



אתגר 10

כלי דיאגנוזטיים

ברק גובן

מטרה

באתגר תמשו קרייה מקובץ באמצעות WinAPI ולאחר מכן תנתחו את הפעולות שלה
אליה השלבים שתעבירו:

כתיבת נזקה	הסרת הנזקה
כתיבת נזקה	רקע התקנת הנזקה הסרת הנזקה

כיווט במסמך

תוכן

1.....	מטרה
2.....	לינקים שימושיים
3.....	הסרת הנזקה.....
4.....	כתבת נזקה (בונוס).....
6.....	זהו!!!
7.....	נספחים.....
7.....	dagshim לתוכנות נכון

נתרגל מיזמנים חשובות

- נבין את מבנה הקריאה לkernel.
- נלמד איך לעבוד עם הדוקומנטציה של API Win.
- נלמד איך לעקוב אחריו תהליכיים עם Procmon.

لينקים שימושיים

- כדאי לקרוא גם [דגשים לתכנות נכון](#).
- בסוף יש [אקליסט שימושי](#) למקבץ אחרי ההתקדמות ביצוע המשימה.

בהצלחה يا אלופות ואלופים!



הסרת הנזקה

בתיבת נזקה

הסרת הנזקה

רמת קושי: בינוני

מחקר – הגשה בקובץ ex9.docx



רקע

בתרגיל זה תתקינו נזקה חינוכית, שפיתחנו במיוחד לצורך התרגיל. הנזקה טוודנית מעט, אך היא אינה עשויה נזק למחשב ולא מדיקה מחשבים אחרים. מטרתכם היא להסיר אותה. מיד תראו שמי שמתקין את הנזקה זה אתם, ויכול להיות שתחשבו שתשאלו את עצמכם האם זה משקף את המציאות? בלומר, מדוע שימושו ית��ן נזקה במחשב שלו עצמו? למעשה זה נפוץ מאד. נזקות רבות מציגות את עצמן בתוכנות SMBצעות דברים טובים ומשכנעות אותנו להוריד ולהתקן אותן. לאחר שהתקנו אותן צריך להתמודד איתן ולמצוא דרך להסיר אותן.

התקנת הנזקה

הקליקו על חבילת ההתקנה windows Naughty. יוצר קיצור דרך על ה-desktop שלכם. הפעילו אותו באמצעות לחיצה ימנית ובחרו Run as administrator (חשוב מאד! בלי הרשות מתאימה ההתקנה לא תעבור במו שצරיך). זהו סימתם, בעת נסxo להסיר אותה. יש לבבות את windows defender וכל תוכנת אנטי וירוס (תוכנות אלה עלולות למנוע ריצה של הוירוס), כמו כן לוודא כי התוכנה בבוי גם לאחר אתחול המחשב.

dagshim:

- השתמשו בכלים שנלמדו בשיעור
- אם אתם חושבים שהסרתם את הנזקה, הדליקו את המחשב מחדש ובידקו שהnazka לא מקפיצה הודעה למסך

מה להגיש?

עליכם לבתוב מדריך להסרת הנזקה. בלומר, אין צורך להסביר את כל שלבי המחקר שלכם אלא מהי הדרך הקצרה והיעילה ביותר להסיר את הנזקה. היבן ללחוץ, מה לשנות.

בtíת נזקָה (בונוס)

בtíת נזקָה רמת קושי: בינונית	הסרת הנזקָה
---------------------------------	-------------



ex8-2.c/cpp – הגשה בקובץ



כיתבו את הנזקָה בעצמכם!

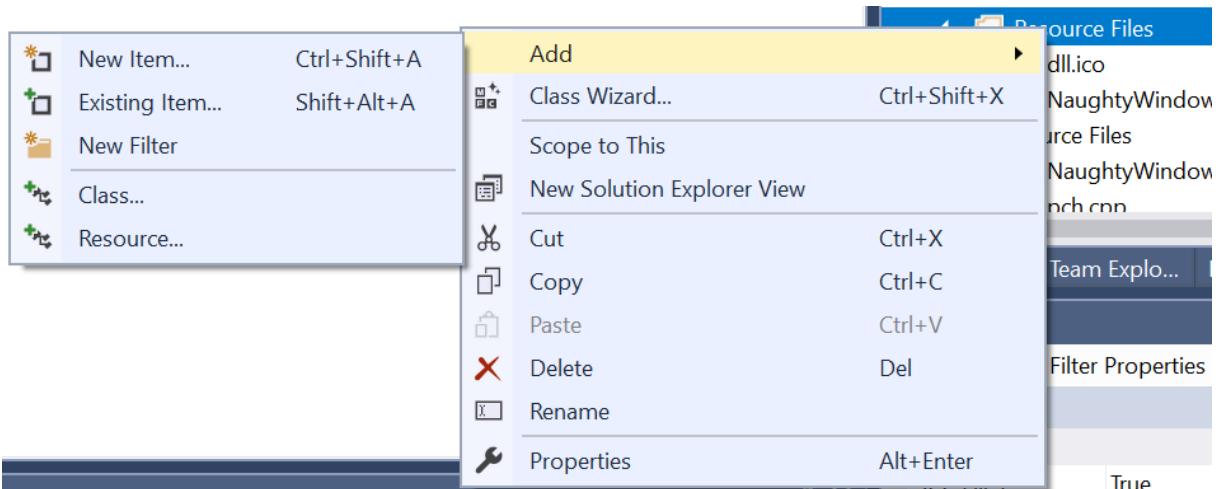
שלבים:

- לימדו אילו פקודות API WinAPI כתובות לרגיטרי ובחרו להיכן ברגייסטרי לכתב את הערכים הנחוצים לבם
- להלן הסבר על איך מוסיףים איקון לתוכנה
- להלן הסבר על איך יוצרים חבילת התוכנה

הוספה Resource

בלי resource התוכנה שלנו חסרת icon ופרטים.

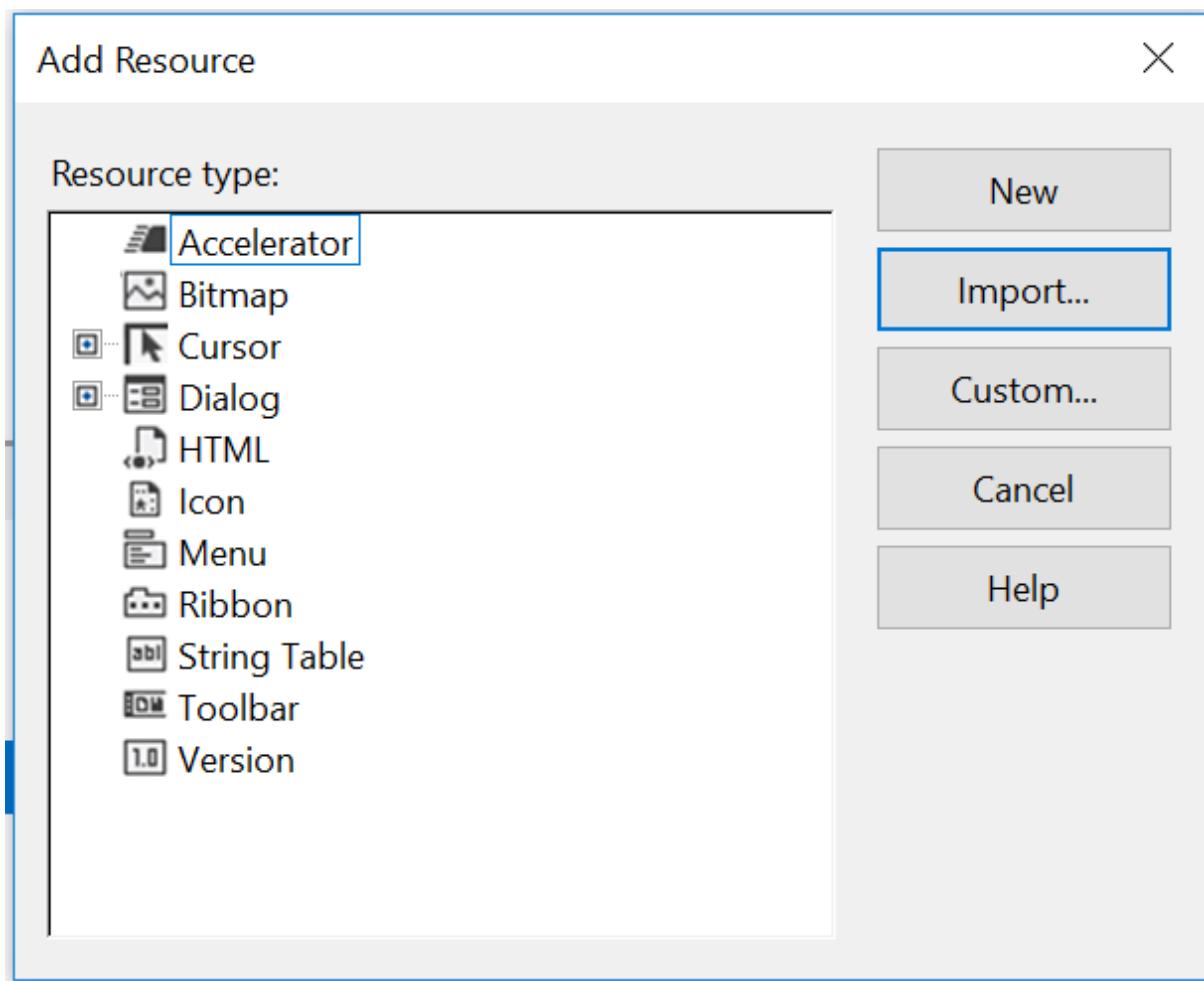
בתוך Solution Explorer נעמוד על Resource Files ונקליק קليك ימני. נבחר Add ואז



ראשית נבחר קובץ Version, מזמן לתוכו את כל השדות בגין יצורן, גרסה.

הכנת קובץ icon: תוריד קובץ icon בפורמט jpg. האתר icon converter dgz. ממיר אותו לקובץ icon. ניתן לקבוע גודל כרצוננו.

בעת נוכל לעשות add לקובץ ה-icon. לאחר ביצוע add ואז resource, בוחרים import ומשנים את סוג הקובץ-icon.



יצירת Installer

לטובת התקנה אוטומטית, נוריד תוכנת Advanced Installer (גרסה 3.15 ומעלה), אשר משתמשת ב- Visual Studio. התוכנה מקבלת את קובץ .hds של visual studio ויוצרת בעצמה את ה-build בתצורה המדרשת. לתוכנה יש wizard נוח. יש לבחור באופציה של ייצור .msi ומשם להמשיך לפי ההוראות.

<https://www.advancedinstaller.com/download.html>

זהו!!!

היעזרו בצ'קליסט כדי להגיש משימה מושלמת

משימה 1 – ex9.docx

- התקנת הנזקקה
- הסרת הנזקקה
- כתיבת הסבר

משימה 2 – ex9-2.c/cpp

- כתיבת נזקה

סיימתם? עבשו רוקדים



נספחים

dagshim-l-tbcnوت נכו

- כדי לקלפל כל מספר שורות קוד ולא לחכות לסוף! הרבה יותר קל לתקן מאשר אין הרבה שגיאות קומפיילציה. בנוסף קל יותר להבין מאיפה השגיאות נובעות.
- כדי לבתוב פונקציה ולבדק אותה לפני שאתם ממשיכים לפונקציה הבאה. למשל, כתבו תכנית ראשית שימושת בפונקציה ובודקת האם היא עבדת נכון. חישבו על מקרים קצה ונסו לראות מה קורה.
- בכל פעם שאתם מתקנים משהו, זכרו שיכל להיות שפגעתם במשהו אחר. לכן עליכם לבדוק שוב מהתחלתה.
- חספו החוצה רק את הממשק המינימלי הדרוש (API minimal), הגדרו את שדות המחלקה כפרטיים, וכמה שפחות מתחזות ציבוריות.