CyberGirlz CLUB

I’ve got the power – חלק ב

ברק גונן

START-UP NATION CENTRAL

קרן רש"י RASHI FOUNDATION

המרכז לחינוך סייבר CYBER EDUCATION CENTER

לאחר שהצלחנו להתגבר על נוזקת השלג,
ההאקרים הגבירו את מאמציהם לפגוע בנו

הנוזקה הבאה שתפגע בנו נראית כמו קובץ אקסל תמים.
אתן חייבות להבין מה הנוזקה מבצעת לפני שהיא תופץ!
השגתי לכן את קובץ האקסל-

https://data.cyber.org.il/CyberGirlzClub/VeryBadFileLOL.xlsm

תרגיל

צרו קובץ אקסל שכאשר פותחים אותו נפתחת אוטומטית תוכנת Notepad

העזרו במדריך "קוד מקרו – השער לנוזקות"

https://data.cyber.org.il/CyberGirlzClub/macro.pdf

תרגיל

מיצאו את קוד המקרו החבוי בנוזקה הלימודית.

נסו לחקור אותו בעצמכן:

- האם יש מחרוזות שאפשר לזהות ולהבין?
- האם יש פקודות שאפשר לזהות?
- מה הקוד עושה?

תרגיל חלקים 1+2 – מבוא ל-Powershell

פיתחו Powershell, שנו את התיקיה בה אתם נמצאים ל- c:\users

https://data.cyber.org.il/CyberGirlzClub/powershell.pdf

תרגיל חלק 3 - Cmdlets

מיצאו Alias של פקודת שמציגה את ההיסטוריה של כל הפקודות שכתבתם ב-Powershell

תרגיל חלק 4 – הרצת תוכנות

היכנסו לתיקיית chrome והריצו את chrome מבלי להכנס לתיקיית Application

תרגיל חלקים 5 + 6- סקריפטים

כיתבו סקריפט שקולט את שם המשתמש ומדפיס הודעה עם המילה Hello ולאחר מכן שם המשתמש

תרגיל חלק 7- Help

צרו קובץ טקסט חדש, בכל דרך שתרצו. קיראו לו help.txt. פיתחו אותו באמצעות Powershell, קיראו את המידע שבקובץ לתוך משתנה והדפיסו את התוכן שלו למסך

תרגיל חלק 8- פרמטרים ל-Cmdlets

מוקדם יותר, כאשר רצינו להריץ את chrome מתוך Powershell, היינו צריכים למצוא בעצמנו את הנתיב שבו נמצא chrome.exe. כעת עשו זאת באמצעות Powershell.

טיפ: התחילו מ – Get-ChildItem

תרגיל חלק 9 + 10 – providers, registry

באמצעות Powershell, צרו רשומה ברגיסטרי והסירו אותה

תרגיל חלק 12 - תנאים

כיתבו סקריפט שקולט ערך מהמשתמש. אם הערך גדול מ-5, הדפיסו "too high". אם הערך קטן מ-5 הדפיסו "too low", אחרת הדפיסו "high five!"

תרגיל חלק 13 + 14 – pipes, objects

קיים אובייקט שנקרא service. לימדו עליו באמצעות help. הדפיסו למסך את כל ה-services שנמצאים בסטטוס Running.

תרגיל חלק 15 – Invoke Execute

הריצו את chrome.exe באמצעות פקודת IEX

הערה: הנתיב שבו אתם נמצאים צריך להיות שונה מהתיקיה שבה נמצא chrome

כל הכבוד! המשיכו ופענחו את הנוזקה