שמונה סוגי מתקפות ושיטות שבאמצעותם ינסו להפיל אתכם ברשת

מתקפת סייבר מסוג פישינג (דיוג) עלולה להביא לנזקים כלכליים ותפעוליים שונים לארגון או למשתמש הפרטי, בהם: הורדת תוכנה מזיקה למכשיר, גניבת כסף, גניבת מידע שעלול להביא למתקפה רחבה יותר, נעילת חשבונות ברשת החברתית, חבלה בעיסקה או בפעילות של הארגון ועוד. בשנים האחרונות השימוש בסוג מתקפה זו נמצא בעלייה לאור הרווח הכלכלי והפוטנציאל לעקוף באמצעותה הגנות של ארגונים. היכרות של השיטות שבהם משתמשים ההאקרים, יכול לעזור להתגונן ולחזק עירנות וחשדנות.

הסוג הראשון של מתקפות פישינג, הנפוץ והמוכר ביותר, הוא **קישור המגיע בהודעה באמצעות מסרון או כל אפליקציה אחרת להעברת מסרים**, או באמצעות הדוא"ל. לעיתים עצם הלחיצה על הקישור תאפשר להאקר גישה למכשיר, ולעיתים הקישור מוביל לאתר אינטרנט מתחזה בו בקשה להזין פרטים אישיים שמגיעים לידי ההאקר.

בסוג השני, **המתקפות ממוקדות לאדם או לקבוצה מסוימת שלהאקר יש עניין להגיע אליה באופן ספציפי.** ההאקר אוסף מידע מקדים לרוב ממקורות גלויים, על האדם או הקבוצה הספציפית ומנסח הודעה שפונה ישירות לתחומי העניין או העיסוק שלהם, כדי להפוך את הפניה למשכנעת במיוחד. כך לדוגמה, האקר שמצא שהאדם שהוא מכוון אליו חובב יין מגלישה בפרופיל שלו ברשת החברתית, ינסה לדוג אותו באמצעות הודעה על מבצע מסוים בתחום היין.

באותו אופן, לעיתים המתקפה הממוקדת תכוון ישירות על ההנהלה הבכירה במטרה לגנוב כסף, מידע רגיש או לקבל גישה לרשת ולמערכות הארגון. בתקיפה מסוג זה מנסים ההאקרים גם להפעיל לחץ על עובדים שעלולים לחשוש לסרב לבקשת מההנהלה.

בסוג המתקפה השלישי, **נסיון הדיוג מתבצע באמצעות התחזות בטלפון לגורם לגיטימי.** לדוגמה בטענה שמתקשרים מהבנק, מהתמיכה הטכנית של הארגון, משירות לקוחות מוכר וכו'. המתחזה מנסה לרכוש את האמון, ופעמים רבות אכן נשמע משכנע מאוד, ולבקש לבצע פעולות כגון מסירת פרטי התחברות, מסירת פרטי אשראי או סיסמה לשירות מסוים ואף להתחברות לארגון שלכם.
זאת ועוד, לעיתים הפונה בטלפון הוא גורם שקיים קשר עימו וקולו נשמע מוכר.

בסוג המתקפה הרביעי, האקר משיג הקלטות קוליות של דמות בכירה בארגון ומתחזה אליה באמצעות שימוש בתוכנה ייעודית להתחזות קולית. ההאקר מתקשר אל אחד העובדים בתור אותה דמות בכירה ומבקש לבצע פעולות שונות כגון העברת כספים או פתיחת קובץ זדוני ברשת הארגונית.

בסוג המתקפה החמישי, מנסים לדוג פרטים באמצעות מודעות ופרסומות קופצות. לרוב בגלישה באתרים פחות מוכרים או ברשתות החברתיות. סוג המודעה לרוב תהיה מפתה: "לחצו על מנת להשתתף בהגרלה ואולי תוכלו לזכות בפרס". לחיצה על מודעות מתחזה, יכולה להוביל להורדה של קובץ זדוני למכשיר, להחדיר וירוס ולהסב נזק למכשירכם. לעיתים לחיצה על המודעה, מובילה לאתר מתחזה אשר ובו בקשה להזנת פרטים אישיים שיועברו מידית לידי ההאקר.

בסוג המתקפה השישי, תוקפים מתחזים לדמויות שונות ברשתות החברתיות ומבקשים מידע אישי תחת אשליה שמדובר בגורם לגיטימי.

בסוג המתקפה השביעי, מופיעה באתר מודעה או אפשרות להורדת אפליקציה חינמית המציעה שירות או יישום שימושי כלשהו. לרוב, כשלא מדובר בחנות רשמית, אפליקציות אלו נחשבות לא בטוחות ואף זדוניות. קיים סיכון גדול שבהורדת האפליקציה מושגת גישה למכשיר שלכם שמאפשרת להאקר שליטה במכשיר וגישה לפרטים האישיים למידע השמור בו.

בסוג המתקפה השמיני והאחרון, האקרים יוצרים אתרים מתחזים ומאנדקסים אותם באופן לגיטימי במנועי החיפוש במטרה להגדיל את רמת החשיפה שלהם. אתרים אלה יכולים להיות אתרים מתחזים הדומים בנראות האתר והדומיין למקור, או אתרים עצמאיים שיציעו מוצרים ודילים במחיר משתלם במיוחד ולא יעוררו חשד במנועי החיפוש. גם כאן, בכניסה לאתר תיתכן בקשה למסירת פרטים או להורדת קובץ מזיק.

אז איך מתגוננים?

1. **לגלות ערנות ולנהוג בחשדנות** - עכשיו שהסכנות והסיכונים מוכרים, חשוב להיות עירניים ולהכיר את דרכי הפעולה והאפשרויות להתחזות.
2. **בדיקת זהות הפונה בשיחה יזומה אליו** - במידה שביקשו מכם להעביר כספים או פרטים אישיים אחרים בהודעת דוא"ל, מסרון או אף בטלפון, מומלץ תמיד לוודא מי הגורם, לפנות אליו בדרך אחרת ואף לבצע אליו שיחה יזומה בעצמכם.

3. **לא מוסרים מידע** - קיבלתם הודעה מוזרה, או הודעה שנראית לגיטימית ואף שיחת טלפון מהבנק בה הודיעו לכם על ביצוע עסקה חריגה, אשר לשם ביטולה אתם נדרשים לתת קוד אימות או את פרטי כרטיס האשראי שלכם- עצרו! היו ערניים לבקשות חריגות בשיחות שלא יזמתם. באותו אופן לא מוסרים קוד אישי, סיסמה, מספר מזהה אחר וכו'.
4. **היו קנאים לפרטיותכם** - צמצמו למינימום את המידע האישי שאתם חושפים ברשתות החברתיות ו/או הגבילו את המידע הציבורי שמי שאינו בקבוצת החברים יכול לראות, באמצעות הגדרות הפרטיות של הרשת החברתית.
5. **חשדו בהצעות חברות של פרופילים לא מוכרים** - בחנו אותם היטב ובדקו שהם אמינים. בפרופילים מתחזים ו/או מזויפים תהיה בדרך כלל רשימת חברים מועטה, מעט תמונות וציר הזמן יראה ריק וללא פעילות רבה.
6. **הורדת אפליקציות מהחנויות הרשמיות** - מומלץ להוריד אפליקציות רק באמצעות החנויות הרשמיות (App Store, Google Play) ולא דרך אתר, אפליקציות חינמיות או קישור ישיר לדף הורדות.