תיעוד עבודה – פרוייקט באבטחת רשתות

מתן אלקיים 208013698 אריאל ג'ייסון 318167855

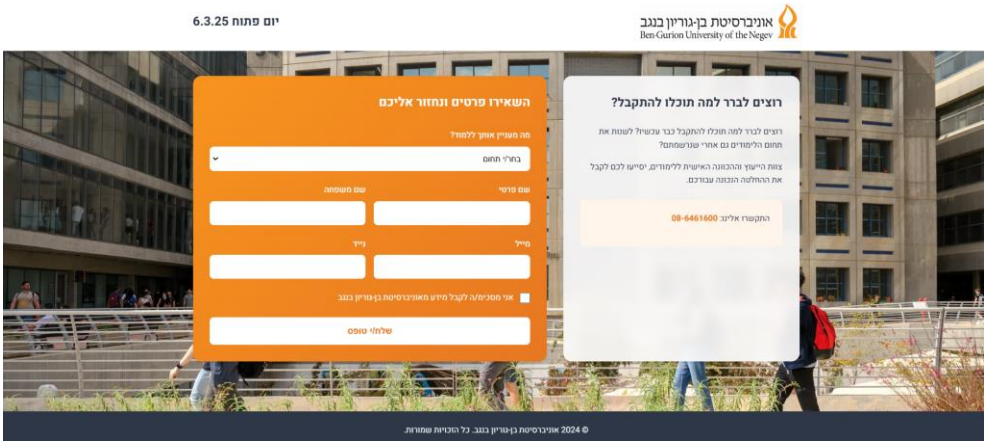
1. תאור הפרוייקט

הפרוייקט משתמש בהנדסה חברתית לצורך הפניית מועמדים ללימודים באוניברסיטת בן גוריון לאתר המדמה את ההרשמה ליום הפתוח לצורך גניבת פרטי זהות של מועמדים ללמוד באוניברסיטת בן גוריון ולאחר מכן השתלת נוזקה בעזרת ההזמנה ליום הפתוח.

הפרוייקט מורכב מ:

a. אתר בסיסי המכיל טופס הרשמה ליום הפתוח
b. דף נחיתה ל"הצלחת ההרשמה" + הורדת הקובץ הנגוע
c. קובץ נגוע אשר במקביל פותח סרטון תדמי וברקע מוציא הודעה על כך שבוצעה תקיפת סייבר ואזהרה עתידית ומייצר קובץ חדש שולחן העבודה עם דגשי בטיחות.
d. מסד נתונים השומר את פרטי המועמדים לצורך שימוש במידע הגנוב.

טופס ההרשמה שלנו (זמין כרגע ברשת על בסיס GITHUB ללא החיבור למסד הנתונים אלא רק הפרונט - https://ariel-j.github.io/fishing-project/):



לשם השוואה – **האתר המקורי של בן גוריון**

צילום של מסד הנתונים הנוכחי

1	engineering	NULL	NULL	arieljayson1@gmail.com	0523780310		1
2	computer-science	לאירא	ווסיי'ג	arieljayson1@gmail.com	0523780310		1
3	computer-science	Ariel	Jayson	arieljayson1@gmail.com	0523780310		1
4	computer-science	aaa	bbb	aaa@vvv.bbb	3333		1
5	computer-science	ben	ben	ben@ben.com	12345		1
6	computer-science	ben	ben	bem@ben.v	1234		1
7	computer-science	Ariel	Jayson	arieljayson1@gmail.com	0523780310		1
8	engineering	לאירא	ווסיי'ג	arieljayson1@gmail.com	0523780310		0
9	computer-science	לאירא	ווסיי'ג	arieljayson1@gmail.com	0523780310		0
10	computer-science	matan	eli	matan@shiti.BGU.AC	5555555		1
11	engineering	Ariel	Jayson	arieljayson1@gmail.com	0523780310		0
12	computer-science	לאירא	ווסיי'ג	arieljayson1@gmail.com	0523780310		1
13	engineering	עכגד	דדגנכנכ	ssss@sss.xxx	66666666666666666666666666666		1
14	engineering	עכגד	דדגנכנכ	ssss@sss.xxx	66666666666666666666666666666		1
15	computer-science	Ariel	Jayson	arieljayson1@gmail.com	0523780310		1
16	computer-science	Ariel	Jayson	arieljayson1@gmail.com	0523780310		1
17	computer-science	ירא	ואירדא	zxc@aas.c	6666		1
18	engineering	השמ	הדש	asd@gmal.com	0542365895		1
19	computer-science	ותנוהי	יירג	aaa@gmail.com	0523780310		1

2. אופן הפעלת הכלי

הרעיון היה להפיץ את הקישור לאתר ברשתות החברתיות בדגש על קבוצות של סטודנטים ומועמדים לקבלה סביב תחילת תהליך ההרשמה לאוניברסיטאות בינואר. לאחר מכן, המועמדים ילחצו על הקישור שנפיץ בשם "אוניברסיטת בן גוריון" וייכנסו לאתר הפיקטיבי. שם, הם יכניסו את הפרטים לטופס ההרשמה שעביר אותם שיירות אלינו לצורך גניבת הפרטים, ולאחר מכן אוטומטית יירד אליהם הקובץ הזדוני. הקובץ במסווה של ההזמנה ליום הפתוח יכיל את הקוד הזדוני. לאחר הפעלת המאקרו, ייפתח אוטומטית סרטון התדמית של בן גוריון ובמקביל תצא הודעת מערכת על כך שבוצעה כאן פעולת סייבר, ויווצר קובץ חדש עם טיפים לביטחון מידע בשולחן העבודה.

סה"כ: הנדסה חברתית, שימוש בפישיניג לגניבת הזהות, הורדת קובץ זדוני אוטומטית והפעלת הקוד.

3. תאור ביצוע הפרוייקט

התחלנו מהסתכלות על האתר הרישמי של בן גוריון ואפיון האלמנטים הנדרשים באתר הרשמה פיקטיבי. לאחר מכן, העתקנו את העיצוב ובנינו בעזרת HTML וCSS אתר דומה במכיל רקאת טופס ההרשמה.

אחרי כתיבת האתר הבסיסית, הרמנו שרת פשוט בעזרת node.js ובחרנו לנהל את מסד הנתונים שלנו בעזרת mysql, והתחלנו לחבר את שלושת החלקים ביחד. במקביל התחלנו לבצע ניסויים בקבצים שונים על מנת ללמוד ולאבחן מהי הדרך הטבוה ביותר להטמיע קוד זדוני.

לאחר מספר רב של כשלונות וחסימות ע"י הדפדפן, אנטיוירוס המקומי או ווינדוס החלטנו להטמיע פקודת מאקרו בPDF או בקובץ וורד שתבצע עבורנו את הפעולה הקשה. כאן נאלצנו לחשוב כיצד ייראה הקובץ שיעטוף אותה בצורה שלא תעורר חשד. לאחר ההחלטה להטמיע אותו בהזמנה רשמית פיקטיבית שיצרנו בשביל היום הפתוח, החלטנו להוסיף את סרטון התדמית של האוניברסיטה שייפתח עם הפעלת הפקודה בשביל להקטין את החשד לאחר הפעלת המאקרו.

לבסוף, איחדנו הכל, הוספנו דף נחיתה רישמי לאחר ה"הרשמה" ליום הפתוח וביצענו ניסויים ותיקונים בהתאם לראות שהכל עובד.

סה״כ צברנו ניסיון ראשוני במעקף בסיסי של אנטיוירוס וכרום, התמודדות עם פקודות מאקרו, סייבר בסיסי, הנדסה חברתית וגניבת נתונים.

4. אתגרים ופתרונות

a. הטמעת הקוד הזדוני

בשל ההתקדמות הטכנולוגית ומודעות הסייבר הגבוהה כיום, קבצים רבים חוסמים את היכולת להטמיע בתוכם קוד זדוני חיצוני, בכלל זה מוצרי ווינדוס, מייקרוספט וגוגל פועלים רבות לזיהוי וחסימה אוטומטית של קבצים העלולים להזיק למשתמש או למחשב. בשל כך, ביצענו ניסויים רבים עד לבחירת הקובץ ותצורת הקוד (מאקרו) בה השתמשנו לצורך הזרקת הקוד הזדוני שגם תעבור את המכשולים. לאחר מספר רב של כשלונות החלטנו לנסות להשתמש בכלים של מייקרוספט לצורך כך, ולכן השתמשנו ביכולת המובנת של קבצי וורד להחזיק ולהפעיל פקודות מאקרו אשר יכולות לתת שליטה רבה לתוקף אפשרי.

b. חסימת הקובץ ע״י כרום

לאחר סיום יצירת הקובץ ובדיקה שהוא פועל בצורה הנכונה נתקענו באתגר נוסף. כרום חסם את הקובץ מאחר והוא זיהה שמדובר בקובץ אשר מחביא בתוכו מאקרו חבוי. ניסנו מספר תצורות להסוואת הקובץ או שינוי היעד אך לא הצלחנו לעקוף זאת. לבסוף, הצלחנו ע״י שינוי סוג הקובץ מבחינת כרום בזמן ההורדה לגרום לו להוריד את הקובץ, ולאחר מכן בפתיחה עצמה, מאחר ומדובר בקובץ וורד, ווינדוס מזהה זו בצורה אוטומטית וממיר אותו מחדש לוורד ופותח אותו ואת המאקרו בצורה ישירה.

c. הורדה אוטומטית שלא תחסם

בהתחלה נתקענו בקשיים בהורדה האוטומטית ללא אישור המשתמש. גם כאן, כרום הערים קשיים רבים. בשל כך בחנו להצמיד את ההורדה ללחיצה על כפתור, כך המשתמש מבצע את ההורדה בעצמו כביכול ולא אוטומטית.

d. הנדסה חברתית לאתר ולקובץ

נתקענו בקושי זה מספר פעמים. ראשית בתחילת הדרך נאלצנו לחשוב על דרך יצירתית אבל אמינה להפניית המשתמשים לאתר הפיקטיבי שלנו. מתוך שיטוט ברשתות החברתיות ולאחר בחינת הפרסומים החצי רישמיים של האוניברסיטה בקבוצות של סטודנטים עלה הרעיון להסוות את עצמנו כך.

לאחר מכן, ביצענו מספר שינויים עיצוביים לאתר עד שקבוצת משתמשים בלתי תלויה לא יכלה לחזות שמודבר באתר לא רישמי (נעזרנו בחברנו שלא ידעו שעוזרים לנו בפרוייקט בשביל לבדוק אמינות לאתר).

בהמשך, נאלצנו למצוא דרך להתמים את הקוד הזדוני. בשביל כך ולאחר בחינה של מספר פתרונות יצרנו הזמנה פיקטיבית ליום הפתוח על בסיס תמונות מהאתר של האוניברסיטה, ועיצבנו ביחד לשם האמינות.

לבסוף, אנו צריכים שהמשתמש יאשר להפעיל את פקודת המאקרו (היכן שזה לא פועל לבד, תלוי הגדרות משתמש). לכן, הוספנו את סרטון התדמית כך שכאשר המשתמש יפעיל את המאקרו הוא יקבל תחילה את הסרטון הרישמי ולא יחשוד כי מודבר בווירוס. כמו כן, בשאיפה אם מספר סטודנטים יסתכלו יחד על הקובץ או ישלחו את ההזמנה אחד לשני הם יאשרו אחד לשני כי הקובץ לגיטימי.

5. **שינויים מהתוכנית**

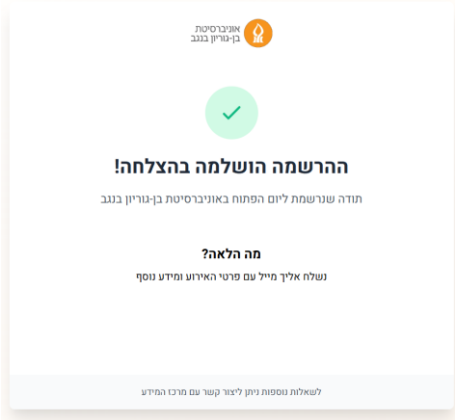
בוצעו שני שינויים מהותיים מהתוכנית המקורית:

1. הראשון היה שינוי **סוג הקובץ** שיורד מPDF ל WORD בשל קשיי אבטחה מורכבים מידי במציגי הPDF הסטנדרטיים.

2. **באופן קבלת הקובץ הנגוע**. תכננו לשלוח אותו במייל אבל מאחר והוא נחסם בכל תצורה שבה בדקנו החלטנו לגרום למשתמש להוריד אותו בעת ההרשמה עצמה ליום הפתוח.

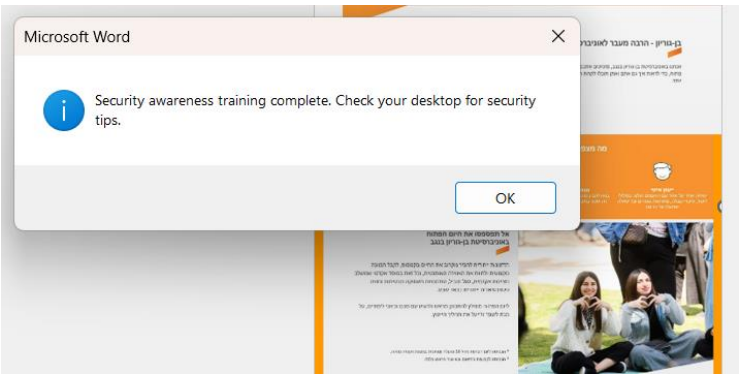
נספח – צילומי מסך של חלקי הפרוייקט (מה שלא הופיע עד כה)

דף הנחיתה



הקובץ הנגוע

הודעת האזהרה



קובץ ההנחיות שיצרנו בשולחן העבודה


```
CYBERSECURITY TRAINING EXERCISE
--------------------------------
In a real attack, a malicious macro could have:
1. Accessed your files
2. Installed unwanted software
3. Compromised your system

Security tips to stay safe:
- Never enable macros in documents from unknown sources
- Be cautious of unexpected attachments
- Verify sender identities carefully
```