גירסה 2.00 - 15.12.2001

איך להתגונן מBack Orifice

מסמך זה ניתן להפצה באופן חופשי, כל עוד הוא נשאר ללא כל שינוי ותוספות.
כל נזק, ישיר או עקיף, שיגרם בעקבות מסמך זה הוא באחריות הקורא בלבד.
כל הזכויות שמורות ל**ניר אדר**.

Nir Adar
Email: underwar@hotmail.com
Home Page: http://underwar.cjb.net

במסמך זה אני אסביר מה היא Back Orifice, איך תוכנה זו עובדת, ואיך מתגוננים ומסירים אותה.
תודה מיוחדת ל Xenoscide מהUnderNet (daemus@digicron.com), שבלעדיו מסמך זה לא היה קיים.

מה זה Back Orifice

Back Orifice (בקיצור BO) זוהי תוכנה שפורסמה בידי the Cult of the Dead Cow במטרה "ליצור קשר בקלות" בין שני מחשבים. למעשה זהו טרוין הנותן גישה למחשבים נגועים.

איך Back Orifice עובדת

BO עובדת כך : מישהו שולח את תוכנת השרת (הטרויין) לאדם שני. האדם השני מריץ את הקוב.. BO מסתירה את עצמה במערכת, וגורמת לעצמה להיטען בכל הפעלת WINODWS. כמו כן היא מסתירה את עצמה משורת המשימות ומתפריט המשימות. לאחר מכן BO פותחת פורט ומקשיבה לו, מחכה שמישהו מהאינטרנט יצור קשר.

איך לגלות האם אתה נגוע

ניתן לגלות האם אנו נגועים בכמה שלבים :

1. פתח חלון דוס.
2. כתוב : NETSTAT -a –n
3. אם אתה רואה את אחד מהפורטים הבאים פתוחים יש סיכוי טוב שאתה נגוע :
   31337, 666, 411.
4. שיטה נוספת היא לחפש את הקובץ windll.dll ששייך לBO. מציאותו היא סימן נוסף לכך שאתה נגוע.

איך לגלות אילו קבצים עושים לך את הצרות

דבר ראשון, עשה חיפוש ומצא את הקובץ windll.dll . לאחר מכן חפש תלחץ בwindows 95 על "התחלה", "חיפוש", "קובץ או ספרייה" ואז :
איפה שכתוב "היכן לחפש" שים את הספרייה בה נמצא windll.dll.
לאחר מכן לחץ על "מתקדם" וכתוב שם bofile ואז לחץ "חיפוש".
תקבל רשימה של הקבצים שקשורים לBO.

איך למחוק את Back Orifice

הרץ את regedit, על ידי "התחלה", "הפעלה", "regedit " וenter.
נווט בעץ עד שתגיע ל :
HKEY_LOCAL_MACHINE\software\microsoft\windows\currentversion\runservices
אז חפש את אחד משמות הקבצים שמצאת קודם, והסר אותו.
הזהר בשיטה זו, כי אתה יכול לפגוע בקלות בwindows אפילו בצורה שתדרוש התקנה מחדש, אם אתה עושה משהו לא נכון.
שיטה שניה היא לצאת מ widnows לגמרי לDOS, ומשם למחוק את הקבצים של BackOrifice, אותם איתרת קודם.

דרכים נוספות למחוק את Back Orifice

כיום כל תוכנות האנטי וירוס החדשות מסוגלות להסיר את Back Orifice מהמערכת.
ניתן לקנות אחת מהן או להוריד דמו לתקופה מסויימת בחינם, ולהוריד את הטרויין.
כמו כן ישנן תוכנות המסתובבות ברשת שכל מטרתן הוא להפוך את תהליך הסרת Back Orifice לאוטומטי. ניתן למצוא בקלות רשימה של תוכנות כאלו על ידי חיפוש Back Orifice Clean במנועי החיפוש השונים.

EOF