# **Remote Administration Tool**

## מגישים: נועה קרמס 208200428 וזאב בר שוכמן 207024001

* **מה הכלי שלנו עושה?**  
    
  בנינו RAT שבעצם הוא מתפקד כshell למחשב כך שלתוקף אחרי התקנת הRAT שליטה מלאה במחשב.

הכלי מומר מקוד לקובץ executable בעזרת PyInstaller ומסתווה בתור קליינט של firefox .  
  
המטרה שלנו הייתה לעשות כלי שיכול לחדור לפרטים הכי אישיים של מישהו אחר בצורה מסוות. אנחנו חושבים שהכלי שבנינו אכן עונה על המטרה שכן דרך הshell יש לנו גישה מלאה לכל הפונקציונליות של המכונה, כמו שיש למשתמש עצמו (הרי המשתמש בעיקר מתקשר עם המחשב דרך GUI של CMD, ולנו גישה ישירה לCMD) ובפרט, אנו יכולים לגשת לכל התיקיות של מחשב אחר ולראות את כל הקבצים הלוקלים שלו.

כמו כן, הצלחנו להסוות את הכלי על ידי התקנה של firefox כך שהקורבן יחשוב שהוא בסך הכל מתקין תוכנתfirefox תמימה שכן זאת תוכנה מאוד נפוצה, אך בעצם כאן אנחנו ניכנס לתמונה, הshell יופעל, ונוכל לדלות מהמחשב הלוקלי של הקורבן איזה מידע שנרצה.

יצרנו קובץ המחלץ את עצמו, הנראה כמו התקנה של firefox, בהרצה של קובץ זה תופעל התקנת הfirefox המקורית, ולאחר סיום תהליך ההתקנה (בין אם בוטל או בין אם לא) יורץ צד הקליינט המאפשר לתוקף לקבל שליטה.

* **בעיות שנתקלנו בהן במהלך העבודה:**  
    
  תחילה, לא ידענו איזה כלי לעשות שיענה לנו לגמרי על הצרכים. הבעיה הייתה שמצד אחד רצינו לעשות כלי שיוכל לדלות כמה שיותר מידע מהקורבן, אך מצד שני שהכלי יהיה מסווה כך שהקורבן לא יחשוב שמדובר בתרמית. את הבעיה הזאת פתרנו על ידי ההסוואה של תוכנה הfirefox.

לאחר מכן, היינו צריכים להבין כיצד בונים shell ומצליחים להתחבר מרחוק למחשב זר, עשינו מחקר באינטרנט ולמען האמת גילינו שיש הרבה מידע בנושא.

לבסוף כמובן האיחוד בין ההתקנה האמיתית של Firefox לבין הקליינט שלנו, ואת זאת פתרנו באמצעות SFX המחלץ ומריץ תחילה את ההתקנה המקורית ולאחר מכן את הקליינט הזדוני.

* **חוזקות של הכלי:**
  + לדעתנו, החוזקה העיקרית של הכלי היא צורת ההסוואה שלו. הסוואה באמצעות תוכנת firefox שכן היא תוכנה מאוד פופולרית, מנגישה את הכלי לקהל הרחב ומאפשרת לנו בתור "פורצים" לפרוץ להמון מחשבים.
  + מעבר לכך, השליטה המוחלטת שהכלי מסב לתקוף במידה והתקיפה מוצלחת, שכן ניתן למחוק מכונה כולה בעזרת פקודה בודדת אם כך התוקף ירצה.
  + פוטנציאל הכלי: בחרנו להטמיע אותו ב%temp% אך באותה מידה ניתן לחלץ ב

%userprofile%\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup

ובכך הקובץ יריץ את עצמו ויאפשר התחברות בכל הפעלה של המכונה.

ובנוסף ניתן להצמיד סקיפט shell לקובץ הSFX.

* **חולשות של הכלי:**
  + לעיתים מתגלה על ידי אנטי-וירוס, אך רק בזמן הרצה.
  + הפצת הכלי, שכן התקנה של הדפדפן הנ"ל זמינה ברשת.

* **תיאור עבודת הכלי:**לאחר שהמשתמש הוריד את ה'התקנה' של הדפדפן (בין אם חיפש עצמאית באינטרנט או שמא קיבל קישור),

באמצעות SFX תופעל קודם כל ההתקנה האוטנטית של firefox ובין אם ההתקנה צלחה או לא, יופעל הקליינט שלנו (שנראה כמו קליינט של firefox, שהרגע התקנו) ויאפשר לנו גישה.

פונקציונליות של הקבצים המצורפים:

* + client.py – קוד הקליינט, היוצר חיבור לשרת מוגדר מראש, ומחכה לקבל פקודות. בקבלת פקודה הקליינט מעביר את הפלט ישירות לשרת, את יעד החיבור יש להגדיר מראש.
  + server.py – קוד השרת, מחכה לחיבור מכל קליינט לport מוגדר מראש, אחרי חיבור מוצלח מאפשר שליחת פקודות וממתין למענה מלקוח.
  + Firefox Installer.exe – קובץ executable אשר בהפעלתו:
    - מחולצים 2 קבצים לתיקיית %temp% של המשתמש, firefoxinstaller.exe + client.exe.
    - רצה התקנת הfirefox (firefoxinstaller.exe)
    - לאחר תום תהליך ההתקנה הנ"ל, רץ הקליינט שלנו (client.exe)
    - הקליינט רץ windowless ומעבר לתהליך client.exe במנהל המשימות של המחשב אין לו זכר (וגם שם, נראה כמו קליינט של firefox רק עם השם client, כמובן שניתן לשנות לו את השם(
* **תיעוד הקוד:**  
    
  כפי שכבר צוין, הקוד מורכב מצד שרת וצד לקוח. תיעוד קוד נוסף ניתן למצוא בקוד עצמו

בנוסף, קוד סקריפט הSFX:

Path=%temp%

SavePath

Setup=%temp%\client.exe

Presetup=%temp%\FireFoxInstaller.exe

Silent=1

Overwrite=1

Title=test

המוגדר בקובץ ההתקנה הזדוני.

* **לסיכום:**  
    
  בתחילת הקורס לא ידענו איך להתחיל את הפרויקט ולמען האמת לא הכרנו את העולם של אבטחת רשתות כלל. גילינו שזה תחום רחב מאוד וקיים מידע רב בתחום באינטרנט. אנחנו חושבים שמעבר לכך שהנושא מאוד מעניין הוא גם חשוב ביותר ושמחים שהעמקנו את הידע שלנו בנושא.

למרות חוסר הידע והניסיון שלנו בתחום, הרגיש לנו שהכלי היעיל ביותר יהיה הכלי החזק ביותר, ולכן פנינו דווקא לRAT

עם הלמידה הבנו שהכלי עצמו יכול להיות פשוט למדי לבנייה אך הקושי האמיתי טמון בהעברת הRAT לקורבן והטמעתו מערכת הקורבן בצורה החשאית ביותר שמגבלת היכולות שלנו.