

פרק 10

קודגורו אקסטרים

- ▶ CodeGuru Extreme: תחרות ארצית יוקרתית, בה קבוצות מתחרות זו בזו על כתיבת תוכנה שתשלוט בזירה וירטואלית.
- ▶ התוכנות נכתבות בשפת אסמבלי ונקראות "שורדים".
- ▶ התחרות מתקיימת אחת לשנה.
- ▶ התחרות מתבצעת בקבוצות של 2-5 תלמידים.

יתרונות ההשתתפות בתחרות

- ▶ הזדמנות לחדד את כישורי התכנות באסמבלי
- ▶ לימוד יכולת חשובה - מחקר תוכנה על ידי Reverse Engineering
- ▶ השתתפות בתחרות היא פרט ראוי לקורות חיים וראיונות
- ▶ תחרות כיפית ומהנה, חווייה



חוקי התחרות בקצרה

- ▶ כל קבוצה מגישה קוד אסמבלי, שנקרא שורד
- ▶ השורדים של כל הקבוצות נטענים אל זירה וירטואלית בגודל 64 קילו בתים
- ▶ כל שורד מריץ כל תור פקודת אסמבלי אחת
 - אפשר לנסות לפגוע בקטע קוד של שורד מתחרה
- ▶ אם שורד מנסה להריץ פקודה לא חוקית הוא נפסל
- ▶ השורד האחרון- מנצח
- ▶ צוות התחרות מכניס לזירה "זומבים"- תוכנות זדוניות
 - כוללים חידת מחשבים או מתמטיקה
 - אפשר לנסות להשתלט עליהם ולגרומ להם לתקוף את היריבים

מקורות ללימוד

▶ מדריך לתחרות:

<http://www.cyber.org.il/assembly/codeguru-guide.pdf>

▶ מצגת:

<http://www.cyber.org.il/assembly/codeguru-slides.pdf>

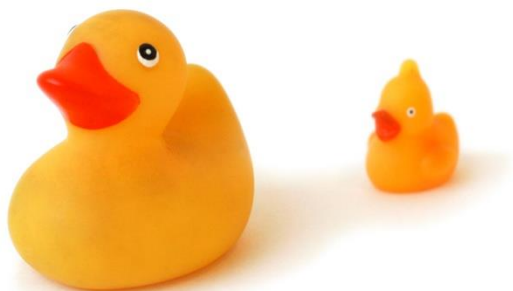
▶ פורום ארצי:

<http://www.codeguru.co.il/wp/?forum=%D7%90%D7%A7%D7%A1%D7%98%D7%A8%D7%99%D7%9D>

Reverse Engineering של זומבים

www.cyber.org.il/assembly/zombies.zip

- ▶ דוגמה 1 - duck.com
- ▶ נסו לגלות מה הוא מבצע?



```

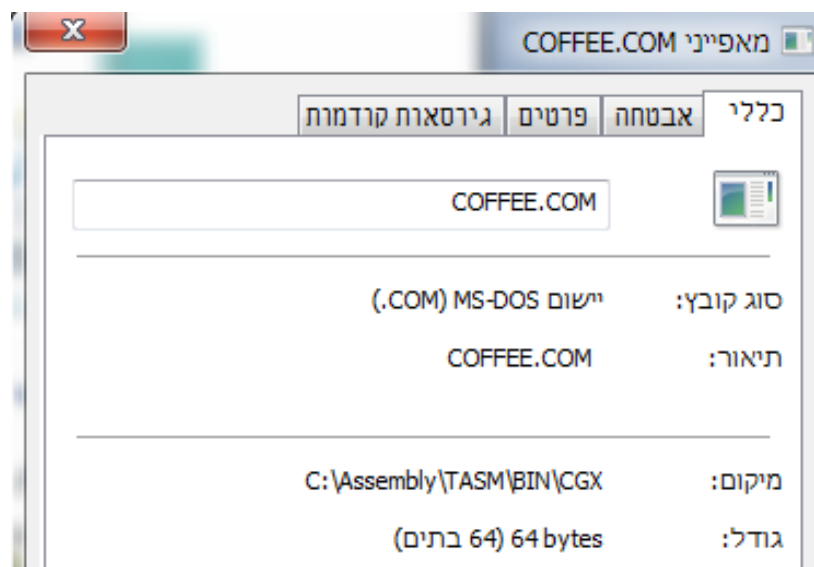
[ ]=CPU 80486
cs:0100 EBFE      jmp     0100 ↓
cs:0102 16       push   ss
cs:0103 A6       cmpsb
cs:0104 08830672  or     [bp+di+7206],al
cs:0108 090A     or     [bp+si],cx
cs:010A C74602FB09   mov    word ptr [bp+02],09FB
cs:010F 2E8E1E0000 mov    ds,cs:[0000]
cs:0114 A1F028     mov    ax,[28F0]
cs:0117 894604   mov    [bp+04],ax
cs:011A 5E       pop    si
cs:011B 5F       pop    di
cs:011C 5A       pop    dx
cs:011D 59       pop    cx
cs:011E 5B       pop    bx
cs:011F 58       pop    ax
  
```

```

start:
        jmp     start
end start
  
```

- ▶ נפתח את הקובץ בדיבאגר
- ▶ נריץ עם F7
- ▶ האם תוכלו לשחזר מהו הקוד שיצר את קובץ ההרצה?
- ▶ מהן הפקודות שאחרי כתובת cs:0102h?

▶ איך אפשר למצוא בוודאות את מיקום סיום הקוד?




```

cs:0100 0E      push  cs
cs:0101 07      pop   es
cs:0102 CD87    int   87
cs:0104 8A160000 mov  dl,[0000]
cs:0108 80FA43   cmp   dl,43
cs:010B 75F7     jne   0104
cs:010D 8A160100 mov  dl,[0001]
cs:0111 80FA30   cmp   dl,30
cs:0114 75F7     jne   010D
cs:0116 8A160200 mov  dl,[0002]
cs:011A 80FA46   cmp   dl,46
cs:011D 75F7     jne   0116
cs:011F 8A160300 mov  dl,[0003]
cs:0123 80FA46   cmp   dl,46
cs:0126 75F7     jne   011F
cs:0128 8A160400 mov  dl,[0004]
cs:012C 80FA45   cmp   dl,45
cs:012F 75F7     jne   0128
cs:0131 8A160500 mov  dl,[0005]
cs:0135 80FA45   cmp   dl,45
cs:0138 75F7     jne   0131
cs:013A 8B1E0600 mov  bx,[0006]
cs:013E 53      push  bx
cs:013F C3      ret
cs:0140 BD00BB    mov  bp,BB00
cs:0143 B82606    mov  ax,0626
cs:0146 6A00    push  0000
cs:0148 50      push  ax
cs:0149 6A04    push  0004
cs:014B 6A00    push  0000

```

נפטר מה"פצצה החכמה"

בודק אם בכתובת 0000
נמצא התו C

בודק אם בכתובת 0001
נמצא התו 0



קופץ לכתובת שנשמרה
בכתובת 0006

- ▶ זומבי אמיתי שהמתחרים הצטרפו לפענח בתחרות 2015
- ▶ לימוד עצמי מהספר:
 - פקודת XLAT
 - הסבר מודרך

