טכנו"צ סייבר – תרגיל 1 – "H3LL0 W0RLD"

הקדמה

ברוכים הבאים לתרגיל הראשון בקורס טכנו"צ סייבר! ראשית נסביר בקצרה כיצד התרגילים השנה יעבדו.

הסבר על תרגילים בקורס

בכל פעם (בין שבוע-לשבועיים), יתפרסם תרגיל חדש בקורס. התרגיל הוא המשך ישיר של החומר הנלמד בהרצאות ובתרגולים, ומטרתו היא **להוריד את החומר הנלמד לקרקע**. למשל – כאשר נלמד בהרצאות על תקשורת בין מחשבים נממש מנגנון תקשורת בעצמנו, וכך **נבנה את העולם התיאורטי והמעשי במקביל**.

בנוסף, כל התרגילים בקורס **נבנים אחד על השני** – מטרת העל היא שכל אחד מכם יבנה נוזקה (וירוס) משלו. בכל תרגיל נוסיף עוד תכולות לנוזקה שמתבססות על הקודמות. קונספט מאוד דומה חלקכם כבר חוויתם בקורס **Nand2Tetris** (ולמי שעוד לא עבר אותו – מומלץ לקרוא עליו באינטרנט!).

לרוב התרגילים בקורס יהיו **שאלות בונוס**, השאלות יוכלו לעזור להשלים את הציון של התרגיל ל-100 ובעיקר נועדו בכדי לאתגר את המחשבה שלכם ולאפשר העמקה בחומר של כל תרגיל.

כמובן, לאורך כל הדרך אתם **מוזמנים לפנות לסגל הקורס בכל שאלה** – נשמח לעזור ולמקד אתכם בחלקים המשמעותיים בכל תרגיל. לבסוף, כיוון שמדובר בקונספט חדשני (כרגע בגדר פיילוט), נעריך כל **פידבק מכם** על איכות התרגילים, נוחות העבודה וחווית הקורס.

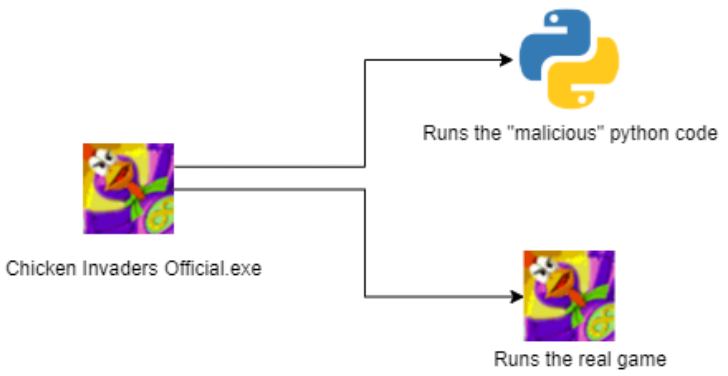
טכנו"צ סייבר – תרגיל 1 – "H3LL0 W0RLD"

תרגיל 1 – התממה של תוכנה זדונית

מטרת העל

בתרגיל זה נרצה להסתיר קוד זדוני (הנוזקה שלנו) בתוך תוכנה שנראית לכאורה לגיטימית (מתקפת front-door). "נתלבש" על תוכנה קיימת, וניצור ממנה תוכנה **חדשה**, שבעת הרצתה תריץ גם את התוכנה עליה התלבשנו **וגם את הנוזקה שלנו**.

התוכנה שעליה נתלבש הינה המשחק "Chicken Invaders": משחק ישן ומוכר שאנחנו מקווים שאין צורך להסביר כאן. בתרגיל נגרום לכך שבעת הרצת התוכנה ירוץ גם קוד הפייתון הזדוני שלנו.



בתרגיל זה קוד הפייתון ייצור קובץ ששמו "malware.txt" וייכתוב בו "Hello, world".
בתרגילים הבאים נפתח התנהגויות יותר מורכבות (זה נבנה, זוכרים?).
נשים דגש משמעותי על **התממה** – לא נרצה שהמשתמש התמים יחשוד באפליקציה שלנו.

הערה: בתרחיש מבצעי נפרסם את התוכנה החדשה שלנו באינטרנט תחת שם כמו FREE CHICKEN INVADERS DOWNLOAD ונקווה להפיל בפח אנשים תמימים (זיכרו – זהו רק תרגיל!)

אנקדוטה: במקור רצינו לבנות את התרגיל על המשחק Tetris (כדי להמשיך את Nand2Tetris בTetris2Virus). באופן אירוני, כשכותב התרגיל עמד להוריד גרסא חינמית של המשחק, האנטיוירוס זיהה נוזקה מפורסמת מותממת בתוך קובץ ההרצה ולכן הרעיון חוזל"ש.

טכנו"צ סייבר – תרגיל 1 – "H3LL0 W0RLD"

חומרי עזר

בתרגיל מסופקים לכם מספר חומרי עזר. נמנה אותם כאן:

1) קובץ zip שמכיל את קבצי המשחק המקורי של chicken invaders. בתוכו יש את "Chicken Invaders.exe", הפונדק של הנוזקה שלנו.
2) קובץ setup.py בסיסי, שמאפשר המרה של קוד פייתון לexe.

תכולת הzip התמים אמורה להיראות בערך כך:

Name	Size	Modified
bass.dll	98 360	2008-10-28 15:00
channel.tga	56 684	2006-04-19 15:17
Chicken Invaders.exe	3 069 440	2010-12-25 10:58
CI4.cfg.static	148	2010-11-03 19:05
CI4.dat	70 727 876	2010-11-29 12:38
iastyle6.css	4 424	2009-07-08 22:00
iconsext.zip	34 712	2021-01-18 03:54
kc_rename.CI4.cfg.static	148	2010-11-03 19:05
logo.ico	93 062	2021-01-18 03:59
sdat64.dll	3 090 940	2007-02-01 10:06

שלבי התרגיל

1) בתור התחלה, הורידו את קבצי העזר הרלוונטים ותוודאו שאתם מצליחים להריץ את המשחק.

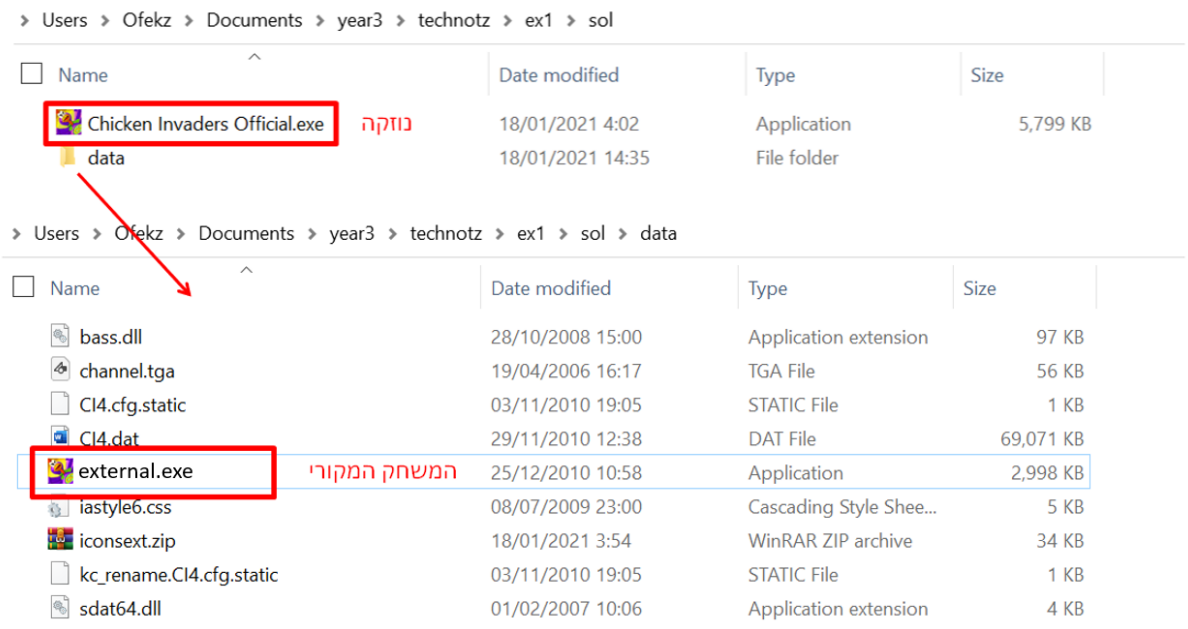
2) צרו באותה התיקיה קוד פייתון משלכם (לא חשוב השם), שמריץ את המשחק Chicken Invaders ומיד לאחר מכן יוצר את הקובץ malware.txt עם התוכן Hello, World. מומלץ לקרוא על הספריה subprocess בפייתון (וספציפית על הפקודה Popen).

3) השתמשו בספריית py2exe (מוזמנים לחפש באינטרנט) ובקוד setup.py שקיבלתם על מנת לקבל exe של הנוזקה שלנו. וודאו שהכל עובד, ותנו לעצמכם טפיחה על השכם – יש לנו MVP!

4) נזכיר שמילת המפתח היא **התממה**. נרצה שלexe שניצור יהיה אותו אייקון כמו למשחק המקורי כדי לתת לו מראה "תמים", קראו כיצד ניתן באמצעות py2exe להחליט מה יהיה האייקון.

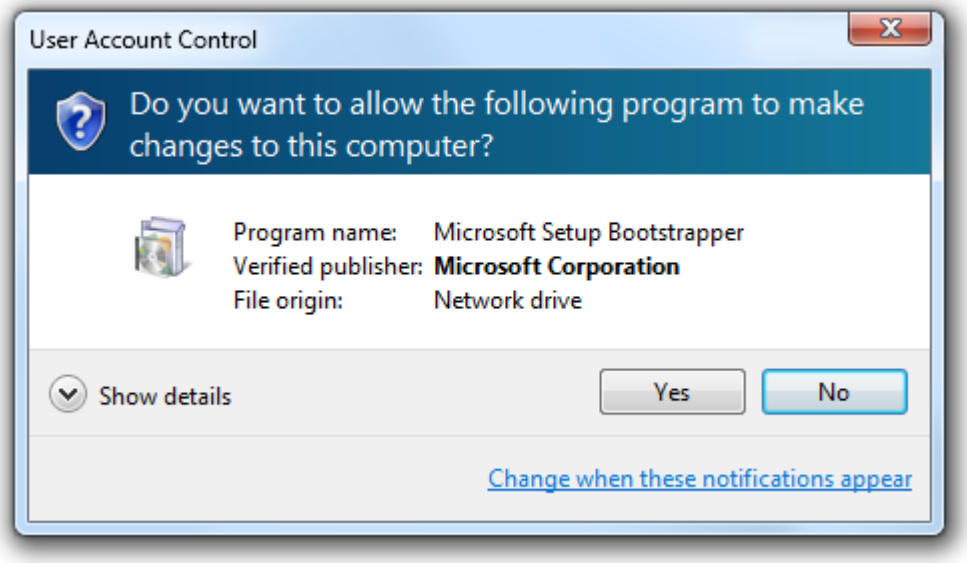
5) בנוסף, נרצה לסדר את כל הבלאגן של הקבצים שנוצר כדי לעטוף את הנוזקה שלנו בצורה יפה ותמימה ולוודא שהמשתמש מריץ **בדיוק** את הנוזקה.
צרו תיקיה ששמה data, והכניסו את כל הקבצים של המשחק שאינם הנוזקה שלכם אליה. בתוך אותה תיקיה, שנו את קובץ ההפעלה של המשחק המקורי לשם פחות אטרקטיבי (ניתן להתפרע פה...), כדי שהמשתמש לא יתבלבל בין המשחק המקורי לבין הנוזקה – אנחנו רוצים שהדבר שייראה לו הכי הגיוני זה להריץ את הנוזקה. שימו לב שצריך לעדכן את קוד הפייתון בהתאם לכל השינויים כדי שיריץ את המשחק המקורי. אמור להיות לכם משהו שנראה ככה:

טכנו"צ סייבר – תרגיל 1 – "H3LL0 W0RLD"



6) נרצה שהexe המרושע שלנו יריץ דברים בהרשאות של מנהל (User Account Control, UAC), כדי שבהמשך הקורס נוכל לבצע דברים יותר "זדוניים". תחפשו באינטרנט כיצד ניתן לגרום לקוד הפייתון שלכם לבקש הרשאות שכאלו. אינדיקציה טובה להאם הקוד שלכם עובד תהיה אם תראו pop-up כמו:

טכנו"צ סייבר – תרגיל 1 – "H3LL0 W0RLD"



7) כעת זה תורכם לחשוב על עוד דרכי התממה של הקוד הזדוני. נציג שתי בעיות התממה לדוגמא שעוד לא כיסינו:
   a) **תאריכים** – exe שלנו מ2022 והשאר מ~2008.
   b) **הקובץ המקורי בתיקיית data** – אמנם בחרנו בשם פחות מפתה, אבל למשתמש חכם יהיה מוזר שהוא בכלל קיים.

בעיות שבאלה עלולות להעלות חשד ולגרום למשתמש לא לרצות להריץ את הנוזקה שלנו. פתרו את בעיית התאריכים, ובנוסף חשבו על דרך יצירתית (וממשו אותה) להתמים את exe המקורי של המשחק.

8) **בונוס מעשי**
   a) דאגו לכך שעבור משתמש תמים שמשווה את התיקייה לפני ואחרי החדרת הווירוס שלנו (רק במראה בלי לעבור על תוכן הקבצים **גם הנסתרים**), שתי התיקיות יראו זהות לחלוטין. תארו בקצרה איך עשיתם את זה.

9) **שאלות בונוס**
   a) פתחו את הקובץ של הווירוס שלנו, נסו להבין כמה שיותר פרטים עליו רק באמצעות הסתכלות על התוכן של הבינארי המקומפל. מה היה כדאי להסתיר ואיך?
   b) מה היתרונות ומה החסרונות של לכתוב ווירוסים בפייתון?
   c) האם יש שפה ספציפית שתמיד נרצה להשתמש בה בכתיבת ווירוסים? אם לא, נסו להסביר מתי עדיף לכתוב בשפה אחת ומתי עדיף בשפה אחרת.

טכנו"צ סייבר – תרגיל 1 – "H3LL0 W0RLD"

הגשה

עליכם להגיש את התיקיה של המשחק העטוף (כלומר, מה שצילמנו בסעיף 5, ולאחר השינויים שלכם), בנוסף **לקובץ README בו תפרטו כיצד התמודדתם עם הבעיה מסעיף 7** (התממת הexe) ואת שאלות הבונוס (במידה ועשיתם אותן). את שני אלו הגישו בקובץ ex1_[FullName].zip ותעלו אותו לmoodle. בהצלחה!