



אתגר 10 כלי דיאגנוסטיקה ברק גובן

מטרה

באתגר תמשו קריאה מקובץ באמצעות WinAPI ולאחר מכן תנתרו את הפעולות שלה
אלה השלבים שתעברו:

הסרת הנוזקה	כתיבת נוזקה
רקע התקנת הנוזקה הסרת הנוזקה	כתיבת נוזקה

ביוט במסמך

תוכן

- 1..... מטרה
- 2..... לינקים שימושיים
- 3..... הסרת הנוזקה
- 4..... כתיבת נוזקה (בונוס)
- 6..... זהו!!!
- 7..... נספחים
- 7..... דגשים לתכנות נכון

נתרגל מיומנויות חשובות

- נבין את מבנה הקריאה לקרנל
- נלמד איך לעבוד עם הדוקומנטציה של Win API.
- נלמד איך לעקוב אחרי תהליכים עם Procmon

לינקים שימושיים

- כדאי לקרוא גם [דגשים לתכנות נכון](#).
- בסוף יש [צ'קליסט שימושי](#) למעקב אחרי ההתקדמות בביצוע המשימה.

בהצלחה יא אלופות ואלופים!



הסרת הנוזקה

כתיבת נוזקה

הסרת הנוזקה
רמת קושי: בינונית

מחקר – הגשה בקובץ ex9.docx

רקע

בתרגיל זה תתקינו נוזקה חינוכית, שפיתחנו במיוחד לצורך התרגיל. הנוזקה טורדנית מעט, אך היא אינה עושה נזק למחשב ולא מדביקה מחשבים אחרים. מטרתכם היא להסיר אותה. מיד תראו שמי שמתקין את הנוזקה זה אתם, ויכול להיות שתחשבו שתשאלו את עצמכם האם זה משקף את המציאות? כלומר, מדוע שמישהו יתקין נוזקה במחשב שלו בעצמו? למעשה זה נפוץ מאד. נוזקות רבות מציגות את עצמן כתוכנות שמבצעות דברים טובים ומשכנעות אותנו להוריד ולהתקין אותן. לאחר שהתקנו אותן צריך להתמודד איתן ולמצוא דרך להסיר אותן.

התקנת הנוזקה

הקליקו על חבילת ההתקנה Naughty Window. יוצר קיצור דרך על ה-desktop שלכם. הפעילו אותו באמצעות לחיצה ימנית ובחרו Run as administrator (חשוב מאד! בלי הרשאה מתאימה ההתקנה לא תעבוד כמו שצריך). זהו סיימתם, כעת נסו להסיר אותה. יש לכבות את windows defender וכל תוכנת אנטי וירוס (תכונות אלה עלולות למנוע ריצה של הוירוס), כמו כן לוודא כי התוכנה כבוי גם לאחר אתחול המחשב.

דגשים:

- השתמשו בכלים שנלמדו בשיעור
- אם אתם חושבים שהסרתם את הנוזקה, הדליקו את המחשב מחדש ובידקו שהנוזקה לא מקפיצה הודעות למסך

מה להגיש?

עליכם לכתוב מדריך להסרת הנוזקה. כלומר, אין צורך להסביר את כל שלבי המחקר שלכם אלא מהי הדרך הקצרה והיעילה ביותר להסיר את הנוזקה. היכן ללחוץ, מה לשנות.

כתיבת נוזקה (בנוס)

כתיבת נוזקה

רמת קושי: בינונית

חסרת הנוזקה

תכנות מחלקה – הגשה בקובץ ex8-2.c/cpp



כיתבו את הנוזקה בעצמכם!

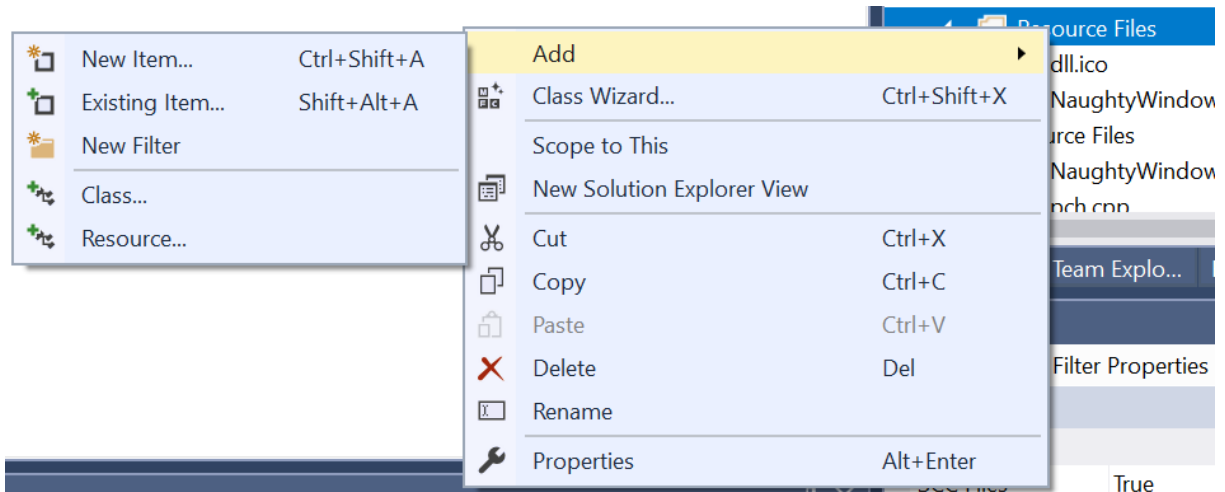
שלבים:

- לימדו אילו פקודות WinAPI כותבות לרגיסטרי ובחרו להיכן ברגיסטרי לכתוב את הערכים הנחוצים לכם
- להלן הסבר על איך מוסיפים אייקון לתוכנה
- להלן הסבר על איך יוצרים חבילת התקנה

הוספת Resource ים

בלי resource ים התוכנה שלנו חסרת icon ופרטים.

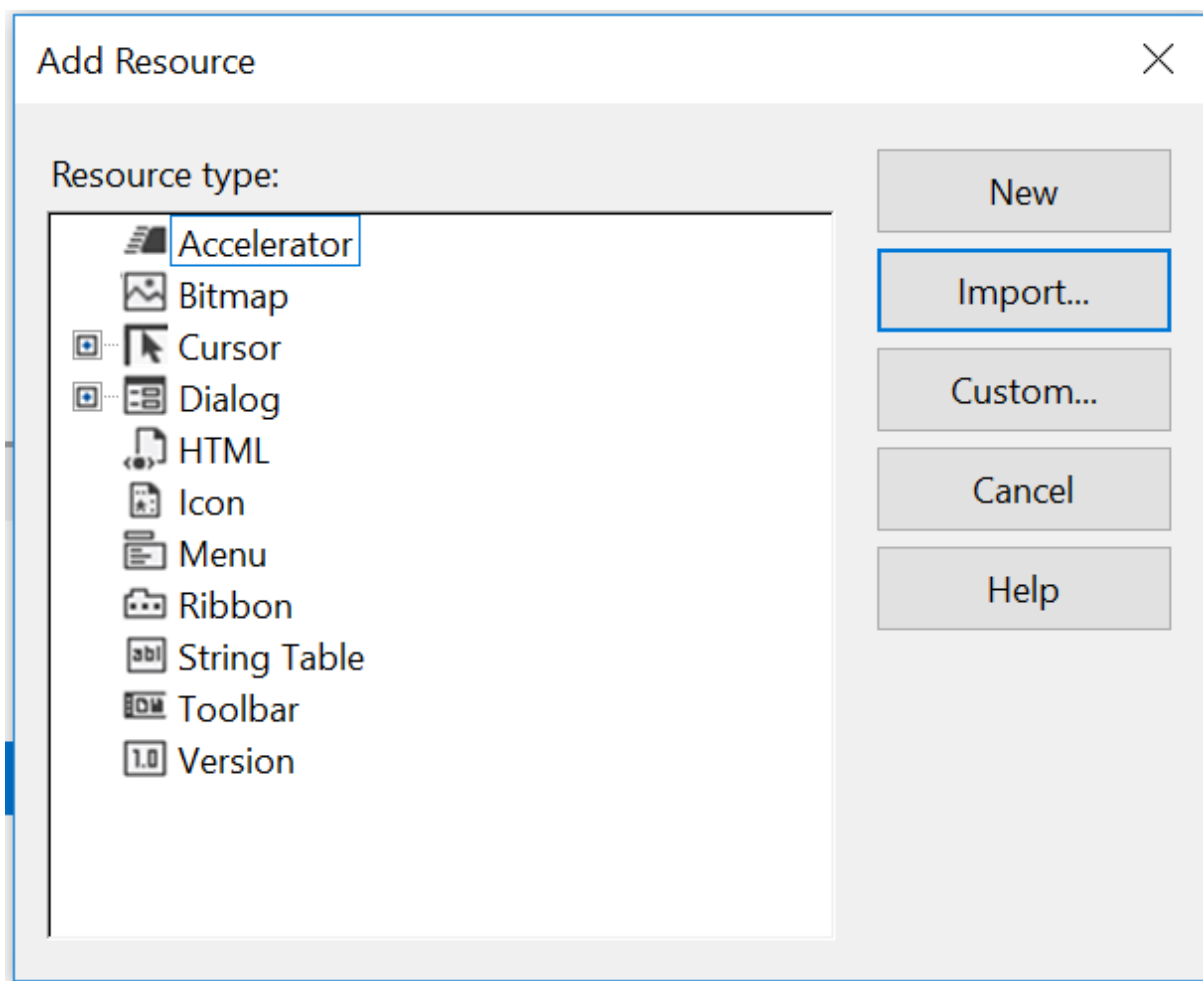
בתוך Solution Explorer נעמוד על Resource Files ונקליק קליק ימני. נבחר Add ואז Resource.



ראשית נבחר קובץ Version, נזין לתוכו את כל השדות כגון יצרן, גרסה.

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

כעת נוכל לעשות add לקובץ ה-ico. לאחר ביצוע add ואז resource, בוחרים import ומשנים את סוג הקובץ ל-ico.



יצירת Installer

לטובת התקנה אוטומטית, נוריד תוכנת Advanced Installer (גרסה 15.3 ומעלה), אשר משתמשת ב- Visual

Studio. התוכנה מקבלת את קובץ ה-sln של visual studio ויוצרת בעצמה את ה-build בתצורה הנדרשת.

לתוכנה יש wizard נוח. יש לבחור באופציה של יצירת msi ומשם להמשיך לפי ההוראות.

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

זהו!!!

היעזרו בצ'קליסט כדי להגיש משימה מושלמת

משימה 1 – ex9.docx

☐ התקנת הנוזקה

☐ הסרת הנוזקה

☐ כתיבת הסבר

משימה 2 – ex9-2.c/cpp

☐ כתיבת נוזקה

סיימתם? עבשיו רוקדים



נספחים

דגשים לתכנות נכון

- כדאי לקמפל כל מספר שורות קוד ולא לחכות לסוף! הרבה יותר קל לתקן כאשר אין הרבה שגיאות קומפילציה. בנוסף קל יותר להבין מאיפה השגיאות נובעות.
- כדאי לכתוב פונקציה ולבדוק אותה לפני שאתם ממשיכים לפונקציה הבאה. כלומר, כתבו תכנית ראשית שמשתמשת בפונקציה ובודקת האם היא עובדת כראוי. חישבו על מקרי קצה ונסו לראות מה קורה.
- בכל פעם שאתם מתקנים משהו, זכרו שיכול להיות שפגעתם במשהו אחר. לכן עליכם לבדוק שוב מהתחלה.
- חשפו החוצה רק את הממשק המינימלי הדרוש (minimal API), הגדירו את שדות המחלקה כפרטיים, וכמה שפחות מתודות כציבוריות.