איתור והפסקת התקפות הודעות

מהן התקפות מסרים?

סמישינג (מילה פורטמנטלית המשלבת סמס ודיוג) הן התקפות המתרחשות כאשר תוקפי סייבר משתמשים בטכנולוגיות סמס, הודעות טקסט או דומות להעברת הודעות כדי להערים עליך לבצע פעולה שאסור לך לבצע. אולי הם מטעים אותך לספק את פרטי כרטיס האשראי שלך, לגרום לך להתקשר למספר טלפון כדי לקבל את פרטי הבנק שלך, או לשכנע אותך למלא סקר מקוון כדי לאסוף את המידע האישי שלך. בדיוק כמו בהתקפות דיוג בדוא"ל, פושעי סייבר משחקים לרוב ברגשות שלך כדי לגרום לך לפעול על ידי יצירת תחושת דחיפות או סקרנות, למשל. עם זאת, מה שהופך את התקפות הודעות למסוכנות כל כך הוא שיש הרבה פחות מידע ופחות רמזים בטקסט מאשר במייל, מה שמקשה עליך הרבה יותר לזהות שמשהו לא בסדר.

הונאה נפוצה היא הודעה שאומרת לך שזכית באייפון, ואתה רק צריך ללחוץ על קישור ולמלא סקר כדי לקבל אותו. במציאות, אין טלפון והסקר נועד לאסוף את המידע האישי שלך. דוגמה נוספת תהיה הודעה המציינת שלא ניתן היה לשלוח חבילה עם קישור לאתר שבו אתה מתבקש לספק מידע הדרוש להשלמת המשלוח, כולל פרטי כרטיס האשראי שלך לכיסוי "דמי שירות". במקרים מסוימים, אתרים אלו עשויים אפילו לבקש ממך להתקין אפליקציה לא מורשית לנייד שמדביקה ומשתלטת על המכשיר שלך.

לפעמים פושעי סייבר אפילו ישלבו התקפות טלפון והודעות. לדוגמה, ייתכן שתקבל הודעת טקסט דחופה מהבנק שלך ושואלת אם אישרת תשלום מוזר. ההודעה מבקשת ממך להשיב כן או לא כדי לאשר את התשלום. אם תגיב, פושע הסייבר יודע בעת שאתה מוכן לעסוק ויתקשר אליך בהתחזות למחלקת ההונאה של הבנק. לאחר מכן הם ינסו לשדל ממך את פרטי כרטיס האשראי והפיננסי שלך, או אפילו את פרטי הכניסה והסיסמה של חשבון הבנק שלך.

איתור ועצירת התקפות הודעות

הנה כמה שאלות שכדאי לשאול את עצמך כדי לזהות את הרמזים הנפוצים ביותר להתקפת הודעות:

- תחושת דחיפות אדירה, כשמישהו מנסה להאיץ אותך לנקוט לפעולה?
- האם ההודעה מובילה אותך לאתרים שמבקשים את המידע האישי שלך, כרטיס האשראי, הסיסמאות או מידע רגיש אחר שלא אמורה להיות להם גישה אליהם?
- .האם ההודעה נשמעת טוב מכדי להיות אמיתית ?לא ,לא באמת זכית באייפון חדש בחינם
- האם האתר או השירות המקושרים מאלצים אותך לשלם בשיטות לא סטנדרטיות כגון ביטקוין, כרטיסי מתנה או העברות ווסטרן יוניון?

- האם ההודעה מבקשת ממך את קוד האימות הרב-גורמי שנשלח לטלפון שלך או שנוצר על ידי אפליקציית הבנקאות שלך?
- האם ההודעה נראית כמו מקבילה ל"מספר שגוי?" אם כן, אל תגיב אליו ואל תנסה ליצור קשר עם השולח; פשוט למחוק את זה

אם אתה מקבל הודעה מארגון רשמי המבהיל אותך, בדוק איתם ישירות. אל תשתמש במספר הטלפון הכלול בהודעה, במקום זאת, השתמש במספר טלפון מהימן. לדוגמה, אם אתה מקבל הודעת טקסט מהבנק שלך ואומרת שיש בעיה בחשבון הבנק או בכרטיס האשראי שלך, צור קשר ישירות עם הבנק או חברת האשראי שלך על ידי ביקור באתר האינטרנט שלהם או התקשר אליהם ישירות באמצעות מספר הטלפון מגב הכרטיס שלך כרטיס בנק או כרטיס אשראי. זכור גם שרוב הרשויות הממשלתיות, כגון רשויות מס או אכיפת חוק, לעולם לא יפנו אליך באמצעות הודעת טקסט, הן יפנו אליך רק בדואר מיושן.

כשמדובר בהתקפות העברת הודעות, אתה ההגנה הטוב ביותר שלך.

עורך אורח

ג'ף לומס הוא בלש בקבוצת החקירות הסייבר של משטרת המטרופולין של לאס וגאס ומלמד את הקורס SANS SEC487 איסוף וניתוח מודיעין בקוד פתוח (OSINT). ג'ף חוקר פשעים פיננסיים בהייטק, כולל השתלטות על דוא"ל עסקי, סחיטה, תוכנות כופר ומקרי גניבה מורכבים של מטבעות קריפטוגרפיים והלבנת הון.

משאבים

לעצור את הדייג: https://www.sans.org/sites/default/files/2018-04/201804-OUCH-April-Hebrew.pdf

הנדסה חברתית: https://www.sans.org/security-awareness-training/ouch-newsletter/2017/social-engineering

וישינג - התקפות שיחות טלפון והונאות: https://www.sans.org/newsletters/ouch/existing

תורגם לקהילה על ידי: גדי מרגלית ודרור ענבר