורה, תפוצת הווירוס קטנה בהרבה, וכתוצאה מכך גם הנזק שהוא גורם.

הסיבה מספר אחת לכך שחלונות הינה מערכת פחות בטוחה בפני וירוסים הינה העירבוביה שבה מתייחסת חלונות למידע ולקוד, דבר הגורם לשליחת קוד להיות קלה ופשוטה. ערבוביה זו אינה נפוצה במערכת לינוקס, ומכאן הקביעה שמערכות אילו עמידות בהרבה בפני וירוסים וקוד זדוני.